POSEBNA ŠTEVILKA

Monitor

ISSN 1318-1017

ZABAVNA ELEKTRONIKA | RAČUNALNIŠTVO | NOVE TEHNOLOGIJE

POLETJE 2019 ◌ LETNIK 29 ◌ WWW.MONITOR.SI

CENA: 4,90 EUR

HEKANJE

IN DRUGI TRIKI ZA VSAKDANJO RABO

- **hekerji**
- **odklepanje** storitev
- domače **izboljšave**
- **varnost** doma
- varnost **v podjetjih**

VARNOST DOMA

- kako ubraniti domače računalnike
- izboljšajmo svoj wifi
- temna stran Androida

VARNOST V PODJETJIH

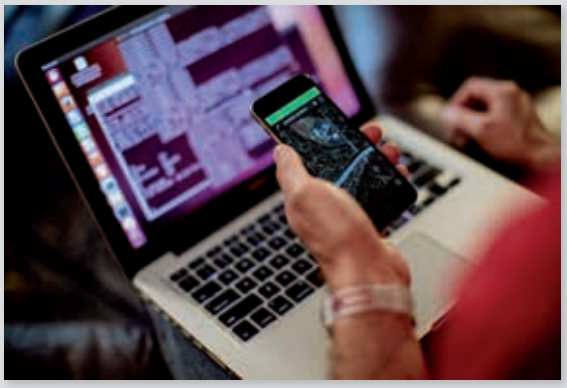
- prepoznavanje resnih ranljivosti
- penetracijski testi
- varnost in oblak

EVIDENCA

POLETJE 2019

12 Hekerji

Že o računalnikarjih krožijo v javnosti zelo popačene podobe, še slabše pa je poznavanje hekanja. K temu ne pripomore dejstvo, da termina ni ne v slovenski zakonodaji ne v standardnih slovenskih slovarjih. Če dodamo še vrsto sorodnih pojmov, kot so na primer krekerji, je zmeda popolna. Kaj sploh je hekanje in kdo so hekerji?

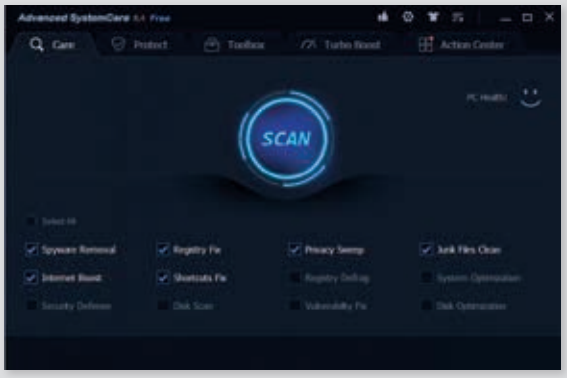


36 Odklepanje

Slovenci filme, serije in glasbo že dolgo uživamo predvsem digitalno. Resda smo spočetka to počeli v sivem območju, ki mu v tujini radi rečejo piratstvo, a smo se s hitro posvojitvijo plačljivih pretočnih storitev v zadnjem času odkupili ter dokazali našo pravo usmerjenost. Vedno smo bili za zabavo pripravljeni plačati pošteno ceno, vendar možnosti v preteklosti nismo imeli. Žal nam tudi pretočne storitve danes niso vse na voljo. Kljub temu se tokrat ne pustimo speljati na kriva pota, temveč se zatečemo k iznajdljivosti.

50 Domače izboljšave

Žice se počasi poslavljajo od naših domov, to velja predvsem za žice, po katerih potujejo računalniški biti. Do interneta večina omreženih naprav danes dostopa brezžično. Vedno pogosteje prihaja do najrazličnejših težav, ki se kažejo v počasnosti, prekinitvah ali celo kapitulaciji brezžične dostopne točke, zato nekaj nasvetov ne bo odveč.



66 Varnost doma

Domači računalniki s stalno internetno povezavo so običajno lahke tarče hekerjev. Kako zaščitimo njihovo vgrajeno programsko opremo, operacijski sistem in aplikacije? Na kaj moramo paziti pri nastavitvah kabelskega modema in delu z računalnikom?

INTERVJU

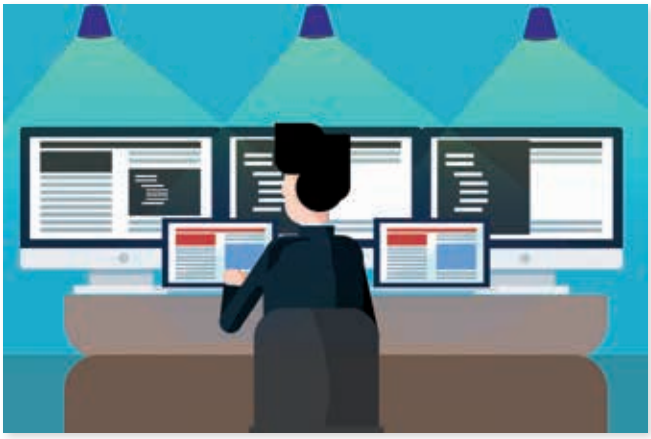
10 Gorazd Božič, SI-CERT

Preventiva ni dovolj – vedno lahko pride do napadov in vdorov v sisteme državne infrastrukture. Rešitev je mehanizem odzivanja na napade. To je prava preventiva.

VARNOST V PODJETJIH

77 Tudi varnostni strokovnjaki se učijo predvsem s prakso

Ste se kdaj vprašali, kakšna znanja in veščine potrebujejo varnostni strokovnjaki in kje jih lahko pridobijo? Verjemite, celo sami si zastavljajo ista vprašanja. Ogromno pa jih lahko nauči tudi ali predvsem praksa.



Resnična zgodba – prav v trenutku, ko pišem ta uvodnik, je v prostore uredništva stopila sodelavka, ki je nepremišljeno kliknila na phishing elektronsko sporočilo in nekomu na drugi strani sveta mirno zaupala geslo do svojega računa Paypal.

MATJAŽ KLANČAR
odgovorni urednik, matjaz.klancar@monitor.si

Ko se beseda »hekanje« znajde v SSKJ

Ni še dolgo tega, kar smo o hekerjih, tistih zlobnežih, ki menda znajo prelisičiti telefonsko centralo, da jim dovoli telefonirati zastonj, pisali le strogo specializirani tehnični časopisi in revije. Danes so hekerji in hekanje nekaj tako vsakdanjega, da o njih beremo tudi v črni kroniki, sama beseda pa je pristala že v Slovarju slovenskega knjižnega jezika (SSKJ).

Zgoraj zapisana misel je seveda logična – računalniki so danes povsod okoli nas, uporabljamo jih prav vsi, od računalniških doktorjev znanosti do delavcev na gradbišču, še največkrat v obliki pametnih telefonov, ki jih imamo v žepu. In prav vsi imamo na njih stvari, za katere ne bi želeli, da bi postale javne, prav vsi jih držimo zase in se vanje (ali v aplikacije/servise na njih) prijavljamo z gesli, vzorci, s prstnimi odtisi ali celo z biometričnimi podatki. Predvsem pa so vsi ti računalniki/telefoni povezani s svetovnim omrežjem in med seboj. Dokler so bili osebni računalniki le samostojni informacijski otočki v naših sobah, je bil edini dostop do njih prek fizičnega dostopa. Danes pač ni več tako.

Logično je torej tudi to, da na ta nekajmilijardni skupek nič hudega slutečih uporabnikov preži množica tistih, ki bi si želeli dostop do informacij na teh računalnikih/telefonih. Vsaka družba ima določen odstotek tistih, ki živijo od tega, da se ukvarjajo s kriminalnimi dejanji, in digitalna družba ni prav nič drugačna. Razen, da je veliko večja.

Še več, v ta milijardni skupek danes sodi kar dobršen del uporabnikov, ki vozijo dovolj sodobne avtomobile ali pa avtomobile, ki so iz varnostnih (!) razlogov opremljeni s sledilnimi napravami. Tudi ti so z internetom povezani neprestano in tudi ti so lahko tarča hekerjev. Hekerjev, ki imajo iz enega samega računalnika (telefona!) nadzor nad množico računalnikov.

In prav zato moramo uporabnike izobraževati, tudi tiste, ki jih tehnika v resnici prav nič ne zanima. Izobraževati o tem, kdo so v resnici hekerji, kaj je hekanje, kako je videti hekerski napad, kako se ga obranimo in kakšne so dobre prakse, ki napad v veliko primerih preprečijo. Mimogrede, resnična zgodba – prav v trenutku, ko pišem ta uvodnik, je v prostore uredništva stopila sodelavka, ki je nepremišljeno kliknila na *phishing* elektronsko sporočilo in nekomu na drugi strani sveta mirno zaupala geslo do svojega računa Paypal. K sreči smo ji ga dovolj hitro pomagali spremeniti.

Hekerje se lahko gremo tudi sami. V izobraževalne namene seveda in tako, da ne škodimo nikomur. Obstajajo distribucije Linux, ki so napolnjene z vsemi orodji, potrebnimi za tako početje. Še več, ta isti Kali Linux je mogoče namestiti celo na telefon. Hekersko orod(ž)je imamo torej lahko kar v žepu, vedno s seboj. Telefoni z Androidom so sploh hudo orožje, saj lahko zanje kupimo tudi aplikacije, ki popolnoma skrito beležijo telefonske klice, esemese in sploh vso komunikacijo, ki jo zmore telefon. Če vas je prešinilo – da, tako početje je celo legalno, zlasti če živimo v ZDA in gre za službeni telefon. Če je telefon/računalnik v lasti delodajalca, ima ta namreč z njim pravico početi karkoli, tudi mu prisluškovati.

Lahko pa svoje znanje usmerimo v kaj bolj koristnega, denimo v to, kako priti do vsebin (in jih plačati!), ki nam jih svetovni medijski ponudniki nočejo prodati, ker živimo na napačnem koncu sveta. Ali pa kako odkleniti telefon, da bo z njim mogoče početi še kaj več kot le tisto, kar nam dovolijo. Ali kako doma izboljšati signal Wifi in si prek njega urediti dober avdio/video sistem.

Kaj pa, če smo podjetje? V tem primeru je na kocki preveč, da bi vse prepustili eni osebi ali celo kar nam samim. Obrnimo se na profesionalne ponudnike varnosti, prepustimo se testnim preizkusom, penetraciji, predvsem pa imejmo načrt, kako rešiti podjetje, če/ko se kaj zalomi.

In o vsem tem in še čem lahko preberete na naslednjih straneh, kjer smo nanizali dvajset zelo tematsko usmerjenih člankov.

Veselo branje!

Mnoge poceni pametne naprave so leglo napak in površno napisanega ter nekakovostnega programja, brez kančka odgovornosti za osebne podatke ali skrbi za digitalno varnost.

DAVID VIDMAR

Varnost, zasebnost in uporabnost **se (ne) izključujejo**

V sodobnih podjetjih je varnost IT-rešitev ena najsvetejših kvalitet. V svetu storitev za končne uporabnike pa smo uporabniki velikokrat prepuščeni sami sebi. Čeprav nekateri proizvajalci na varnost gledajo kot na dodaten strošek, smo vseeno ravno uporabniki tisti, ki imamo vse niti v rokah.

Med pripravo na pisanje tega mnenja sem za preizkus zahteval arhiv svojih podatkov, ki jih o meni zbirajo spletni velikani. Tudi če smo le zmerni uporabniki, se zbrani podatki skozi leta nakopičijo, saj marsikdo uporablja te storitve že deset let ali več. Čeprav sem zmeren uporabnik Googlovih storitev, mi ta ponudi za prenos več kot 50 GB »mojih« podatkov, pa med njimi sploh ni slik ali video posnetkov. Facebooka skoraj ne uporabljam, pa je arhiv mojih podatkov velik nekaj sto megabajtov. Koliko je podatkov, ki so jih o meni zbrali posredno, je zelo težko oceniti, a gotovo jih je vsaj še enkrat toliko.

O množičnem zbiranju in obdelovanju je (bilo) napisanih veliko knjig in še mnogo več člankov ter razprav, mnogi so se začeli zavedati nevarnosti, ki zaradi tega pretijo. Tehnološka podjetja so se kmalu odzvala. Zadnje mesece Google, Facebook, Apple in ostali kar tekmujejo, kdo bo bolj proaktiven pri izpostavljanju varovanja zasebnosti, spodbujanju manjše uporabe družabnih omrežij in naprav. Očitno je, da želijo obrniti plimo ter se v zavesti povprečnega uporabniki iz zbiralcev podatkov preleviti v varuhe digitalne varnosti in zasebnosti.

Ne štejem se med tiste, ki bi jih trenutno stanje potrlo. Mnogi trdijo, da so družabna omrežja in druge brezplačne storitve, katerih komercialni namen je zbirati in izkoriščati podatke o svojih uporabnikih, cigarete te generacije. Upam, da bomo na njih kmalu gledali kot danes na stare čase, ko so ljudje kadili vsepovsod in ves čas.

Podrobneje spremljam napredke in »napredke« domačih pametnih naprav, ki jim marsikdo posmehljivo pravi »*internet of shit*«. Mnoge poceni pametne naprave so leglo napak in površno napisanega ter nekakovostnega programja, brez kančka odgovornosti za osebne podatke ali skrbi za digitalno varnost, a na trgu se pojavlja vedno več naprav in storitev, ki nas, uporabnike, spoštujejo kot lastnike naprav in z njimi povezanih podatkov. Marsikatera pametna naprava omogoča delovanje le v lokalnem omrežju priklop v svetovni splet pa je nadzorovan in možen le ob odobritvi lastnika. Še nedavno so bile takšne naprave bolj zapletene, manj prijazne ob priklopu, a danes to niso več samo naprave za tehnološke navdušence, ampak tudi naprave priznanih proizvajalcev, primerne za vsakogar. Ti znanilci digitalne pomladi dokazujejo, da ni res, da moramo za dobro uporabniško izkušnjo potrpeti in da mora za zanesljivo delovanje ameriški ali kitajski proizvajalec vedeti za vsak vklop ali izklop luči, menjavo televizijskega kanala in vsako odpiranje garažnih vrat.

A, žal, se zgodi tudi korak v drugo smer, ko naprava po nadgradnji deluje samo še prek povezave z oblačno storitvijo, čeprav je nekoč delovala bolj premišljeno. V zadnjih mesecih sta se zgodila dva odmevna incidenta te vrste. V prvem je Logitech ukinil lokalni dostop do programskih vmesnikov pametnih univerzalnih daljinskih upravljalnikov družine Harmony, ki so jih uporabljale mnoge rešitve za upravljanje doma. Po hitrem in burnem odzivu uporabnikov so si premislili in objavili opravičilo ter zavezo, da bodo z naslednjo nadgradnjo povrnili prejšnje stanje. Nisem povsem prepričan, da je to trajna obljuba, saj verjetno samo kupujejo čas, a upanje ostaja.

Povsem drugače se je končala zgodba, v kateri je Google uporabnikom pametnih termostatov Nest zagrenil življenje z napovedjo ukinitve izjemno priljubljenega vmesnika Works with Nest. Uporabljajo ga mnoge storitve in pametne naprave za dom, med njimi tudi zelo priljubljena storitev IFTTT. Stari način upravljanja termostatov bo Google enostavno ukinil in ga integriral v svoje storitve Google Home. Uradno navajajo, da bodo to storili zaradi boljšega varovanja zasebnosti in podatkov uporabnikov, a to prinaša še močnejše povezovanje z Googlovimi storitvami, kar lahko razumemo kot še večje kopičenje podatkov o uporabnikih. Proizvajalcem in uporabnikom naprav, ki so še do nedavno znale sodelovati z Nest, ne preostane nič drugega, kot da se velikanu podredijo in prilagodijo. Da bi si Google vsaj začasno premislil, kot si je Logitech, namreč ni pričakovati.

Mogoče se bodo v Evropi prebudili regulatorji in poskusili urediti razmere tudi na trgu naprav, a zgodovina nas uči, da bo ta proces dolgotrajen in preveč okoren, da bi prinesel resne izboljšave. Uporabniki bomo sami najbolje povedali, kakšno prihodnost si želimo - s kupovanjem naprav in z najemom storitev, ki uporabljajo odprte protokole (in po možnosti objavljajo kodo programske opreme), jo tudi redno nadgrajujejo in tako omogočajo, da ostanemo lastniki svojih podatkov. Te pa le z izrecnim dovoljenjem prepustimo komu drugemu in še to le v transparentno obdelavo. ◀

Izbor novic z varnostnega področja iz druge polovice leta 2018

Ogroženi vsi androidni telefoni od leta 2012

4. 7. 2018. Vsi androidni mobilni telefoni od leta 2012 so potencialno ranljivi zaradi luknje, ki so jo prvikrat odkrili na osebnih računalnikih leta 2014, dve leti pozneje izpostavili tudi na mobilnih telefonih in tedaj domnevno tudi zakrpali. Toda raziskovalci iz Amsterdama so pokazali, da Googlov popravek iz leta 2016 ni dovolj.

Gre za naslednika napada Rowhammer, ki se v novi preobleki imenuje RAMpage. Osnovna premisa je enaka. Kadar intenzivno beremo podatke iz iste vrstice pomnilnika, lahko vplivamo na stanje v sosednji vrstici. To ni programska napaka, temveč posledica zgradbe pomnilnika. Od tod pa do izrabe nas loči le še pametna izvedba napada, torej, vedeti kam in kdaj vplivati.

Ko je Google pred dvema letoma videl, da to v praksi deluje, je popravil svoj upravljalnik pomnilnika. Ideja je bila zagotoviti, da noben program nima dostopa do dolgih zaporednih fizičnih naslovov v pomnilniku. Kazalo je, da to zadostuje, a je bila izvedba pomanjkljiva. Na univerzi v Amsterdamu so namreč pokazali, da je mogoče vseeno dobiti dostop do celotnih vrstic, kar odpira vrata zlorabam.

Preizkusili so Google Pixel 1, Nexus 4 in Nexus 5, ki so bili ranljivi. Ugotavljajo, da so potencialno ranljivi vsi telefoni s pomnilnikom LPDDR2, LPDDR3 ali LPDDR4. V praksi pa se lahko zgodi, da sta različna telefona istega modela različno občutljiva, zato so pripravili program, s katerim lahko preverimo, ali je naš telefon med občutljivimi. Ob tem mirijo, da se omenjena ranljivost verjetno ne bo množično izkoriščala, ker jo je precej zapleteno izkoristiti. Toda če ima kdo resen namen in eno tarčo, je mogoče tudi to.

Facebook želi dostop do bančnih podatkov svojih uporabnikov

Facebook je idejo o sodelovanju z bankami za bančne storitve naslovil na vodilne ameriške banke JPMorgan Chase, Wells Fargo, US Bank in Citigroup. Po zamisli Facebooka naj bi banke omogočile uporabnikom pregled bančnih in kreditnih transakcij, stanje na računu in druge storitve v okviru Facebookovega omrežja Messenger. V zameno naj bi Facebook bankam omogočal dostop do uporabnikov omrežja.

Facebook obenem zagotavlja, da podatkov ne bo izkoriščal za ciljano oglaševanje niti jih delil z drugimi, kar je bilo jedro afere v zvezi z družbo Cambridge Analytica. Toda njihova kredibilnost in javna podoba sta v teh časih na trhlih temeljih, zato je težko pričakovati, da bo zamisel dobila hitro in široko podporo. Vsaj ena banka, JPMorgan Chase, je predlog že zavrnila.

Raziskava: Kitajska redno preusmerja in prestreza internetni promet

V raziskavi, ki so jo opravili na ameriški visoki šoli za vojno mornarico (US Naval War College) in univerzi v Tel Avivu, so odkrili, kako Kitajska pogosto in za dlje časa preusmerja internetni promet na svoje ozemlje. Tam ga prekopira in analizira za potrebe industrijskega vohunjenja ter razbijanja šifriranja.

Promet med različnimi točkami na internetu načelno poteka po najhitrejših (često najkrajših) poteh. Za to skrbi protokol BGP (Border Gateway Protocol). Vsak skrbnik omrežja na internetu oznanja, za katere avtonomne sisteme (AS), torej dele interneta, je zadolžen, da jim lahko dostavlja promet. Večkrat pa se je že zgodilo, da so bodisi zaradi napake ali malomarnosti bodisi namerne manipulacije določeni upravljavci oznanjali nápak. Rezultat so neobičajne poti prometa, kar je še posebej sumljivo, kadar večji deli daljše časovno obdobje potujejo skozi Kitajsko.

Šifrirana vsebina diskov v resnici ni … šifrirana

Raziskovalci nizozemske univerze Radboud so odkrili, da je kar nekaj proizvajalcev pogonov SSD, ki omogočajo strojno šifriranje vsebine, te implementiralo zelo površno.

Razbrali so strojno programsko opremo (*firmware*) več pogonov SSD (skupno predstavljajo približno 50 odstotkov SSD, ki so danes v prodaji) in ugotovili, da hekerji lahko razberejo vsebino na pogonih brez vpisa kakršnegakoli gesla ali šifrirnega ključa. Navajajo, da so vsebino na enem disku odklenili kar s »katerimkoli geslom«, ker sistem preverjanja sploh ni deloval, na nekem drugem pa tako, da so vpisali prazno geslo, torej je bilo treba pritisniti le tipko *Enter*.

Raziskovalci odkrili nove različice ranljivosti Spectre v procesorjih

19. 7. 2018. Vse kaže, da z ranljivostjo sodobnih mikroprocesorjev povezana afera, ki se tiče tako imenovanega špekulativnega izvajanja ukazov, še ni končana. Strokovnjaka za varnost Vladimir Kiriansky in Carl Waldspurger sta pravkar objavila novo poročilo, kjer razkrivata dve novi različici ranljivosti, ki po njunem mnenju odpirata nove možnosti zlorabe.

Ranljivosti, ki sta ju poimenovala Spectre 1.1 in 1.2, menda dosedanji popravki, ki jih je v zadnjih mesecih pripravila računalniška industrija, v prvi vrsti Intel, ne odpravljajo. Vse kaže, da bodo potrebni novi.

Spomnimo, da je dosedanja ranljivost Spectre potrebovala cel niz popravkov, od katerih nekateri sploh niso delovali, kar je industrijo ter končne uporabnike stalo veliko denarja in časa. Ob tem je večina računalniških sistemov in programov zabeležila degradacijo zmogljivosti in porabe sistemskih sredstev. Nazadnje smo pisali o tem, da bo, denimo, novi brskalnik Chrome zaradi »obvoza« za Spectre 10–13 odstotkov bolj potraten pri porabi pomnilnika.

Po trditvah avtorjev so novo ranljivost našli v procesorjih Intel in ARM, najbrž pa to velja tudi za AMD. Odzivov računalniških podjetij še ni, avtorja pa upata, da bo industrija našla generično rešitev za probleme, povezane s špekulativnim izvajanjem ukazov. Dosedanji popravki so, kot kaže, najbrž zaradi ohranjanja še sprejemljive zmogljivosti naslavljali zgolj specifične primere zlorabe.

PODATKI

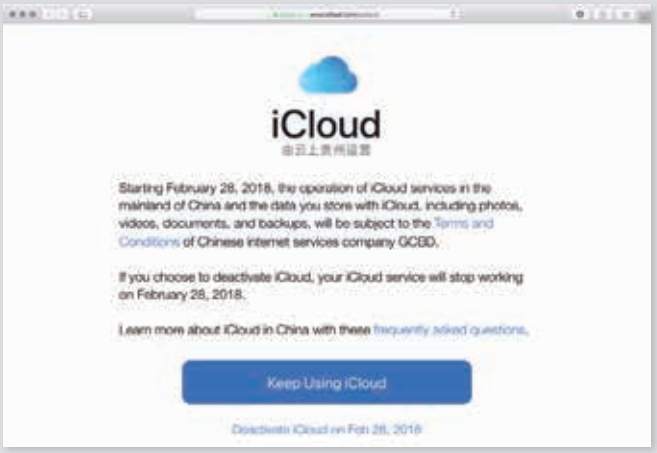
Podatke za kitajske uporabnike iClouda **bo hranilo kitajsko državno podjetje**

Kitajska ne skriva želja po dostopu do vseh podatkov svojih državljanov. Tuji ponudniki komunikacijskih in družbenih omrežij storitev velikokrat nimajo druge izbire, kakor da se uklonijo zahtevi po hranjenju podatkov uporabnikov na kitajskih tleh, kjer ima Kitajska seveda lahek dostop do njih. Tudi Apple je moral popustiti in kitajske podatke iz iClouda zdaj hrani državno podjetje, ki je *de facto* pod nadzorom kitajske vlade.

Apple je že lani napovedal, da bo pri upravljanju iClouda na Kitajskem sodeloval s podjetjem GCBD (Guizhou-Cloud Big Data Industry Development), februarja letos pa so sporočili, da bodo podatke kitajskih uporabnikov v iCloudu prenesli v nov podatkovni center v provinci Gvidžov. Apple je ob tem dejal, da je bilo to nujno zaradi kitajskih internetnih zakonov.

Zdaj pa je GCBD začel sodelovati s China Telecomom, ki je v lasti kitajske države. Njegov oddelek za oblačne storitve Tianyi Cloud bo GCBD nudil gostovanje za iCloud. Z drugimi besedami to pomeni, da ima podjetje v lasti kitajske države dostop do vseh sporočil, fotografij, osebnih podatkov in drugih informacij v iCloudu kitajskih uporabnikov. Podatki so sicer šifrirani, a bodo ključi shranjeni na kitajskih strežnikih, torej lahko kitajske oblasti pridobijo dostop do njih – po pravni poti ali kako drugače.

Apple kaj dosti besede pri tem ni imel, saj bi v nasprotnem primeru verjetno izgubil licenco za poslovanje na Kitajskem. Kitajske oblasti izganjajo podjetja že zaradi manjših stvari, denimo



pred leti je imel Google težave zaradi nezadostne cenzure iskalnih rezultatov.

Joshua Rosenzweig iz hongkonške izpostave Amnesty International je povedal, da nov dogovor predstavlja veliko tveganje za kitajske uporabnike Applovih storitev in da postavlja na laž Applov moto, da jemlje zasebnost uporabnikov resno. Apple sicer zagotavlja, da v sistemu ne bo stranskih vrat in da bo nadzor nad ključi ostal Applu, a kaj ko bodo fizično shranjeni na Kitajskem.

Tujci nam berejo **Gmail sporočila**

4. 7. 2018. Google je razkril, da do elektronske pošte uporabnikov Gmaila dostopajo razvijalci s storitvijo povezanih aplikacij.

Znano je, da je Google razvijalcem aplikacij že pred časom odprl dostop do storitve Gmail, a šele zdaj je jasno, da sporočil v nabiralnikih ne berejo zgolj računalniki. Eden izmed razvijalcev je časniku *Wall Street Journal* zaupal, da je tovrstna praksa običajna, a strogo varovana skrivnost. Med razvijanjem algoritma je lastnoročno prebral na tisoče sporočil nič hudega slutečih uporabnikov pošte Gmail. Google se zagovarja, da v početju ni nič spornega, saj se uporabnik s podpisom splošnih določil uporabe z njim strinja. Poraja se vprašanje, koliko od 1,4 milijarde uporabnikov pošte Gmail je določila pred podpisom dejansko prebralo. Praksa kaže, da zelo malo. Na srečo nikoli ni prepozno, da dodeljene pravice tujim razvijalcem prekličemo. Seznam najdemo na Googlovem naslovu *Security Check-Up*.

Spletne strani brez HTTPS so po novem »ne varne«, pravi Chrome

26. 7. 2018. Kot smo že pisali, ima Google strogo časovnico, ki določa strategijo označevanja spletnih strani s podporo šifriranju (HTTPS) in brez nje. Od torka je tako na voljo Chrome različica 68, ki spletne strani, če ne podpirajo šifriranega prenosa podatkov, označuje kot »ne varne« (*Not secure*).

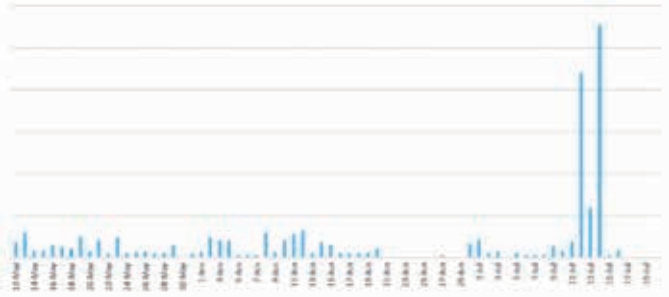
Zanimivo je, da je v svetu še zelo veliko resnih spletnih strani, ki nešifriranega prometa samodejno ne preusmerjajo na strežnik s podporo za HTTPS. Najbolj preseneča kitajski iskalnik baidu.com, ki je četrta največja spletna stran na svetu, med večjimi pa izstopajo tudi še bbc.com (v nasprotju z bbc.co.uk, denimo), businessinsider.com, fedex.com, espn.com in podobni.

Srečanje Trump-Putin poskrbelo za **porast hekerskih napadov na Finsko**

21. 7. 2018. Finska običajno ne beleži velikega števila hekerskih napadov na svojo internetno infrastrukturo, a se je to močno spremenilo pred srečanjem Donalda Trumpa in Vladimirja Putina, ki je v ponedeljek potekalo v Helsinkih. Štiri dni pred obiskom se je število napadov povečalo za 28-krat, v poročilu ugotavlja podjetje *F5*.

Večina poskusov vdorov je izvirala iz Kitajske, od koder na povprečen dan pride 29 odstotkov vseh svetovnih vdorov, pred omenjenim srečanjem pa je ta odstotek poskočil na 34 odstotkov. Povečalo se je tudi število napadov iz ZDA, Francije in Italije. Število napadov se je okrepilo za 2.800 odstotkov, merili pa so v glavnem prek vrat 22 (SSH). Šlo je za napade s surovo silo, ki so iskali ranljive, z internetom povezane pametne naprave (IoT). To so med drugim različne kamere, usmerjevalniki itd. Mnogokrat imajo te naprave kar privzeta tovarniška gesla, poleg tega pa jih ne posodabljajo tako pogosto kakor računalnike, zato so posebej pripravne tarče napadov.

Druga tarča so bile naprave, ki poslušajo na vratih 5060 (Session Initiation Protocol), kamor sodijo tudi programska oprema za internetno telefonije in



videokonference. Hekerji so očitno iskali načine, kako pridobiti čim več informacij o obisku in njegovem poteku.

Kibernapadi so čedalje pomembnejši del vohunjenja in obveščevalnih aktivnosti, česar države niti ne skrivajo več. Kitajsko pogosto izpostavljajo kot najaktivnejšo na tem področju, a še zdaleč ni edina. Bitke se danes bijejo v računalnikih.

VirtualBox z varnostno luknjo, ki omogoča »pobeg« iz virtualnega okolja

Ruski varnostni raziskovalec Sergey Zelenyuk je na GitHubu objavil podroben opis še neodkrite varnostne luknje (t. i. »0-day«), ki omogoča, da program v navideznem okolju VirtualBox upravlja okoljee v operacijskem sistemu, ki ga gosti.

Ustrezno napisana programska koda v VirtualBoxu lahko odpre ukazno vrstico v gostujočem sistemu. Res pa je, da odprto okno ne teče v privilegiranem načinu (ring 0), ampak ima običajne pravice (ring 0). Vendar Zelenyuk opozarja, da je na voljo kar nekaj drugih trikov, s katerimi je mogoče pravice takšnega okna naknadno dvigniti.

Hrošč omogočal **brezplačne igre na Steamu**

Podjetje Valve je nagradilo strokovnjaka za varnost, ker je na največjem igričarskem portalu na svetu našel programsko luknjo, ki je omogočala brezplačen prenos sicer plačljivih iger.

Napako je gospod Moskowsky odkril po naključju, ko je obiskal spletišče enega izmed partnerjev servisa, ki omogoča založnikom iger ustvarjanje zaščitnih ključev za kopije, namenjene novinarjem, kritikom, ljubiteljem in drugim. Z eno samo spremembo programske zahteve je prelisičil sistem za določanje pristnosti uporabnika, ki preveri, ali je igra, za katero se ključ izdeluje, res v lasti uporabnika, ki je podal zahtevo. Tako bi lahko vsakdo ustvaril na tisoče ključev za poljubne igre in jih prodal na črnem trgu. Pri podjetju Valve so napako že odpravili.

Japonski minister za računalniško varnost **še ni uporabljal računalnika**

Japonski minister za računalniško varnost Jošitaka Sakurada je šokiral javnost z izjavo, da nikoli v življenju ni uporabljal računalnika.

Minister, ki bo med drugim skrbel za informacijsko varnost olimpijade 2020 v Pekingu, trdi, da je dela, ki vključujejo računalnike, od 25. leta starosti uspešno prelagal na podrejene. Oseminšestdesetletnik, ki je funkcijo prevzel šele pred mesecem dni, se je nemudoma znašel pod plazom kritik. Najglasnejša je bila opozicijska stranka demokratov, ki ne more verjeti, da za kibernetsko varnost v državi skrbi človek, ki o računalnikih nima pojma. Svoje so dodali tudi spletni troli, ki jim hudomušnih objav na temo računalniško nepismenega ministra ne zmanjka.

Kriptodenarnica Bitfi umika naziv »nezlomljiva«

4. 9. 2018. Kontroverzni John McAfee, ki je dal ime legendarnemu protivirusnemu programu in ostalim izdelkom istoimenskega podjetja, danes pa je bolj znan po svojih čudaških izjavah, je sporočil, da Bitfi ni več nezlomljiv. Gre za 120 dolarjev vredno fizično kriptodenarnico, ki jo trži istoimensko podjetje, v katerem ima svoj delež tudi McAfee. Doslej se je Bitfi oglaševala kot nezlomljiva (*unhackable*) denarnica, čeprav so hekerji večkrat pokazali, da to ni povsem res.

Razvijalci so ponujali celo 250.000 dolarjev nagrade tistemu, ki bi mu uspelo vdreti vanjo. Ob tem povejmo, da je bil pogoj precej čudaški, saj so zahtevali dejanski prenos bitcoina, kar je že kaznivo dejanje. Običajno dobri hekerji (*white hats*) ranljivosti odkrijejo, a jih ne izkoristijo, temveč o njihovem obstoju obvestijo proizvajalca. Zato so vsakokrat ostali brez nagrade, kar je v nasprotju z uveljavljenimi programi nagrajevanja hroščev (*bug bounty*). Kakorkoli, od McAfeeja smo čudaški izjav že vajeni, saj se je pred dvema letoma zaklinjal, da bo pojedel čevelj, če mu ne bo uspelo »zlomiti« iPhona. Vdora v iPhone ni nikoli izvedel, čevlja pa tudi ni pojedel. Lani je trdil, da bo bitcoin v naslednjih treh letih vreden 500.000 dolarjev, sicer bo pojedel svojo moškost. Bitcoin je danes vreden 7.200 dolarjev, a nekaj časa še ima.

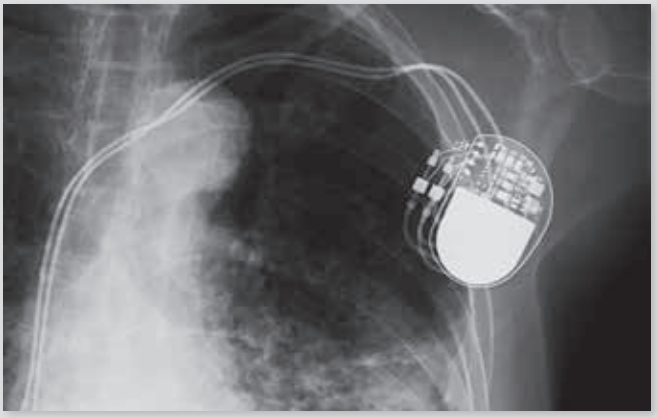
Vrnimo se k Bitfiju. Raziskovalci so odkrili resno ranljivost v tej denarnici, zaradi česar so celo v Bitfiju podali uradno izjavo, da umikajo oznako nezlomljiva. Da se je Bitfi oglaševal kot nezlomljiv, je tako in tako neumno, saj je vsem jasno, da nezlomljivih sistemov ni. Ob tem pa dodajajo, da raziskovalci (spet!) ne bodo dobili 250.000 dolarjev, ker niso izmaknili nobenega bitcoina, temveč so le opozorili na napako. Skupnost je to že označila za najbolj patetičen odziv. McAfee je medtem za konkretnega hekerja povišal nagrado na 20 milijonov dolarjev, čeprav je vsem jasno, da bi tudi v primeru vdora našel kakšen izgovor, da tega ne bi izplačal. Splošen *bug bounty* pa je Bitfi končal.

RANLJIVOST

Srčnega spodbujevalnika **ni težko shekati**

Moderni medicinski pripomočki so računalniki v malem, kar olajša njihovo nastavljanje in odčitavanje podatkov, a jih hkrati odpira številnim tveganjem, da hekerji izkoristijo luknje. Na konferenci *Black Hat* v Las Vegasu sta Billy Rios iz podjetja Whitescope in Jonathan Butts iz podjetja QED Secure Solutions pokazala, da so tudi najnovejši srčni spodbujevalniki ranljivi.

Gre za Carelink 2090 podjetja Medtronic, o čemer sta podjetje obvestila že lani, pa še vedno nimamo popravka, s katerim bi bila zadovoljna. V podjetju medtem trdijo, da obstoječe zaščite povsem zadostujejo. Potrebovali so 10 mesecev, da so se odzvali z besedami, da odkritja ne kažejo nobenih novih ranljivosti ter da so tveganja pod nadzorom in sprejemljiva.



Problem je, da se *firmware* na napravi posodablja prek nezaščitene povezave in da ne uporablja digitalnih podpisov. To pomeni, da lahko zlikovec namesti lažni *firmware*, ki zdravnika ob kontroli zavaja, bolniku pa lahko celo škoduje. Rios in Butts sta odkrila ranljivosti tudi v internem omrežju podjetja, kjer se pripravljajo posodobitve spremljevalne opreme, denimo monitorjev in programov za srčne spodbujevalnike.

Če se vam zdi novica znana, niste edini. Že lani smo pisali o drugih srčnih spodbujevalnikih in defibrilatorjih, ko so bili v nevarnosti, da jih hekerji napadejo. Popravek *firmwara* naj bi tedaj težavo odpravil. Komur seže spomin še dlje, pa se bo spomnil, da se je na internetu prvikrat o hekanju spodbujevalnikov govorilo daljnega leta – 2008. In do danes nismo našli pametne rešitve za to težavo.

Priznava jo tudi stroka, saj sodelujeta celo FDA (Agencija za hrano in zdravila) in DHS (Oddelek za domovinsko varnost). Ker so medicinski pripomočki zelo občutljive naprave, ki ne smejo imeti lukenj, hkrati pa vsaki popravki trajajo, saj je treba spremembe temeljito preizkusiti in pridobiti odobritev FDA, enostavne rešitve ni na vidiku. FDA je aprila zagnala *Medical Device Safety Action Plan*, v okviru katerega želijo ustvariti odbor za analizo računalniške varnosti v medicinski opremi (*cybermed safety expert analysis board*).

Z ukradeno telefonsko številko **do kriptomilijonov**

20. 8. 2018. Ameriški poslovnež in direktor družbe TransformGroup Michael Turpin toži ameriškega operaterja AT&T, češ da so mu zaradi njegove malomarnosti hekerji ukradli za 24 milijonov dolarjev kriptovalut. Od AT&T zahteva prav toliko odškodnine in še 200 milijonov kazenske odškodnine zaradi malomarnosti.

Turpin trdi, da je napadalcem uspelo od AT&T pridobiti kopijo njegove SIM-kartice, ki je bila povezana z isto telefonsko številko. S telefonsko številko so zavarovane identitete v številnih spletnih storitvah, kjer lahko pozabljeno geslo ponastavimo s prejemom gesla v SMS. Problem pa je, da mobilno omrežje še zdaleč ni odporno proti napadom. Poleg klasičnih napadov SS7, ki izrabljajo pomanjkljivo zaščito v dizajnu mobilnih omrežij, je šibka točka tudi operater, kar naj bi se zgodilo v primeru Turpin.

Napadi s prevzemom kartice SIM niso nič novega. Terpin trdi, da so mu napadalci telefonsko številko ukradli kar dvakrat. Prvikrat naj bi se bilo to zgodilo 11. junija lani, drugič pa 7. januarja letos. Ko so imeli pod nadzorom njegovo telefonsko številko, so pridobili dostop do enega izmed njegovih računov pri spletnih menjalnicah in odtujili za 24 milijonov dolarjev kriptovalut.

Načina sta dva, oba pa vključujeta človeški dejavnik. V nekaterih primerih napadalci pokličejo tehnično podporo pri operaterju ali se osebno zglasijo ter se izdajajo za žrtev, po možnosti posredujejo še nekaj osebnih podatkov in tako pretentajo operaterja. V drugem načinu pa uporabljajo »insajderje«, ki so zaposleni pri operaterju in v zameno za podkupnino skopirajo SIM-kartico oziroma prenesejo številko.

Turpin naj bi odkril, da so mu junija lani po 11 neuspelih poskusih v 12. ukradli številko, ko je njegov telefon izgubil povezavo z omrežjem. Že tedaj so mu ukradli nekaj denarja, AT&T pa mu je ob vrnitvi dostopa do računa zagotovil, da bodo po novem njegovo številko obravnavali s posebno skrbnostjo (namenjeno zvezdnikom, poslovnežem in ostalim pogostim tarčam). Vseeno je pol leta pozneje hekerjem spet uspelo prevzeti njegovo številko in tedaj so ukradli za 24 milijonov dolarjev kriptovalut.

AT&T je v izjavi za *Reuters* zanikal tožnikove navedbe in dejal, da bodo to na sodišču tudi dokazali.

Ne glede na končni razplet in resnični razlog pa ostaja dejstvo, da je mobilno omrežje samo po sebi zelo luknjičasto, ker je bilo zgrajeno v nekem drugem času z drugimi prioritetami. Uporaba esemesov za dodatno avtentikacijo ali ponastavitev računa je zelo tvegana in bi jo morali ukiniti.

Vodja varnosti **zapušča Facebook**

2. 8. 2018. Alex Stamos, vodja varnosti pri Facebooku, bo podjetje zamenjal za Stanford University.

Njegov odhod je bil pričakovan, saj so pri Facebooku že marca napovedali reorganizacijo varnostnega oddelka. Stamos je pred Facebookom delal pri Yahooju, glavna izvršna direktorica Facebooka, Sheryl Sandberg, pa je povedala, da je imel v Facebooku pomembno vlogo. Stamos je za *New York Times* izjavil, da so bila njegova tri leta pri Facebooku naporna, saj da podjetje deluje v zelo nevarnem okolju.

Pri Facebooku pravijo, da ne nameravajo iskati oziroma postaviti zamenjave, saj da so po novem vsi, ki delajo na področju varnosti, del posameznih inženirskih ekip. Stamos je sicer požel kar nekaj kritik v začetku leta, ko je zaradi pisanja o škandalu s podjetjem Cambridge Analytica napadel medije.

Ljudje s(m)o **temelj varnosti**

Z Gorazdom Božičem, direktorjem slovenskega centra za posredovanje pri omrežnih incidentih SI-CERT, ki deluje v okviru javnega zavoda Arnes, smo se pogovarjali o kondiciji kibernetske varnosti v državi.

Miran Varga

▶ Ves svet govori o hekerjih. So res tako zlobni, kot mnogi menijo?

Ne, hekerji sami po sebi niso zlobni. Heker je oznaka za posameznika s specifičnim znanjem in z željo po globljem raziskovanju rešitev ter sistemov. Išče namreč načine, kako naprave ali sisteme izkoristiti za doseganje rezultatov ali drugačno delovanje, tako, ki v osnovi ni bilo zamišljeno. Skratka, želijo prelisičiti sistem, da bi deloval drugače, kot je bil zasnovam. Delovanje hekerja je lahko zabava, učenje ali pa slab cilj, tudi protizakonito dejanje. Pojem heker je bil pred 20 leti sinonim za mozoljastega fanta starega med 15 in 23 leti, ki je užival v računalništvu in se ni kaj prida družil z vrstniki. To je bil stereotip, ki je temeljil na lastnostih najbolj znanih hekerjev tistega časa. Danes je heker večplastna oznaka. Lahko gre za etično osebo ali pa kriminalca, nekoga, ki svoje znanje uporablja za protipravno doseganje finančne koristi.

▶ Kaj pa etični hekerji? Oni so »dobri fantje«. Kako velik je razkorak med enimi in drugimi?

Težko je dati splošen odgovor, saj je na delu več dejavnikov, veliko je odvisno od posameznika in njegovih nazorov. Priročnik o etičnih hekerjih ne obstaja. Različni ljudje se danes opredeljujejo kot etični hekerji. Hkrati si zelo različno predstavljajo meje, do katerih lahko gredo. Tako kot etos tudi te meje niso točno določene. Etični hekerji naj bi skrbeli za odgovorno razkrivanje ranljivosti, a lahko kaj hitro storijo kak korak preveč. Nekateri imajo jasne omejitve, spet drugi so v svojem raziskovanju bolj prožni. Toda prožnost je problematična, saj se lahko hitro znajdejo v območju, kjer bodo preganjani. Stvar je podobna analogiji iz potapljaštva – če gre potapljač pregloboko in to prepozno ugotovi, ima težave.

▶ Etični hekerji nam mahajo z različnimi certifikati. Kako zanesljivi so?

Certifikat še ne naredi etičnega hekerja. Odvisno, na kakšni osnovi je podeljen. Nekateri certifikati se sčasoma uveljavijo, drugi nikoli. Le čas bo pokazal, kateri so pravi. Kdor najema etičnega hekerja, mora poleg njegovih certifikatov preveriti predvsem reference in kompetence.

▶ Toda tisti, ki najemajo etične hekerje, navadno nimajo teh kompetenc, da bi znali (raz)soditi.

Drži. Zato pa naj poiščejo strokovnjaka, ki bo to oceno opravil zanje. Podobno kot v podjetjih, kjer nimajo lastnega IT-oddelka – najamejo zunanjega IT-izvajalca na osnovi dokazljivih rezultatov.

▶ Česa bi se morala slovenska podjetja najbolj bati in zakaj? To verjetno niso hekerji?

Podjetja bi se morala najbolj bati scenarija, po katerem bodo ranljivost prepoznala, ko bo že prepozno. Šele takrat se bodo zavedela, da bi morala vlagati v sposoben kader. Ta je namreč osnova informacijske varnosti. Podjetja preprosto potrebujejo ljudi, ki so ustrezno usposobljeni in spremljajo dogajanje v svetu varnosti. Taka oseba (ena ali več) je lahko zaposlena v podjetju ali pa je zunanji sodelavec. Brez tega pa letijo v megli in upajo, da bodo dosegli cilj. Nekateri se, žal, tudi zaletijo. Opažam, da veliko podjetij, sploh manjših, že na kader s področja IT gleda kot na strošek, ki je morebiti nepotreben. In ga želi minimizirati. Na področju kibernetske varnosti je še slabše. Podjetja si ne predstavljajo, zakaj bi potrebovala nekoga za kibernetsko varnost.

▶ Danes med napadalci niso le posamezniki in kriminalne združbe – napadajo celo države oziroma njihovi hekerji. Obstaja sploh obramba pred napadalci, ki jih sponzorirajo države?

Seveda obstaja. Ta je lahko uspešna, a odvisno od tega, kako je zastavljena. Treba je imeti vizijo in načrt. Začne se pri osnovnem dejstvu, da sama preventiva ni dovolj – vedno lahko pride do napadov in vdorov v sisteme državne infrastrukture. Rešitev je mehanizem odzivanja na napade. To je prava preventiva. Obrambni zid je sicer dobrodošel, a organizacije potrebujejo mehanizme, s katerimi omejijo škodo ob napadu oziroma odstranijo posledice vdora in storilce iz sistemov.

Ti napadi so zapleteni, uporablja se skrbno načrtovana škodljiva koda, trojanci, virusi, spletna napajališča ... Napadalci najprej vdrejo v strežnike, ki jih obiskujejo državni uporabniki, in podtaknejo zlonamerno kodo. Njena analiza zahteva določena znanja. Za obrambo so potrebni čas in sposobni ljudje, predvsem ti. Nič ne pomaga nakup bleščečih škatel, če jih ne zna nihče uporabiti. Ljudje so temelj varnosti. Oni vedo, kako sistem deluje in kako ga zavarovati.

▶ Pa je Slovenija pogosto tarča takih napadov?

Toliko kot druge države. Čeprav smo majhni, nismo nezanimivi. Četudi ne izdelujemo letal, smo še vedno zanimivi, saj smo člani EU in Nata. Če smo mi šibki člen, predstavljamo nevarnost tudi za ostale države članice, zato ne smemo dovoliti, da bi bili odskočna deska do zanimivejših sistemov. Vpeti smo v evropska omrežja, kjer poteka izmenjava občutljivih podatkov in dokumentov. Tudi vemo, kdaj smo tarča napadov. SI-CERT je v preteklosti obravnaval različne napade na državni ravni. Bojim se, da se bo kmalu ponovil scenarij iz leta 2009, ko smo predsedovali Evropski uniji. To čast bomo znova imeli v 2021, zato pričakujem, da bomo takrat še večja tarča kot sicer in da bo število državnih napadov zelo poraslo.

▶ Sloveniji že sicer primanjkuje kompetentnega kadra, na tem seznamu so tudi varnostni inženirji. Za kakšen primanjkljaj gre in kako ga zmanjšati oziroma odpraviti?

Ni natančnih raziskav o tovrstnih potrebah industrije in javnega sektorja. Empirično pa je očitno, da tovrstnega kadra primanjkuje. Težava je že v tem, da se varnostni strokovnjaki enačijo z informatiki, toda menjava tonerja in papirja v tiskalniku ni enaka reverznemu inženiringu virusa. To zahteva izkušenega strokovnjaka. Kibernetska varnost je specializacija, kjer štejejo izkušnje. Te dobiš z leti dela. Analiza virusa zahteva izkušnje – preizkus na različnih vzorcih, da vidiš, kaj ti orodje omogoča, in da znaš dobiti rezultate. Vsekakor je del težave dejstvo, da imamo premalo specializiranih študijskih programov, kibernetsko varnost je dolgo zanemarjala tudi država pa tudi zasebni sektor v preteklosti ni čutil potrebe po tovrstnem kadru. V situaciji, ko večina podjetij na varnost gleda kot na strošek, je povpraševanja zato manj, manj je tudi naravnega razvoja.

▶ Kaj pa SI-CERT lahko stori na tem področju?

SI-CERT si prizadeva ohranjati visoko raven varnosti, kolikor ga v svoji omejeni vlogi lahko. Naša skrb je predaja znanja. Za kibernetsko varnost usposabljamo vojsko, vladni CERT, sodelujemo z upravo za jedrsko varnost, bančnim sektorjem … A smo le kamenček v velikem mozaiku.

▶ Kaj lahko na področju izobraževanja kadra s področja informacijske varnosti naredijo domače fakultete?

Vsekakor več, kot trenutno počno. Znanje v Sloveniji obstaja, tudi denar. Neka varnostna raven v izobraževalnih ustanovah je vzpostavljena, čeprav le osnovna. Jaz in moji kolegi redno predavamo na fakultetah po državi in študente učimo o našem delu, tehničnih značilnostih in izkušnjah, bi pa slovenske izobraževalne ustanove na področju kibernetske varnosti potrebovale dodaten pospešek.

▶ Naj ustrezen kader vzgajajo kar podjetja sama? Marsikatero namreč to danes že počne.

To počno predvsem tista podjetja, ki se z informacijsko varnostjo že sicer ukvarjajo. Ta vzgajajo kader podobno kot mi – ob pomoči tečajev v tujini in prek internih mentorstev. Ker pač ni na voljo nič drugega.

▶ Kako pa bi zajezili odtekanje možganov, med katerim je vedno več informatikov in varnostnih strokovnjakov, v tujino?

Težavo vidim v rigidnosti sistema, v tem, da je zelo težko pokazati na krivca. Slika se zamegli, zato se ne gradi na preventivi. Je pa tudi res, da je Slovenija dovolj stabilno okolje, zato velikega bega možganov čez noč ne pričakujem.

▶ So varnostni strokovnjaki pri nas cenjeni in dobro plačani?

Varnostni strokovnjaki so sicer cenjeni, a niso ustrezno plačani.

▶ Zanimiv trend predstavljajo varnostno-operativni centri, ki jih je tudi v Sloveniji vedno več. Kakšna je njihova vloga?

Njihova vloga je skrb za kibernetsko varnost. V preteklosti smo varnostno-operativne centre (VOC) našli predvsem v velikih podjetjih in sistemih, npr. operaterjih, kjer so skrbeli za zaščito in odzivanje na varnostne dogodke. VOC pa vse bolj postaja tudi storitev, ki jo specializirani ponudniki nudijo drugim podjetjem.

▶ Pa VOC v praksi deluje?

Ne vemo še. Nismo še na točki, da bi lahko rekli da ali ne. Ideja je smiselna, trg bo pa pokazal, ali bodo VOC zaživeli.

▶ Bomo kdaj priče panožnim VOC?

Ti so na ravni ideje. Gre za teoretični pristop. Vprašal bi se, ali so sploh potrebni. Je pri omrežnem napadu sploh pomembna panoga? Značilnosti napada so enake ne glede na to, ali napadalec pridobi dostop do sistemov v banki ali elektrarni. Mar rabimo panožne gasilce?

Leta 2021 bomo spet predsedovali Evropski uniji, zato pričakujem, da bo takrat število državnih napadov zelo poraslo.

▶ Storitev VOC si vendarle ne more privoščiti vsako podjetje. Kaj naj storijo manjša podjetja, da varnostno letvico dvignejo više?

Predvsem to, da se pozanimajo o najpogostejših tveganjih pri delovanju na spletu in osnovnih zaščitnih ukrepih. Program SI-CERT Varni na internetu prav malim podjetjem daje jasne in enostavne napotke, kako zmanjšati tveganja. Podjetja osveščamo o aktualnih nevarnostih, saj na podlagi prijav, ki jih prejemamo, vemo, da so trenutno v porastu direktorske prevare, vrivanje v poslovno komunikacijo itd.

▶ Pa vaše napotke upoštevajo?

Kakor katero. Težava je v tem, da dostikrat nimamo sogovornika na drugi strani. Večina podjetij se svojih napak in slabih praks sploh ne zaveda. A sem optimist – osnova varnostna higiena vendarle ni zapletena.

▶ Za kakšne slabe prakse gre?

Za takšne, da podjetju sošolec direktorjevega sina postavi spletno stran. To, posebej pa spletno trgovino, je treba dati v izdelavo podjetju, ki se s tem ukvarja. Tudi skladišče podjetju postavi gradbeno podjetje in ne sinov prijatelj, ki študira arhitekturo. Veliko slabih praks je tudi na področju varnostnih kopij. Tudi tisti, ki jih izdelujejo, pogosto nimajo ustreznega scenarija varovanja pred požarom poslovnega prostora ali pa napada z izsiljevalskim virusom.

▶ Kako te izzive odpraviti?

Zgolj z izobraževanjem zaposlenih. Ti se morajo zavedati, da ne smejo kar povprek klikati priponk v elektronski pošti, računovodkinja mora vedeti, da se ne sme slepo odzvati na e-pošto z zahtevkom po nakazilu večjega zneska itd.

▶ Kdo in kako naj skrbi za informacijsko varnost v podjetju?

Direktor za informacijsko varnost, t. i. CISO. Žal ga premorejo samo velika podjetja, zato skrb za informacijsko varnost pogosto pade na šefa informatike.

▶ Na področju varnosti se veliko govori o tehnologijah s področja umetne inteligence. Kakšen je njihov domet, kako lahko izboljšajo informacijsko varnost?

Za zdaj veliko poslušamo in beremo o tem, konkretnih rezultatov pa je precej manj. Marsikaj se v svetu varnosti prodaja kot umetna inteligenca. Paziti moramo, ali gre samo za marketinški prijem ali pa se za varnostno rešitvijo skriva res inovativen mehanizem. Ob lastnih pogovorih s strokovnjaki za umetno inteligenco še nisem zaznal resnično učinkovite rešitve. Skoraj vsi ponudniki varnostnih rešitev obljubljajo, da bodo njihove rešitve prepoznale nove grožnje, še preden bi se te realizirale. Menim, da je to velika puhlica. Dokazov še ni. Menim, da je za zdaj umetna inteligenca precej bolj učinkovita na drugih področjih kot pa pri zagotavljanju kibernetske varnosti. ◀

HEKERJI

- Hekerji, krekerji ali zgolj kriminalci?
- Beli klobuki
- Luknje naprodaj
- Ukradena družba
- Kar zna Sova, zna tudi Android
- Smo varni pred hekerskimi napadi?

Hekerji, krekerji ali **zgolj kriminalci?**

Že o računalnikarjih krožijo v javnosti zelo popačene podobe, še slabše pa je poznavanje hekanja. K temu ne pripomore dejstvo, da termina ni ne v slovenski zakonodaji ne v standardnih slovenskih slovarjih. Če dodamo še vrsto sorodnih pojmov, kot so na primer krekerji, je zmeda popolna. Kaj sploh je hekanje in kdo so hekerji? So to dobri ali slabi fantje in dekleta? In zakaj so nekateri aktivisti?

Matej Huš

Besedo heker najdemo celo v dveh slovenskih slovarjih. Najnovejša inačica SSKJ označuje, da je heker oseba: 1. ki vdira v tuje računalniške sisteme in 2. ki z navdušenjem spreminja programsko opremo. V pogovornem jeziku nestrokovnjakov z besedo heker največkrat poimenujemo zlonamerne napadalce, ki vdirajo v računalniške sisteme z namenom povzročanja škode. A ni bilo vedno tako.

Izraz heker izvira iz angleščine (*hacker*). V 60. letih so ga popularizirali študentje na ameriški univerzi MIT, ki so se ukvarjali z računalništvom. Prvikrat se je v modernem smislu pojavil že v zapisniku sestanka aprila 1955. Prvotni pomen je obsegal delo pri tehničnem problemu, običajno zunaj običajnih postopkov ali navodil. Ko se je izraz začel širiti, je kmalu označeval zelo spretne posameznike, ki so obvladali računalniške jezike, denimo Fortran ali zbirnik. V začetku sta bila izraza heker in hekati vsaj nevtralna, če že ne pozitivna. Še danes izraz *hek* na MIT pomeni domiselno, izvirno in tehnično dovršeno potegavščino, ki sodi med tradicijo in nima povezave z računalništvom.

V računalniškem slovarju *The Jargon File* iz leta 1975 pa ima beseda heker že osem pomenov, med katerimi je prvih sedem pozitivnih. Le zadnjih pomen opisuje človeka, ki poskuša odkriti občutljive informacije z nepooblaščenim brskanjem. Ob zapisu je opomba, da se takemu človeku pravilno pravi kreker (*cracker*). Več o moderni terminologiji pa v okvirju.

Prvotni hekerji so se lotevali telefonskih omrežjih, kjer je bil cilj opravljati medkrajevne klice brezplačno, za ceno lokalnih ali pa stroške prevaliti na drugo organizacijo. Zanje se je razvil izraz *phreakers* in označuje subkulturo ljudi, ki raziskujejo, eksperimentirajo in vdirajo v telefonske sisteme. V preteklosti so, na primer, z vzvratnim inženiringom ugotovili tonske sisteme central in preusmerjali klice tako, da so medkrajevno klicali za celo lokalnih klicev. Ko so uvedli digitalne računalniške sisteme, so *phreakerji* hitro ostali brez prvotnega posla. Hekerji so se preusmerili na računalnike.

Računalniški kriminal

Hekerje povezujemo z računalniškim kriminalom, ki je prerasel nekdanje romantično in neškodljivo vdiranje v državne, vojaške ali univerzitetne sisteme. To je precej netočno, saj le manjši del svoje znanje izrablja za povzročanje škode, je pa računalniški kriminal danes postal zelo razširjen in raznolik, v nekaterih primeri pa sploh ne uporablja hekerskih znanj. Socialni inženiring izkorišča dejstvo, da je pogosto najšibkejši varnostni člen. Ljudje si gesla zapisujejo na liste papirje, občutljive

Tekmovanja

Hekerji, vsaj tisti s srcem na pravi strani, se udeležujejo tekmovanj, med katerimi je najbolj znani *Pwn2Own*, ki od leta 2007 poteka v Vancouvru ob robu konference *CanSecWest*. Prireditelji vsako leto razpišejo programsko in strojno opremo, v kateri bodo hekerji iskali ranljivosti, ter nagrade, ki jih prispevajo pokrovitelji.

Hekerske skupine več mesecev pred dogodkom začno iskati ranljivosti in pripravljati napade, potem pa imajo na tekmovanju nekaj časa (običajno pol ure), da demonstrirajo vdor v tekmovalno napravo. Vrstni red nastopa žrebajo in tisti, ki mu prvemu uspe vdreti, dobi nagrado v višini nekaj tisoč dolarjev (odvisno od resnosti ranljivosti), v zameno pa mora ranljivost podrobno razkriti proizvajalcu. Tekmovalci se pogosto pridušajo, da so nagrade bistveno premajhne, da bi se jim izplačalo razkriti najhujše luknje, saj lahko na sivem trgu zanje iztržijo bistveno več, o čemer pišemo v sosednjem članku.

▽ **Zmagovalci lanskega Pwn2Own: Georgi Geshev, Fabi Beterke, Niklas Baumstark, Samuel Groß, Richard Zhu, Alex Plaskett. Slika: Zero Day Initiative.**

dokumente z osebnimi podatki nezaščiteno mečejo v smeti in verjamejo elektronskim sporočilom ter na lažnih spletnih straneh vpisujejo svoja gesla.

Med računalniški kriminal danes sodijo kraje identitete, razkrivanje osebnih podatkov, nezakonito širjenje avtorskih del (programska oprema, glasba, filmi …), zloraba plačilnih kartic, vdiranje v elektronsko bančništvo, napadi DDoS, pošiljanje spama, hekanje bankomatov, izsiljevalski napadi s šifriranjem programske opreme, prisluškovanje in vohunjenje, uničevanje strojne opreme (prepisovanje firmwara), širjenje neresničnih informacij in lažnih novic itd.

Nekateri zlonamerni hekerji delujejo samostojno, drugi se povezujejo v bolj ali manj tesne hudodelske združbe, tretji pa delajo za vojsko in državne agencije. ZDA, Kitajska, Rusija, Južna in Severna Koreja so znane po tem, da imajo v svojih oboroženih silah organizirane hekerske oddelke. Ti se ukvarjajo s krajo informacij, prisluškovanjem, sabotažami in z onesposabljanjem konkurenčne opreme. Prvi nas je na to opozoril virus Stuxnet za sabotažo iranskih centrifug za bogatenje urana, ki je bil delo izraelskih in ameriških hekerjev. Desetletje pozneje je dejstvo, da imajo najboljše hekerje, največ opreme in največ denarja ravno države, postalo samoumevno.

Dobre plati

Kakor je koristno, da znajo ključavničarji vlomiti ali gasilci sneti vrata, tako so tudi veščine hekerjev lahko koristne. Dobra varnostna praksa je, da se pred komercialnim zagonom občutljivega sistema, ki mora biti čim bolj odporen proti manipulacijam in kjer so lahko njihove posledice hude, v sistem namenoma poskusi vdreti. Švicarji nameravajo letos prvikrat na zveznih volitvah glasovati elektronsko, zato so razviti sistem postavili na ogled in k napadu povabili hekerje. Kodo, ki poganja sistem, so javno odprli, potem pa ponudili za 150.000 švicarskih frankov nagrad. Mesec dni pozneje je bilo že jasno, da je koda precej luknjičasta. Neodvisni raziskovalci so odkrili, da bi bilo mogoče spreminjati glasove, ne da bi za tem ostajala sled. Švicarska pošta, ki je sistem naročila pri španskem podjetju Scytl, je dejala, da gre za starejšo ranljivost, ki pa jo zaradi napake v popravku še niso odpravili. Švicarska vlada se je odzvala z izjavo, da sistem še ne izpolnjuje pogojev za uporabo. Ni še jasno, ali bodo jeseni Švicarji glasovali elektronsko ali ne.

Poleg hekerskih tekmovanj in odprtih akcij iskanja ranljivosti imajo številni proizvajalci programske opreme stalno odprte razpise (*bug bounty*), s katerimi nagrajujejo vse odkrite in odgovorno prijavljene ranljivosti v svoji programski opremi. Podjetja so pač ugotovila, da je to ceneje kakor redno zaposlovati kopico hekerjev, ki bi bdeli nad kodo. In etični hekerji, ki so zaposleni v podjetjih, se običajno raje poimenujejo varnostni strokovnjaki, sistemski inženirji, omrežni administratorji, arhitekti omrežji in podobno. Kot na ostalih področjih IT je tudi tu pomembneje, kaj znaš, kot pa, kako se imenuješ.

Največje združenje hekerjev je evropski *Chaos Computer Club* (CCC), ki je registriran v Nemčiji, ima pa več kot 7.700 članov iz nemško govorečega dela Evrope. CCC se zavzema za več transparentnosti, prost dostop do informacij, pravico do komuniciranja, uporabo odprte kode, univerzalen dostop do računalnikov in etično hekanje. Gre za eno najpomembnejših in najvplivnejših organizacij, ki organizira dogodke in konference s področja varnosti, pripravlja tožbe in kampanje, večkrat nastopa kot strokovni izvedenec na nemških sodiščih ipd. Vsakoletni *Chaos Communication Congress* je največje srečanje hekerjev oziroma varnostnih strokovnjakov v Evropi.

Etični hekerji so pomemben steber računalniške varnosti, ki imajo tudi svoj kodeks, o čemer pišemo v sosednjem članku. Njihovo gibanje pa prerašča okvire zgolj računalniške varnosti in se zavzema za širok spekter pravic ter transparentnosti, ki so povezane z dandanašnjim digitalnim svetom. Boj za odprto programsko opremo, spoštovanje standardov, dobre prakse programiranja in varnostnega projektiranja je pomembnejši kot kadarkoli. ◀

Heki na MIT

Na slavnem *Massachusetts Institute of Technology*, kjer so besedo heker popularizirali in prinesli v širšo zavest, so heki del kulture. Gre za praktične potegavščine, s katerimi dodiplomski študentje pokažejo svoje sposobnosti, inteligentnost in praktičnost. Dolga desetletja je uradni muzej MIT imel tudi sobano hekov, kjer so predstavljali najboljše.

Znameniti heki vključujejo premik policijskega avtomobila na streho glavne stavbe kampusa, »preobleko« te stavbe v gigantskega robota R2-D2, postavitev replike Wrightovega letala v naravni velikosti, postavitev obrnjene (viseče) sobe s pohištvom pod zunanji obok stavbe in še številne druge potegavščine. Na spletni strani hacks.mit.edu natančno dokumentirajo vsakoletne heke.

▽ **Aprila 2010 so študentje na MIT postavili na glavo obrnjeno dnevno sobo. Slika: Andrew Whitacre**

Hekerski leksikon

Hekerji (*hacker*) so posamezniki, ki iščejo in uporabljajo ranljivosti v računalniških sistemih ali omrežjih, da dobijo dostop do njih. Običajno so to zelo usposobljeni posamezniki. Delijo se na dobre in slabe fante (in dekleta).

Etični hekerji (*white hats*) po pisnem naročilu lastnikov sistemov poskušajo vdreti vanje, da bi našli ranljivosti, ki jih potem lastnik zakrpa.

Kreker (*cracker*) so hekerji, ki uporabljajo svoje sposobnosti za nezakonit dostop in za lastno korist, denimo za krajo podatkov, denarja itd.

Script kiddie je slabšalni izraz za zlonamerne hekerje, ki nimajo znanja, temveč uporabljajo zgolj že pripravljena orodja, ne da bi razumeli njihovo delovanje.

Hektivisti (*hacktivist*) so hekerji, ki vdirajo, da bi svetu predstavili sporočilo. Običajno vdirajo v spletne strani in širijo družbene, politične ali verske nazore.

Phreakerji, ki so bili nekoč bistveno bolj razširjeni kakor danes, izkoriščajo varnostne luknje v telefonskih sistemih.

Beli klobuki

Niso vsi hekerji kriminalci, ki želijo konec sveta, kot ga poznamo, ali, danes še pogosteje, mastno zaslužiti. Hekerji, ki se držijo etičnega kodeksa, delajo v dogovoru ter svoja odkritja odgovorno delijo s proizvajalci programske in stroje opreme, so v resnici izjemno pomemben člen informacijske varnosti. Prijelo se jih je ime beli klobuki.

Matej Huš

Avtomobilska industrija že dolgo vrsto let razbija in zaletava nove avtomobile, da bi preverila njihovo varnost. To navsezadnje od njih zahtevajo tudi regulatorji, saj lahko le tako nedvomno pokažejo, kaj se zgodi ob nesreči. Nenavadno je, da je trajalo desetletja, da si je to spoznanje utrlo pot tudi med informacijske sisteme. Njihovo varnost in odpornost bomo najučinkoviteje preverili tako, da bomo hekerji povabili k vdorom.

Hekerje, čeprav formalno ta izraz v slovenski zakonodaji sploh ne obstaja, delimo v tri velike skupine: bele, sive in črne. Simbolika izvira iz ameriških vesternov, v katerih so dobri liki pogosto nosili svetle klobuke, negativci pa temne. Kdo se je prvi spomnil uporabiti to terminologijo za računalniške hekerje, ni povsem jasno. Richard Stallman, ki mu pogosto pripisujejo prvo uporabo tega izraza, to zanika, ker sam sploh ne odobrava besede heker. Izraz *etični heker* pa je prvikrat uporabil podpredsednik IBM John Patrick leta 1995, čeprav je koncept starejši.

Beli, sivi in črni klobuki

Črni klobuki so hekerji, ki nimajo nobenih plemenitih namenom. V sisteme vdirajo po lastni volji in z nezakonitimi motivi. V najboljšem primeru želijo zgolj dokazati svoje sposobnosti in cilj ni povzročiti škode, a tudi to sodi med nezakonito vdiranje. Drugi črni klobuki pa vdirajo bodisi zaradi materialnih koristi bodisi zgolj za povzročanje škode. Rezultat vdiranja koristi njim.

Sivi klobuki so hekerji, ki so v spektru zakonitosti nekje v sredini. Njihov cilj ni povzročati škode, a vseeno vdirajo nepovabljeni in iz lastnih vzgibov. Morda imajo dobre namene, a odkritih ranljivosti ne razkrijejo upravljavcu. Ravnajo se po lastnem moralnem kompasu, ki je včasih bolj, včasih pa manj poravnan z zakonodajo.

Hekerje, čeprav formalno ta izraz v slovenski zakonodaji sploh ne bstaja, delimo v tri velike skupine: bele, sive in črne.

Tretja skupina so beli klobuki ali etični hekerji. To so strokovnjaki, ki vdirajo v sisteme zgolj z dovoljenjem, s povabilom ali v dogovoru z lastnikom sistema. Odkrite ranljivosti odgovorno delijo z lastnikom sistema, njihovo početje pa je ves čas na prvi strani zakona. Seveda so za svoje dejanje tudi primerno finančno nagrajeni. Rezultati vdiranja koristijo naročniku, torej »tarči«.

Biti etični heker pa ni enostavno, saj je treba poznati zakonodajo in spoštovati etični kodeks, sicer se lahko tudi dobronamerni etični heker spremeni v neetičnega. Klobuki se hitro umažejo.

Dogovor

Pri tako občutljivi stvari, kot je vdiranje v informacijski sistem, je zelo priporočljivo, da je dogovor pisen. V njem se morata naročnik (oziroma »tarča«) in heker dogovoriti o več stvareh. Najprej se je treba dogovoriti, kaj je cilj vdora in v kolikšnem obsegu ter katere tehnike napada bodo uporabljene. V primeru prekoračitve tega obsega namreč preizkus varnosti postane navaden vdor.

Zelo pomembno je določiti, koga in kdaj je treba seznaniti z izsledki. Ta seznanitev mora biti izčrpna, torej mora omogočati zakrpanje luknje. Etični heker odkritih ranljivosti ne sme razkrivati tretjim osebam, razen če mu po odpravi ranljivosti naročnik to dovoli – denimo na kakšni konferenci. Odveč je poudariti, da mora biti naročnik lastnik informacijskega sistema in da mora imeti pravico, da sploh odobri vdiranje.

To ni tako nepomembna opomba. Nekatere licenčne pogodbe za program ali infrastrukturo (na primer v oblaku) ne dovoljujejo samovoljnega vdiranja, četudi je naročnik uporabnik. V takem primeru bi šlo vseeno za nepooblaščeni dostop. Druga zelo pomembna točka pa so osebni podatki, do katerih bi etični heker pri svojem delu lahko imel dostop. Vpogled v zasebno komunikacijo zaposlenih, njihove osebne podatke in podobno je nezakonit. Ker upravljavec informacijskega sistema niti sam nima splošne pravice do dostopa do teh podatkov, je seveda ne more podeliti etičnemu hekerju. Tudi kadar heker teh podatkov ne prebira, je treba paziti na morebitno odtekanje iz EU. Strežniki v tujini večinoma niso primerni za hranjenje osebnih podatkov.

Zakonodaja

Etični heker mora poznati zakonodajo s področja zasebnosti posameznika, varovanja osebnih podatkov in vdiranja v informacijske sisteme. Ne glede na dogovor med naročnikom in etičnim hekerjem se mora ta zakonodaja spoštovati.

Tajnost občil, ki jo zagotavlja večina držav na svetu (Slovenija konkretno v 139. členu kazenskega zakonika, splošno pa tudi v ustavi), prepoveduje neupravičeno seznanitev s sporočili, ki se prenašajo elektronsko. Kazen je predpisana tudi za osebo, ki komu omogoči to neupravičeno seznanitev (v našem primeru torej tudi naročnik). V 137. členu sta izrecno prepovedana

Zgodi se, da hekerji posredujejo ustrezne informacije, potem pa se v najboljšem primeru ne zgodi nič.

neupravičeno prisluškovanje in zvočno snemanje, v 143. členu pa še zloraba osebnih podatkov, kamor sodi tudi vdor v računalniško vodeno zbirko podatkov.

V praksi se ta problem rešuje tako, da se preizkusi z vdiranjem opravljajo na kopijah produkcijskih informacijskih sistemov, ki ne vsebujejo osebnih (ali kakršnikoli drugih pomembnih) podatkov. Običajno se vdiranje naroči, preden je sistem implementiran, lahko pa se seveda tudi kasneje, zlasti ob večjih nadgradnjah.

Drugi problem so licenčni pogoji proizvajalcev programske opreme, ki pogosto prepovedujejo vdiranje, četudi bi šlo za naročene preizkuse. V takih primerih je treba pred naročilom pridobiti dovoljenje. Tega ne more storiti etični heker, temveč naročnik. Seveda pa se mora etični heker pozanimati, ali je naročnik pridobil ustrezna dovoljenja.

Kazenski zakon v 221. členu tudi določa, da je neupravičen vstop ali vdor v informacijski sistem ali prestrezanje podatkov kaznivo in lahko pomeni do enega leta zapora. Če pri tem storilec povzroči škodo (kakršnokoli uporabo, spremembo, kopiranje, uničenje podatkov ali dodajanje vnosov), je zagrožena kazen tudi do petih let zapora. Podobno zakon sankcionira tudi zlorabo informacijskega sistema pri gospodarskem poslovanju (237. člen).

Zanimiv je še 306. člen, ki ureja izdelovanje in pridobivanje orožja ter pripomočkov za izvajanje kaznivih dejanj. Prepovedani so izdelovanje, posest, prodaja, uvoz, izvoz in druge oblike zagotavljanja pripomočkov za vdor ali neupravičen vdor v informacijski sistem, če se to počne z namenom storitve kaznivega dejanja.

Odgovorno razkrivanje

Etični hekerji se običajno držijo svojega kodeksa, ki poleg spoštovanja zakonodaje vsebuje še nekaj častnih zavez. Ena izmed najpomembnejših je odgovorno razkrivanje ranljivosti. Pogosto se namreč zgodi, da etični hekerji ne vdirajo v noben poseben sistem, temveč odkrijejo kakšno ranljivost v običajni programski opremi, ki jo uporabljajo ljudje. Odkritje ranljivosti v Microsoftovem Officeu, Adobovem Flashu ali Applovem iOS seveda ni nezakonito, če heker preizkuša lastne sisteme. Toda ko enkrat odkrije takšno informacijo, jo mora posredovati avtorju programa. Večina večjih programskih hiš ima odprte stalne razpise za nagrajevanje odkritih ranljivosti (*bug bounty*) v svoji programski opremi. Hekerji, ki pošljejo natančen opis ranljivosti, si lahko obetajo nekaj deset tisoč dolarjev. Šele ko je izdan popravek, imajo hekerji pravico razkriti to ranljivost javnosti.

Žal so tudi med proizvajalci programske opreme gnila jajca. Zgodi se, da hekerji posredujejo ustrezne informacije, potem pa se v najboljšem primeru ne zgodi nič, v najslabšem primeru pa hekerja obtožijo vdiranja in ga sodno preganjajo. Če etični heker odkrije resno ranljivost in je proizvajalec kljub opozorilu ne popravi, je včasih upravičeno to informacijo priobčiti svetu. Koliko časa mora heker čakati, ni nikjer določeno. Nekako pa velja, če se niti po šestih mesecih nič ne premakne, lahko heker z javno objavo ustvari javni pritisk na podjetje, da luknjo zakrpa. Včasih si tako nagajajo celo podjetja. Google meni, da je 90 dni dovolj, zato nekritično objavlja vse ranljivosti po 90 dneh od odkritja, kar je Microsoft v preteklosti že močno ujezilo. Postopek priprave popravka namreč lahko traja dlje.

Čedalje popularnejši poklic

Biti etični heker postaja čedalje pogostejši poklic, ki pa ga pestijo težave prekarnosti. Razen največjih podjetij, ki zaposlujejo lastne bele klobuke ali redno sodelujejo s strokovnjaki za varnost, so čedalje pogostejši *bug bountyji*. Podjetja ugotavljajo, da je ceneje razpisati nagrade za odkrite ranljivosti kakor pa redno zaposlovati strokovnjake, ki bi preverjali varnost sistemov. Te nagrade niso pretirano visoke, podjetja pa pogosto iščejo izgovore, zakaj bi jih znižala (»ranljivost ni tako resna«) ali sploh ne bi izplačala (»za ranljivost že vemo, samo odpravili je še nismo«).

Zato postanejo mikavne ponudbe sivih igralcev (denimo podjetja Zerodium), ki prekupčujejo z ranljivostmi in si lahko privoščijo za luknjo v iOS plačati tudi pol milijona dolarjev. To pa je že tema naslednjega članka. ◀

HEKERJI

Spreobrnjenci

Niso tako redke zgodbe o hekerjih, ki so v mladih letih delovali onkraj zakona, kasneje pa so se spametovali, odslužili svoj dolg družbi in zdaj svoje znanje uporabljajo v njeno dobrobit. Najbolj znani primer je Kevin Mitnick, ki se je že kot najstnik lahko zastonj vozil z mestnimi avtobusi. Pri 16 letih je vdrl v računalniški sistem DEC, kasneje pa je našel pot v več deset informacijskih sistemov. Po odmevni aretaciji leta 1995 je bil obsojen zaradi več kaznivih dejanj. V zaporu je preživel pet let. Danes je eden najbolj znanih hekerjev, vodi podjetje za računalniško varnost in je svetovalec za največja podjetja.

Kevin Poulsen je bil v mladih letih heker, ki mu je uspelo vdreti v vojaški Arpanet in številna druga omrežja. Ko so ga ujeli pri 17 letih, je dobil le opozorilo, a ni zaleglo. Ko so ga želeli aretirati v drugo, je leta 1989 izginil, a so ga naslednje leto prijeli. Po petletni zaporni kazni in še triletni prepovedi uporabe računalnikov ali interneta je postal novinar, ki med drugim piše tudi za Wired.

Robert Tappan Morris je znan kot avtor virusa Morris Worm, ki je bil leta 1988 prvi internetni virus. Leta 1990 je bil obsojen na tri leta zapora, danes pa je profesor računalništva na MIT in uspešen podjetnik.

Vsi trije opisani (seveda so še druge zgodbe) so danes v 50. letih. Tovrstne zgodbe so dandanes redkejše, ker so kazni za hekerje strožje. Če so jo včasih odnesli z nekaj leti zapora, danes 20-letne zaporne kazni (zlasti ko gre za vdore v državne informacijske sisteme) niso nič nenavadnega. Zato mlajših hekerjev, ki bi sneli črni klobuk, skorajda ni. Današnji mladi etični hekerji so etični že od samega začetka.

▽ **Adrian Lamo, Kevin Mitnick, Kevin Lee Poulsen. Slika: Matthew Griffiths/v javni lasti**

Luknje naprodaj

Niso vsi hekerji plemeniti aktivisti, ki se zavzemajo za transparentnost in varnost ter vse ranljivosti javijo proizvajalcem in podrobnosti ne razkrivajo svetu, dokler niso popravljene. Niti niso vsi hekerji manijaki, ki želijo onesposobiti jedrske elektrarne in prebirati vojaške skrivnosti na domačih računalniki. Nekateri so zgolj oportunisti, ki odkrivajo in prodajajo varnostne ranljivosti, ki jih različne organizacije, države in kriminalno podzemlje bogato odkupujejo.

Matej Huš

Pred štirimi leti je neimenovana hekerska skupina našla ranljivost v Applovem operacijskem sistemu iOS 9, ki je omogočala oddaljeni predvsem nadzora (in s tem tudi *jailbreak*) brez uporabnikove interakcije ali vednosti. Za svoje odkritje so bili nagrajeni z okroglim milijonom dolarjev, ki pa jih ni izplačal Apple, neprofitna organizacija ali nemara kakšna država, kot bi pričakovali. Nagrado je izplačalo zasebno podjetje Zerodium iz Washingtona, ki se ukvarja s kupovanjem, z zbiranjem in s preprodajo ranljivosti v programski opremi. Zerodium ranljivosti namreč še dražje prodaja naprej.

To ni bil prvi tovrstni primer. Leto pozneje je Zerodium za delujoč vdor v iPhone ponudil že poldrugi milijon dolarjev. Bogato nagrajujejo tudi ostale ranljivosti, denimo za neopazen vdor v Android so ponujali 200.000 dolarjev, za že tako luknjičav Flash 80.000 dolarjev. Zerodium je bilo prvo podjetje, ki je leta 2015 javno objavilo celoten cenik, po katerem odkupujejo ranljivosti v večini priljubljene programske opreme. V današnji različici cene segajo od 10.000 dolarjev za izvajanje oddaljene kode (*remote code execution*) v Joomli ali phpBB ter do dveh milijonov dolarjev za oddaljeni, trajni *jailbreak* brez uporabnikove interakcije na iPhonu. Na spletni strani imajo v obliki dveh periodnih sistemov objavljenih 70 različnih kategorij, kupujejo pa seveda tudi zanimive ranljivosti za programe, ki jih ni na seznamu. Še pred desetletjem je bila zamisel o prodaji ranljivosti slišati kot znanstvena fantastika, danes pa je postala realnost z nakupovalnega seznama.

▽ **Zerodium je javno objavil cenik za odkup ranljivosti.**

Ranljivosti *zero-day*

Tipična ranljivost ima življenjski cikel, ki ga sestavlja sedem dogodkov. Najprej se ranljivost rodi, ko jo proizvajalec zapiše v programsko kodo. Drugi, zelo pomemben dogodek je njeno odkritje, kar običajno sovpada z razvojem kode (ali pa vsaj delujočega koncepta) za njeno izrabo. Če proizvajalec ni obveščen o ranljivosti, nikoli ne nastopi tretja točka, to je njegova seznanitev z luknjo. Do tega trenutka se ranljivost imenuje *zero-day*, tj. ranljivost ničtega dne, ker proti njej ni učinkovite zaščite in ker je proizvajalcu znana nič dni.

Četrta prelomnica je javna objava ranljivosti, ki ji v petem koraku sledi vnos kode v knjižnice protivirusnih programov ter v šestem koraku izdaja popravka. Življenjska pot ranljivosti se sklene v sedmem koraku, ko uporabniki namestijo popravek oziroma posodobijo programsko opremo. Odgovorno razkritje pomeni, da je javnost o luknji obveščena šele tedaj, ko je proizvajalec že imel čas pripraviti popravek.

Največ so na sivem trgu seveda vredne ranljivosti, katerih obstoja proizvajalci programske opreme ne poznajo (*zero-day*). To pomeni, da ne razvijajo popravka in da lahko ranljivost potencialno izkoriščamo leta. To ni tako neverjetno, kot bi mislili. Leta 2017 so, na primer, v TLS odkrili 19 let staro ranljivost, leta 2010 pa v Windows 17 let staro luknjo v navideznem stroju za DOS. Omenjenih ranljivosti, tako se zdi, niso nikdar aktivno izrabljali, a to ne pomeni, da v današnjih programih ni drugih, starih ranljivosti, ki so jih zlikovci obdržali zase in jih s pridom izrabljajo.

Marsikdo predpostavlja, da je odprta koda zagotovilo, da ranljivosti ni, a to ne drži. Odprta koda pomeni le, da jo lahko vsakdo pogleda, ni pa nujno, da dejansko jo. Razlika je bistvena in kljub odprtosti kode poznamo posebne plačane preglede (*audit*), kot je bil primer odprtokodnega orodja za šifriranje VeraCrypt. Šele odtlej smo lahko resnično prepričani, da je orodje varno.

Če pregleda ni, se lahko zgodi, kar se je odprtokodni knjižnici GnuTLS. V njej so leta 2014 odkrili devet let staro luknjo, v OpenSSL pa zloglasnega hrošča HeartBleed. Bloomberg je pisal, da je luknjo izkoriščala vsaj ameriška agencija NSA, torej je mogoče sklepati, da jo je še kdo drug.

Žal pred ranljivostmi *zero-day* po definiciji ni učinkovitih rešitev, ker zanje ne vemo. Lahko si pomagamo s pasivno zaščito (dobrimi varnostnimi praksami, požarnimi zidovi, primerno segmentacijo sistemov in določanjem privilegijev), dolgoročno pa

△ **Življenjski cikel ranljivosti.**

je še najbolj koristno, če raziskovalce motiviramo, da luknje odkrivajo in odgovorno prijavljajo.

Nagrajevanje najdenih hroščev

Podjetja, ki razvijajo programsko opremo, že zelo dolgo časa vedo, da kompleksne kode brez hroščev in lukenj ni. Kadar gre za varnostne ranljivosti, ki jih pred proizvajalcem odkrijejo hekerji in po jih možnosti začno izrabljajo, to ni le slaba publiciteta, temveč je lahko tudi resen problem. Ena izmed preprostih rešitev je nagrajevanje odkritih in odgovorno prijavljenih ranljivosti. Tem programom se pravi *bug bounty* in jih imajo danes vsa večja podjetja, čeprav ni bilo vedno tako. Dolgo časa so namreč podjetja vrhunske strokovnjake za ranljivosti raje poskušala zaposliti.

Prvi znani program nagrajevanja ranljivosti je imelo podjetje Hunter & Ready že leta 1983. Za prijavljene hrošče v operacijskem sistemu VRTX (Versatile Real-Time Executiv), ki je tekel na vgradnih sistemih, denimo Hubblovem teleskopu, so ponujali Volkswagnovega hrošča pod geslom Hrošč za hrošča.

Množičnejši je bil Netscapov program, ki so ga zagnali leta 1995 in je prvi uporabil frazo *bug bounty*. Na voljo je bilo 50 tisoč dolarjev, ki so jih počasi delili za odkrite ranljivosti v (zdaj že izumrlem) brskalniku Netscape Navigator. Čeprav je to danes vsakdanja praksa, so nekateri vodje v Netscapu programu nasprotovali in inženir Jarrett Ridlinghafer je potreboval dlje časa, da je vse prepričal. Ostala podjetja pa so se temu pristopu ogibala še nekaj let.

Šele na prelomu tisočletja se jih je opogumilo več. Leta 2002 je tak program uvedel iDefense (kot posrednik za ostala podjetja), kmalu sta sledila še Mozilla Foundation in iDefensov konkurent TippingPoint. Ponujali so piškavih 500 dolarjev. Mozillin program teče še danes, vmes pa so zneski narasli do 5000 dolarjev za najhujše ranljivosti. TippingPoint je leta 2005 ustanovil ZDI (Zero Day Initiative), ki poteka danes in, na primer, organizira tekmovanje Pwn2Own, o katerem pišemo v sosednjem članku. Pwn2Own teče od leta 2007 in vsako leto pritegne številne hekerje. Razlog za njegovo ustanovitev je bilo razočaranje nad Applom, ki je včasih malomarno jemal varnost, zato so na prvem Pwn2Own napadali Mac OS X. ZDI je po več lastnikih danes v rokah TrendMicra.

Leta 2010 je Google ugotovil, da bi se izplačalo ponuditi nagrade za prijavljene ranljivosti v Googlovi in Chromiumovi kodi. Tistega leta so nagrade začela razpisovati tudi podjetja, ki se ne ukvarjajo primarno z razvojem programske kode, na primer Deutsche Post. Leto pozneje je sledil Facebook in do danes so se pridružili vsi veliki igralci.

Še leta 2013 je Yahoo menil, da so strokovnjaki pripravljeni delati zastonj in ranljivosti razkrivati povsem altruistično. Septembra tistega leta so v podjetju High-Tech Bridge odkrili vrsto ranljivosti XSS v Yahoojevi kodi, kar so podjetju sporočili. Nagradili so jih s kuponoma za 12,5 dolarja, ki ju je bilo moč unovčiti le v Yahoojevi trgovini z majicami, s skodelicami, čepicami ipd. To je na internetu sprožilo ogromno nezadovoljstva. Kmalu se je oglasil Ramses Martinez, ki je v Yahooju vodil oddelek za varnost, in pojasnil, da uradne politike sploh ni. Majice in kasneje kupone, ker so nekateri majice že imeli, je plačal s svojim denarjem, ker se mu je zdelo prav, da bi poleg uradnega elektronskega sporočila poslal še manjšo pozornost. Do konca leta je Yahoo ugotovil, da bo treba uvesti sistem nagrajevanja s plačilom, in to tudi storil.

Danes finančno nagrado za odkrito ranljivost ponuja več kot 500 podjetij, med katerimi so tudi Microsoft, Mozilla, Intel,

▷ **Prvi znani program za nagrajevanje odkritih hroščev sega v leto 1983.**

ZAKONODAJA

Ali je prekupčevanje z ranljivostmi **legalno**

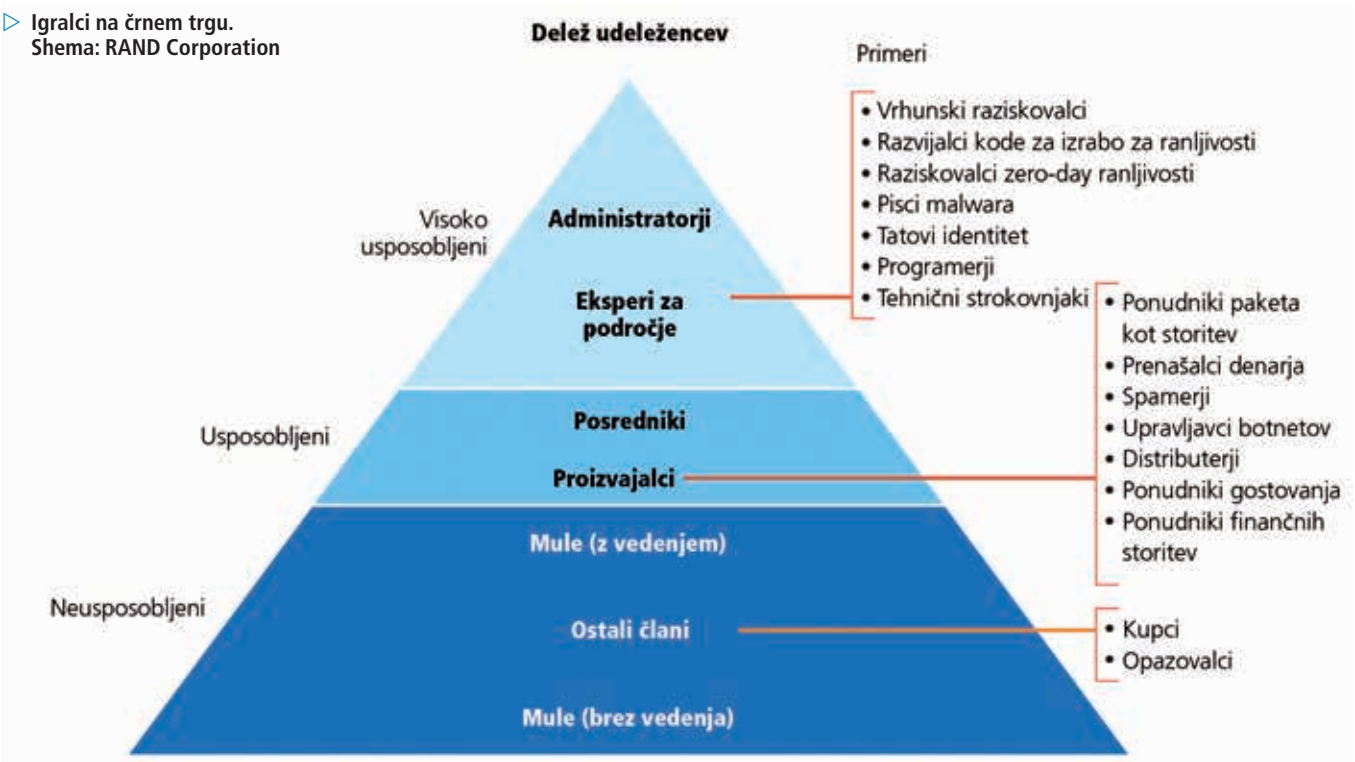
Nepooblaščeno vdiranje v računalniške sisteme je v vsem razvitem svetu prepovedano, tudi pri nas. Slovenski kazenski zakon pa ima tudi zanimiv 306. člen, ki prepoveduje izdelovanje, posest, prodajo, uvoz, izvoz in ostale oblike zagotavljanja pripomočkov za vdor v informacijski sistem, če to počnemo z namenom storiti kaznivo dejanje. Sodne prakse na tem področju v Sloveniji ni.

V ZDA, ki je največji trg programske opreme in tudi ranljivosti, je prodaja informacij o znanih ranljivostih načelno zakonita, a obstaja cel kup izjem. Če ranljivost prodamo nekomu, ki namerava z njo storiti kaznivo dejanje (in v resnici je ranljivosti težko uporabljate kako drugače), je to nezakonito.

Prav tako ni zakonito vdiranje ali izsiljevanje. Kdor odkrije ranljivost in z njo potrka na vrata proizvajalca z zahtevo po nekem znesku (četudi je ta povsem razumen), se hitro lahko znajde v obtožnici za izsiljevanje. Prav tako lahko hekerji hitro prestopijo mejo zakona pri iskanju ranljivosti. Analiza kupljenih programov na lastnih računalnikih je dopustna, aktivno iskanje lukenj v postavljenih tujih sistemih pa seveda predstavlja vdor. Etično in najvarneje je odkrite ranljivosti prijaviti proizvajalcu v skladu z njegovim programom nagrajevanja. Prav tako je nezakonita prodaja narejenih orodij (exploit kits) za vdiranje v računalniške sisteme ali povzročanje škode.

Enostavnega odgovora ni tudi zato, ker lahko prodajalca preganja več držav: država, katere državljan je, država, v kateri izvede prodajo, in država, v kateri je tarča.

▷ Igralci na črnem trgu.
Shema: RAND Corporation



Apache, Apple, Facebook, Google, HP, Twitter, Yahoo in drugi. Tudi višina finančnih nagrad se je zvišala. Microsoft je lani izplačal dva milijona dolarjev, najvišje izplačilo pa je znašalo 200.000 dolarjev. Google je lani izplačal 3,4 milijona dolarjev (skupno pa že 15 milijonov dolarjev), najvišja nagrada je znašala 41.000 dolarjev. Facebook je doslej izplačal 7,5 milijona dolarjev, največja posamična nagrada pa je bila lani 50.000 dolarjev. Včasih nagrade niso finančne. United Airlines je lani podaril milijon milj nizozemskemu študentu, ki je v njegovih sistemi odkril 20 resnih lukenj.

Podjetja so spoznala, da morajo biti s svojimi nagradami konkurenčna prekupčevalcem z ranljivostmi, ki jim ni težko ponuditi več sto tisoč dolarjev, v izjemnih primerih pa tudi milijon ali dva.

Črni trg

Pri prijavljanju napak proizvajalcem po programih *bug bounty* so odkritelji v resnici prepuščeni dobri volji podjetja. To lahko mirno ranljivost razglasi za že znano, manj pomembno ali poišče kakšen drug izgovor, da nagrade ne izplača. V takem primeru se odkritelj nima kam zateči. Da podjetje sploh začne razmišljati o izplačilu, vsi programi *bug bounty* najprej zahtevajo polno razkritje, kakršnokoli pogojevanje tega pa je izsiljevanje in kaznivo. Včasih uspe tudi to, kot na primer leta 2016 neimenovanemu hekerju, ki je z vdorom v Uber dobil podatke o 57 milijonih uporabnikov. V zameno za razkritje ranljivosti *in* izbris svoje kopije podatkov je zahteval 100.000 dolarjev, ki jih je Uber tudi izplačal. A v resnici podjetja v takih primerih največkrat pokličejo organe pregona.

Hekerji se zato pogosto obrnejo na sivi oziroma črni trg. V zadnjih petnajstih letih smo bili priče spremembi v organiziranosti, saj hekerji niso več osamljeni jezdeci, temveč se združujejo v skupine. Tudi trgi so postali učinkovitejši, razmere na njih pa zahtevnejše. Ko so leta decembra 2013 hekerji napadli verigo trgovin Target in ukradli bančne podatke 70 milijonov strank, so se ti v nekaj dneh pojavili na spletnih črnih tržnicah.

Ločiti je treba črni in sivi trg. Prvi so nezakonite tržnice, forumi in druga zbirališča, kjer se prodajajo orodja za vdore, botneti, napadi DDoS, storitve drugih napadov in ukradeno (prijavni podatki, osebni podatki, bančni podatki). Sodelovanje na črnem trgu je nezakonito. Po statistikah RAND Corporation je na črnem trgu 70 odstotkov posameznikov ali majhnih skupin, 20 odstotkov večjih združb, pet odstotkov teroristov, štiri odstotke državnih služb in odstotek aktivistov. V preteklosti je bilo denarno poslovanje večji problem, kjer so pogosto uporabljali mule (posameznike, ki so odstopili svoje transakcijske račune za prejem denarja), dandanes pa to vlogo bolje opravljajo kriptovalute.

Večina igralcev na črnem trgu prihaja iz Kitajske, Južne Amerike in vzhodne Evrope. Po kakovosti prednjači Rusija, zanimiv pa je tudi razrez glede na tarče. Medtem ko se azijske skupine osredotočajo na trgovce, se vzhodnoevropske skupine na finančne institucije. V zadnjem času se meje brišejo, skupine več sodelujejo in se lotevajo tudi področij, ki se jih včasih niso.

Komunikacija, ki je včasih potekala prek IRC, ICQ, Jaberrja, QQ in podobno, se je danes v glavnem preselila na forume, do katerih je dostop mogoč le prek omrežja Tor, in v šifrirane (*end-to-end*) pogovore v aplikacijah za hipno sporočanje. Angleščina tam ni univerzalni jezik, saj obstajajo ločeni forumi za angleško, rusko, kitajsko, nemško, vietnamsko govoreče skupine in druge. Medtem ko je pri vdorih najpogosteje uporabljana ruščina, je pri ribarjenju in drugih tehnikah družbenega inženiringa to angleščina.

O cenah na črnem trgu je težko dobiti realne podatke. Načelno so ti trgi precej *učinkoviti*, kar pomeni, da se cene hitro prilagajajo ponudbi in povpraševanju. Medtem ko posamezne kreditne kartice z visokim limitom stanejo nekaj deset dolarjev in hitro izgubljajo ceno, saj so običajno kmalu preklicane, gredo cene res dobrih ranljivosti v več deset ali sto tisoč dolarjev. Odvisno je od tega, ali se najde pravi kupec.

Zanimivo je, da na črnem trgu

Komponente trgov ranljivosti

Blago: digitalne dobrine z nizkimi stroški distribucije, ki pa ob razkrivanju hitro izgubijo vrednost, a ta ne pade povsem na ničlo.
Valuta: posli se v glavnem poravnavajo s kriptovalutami, redkeje prek ukradenih kreditnih kartic. Vrednost pa je zaradi volatilnosti kriptovalut običajno denominirana v dolarjih.
Trg: črne tržnice ali legalni sivi trg. Na njem pogosto sodelujejo državni organi.
Ponudba: na vrhu piramide sedijo administratorji, pod njimi pa tehnični strokovnjaki, ki jim sledijo posredniki in prodajalci.
Povpraševanje: kriminalci kupujejo na črnem trgu, podjetja in državne službe pa navadno na sivem trgu. Cene so nekajkrat višje od zneskov, ki jih ponujajo proizvajalci za odkrite ranljivosti v lastni kodi.

običajno ni veliko *zero-day* ranljivosti. Te so redke, dragocene in predvsem hitro pokvarljivo blago, saj jih neprevidno razkritje hitro spremeni v znane ranljivosti. Bistveno več pa je na črnem trgu *half-day* ranljivosti. O teh so bili avtorji programske opreme že obveščeni in so morda že izdali popravek, a ga večina uporabnikov še ni namestila. Običajno te ranljivosti, običajen *malware* ali ribarjenje povsem zadostujejo.

Sivi trg

Sivi trgi pa so po definiciji omejeni na legalno izmenjavo informacij o ranljivostih in načinih izrabe. Na njih sodelujejo proizvajalci programske opreme, ki kdaj odkupijo kakšno lastno ranljivost, posredniki (npr. Zerodium), ponudniki orodij za varovanje ter tudi obveščevalne službe in druge državne agencije. Raziskave kažejo, da se vrhunskim hekerjem bistveno bolj izplača prodajati ranljivosti podjetjem na sivem trgu kakor na črnem. Poleg tega, da je možnosti za prevaro bistveno manj, so s tem še na pravi strani zakona, lahko pa dobijo celo kakšno ponudbo za zaposlitev.

Zerodium je medijsko najbolj izpostavljeno podjetje, ki odkupuje ranljivosti, ni pa edino. Pred štirimi leti je zaslovelo že leta 2003 ustanovljeno milansko podjetje Hacking Team, ki se ukvarja s prodajo informacij o ranljivostih in hroščih vladam, organom pregona in podjetjem. Neznani hekerji so namreč vdrli v Hacking Team in na internetu objavili 400 gigabajtov podatkov: elektronsko pošto, račune, izvorno kodo itd. S tem so odstrli dotlej slabo poznan svet prodajanja ranljivosti.

Izkazalo se je, da je imel Hacking Team 70 aktivnih strank, med katerimi so bili tako napadalci kakor podjetja, ki se želijo braniti. Med prvimi so bili, denimo, FBI, CIA, turška policija, mehiška vlada, obveščevalna agencija Savdske Arabije in italijanska policija, med drugimi pa Deutsche Bank, British Telecom, Barclay's Bank itd.

Ko postane ranljivost znana, je v resnici kratek čas še bolj nevarna. Dokler uporabniki ne namestijo popravkov, so še vedno ranljivi. Raziskave pa kažejo, da se tedaj število kosov zlonamerne programske opreme za to ranljivost poveča za vsaj 200-krat, število napadov pa do 100.000-krat.

Uporaba

Motivi iskalcev in prodajalcev ranljivosti so torej jasni. Kaj pa konkretno z ranljivostmi naredijo kupci? NSA je znana po tem, da ranljivosti potihoma skladišči za prihodnjo rabo. S tem posredno ogroža vse, ker programska oprema ostaja nezakrpana, kar se lahko maščuje. To najlepše ilustrira zgodba o ranljivosti SMB, ki jo najdemo pod oznakama CVE-2017-0143 in CVE-2017-0144.

Symantec je letos maja razkril zgodbo o hekerski skupini Buckeye (poimenovana tudi APT3, Gothic Panda), ki najverjetneje dela za kitajsko vlado. Ranljivost je najprej odkrila ali na sivem trgu kupila NSA, najverjetneje pred letom 2016, česar uradno ne priznajo. Marca 2016 je do ranljivosti z vdorom v NSA prišla kitajska skupina Buckeye, ki jo je uporabljala za vohunjenje. Buckeye je ranljivost uporabljala za širjenje prisluškovalne opreme DoublePulsar, ki je nastala v NSA. Ni jasno, kako so jo Kitajci dobili. V poldrugem letu je Symantec po svetu zabeležil vsaj pet velikih vdorov (operaterji, univerze in inštituti v Belgiji, Hongkongu, Luksemburgu, Vietnamu in na Filipinih), kjer so uporabljali luknjo v SMB in DoublePulsar.

Aprila 2017 se je zgodil znameniti hek Shadow Brokers, ko je istoimenska skupina vdrla v NSA in na internetu objavila kopico izvorne kode, med njimi EternalBlue, EternalRomance, EternalSynergy in tudi DoublePulsar. Kako so vdrli v NSA, ni znano; bodisi jim je kodo nekdo predal bodisi so naleteli na zunanji nezaščiten strežnik. Microsoft je šele tik pred tem dobil opozorilo od NSA, da je ranljivost aktivna, in izdal popravek.

Kljub temu je Severna Koreja dva meseca pozneje napisala WannaCry, ki je pustošil po svetu, še mesec dni kasneje pa so Rusi izdelali Mimikatz, ki je v Ukrajini onesposobil 10 odstotkov računalnikov, kmalu pa se je še razširil. Ohromil je velikane, kot so Maersk, FedEx, Merck. Škode je bilo za 10 milijard dolarjev.

NSA je sicer tik pred javno objavo ranljivosti, ko je že bilo jasno, da so jo hekerji odnesli, Microsoftu pomagala zakrpati luknjo, a je bilo prepozno. Vsi računalniki niso bili posodobljeni pravočasno, zato sta se WannaCry in Mimikatz razširila kot ogenj.

Omenjena zgodba je med bolj nenavadnimi, saj običajne ranljivosti nimajo tako burnega življenja. Kaže pa, da je povsem mogoče, da proizvajalec programske opreme ne ve za luknjo, čeprav jo leta uporabljajo številne obveščevalne službe in kriminalci. Z ranljivostmi, ki so resnično poznane le enemu igralcu, je še slabše. Zanje morda nikoli ne izvemo. Vsi, ki skladiščijo ranljivosti za lastno uporabo (ofenzivno ali defenzivno) in o njih ne obveščajo proizvajalcev ter kasneje javnosti, so krivi, da smo vsi manj varni. ◀

Kdo bo koga

Ranljivosti v programski opremi odkrije tudi konkurenca, ki včasih ne izkoristi priložnosti za nagajanje. Posebej živahen odnos imata Microsoft in Google, ki redno odkrivata luknje v kodi drug drugega, potem pa tu in tam kakšno obelodanita, preden jo konkurent zakrpa.

Ni namreč predpisano, koliko časa mora odkritelj ranljivosti dati proizvajalci na voljo za izdajo popravka, preden sme nanj pritisniti tudi tako, da jo javno priobči na svetu. Google meni, da je 90 dni dovolj, in razkriva luknje po treh mesecih, Microsoftu pa včasih ne uspe tako hitro, ker popravki izhajajo enkrat mesečno. Microsoft je potem večkrat Googlu tudi vrnil, ko je izpostavil kakšno ranljivost v kakšni malo starejši (a še vedno izjemno popularni) različici Androida, ki je Google ni želel zakrpati, ker je pač popravljena v novi verziji. Toda na številne telefone najnovejše inačice Androida sploh ni mogoče namestiti.

▷ **WannaCry se je širil z ranljivostjo, ki jo je poznala NSA in so jo v svet odnesli hekerji.**

Ukradena družba

Z razvojem družabnih omrežij so na internet priplavala skladišča osebnih podatkov, kot jih še ni bilo. Z vsemi podrobnostmi naših življenj prostovoljno napolnjeni profili so mikavna tarča za hekerje, ki v številnih primerih sploh ne potrebujejo posebnega znanja. Še največkrat vpisne podatke uporabniki nevede izdajo sami.

Matej Huš

Avgusta 2014 se je na spletni strani 4chan znašla zbirka skoraj 500 fotografij večinoma zvezdnic (in nekaj zvezdnikov), na katerih so bile osebe pomanjkljivo oblečene ali gole. Posnetki so se hitro razširili po internetu, sprva po Imgurju in Redditu, v nekaj dneh pa tudi v obliki torrentov. Poti nazaj ni bilo, začelo pa se je ugotavljanje, od kod so bili posnetki. Njihova narava je kazala, da imajo isti vir, najverjetneje neko družbeno omrežje. Hekerji niso objavili vseh fotografij hkrati. Druga in tretja šarža sta sledili septembra istega leta, varnostni strokovnjaki pa predvidevajo, da imajo hekerji še več fotografij in tudi druge osebne podatke, ki jih niso objavili.

Hitro je postalo jasno, da izvirajo iz Applove platforme iCloud, kamor lahko naprave z iOS shranjujejo varnostne kopije vsebine, tudi fotografij. Začel se je lov na ranljivost v API za iCloud, ki je očitno omogočila neomejeno preizkušanje gesel (napad s surovo silo), ali sledove vdora v Applov oblak. Oboje bi pomenilo, da so hekerji odkrili neko luknjo v Applovih strežnikih, toda našli niso ničesar.

Apple je po temeljiti preiskavi ugotovil, da hekerji niso nikoli kompromitirali infrastrukture iCloud ali storitve Find My iPhone, kot se je bilo domnevalo. Šlo je za natančen, dobro načrtovan in skrbno premišljen ciljani napad z ribarjenjem. Hekerji so prijavne podatke pod različnimi pretvezami dobili kar od žrtev samih. Ustvarili so račun z imenom »appleprivacysecurity« in od žrtev dobili podatke, ki so jih potrebovali za prijavo v iCloud. Telefoni iPhone pa so s privzetimi nastavitvami samodejno shranjevali kopije fotografij v iCloud, česar se uporabniki sploh niso zavedali. Afera, ki je dobila imeni *Celebgate* in *The Fappening*, je pokazala nevarnosti, ki se jim izpostavljamo tudi na družbenih omrežjih in moč socialnega inženiringa, kakor imenujemo zvito pridobivanje podatkov za dostop od uporabnikov samih.

Socialni inženiring

V informacijski varnosti z izrazom socialni inženiring označujemo psihološko manipulacijo, s katero ljudi pretentamo, da razkrijejo informacije ali storijo dejanja, ki jih sicer ne bi. Načinov je nešteto, vsem pa je skupno, da v nobeni točki ne gre za vdor, ki bi izkoriščal kakšno tehnično luknjo ali infrastrukturno pomanjkljivost v sistemu. Napadalci vse potrebno za nepooblaščeni dostop dobijo od ljudi samih.

Drži pa, da je socialni inženiring mnogokrat prvi korak v bolj kompleksnih načrtih za vdor. Neredko se vdori v banke, podjetja ali državne ustanove začnejo tako, da napadalci pretentajo katerega izmed zaposlenih, da klikne škodljivo povezavo, namesti zlonamerno programsko opremo ali preprosto razkrije potrebne informacije. To potem napadalci izkoristijo kot odskočno desko za nadaljnje rovarjenje po omrežju organizacije.

Vrste napadov

Ena najuspešnejših tehnik za vdiranje v družbena omrežja (in tudi drugam) je ribarjenje (*phishing*), kjer v resnici sploh ni treba najti nobenih ranljivosti. Najpogostejši način ribarjenja je postavitev kopije prijavne strani, na katero z elektronskimi sporočili ali kako drugače speljemo uporabnike. Ko se ti poskusijo prijaviti na lažno stran, napadalci shranijo prijavne podatke. Običajno v lažnih elektronskih sporočilih piše, da bo račun ob neaktivnosti deaktiviran, da je treba obnoviti kakšne podatke ali kaj podobnega. Da uporabniki ne posumijo, kaj se je zgodilo, jih seveda potem preusmerijo na pravo stran.

Drugi način napadov, kjer prav tako ni prizadeta infrastruktura ponudnika storitev, je beleženje vnosov prek tipkovnice (*keylogging*). Če uspe napadalcem tarči na računalnik podtakniti zlonamerno programsko opremo, ta beleži vse vnose, torej vdor ni omejen le na družabna omrežja.

Nekoliko bolj dovršeni so napadi z metodo MITM (*man-in-the-middle*). Tu gre za vrivanje hekerjev med uporabnika in spletno stran, ki jo želi obiskati. Najlaže se napadi MITM zgodijo, če uporabljamo okužene računalnike ali pa če se s svojimi napravami povezujemo z nezaščitenimi (brezžičnimi) omrežji. Pri tovrstnih napadih se naš brskalnik pogovarja s strežnikom napadalcev, ne da bi to vedeli, zadnji pa s pravim strežnikom v našem imenu. Razen kratke zakasnitve je vse videti normalno. Pred MITM se strani branijo tako, da uporabljajo šifriranje HTTPS s sistemom certifikatov. V tem primeru bi moral namreč vmesni strežnik »izdati« svoj certifikat za šifriranje prometa do uporabnika, kar bi njegov brskalnik ugotovil in ga označil kot neveljavnega. A se je že zgodilo, da je kakšen posebej malomaren sestavljavec računalnikov (npr. Lenovo pred tremi leti) na svoje računalnike kot zaupanja vreden dodal lastni certifikat, kar bi lahko omogočalo izvajanje napadov MITM.

Klasični socialni inženiring je zbiranje osebnih podatkov uporabnikov, denimo rojstnega datuma, telefonske številke ali odgovorov na varnostna vprašanja,

▽ **Lažne strani so na prvi pogled videti enako kakor prave.**

ki jih potem uporabi v obrazcu za ponastavitev gesla ali celo v pogovoru s tehnično podporo ponudnika storitve.

Ugrabitev seje (*session hijacking*) je mogoča za tem, ko se prijavimo v družabno omrežje. Brskalnik in strežnik namreč vzdržujeta odprto sejo, da lahko normalno brskamo po strani in se ni treba vsakokrat prijaviti. To vidimo, če, na primer, zapremo zavihek, potem pa ponovno obiščemo isto družabno omrežje – verjetno bomo še vedno prijavljeni. To je posledica piškotka (oziroma žetona), ki za čas trajanja seje ostane v brskalniku. Če napadalec pridobi ta piškotek, se lahko prijavi v družabno omrežje v imenu žrtve. Zlasti problematično je to, kadar do strani dostopamo nešifrirano (HTTP).

Še en način, ki spet ne sodi med pravo vdiranje, temveč bolj med socialni inženiring, je uporaba shranjenih gesel. Tu ne mislimo samo na gesla, ki so zapisana na samolepljivih lističih na monitorjih, temveč tudi shranjena v brskalniki ali upravljalnikih gesel (*password managers*). Če napadalci dobijo fizični dostop do računalnika, ki ima shranjena ta gesla in nima zaščite z glavnim geslom (*master password*), se bodo zlahka prijavili v profile na družbenih omrežjih.

Z zastrupljanjem DNS (*DNS spoofing*) napadalci poskrbijo, da se uporabnik kljub vpisu pravilnega naslova spletne strani poveže na napačen strežnik, ker mu strežnik DNS posreduje napačen naslov IP. Običajno brskalnik uporablja strežnik DNS, ki ga zagotavlja ponudnik dostopa do internet (ISP) ali upravljavec lokalnega omrežja (npr. v večjih organizacijah). Kadar pa napadalcem uspe prepričati računalnik, da posluša njihov, tj. lažni strežnik DNS, lahko uporabnike speljejo na lažne spletne strani. Od tod je potem napad enak kakor pri ribarjenju, le da to pot žrtve ne kliknejo ali obiščejo napačne domene, temveč jih DNS kljub vpisu pravilne domene usmeri na napačen naslov.

Spam

Eden izmed klasičnih napadov je tudi pošiljanja spama, ki se je sprva razširilo po elektronski pošti, danes pa pustoši tudi po družabnih omrežjih. K sreči večina družabnih omrežij omogoča pošiljanje neposrednih sporočil le, če smo s pošiljateljem povezani, ali pa sporočila nepovezanih avtorjev vsaj prestavi v manj viden, oddaljen del mape prejetih (denimo Facebook to počne). Zato napadalci pogosto pošiljajo spam z računov, ki so med našimi prijatelji – bodisi smo ga dodali nevede bodisi so ugrabili račun katerega od prijateljev.

Svojčas so bile pogoste prevare, ko so hekerji na neki način (glej zgoraj) dobili dostop do profila nekega uporabnika, potem pa so njegovim prijateljem pisali, da je obtičal v zakotnem delu sveta in da potrebuje denar. Seveda so predlagali nakazilo prek Western Uniona, nato pa je denar izginil. Včasih pa spam vsebuje zgolj povezave, katerih obisk nam nakoplje virusno okužbo.

Zaščita

Najboljši način za varovanje pred hekerskimi napadi je, da računov v družabnih omrežjih nimamo. Ker je to precej brutalen nasvet (tudi prometnih nesreč ne bo, če ukinemo promet), si oglejmo alternativne načine boja. Zelo priporočljivo je vključiti dvostopenjsko preverjanje pristnosti (*two factor authentication*), kar omogoča večina ponudnikov. To pomeni, da moramo poleg vpisa uporabniškega imena in gesla prijavo potrditi še z geslom prek esemesa, na eksterni aplikaciji za mobilni telefon ali kaj podobnega. Žal pa to ni praktično.

Najboljši način za varovanje pred hekerskimi napadi je, da računov v družabnih omrežjih nimamo.

▽ **Pri ugrabitvi seje napadalec prestreže veljaven žeton ali piškotek, ki mu omogoča prijavo.**

PSIHOLOGIJA

Šest principov socialnega inženiringa

Pri socialnem inženiringu napadalci tarče prepričajo, da delujejo legitimno ali iskreno, in jih tako pretentajo, da razkrijejo osebne podatke, ki zadostujejo za prijavo v njihove profile in račune. Načinov je več in se med seboj razlikujejo, vsi pa uporabljajo kombinacije naslednjih psiholoških principov.

Recipročnost: Ljudje načelno vrnejo »uslugo« oziroma se čutijo dolžne odzvati se na pozitivno gesto, na čemer na primer temeljijo brezplačni vzorci, strategija dobri/slabi policaj itd.

Zavezanost in **konsistentnost**: Če se ljudje zavežejo nekemu cilju, je večja verjetnost, da ga bodo na vsak način poskusili doseči. To drži, četudi še pred dosego cilja odstranimo obljubljeno spodbudo.

Družbeni vpliv: Ljudje bodo verjetneje počeli stvari, ki jih počno tudi ostali.

Avtoriteta: Ljudje načelno ubogajo ukaze ljudi z avtoriteto, četudi ti nasprotujejo nekaterim vrednotam.

Všečnost: Ljudi najlaže prepričajo tisti, ki so jim všeč, kar izkoriščajo zlasti pristopi mrežnega marketinga.

Redkost: Če se zdi, da je ponudba kakšne dobrine močno omejena, si jo bodo ljudje bolj želeli.

PREVARE

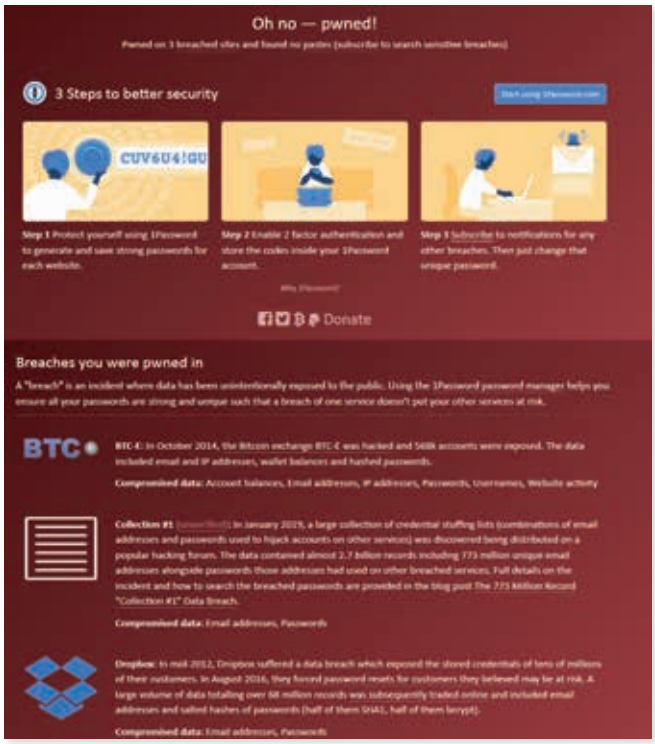
Štirje vektorji socialnega inženiringa

Ribarjenje (*phishing*): Napadalec z elektronskim sporočilom, ki je videti kakor legitimno, od žrtve zahteva vnos gesel, kod PIN ipd. v obrazec ali na spletno stran, ki je pod njegovim nadzorom.

Vishing (*voice phishing*): Napadalec tarčo pokliče po telefonu in se predstavi kot uslužbenec banke, operaterja ali kakšnega drugega podjetja ter od tarče zahteva osebne podatke za rešitev nekega »problema«.

Smishing (*SMS phishing*): Napadalec tarči pošlje sporočilo SMS, ki je videti, kot da izvira od podjetja, s katerim žrtev posluje (npr. banka). V njem od žrtve zahteva razkritje osebnih podatkov, obisk spletne strani pod nadzorom napadalca ali podobno.

Lažno predstavljanje: Redkeje, a zgodi se tudi, se napadalci v živo predstavljajo z lažno identiteto, običajno da bi dobili fizično dostop do kakšnega prostora.



△ **Spletna stran HaveIBeenPwned.com prikaže, ali je bil kateri od računov z našim elektronskim naslovom del znanih varnostnih incidentov.**

Odveč je poudariti, da moramo primerno skrbeti tudi za higieno naprav, s katerimi dostopamo do družabnih omrežij. To vključuje redne posodobitve programske opreme, uporabo protivirusnega programa, izogibanje povezovanja prek nezaščitenih brezžičnih omrežij. Klikanje na sumljive povezave v elektronski pošti ali hipnih sporočilih se odsvetuje, kjer nam majhnost našega jezika pomaga. Če nam prijatelji nenadoma pišejo v angleščini, je zelo verjetno nekaj narobe.

Spletni velikani nikoli ne bodo pošiljali elektronske pošte, v kateri bodo zahtevali vpis kakršnihkoli gesel ali drugih osebnih podatkov. Če nismo prepričani, ali je zahteva morebiti legitimna, se odpravimo na spletno stran družbenega omrežja tako, da v brskalniku sami vpišemo naslov, prijavimo in poglejmo, ali kaj zahtevajo od nas. Razne grožnje, da nam bodo v naslednjem tednu zaprli račun, da bo uporaba postala plačljiva, da moramo nujno takoj posodobiti osebne informacije in podobno, so zagotovo lažne.

Posebno pozornost velja nameniti uporabi manj varnih gesel ali recikliranju gesel (večkratni uporabi istega gesla na različnih straneh). Medtem ko je infrastruktura Googla, Facebooka, Instagrama in ostalih velikanov sorazmerno trdna, to ne velja za vse strani. Če se z istimi podatki vpisujemo na različne strani, potem pa hekerji vlomijo v eno izmed njih, ki po možnosti gesel ni primerno hranila (to je v šifrirani obliki z naključnim semenom), se bodo ti podatki znašli v temnem delu interneta. Le vprašanje časa je, kdaj jih bo kdo uporabil za poskus prijave v vse večje storitve.

Spletna stran haveibeenpwned.com omogoča vpis elektronskega naslova, potem pa nam prikaže znane varnostne incidente. Tako lahko vidimo, katere spletne strani, na katere smo se prijavili s tem elektronskim naslovom, so bile žrtve vdorov. Če smo na kateri izmed teh uporabili isto geslo kot kod drugod, ga je priporočljivo zamenjati. Zaradi tega je toplo priporočljiva uporaba upravljavcev gesel (*password manager*), ki za vsako spletno stran ustvarijo unikatno naključno geslo, ki si ga ni treba zapomniti, saj to storijo za nas. Poznati moramo le eno glavno geslo.

Ukradeno javno mnenje

Družabna omrežja so postala platforme za širjenje dezinformacij, lažnih novic, ekstremizma in spreminjanje javnega mnenja. Na eni strani imamo neizpodbitne dokaze, da se po njih pretaka veliko lažnih novic, proti čemur se poskušajo boriti tako upravljavci kakor uradni organi, po drugi strani pa se ljudje (morda upravičeno) bojijo, da bodo lažne novice priročen izgovor za uvedbo cenzure in nadzora. Oboje je slabo.

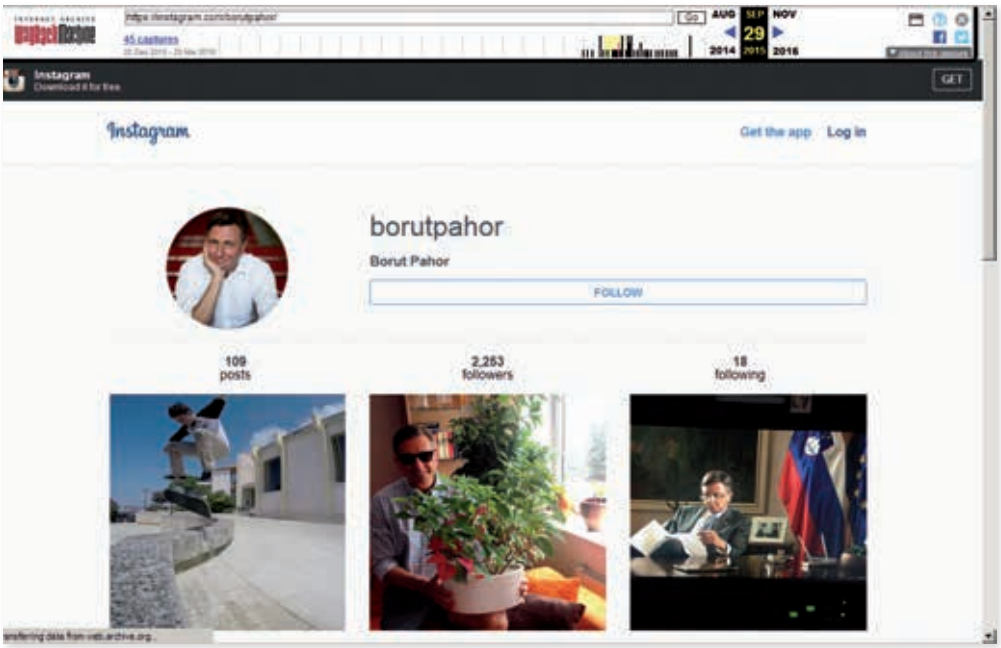
Facebook, Google, Mozilla in Twitter so oktobra lani v Bruslju podpisali kodeks o ravnanju z dezinformacijami. V njem so definirali dobre prakse, kot so onemogočanje financiranja širjenja lažnih novic iz oglasov, jasno označevanje političnih vsebin z imenom naročnika, brisanje evidentno lažnih informacij, omejevanje lažnega predstavljanja, boj proti spamu, postavitev orodij za prijavljanje nezakonitih ali lažnih vsebin, brisanje lažnih računov in profil itd. Evropski komisiji tudi mesečno poročajo o napredku v boju proti dezinformacijam.

Evropska komisija je letos maja ugotovila, da se podjetja zelo trudijo izkoreniniti lažne vsebine ter da stopnjujejo ukrepe, a da so rezultati še vedno slabi. Boj proti lažnim vsebinam in povečanje transparentnosti je označila kot ključna za zaščito integritete volitev.

Na ameriških predsedniških volitvah leta 2016 so družabna omrežja prvikrat odigrala vidno vlogo, ki ni bila v celoti pozitivna. Raziskava Univerze Stanford je pokazala, da več kot 60 odstotkov Američanov dobi novice na družabnih omrežjih. Hkrati so odkrili, da so bile na Facebooku lažne zgodbe deljene večkrat kakor resnične zgodbe uglednih medijev in da so jim ljudje v veliki meri verjeli. V času celotne kampanje se je zgodilo najmanj 760 milijonov klikov na lažne zgodbe (torej povprečno tri na vsakega Američana).

Kaj lahko pohekamo sami

Sami ne moremo vdreti v Instagram ali Facebook v pravem



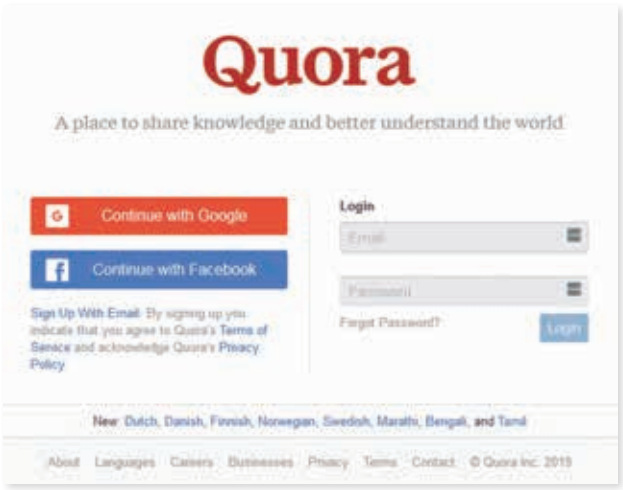
▷ **Kar objavimo na internetu, tam tudi ostane.**

smislu besede. Lahko pa si z nekaj spretnosti ogledamo vsebine, ki so sicer javne, a so uporabniki nanje pozabili, saj se ne prikazujejo na prvi strani. Prav tako je ogromno informacij moč dobiti, če povezujemo javno dostopne informacije o povezanih osebah s kombiniranjem informacij z različnih družabnih omrežij. Ne pozabimo, kar je bilo nekoč javno, potem pa smo dostop omejili na zasebno, ostaja razkrito v internetnih arhivih (archive.org).

Značilen primer so objavljene fotografije na Facebooku. V profilu naše fotografije načelno vidijo le prijatelji, a ne smemo pozabiti na vse javno dostopne fotografije, na katerih smo bili označeni. Do teh enostavno pridemo tako, da v iskalno polje na vrhu strani vpišemo »Ime priimek photos«. Če imamo soimenjake, bo zadetkov več, a to pomeni le, da bo prečesavanje trajalo dlje. V resnici že samo iskalni termin »Ime priimek« vrne veliko zanimivih informacij. Kdor ima javno dostopen seznam prijateljev, daje dodatno izhodiščno točko za nadaljevanje kopanja po družbenem omrežju. Zagotovo bo kdo izmed prijateljev imel objavljeno (ali pa bo le označen na kakšni javni fotografiji), kjer bomo tudi mi, čeprav morebiti *sploh ne označeni*. Metodični napadalec z dovolj časa lahko natančno pregleda, s kom se družimo in kje se zadržujemo.

Na internetu obstaja še cel kup javno dostopnih zbirk z osebnimi podatki, ki so tam iz povsem legitimnih razlogov.

Instagram, Twitter in druga družabna omrežja nudijo komplementarne informacije. Včasih kdo nepremišljeno objavi telefonsko številko na kakšnem forumu ali Facebooku, potem pa iskanje po internetu te telefonske številke vodi do kakšnega oglasa na Bolhi, kjer smo prijavljeni z vzdevkom. Ta vzdevek se potem najde na Instagramu, kjer profil po možnosti ni zaklenjen, na Pinterestu ali kje drugje.



△ **Številne zunanje strani omogočajo prijavo s profilom za Google ali Facebook.**

Na internetu obstaja še cel kup javno dostopnih zbirk z osebnimi podatki, ki so tam iz povsem legitimnih razlogov. Ob vsakih volitvah se objavijo kandidatne liste, na katerih so osebni podatki (skupaj s starostjo, z prebivališčem, s poklicem) vseh kandidatov. Državni izpit center (RIC) vsako leto objavi letno poročilo iz mature, kjer so poimensko navedeni vsi zlati maturantje (to so osebni podatki, ker se da iz tega precej natančno sklepati o starosti). Podobno šole na spletnih straneh z veseljem objavljajo imena vseh dijakov, ki jim je uspel kak izjemen dosežek (na tekmovanjih). Državni organi in javni zavodi na svojih spletnih straneh običajno navajajo seznam vseh zaposlenih. S poznavanjem teh podatkov, z iskanjem po Googlu in s prečesavanjem družbenih omrežij (npr. LinkedIn) je moč izvedeti marsikaj.

Zunanje aplikacije

Še eden izmed načinov, kako lahko napadalci pridejo do osebnih podatkov na družabnih omrežjih (zlasti na Facebooku pa tudi do Googlovega profila), so zunanje aplikacije ali uporaba uporabniškega računa za prijavo. Številne strani in aplikacije ponujajo možnost, da jih uporabljamo brez posebne registracije, saj lahko služi kar obstoječi profil na družbenih omrežjih. Z vpisom prijavnih podatkov in klikom na gumb Dovolim strani dovolimo dostop do nekaterih osebnih podatkov.

Podobno velja za aplikacije (znan primer so številne igre za Facebook), ki jim z dodajanjem v profil odpremo vpogled v lastne osebne podatke. Kaj točno bodo videle in katera dovoljenja bodo imele, vidimo ob podelitvi dovoljenja, a večina tega ne prebere.

Več se v javnosti o tem govori od izbruha afere Cambridge Analytica v začetku preteklega leta. Istoimensko podjetje je nezakonito zbiralo podatke s Facebooka, do katerih je pridobilo dostop, ko so uporabniki namestili namensko aplikacijo This Is Your Digital Life. Toda zaradi tedanjih nastavitev Facebooka je aplikacija lahko nabrala tudi podatke o vseh prijateljih uporabnika, ki jo je namestil. Facebook je za to nezakonito početje vedel, a ga ni preprečil do razkritja afere. Danes imajo aplikacije manj privilegijev, a še vedno je vsaka povezava do profila potencialna možnost za odtekanje osebnih podatkov.

Rešitve ni

Povsem učinkovite rešitve ni. Družbena omrežja so po definiciji namenjena deljenju osebnih podatkov in povezovanju z ljudmi. Na njih imamo dandanes toliko stikov (precej več od 150, kolikor je antropolog Robin Dunbar v 90. letih izračunal, da jih lahko resnično *poznamo*), da težko nadzorujemo, s kom kaj delimo. Poleg tega nas ogrožajo še hekerski napadi na naše računalnike, napadi na infrastrukturo ponudnikov in lastna neprevidnost. Zato še vedno velja zlato pravilo: kar želimo, da ostane skrito, naj ostane proč od interneta ne glede na nastavitve zasebnosti, privilegije in pravice dostopa. Problem je le, da imamo tudi prijatelje in znance, ki prav tako kdaj objavijo kaj – o nas. ◀

LAŽNI RAČUNI

Informacijska **vojna**

V širšem pomenu je hekanje družbenih omrežij tudi množično ustvarjanje lažnih profilov in širjenje preverljivo lažnih novic, s katerimi akterji poskušajo vplivati na javno mnenje. Problematičnosti tega početja se je javnost zavedela šele po ameriških predsedniških volitvah, ko se je v medijih začel bolj izpostavljati fenomen lažnih novic in družbena omrežja kot odlično platformo za njihovo širjenje.

Facebook je maja letos v rednem poročilu o uveljavljanju standardov razkril, da so v zadnjih šestih mesecih odstranili 3,4 milijarde lažnih računov! Večino jo polovijo že v nekaj minutah po ustvaritvi, še preden avtorjem uspe kakorkoli »spregovoriti« in povzročati škodo. Vseeno pa ocenjujejo, da je pet odstotkov aktivnih računov lažnih in jih tudi redno brišejo.

Izbrisali so sedem milijonov objav, ki so ščuvale k sovraštvu (*hate speech*), 1,8 milijarde spamerskih sporočil, 6,4 milijona objav s terorističnih propagando itd. Facebook pravi, da samodejni filtri najdejo okrog 65 odstotkov vsebin, ki jih prijavijo ljudje.

Podobno velja tudi na drugih družbenih omrežjih. Twitter je lani pobrisal več deset milijonov lažnih profilov, podobno počne tudi letos.

Kar zna Sova, **zna tudi Android**

Pametni telefon z operacijskim sistemom Android je priljubljeni življenjski sopotnik, ki s sončnimi žarki obsije vsakdan sodobnega človeka. Kljub nedvomni priročnosti, ki riše nasmeh na obraz slehernika, ima naprava svojo temno stran. Z njo je namreč mogoče početi nečedne in prepovedane reči. Ker je znanje najboljša obramba, si oglejmo, kako se izvedejo.

Boris Šavc

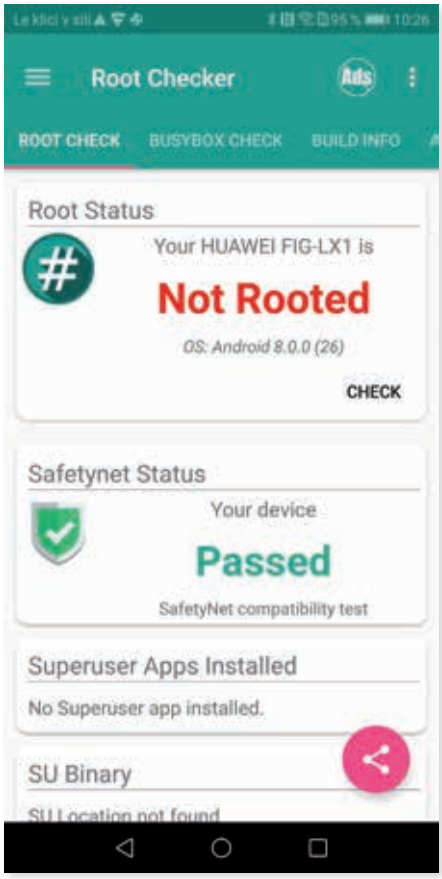
Korenski dostop

Največ nam pametni telefon z operacijskim sistemom Android ponudi, če ga odklenemo oziroma si zagotovimo tako imenovani korenski (angl. *root*) dostop. S korenskim dostopom dobimo popoln nadzor nad dogajanjem v operacijskem sistemu našega telefona. Žal to pomeni, da smo spremenili programsko opremo, kot si jo je zamislil izdelovalec, zato se moramo posloviti od morebitnega uveljavljanja garancije. Smo pa korenski uporabniki uspešno preskočili ovire in omejitve, ki so nam jih skrivaj podtaknili pri izbranem prodajalcu. Korenskemu dostopu pritičejo pravice, s katerimi lahko zmožnosti kupljene naprave razširimo do meja domišljije. Na spletu najdemo kup domačih programov in pripomočkov, ki telefon povsem predrugačijo. Navsezadnje vanj zlahka namestimo drugačno različico Androida.

Ime korenskega dostopa izvira iz operacijskega sistema Unix/Linux, kjer je korenski uporabnik enak upravitelju operacijskega sistema Windows. Korenski dostop ni isto kot namestitev prirejenega ROM, ki ga uporabimo, če želimo operacijski sistem telefona popolnoma zamenjati. Dodatne pravice tega ne zahtevajo, zato smo lahko korenski uporabnik tudi na priloženem sistemu po željah izdelovalca. Čeprav se načelno vse tovrstne stvari, na primer razbijanje zaščite na igralni konzoli, čez čas poenostavijo, tega za odklepanje telefona z Androidom ne bi mogli trditi. Če je Huawei, na primer, pred časom odklepanje zagonskega nalagalnika (angl. *bootloader*) podpiral, danes ni več tako. Omogočanja korenskega dostopa Kitajci ne podpirajo več, bojda zaradi varnosti in zaščite uporabnikov, zato se obrnemo na druge ponudnike, eden takšnih je DC-Unlocker.

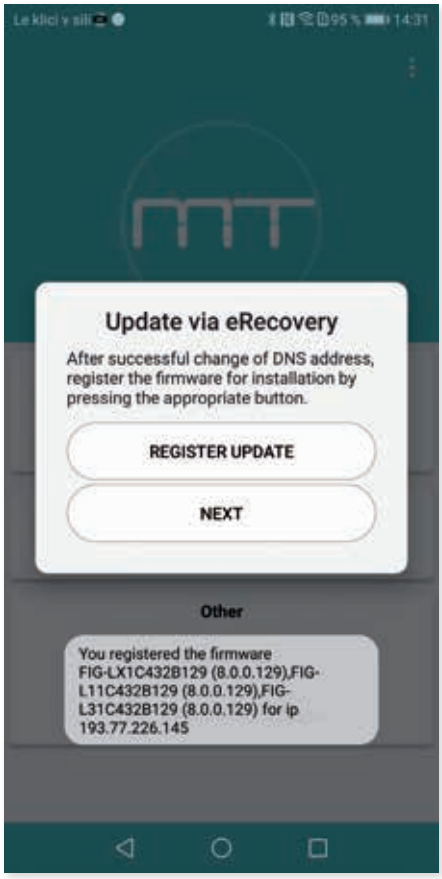
Postopek odklepanja je precej zapleten in stane, štiri evre nam ponudnik zaračuna za posebno kodo, ki jo bomo potrebovali za odklepanje zagonskega nalagalnika. Preden se lotimo tega, moramo na telefon namestiti starejšo različico operacijskega sistema, nadgradnjo v obratni smeri, ki bo podpirala odklepanje zagonskega nalagalnika. V primeru telefona Huawei P Smart s tržnice Google Play namestimo program Firmware Finder for Huawei, ki nam ob zagonu prikaže model telefona, na primer FIG-LX1C432. Ko pritisnemo nanj, se na zaslonu pojavi seznam z verzijami operacijskega sistema. Poiščemo ustrezno različico, na primer FIG-LX1C432B129 FULLOTA-MF, ki

▽ **Status korenskega dostopa na telefonu ali tablici z operacijskim sistemom Android preverimo s programom Root Checker.**

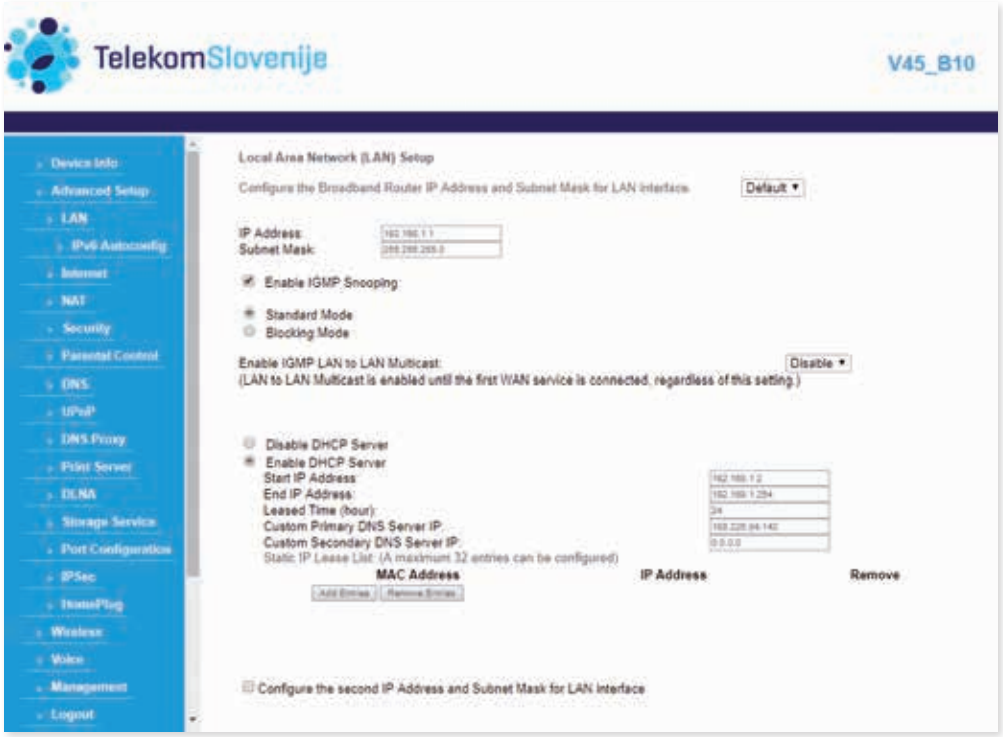


▽ **Firmware Finder for Huawei je program, ki nam pomaga iskati želeno programsko nadgradnjo za telefone priljubljenega kitajskega proizvajalca.**

▽ **Napravo z zunanjo številko IP registriramo za lažno nadgradnjo v programu Firmware Finder.**



▷ **Napravo na napačen strežnik DNS speljemo tako, da ga njegovo številko oziroma naslov vstavimo v dežurni usmerjevalnik.**



je težka malce več od gigabajta, nato izberemo možnost *eRecovery for all versions*.

Odločili smo se za nadgradnjo, ki jo običajno dobimo od proizvajalca. Da bi zadeva delovala, moramo napravo malce prelisičiti. Namesto proizvajalca nam bo nadgradnjo posredoval razvijalec programa za iskanje posodobitev Firmware Finder for Huawei. Telefon bo nadgradnjo iskal na pravem mestu (v Rusiji), če bomo dežurnemu usmerjevalniku spremenili nastavitve DNS na 188.255.84.142. Na usmerjevalniku, ki ga nudi naš največji ponudnik interneta, nastavitev najdemo pod razdelkom *Local Area Network (LAN) Setup*. Brezžično povezavo na telefonu onemogočimo in znova povežemo z usmerjevalnikom, nakar preverimo pravilnost nastavitev z obiskom spletne strani query.hicloud.com. Če na povezavo kliknemo iz mobilne aplikacije Firmware Finder for Huawei in se nam odpre spletni brskalnik s sporočilom *Connected to TeamMT Server*, je prevara uspela. Pripravljeni smo na nadgradnjo v obratni smeri.

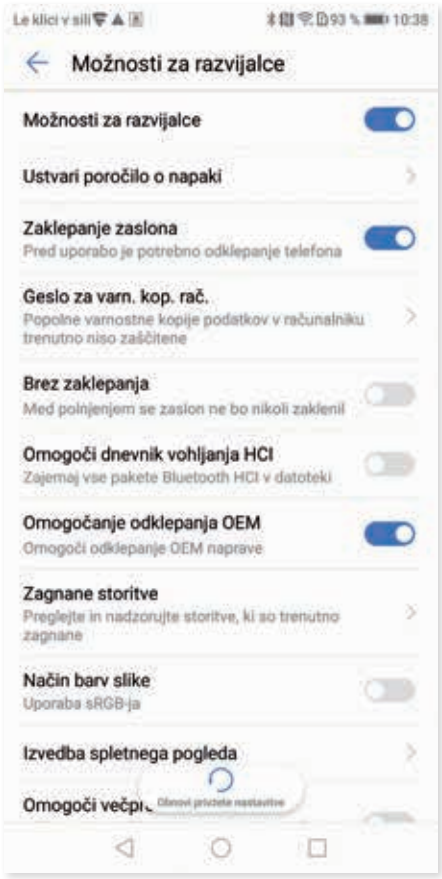
Naslednji korak v postopku aplikacije Firmware Finder for Huawei je registracija posodobitev. S spremenjenim strežnikom DNS registriramo domačo številko IP, da od razvijalcev TeamMT prejme izbrano nadgradnjo. To storimo tako, da najprej preverimo ustreznost posodobitve s *Check Availability* ter zahtevamo nadgradnjo z *Register Update*. Ko se na zaslonu za hip prikaže potrdilno sporočilo, telefon ugasnemo, ga priklopimo na električno omrežje in takoj ponovno zaženemo z držanjem gumba za povečanje glasnosti. Telefon se bo zagnal v načinu *Huawei eRecovery*, v katerem izberemo *Download latest version and recovery* in na zaslonu *Restore your system with WIFI* še *Download and recovery*. Če je šlo vse po načrtu, se naprava poveže z lokalno brezžično točko in prevarantskim strežnikom DNS ter začne prenašati lažno, a želeno posodobitev.

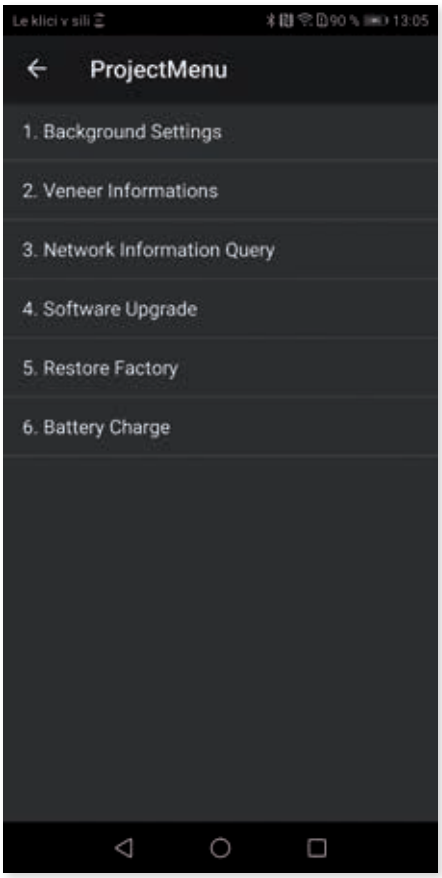
Po posodobitvi se telefon ujame v krožno zanko večnega zaganjanja sistema, ki jo odpravimo z držanjem gumbov za povečanje glasnosti in vklop. Naveza nas popelje v običajen upravitelj-ski način, kjer z *Wipe data / Factory reset* izbrišemo podatke in telefon nastavimo na tovarniške nastavitve. Ko smo znova v sistemu, preverimo različico telefona v nastavitvah Sistem / O telefonu / Delovna različica (angl. *System / About phone / Build number*. Če v prejšnjih korakih nismo naleteli na kakšno težavo, bi morala biti na tem mestu zdaj nižja številka, ki med drugim omogoča tudi odklepanje zagonskega nalagalnika ter korenski dostop do sistema.

Proizvajalci pametnih telefonov svoje naprave običajno zaklenejo, da bi uporabniki ne počeli neumnosti in ostali pri operacijskem sistemu, kakršnega so si zamislili njihovi razvijalci. Iz istega razloga skrijejo možnosti, ki omogočijo odklepanje. Do njih se dokopljemo, če sedemkrat pritisnemo na nastavitev O telefonu / Delovna različica, dokler se na zaslonu ne izpiše Zdaj ste razvijalec. V nastavitvah Sistem se pojavi nov razdelek Možnosti za razvijalce, kjer najprej vklopimo Odpravljanje težav s povezljivostjo USB, nato še Omogoči odklepanje OEM.

▷ **Proizvajalci telefonov možnosti za razvijalce privzeto skrijejo, da uporabniki ne bi počeli neumnosti in ostali pri operacijskem sistemu, kakršnega so si zamislili njihovi razvijalci.**

Naslednja skrita možnost, ki jo potrebujemo, se prikaže, ko odtipkamo številko *#*#2846579#*#*. Brez pritiska tipke Kliči se odpre *ProjectMenu*, kjer poiščemo nastavitev *Background Settings* in *USB Port Settings* prestavimo na *Manufacture Mode*, način, ki bo omogočil povezavo s programom DC-Unlocker. Tega prenesemo s spletne strani dc-unlocker.com, ga namestimo,

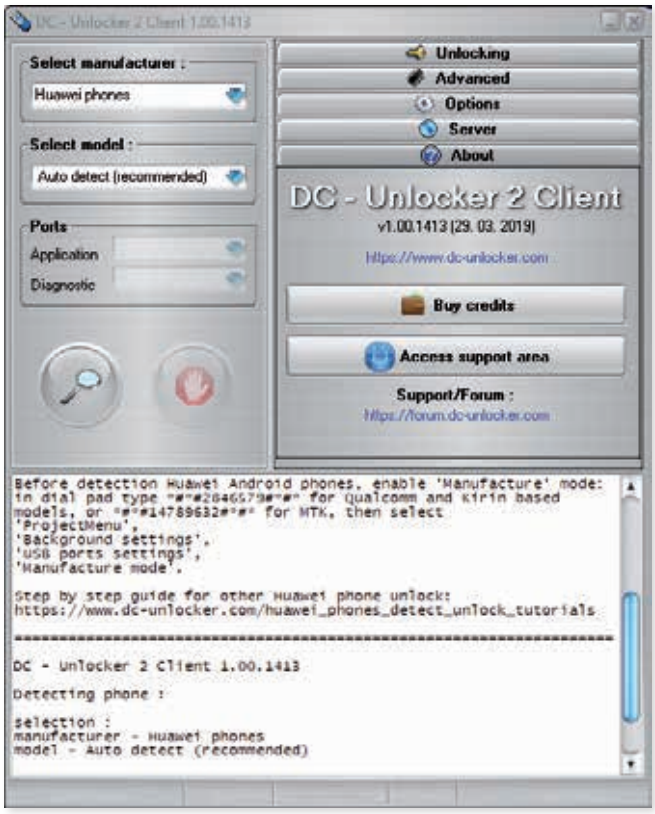




△ **Opcija Background Settings je v operacijskem sistemu Android tako skrita, da je niti prevajalci v slovenščino niso našli.**

nato telefon povežemo s kablom USB in zaženemo program. V njem pod *Select manufacturer* izberemo proizvajalca telefona, v našem primeru je to kitajski Huawei, nakar model, če gre vse po sreči, program prepozna sam. Prišel je čas nakupa žetonov za odklep.

Za odklep zagonskega nalagalnika potrebujemo štiri žetone. Po plačilu v elektronski poštni nabiralnik prispe geslo, s katerim v programu pod *Server / Unlocking* z ukazom *Read Bootloader Code* preberemo kodo za odklep. V ukazni vrstici na računalniku z operacijskim sistemom Windows se prestavimo v imenik, kjer je nameščen DC-Unlocker in vpišemo *adb devices*, da preverimo, ali je naš telefon na izpisanem seznamu, nato *adb reboot bootloader*, *fastboot devices* ter *fastboot oem unlock* ŠTEVILKA, kjer številko zamenjamo s kodo, ki smo jo prejeli z branjem *Read Bootloader Code*. Na vprašanje *Unlock bootloader* zadnjega ukaza kljub opozorilu, da s početjem kršimo garancijske pogoje, odgovorimo pritrdilno in ponovno zaženemo telefon.



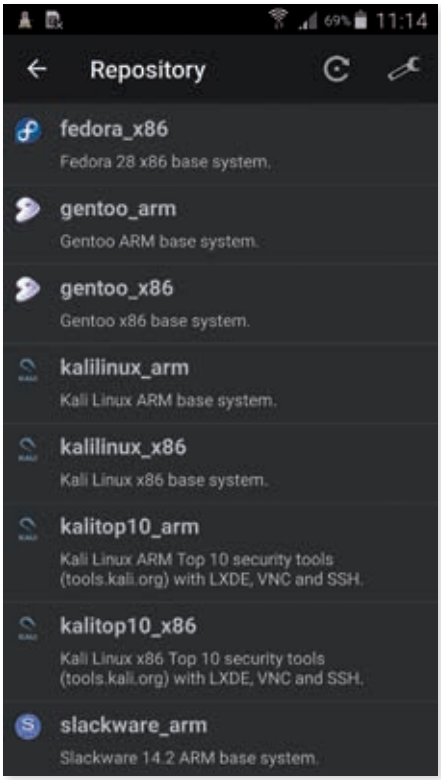
Linux

Na telefon s korenskim dostopom lahko namestimo različne programske pripomočke, ki potrebujejo neposredni dostop do slehernega dela strojne opreme, da nam z njim lažje pomagajo pri manj čednih stvareh, kakršno je vdiranje v druge telefone (in računalnike). Hekerji za nečedna opravila običajno uporabljajo računalnik z operacijskim sistemom Linux. S programom Linux Deploy, ki ga dobimo na tržnici Google Play, lahko poljubno distribucijo Linuxa namestimo tudi na pametni telefon in ga v hipu spremenimo v odlično hekersko orodje. Največ hekerskih pripomočkov na enem kupu premore distribucija Kali, ki jo pripravljeno za dobrih pet evrov dobimo znotraj programa pod opcijo *Repository*.

Kali je vodilna distribucija operacijskega sistema Linux na področju testiranja vdorov v računalniške sisteme in etičnega hekanja. Odlični programski pripomočki, ki jih Kali Linux privzeto in brezplačno ponuja, so pritegnili številne uporabnike z najrazličnejšimi nameni in s pisano paleto predznanj. Med slabe vzgibe spadajo kraja sosedovega brezžičnega interneta, zasledovanje dekleta ali zabavanje prijateljev. Kali Linux vsebuje zelo učinkovita programska orodja, s katerimi je mogoče narediti veliko škode. Sami nosimo odgovornost pri njihovi uporabi, neznanje pred zakonom ni izgovor. Čeprav uporaba distribucije Kali Linux zagotavlja določeno stopnjo anonimnosti, nismo neprebojno zaščiteni. Če kršimo zakon, nam bodo prej ali slej stopili na prste. Uporaba orodij distribucije Kali na tuji opremi brez izrecnega dovoljenja lastnika je kazniva. Uporaba ni preprosta, Kali Linux ni namenjen začetnikom. Če nam nameščanje programov, tiskanje dokumentov in podobna vsakodnevna opravila v operacijskem sistemu Linux delajo težave, potem distribucija Kali ni za nas, v nasprotnem primeru se lotimo namestitve na telefon ob pomoči

▽ **Sony odklep zagonskega nalagalnika ponuja brezplačno, preostali del postopka je podoben, zaključi se z nalaganjem sistema s korenskim dostopom.**

◁ **Odklep zagonskega nalagalnika naprav kitajskega proizvajalca Huawei nas stane štiri žetone, kar znese natanko štiri evre.**



△ **Linux Deploy uporabnikom naprav z Androidom olajša nalaganje operacijskega sistema Linux z vnaprej pripravljenimi distribucijami.**

△ **Namestitev distribucije Kali Linux z desetimi najbolj uporabnimi orodji ni mogoča brez skript razvijalca Meefik. Najdemo jih na tržnici Google Play z imenom Busy Box.**

mobilne aplikacije Linux Deploy.

Poleg aplikacije Linux Deploy potrebujemo še vsaj 5 GB prostora na lokalni ali dodatni shrambi telefona z Androidom in s korenskim dostopom, povezavo z internetom, nameščeno skripto BusyBox razvijalca Meefik in plačljivi program Piggy Helper, ki je v bistvu donacija in omogoča dostop do knjižnice že pripravljenih distribucij operacijskega sistema Linux za različne telefone. Najprej zaženemo BusyBox in ga namestimo, nato v programu Linux Deploy izberemo distribucijo kalitop10_arm in jo potrdimo z gumbom *Import*. Če namesto gumba *Import* vidimo *Purchase*, smo pozabili na donacijo razvijalcu in skrbniku zbirke.

Izbrano distribucijo z desetimi najbolj priljubljenimi orodji za hekanje naložimo z ukazom *Install*. Namestitev traja precej časa, zato je pomembna lastnost nadobudnega hekerja tudi potrpljenje. Po namestitvi v nastavitvah spremenimo uporabniško ime in geslo, s katerima se bomo kasneje prijavljali v nameščeni Linux, nato navidezni računalnik zaženemo z gumbom *Start*. Z Linuxom se povežemo prek aplikacije VNC Viewer, ki jo prav tako najdemo na tržnici Google Play. V njej z ukazom *Create new connection* ustvarimo povezavo na naslov (angl. *Address*) *Localhost* in jo poljubno poimenujemo z vnosom želenega izraza v polje *Name*. Povežemo se z gumbom *Connect*, nakar vpišemo prej vstavljeno uporabniško ime in geslo. Na zaslonu se pojavi namizje operacijskega sistema Kali Linux. Od tod naprej delo poteka tako kot v vseh drugih oddaljenih povezavah na računalnik. Pomembno je, da so nam na voljo vsa hekerska orodja, ki jih ponuja priljubljena distribucija operacijskega sistema Linux.

Med orodji v distribuciji Kali Linux je pripomoček Wireshark, ki omogoča iskanje gesel po omrežju. V *Capture/Options* nastavimo aktivni omrežni vmesnik in z gumbom *Start* sprožimo iskanje. V primeru gneče na mreži bo izhod programa Wireshark dokaj neberljiv, zato prikaz omejimo s filtri. Gumb *Expression* v desnem zgornjem kotu pokaže vse mogoče omrežne protokole. Če filter nastavimo na spletni protokol HTTP in uporabimo *CONTAINS* ter besedo *tomcat*, bo Wireshark prikazal le ujete vnose strežnika Tomcat. Za pridobivanje uporabniškega imena in gesla servisa Tomcat rezultate prečistimo s *http contains manager*, ki izdaja, da se je prek spleta nekdo pravkar prijavil na ciljani strežnik. Ob kliku na želeni vnos *GET / manager / html* se v spodnjem oknu uporabniškega vmesnika pripomočka Wireshark pojavi vsebina spletnega paketa. V njej je beseda *Authorization*, ki nakazuje, da gre za prijavne podatke. Čakata nas slaba in dobra novica: informacije so šifrirane, a na srečo s premagljivim šifriranjem, ki ga razvozlajo že osnovna spletna orodja. Vsebino kopiramo z desnim miškinim klikom ter ukazom *Copy / Value* ter jo prepišemo v najdeni spletni pripomoček.

Pravi švicarski nožek med tovrstnimi programskimi pripomočki, ki ga premore tudi distribucija Kali Linux, se imenuje Armitage. Gre za priljubljen programski pripomoček etičnih hekerjev, ki ga zlikovci ne marajo. Armitage je grafično orodje, ki mnogo stvari postori samodejno in v ozadju. Uporabimo ga le v nadzorovanem okolju. Ker hekerji z nečednimi nameni ne želijo, da bi pripomoček počel nekaj brez njihove vednosti, raje uporabljajo osnovnejša orodja s strmejšo učno krivuljo. Tistim s čisto vestjo Armitage pomaga na tisoč in en način. Primer avtomatizacije pripomočka je viden takoj, ko iz nabora možnosti izberemo ukaz *Hosts / Nmap Scans / Quick Scan* (*OS detect*), ki v zgornje okno izriše ikone najdenih računalnikov v omrežju, ter poiščemo vse mogoče napade z *Attacks / Find Attacks*. Preostaneta nam le še desni klik na izbrano tarčo ter izbira želenega napada. Delo z Linuxom in s priloženimi orodji je precej zapleteno in bi razlaga zahtevala preveč prostora za pričujoči članek, zato se ozremo za precej bolj usmerjenimi, in kar je še pomembneje, enostavnejšimi orodji, ki jih zlahka uporablja slehernik.

Oddaljeni nadzor

Programov, ki tudi manj izkušenim ponujajo nečedne usluge, je precej, a jih je malo na uradni Googlovi tržnici Play Store. Razlog je preprost, Google zanje noče niti slišati. Največ, kar stroga varnostna politika še prebavi, je Shadow – Kid's Key Logger, program za beleženje pritiskov tipk. Namenjen je predvsem sledenju aktivnosti otrok, ki so dovolj neizkušeni, da ga ne odkrijejo. Program se namreč slabo skriva, je viden na seznamu nameščenih aplikacij in ima veliko hibo, ki se vidi z lune. Namesto trenutno nastavljene navidezne tipkovnice uporabi svojo, za nameček angleško. Če otroku dajemo prvi telefon, ukane morda ne bo opazil. Drugače je Shadow preprosta stvar, ki je ni težko nastaviti. Ko program prenesemo s tržnice Play, mu je treba odobriti vrsto zahtevanih dovoljenj. Na srečo nas ob vsaki zahtevi sam pelje do ustrezne nastavitve. Najpomembnejša je zamenjava navidezne tipkovnice, Shadow uporablja tipkovnico Simple IME, s katero sledi slehernemu pritisku uporabnika. Sledenje zaženemo z gumbom *Activate Shadow*. Ko želimo ujeto vsebino prebrati, se vrnemo v aplikacijo na nadzorovani napravi in zapisano preberemo z *View Log*.

Zmogljivejše in bolj skrite mobilne programe poiščemo na spletu. Zlahka jih najdemo, saj gre za izredno priljubljeno kategorijo programskih izdelkov, nad

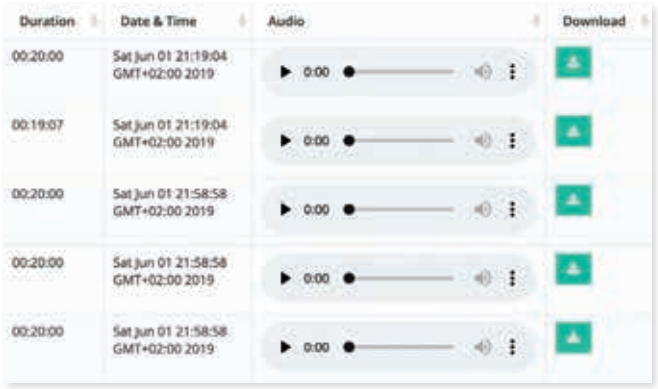
katerimi se navdušujejo prevarani partnerji, zaskrbljeni starši, maščevalni zaposleni in drugi razočarani ljudje. Večina ponudnikov prodaja zmogljive programske pakete, ki vsebujejo vse, kar si poželi prevarano srce. Levji delež aplikacij je zasidran na spletu, zato ga podjetja po večini prodajajo v obliki naročnine. Podobno velja za rešitev SpyHuman.com, ki je za deset dolarjev na mesec med cenejšimi. V nasprotju z večino drugih SpyHuman ponuja tudi brezplačno storitev, ki sledi klicem, sporočilom, brskanju po spletu in lokaciji naprave.

V prvem koraku na spletišču SpyHuman ustvarimo uporabniški račun, se vanj prijavimo, prenesemo s spleta ponujeno datoteko APK in jo namestimo na žrtvin telefon. Da moramo imeti fizični dostop do ciljne naprave in na njej omogočiti nameščanje aplikacij iz neznanih virov, na tej točki verjetno ni treba več poudarjati. Po vnovičnem zagonu se telefon zbudi z uporabniškim vmesnikom zasledovalnega programa. V prijavni obrazec odtipkamo zahtevane podatke in telefon bi se moral povezati s spletnim računom. Ko je telefon uspešno registriran, ga vrnemo lastniku. Od tod naprej delo s programom poteka od daleč. SpyHuman ima pregledno razdelan vmesnik. Na levi strani so orodja za delo z računom, od starševskega nadzora, zaščite proti kraji do nadzora naprave. Večji del zaslona na desni zavzema nadzorna plošča s hitrimi gumbi do najpogosteje uporabljenih funkcij sistema ter pomembnejših informacij o nadzorovani napravi, med katerimi so največkrat klicane številke, zagnane aplikacije in lokacija telefona.

▷ **Pogovori se na oddaljenem telefonu snemajo, nato prenesejo na spletišče, kjer jih je mogoče poslušati in analizirati.**

Prikaz klicev nam izpiše zgodovino pogovorov na oddaljeni tarči. Vmesnik nam ne prikaže le vrste klica, številke, časovne umestitve in izračuna trajanja, ampak za nameček poveže informacijo o klicu s pravim stikom in nam tako še olajša delo. Plačljivi račun, ki je spočetka brezplačno na voljo tri dni, omogoča tudi snemanje pogovorov na oddaljeni napravi. Vsak klic se v napravi posname in nato v ozadju prenese na spletišče SpyHuman. Tega lahko kopiramo k sebi in ga do onemoglosti analiziramo. Zaradi tehnologije snemanja sogovorca težje slišimo, zato se bomo morali ob takem prisluškovanju večkrat zanesti na kontekst pogovora.

Branje sporočil SMS je približno enako enostavno in pregled stikov približno tako podroben. SpyHuman nam omogoča gledanje pod prste ob brskanju po spletu in sprehajanje po priljubljenih spletnih naslovih tarče. Od daleč beremo elektronsko pošto, ki prispe v »okuženo« napravo, in pokukamo v pogovor neposrednega sporočanja, ki se odvija na njem. Zelo dobra so orodja za zasledovanje. Uporabniški vmesnik zna prikazati trenutno lokacijo in zgodovino gibanja, pri čemer na oddaljenem telefonu sploh ni treba vklopiti tipala GPS, saj ob pomoči trikotniških pravil in dveh točk z znanima koordinatama (triangulacija) sistem določi lego brez njega. Med plačljivimi zmožnostmi sistema najdemo še oddaljeni nadzor, s katerim na daljavo vklopimo kamero, posnamemo fotografijo ali zaslonsko sliko. Brskamo lahko po večpredstavnostnih datotekah na oddaljenem telefonu in spremljamo dogajanje na družabnih omrežjih, kjer se tarča zadržuje.



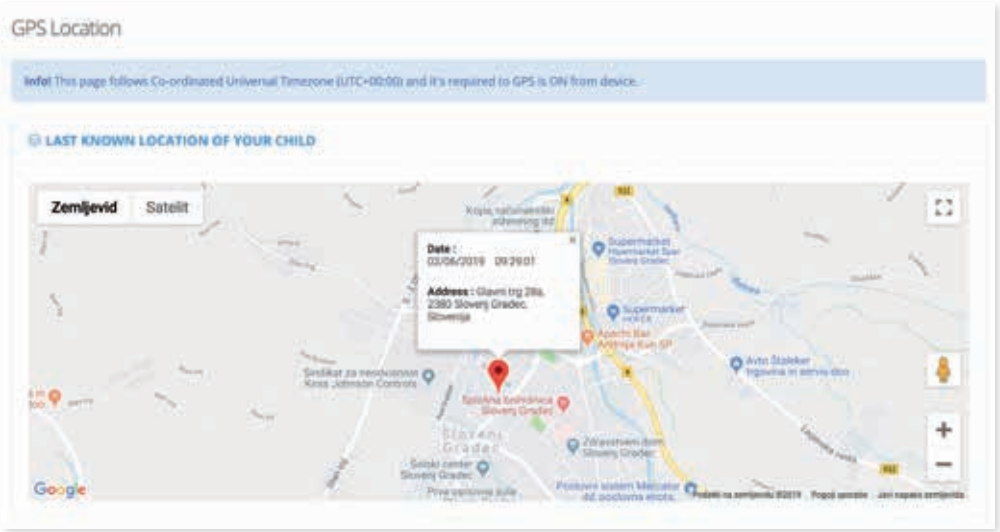
Drugi nečedni programi

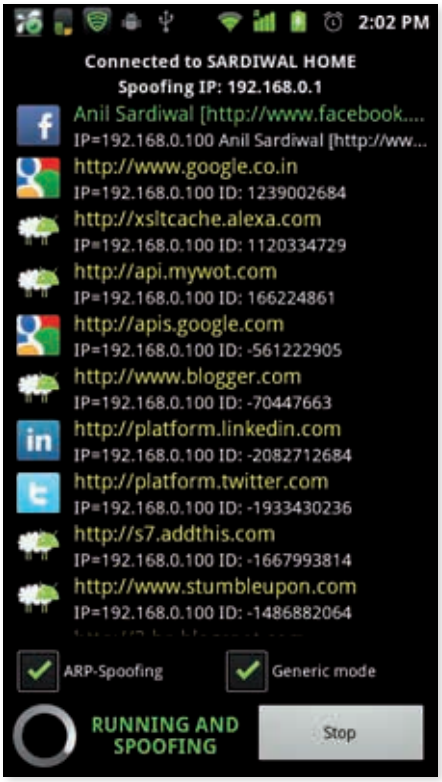
Slabost igranja vohuna s storitvijo SpyHuman in podobnimi je nujnost fizičnega posedovanja ciljne naprave. Vsaj za kratek čas mora biti žrtvin telefon v naših rokah, drugače lahko na vlogo tajnega agenta kar pozabimo. Če pogoju ni mogoče zadostiti, poiščemo programe, ki izkoriščajo luknje v omrežju. Ena takšnih se skriva v omrežnem protokolu ARP.

ARP je eden izmed osnovnih protokolov v omrežni plasti TCP/IP, zato ni čudno, da je priljubljena tarča hekerjev, ki želijo vstopiti v izbrano krajevno omrežje. Z njegovo zlorabo zlikovci prestrezajo podatkovne bloke znotraj krajevnega omrežja. Promet lahko preusmerijo, spremenijo ali ga popolnoma zaustavijo. Najpogostejši napad je enostavno zastrupljanje tabele ARP (angl. *ARP spoofing* ali *ARP cache poisoning*). To je eden izmed načinov metode *Man in The Middle*, kjer ves promet med dvema računalnikoma poteka prek napadalčevega računalnika. Tak napad je najučinkovitejši, kadar napadalci želijo prestreči komunikacijo protokolov, ki so prosto berljivi. Za prestrezanje šifrirnega protokola so potrebna dodatna orodja in več znanja. Druga vrsta napada, ki jo bomo prav tako srečali pri uporabi v članku opisanih programov, je podvajanje naslova MAC. Gre za napad DoS (*Denial of Service*), pri katerem ponarejeni paketi ARP vsebujejo podvojeni naslov MAC ene izmed naprav v omrežju, kar zmede omrežno stikalo in ovira, če že ne onemogoči, pravega uporabnika pri njegovem delu.

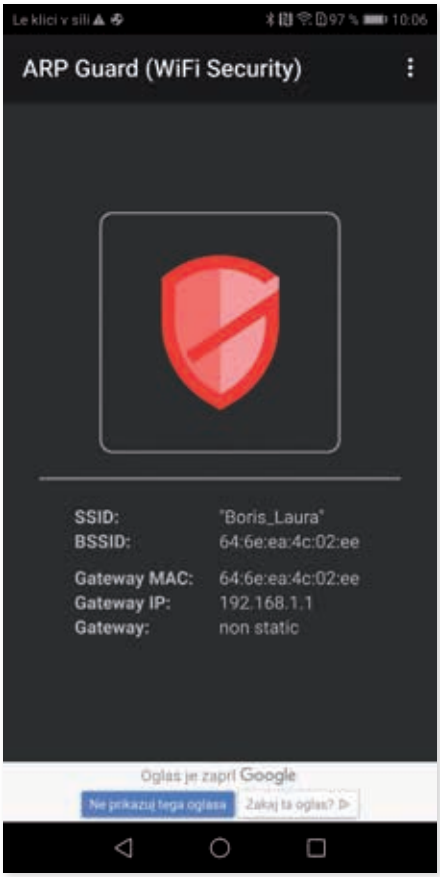
ARP med drugim zlorablja program DroidSheep, ki prestreže vse nezaščitene povezave v omrežju in prepusti nadzor nad njimi lastniku telefona, na katerem je nameščen. DroidSheep je videti kot program za krajo identitete, a je bil ustvarjen v veri, da bo naredil splet varnejši. Vsaj tako trdi njegov avtor Andreas Koch, ki je bil v preteklosti razočaran nad varnostjo velikih spletišč, kakršna so, na primer, Facebook, Ebay in Yahoo. Več milijonov uporabnikov je vsak dan prek njih nezaščiteno pošiljalo nepregledne količine podatkov in se nevarnosti sploh niso zavedali. Informacije niso bile

▽ **Nadzor ciljnega telefona omogoča tudi pregled trenutne lokacije in preteklih, kjer se je naprava nahajala.**





△ **Prizora s slike danes ne bomo več ugledali, saj so ponudniki družabnih omrežij privzeto uvedli zaščitene povezave https in je morebitnih žrtev manj kot poštenjakov med tajkuni.**



△ **Pred ugrabitvijo brezžične povezave, seje družabnega omrežja, krajo piškotkov in drugih napadov v podobi prestrezanja spletnega prometa nas učinkovito obrani programski pripomoček ARP Guard.**

△ **F-Secure je v osnovi protivirusni program za pametne telefone, ki ponuja tudi zaščito pred vohunskimi aplikacijami ter vdori v zasebnost.**

šifrirane, saj so se za izmenjavo uporabljali običajni kanali. Danes je situacija precej boljša, a se še vedno najdejo uporabniki, ki prisegajo na šibkejše spletne brskalnike ter nezaščitene internetne povezave. Bojda so hitrejše.

Pri uporabi družabnega omrežja Facebook lahko, na primer, uporabimo nezaščitene piškotke za podatke o začeti seji, kar zna izkoristiti DroidSheep. Ta po zagonu vohlja po omrežju in takoj, ko zazna kakšno dejavnost, sporoči lastniku podatke o ujeti seji. Ta se s takimi informacijami zlahka prijavi na spletno stran kot uporabnik, katerega identiteto mu je pomagal ukrasti DroidSheep. Program deluje v brezžičnih omrežjih in podpira tako odprte (OPEN) kot zaščitene povezave (WEP, WPA, WPA2). Če uporabimo način ARP spoofing, lahko krademo podatke tudi ožičenim uporabnikom. Za delovanje potrebuje DroidSheep root dostop. DroidSheep je mobilna različica priljubljenega pripomočka Firesheep. Oba sta naletela pri uporabnikih na topel sprejem in uspelo jima je doseči velike premike na področju varnosti na spletu. Facebook in drugi so pod pritiskom uvedli varne povezave SSL, zato je danes težje najti naivneže, ki bi se zavestno igrali z lastno varnostjo.

Obramba

Ob preizkušanju opisanih programov se zavemo, kaj vse preži na nas ob povezanosti pametnjakovič z internetom. Aplikacije, tako dobre kot slabe, iz dneva v dan napredujejo in nas pustijo odprtih ust. Presenečeni smo nad zmogljivostjo in dovršenostjo mobilnih izdelkov kot tudi nad njihovo učinkovitostjo. Da bi se pred morebitno nevarnostjo obvarovali, je treba pred nameščanjem vsakega programa dobro preveriti informacije o njem. Sploh če je aplikacija bolj obskurne narave, je takšna bojazljivost nujna. Med nameščanjem aplikacije nas Android vedno opozori, kakšna dovoljenja ta zahteva. Nikoli jih ne smemo preskočiti. Tam črno na belem piše, kaj bomo programu dovolili. Še vedno velja, da so aplikacije na tržnici Google Play varnejše od tistih, ki smo jih dobili na kakšni čudni spletni strani. Kljub naštetim ukrepom nas bodo zagotovo najbolje obvarovali namenski programi.

Pred ugrabitvijo brezžične povezave, seje družabnega omrežja, krajo piškotkov in drugih napadov v podobi prestrezanja spletnega prometa nas učinkovito obrani programski pripomoček ARP Guard. Mobilna aplikacija ponuja stalno zaščito pred krajo in zastrupljanjem podatkovnih paketov ARP, nas na njih opozori in napade onemogoči. Med drugimi zmožnostmi programa velja omeniti opcijo, ki ob zaznanem napadu samodejno prekine vse povezave telefona s svetom. Z ARP Guardom na telefonu je bojazen pred krajo zasebnih informacij ter drugim nečednim početjem, ki se drugače izvaja v ozadju brez naše vednosti, odveč.

Širšo zaščito ponuja protivirusni program F-Secure Mobile Security. Gre za tako raznovrsten program, da ga velja izpostaviti. Ponuja predvsem zmogljiv protivirusni program, ki brez posebnega dolgovezenja varuje pomnilniško kartico in programe, ki jih nameščamo. Deluje zanesljivo, ni preveč nadležen ali energijsko potraten. Učinkovito zaustavi viruse, vohunske programe in ostale škodoželjne koščke kode, na katere naletimo ob vsakdanji rabi povezave s spletom. Za odkrivanje nedovoljene komunikacije ima vgrajen požarni zid. Kljub temu boj proti virusom ni edino, kar F-Secure zna. Varuje nas med spletnim brskanjem in v ta namen dostavi kar svoj zaščiteni brskalnik. Dodatne omejitve pri spletnem udejstvovanju so namenjene mlajšim uporabnikom telefona. S starševskim nadzorom (angl. *Parental Control*) lahko nastavimo različne profile, ki omejijo dostop do spletnih vsebin glede na starost uporabnika. Vse našteto, vključno z varovanjem zasebnosti in zaščito spletnega bančništva, je prvi mesec brezplačno, nato program svoje usluge ponuja v obliki naročnine. Pol leta zaščite stane sedem evrov in pol. ◀

Smo varni pred **hekerskimi napadi?**

Ko menimo, da smo naredili vse, da bi hekerjem preprečili vdor v lastno intranetno omrežje, je pametno to tudi preizkusiti. Kako testiramo? Katero programsko opremo uporabljamo? Lahko testiranje naročimo?

Simon Peter Vavpotič

Namen varnostnega testiranja je razkritje napak in pomanjkljivostih v intranetni strojni in programski opremi, ki lahko poslabšajo informacijsko varnost. Nepooblaščeni dostop in kraje osebnih podatkov, osebnih digitalnih potrdil, zbirk znanj in avtorskih del imajo lahko za prizadete uporabnike hude moralne, materialne in pravne posledice. Za osnovno zagotavljanje kibernetske varnosti mora skrbeti operater dostopa do interneta, ki je k temu običajno tudi zakonsko zavezan, medtem ko je naša naloga varovanje intranetne računalniške strojne in programske opreme.

Čeprav je včasih veljalo, da smo vsaj doma varni pred hekerji, danes to zaradi vsako leto odkritih novih ranljivosti računalniške opreme in zmogljivejših hekerskih programskih orodij iz temnega dela interneta več ne drži. Zlonamerna vohunska programska oprema, ki se neopazno prikrade v naše računalnike, lahko pomeni potencialno nevarnost usmerjenega hekerskega napada v prihodnosti, če bi hekerji ocenili, da bodo imeli od njega koristi. Denimo, lahko bi namestili ransomware in čez čas zahtevali odkupnino.

▽ **Domača stran BlackArch, s katere lahko prenesemo posebno distribucijo Arch Linux za izvajanje prebojnih testov.**

Prebojni test

Prebojni test (angl. penetration test) simulira hekerski napad na intranet z namenom preverjanja kibernetske varnosti, vendar je izveden izključno z našim dovoljenjem. Pokaže šibke točke oziroma ranljivosti, zaradi katerih bi lahko nepooblaščeni zunanji uporabnik dostopal do storitev ali podatkov v naših računalnikih in omrežni infrastrukturi, programska oprema pa v poročilu pa navede tudi dobre lastnosti obstoječih zaščit.

V splošnem ločimo dva načina prebojnega testiranja: testiranje varnosti intraneta s poznavanjem njegovih arhitekture, zgradbe in delovanja (t. i. bele škatle, angl. white box) in testiranje intraneta kot neznanega informacijskega sistema (t. i. črne škatle, angl. black box). Vmesna možnost je testiranje intraneta kot sive škatle (angl. gray box), pri katerem pred začetkom izvajalcu in/ali programskim orodjem za testiranje podamo le tiste podatke, za katere verjamemo, da bi jih lahko hekerji dovolj enostavno izvedeli.

Cilji prebojnega testa so odvisni predvsem od mogočih aktivnosti intranetnih računalnikov in njihovih uporabnikov. Pri iskanju ranljivosti upoštevamo arhitekturo in nastavitve intranetne strojne ter programske opreme. Denimo, če dovolimo samo namestitev in uporabo enega spletnega brskalnika (npr. Microsoft Internet Explorer), ranljivosti drugih spletnih brskalnikov (npr. Google Chrome) ni treba preverjati.

Rezultati prebojnega testa so ponavadi vsaj nekaj časa skrivnost, saj ne želimo, da bi za morebitne odkrite ranljivosti izvedeli tudi spletni kriminalci, ki bi jih lahko s pridom izkoristili za kasnejši zlonamerni vdor v naše računalnike, še preden bi nam uspelo ranljivosti odpraviti.

Kako poteka testiranje?

Najprej se lotimo pregleda in preverjanja podatkov o intranetnih omrežnih napravah in računalnikih ter sistemski in aplikacijski programski opremi, ki jo uporabljamo. Tako lažje predvidimo morebitne ranljivosti in s spleta prenesemo ustrezno programsko opremo za njihovo odkrivanje.

Sledi preverjanje možnosti vdora z interneta na načine, ki bi jih lahko uporabil zunanji napadalec. Pri tem imamo na voljo različne zastonjske in plačljive programske pakete, kot so Nmap, FScan in Free Port Scanner, s katerimi lahko poiščemo različne vrste strežnikov in storitev v intranetu, za katere morda za zaradi kompleksnosti novodobnih operacijskih sistemov in druge sistemske programske opreme niti ne vemo. Obenem izvemo tudi njihove naslove IP in vrata IP ter nato poskušamo s posebnimi programskimi orodji odkriti njihove ranljivosti, pri čemer si lahko pomagamo z različnimi javno dostopnimi spletnimi zbirkami znanja.

V tretjem koraku posnemamo delo hekerjev in poskušamo na različne načine izrabiti odkrite ranljivosti in zaobiti zaščite posameznih spletnih storitev ter »nepooblaščeno« pridobiti podatke iz vsakega od (ključnih) računalnikov v intranetu ali jih celo spremeniti.

Dejavnost hekerjev se navadno ne konča z vdorom v intranet in enkratnim kopiranjem podatkov, temveč v računalnikih pustijo odzadnja vrata ter drugo neželeno in vohunsko programsko opremo, ki omogoča zajemanje tipk s tipkovnice, snemanje zaslona med delom uporabnikov, zvokovno in slikovno snemanje, če ima računalnik mikrofon in kamero, namerno namestitev programske opreme za predvajanje oglasov med našim brskanjem po spletu (adware)

PORTAL

Obsežna zbirka znanja na **GitHubu**

GitHub je dandanes eden izmed glavnih svetovnih portalov, na katerem lahko programerji in programerski timi objavljajo svojo izvorno in izvedljivo kodo, v zadnjem času pa tudi zbirke znanja. Projekt Strahospoštovano prebojno testiranje (angl. Awesome Prenetration Testing) je v resnici le zbirka spletnih naslovov: literature, izobraževanj, programerskih okolij, orodij, pripomočkov in knjižnic, primerov programov ter programskih okvirov za socialno inženirstvo, ki je ena od temeljnih hekerskih dejavnosti v spletu. Vključuje tudi spletne povezave do zbirke znanih ranljivosti in orodij za raziskovanje računalniških omrežij. Ne manjkajo niti ofenzivna programska orodja, s katerimi lahko simuliramo napad na svoj intranet. Najdemo tudi orodja za zagotavljanje spletne anonimnosti, s katerimi lahko po eni strani komurkoli otežimo ali preprečimo, da bi sledil našim spletnim aktivnostim, če tega ne želimo, po drugi strani pa enaka orodja uporabijo tudi hekerji, da zakrijejo sledi svojih kriminalnih dejanj.

Še posebej velja izpostaviti izčrpen seznam literature o računalniški varnosti. Defenzivno programiranje je namenjeno avtorjem, tehnologom in programerjem spletnih aplikacij, ki želijo svoje izdelke zasnovati na celovitih in varnih programerskih praksah. Številni hekerski priročniki predstavijo logiko in način razmišljanja hekerjev, da bi tako sami lažje izdelali varne programske aplikacije. Avtorji se lotevajo najrazličnejših področij: od varnosti spletnih brskalnikov, podatkovnih zbirk, operacijskih sistemov (Mac OS X, iOS in Microsoft Windows), varnosti programiranja v skriptnih programskih jezikih do varnosti in ranljivosti spletnih aplikacij.

Celovito prodorno testiranje predstavlja obsežen seznam literature, pri čemer so nekateri priročniki v celoti posvečeni rabi določenih programskih orodij in programskih okvirov, kot je Metasploit. Drugi obravnavajo različne tehnike vdora v intranetna omrežja, denimo fuzzing, ki spada med načne vdora z uporabo grobe sile. Tretji se lotevajo raziskovanja zlonamerne programske opreme v popularnih skriptnih programskih jezikih (npr. Python). Med hekerskimi priročniki najdemo tudi take, ki se že v naslovu pohvalijo s t. i. vlamljanjem ključavnice (angl. lock picking), ki je v računalniškem žargonu sinonim za prodorno testiranje, vendar namiguje tudi na zlonamerno vlamljanje v informacijske sisteme. Veliko pozornosti je namenjene tudi forenzični analizi zlonamerne programske opreme in praktičnim rešitvam za njeno odkrivanje ter obravnavo intranetnih ranljivosti.

Na svoj račun lahko pridejo tudi ljubitelji povratnega inženirstva. Vsekakor pa sta tu v ospredju preprečevanje tovrstnih nezakonitih programerskih praks in pisanje lastne programske opreme na način, ki otežuje povratno inženirstvo.

Številni priročniki na temo socialnega inženirstva pojasnjujejo, kako hekerji brez uporabe visoke tehnologije z raznimi zvijačami (npr. lažno predstavljanje za skrbnika informacijskega sistema, ki od uporabnika zahteva njegovo geslo, da bi lahko nekaj preveril …) od uporabnikov pridobijo različne podatke, ki jim nato omogočijo vdore v intranetna omrežja.

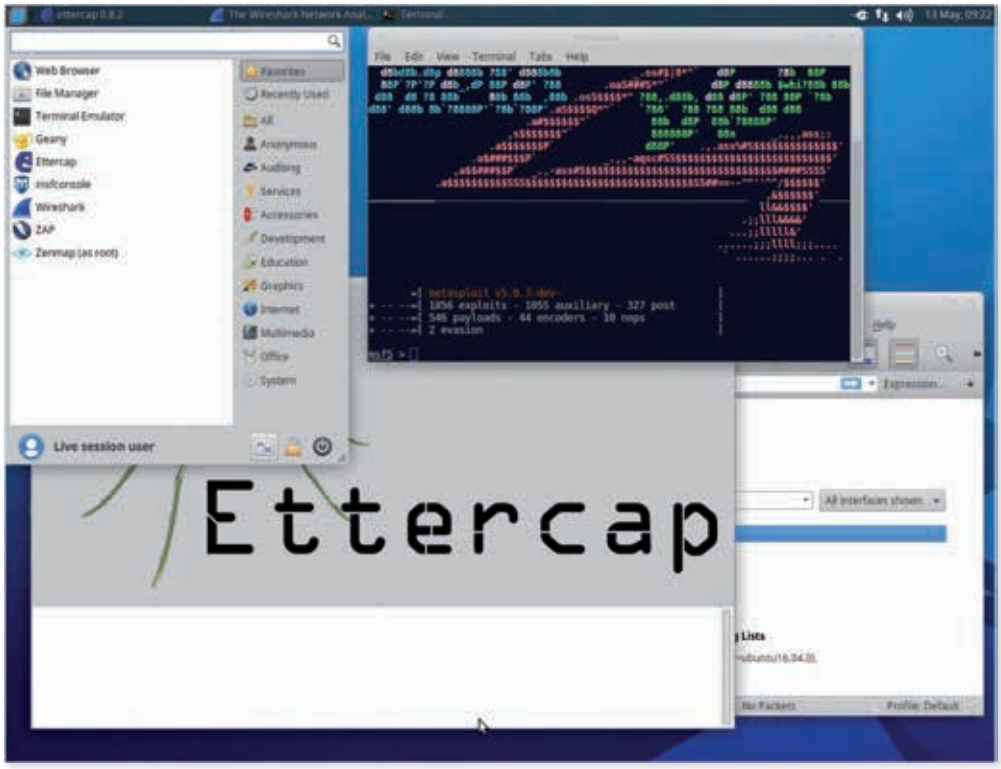
Kot jagodo na torti najdemo na koncu še obsežen seznam povezav do spletnih strani varnostnih konferenc, kjer strokovnjaki za računalniško varnost, pogosto pa tudi hekerji (odvisno od organizatorja in tipa konference), predstavijo izsledke svojih raziskav, eksperimentalno programsko opremo za prodorno testiranje in na novo odkrite ranljivosti v velikoserijski strojni in programski opremi. Še posebej velja izpostaviti ameriške konference Black Hat, Hackfest, RSA Conference USA in DEF CON. Kot zanimivost pa povejmo, da se tovrstne konference odvijajo tudi na področju bivše Jugoslavije, denimo varaždinski Fsec in novosadski BalCCon. Pri nas je najbolj odmevna konferenca na temo računalniške varnosti BSidesLjubljana, ta se odvija spomladi.

pa tudi spreminjanje v računalniku shranjenih uporabniških podatkov in vsebine sistemskega registra ter drugih sistemskih datotek.

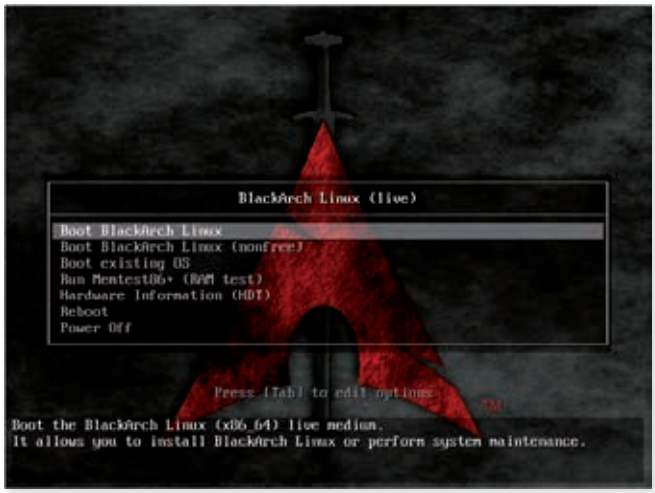
Zadnji korak je iskanje možnosti, ki jih ima heker za prikrivanje svojih aktivnosti v sistemskih in aplikacijskih dnevnikih. Zanima nas predvsem, ali je v programski in/ali strojni opremi zagotovljeno trajno hranjenje neizbrisljivih sledi skrbniških in uporabniških dostopov. To je pri strojni in programski opremi za domače računalnike pogosto neizvedljivo, je pa mogoče namestiti dodatno programsko opremo za hrambo kontrolnih sledi, s katero se te shranijo na težko izsledljiv in izbrisljiv način. Ta je neodvisen od zapisov, ki ga tvori storitev za beleženje sistemskih dogodkov operacijskega sistema.

Programska oprema

Odkrivanje ranljivosti ni vselej trivialno, zato na spletu najdemo kar nekaj namenskih distribucij operacijskih sistemov (predvsem Linuxa) s priloženimi programskimi orodji za prebojno testiranje, kot so BlackArch na osnovi Arch Linuxa, BackBox na osnovi Ubuntuja, Kali Linux in Parrot Security OS na osnovi Debiana,



▽ **BackBox, posebna distribucija različice Linuxa Ubuntu, z orodji za izvajanje prebojnih testov.**



△ **Opcije za namestitev BlackArch, kjer pri opciji "nonfree" dobimo tudi programske pakete, ki niso povsem odprto-kodni.**

Pentoo na osnovi Gentooja in WHAX na osnovi Slackwareja, ki se osredotočajo na različna področja prebojnega testiranja. Na voljo so tudi različice, ki so posebej prilagojene za delovanje v navideznih računalnikih, najpogosteje za okolji VMware in VirtualBox. Ni odveč, če rezultate testiranj vsaj v grobem dodatno preverimo vsaj še z eno distribucijo.

Na spletu najdemo tudi različne programske okvire s programskimi orodji za prebojno testiranje in varnostno analizo, kot so Buro Suite, Metasploit Project, Nessus, Nmap, OpenVAS, OWASP ZAP in W3af. Namenjeni so predvsem izkušenim inženirjem s področja informacijske varnosti, ki jih želijo sami namestiti v ustrezno predpripravljene operacijske sisteme svojih računalnikov.

Po drugi strani lahko na spletu poiščemo tudi posebne distribucije operacijskih sistemov z namerno vgrajenimi ranljivostmi (Damn Vulnerable Linix (DVL), OWASP Web Testing Environment (WTW), Metasploitable …), ki jih lahko poganjamo kot učne tarčne operacijske sisteme za odkrivanje in odpravljanje različnih vrst ranljivosti.

Nevarne ranljivosti

Ena ranljivost v zgradbi kompleksne programske opreme navadno še ne pomeni katastrofe oziroma nenamernih odzadnjih vrat. Kljub temu je kombinacija velikega števila varnostnih lukenj nemalokrat usodna, saj lahko hekerji s svojimi samodejnimi programskimi orodji izkoriščajo vse ranljivosti hkrati in si pri tem postopno ustvarijo odzadnja vrata.

Mnogi računalniški laiki verjamejo, da prek spletnega strežnika in zalednega strežnika podatkovne zbirke ni mogoče vdreti v intranet, vendar to ne drži. Programerji morajo pri pisanju programske kode še kako paziti, da ne vgrajujejo (usodnih) ranljivosti, in morajo vsako aplikacijo pred namestitvijo na produkcijske strežnike temeljito preizkusiti. S samodejnimi programskimi orodji za prebojno testiranje lahko ugotovijo, ali morebiti obstajajo nepodprte podatkovne poti, pri katerih spletni strežnik uporabniku posreduje podrobna obvestila o sistemskih napakah, ki nastanejo pod ravnjo aplikacije. Heker lahko iz njih pridobi veliko podatkov o sistemski programski opremi ter spletnem in podatkovnem strežniku, ki poganjata spletno stran.

Hekerji lahko poskušajo na spletni strežnik tudi injicirati zlonamerno programsko kodo prek morebiti nezaščitenih izravnalnikov (bufferjev) za branje vhodnih podatkovnih tokov (podatki o seji, vnosna polja spletne strani, kolački, preverjanje in nalaganje datotek na spletni strežnik …), ki pritekajo. Ta nevarnost obstaja predvsem v primerih, ko si programerji obravnavo podatkov iz vhodnih polj spletne strani in drugih vhodnih tokov poenostavijo z uporabo posebnega programskega stavka (execute), ki omogoča izvajanje poljubnega stavka SQL iz poljubnega znakovnega niza. Z dinamično tvorbo stavkov SQL v programski kodi si resda olajšajo izvajanje kompleksnejših poizvedb v podatkovni zbirki, a obenem lahko hekerji prek vnosnih tokov namesto pričakovane alfanumerične vsebine podtaknejo celoten ugnezdeni stavek SQL, ki ga podatkovni strežnik izvede brez potrebnega pregleda. Z dodatnimi programerskimi triki se lahko prek izpisov napak pri dostopu do spletne strani dokopljejo

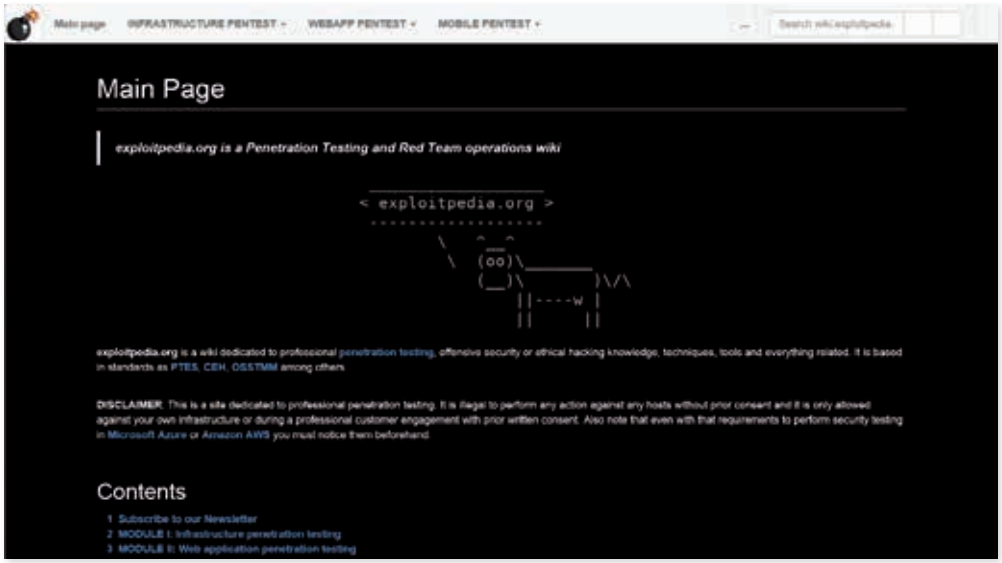
Samo za lastno uporabo, lastno strojno opremo in na lastno odgovornost!

Časi, ko so nadobudne najstniške hekerje, ki so vlomili v strogo varovane informacijske sisteme, slavili kot junake, ki so s svojimi dejanji pomembno prispevali k večji informacijski varnosti, in mnoge kasneje zaposlili kot strokovnjake za informacijsko varnost, so davno mimo. Danes vemo, da imata lahko vlom v tuj informacijski sistem in morebitno kopiranje podatkov iz njega zaradi kršenja osnovne človekove pravice do zasebnosti veliko hujše posledice kot vlom v tuje stanovanje. Metode za preverjanje ranljivosti intranetnih omrežij moramo zato uporabljati izključno v lastnem informacijskem sistemu, za tuj informacijski sistem pa kvečjemu v dogovoru z njegovim lastnikom in skrbnikom.

Testiranje ranljivosti po naročilu

V svetu ne manjka ponudnikov testiranja ranljivosti intranetnih omrežij, nekaj pa jih je tudi v Sloveniji. Prednost zunanjega testiranja je v tem, da preizkus opravi neodvisna ekipa strokovnjakov za informacijsko varnost, v kateri so pogosto tudi (bivši) hekerji. Pri odkrivanju ranljivosti lahko zato uporabi tudi alternativno programsko opremo in metode, ki jih morda sami ne poznamo.

Pri odkrivanju ranljivosti domačega interneta smo (predvsem finančno) omejeni le na uporabo takih ali drugačnih (zastonjskih) preizkuševalnih orodij in gradiv z interneta, saj si dragega zunanjega testiranja ne bi mogli privoščiti.



▷ **Domača stran Exploitpedije z zbirko znanja za izvajanje prebojnih testov in odkrivanje ranljivosti.**

celo do shranjenih procedur na podatkovnem strežniku ali pa jih nemara spremenijo in dodajo svoje.

Dobro je razmišljati tudi o varnostnem kodiranju ali drugih zaščitah neprevedene programske kode, ki jo izvajajo interpreterji številnih skriptnih programskih jezikov (npr. VBscript) pa tudi Jave. Tovrstno enostavno berljivo programje pogosto povezuje različne programske aplikacije na intranetnih strežnikih na najvišji ravni in s tem hekerju omogoči spoznavanje z arhitekturo strojne in programske opreme intraneta.

Prebojno testiranje domačega računalnika

Domači računalniki, ki so stalno vklopljeni in povezani z internetom, navadno ne dajejo znakov, da bi bilo z njimi kaj narobe. Kljub temu pa ni izključeno, da nimajo varnostnih pomanjkljivosti ali odzadnjih vrat, prek katerih so morda že vključeni v temne dele interneta in ob pomoči katerih hekerji zakrivajo sledi svoje dejavnosti predvsem takrat, ko se lotevajo napadov na večje tarče, pri katerih potrebujejo veliko zasužnjenih računalnikov.

Domači računalnik lahko najhitreje začnemo celovito testirati, če v operacijski sistem namestimo podporo za gostovanje navideznih računalnikov ali pa imamo na voljo star PC, ki ga sicer ne uporabljamo in ga lahko izkoristimo kot računalnik, iz katerega izvajamo prebojno testiranje. Nato s spleta potegnemo eno izmed prej omenjenih distribucij operacijski sistemov za prebojno testiranje in jo namestimo. Po drugi strani v sodobnih pecejih z 8 GB ali več delovnega pomnilnika s poganjanjem navideznih računalnikov ne bi smeli imeti težav, saj je na spletu voljo tudi zastonjska podpora za gostovanje navideznih računalnikov, kot sta VirtualBox in VMware (le za osebno uporabo).

Osnovna uporaba namenskih distribucij operacijskih sistemov je sorazmerno enostavna, vendar ne smemo pozabiti prepisati pristopnih gesel in uporabniških imen, ki jih ponudniki namenskih distribucij operacijskih sistemov navajajo na svojih spletnih straneh. Večina orodij za izvajanje prebojnih testov je v veliki meri avtomatiziranih in omogočajo sorazmerno enostaven začetek uporabe (npr. Wire Shark za spremljanje podatkovnega prometa po omrežjih IP). Vsekakor pa so za napredno uporabo potrebna številna teoretična in praktična računalniška znanja.

Komu zaupati?

Vsakoletna nova strojna in programska oprema z več varovali pred vdori hekerjev s spleta nas sili v pogoste posodobitve strojne opreme, ki poganjajo računalniško industrijo, zato je malo verjetno, da bomo v prihodnosti dobili strojno in programsko opremo, ki bo popolnoma varna pred napadi hekerjev. Bolj verjetno je, da bomo prisiljeni še naprej nalagati številne varnostne popravke operacijskih sistemov in večjih paketov programske opreme, kot je Microsoftov Office.

Ob vsem napisanem se lahko kaj hitro začnemo spraševati, kako se najučinkoviteje lotiti preverjanja varnosti in prebojnosti svojega intraneta. Redno varnostno testiranje z zadnjimi različicami namenske programske opreme sproti razkriva nezakrpane stare in nove ranljivosti. Če te poznamo, svoje računalnike, omrežno strojno opremo in vso programsko opremo veliko lažje zavarujemo.

Vendar tudi posvet z računalniškim strokovnjakom s področja informacijske varnosti ali z dobrim (etičnim) hekerjem vsekakor ni odveč. Ta bo znal svetovati o mogočih ranljivostih intraneta in predlagal najučinkovitejši način izvedbe prebojnega testa. Če te možnosti nimamo, se lahko odpravimo v knjigarno (npr. Amazonovo) in (prek spleta) nabavimo katerega od obsežnih priročnikov. Žal splošnega recepta, kako neprebojno zaščititi sodobne domače računalnike pred vdori z interneta, za zdaj še ni … ◀

TESTIRANJA

Standardizirane vladne prebojne storitve

Razvite države dajejo informacijski varnosti velik pomen. V ZDA je za standardizacijo storitev izvajanja prebojnih testov za računalniško programsko in strojno opremo zadolžena vladna služba GSA (angl. General Services Administration), ki ima na svoji spletni strani objavljen prebojni test za hitro oceno potencialnih ranljivosti in preprečevanje njihovega izkoriščanja, s katerim želijo preprečiti hekerske vdore v informacijske sisteme državne administracije. Na svoji spletni strani redno posodabljajo seznam visoko prilagodljivih storitev na področju kibernetske varnosti, HACS (angl. Highly Adaptive Cybersecurity Services). GSA vodi tudi seznam ključnih tehnično usposobljenih ponudnikov storitev preverjanja spletne varnosti, ki omogoča vladnim službam hitro naročanje in namestitev tovrstnih storitev ter zagotavlja varovanje in zaščito informacijske infrastrukture administracije ZDA.

Standardizirano prebojno testiranje 132-45A posnema izvedbo dejanskih hekerskih napadov z metodami, s katerimi hekerji zaobidejo varovalne elemente aplikacije, informacijskega sistema ali računalniškega omrežja. Storitve prebojnega testiranja, HACS, so namenjene strateškemu testiranju preventivnih in detekcijskih ukrepov (vladnih) organizacij za zaščito podatkov in dobrin. Testiranje 132-45A vključuje tudi sodelovanje certificiranih etičnih hekerjev, ki izvedejo simulacijo napada na informacijske sisteme, sistemske aplikacije ali druge izbrane tarče, v katerih iščejo ranljivosti.

Po testiranju varnostni inženirji in certificirani etični hekerji pripravijo poročilo s popisom ranljivosti in pregledom učinkovitih obrambnih postopkov ter programske opreme in tistih obrambnih postopkov ter programske opreme, ki jih lahko hekerji premagajo ali izkoriščajo za napade na druge informacijske sisteme.

△ **Eno izmed spletnih izobraževanj v obliki predstavitve, ki jih lahko prenesemo z interneta.**

Zanimivo branje

Koncept in pomen varnostnega testiranja, ki vključuje tudi prebojno testiranje
en.wikipedia.org/wiki/Security_testing

Zbirka znanja oziroma spletnih naslovov, Awesome Prenetration Testnig
github.com/enaqx/awesome-pentest

Zbirka znanja, organizirana podobno kot Wikipedija, za varnostne strokovnjake, ki se profesionalno ukvarjajo s prebojnim testiranjem
wiki.exploitpedia.org

ODKLEPANJE

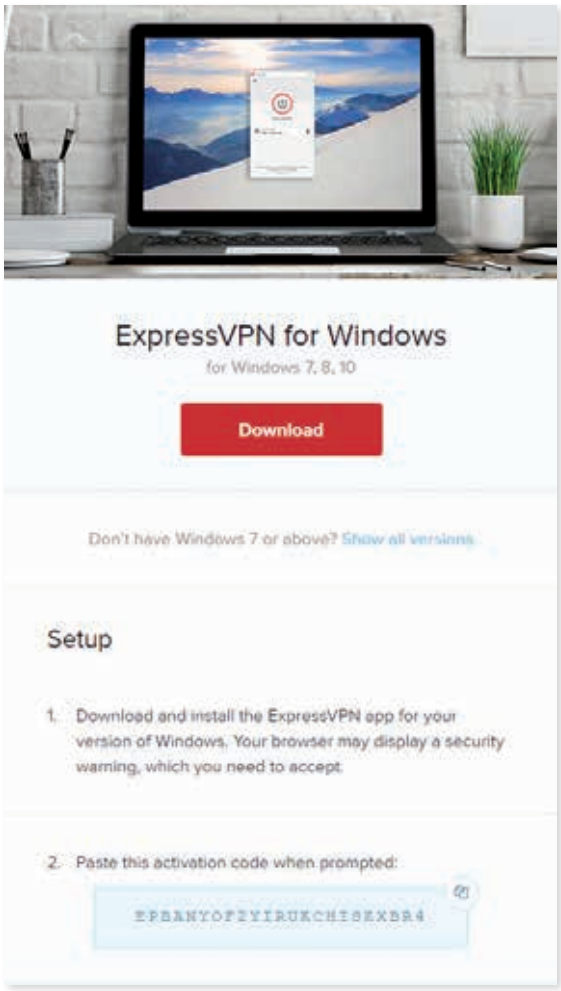
- Ameriške dobrote v Sloveniji
- Popolni nadzor nad pametnim telefonom
- Temna plat sodobnih vozil

Ameriške dobrote v Sloveniji

Slovenci filme, serije in glasbo že dolgo uživamo predvsem digitalno. Resda smo spočetka to počeli v sivem območju, ki mu v tujini radi rečejo piratstvo, a smo se s hitro posvojitvijo plačljivih pretočnih storitev v zadnjem času odkupili ter dokazali našo pravo usmerjenost. Vedno smo bili za zabavo pripravljeni plačati pošteno ceno, vendar možnosti v preteklosti nismo imeli. Žal nam tudi pretočne storitve danes niso vse na voljo. Kljub temu se tokrat ne pustimo speljati na kriva pota, temveč se zatečemo k iznajdljivosti.

Boris Šavc

Nerepovedan dostop sta besedi, ki ju zagovorniki svobodnega interneta ne slišimo radi. Žal nam avtorske pravice in telovadba z njimi grenijo življenje pri uživanju v vsebinah pretočnih storitev. Želje filmskih in glasbenih studiev ter televizijskih mrež se ne skladajo z našimi pričakovanji. Čeprav plačujemo (približno) enako ceno, se ponudba med državami in pretočnimi storitvami zelo razlikuje, nekatere med njimi pa nam niti niso na voljo. Zatečemo se k povezavam VPN, ki naše poreklo zakrijejo in nas pretočnim storitvam predstavijo kot prišleka iz ene od dovoljenih držav. Tovrstne, dokaj poštene prakse ponudniki pretočnih vsebin ne prepovedujejo izrecno, ker vsi na naš račun prav lepo služijo. Sprenevedanje je logično, saj nihče noče, da bi bili primorani spet seči po »sivi« robi. Še vedno je stopnja piratstva v Sloveniji visoka, brez storitev VPN pa bi zagotovo bila še višja.



◁ **ExpressVPN že ob namestitvi na računalnik zahteva aktivacijsko kodo, ki jo dobimo ob plačani naročnini.**

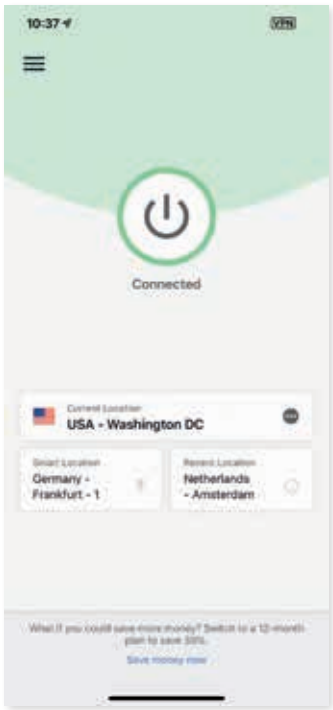
VPN

Navidezno zasebno omrežje VPN je običajno plačljiva storitev, ki skrbi za zasebnost spletnega pohajkovanja in obide regijske zaščite večpredstavnostnih vsebin. Tovrstne usluge uporabimo, če želimo biti anonimni, si na pretočnem servisu ogledati film, ki ni namenjen deželi na sončni strani Alp, ali odigrati partijo pokra na spletišču, kjer Slovenci nismo (več) dobrodošli. VPN je skrivni prehod med domačim računalnikom in ciljno destinacijo, ki jo želimo obiskati na spletu. PC se najprej poveže z oddaljenim strežnikom, ki je ponavadi nastanjen v drugi državi, nakar nam ta servira ves spletni promet, ki si ga zaželimo. Rezultat tega početja je, da obiskana spletišča ne vedo, od kod smo. Kar se tiče njih, prihajamo iz države, od koder je strežnik VPN.

Dobra stran uporabe povezav VPN je, da smo med spletnim sprehajanjem veliko bolj zaščiteni kot običajno. Zlikovci nam težje sledijo, kradejo podatke o spletnih prijavah ter izzivajo z lažnimi stranmi. O dogajanju med našimi spletnimi sprehodi se jim le sanja. Kam gremo, kaj tam delamo, vemo le mi, naš ponudnik navideznega zasebnega omrežja VPN in ciljno spletišče, ki smo ga obiskali. Drugi, vključno s ponudnikom interneta, tavajo v temi. Postranski priboljšek brskanja z VPN je skrivanje lokacije, saj obiskana stran »misli«, da prihajamo iz dežele, kjer je nastanjen strežnik. To s pridom uporabimo v primeru državne cenzure ali pri uporabi pretočnih storitev, ki glasbo, filme in serije pri nas ponujajo v zelo okleščenem obsegu. Če smo, na primer, naročnik storitve Netflix, ki je na voljo tudi v Sloveniji, nas ob zagonu odjemalca, priklopljenega na navidezno zasebno omrežje v ZDA, pričaka skorajda desetkrat bogatejša ponudba filmov in nadaljevank kot sicer.

Na spletni strani Comparitech so objavili zanimivo študijo o tem, katere države za Netflix glede na dostopno vsebino plačujejo največ in katere najmanj. Da bi prišli do vrednosti storitve v vsaki državi, so vzeli število filmov in serij, ga delili z zneskom mesečne naročnine in tako dobili ceno za posamezen naslov. Največjo ponudbo imajo logično Američani, izbirajo lahko med skoraj 6.000 naslovi. Kljub temu in razmeroma nizki naročnini (8 USD) jih po vrednosti prekašajo Kanadčani, ki za malenkost tanjši katalog plačajo dolar manj. V Evropi dobijo za svoj denar največ v Veliki Britaniji – na voljo imajo nekaj čez 5.500 naslovov, cena mesečne naročnine pa je 7,8 dolarja.

V Sloveniji imamo v zbirki dobrih 3.800 filmov in serij, kar je primerljivo z nekaj drugimi evropskimi državami (Hrvaška, Nemčija, Francija), ki imajo večinoma enako ceno. V svetovnem merilu smo pod povprečjem. Osnovna naročnina Basic v Sloveniji nas olajša za osem evrov. Ker je namenjena zgolj uporabi na enem zaslonu s šibkejšo ločljivostjo in z možnostjo prenosa video posnetkov na osamljen telefon ali tablico, se večina odloči za paket Standard, kjer



△ **Uporabniški vmesnik VPN storitve ExpressVPN, ki je na telefonu in računalniku skorajda enak, odlikujeta preprostost in učinkovitost.**

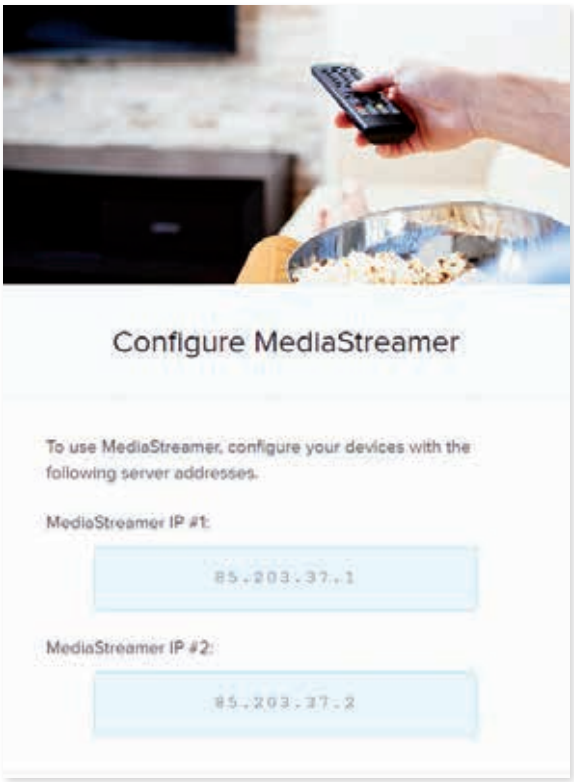
se plačuje deset evrov na mesec, naročnik pa uživa v vsebinah visoke ločljivosti HD na dveh zaslonih hkrati. Najdražja je možnost Premium z ločljivostjo Ultra HD, gledanjem na štirih zaslonih hkrati, prenosom na štiri telefone ali tablice ter ceno 12 evrov na mesec. Da bi za svoj denar dobili več, uporabimo povezavo VPN. Ker tovrstne rešitve ameriški pretočni velikan preganja, je treba izbrati zanesljivega ponudnika. Med boljšimi (in dražjimi), ki svoje strežnike redno posodabljajo in se spretno izogibajo cenzuri, je ExpressVPN.

Povezovanje s strežniki izbranega ponudnika navideznega zasebnega omrežja VPN je ne glede na predvajalno napravo načelno preprosto. Nič drugače ni v primeru uporabe storitve **ExpressVPN**. Na pametnem telefonu izbranega okusa, lahko je tudi jabolčni, si omislimo brezplačno mobilno aplikacijo želenega ponudnika, nakar vanjo vnesemo prijavne podatke, ki smo jih dobili ob plačilu naročnine, izberemo nadomestno državo in gumb Poveži oziroma *Connect*. Preizkus pretočne storitve Netflix z ameriškim strežnikom VPN nam pokaže izdatno bogatejši katalog filmov in serij, ki jih na telefonu tudi uspešno predvajamo. Težave nastopijo, ko želimo sliko zrcaliti na omreženi televizor, ne glede na to, ali uporabimo predvajalnik Apple TV, Googlov Chromecast ali kar povezovalne sposobnosti izbranega televizorja, saj stopi na sceno Netflixova zloglasna zaščita pred goljufanjem s proxy strežniki. Pretočna storitev zazna, da nekaj ni v redu, in izpiše napako.

Enako preprosta je uporaba vmesnika VPN na računalniku. Na računalniku z operacijskim sistemom Windows prenesemo ustrezno aplikacijo, jo namestimo in prilepimo aktivacijsko kodo, ki jo pridobimo z obiskom spletišča expressvpn.com. Uporabniški vmesnik je minimalističen, med maloštevilnimi zmožnostmi najdemo test hitrosti *Speed Test*, ki preveri, kateri od dostopnih strežnikov nam bodo nudili najhitrejšo povezljivost. Test je uporaben, a dolgotrajen, preden namreč postreže z rezultati, mine kar precej časa. Uporaba preprostega programskega pripomočka je identična uporabi istoimenske mobilne aplikacije. Najprej izberemo nadomestno državo, v kateri se nahaja VPN-strežnik (Choose Location), in pritisnemo gumb za povezovanje. Z izbiro ameriškega strežnika pri Netflixu nimamo sreče, zato uporabimo francoskega. Netflix začne predvajati izbrano (prepovedano) vsebino, a pri prenosu na televizor spet odpove poslušnost. Na podporni spletni strani storitve ExpressVPN svetujejo uporabo posebej prilagojenega usmerjevalnika. Lahko ga kupimo ali ustrezno programsko opremo naložimo na enega izmed podprtih modelov. Ker na testu ustreznega usmerjevalnika nismo imeli, smo se lotili ročnih nastavitev.

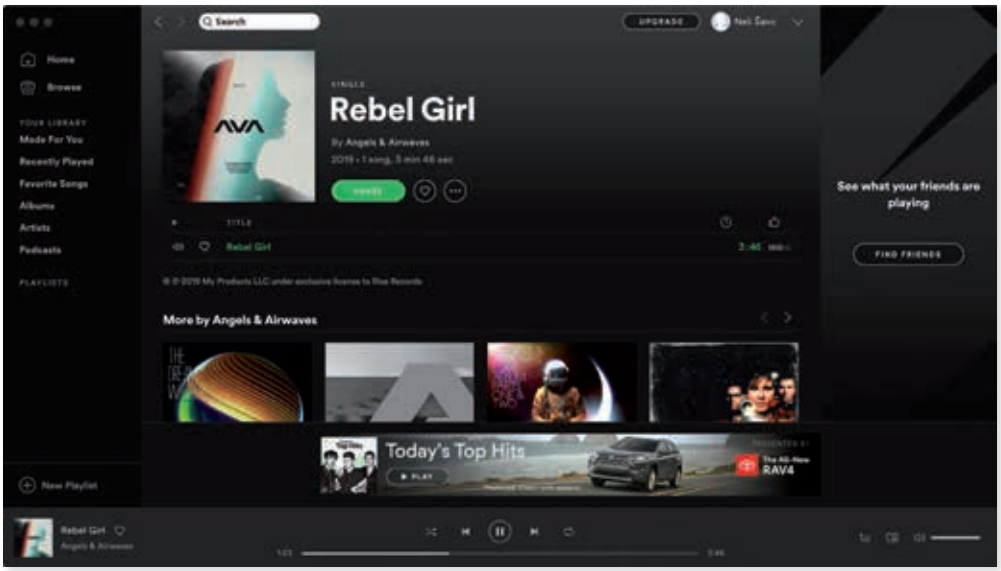
Spletišče storitve ExpressVPN prijazno ponuja vodnike skozi nastavitve številnih naprav, med drugim poleg najočitnejših kandidatov tam najdemo navodila, kako s povezavo VPN sparitи igralni konzoli PlayStation in Xbox, tablico Kindle Fire, predvajalnik Apple TV ali računalnik z operacijskim sistemom Linux. Ker plačana naročnina omogoča neomejeno povezovanje hkrati, si jih velja ogledati in kasneje tudi nastaviti več. Pri ročnem nastavljanju usmerjevalnika najprej izberemo tip primerka, s katerim se bomo lotili posla. Za

▷ **MediaStreamer je opcija storitve ExpressVPN, ki nas obleče v tujca ob pomoči strežnika DNS, kar olajša uporabo na napravah brez ustreznega programskega odjemalca.**



△ **Pri povezovanju različnih naprav, vključno z usmerjevalniki, nas storitev ExpressVPN prijazno vodi za roko.**

Med boljšimi (in dražjimi) ponudniki VPN, ki se spretno izogibajo cenzuri, je ExpressVPN.



◁ **Zelo priljubljena glasbena pretočna storitev Spotify v Sloveniji uradno ni na voljo, omislimo si jo lahko prek povezave VPN.**

usmerjevalnik TP-LINK spletišče pravi, da bomo povezavo uspešno vzpostavili s protokolom L2TP. Da bo naše čaranje uspešno, mora usmerjevalnik priljubljeni protokol za navidezna zasebna omrežja seveda podpirati.

Podrobnejša navodila nas v prvem koraku opozorijo na podatke, ki jih bomo pri nastavljanju potrebovali, ter opomnijo, da je pametno narediti kopijo trenutnih nastavitev za hitrejše vračanje na staro stanje. Uporaba storitve ExpressVPN na usmerjevalniku podjetja TP-LINK je seveda pogojena z uporabniškimi podatki, ki strežniku pokažejo, da smo aktivni naročnik. Imamo jih v nabiralniku elektronske pošte, na povezavi Licences ali na spletišču pod zavihkom *My Account*. Ko izberemo Set Up ExpressVPN / Router / TP-Link, pritisnemo še gumb PPTP & L2TP-IPSec. Prikažejo se uporabniško ime in geslo ter seznam strežnikov po vsem svetu. Strežniki, žal (in logično), niso v številčni obliki, zato mora usmerjevalnik podpirati vnos domenskih imen, če želimo, da bo povezovanje uspešno.

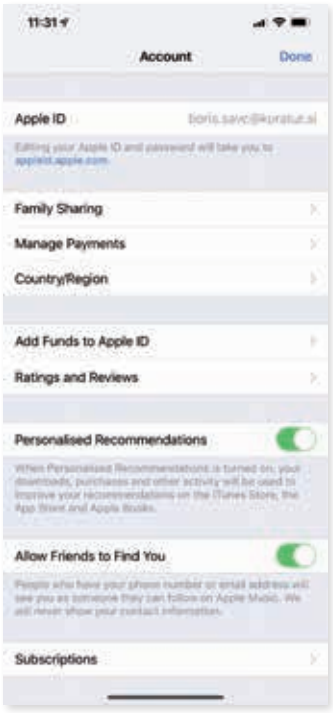
Ko se dokopljemo do vsega potrebnega, brskalnik usmerimo na lokalni naslov, kjer prebiva administratorska stran našega usmerjevalnika. Prijavimo se na nadzorno ploščo in odpremo podstran Network / WAN. V polju WAN Connection Type izberemo vrednost L2TP/Russia L2TP, vpišemo uporabniško ime, geslo in naziv strežnika, ki smo jih dobili na spletišču ExpressVPN, MTU Size pustimo na 1460, Max Idle Time spremenimo na 0 ter vneseno shranimo z gumbom *Save*, nakar usmerjevalnik zahteva ponovni zagon.

Ob naslednji prijavi v administratorsko nadzorno središče nas pod Network / WAN že čaka pripravljeno vozilo, ki nas bo popeljalo v drugo državo, kjer bo dostopen bogatejši Netflix (in druge dobrine, ki jih sicer nismo deležni). Z gumbom *Connect* se povežemo z oddaljenim strežnikom VPN in nove omrežne nastavitve preizkusimo na prej neposlušnih napravah. Če doma nimamo podprtega usmerjevalnika, ki bi nas samodejno izdajal za tujca, lahko na pametnem televizorju (ali ustreznem predvajalniku) uporabimo povezano storitev MediaStreamer. Z naročnino nam namreč pripada strežnik DNS, ki nas tudi na napravah brez namenske aplikacije za ExpressVPN poveže s spletom v imenu drugega.

MediaStreamer deluje odlično in brez težav. Edino, kar zahteva, je registracija zunanjega naslova IP, ki ga bo uporabljal. Registriramo ga na uradnem spletišču storitve ExpressVPN, tako da izberemo *My Account*, zavihek *DNS Settings* in pod *IP address registration Register my IP address*.

S povezavami VPN si lahko omislimo tudi naročnino na storitve, ki jih v Sloveniji ni, na primer Spotify.

▽ **Tržnice z mobilnimi programi za posamezne izdelke, kakršen je odjemalec pretočne storitve Spotify, preverjajo poreklo obiskovalca oziroma kupca. Na telefonu iPhone državljanstvo spremenimo ročno v nastavitvah Settings.**

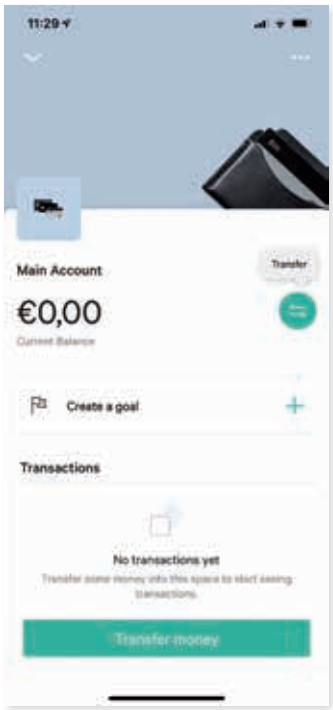


Če ponudnik vsakodnevno menja zunanjo številko IP, je treba registracijo naslednji dan ponoviti. Če nameravamo VPN-storitve prek MediaStreamerja uporabljati dlje časa, velja razmisliti o statičnem IP-naslovu, ki ga ponudniki interneta običajno zagotavljajo brezplačno. Za konec pregleda storitve ExpressVPN naj opozorimo, da MediaStreamer ni VPN, je manj varen in ne varuje zasebnosti tako dobro. Podpira pa Netflix in druge pretočne storitve, ki nam ob njegovi uporabi prikažejo povsem drug obraz. Med drugim si lahko omislimo tudi naročnino na storitve, ki jih v Sloveniji sicer ni, na primer glasbeno storitev Spotify.

Spotify

Pretočna glasba v Sloveniji je prisotna že precej časa, med bolj priljubljenimi tovrstnimi storitvami so Google Play Music, Apple Music in Deezer. V podalpskem naboru ni pretočne storitve Spotify, ki jo odlikujeta brezplačen paket z oglasi ter nadmočno iskanje nove glasbe, prilagojene posameznikovemu okusu. Zaradi zmožnosti, ki jih tekmeci nimajo, je Spotify po mnenju mnogih najboljša glasbena pretočna storitev na svetu. Ker Spotify za brezplačen paket z oglasi ne zahteva kreditne kartice, je dovolj, da zaženemo izbrano VPN-storitev, se z njo virtualno preselimo v Združene države Amerike ter na uradni spletni strani ustvarimo uporabniški račun.

Naslednji korak je namestitev aplikacij. Medtem ko je Spotify na računalniku zlahka dostopen, pri mobilnih aplikacijah naletimo na težavo, saj tržnici Google Play in App Store pri našem načrtu nočeta sodelovati. Če uporabljamo slovensko različico trgovine, aplikacije Spotify v njej ne bomo našli. A k sreči so na voljo načini, kako preskočiti tudi to oviro. Uporabniki mobilnikov s sistemom Android svežo različico programa Spotify v obliki APK poiščemo na spletu. Datoteko nato



△ **Tuje plačilno sredstvo nam tudi v Sloveniji zagotavlja nemška banka N26.**

prenesemo v telefon ali tablico in jo namestimo. Pred tem moramo sistemu dovoliti nameščanje aplikacij iz neznanih virov. Uporabniki Applovih naprav imamo nekoliko lažje delo, saj v Cupertinu dovolijo menjavo države trgovine. Postopek je zapisan na straneh za podporo uporabnikom. Na telefonu iPhone v nastavitvah *Settings / iTunes & App Stores* izberemo *Apple ID / View Apple ID*, kjer pod *Country/Region* spremenimo državo. Če imamo na računu aktivno kakršnokoli naročnino, jo moramo pred menjavo države prekiniti, na kar nas opozori tudi sistem. Ker Apple zahteva ustrezno plačilno sredstvo in za tujo državo najverjetneje ne bo hotel sprejeti slovenske kreditne kartice, se spet znajdemo pred zagato. Reši jo ena izmed tujih plačilnih storitev, na primer nemška banka N26.

Kdor je že odpiral račun v slovenskih bankah, ve, da zakonodajo o preprečevanju pranja denarja jemljejo hudo resno, tako da vprašajo vse – tudi o zaposlitvi, delodajalcu, delovnem mestu, mesečnih prihodkih itd. Pri N26 pa se odpravimo na njihovo spletno stran, kliknemo *Open Bank Account* ter vpišemo elektronski naslov, državo, telefonsko številko, ime in priimek, rojstni datum, državljanstvo in naslov. In to je to. N26 je izvrstna rešitev za vse, ki bi radi imeli dodaten MasterCard za internetno plačevanje, dvigovanje gotovine brez provizije ali pa zgolj skladiščenje denarja v Nemčiji.

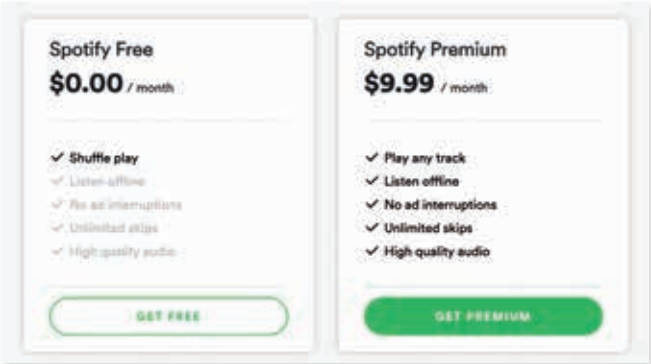
Podatke moramo nato le še potrditi. Na mobilni telefon prenesemo aplikacijo N26, med delovnim časom opravimo videoklic v centralo, kjer se pogovorimo z zaposlenim, ki mu pokažemo osebni dokument. Čez približno en teden prispe domov ličen prozoren MasterCard, ki ima dodatno desetmestno številko (ID). To številko najprej vnesemo v spletno banko, da kartico aktiviramo, potem pa jo potrebujemo za vsako spremembo funkcij – nastavljanje limitov, številke PIN in podobno. Sredstva na račun oziroma kartico, ki je debetna in ne kreditna, nakažemo z nalogom UPN. Kartica banke N26 je kot nalašč za spremljanje vsebin, ki nam kot Slovencu niso dostopne. Med drugim lahko Spotify z njo nadgradimo na plačljivi račun Premium, ki je brez oglasov in omogoča prenos glasbe na napravo za poslušanje brez internetne povezave.

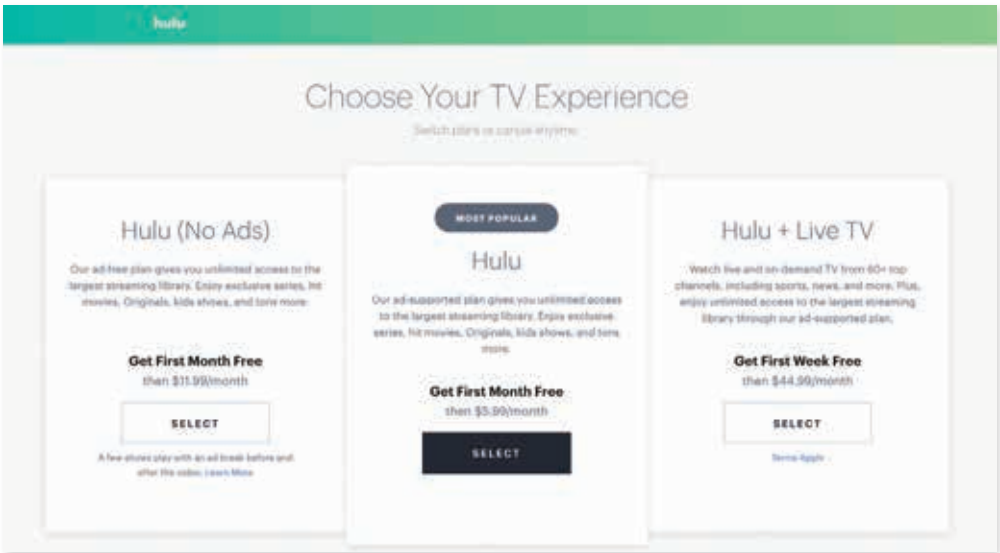
Plačljivi račun Spotify odpremo tako, da vzpostavimo povezavo VPN, ki nas storitvi predstavi kot Nemca. Priporočamo, da na uradni spletni strani naredimo nov uporabniški račun, saj bo v nasprotnem primeru prehod težaven. Ob odpiranju računa je potreben vnos domačega naslova. Pomagamo si z Google Maps in se navidezno preselimo v Nemčijo. Izberemo plačljivo storitev Premium, ki je prvi mesec brezplačna, a kljub temu zahteva vnos podatkov s kreditne kartice. Če bi v tem koraku vpisali slovensko kartico, bi se postopek ustavil, N26 pa je prepoznana kot nemško plačilno sredstvo in nam omogoča tudi naročnino Family, v kateri lahko uživa do pet družinskih članov. A, pozor, Spotify je precej strog do tega, komu dodelimo dostop. S sprejetjem pogojev se strinjamo, da vsi uporabniki istega računa živijo pod isto streho. To je treba dokazati tako, da članom ob ustvarjanju računa vpišemo enak naslov, kar pomeni natanko iste podatke iz Nemčije, ki smo jih vpisali pri stvaritvi glavnega računa. Po uspešno izvedenem postopku postanemo ponosni naročnik storitve Spotify Premium. Povezave VPN in drugih zvijač ne potrebujemo več, saj je Spotify naročnikom na voljo tudi v tujini, v našem primeru Sloveniji.

Zaključek

S povezavo VPN so nam dostopne privlačne ponudbe z vseh koncev sveta. Čeprav spletne cenzure v Sloveniji ni, nam tujci običajno ne privoščijo vsega. Kot čokolada Milka z zahoda je tako tudi pri nas dostopna pretočna storitev Amazon Prime z VPN boljša. Poleg bogatejše bere vsebin nas preseneti uporabniški vmesnik, ki med drugim ob zaustavitvi predvajanja omogoča iskanje informacij o igralcih s prizora na televiziji. Na podoben način si privoščimo ameriško video storitev Hulu, ki ob sklenitvi naročnine zahteva tudi tuje plačilno sredstvo, Applove časopise, knjige in še kaj bi se našlo. ◀

▽ **VPN običajno potrebujemo zgolj pri naročanju izbranega paketa, ob naslednjem obisku aplikacije Spotify se glasba ponavadi predvaja tudi brez maskirane povezave.**





▷ **Ameriška pretočna storitev Hulu podobno kot Spotify ob sklenitvi naročnine zahteva tuje plačilno sredstvo.**

Popolni nadzor nad pametnim telefonom

V pametni telefon vgrajena programska oprema proizvajalca je pogosto precej omejujoča in ne dovoljuje poljubnih načinov uporabe njegovih funkcionalnosti. Ga lahko odklenemo? Je to legalno? Se izplača?

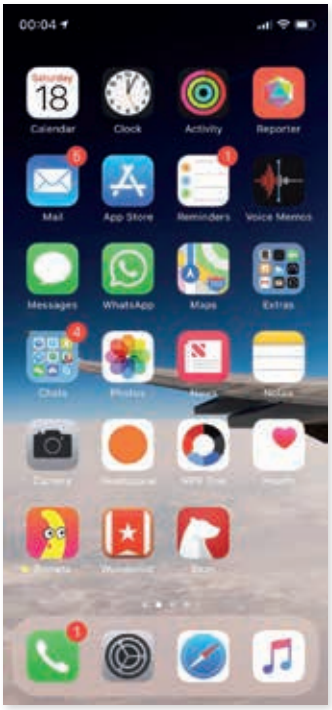
Simon Peter Vavpotič

Odkar je v devetdesetih letih preteklega stoletja odprta arhitektura IBM PC zavladala svetu računalništva, smo bili vajeni domače računalnike z vso programsko opremo v njih pomili volji sestavljati in spreminjati. A s prihodom zmogljivih nosljivih naprav, predvsem pametnih telefonov, smo ponovno soočeni s celovitimi računalniškimi rešitvami s prednaloženimi strojno in sistemsko programsko opremo ter osnovno aplikacijsko programsko opremo.

Večina proizvajalcev se je zaradi varovanja svojih poslovnih interesov, zakonodaj različnih držav, zanesljivejšega varovanja osebnih podatkov manj izkušenih uporabnikov, zmanjševanja stroškov zaradi odprave okvar programske opreme v jamstvenem roku in preprečevanja hekerskih vdorov, odločila navadnim uporabnikom onemogočiti neposredno poseganje v sistemsko programsko opremo. Kljub temu so za razvijalce aplikacijske programske opreme vgradili posebne postopke, s katerimi lahko odklenejo (del) zaklenjenih funkcionalnosti in na ta način lažje razvijajo ter testirajo novo aplikacijsko programsko opremo. Prav tako so jim omogočili (omejen) dostop do nekaterih sistemskih sredstev, kot so zaslon, kamere in mikrofoni, saj se njihove aplikacije le tako lahko enakovredno kosajo s serijsko vgrajenimi.

Drugi razlog za odklepanje pametnega telefona so prednaložene aplikacije in storitve, s katerimi lahko proizvajalci, operaterji mobilne telefonije in ponudniki internetnih storitev nemalokrat posredno (anonimno) spremljajo naše delo in navade uporabe mobilnega telefona. Teh večinoma brez naložitve alternativnega (»čistega«) operacijskega sistema ne moremo odstraniti. Med njimi so tudi nadvse uporabne storitve, denimo sprejemanje signala GPS s prikazom uporabnikovega položaja na zemljevidu, ki potrebujejo dostop do strežnika z zemljevidi, vendar ob njihovi uporabi ponudnik storitve zemljevida natančno ve, kje se uporabnik v nekem trenutku nahaja. Večina telefonov hkrati nima aplikacije z lastnim zemljevidom (četudi grobim) in s prikazom koordinat zemljepisne dolžine ter širine, ki bi jo lahko uporabljali brez povezave z internetom.

Tretji razlog so neprestane (samodejne) spletne posodobitve vgrajenih aplikacij in vgrajene sistemske programske opreme, ki lahko ustvarijo tudi dobršen del mesečnega spletnega prometa brez naše vednosti, hkrati pa predstavljajo potencialno tveganje za hekerski vdor v pametno napravo. Zato ne



△ **Namizje sodobnega pametnega telefona z iOS 12.**

preseneča, da je uporabnikov, ki si želijo prevzeti popoln nadzor nad programsko opremo v svojih pametnih napravah, iz leta v leto več. Veliko je tudi takih, ki želijo povsem odkleniti in do potankosti raziskati svojo napravo ter izkoriščati vse njene zmogljivosti.

Kaj zmore odklenjeni pametni telefon?

Odklenjen pametni telefon ali drug računalnik, katerega vgrajeno programsko opremo zamenjamo z alternativno, lahko omogoča načine uporabe, ki jih proizvajalci in ponudniki storitev mobilne telefonije z zaklepanjem načrtno onemogočajo. Razlog so navadno zahteve zakonodajalcev ali celo neformalne zahteve varnostnih služb različnih držav.

Odklenjen pametni telefon se lahko z zamenjavo vgrajene programske opreme in/ali dodatkom ustrezne aplikacijske opreme spremeni v napravo za (tajno) snemanje in opazovanje, kar je gotovo lahko razlog za preplah. Čeprav so strojne arhitekture pametnih telefonov skrbno varovane skrivnosti njihovih proizvajalcev, temeljijo le na nekaj različnih tipih procesorskih jeder (ARM, redko Intel …) in uporabljajo podobne periferne enote (npr. kamere, avdio kodeke, zaslone), katerih gonilniki so medsebojno združljivi na ravni

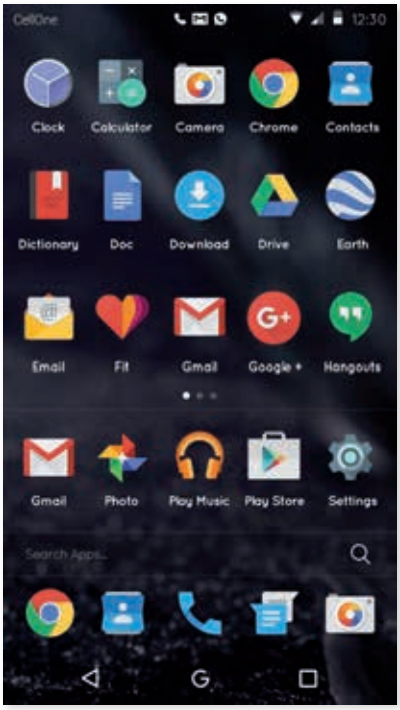
JAMSTVO

Je zamenjava vgrajene programske opreme legalna? Lahko izgubimo jamstvo?

Večina držav nima nič proti, če prelisičimo varnostne protokole lastnega pametnega telefona, si pridobimo polne skrbniške pravice in vgrajeno programsko opremo v njem zamenjamo z drugo združljivo legalno programsko opremo. A, pozor! Evropska direktiva o avtorskih pravicah iz leta 2001 le izjemoma dovoljuje tovrstno početje z namenom nameščanja in poganjanja alternativne vgrajene programske opreme, vendar ga prepoveduje za namene kopiranja in povratnega inženirstva. Obenem evropska direktiva 1999/44/EC določa, da z zamenjano vgrajene programske opreme ne izgubimo jamstva za strojno opremo, če nova vgrajena programska oprema ne bi mogla povzročiti odpovedi strojne opreme. Implementacija omenjenih direktiv je kljub temu odvisna od držav članic Evropske unije.

Po drugi strani lahko v nekaterih državah po svetu proizvajalec med licenčne pogoje izrecno zapiše in uveljavlja pravico do preklica veljavnosti jamstva v primeru zamenjave vgrajene programske opreme. V takih primerih moramo pred kakršnimikoli posegi v napravo dobro pretehtati, ali se nam ti dejansko izplačajo.

Še to! Zakonodaje določenih držav po svetu odklepanje in posege v zaklenjeno v sistemsko programsko opremo pametnih telefonov in drugih elektronskih naprav v vsakem primeru štejejo za nezakonite. V teh jamstva ne bomo mogli uveljavljati. Vprašljivi so lahko tudi legalnost pridobitve, uporabe in posedovanja programske opreme za odklepanje ter nameščanje nove vgrajene programske opreme in njena uporaba v elektronski napravi. Lahko pa namesto tega kupimo odklenjen pametni telefon za razvijalce ali takega, za katerega orodja za odklepanje nudi proizvajalec.



△ **Android 8.0 – OREO je zahvaljujoč nadobudnim programerjem na voljo tudi na starejših telefonih, iz GitHub pa dobimo tudi izvorno kodo.**

operacijskega sistema. Pri zaklenjeni pametni napravi je njihova uporaba običajno vezana na kontekst dela. Ko nas nekdo pokliče po telefonu, se snemanje iz mikrofona in/ali video kamere prekine in upravljanje obeh naprav prevzame aplikacija za sprejem telefonskih klicev. Obenem sta video in avdio snemanje mogoča le takrat, ko je namenska aplikacija v ospredju.

Odprt dostop do funkcionalnosti gonilnikov uporabniku omogoči uporabo funkcionalnosti telefona ne glede na kontekst. Denimo aplikacija za video in zvokovno snemanje lahko shranjuje video in avdio tudi med telefonskim pogovorom. Še več! S posebno aplikacijsko programsko opremo, ki daje nepoučenemu videz nedolžnega brskanja po Facbooku, lahko uporabnik upravlja vgrajene kamere in mikrofone ter shranjuje video in avdio posnetke ali pa prek omrežij 4G sproti v živo posreduje sliko in zvok na oddaljen spletni strežnik. S prirejenimi gonilniki za strojno opremo lahko pametni telefon izvaja programske aplikacije celo, ko je njegov zaslon povsem izklopljen, pri čemer ga tipka za vklop in izklop le na videz izklopi.

Alternativni operacijski sistemi in aplikacije

Nalaganje alternativne sistemske programske opreme in sistemske aplikacijske programske opreme, ki dostopa do zaščitenih sistemskih sredstev, zahteva največje skrbniške pravice, do katerih lahko pridemo le z odklepanjem pametne naprave ali tako, da kupimo posebno nezaklenjeno različico za razvijalce, ki je pogosto na voljo le ob dodatnem plačilu in podpisu pogodbe s proizvajalcem.

Nekateri veliki proizvajalci, med katerimi so Asus, Sony in Google, so zato sami za vse uporabnike zagotovili (brezplačna) programska orodja za (legalno) odklepanje svojih izdelkov, ki omogočajo tudi nalaganje alternativnih operacijskih sistemov. Ostali uporabniki se morajo zanesti na nadobudne razvijalce in hekerje ter najti podobna programska orodja za svoje pametne telefone na spletu.

S podobnimi problemi se spopadajo tudi lastniki Applovih pametnih telefonov z operacijskim sistemom iOS, katerih zaklenjeni zagonski nalagalnik programov ne dovoljuje dodajanja aplikacij, razen uradno potrjenih iz trgovine Apple Application Store. Vendar se morajo pri t. i. Jailbreakingu zanesti le na alternativne programske rešitve s spleta, saj si pri Applu zelo prizadevajo preprečevati tovrstne prakse.

Kako do polnih skrbniških pravic v Androidu?

Pred odklepanjem pametnega telefona ali druge pametne naprave oziroma poskusom pridobitve polnih skrbniških pravic se je treba zavedati, da lahko z nekaj neznanja in/ali smole svoj telefon tudi nepovratno zaklenete (ga spremenite v t.i. opeko oz. »brick«), zato se tega lotite zelo resno, previdno in odgovorno. Predvsem pa je pametno izdelati in shraniti varnostno kopijo svojih osebnih podatkov in izdelati sliko obstoječe vgrajene programske opreme (vendar samo za lastno uporabo!), saj bomo lahko le tako v primeru neuspešne odklenitve ali zamenjave operacijskega sistema ponovno namestili starega.

Osnovna programska orodja za pridobitev polnih skrbniških pravic izkoriščajo različne programske hrošče in varnostne pomanjkljivosti v vgrajeni sistemski programski opremi ter strojni opremi različnih pametnih naprav, s katerimi je mogoče zaobiti zaščite pred spreminjanjem jedra Androida. Njihov cilj je izdelati prilagojeno obnovitveno kopijo vgrajene programske opreme, ki ne preverja digitalnih podpisov posodobitev operacijskega sistema, in s tem omogočiti njegovo spreminjanje ter pridobitev polnih skrbniških pravic.

Starejše metode za odklepanje pametne naprave se zanašajo na most za razhroščevanje, o katerem lahko več preberete v

TEHNIČNO

Inženirski pogled na notranjo zgradbo pametnega telefona

V zadnjih desetih letih smo bili priče bliskovitemu razvoju mikrokrmilnikov in računalnikov v enem čipu s procesorskimi jedri ARM. Če so ti včasih delovali predvsem kot krmilniki analognih preklopnih vezij, digitalni signalni procesorji ter zajemalniki in analizatorji analognih in digitalnih signalov, lahko danes prek brezžičnih modulov (WiFi, GSM, Bluetooth …) prisostvujejo v različnih digitalnih omrežjih ter obenem na zaslonih LCD prikazujejo barvno grafiko in sprejemajo pritiske z zaslona na dotik ter celo zajemajo slike in videe z digitalnih kamer.

Razvojna tiskana vezja, s katerimi proizvajalci mikrokrmilnikov snovalcem novih elektronskih naprav ponudijo možnost hitrega začetka prototipiranja, postajajo zato vsako leto bolj podobna notranji zgradbi pametnih telefonov. Najzmogljivejšim moramo pogosto dodati le še ustrezen komunikacijski modul in ob pomoči številnih programskih knjižnic ter primerov njihove uporabe izdelati ustrezno vgrajeno programsko opremo in že imamo pametni telefon s popolno podrobno dokumentacijo.

HROŠČI

Vzpostavitev mostu za razhroščevanje

Razvojno okolje za Android komunicira z mobilno napravo prek ADB (*Android Debug Bridge*, slov. Androidov most za razhroščevanje), ki je del Android SDK. Za vzpostavitev ADB je potreben tudi poseben gonilnik, ki ga izda proizvajalec mobilne naprave. Hkrati je potrebno delovanje ADB omogočiti tudi na sami mobilni napravi. Proizvajalci mobilnih naprav uporabljajo razne trike, s katerimi preprečijo nehoten vklop ADB. Pogosto je predpogoj za ADB vklop način za razvijalce, ki ga dosežemo prek nastavitev mobilne naprave. V nastavitvah (angl. *Settings*) moramo navadno poiskati meni *About phone* (slov. O telefonu), znotraj tega pa postavko *Build number* (slov. Številka izgradnje), na katero od 7- do 10-krat kliknemo. S tem v nastavitvah omogočimo dodatni meni, *Developer options* (slov. Opcije za razvijalce). Nato v opcijah omogočimo ADB prek USB.

Vzpostavitev ADB je predpogoj za hitro razhroščevanje in testiranje mobilnih aplikacij, ne da bi jih morali ročno nameščati na mobilno napravo v obliki paketov *.APK.

Za uporabo ADB moramo ustrezno programsko opremo namestiti tudi v osebni računalnik. Še posebej pomembna je namestitev ustreznega gonilnika, ki odpre funkcionalnosti ADB pametnega telefona.

NASVET

Primer nalaganja **alternativne vgrajene programske opreme za Android** po korakih

Na spletu poiščemo specializirani gonilnik USB za svoj pametni telefon ter aplikaciji za vzpostavitev ADB (programski paket *Minimal ADB and Fastboot*) ter varnostno shranjevanje vgrajene programske opreme in obnovo telefona (npr. recovery.img) in jih namestimo.

Namestimo posebni gonilnik za razhroščevanje za pametni telefon in programski paket *Minimal ADB and Fastboot* (samo razširjanje in kopiranje v izbrano mapo) v operacijski sistem osebnega računalnika.

V pametnem telefonu vklopimo način za razvijalce (glej okvirček Vzpostavitev mostu za razhroščevanje).

Odpremo mapo, kjer je nameščen paket *Minimal ADB and Fastboot*, povežemo pametni telefon prek priključka USB in izvedemo ukaz *adb devices*, ki pokaže, koliko naprav na vodilu USB podpira ADB. Če take naprave ni, morda posebni gonilnik za pametni telefon ni pravilno nameščen ali pa ne more delovati. Na primer, če ni digitalno podpisan, moramo operacijski sistem zagnati v ustreznem načinu delovanja, da ga bomo lahko uporabili. Mogoče je tudi, da smo na pametnem telefonu pozabili vključiti način za razvijalce.

Zaženemo ukaz *adb reboot bootloader*, s katerim zaženemo pametni telefon v načinu, ki omogoča uporabo orodij za obnovo vgrajene programske opreme. Alternativno lahko ta korak navadno izvedemo tudi s posebno opcijo iz menija za ponovni zagon v operacijskem sistemu pametnega telefona, ko je vključen način za razvijalce.

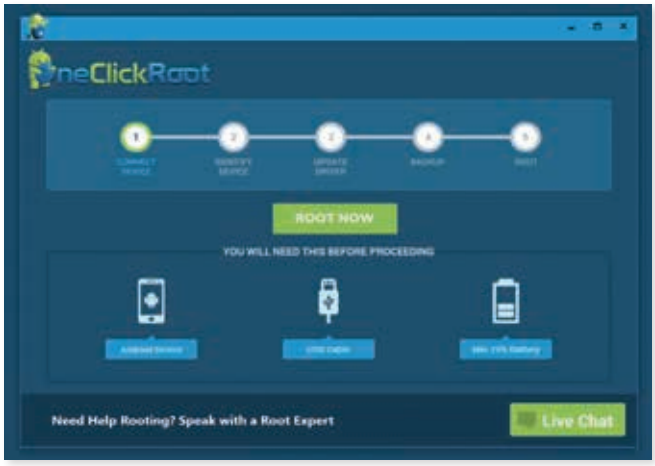
Ko je pametni telefon pripravljen, iz konzole zaženemo ukaz *fast boot recovery.img* (namesto *recovery.img* zapišemo dejansko ime orodja), s katerim zaženemo programsko orodje za varnostno shranjevanje in obnovo vgrajene programske opreme.

Zdaj potrebujemo le še kako kartico microSD, kamor lahko odložimo staro vgrajeno programsko opremo oziroma z nje prenesemo novo, ki smo jo poprej pobrali s spleta.

Naložimo alternativno vgrajeno programsko opremo za svojo pametno napravo, ki smo jo poprej v posebni datoteki prenesli s spleta.

okvirčku, druge pa na posebne aplikacije, pri katerih zadošča že pritisk enega samega gumba na zaslonu. Kljub temu ni nujno, da bomo v katerikoli pametni napravi lahko uporabili poljubno metodo. V zadnjem času so se na spletu pojavile tudi nove metode pridobitve skrbniških pravic brez spreminjanja sistemske particije v podatkovnem pogonu pametnega telefona.

▽ **Pridobitev polnih skrbniških pooblastil v Androidu z enim klikom.**



Ko prelisičimo varnostno programsko opremo, je polne skrbniške pravice mogoče pridobiti, na primer, z nadomestitvijo originalnega programčka su, ki omogoča izvajanje aplikacij s povečanimi pooblastili, s takim, ki zagotavlja neomejene skrbniške pravice. Pri tem z novo datoteko v mapi /system/xbin/ najprej nadomestimo stari su, nakar novemu z običajnim ukazom chmod podelimo pravico izvajanja v operacijskem sistemu. Za lagodnejše delo so hekerji izdelali tudi posebne sistemske aplikacije za selektivno podeljevanje največjih pooblastil posameznim uporabniškim aplikacijam. Tako imajo največja pooblastila zgolj tiste, ki jim to sami dopustimo.

Ker pa večina nadobudnih uporabnikov pametnih telefonov ni veščih programiranja in sistemskega skrbništva, najdemo na spletu veliko programskih orodij, ki so veliko enostavnejša za uporabo. Denimo Magisk omogoča največje skrbniške pravice le določenim aplikacijam, medtem ko jih nikoli ne podeli tistim, ki bi iz varnostnih razlogov prenehale delovati. Med najpopularnejšimi orodji za pridobitev polnih skrbniških pravic v operacijskem sistemu Android je tudi SuperOneClick, ki deluje v skoraj vseh pametnih telefonih in različicah Androida prek povezave USB.

Po drugi strani so nekateri proizvajalci pametnih telefonov, med katerimi so tudi LG, HTC in Motorola, za določene tipe svojih pametnih telefonov zagotovili t. i. legalna orodja za pridobitev polnih skrbniških pravic, ki odklenejo nalagalnik operacijskega sistema. Zelo enostavno lahko odklenemo tudi Googlove pametne telefone Nexus, za katere je dovolj, da jih prek priključka USB povežemo z osebnim računalnikom, nakar prek protokola Fastboot izvedemo ukaz fastboot oem unlock.

Kljub temu je veliko proizvajalcev v preteklosti izbralo nasprotno pot in poskušalo izdelati pametne naprave s kompleksnejšimi zaščitami, za katere ne bi bilo moč izdelati orodij za pridobitev polnih skrbniških pravic, vendar se je kasneje izkazalo, da so bila ta na voljo na spletu že nekaj mesecev po začetku prodaje takih izdelkov.

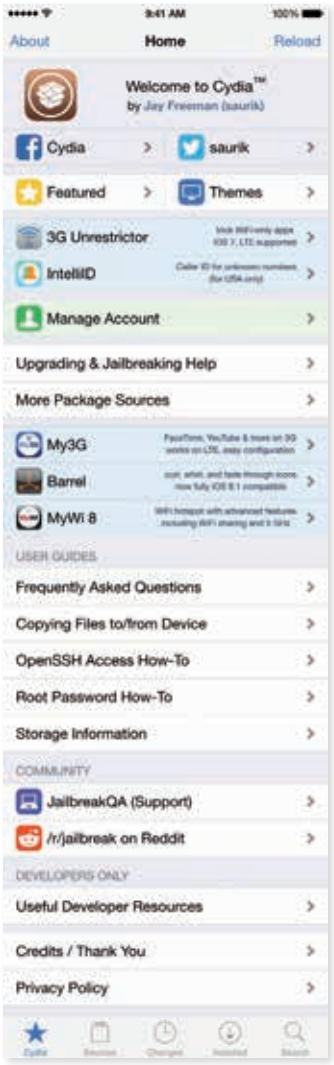
Zamenjava operacijskega sistema Android

Googlov operacijski sistem Android je odprtokoden, vendar morajo proizvajalci pametnih naprav zanj pripraviti ustrezne gonilnike, a večina tudi nekoliko prilagodi videz namizja in sistemskih nastavitev ter doda svoje aplikacije. Kljub temu za večino pametnih telefonov in drugih pametnih naprav na spletu najdemo (novejše) ljubiteljske različice Androida, ki se bolj ali manj opirajo na osnovno Googlovo različico, gonilniki pa so pogosto prekopirani iz različic proizvajalcev. In prav to je razlog, da novejše različice Androida za posamezno pametno napravo dobimo le toliko časa, dokler so združljive z razpoložljivimi različicami gonilnikov. Navadno je v ločeni namestitvi na voljo tudi programski paket s priljubljeno dodatno programsko opremo, ki se ga izplača namestiti tistim, ki želijo približno enako ali večjo funkcionalnost, kot jo nudita programski opremi proizvajalca in operaterja mobilnih storitev. Namesto tega lahko dodatno programsko opremo posamezno prenesemo s spleta.

Kako osvoboditi iOS?

Naprave z operacijskim sistemom iOS niso samo pametni telefoni, temveč tudi tablični računalniki in televizorji. Podobno kot pri pridobivanju polnih skrbniških pravic za Android tudi za pridobitev polnih skrbniških pravic v iOS potrebujemo posebna programska orodja, ki izkoriščajo varnostne luknje operacijskega sistema. Apple se zato v vsaki novi različici iOS (po)trudi zakrpati vse stare varnostne luknje in obenem v novejših različicah ne dovoljuje poljubne povrnitve svojih starih različic z nezakrpanimi ranljivostmi (angl. arbitrary downgrades), temveč le za nekaj podrazličic nazaj (npr. z iOS 12.1.4 na iOS 12.1.2). Kljub temu hekerjem še vedno uspeva priprava ustreznih programskih orodij za osvobajanje iz ječe že nekaj mesecev po izidu nove različice iOS.

A osvoboditev iz ječe ni vedno trajna, saj moramo pri t. i. osvoboditvah na povodec (angl. tethered jailbreaks) ob vsakem ponovnem zagonu pametne



△ **Alternativni nalagalnik aplikacij s spleta Cydia za iOS 12.**

naprave to predhodno povezati z osebnim računalnikom prek priključka USB. V nasprotnem lahko med zaganjanjem obstane ali pa se zbudi v napol delujočem stanju. Težavam ob ponovnem zagonu se lahko pogosto izognemo tako, da ponovno zaženemo le namizje, imenovano SpringBoard. Temu postopku žargonsko pravijo tudi respringing.

Drug način osvoboditve iz ječe je polovična osvoboditev na povodec, pri kateri pametno napravo sicer lahko ponovno zaženemo brez pomoči osebnega računalnika, vendar v tem primeru nudi le zelo okrnjeno osnovno funkcionalnost. Odklenjene funkcionalnosti in aplikacije brez veljavnih elektronskih podpisov (npr. tiste, ki jih urejamo z nalagalnikom alternativnih programskih paketov, Cydia) namreč niso več na voljo, saj zaščiteni nalagalnik programov ponovno deluje.

Najbolj priljubljeni način odklepanja je trajna osvoboditev iz ječe brez povodca, pri kateri v pametno napravo naložimo spremenjeno jedro operacijskega sistema in jo lahko vsakokrat v odklenjenem stanju ponovno v celoti zaženemo brez pomoči osebnega računalnika. Žal je ta način na voljo zgolj za starejše različice iOS, medtem ko lahko za najnovejše od leta 2016 uporabljamo tudi polovično osvoboditev brez povodca, pri kateri ob ponovnem zagonu pametne naprava ne potrebujemo pomoči osebnega računalnika, a moramo namesto tega ponovno namestiti aplikacijo, ki iOS spet reši iz ječe.

Se izplača?

Pridobitev polnih skrbniških pooblastil in odklenitev nalagalnika programov v pametni napravi ima dobre in slabe lastnosti. Dobro je to, da lahko v odklenjeni napravi poganjamo alternativno programsko opremo, med drugim tudi tako, ki ni potrjena pri proizvajalcu, slabo pa to, da je v odklenjeno napravo hekerjem nemalokrat dosti lažje vlomiti, hkrati pa lahko z neprimerno programsko opremo napravo tudi fizično poškodujemo (npr. preveč izpraznimo akumulatorsko baterijo, »skurimo« mikrokrmilnik itn.).

Že leta 2009 je neki 21-letni študent iz avstralskega Wollongonga izdelal prvega spletnega črva, in sicer iKee, ki se je lahko naselil le v iz ječe osvobojene pametne telefone z operacijskim sistemom iOS. Na ta način naj bi opozoril imetnike pametnih naprav na nevarnosti njihovega odklepanja. Odklenjena naprava, denimo, omogoča namestitev storitve SSH, ki jo moramo po namestitvi sami zakleniti oziroma zavarovati, saj ima prednastavljeno geslo. A zanimivo je, da so že istega meseca, kot je bila objavljena novica o iKee, iz podjetja F-Secure sporočili, da so na Nizozemskem odkrili zlonamernega spletnega črva, ki je vlamljal v zaščitene bančne transakcije uporabnikov iz ječe rešenih naprav z iOS.

Dober premislek o tem, ali zares potrebujemo odklenjeno funkcionalnost, tako ni odveč. Vsekakor je mogoče v odklenjeni pametni napravi tudi bistveno povečati informacijsko varnost v primerjavi z zaklenjeno, vendar to zahteva veliko računalniških znanj in posebnih programskih orodij, ki jih nima niti večina izkušenih uporabnikov in programerjev. Pri vsakdanji uporabi pametne naprave, v skladu z navodili in nameni proizvajalca, odklenjene funkcionalnosti skoraj gotovo ne bomo potrebovali. Če pa želimo napravo uporabljati predvsem v raziskovalne namene ali za igranje zastonjskih/ukradenih računalniški iger s spleta, je raje ne uporabljajmo tudi za varno elektronsko poslovanje … ◀

▷ **Ena izmed spletnih strani, s katerih lahko prenesemo orodja za pridobitev polnih skrbniških pooblastil za različne pametne naprave.**

NASVET

Primer »reševanja iOS 12 iz ječe« z orodjem Unc0ver po korakih

Predpogoji: Izdelamo varnostno kopijo svojih podatkov, pobrišemo vse datoteke 12 OTA v *Settings->Storage* in ponovno zaženemo napravo, namestimo profil tvOS 12 na napravo, s čimer preprečimo posodobitve iOS, ter ponovno zaženemo napravo. Različice iOS, od 12.1.3 in do 12.1.4, ki jih Unc0ver ne podpira, lahko pred postopkom nadomestimo z iOS 12.1.1 beta ali iOS 12.1.2, vendar z zadnjim le, če naložimo povsem zadnjo različico Unc0ver.

S spleta prenesemo zadnjo različico Unc0ver in gremo v mapo *ignition.fun*, kjer poiščemo preneseno namestitveno datoteko z Unc0ver in jo namestimo.

V *Settings->General->Device Management* kliknemo na ime razvijalca (*developer name)* in nato izberemo možnost zaupanja certifikatu. V nasprotnem Unc0ver ne bo mogoče zagnati.

Zaženemo Unc0ver in pritisnemo gumb *Jailbreak*, nakar se mora na domačem ekranu pojaviti ikona *Cydia*. Če se ne, moramo ponovno zagnati pametno napravo in poskusiti znova.

Nadaljnje branje

Vse o odklepanju naprav z operacijskim sistemom Android
www.androidrootguide.com

Pregledni članek o tem, kako rešiti iOS iz ječe
en.wikipedia.org/wiki/IOS_jailbreaking

Temna plat sodobnih vozil

Hollywoodski scenarij, po katerem hekerji prevzamejo nadzor nad vozilom v salonu in se iz njega zapodijo na ulico, je resda malo verjeten, a informacijska varnost vse bolj digitaliziranih vozil je na resni preizkušnji – ki je pogosto ne prestane.

Miran Varga

△ **Sistemi odklepanja vozila brez ključa tatovom še dodatno olajšajo delo.**

Uporabniki od sodobnih vozil ne pričakujemo zgolj prevoza od točke A do točke B, temveč predvsem odlično uporabniško izkušnjo. To želijo proizvajalci oziroma ponudniki vozil (če jih najemamo kot storitev) zagotoviti z različnimi pristopi, pri čemer prednjačijo info-zabavni sistem in rešitve, ki vozniku pomagajo upravljati vozilo, ohraniti smer vožnje ter varovati vozilo pred najrazličnejšimi nevšečnostmi.

V manj kot desetletju smo dobili izjemne sisteme za pomoč pri vožnji in povezljivost vozil z zunanjim okoljem. Od integracije pametnih telefonov oziroma mobilnih aplikacij do avtonomne vožnje – trendi so očitni, čez nekaj let si lahko obetamo javno uporabo vozil brez voznikov. Ali pa tudi ne. Odvisno od tega, kako bodo načrte avtomobilske in tehnološke industrije ter vlad in regulatornih organov prekrižali napadalci. Skrb za varnost in zasebnost posameznika oziroma voznika ali potnika v vozilu mora biti na prvem mestu. A groženj v svetu današnjih povezanih vozil kar mrgoli, v prihodnje pa bo treba (za)ščititi ne le avtonomna vozila, temveč tudi ekosisteme, v katerih bodo delovala.

Izziv je očiten: v prihodnje bodo morala povezana vozila sprejeti vedno več odločitev, ki bodo odločale med življenjem in smrtjo (potnikov ali drugih udeležencev v prometu), zaznavati fizične objekte in različne digitalne sisteme v svoji bližini ter sočasno zbirati, obdelovati in hraniti goro podatkov, tudi osebnih, ki jih bodo potrebovala bodisi za delovanje bodisi za monetizacijo storitve prevoza. Največji izziv bo, kako zagotoviti, da bodo najrazličnejši sistemi varno vzajemno delovali v »napravi«, ki se premika z veliko hitrostjo. Varnostni strokovnjaki že opozarjajo tudi na skrita tveganja, ki niso nujno povezana s samimi vozili. Sistem vozila oziroma njegovo odločanje ogrozi že manipulacija zunanjih dejavnikov – če pametna cesta ali ulična razsvetljava vozilu sporoča povsem napačne podatke, se to lahko napačno odloči in nesreča je neizogibna. Varnost pa mora biti in ostati ključna prioriteta prometa prihodnosti. Ta bo deloval kot svojevrsten internet stvari, v katerem bodo vozila povezana med seboj, z infrastrukturo in najrazličnejšimi sistemi ter bodo morala biti kos cunamiju podatkov, ki jih bo stalno zalival.

△ **Faradayevo kletko za avtomobilske ključe lahko izdelamo tudi sami. Kovinsko posodo obložimo z aluminijasto folijo.**

▽ **Sodobna vozila so skupek računalniških sistemov. Že ranljivost posameznega dela je dovolj, da napadalci pridobijo delni ali popolni nadzor nad vozilom.**

Odklepanje elektronskih ključavnic – v 60 sekundah

Odklepanje vozil brez ključa, t. i. *keyless* sistemi, prinaša dodatno udobje lastniku vozila, a hkrati tudi skrbi. Policijska statistika po svetu beleži znaten porast kraj teh vozil, varnostne kamere, nameščene na objektih, kjer so bila vozila ukradena, pa so razkrile, za kako relativno preprosto tatvina poteka. Napadalca sta navadno dva. Njuna oprema sta le oddajnik in ojačevalnik signala, ki ju lahko tako rekoč vsakdo na trgu kupi za nekaj sto evrov. Napadalec z ojačevalnikom signala se približa stavbi v upanju, da bo ojačevalnik zaznal ključ vozila in okrepil njegov signal ter ga prenesel

NAPREDEK

Zahtevne in pogosto računalniško gnane **inovacije**

Sodobni avtomobili so računalniški centri v malem, saj v povprečnem vozilu že najdemo več deset računalnikov. Ti krmilijo delovanje motorja, pospeševanje, zavijanje, zavore, ključavnice, stekla, klimatsko napravo, navigacijo, info-zabavni sistem in še številne druge gradnike vozil, predvsem asistenčne sisteme. Medtem ko parkirne senzorje, ki voznikom pomagajo natančneje parkirati, poznamo že več desetletij, so avtomobili s funkcijo samodejnega parkiranja na voljo bistveno manj časa. Pionir na tem področju je bil Toyotin prius z letnico 2003, in čeprav so takrat vsi napovedovali, da bodo v nekaj letih to funkcijo ponujali vsi proizvajalci vozil, se to vendarle ni zgodilo. Celo premijska znamka BMW ali pa bolj ljudska Ford sta rabili kar šest let, da sta postregli s podobno rešitvijo. Poleg tega samodejno parkiranje vedno ne deluje, kot je oglaševano, kar je na lastni koži oziroma plastiki izkusil tudi pisec teh vrstic. V zadnjem desetletju so inovatorji v avtomobilski industriji prestavili eno, če ne kar dve prestavi više. Parkirni pomočniki, zaznavala voznega pasu in sistemi za preprečevanje trkov so vse pogosteje na seznamih standardne (pogosto pa še vedno doplačilne) opreme modernih vozil.

Združenje avtomobilskih inženirjev se osredotoča predvsem na sveti gral – avtonomno vožnjo. Ta ima po njihovi lestvici šest ravni – od 0 do 5. Večina avtomobilov, ki se danes »kotalijo« po cestah, je na stopnji 0. Opremljeni so z avtomatiziranimi sistemi, ki vozniku pošiljajo takšna in drugačna opozorila in lahko zgolj začasno posežejo v upravljanje vozila, a tega ne prevzemajo v celoti. Na stopnji 1 najdemo sisteme, ki prevzemajo krmilo ali upravljanje hitrosti, ne pa obojega hkrati. Najzgovornejši sistem je prilagodljivi tempomat. Zanimivo postane šele na stopnji 2, kjer najdemo avtonomne sisteme, ki lahko v določenih situacijah prevzamejo krmiljenje vozila, pospeševanje in zaviranje, čeprav pri tem zahtevajo, da je za volanom ves čas tudi voznik, ki kadarkoli lahko poseže v upravljanje.

Letošnje leto bomo priče več avtomobilom, ki bodo dosegli stopnjo 3. Eden takšnih je, denimo, povsem novi audi A8, ki vozniku ob določenih pogojih dovoljuje, da se prepusti samodejni vožnji – npr. ob počasnem premikanju v prometnem zastoju. Omenjeno vozilo je opremljeno s kar 24 video, zvočnimi, radarskimi in laserskimi senzorji, ki skrbijo za to, da vozilo lahko zagotavlja avtonomno vožnjo v omejenem obsegu – predvsem pri manjših hitrostih in na cestah, kjer fizične ovire ločijo nasproti vozeči promet.

Od ideala smo torej še precej daleč. Na zadnji, povsem avtonomni stopnji 5 je vožnja človeka izključena, avtonomno vozilo pa brez poseganja voznika samostojno vozi po katerikoli cesti in v vseh pogojih. Takega primera še ni, a zdi se, da je najbliže temu dosežku podjetje Waymo, ki razvija Googlovo idejo avtomobila brez voznika. Po najbolj optimističnih napovedih naj bi podjetju res avtonomno vožnjo uspelo doseči že prihodnje leto. Množična tehnologija za povsem avtonomno vožnjo vozil pa bo verjetno nared vsaj desetletje pozneje.

do drugega napadalca, ki stoji ob avtomobilu z oddajnikom. V tem primeru bo drugi napadalec preprosto odprl vrata, sedel v vozilo, ga zagnal in se odpeljal. V skoraj popolni tišini, kar je še dodaten motiv za napadalce, da vozilo odtujijo skorajda nezaznavno. Celoten napad lahko traja manj kot minuto! Poročila o tatvinah ugotavljajo, da ta metoda deluje na razdalji med petimi in 20 metri, zato lahko napadalci enostavno odpeljejo večino vozil izpred hiš ali drugih nizkih objektov. Učinkovite zaščite pred to vrsto napada ni, saj napadalci z ojačanjem signala ključa vozilo pretentajo, da se ključ nahaja v neposredni bližini. Da bi preprečili tovrstne napade, bi morali lastniki vozil ključe hraniti v faradayevi kletki (nekateri kitajski podjetniki so že začeli izdelovati ovitke za ključe z ustrezno zaščito), uporabiti palice za zaklep volanskega obroča ali pa uporabljati parkirna mesta z zapornicami. Raziskovalci so to metodo preizkusili na različnih vozilih s šokantnimi rezultati – praktično ni proizvajalca in modela, ki bi bil imun za to težavo.

Heker L&M pravi, da bi lahko povzročil pravi prometni kaos po vsem svetu, tudi v Afriki.

Problematične mobilne aplikacije

Aprila letos je podjetjema, ki nudita mobilni aplikaciji iTrack in ProTrack za sledenje in upravljanje flot vozil, življenje močno zagrenil heker, ki se skriva za oznako L&M. Zlorabil je namreč več kot sedem tisoč uporabniških računov prvega podjetja in več kot 20 tisoč drugega. Heker je tako lahko prek sistema GPS spremljal lokacijo teh vozil po vsem svetu in v primeru nekaterih novejših vozil lahko tudi ugasnil motor na daljavo.

"Če bi želel, bi lahko povzročil pošteno prometno zmedo po svetu, saj imam popoln nadzor nad več sto tisoč vozili." Heker L&M

K sreči gre za varnostno funkcijo, ki jo je lahko aktiviral šele, ko je vozilo vozilo z 20 km/h ali manj. Kako mu je to uspelo? Relativno preprosto. S povratnim inženirингom omenjenih mobilnih aplikacij je ugotovil, da vsi uporabniki teh ob prijavi dobijo privzeto dodeljeno geslo 123456, ki ga očitno veliko uporabnikov sploh ni spremenilo. Nato je z napadom z grobo silo na vtičnik API omenjenih aplikacij pridobil več tisoč uporabniških imen, ki so omogočila prijavo s privzetim geslom. Tako je lahko odtujil veliko podatkov iz uporabniških računov, vključno s številkami in sistemi v vozilih. L&M je za spletno mesto *Motherboard* še povedal, da sta bila njegov cilj ponudnika aplikacij iTrack in ProTrack, ne pa na njune stranke, saj je želel, da odpravita varnostne pomanjkljivosti. »Če bi želel, bi lahko povzročil pošteno prometno zmedo po svetu, saj imam popoln nadzor nad več sto tisoč vozili, ki jim lahko s pritiskom na gumb ugasnem motor,« je še dejal heker L&M, ki je od podjetij zahteval nagrado, a sta se nato ti z njim začeli pogajati o ceni in hekerskem orodju.

Popolni prevzem nadzora

Hekanje mirujočih vozil je vse pogostejše. Prevzem nadzora, medtem ko je vozilo v gibanju, pa je precej redkejši pojav. Najpogosteje se ga lotijo raziskovalci. Pred skoraj štirimi leti je tehnološki svet osupnil posnetek dveh varnostnih strokovnjakov, ki sta se lotila iskanja pomanjkljivosti lastnega vozila. Charlie Miller in Chris Valasek sta v zadrego spravila proizvajalca Jeep, saj sta avtomobil cherokee lahko upravljala na daljavo. Z razdalje 15 kilometrov sta prevzela nadzor nad digitalnimi prikazovalniki, zavorami, menjalnikom, klimatskim sistemom, info-zabavnim sistemom, brisalci in motorjem. Miller in Valasek sta razvila vrsto lastnih orodij in že od leta 2013 dokazujeta, kako ranljiva so pravzaprav vozila, saj

△ **Miller in Valasek še posebej rada razkrivata pomanjkljivosti najrazličnejših sistemov v vozilih. Leta 2015 sta naredila velik preskok – prevzem nadzora nad vozilom sta opravila na daljavo in ko je bilo vozilo v gibanju.**

proizvajalci nimajo dovolj strokovnjakov za kibernetsko varnost, medtem ko želijo ugoditi zahtevam strank po povezljivosti v avtomobilih. A s tem, ko vozila spremenijo v pametne telefone na kolesih, močno povečajo tudi tveganje hekerskega napada in (popolnega ali delnega) prevzema nadzora nad vozilom.

So nevarnejši hekerji ali avtomehaniki?

Čeprav je nevarnost hekerskega napada na posamezno vozilo še vedno relativno majhna, varnostni strokovnjaki opozarjajo na vrsto drugih, nekoliko bolj pogostih težav. Ena od njih so nepošteni mehaniki. Ti skoraj ob vsakem servisu vozilo priklopijo na računalnik – najprej z namenom branja morebitnih napak in prepoznavanja okvar, resetiranja intervala vzdrževanja in/ali posodobitve sistemov v vozilu. A prek univerzalnih diagnostičnih vrat (*OBD – On Board Diagnostic*), ki jih premore sleherno vozilo, izdelano v tem tisočletju, lahko mehaniki z manj poštenimi nameni spremenijo marsikaj. Npr. nastavitve zavornega senzorja, ki se bo tako prožil hitreje in hitreje obrabil zavore, stranka pa bo na servisu pustila več denarja za nove zavorne diske in ploščice. Lahko tudi spremenijo štetje števca kilometrov, da bo prej dosegel želeno številko, uporabnik pa znova zavil na servis. S programsko opremo lahko vzdrževalec vozila izdela tudi kopijo ključa oziroma kode ključa in se čez nekaj časa sam ali z drugimi kriminalci pripelje po vozilo … Možnosti, ki jih imajo mehaniki pri manipulaciji vozil, so še precej večje od hekerjev, saj imajo ne le fizični dostop do vozila, temveč jim stranke vozilo v delavnici pustijo tudi po več ur.

▽ **Mar lahko popolnoma zaupamo mehanikom?**

Zasebnost je pomembna, a skoraj nemogoča

Ne le varnost, v času, ko sistemi v vozilih zbirajo in obdelujejo na tone podatkov, tudi osebnih, je še kako pomembna tudi zasebnost. T. i. črnih skrinjic ne poznajo le letala, temveč se po letu 2013 precej množično vgrajujejo tudi v vozila in so pri tem v izdatno pomoč preiskovalcem prometnih nesreč, saj jim omogočajo analizo podatkov vozila v trenutkih pred nesrečo.

V sodobnih vozilih je okoli 20 računalnikov, ki stalno zbirajo in obdelujejo podatke – od zavor do brisalnikov stekla obstaja skoraj sto točk, ki sporočajo različne podatke. Z opremo najbolj založena vozila lahko že danes vsako uro ustvarijo okoli 25 gigabajtov podatkov – nekaj od njih jih seveda pošljejo tudi »domov«, k proizvajalcu. Ti si prizadevajo poiskati načine, kako te podatke spremeniti v prihodke. In so pri tem uspešni.

Zasebnosti v današnjih vozilih ni prav veliko. Nekateri proizvajalci so že opravili eksperimente s prodajo lokacijskih podatkov proizvajalcem zemljevidov pa tudi s prodajo podatkov iz nameščenih kamer in senzorjev v vozilih najvišjim ponudnikom. Ker proizvajalci sodobnih vozil, opremljenih z brezžičnim vmesnikom ter GPS-povezavo, precej dobro vedo, kakšno glasbo poslušamo, kakšno kavo pijemo, kako vozimo, ali smo utrujeni in še marsikaj drugega, te podatke že prodajajo oglaševalcem in celo zavarovalnicam – ne da bi lastniki vozil to vedeli. Podjetja za izposojo vozil (t. i. *rent-a-car*) običajno pozabijo pobrisati vnose v info-zabavnih sistemih in navigaciji, pa čeprav bi lahko marsikdo po tem prepoznal prejšnjega voznika.

Pričakujemo lahko, da bomo v vozilih prihodnosti vozniki in potniki morali »poklikati« več odobritev za zbiranje in obdelavo podatkov – podobno kot to danes počnemo ob namestitvi novih mobilnih aplikacij na pametne mobilnike. Več ravni odobritev bo bržkone vgrajenih že v varnostne sisteme in se bomo z njimi morali samodejno strinjati. Sicer pa bo zagotavljanje zasebnosti v vozilu še precej pereča tema, saj številne strani navijajo za bolj razrahljane pogoje, ki bi jim omogočili monetizacijo ogromne količine podatkov. Če nas bo avtonomno vozeči avtomobil prevažal okoli, bi nam lokalni in globalni ponudniki nadvse radi servirali personalizirane oglase – na tako rekoč vse zaslone, ki nas bodo obkrožali.

Proizvajalci vozil pa bodo spletli povezave s trgovci in

RANLJIVOST

Ranljivih več kot 100 milijonov vozil skupine Volkswagen

Računalniški raziskovalec Flavio Garcia je s skupino sodelavcev z univerze v Birminghamu že leta 2013 odkril izjemno ranljivost, ki mu je omogočala zagon več milijonov vozil proizvajalca Volkswagen brez ključa. Namesto da bi nemški proizvajalec začel množični vpoklic in odpravo težav, se je odločil za tožbo skupine raziskovalcev, ki je razkritje te informacije prestavila za celi dve leti. A Garcie in kolegov to ni ustavilo, nasprotno, odločili so se, da bodo poiskali še več napak v sistemih omenjenega proizvajalca vozil. V 2016 so tako objavili še eno študijo, v kateri so razkrili, da ni ranljiv le sistem vžiga vozil, temveč tudi sistem, ki omogoča odklepanje vozila brez ključa. Podrobno raziskovanje težave je pokazalo na pomanjkljivosti, za katerimi »bolehajo« praktično vsi modeli vozil Volkswagen že od leta 1995 dalje. Še več, ker omenjene sisteme uporabljajo vsa vozila v skupini Volkswagen (torej tudi Audi, Seat in Škoda), je ranljivih več kot 100 milijonov vozil. S tehniko povratnega inženiringa so raziskovalci odkrili, da napadalcu zadostuje že eno samo prestrezanje pritiska na gumb ključa – ko so odkrili vrednost šifrirnega ključa, so ugotovili, da ga deli več milijonov vozil. V zadnjih 20 letih so namreč v VW za skoraj 100 milijonov vozil uporabili le štiri skupne ključe!

△ **Težave z daljinskim odklepanjem imajo številne znamke, a pri skupini Volkswagen so še posebej pereče.**

ponudniki storitev, zato nas bo vozilo ne le obvestilo o majhni količini goriva v rezervoarju, temveč tudi ponudilo nakup hrane in pijače v bližini bencinske črpalke (ali električne polnilnice) ter plačilo neposredno prek na dotik občutljivega zaslona v vozilu – iz tega nam ne bo treba niti izstopiti. Da pa bi ti scenariji zaživeli v praksi, bo treba poskrbeti za ustrezno varovanje vseh gradnikov in ekosistemov. Sicer bodo hekerji poskrbeli, da bodo vozila postala njihov novi poligon. ◀

▽ **Tako kot nas danes z oglasi bombardirajo na spletu in mobilnih napravah, nas bodo oglaševalci želeli doseči tudi v vozilu.**

IZBOLJŠAVE

- Izboljšanje brezžičnega signala
- Digitalno posojanje
- Glasba brez iTunes
- Kodi ali Plex?

Izboljšanje **brezžičnega signala**

Žice se počasi poslavljajo od naših domov. Trditev velja predvsem za žice, po katerih potujejo računalniški biti. Do interneta večina omreženih naprav danes dostopa brezžično. Temu primerna mora biti oprema, ki skrbi za nemoten promet po zraku. Vedno pogosteje prihaja do najrazličnejših težav, ki se kažejo v počasnosti, prekinitvah ali celo kapitulaciji brezžične dostopne točke.

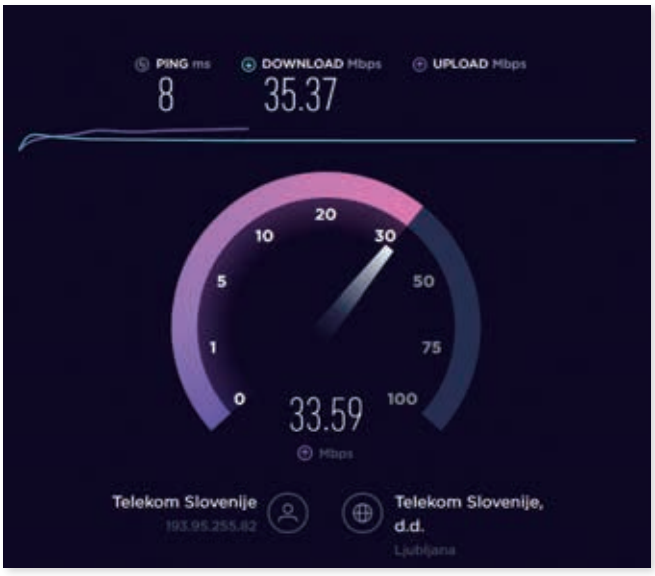
Boris Šavc

Test brezžične povezave

Brezžična omrežja so iz dneva v dan pomembnejši dejavnik pri razvoju in evoluciji interneta. Naprav, ki bi bile prikovane za mizo, je vedno manj, ljudje se veliko raje poslužujemo prenosljivih spletnih odjemalcev. Pametni telefoni postajajo osrednja komunikacijska naprava in glavna vrata v povezani svet. Na področju mobilnega interneta so povezave skoraj že tako hitre kot doma. Mobilnosti se ne odrečemo niti med štirimi stenami, tu stopijo na sceno brezžične točke, ki bite do uporabnikov prenašajo po zraku namesto po žici. Težava nastopi, ko je povezava iz neznanega vzroka slaba ali pa se pojavijo pogoste prekinitve in izpadi. Eden prvih korakov, ki jih velja storiti ob sumu na slabše delovanje brezžične ali mobilne omrežne povezave, je preizkus hitrosti prenosa podatkov.

Hitrost brezžične povezave izmerimo podobno kot preverimo hitrost interneta. Z računalnikom ali mobilno napravo se povežemo z izbrano brezžično točko, izklopimo morebitne porabnike, onemogočimo povezavo VPN in odpravimo druge motnje, nakar zaženemo Ookla Speedtest (www.speedtest.net), ki deluje z vsemi brskalniki in je na voljo tudi v obliki mobilne aplikacije. Uporaba testa ne bi mogla biti bolj preprosta. Vse, kar moramo storiti, je pritisk gumba Go. Proces se zaključi v manj kot minuti, krajša nam jo dinamičen prikaz dogajanja. Meritve program razodene v megabitih na sekundo (Mbps). Rezultate po želji delimo na družabnih omrežjih ali pripnemo na poljubno spletno stran. Test zaženemo večkrat, da na dobljeni rezultat ne vpliva morebitna trenutna gostota prometa. Večkrat ko uporabimo gumb Go, bolj verodostojne bodo končne številke. Naprednejšim uporabnikom je na voljo račun, s katerim lahko spreminjajo nastavitve po lastnem okusu, izberejo želeni strežnik, shranijo spremembe in posamezne teste. Zgodovina uporabe nam pride prav pri ugotavljanju zunanjih vplivov na povezavo čez čas, če zamenjamo dežurni usmerjevalnik ali delovno sobo pregradimo z montažno steno.

▽ **Najboljši spletni pripomoček za merjenje tako hitrosti interneta kot brezžične povezave je Speedtest.**



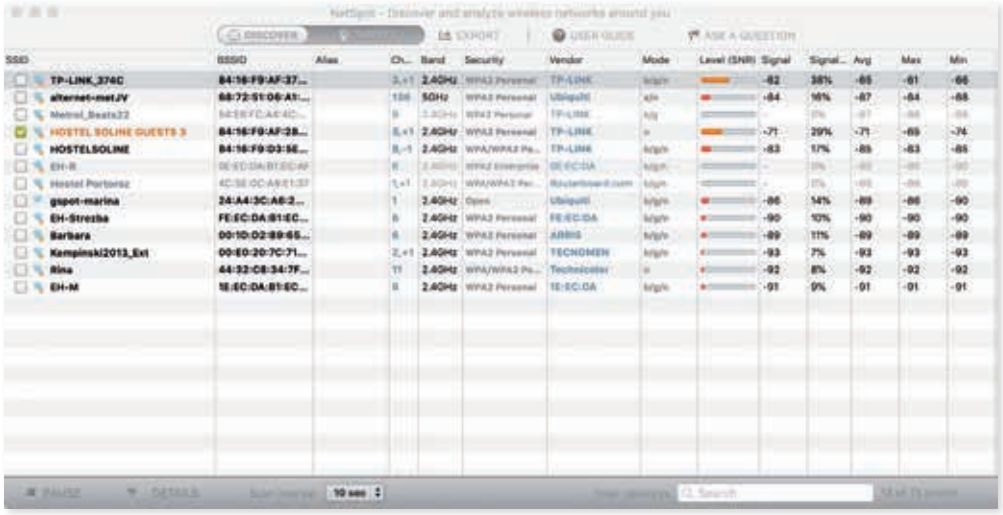
△ **Na pametnem telefonu z operacijskim sistemom Android ali iOS za merjenje hitrosti poskrbi aplikacija OpenSignal.**

Preprosto preverjanje brezžične in internetne povezave ponuja tudi pretočni kralj Netflix, katerega spletišče Fast.com izmeri kakovost povezave samodejno ob obisku strani. Zelo dobra alternativa je storitev OpenSignal (www.opensignal.com), ki je prav tako na voljo kot mobilna aplikacija za sistema iOS in Android, preveri pa lahko hitrosti različnih omrežij, tudi Wi-Fi in 4G, ter nam prikaže, kako dobro se naš ponudnik mobilnega omrežja na določeni lokaciji odreže v primerjavi s konkurenčnimi ponudniki. Aplikacija OpenSignal lahko mobilni in brezžični promet spremlja dlje časa in nam pomaga ugotoviti, katere aplikacije in navade so med podatkovno bolj požrešnimi.

Analiza pokritosti

V hiši ali stanovanju z debelimi zidovi in železobetonskimi ploščami brezžični signal verjetno ni dosegljiv povsod. Analizo stanja izvedemo s programom NetSpot. Na voljo sta dva načina dela. Prvi je Discover, ki prečeše okolico in najde dostopne brezžične točke. Informacije o njih prikaže dinamično, z osveževanjem na 10, 30 ali 60 sekund, ureditvijo po jakosti signala, komunikacijskem šumu, zaščiti, frekvenčnem območju, načinu dela in še čem. Vse podatke lahko izvozimo v obliki CSV, kar nam omogoči nadaljnjo analizo v drugih programih. NetSpot odkrije vse brezžične točke v dosegu, vključno s skritimi, ter izlušči informacije ne glede na njihovo stopnjo zaščite.

Drugi način dela s programom NetSpot je Survey. Gre za funkcionalnost, katere vrednosti se zavemo šele, ko jo prvič uporabimo v domačem brezžičnem omrežju. Ob njeni pomoči se sprehodimo od točke do točke in odkrijemo, kje je signal najmočnejši, kje najšibkejši, kje nanj vplivajo mikrovalovi in kje se prekriva z drugimi brezžičnimi omrežji. Analizo Survey začnemo z načrtom prostora, ki ga lahko uvozimo ali narišemo v aplikaciji. Na voljo so predloge in prazen načrt. Ko preverimo



◁ **Program za analizo brezžičnih dostopnih točk ponuja dva načina dela. Prvi je odkrivanje omrežij v bližini, imenovan Discover.**

△ **Pravo pokritost brezžičnega omrežja razkrije način dela programa NetSpot Survey.**

meritve prostora in izberemo ciljno omrežje, se zabava začne. Pasivno pregledovanje meri zgolj kakovost brezžičnega signala, medtem ko aktivno v pregled vključi še merjenje hitrosti.

Merjenje točke poteka tako, da se postavimo na ustrezno mesto v prostoru in kliknemo na enakovreden položaj na načrtu. NetSpot nato preveri signal in v primeru aktivnega preveri tudi hitrost povezave. Ko je postopek zaključen, se oglasi zvočni signal, ki sporoča, da se lahko premaknemo do druge točke, kjer zadevo ponovimo. Večkrat ko merjenje izvedemo, bolj natančne bodo meritve in informacije o pokritosti, moči ter hitrosti brezžičnega omrežja. Po pritisku na gumb za zaključek meritev Stop Scan program izdela grafični prikaz pokritosti brezžičnega omrežja, s katerim lažje identificiramo ozka grla in jih odpravimo z morebitnim premikanjem usmerjevalnikov, ojačevalcev signala ali anten.

Ukrepi

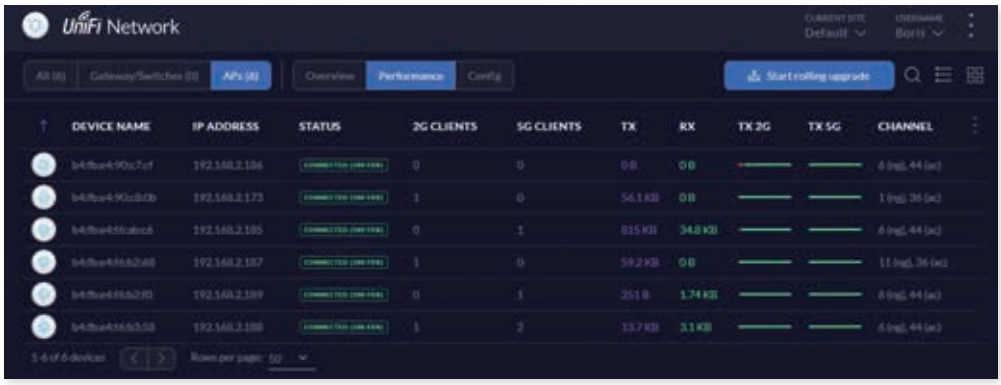
Če uporabljena strojna oprema ne zadostuje, gradnike dokupimo. Podaljševalnik brezžičnega signala bo, na primer, denarnico olajšal za 20 do 100 evrov, odvisno od tega, kako zmogljiv model potrebujemo. Gre za preprosto majhno napravo, ki jo vstavimo v električno vtičnico v prostoru, kjer še je brezžični signal, in povežemo z usmerjevalnikom (pogosto samo z držanjem gumba WPS na podaljševalniku in usmerjevalniku, drugače pa ročno). Z nekaj iznajdljivosti lahko kot podaljševalnik uporabimo tudi kak starejši usmerjevalnik.

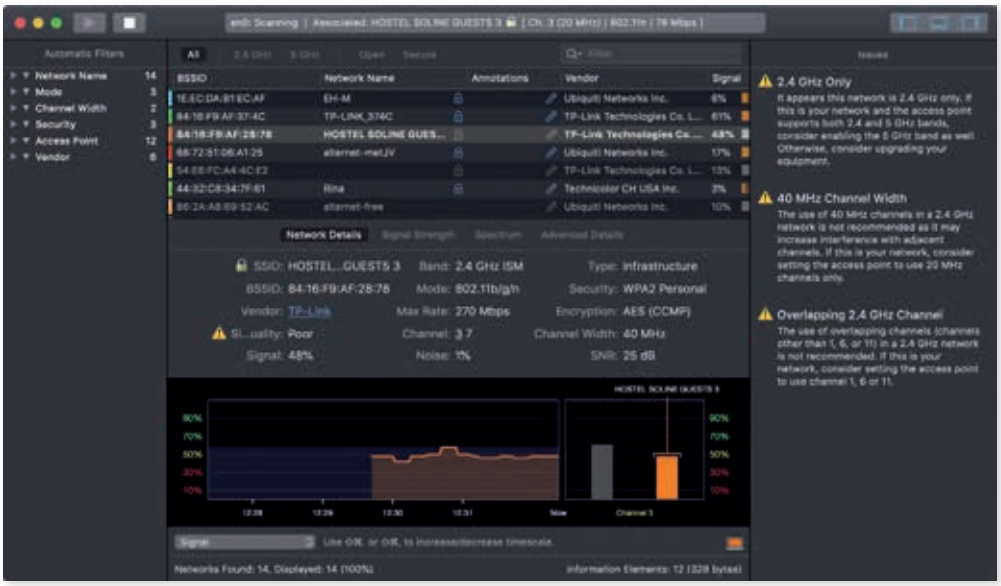
Signal ojačamo še z nakupom boljših anten ali domačo rešitvijo v obliki pločevinke, kjer prazni in očiščeni embalaži za pijačo spodnji del odrežemo, na vrhnji strani pa naredimo večjo zarezo, ki nam bo omogočila, da daljšo stranico pločevinke zvijemo v valjasto obliko, podobno radarju. Prek odprtine tako oblikovano pločevinko zgolj poveznemo čez anteno usmerjevalnika in dobili bomo precej bolje usmerjen brezžični signal. Če nam zamisel s pločevinko ni všeč, lahko za podoben učinek uporabimo tudi aluminijasto folijo, ki jo najdemo v skoraj vsakem gospodinjstvu – brezžični signal bi se moral vsaj v določeni smeri korenito izboljšati.

Vse bolj priljubljena postajajo tudi tako imenovana modularno grajena brezžična omrežja, ki ponujajo hitro in stabilno povezavo, predvsem pa so enostavno razširljiva z dodatnimi napravami. Takšna rešitev je resda dražja, a bolj elegantna, po svetu sta priljubljeni predvsem rešitvi Google Wifi in Linksys Velop. Zadnja podpira tudi storitev Amazon Alexa, ki v primeru, da že imamo kakšno napravo s področja pametnega doma, omogoča, da stanovanju poveljujemo z govornimi ukazi.

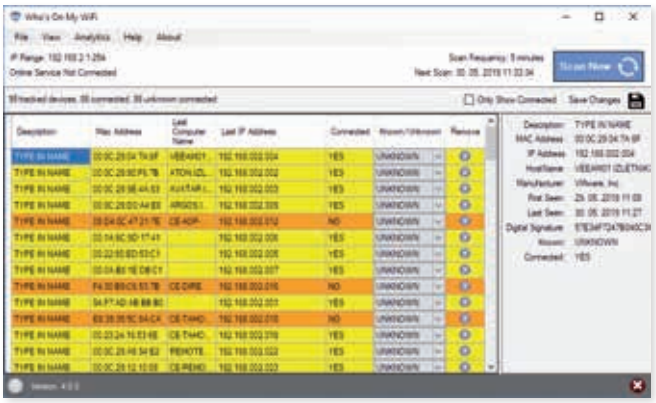
Če brezžično omrežje ne deluje skladno z željami, pred zamenjavo strojne opreme preverimo nastavitve obstoječe. Prevečkrat se zgodi, da usmerjevalniki ne dajejo maksimuma zaradi neznanja uporabnika. Prvi korak je nadgradnja strojne opreme usmerjevalnika in drugih omrežnih naprav. Proizvajalci redno izdajajo posodobitve, ki odpravljajo napake in večajo

▽ **Veliko sodobnih usmerjevalnikov nadgradnjo programske opreme omogoča zgolj s pritiskom ene same tipke v uporabniškem nadzornem programu.**





△ Prekrivanje brezžičnega signala odkriva program WiFi Explorer.



△ Nepovabljene sosede in druge tatove brezžičnega omrežja najlažje odkrijemo s programskim pripomočkom, kakršen je Who's On My Wifi.

prepustnost. Postopek nadgradnje je od proizvajalca do proizvajalca drugačen, zato je priporočljivo prebrati navodila. Sodobni usmerjevalniki imajo nadgrajevanje vključeno v administratorsko nadzorno ploščo, medtem ko starejši še vedno zahtevajo obisk uradne spletne strani, prenos datoteke s posodobitvijo in nameščanje prek uporabniškega vmesnika. Redno posodabljanje je vsaj zaradi varnosti priporočljivo tudi v primeru, ko brezžično omrežje deluje dobro.

Drugi, med računalniškimi znalci precej priljubljen ukrep pa je namestitev namenske strojne programske opreme na usmerjevalnik, kot je DD-WRT ali Tomato. DD-WRT je odprtokodna strojna programska koda, ki je na voljo za vrsto usmerjevalnikov, prinese pa jim mnoštvo dodatnih funkcij, ki jih privzeto ne poznajo. Tako lahko tudi na cenejših usmerjevalnikih vklopimo funkcijo omejevanja prometa po uporabnikih, QoS, napredno šifriranje, vzpostavimo varne povezave VPN in še marsikaj drugega. Najdemo jo na spletni strani www.dd-wrt.com, ki je tudi sicer bogat vir informacij o usmerjevalnikih najrazličnejših proizvajalcev.

Večje hitrosti prenosa v brezžičnem omrežju dosežemo, če napravam, ki podpirajo večfrekvenčna omrežja, ukažemo le uporabo frekvenčnega pasu 5 GHz. Seveda moramo zato najprej imeti ustrezno zmogljiv brezžični usmerjevalnik, katerega nakup je danes skorajda nujen. Z uporabo omrežja 5 GHz se otresemo gneče, saj je tistih s frekvenco 2,4 GHz precej več, za nameček pa je višje frekvenčno omrežje sposobno hitrejšega prenosa podatkov, kar je dobra novica predvsem za prenose velikih datotek in nalaganje pretočnih video posnetkov. V nadzorni plošči ustreznega usmerjevalnika zato poiščemo opcijo 5 GHz in ji dodelimo isto ime SSID in geslo kot 2,4 GHz, tako da bodo naprave samodejno izbrale boljšo možnost, če bo ta na voljo.

Nekaterim androidnim telefonom in tablicam lahko zapovemo zgolj povezovanje s hitrejšimi omrežji. V nastavitvah se odpravimo v brezžična omrežja Wi-Fi, kjer kliknemo tri pikice oziroma ikono zobnika ter izberemo napredne zmožnosti. V meniju, ki se prikaže, nato poiščemo frekvenčni pas Wi-Fi in možnost 5 GHz (5 GHz only). Popolnoma drugačna logika velja pri drugih androidnih telefonih ter Applovih mobilnih napravah z operacijskim sistemom iOS, kjer telefon iPhone in tablica iPad pregovorno slabo izbirata med znanimi omrežji. Rešitev je v različnem poimenovanju omrežij 2,4 GHz in 5 GHz. Napravi lahko ukažemo, da nižje frekvenčno omrežje pozabi, tako da ji ostane zgolj hitrejša opcija povezovanja 5 GHz.

Brezžični signal potuje podobno kot radijski valovi, poleg določene frekvence uporablja tudi vnaprej nastavljeni kanal. Prav tako kot radijski signal se tudi brezžični slabo odziva ob morebitnem prekrivanju. Usmerjevalniki signal delijo na določenih kanalih, ki so povezani s frekvencami. Če brezžični usmerjevalnik našega soseda uporablja isti kanal kot naš, bo to vplivalo na hitrost prenosa podatkov po brezžični povezavi. Cilj je najti prosti kanal oziroma najmanj zasedenega. Na računalniku Mac lahko v ta namen uporabimo aplikacijo WiFi Explorer, ki prečeše okolico ter izpiše brezžične točke v bližini z jakostjo in s kanalom povezave med številnimi drugimi informacijami o posameznem priključku. Opremljeni z bogato bero podatkov zlahka izluščimo svobodnejši kanal od našega.

Kanal usmerjevalniku spremenimo v njegovih nastavitvah. V splošnem velja, da v spletnem vmesniku poiščemo nastavitev, poimenovano Channels. Večina novejših brezžičnih usmerjevalnikov samodejno izbira brezžični kanal, prek katerega oddaja in sprejema WiFi-signal, a to nastavitev lahko kadarkoli ročno popravimo. Pogosto med kanali izbiramo iz padajočega menija. V praksi velja, da so v frekvenčnem pasu 2,4 GHz najbolj zasedeni kanali ena, šest in enajst, ker jih privzeto uporablja največ brezžičnih usmerjevalnikov, zato velja izbrati enega od preostalih.

Včasih težave z brezžičnim omrežjem povzročijo tatovi v bližini. Če smo ustrezno poskrbeli za zavarovanje brezžičnega omrežja z močnim geslom, so možnosti, da se vanj prikrade nepovabljen gost, sicer majhne, vendar lahko stanje vseeno kadarkoli preverimo in popravimo. Hitri test naredimo z brezplačnim orodjem Bitdefender Home Scanner, ki bo najprej prečesalo naše Wi-Fi omrežje in iskalo naprave z morebitnimi šibkimi gesli ter slabše zaščitenimi (šifriranimi) povezavami. Poleg informacije o tem, ali so v našem omrežju morebitni neželeni gosti, ki upočasnjujejo povezavo, bo aplikacija prikazala tudi več varnostnih priporočil za naše omrežje. Drug način iskanja sosedov, ki si izposojajo našo omrežno povezavo, je raba rešitve Who's On My Wifi. Ta deluje v ozadju in spremlja vse z omrežjem povezane naprave, osveži se vsakih pet minut in nas takoj obvesti, če zazna novo oziroma neznano napravo.

Omejevanje porabnikov

Brezžična omrežja s številnimi odjemalci se hitro znajdejo v težavah, saj nekatere aplikacije na

posameznih napravah preprosto porabijo preveč pasovne širine domačega omrežja. Spletno igranje iger, posodabljanje operacijskega sistema ali zahtevne programske opreme, predvajanje pretočnih vsebin, prenašanje torrentov in drugih večjih datotek, video pogovori in druge potratne aplikacije brez ustreznega nadzora upočasnijo delovanje celotnega brezžičnega omrežja.

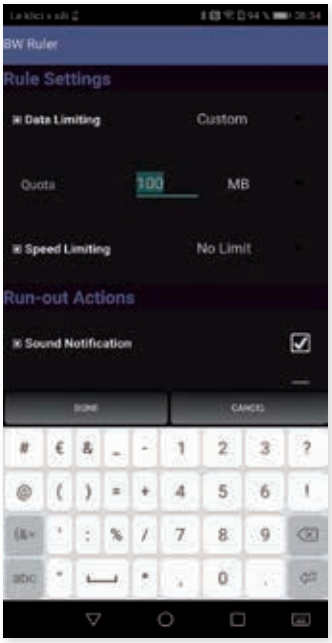
Odzivnost brezžičnega omrežja (VPN in mobilnega) na telefonu iPhone, na primer, preverimo s programom Pingify, ki s pošiljanjem majhnih podatkovnih paketov z vgrajenim algoritmom preveri kakovost in zanesljivost povezane točke. Delovanje programa je preprosto. Preizkušanje povezav zaženemo z ukazom Start Test, nakar program pošlje kratka sporočila, imenovana ping, na vse z napravo povezana internetna omrežja, vključno z brezžično povezavo. S pingom program izmeri reakcijski čas omrežja, ki je odvisen od tega, kako hitro dobi odgovor na poslano zahtevo. Pingify med delovanjem zabeleži lokacijo, čas odgovora, morebitne napake, zamude in druge informacije ter na podlagi njih oceni kakovost storitve posamezne povezave. Naprednejšo analizo omogoči z grafičnim prikazom in izvozom meritev v druge programe.

Telefon iPhone pri porabi tako mobilnega kot brezžičnega omrežja omejimo na več načinov. Najprej preverimo, kaj se dogaja z aplikacijami v ozadju. Osveževanje nameščenih programov izklopimo z nastavitvijo *Settings / General / Background App Refresh / Off*. Isto nastavitev uporabimo, ko želimo izklopiti osveževanje zgolj nekaterih aplikacij. Takrat v *Settings / General / Background App Refresh* poiščemo potencialnega krivca in z drsnikom na desni strani imena prekinemo njegovo (skrivno) komunikacijo s svetom. Naslednji korak je izklop samodejnih posodobitev, kar storimo tako, da v nastavitvah *Settings / iTunes & App Store / Updates* zeleni drsnik obarvamo sivo. Čeprav telefon iPhone zaradi omejitev proizvajalca ne zna slediti WiFi-porabi, lahko največje porabnike odkrijemo v poročilu o mobilni potrošnji. Tega najdemo pod *Settings / Mobile Data / Mobile Data*.

Na telefonih in tablicah z operacijskim sistemom Android je uporabnikom življenje olajšano z aplikacijami, kakršni sta NetCut in Bandwidth Ruler. Medtem ko prvi za delovanje potrebuje korenski dostop do naprave, lahko Bandwidth Ruler uporabljamo brez drastičnih posegov v sistem. Uporaba programa ni zapletena, promet omejimo z dodajanjem pravil *Add,* kjer določimo podatkovno kvoto ter hitrost povezave za posamezno aplikacijo, aplikacije pa razdelimo med blokirane, omejene in neomejene z gumbom *Apps*.

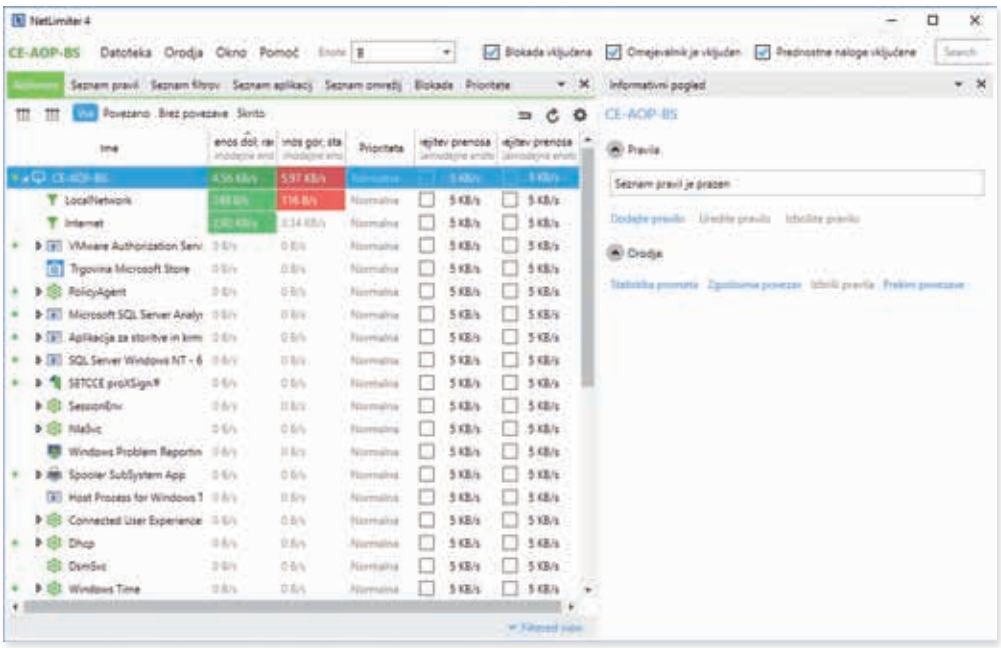
Omejevanje porabe posameznih aplikacij pride prav tudi na računalniku z operacijskim sistemom Windows. Če, na primer, prenašamo s spleta zelo veliko datoteko, nam omejitve spletnega brskalnika medtem omogočajo normalno delo v drugih programih. Posamezne aplikacije imajo omejevanje privzeto vgrajeno, na primer odjemalec igričarskega servisa Steam, kjer v nastavitvah *Settings / Downloads* določimo, koliko pasovne širine želimo nameniti igram. Podobne rešitve poznajo še Dropbox, Google Drive in drugi. Posodobitve operacijskega sistema omejimo v Nadzorni plošči / Posodobitev in varnost / *Windows Update /* Dodatne možnosti / Optimizacija prenašanja / Dodatne možnosti / Omejite količino pasovne širine, ki se uporablja za prenašanje posodobitev v ozadju (angl. *Update & Security / Windows Update / Advanced Options / Delivery Optimization / Advanced Options / Limit how much bandwidth is used for downloading updates in the background*). Če vgrajenega omejevanja požrešen program ne pozna, posežemo po namenskih aplikacijah, kakršna je NetLimiter.

△ **Mobilni program Pingify nam preveri odzivnost povezanega brezžičnega omrežja.**



△ **Z aplikacijo Bandwidth Ruler uspešno omejimo dostop do interneta in brezžične povezave posameznim programom, četudi nimamo korenskega dostopa na telefonu z Androidom.**

NetLimiter se ponaša s preprostim uporabniškim vmesnikom, ki omogoča, da omejimo poljubno število aplikacij. Vse, kar moramo storiti, je, da ob ustreznem imenu obkljukamo in določimo omejitve prenosa. Program je sicer plačljiv, a ga lahko mesec dni preizkušamo, da ugotovimo, ali se nakup izplača. Glede na zapletenost drugih tovrstnih programskih pripomočkov je trideset ameriških dolarjev, kolikor zahtevajo zanj, dobra kupčija. ◀



▷ **Za omejevanje požrešnih programov na računalnikih z operacijskim sistemom Windows odlično skrbi plačljivi pripomoček NetLimiter.**

Digitalno **posojanje**

Danes je vse digitalno. Minili so časi otipljivih dobrin, domačih zbirk plošč, knjižnic v dnevni sobi, ljubiteljskih videotek ter zaprašenih igričarskih brlogov s preigrano plastiko. Medtem ko smo nadpovprečni ljubitelji glasbe, knjig, filmov in iger veseli, da imamo končno urejene in širne prostore, so prijatelji žalostni, ker niso deležni dobrot, ki jih ponujajo naše digitalne zbirke. Da bi jim ustregli, se naučimo, kako se ničle in enice najrazličnejših porekel lahko posojajo.

Boris Šavc

△ **Netflix spodbuja deljenje uporabniškega računa z dražjima paketoma.**

△ **Odkrivanje prisklednikov, ki digitalne dobrote uživajo na naš račun, omogoča opcija Recent device streaming activity.**

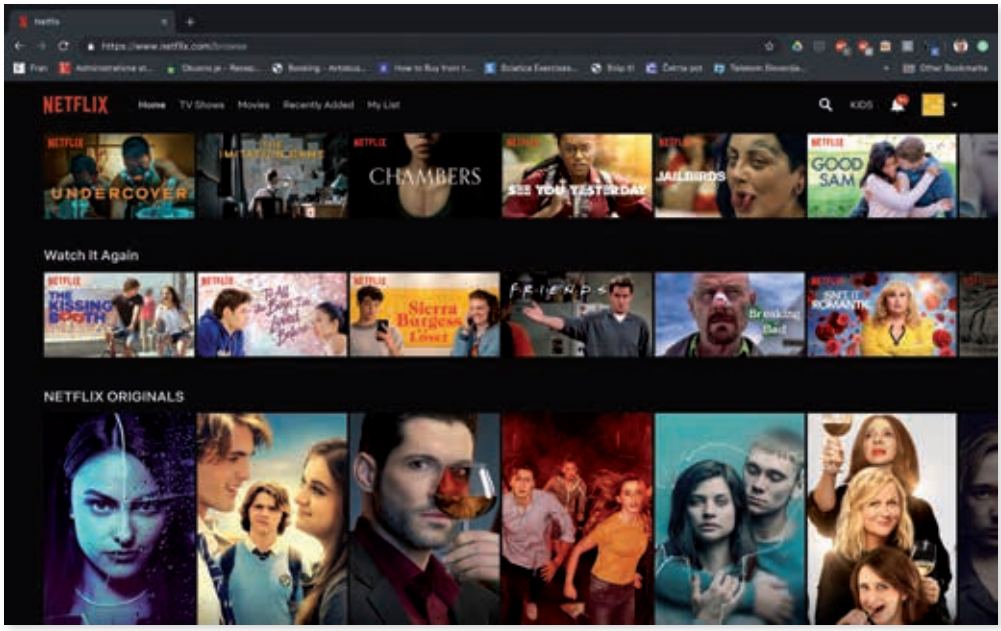
Netflix

Najbolj priljubljena pretočna video storitev na planetu Netflix priznava, da dobra desetina gledalcev uživa v ponujenih vsebinah zastonj, ker uporabijo naročnino nekoga drugega. Ker ponudnik s tovrstnim izkoriščanjem izgublja ogromno denarja, nad početjem logično ni navdušen. Kljub temu se zdi, da s posojo ni prav nič narobe, saj naročnik spremljanje vsebin na več zaslonih plača. Čeprav je praksa zakonsko prepovedana in ima vsak ponudnik svoje pogoje uporabe, jo le redki preganjajo. Na koncu ostane predvsem moralna dilema posameznika, kjer z zastonjkarstvom škodimo ustvarjalcem. Če nihče ne bi plačal za film, ga sploh ne bi posneli. Več kot je brezplačnih ogledov nadaljevanke, manjša je možnost njenega »preživetja«.

Netflix ponuja tri naročniške pakete, Basic, Standard in Premium, od katerih sta le zadnja dva dejansko namenjena deljenju oziroma spremljanju vsebin na več zaslonih hkrati. Ker število naprav v nobenem paketu ni omejeno, je Netflix kot nalašč za deljenje uporabniškega računa. Deljenje med družinskimi člani storitev uradno podpira, medtem ko je podpora širšemu krogu uporabnikov enega računa bolj skrita. Moralno sporna deljenja Netflix ne preganja, saj mu na dolgi rok koristi. Zastonjkarji se na storitev navadijo in sčasoma postanejo plačljivi uporabniki.

Nosilec naročniškega razmerja z deljenjem storitve Netflix običajno nima težav, privzeto je omogočeno in do določene mere dovoljeno. Ker se dobre stvari hitro širijo, število naprav na posamezni račun pa tudi, je priporočljivo redno spremljanje dogajanja znotraj deljenega uporabniškega računa. Z opcijo *Account / Recent device streaming activity* pogledamo, katere naprave so v zadnjem času dostopale do vsebin storitve Netflix z našim uporabniškim računom, pod *Account / Manage download devices* pa preverimo ustreznost naprav, ki jim je dovoljeno vsebine prenašati za kasnejše uživanje v njih. Če napravo s seznama odstranimo, prenesene vsebine ne bodo več delovale. Če se znajdemo v preveliki zmešnjavi, začnemo deliti znova z uporabo *Account / Sign out of all devices*.

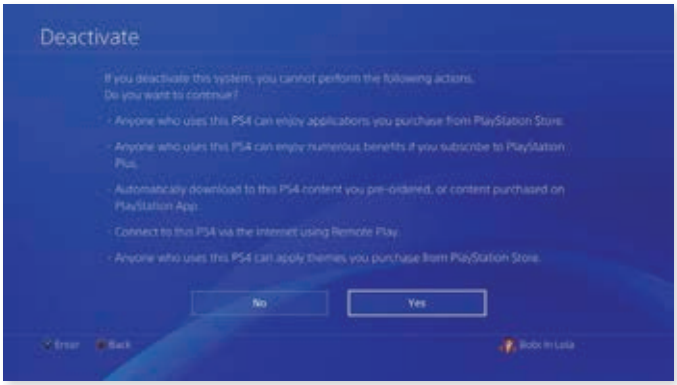
▽ **Netflix je najbolj priljubljena pretočna storitev na planetu, ki za ogled ponujenih nadaljevank in filmov zaračunava mesečno naročnino.**



Playstation 4

Deljenje iger je od nekdaj priljubljena aktivnost slehernega igričarja, ki je v preteklosti preigrani naslov nemudoma posodil prijatelju ali ga prodal znancu. Danes ima ta igričar težavo, saj igre po večini kupuje v digitalni obliki, kar mu preprečuje tako posodo kot prodajo. Digitalni nakupi so vezani na igralni račun, ki ga že v osnovi ni dobro deliti naokoli. Ker je vezan na plačilno sredstvo, se ga običajno ne posoja ljudem zunaj družine in kroga najtesnejših prijateljev. Ponudniki vsebin deljenje z najrazličnejšimi sredstvi zavirajo, saj tako prodajo več izvodov posameznega naslova. Na srečo lahko ovire za deljenje digitalnih dobrin na najbolj priljubljeni igralni konzoli ta hip z nekaj truda preskočimo.

Tipičen primer zapletenosti deljenja je igralna konzola podjetja Sony. Digitalni nakupi so na konzoli Playstation vezani na uporabniški račun PSN, ki nam omogoča, da igre igramo na katerikoli konzoli, kjer smo prijavljeni z ustreznimi poobla-stili. Dodatno je omogočena



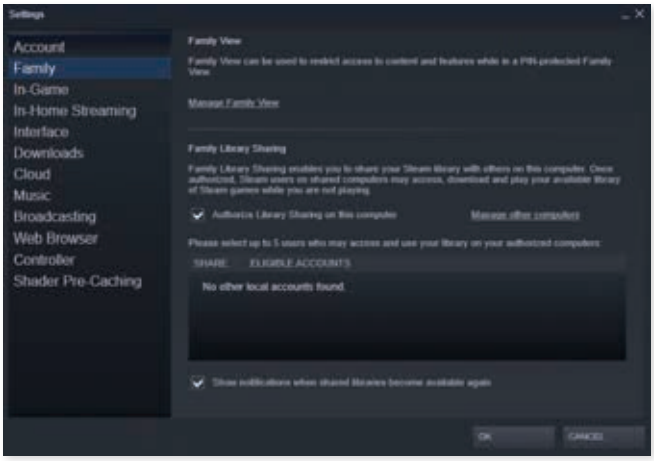
△ **Deljenje uporabniškega računa in digitalne robe na igralni konzoli Playstation 4 je mogoče le z aktivacijsko telovadbo.**

aktivacija primarne igralne naprave, ki dovoli, da smo na konzoli prijavljeni s tujim uporabniškim računom, a vseeno igramo igre primarnega lastnika. V praksi je zadeva videti takole: prijatelju nastavim njegovo konzolo kot primarno za moj uporabniški račun, nakar se on prijavi s svojim. Tako bova oba lahko igrala moje igre, on zato, ker ima primarno napravo mojega uporabniškega računa, jaz, ker sem prijavljen z ustreznimi (lastnimi) pooblastili.

Ker je račun PSN lahko aktiviran le na eni konzoli hkrati, je prvi korak na poti k deljenju jasen. Račun deaktiviramo, tako da na igralnem ploščku DualShock4 pritisnemo osrednji gumb PS, nakar v nastavitvah *Settings* poiščemo opcijo *Account Management*. Pod *Activate as Your Primary PS4* uporabimo ukaz *Deactivate* in izbiro potrdimo z *Yes*. Z obratno potjo nadaljujemo na prijateljevi konzoli, kjer njegov račun odjavimo s *Settings / Account Management / Sign Out* ter vpišemo svojega, nato v nastavitvah *Settings / Account Management / Activate as Your Primary PS4* izberemo možnost *Activate*. Ko se prijatelj naslednjič prijavi s svojim uporabniškim računom PSN, mu bodo na voljo tudi kupljene igre z mojega.

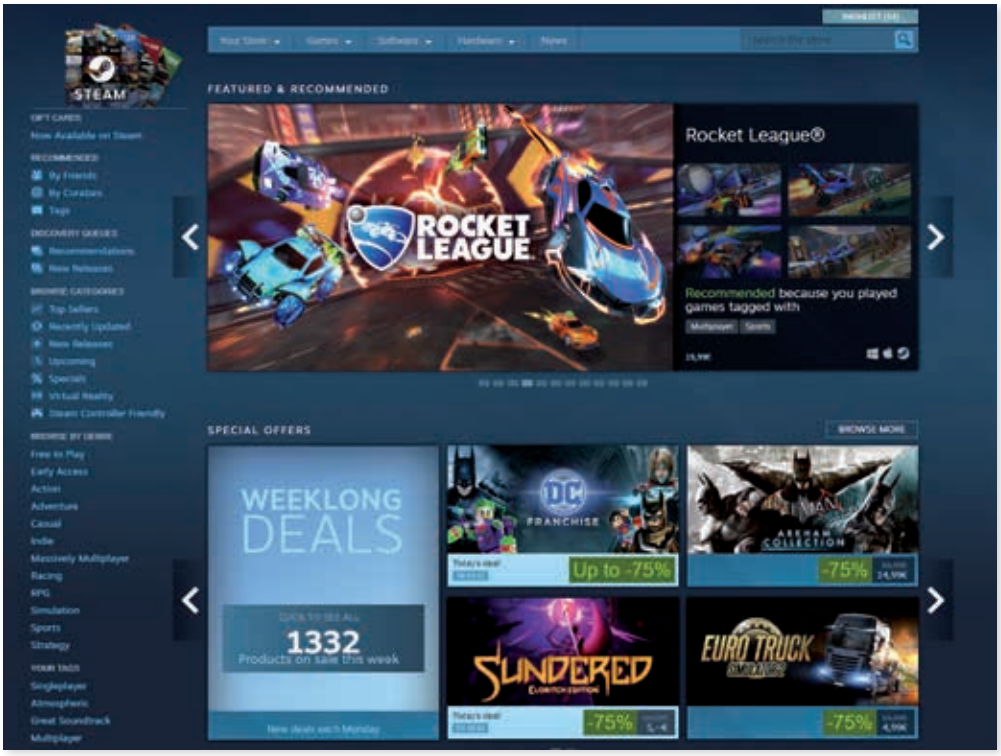
Steam

Steam je največja digitalna tržnica z igrami za računalnike. Ponaša se z bogato zbirko velikih in majhnih naslovov ter z družabnim vidikom, ki prijateljem omogoča, da se skupaj igrajo. Kljub podprti družabnosti Steam ne dovoli dveh sočasnih prijav, kar v praksi pomeni, da računa na tak način ne moremo deliti s prijatelji in z družino, saj v nasprotnem primeru kratimo lastni igralni užitek. Deljenju računa je na servisu Steam namenjena storitev Steam Family Sharing, ki podpira deset različnih dostopov do ene zbirke. Družinsko deljenje Steam ima svoje prednosti in slabosti.



△ **Deljenju računa servisa Steam med družinskimi člani in bližnjimi prijatelji je namenjena storitev Steam Family Sharing.**

▷ **Pogoj za uporabo družinskega deljenja Steam Family Sharing je dvostopenjsko preverjanje pristnosti Steam Guard.**



Storitev Steam Family Sharing je namenjena deljenju znotraj družine ali ožjega kroga prijateljev. Če imata otroka vsak svoj računalnik, jima ni treba dvakrat kupiti iste igre. Vendar ni vse tako lepo, kot se zdi na prvi pogled. Dostop do deljenih naslovov ima naenkrat samo en uporabnik, omrežno igranje z eno kopijo igre tako odpade, otežkočena pa je tudi uporaba deljene zbirke. Če podrejeni uporabnik igra igro, ko se v zbirko želi prijaviti lastnik, ga sistem na to opozori in mu odmeri zelo malo časa, da shrani položaj v igri ter zaključi igranje. Obratna težava je še večja: če igra igro iz zbirke lastnik, je dostop do zbirke drugim članom onemogočen.

Prvi korak pri vzpostavitvi deljenja Steam Family Sharing je vklop vgrajene zaščite Steam

◁ **Steam je največja digitalna tržnica z igrami za računalnike.**

Guard, kar storimo z nastavitvijo *Steam / Settings / Account / Manage Steam Guard Account Security*. Ko je dvostopenjska zaščita omogočena, v nastavitvah *Steam / Settings / Family* zaženemo še družinsko deljenje. Pod zavihkom *Family* in opcijo *Share / Eligible Accounts* so navedeni Steamovi računi, s katerimi smo se prijavljali na uporabljenem računalniku. Če želimo naslove iz deljene zbirke drugje, se moramo prijaviti na novem računalniku in ga potrditi s *Steam / Settings / Family / Authorize Library Sharing on this computer*.

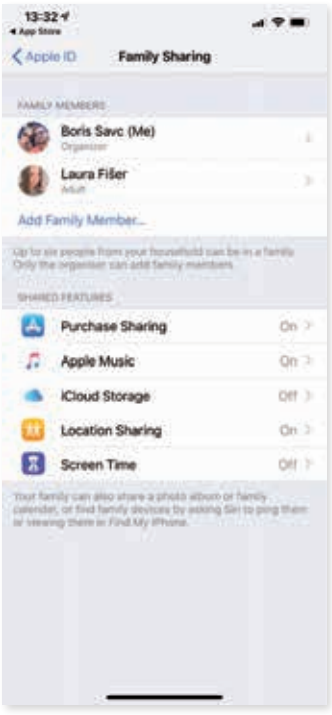
Apple

Apple na mobilnih napravah ter računalnikih deljenje digitalnih vsebin med družinskimi člani in bližnjimi prijatelji podpira z uradno možnostjo Family Sharing. Operacijska sistema iOS in macOS privzeto omogočata deljenje nakupov s tržnice App Store, iz trgovine iTunes, knjigarne Books in drugih jabolčnih prodajnih kanalov, med njimi je tudi naročniška storitev Apple Music. Z opcijo Family Sharing ima dostop do programov, iger, filmov, TV serij, glasbe in knjig vsa družina oziroma krog prijateljev.

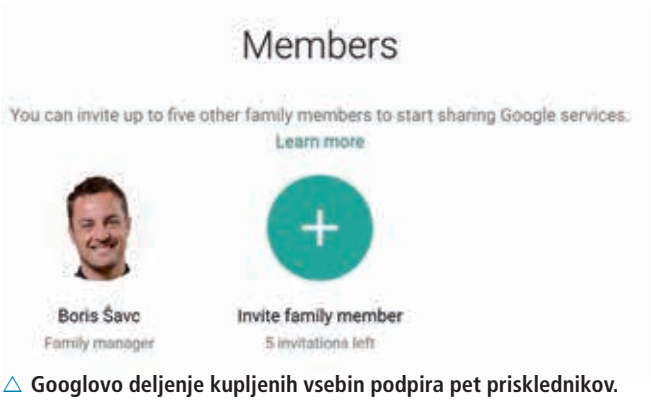
Vsak izmed članov družine ali prijateljev, ki bi radi bili povezani z možnostjo Family Sharing, potrebuje lasten uporabniški račun iCloud. Pred vklopom deljenja moramo določita nosilca nakupov Family Organizer in mu dodati veljavno plačilno sredstvo. Na Macu to storimo v programu iTunes v nastavitvah *Account / View My Account / Manage Payments*, na telefonu iPhone ali tablici iPad pa z dotikom na uporabnika v *Settings* ter izbiro *Payment & Shipping / Add Payment Method*. Plačilno sredstvo potrebuje le nosilec deljenja Family Sharing.

Deljenje Family Sharing omogočimo v nastavitvah *System Preferences / iCloud / Manage Family*, kjer najprej preverimo pravilnost prikazanih podatkov, nato ustoličimo organizatorja ter z znakom plus dodamo do pet članov skupine. Če kdo iz skupine nima lastnega uporabniškega računa Apple ID, mu ga lahko na ekranu za dodajanje ustvarimo. Privzeto so vsi dodani člani odrasli, otroke določimo z vnosom ustreznega rojstnega datuma in zaščito plačilnega sredstva. Ker vsi člani družine znotraj deljenja Family Sharing uporabljajo

▽ **Apple deljenje kupljenih digitalnih dobrin in skupnega plačilnega sredstva omogoča z opcijo Family Sharing, ki je pripravna tudi za nadzor otrok.**



▽ **Družinsko deljenje Apple Family Sharing pokriva tudi glasbeno storitev Apple Music, ki pa za uspešno skupinsko poslušanje zahteva dražjo naročnino.**



△ **Googlovo deljenje kupljenih vsebin podpira pet prisklednikov.**

plačilno sredstvo organizatorja, mora glava skupine nakup otroka pred izvedbo odobriti. Ob kreaciji otroškega uporabniškega računa se po želji odločimo za deljenje otrokove lokacije z drugimi družinskimi člani oziroma pripadniki skupine.

Uporaba deljene vsebine je precej odvisna od porekla, Apple Music, na primer, zahteva zgolj plačilo družinske naročnine, nakar je dostop enak polnemu. Enako velja za plačljivi oblačni prostor iCloud, medtem ko je nameščanje aplikacij iz tržnice (Mac) App Store pogojeno s podporo razvijalcev. Če aplikacija podporo ima, jo bomo našli pod uporabniškim računom ter razdelkom *Purchased / Family Purchases*.

Google Play

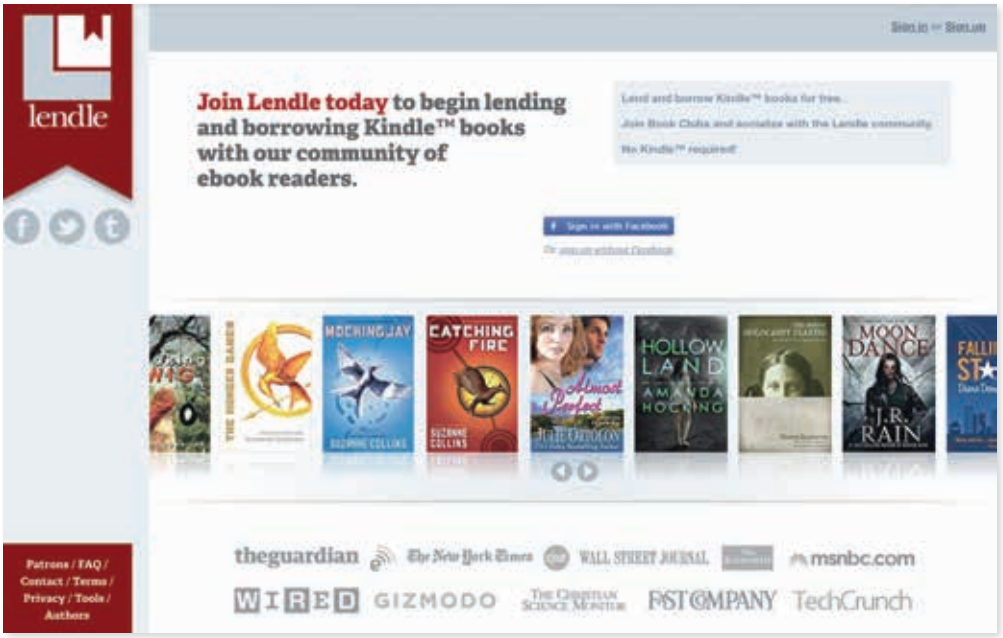
Deljenje aplikacij, iger, filmov, serij, glasbe, knjig in še česa omogoča tudi Google. Naprave z Androidom robo s tržnice Google Play delijo prek storitve Google Play Family Library. Da bi kupljene digitalne dobrote lahko delilo do pet ljudi, je treba najprej ustvariti družino. Po prijavi in vpisu podatkov o plačilni kartici v aplikaciji Google Play izberemo opcijo Račun (*Account*) in nato zavihek Družina (*Family*), kjer dodajamo družinske člane s povabili. Na voljo sta dva osnovna tipa članstva. Omejeno je namenjeno otrokom in uveljavljanju določenih omejitev. Osrednja omejitev vsekakor leti na plačilno sredstvo, ki veže vsako Googlovo družino in ga moramo potrditi ob dodajanju članov. S storitvijo Google Play Family Library delimo poleg vsebine tudi vezano plačilno sredstvo, s katerim člani kupujejo digitalne dobrote, če jim tega nismo izrecno prepovedali.

Družinska zbirka vsebin se načelno polni samodejno, lahko pa ponudbo v njej oblikujemo tudi ročno. Aplikacije in igre dodajamo in odstranjujemo v nastavitvah tržnice Google Play Moje aplikacije in igre (*My Apps & Games*), kjer so nakupi, upravičeni do deljenja, opremljeni z namenskim drsnikom Družinska zbirka. Ves katalog, ki ga delimo, vidimo v aplikaciji Google Play, če pod ikono s tremi črtami izberemo možnost Družinska zbirka. Katalog po želji filtriramo po osebi, ki je dobrote vanj dodala. Na ta način lahko vsaj za silo sledimo zapravljanju polnoletnih družinskih članov.

Kindle

Najboljša lastnost knjige je, da jo zlahka posodimo in s črkami okužimo prijatelja ali člana družine. Posojanje knjig je tako priljubljena dejavnost, da obstajajo celo ustanove, ki so namenjene zgolj njej. Elektronske knjige so zagodle tako knjigoljubcem kot knjižnicam. Čeprav se te trudijo z najrazličnejšimi sistemi uvesti elektronsko izposojo, jim za zdaj ne uspeva najbolje. Posamezniki smo prepuščeni lastni iznajdljivosti, elektronske knjige so resda cenejše, obstojnejše in ne zahtevajo fizičnega prostora za hrambo, a kaj, ko z njimi vsaj uradno težko razveseljujemo bližnje.

Lep primer je uradna rešitev posojanja elektronskih knjig za bralnik Kindle. Amazon podpira posojanje knjig drugim uporabnikom, ki ne potrebujejo bralnika, saj zadostuje že aplikacija Kindle, ki je na voljo za računalnike in mobilne naprave. Edini pogoj je lasten uporabniški račun, to je elektronski naslov, povezan z Amazonom. Posojanje elektronskih knjig ima kar nekaj prednosti, saj čtivo lahko, na



△ **Uradno posojanje Amazonovih elektronskih knjig se je v ZDA dobro prijelo. Dokaz je spletna knjižnica Lendle.**

△ **Članom družine v Amazonovem deljenju po želji namenimo zgolj posamezne elektronske knjige.**

primer, posodimo oddaljenemu uporabniku, e-knjigo pošljemo po omrežju, medtem ko je treba fizično kopijo dostaviti ročno. Posojeno knjigo Amazon po izteku štirinajstih dni samodejno vrne v zbirko, tako da jo brez skrbi posodimo tudi prijatelju, ki stvari rad izgubi ali jih pozabi vrniti. Okoli posojanja elektronskih knjig za bralnike Kindle se je spletlo kar nekaj spletnih skupnosti, največja ljubiteljska e-knjižnica je Lendle, kjer velja pravilo, več kot daš, več dobiš. Slabosti posojanja na Amazonov način je na žalost tudi precej. Za zdaj je namreč na voljo le ameriškim računom, posamezno knjigo lahko posodimo le enkrat, časa izposoje ne moremo prilagajati, obenem pa je knjig, ki jih lahko posojamo, izredno malo.

Ko se sprijaznimo z omejitvami, če imamo ameriški račun, in se seznanimo s prednostmi, je čas, da posodimo prvo knjigo. Eden izmed načinov je, da na Amazonovem spletišču pod uporabniškimi nastavitvami poiščemo *Digital content and devices / Content and Devices*, nakar ob želenem naslovu izberemo kvadrat s tremi pikami in opcijo *Loan this title*. Če opcije ne najdemo, knjige ni mogoče posoditi. Drugi način je iz trgovine Amazon.com, kjer v knjižnici Kindle najdemo že kupljeno knjigo, na kar nas sistem opozori in ponudi možnosti, ki jih imamo na voljo. Če je knjiga med naslovi za izposojo, je navedena tudi možnost *Loan this book*. V obeh primerih nas sistem preusmeri na vpisovanje elektronskega naslova osebe, ki ji knjigo posojamo. Kot smo že omenili, mora imeti prejemnik svoj račun trgovca Amazon. Ko pritisnemo gumb *Send now*, bo prejemniku poslana povezava, s katero si knjigo izposodi. Časa za prevzem ima teden dni, za branje dva tedna. Podobno je izvedeno vračanje. Če ne počakamo na samodejno vrnitev, ki se sproži po štirinajstih dneh od začetka izposoje, knjigo vrnemo prek seznama *Digital content and devices / Content and Devices*, kjer posojeni naslov z ukazom *Delete* preprosto izbrišemo.

Opisani postopek posojanja elektronskih knjig na srečo ni edini način deljenja knjižne zbirke na bralniku Kindle. Posojanje ožjemu krogu prijateljev in članom družine je namenjena Amazonova storitev Family Library. Gre za povezovanje Amazonovega računa z enim odraslim in s štirimi otroki. V družino povezani računi bodo deležni skupnih Prime dobrot in digitalne robe, med katero so tudi elektronske knjige za bralnik Kindle. Omejitve pri družinskem deljenju odpadejo, člani si lahko izposodijo poljubno knjig za dlje časa in jih istočasno berejo. Edini pogoj za družinsko deljenje je skupno plačilno sredstvo, ki ga odrasla člana družine tako in tako verjetno že delita.

V prvem koraku vzpostavitve družinskega deljenja Family Library je treba povezati odrasla računa. Na spletišču Amazon v nastavitvah uporabniškega računa v ta namen poiščemo *Shopping programs and rentals / Amazon Household* in izberemo *Add Adult*. Ko izpolnimo zahtevane podatke, se povabljencu pošlje elektronsko sporočilo, na katero se mora odzvati v štirinajstih dneh. Zbirko družinskih digitalnih dobrin na spletišču Amazon ustvarimo z možnostjo *Shopping programs and rentals / Amazon Household / Create your Family Library*, naknadno pa jo oblikujemo z *Manage Your Family Library*.

Z družino in ožjimi prijatelji lahko delimo aplikacije, igre, zvočne in elektronske knjige ter naročnino Prime. Z ustreznim drsnikom delimo celotno zbirko. Če želimo deliti le posamezne naslove, drsnik izklopimo in v nastavitvah *Shopping programs and rentals / Amazon Household / Manage Your Family Library / Manage Your Content and Devices / Content* izberemo želeni naslov, ikono kvadrata s tremi pikami ter uporabimo ukaz *Manage Family Library*. Naslov posodimo povezanemu računu z *Add to Library*.

Poleg opisanih bolj ali manj dostopnih načinov posojanja elektronskih knjig za bralnik Kindle obstajata še dve celo bolj očitni poti. Bližnjemu lahko posodimo fizično napravo z naloženimi knjigami, ki jih lahko bere brez omejitev, ali pa njegovo bralno napravo prijavimo v svoj Amazonov račun. Amazon dovoli šest naprav (ali aplikacij) Kindle na en uporabniški račun oziroma eno zbirko kupljenih elektronskih knjig. V vsakem primeru moramo prejemniku seveda zaupati, saj mu bodo z dostopom dosegljive vse naše transakcije, na čelu z veljavnim plačilnim sredstvom. ◀

△ **Ker Amazon dovoli le šest aktivnih bralnih naprav na en uporabniški račun, je stare naprave, s katerimi ne beremo več, priporočljivo redno brisati z ukazom Deregister.**

Glasba brez iTunes

Uporabniki pametnih telefonov brez logotipa ugriznjenega jabolka že od nekdaj nejeverno poslušamo lastnike Applovih naprav in se čudimo mukam, ki jih trpijo med nalaganjem glasbe na ljubega pametnjakoviča. Vzrok za njihove težave je zgolj eden, sliši pa na ime iTunes. V Cupertinu so zloglasni program v zadnjih letih sicer izboljšali, a preprostost še vedno ni beseda, ki bi jo Applov skupek kode poznal.

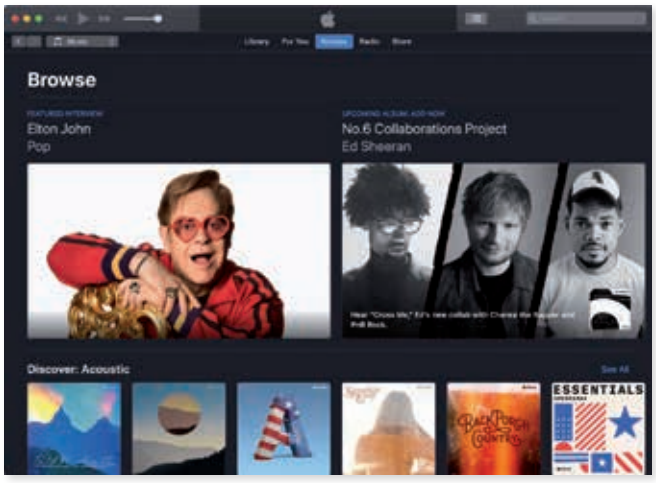
Boris Šavc

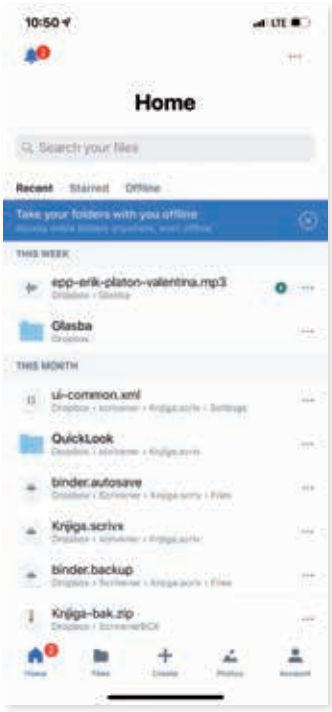
Applov telefon iPhone je užitek uporabljati, ima vrsto zmožnosti, ki so bolje izvedene kot pri tekmecih. Nalaganje glasbe na mobilno napravo pa ni ena izmed njih. Če želimo izbrano pesem prenesti na telefon iPhone, je edina prava pot uporaba programa iTunes. Vsaj tako pravijo v Cupertinu. Medtem ko je iTunes dober za vodenje domače glasbene zbirke in nakup glasbe v digitalni obliki, je za prenos posameznih pesmi z računalnika na telefon na voljo precej boljših alternativ.

iTunes

Prva postaja slehernega glasbenega navdušenca s telefonom iPhone je vseeno program iTunes. Prenos glasbe z računalnika na telefon iPhone s programom iTunes poteka tako, da obe napravi najprej povežemo s kablom, nakar se nameščeni Applov program zažene samodejno. V levem zgornjem kotu nato preverimo, ali je trenutno prikazana knjižnica *Music*, ter zbirki dodamo pesmi po izboru s *File / Add to Library*. Na žalost s tem še nismo končali. Prestavimo se na zavihek *Library*, izberemo ikono s telefonom, opcijo *Music* ter gumb *Sync*. Da vse našteto komaj polovimo v zmedenem uporabniškem vmesniku, je še najmanjša težava. Vedeti moramo, da sinhronizacija vso glasbo, ki je predhodno na telefonu, izbriše. Prav tako podpira prenos samo določene oblike zapisa, na primer mp3, tako da je treba drugače shranjeno glasbo najprej pretvoriti v ustrezen format. Zaradi tovrstnih nerodnosti skoraj vsak uporabnik telefona iPhone, ki je hkrati tudi ljubitelj glasbe in ima zajetno zbirko pesmi na domačem računalniku, prej ali slej začne iskati boljši način.

▽ **Applov program iTunes je za prenašanje glasbe z računalnika na telefon preveč okoren in zmeden, da bi bil prva izbira lastnikov telefona iPhone.**





△ **Brezplačna naročnina na oblak Dropbox uporabniku nudi 2 GB prostora za nalaganje lastne glasbe in drugih datotek.**

Dropbox

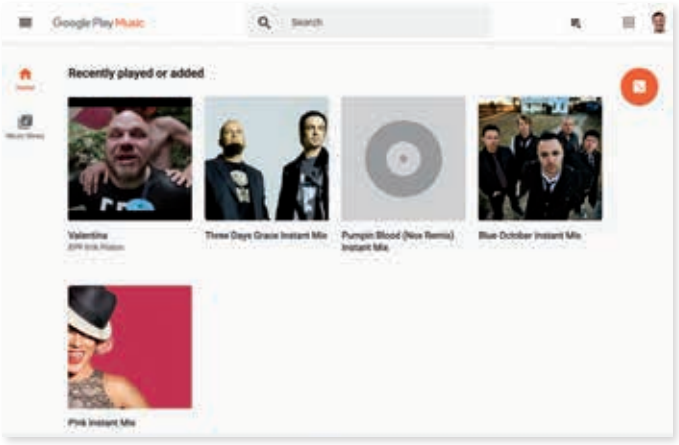
Najočitnejša pot nalaganja glasbe na telefon iPhone brez programa iTunes se skriva v oblačnih storitvah. Oblačna shramba Dropbox uporabnikom, na primer, ponuja 2 GB brezplačnega prostora ter plačljiva paketa z 1 ali 2 TB prostora za glasbeno zbirko in druge podatke. Po prijavi na oblačno storitev priporočamo namestitev namenskega odjemalca na računalnik, ki bo olajšal urejanje zbirke v oblaku. Ko na računalniku z nameščenim odjemalcem določimo z oblakom sinhronizirani imenik, prenesemo vanj želeno glasbo. Dropbox podpira zapis glasbe v oblikah mp3, aiff, m4a in wav.

V naslednjem koraku na tržnici App Store poiščemo aplikacijo Dropbox in jo namestimo na telefon iPhone. Po vpisu najdemo imenik z glasbo in izberemo poljubno pesem. S klikom jo ob vzpostavljeni povezavi z internetom lahko nemudoma poslušamo. Če želimo v njej uživati tudi brez povezave s spletom, jo na mobilno napravo prenesemo z izbiro treh pik in ukaza *Make Available Offline*. Dobra lastnost poslušanja glasbe prek aplikacije Dropbox je v nadaljevanju predvajanja ob menjavi aplikacije. Medtem ko, na primer, YouTube postane nem, ko preklopimo telefon na drugo nameščeno aplikacijo, glasba iz Dropboxa nikoli ne zapusti zvočnikov.

Google Play Music

Google Play Music je ena boljših oblačnih glasbenih storitev, ki uporabnikom med drugim omogoča, da v oblak prenesejo 50.000 lastnih skladb. Uporabnik Googlovega glasbenega oblaka lahko brezplačno prenese svojo glasbo v oblak, jo posluša na številnih napravah in pretočno predvaja celotno Googlovo zbirko z nekaj vmesnimi oglasi. Za predvajanje lastnih skladb na telefonu iPhone je treba na računalnik najprej namestiti program Google Play Music

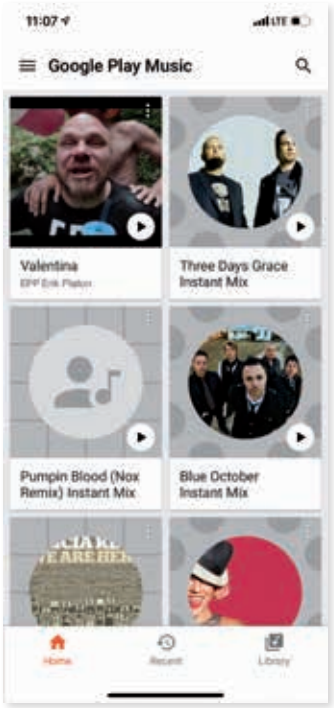
▽ **Glasbo na Googlovo storitev Play Music med drugim nalagamo prek vtičnika za brskalnik Chrome.**



Manager, v katerega se prijavimo z Googlovim računom. V naslednjem koraku v oblak prenesemo želene pesmi, do katerih bomo kasneje dostopali z različnimi napravami, tudi s telefonom iPhone. Podobno funkcionalnost nam omogoča istoimenski vtičnik za brskalnik Chrome. Ko je glasba prenesena v Googlov oblak na tržnici App Store, poiščemo program Google Play Music, ga namestimo in se vpišemo z ustreznimi pooblastili.

Storitev Google Play Music deluje podobno kot iTunes, v osnovi gre za trgovino z glasbo, kjer so nakupi nemudoma dodani zbirki glasbe posameznika, omogočen je tudi prenos pesmi v obliki mp3 na računalnik ali telefon. Ena izmed možnosti je mesečna naročnina, ki omogoča oboje, tako poslušanje prek interneta kot prenos na izbrano napravo, a je predvajanje prenesenih skladb mogoče le z aktivnim naročniškim razmerjem.

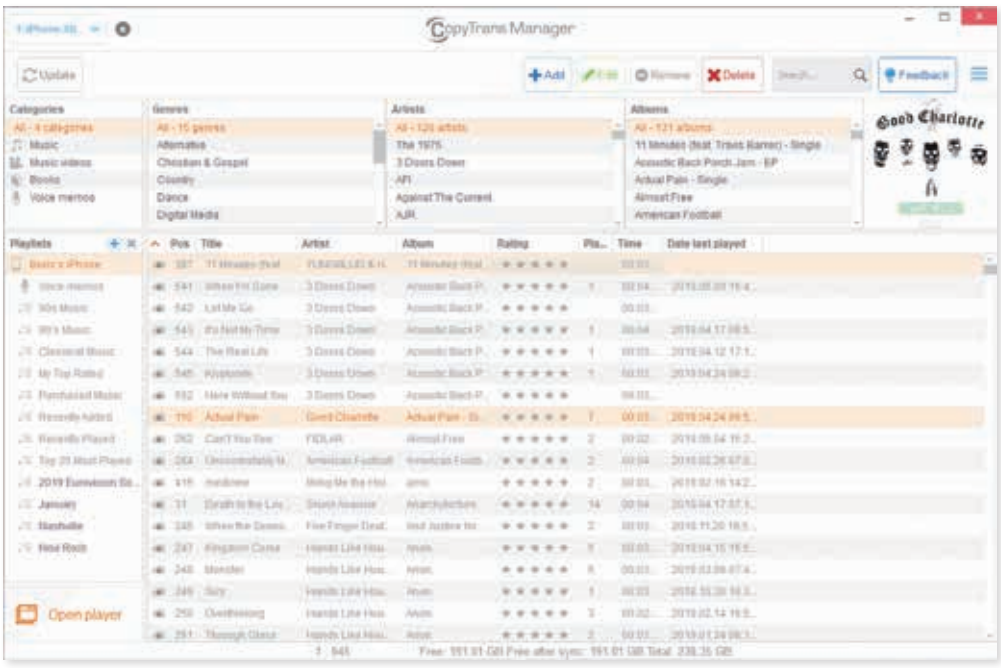
▽ **Lastne pesmi s storitve Google Play Music na telefonu poslušamo z istoimensko aplikacijo, ki jo najdemo na tržnici App Store.**



CopyTrans Manager

Uporabniki računalnikov z operacijskim sistemom Windows imajo za prenos glasbe na telefon iPhone na voljo dostojno in brezplačno alternativo v programu CopyTrans Manager. Program v celoti nadomesti aplikacijo iTunes, omogoča tudi prenos zbirke iz Applovega programa v lastni predvajalnik, kar je dobrodošlo za uporabnike, ki si lastijo glasbo v iTunes in je ne želijo izgubiti z uporabo druge rešitve. Opozoriti velja, da CopyTrans Manager za delo potrebuje vsaj Applove gonilnike, če že ne nameščenega programa iTunes.

▽ **CopyTrans Manager je dostojna alternativa programu iTunes, namenjena uporabnikom računalnikov z operacijskim sistemom Windows.**



△ **Poleg prenašanja glasbe ima AnyTrans v rokavu še precej drugih adutov, med njimi sta uporaba telefona iPhone kot USB-ključka ter urejanje mobilnega vmesnika na daljavo.**

AnyTrans

Najboljša alternativa programu iTunes po mnenju številnih uporabnikov je program AnyTrans razvijalcev iMobie. Odlikuje ga preprostost, hitrost in učinkovit uporabniški vmesnik, ki je skorajda v vsakem pogledu boljši od Applovega programa. AnyTrans v osnovi deluje kot iTunes, skrbi za kopiranje, prenašanje in sinhronizacijo vsebine na mobilno napravo z operacijskim sistemom iOS, a naboru zmožnosti doda vrsto funkcionalnosti, med katerimi ne manjkajo upravitelj nameščenih aplikacij, datotečni raziskovalec, delo z oblakom iCloud in seveda prenos glasbe ter drugih datotek z računalnika na telefon iPhone in v obratni smeri ter med dvema napravama z iOS.

AnyTrans prepriča na področju, kjer se Apple trudi že od vsega začetka. Sicer je iTunes iz leta v leto boljši pri služenju uporabnikom, a ga programski pripomoček podjetja iMobie vseeno prekaša na celi črti. Osrednje pravilo slehernega uporabniškega vmesnika je preprost dostop do funkcionalnosti programa in v AnyTransu res ni težko poiskati vsega, kar nas zanima. Glasbo z računalnika prenesemo z izbiro opcije *Add Content / Add computer content to iPhone*, kjer izberemo datoteko z diska in jo prenesemo v predlagani program. Sistem lokacijo na cilju predlaga samodejno, v primeru glasbe je to aplikacija Apple Music. Po želji lahko mesto izberemo sami.

AnyTrans na željo uporabnika igra vlogo dežurnega upravitelja datotek, spremeni telefon iPhone v USB-ključek, sinhronizira (posamično ali skupinsko) vsebino z oblakom iCloud in skrbi za izdelavo varnostnih kopij telefona. Zadnje sicer učinkovito izvaja tudi program iTunes, kjer pa uporabnik nikoli ne ve natančno, kaj vse je shranjeno v varnostni kopiji. V aplikaciji AnyTrans je omogočen natančen pogled v vsebino varnostne kopije, tako da po želji iz nje povlečemo posamezno besedilno sporočilo, zapisek v programu Notes ali katero drugo, z določenim programom povezano datoteko. Vse naštete dobrote niso zastonj, saj AnyTrans olajša uporabnika za 50 evrskih bankovcev, na katere pa hitro pozabimo med odstranjevanjem programa iTunes, ki ga ne bomo nikoli več potrebovali. ◀

Kodi ali Plex?

Dostop in način konzumacije večpredstavnih vsebin sta se v zadnjih letih močno spremenila. V današnjih časih prevladujejo pretočne storitve in vsebine na družabnih omrežjih, telefoni pa so po priljubljenosti prehiteli televizorje. Ali je v takem okolju sploh še kaj prostora za klasične programske rešitve za hišni kino oziroma večpredstavni center, kot sta Kodi in Plex? Kateri od njiju pa je boljši?

Vladimir Djurdjič

Zanimivo je, da je internet področje medijev v zadnjih letih drastično spremenil, a so glavni gradniki ostali enaki. Uporabniki še vedno poslušamo glasbo, gledamo filme, spremljamo TV-nadaljevanke, gledamo slike. Resda so se pojavili še nekateri derivati, kot so kratki video posnetki (YouTube), podcasti in predvsem video vsebine na družabnih omrežjih, a osnova je že leta enaka.

Spremenil pa se je način, kako in kdaj dostopamo do vsebin. Nekdanjo glasbo na cedejih je že davno nadomestila glasba v računalniških zapisih (MP3 in podobni), to pa zdaj že pošteno izpodriva dostop na zahtevo prek pretočnih storitev (Pandora, TuneIn, Deezer, Apple Music, Google Play Music, Amazon Music ...). Nekaj podrobnega se prav zdaj dogaja na področju filmov, predvsem TV-nadaljevank, kjer kraljujejo pretočni servisi, kot je Netflix.

Spremenil se je tudi način, kako dostopamo do vsebin. Vse našteto nam je na voljo kadarkoli, brez predhodnega prenašanja na lokalno napravo, če le imamo pametni telefon, tablico, računalnik in dovolj hitro internetno povezavo. Zadnja moda so, denimo, digitalne pomočnice, ki znajo gradivo izbrati in predvajati glede na posameznikove preference iz bogate zbirke na internetu.

Kaj pa se je ob vsem tem zgodilo z nekoč priljubljenimi programi in s predvajalniki za hišni kino? Nekateri izdelki so dejansko zamrli, najboljši pa so se prilagodili novim razmeram, a pri tem ohranili združljivost s tem, kar smo uporabniki v vseh preteklih letih nabrali in shranili doma. Večina namreč še vedno hrani fotografije in video posnetke, če ne drugega, iz lastne produkcije.

Med vsemi platformami sta obstala in se okrepila predvsem dva programa – Plex in Kodi, ki danes krojita vrh ponudbe pri hišnem kinu, če odmislimo lastniške sisteme, kot jih ponujajo Apple, Google, Amazon, Netflix, Hulu in drugi. Oba programa imata zveste skupnosti uporabnikov, med katerimi poteka neskončna debata, kateri je boljši.

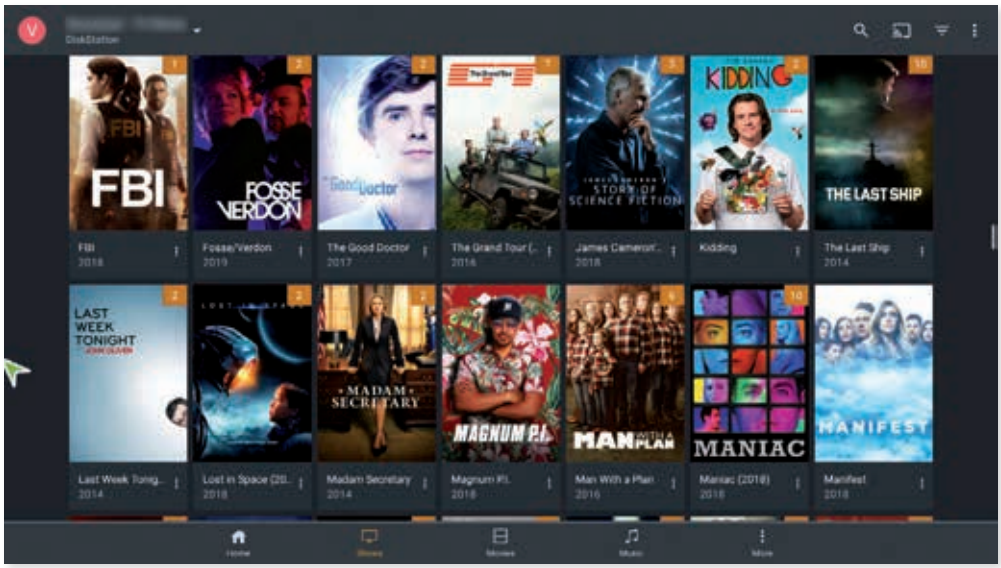
Skupna osnova, a veliko razlik

Preden podrobneje pogledamo trenutno stanje obeh programov, se je modro spomniti, da Plex in Kodi pravzaprav izhajata iz iste osnove. Oba temeljita na nekdanjem projektu XBMC (Xbox Media Center), ki se je kasneje vejil na dva sorodna, a precej drugačna izdelka. Kodi je neposredni naslednik XBMC, s katerim deli nekatere arhitekturne zasnove in celo koncept uporabniškega vmesnika.

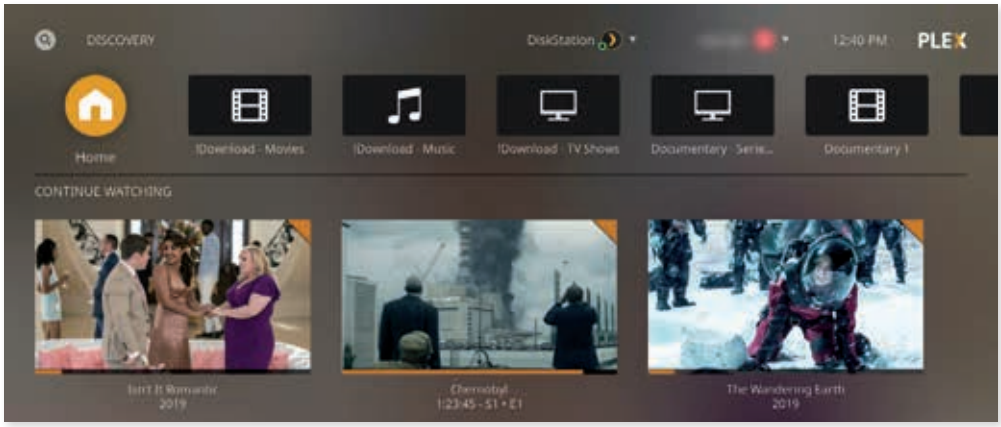
Plex je po drugi strani ubral povsem svojo smer in tudi uporabniški vmesnik se danes znatno razlikuje od tistega, ki ga srečamo v Kodiju. Kar je razumljivo, saj sta se projekta razšla že leta 2008.

Pričakovano je, da obe večpredstavni platformi tekmujeta v funkcionalnostih, kjer je včasih v ospredju eden, nato spet drugi. Kodi je, denimo, na začetku slovel predvsem kot predvajalnik lokalno shranjenih vsebin (filmov, glasbe), pretočni video pa je bil zgolj dodatek. Plex se je kmalu po začetku uveljavil zlasti kot predvajalnik pretočnih vsebin. Pred leti so tako izrabljali javne vsebine servisov Netflix in Hulu za prikaz kot »kanale« v svojem uporabniškem vmesniku,

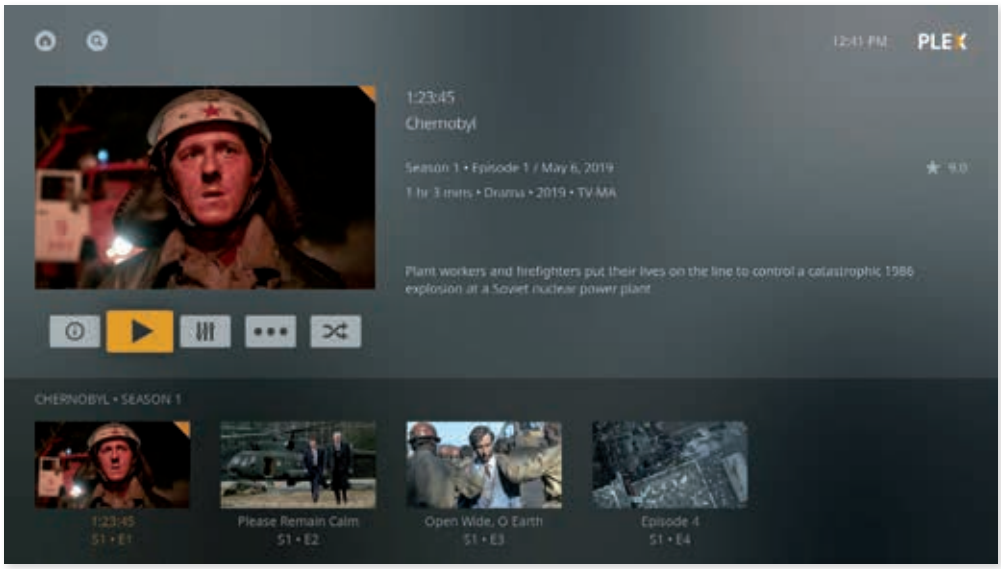
▽ **Plex nudi preprost, a pregleden uporabniški vmesnik, ki je podoben na vseh napravah.**



◁ **Uporabniški vmesnik v programu Kodi lahko povsem spremenimo z oblekami (*skins*).**



▷ **Plex kot plugin v Kodiju deluje pogosto bolje kot osnovni odjemalec za Plex.**



△ **Plex zna serije razvrstiti po sezonah, epizodah in za vsako napisati povzetek.**

kar sta oba spletna pretočna velikana kmalu tehnično in pravno preprečila.

Plex je nato lep čas veljal za najboljšega urednika lokalne zbirke posnetkov in se je v svet pretočnih vsebin vrnil šele v zadnjih dveh letih, toda tokrat podporo za pretočne vsebine dodajajo načrtno, v partnerstvu s ponudniki vsebin. Pred časom so se tako povezali s ponudnikom glasbe Tidal, ki ga lahko naročniki Plexa dobijo z občutnim popustom. Če je uporabniki Plexa seveda v državi, je je Tidal sploh na voljo. Že lep čas krožijo govorice, da se Plex pogovarja s ponudniki pretočnih vsebin s področja filma in TV-serij, vendar za zdaj še ni konkretnejših podatkov o partnerjih.

Kodi po drugi strani še vedno stavi na svoje korenine in se distancira od vsebin, ki jih uporabniki uporabljajo v tej programski opremi. To je tudi omogočilo, da v skupnosti, ki podpira Kodi, nastalo kup repozitorijev s pretočnimi vsebinami, kjer lahko dobimo dobesedno vse, od najnovejših filmov do zadnjih epizod TV-serij in celo posnetkov v živo športnih dogodkov, tudi takih, ki jih sicer v teh krajih legalno skoraj ne moremo (recimo tekem NBA).

Cena tega je, da medijske hiše in ponudniki Kodi preganjajo in zapirajo pipe (repozitorije), a se nenehno odpirajo nove. Pred leti je bilo celo videti, da bo Kodi postal eden rednih programov na sodobnih pametnih televizorjih, a so medijske hiše zagrozile proizvajalcem televizorjev, tako da združljivosti s platformo Kodi nobeden ne obeša več na veliki zvon. Toda če imate pravi operacijski sistem (navaden Android, še raje kot Android TV), obstaja odvod, ki hitro pripelje do spornih repozitorijev.

Tekma za vsebine

Tako Kodi kot Plex poskušata pridobiti privržence s kar se da širokim naborom podprtih vsebin, ki jih znata predvajati. Oba enako dobro podpirata osnovne storitve, torej predvajanje filmov, TV.nadaljevank, glasbe in fotografij. V obeh primerih so podprti številni večpredstavni formati, oba znata z interneta potegniti posterje, opise, podnapise (filmi, serije) in besedila (glasba), kar obvladata celo bolje od nekaterih komercialnih pretočnih servisov. Ta del je dodelan že vrsto let, zato so novosti pogosto manjše, a za redne uporabnike koristne.

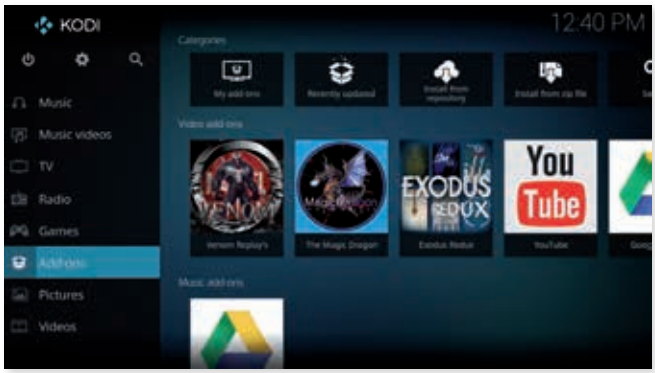
Plex želi predvsem ponoviti uporabniško izkušnjo IP-televizije in servisov, kot je Netflix, kjer poskušajo pred uporabnikom skriti večino kompleksnosti izbire in konfiguracij za dostopov do virov. S te plati je precej prijaznejši do tistih, ki imajo manj izkušenj. Že lep čas podpirajo predvajanje podcastov, prav tako so začeli zbirati sveže video novice iz različnih virov in jih predvajati kot tematski kanal (News), ki je dostopen na zahtevo. Če je v napravi (to velja predvsem za računalnike PC) vgrajena kartica za dostop do TV-signala, lahko Plex uporabljamo tudi kot snemalnik oddaj, kar Plex počne neposredno, medtem ko Kodi za to potrebuje programe tretjih partnerjev. Resnici na ljubo je v današnjih časih zaradi možnosti predvajanja na zahtevo in možnosti ogleda programov z zamikom to manj zanimivo kot nekoč.

Kjer je Plex nekoliko slaboten, so vtičniki za dodatne vsebine, predvsem spletne servise. Vsaj v primerjavi s Kodijem, ki na tem področju kraljuje, je vtičnikov malo in ti so manj zanimivi. To je zanimivo, saj so ponudniki vsebin, kot sta YouTube in Netflix, tovrstne vtičnike že pred leti prepovedali, zato Plex ni več toliko vlagal v razvoj. Mimogrede, kljub nekdanji skupni osnovi obeh programov vtičniki za Plex niso združljivi s Kodijem in obratno.

Če Plex poskuša kompleksnost nastavitev skriti pred uporabniki, je Kodi pravo orodje za poznavalce, saj brez izdatnega konfiguriranja in dodajanja dodatkov iz programa ne bomo znali izvleči vsega, kar zna. Toda ta konfiguracija zna biti kar precej kompleksna in nekako zahteva, da spremljamo forume in izkušnje iz skupnosti. Torej se moramo bolj posvetiti programu namesto vsebinam.

Kodi je močan predvsem tam, kjer je Plex šibek, torej pri vtičnikih in predvsem pri tako imenovanih repozitorijih (internetnih strežnikih) vsebin. Toda takoj je treba zapisati, da priljubljenost izhaja predvsem iz ponudbe, ki ni legalna. Na spletu kar mrgoli strežnikov, kjer uporabniki na lastno pest pretočno strežejo vsebine vseh tipov, od filmov, glasbe, najnovejših nadaljevank (ko so te predvajane v domači državi) do koncertov, športnih dogodkov, celo v živo.

Čeprav se zdijo repozitoriji uresničitev sanj za video navdušence, je njihova uporaba pogosto problematična. Prvič, repozitoriji nastajajo in se ugašajo kot gobe po dežju, pač glede na to, kako jih oblasti izsledijo in blokirajo. Drugič, kakovost posnetkov v njih močno niha, tako pri ločljivosti kot kakovosti.

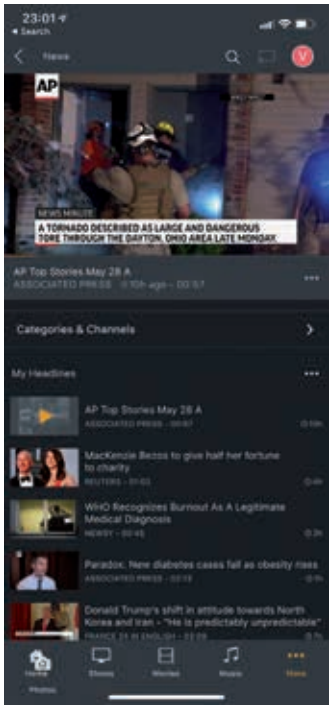


△ **Glavni adut v Kodiju so dodatki (*plugins*) in repozitoriji.**

Zanesljivost predvajanja je tudi vprašljiva, ne glede na to, kako kakovostno povezavo ima uporabnik, saj sta vprašljivi obremenjenost in kakovost povezave nelegalnih strežnikov. Ne nazadnje pa je repozitorije treba najti in jih pravilno konfigurirati, kjer bi si upal trditi, da to presega sposobnost in voljo tehnično manj poučenih. Toda navdušencev to ne bo odvrnilo.

Odprtost programa Kodi se kaže tudi pri možnosti rabe drugačnih vsebin. Znano je, da je mogoče v nekaterih primerih Kodi povezati z možnostjo predvajanja programov IPTV, torej takih, kot jih danes pretežno uporabljamo tudi v Sloveniji. Seveda pod pogojem, da ponudnik storitev podpira dostop do teh pretočnih zapisov pri drugih programih, ne samo pri lastnih škatlah STB. Plex česa podobnega ne podpira.

▽ **Plex se obnese tudi na malih zaslonih telefonov, v tem primeru kot agregator za novice.**



Arhitektura in podprte naprave

Če sta si Kodi in Plex zelo podobna po vsebinah, ki jih lahko predvajata, pa se močno razlikujeta v sami arhitekturi in napravah, na katerih delujeta. Plex je v prvi vrsti strežnik, s katerim lahko povežemo odjemalec. Najbolj deluje seveda v kombinaciji z odjemalci Plex, a ga lahko uporabljamo tudi z drugimi, ki znajo uporabljati vire po protokolu DLNA. Do strežnika lahko dostopa seveda hkrati več odjemalcev in vsi imajo na voljo iste podatke.

Strežnik Plex je več kot samo shramba za datoteke. Ena od pomembnih funkcij je ta, da lahko strežnik na zahtevo (med predvajanjem) pretvarja podatke iz enega zapisa v drugega, kar je izredno koristno, če ciljna naprava, denimo predvajalnik v televizorju, ne podpira kodeka, s katerim je narejen posnetek. Seveda potrebujemo dovolj zmogljiv strežnik, da bo pretvorba potekala dovolj hitro, sicer bo uporabnik na odjemalcu izkusil zaustavitve ob predvajanju, da bo strežnik lahko dohitel potrebe odjemalca.

Za strežnik Plex lahko uporabimo poljuben računalnik v okolju Windows, MacOS ali Linux (zanimivo, podprto je tudi virtualno okolje Docker), zelo pa je priljubljena možnost, da strežnik Plex poganjamo na napravi NAS. V mojem primeru je to že vrsto let izdelek družbe Synology, podprti pa so tudi QNAP, Netgear, Drobo, Western Digital in številni drugi. Učinkovita in elegantna rešitev. Strežnik Plex ima še nekaj drugih posebnosti, ki jih Kodi ne zmore. Posnetke lahko, denimo, na varen način strežе tudi zunaj domačega omrežja, onkraj požarnega zidu, kar pride prav, če želimo do vsebin dostopati, kadar smo od doma.

Kodi je po drugi strani odjemalec, ki je mišljen predvsem za rabo na eni napravi. Čeprav ima podporo za spletno strežbo, pravega strežnika tu ni oziroma uporablja druge strežnike, ki ponujajo vsebine po protokolu DLNA. V tem primeru postane podpora za različne funkcije in vsebine nekoliko bolj omejena, zato večina nameščenih sistemov uporablja lokalno nameščene ali prek omrežnega diska oziroma USB-medija dodane vsebine.

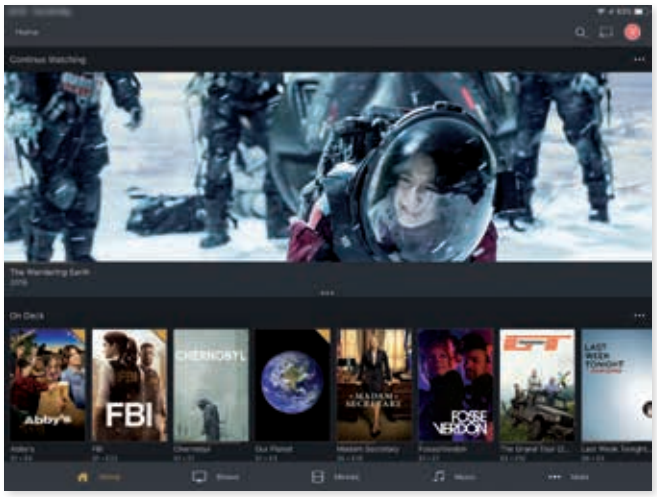
Kodi bo najbrž prva izbira za vsakogar, ki bo večpredstavni program poganjal v okoljih Windows, Linux ali Android, celo Raspeberry Pi. Toda, pozor, za predvajanje video posnetkov, zlasti v visokih ločljivostih (4K), utegne strojna oprema tudi poklekniti pod bremenom. Zlasti mali Raspberry in številni predvajalniki z Androidom kitajskega izvora utegnejo tu doživljati neželene zaustavitve.

Po drugi strani bomo Kodi neuspešno iskali na Applovih platformah iPad, iPhone in Apple TV. No, spletna stran navaja, da Kodi deluje na iOS, ampak moramo v tem primeru uporabljati napravo, ki je odklenjena (*jailbreak*) za namestitev programa mimo Apple App Stora. Dvomimo, da je veliko takih, ki bi to počeli. Prav tako Kodija ne moremo uporabljati s predvajalniki Chromecast, Amazon Fire TV in številnimi drugimi (Roku …), ki pa v naših krajih niso tako zelo razširjeni. Za vse naštete pa najdemo ustrezne predvajalnike za Plex, kar je izredno pomembno. Plex je kot odjemalec na voljo tudi za kup pametnih televizorjev, kjer Kodi zaradi prej omejenih nasprotovanj založnikov ni prisoten.

Kljub široki razširjenosti in raznolikosti podprtih naprav Plex zagotavlja enotno uporabniško izkušnjo na skoraj vseh platformah. Še več, če ga uporabljamo na mobilnih napravah, omogoča, da določene vsebine prenesemo na lokalno napravo in posnetke nemoteno predvajamo, tudi če nimamo internetne povezave (pogost scenarij – med letom na letalu).

V današnjih časih je nekaj povsem običajnega, če imamo doma več odjemalcev, kot so televizorji, telefoni, tablice. Plex tu omogoča enoten dostop in sinhronizacijo podatkov, video posnetkov in fotografij z lokalne naprave na strežnik, kjer so vselej dostopni vsem. Seveda lahko omejimo dostop glede na profil uporabnika. S Kodijem je veliko tega zelo težko narediti ali celo nemogoče.

Ne nazadnje, če, denimo, danes uporabljamo Alexo kot digitalno pomočnico, jo lahko z ustrezno spretnostjo (Plex skill) naprosimo, da predvaja točno določeno skladbo ali izvajalca iz zbirke posnetkov na domačem strežniku Plex. Pri Kodiju je ta korak nekoliko težavnejši,



◁ **Plex na iPadu je zelo enostavno krmiliti zaradi zaslona na dotik.**

saj moramo odjemalec za Kodija spremeniti tudi v spletni strežnik in ga kot takega povezati z Alexo. Plexovi strežniki, ki delujejo na dediciranih napravah (NAS, PC) so po tej plati precej lažja pot.

Uporabniška izkušnja

Najbrž se strinjamo, da pri gledanju filmov, sploh pa pri poslušanju glasbe, ne želimo preveč ukvarjanja s programom, temveč z vsebinami. Če se preveč ukvarjamo s programom, je že nekaj narobe.

S te plati tako Kodi kot Plex zaostajata za nekaterimi bolj domišljenimi odjemalci, kot sta Youtube in Netflix, a se avtorji močno trudijo, da bi ta razkorak nadomestili. Dejanska uporabniška izkušnja je zelo odvisna od naprave, kjer deluje odjemalec. Če sta to tablica in telefon, je uporabniška izkušnja najbolj tekoča. Lep je primer, če imamo Chromecast, lahko celotno vsebino izberemo s telefonom ali tablico in samo rezultat »pretočimo« na ciljno napravo. Elegantno, preprosto, učinkovito.

Tam, kjer zaslon na dotik ni na voljo, nam ne preostane drugega kot krmiljenje s tipkovnico ali daljincem. Daljinci so v večini primerov silno nerodni, ampak delujejo. V pomoč pri obeh platformam so razni programi za pametne telefone, ki jih spremenijo v priložnostne napredne daljince, kar je že bolje, v nekaterih primerih (Yatse za Kodi) celo odlično. Zanimivo, da oba programa še naprej podpirata navigacijo prek smerniških tip na tipkovnici. Resnici na ljubo je to najboljši način, in če premoremo dvostranski daljinec z alfanumerično tipkovnico, smo zmagali. Ali pa tovrstno navigacijo uporabimo v programskem daljincu (denimo omenjenem Yatse).

Kar se tiče videza programa, o zmagovalci ni dvoma. Eden od adutov programa Kodi so različne obleke (*skins*), s katerimi lahko povsem spremenimo videz in predstavitev vsebin. Plex je s te plati močno zaostal, a zasleduje drugačno strategijo. To je res stvar osebnega okusa, velja pa paziti, da v Kodiju s prilagajanjem ne pretiravamo, saj lahko naletimo na težave, iz katerih nas reši le ponovna namestitev programa. Kar je nekako značilno za ljubiteljske programe, mar ne?

Kaj torej, Plex ali Kodi?

Vprašanje, zastavljeno v naslovu tega članka, je pravzaprav napačno. Morda je prava odločitev, da ne izberemo enega ali drugega, temveč kar oba. Izdelka se namreč dopolnjujeta in lahko povsem koristno sobivata v domačem kinu. Še več, razvijalci obeh projektov so začeli spet sodelovati, rezultat pa je Plex for Kodi, vtičnik za platformo Kodi, na katerega lahko prikazujemo in predvajamo vsebine na strežnikih Plex.

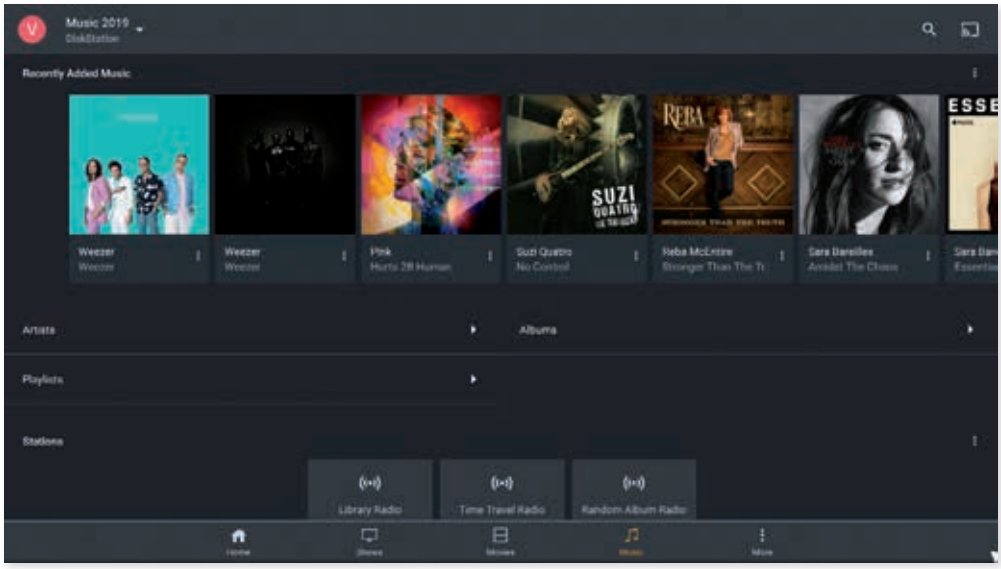
Da bi bila stvar še bolj hecna – Plex for Kodi v številih primeri celo prekaša uradni odjemalec za Plex! Kar se sliši skoraj neverjetno, toda dejstvo je, da je Plex svoje kompetence vgrajeval predvsem v strežnik, Kodi pa v odjemalec, zato je Kodi in s tem Plex na Kodiju bolj odziven, manj problematičen pri podpori za nekatere manj pogoste video standarde in podobno. V praksi se je že večkrat zgodilo, da sem pri težavah z odjemalcem Plex določeno vsebino brez težav predvajal v vtičniku za Plex za Kodi. Neverjetno, a resnično.

Pri odločitvi lahko pomaga, kot je to običajno, tudi cena. Kodi je vselej brezplačen, ne glede na dodatke in vtičnike. Če ga namestimo na Raspberry Pi, star računalnik ali enega od kitajskih Android predvajalnikov, se približujemo brezplačnosti.

Plex obstaja v brezplačni različici, a so številne dobrote plačljive. Denimo dodatki za filme, besedila za pesmi, napredne funkcije za pregledovanje fotografij na časovni osi, možnost izbranih vsebin v lokalnem pomnilniku mobilne naprave in drugo. Po mojih izkušnjah te dodatne lastnosti kot tudi možnost pogostejših dostopov do nadgradenj in popravkov (vsakih nekaj tednov) več kot odtehtajo 40 evrov letne naročnine, kolikor stane storitev Plexpass.

Kjer naprave to omogočajo, svetujem torej namestitev in uporabo obeh izdelkov. Kasneje vzdrževanje stanja ne bo vzelo dosti dodatnega časa, še zlasti, če vsebine shranimo na enotnem (Plex) strežniku. V mojem domačem okolju je taka konfiguracija v uporabi že vrsto let in med drugim je preživela tudi večjo katastrofo z diski, kjer sem jo odnesel brez izgube samega posnetka.

▽ **Plex omogoča, da lokalno shranjeno glasbo spremenimo v virtualni radio.**



Domači kino proti pretočnim servisom

V današnjih časih bo marsikdo oporekal, da je pravi odgovor na vprašanje v naslovu prispevka pravzaprav: nobeden. Zakaj bi filme, glasbo, TV-serije, fotografije shranjevali in predvajali lokalno, če lahko uporabimo enega od vse bolj priljubljenih spletnih servisov?

V Sloveniji smo bili lep čas pri tovrstnih storitvah omejeni, saj številni plačljivi servisi niso bili dosegljivi pri nas. V zadnjih letih se je to spremenilo. Netflix, Apple Music, Deezer in številni drugi so na voljo tudi pri nas, in to s sprejemljivimi mesečnimi naročninami. Zakaj bi se sploh še kdo ukvarjal s programi, kot sta Kodi in Plex?

Odgovor ni preprost in je odvisen od potreb ter želja vsakega posameznika. Če se zadovoljimo s ponudbo spletnih servisov in nimamo domače zbirke, programov Plex in Kodi najbrž ne potrebujemo. Pretočno predvajanje se poleg naročnin pozna zgolj na strošku prenosa podatkov na napravo, kar pa je vse manjša omejitev, če sploh. Poleg tega veliko odjemalcev kljub osnovnemu načinu dela omogoča, da podatke začasno premaknemo na lokalno napravo in tam uporabljamo, kadar nimamo internetne povezave.

Toda omenjeni spletni servisi ne nudijo vseh iskanih vsebin. Ponudba Netflixa v Sloveniji je še naprej precej skromnejša od tiste v ZDA. Če gledamo serije Netflixa, HBO in Amazona začne nabor naročnin hitro naraščati, nekaterih (Hulu) pa pri nas sploh ne moremo spremljati. Prav tako ne smemo pozabiti na lastno preteklost in pogosto dragocene posnetke, ki bi jih morda kdaj še radi našli in pogledali oziroma poslušali. Ne nazadnje pa Kodi in Plex ponujata enovito uporabniško izkušnjo, spletni servisi pa so vsak zase. Vsaj za zdaj, toda pričakujemo lahko, da se bo to morda tudi spremenilo. ◀

VARNOST DOMA

- Kako ubraniti domače računalnike
- Izdelajmo odprtokodni usmerjevalnik

Kako ubraniti domače računalnike

Domači računalniki s stalno internetno povezavo so običajno lahke tarče hekerjev. Kako zaščitimo njihovo vgrajeno programsko opremo, operacijski sistem in aplikacije? Na kaj moramo paziti pri nastavitvah kabelskega modema in delu z računalnikom?

Simon Peter Vavpotič

Verjetnost usmerjenega hekerskega napada na domače računalniško omrežje (intranet) je majhna, saj bi hekerji le s težavo pridobili uporabne informacije, razen če iščejo prav vaše osebne podatke, vam želijo načrtno onemogočiti internetno delo, vam sledijo ali pa želijo vaš računalnik izrabiti pri spletnih napadih na večje tarče. Verjetnost vdora v spletno banko ali druge varne storitve v računalniku je majhna, saj hekerji vedo, da bi bili pri takem dejanju hitro zasačeni, če bi imeli od njega kakršnekoli koristi. Kljub temu je občutek, da lahko nekdo sorazmerno hitro vlomi v naš intranet in domači računalnik, srh vzbujajoč.

Čeprav se večina vseeno sprijazni z mislijo, da se to njim pač ne more zgoditi, ker niso pomembne javne osebnosti, je bolje intranet zavarovati prej, saj pri zlonamernih spremembah vgrajenih programskih oprem domačih računalnikov in drugih računalniških naprav navadno ni več poti nazaj in smo prisiljeni k nakupu nove strojne opreme. Tudi obsežnejši hekerski napad, ki bi naključno zajel naše računalnike, ni izključen. V preteklosti so hekerji pri takšnih napadih vselej izrabili nezakrpane varnostne luknje v priljubljeni velikoserijski strojni in programski opremi, tako da so z zlonamerno programsko opremo okužili čim več računalnikov.

Kritične točke intraneta

Najenostavneje se pred nevarnostmi s spleta zavarujemo tako, da poiščemo šibke točke intraneta, ki jih predstavljajo ključna omrežna oprema in izpostavljeni domači računalniki. Pri tem se moramo vprašati, na katere načine lahko v domače računalnike vstopajo informacije in programska koda z interneta. Potencialno nevarnost predstavlja tudi možnost samodejne vzpostavitve brezžičnih povezav za prenos podatkov Bluetooth (angl. autopairing).

Manj zahtevni uporabniki se pri omrežni opremi pogosto zanašajo na enostavne brezžične rešitve, kot je brezžični modem, ki je obenem most ali usmerjevalnik med javnim brezžičnim podatkovnim omrežjem (npr. UMTS G4) in lokalnim Wi-Fi. Vendar se moramo zavedati, da brezžičnih povezav skoraj ni mogoče popolnoma zaščititi, so pa lahko dostopne le v določenem prostorskem dosegu, kar pomeni, da morajo hekerji prvi napad izvesti z ne preveč oddaljene lokacije. Če jim pri tem uspe namestiti odzadnja vrata v naše računalnike, lahko napad nadaljujejo iz kateregakoli računalnika z internetno povezavo.

Vendar bo samo amaterski heker prvi napad izvedel tako, da bo sedel v avtomobilu. Profesionalec bo raje vanj skril računalniško komunikacijsko opremo (npr. prenosni računalnik z internetno povezavo prek mobilnega omrežja in povezavo Wi-Fi) in avto parkiral v bližino vašega doma, nečednosti pa bo izvajal s čim bolj oddaljene lokacije prek temnega dela interneta.

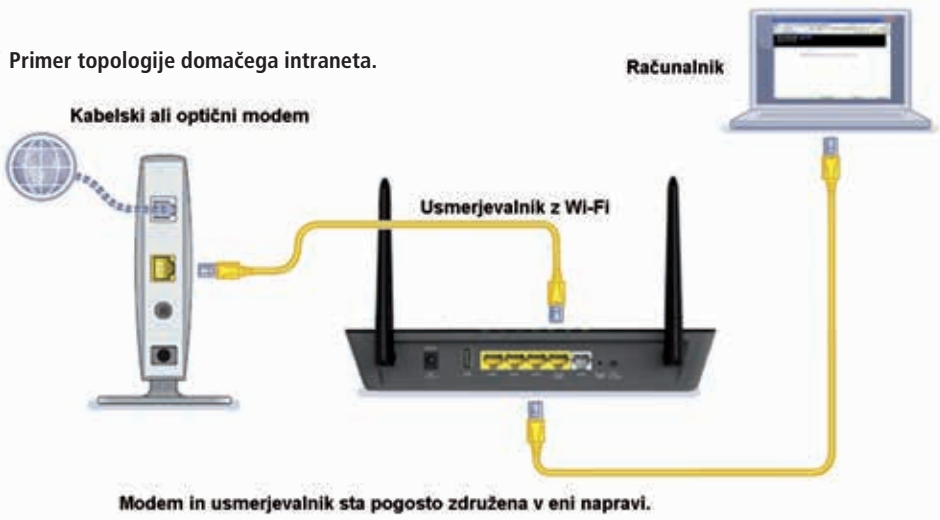
V tem pogledu je žična povezava z internetom ob pravilnih nastavitvah usmerjevalnika v kabelskem modemu veliko varnejša, saj mora imeti napadalec fizični dostop do kabelskega omrežja, kar pa ni nemogoče, razen če mu pomaga kdo od zaposlenih pri ponudniku dostopa do interneta ali pa ta ne zmore zagotavljati celovite informacijske varnosti svojih strežnikov in omrežja usmerjevalnikov, s katerim je povezana modemska naprava.

Kritične točke predstavljajo tudi računalniki v intranetnem omrežju, s katerimi pogosto dostopamo do različnih spletnih storitev (npr. Skype, e-pošta …) in spletnih strani ter nanje pogosto nameščamo novo

△ Sodobni brezžični usmerjevalnik.

▽ Enostavni kabelski modem z enim ethernetnim priključkom.

▽ Primer topologije domačega intraneta.



Modem in usmerjevalnik sta pogosto združena v eni napravi.

programsko opremo s spleta. Posebno skrb velja nameniti računalnikom, ki so stalno vklopljeni in povezani z internetom, saj imajo hekerji pri teh več časa za izvajanje svojih nečednosti.

Zaščita primarnega dostopa do interneta

Pri postavitvi domačega intranetnega omrežja se pogosto zanašamo na infrastrukturo, ki jo zagotavlja ponudnik dostopa do interneta. Večina ima doma brezžični ali kabelski modem, ki je v lasti ponudnika. Redki srečniki, ki živijo v središčih velikih mest (med njimi je tudi Ljubljana), lahko shajajo celo brez lastne omrežne infrastrukture, saj imajo na voljo javno omrežje Wi-Fi, s katerim lahko neposredno povežejo svoje računalnike in pametne telefone.

Kljub temu moramo za vsak način povezovanja izbrati primerno zaščito. Pri neposrednem povezovanju z javnim omrežjem Wi-Fi moramo ustrezno zaščititi tako vhodni kot izhodni podatkovni promet. Vendar pri upravljanju teh naprav nimamo popolne svobode, saj ima glavno skrbniško geslo ponudnik dostopa do interneta, ki zagotavlja tudi redne posodobitve vgrajene programske opreme. Kljub temu lahko z omejevanjem dovoljenih protokolov in vrat IP za prenos podatkov v dobršni meri tudi sami vplivamo na možnosti komunikacije programske opreme s temnimi podomrežji interneta, prek katerih hekerji izvajajo svoje aktivnosti.

▽ **Tiskano vezje odprtokodnega usmerjevalnika, za katerega lahko razvijamo lastno programsko opremo Banana Pi.**

operacijski sistem, tako da uporabimo vsaj požarni zid (vgrajen v vse novejše Windows) oziroma izberemo priporočene nastavitve za povezovanje z javnimi omrežji. Zaradi številnih ranljivosti operacijskih sistemov je dobro, da brezžično povezavo vzpostavimo le v času, ko dejansko potrebujemo dostop do interneta.

Brezžični in kabelski modem po drugi strani omogočata večjo varnost, saj zna večina filtrirati

Kako nastaviti usmerjevalnik in požarni zid modema?

Nastavitve kabelskega ali brezžičnega modema so izredno občutljivo področje, kjer moramo vsako spremembo najprej premisliti s stališča *informacijske* varnosti in šele nato razmišljati o udobnejšem delu. Navadno lahko z uporabniškim geslom iz intranetnega omrežja tudi sami nastavljamo v modem vgrajeni usmerjevalnik ali filter za prenos podatkov. Smiselno je, da stanje svojih nastavitev nato redno pregledujemo, saj se lahko med posodobitvami vgrajene programske opreme, ki jih prek kabelskega ali optičnega omrežja izvaja ponudnik internetnih storitev, nehote zgodi, da nekatere nastavitve spremenijo svoj pomen ali pa se izgubijo.

Med pregledom nastavitev je dobro preveriti predvsem nastavitve filtra za pakete IP oziroma požarnega zidu, ki varuje intranet pred vdori z interneta. Omogoča naj le tiste povezave, vrste paketov in protokole, ki jih zares potrebujemo. Posebno pozornost velja nameniti omogočanju protokola za dostop do spletnih strežnikov DNS. Večjo varnost zagotovimo tako, da računalnikom v intranetu omogočimo dostop le do enega tovrstnega strežnika, denimo tistega, ki ga omogoča ponudnik dostopa do interneta. Ob morebitnem hekerskem vdoru v katerega od računalnikov z internetno povezavo tako hekerji ne bodo mogli preusmeriti storitve DNS na kak strežnik v temnem delu interneta in si tako ne bodo olajšali nameščanja zlonamerne programske opreme.

Obenem velja preprečiti vhodne povezave in protokole, prek katerih lahko hekerji dosežejo različne storitve računalnikov v intranetu, kot sta terminalska povezava in upravljavska povezava, ki omogoča oddaljene posege v sistemski register. Čeprav tovrstne dostope z interneta omejujejo požarni zidovi operacijskih sistemov, je varneje, če jih preprečimo že na ravni usmerjevalnika, saj tako morebitna namestitev

VDOR

Kako poteka usmerjeni hekerski napad?

Vdor v domače računalnike je za nepoučenega uporabnika neopazen, razen ko se hekerju kaj zalomi ali pa sam želi vzbuditi pozornost. V prvem koraku si poskuša heker zagotoviti stalno spletno sledljivost izbranega računalnika, na primer, tako, da v njem aktivira katero od storitev, ki določen spletni strežnik v temnem delu interneta stalno obvešča o njegovi prisotnosti na internetu, saj večina domačih računalnikov ne uporablja stalnega naslova IP. Sledljivost lahko v nekaterih primerih heker zagotovi tudi z aktivacijo storitev, kot je UPNP (univerzalni priključi in uporabljaj, angl. Universal Plug & Play), ob pomoči katerih ciljni računalnik ali usmerjevalnik, prek katerega je ta povezan s svetovnim spletom, samodejno periodično razpošilja informacijske pakete, s katerimi druge naprave v omrežju obvešča o svoji prisotnosti. K sreči je tovrstno razpošiljanje omejeno na določeno globino internetnega omrežja (npr. do 5 usmerjevalnikov) in mora imeti heker zato v tem dosegu na voljo dodatne zmogljivosti.

V drugem koraku poskuša v operacijski sistem namestiti vohunske storitve, s katerimi lahko, na primer, zajema pritiske na tipke s tipkovnice ali dostopa do zaščitenega dela računalnikovega pomnilnika, v katerem se izvaja jedro operacijskega sistema, kar mu omogoči, da se na koncu dokoplje do skrbniških gesel. Zaradi ranljivosti Spectra in Meltdown pri večini računalnikov za izvedbo druge faze napada zadošča že zagon zlonamerne programske kode pod katerimkoli uporabnikom.

Tretji korak je prikrajanje sistemske programske opreme in vgrajene programske opreme računalnika. Heker lahko z glavnim skrbniškim geslom dostopa do vseh funkcionalnosti, spremeni nastavitve BIOS in v vgrajeno programsko opremo računalnika vsadi svojo programsko kodo, ki mu omogoči neomejen nadzor nad računalnikom ne glede na to, kateri operacijski sistem namestimo. Pomagata le brisanje vseh diskov in popolna nadomestitev vse vgrajene programske opreme z originalno, a kaj, ko je to pogosto misija nemogoče, saj proizvajalci navadno objavljajo le nujne posodobitve vgrajene programske opreme, ne pa tudi vgrajene programske opreme v celoti.

Varne poverilnice

Ker je dostop do sistemskih nastavitev usmerjevalnika ali operacijskega sistema varovan zgolj z uporabniškimi imenom in geslom, sta zelo pomembni njuna dolžina in zgradba. Vsaj geslo naj ne bi bilo beseda iz kakega naravnega jezika ali lastno ime, vsebovalo pa naj bi tudi številke in posebne znake. Tako geslo si je težko zapomniti na pamet, zato si lahko pomagamo z elektronsko shrambo za gesla oziroma s strojnim upravljalnikom gesel, ki ga lahko izdelamo tudi sami. Več na spletni strani sites.google.com/site/pcusbprojects. Obenem je dobro, da tudi uporabniško ime skrbnika ni ravno *administrator*.

zlonamerne programske opreme v osebnem računalniku ne more vplivati nanje.

Sodobni kabelski modemi omogočajo tudi brezžični dostop, ki lahko hekerjem bistveno olajša delo, saj v modem z bližnje lokacije neopaženo vdrejo kar ob pomoči napak v protokolih WAP in WAP 2. Pomaga le, če takega dostopa ne omogočimo oziroma ga ne uporabljamo.

Dodatni usmerjevalnik

Lastni usmerjevalnik s požarnim zidom lahko bistveno poveča zaščito pred vdori pobesnelih hekerjev z interneta, saj ga samostojno upravljamo in tudi zaščitimo z lastnimi skrbniškim geslom. Običajno ga upravljamo le iz intraneta, zato lahko hekerji vanj vdrejo kvečjemu, če predhodno z zlonamerno programsko kodo okužijo katerega od računalnikov v intranetu in ga uporabijo kot most.

Za usmerjevalnik lahko uporabimo namensko napravo enega od svetovnih proizvajalcev ali pa (star) PC, v katerega namestimo dve omrežni kartici ali več ter ustrezno (namensko) programsko opremo. Tako heker ob morebitnem vdoru v kabelski modem še vedno ne bo mogel neposredno dostopati do intraneta, ampak bo v naslednjem koraku naletel na zanj neznano strojno in programsko opremo (tj. naš usmerjevalnik), ki ga bo zelo verjetno odvrnila od nadaljnjih poskusov vdora intranetno omrežje.

Vseeno predstavlja postavitev lastnega usmerjevalnika tudi določeno tveganje, ki je pogojeno predvsem z možnostmi samodejnega posodabljanja njegove programske opreme s spletnih strežnikov proizvajalca (ali proizvajalcev) in možnostmi za skrbniški dostop proizvajalca do njegovih nastavitev. Oboje lahko hekerji izkoristijo za vdor vanj in nameščanje svoje zlonamerne programske opreme vanj.

Večino sodobnih usmerjevalnikov, podobno kot modeme ponudnikov dostopa do interneta, upravljamo prek spletnega brskalnika in izbranih vrat po protokolu TCP/IP. Čeprav je tovrstni dostop (običajno) mogoč samo iz intranetnega omrežja, nevarnost, da bi heker prek obvoda v katerem od intranetnih računalnikov onesposobil požarni zid usmerjevalnika, vseeno obstaja.

Hekerji lahko za vdor v intranet uporabijo tudi lažne strežnike DNS, s katerimi pretentajo usmerjevalnik, da prevzame posodobitve programske opreme s strežnika v temnem delu interneta. Če posodabljanja programske opreme usmerjevalnika prav zato ne želimo, lahko to možnost izklopimo v nastavitvah, možnost vsiljenih posodobitev pa preprečimo tako, da namesto naslova strežnika DNS v omrežju IPv4 ali IPv6 vnesemo ničelno vrednost (za IPv4 je to 0.0.0.0).

Med nastavitvami velja močno omejiti tudi možnosti upravljanja usmerjevalnika, tako da je to mogoče le prek namenske povezave z varnim PC v intranetu (npr. namenski ethernetni priključek, USB) ali pa le prek lastne tipkovnice in zaslona usmerjevalnika, če smo ga zgradili na osnovi (odsluženega) peceja ali odprtokodnega usmerjevalnika.

Kakšnemu usmerjevalniku zaupati?

Čeprav je zaupanje v namenske naprave pogosto večje kot v tiste, ki jih na osnovi PC in namenske programske opreme izdelamo sami, je dobro vedeti, da tudi prve pogosto temeljijo na arhitekturi PC, zato so v določenih primerih izpostavljene hekerskim napadom z ranljivostmi Spectra in Meltdown ter drugim ranljivostim te arhitekture. Visoko stopnjo varnosti zagotavljajo tudi namenski odprtokodni usmerjevalniki, za katere je na voljo programska oprema s spleta, vendar se odprtokodni projekt zares izplača predvsem računalniškim navdušencem z dovolj računalniškega znanja, izkušenj in predvsem časa.

V splošnem so popolnoma varne le tiste naprave, katerih upravljavski del je strogo ločen od kateregakoli omrežnega dela, kar pomeni, da se nikakor ne sme zgoditi, da bi imel nekdo iz intraneta ali z interneta dostop do nastavitev, ali da bi lahko na kakršenkoli način izvajal posodobitve vgrajene programske opreme oziroma kakorkoli vplival na delovanje usmerjevalnika.

Nekateri zmogljivejši profesionalni usmerjevalniki omogočajo vzpostavitev več navideznih

▽ **Splošne nastavitve požarnega zidu v Windows.**

SKRBNIŠTVO

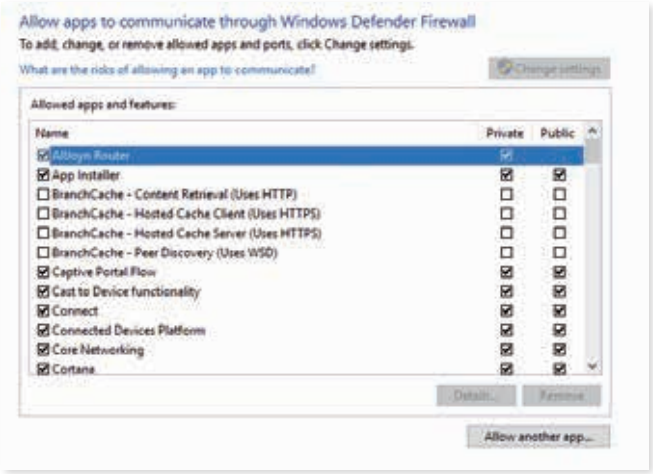
Lahko skrbniške nastavitve **lažejo?**

Večina uporabnikov verjame, da slika nastavitev računalnika ali druge digitalne naprave v skrbniškem oknu vselej kaže dejansko stanje, vendar včasih ni tako. Nemalokrat hekerji ob vdoru v računalnik ali drugo napravo v intranetu zamenjajo določene sistemske programske datoteke, s čimer zagotovijo delovanje določenih storitev kljub drugačni sliki v upravljavskem oknu. Denimo uporaba posameznih vrat ali pošiljanje paketov IP prek protokola TCP/IP ter delovanje protokola UPNP so lahko v nastavitvah prepovedani, vendar so v ozadju vseeno dovoljeni.

Denimo protokol UPNP lahko hekerji uporabijo za obvod, za vohunjenje po naših računalnikih tako, da informacije vgradijo v standardne sporočilne podatkovne pakete, ki jih razpošiljajo prek distribucijskih spletnih naslovov, kot je denimo 239.255.255.255, vsem računalnikom in drugim napravam v intranetnem omrežju. Med skritimi podatki v standardnih sporočilih so lahko celo kodirana pristopna gesla in uporabniška imena.

lokalnih omrežij, ki jim lahko v nastavitvah dodelimo omrežne priključke na ohišju, pri čemer lahko napravo upravljamo le prek upravljavskega navideznega omrežja. Enostavnejši omogočajo upravljanje prek priključka USB.

Po drugi strani (namenski) usmerjevalniki, ki jih vzpostavimo na enem od pecejev v intranetu kot samostojno napravo ali navidezni računalnik, navadno ne zagotavljajo ločitve upravljavskega omrežja in omrežja za prenos podatkov. Tako so upravljavske storitve večinoma dostopne tudi prek intranetnega omrežja, zaščita pred vdorom vanje pa je pogojena z informacijsko varnostjo operacijskega sistema, na katerem temeljijo, oziroma ga poganja gostiteljski strežnik za virtualizacijo.



△ **Nastavitve dostopa aplikacij do domenskega in intranetnega omrežja ter interneta.**

Sistemska programska oprema

Sodobni operacijski sistemi vsebujejo varnostne elemente, med katerimi so najpomembnejši: zaščita jedra operacijskega sistema, digitalno podpisovanje gonilnikov, požarni izd in osnovno varovanje pred zlonamerno programsko opremo. Dodatno zaščito nudijo protivirusni programi in programi za ohranjanje računalnikove kondicije (pravilne strukture sistemskega registra in medpomnilnikov, optimalne nastavitve razpoložljivosti sistemskih storitev, odkrivanje varnostnih lukenj ter odstranjevanje nepotrebnih vtičnikov spletnih brskalnikov).

Napredni uporabniki, vešči skrbništva operacijskih sistemov, znajo sami pravilno vklopiti varnostne elemente operacijskih sistemov, ostali pa se raje zanesejo na programsko opremo za ohranjanje računalnikove kondicije, ki lahko, poleg čiščenja sistemskega registra, sama izklopi nekatere nepotrebne storitve (npr. terminalski dostop) in preveri pravilnost nastavitev požarnega zidu. Vsekakor je dobro, če ustreznost nastavitev ključnih delov operacijskega sistema, predvsem požarnega zidu, občasno preverimo tudi sami.

Aplikacijska programska oprema

Nemalo večjih aplikacij ima vgrajene funkcije za izvajanje samodejnih posodobitev vsakokrat, ko se računalnik poveže z internetom. Po eni strani take posodobitve varujejo računalnik pred hekerskimi vdori, po drugi pa si lahko hekerji s podtikanjem lažnih posodobitev računalnik hitro podredijo. Še posebej na udaru so aplikacije, ki si pri delovanju pomagajo s sistemskimi moduli ali javanskimi stroji, ki lahko ob spletnih napadih hitro »pogoltnejo« zlonamerno programsko kodo iz temnih internetnih podomrežij.

K sreči dostop aplikacij do interneta upravljamo v nastavitvah požarnega zidu operacijskega sistema, v katerih ga izbranim aplikacijam (npr. spletnim brskalnikom) dovolimo, drugim pa ne. Pri odločanju za dovolitev dostopa posamezni aplikaciji morajo imeti ključno vlogo realne potrebe. Marsikatera računalniška igra za svoje delovanje ne potrebuje interneta, vendar proizvajalec izkorišča morebitno internetno povezavo za anonimno zbiranje statističnih podatkov, s katerimi usmerja razvoj novih iger.

Povezavo z internetom pogosto rabimo za obvezno registracijo oziroma aktivacijo, s katero zagotovimo trajno delovanje aplikacij in iger, kasneje pa je ne potrebujejo več. Višjo stopnjo varnosti intraneta zagotovimo tako, da tovrstni programski opremi dostop do interneta s prenastavitvijo požarnega zidu preprečimo takoj, ko ni več potreben. Po drugi strani je dobro preveriti nastavitve požarnega zidu tudi po namestitvi katerekoli aplikacije, pri kateri potrebujemo skrbniško geslo, saj nekateri namestitveni programi brez posebnega razloga aplikacijam omogočijo tudi dostop do interneta.

Spletne storitve

Dostop do domačih računalnikov s spleta je v informacijski dobi več kot mikavna zamisel, saj lahko, na primer, prek spletne kamere tudi med počitnicami preverimo, ali je z našo hišo ali stanovanjem vse v redu. Vendar si ne želimo, da bi živo sliko iz našega bivališča spremljali tudi spletni kriminalci. Žal mnogi na tem področju uporabijo preenostavne rešitve, zaščitene zgolj z geslom in uporabniškim imenom, kar lahko hekerji izkoristijo za vdor v intranet in namestitev svoje zlonamerne programske opreme. V takem primeru med zasluženimi počitnicami ne smemo biti presenečeni nad morebitnim telefonskim klicem našega ponudnika dostopa do interneta in opozorilom na neželene vrste spletnega prometa iz našega modema v temna internetna podomrežja, pri čemer jih ponudnik prosi, da pregledamo in uredijo delovanje svojih računalnikov.

Smo dovolj varni?

Neprestane redne varnostne posodobitve operacijskih sistemov in aplikacijske programske opreme nas venomer opominjajo, da moramo za varnost intraneta nenehno skrbeti tudi sami. Eden od enostavnih ukrepov je, da med dopustom doma ne puščamo prižganih računalnikov z vklopljeno internetno povezavo. Hekerji bodo imeli v času poletnih dvotedenskih počitnic več kot dovolj časa, da si podredijo naše računalnike in jih vključijo v temna internetna podomrežja. Dovolj varni pred njimi smo le, če smo na področju informacijske varnosti vselej vsaj korak pred njimi … ◀

IP

Stalni naslov IP, da ali ne?

Nemalokrat podjetja in organizacije ključnim zaposlenim omogočajo varen dostop do službenega računalnika od doma. Na počitnicah si marsikdaj želimo terminalski dostop tudi do domačega intraneta, ki ga najenostavneje zagotovimo, če nam ponudnik dostopa do interneta določi stalni naslov v javnem omrežju IP, a nas pri tem opozori tudi na povečano nevarnost hekerskih vdorov v domačo računalniško opremo.

S spremenljivim naslovom IP, ki ga ponudnik dostopa do interneta običajno zamenja z vsakim novim dnem, imajo hekerji ob morebitnem naključnem odkritju našega intraneta samo dan časa, da v usmerjevalnik ali katerega od računalnikov namestijo sledilno in vohunsko programsko opremo. Brez nje naslednji dan ne bodo vedeli, na katerem naslovu IP je prehod iz našega intraneta na internet, zato je verjetnost usmerjenega hekerskega napada bistveno manjša, kot če bi imeli stalni naslov.

Nadaljnje branje

Seznam namenskih distribucij Linuxa za vzpostavitev usmerjevalnika na osnovi (starega) PC
en.wikipedia.org/wiki/List_of_router_and_firewall_distributions

Strojni upravljalnik gesel in drugi projekti, ki se jih lahko lotimo sami
sites.google.com/site/pcusbprojects

Izdelajmo odprtokodni usmerjevalnik

Odprtokodni usmerjevalnik s požarnim zidom lahko omogoča kakovostno in poceni zaščito domačih računalnikov pred nevarnostmi z interneta. Kako izbrati strojno osnovo? Katero programsko opremo namestiti in kako jo prilagoditi svojim željam, dopolniti ali popraviti? Je lahko usmerjevalnik tudi omrežna podatkovna shramba ali predvajalnik filmov?

Simon Peter Vavpotič

Razvoj namenske odprtokodne programske opreme za omrežne usmerjevalnike poteka že vsaj tri desetletja. Najprej so razvijalci prisegali na peceje, ki so jih opremili z več omrežnimi karticami, in v operacijskem sistemu vzpostavili ustrezne dodatne funkcionalnosti za usmerjanje paketov IP ter požarni zid. Osnovne funkcionalnosti so bile že vgrajene v operacijske sisteme, za podporo kompleksnejšim pa smo morali s spleta prenesti dodatno sistemsko programsko opremo in jo namestiti, kar velja še danes. Vendar so bili peceji energetsko potratni, sorazmerno dragi in ne preveč varni usmerjevalniki, v njihovih operacijskih sistemih pa so hekerji kmalu odkrili številne varnostne luknje. Hkrati so računalniški trg profesionalne omrežne opreme v tem času preplavile hitrejše, zmogljivejše in učinkovitejše namenske naprave, ki so združevale tako strojno kot programsko opremo.

Ko se je pred dobrimi desetimi leti izkazalo, da tudi te niso več kos hekerjem ali pa ne zmorejo dovolj dobro zaščititi računalnikov v intranetu, je razvoj odprtokodne programske opreme dobil nov zagon. Predvsem velika podjetja, ki so zaradi vdorov hekerjev utrpela največjo škodo, so si zaželela neprebojnih odprtokodnih rešitev, v katerih bi lahko njihovi programerji enostavno preverili obstoj morebitnih odzadnjih vrat ali pa programje sami dopolnili in s tem izboljšali varnost.

Namenska strojna oprema z odprto arhitekturo

Pomen odprtokodne programske opreme so končno zaznali tudi nekateri proizvajalci namenske strojne opreme, ki so bili pripravljeni razkriti podrobno zgradbo in delovanje svojih izdelkov ter se s tem odreči ekskluzivnosti svoje vgrajene programske opreme. Nekateri so v postopnem opuščanju razvoja lastne programske opreme in prehodu na odprtokodne rešitve videli celo prednost. V razvoj odprtokodnih rešitev so se vključili tudi nekateri proizvajalci namenskih mikrokrmilniških čipov za omrežne usmerjevalnike, ki so prej dokumentacijo nudili le pooblaščenim proizvajalcem strojne opreme, danes pa je na voljo vsem uporabnikom interneta.

V pestri ponudbi majhnih usmerjevalnikov različnih proizvajalcev strojne opreme na spletu danes ni malo takih, ki omogočajo zamenjavo vgrajene programske opreme z alternativno odprtokodno. Taka sta, na primer, ASUS RT-N16, naslednik uspešne serije usmerjevalnikov WRT54GL, ki temelji na procesorju 533 MHz z jedri ARM (v usmerjevalniku tečejo samo s 480 MHz) in Broadcomovem usmerjevalniškem čipu BCM53115S, ter Netgate ALIX m1n1wall 2D3 s procesorjem AMD Geode LX800 CPU, pecejevsko arhitekturo in z ukazi x86.

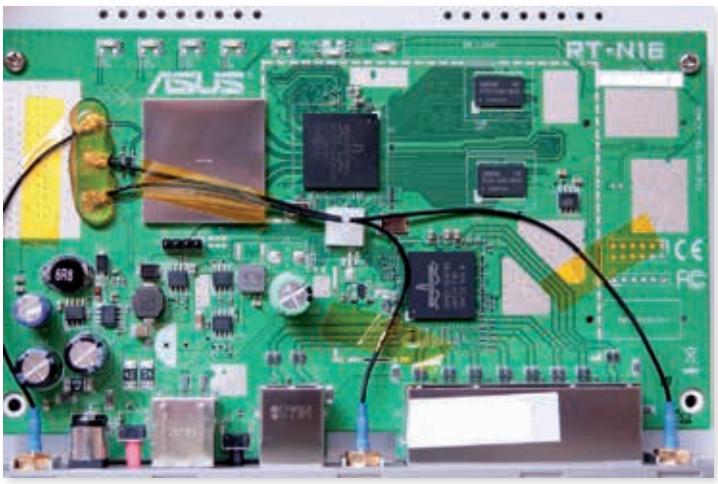
Oba omogočata tudi brezžično povezljivost oziroma usmerjanje v brezžična omrežja. Pri tem ima ASUS RT-N16 celo tri antene, s katerimi omogoča hitrejši brezžični prenos podatkov prek omrežja Wi-Fi in prilagajanje moči signala dejanskim potrebam. Podobno zgradbo ima tudi Netgate ALIX, le da moramo kartico za Wi-Fi za vodilo miniPCI kupiti posebej in jo sami vgraditi. Cena ASUS RT-N16 je v ZDA okoli 85 USD, za Netgate ALIX pa bomo morali odšteti 225 USD oziroma približno toliko kot za nov mini PC brez podatkovnega pogona. Je pa res, da ima Netgate ALIX tri ethernetne priključke.

Mikroračunalniki Banana Pi

Visoka cena in nezaupanje v varnost lastniške vgrajene programske opreme sta k razvoju preprostih odprtokodnih rešitev, namenjenih predvsem domači rabi, spodbudila tudi snovalce mikroračunalnikov, med katerimi je bil dolgo najuspešnejši Raspberry Pi. Vendar so ga na tem področju prehiteli nekateri mikroračunalniki iz družine Banana Pi, ki obsega od z Raspberry Pi Zero primerljivih mikroračunalnikov do takih s štirimi procesorskimi jedri ARM, vgrajenimi stikalno-usmerjevalni čipi in vodili SATA, ki omogočajo priklop diskov in SSD.

▽ Razvojna plošča Banana Pi BPI-R1 z odprto arhitekturo .

▽ Usmerjevalnik ASUS RT-N16.



VARNOST

Je Wi-Fi lahko (ne)varen in kako se ga znebimo?

Glavni usmerjevalnik mora omogočati kakovostno zaščito pred nevarnostmi z interneta. Brezžične povezave so vtem pogledu ahilova peta, saj vemo, da so v komunikacijskih protokolih luknje, ki lahko omogočijo napadalcu vdor v intranet z ne preveč oddaljene lokacije. Obenem pri testiranju različne odprtokodne programske opreme za usmerjevalnike hitro ugotovimo, da pogosto že začetne nastavitve omogočajo enakovredno rabo Wi-Fi in ethernetnega omrežja ter so tako upravljavske storitve na voljo tudi prek brezžičnih povezav.

Če brezžične povezljivosti ne potrebujemo, je morda najbolje, da brezžični modul električno onemogočimo ali odstranimo, kar lahko storimo tudi pri številnih prenosnih računalnikih. Bojazni, da bi odprtokodna programska oprema zaradi tega ne delovala, skoraj ni, saj operacijski sistem za neobstoječo strojno opremo preprosto ne naloži gonilnikov, ostali gonilniki pa delujejo normalno (kar sem tudi sam preveril pri odprtokodnem operacijskem sistemu Bananian, ki je podrazličica OpenWRT).

V Banana Pi BPI-R1 skrbi za komunikacijo prek Wi-Fi poseben modul z mikrokrmilniškim čipom RTL8192CU WLAN, ki je z glavnim mikroprocesorjem AllWinner A20 povezan prek posebnega notranjega priključka USB. Brezžični modul je k sreči na majhni ploščici tiskanega vezja, ki je na glavno tiskanino prispajkana z le dvanajstimi robnimi kontakti. Najlažje jo odstranimo tako, da najprej odspajkamo šest kontaktov na tisti strani, kjer so priključki za anteni. Upoštevati moramo, da je brezžični modul tudi prilepljen, zato si lahko pomagamo tudi z nožkom olfa, ki ga počasi porinemo med komunikacijski modul in glavno tiskanino. Vsekakor moramo nekoliko segreti tudi kontakte na drugi strani, da jih omehčamo. Ko lepilo popusti in lahko komunikacijski modul z ene strani znatno privzdignemo, je potrebno samo še malo gibanja gor in dol, da kontakti popustijo tudi na drugi strani in lahko modul odstranimo. Modul je tako še vedno uporaben za kak drug projekt.

Vseeno opozorimo, da je pravkar opisana »kirurška« operacija primerna samo za izkušene elektrotehnike, pa tudi, da se je lotevate izključno na lastno odgovornost in da s spreminjanjem vezja lahko izgubite jamstvo! Če ne potrebujete Wi-Fi, raje izberite razvojno ploščo, ki ga nima.

Za gradnjo odprtokodnega usmerjevalnika in/ali omrežne shrambe so trenutno najprimernejše štiri razvojne plošče Banana Pi BPI: R1, R2, W2 in R64. Banana Pi BPI-R1 je najstarejša in temelji na sorazmerno počasnem 32-bitnem mikroprocesorju Allwinner A20 z jedroma ARM Cortex A7, ki delujeta pri frekvenci 1 GHz. 1 GB glavnega pomnilnika jedri delita z grafičnim jedrom ARM Mali 400 MP2, ki tiktaka pri 432 MHz. Od petih ethernetnih priključkov (vse naštete plošče Banana Pi omogočajo povezovanje z 10/100/1000 Mb/s) je eden namenjen priklopu na internet, ostali pa intranetu. Povezljivost z omrežji Wi-Fi zagotavlja vgrajeni brezžični modul. Razvojna plošča omogoča tudi neposredno vgradnjo diska 2,5" ali SSD in dobro podpira večpredstavnost, ki poleg priključka za digitalno kamero vključuje še vgrajeni mikrofon, tri priključke USB (2x USB 2.0 in napajalni USB), priključek HDMI za monitor, infrardeči sprejemnik za daljinsko upravljanje in banansko vtičnico za stereo zvok.

Banana Pi BPI-R2 ima precej zmogljivejši 32-bitni procesor MTK MT7623N s štirimi jedri Cortex-A7, ki tiktakajo pri 1.3 GHz, ter 2 GB RAM, ki ga procesorska jedra delijo z grafičnim jedrom ARM Mali 450 MP4. Priključkov za ethernetno povezovanje je prav tako pet, pri čemer je le eden namenjen povezavi z internetom. Vgradimo lahko tudi SSD 1,3" ali disk z vodilom SATA III in krmilnik MT7615 za brezžične povezave Wi-Fi. Večpredstavna podpora obsega priključek HDMI, ki podpira tudi prenos zvoka po protokolu I^2S, infrardeči sprejemnik in tri zunanje priključke USB, od katerih sta dva USB 3.0.

Banana Pi BPI-R64 temelji na 64-bitnem dvojedrnem mikroprocesorju MediaTek MT7622 z jedroma ARM Cortex-A53, ki tiktakata z 1,36 GHz. Ima 1 GB RAM in omrežni krmilnik s štirimi intranetnimi priključki ter posebnim priključkom za priklop na internet. Integriran je tudi krmilnik Wi-Fi, MTK7615, vendar je to strogo namenski mikroračunalnik, namenjen izključno gradnji usmerjevalnikov omrežnih shramb, ki v primerjavi s svojimi predhodniki nima večpredstavnih priključkov in tudi ne priključka za monitor. Zato ga moramo upravljati prek žične ali brezžične povezave. Vseeno lahko vgradimo tudi SSD 1,3" ali disk z vodilom SATA III.

Banana Pi BPI-W2 ima 64-bitni Realtekov mikroprocesor s štirimi jedri ARM Cortex-A53 in je zato po procesorski moči trenutno najzmogljivejši. Vsebuje tudi grafično jedro ARM Mali T820 MP3, ki s procesorskimi jedri deli 2 GB RAM. Ethernetna priključka sta v nasprotju ostalimi ploščami samo dva, zato moramo za priklop več računalnikov kupiti še omrežno stikalo.

△ Usmerjevalnik Netgate ALIX med vgradnjo modula Wi-Fi.

Možnosti za vgradnjo modula Wi-Fi ni. Kljub temu imamo kar dva priključka SATA z napajanjem, v katera lahko pokončno vstavimo diska 2,5" ali SSD. Po drugi strani imamo poleg izhodnega priključka HDMI na voljo še vhodnega. Ob tem je tudi več vhodnih in izhodnih avdio priključkov ter priključka USB 2.0 in USB 3.0.

Vsekakor je zato Banana Pi BPI-W2 primernejši za gradnjo večpredstavnih naprav, denimo predvajalnika filmov, kot gradnjo usmerjevalnika. Na to nas navaja tudi priključek za napajanje ventilatorja, ki lahko v vročih poletni dneh hladi razbeljeno čipovje brez hladilnih reber.

Povejmo še, da potrebujejo omenjene razvojne plošče napajanje 12 V s tokovno zmogljivostjo 2 A ali več, medtem ko za Banana Pi BPI-R1 potrebujemo napajanje 5 V z enako tokovno zmogljivostjo.

Programska oprema

Ker je bil Raspberry Pi prvi ceneni mikroračunalnik, so ga nadobudni programerji hitro usvojili in pripravili različne programske rešitve za posamezne omrežne funkcionalnosti, kot so usmerjevalnik, požarni zid, omrežna vrata, omrežna shramba itn. Zadnje so kasneje prenesli tudi na zmogljivejše Banana Pi s stikalno-usmerjevalnimi čipi in fizično ločitvijo interneta in intranetnih segmentov. Tako ni nevarnosti, da bi kateri od intranetnih računalnikov, ki bi se okužil z zlonamerno programsko opremo, zaobšel usmerjevalnik tako, da bi nekaj podatkovnega prometa mimo vidnih sistemskih nastavitev preusmeril neposredno na internet.

Danes je na internetu veliko namenske odprtokodne vgradne programske opreme. Ločimo jo na vgradno, ki jo prenesemo na ustrezen pomnilniški medij in ga nato preprosto vstavimo v usmerjevalnik, in klasično programsko opremo, ki jo namestimo z zunanjih podatkovnih nosilcev. Med prvo so najpopularnejši OpenWrt, DD-WRT, DebWRT, HyperWRT in Tomato, med drugo pa pfsense, OPNsense in m0n0wall (katerega razvoj je opuščen) za operacijski sistem FreeBSD ter Zeroshell in IPFire za Linux.

Vseeno ne smemo pričakovati, da bomo z vgradnjo programske opreme v hipu rešili vse težave. Največ dela je z nastavitvami in dodajanjem manjkajočih funkcionalnosti, ki jih potrebujemo za zagotavljanje želene stopnje varnosti.

Ne združujte preveč funkcionalnosti!

Čeprav ima večina razvojnih plošč Banana Pi za omrežne usmerjevalnike na voljo sorazmerno veliko večpredstavnih komponent, z združevanjem funkcionalnosti v eni napravi vseeno ne gre pretiravati. Še posebej tvegana bi bila uporaba mikroračunalnika s funkcionalnostmi večpredstavne naprave, igralne konzole, požarnega zidu, usmerjevalnika med intranetom in internetom ter strežnika v omrežju točka-točka (P2P, angl. *peer-to-peer*), saj bi lahko ob morebitnem vdoru vanj heker ob pomoči mikrofona prek interneta celo prisluškoval našim domačim pogovorom.

Fizična ločitev namenskih računalnikov, ki zagotavljajo varen dostop do interneta, in ostalih intranetnih računalnikov je vsekakor potrebna, saj je računalnik, kamor ne nameščamo nove programske opreme ali ne posodabljamo obstoječe vsakih nekaj dni, varnejši pred vdori hekerjev. Obenem v sodobnih operacijskih sistemih tipa Linux pogosto uporabljamo tudi spletne namestitve, ki črpajo manjkajoče programske module iz različnih javnih računalniških oblakov, ki so lahko prav tako tarče hekerjev.

Razvoj programske opreme za Banana Pi

Čeprav Banana Pi še zdaleč ni edina odprtokodna računalniška zasnova, ki omogoča varno usmerjanje podatkov med internetom in intranetom, so možnosti razvoja programske opreme zanjo omejene samo z zmogljivostjo strojne opreme.

Snovalci odprtokodnih usmerjevalnikov so se potrudili, da so na internetu vsem na voljo podrobne informacije o njihovi arhitekturi in delovanju posameznih čipov kakor tudi o že pripravljeni (zastonjski) programski opremi, s katero jih lahko takoj začnemo uporabljati. Čeprav se moramo za nekatere tehnične podrobnosti sprehoditi po spletnih straneh njihovih proizvajalcev, kljub temu najdemo vse. V veliko pomoč pri pregledovanju odprtokodnih arhitektur so nam tudi seznami spletnih strani, ki so jih pripravili snovalci, ter podrobne električne sheme, s katerih lahko razberemo oznake in povezave med ključnimi čipi, ki sestavljajo usmerjevalnik.

Zbrana dokumentacija je dovolj podrobna, da bi se lahko na njeni osnovi izkušen računalniški arhitekt, tehnolog in programer samostojno lotili razvoja lastne odprtokodne programske rešitve za podpro delovanju usmerjevalnika, vendar bi za njeno realizacijo skoraj gotovo potreboval več let. Zaradi kompleksnosti strojne opreme in funkcionalnosti, ki bi jih bilo treba podpreti, bi verjetno za osnovo uporabil katerega od odprtokodnih operacijskih sistemov tipa Linux.

Sestavimo vgrajeno programsko opremo brez programiranja

V že izdelanih slikah sistemskih pogonov, ki jih lahko prekopiramo z interneta in prenesemo na kartico microSD, nimamo možnosti izbire funkcionalnosti, ampak moramo neželene funkcionalnosti ročno odstraniti med delovanjem, manjkajoče

PODATKI

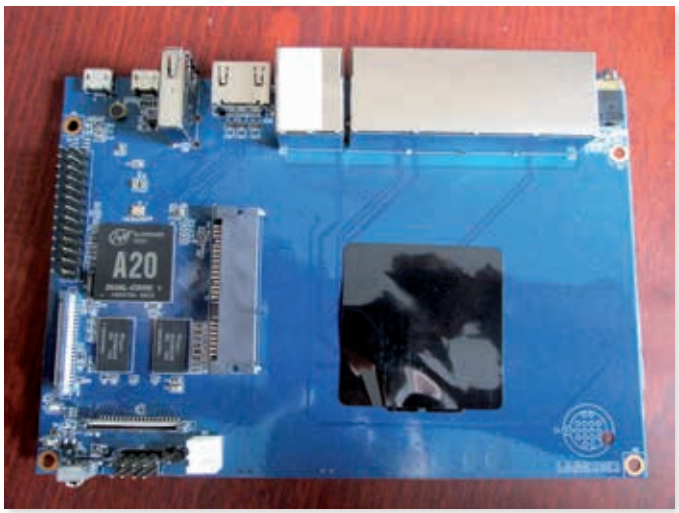
Kaj je **vgradna programska oprema?**

Čeprav odprtokodno programsko opremo za usmerjevalnike ločimo na vgradno in splošnonamensko, za katero moramo predhodno namestiti operacijski sistem, vseeno vgradna programska oprema ni en sam program, kot smo je vajeni pri programiranju mikrokrmilnikov, temveč gre za datoteko, katere vsebino prenesemo na ustrezen pomnilniški medij (pomnilniška kartica microSD, SSD, disk).

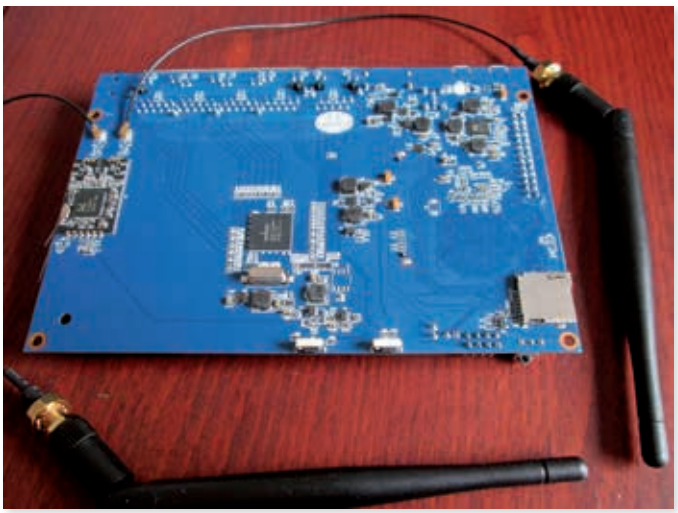
Sestavlja jo predpripravljena podatkovna vsebina sistemskega pogona, na katerem sta nalagalnik operacijskega sistema (navadno na ločeni zagonski particiji) ter operacijski sistem z gonilniki in vso potrebno sistemsko ter aplikacijsko programsko opremo. Zato moramo na internetu poiskati vgradno programsko opremo, ki je natanko prilagojena za naš usmerjevalnik. K sreči je za najbolj popularne strojne osnove, kot je Banana Pi, vseeno veliko izbire vgradne programske opreme.

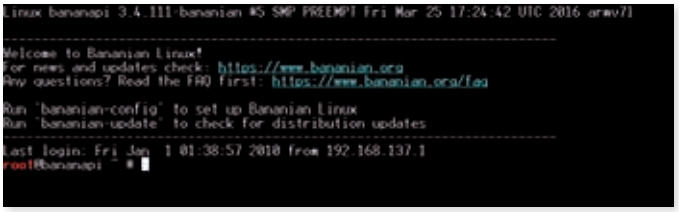
Vendar moramo v nasprotju z osebnim računalnikom, kamor operacijski sistem naložimo s cedeja ali podatkovnega ključka, vgradno programsko opremo najprej ob pomoči osebnega računalnika iz datoteke s sliko sistemskega diska (npr. *.img) prenesti na ustrezen pomniški medij, ki ga nato preprosto vstavimo v napravo. Nato s spleta dodamo manjkajočo programsko opremo in izvedemo nastavitve. S tem je usmerjevalnik pripravljen za uporabo. Po želji lahko omogočimo tudi samodejne posodobitve programske opreme z interneta.

▽ **Mikroprocesor A20 na Banana Pi BPI-R1 in z nalepko prekrit del tiskanega vezja, kamor lahko vgradimo SSD ali disk.**



▽ **Spodnja stran Banana Pi BPI-R1, na kateri je brezžični modul z antenama.**





△ **Bananian s tekstovnim uporabniškim vmesnikom.**

pa dodati. Denimo, za izkušene uporabnike pogosto okensko grafično okolje ne pomeni prednosti, zato na spletu najdemo veliko slik sistemskih pogonov brez njega. Če pa si ga vseeno želimo, ga lahko kasneje prenesemo z interneta in vgradimo.

Snovalci vgrajene programske opreme OpenWRT, ki temelji na Ubuntu 14.04, so namesto tega pripravili postopek za sestavljanje in prevajanje vgrajene programske opreme z možnostjo izbora funkcionalnosti. Za prevajanje programske opreme potrebujemo računalnik z Ubuntu 14.04 (oziroma OpenWRT) ali novejšim, v katerega namestimo razvojno okolje z ukazom:
apt-get install subversion build-essential libncurses5-dev zlib1g-dev gawk git ccache gettext libssl-dev xsltproc unzip subversion file.

Nato z ukazom
git clone github.com/BPI-SINOVOIP/BPI-OpenWRT.git
iz GitHub prenesemo še razvojno okolje za OpenWRT. Iz imenika *BPI-OpenWRT* nazadnje zaporedoma zaženemo ukaza
./scripts/feeds update -a
in
./scripts/feeds install -a,

nakar v grafičnem vmesniku izberemo želene module sistemske programske opreme in ciljno strojno osnovo. Po prevajanju, ki ga zaženemo z ukazom *make*, v imeniku *bin/sunxi* v datoteki tipa **.img* najdemo sliko sistemskega pogona, ki jo lahko prenesemo na kartico microSD. Povejmo še, da lahko ukazu *make* dodamo še opcijo -j4, če potrebujemo kodo za štirijedrni procesor oziroma želimo izkoristiti vsa štiri jedra.

Se izplača?

Odprtokodni usmerjevalniki z odprto strojno arhitekturo omogočajo sestavljanje in gradnjo učinkovite programske opreme, s katero si lahko iz domačega intraneta zagotovimo varen dostop do interneta in internetnih storitev. Vseeno moramo pri tem upoštevati dejstvo, da »vgrajena« programska oprema na kartici microSD še zdaleč ni edina. Za njen zagon mora procesor najprej zagnati poenostavljen BIOS, ki podobno kot pri peceju najprej ugotovi, da je v reži vstavljena kartica microSD z zagonsko in s sistemsko particijo. Nato zažene nalagalnik operacijskega sistema iz zagonske particije itn.

Vendar smo pri vzpostavitvi varnega usmerjevalnika spet pred dilemo, ali lahko zaupamo vgrajenemu BIOS. Vsekakor ni odveč, če se prepričamo o njegovi pristnosti in na spletu preverimo možnosti za njegovo zamenjavo z alternativno programsko opremo ali posodobitev.

Vendar priznam, da do tod v slabem dnevu časa, odkar so mi 16. maja v obtolčeni in nekoliko raztrgani kartonasti pošiljki dostavili Banana Pi BPI-R1, še nisem prišel. No, k sreči je omrežni usmerjevalnik, ki sem ga za okoli 100 evrov naročil v eni od slovenskih spletnih trgovin, »odisejado« prestal brez poškodb. Res pa je, da lahko za krmilnik Wi-Fi, RTL8192CU WLAN z interneta prenesemo datoteko z originalno vgrajeno programsko premo. Le zakaj tega ne bi mogli storiti tudi za procesor Allwinner A20? O tem pa kaj prihodnjič … ◀

VARNOST

Varnost na **prvem mestu**

Čeprav lahko le prebojni test pokaže, kako varno je pred vdori hekerjev naše intranetno omrežje, nam odprtokodne rešitve omogočajo vpogled v ključno sistemsko programsko opremo in tudi njeno prikrajanje po lastnih željah. Pri tem igrajo pomembno vlogo možnosti za zavarovanje pretoka podatkov in omejitev uporabe premalo varnih komunikacijskih protokolov. Zagotoviti moramo predvsem varno upravljanje omrežne naprave, ki mora biti po možnosti v celoti izven dela njenega komunikacijskega sestava, saj to onemogoča hekerjem, da bi na kakršenkoli način prodrli v njen operacijski sistem.

Zadnje bi bilo mogoče le v primeru grobih napak v osnovnih programskih knjižnicah za podporo protokolom IP ali vgrajeni programski opremi usmerjevalniških čipov, ki bi, denimo, zaradi nezaščitenih podatkovnih struktur, v določenih primerih v glavnem pomnilniku, lahko izvedla del predolge podatkovne vsebine kot programsko kodo.

Nadaljnje branje

Domača stan večnamenskih mikroračunalnikov Banana Pi
wiki.banana-pi.org

Seznam projektov razvoja vgrajene programske opreme za omrežne usmerjevalnike
en.wikipedia.org/wiki/List_of_router_firmware_projects

VARNOST V PODJETJIH

- Tudi varnostni strokovnjaki se učijo predvsem s prakso
- Predvidevanje za poslovanje kritičnih ranljivosti
- Kaj morate vedeti o penetracijskih testih?
- Oblak ni kar privzeto varen
- Gospodarstvo vtičnikov API in varnostni izzivi

Tudi varnostni strokovnjaki se učijo **predvsem s prakso**

Ste se kdaj vprašali, kakšna znanja in veščine potrebujejo varnostni strokovnjaki in kje jih lahko pridobijo? Verjemite, celo sami si zastavljajo ista vprašanja. Ogromno pa jih lahko nauči tudi ali predvsem praksa.

Miran Varga

Ne glede na to, ali gre za vojaško omrežje, spletno trgovino ali neprofitno organizacijo, vsem je skupna varnostna komponenta – danes se podjetja ter organizacije vseh vrst in velikosti stalno soočajo z napadi najrazličnejših oblik. Od svojih varnostnih ekip pričakujejo, da jih ustrezno zavarujejo. To pa je zelo zahtevna naloga, saj je groženj v digitalni obliki tako rekoč nešteto, napadalci pa nekje daleč stran – no, vsaj s prsti ne moremo kar takoj pokazati nanje.

Kakšna znanja in veščine torej potrebujejo varnostni strokovnjaki? To, da jim je tehnologija blizu, je samoumevno, zaradi nje so se bržkone sploh začeli ukvarjati s področjem informacijske varnosti. A tisti najboljši niso le tehnični guruji, pohvalijo se lahko tudi s komunikacijskimi in poslovnimi veščinami, predvsem pa praktičnimi izkušnjami. Praksa je v svetu informacijske varnosti zagotovo ena najboljših učiteljic. Varnostni strokovnjaki oziroma njihove službe so najzgovornejši primer delovnega mesta, kjer je prisotno vseživljenjsko učenje. Delujejo namreč v izjemno dinamičnem okolju, ki se malodane stalno spreminja in raste. Žal ne vedno v smer, kot bi jo oni izbrali.

Izbrali smo sedem praktičnih primerov, ki bi jih moral izkusiti oziroma opraviti vsak posameznik, ki želi biti del varnostne ekipe podjetja ali pa se zaposliti v varnostno-operativnem centru.

Doživeti hekerski napad/vdor

Doživetje hekerskega napada ali vdora v podjetje in njegovo preživetje okrepita slehernega varnostnega strokovnjaka. Čeprav gre predvsem za psihično zelo bolečo izkušnjo, ta prispeva k strmejši krivulji učenja. Hekerski vdor namreč varnostnega strokovnjaka nauči, da neprebojne rešitve in sistemi ne obstajajo. Hekerji se namreč lahko lotijo prav vsakega podjetja in organizacije, za tiste, ki skrbijo za varovanje pred hekerji, pa je pomembno, da se znajo pravilno odzvati na napad ali vdor. To pomeni, da morajo čim prej omejiti oziroma omiliti škodo ter poiskati in zakrpati ranljivosti in druge varnostne pomanjkljivosti, ki so privedle do napada/vdora.

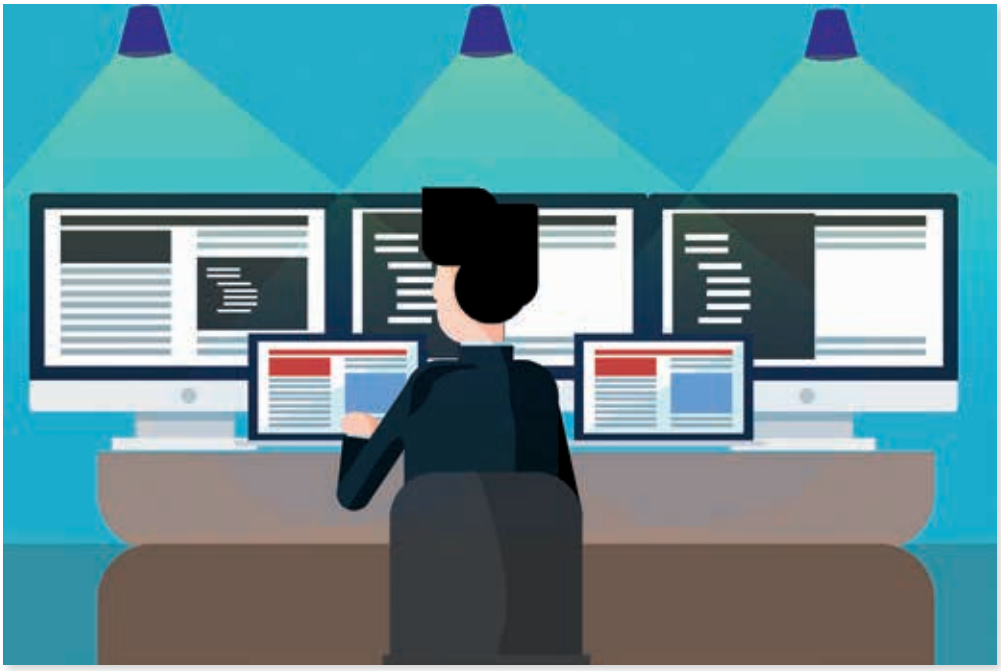
Ustrezno odzivanje na varnostne incidente je namreč v praksi vredno več kot zgolj (naj)novejša oprema. Prav tako pa se bodo varnostni strokovnjaki, ki so se že soočili s kakšnim hekerskim napadom, znali bolje odzvati ob naslednjem napadu. Kot rečeno, hekerski napadi najhitreje opozorijo na varnostne pomanjkljivosti in naučijo ekipo informatike, da ni vsemogočna. Tudi za druge strokovnjake s področja IT (torej tiste, ki so v sekundarni vlogi) je hekerski napad pomembna izkušnja, saj spoznajo, kje so še priložnosti za izboljšave njihovega dela.

Udeležba na varnostnih tekmovanjih

Varnostne ekipe podjetij bi se morale udeleževati tudi varnostnih tekmovanj, organiziranih po vzoru strateških iger, kjer se med seboj pomerijo pri doseganju zastavljenega cilja (angl. *Capture the flag*). Na takšnem tekmovanju se namreč člani ekipe naučijo boljše komunikacije in sodelovanja, saj morajo cilj doseči v omejenem času, proti večinoma neznanim nasprotnikom in njihovim nameram. Tudi ekipe, ki ne končajo med zmagovalci, se zagotovo veliko naučijo in tako lažje odpravijo lastne pomanjkljivosti ali napake oziroma prevzamejo dobre prakse tistih, ki so bili boljši. Pomembno je, da se varnostna znanja širijo in krepijo.

Razvoj IT in varnostnih znanj

Nihče ne pričakuje, da bodo varnostni strokovnjaki obvladali prav vsa IT-področja, vsekakor pa je priporočljivo, da premorejo čim več znanja in izkušenj na naslednjih področjih: omrežja, upravljanje sistemov in operacijski sistemi. Prav tako je pomembno, da imajo vsaj del znanja tudi na področju programiranja in programske kode. Potem pridejo na vrsto varnostna znanja, npr. upravljanje identitete in dostopa, odkrivanje težav in ranljivosti naprav, varnost v oblaku, nadzor omrežja, upravljanje ranljivosti in upravljanje orodij v varnostno-operativnem centru. Varnostnih orodij danes resnično ne manjka, je pa res, da lahko kaj hitro zastarijo, še posebej če so povezana zgolj s posameznimi napravami proizvajalcev. Jasno je, da nihče ne more obvladati vseh orodij, si pa



varnostni strokovnjaki pri svojem delu kljub temu želijo več univerzalnih orodij, pač takih, ki ne bodo vezana zgolj na posamezno opremo.

Ustvarjanje varnostne ekipe

Tako kot v športu je tudi na področju informacijske varnosti nadvse pomembna ekipa strokovnjakov – omenili smo že, da nihče ne ve in zna vsega. Poleg tega mora vodja ekipe poskrbeti tudi za njeno dobro delovanje, da se zaposleni razumejo in dopolnjujejo. Terminologija varnostnih strokovnjakov pozna več ekip: rdečo, modro in vijoličasto. Medtem ko so v rdeči ekipi strokovnjaki, ki odkrivajo vzroke in razloge napada ali vdora in se osredotočajo na napadalce, se modra ekipa osredotoča na obrambo – kako zaustaviti napad, minimirati nastalo škodo in se pravilno odzvati. Strokovnjaki sicer priporočajo, da se ekipe vsaj v fazi izobraževanja in treninga tudi kdaj premešajo ali celo zamenjajo vloge, saj bodo tako bolje razumele delo obeh strani.

Če imamo v varnostni ekipi mešane strokovnjake iz rdeče in modre ekipe, smo ustvarili vijoličasto ekipo. Ta je lahko učinkovitejša od obeh. Npr. če napadalec pridobi višje pravice, mora to modra ekipa takoj ugotoviti, rdeča ekipa pa preuči, kaj je šlo narobe, da se je napadalec prebil tako daleč – in seveda te informacije posreduje modri ekipi. Boljša kot sta komunikacija in sodelovanje, večja je verjetnost, da ima podjetje učinkovito vijoličasto ekipo.

Spremljanje poslovnežev/vodstva

Varnostni strokovnjaki se pogosto posvečajo iskanju injekcij SQL-ukazov v programsko kodo in porazdeljenih napadov z zavrnitvijo storitve. Čeprav so strokovnjaki za tehnologijo in sledijo vsem najnovejšim raziskavam varnostnih groženj, ne razumejo vedno, kaj se v podjetju dogaja okoli njih. Že sicer je priporočljivo, da se varnostni strokovnjaki poučijo o tem, kaj podjetje dela in kako, saj lahko tako bolje predvidijo, kakšne varnostne grožnje in napadi so uperjeni proti njim. Strokovnjaki tudi priporočajo, da bi morali varnostni strokovnjaki pogosteje spremljati aktivnosti vodstva podjetja in se pogovoriti z njim ter ugotoviti, kaj je za podjetje najpomembneje – katere aplikacije in sistemi morajo nujno delovati, če naj podjetje opravlja svoje poslanstvo. Ko to razumejo, lahko izvedejo analizo varnostnega tveganja za poslovanje ključnih podatkov in sistemov.

Razvoj storitvenega pristopa

Obstaja veliko teorij o tem, kako delujejo najboljše varnostne ekipe in kako so sestavljene. Stroka priporoča varnostne ekipe, ki so mešanica profilov različnih veščin in osebnosti. V praksi so se na varnostnem

Ustrezno odzivanje na varnostne incidente je namreč v praksi vredno več kot zgolj (naj)novejša oprema.

področju v povprečju najbolj dokazali kadri, ki so imeli ozadje v vojski ali policiji. Seveda pa ni nujno, da ima varnostni strokovnjak vcepljen »vojaški dril«. V ospredje vedno bolj stopa storitvena miselnost oziroma pristop – varnost je storitev varovanja in tudi varnostni strokovnjaki morajo razumeti, da imajo v podjetjih opravka z ljudmi, ki so na neki način njihove stranke.

Stalno iskanje in odpravljanje pomanjkljivosti v IT-okolju

Informacijska varnost je močna le toliko, kolikor je močan njen najšibkejši člen – prav nanj tudi merijo napadalci. Podjetja se pogosto zavedajo svojih adutov in konkurenčnih prednosti, precej manj podrobno pa raziskujejo šibke točke poslovanja, ki so pravzaprav kritične z vidika informacijske varnosti. Penetracijski testi in redna varnostna preverjanja IT-okolja ter zaposlenih morajo postati praksa, saj je za podjetje ceneje, če sama odkrijejo in odpravijo varnostne pomanjkljivosti, kot pa da pride do napada ali vdora oziroma celo kraje finančnih ali osebnih podatkov in druge intelektualne lastnine. Varnostne ekipe se morajo tako posvetiti predvsem analizi IT-okolja in tudi dela zaposlenih – predvsem pa veliko delati na področju izobraževanja zaposlenih, saj prav vsak zaposleni v podjetju lahko predstavlja bodisi varnostno tveganje ali pa steber obrambe. ◀

Predvidevanje za poslovanje **kritičnih ranljivosti**

Učinkovita kibernetska varnost zahteva več časa in sredstev, kot jih imajo na voljo ekipe za kibernetsko varnost in oddelki IT. Za učinkovito varovanje podjetja velja zato prednostno obravnavati kritične ranljivosti in se izogibati zapravljanju časa za odvečne dejavnosti. Toda kako?

Miran Varga

Prepoznavanje ranljivosti in šibkih točk, ki so najpomembnejše za podjetje ali organizacijo, je težko, posebej v današnjem času, ko si večina javno razkritih ranljivosti prisluži oceno visoka stopnja pomembnosti ali kritična ranljivost. Natančnejše informacije omogočajo boljšo porabo časa, denarja in ljudi. Uporaba prediktivnega določanja prioritet krpanja ranljivosti, kjer gre za postopek določanja prednostnih ranljivosti, ki temelji na verjetnosti, da bodo izkoriščene v kibernetskem napadu, lahko močno izboljša učinkovitost in uspešnost sanacije napada.

Število tehnoloških virov v podjetjih se stalno povečuje, njihovo varovanje pa postaja vse težje. Tudi naraščajoča kompleksnost ustvarja ranljivosti, ki jih je težko prepoznati in odpraviti. Varnostni strokovnjaki pogosto nimajo vpogleda v vse vire podjetja, ki sestavljajo t. i. napadalno površino organizacije. Tudi če bi ga imeli, pa bi bilo odpravljanje vseh ranljivosti z omejenimi finančnimi in človeškimi viri izjemno zahtevno – če ne celo nemogoče.

Številke so zastrašujoče: v letu 2017 je bilo objavljenih 15.038 novih ranljivosti v primerjavi s 9.837 v letu 2016. V enem samem letu smo doživeli 53-odstotno povečanje. Lani je bilo objavljenih 16.500 novih ranljivosti. V povprečju podjetja dnevno najdejo 870 ranljivosti v svojih 960 IT-virih. Skupine za kibernetsko varnost in oddelki IT preprosto nimajo časa ali virov za obravnavanje vseh ranljivosti, zato je potreba po uvajanju prednostnih nalog na področju odkrivanja in krpanja ranljivosti očitna.

Tradicionalno upravljanje ranljivosti je vse manj učinkovito

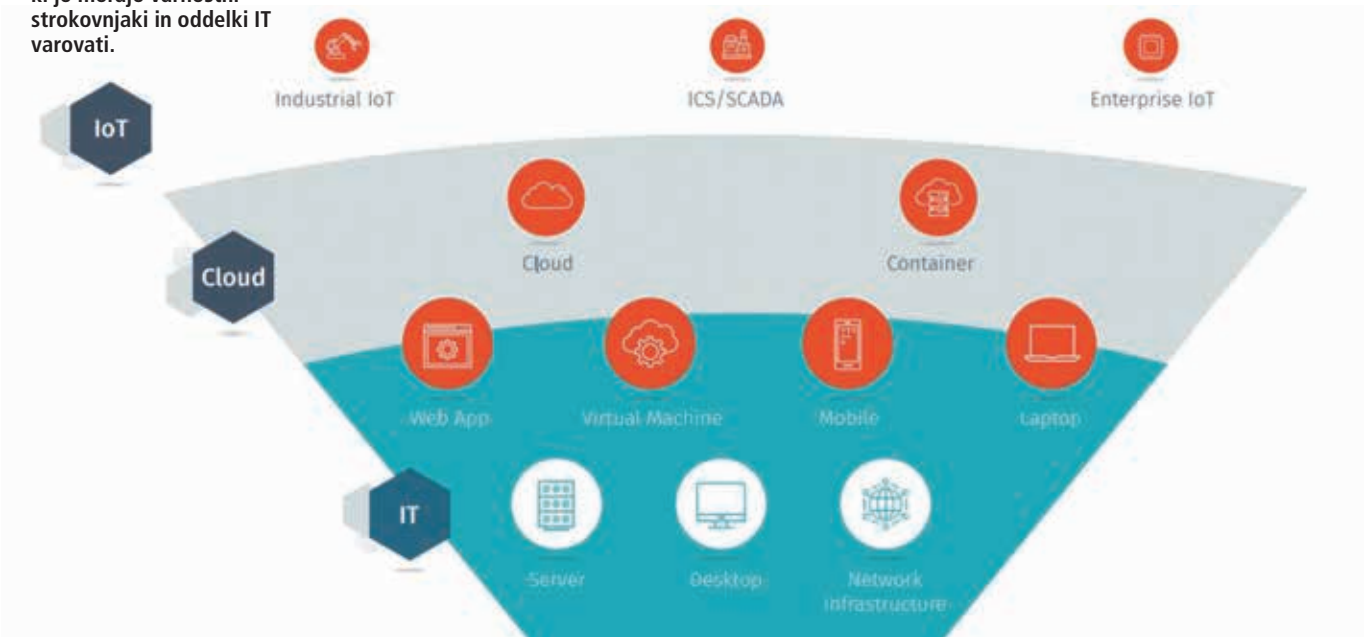
V popolnem svetu bi podjetja odpravila oziroma zakrpala vse ranljivosti, vendar pa število potrebnih popravkov v IT-virih preprosto presega finančna in človeška sredstva, ki jih imajo podjetja na voljo za kibernetsko varnost in IT. Ameriška nacionalna zbirka podatkov o ranljivostih (NVD; nvd.nist.gov) je od leta 1999 objavila že več kot 110.000 ranljivosti. A vseh napadalci niso izkoristili niti jih ne bodo. Pravzaprav ti pri svojem delu uporabljajo le delček odkritih ranljivosti.

Po podatkih NVD je bilo lani odkritih 16.500 novih ranljivosti, napadalci pa so napisali škodljive kode le za sedem odstotkov teh ranljivosti ali jih kako drugače izkoristili. Še manjši je bil delež ranljivosti, ki so omogočile dejanski napad na podjetja. To pa pomeni, da je velika večina odkritih ranljivosti predstavljala zgolj teoretično tveganje. Za večino organizacij se razlika med ranljivostmi, ki jih je mogoče izkoristiti, in tistimi, ki bodo najverjetneje izkoriščene, meri v tisočih, zaradi česar je zelo težko določiti, katere ranljivosti najprej sanirati, če sploh. Dodatna težava podjetij, ki dejansko spremljajo nastanek novih ranljivosti, je tudi v tem, da ocene (CVSS), ki jih ranljivostim prisodijo varnostni analitiki, ko skrbijo za NVD, že v več kot 60 odstotkih primerov pridobijo oznako kritično ali visoka stopnja pomembnosti. Če naj bo odpravljanje ranljivosti učinkovito, mora določanje prednostnih nalog krpanja ranljivosti postati natančnejše.

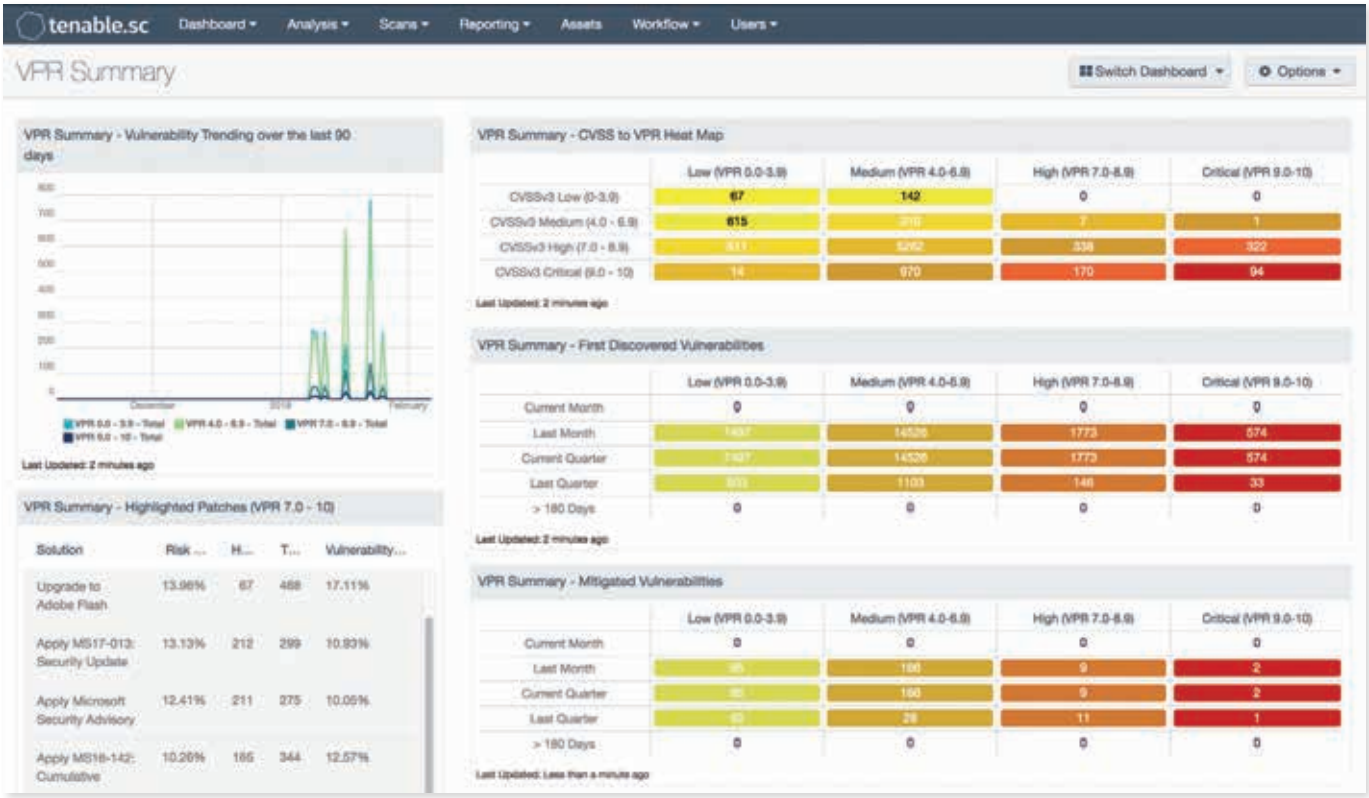
Površina za napade se povečuje

Napadalci imajo vedno večjo površino, ki jo izkoristijo za napad, saj podjetja premorejo vse več naprav in povezav oziroma točk, skozi katere napadalec lahko vstopi v podjetje. Digitalna preobrazba podjetij je poskrbela, da se je napadalna površina iz tradicionalnih IT-virov razširila še na mobilne naprave, računalniške oblake, virtualne zabojnike, internet stvari in industrijske nadzorne sisteme. Preprosto povedano, več naprav v poslovnih okoljih prinaša več ranljivosti.

Podjetja so precej spretna in uspešna pri obravnavanju tradicionalnih ranljivosti, ki vključujejo posodabljanje in krpanje



▽ **Več naprav širi površino za napade oziroma krajino, ki jo morajo varnostni strokovnjaki in oddelki IT varovati.**



△ **Takole je videti upravljavska konzola rešitve Tenable.sc, ki stalno spremlja kritične ranljivosti in jim dodeljuje ocene tveganja za poslovanje podjetja.**

strežnikov, namiznih računalnikov in omrežne opreme. Kar je tudi logično, saj so orodja za ta področja tudi najbolj razširjena in »zrela«. Mobilna varnost še vedno ostaja izziv ob upoštevanju različnosti naprav, operacijskih sistemov, brskalnikov in predvsem mobilnih aplikacij, ki naj bi jih (za)varovali. Poleg kompleksnosti mobilne infrastrukture bodeta v oči še slaba varnostna zasnova aplikacij in splošno pomanjkanje kibernetske higiene pri končnih uporabnikih mobilnih naprav. Sredstva v oblaku, vključno z navideznimi stroji in zabojniki, so pogosto kratkotrajna in jih je težko upravljati. Industrijske naprave in njihovi nadzorni sistemi (SCADA) pa so bili zasnovani še v času pred internetom in niso bili grajeni z mislijo na kibernetsko varnost.

Poleg tega se velja zavedati, da ima posamezen IT-vir oziroma naprava lahko več ranljivosti. V času pisanja tega prispevka je bilo z operacijskim sistemom Windows 10, ki je nameščen na največ računalnikih v današnjih poslovnih okoljih, po podatkih NVD povezanih kar 5.718 ranljivosti!

Nezmožnost podjetij, da bi odpravila vse ranljivosti, ustvarja priložnosti za napadalce. Raziskava inštituta Ponemon je decembra lani ugotovila, da je v zadnjih dveh letih 91 % organizacij doživelo vsaj en kibernetski napad s škodljivimi posledicami, 60 % pa jih je doživelo dva napada ali več.

Uvedba predvidevanja prednostnih nalog na področju krpanja ranljivosti

Vsako podjetje bi rado vedelo, kje naj začne krpanje ranljivosti. Isto vprašanje so si postavili tudi pri varnostnem ponudniku Tenable in razvili postopek prediktivnega napovedovanja ranljivosti, ki zahtevajo prednostno obravnavo za posamezno podjetje oziroma njegovo digitalno krajino. Proces izkorišča tehnologijo strojnega učenja in razvršča ranljivosti glede na verjetnosti, da jih bodo napadalci izkoristili v napadu na podjetje.

Postopek, poimenovan *Predictive Prioritization*, združuje več kot 150 podatkovnih virov o ranljivostih iz vsega sveta. Algoritem analizira vsako ranljivost v zbirki NVD in ji dodeli oceno verjetnosti uporabe v napadu na podjetje. Izid je nadvse uporaben: varnostni strokovnjaki in informatiki lahko svoj čas in znanja osredotočijo le na 3 odstotke ranljivosti, ki so dobile oceno, da bodo zelo verjetno izkoriščene v namene napada na podjetje. Praksa kaže, da omenjeni postopek loči med resničnimi in teoretičnimi tveganji, zato lahko podjetja zmanjšajo število ranljivosti, ki jih morajo nujno zakrpati za kar 97 %. Seveda je priporočljivo, da, četudi oboroženi s tem znanjem, podjetja zakrpajo kar največ ranljivosti, začenši s tistimi, ki so za njihovo poslovanje najbolj kritične.

Lani je bilo odkritih 16.500 novih ranljivosti, vendar pa so napadalci napisali škodljive kode le za sedem odstotkov teh ranljivosti ali jih kako drugače izkoristili.

Kako deluje predvidevanje prednostnih nalog krpanja ranljivosti? Postopek prediktivnega določanja prioritet krpanja ranljivosti omogoča podjetjem, da se osredotočijo na ranljivosti, ki bodo najverjetneje izkoriščene in bodo imele velik vpliv na poslovanje. Omenjeni algoritem vsakemu podatkovnemu viru ranljivosti dodeli neko verjetnost, pri čemer analizira značilnosti ranljivosti v sedmih kategorijah, kot so: vzorec pretekle nevarnosti, prejšnji vir grožnje, meritve ranljivosti, metapodatki o ranljivosti, pretekli napadi, prizadeta podjetja in razpoložljivost škodljivih kod. Rezultat analize je prednostna ocena ranljivosti (VPR – *vulnerability priority rating*), ki je je deležna vsaka objavljena ranljivost. Ocena se giblje na intervalu med 1 in 10, pri čemer 10 predstavlja za podjetje najbolj varnostno kritično ranljivost. Poleg tega se ocene več kot 111.000 znanih ranljivosti osvežijo vsakih 24 ur, saj krajina digitalnih groženj in napadalcev seveda ne miruje. ◀

Kaj morate vedeti o **penetracijskih testih?**

Penetracijski testi so sestavni del celovitega načrta zagotavljanja kibernetske varnosti. Bistvenega pomena je, da obrambne sisteme preizkusijo pravi profesionalci, saj je le tako moč najti in odpraviti različne ranljivosti in slabosti.

Vinko Seliškar

Penetracijski test je postopek, s katerim tretja oseba oziroma organizacija preveri zmožnost varnostnih zaščit podjetja. Gre za naložbo v kibernetsko in informacijsko varnost. A tudi penetracijski testi med seboj niso enaki, zato velja vedeti, kaj si podjetja sploh želijo, preveriti, kakšnega izvajalca najemajo, kako o testu komunicirajo v podjetju in kaj bodo z rezultati. Pojdimo lepo po vrsti.

Odločitev o cilju ali ciljih

Ko se podjetje odloči, da bo najelo zunanje strokovnjake za preizkus svojih varnostnih mehanizmov in rešitev, se težko upre skušnjavi in naroči preizkus »vsega«. Napaka. Penetracijski testi so ciljne vaje. Cilj je seveda lahko velik: preizkus IT-okolja ali omrežja. Podjetje se mora iskreno izprašati, zakaj naroča penetracijski test. Nekatera ga morajo opraviti zato, da zadostijo zahtevam regulatorjev in/ali zakonodaje, spet druga zato, da bi ugotovila, kaj je šlo narobe ob zadnjem vdoru v podjetje. Seveda se bodo ti penetracijski testi močno razlikovali, predvsem pa postregli z drugačnimi podatki in zaključki. Podjetje mora zato izvajalcu penetracijskega testa jasno izraziti namen preizkusa, s katerim se morata nato obe strani strinjati (in ga pisno potrditi).

Preverjanje referenc

Upoštevaje, da bo skupina ljudi pri izvajalcu poskušala prebiti obrambo podjetja, mora podjetje seveda vedeti, da gre za etično skupino ljudi. Tega pa ne more izvedeti iz brošure ali grafično lepo urejene spletne strani. To lahko izve le od pogovorov z drugimi podjetji, ki so tak preizkus že naročila in izkusila. Priklic podjetij, ki jih navaja ponudnik kot reference, in preverjanje izkušenj naj bo na vrstnem redu še pred podpisom pogodbe o izvedbi penetracijskega testa. Stranke vprašajte, kako zadovoljne so bile z delom ponudnika (posebej če je penetracijski test vseboval preizkus s socialnim inženiringom), kako je ta poznal njihovo okolje in kako je pripomogel k izboljšanju varnosti.

△ **Sestavni deli penetracijskega testa.**

Zavarovanje odgovornosti

Ob gradnji objekta se uporabljajo le materiali (beton, jeklo, aluminij in podobni), ki so prestali določene preizkuse. Pri penetracijskem testu pa je drugače, saj lahko povzroči kritično okvaro produkcijskega sistema. Prav zato mora naročnik poskrbeti za ustrezno zavarovanje odgovornosti za kritje nenačrtovanih posledic preizkusa varnostnih rešitev. Te lahko pridobi pri zavarovalnici (nekatere že nudijo zavarovanja s področja kibernetskih napadov) ali pri izvajalcu. V obeh primerih naj bodo podrobnosti preizkusa predstavljene zavarovalnici oziroma pisno potrjene z obeh strani. Žal večina podjetij na tovrstno zavarovanje niti ne pomisli, dokler ga ne potrebuje.

Podrobnosti preizkusa

Ko bodo vsi testni parametri dogovorjeni, mora podjetje z izvajalcem doreči še, kako bo penetracijski test izvedla v praksi. Informatiki in varnostni inženirji, ki branijo omrežje in sisteme podjetja, verjetno o njem ne bodo niti obveščeni, toda vodstvo podjetja bi moralo imeti zelo jasno in natančno predstavo o tem, kaj se bo zgodilo.

Spremljanje preizkusa

Vodstvo pogosto prejme le končno poročilo o rezultatih penetracijskega testa. Povsem drugače pa je, če lahko testni napad (in odziv) spremlja v realnem času in nato zaposlenim ob analizi postreže s komentarji. Nekateri izvajalci naročniku omogočijo, da sproti spremlja izvajanje penetracijskega testa. Sicer pa velja vztrajati pri tem, da se spremlja in beleži vse, kar se zgodi med njim.

Izdelava načrta nadgradnje obrambe

Nekatera podjetja zgolj shranijo ugotovitve ob zaključku penetracijskega testa oziroma jih pošljejo revizorjem, toda rezultate velja uporabiti za nadgradnjo varnostnih in obrambnih mehanizmov. Na vseh napravah in pri vseh zaposlenih v podjetju. Ugotovitve preizkusa je modro ustrezno predstaviti prav vsakemu zaposlenemu in preveriti, kaj se da na njegovem delovnem mestu izboljšati v prid večji kibernetski varnosti. Seveda varnostni strokovnjaki in IT-osebje dobijo bolj podrobno tolmačenje rezultatov, posamezne skupine zaposlenih pa priporočila, kako bolje opravljati delo v prid večji varnosti.

Vodstvo podjetja pričakuje poročilo o penetracijskem testu v poslovnem jeziku. Želi vedeti, kako sta se odrezala varnostno osebje in oprema ter kaj bi veljalo v prihodnje storiti za izboljšanje stanja varnosti v podjetju (in koliko bo to podjetje stalo). Penetracijski test je vendarle nujna naložba v varnost poslovanja. ◀

Oblak ni kar **privzeto varen**

Analitsko podjetje Gartner napoveduje, da bodo leta 2022 za kar 95 odstotkov varnostnih težav v oblačnih okoljih krive stranke oziroma odjemalci. Zakaj? Ker ima model deljene odgovornosti tudi slepe točke.

Vinko Seliškar

Varna uporaba oblačnega okolja od podjetij zahteva oblikovanje strategije za varnost v oblaku, ki bo v popolnosti razumela in upoštevala model deljene odgovornosti – torej kateri deli varovanja so v domeni ponudnika in kateri v domeni stranke. Oglejmo si, katere varnostne pomanjkljivosti bi veljalo urediti v primeru rabe oblačnih storitev velikana Amazon Web Services (v nadaljevanju AWS), seveda pa tovrstne ukrepe lahko kar podaljšamo tudi do vseh drugih ponudnikov infrastrukture, platform in programske opreme v oblaku.

Zaščita zabojnikov

Eno največjih vprašanj pri uporabi AWS je varovanje kontejnerskega omrežja. To je posledica pomanjkanja konteksta, saj Amazonov virtualni zasebni oblak (VPC) uporablja interno omrežje. Amazonove varnostne skupine lahko uporabijo varnostne politike za vsak grozd, vendar tega ne morejo storiti s posameznimi stroki, zaradi česar je ta tehnologija nezadostna. Ko podjetje poskuša odpraviti težave ali doseči boljši vpogled v komunikacijo, se bo ta ustavil na prometu med gostitelji v gruči in ne na strokih, ki povzročajo t. i. varnostne slepe točke.

Podjetje, ki najema oblačne infrastrukturne storitve AWS, zato potrebuje dve rešitvi za nadzor omrežja v oblaku. Ena obravnava varnostne pravilnike virtualnih strojev, druga pa skrbi za nadzor zabojnikov. Ustvarjanje omrežnih pravil za eno samo aplikacijo, ki vključuje zabojnike in virtualne sisteme, zahteva uporabo ločenih rešitev. Podjetje tako uporablja dva nadzorna sistema – enega za vzdrževanje in drugega za upravljanje. Takšna praksa dodaja kompleksnost in veča tveganje, kar verjetno ni v skladu z željo podjetij po tem, da jim premik v oblak poenostavi upravljanje infrastrukture in poveča varnost.

Slab(š)a preglednost

Kar 62 % vodij informatike v velikih podjetjih (v ZDA) je prepričanih, da je za informacijsko varnost bolje poskrbljeno na lokaciji podjetja kot pri ponudniku oblačnih storitev. Menijo namreč, da imajo njihovi varnostni strokovnjaki boljši nadzor nad svojim IT-okoljem, podatki in komunikacijami, s premikom v oblak pa izgubijo tako na področju nadzora kot preglednosti.

V primeru pametne mikrosegmentacije seveda ni nujno tako. Na trgu obstajajo rešitve, ki podjetjem omogočajo boljši varnostni vpogled v delovanje njihovega oblačnega okolja, kot jim ga zagotavlja AWS. Rešitev Guardicore Centra, denimo, samodejno odkriva vse aplikacije in sega do procesne ravni (t. i. *Layer 7*), podobno pa delujejo tudi druge rešitve, ki prek vtičnika AWS API črpajo podatke za orkestracijo in podatke, iz katerih pridobijo kontekst za preslikavo aplikacij. Tako te varnostne rešitve ves čas spremljajo, kako se aplikacije obnašajo in komunicirajo z njimi, kar varnostnim strokovnjakom omogoča hitro odkrivanje anomalij in opozarjanje na spremembe. Seveda neodvisne programske rešitve to počno v različnih oblačnih okoljih.

Varnostna politika za aplikacije in stalni nadzor

Podjetja so se že navadila na rabo požarnih zidov nove generacije, katerih napredne funkcije uporabljajo tudi za zaščito in segmentiranje aplikacij. Oblačno okolje AWS (in še marsikatero drugo) pa ne zagotavlja enake funkcionalnosti. Segmentiranje aplikacij se lahko v omejenem obsegu izvede z uporabo varnostnih skupin AWS, pri čemer so podprti le nadzor prometa (do ravni 4), vrat in IP-naslovov. Podjetja se morajo tako spet obrniti na dodatne varnostne aplikacije, ki jim zagotovijo varovanje komunikacij in podatkov vse do procesne ravni.

Iskanje in upravljanje slepih točk

Za varno rabo oblačnih storitev AWS mora podjetje razumeti, da je za varovanje svojih podatkov pa tudi platforme, aplikacij, upravljanje identitete in dostopa ter vseh konfiguracij operacijskega sistema, omrežja in/ali požarnega zidu odgovorno samo. Amazon podobno kot drugi ponudniki oblačnih storitev v bistvu varuje le svojo infrastrukturo.

Kaj storiti? Odgovor ponuja mikrosegmentacija omrežja in aplikacij – če je pravilno izvedena, ponuja preprost način zagotavljanja varnosti hibridnega okolja, vključno z reševanjem edinstvenih izzivov zabojnikov v AWS. Z mikrosegmentacijo podjetje pridobi tudi možnost ustvarjanja dinamičnih aplikacijskih varnostnih politik na ravni procesov. Seveda mora poskrbeti tudi za implementacijo neodvisnih varnostnih rešitev, ki znajo samodejno odkrivati aktivnosti v omrežnih tokovih in povezavah, prepoznati slepe točke in jih zavarovati.

Varnost v oblačnih okoljih (tudi največjih) ponudnikov torej ni samoumevna. Le kdor se tega zaveda, lahko poskrbi za ustrezno zaščito svojega poslovanja v oblaku. ◀

Gospodarstvo vtičnikov API in varnostni izzivi

Programabilni vtičniki API so informatikom in razvijalcem omogočili, da medsebojno povežejo najrazličnejše sisteme, aplikacije, storitve in vsebine, toda zagotavljanje varnosti hiperpovezanih okolij in vsebin je seveda velik izziv.

Miran Varga

Pomen vtičnikov API v gospodarstvu narašča iz leta v leto. Tudi v Sloveniji se podjetja vse bolj zavedajo priložnosti in pomena novih vrednostnih verig ter novih poslovnih modelov, ki jih ti omogočajo. Vedno več je primerov poslovnih modelov in procesov, v katerih lahko podjetja sodelujejo le, če imajo uspešno izpostavljene API in če imajo vzpostavljene kompetence, kako uporabljati API podjetij, s katerimi sodelujejo.

Oglejmo si nekaj primerov. Prodaja vstopnic za različne dogodke temelji na uporabi API različnih ponudnikov, različne rešitve, od spletnih do mobilnih aplikacij, pa uporabljajo vtičnike različnih ponudnikov. Uporaba vtičnikov API narašča na področju zavarovalništva, kjer se določene oblike zavarovanja, npr. nezgodno ali turistično, že tržijo prek njih. V tem primeru lahko spletna trgovina, ki prodaja gorska kolesa ali aktivne počitnice, stranki ponudi tudi zavarovanje, ki ga stranka kupi kar kot del enotnega procesa nakupa v trgovini, samo zavarovanje pa se izvede v ozadju s klicem ustreznih API.

Najbolj bomo občutili reformo v svetu plačil

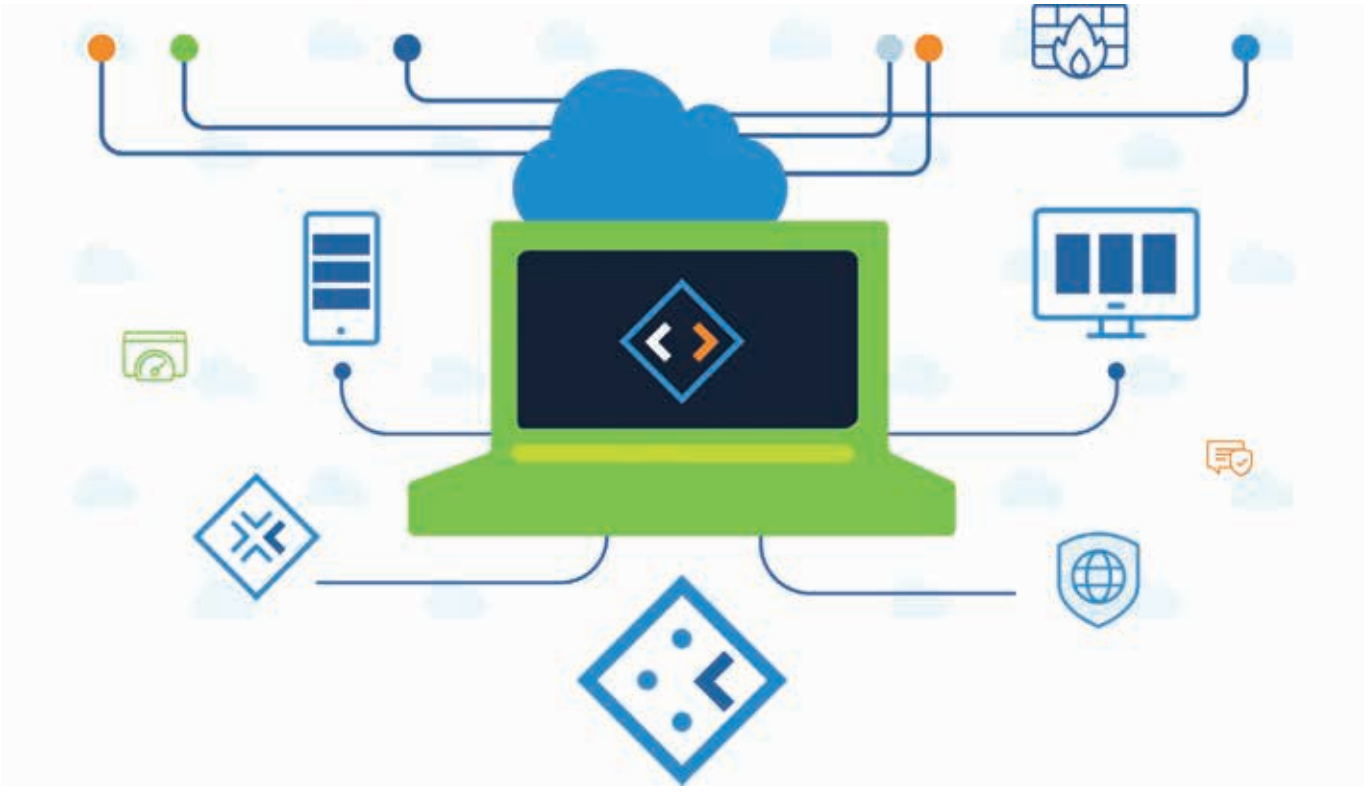
Za vtičnike API pomembno področje je tudi bančništvo, saj direktiva PSD2 nalaga bankam, da odprejo svoje sisteme preko API in omogočijo dostop tretjim osebam. Kaj to pomeni v praksi? Predvsem dvoje: ker bo mogoče prek vtičnikov dostopati do podatkov o računih strank v posameznih bankah, se pospešeno razvijajo rešitve za boljše ali bolj prilagojene uporabniške izkušnje, ki bodo, na primer, uporabnikom omogočile upravljanje računov več bank na enem mestu in še marsikaj drugega. Druga, še pomembnejša novost pa je, da za digitalno (spletno, mobilno) plačevanje ne bodo več potrebne plačilne kartice, PayPal in podobni sistemi, saj bodo lahko spletne trgovine plačilo izvedle neposredno pri banki prek uporabe ustreznih API. Takih primerov je še veliko, vse pa povezuje neizpodbitno dejstvo, da vtičniki API postajajo pomemben poslovni instrument.

Poslovni API

Eden od problemov razvoja vtičnikov API predstavlja dejstvo, da je celo stroka kratico API (angl. *Application Programming Interface*) do nedavnega razumela kot popolnoma tehnični koncept, povezan s programiranjem. Razvijalci in programerji uporabljajo API že desetletja kot način za komunikacijo med različnimi deli in ravnmi aplikacij, operacijskih sistemov ter nivoji »nekega računalniškega sistema«.

Poslovni API na drugi strani pa prek tehnoloških vmesnikov izpostavljajo poslovne operacije, katerih namen je omogočati in podpirati določene modele poslovanja, zato je za podjetja zelo pomembno, da se začno zavedati, da so API postali poslovni člen, pri načrtovanju katerega morajo sodelovati.

»Ko podjetja gradijo svoje API-vmesnike, so ti navadno strukturirani v nekaj nivojev. Najvišji nivo API, torej tiste, ki so namenjeni poslovnemu povezovanju s partnerji, imenujemo izkustveni API. Njihov namen je, da na učinkovit, nezapleten in poslovno smiseln način izpostavljajo operacije in podatke tako, da bo integracija ostalih deležnikov, na primer mobilnih in spletnih rešitev, partnerskih sistemov, tržnic in podobno, čim bolj učinkovita,



hitra in preprosta,« je pojasnil prof. dr. Matjaž B. Jurič, ki se že desetletja ukvarja z vtičniki API.

Marsikdo se niti ne zaveda, kako zahtevno (beri: kompleksno) je zgraditi ustrezen nabor izkustvenih API ter ob tem vzpostaviti celoten življenjski cikel, ki obsega razvoj, posodobitve, spremljanje, celostno skrb za uporabnike API in vse ostale vidike. To je eden glavnih odgovorov, zakaj podjetjem ponavadi v prvem poskusu ne uspe zgraditi ustreznih API-jev ali pa njihov razvoj traja predolgo. Najslabša možnost je, da podjetje ponudi slabe API in se tega niti ne zaveda. Tako podjetje bo živelo v iluziji, da je za razvoj »API-ekonomije« naredilo dovolj ter se morda prepričevalo, da se preko vtičnikov API pač ne da ustvarjati prometa, karavana pa ga bo prehitela po levi in desni.

»Tedensko smo priče primerom, ko podjetja ponujajo tako slabe API, da se jih enostavno ne da vključiti v vrednostne verige. Npr. ponudniki plačilnih storitev ali e-denarnic, ki jih podjetja želijo vključiti v svoje spletne ali mobilne trgovine, ne ponujajo dvostopenjskega mehanizma izvedbe plačila (rezervacija in izvedba). Taki API so za resno poslovanje tako rekoč neuporabni. Niso pa to edini primeri,« razlaga prof. Jurič.

(Ne)varnost vtičnikov API

Glede na poslovni pomen API je na mestu vprašanje, kako jih ustrezno zavarovati. Posebej takrat, ko so uporabljeni kot temelj za poslovne transakcije, je varnosti treba posvetiti veliko pozornosti. Najprej se velja zavedati varnostnih tveganj pri razvoju in uporabi API.

Rok Povše, direktor projektov v podjetju Sunesis, ki se ukvarja z razvojem poslovnih API in mikrostoritev, je pojasnil: »Pri razvoju poslovnih API je z varnostnega vidika ključno dvoje. Ustrezne varnostne mehanizme je treba načrtovati in vgraditi že med razvojem. Poleg tega je treba poskrbeti za operativne vidike varnosti, kar vključuje spremljanje izvajanja API, zaznavanje nepooblaščenih pristopov, identifikacijo napadov DDoS in vse ostalo, kar je s tem povezano. Katere varnostne mehanizme uporabiti, pa je odvisno tudi od tehnologije API, ki je lahko REST, Kafka, gRPC, uporaba reaktivnih programskih modelov itn.«

Izpostavljanje občutljivih podatkov

Med največje varnostne težave API vsekakor sodi izpostavljanje občutljivih podatkov tretjim osebam, ki lahko prek klic API do teh podatkov dostopajo, ne da bi bili za to pooblaščene. V zadnjem obdobju smo bili priče številnim primerom tovrstnih zlorab. Facebook je prek svojih API nehote izpostavljal številne podatke o uporabnikih, enako se je (z)godilo Googlu s storitvijo Google+. Nedavno je ameriški zavarovalnici First American Financial Corp. na internet ušlo vsaj 885 milijonov osebnih podatkov. Podobno usodo so doživele nekatere slovenske spletne trgovine.

Nepopolna avtentikacija

Druga pogosta varnostna težava vtičnikov API je nepopolna ali nedelujoča avtentikacija, ki zlonamernemu uporabniku omogoči, da dostopa do operacij vtičnika in tako do podatkov, čeprav napadalec za to ni pooblaščen. »Sodobni API danes za avtentikacijo pogosto uporabljajo rešitvi OAuth2 in OpenID Connect, a bi morali razvijalci aplikacij dovolj pozornosti posvetiti pravilni uporabi žetonov, njihovi veljavnosti, postopkom in protokolom avtentikacije, ustreznemu načrtovanju celotnih postopkov, sami implementaciji in izbiri avtentikacijskih strežnikov, ki morajo biti tudi pravilno konfigurirani«, je pogoste vzroke za napake izpostavil Povše.

Napadi DDoS

API so pogosto tarče napadov s prekinitvijo delovanja storitve (DoS ali DDoS), podobno kot spletne strani. Razlika je le v tem, da je preobremenitev vtičnika API pogosto veliko bolj preprosto doseči pa še posledice so lahko hujše. Napadeni API se namreč neha delovati, to pa pomeni neposredno poslovno škodo. Preprečevanje napadov DDoS na API je kompleksno in zahteva več sklopov ukrepov. Prvi se nanaša na samo zasnovo vtičnikov, kjer velja upoštevati nekaj osnovnih pravil.

Preprečevanje napadov DDoS na API je kompleksno in zahteva več sklopov ukrepov.

»API nikoli ne zvežemo neposredno na zaledni sistem, ampak vedno postavimo vmesni nivo, ki odklopi API od zalednega sistema. Lahko si pomagamo tudi z nivojem predpomnenja. S tem preprečimo, da bi DDoS-napad na API zrušil tudi zaledni sistem – predstavljajte si, da se to zgodi kaki banki ali zavarovalnici. Drugi pomemben vidik pa je ta, da nikoli ne omogočimo neposrednega dostopa do API, ampak to storimo preko API-prehoda, pri čemer izberemo taka vrata, ki znajo zaznavati vzorce klicev oziroma DDoS-napade in ustrezno omejiti dostop. API velja namestiti na elastično platformo in infrastrukturo tipa Kubernetes. S tem omogočimo, da API preživi prvi del napada, dokler vrata ne zaznajo preobremenitve in zato omejijo dostop. Zadnji sklop ukrepov pa je učinkovit nadzor oziroma spremljaje delovanja vtičnikov,« je strnil svoja priporočila prof. Jurič.

Človek v sredini

Napad tipa »*man in the middle*« je že vrsto let znana varnostna nevšečnost, zato je treba tudi API ustrezno zavarovati pred tovrstnimi napadi, pri katerih bi napadalec lahko prestrezal zahteve in serviral lažne odgovore/podatke. Na srečo je pri tem učinkovita že uporaba šifrirnih protokolov TLS/SSL, zato danes velja, da mora vsa komunikacija z API, tudi taka, ki se nam zdi, da ni varnostno občutljiva, obvezno potekati prek zaščitenih povezav.

Vrivanja in napačni parametri

Med varnostnimi tveganji v svetu vtičnikov API velja omeniti še t. i. vrivanja podatkov in uporabo napačnih parametrov, katerih namen je pridobitev nepooblaščenega dostopa. »Oba pristopa sta razvijalcem dobro znana in proti njim se borimo s striktnim preverjanjem parametrov, URL-naslovov in vseh ostalih vrednosti, npr. piškotkov, poizvedb itd. Poleg tega moramo poskrbeti, da bo programska koda, ki iz API omogoča dostop do zalednih sistemov, podatkovnih zbirk in drugih virov, napisana tako, da ji vrivanja in napačni parametri ne bodo prišli do živega,« je še pojasnil Povše.

Z API ni šale

Pod črto so principi zagotavljanja varnosti in zaščite vtičnikov API kompleksni, vendar dobro definirani. Z njihovo varnostjo se morajo podjetja oziroma razvijalci ukvarjati že pri načrtovanju in razvoju ter jo udejanjati skozi celoten življenjski cikel in delovanje posameznega API. Le tako lahko zagotovijo njihovo nemoteno, varno in učinkovito delovanje. Glede na njihov pomen in vlogo v gospodarstvu to zagotovo zaslužijo. ◀

Je res smiselno odklepati drago kupljene naprave in se igrati z garancijskim jamstvom le teh?

Vsekakor, za svoj denar hočem dobiti vse!

Pred davnimi časi je ob nakupu nekega izdelka veljalo, da višja cena pomeni superioren model. Danes ni več tako. Proizvajalci so spoznali, da se veliko bolj izplača proizvajati enake izdelke ter jim naknadno omejiti zmožnosti. Lep primer tovrstne prakse so avtomobilski in drugi motorji, ki imajo del vgrajenih karakteristik zaklenjenih. Čeprav kupimo šibkejši avto, ga lahko s programskim odklepom nadgradimo v močnejšega. Nadgradnja vozila je navidezna, precej bolj fizični pa sta hitrost in moč, ki ju po njej ponudi sicer cenejši jekleni konjiček.

Podobno velja za pametne telefone. Korenski dostop in druge vrste odklepanja omogočijo nalaganje aplikacij, ki jih naprava privzeto ne podpira. Telefonu po želji zamenjamo celo operacijski sistem ali odstranimo neželene programe, ki jih je v podobi preoblečenega Androida na napravo »zapekel« proizvajalec. Navedene in sorodne aktivnosti v zvezi z odklepanjem telefona imajo le en namen, tj. do konca izkoristiti strojni potencial izbranega pametnjakoviča. S posebnimi programi napravi navijemo procesor, sprostimo delovni pomnilnik ali počistimo lokalno shrambo. Sleherni odklenjeni telefon ima možnost hitrejšega delovanja kot sicer, hkrati pa se izognemo načrtnemu upočasnjevanju naprave, ki ga proizvajalec vrši z uradnimi posodobitvami sistema.

Igralne konzole se običajno odklepajo zaradi igranja piratskih iger. To je opravičljivo le v primeru, ko si igro v resnici tudi lastimo. Primer je igralna konzola Playstation 4, ki ne podpira iger tretje generacije, zato nam Japonci želijo marsikateri naslov prodati še enkrat. Zakaj bi isto igro kupovali dvakrat? Na odklenjeno konzolo lahko poleg uradnih programskih izdelkov naložimo tudi domače umotvore. Navsezadnje si strojno opremo lastimo in pošteno je, da na njej zaganjamo, kar nam srce poželi. Odklenjeno konzolo je lažje vzdrževati, ji zamenjati disk in drugo strojno opremo. Naslednja generacija japonske konzole bo bojda imela hitri disk SSD, ki bo igre nalagal desetkrat hitreje. Na odklenjenem Playstationu si ga zlahka omislimo že danes in uživamo v brzini prihodnosti.

Za konec omenimo pozitivni vidik odklepanja, ki se kaže v pridobljenem znanju uporabnika. Odklepanje tovarniško zaklenjenih naprav je odlična priložnost za učenje, aktualni stik s tehnologijo, ki kroji življenje vsakdanjiku. S postopki odklepanja pridobimo samozavest, občutek izrednega dosežka, s katerim se bomo lažje lotili tudi resnejših projektov ali spočeli obetajočo kariero na področju informacijske in tehnologije nasploh.

Boris Šavc

Ne vidim potrebe

Priznam, tudi sam sem bil nekoč med tistimi, ki so vsak novi telefon programsko razstavili na prafaktorje, nanj namestili najnovejši in seveda (naj)boljši Android, prek njega pa potem množico sistemskih aplikacij, s katerimi smo ga še razširili. Na ta način sem imel v rokah vedno »oh in sploh« najnovejši telefon, ki je bil v vseh pogledih boljši od originala. No, razen, da je bolj ali manj redno »crkoval«. K sreči se mi vsaj z mojim programsko nadgrajenim avtomobilom to ne dogaja. Še.

Življenje na konici rezila je zanimivo, če ne kar razburljivo, vendar si človek sčasoma vendarle zaželi umirjenosti, zanesljivosti in lagodja. Uporabe naprave, kot si jo je zamislil proizvajalec.

Množica navdušencev sicer še vedno izdeluje t. i. »ROM«, kamor »zapečejo« prav vse novosti, ki jih Google predvidi za naslednjo inačico Androida, in še marsikaj. Omogočajo celo spreminjanje hitrosti delovanja vgrajenega procesorja, moči oddajnika WiFi, frekvenčnih kanalov in varčevalnih načinov celotnega sistema, natančno »uspavanje« le določenih programov in podsistemov, odnamestitev prav vseh sistemskih aplikacij in platform ter še kaj. Igranje s takimi ROM je zanimivo in zabavno, vendar v resnici smiselno le na ločeni napravi, ne na tisti, ki jo potrebujemo vsakodnevno. ROM so namreč največkrat nedokončani, ker se »sestavljavcem« ne da ukvarjati z manj zanimivimi deli in ker za vse navadno zmanjka časa. Imeti telefon, ki je sicer dva odstotka hitrejši, ker smo mu zvišali procesorski takt, je sicer res »kul«, toda če ta isti telefon občasno pozabi zvoniti, ko nas kdo pokliče, je jasno, da gre le za igračo.

Predvsem pa – razlika med tovarniško programsko opremo in zgoraj omenjenimi predelanimi ROM je čedalje manjša. Včasih so bili mobilni operacijski sistemi dejansko zelo omejeni in zaklenjeni, uporabniku je res proste roke omogočil le skrbniški način dostopa. V vseh teh letih je Google v svoj operacijski sistem vnesel marsikaj izmed tistega, za kar je bilo včasih treba Android »rutati«. Še celo programi za polno varnostno kopijo celotnega datotečnega sistema so že skorajda nepotrebni, odkar za varnostne kopije skrbi Googlov oblak.

Stanje je drugačno na platformi Apple, predvsem zato, ker je na Androidu že v osnovi omogočeno nalaganje aplikacij tudi mimo uradne trgovine, na sistemu iOS pa tega ni. Toda iOS je tako neprodušno zaprt, da se tam odklepanja še posebej ni smiselno lotiti.

Matej Šmid

26. junija nadaljujemo

Tradicionalni **poletni test televizorjev**

Približuje se poletje, ko se pri Monitorju tradicionalno spopademo s kopico velikih pametnih televizorjev. Preizkusili bomo, kateri modeli so trenutno aktualni, kateri med njimi so najboljši in kateri ponujajo najboljše razmeje med ceno in kakovostjo.

Pametna mesta, v Sloveniji

Pisali smo že, kako se pametnih mest lotevajo v tujini (Google, Huawei…), tokrat pa se bomo posvetili rešitvam, ki jih obljubljata naša dva največja mobilna operaterja – Telekom in A1.

MonitorPRO

V prilogi MonitorPro bomo pisali o poslovni analitiki in poslovnem obveščanju.

Monitor

ODGOVORNI UREDNIK
Matjaž Klančar

POMOČNIK ODGOVORNEGA UREDNIKA
Jure Forstnerič

UREDNIK
Uroš Mesojedec

LEKTURA
Simona Mikeln

PREVAJANJE
Petra Piber

LIKOVNA ZASNOVA
Peter Gedei

OBLIKOVANJE NASLOVNICE
Peter Gedei

RAČ. GRAFIKA IN STAVEK
Peter Gedei

FOTOGRAFIJE
Peter Gedei, fotoarhiv Monitorja, iStock

NASLOV UREDNIŠTVA
Monitor, Dunajska 51, 1000 Ljubljana,
tel.: (01) 230 65 00
faks: (01) 230 65 10
e-pošta: urednistvo@monitor.si

MONITOR V SPLETU
www.monitor.si

IZDAJATELJ
Mladina d.d., Dunajska cesta 51,
1000 Ljubljana, dav. št. 83610405

PREDSEDNICA UPRAVE
Denis Tavčar

PRODAJA OGLASNEGA PROSTORA
tel.: (01) 230 65 36,
e-pošta: marketing@monitor.si

VODJA MARKETINGA IN OGLASNEGA TRŽENJA
Ines Markovčič, tel.: (01) 230 65 33

NAROČNINE IN PRODAJA
tel. 080 98 84, (01) 230 65 30,
e-pošta: narocnine@monitor.si

TISK
Shwartz Print, Ljubljana

NAKLADA
3.850 izvodov

DISTRIBUCIJA
Izberi d.o.o., Ljubljana

Poštnina za naročnike plačana pri pošti 1102, Ljubljana. V ceno izvodov v maloprodaji s priloženim DVDjem je vključen DDV v višini 22%, v ceno ostalih izvodov pa DDV v višini 9,5%. ISSN 1318-1017

Izid je finančno podprla Javna agencija za raziskovalno dejavnost Republike Slovenije.