Prikaz knjige UDK: 621.391:351.746.1(049.3)

PRIROČNIK KIBERNETSKE VARNOSTI

Ivana Boštjančič Pulko, Gorazd Božič, dr. Denis Čaleta, Matic Čaleta, Borut Jakopin, mag. Polona Jerina, Matjaž Mravljak, Maja Obreht: Priročnik kibernetske varnosti. Urad Republike Slovenije za informacijsko varnost, Ljubljana 2025, 188 strani.

Urad Vlade RS za informacijsko varnost (URSIV) je zaradi povečane potrebe pri zavezancih ter na splošno za krepitev odpornosti informacijsko-komunikacijskih sistemov pred kibernetskimi incidenti v slovenskih organizacijah sprejel odločitev o pripravi priročnika kibernetske varnosti, za pomoč pri izvedbi te naloge pa je pritegnil Institut za korporativne varnostne študije (ICS).

1. SUBJEKTI SE MORAJO ZAVEDATI LASTNE ODGOVORNOSTI – PRIROČNIK JE (ZGOLJ) POMOČ

Priročnik[1] ponuja ključne smernice in priporočila za zaščito informacijskih sistemov pred kibernetskimi grožnjami. Namenjen je tako zavezancem kot tudi nezavezancem v javnem in zasebnem sektorju, vsem posameznikom, ki želijo izboljšati svojo varnostno pripravljenost ter odpornost na incidente, ki bi lahko ohromili njihov kibernetski prostor ter posledično vplivali tudi na ključne storitve in dejavnosti. Obravnava ključne izzive in grožnje, s katerimi se soočamo v digitalni dobi, in ponuja konkretne smernice za vzpostavitev učinkovitega sistema kibernetske varnosti.

Priročnik lahko uporabljajo organizacije in osebe, odgovorne za pripravo varnostne dokumentacije, saj podaja osnovne informacije ter napotke, kje pridobiti dodatne vsebine za posamezna področja. Namen priročnika ni posredovati primere dokumentacije v smislu vzorčne dokumentacije za doseganje zakonodajne skladnosti. Pri URSIV namreč verjamemo, da organizacije razumejo zakonodajno skladnost kot svojo nalogo in odgovornost, pri tem pa jim omenjeni priročnik lahko nudi dodatne potrebne informacije.

[1] Na voljo je na <https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf> (2. 6. 2025).

1.1. Nacionalni sistem kibernetske varnosti

V uvodnih poglavjih priročnik pojasnjuje vlogo URSIV kot osrednjega nacionalnega organa za kibernetsko varnost in njegovo sodelovanje z drugimi deležniki. Predstavljeni so temelji nacionalnega sistema kibernetske varnosti, ki vključujejo Nacionalni načrt za odzivanje na kibernetske incidente (NOKI). Dokument poudarja pomen tesnega sodelovanja med državnimi organi, ključno infrastrukturo in zasebnim sektorjem ter zagotavlja jasna navodila za odzivanje na kibernetske grožnje. Podaja pa tudi pomembne, že naučene lekcije, ki so bile pridobljene prek izvedenih inšpekcijskih nadzorov. Pomembno vlogo pri obravnavi informacijskih incidentov imata odzivni skupini za kibernetske incidente (CSIRT), in sicer SI-CERT, umeščen v javni infrastrukturni zavod ARNES in SIGOV-CERT kot del URSIV.

SI-CERT koordinira reševanje incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah na elektronskih omrežjih. V skladu s trenutno veljavnim Zakonom o informacijski varnosti (ZInfV) ter Zakonom o elektronskih komunikacijah (ZEKom-2) je pristojen za izvajalce bistvenih storitev, ponudnike digitalnih storitev in operaterje elektronskih komunikacij, v primeru prostovoljnih priglasitev pa tudi za vse preostale poslovne subjekte in tudi državljane. Izvaja tudi nacionalni program ozaveščanja Varni na internetu[2] in sodeluje v projektu SAFE-SI.[3]

SIGOV-CERT je odzivni center za incidente v informacijskih sistemih organov državne uprave. Pristojen je za sprejem in obravnavo kibernetskih incidentov v organih državne uprave, ki upravljajo informacijske sisteme in dele omrežja oziroma izvajajo informacijske storitve, nujne za nemoteno delovanje države ali za zagotavljanje nacionalne varnosti.

1.2. Pravne podlage in mednarodna vpetost

Del priročnika vsebuje pregled trenutno veljavnih pravnih podlag, ki urejajo področje informacijske varnosti v Sloveniji in EU. Predstavljeni so ključni zakonski, podzakonski in drugi pomembni nacionalni dokumenti, ki podajajo okvir tega področja v Sloveniji. V nadaljevanju je pregled aktualnih evropskih dokumentov in institucij, ki podajajo pomemben okviru tudi za slovenski pravni red. Ta sklop je sklenjen s pregledom ključnih mednarodnih standardov.

[2] Glej <https://varninainternetu.si/>.

[3] Več na <http://safe.si/>.

1.3. Vzpostavitev sistema informacijske varnosti v organizacijah

Priročnik podaja praktične smernice za vzpostavitev sistema informacijske varnosti v organizacijah. Obravnava načrtovanje krovne varnostne politike, izvedbo analize tveganj, upravljanje in obvladovanje tveganj, pripravo ocene vpliva na poslovanje ter tudi napotke za oblikovanje ukrepov za zmanjševanje varnostnih tveganj. Poudarjeni so tudi upravljanje s kibernetskimi incidenti, izvedba vdornih testiranj, upravljanje varnostnih kopij in tudi kaj pričakovati v okviru storitev varnostno operativnih centrov.

Dodana so tudi področja, vezana na orodja, ki omogočajo učinkovito spremljanje informacijskih sistemov v organizacijah, napotki za sklepanje pogodb z zunanjimi izvajalci in tudi za izvedbo javnih naročil. Tem področjem se v praksi nameni premalo pozornosti, hkrati pa vplivajo na vse organizacije. Priročnik poudarja tudi pomembnost varovanja podatkov, upravljanje z dnevniškimi zapisi in fizično varovanje prostorov organizacij.

1.4. Krizno komuniciranje v primeru kibernetskega incidenta

Posebno poglavje je namenjeno kriznemu komuniciranju v primeru kibernetskega incidenta. Priročnik podrobno opisuje, kako organizacija pripravi komunikacijsko strategijo, kdo so ključni deležniki v postopku obveščanja in kako preprečiti širjenje napačnih informacij ter panike v primeru večjega incidenta. Določeni so postopki za obveščanje zaposlenih, strank, regulatorjev in javnosti ter priporočila za sodelovanje z mediji. Jasna in usklajena krizna komunikacija je namreč lahko ključna za ohranjanje zaupanja in učinkovito komuniciranje z deležniki in javnostmi v takih primerih.

2. POMEMBEN KORAK K VEČJI KIBERNETSKI VARNOSTI

Kibernetska varnost postaja vse pomembnejša, tako za organizacije kot tudi za posameznike, saj digitalne grožnje nenehno rastejo in se razvijajo. Priročnik ponuja celovite smernice in praktične rešitve, ki pomagajo pri vzpostavitvi varnejšega digitalnega okolja. Z ustreznimi preventivnimi ukrepi, pravilnim odzivanjem na incidente in učinkovitim kriznim komuniciranjem lahko organizacije zmanjšajo tveganja in zaščitijo svoje podatke ter infrastrukturo. Deljenje informacij o incidentih v organizacijah je lahko pomembna izkušnja in lekcija. Smiselno jo je predati tudi drugim organizacijam, saj sta skupnost in sodelovanje lahko zelo pomembna dejavnika v primeru posameznih informacijskih incidentov. Na URSIV deljenje informacij vidimo kot krvodajalsko akcijo. Deli in sodeluj, kajti nikoli ne veš, kdaj ti bo uporaba deljene tuje iz-

kušnje pomagala preživeti kibernetski incident oziroma čim prej okrevati in vzpostaviti normalno delovanje sistemov.

Priročnik ni pravno zavezujoč dokument in tudi ne posega ali spreminja zakonskih obveznosti. Lahko pa je napotek za vse organizacije in posameznike, ki bodo pripravljali varnostno dokumentacijo za informacijske sisteme v svojih organizacijah. URSIV bo vesel vsakršne povratne informacije o vsebinah v priročniku in ga vidi kot pomemben korak, ki se bo z razvojem področja in zakonodaje tudi ustrezno nadgrajeval in dopolnjeval.

Uroš Svete,
univerzitetni diplomirani obramboslovec, doktor obramboslovja, direktor Urada Vlade Republike Slovenije za informacijsko varnost ter docent za področje obramboslovja na Fakulteti za družbene vede Univerze v Ljubljani