Varno in učinkovito elektronsko poslovanje

Andrej Zimšek, Maček d.o.o., Celje
andrej.zimsek@macek.si

1 Uvod

V informacijski družbi težimo k čim večji uporabi elektronskih medijev. Poslovanje selimo s papirja na elektronske medije. Z uporabo novih tehnologij moramo zagotoviti tudi določeno varnost in učinkovitost. Zahteve uporabnikov se hitro večajo s spoznavanjem novih tehnologij. Hkrati z večanjem zahtev se omrežja tudi čedalje bolj odpirajo in zato zahtevajo učinkovito varovanje. Za povezovanje omrežij je pomembno zagotavljanje kvalitete storitve in zadostne pasovne širine za ključne aplikacije.

S hitrimi koraki se približujemo informacijski družbi. V tako okolje se najlaže vklopimo z uporabo sodobnih informacijskih tehnologij, ki omogočajo elektronsko poslovanje. To je pravzaprav popolnoma običajno poslovanje preko omrežja – trgovanje, bančne storitve, sporočilni sistemi in podobno. Trgovina in bančništvo sta področji, ki ju največkrat omenjajo kot primera elektronskega poslovanja. To sta tudi dve najbolj odmevni področji, preko katerih se uveljavljajo novi standardi kot so SET (Secure Electronic Transaction) in plačilni sistemi za plačevanje malih vrednosti [1],[2],[5]. V svetu obstajajo podjetja, ki delujejo samo preko omrežja - npr. Amazon - in nimajo svoje poslovalnice v običajnem smislu. Manj odmevni sistemi elektronskega poslovanja so varne povezave med podjetji ali posamezniki preko javnih omrežij. Možnost stalne povezave s podjetjem in s tem dostop do vseh informacij je pomembna predvsem za ljudi, ki veliko potujejo. Za takšno povezovanje je nujno potrebno zagotoviti tudi ustrezno varovanje podatkov [4],[5].

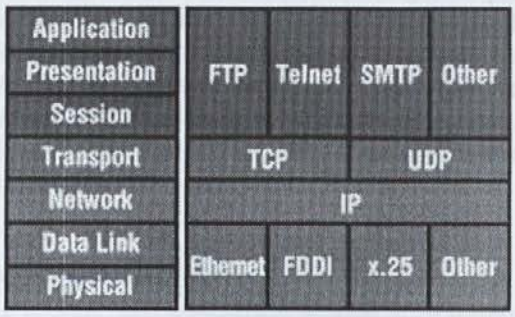
V prispevku se ne bomo ustavljali ob dilemah, povezanih s širjenjem informacij, in čedalje večji vrednosti informacij za podjetje. Predvsem bi radi predstavili možnosti, ki jih ponuja sodobna tehnologija za varovanje podatkov (informacij) pred nepooblaščenimi osebami in za zagotavljanje sredstev, s katerimi te informacije širimo. Pri zaščiti moramo pomisliti tudi na čedalje večje število virusov in na ozaveščenost ljudi, ki uporabljajo sodobne tehnologije.

2 Vrste požarnih zidov

Pri zagotavljanju varnosti za poslovanje preko javnih omrežij (internet) takoj pomislimo na požarni zid. Požarni zid najbolje opredelimo kot skupek naprav in postopkov, ki skrbijo za nadzor in kontroliran dostop uporabnikov v ščiteno omrežje in iz njega [8],[9],[10],[11].

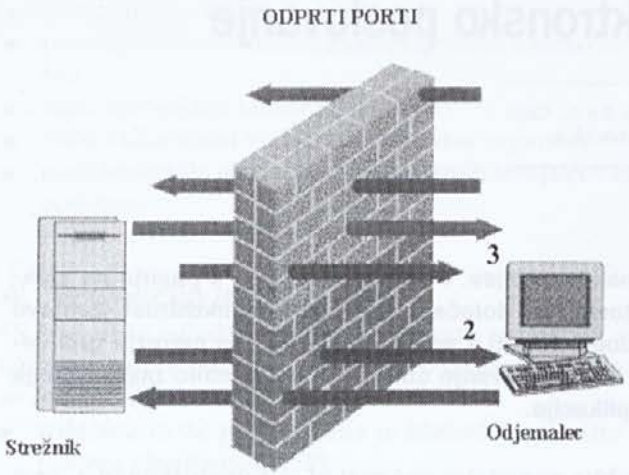
Napadi na omrežje so zelo različni. Skupni cilj vseh napadov je bodisi okoriščanje z informacijami, dokazovanje ali povzročanje škode. Glede na cilj napada uporablja napadalec več metod, od prisluškovanja, pretvarjanja, prevzemanja sej do socialnega inženiringa. Za dobro zaščito privatnega omrežja moramo varovalne ukrepe postaviti na vseh ravneh. Ni dovolj postaviti požarni zid in za njim še vedno imeti nekatere računalnike z modemi zaradi "lažjega" dela od doma. Poskrbeti je potrebno za ustrezno izobraževanje uporabnikov, njihovo ozaveščanje in prevzemanje odgovornosti.

Za zaščito omrežja poznamo več pristopov k postavljanju požarnih zidov. Pristopi se razlikujejo med sabo po mestu kontrole paketov v modelu ISO/OSI (International Organization for Standardization/ Open Systems Interconnection) (Slika 1).



Slika 1: Model ISO/OSI

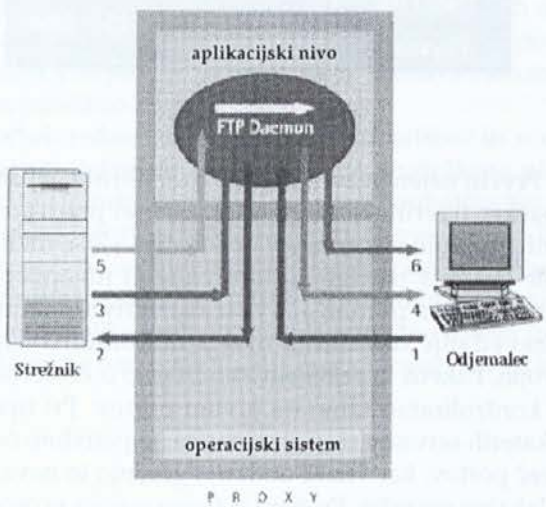
Prvi in najenostavnejši pristop je filtriranje paketov (»packet filtering«), ki ga uporabljamo predvsem pri konfiguriranju na usmerjevalnikih (Slika 2). Zaradi kontrole paketov na tretjem (omrežnem) nivoju so zelo hitri. Glavna pomanjkljivost filtriranja paketov je nezavedanje dogajanja na višjih komunikacijskih nivojih. Pakete, ki prihajajo ali odhajajo iz omrežja, lahko kontroliramo samo na nivoju portov. Pri uporabi nekaterih servisov smo omejeni, saj je potrebno odpreti več portov, kar vnaša dodatno grožnjo in nevarnost za lokalno omrežje. Primer takšnega servisa je protokol FTP (File Transfer Protocol), namenjen prenosu datotek. Komunikacija med strežnikom in odjemalcem poteka



Slika 2: Filtriranje paketov

najprej po vnaprej znanem portu, pozneje se preseli na en izmed prostih portov nad 1024. Zaradi narave protokola moramo omogočiti komunikacijo do strežnika prek vseh portov nad 1024. Pri filtriranju paketov ne preverjamo vsebine paketa, ampak se omejimo samo na porte, po katerih se komunikacija izvaja. Nadgradnja običajnih pravil je časovna omejitev, v kateri so pravila (»access liste«) veljavna. Prednost uporabe filtriranja paketov je hitrost.

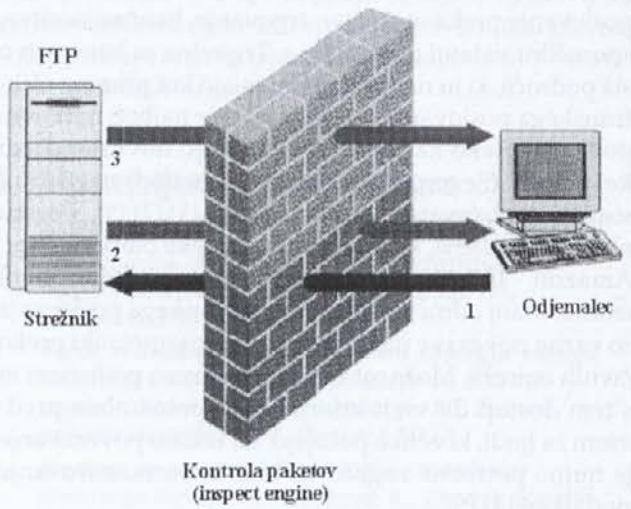
Drugi tip požarnega zidu (Slika 3) postavlja kontrolo na aplikacijskem nivoju. Pri tem pristopu se poruši standardni model odjemalec-strežnik, ker se povezava razdeli na dva dela, kar podvoji število sej. Prvi del predstavlja komunikacijo od strežnika do požarnega zidu, drugi pa od požarnega zidu do strežnika. Ker mora za vsako aplikacijo na požarnem zidu teči svoj



Slika 3: Kontrola na aplikacijskem nivoju

proces, se pojavi problem podpore novim storitvam in aplikacijam. Z večanjem števila procesov (»proxy serverjev«), se veča tudi ranljivost sistema, na katerem tečejo ti procesi. Veča se tudi procesorska moč, potrebna za izvajanje vseh procesov. Prednost požarnega zidu na aplikacijskem nivoju je popoln nadzor nad aplikacijo, slabost pa velika procesorska moč in težka prilagodljivost novim servisom.

Tretji tip požarnega zidu (Slika 4) je kombinacija obeh prej opisanih. Paket se pri popolnem pregledu paketov (»statefull inspection«) prevzame med drugim (»data link«) in tretjim, omrežnim nivojem. Potem sledi popoln pregled paketa in stanj, ki so jih povzročili prejšnji paketi. Vsi podatki o paketih se hranijo v tabelah, ki služijo za kasnejše odločanje pri izvajanju varnostne politike. Ker so pri tem načinu nadzora pake-



Slika 4: Popoln pregled paketov

tov na voljo vsi podatki, je možna kontrola ne samo sej TCP (Transmitission Control Protocol) ampak tudi UDP (User Datagram Protocol) in ICMP (Internet Control Message Protocol). Na primer, omogočimo lahko prehod SNMP (Simple Network Management Protocol) »get« paketov, onemogočimo pa SNMP »set«. Za pravilno odločanje in popolno kontrolo komunikacijskih poti potrebujemo informacije o celotni komunikaciji in podatke iz ostalih aplikacij. Odvisno od aplikacije ali komunikacije, ki jo želimo preveriti, potrebujemo komunikacijsko stanje, dobljeno iz prejšnjih paketov v tej seji, in aplikacijsko stanje, dobljeno iz drugih aplikacij. Vsa stanja se shranjujejo v tabelah.

Pregled paketov se izvaja pred vsemi programskimi moduli v računalniku (»kernel mode«). S tem preprečimo možnost vdora v računalnik, na katerem teče programska oprema požarnega zidu in onemogočimo

napadalcu izkoriščanje "varnostnih lukenj" na aplikacijskem nivoju.

3 Navidezna privatna omrežja

Zaščita omrežij se v današnjem času velikega pretoka informacij ne izvaja samo na meji med javnim in privatnim omrežjem, ampak se čedalje bolj seli na eni strani k strežnikom, ki informacije nudijo, in na drugi strani uporabnikom, ki informacije pregledujejo. Še pred nekaj leti je bilo enostavno postaviti vmesno omrežje (demilitarizirano cono), v katero smo postavili strežnike, do katerih so imeli dostop vsi uporabniki, iz njih pa ni bil mogoč dostop nikamor. S takšnim pristopom smo izolirali strežnike in onemogočili napade na lokalno omrežje. Zaradi čedalje večjih zahtev uporabnikov vmesno omrežje ne zadošča več. Uporabniki zahtevajo dostop do virov podatkov v lokalnih omrežjih in direktno povezavo z informacijskim sistemom podjetja s kateregakoli mesta. Po drugi strani to vnaša v zaščito omrežja luknje, ki jih je potrebno ustrezno zavarovati. Varovanje v prvi vrsti zagotovimo s strogim overjanjem vseh uporabnikov in uvedbo navideznih privatnih omrežij (»virtual private network«).

Navidezna privatna omrežja gradimo na več načinov. Uporabimo lahko za ta namen razvite naprave ali uporabimo dodatne funkcije sistema požarnega zidu. Pri uporabi strojne opreme gradimo dva ločena sistema, sistem zaščite omrežja pred vdori iz javnih omrežij in sistem za navidezna privatna omrežja. Pri uporabi sistema požarnega zidu združimo ti dve področji v en sistem. S tem se izognemo dvojni administraciji sistemov in predvsem pridobimo preglednost celotne rešitve.

4 Overjanje uporabnikov

Zaščita omrežja je povezana tudi z učinkovitim preverjanjem identitete. Uporabnik z določenimi pravicami se mora najprej predstaviti sistemu, ki mu glede na njegove pravice dodeli dostop do podatkov in storitev. Za preverjanje identitete je najenostavneje uporabiti par statičnih besed, ki predstavljajo uporabniško ime in geslo. Za sisteme, ki zahtevajo večjo varnost, je to vsekakor premalo. V teh primerih uporabimo metode enkratnih gesel, ki lahko temeljijo na časovno generiranih geslih, geslih tipa izziv-odgovor (»challenge-response«) ali kombinacije obeh sistemov. Ker je geslo v teh primerih vsakič drugačno, mora uporabnik imeti posebno napravo za generiranje gesel.

V zadnjem času se je pričela tudi uporaba pametnih kartic, na katere shranimo elektronski podpis. Podpis moramo najprej overiti pri elektronskem notarju, ki mu verjameta obe strani. S takšnim podpisom se lahko prijavimo v sistem ali ga uporabimo tudi za podpisovanje in kodiranje podatkov, ki jih prenašamo preko omrežja. V vsakdanjem življenju uporabljamo pri notarju overjen podpis. Ker so notarji overjeni in jih potrjuje država, ki ji zaupamo, zaupamo tudi v verodostojnost tako podpisanih dokumentov. Podobno se dogaja v "navideznem svetu", kjer poznamo elektronske notarje. Ker fizičnega kontakta pri elektronskem poslovanju ni potrebno vzpostaviti, se je potrebno še dodatno zavarovati pred morebitnimi zlorabami. Za podpis v ta namen uporabljamo par nizov naključno generiranih števil. Prvi del predstavlja javni ključ, drugi pa zasebni ključ, ki ga moramo varovati. S kombinacijo obeh ključev učinkovito šifriramo sporočila, ki jih lahko potem prebere le naslovnik.

Kodiranje lahko izvedeno s pomočjo algoritma Diffie-Hellman [6]. Za enostavnejši prikaz algoritma si zamislimo dva uporabnika (Janko in Metka) s skrivnimi ključi. Edini problem, ki ostaja pri tej shemi odprt, je garancija, da javni ključ Metke res pripada Metki. Ta problem reši elektronski notar ali overitelj, ki s svojim podpisom jamči o pristnosti elektronskega podpisa.

Pri transakcijskem poslovanju je potrebno poskrbeti tudi za potrjevanje vsake transakcije in ob posebnih zahtevah za ugotavljanje resničnosti podatkov ali zahtev tudi za podpisovanje [7].

Z zgoraj omenjeno tehnologijo je možno enostavno dokazati, kdo je poslal zahtevo in kaj je zahteval. Edini problem, ki se pojavlja pri nas, je priznavanje elektronskega podpisa od države in s tem sodišča v primeru tožbe ipd. Za takšne primere je potrebno med strankama podpisati dokument, v katerem obe strani priznavata elektronski podpis kot pristojen za reševanje in dokazovanje spornih primerov. V parlamentarni obravnavi je *Predlog zakona o elektronskem poslovanju in elektronskem podpisu* [12], ki bo rešil problem veljavnosti elektronskega podpisa

5 Kvaliteta storitve

Pretok podatkov je z višanjem zahtev uporabnikov čedalje večji. Za zagotavljanje kvalitete storitve je poleg varnostnega vidika potrebno upoštevati tudi razpoložljivost informacij v določenem trenutku. V teh primerih se pojavi nov element v varnostni politiki, ki mu bomo v prihodnosti posvečali precej pozornosti, to je kvaliteta storitve (quality of service).

Določene aplikacije zahtevajo večjo pasovno širino in so za poslovanje pomembnejše kot druge. Zagotavljanje dostopa do elektronskega plačevanja storitev je za določeno podjetje najpomembnejša storitev. Dostop uslužbencev preko te linije do interneta je drugotnega pomena, vsaj v času ko se izvaja prenos plačilnih nalogov. V takšnem primeru ima večjo težo promet "strank", ki izvajajo elektronsko plačevanje storitev tega podjetja.

Ker ima lahko podjetje več točk dostopa do interneta in več notranjih oddelkov, potrebuje več požarnih zidov, ki ta omrežja med seboj ločujejo. Na vsakem od požarnih zidov se prav tako pojavljajo potrebe po zagotavljanju pasovne širine za določene aplikacije. Zaradi lažje administracije in nadzora je ena izmed zahtev tudi centralna administracija. S takšnim načinom lahko iz enega mesta pregledujemo celotno varnostno politiko in jo potem ustrezno tudi prilagajamo potrebam podjetja. S produktom, ki omogoča centralno administracijo, je možno enostavno in učinkovito pregledovati in beležiti dogajanje na vseh varovanih prehodih med omrežji. Beleženje dogodkov je pomembno bodisi zaradi rekonstrukcije preteklih dogodkov, dokazovanja ali za zaračunavanje storitev. Skrbnik varnostnega sistema ima pri centralnem nadzornem mestu vpogled v vse parametre varnostnega sistema in se laže odloča o ukrepih za zagotavljanje največje možne varnosti varovanih omrežij.

6 Izbira rešitve

Noben produkt ne more rešiti vseh zahtev, zato je pri izbiranju rešitve potrebno izbirati produkte, ki omogočajo kasnejše združevanje in upoštevajo standarde.

Za nadzor omrežja je pomembna zaščita pred virusi. Z zaščito vstopne točke izvedemo centralno kontrolo prenesenih datotek iz javnega omrežja. Pri vsakem prenosu datoteke se sproži preverjanje in odpravljanje virusa iz datoteke, če je to mogoče. Za dobro delovanje takšne zaščite je pomembno tudi stalno obnavljanje vzorcev virusov in načinov za njihovo odstranitev. Obnavljanje vzorcev mora potekati avtomatsko v določenih časovnih intervalih.

Na internetu niso na voljo samo informacije, ki so potrebne za delo uslužbencev, ampak tudi strani namenjene samo zabavi. Če se želimo izogniti nepravilni uporabi interneta v službenem času, lahko omejimo uporabo interneta glede na vsebino. Prav tako kot pri protivirusni zaščiti, moramo tudi pri produktih, ki omogočajo selekcijo vsebine po področjih, stalno osveževati podatkovno bazo z naslovi spletnih mest.

Pred napadi se lahko dodatno varujemo s posebnimi produkti, ki nadzorujejo komunikacije med sistemi. Brž ko se pojavijo vzorci napadov, se sproži serija dogodkov, ki zapre vse poti do napadenega računalnika in tako prepreči napadalcu nadaljnje postopke. Glede na resnost napada se prepreči dostop do določene storitve ali celo do celotnega računalniškega sistema, dokler ne odpravimo morebitne napake ali ponastavimo sistem. Ti sistemi so primerni za dodatno zaščito storitev, ki jim dopuščamo vstop preko sistema požarnega zidu.

Za analizo podatkov, poročila in nadzor uporabljamo produkte za analizo dnevnikov obdelave, v katere se zapisujejo vsi podatki. S pomočjo teh podatkov je možno rekonstruirati dogodke ali točno analizirati šibke točke sistema varovanja in ga ustrezno izboljšati. Z analizo dnevnikov obdelave dobimo podatke o rabi določenih storitev. S tako dobljenimi podatki enostavno spremljamo uporabo storitev in v naprej načrtujemo rast sistemov, dostopnih linij itd.

Pri uvajanju varnostne politike je pomembno, da določimo odgovorne ljudi, ki skrbijo za izvajanje varnostne politike. Pri večjih podjetjih je potrebno imeti ljudi, ki se bodo ukvarjali izključno z varovanjem omrežja in podatkov v omrežju, podobno kot že zaposlujemo ljudi za fizično varovanje premoženja. S takšnim pristopom je možno uvesti zelo dobro varovan sistem s stalno kontrolo in hitrim ter učinkovitim odzivom na morebiten napad.

Pri manjših podjetjih je nemogoče pričakovati ustanovitev posebnega delovnega mesta za nadzor varnosti v omrežju, zato je toliko bolj pomembna uporaba orodij, ki pomagajo administratorju omrežja pri preverjanju varnostne politike. Med ta orodja spadajo produkti za odkrivanje in odpravo slabosti – varnostnih lukenj operacijskih sistemov ter orodja za sproten nadzor dogajanja v omrežju.

7 Zaključek

Tudi ob uporabi najsodobnejše tehnologije moramo še vedno ozaveščati ljudi in jih v skladu z uporabljeno informacijsko tehnologijo tudi ustrezno izobraževati. Niti najsodobnejša tehnologija ne more preprečiti vseh zlonamernih dejanj zaposlenih. S tehnologijo se lahko do določene mere zaščitimo in zgradimo sistem beleženja dogodkov, ne moremo in tudi ne smemo pa ovirati dela zaposlenih na račun večje varnosti. Za učinkovito zaščito omrežja je potrebno upoštevati celotno zgradbo omrežja in načine uporabe virov v omrežju. Zelo pomembno je sledenje novih tehnologij in sprotno posodabljanje in dograjevanje celotnega varnostnega sistema. Prav zaradi možnosti nadgradnje sistemov je potrebno ob nakupu ali naročilu opreme za zagotavljanje varnosti pregledati vse zmožnosti produktov in predvsem možnosti nadgradnje produkta oz. povezovanja z drugimi produkti.

Vsaka programska oprema zahteva tudi precej nastavitev in znanja o produktu, zato je najbolje začetno nastavitev prepustiti strokovnjakom. To je tudi najhitrejši način spoznavanja produkta in priprava na kasnejše upravljanje in uporabo.

Literatura

[1] J.Bos and D.Chaum. Smart Cash: A Practical Electronic Payment System. Technical Report, CWI-Report:CS-R9035, August 1990.

[2] DigiCash Press Release. World's First Electronic Cash Payment over Computer Networks, May 27th 1994.

[3] Phil Zimmermann. PGP User's Guide, Volume I: Essential Topics. Phil's Pretty Good Software, http://www.chemistry.mcmaster.ca/pgp/pgpdoc1/pgpdoc1.html

[4] Phil Zimmermann. PGP User's Guide, Volume II: Special Topics. Phil's Pretty Good Software, http://www.chemistry.mcmaster.ca/pgp/pgpdoc2/pgpdoc2.html

[5] Michael Peirce,Donal O'Mahony: Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set, http://www.w3.org/Conferences/WWW4/Papers/228/

[6] Understanding PKI, http://verisign.netscape.com/security/pki/understanding.html

[7] Encryption and Digital Certificates, http://www.verisign.com/whitepaper/enterprise/overview/index.html

[8] Mark Grennan: Firewall and Proxy Server HOWTO, http://metalab.unc.edu/mdw/HOWTO/Firewall-HOWTO.html

[9] CheckPoint Firewall1, Arhitecture and Administration, September 1998

[10] CheckPoint Firewall1, Getting Started, September 1998

[11] CheckPoint Firewall1, Virtual Private Networking, September 1998

[12] Predlog zakona o elektronskem poslovanju in elektronskem podpisu, http://www.gov.si:80/cvi/slo/ep/pzep.doc

◆

Andrej Zimšek se je po končanem univerzitetnem študiju zaposlil kot mladi raziskovalec in nadaljeval s študijem v Laboratoriju za robotiko na Tehniški fakulteti Maribor. Svoje znanje je izpopolnjeval v letih 1994/95 na dunajski tehniški fakulteti. Magisterski študij je posvetil proučevanju paralelnih računalniških sistemov in računalniških mrež. Zdaj je zaposlen v podjetju Maček d.o.o. Njegova glavna dejavnost je priključevanje omrežij na internet in zagotavljanje varnega elektronskega poslovanja. Na področju požarnih zidov je opravil tudi izpit CCSA in CCSE podjetja CheckPoint.

◆

Elektronsko poslovanje in XML

Mitja Dečman,Visoka upravna šola, Kardeljeva pl. 5, 1000 Ljubljana
mitja.decman@vus.uni-lj.si

1. Uvod – o elektronskem poslovanju

Vse kaže, da se na področju elektronskega poslovanja pojavlja nova razširitev. Ob neverjetno hitrem tehnološkem razvoju, neprestanem pojavljanju novih idej na tem področju in hitremu udejanjanju le-teh, je prišlo do ugodnih razmer za uvajanje tehnologije, imenovane eXtensible Markup Language (XML, extensible-razširljiv). Sicer bi temu težko rekli nova tehnologija, saj je nova samo ideja o uporabi ob kombinaciji in predelavi že obstoječih tehnologij. Čemur lahko rečemo novo, konec koncev celo revolucionarno, je ideja, kako popraviti obstoječo situacijo na področju elektronskega poslovanja in zapolniti vrzel, ki se je pojavila ob globalizaciji in širitvi svetovnega trgovanja na področju Interneta.

"V elektronskem poslovanju med podjetji (Business-To-Business) obstaja vrzel, ki jo trenutno lahko uspešno zapolni XML (John Ousterhout, Scriptics Corp.)"

Kot vemo, segajo začetki elektronskega poslovanje desetletja v preteklost, nekateri bi rekli, v prejšnje tisočletje. Danes si lahko predstavljamo pod elektronskim poslovanjem vse od prodaje preko spletnih strani, pošiljanja raznih dokumentov po elektronski pošti, do kompleksnih aplikacij, ki temeljijo na standardih kot je Računalniška izmenjava podatkov (rip) ali Electronic data interchange (EDI). Vendar se je med vsemi temi možnimi uporabami pojavila praznina, katero je uspešno zapolnil XML.

2. XML in primeri uporabe

"Vlak za XML stoji na postaji in je trenutek pred tem, da odpelje, toda mnoga podjetja še vedno ne vedo, kam gre in kako vstopiti na vlak (Information week, Jan 2000)"

S pojavitvijo jezika HTML v letu 1989 se je pojavil zametek tehnološke revolucije (danes jo že lahko imenujemo tako), ki je spremenila raziskovalno omrežje znanstvenikov, profesorjev in raznih državnih ustanov v družbeni in socialni fenomen, znan kot Svetovni splet (World Wide Web). Sedaj je na obzorju nova revolucija.