Viktor Kanižai, master*
OTP banka Srbija a.d. Novi Sad, Novi Sad,
Republika Srbija

UDK 004.492.2
Stručni članak

IT BEZBEDNOSNA OBUKA KAO PREVENTIVNA ZAŠTITA PODATAKA

SAŽETAK: Nagli razvoj informacionih tehnologija (IT) omogućio je čovečanstvu razne olakšice u oblasti komunikacije, obrade podataka, poslovanja, i dr. Danas, gotovo da nema kompanije koja ne upotrebljava računar u toku svog poslovanja, bilo kao podršku ili kao osnovni proces izvršavanja svojih delatnosti. Pojedinci takođe koriste rešenja IT-a u svom svakodnevnom životu, računar za olakšanje sticanja znanja, izvršavanja posla ili pak igranja igrica, mobilni telefon sada već kao osnovni resurs za komunikaciju, itd. Međutim, razvojem IT-a, tj. sve više funkcionalnosti IT-a, prisutan je i razvoj metoda i načina vršenja prevara i zloupotreba pomoću tih tehnologija, koji često mogu dovesti do direktne materijalne štete, kako za pojedince, tako i za kompanije. Najslabija karika u smislu napada na podatke i IT, jeste korisnik, ali on ujedno predstavlja i prvu liniju odbrane. IT bezbednosna obuka predstavlja prvi vid preventivne zaštite podataka i IT-a.

KLJUČNE REČI: IT bezbednost, zaštita podataka, bezbednosna obuka.

1. Uvod

Razvoj informacionih tehnologija (IT) poslednjih godina toliko je značajan i snažan, da su one postale deo naše svakodnevnice. Njihovo stvaranje novih mogućnosti je konstantno. Nikada nije bila komunikacija tako laka kao što je sada, podaci su putem umrežavanja računara (Internet) dostupni uvek i u velikim obimima. Često nismo ni svesni mogućnosti i izazova koje nam IT pruža. Ne treba zaboraviti ni činjenicu, da su najbogatiji ljudi upravo iz oblasti IT-a.

U većini institucija osnovni pokretač poslovnih procesa predstavlja IT infiastruktura. Neophodni su komunikacioni tokovi, baze podataka i njihova automatizovana obrada. Na taj način dolazi do ubrzanja poslovnih procesa, povećanja produktivnosti i obima radnih aktivnosti.

Za upravljanje IT-em neophodna je dobra obučenost i adekvatno znanje. Obavljanje dnevnih aktivnosti gotovo je nezamislivo bez dobrog poznavanja rada na računaru.

Sa druge strane, razvoj IT-a rezultirao je i pojavu novih načina izvršavanja prevara, zloupotreba, napada, tj. visokotehnološkog kriminala, krivičnih dela. Živimo u eri kompjuterizacije, novih mogućnosti i razvoja IT-a, ali ujedno i u eri Stuxneta, Vikiliksa i Fejsbuka. Upravo zbog toga je neophodno da IT em upravljaju lica koja su dobro obučena ne samo iz oblasti pravilne upotrebe iste, već i bezbednosti i zaštite podataka koji se pohranjuju i obrađuju. Korisnici treba da imaju osnovnu IT bezbednosnu svest, adekvatno osnovno znanje iz ove oblasti, kao i da im je jasno kako mogu da zaštite podatke i IT sistem, i kako taj sistem mogu da iskoriste za zaštitu.

*kanizsai.viktor@gmail.com

2. IT bezbednosna obuka

Ishodi i rezultati upotrebe računara skoro isključivo zavise od korisnika. Korisnik predstavlja najslabiju kariku u lancu obrade podataka. Računar izvršava to što mu se „naredi", a korisnik je taj koji daje naredbe za izvršenje. Nije dovoljno posedovati najsavremenije tehnologije, potrebno je znati njima i upravljati. A za to su neophodni stručni i obrazovani kadrovi.

U svetu korisnika IT-a mali je broj onih koji su svesni da pored „dobronamernih" korisnika postoje i oni sa lošom namerom – vršenje kriminalnih delatnosti iz oblasti visokotehnološkog kriminala, bilo sa namerom sticanja protivpravne imovinske koristi, ili iz radoznalosti, testiranja svojih mogućnosti, dokazivanja pred drugima, itd. Obuka u cilju povećanja bezbednosne svesti i sticanja osnovnog znanja iz oblasti zaštite podataka je neophodna kako bi se osigurala svrsishodna upotreba IT-a. Svim korisnicima mora da je jasno da svako IT rešenje može biti zloupotrebljeno i zato je značaj obuke veoma velik. IT bezbednosna obuka mora biti sastavni deo obrazovnog procesa korisnika, jer već živimo u svetu u kojem je zavisnost od IT-a nepremostiva.

Sticanje bezbednosne svesti i osnovnog znanja iz domena bezbednosti i zaštite podataka i IT, ne može se realizovati samoobukom ili posmatranjem drugih. Neophodna je primena propisanog, programski definisanog sistema obrazovanja i obuke. Bez toga, ispuniće se samo prvi uslov bezbednosti, a to je povećanje svesti, međutim, ne i sticanja adekvatnog znanja. Obuka ne sme biti predmet kursa – kao što se na tržištu mogu naći kratkotrajni kursevi, koji ponekada traju svega nekoliko sati. Obuka mora biti ciljna, programski dobro definisana i sistematična.

2.1. Upotreba računara

Prva tematika koju IT bezbednosna obuka treba da pokriva jesu mogućnosti rada na računaru i uopšte o načinu njihovog korišćenja od strane korisnika. Primarni cilj je da se ukaže na to da računar može biti objekat napada. I to ne fizičkog, već logičkog napada, jer meta napada nije sam računar, već podaci pohranjeni u njemu. Računar je veoma lako zameniti, ali podaci sadržani u njemu su nezamenljivi.

U smislu visokotehnološkog kriminala, računar ne samo da može biti objekat napada, već i resurs za:

– izvršenje kriminalnih delatnosti i

– planiranje, prikrivanje i organizovanje vršenja krivičnih dela.

Mogućnost upotrebe računara treba da se sagleda i sa aspekta savremenog sredstva za zaštitu podataka i IT-a. Tako, računar se može posmatrati i kao resurs za:

borbu protiv kriminalnih delatnosti koji ugrožavaju obradu podataka – što predstavlja preventivnu zaštitu,

otkrivanje, razjašnjavanje i dokazivanje kriminalnih dela ugrožavanja podataka – što predstavlja represivnu zaštitu.

Na kraju je važno istaći i mogućnosti korišćenja računara kao sredstva za bezbednosnu obuku. Oblici obuke upotrebom računara mogu biti:

Na licu mesta, koristeći razne oblike prezentacija,

Daljinska obuka, koja se može realizovati onlajn u okviru interne računarske mreže (intranet), preko javno dostupne mreže (internet), ili „zatvorene mreže" koja koristi javno dostupnu mrežu (VPN).

2.2. Zaštita podataka

Da bi obuka bila uspešna ljudi treba da budu svesni potrebe za obukom. Tako, IT bezbednosna obuka u cilju zaštite podataka treba da bude usmerena i ka podizanju svesti o neophodnosti bezbednosnog aspekta obrade podataka i rukovanja IT-em u celini. Treba da je jasno da bezbednost ne služi za sprečavanje izvršavanja željenih aktivnosti, bili poslovne ili privatne, već da osigura te aktivnosti, da ih učini, koliko je moguće, bezbednim. Mnogi korisnici zanemaruju bezbednost zbog eventualnog dodatnog opterećenja ili neke komplikacije u radu, i time nesvesno preuzimaju rizik na sebe. Tek kada se nešto zaista desi, ljudi počinju da razmatraju načine zaštite. Na primer, u jednoj od banaka u regionu, desilo se da su podaci izvesnog broja platnih kartica dospele u treće ruke, i to usled virusnog napada, zahvaljujući raznim propustima. Banka je pretrpela veliku materijalnu i reputacionu štetu. Tek su nakon ovog događaja shvatili da zaštitu podataka i bezbednost IT-a moraju shvatiti ozbiljno, da ulaganje u ovu oblast ne znači trošak već investiciju. Ta banka je potom među prvima postala PCI DSS (Payment Card Industry Data Security Standard) usaglašena u regionu.

Bezbednosna obuka treba da osigura da se ne sačeka nastanak štete, već da se preduzmu sve preventivne mere kako do štete ne bi ni došlo. IT bezbednosna obuka sama po sebi predstavlja preventivnu zaštitu podataka, a pored toga i dodatno iziskuje preduzimanje daljih preventivnih mera.

2.2.1. Objekat zaštite

Kroz IT bezbednosnu obuku potrebno je definisati objekte zaštite, tj. dati odgovor na pitanje šta treba štititi. A kao odgovor na ovo pitanje mogu se podrazumevati podaci pohranjeni na računaru, podaci u obradi, baze podataka, komunikacioni tokovi, programi, kao i sami računari, prenosivi mediji sa podacima, mrežna oprema. Korisnici moraju biti svesni šta treba da zaštite, odnosno koje su to vrednosti koje treba štititi.

2.2.2. Izvori pretnji

Neophodno je identifikovati izvore pretnji i rizike koji ugrožavaju bezbednost podataka i IT a. To daje odgovor na pitanje od čega i od koga treba štititi podatke. Izvori pretnji se sa jedne strane mogu klasifikovati u tri grupe:

ljudski izvori pretnji (namerne ili nenamerne pretnje; namerna greška, sabotaža, revanšizam, nezadovoljstvo, pribavljanje protivpravne imovinske koristi sebi ili drugima, špijunaža, ili neznanje, slučajna greška, i dr.);

– prirodni izvori pretnji (poplava, požar, zemljotres, itd.), i

izvori pretnji iz okruženja (dugoročni nestanak struje, rat, greška na hardveru, itd.).

Sa druge strane, izvori pretnji se mogu klasifikovati i kao: interni, eksterni, i sprega interno-eksternih faktora.

U lancu zaštite najslabija karika jeste korisnik, tj. najveće rizike predstavljaju ljudski izvori pretnji, iliti interni faktori. Najveću materijalnu štetu može naneti sprega interno-eksternih faktora. Na primer, ponovo iz sveta bankarstva, budući klijent banke aplicira za kredit, ali sa falsifikovanom dokumenracijom (npr. lična karta). Službenik banke koji razmatra zahtev jeste „njegov čovek", i tako on „ne primeti" da je predat dokumenat falsifikat, i unosi netačne podatke u informacioni sistem banke. Na taj način kredit bude odobren, i nikada neće biti vraćen.

Kroz IT bezbednosnu obuku korisnici moraju biti svesni pretnji i opasnosti kako bi se bolje zaštitili podaci i IT.

2.2.3. Moguća šteta

Potrebno je utvrditi moguće posledice i gubitke, odnosno štetu koju korisnici mogu imati od eksploatacije nekih od pretnji. Ovo u suštini daje odgovor na pitanje zašto treba štititi podatke. Utvrđuje se šteta, posledice ili gubitak usled ostvarenja pretnji na objekte zaštite. Te posledice mogu biti, delimično ili potpuno fizičko oštećenje (hardvera, softvera, podataka, itd.), otuđenje (hardvera, podataka, informacija, itd.) i modifikacija (hardvera, softvera, podataka, itd.). Gledano u terminologiji IT bezbednosti, posledice su narušavanje CIA trojstva: integriteta, raspoloživosti i poverljivosti podataka.

2.2.4. Izbor mera i sredstava zaštite

Pri obuci neophodno je dati odgovor i na pitanje čime i kako štititi podatke. Mere zaštite podataka mogu se posmatrati kao: normativno uređenje (zakoni i druga akta), mere fizičko-tehničke zaštite, logička zaštita, bezbednosna obuka i bezbednosni monitoring. Sve treba da ima za osnovni cilj podizanje svesti o potrebi zaštite podataka. Značaj obuke je ogroman, jer korisnici postaju sigurniji i time i efikasniji u svojim aktivnostima, u svom poslu.

U osnovi, zaštita može biti preventivna i represivna. Svima je poznata izreka: „Bolje sprečiti, nego lečiti", što naravno važi i u svetu zaštite podataka. Preduzimanjem preventivnih mera smanjuje se broj zloupotreba, prevara, kriminalnih dela koji se preduzimaju, kako protiv jedinca tako i protiv kompanija.

Sistem zaštite mora uvek da pobedi, dok je napadaču dovoljno samo jednom da pobedi.

3. Metode IT bezbednosne obuke

Savremeni oblik obuke podrazumeva korišćenje cikličnog usvajanja znanja. Obuka treba da se zasniva na primeni savremenih tehnologija uz angažovanje usko specijalizovanih profesionalaca iz ove oblasti. Obuka treba da je aktivna, da se zasniva na podsticanju i usmeravanju. U obuku obavezno treba uključiti i analizu iskustava, kako kod nas tako i u svetu. Obuka mora biti sveobuhvatna, planska i dobro organizovana, kako bi se izbegle određene vrste komercijalne obuke, kroz nuđenje kratkotrajnih kurseva, jednodnevnih ili poludnevnih treninga od često i nekompetentnih agencija i pojedinaca. Neophodna je neposredna saradnja naučno-obrazovnih

ustanova sa tržišnim subjektima, koja treba da bude dobro planirana i organizovana u cilju izvođenja kvalitetne obuke u domenu zaštite podataka. Oblik obuke u kojoj korisnik ima aktivnu ulogu najdelotvorniji je način da se ispune zahtevi za stručnu obuku, poveća znanje i svest o zaštiti podataka.

Savremeni model obuke podrazumeva upotrebu usvajanja cikličnog znanja. Na tržištu postoje razni komercijalni, kratkoročni kursevi, koji traju samo jedan dan, ili svega nekoliko sati. Međutim, IT bezbednosna obuka ne treba da bude pitanje kursa, već obrazovanja. Ključno je posedovanje sveobuhvatnog i efikasnog obrazovanja, iako to u nekim slučajevima znači dodatno opterećenje za pojedince.

Obuka je najefikasnija mera preventivne zaštite podataka. Ako korisnici poseduju odgovarajuću svest i znanje iz oblasti zaštite podataka, tada je i samo izvršavanje aktivnosti putem IT-a bezbednije, i to nezavisno od tehničko-tehnoloških rešenja zaštite. Ne treba zaboraviti, prvu liniju odbrane čine sami korisnici.

Obuka se može izvoditi na licu mesta ili udaljeno. U slučaju obuke na licu mesta, potrebno je da se pripremi prezentacija za datu priliku, a treba i da organizuje mesto održavanja obuke. Pored toga, neophodno je i organizovati korisnike koji će prisustvovati i učestvovati na obuci, što često i nije tako trivijalan zadatak. U slučaju da korisnicima na predavanju nešto nije jasno, oni svoja pitanja mogu trenutačno postaviti predavaču, koga mogu zaustaviti u svakom trenutku. Kod izvođenja obuke udaljenom metodom, ona se može realizovati ili preko e-mailova ili preko onlajn sistema u ili izvan IT mreže neke kompanije. Ako se predavač odluči za model izvođenja obuke putem e-mailova, treba da bude svestan da slanje materijala za obuku velikom broju primaoca može imati negativan uticaj na opterećenje datog e-mail servera, kao i mrežne komunikacije. Ako neko od korisnika ima pitanje, ono se može postaviti putem e-maila. U slučaju odabira onlajn obuke, predavač ima nekoliko mogućih izbora: realizacija obuke preko intraneta (u slučaju kompanije) ili interneta. Mrežno opterećenje i pristup internetu je u ovom slučaju ključno za razmatranje ove opcije.

Onlajn obuka može biti realizovana na nekoliko načina:

- kreirati prezentaciju sa slajdovima (npr. PowerPoint odštampan u PDF) i učiniti ga dostupnim za daunloadovanje;
- kreirati internet prezentaciju (sajt) i poslati link korisnicima na taj sajt

Koristeći opciju internet prezentacije postoje razne mogućnosti, upotreba PHP, HTML, SharePoint, itd.

U slučaju dobre IT infrastrukture i širokopropusne IT mreže, obuke se mogu organizovati i u obliku video konferencija, „webinara". Vrlo je važno dobro proceniti očekivani broj učesnika i očekivano mrežno opterećenje.

Izvođenje udaljene obuke takođe donosi i uštedu troškova, što u vreme finansijske krize predstavlja možda i najveći adut u odnosu na obuku na licu mesta. Nema troškova putovanja, organizovanja prostora za izvođenje obuke, ili pak plaćanja parking mesta. Takođe, udaljena obuka znači i vremensku uštedu, što je isto tako ključno kada vreme znači i novac.

Nakon završenog kruga obuke, treba da postoji i način procene uspešnosti njenog izvođenja, da bi se mogla utvrditi efikasnost same obuke, kao i potrebna poboljšanja u vezi sa izvođenjem obuke za sledeći ciklus. Nakon svakog završenog kruga obuke, neophodna je njena analiza, u cilju otklanjanja uočenih nedostataka, ili uvođenja novih ideja. Jedan od načina koji bi

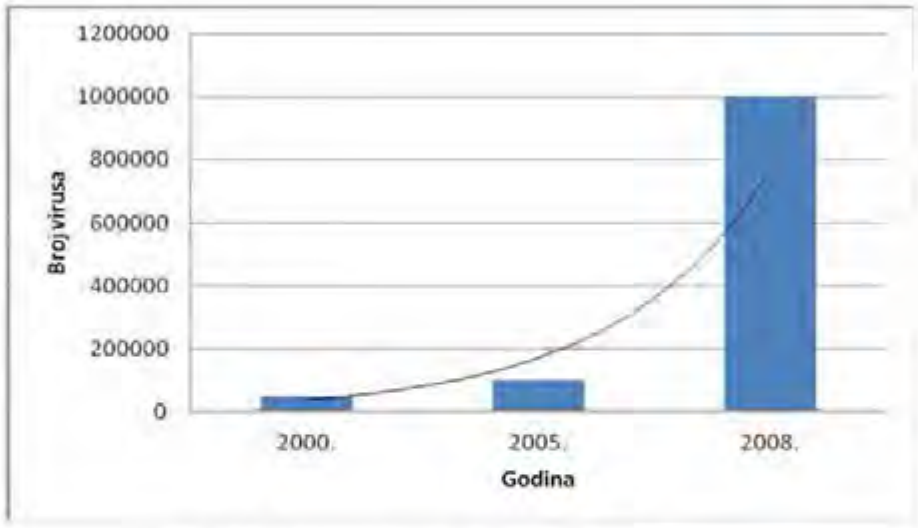
ovo obezbedio jeste testiranje korisnika nakon održane obuke, pri čemu bi se testiranje koristilo isključivo za procenu efikasnosti obuke.

Testiranje se, takođe, može izvršiti na licu mesta ili udaljeno. Test se može uraditi na papiru, potpisanu verziju uvek treba poslati predavaču, ili se može realizovati i preko popunjavanja onlajn upitnika. U slučaju papirnatog oblika testa, predavač mora da sakupi sve popunjene testove i da ih ručno ocenjuje i analizira. Dok kod onlajn testiranja, obrada podataka vrši se preko nekog, automatizovanog IT sistema koji ima razne mogućnosti analiza i kreiranja statističkih izveštaja u vezi sa rezultatima. Pri onlajn testiranju, kako bi se izbegli neki od mogućnosti varanja, može se uvesti i autorizovan pristup samom testu, tj. da pristup bude ograničen korisničkim nalogom i lozinkom. Trajanje, kao i link na test, može biti vremenski ograničeno. Može se podesiti da nakon popunjavanja prve stranice testa (ukoliko ih ima više), korisnik pre laskom na sledeću stranicu nema mogućnost povratka na prethodnu. Takođe, postoji i mogućnost da se test automatski zatvori ukoliko korisnik napusti dati prozor u kojem je otvorio test, kako bi pronašao odgovor na internetu.

4. Opravdanost IT bezbednosne obuke

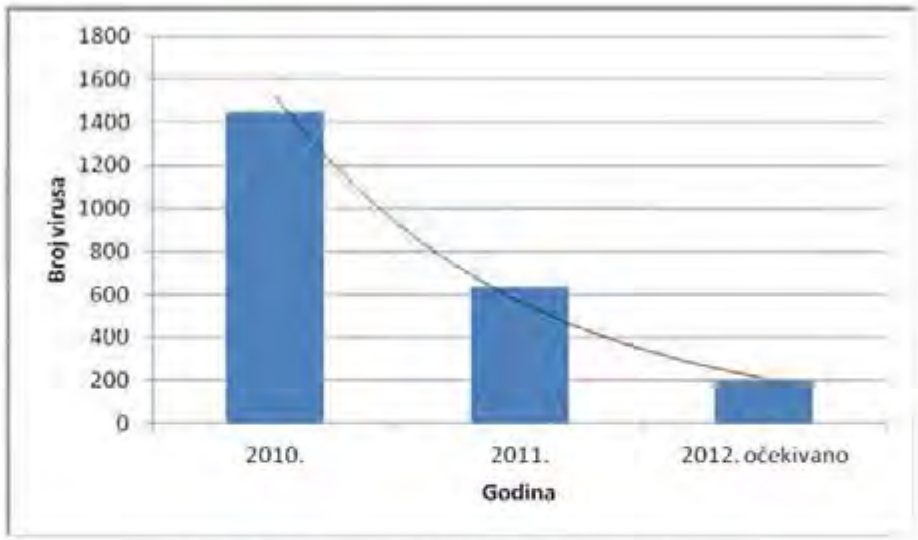
Broj računarskih virusa u svetu konstantno raste. Oni se šire i vrše zarazu računara najčešće preko interneta, deljenih mreža i prenosivih medija sa podacima. Za cilj imaju narušavanje integriteta, poverljivosti i dostupnosti podataka. Motiv za zarazu može biti nanošenje nematerijalne štete – npr. dokaz da je tvorac virusa sposoban da zarazi veliki broj računara – kao i materijalne štete – npr. iznuda (virus enkriptuje podatke i traži novčanu uplatu da bi te podatke dekriptovao), korporativna sabotaža (npr. Stuxnet), špijunaža, itd. Postoje razna softverska rešenja za borbu protiv zaraza sa računarskim virusima. Neka od njih su čak i besplatna za upotrebu. Međutim, pored tehničkih rešenja borbe protiv računarskih virusa, neophodno je i adekvatno ponašanje od strane korisnika kako do pojave virusa ne bi ni došlo. Dobar, osmišljen i održavan antivirusni program će reagovati na propisan način, u skoro svim slučajevima. Ali ne i u svim. Napadi poznati kao napadi nultog dana („0-day attacks“) se teško odbranjuju i od strane najboljih rešenja. Međutim, ako korisnik ima osnovnu svest i adekvatno znanje iz oblasti zaštite podataka, tada će on primeniti sve preventivne mere koje će smanjiti izloženost na virusne napade na najmanji mogući nivo – neće se pokretati programi nepoznatog porekla, atačmenti nepoznatog pošiljaoca se neće otvarati, itd.

U 2000. godini, ukupan broj registrovanih računarskih virusa u svetu iznosio je oko 50.000, u 2005. godini preko 100.000, a u 2008. godini preko 1.000.000.



Slika 1. Broj virusa u svetu konstantno raste

Dok se u svetu primećuje trend konstantnog rasta broja virusa, u jednoj od banaka u Srbiji evidentira se sve manji broj virusa u njihovom informacionom sistemu. U toj banci redovno se održavaju IT bezbednosne obuke zaposlenima, godišnje barem jedanput, a po potrebi organizuju se i vanredne obuke. Naravno, implementirana su i razna tehnička rešenja za borbu protiv virusa, ali ponašanje zaposlenih po pitanju upotrebe interneta, sistema elektronske pošte i prenosivih medija sa podacima su od ključnog značaja. Nijedan sistem se neće uspešno odbraniti ako je konstantno bombardovan raznoraznim napadima.



Slika 2. Broj virusa u jednoj srpskoj banci opada

5. Zaključak

IT bezbednosna obuka kao preventivna zaštita podataka jeste od ključnog značaja, kako za korisnike, tako i za poslovne procese. Obuka mora biti ciklična i kontinuirana. Korisnicima treba da je jasno da oni predstavljaju prvu liniju odbrane u zaštiti podataka od kriminalnih delatnosti, koji mogu biti rezultat internih, eksternih i kombinovanih zloupotreba sa ciljem narušavanja poverljivosti, integriteta i dostupnosti podataka. IT bezbednosna obuka korisnika predstavlja prvi vid preventivne zaštite.

LITERATURA

Informatikai Tárcaközi Bizottság ajánlásai, Informatikai Koordinációs Iroda, Miniszterelnöki Hivatal, http://www.itb.hu/ajanlasok/a8/, posledniji put pristupano 9. 5. 2012.

Mitnick, D. K., Simon, L. V. (2003). *A megtévesztés művészete, Perfact-Pro Kft.* Budapest.

Mitnick, D. K., Simon, L. V. (2006). *A behatolás művészete, Perfact-Pro Kft.* Budapest.

Number of Viruses, http://www.cknow.com/cms/vtutor/number-of-viruses.html, posledniji put pristupano 7. 5. 2012.

Viktor Kanižai, M. A.

IT SECURITY TRAINING AS PREVENTIVE DATA PROTECTION

Summary

The rapid development of Information Technology (IT) has enabled a variety of benefits to mankind in the field of communications, data processing, business, and others. Today there is almost no company that does not use a computer in the course of its business, either as support or as a basic process of carrying out its activities. Individuals are also using IT solutions in their daily lives, a computer to facilitate knowledge acquisition, execution of work or playing games, mobile phone as a basic resource for communication, etc. However, with the development of IT, ie. increasing the functionality of IT, there is also the development of methods of carrying out fraud and abusing these technologies, which can often lead to direct material damage, both for individuals and for companies. The weakest link in terms of attacks on IT, is the user, but the user also represents the first line of defense. IT security training is the first preventive aspect of data protection and IT security.

Key words: IT security, data protection, security training.