HRVATSKO DRUŠTVO INŽENJERA SIGURNOSTI

VISOKA ŠKOLA ZA SIGURNOST

s pravom javnosti

ZBORNIK RADOVA

VII. ZNANSTVENO-STRUČNE KONFERENCIJE S MEĐUNARODNIM SUDJELOVANJEM

MENADŽMENT I SIGURNOST

UPRAVLJANJE LJUDSKIM RESURSIMA I SIGURNOST

HRVATSKO DRUŠTVO INŽENJERA SIGURNOSTI
CROATIAN SOCIETY OF SAFETY ENGINEERS
www.safety.hr

VISOKA ŠKOLA ZA SIGURNOST
s pravom javnosti
UNIVERSITY COLLEGE OF APPLIED SCIENCES IN SAFETY
accredited
www.vss.hr

VII. ZNANSTVENO-STRUČNA KONFERENCIJA S MEĐUNARODNIM SUDJELOVANJEM
THE 7th SCIENTIFIC AND PROFESSIONAL CONFERENCE WITH INTERNATIONAL PARTICIPATION

MENADŽMENT I SIGURNOST
MANAGEMENT AND SAFETY

TEMA KONFERENCIJE: **UPRAVLJANJE LJUDSKIM RESURSIMA I SIGURNOST**
CONFERENCE THEME: **HUMAN RESOURCE MANAGEMENT AND SAFETY**

PROGRAMSKI CIKLUS: **OSNOVNE FUNKCIJE MENADŽMENTA I SIGURNOST**
PROGRAM CYCLE: **BASIC MANAGEMENT FUNCTIONS AND SAFETY**

Čakovec, Toplice Sveti Martin, Međimurje, Hrvatska
Cakovec, Spa Sveti Martin, Medjimurje, Croatia

Spa & Sport Resort Sveti Martin
www.toplicesvetimartin.hr

14.-15.6.2012.

Urednik
mr. sc. Josip Taradi, mr. sig.

Tematska urednica
prof. dr. sc. Vesna Nikolić

Tehnički urednik
Antun Matija Filipović, bacc. ing. sec.

Oblikovanje omota
Antun Matija Filipović, bacc. ing. sec.

Nakladnik
Hrvatsko društvo inženjera sigurnosti
Zagreb, Valentina Vodnika 19
www.safety.hr

Za nakladnika
mr. sig. Liljana Dolšak

Naklada
200 primjeraka

Tisak
Promel d.o.o.

Recenzije radova proveli su članovi Programskog odbora.

Odgovornost za stručnu i jezičnu ispravnost teksta preuzeli su autori.

CIP - Katalogizacija u publikaciji
Nacionalna i sveučilišna knjižnica - Zagreb
UDK/UDC 005.96:614.8(063)

Grupa autora
Zbornik radova: VII. Znanstveno-stručna konferencija s međunarodnim sudjelovanjem "Menadžment i sigurnost" Tema konferencije: "Upravljanje ljudskim resursima i sigurnost" / Čakovec: Hrvatsko društvo inženjera sigurnosti : Visoka škola za sigurnost, 2012. - 796 str.: ilustr.: 29 cm

ISSN 1848-5251

ORGANIZATORI

HRVATSKO DRUŠTVO INŽENJERA SIGURNOSTI
www.safety.hr

VISOKA ŠKOLA ZA SIGURNOST s pravom javnosti
www.vss.hr

MENADŽMENT KONFERENCIJE

prof. dr. sc. Vesna Nikolić
Predsjednica Programskog odbora
vesna.nikolic@znrfak.ni.ac.rs

Antun Matija Filipović, bacc. ing. sec.
Predsjednik Organizacijskog odbora
antun.matija.filipovic@vss.hr

mr. sc. Josip Taradi, mr. sig.
Tajnik Konferencije
ms2012@safety.hr

PROGRAMSKI ODBOR

prof. dr. sc. Vesna Nikolić (Srbija), Predsjednica Programskog odbora

Članovi Programskog odbora (abecedni redoslijed):
prof. dr. sc. Vesna Dušak (Hrvatska), Mahir Hodžić, dipl. krim. (Bosna i Hercegovina), prof. dr. sc. Želimir Kešetović (Srbija), prof. dr. sc. Ksenija Klasić (Hrvatska), prof. dr. sc Zdravko Krakar (Hrvatska), prof. dr. sc. Mirko Markič (Slovenija), mr. sig. Sanja Miketić-Curman (Hrvatska), mr. sc. Perica Miletić (Srbija), prof. dr. sc. Elmedin Muratbegović (Bosna i Hercegovina), mr. sc. Darko Palačić (Hrvatska), mr. sig. Miran Pavlič (Slovenija), prof. dr. sc. Suzana Savić (Srbija), prof. dr. sc. Dragan Spasić (Srbija), prof. dr. sc. Miomir Stanković (Srbija), mr. sc. Josip Taradi (Hrvatska), Ivana Varičak, dipl. oec. (Hrvatska), mr. sig. Leon Vedenik (Slovenija), Nikolina Vojak, univ. spec. oec. (Hrvatska), prof. dr. sc. Branko Wasserbauer (Hrvatska), prof. dr. sc. Snežana Živković (Srbija).

ORGANIZACIJSKI ODBOR

Antun Matija Filipović, bacc. ing. sec. (Hrvatska), Predsjednik Organizacijskog odbora

Članovi Organizacijskog odbora (abecedni redoslijed):
mr. sig. Liljana Dolšak, Ksenija Jovanović, Anton Kalačić, Željka Lalić, Nikica Petričević, struč. spec. ing. sec., Hrvoje Plazonić, Dino Pleić, Sandra Sabljak, Mario Štimac, Neven Taradi, dipl. ing. sig., Jelena Vuk, bacc. ing. sec., Mile Žarak, struč. spec. ing. sec.
(Hrvatska)

Hrvatski jezik
UDK/UDC 005.96:004.056
Stručni članak/Professional paper

Nikola Protrka, Kristijan Marić, Krešimir Buntak

CYBER-KRIMINAL U TVRTKAMA I ULOGA LJUDSKIH RESURSA U PREVENCIJI

Sažetak

Poslovanje poslovnog sustava se prvenstveno oslanja na ljudske resurse, te u značajnijoj mjeri na informatičko-komunikacijsku tehnologiju (ICT). Osim niza prednosti nad konkurencijom koje se mogu ostvariti korištenjem suvremene informatičke tehnologije, evidentni su i rizici što dokazuju sve učestaliji primjeri kompjutorskog kriminala počinjenog od ljudi unutar organizacije (insideri), odnosno van organizacije (outsideri) kao i konkurencije. Tvrtke moraju u obzir uzeti i ljudski faktor, a pitanje sigurnosti promatrati kao proces. Velika prijetnja u zadnje vrijeme je i pojava društvenih mreža kao što je Facebook, zbog odavanja kako osobnih, tako i poslovnih podataka. U Narodnim novinama br. 125 od 7. studenog 2011. objavljen je novi Kazneni zakon koji stupa na snagu dana 1. siječnja 2013., u kojem postoji osam novih članaka koji se isključivo bave kaznenim djelima iz područja cyber-kriminaliteta.

Ključne riječi: kibernetički kriminal, digitalni dokazi, društvene mreže, informacijska tehnologija, ljudski potencijal.

CYBER-CRIME IN COMPANIES AND THE ROLE OF HUMAN RESOURCES IN PREVENTION

Abstract

Business of every business system relies primarily on human resources, and to a significant level of activity on information and communication technology (ICT). In addition to a number of advantages over competitors that can be achieved by using modern information technology, the risks are evident and are proved by common examples of computer crime committed by people within the organization (insiders), or outside the organization (outsiders) or competition. Companies must take into account the human factor and safety issue viewed as a process. Lately, one major threat is the emerging of social networks such as Facebook, due to disclosure of personal, and business data. In the Official Gazette no. 125 of 7 November 2011. , the new Penal Code which comes into force on 1 January 2013., presents eight new articles dealing exclusively with criminal offenses in the field of cyber-crime.

Keywords: cybercrime, digital evidence, human resources, information technology, social networks.

UVOD

U posljednje vrijeme javnost je bila svjedokom bankrota ili značajnih financijskih gubitaka niza tvrtki, kao i reputacijskih, što je često još važnije,. Ono što je zajedničko mnogim slučajevima jest da je do financijskih gubitaka došlo zbog nezakonitog korištenja kompjutorske opreme tj. radilo se o kompjutorskom kriminalitetu. U posljednjih desetak godina, informatička dostignuća su ne samo izmijenila društvo, nego prirodu i metodologiju određenih tipova kriminalnih radnji. Na žalost, reakcija onih koji bi morali učiniti više na prevenciji i suzbijanju ovih zločina nije uvijek bila adekvatna.

Različiti su tipovi aktivnosti iz domene kompjutorskog kriminaliteta: neovlašteni pristup podacima, neovlaštena ili nedopuštena izmjena podataka i programskog koda, neovlašteno ili nedopušteno korištenje aplikacija, programsko piratstvo (*software piracy*), virusi, onemogućavanje rada računalne opreme (*denial of service*), fizičko uništavanje računalne i komunikacijske opreme, itd. Za definiciju obrambenih pristupa je neophodno razumijevanje različitih tipova kompjutorskog kriminaliteta. Strategija za obranu od jednog tipa napada ne mora biti prikladna za sve ostale.

Stručnjaci za sigurnost kompjutorskih sustava slažu se da se prijavi svega 15% od svih počinjenih kriminalnih radnji. Ostale nedopuštene radnje ili prođu nezapaženo zbog nedovoljno kvalitetnih operativnih kontrolnih mehanizma i lošeg rada internih kontrola i/ili menadžmenta, ili budu uočene, ali ih organizacije rješavaju "u tišini" ne prijavljujući slučaj nadležnim organima zbog toga što menadžment ne želi izložiti organizaciju negativnom publicitetu, ili treći razlog da neopuštene radnje budu uočene, ali se ne radi na unapređenju sigurnosnih mjera zbog loše procjene i evaluacije rizika zbog nerazumijevanja i/ili nespremnost menadžmenta da se ulože odgovarajući resursi s ciljem implementacije sigurnosnih/obrambenih mehanizama.

INFORMACIJSKA TEHNOLOGIJA

Protok velikih količina informacija među informacijskim sustavima otvara informacijske sustave zlonamjernim napadima neovlaštenih korisnika. Napadači prodiru u informacijske sustave uzrokujući velike štete cjelokupnom poslovanju organizacije. Unutar samih organizacija, zaposlenici su putem računala spojeni direktno na Internet, što otvara mogućnosti namjernih i nenamjernih otkrivanja povjerljivih podataka kao i otvaranja potencijalnih sigurnosnih ranjivosti sustava. Uzrok tome je često neupućenost, nedovoljna obrazovanost o problemima sigurnosti informacijskih sustava, ili jednostavno nepažnja.

Brzim razvojem informacijskih tehnologija okruženje informacijskih sustava se u velikoj mjeri mijenja. Upotrebom operacijskih sustava opće namjene i distribuiranog procesiranja, te proširenjem izvora pristupa sustavu dodatno se povećavaju i izvori potencijalnih ranjivosti sustava. Kao rezultat ovih pojava, organizacije prepoznaju potrebu za implementiranjem i dokumentiranjem sustava upravljanja sigurnošću informacija.

Sustav upravljanja sigurnošću informacija može se jednostavno protumačiti kao sigurnosna mjera kojom se smanjuju mogućnosti napadača, bilo vanjskog ili unutarnjeg. Sustav upravljanja sigurnošću informacija je jednako tako i sredstvo pomoću kojeg više poslovodstvo organizacije prati i nadzire sigurnost informacijskih sustava organizacije, svodeći poslovni rizik na minimum i osiguravajući da sigurnosni zahtjevi poslovanja ispunjavaju korporacijske i pravne obveze.

Norma ISO/IEC 17799 predstavlja široki spektar smjernica za implementaciju sigurnosnih kontrola, te pokriva sigurnosne politike, pravne, organizacijske, fizičke i ljudske komponente informacijskih sustava. Norma ISO/IEC 27001 predstavlja specifikaciju s postupcima korištenja i implementiranja sustava upravljanja sigurnošću informacija, dajući pri tome upute što je sve potrebno napraviti kako bi se uspostavila prihvatljiva razina informacijske sigurnosti.

Sigurnosni zahtjevi svake organizacije dolaze iz tri glavna izvora:

- prijetnje i ranjivosti koje mogu rezultirati velikim gubicima ako se realiziraju,
- zakonski i ugovorni zahtjevi,
- svi principi, ciljevi i zahtjevi organizacije na koje se oslanjaju poslovni procesi, a koji
- se odnose na informacijske sustave organizacije.

Prilikom procjene vrijednosti resursa potrebno je razmotriti ove zahtjeve i formulirati ih u skladu s zahtjevima povjerljivosti, integriteta i raspoloživosti.

RAČUNALNI KRIMINALITET (CYBERCRIME)

Izmjenama Kaznenog zakona i njegovim usuglašavanjem s europskom Konvencijom o kibernetičkom kriminalitetu, Hrvatska je dobila nova, kvalitetna, premda još uvijek ne i potpuna zakonska rješenja u ovom području.

Najvažnija novina u Kaznenom zakonu je njegovo usuglašavanje sa obavezama preuzetim potpisivanjem *Konvencije o kibernetičkom kriminalitetu* Vijeća Europe (NN-MU 9/02, 4/04). Radi se o do sada najvećem, najopsežnijem ali i najkvalitetnijem europskom dokumentu o takvoj vrsti kriminaliteta, koju su potpisale i neke ne-europske informatičke velesile, prvenstveno Sjedinjene američke države, Kanada i Japan.

Konvencija je svečano potpisana 23. studenog 2001. u Budimpešti, te je predstavljena kao međunarodno pravni instrument kojim se po prvi put reguliraju problemi vezani uz korištenje i prijenos informacija i podataka preko informatičkih i telekomunikacijskih sustava. Upravo se zato i zove Konvencija o kibernetičkom, a ne računalnom kriminalu. Prema jednoj od definicija, kibernetički kriminal obuhvaća sva kaznena djela počinjena unutar kibernetičkog prostora, popularnog cyberspace-a, uz pomoć ili na samoj informatičkoj i telekomunikacijskoj tehnologiji, koja čini njegovu infrastrukturu.

Temeljnu infrastrukturu cyberspace-a čini Internet, koji svojom globalnošću, otvorenošću, dostupnošću postaje izvorom sve većih i opasnijih zloupotreba, a borba protiv takvih zlouputreba zahtjeva čvrstu međunarodnu suradnju.

Velika reforma hrvatskog kaznenog zakonodavstva 1997. prvi put je uvela računalni kriminal, i to u članku 223. KZ-a, kazneno djelo Oštećenje i uporaba tuđih podataka. Republika Hrvatska je Konvenciju o kibernetičkom kriminalitetu potpisala 23. studenog 2001., a obveze koje su time preuzete odnosile su se na izmjenu Kaznenog zakona u koji je trebalo unijeti nova kaznena djela, i to nezakoniti pristup, nezakonito presretanje, ometanje podataka, ometanje sustava, zloporaba naprava, računalno krivotvorenje, računalnu prijevaru, djela povezana uz dječju pornografiju i autorska prava, u slučajevima kada se računala i internet koriste za kažnjivu radnju. Najveća intervencija bila je u spomenutom članku 223. KZ-a.

Inkriminirane su nove zloupotrebe, tako da su sada, uz "oštećenje, izmjenu, brisanje, uništenje ili druge načine zlouporabe podataka" koji ih čine neuporabljivim, kažnjivi i svi načini kojima se oni čine *nedostupnima*. Ta je novost posebno bitna u situacijama u kojima podaci nisu izbrisani ili oštećeni, ali im se ne može pristupiti zbog djelovanja malicioznih programa, prvenstveno virusa, crva i trojanskih konja ili popularni DDOS napadi kojima smo svjedoci u zadnje vrijeme od skupine koja se naziva Anonymous. Time se napokon programima i podacima osigurava jednaka zaštita kao i materijalnim predmetima. Naime, do sada se krađa računalnih podataka nije smatrala krađom, jer podaci nisu fizički ukradeni iz računala. Činjenicu da su prekopirani i dostupni drugima zakon nije uvažavao.

Stavak 3. članka 223. KZ-a sankcionira *"onemogućavanje ili otežavanje rada ili korištenja"* računala ili računalne komunikacije, prvenstveno kao još jedan način kažnjavanja izrade i prijenosa malicioznih programa, ali i sve druge načine uskraćivanja usluga, tzv. Denial of Service (DoS) napada. Interpretacija ove norme daje i mogućnost kažnjavanja tzv. *spamminga* (eng. *Spam* – neželjena pošta), slanja velikog broja e-mail poruka s namjerom zagušenja servera ili računala primatelja, uslijed kojeg sustav prestaje raditi.

Predviđena sankcija za sva navedena djela je novčana kazna ili kazna zatvora do tri godine. To nas dovodi do druge bitne novosti, povećanja sankcija za počinitelje, koje se sada i razlikuju ovisno o tome je li kazneno djelo počinjeno na privatnom računalu (novčana kazna ili kazna zatvora do tri godine) ili "računalu, sustavu, podatku ili programu tijela državne vlasti, javne ustanove ili trgovačkog društva od posebnog javnog interesa", u kojem slučaju je sankcija isključivo kazna zatvora, od tri mjeseca do pet godina.

Osim nabrojanih intervencija u članku 223. KZ-a, uvedena su i dva potpuno nova kaznena djela, *računalno krivotvorenje* i *računalna prijevara*. Svrhu inkriminiranja računalnog krivotvorenja ne treba posebno objašnjavati.

U Narodnim novinama br. 125 od 7. studenog 2011. objavljen je novi Kazneni zakon koji u glavi XXIII u člancima od 266.-273. donosi izmjene postojećeg Kaznenog zakona, a koji članci se bave isključivo kaznenim djelima iz područja cyber-kriminaliteta.

Popis članaka koji će stupiti na snagu dana 1. siječnja 2013.:

- Članak 266. Neovlašteni pristup
- Članak 267. Ometanje rada računalnog sustava
- Članak 268. Oštećenje računalnih podataka
- Članak 269. Neovlašteno presretanje računalnih podataka
- Članak 270. Računalno krivotvorenje
- Članak 271. Računalna prijevara
- Članak 272. Zloporaba naprava
- Članak 273. Teška kaznena djela protiv računalnih sustava, programa i podataka

Iako Republika Hrvatska prati suvremene pravne trendove na području kibernetičkog kriminala, brzina kojom se on razvija zahtjeva stalne prilagodbe kako bi zakon pratio promjene u virtualnom svijetu.

PREDUVJETI POTREBNI ZA CYBERCRIME

Četiri su osnovna preduvjeta koja moraju biti ispunjena da bi potencijalni počinitelj izvršio kriminalnu radnju:

- motiv
- sposobnost
- prigoda
- pristup do imovine

U današnjem svijetu Interneta i dostupnosti ogromne količine informacija, nema smisla razmatranje da li uopće postoji motiv da bi napadač počinio kriminalnu radnju. Zabilježeni su brojni slučajevi u kojima je motiv napadača bio isključivo zabava ili iskušavanje vlastitih sposobnosti, ali su zapravo počinjene štete koje često nije moguće jednostavno izmjeriti.

Prema tome, ostaju tri pretpostavke: sposobnost, prigoda i pristup do imovine. Menadžment mora učiniti sve što je moguće kako bi se preventivno djelovalo s ciljem da sve tri pretpostavke ne postanu dostupne jednoj osobi. Na nesreću, neki tipovi kompjutorskog kriminala, mogu zahtijevati ispunjenje samo jedne ili dviju pretpostavki.

Nadalje, broj ljudi koji imaju sposobnost i znanja za počiniti određeni kriminalni čin je obrnuto proporcionalan neophodnim vještinama. Na primjer, ako kriminalni čin zahtjeva znanje programiranja, manji je broj potencijalnih počinitelja. Također, za krađu osobnog, a posebno prijenosnog, računala je potencijalni broj počinitelja veći zbog manje potrebnih vještina i znanja.

Pojednostavljeno, svaki računalni sustav se sastoji od tri komponente: ulaza - priprema i unos podataka, obrade podataka i izlaza - kreiranje izvješća. Većina kriminalnih radnji se događa u području ulaza i izlaza jer:

1. za to uglavnom nije potreban visok nivo znanja,
2. zbog 1. relativno veći broj osoba posjeduje ove znanja,
3. veći broj osoba ima prigodu i sposobnost za počiniti ovakve radnje zbog nedostatka principa razdvajanja dužnosti (segregation of duties) što je posljedica intenzivnijeg korištenja on-line rada i nedovoljnog razumijevanja ove problematike od strane menadžmenta.

Menadžment je dužan voditi brigu o ljudskim potencijalima, a tu podrazumijevamo ukupnu intelektualnu i psihofizičku energiju koju tvrtka može organizirati u ostvarenju svojih poslovnih i razvojnih ciljeva, te zaštiti svoje najvrednije imovine, a to su podaci. Menadžment mora biti sposoban uočiti bitne razlike svih ljudi i iskoristiti (usmjeriti) sve njihove snage prema dobrobiti tvrtke.

DIGITALNI DOKAZI

Analiza podataka i forenzika su ulazna vrata u polje računalnog kriminaliteta. Kao i u stvarnom svijetu, detektivi i forenzičari otkrivaju nove slučajeve računalnog kriminaliteta skoro svaki dan. Elektronički dokazi su osjetljivi, lako se brišu, mijenjaju i time kompromitiraju. S obzirom da se računalo može koristiti kao oruđe za počinjenje nedozvoljenih radnji, ono može, odnosno mora sadržavati barem dio dokaza.

Istražitelj koji sakuplja dokaze sa računala ili računalne mreže, mora znati pravila postupanja glede prikupljanja tih podataka, jer, ako on sakupi te podatke nezakonito, ti se podaci neće moći koristiti u sudskom postupku. Pojam digitalni dokazi koristi se u američkom zakonodavstvu i označava bilo koji računalni podatak koji može potvrditi da je počinjeno kazneno djelo, ili koji može ukazati na povezanost između zločina i žrtve, ili zločina i njegovog počinitelja.

Elektronički dokazi su vrlo važni, jer predstavljaju kombinaciju različitih informacija poput teksta, slike, audio i video snimke. Ponekad informacija koja je pohranjena na računalu može biti jedini trag koji će kriminalističko istraživanje dovesti na pravi put. Postoji cijeli niz elektroničkih dokaza koji nas okružuju u našem svakodnevnom životu, a kojih smo skoro u potpunosti nesvjesni. Tvrdi disk može sadržavati cijelu biblioteku informacija, digitalna kamera u svojoj memoriji može pohraniti tisuće fotografija, a računalna mreža može sadržavati još više informacija o osobama i njihovom ponašanju. Brojevi bankovnih računa, novčane transakcije, povjerljivi dokumenti i drugi različiti podaci putuju oko nas kroz zrak ili putem žičnih vodova, a svaki od njih predstavlja potencijalni izvor elektroničkog dokaza. Forenzika osigurava načela i tehnike koje omogućuju kriminalističko istraživanje i progon počinitelja računalnog kriminaliteta. Općenito gledajući, forenzika je primjena pravnih znanosti i drugih znanstvenih procesa i tehnika koje se mogu iskoristiti u identifikaciji, povratku, rekonstrukciji ili analizi dokaza tijekom kriminalističke istrage. Forenzičari pokušavaju uz pomoć elektroničkih dokaza rekonstruirati događaj te ga približiti i na taj način pojasniti istražiteljima.

Načelom "ledenog brijega" samo mali postotak elektroničkih dokaza moguće je otkriti "klasičnim alatima" kao što je Windows Explorer (alat za rad sa datotekama u operacijskom sustavu Windows). Ostatak elektroničkih dokaza moguće je otkriti samo posebnim alatima (bilo komercijalnim bilo freeware [eng. *Freeware* – besplatni alati]). Čak i onda kada su "obrisani" elektronički se dokazi mogu povratiti sa računalnog diska ili nekog drugog medija za pohranu podataka.

Elektroničke je dokaze jednostavno pohraniti, a zbog lakoće izrada kopija gotovo ih je nemoguće uništiti ili izgubiti. Zbog toga što se elektroničkim dokazima može lako manipulirati i prenositi ih, istražitelji koji se bave računalnim kriminalom nailaze na nove izazove u radu s ovakvom vrstom dokaza. Ti se dokazi nalaze svugdje oko nas. Računalne mreže u svom svakodnevnom radu uključuju cijeli niz procesa od telefonskih poziva, prijama i slanja elektroničke pošte, plaćanje računa i druge ostale pogodnosti, a što u biti predstavlja elektroničke dokaze. Sve te pogodnosti danas su dostupne svakom čovjeku iz sigurnosti i udobnosti njegova doma. Međutim, računalne mreže sa sobom donose i određeni rizik. Računalne mreže su široko uključene u kriminalni milje, koji uključuje dječju pornografiju, prijetnje, špijunažu, sabotaže, prijevare, uznemiravanje privatnosti itd.

Elektronički dokazi najvažniji su čimbenik onoga što danas poznajemo pod pojmom *cybercrime* ili kibernetički kriminal, a to je računalni kriminal. Ovaj se pojam koristi u označavanju kriminalnog djela u koje je uključeno računalo, računalna mreža, uključujući u sebe i kazneno djelo koje nije u potpunosti počinjeno na računalu. Ovaj se pojam koristi i za opise situacije u kojoj računalna mreža nije korištena u počinjenju kriminala, ali sadržava elektroničke dokaze povezane sa kriminalom. Iako nema direktan učinak na slučaj, računalo sadrži elektronički dokaz koji je vrlo važan za istraživanje. Ako je kriminalno djelo počinjeno u stvarnom fizičkom svijetu i ako postoji računalo sa mrežnim pristupom na mjestu počinjenja djela, istražitelji će učiniti pretraživanje računala i računalne mreže u potrazi za elektroničkim dokazima koji im mogu poslužiti u istraživanju. Slično tomu, ako je kriminalni čin zabilježen na računalu ili računalnoj mreži, kriminalistički istražitelji mogu utvrditi mjesto gdje se nalazi to računalo, te na taj način pokušati locirati mjesto počinjenja djela.

Ako su informacije i podaci koji se nalaze na računalu pravno relevantni, a istražitelji znaju što traže, bit će moguće u vrlo kratkom roku prikupiti potrebite dokaze, s druge strane ako istražitelji ne znaju što traže potrebno je proširiti opseg istraživanja i u nju uključiti svu računalnu opremu kako bi se prikupili i istražili materijali koji bi mogli poslužiti kao dokaz [1].

LJUDSKI FAKTOR KOD PRISTUPA RAČUNALNIM PODACIMA

Kada jedna osoba koristi identitet druge osobe s ciljem da na taj način pristupi računalnoj infrastrukturi govorimo o lažnom predstavljanju ili maskiranju. Sigurnosne metode koje koriste sustavi zaštite računalne infrastrukture moraju biti dovoljno aktivni kako bi otkrili i spriječili lažno predstavljanje.

Kada se govori o lažnom predstavljanju moramo razlikovati fizičku i elektroničku formu lažnog predstavljanja. O fizičkom predstavljanju govorimo kada korisnik koristi ovlašteni korisnički identitet ili pristupnu karticu kako bi pristupio povjerljivim područjima i stekao pristup računalnoj infrastrukturi i podacima. Za lažno predstavljanje kažemo da je elektroničko, kada korisnik u stvari koristiti legalni korisnički identifikacijski broj ili zaporku kako bi se prijavio u računalni sustav te na taj način nelegalno došao u posjed podataka i informacija.

Da bi se što bolje razumio način funkcioniranja lažnog predstavljanja potrebno je znati nekoliko temeljnih pojmova o načinu ostvarivanja korisničkog ulaska u računalni sustav. Korisnici ostvaruju ulazak u računalni sustav kroz dvostruki proces poznat kao identifikacija i potvrđivanje vjerodostojnosti. Identifikacija je način na koji korisnik govori računalnom sustavu tko je, te upisuje svoju korisničku zaporku ili osobni identifikacijski broj. Potvrđivanje vjerodostojnosti je način na koji korisnik dokazuje računalnom sustavu da je onaj za kojeg se predstavlja da je.

Poznajemo tri načina dokazivanja korisničkog identiteta, i to:

1. Nešto što osoba zna–uobičajen primjer je zaporka. Shvaćanje je ako osoba zna zaporku sigurno je i vlasnik korisničkog računa.
2. Nešto što osoba ima–primjeri su ključevi, pametne kartice ili druga tehnološka dostignuća u fizikom obliku, a u svrhu prijavljivanja i dokazivanja identiteta nositelja.
3. Nešto što osoba je ili radi–primjeri su psiho-fizičkih osobina ljudi, poput otiska prsta, glasa i sl.

Nažalost, postalo je uobičajeno za računalne počinitelje da kradu, pogađaju ili nekim drugim načinom (socijalni inženjering) osiguraju imena računa i zaporki. I kad se netko lažno predstavlja korisničkim imenom, on virtualno može činiti što god hoće. Ne samo da može ukrasti zapise osobe čiji identitet koristi veći ih može promijeniti ili trajno uništiti. Ono što je još pogubnije od samog mijenjanja ili uništavanja zapisa na računalu, činjenica je da se počinitelj može ″cijelom svijetu″ predstaviti kao legalni korisnik.

Postoje metode i aplikacije koje u programskoj podršci osiguravaju da onaj tko počini nešto unutar sustava bude otkriven, ali se radi o metodama koje su vrlo složene i za koje je potrebno dulje vrijeme. Danas sve veću ulogu u zaštiti od lažnog predstavljanja imaju biometrijske karakteristike i na njima zasnovani sigurnosni sustavi.

Upravljanje ljudskim resursima u sebi nerazdvojno ujedinjuje odlike koje imaju presudne i dugoročne efekte za poslovno ponašanje i uspješnost poduzeća i da ono treba polaziti od ostvarivanja strategijskih ciljeva i biti na njih usmjereno. Zapravo ističe ključnu ulogu ljudskih potencijala u oblikovanju i provedbi poslovne strategije, ali i utjecaj strategije na strategiju i programe upravljanja ljudskim potencijalima. Poslovna poduzeća imaju dvije vrste strategija koje moraju biti usko povezane: eksterna i interna.

- Eksterna strategija izabrani je način natjecanja, odnosno konkuriranja na tržištu.
- Interna strategija odnosi se na to kako razvijati, angažirati, usmjeravati, motivirati i kontrolirati unutarnje resurse.

Specifičnost ljudskih potencijala pri tome je da kvaliteta ljudi, njihove specifične sposobnosti, znanja i vještine presudno određuju i ograničavaju izbor vanjske, konkurentske strategije i njezinu uspješnu primjenu i da su mnogi programi upravljanja i razvoja ljudskih resursa, kao što su stalno obrazovanje i razvoj, motiviranje i nagrađivanje, u neposrednoj funkciji uspješnog provođenja strategije [2].

Oko šezdeset posto svih nedozvoljenih aktivnosti usmjerenih prema tvrtkama je počinjeno od ljudi unutar tvrtke, ili insidera. Ukoliko nedozvoljenu ili kriminalnu radnju počini menadžer, imamo veći gubitak, što je inače i rjeđi slučaj u praksi, dok nedozvoljenu radnju počini obični zaposlenik, manja je šteta jer su manja prava pristupa povjerljivim podacima. Najlošija varijanta za organizaciju je postojanje savezništva na različitim nivoima hijerarhije, gdje se insideri služe prikrivanjem.

SIGURNOSNA POLITIKA ORGANIZACIJE

Menadžeri i ostale odgovorne osobe moraju osigurati da svi zaposlenici organizacije budu upoznati sa sadržajem dokumenta sigurnosne politike i obvezom pridržavanja njegovih odredaba, te utvrditi odgovarajuće standarde, kontrolne mjere, te postupke kojima se osigurava pridržavanje svih zaposlenika organizacije politike informacijske sigurnosti.

Prilikom definiranja sigurnosne politika, naglašava se važnost postojanja dokumenta sigurnosne politike. Sigurnosna politika može biti dio opće politike organizacije, ne mora nužno predstavljati poseban dokument. Cilj sigurnosne politike je dati smjernice za upravljanje informacijskom sigurnošću u skladu s poslovnim zahtjevima organizacije i relevantnim zakonima i propisima. Uprava treba definirati jasnu sigurnosnu politiku koja je usklađena s ciljevima organizacije i koja pruža potporu informacijskoj sigurnosti na svim razinama organizacije.

Dokument sigurnosne politike treba sadržavati:

a) definiciju informacijske sigurnosti, njezine glavne ciljeve i opseg te važnost sigurnosti kao mehanizma koji omogućuje dijeljenje informacija;
b) izjavu o namjerama uprave koje će podupirati ciljeve informacijske sigurnosti u skladu s poslovnom strategijom;
c) okvir za uvođenje kontrola, kao i strukturu procjene rizika i upravljanja rizikom;
d) objašnjenje sigurnosne politike, principe, standarde i zahtjeve od posebnog interesa koje organizacija treba usvojiti, a to su:
    1. zakonski, pravni i ugovorni zahtjevi;
    2. edukacija o sigurnosti, svijest o sigurnosti i sigurnosni trening;
    3. upravljanje kontinuitetom poslovanja;
    4. posljedice narušavanja sigurnosne politike;
e) definiciju odgovornosti u procesu upravljanja sigurnošću, uključujući i prijavu sigurnosnih incidenata;
f) referencu na dokumente koji podupiru sigurnosnu politiku.

Sigurnosnu politiku je nužno provjeravati u unaprijed određenim intervalima, kako bi se osiguralo da sve relevantne promjene budu registrirane i uključene u sigurnosnu politiku. Cilj kontrole je dati smjernice za upravljanje informacijskom sigurnošću u skladu s poslovnim zahtjevima organizacije te relevantnim zakonima i propisima koje propisuje Vlada RH i Hrvatska akademska i istraživačka mreža CARNet.

ZAŠTITA POSLOVNIH I OSOBNIH PODATAKA NA DRUŠTVENIM MREŽAMA

Čovjekova želja za druženjem pronalazi uvijek nove načine interakcije koji, u sprezi s brzim razvojem novih tehnologija, definiraju društvenost na posve novi način. Facebook, trenutno najpopularnija društvena mreža, je ujedno najpopularnije mjesto za objavljivanja fotografija, s više od 14 milijuna novih dodanih fotografija dnevno, a znamo da danas gotovo svaki mobitel posjeduje kameru, te da se razni poslovni dokumenti, projekti, proizvodi i ostalo, jednim klikom kamere na mobilnom telefonu u sekundi nađe u bespućima Interneta, na dohvat ruke potencijalnoj konkurenciji. S rastom mreže, njezini korisnici dijele podatke s drugim stranama, pri čemu nisu svjesni da one uopće postoje, te ne vode računa koliko i koje informacije zaista žele podijeliti sa drugima. Sama društvena mreža Facebook imala je silovit uspon, te stekla veliku popularnost u malo vremena.

Tablica 1. Prikaz nastanka Facebook-a

veljača 2004.	počeci Facebooka na Harwardu
ožujak 2005.	ostvarena suradnja s tvrtkom Accel
kolovoz 2005.	registrirana domena Facebook.com

Izvor: vlastiti izvor

Tablica 2. Prikaz broja aktivnih korisnika Facebook-a

prosinac 2005.	5.5 milijuna korisnika
prosinac 2006.	12 milijuna korisnika
travanj 2007.	20 milijuna korisnika
kolovoz 2008.	100 milijuna korisnika
travanj 2009.	200 milijuna korisnika
rujan 2009.	300 milijuna korisnika
veljača 2010.	400 milijuna korisnika
srpanj 2010.	500 milijuna korisnika
siječanj 2011.	600 milijuna korisnika
svibanj 2011.	700 milijuna korisnika
rujan 2011.	800 milijuna korisnika

Izvor: Facebook, http://www.facebook.com (22.02.2012.)

Jedna od mogućnosti društvenih mreža, pa tako i Facebooka, je mogućnost kontrole privatnosti svakog korisnika. Prema vlastitim željama korisnik može sakriti svoj profil i fotografije od nepoznatih ljudi. Unatoč tome, Facebook se tijekom svog postojanja našao na meti brojnih kritičara upravo zbog problema privatnosti korisnika, ali također i zbog pitanja cenzure. Kritike dolaze i zbog toga što su informacije koje korisnici odaju o sebi korištene za marketinška istraživanja, interne istrage sveučilišta i organizacija, i naravno policije.

Neke od mogućih zlouporaba su:
· uzrokovanje štete ugledu organizacije ili osobe
· prepoznavanje osoba pomoću lica (iz fotografija)
· krađa potpomognuta informacijama prikupljenih s mreže
· krađa identiteta i lažno predstavljanje
· uhođenje (uključujući industrijsku špijunažu)

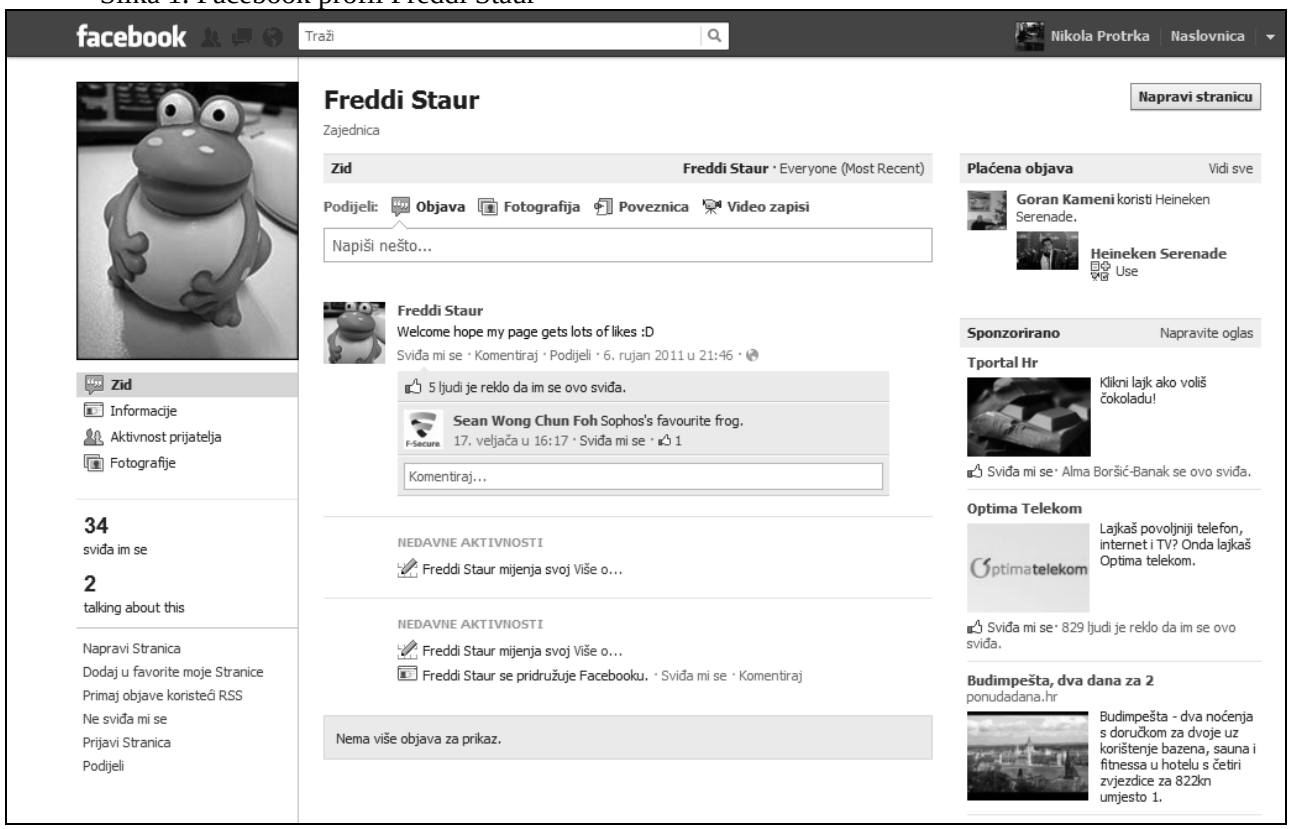
Postoje zabilježeni slučajevi gdje su zaposlenici ostali bez posla zbog neprimjerenih fotografija ili komentara o poslu koje je nažalost po njih pronašao njihov šef te ih očito nije „lajkao". Također se spominju slučajevi "bolovanja", dok zaposlenici stavljaju svoje slike iz kojih je vidljivo da nisu baš tako bolesni, kao što se čini iz dostavljene liječničke dokumentacije.

Istraživanje koje je provela sigurnosna tvrtka Sophos na uzorku od 200 nasumce odabranih korisničkih profila, pokazuje da veliki dio korisnika društvene mreže Facebook ne poštuje minimalne sigurnosne preporuke koje se odnose na zaštitu kako osobnih, tako i poslovnih podataka. Javnost mora biti upozorena, kao i organizacije čiji su zaposlenici korisnici društvenih mreža, kao što je Facebook, na opasnosti koje se kriju u dobivanju pristupa njihovim online profilima.

Facebook je internetski fenomen čija mreža trenutno broji skoro milijardu korisnika, te se svaki dan priključuju na tisuće i tisuće novih korisnika, no istraživanje Sophosa dokazalo je da oni ne postupaju oprezno sa svojim privatnim podacima koji mogu predstavljati sigurnosni rizik za njih i za organizaciju za koju rade.

Djelatnici tvrtke Sophos izradili su Facebook profil sa imenom Freddi Staur (anagram od "ID Fraudster", što znači prevarant) i stavili sliku male plastične igračke u obliku žabe, te je zahtjev za prijateljstvo je poslan na 200 nasumce odabranih Facebook profila. 82 korisnika Facebooka je odmah dodalo korisnika Freddi u prijatelje i omogućilo uvid u svoje osobne podatke.

Slika 1. Facebook profil Freddi Staur



Izvor: http://www.facebook.com/pages/Freddi-Staur/267770809909220?sk=wall (22.2.2012.)

Tablica 3. Analiza uzorka od 200 korisnika Facebook-a

Broj korisnika	Postotak	Uvid u podatke korisnika
87	43.5%	odgovorilo na zahtjev za prijateljstvo
82	41%	dopustilo pristup svojim osobnim podacima
144	72%	otkrilo adresu e-pošte
168	84%	naveden puni datum rođenja
174	87%	detalji o obrazovanju ili radnom mjestu
156	78%	trenutna adresa ili mjesto boravka
46	23%	trenutni broj telefona
52	26%	korisničko ime za IM servise (MSN, Skype, Gtalk…)

Izvor: Sophos, http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx (22.02.2012.)

Nadalje, bockano je još 100 nasumce odabranih korisnika, od kojih je 8 korisnika odmah dodalo korisnika Freddi u prijatelje, a od tih osam, pet korisnika je dopustilo pristup svojim osobnim podacima.

U većini slučajeva, Freddi je bio u mogućnosti pristupiti fotografijama obitelji i prijatelja, statusu osobe (bračno stanje i slično), hobijima, detaljima poslodavca i ostalim osobnim podacima. Osim toga, mnogi korisnici također objavljuju imena svojih supružnika ili partnera, nekoliko korisnika navodi svoju biografiju, dok jedan korisnik otkriva čak i majčino djevojačko prezime.

Sve te informacije služe nam da pomoću socijalnog inženjeringa saznamo pojedinosti osobi, a sami time i podatke o korisničkom računu. Kao i kod prihvaćenih zahtjeva za prijateljstvo, određeni broj korisnika nesvjesno omogućava pristup svojim podacima slanjem poruke na zahtjev za prijateljstvo kao što su "Tko si ti?" i "Da li se znamo?".

Zanimljivo je kako su mnogi korisnici savršeno spremni da se sprijatelje s korisnikom Freddi iako o njemu ne znaju ništa.

Navedeno istraživanje pokazuje da je 41% korisnika Facebook-a spremno odati osobne ili poslovne podatke potpunom strancu. Svi ti podaci omogućuju potencijalnom zlonamjernom napadaču izraditi e-mail za phishing ili malware, specifično ciljajući individualne ili poslovne korisnike, olakšavaju mu pogađanje korisničkih lozinki, omogućuju praćenje korisnika i/ili krađu identiteta.

Facebook opcije zaštite privatnosti korisnika su napredne u odnosu na neke druge društvene mreže, no korisnici ih rijetko koriste i tako dovode u opasnost svoju privatnost i ugled organizacije za koju rade. Većina ljudi ne bi dala svoje podatke strancu na ulici, ili čak odgovorilo na spam e-pošte, ali nekoliko korisnika koje je kontaktirao korisnik Freddi, otišlo je toliko daleko da ga je jedan od korisnika naveo kao najboljeg prijatelja.

Ukratko opće sigurnosne preporuke pri korištenju društvenih mreža su:

- Koristite napredne postavke za zaštitu privatnosti.
- Dvaput razmislite i provjerite kome ćete dopustiti da Vam postane prijatelj.
- Koristite ograničeni profil "limited profile" za prikazivanje skraćene verzije Vašeg profila.
- Isključite sve opcije, a potom ih jednu po jednu uključite po potrebi.

ZAKLJUČAK

Poslovanje svakog ozbiljnog poslovnog sustava se prvenstveno oslanja na ljudske resurse, te u značajnijoj mjeri na informatičko-komunikacijsku tehnologiju (ICT). Osim niza prednosti nad konkurencijom koje se mogu ostvariti korištenjem suvremene informatičke tehnologije, evidentni su i rizici što dokazuju sve učestaliji primjeri kompjutorskog kriminala počinjenog od ljudi unutar organizacije (insideri) i konkurencije, odnosno van organizacije (outsideri). Tvrtke moraju u obzir uzeti i ljudski faktor, a pitanje sigurnosti promatrati kao proces.

Da bi borba protiv kompjutorskog kriminala bila učinkovitija, mora se unaprijediti rad internih i eksternih kontrola, a menadžment mora shvatiti da je neophodna njegova aktivna podrška i sudjelovanje u analizi rizika te definiranju adekvatnih kontrolnih mehanizama.

Mnoge organizacije su na svojim mrežama zabranile pristup društvenim mrežama svojim zaposlenicima zbog neproduktivnosti, dok su nekim organizacijama društvene mreže poslovna prednost sa svojim načinom interakcije, stoga je važno da se takve mreže koriste razumno i sigurno, sukladno sa sigurnosnom politikom organizacije.

Uz zabrinutost zbog dijeljenja osjetljivih podataka, organizacije su zabrinute i zbog objavljivanja tekstova i objavljivanja fotografija i video snimaka koji štete ugledu organizacije. Iako se stranice društvenih mreža mogu koristiti za legitimne poslovne svrhe, IT administratori morali bi imati opciju odlučiti da li je pristup takvim društvenim mrežama dopustiv u okvirima propisane sigurnosne organizacijske politike.

Za napomenuti je da velika većina korisnika društvenih mreža ne zna obrisati svoj korisnički račun nakon što se više ne želi koristiti uslugama društvenih mreža, nego većinom samo deaktiviraju svoj račun, pri čemu svi tekstovi, fotografije i sve ostalo ostaje trajno dostupno na serveru. Na kraju, neke društvene mreže uopće ne nude mogućnost brisanja svojih korisničkih profila!

LITERATURA

[1] Ashcroft, J., Deborah, J. D., Sarah, V. H.: **Forensic Examination of Digital Evidence: A Guide for Law Enforcment**. Washington: U.S. Department of Justice, 2004.

[2] Baker S.: **The Numerati**. Montclair, New Jersey. Houghton Mifflin Company, 2008.

[3] Ivandić Vidović D., Karlović L., Ostojić A.: **Korporativna sigurnost**. Zagreb, Agencija za komercijalnu djelatnost, 2011.

[4] Mason, S.: **International electronic evidence**. London: British Institute of International and Comparative Law, 2008.

[5] Pavišić B., Modly D. Veić P.: **Kriminalistika knjiga 2**. Rijeka, Dušević & Kršovnik, 2012, 615-623.

[6] Protrka, N.: **Računalna forenzička analiza**. Varaždin, Fakultet organizacije i informatike, 2009.

[7] Protrka, N.: **Računalni podaci kao elektronički (digitalni) dokazi**. Zagreb. Policija i sigurnost 1, 2011.

[8] Reyes, A., Brittson, R., O'Shea, K., Steel, J.: **Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors**. Rockland: Syngress Publishing Inc. 2007.

[9] Tipurić, D.: **Konkurentska sposobnost poduzeća**. Zagreb : SINERGIJA, 1999.

Propisi

- Kazneni zakon, N.N., br. 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11, 125/11.
- Konvencija o kibernetičkom kriminalitetu, Vijeće Europe br. NN-MU 9/02, 4/04.

Norme

- Norma ISO/IEC 17799
- Norma ISO/IEC 27001

Internet

- International Organization for Standardization, http://www.iso.org (22.2.2012.)
- Jurman, D. *Internet – Kibernetički kriminal*, http://www.djurman.com/index.php (22.2.2012.)
- Sophos, http://www.sophos.com/en-us/press-office/press-releases/2007/08/facebook.aspx (22.2.2012.)

BIOGRAFIJA PRVOG AUTORA

Nikola Protrka, univ. spec. inf., struč. spec. crim.
Sveučilište u Zagrebu, Fakultet organizacije i informatike
Varaždin, Hrvatska
Policijska akademija
Zagreb, Hrvatska
vjestak@protrka.hr

Predavač na Policijskoj akademiji u Zagrebu. Završio specijalistički diplomski stručni studij kriminalistike – stuč.spec.crim. na Policijskoj akademiji u Zagrebu. Završio za sveučilišnog specijalista upravljanja sigurnošću i revizije informacijskih sustava – univ.spec.inf. na Sveučilištu u Zagrebu, Fakultetu organizacije i informatike u Varaždinu. Objavljeni članci u stručnim časopisima i knjigama u području računalne sigurnosti, zaštite osobnih i poslovnih podataka. Gost predavač na Veleučilištu VERN u predmetu Poslovna sigurnost i zaštita podataka. Stalni sudski vještak za informatiku na županijskim, trgovačkim i općinskim sudovima za područje cijele Republike Hrvatske. Tijekom zadnjih tri godine mentor na 70 završnih radova u izobrazbi odraslih za zanimanje policajac.

BIOGRAPHY OF THE FIRST AUTHOR

Nikola Protrka, univ.spec.inf., struč.spec.crim.
Teacher at the Police Academy in Zagreb. He completed specialist graduate professional study of criminology – professional specialist at the Police Academy in Zagreb. He graduated as a University specialist in information systems security management and auditing - univ.spec.inf. at the University of Zagreb, Faculty of Organization and Informatics in Varaždin. He published articles in professional journals and books in the field of computer security, protection of personal and business data. Guest lecturer at the University of Applied Sciences VERN in the Business security and data protection. Forensic expert of informatics at the county, commercial and municipal courts for the territory of the Republic of Croatia. Over the past three years, a mentor to 70 final works in adult education for the police profession.

PODACI O SUATORIMA (DATA ON CO-AUTHORS)

2)
Kristijan Marić, spec. oec.
Visoka poslovna škola Nikola Šubić Zrinski
Zagreb, Hrvatska
kristijan.maric@mf-creative.net

3)
prof. dr. sc. Krešimir Buntak
Državni zavod za mjeriteljstvo
Zagreb, Hrvatska
kresimir.buntak@dzm.hr