Darko Dundović

UDK 005.958 005.962:005.32 005.334:005.51

Pregledni rad / Review article

ZAPOSLENICI – MOGUĆA UNUTARNJA PRIJETNJA

Mr.sc. Darko Dundović,

INA d.d., Zagreb, R. Hrvatska

Sažetak

U radu se nastojalo definirati unutarnju prijetnju sa stajališta različitih autora ili organizacija. Namjera je sagledati unutarnju prijetnju prvenstveno u odnosu na zaposlenika kompanije, ali i drugih osoba koje imaju pristup kompanijskim podacima ili prostorima i na taj način mogu biti unutarnja prijetnja za kompaniju. Motivi i indikatori rizika također su se nastojali sagledati s tog stajališta. Pojava unutarnje prijetnje sagledana je kroz osnovne čimbenike koji mogu utjecati na pojavu unutarnje prijetnje, pa su tako analizirani osobni čimbenici, organizacijski čimbenici, kao i indikatori u ponašanju zaposlenika. Nastojalo se zadržati na osnovnoj razini objašnjenja ovih čimbenika bez detaljnog ulaženja u analizu, primjerice psihološkog profila pojedinih zaposlenika ili njihovog (kompulzivnog) ponašanja. Navedena su mjesta mogućeg nastanka štete u slučajevima ostvarenja unutarnje prijetnje, te je dan prikaz mjera za smanjenje ili rano otkrivanje moguće unutarnje prijetnje. Cilj rada bio je (osim pokušaja definiranja spomenutih pojmova), pokrenuti kritičku raspravu o ovom problemu u poslovanju kompanija, te raspravu o stavovima autora o unutarnjoj prijetnji iznesenim u ovom radu.

Ključne riječi: unutarnja prijetnja, zaposlenici, kompanija, rizik

Uvod

Današnja dinamika razvoja kompanija iziskuje stalni pritisak na osobe koje vode kompaniju i koji odlučuju o njezinom razvoju, dobiti, imidžu, zapošljavanju zaposlenika, otpuštanju zaposlenika i dr. Njih neki autori nazivaju „liderima“, bez obzira vode li korporaciju, vladinu agenciju ili neprofitnu organizaciju. Tako Frances Hesselbein (predsjednica Instituta Peter Drucker) navodi da nam „… trebaju lideri s iskrenim vjerovanjem, ljudi koji svojim mislima, riječima i djelima utjelovljuju postavku da se vođenje odnosi na to kako biti vođa, a ne (samo) kako djelovati. Trebaju nam lideri koji znaju da u konačnici karakter određuje uspješnost i rezultate. Trebaju nam lideri koji svojim vlastitim primjerom pokazuju da su ljudi najveće bogatstvo svake organizacije, koji iskreno i stvarno tako djeluju, ljudi za koje ta izreka nije puki slogan. To su ljudi koji stvaraju organizacije koje obiluju raznolikošću, snažno zastupljenom na svim razinama, u svim timovima i u svim grupama. Oni razumiju da raznolikosti u rasi, spolu, naobrazbi, godinama, iskustvu i svjetonazoru predstavljaju mogućnosti, a ne problem.“(F. Hesselbein1, Internet, 2005). Međutim, osim što „….su ljudi najveće bogatstvo svake organizacije..“, isti mogu predstavljati i prijetnju po kompaniju zbog koje može doći do znatne štete u bilo kojem smislu. Upravo zbog toga, od „lidera“ koji vode kompaniju očekuje se da uz prednosti svega spomenutog, prepoznaju i rizike koji bi se mogli pojaviti i tako naštetiti kompaniji. U tom „prepoznavanju“ i onemogućavanju mogućih unutarnjih prijetnji od strane zaposlenika, „liderima“ treba pomoć od, između ostalih i „korporativne sigurnosti“, čiji je zadatak u potpunosti informirati o mogućim rizicima kod prijema novih zaposlenika na određene pozicije, prekidu ugovora i dr., ali i o prijetnjama koje se mogu pojaviti od strane stalnih zaposlenika te vanjskih zaposlenika izvoditelja radova.

Prema Hunker i Probst (Internet, 2010), uspješna zaštita od unutarnjih prijetnji od strane zaposlenika zahtijeva kombinaciju pristupa s tehničke, sociološke i „socio-tehničke“ domene, a sve u cilju što boljeg otkrivanja prijetnji i njihovog ublažavanja. Nadalje, isti autori navode da se u praksi gubi značaj razlike između unutarnje i vanjske prijetnje kada se informatička infrastruktura kompanije koristi kao alat za „napad“.

1 Frances Hesselbein, predsjednica Leader- to-Leader Institute (Instituta Peter Drucker). Dobitnica je mnogih nagrada, Predsjednikove nagrade za slobodu, najvišeg civilnog priznanja Amerike i nagrade Dwight D. Eisenhower za zasluge u razvoju američke mornarice. Autorica je nagrađivane knjige "Hesselbein on Leadership" i koautorica 20 knjiga iz područja liderstva prevedenih na 28 jezika

1. Unutarnje prijetnje (eng. insider threats), definicije i moguće podjele

Zaštita osjetljivih informacija od neovlaštenog otkrivanja, zaštita od namjernog nanošenja bilo kojeg oblika štete kompaniji od strane zaposlenika, postaje sve prioritetnija briga za kompanije u cijelom Svijetu. Sadašnji i bivši zaposlenici, rukovoditelji, vanjski izvođači radova i druge osobe koje imaju pristup „unutrašnjosti" kompanije, predstavljaju značajnu prijetnju zbog svojeg znanja i ovlaštenih pristupa sustavima i podacima kompanije. Ovi pojedinci mogu djelovati samostalno i svojevoljno, ali i uz poticanje i pomoć osoba „izvan" kompanije. Povijesno gledano, tvrtke su se uglavnom usmjerile na zaštitu informacijskih sustava i sredstava protiv „uljeza" izvana. Gotovo svaka korporacija implementirala je različite sigurnosne alate za zaštitu, od najjednostavnijih zaštita kao što su ograde perimetra, do sofisticiranih zaštita informacijskih sustava uključujući firewall, anti-virus, anti-spam, anti-spyware i druge alate. Međutim, danas se sve više pojavljuju prijetnje korporativnoj sigurnosti koje dolaze iz unutrašnjosti korporacije.

Prije predstavljanja različitih pristupa koji se bave definiranjem unutarnje prijetnje, prvo bi trebalo definirati što mislimo pod tim pojmovima. Tako „prijetnju" možemo definirati kao mogući uzrok događaja koji nanosi štetu nekim sustavima u organizaciji ili cijeloj organizaciji (ISO/IEC, 17799, 2005).

Pod pojmom „unutarnje" definiramo zaposlenike, koji u nekim slučajevima i nesvjesno, pod različitim vanjskim utjecajima (npr. obitelj, prijatelji, i dr.), utjecajem suradnika, dostavljaju osjetljive, tajne informacije ili čine druge radnje koje mogu nanijeti štetu organizaciji (Deloitte, 2011). Dakako, šire gledajući to mogu biti i zaposlenici drugih poduzeća koji imaju ugovor o obavljanju određenih poslova, te na taj način imaju pristup nekim prostorima, sustavima, ali i zaposlenicima kompanije. Tu svakako treba spomenuti i bivše zaposlenike, oni kojima je iz bilo kojih okolnosti prekinut ugovor o radu ili koji su otišli u mirovinu.

Mnoge različite skupine proučavale su problem unutarnje prijetnje, od vladinih organizacija (kao što su tajne službe), nevladinih organizacija, sve do znanstvenika Osim toga, mnogi dijelovi privatnog sektora zainteresirani su za ovaj problem, naročito oni u financijskom sektoru. Međutim, unatoč tom interesu, nema zajednički prihvatljive definicije pojma „unutarnja prijetnja".

Kada bi pokušali definirati na koji način neka osoba može doći do podatka ili informacija koja bi mogle nanijeti štetu na bilo koji način kompaniji, onda možemo takve osobe svrstati u dvije osnovne skupine.

1. osobe koje imaju legitiman, dopušten pristup takvim podacima

2. osobe koje nemaju legitiman, dopušten pristup takvim informacijama.

Na ovaj način „unutarnju prijetnju" je moguće definirati obzirom na ovlast pristupa određenim podacima, što smatramo preusko.

Prema Hunker i Probst (2010), unutarnja prijetnja je (predstavlja) pojedinca s povlasticama koji ih zlorabi ili čiji pristup rezultira zlouporabom.

Nešto širu definiciju navodi Lieberman (Internet,2011), navodeći da je unutarnja prijetnja svaki napad pokrenut iz unutrašnjosti „mreže" od strane zaposlenika, ugovornog izvoditelja ili posjetitelja gdje je nastala šteta iskorištavanjem sredstava i iskoristivši priliku.

Nadalje, CERT (The United States Computer Emergency Readiness Team (US-CERT), dio United States' Department of Homeland Security) navodi u svojem istraživanju slijedeću definiciju unutarnje prijetnje: „Unutarnja prijetnja su trenutni ili bivši zaposlenici ili vanjski suradnici koji su namjerno prekoračili ili zlouporabili ovlaštenu razinu pristupa mreži, sustavu ili pristupu podacima tako da utječu na sigurnost „organizacije“ podataka, sustava, ili dnevno poslovanje“. (http://www.secretservice.gov/ntac_its.shtml). Kao što je vidljivo, ova definicija odnosi se na unutarnju prijetnju koja proizlazi iz zlouporabe pristupa mreži, sustavu, odnosno podacima koji se nalaze na istima. Istina je da su „cyber“ napadi popularan način za osobu koja je unutarnja prijetnja za počinjenje štetnih radnji, jednostavno zato što se veliki dio poslovanja u javnom i privatnom sektoru obavlja elektronskim putem. No provođenje zaštite samo na pristupe i korištenje „cyber“ prostora je pogrešno (M. Blades, Internet, 2011)

Širu definiciju unutarnje prijetnje daje Bishop (2005) koji navodi da je unutarnja prijetnja osoba od povjerenja koja je dobila određene ovlasti, i koja krši jedno ili više pravila sigurnosne politike, odnosno zlouporabi svoje ovlasti. Ovakva definicija upućuje na potrebu da se unutarnja prijetnja određuje u odnosu na neki skup ili pojedinačno pravilo koje je dio sigurnosne politike.

Iz do sada navedenog može se zaključiti da je unutarnja prijetnja uglavnom definirana kao osoba koja je zlorabila ovlašten pristup određenim podacima (ili sustavima na kojima su bili pohranjeni takvi podaci) ili je pak neovlašteno došla do takvih podataka. Naglašavamo i mogućnost da je takva osoba došla i do podataka u osobnoj komunikaciji s drugim osobama koje su joj priopćile takve podatke. Obzirom na „odnos“ osoba koje su moguća unutarnja prijetnja prema kompaniji, iste možemo podijeliti na osobe koje su zaposlenici kompanije, koji su bili zaposlenici kompanije, osobe koje su u poslovnom odnosu s kompanijom (primjerice izvode radove za nju ili kompanija njima pruža uslugu i sl.). Ovdje se kao unutarnju prijetnju mogu promatrati i budući zaposlenici, te sukladno tome treba provoditi kod zapošljavanja i određene selekcijske postupke. Vrlo značajan element ostvarivanja unutarnje prijetnje je svakako mogućnost pristupa do određenih podataka, a jedna od takvih mogućnosti je i radno mjesto na kojem zaposlenik radi, ili na kojem je radio. Iako je sasvim normalno da sa takvim podacima raspolažu visoki menadžeri kompanija, većina takvih podataka dostupna je, i primjerice, tajnicama menadžera, IT stručnjacima koji imaju administratorska prava na informacijskim sustavima i sl. Kada govorimo o ostvarenju unutarnje prijetnje, treba naglasiti da smatramo da je unutarnja prijetnja u potpunosti ostvarena onog trenutka kad je osoba-unutarnja prijetnja, nanijela štetu, ili imala ozbiljnu namjeru nanijeti štetu kompaniji u bilo kojem obliku.

U ovom poglavlju pokušali smo predstaviti početni pristup definiciji unutarnje prijetnje, te moguću podjelu . Kao što je vidljivo iz spomenutih definicija, velik dio njih odnosi se na unutarnju prijetnju usko vezanu na ranjivost informacijskih sustava i kontrole pristupa istima. Međutim, vidljivo je da pojedini autori unutarnju prijetnju promatraju i šire od toga, a koji pristup ćemo nastojati zadržati i u ovom tekstu.

2. Osnovni motivi i indikatori rizika

Jedan od važnih faktora koji se treba uzeti u obzir kod razmatranja unutarnje prijetnje je motiv poradi kojeg pojedina osoba namjerno poduzima određene radnje koje za posljedicu imaju nastanak štete za kompaniju u bilo kojem obliku. Motiv može biti od zabave, tehničkog izazova u odnosu na sustav ili kompaniju, pribavljanje kakve imovinske koristi, do špijunaže ili kombinacija svakog od ovih motiva. Dakako, motiv može biti i namjerno nanošenje štete kompaniji, bez nekog posebnog razloga. Iako bi

mogli očekivati da bi ovisno o motivu i nastala šteta za kompaniju mogla biti veća ili manja, upravo suprotno, bilo koji od ovih motiva mogu prouzročiti znatnu štetu za kompaniju, a što čini otkrivanje unutarnje prijetnje još složenijom (Hunker i Probst , 2010).

Istraživanja psiholoških profila osoba koje su namjerno počinili neki oblik štete svojoj kompaniji (ili u javnom sektoru), uglavnom su se temeljila na proučavanju konkretnih slučaja te intervjuiranja pojedinaca koji su osuđeni za špijunažu ili sabotažu (Hunker i Probst , 2010).

Band i dr. (2006), te Moore i dr. (2008), saželi su rezultate koji pokazuju ponašanja, motive i poremećaje ličnosti (narcisoidnost) koji su kao zaposlenici počinili neki prijestup ili kažnjivu radnju nanijevši štetu kompaniji. Ovakva istraživanja uglavnom su naknadna („post hoc“), i najčešće se temelje na razgovorima s osuđenim osobama. Također, procjene poremećaja ličnosti i motiviranosti teško je provoditi stalno, a i tada s upitnom razinom točnosti, jer tipična organizacija ljudskih resursa u nekoj kompaniji ne provodi stalne testove osobnosti ili neka psihološka testiranja koja bi mogla ukazati na neku osobu kao moguću prijetnju. Drugi problem je da ne postoje studije procjene i usporedivosti stope unutarnje prijetnje od uposlenika, u odnosu na ukupnu stopu zaposlenih, a što je važno za provjeru mogućih hipoteza u međusobnim odnosima (Hunker i Probst , 2010).

Većina radova koji se bave motivacijom osoba koje su moguća unutarnja prijetnja bave se promatranjem prediktivnih modela koji se odnose na psihološke profile ili ponašanja osoba u konkretnim slučajevima unutarnje prijetnje. Često se spominju osobne predispozicije koje se odnose na neprimjerene reakcije na stres, financijske ili druge osobne potrebe, što dovodi do osobnih sukoba i povrede propisanih pravila, kroničnog nezadovoljstva, neprimjerene reakcije na sankcije od strane kompanije, te sklonosti na eskaliranje svakog „sukoba“ tijekom rasprave u radnim procesima (Band i dr., 2006).

Greitzer i Frincke (2010) napravili su popis psihosocijalnih pokazatelja za koje smatraju da su indikatori koji ukazuju da je neka osoba potencijalna unutarnja prijetnja. Navedeno temelje na razgovorima s menadžerima ljudskih resursa i drugih dostupnih informacijama o osobama za koje se smatralo da su unutarnja prijetnja.

Tako su prema Greitzer i Frincke (2010) to slijedeći psihosocijalni pokazatelji:

- osobno nezadovoljstvo osobe

- neodgovarajuće prihvaćanje povratne informacije

- nezadovoljstvo rukovodstvom

- „isključivanje“ iz poslovnih procesa

- nepoštivanje pretpostavljenih

- problemi s radnim rezultatima

Važno je napomenuti da bilo koji od ovih pokazatelja (indikatora) treba uzeti u obzir samo ako zaposlenik pokazuje iznimno ozbiljno manifestiranje nekog od njih (Bishop i dr., 2010).

Prema Turner i Gelles (2004), postoji nekoliko osnovnih indikatora rizika kod zaposlenika. Tako navode slijedeće:

- neprihvatljivo ponašanje koje pojedinac svjesno ima i koje se događa kroz duže razdoblje, (takvo ponašanje rezultira složenim nizom problema, sukoba, a koji se uglavnom odražavaju i u osobnom životu pojedinca)

-pojedinci traže potvrdu „ispravnosti“ svoje prevelike procjene svojih sposobnosti i postignuća

- pojedinci koji su sebični, koji smatraju da su uvijek u pravu i da su podcijenjeni

- pojedinci koji osjećaju da organizacija ne reagira na njihove potrebe

-pojedinci koji traže trenutnu zahvalnost

-pojedinci koji se, ako njihove potrebe nisu zadovoljene, ponašaju buntovnički, pasivno, agresivno ili destruktivno

-pojedinci koje neprestano traže nekog drugog tko će zadovoljiti njihove potrebe, ili će potkopavati napore onih zbog kojih se osjećaju zanemareno ili koji nisu prepoznali njihove potencijale

-netolerancija vlastite kritike, nemogućnost preuzimanja odgovornosti za svoje djelovanje, okrivljivanje drugih za vlastite pogreške, te umanjivanje svojih grešaka.

Nadalje, prema Krofcheck (2003) postoje i određeni „ublaživači rizika“, a od koji autor kao neke navodi pojedince koji dobro surađuju s drugima u organizaciji, pojedince koji pokazuju toplinu i suosjećanje prema drugima i koji poštuju prava drugih, pojedince koji dobro primaju kritike bez zauzimanja obrambenog stava, pojedince koje drugi karakteriziraju kao dobroćudne, pojedince koji na jasan način mogu izraziti svoju ljutnju i frustracije.

Treba napomenuti da indikatori rizika kao i „ublaživači rizika“ ovise o konkretnom okruženju gdje osobe rade, poslu kojim se bave i dr.

3. Osnovni čimbenici koji mogu utjecati na pojavu unutarnje prijetnje

3.1. Osobni čimbenici

Postoji niz motiva i osobnih situacija (čimbenika) koje mogu povećati vjerojatnost da će netko nastojati (iz raznih motiva) nanijeti štetu svojem poslodavcu/kompaniji i time postati unutarnja prijetnja:

-pohlepa ili financijska potreba: uvjerenje da novac može riješiti sve probleme, primjerice nastale zbog dugova i pretjeranog trošenja

- ljutnja / osveta: Nezadovoljstvo do te mjere da želi naštetiti na bilo koji način kompaniji.

-problemi na poslu: nerazumijevanje i neslaganje sa suradnicima i menadžerima, nezadovoljstvo na poslu općenito, čekanje otpuštanja/otkaza ugovora o radu

- ideologija / identifikacija: želja da se pomogne "gubitnicima"

- podijeljena lojalnost: odanost drugoj osobe ili kompaniji, ili drugoj državi

- avantura: želja za dodatnim uzbuđenjima u životu, zaintrigirana je tajnim

aktivnostima

- ranjivost od ucjene zbog izvanbračnih veza, kockanja, prijevara

-ego / slika o samom sebi: stav "ja sam iznad pravila" ili želja za podizanjem svojeg

samopoštovanja.

-dodvoravanje: želja da se dodvori nekome tko bi mogao imati koristi od ekskluzivne

informacije s očekivanjem favoriziranja od strane te osobe

-kompulzivno (prinudno, prisilno) ponašanje i destruktivno ponašanje -(pod utjecajem droga, alkohola ili druga sredstva ovisnosti koja utječu na ponašanje)

- obiteljski problemi: bračni sukobi ili odvajanje od obitelji

-stalna opsjednutost životnim krizama i razočarenjima u karijeri.

Iz navedenog se može zaključiti da su neki motivi zaposlenika za ostvarenje unutarnje prijetnje značajno povezani s osobnim čimbenicima. Ovaj podatak nije posebno analiziran u ovom radu.

3.2. Organizacijski čimbenici

Organizacijski čimbenici mogu olakšati ostvarenje unutarnje prijetnje u nekoj kompaniji/organizaciji. Navesti ćemo neke od takvih primjera:

- dostupnost i jednostavnost dobivanja pristupa povjerljivim ili drugih zaštićenim podacima i davanje takvog pristupa onima kojima nije potrebno

- neodgovarajuće označavanje stupnjem tajnosti povjerljivih informacija, ili pogrešno označavanje

- lakoća izlaska iz objekata bez kontrole iznošenja dokumenata ili drugih stvari

- nedefinirane politike u vezi s radom od kuće na projektima s povjerljivim informacijama, ili općenito nošenje službenih materijala kući

- percepcija da je sigurnost slaba i da su posljedice za krađe minimalne ili ne postoje

-„vremenski pritisak“- zaposlenici koji su zbog ograničenog vremena za neku poslovnu aktivnost u nedovoljnoj mjeri osigurali povjerljive informacije

-zaposlenici nisu obučeni kako na odgovarajući način zaštititi povjerljive podatke

Jedan od osnovnih načina prevencija štete od unutarnjih prijetnja koje nastaju poradi organizacijskih čimbenika je donošenje jasnih pisanih procedura za radne procese gdje postoje sigurnosni rizici za nanošenje štete kompaniji. Tako primjerice treba propisati razine pristupa pojedinim razinama

intranet mreže, označavanja stupnjevima tajnosti pojedinih dokumenata ili medija (cd, dvd, prijenosne memorije…) i postupanje s takvim dokumentima, pristup pojedinim prostorima i kontrola ulaska/izlaska iz takvih prostora i dr. Također, važno je da su za svako nepridržavanje propisanih pravila i procedura propisane sankcije, a sve poradi mogućih radno-pravnih sporova.

3.3. Indikatori u ponašanju

Neka ponašanja zaposlenika mogu biti indikator da zaposlenik nastoji doći do povjerljivih informacija ili da ih s njima raspolaže i zlorabi ih. Neki od primjera su:

- bez potrebe ili ovlaštenja povjerljive podatke nastoji iznijeti ili ih dostaviti izvan organizacije, npr. na svoj privatni e-mail. Neprimjereno traži ili pribavlja povjerljive informacije o temama koje nisu povezane s njegovim poslom

- pokazuje interes o stvarima izvan djelokruga svojih poslova, a posebice onih od interesa poslovnih konkurenata

-nepotrebno kopiranje ili printanje materijala, posebice onih koji sadrže povjerljive informacije

- daljinski pristupa računalnoj mreži bez potrebe za vrijeme godišnjeg odmora, bolovanja ili u neuobičajeno vrijeme

- zanemarivanje informatičkih sigurnosnih politika o instaliranju osobnih softvera ili hardvera, pristup ograničenim web stranicama, koje obavljaju neovlaštena pretraživanja

- rad u neuobičajeno vrijeme bez odobrenja; ističe entuzijazam za prekovremeni rad, rad vikendom, kada je lakša dostupnost ili poduzimanje nekih aktivnosti s ciljem pribavljanja povjerljivih podataka

-neprijavljivanje kontakata sa predstavnicima konkurentskih kompanija ili kompanija koje su u bilo kakvom (ili je poznato da će biti) poslovnom odnosu

-kupovina stvari ili imovine koja nije u skladu s prihodima

- zabrinutost da ih se istražuje, provjeravaju dali je netko pretraživao radno mjesto ili kuću; traži prislušne uređaje i kamere.

Treba naglasiti da mnogi zaposlenici povremeno imaju ili pokazuju neke, ili sve od navedenog u različitim stupnjevima i situacijama, međutim, većina njih neće prijeći liniju i počiniti štetu kompaniji na bilo koji način.

4. Nastanak štete

Kako bi mogli poduzeti određene mjere u cilju smanjenja ili potpunog otklanjanja unutarnje prijetnje, važno je odrediti gdje sve može nastati šteta zbog takve prijetnje. Današnji poslovni procesi, od najjednostavnijih do najsloženijih nezamislivi su bez uporabe računala, računalnih mreža, i drugih oblika IT tehnologije.

Nedavna studija Aberdeen Group (Deloitte, 2011) je pokazala da je 80% od 116 ispitanih kompanija zabilježilo gubitak povjerljivih informacije zato što je netko iz kompanije bilo „presreo“ ili sam imao i dostavio povjerljivu informaciju. Ipak, samo 43% kompanija ima sustav za praćenje i kontrolu protoka

izlazne e-mail pošte, a 79% kompanija kontrolira ulaznu e-mail poštu. 16 % kompanija promatranog uzorka je izjavilo da namjeravaju provesti sustav kontrole praćenja ulazno/izlazne e-mail pošte unutar iduće godine. Mogući problemi kod ovakve vrste kontrole predstavljaju različita tumačenja zaštite privatnosti, ali obzirom na temu ovog rada, istima se nećemo baviti.

Kada govorimo o primjerima unutarnje prijetnje, te gdje može nastati šteta u kompaniji poradi te unutarnje prijetnje, navesti ćemo osnovna (posebno „ranjiva“) područja.

1. Korupcija kao prijetnja koja može nanijeti štetu kompaniji na bilo kojoj razini, no svakako najveća na mjestima gdje pojedini zaposlenici ili visoki menadžment može donijeti određene odluke, a da ne poštuje propisane procedure (ako iste uopće postoje).

2 .Korporativna špijunaža ili industrijska špijunaža kao prijetnja koja je usmjerena na prikupljanje povjerljivih informacija o kompaniji ili njezinim zaposlenicima radi stjecanja prednosti nad poslovnom konkurencijom.

3. Pronevjera kao prijetnja koja je moguća od strane zaposlenika na način da su isti zlorabili opremu, sredstva, novac i dr. koja su im povjerena, koristeći ili prisvojivši ta sredstva

4. „Sabotaža“ kao unutarnja prijetnja gdje se namjerno ometa normalno poslovanje, ili namjerno uništava oprema ili proizvod.

5. Otkrivanje osobnih i drugih podataka o zaposlenicima i imovini kompanije kao prijetnja koja za posljedicu može imati nanošenje štete ne samo kompaniji, nego i zaposlenicima osobno.

6. Uništenje ugleda kompanije kao prijetnja koja indirektno nanosi štetu kompaniji na svim ili pojedinim područjima poslovanja.

5. Mjere za smanjenje ili rano otkrivanje moguće unutarnje prijetnje

Iako je u nekim dijelovima teksta spomenuto koje mjere bi trebalo poduzeti kako bi spriječili ili smanjili posljedice unutarnje prijetnje, ovdje ćemo navesti nekoliko mjera koje utječu na smanjenje ili rano otkrivanje moguće unutarnje prijetnje. Ključ za prevenciju i rano otkrivanje unutarnje prijetnje u osnovi se nalazi u osobnom zadovoljstvu zaposlenika u radnom okruženju te organizacijskim rješenjima kojima se može identificirati unutarnja prijetnja ili u potpunosti spriječiti.

Neki od organizacijskih rješenja uključuju slijedeće:

- edukacija i redoviti treninzi zaposlenika o važnosti sigurnosti ili drugim protokolima koji utječu na razinu sigurnosti kompanije.

- primjereno osigurati i zaštiti sve informacije čija bi zlouporaba mogla nanijeti štetu kompaniji na bilo koji način

- propisati odgovarajuće procese postupka za odabir novih zaposlenika

- osigurati odgovarajuće načine da zaposlenici mogu sigurno prijaviti sumnje u moguće unutarnje prijetnje

- stalni nadzor računalnih mreža za sumnjive ili nedopuštene aktivnosti

Jedno od vrlo značajnih faktora koji mogu utjecati na smanjenje unutarnje prijetnje od zaposlenika je stvaranje okruženja koje samim zaposlenicima omogućuje da budu „sigurnosni senzori“ i „sakupljači informacija“ o potencijalnim unutarnjim prijetnjama. Neki od koraka koji predlaže „Deloitte“ (2011) kako bi se to moglo i ostvariti su:

- procijeniti stupanj rizika korištenja zaposlenika u takve svrhe obzirom na osjetljivost

- razviti standardne postupke za ublažavanje rizika

- razviti postupke kod zapošljavanja u skladu sa sigurnosnim zahtjevima

- razviti postupak koji se primjenjuje u slučajevima „problematičnih zaposlenika“

- razviti jasni disciplinski postupak kod nepridržavanja kompanijskih pravila i uputa

- razviti postupak za upravljanje u kriznim situacijama

- osigurati sredstava ili drugu pomoć za zaposlenike u osobnim krizama

- izraditi program koji uključuje razvijanje vještina „promatranja“ neprihvatljivih ponašanja

- izrada protokola o izvješćivanju o neprihvatljivim ponašanjima ili situacijama, te izrada mehanizama za osiguranje kvalitete ovakvih izvješća

- razviti skup specifičnih ciljanih ponašanja zaposlenika koja su u skladu s preventivnim aktivnostima usmjerenim na smanjenje ostvarenja unutarnje prijetnje

- razviti trening za izvještavanje o sumnjivim i pogrešnim ponašanjima u skladu s procesom koji se koristi za prikupljanje takvih informacija od zaposlenika

- razviti kontinuirani obrazovni program za sve zaposlenike i stalno ga ažurirati uz jačanje svijesti i opreza temeljem prakse iz slučajeva gdje je ostvarena unutarnja prijetnja

- razviti sigurnosni plan koji uključuje povremene intervjue sa zaposlenicima

Važno je naglasiti da planiranje i provođenje gore navedenih aktivnosti iziskuje vrlo dobro razrađenu pripremu, s naglaskom na objašnjenju svrhe provođenja ovakvih aktivnosti, a možda i ne obuhvaćanje svih zaposlenika u provođenju aktivnosti, što ovisi o konkretnoj kompaniji i procjeni.

Organizacija ljudskih resursa (engl. human resource, HR) u svakoj kompaniji mora biti i u funkciji pomaganja da se unutarnja prijetnja od strane zaposlenika ne ostvari. HR osoblje je uglavnom prvo i posljednje u kontaktu sa zaposlenicima, dakle kod prijema i odlaska iz kompanije. Potrebno je osim redovnih intervjua koji se obavljaju kod primanja novih zaposlenika (o čemu nešto više u nastavku), predvidjeti stalne ili povremene tzv. izlazne intervjue sa zaposlenicima koji odlaze iz kompanije. Oni bi trebali biti osmišljeni i vođeni na način da se pokuša utvrditi koje su to najčešće krizne situacije kod zaposlenika, kakve su mogućnosti uvida u informacije koje su zaštićene, ili neke druge situacije a koje smatramo mogućom unutarnjom prijetnjom. Uloga HR jedna je od ključnih kada trebamo procijeniti rizik od unutarnje prijetnje kad dolazi od zaposlenika. Prijem novih zaposlenika u kompaniju, jedan je od važnih postupaka kojim, ako se pravilno provodi, možemo značajno smanjiti rizik od unutarnje

prijetnje od strane zaposlenika. Propisane opće i posebne procedure za pojedina radna mjesta mogu značajno doprinijeti smanjenju rizika od unutarnje prijetnje. Prije svega trebalo bi odrediti koja su to radna mjesta (ili poslovi) za koje bi trebalo primijeniti nešto drugačiju proceduru kod prijema zaposlenika nego za ostala radna mjesta. Primjerice, iako je radno mjesto tajnice/tajnika u nekoj kompaniji uglavnom isto rangirano s potrebom istih znanja i vještina, tajnica/tajnik člana uprave kompanije ili direktora za financije, nabavu, ili osobe koja je zadužena za informatičku sigurnost i dr., trebala bi kod prijema proći i neke posebne procedure. Moguće rješenje je obavljanje intervjua u kojem bi se postavljala pitanja koja omogućuju ispravnu procjenu rizika zapošljavanjem te osobe. Tu se uvijek pojavljuje problem u kojem trenutku pitanja prelaze granicu zadiranja u privatni život, od „materijalno-financijskih" podataka (posjedujete li dionice, čije, posjeduje li dionice netko od članova obitelji, prijatelja), do osobnih, npr. s kim stanujete, imate li partnera ili supružnika, čime se oni bave, čime se bave vaši roditelji, bliža rodbina, kumovi i sl. Upitnost istinitosti podataka prikupljenih tijekom intervjua je također problem, a koji je moguće djelomično riješiti provjerom putem „otvorenih izvora" (Internet, javne baze podataka…), ali i angažiranjem ovlaštenih detektivskih agencija. Prije svega bi trebalo definirati koja su to radna mjesta ili poslovi za koje bi novi zaposlenici trebali proći dodatni intervju, uz njihov pristanak, i uputu da ne moraju odgovoriti na pitanje.

Za takvu proceduru potrebno je osmisliti upitnike za specifična radna mjesta za koja isti kandidiraju, ali i moguće dodatne provjere za pojedina radna mjesta.

Osim propisanih procedura kod prijema zaposlenika, vrlo je važno provoditi i procedure kod odlaska zaposlenika. Tako smatramo potrebitim provoditi intervju s zaposlenicima koji odlaze iz kompanije npr. u mirovinu ili na rad u neku drugu kompaniju, ali i s onima kojima se prekida ugovor o radu jer su počinili disciplinske prekršaje. Svakako da bi intervjue i kod prijema novih zaposlenika na pojedina radna mjesta ili kod odlaska istih iz kompanije, trebali voditi dodatno osposobljene osobe.

Treba naglasiti da su poslovi ljudskih resursa u kompaniji jedna od glavnih „poluga" pomoću kojih se može prevenirati ili otkriti unutarnja prijetnja. Možemo reći da se zaposlenici kompanije pojavljuju u dvostrukoj ulozi, kao zaposlenici koje treba zaštiti od svih ugroza, ali dio njih i kao zaposlenici koji mogu nanijeti štetu kompaniji. Ovakva dvojnost uloge zaposlenika dodatno usložnjava poslove i ulogu korporativne sigurnosti i svih ostalih dijelova kompanije koji mogu doprinijeti sigurnosti kompanije.

6. ZAKLJUČAK

U radu se je pokušalo na više različitih načina i sa različitih stajališta definirati unutarnju prijetnju, a u svim pristupima različitih autora zajedničko je da je u fokusu unutarnje prijetnje kao potencijalni izvršitelj zaposlenik kompanije. Uzimajući u obzir tvrdnju koja je iznesena na početku ovog rada da „su ljudi najveće bogatstvo svake organizacije..", složenost pristupa ovom problemu još je veća. Motivi, kako osobni, tako i oni koji nisu određeni osobnim razlozima, neodgovarajuća kompanijska sigurnosna pravila, ne postojanje bilo kakvih preventivnih ili edukacijskih programa za sprečavanja nastanka unutarnje prijetnje ili za smanjenje štete ukoliko se prijetnja ostvari, neka su od područja koja treba istražiti u svakoj kompaniji koja je ugrožena od unutarnje prijetnje. Uloga upravljanja ljudskim resursima jedna je od ključnih u smanjenju rizika od unutarnje prijetnje u svakoj kompaniji, kao i jasno definirana pravila korištenja i pristupa informacijskih sustava u kompaniji. Poseban naglasak kod svih postupaka i rada sa zaposlenicima na preveniranju unutarnje prijetnje, predstavlja granica zadiranja u privatnost svakog od zaposlenika, (čime se u ovom radu nismo detaljno bavili), a

što bi uvelike moglo utjecati na procese koji se trebaju provoditi u kompanijama u cilju sprječavanja unutarnje prijetnje.

Svakako treba naglasiti, da, ovisno o kompaniji, poslovnom okruženju u kojem posluje, zaposlenicima koji su uposleni, djelatnošću kojom se bavi, te niza drugih okolnosti, ovise i postupci i rizici unutarnje prijetnje. Cilj rada bio je potaknuti kritičko razmišljanje, prvenstveno onih koji su odgovorni za kompanijsku sigurnost, ali i drugih dijelova kompanije (ljudski resursi, IT...) koji mogu doprinijeti u sprečavanju ili nastanku unutarnje prijetnje.

LITERATURA

Knjige:

Probst C. W., at al. (2010): Insider Threats in Cyber Security, Chapter: A Risk Management Approach to the ”Insider Threat”. Springer.

Turner, J. and Gelles, M. (2003): Threat Assessment a Risk Management Approach, Insider Threat Chapter, Haworth Press, New York

Izvori preuzeti s Interneta:

Band S. R., at al. (2006): Comparing insider IT sabotage and espionage: A model-based analysis, Carnegie Mellon University, www.cert.org/archive/pdf/06tr026.pdf (24. travnja, 2012.)

Hesselbein F. (2005),: Kakve lidere trebamo?,

http://www.quantum21.net/slike/src/2009/11/02/125719713312091clanakhesselbein.pdf, (17.5.2012.)

Blades M. (2010),: The Insider Threat

http://www.securityinfowatch.co/article/10510466/the-insider-threat, (27. travnja, 2012.)

Lieberman D. (2011): Defining the Insider Threat

http://www.infosecisland.com/blogview/12824-Defining-the-Insider-Threat.html, (14. svibnja, 2012)

Moore A. P., Cappelli D. M., Trzecia R. F., (2008): The ’Big’ Picture’ of IT Sabotage Across U.S. Critical Infrastructures. Software Engineering Institute Carnegie Mellon University,

www.cert.org/archive/pdf/08tr009.pdf, (18.5. 2012.)

Službene publikacije:

System Sciences, (2009)., HICSS '09. 42nd Hawaii International Conference on, Conference Publications; Position: Insider is relative. In Proceedings of the New Security Paradigms, str.1-10, Sprague, R.H.

Delloite, (2011), Security along the Border: the Insider threat, Building a secure workforce, Delloite Development LLC.

Pacific Northwest, National laboratory, (2010),: Greitzer F. L. at al.: Predictive Modeling for Insider Threat Mitigation. Richland, WA

ISO/IEC 17799, (2005), Information technology - Code of practice for information security management

Časopisi:

Hunker J., Probst C. W., (2010): Insiders and Insider Threats, An Overview of Definitions and Mitigation Techniques, Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications Vol. 2, str. 4-27

Ostalo:

Krofcheck, J., (2003): The Study of the Unspy, unpublished manuscript and personal communications. Yarrow Associates, Virginia.

EMPLOYEES – POSSIBLE INTERNAL THREAT

Darko Dundović, M.A.

Abstract

The paper attempts to define the internal threat from the perspective of different authors or organizations. The intention is to look at the internal threat primarily in relation to company employees, and other persons who have access to the company data or areas and thus may be an internal threat to the company. Motives and risk indicators have also been considered from this viewpoint.The appearance of internal threat is perceived through the basic factors that can affect the occurrence of internal threat, thus analyzing personal factors, organizational factors, as well as indicators of employee behavior. An effort was made to maintain a basic level explanation of these factors without going into detailed analysis, such as the psychological profiles of individual employees or their (compulsive) behaviour. Mentioned are places of potential damage in cases of realizing internal threats, and an overview of the measures for reducing or for early detection of possible internal threats is given.The aim (besides trying to define these terms) was to initiate a critical discussion on this problem in the business operations of the companies, as well as a debate on the author's attitudes to internal threats outlined in this paper.

Keywords: internal threat, employee, company, risk