VI. ZNANSTVENO-STRUČNA KONFERENCIJA S MEĐUNARODNIM SUDJELOVANJEM
MENADŽMENT i SIGURNOST
Čakovec, 8.6.2011.

PRINCIPI SIMPLIFICIRANJA SUSTAVA ZAŠTITE ZA PODUZEĆA

SECURITY SYSTEM SIMPLIFICATION PRINCIPLES FOR BUSINESSES

Aleksandar Pašagić
General Security d.o.o., Zagreb, Hrvatska, aleksandar@generalsecurity.hr

Sažetak
Cijena i opseg posla uključeni u izradu profesionalnog sustava zaštite za određeno poduzeće često negativno utječu na inicijalnu odluku odgovornih osoba o upuštanju u implementaciju tog sustava. U ovom radu elaborira se metodika pristupa kojim se teži razraditi sustav dovoljno robustan da pokriva kritične osjetljive točke infrastrukture i poslovnih procesa, a istovremeno prihvatljiv sa stajališta financijskih ulaganja i praktičnosti korištenja. Cilj rada je postaviti praktično primjenjive parametre unutar kojih se mogu sklapati kompromisi po pitanju apsolutnog stupnja sigurnosti, a u svrhu poticanja šireg usvajanja osnovnih mjera zaštite u poduzećima koje taj segment ignoriraju zbog njegove percipirane složenosti i vezanih troškova.

Ključne riječi
simplifikacija zaštite, smanjenje ulaganja, sustav zaštite

Abstract
The cost and volume of work required to build a professional security system for a given business often have a negative influence on the initial decision of responsible personnel to engage in the implementation of such a system. This paper elaborates on the methods of approach whose objective is the development of a system robust enough to cover critical points of infrastructure and business processes, while at the same time being acceptable with regard to financial investments and practicality of use. The objective of this paper is to establish applicable parameters within which one can make compromises regarding the absolute level of security in order to stimulate wider application of basic security measures in firms that tend to ignore that segment of business due to its perceived complexity and associated expenses.

Keywords
investment reduction, security simplification, security system

UVOD – IDEJA, DEFINICIJE I PRETPOSTAVKE RADA

Osnovna ideja ovog rada počiva na pretpostavci da su financijska ograničenja čest razlog suboptimalne kvalitete sustava zaštite u nemalom broju poduzeća, posebice u privatnom sektoru. Zbog popularnog mišljenja da će ulaganje u zaštitu opteretiti budžet poduzeća, a da implementacija sustava zaštite neće donijeti ekvivalentnu ili veću uštedu odnosno dobit, može se javiti sklonost ka općenitom ignoriranju problematike zaštite, ili težnji minimalizaciji ulaganja samo do mjere koja je propisana zakonom. Cilj rada je obratiti pažnju na neke od pristupa kojima se trošak za zaštitu može smanjiti, a da se njezina razina pritom ne smanji ispod prihvatljivih granica.

Iako se u ovom radu navode neke od praktičnih metoda za postizanje gore opisanog cilja, primarna svrha tih navoda jest ilustrirati principe iz kojih te metode slijede. Podrazumijeva se da su konkretni koraci u smjeru optimizacije troškova sustava zaštite uvelike ovisni o specifičnostima objekta, poduzeća i djelatnosti koja se štiti, kao i o nizu drugih faktora, no općenita načela iznesena ovdje mogu poslužiti kao okvir za reevaluaciju postojećeg stanja i možebitne promjene koje bi dovele do povećanja razine zaštite uz minimalne prateće troškove.

U kontekstu ovog rada govori se o sustavima zaštite ili sigurnosti, te se tim izrazom podrazumijeva ukupni zbir mjera, procedura, tehničkih i tehnoloških sredstava čija je primarna namjena spriječiti nanošenje štete poslovanju poduzeća izazvane namjernim djelovanjem ljudskog faktora. Iako se ovaj rad ne bavi sigurnosnim sustavima u smislu zaštite od šteta izazvanih prirodnim silama, prirodom samog posla ili nenamjernim postupcima ljudi, osnovna načela koja se u njemu razmatraju djelomično su primjenjiva i na tu problematiku. U tom smislu, pojmovi zaštite i sigurnosti tretiraju se kao sinonimi za praktične potrebe ovog rada, ukoliko nije posebno navedeno drugačije.

Također, ovaj rad usvaja pragmatičan pristup u smislu prepoznavanja činjenice da zaštita nije svrha samoj sebi, već se na nju mora gledati kao na dio ukupnog poslovanja poduzeća. Kao takva, podložna je kompromisima koji će ponekad nužno uključivati svjesno smanjenje stupnja sigurnosti kada to pogoduje općem poboljšanju poslovanja. Moralnost i etičnost namjernog smanjenja razine sigurnosti uvijek će biti podložni raspravi, posebice kada se radi o mjerama koje izravno utječu na sigurnost samih djelatnika. Ta problematika je osjetljiva i složena, i prelazi okvire ovog rada. Ipak, činjenica je da će se u okvirima stvarnog svijeta osobe zadužene za osmišljavanje i implementaciju sustava zaštite često naći u situacijama kada će morati učiniti najbolje što mogu s ograničenim sredstvima. Ovaj rad pretpostavlja da su realne mogućnosti za dodatno ulaganje u zaštitu iscrpljene, te se koncentrira na pitanje kako izvući najviše zaštite iz onoga što je na raspolaganju.

1. ZAŠTITA KAO KOMPROMIS

Za praktične potrebe, ukupnu razinu sigurnosti možemo promatrati kao neku vrstu ravnoteže ili kompromisa između financijskog ulaganja, stupnja zaštite i jednostavnosti implementacije. To znači da će korisnik za svoj sustav zaštite morati platiti cijenu koja u većoj ili manjoj mjeri sadrži svaki od tri navedena faktora. Raspoloživa sredstva, priroda poslovnog procesa i filozofija pristupa zaštiti osobe koja dizajnira sigurnosni sustav odredit će relativne postotke tih faktora. Valja navesti da prikaz sigurnosti kao konstantne sume financija, zaštite i praktičnosti pretpostavlja planiranje sustava sigurnosti optimalno prilagođenog potrebama korisnika. Podrazumijeva se da kvalitativni pomak u osmišljavanju samog sustava može podići razinu sigurnosti bez da se pritom odrazi na neki od tri spomenuta čimbenika, te da uvijek treba težiti napretku na tom području.

S čisto teoretskog stajališta, lako je doći u iskušenje da se kategorički tvrdi kako sigurnost nije područje gdje se mogu raditi kompromisi, posebice ako govorimo o štićenim resursima veće vrijednosti, ili čak životima osoblja. Nažalost, usvajanje takvog stava pokazuje nerealno shvaćanje stvarnog svijeta i naivan pogled na sigurnosnu problematiku. Sigurnost u stvarnom svijetu uvijek će biti kompromis između razine zaštite koju želimo ostvariti i cijene koju smo za to voljni ili sposobni

platiti. Očito je da je apsolutna sigurnost neostvarivi ideal; no možda je manje očito kako i sama težnja apsolutnoj sigurnosti može djelovati kontraproduktivno. Osobe zadužene za sigurnost neke organizacije izlažu se riziku od obeshrabrenja i odustajanja od pokušaja implementacije praktičnih mjera zaštite u trenutku kada uvide realna ograničenja unutar kojih moraju djelovati, ukoliko im se profesionalna filozofija bazira na težnji ka apsolutnoj sigurnosti.

Dobro osmišljena sigurnosna strategija neće biti savršena u apsolutnom smislu te riječi, ali će uspjeti optimalno raspodijeliti ograničena sredstva koja ima na raspolaganju kako bi se zaštitili najvažniji i/ili najugroženiji resursi. Točan način na koji će ta raspodjela biti sprovedena varirat će od organizacije do organizacije, ovisno o njihovim specifičnim potrebama i raspoloživim sredstvima. No nužno je u samom početku usvojiti stvarnost zaštite kao kompromisnog rješenja u svojoj biti kako bismo uspostavili manevarski prostor za optimizaciju sigurnosnog sustava i prikladno alocirali raspoloživa sredstva.

Nešto sigurnosti uvijek je bolje od ništa sigurnosti, ali još više sigurnosti nije nužno uvijek bolje od puno sigurnosti. Naime, osobe koje su zadužene za sigurnost u nekom poduzeću ponekad su sklone shvaćati svoje područje djelatnosti kao zatvoren sustav, te se prema njemu odnositi kao nečemu što je samo sebi svrha. Razumljivo je da su profesionalci na području sigurnosti osjetljiviji na sigurnosne propuste od ostalih djelatnika svog poduzeća, ili bi to barem trebali biti. Isto tako intenzivnije i osobnije doživljavaju ograničenja budžeta za zaštitu, budući da su svjesni velikog broja potencijalnih rizika. Kao posljedica toga, izloženi su opasnosti da na sigurnost gledaju kao na nešto odvojeno od ukupnog poslovanja poduzeća. Tako se osobe zadužene za sigurnost mogu sukobljavati s nadređenima koje percipiraju kratkovidnima za pitanja zaštite. Ali svrha sigurnosti na prvom mjestu se svodi na omogućavanje učinkovitog i neprekinutog odvijanja primarne djelatnosti poduzeća u pitanju. Gledano iz tog kuta, postaje očito da je sigurnost samo jedan od faktora u poslovanju poduzeća, te kao takva podliježe istim zakonitostima poslovanja kao i s njome nevezane grane. U idealnom svijetu kako ga zamišlja menadžer sigurnosti, sigurnost i zaštita uvijek bi imali prioritet i na raspolaganju bi im stajala sva potrebna sredstva. U stvarnom svijetu to čak ni teoretski nije moguće, budući da bi ulaganje u sve veću razinu sigurnosti u jednom trenutku premašilo vrijednost dobara koje taj sustav štiti.

2. ZAKON PADAJUĆIH PRINOSA I NEISPLATIVA ULAGANJA U SIGURNOST

Jedan od poznatijih zakona u ekonomiji poznat je pod nazivom zakon padajućih prinosa. Općenito govoreći, on tvrdi da se vrijednost dodatnog povrata smanjuje nakon što se premaši određena granica jedne vrste ulaganja, uz pretpostavku da su sva ostala ulaganja fiksna [1]. Ukoliko taj zakon u njegovom najopćenitijem obliku primijenimo na područje sigurnosti, slijedi da ulaganje sve veće količine sredstava u poboljšanje sigurnosti nije nužno optimalan pristup s holističkog stajališta. Naime, nakon što se na sustav sigurnosti potroši određena količina resursa, dodatna ulaganja iznad te granice neće polučiti rezultate razmjerne troškovima. Drugim riječima, ta ulaganja su neisplativa jer su vezani troškovi veći od realno očekivanog rizika kojem bi ulagač bio izložen kada ne bi implementirao ta dodatna sredstva ili mjere zaštite.

Računanju isplativosti određenih sredstava zaštite može se pristupiti na više načina. Najčešće korištena formula mogla bi se u pojednostavljenom obliku prikazati na sljedeći način:

$$\text{ako } (T_d < P_d \times C_d) \text{ uloži u } T_d$$

gdje je P_d vjerojatnost da će nastupiti događaj d koji će uzrokovati štetne posljedice, C_d iznos predviđene štete uzrokovane događajem d, a T_d ukupna cijena implementacije protumjera za događaj d. Iz toga slijedi da je $P_d \times C_d$ iznos do kojega je racionalno uložiti kako bi se događaj d spriječio [2]. Svako ulaganje preko tog iznosa teoretski košta poduzeće više nego što bi stajala sanacija štete. Vezano uz opisani pristup, potrebno je istaknuti postojanje nekoliko čimbenika koji se

gube na ovoj razini simplifikacije izračuna, a uključuju, između ostaloga, tržišnu poziciju poduzeća, percipiranu pouzdanost od strane klijenata i opći negativni dojam koji mogući štetni događaj može izazvati. Ti i slični čimbenici mogu stvarnu cijenu štetnog događaja podići na razinu znatno veću od neposrednih gubitaka koji se očekuju u slučaju nastupanja tog događaja. Također, s čisto teoretskog stajališta, moguće je rezonirati da nije moguće predvidjeti sve potencijalne štetne događaje, pa je samim time nemoguće objektivno ocijeniti stvarni rizik za poslovanje [3]. No s druge strane, podrazumijeva se da je određeni stupanj pojednostavljenja nužan za praktične primjene.

Resursi na koje se zakon padajućih prinosa može primijeniti u kontekstu sigurnosti nisu ograničeni na financijska sredstva. Oni uključuju i radne sate djelatnika, dodatnu obuku potrebnu za rukovanje tehničkim sustavima i provođenje novih procedura, pa i mogući pad produktivnosti kao posljedica nezadovoljstva djelatnika mjerama koje doživljavaju kao nepotrebno opterećivanje ili narušavanje privatnosti. Kao što smo već spomenuli, sigurnost je kompromis između financijske investicije, stupnja zaštite i jednostavnosti implementacije. To znači da stvarna cijena nekog sigurnosnog sustava ili proceduralne mjere može biti skrivena u čimbenicima koji nisu isključivo financijske prirode. Ti „skriveni“ faktori također se moraju uzeti u obzir prilikom optimizacije sustava zaštite.

3. HOLISTIČKI PRISTUP PROBLEMATICI ZAŠTITE

Poduzeća koja se odlučuju na implementaciju određenog sustava zaštite, ali koja istodobno ne pridaju preveliku pažnju njegovoj optimizaciji, bilo zbog nedostatka razumijevanja važnosti zaštite, bilo zbog procjene (ispravne ili neispravne) da razina rizika ne opravdava ozbiljnije ulaganje u prevenciju, obično usvajaju jedan od tri pristupa opisanih u nastavku ovog poglavlja.

Prvi pristup je jednodimenzionalna zaštita. U ovom slučaju korisnik se odlučuje na jedno sredstvo kojem povjerava brigu o sigurnosti svog poslovanja. To sredstvo može poprimiti različite oblike, od lokota na vratima do police osiguranja sklopljene s osiguravajućom kućom. Sredstvo u pitanju ne mora biti jeftino da bi zadovoljavalo definiciju jednodimenzionalnosti, te može biti i u obliku tjelesne zaštite. Iako se radi o maksimalno simplificiranom modelu sigurnosti, jednodimenzionalna zaštita ima svoje primjene u izuzetno jednostavnim slučajevima.

Drugi pristup je sekvencijalna zaštita, gdje se elementi sustava zaštite dodaju dio po dio kako se identificira potreba za njima. Ovakav pristup počinje s osnovnim modelom koji se nadograđuje na onim mjestima gdje praksa pokaže da trenutni stupanj zaštite nije adekvatan. Troškovi koje može očekivati poduzeće koje koristi sekvencijalni pristup u konačnici vjerojatno neće biti isplativi. Iako primamljivost ovog načina izgradnje sustava zaštite može ležati u maloj početnoj cijeni, dodavanje elemenata nakon što se pokaže njegova manjkavost koštat će više budući da nove komponente neće nužno biti kompatibilne s postojećima. Također, detekcija ranjivih točaka na ovaj način pretpostavlja da će poduzeće pritom pretrpjeti određenu štetu čiji se opseg ne može predvidjeti na zadovoljavajući način. Takva zaštita u svojoj biti previše je pasivne prirode da bi bila primjenjiva na ozbiljnije slučajeve, što ne odvraća relativno veliki broj poduzeća da ga usvoje zbog manjih inicijalnih ulaganja.

Treći pristup je sigurnost u kompletu, koji se temelji na instalaciji sustava zaštite s prethodno definiranim elementima neovisnim o specifičnim potrebama korisnika. Financijska privlačnost ovog pristupa leži u činjenici da su gotova rješenja često jeftinija u odnosu na kupovinu pojedinačnih komponenti. S druge strane, ti kompleti mogu uključivati komponente koje korisniku objektivno nisu potrebne, odnosno prisiliti ga na prihvaćanje suboptimalnih elemenata zato jer dolaze kao dio kompleta.

Treba napomenuti da niti jedan od tri gore navedena pristupa ne mogu biti a priori prozvani „pogrešnima“. Moguće je konstruirati situacije u kojima je potpuno primjereno aplicirati neki od njih uz zadovoljavajuće rezultate [4]. S druge strane, nužno je imati na umu njihove inherentne nedostatke koji postaju tim izraženiji što je kompleksniji objekt/operacija koja se štiti. Vjerojatnost da

će bilo koji predefinirani sustav zaštite biti optimalan pada razmjerno rastu zahtjeva na taj sustav. Stoga optimalan pristup problematici zaštite treba biti holistički po svojoj prirodi.

Holistički sustav zaštite pretpostavlja gledanje na samu zaštitu kao na problem koji treba riješiti, a ne kao na dilemu koji od ponuđenih pristupa, odnosno tehnologija odabrati. Valja imati na umu da se sigurnosni problemi mogu riješiti na cijeli niz načina, od kojih se većina ne nalazi u katalozima proizvođača uređaja tehničke zaštite ili brošurama zaštitarskih poduzeća. Određena količina ulaganja u strogo namjenska sredstva može biti nužna, no vrlo je vjerojatno da se barem dio problema može riješiti razumijevanjem njihovih uzroka, odnosno faktora koji pogoduju njihovom nastanku ili razvoju.

U praktičnom smislu, to također znači da je preporučljivo svaku predloženu mjeru zaštite razmotriti u kontekstu njezinih učinaka, a ne samo oblika. Ako se, na primjer, razmišlja o angažiranju tjelesne zaštite, potrebno je postaviti pitanje koji je ciljani ishod takve mjere. Ukoliko se razmišlja samo o funkciji neke mjere zaštite, može se zanemariti činjenica da funkcija i svrha nisu nužno identični. Ako je primarni cilj postavljanja tjelesne zaštite na nekom objektu kontrola pristupa u prostorije za koje je potrebno posebno dopuštenje, možda se taj cilj ekonomičnije može ostvariti instalacijom odgovarajućeg sustava tehničke zaštite. Niti jedna komponenta zaštite ne bi smjela biti samoj sebi svrha. Uz izuzetak mjera propisanih zakonom, izgled i funkcioniranje sustava zaštite fleksibilni su unutar granica koje postavljaju samo dva čimbenika: raspoloživa financijska sredstva i sposobnost osoba odgovornih za njegovo osmišljavanje i implementaciju.

Popularan pristup osmišljavanju sustava zaštite koji često usvajaju osobe nedovoljnog iskustva ili samostalnosti temelji se na kopiranju sustava nekog drugog poduzeća ili organizacije. Učinkovitost i isplativost takvog pristupa u najvećoj će mjeri ovisiti o stupnju sličnosti ta dva poduzeća. No čak i ako se radi o naizgled vrlo sličnim organizacijama, doslovno preslikavanje „najboljih praksi“ vjerojatno neće biti optimalno, budući da uvijek postoji cijeli niz suptilnih razlika koje mogu imati izražen utjecaj na oblikovanje sustava sigurnosti. Poduzeće koje želi smanjiti troškove svog sustava zaštite, a u slučaju da je isti formiran po uzoru na neko drugo poduzeće, trebalo bi razmotriti koliko su kapaciteti tog sustava prilagođeni njihovim specifičnim potrebama.

4. METODE OPTIMIZACIJE SUSTAVA ZAŠTITE PODUZEĆA

U ovom poglavlju iznesene su neke ideje i principi koje je preporučljivo razmotriti kada se dizajnira sustav zaštite za poduzeće s ograničenim budžetom, odnosno kada se pokušava optimizirati postojeći sustav tako da se smanje izdaci, a pritom ne ugrozi poslovanje neprimjerenim smanjenjem razine sigurnosti. Kao što je to navedeno u poglavlju 1, specifičnosti poduzeća diktirat će primjenjivost ili neprimjenjivost pojedinih pristupa.

4.1. Revizija rizika

Revizija ulaganja u sustav zaštite trebala bi početi od početka, odnosno procjene rizika i opasnosti. Ulaganje je smisleno samo u onoj mjeri u kojoj je usmjereno prema zaštiti od pravih opasnosti. Nažalost, procjena opasnosti uvijek će u određenoj, često nezanemarivoj mjeri biti subjektivna. Tablica 1 sadrži prikaz niza čimbenika koji utječu na percepciju opasnosti, odnosno rizika.

Tablica 1. Čimbenici koji utječu na percepciju opasnosti/rizika

Suglasnost	Rizici s kojima pojedinac nije suglasan percipiraju se većima od onih s kojima jest.
Kontrola	Rizici koje kontroliraju drugi percipiraju se većima od rizika pod kontrolom pojedinca.
Poznatost	Nepoznati rizici percipiraju se većima u odnosu na poznate rizike.
Ravnomjernost	Neravnomjerno distribuirani rizici percipiraju se većima od ravnomjerno raspoređenih rizika.

Korist	Rizici s nejasnom koristi percipiraju se većima od rizika s jasnom koristi.
Razumijevanje	Rizici koje je teško razumjeti percipiraju se većima od onih koje je lagano razumjeti.
Nesigurnost	Neznani rizici percipiraju se većima od znanih rizika.
Strah	Rizici koji generiraju intenzivne emocije poput straha percipiraju se većima od onih koji ne uzrokuju tako snažne emotivne reakcije.
Povjerenje	Rizici povezani s osobama ili ustanovama niskog kredibiliteta percipiraju se većima od onih vezanih uz pouzdane osobe ili organizacije.
Reverzibilnost	Rizici s nereverzibilnim učincima percipiraju se većima od rizika vez takvih učinaka.
Osobni ulog	Rizici na osobnoj razini percipiraju se većima od manje osobnih rizika.
Etička i moralna priroda	Rizici uz koje se vežu negativne etičke ili moralne konotacije percipiraju se većima od onih uz koje se vežu pozitivne etičke ili moralne konotacije.
Porijeklo	Rizici koje uzrokuje čovjek percipiraju se većima od prirodnih rizika.
Identitet žrtve	Rizici koji uključuju žrtve koje se mogu identificirati percipiraju se većima od onih gdje su žrtve izražene isključivo statističkim podacima.
Katastrofični potencijal	Rizici koji stvaraju prostorno ili vremenski zgusnute žrtve percipiraju se većima u odnosu na one koji su difuzni u odnosu na prostor i vrijeme.

Izvor: Proske, D.: Catalogue of Risks. - Springer-Verlag, 2008.

Jedan od čimbenika koji često dovode do pogrešne slike o stvarnosti sigurnosnih potreba nedvojbeno su mediji. Sklonost medija da preuveličavaju opseg, neposrednost i stupanj prijetnje koja je u danom trenutku popularna može iskriviti sliku o opasnostima koje prijete danom poduzeću. Iako praćenje sigurnosnih rizika eksponiranih u medijima može biti korisno za osobu zaduženu za sigurnost određene organizacije u smislu proširivanja razumijevanja potencijalnih opasnosti, te opasnosti moraju se staviti u njihov kontekst kako bi se ispravno odredilo koliko je nešto što se događa u osjetno različitim okolnostima relevantno za konkretnu situaciju u pitanju. Također, u takvim situacijama za očekivati je da će poduzeća koja se bave tjelesnom i tehničkom zaštitom pokušati iskoristiti nastalu tržišnu situaciju i početi nuditi dodatna sigurnosna rješenja dizajnirana za zaštitu od tih specifičnih prijetnji, te iste prezentirati potencijalnim klijentima kao nužnost u svjetlu novonastalih opasnosti. Stalan kontakt sa stvarnim stanjem na terenu i mentalna imunizacija na medijski senzacionalizam nužni su odgovornoj osobi kako bi izbjegla preusmjeravanje sredstava namijenjenih štićenju od realnih opasnosti u nepotrebna sredstva i metode.

U kontekstu optimizacije sustava zaštite u odnosu na reviziju rizika, treba se ukratko osvrnuti i na koncept „sigurnosne predstave“ [5]. „Sigurnosna predstava“ ili „sigurnosno kazalište“ termin je kojim se opisuje jedan od sljedeća dva pristupa: a) uvođenje sigurnosnih mjera upitne ili znano niske učinkovitosti kako bi se kod ciljane publike stvorio osjećaj veće sigurnosti u slučajevima kada se na stvarnu prijetnju zbog bilo kojeg razloga ne može odgovoriti učinkovitim protumjerama, ili b) uvođenje učinkovitih mjera zaštite usmjerenih prema malo vjerojatnim, ali u danom trenutku naglašeno razvikanim prijetnjama kako bi se kod ciljane publike stvorio osjećaj veće sigurnosti. Neovisno o tomu radi li se o slučaju a ili b, „sigurnosna predstava“ formalno se ne može svrstati u skup procesa optimizacije sigurnosti, posebice s financijskog stajališta. S druge strane, zahtjevi stvarnog svijeta nerijetko će ju uključivati kao nužnost, posebice kada se radi o poduzećima koja su naglašenije okrenuta javnosti u svojem poslovanju. Kao posljedica trenutno najpopularnije prijetnje eksponirane u medijima, stručnjaci za sigurnost naći će se u položaju u kojem će biti prisiljeni implementirati neke od mjera koje će po svojoj prirodi potpadati pod definiciju „sigurnosne predstave“. Ukoliko žele ostati konkurentna na tržištu, poduzeća moraju biti spremna dati odgovor svojim klijentima na pitanje što poduzimaju u vezi prijetnji koje mediji u danom trenutku ističu kao relevantne. U takvim situacijama, pokušaji objašnjenja da te prijetnje nisu realne ili da je njihova priroda takva da nije moguće učinkovito se štititi od njih izlažu poduzeće opasnosti da bude percipirano kao nespremno ili nesposobno. Promatrajući tu problematiku u kontekstu cjelokupnog

poslovanja, odgovorne osobe mogu doći do zaključka da je ulaganje u probrana sredstva „sigurnosne predstave“ nužno u cilju održavanja pozitivnog imidža poduzeća, te kao takvo ne podliježe reviziji u cilju smanjenja troškova, budući da je postojanje tih mjera samo sebi svrha.

4.2. Tehnička zaštita

Pod utjecajem okruženja koje uzdiže nove tehnologije i predstavlja ih kao nužnost, odgovornim osobama može biti teško ostati dovoljno objektivan. Za očekivati je da će prodavač opreme za tehničku zaštitu potencijalnom klijentu prvo ponuditi najnovije, najkvalitetnije i, vrlo vjerojatno, najskuplje inačice svojih sustava i komponenti. U tom segmentu nužno je jasno razlučiti želje od potreba. Kao što je to najčešće slučaj i s drugim sofisticiranim tehničkim proizvodima, modeli koji su tek izašli na tržište uglavnom su neproporcionalno skupi u odnosu na kvalitativni pomak koji nude svojim performansama. Drugim riječima, dvostruko skuplja kamera za video nadzor nije nužno dvostruko bolja. No čak i uz pretpostavku da jest, to još uvijek ne znači da njezina kvaliteta opravdava takav izdatak. Budući da se sustav tehničke zaštite nikada ne bira isključivo na osnovu njegovih tehničkih specifikacija, već se uzimaju u obzir karakteristike lokacije i predviđena primjena, realna situacija rijetko će zahtijevati investiciju u najbolji dostupni model. Svaka sposobnost sustava koju nije moguće ili potrebno koristiti na lokaciji predstavlja potencijalnu uštedu.

Implementacija mjera štednje na području sustava tehničke zaštite pretpostavlja da odgovorna osoba bude upoznata sa sredstvima tehničke zaštite, kao i sa specifičnostima štićenog prostora. Pokušaj ostvarivanja uštede uz zanemarivanje bilo kojeg od ta dva uvjeta bit će suboptimalan s jedne strane, odnosno štetan s druge, ukoliko se odaberu sredstva nezadovoljavajućih kapaciteta. Također, sustav tehničke zaštite mora se promatrati kao integralni dio cjelokupnog sustava zaštite. Iako je određeni stupanj redundancije teoretski uvijek poželjan kada se radi o zaštiti, preporučljivo je razmotriti u kojem se stupnju različiti vidovi zaštite preklapaju, te mogu li se neki od njih smanjiti ili u potpunosti eliminirati a da ukupna razina zaštite ostane zadovoljavajuća.

U konačnici, tehnički elementi sustava zaštite samo su onoliko učinkoviti koliko je učinkovit ljudski faktor zadužen za brigu o njima. Bez ozbiljnog i savjesnog pristupa osoblja odgovornog za reakciju u slučaju dojave sa sustava tehničke zaštite, preventivna vrijednost tog sustava gotovo je ravna nuli. U takvim slučajevima najviše što se može očekivati od sredstava tehničke zaštite jest pomoć pri rekonstrukciji zbivanja nakon što je šteta već počinjena. Drugim riječima, ulaganje u skupi i sofisticirani sustav tehničke zaštite mora biti združen s ulaganjem u kvalitetni operativni kadar ukoliko se želi maksimalno iskoristiti njegov preventivni potencijal.

4.3. Tjelesna zaštita

Odluka za ili protiv tjelesne zaštite na objektu je dvosjekli mač. S jedne strane, moderni sustavi tehničke zaštite uspješno smanjuju potreban broj osoblja posvećenog pružanju zaštite; s druge strane, time se ne uklanja u potpunosti potreba za prisutnošću živog djelatnika, posebice u određenim situacijama koje zahtijevaju brzu reakciju. Ukoliko se odgovorne osobe odluče za tjelesnu zaštitu, ona može biti jedna od najskupljih stavaka u budžetu za sigurnost objekta, budući da se radi o redovitim mjesečnim izdacima koje nije moguće smanjiti ispod određene granice.

Ako će u jednom trenutku u budućnosti i nastupiti vrijeme kada neće biti potrebe za tjelesnom zaštitom, ono je još uvijek vrlo daleko od nas. Kvalitetna osoba s primjerenom obukom i zakonskim ovlastima ostaje nužnost za određeni broj poduzeća. Potreba za tjelesnom zaštitom mora se objektivno i kritički razmotriti. Ako se zaključi da ona postoji, nužno je prihvatiti i činjenicu da ona ima svoju cijenu. Pokušaj smanjenja troškova odabirom najnižeg ponuđača usluga nije nužno mudro rješenje, budući da eventualna ušteda nije vrijedna rizika koji slijedi iz povjeravanja brige o sigurnosti poduzeća nesposobnim ili nepouzdanim osobama. Nekoliko faktora koji bi se trebali uzeti u obzir pri optimiziranju modela odabira dobavljača zaštitarskih usluga jesu:

a) kvaliteta zaštitarskih djelatnika. Jesu li zaštitari dodijeljeni štićenom objektu kvalificirani, opremljeni i sposobni za obavljanje svojih svakodnevnih zadaća? Kao što je slučaj sa sustavima

tehničke zaštite, atraktivnije nije nužno bolje ako se radi o kapacitetima koji nisu primjenjivi na konkretnom objektu. Uključuje li ponuđena cijena sposobnosti koje izgledaju dobro na papiru ali koje nikada neće doći do izražaja? Kao što nije racionalno za poduzeće da zapošljava prekvalificirane radnike na drugim radnim mjestima, plaćanje prekvalificiranih zaštitara, koliko god njihove deklarirane sposobnosti zvučale atraktivno, troši sigurnosni budžet koji bi se mogao bolje raspodijeliti. Kvalitetni djelatnici imaju svoju objektivnu cijenu koju opravdavaju svojim radnim učinkom. Sve više od toga u većini slučajeva predstavlja neopravdan trošak.

b) fleksibilnost dobavljača zaštitarskih usluga. Koliko pažnje zaštitarsko poduzeće posvećuje specifičnim potrebama svakog klijenta? Možete li tražiti zamjenu djelatnika ukoliko niste zadovoljni nekim od postojećih koji su dodijeljeni vašem objektu? Može li zaštitarsko poduzeće osigurati dodatne djelatnike van redovnog rasporeda u kratkom vremenskom roku, i koliko se razlikuje cijena izvanrednih od redovitih usluga tjelesne zaštite? Je li zaštitarsko poduzeće u mogućnosti pružiti objedinjenu sigurnosnu uslugu, ili je usko specijalizirano? Davatelj zaštitarskih usluga mora od samog početka pokazati razumijevanje za specifične potrebe štićenog objekta i biti motiviran dugotrajnom uzajamno korisnom suradnjom, kako bi korisniku mogao ponuditi optimalan održivi model zaštite, a ne samo što veći broj svojih djelatnika u cilju povećanja zarade.

4.4. Informatička sigurnost

Područje informatičke sigurnosti kompleksno je i podložno konstantnim promjenama, budući da evolucija prijetnji zahtijeva adekvatni odgovor u obliku poboljšanja obrambenih mjera. U skladu s time, za informatičku sigurnost unutar većih poduzeća obično postoje specijalizirana radna mjesta. Opravdava li opseg poslovanja i potencijalna izloženost napadima ta radna mjesta, pitanje je na koje nije moguće dati općeniti odgovor. Za većinu manjih poduzeća, osoblje zaduženo za brigu o informatičkim sustavima obično će posjedovati dovoljno znanja o prijetnjama računalnim sustavima da te prijetnje svede na prihvatljivo nisku mjeru. Ukoliko postoji sumnja o dovoljnoj kvalificiranosti u tom segmentu, ulaganje u dodatnu edukaciju može se pokazati isplativije od angažiranja vanjskih suradnika ili otvaranja radnog mjesta isključivo za taj dio posla. U svakom slučaju, količina i raznolikost prijetnji računalnom poslovanju u porastu je, i trenutno ne izgleda realno očekivati da će takav trend usporiti ili prestati. Sukladno tomu, važnost solidne informatičke sigurnosti rasti će, budući da će potencijal štete koju uspješan napad na računalne sustave može nanijeti također rasti. To će u velikoj mjeri dovesti do premještanja težišta u budžetu za sigurnost u korist informatičke sigurnosti. Paralelno s time, tržište će postajati sve zasićenije raznovrsnim proizvodima čiji će proizvođači naglašavati njihovu jedinstvenost i nužnost za učinkovitu obranu od novih prijetnji. U tom kontekstu kvalificirani stručni kadar pokazat će se najboljom mjerom uštede, budući da će isti biti u stanju razlučiti nužna ulaganja od reklamnih trikova, i biti manje podložan pomodnim trendovima koji objektivno pridonose vrlo malo stvarnom povećanju razine informatičke sigurnosti.

4.5. Procedure i interni propisi

Jedan od financijski najnezahtjevnijih načina za poboljšanje sigurnosti operacije ili poduzeća sastoji se od osmišljavanja i implementacije zdravih sigurnosnih procedura i internih propisa. To je istovremeno i jedno od najmoćnijih oruđa za povećanje razine zaštite, budući da je ljudski faktor još uvijek odgovoran za većinu slučajeva narušene sigurnosti. Njegovi glavni aduti su fleksibilnost i mogućnost savršenog prilagođavanja upravo onoj operaciji ili poduzeću kojoj je namijenjeno. Kao primjer proceduralne mjere možemo uzeti podjelu dužnosti unutar poduzeća, zajedno s pripadnim ovlastima, na način koji pojedincu otežava samostalno izvođenje nedopuštenih aktivnosti [6]. Budući da niti jednom pojedincu nisu dodijeljene ovlasti koje bi mu omogućile da neotkriveno poduzme korake na štetu poduzeća, općenita razina sigurnosti raste jer se sa svakom novom osobom koju je nužno uključiti u planiranje spomenutih aktivnosti povećava vjerojatnost pravovremenog otkrivanja i prevencije. Podjela dužnosti i ovlasti kao proceduralna mjera često se može izvesti uz minimalna financijska ulaganja ili čak bez ikakvih financijskih troškova.

Ipak, nužno je imati na umu da niti jedna mjera zaštite, pa tako ni ona u obliku procedura i propisa, nije u potpunosti besplatna. Svako povećanje razine zaštite nosi sa sobom određenu cijenu, makar

ona ne bila nužno u obliku novca. Jedan oblik plaćanja za proceduralnu sigurnost može se manifestirati u obliku nezadovoljstva djelatnika. Izvođenje neke operacije sigurnije gotovo je uvijek zahtjevnije nego njezino izvođenje na nesiguran način. Nakon što se provede dovoljan broj ponavljanja nekog postupka, djelatnik ga internalizira i time on postaje automatski, odnosno prestaje biti percipiran kao teret. No tijekom prijelaznog razdoblja realno je očekivati određen stupanj otpora od strane djelatnika, posebice ako opća sigurnosna svijest nije naročito visoka. To je vrijeme kada osoba zadužena za sigurnost mora posvetiti posebnu pažnju načinu na koji se nove mjere sprovode u praksu. Samo informiranje djelatnika o novom obaveznom načinu postupanja nije dovoljno jamstvo da će taj način postupanja biti usvojen, budući da su ljudi prirodno skloni domišljanju naizgled uvjerljivih razloga da zaobiđu sigurnosne procedure. Ti razlozi objašnjavaju se kao težnja za većom produktivnošću, iako su često samo posljedica inercije i prirodnog otpora novom načinu obavljanja već dobro poznatih zadataka. Ukoliko se u toj fazi djelatnici ne nadgledaju, odnosno ako se tolerira ignoriranje sigurnosnih procedura, prijeti opasnost da se stvori iluzija sigurnosti koju bi trebale pružati nove mjere, dok u stvarnosti te sigurnosti nema jer se mjere ne primjenjuju dosljedno. Dosljednost je u ovom kontekstu ključna riječ, jer je ona jedino jamstvo pouzdanosti. Uzevši gore navedeno u obzir, razvidno je da i proceduralne mjere zaštite imaju svoju cijenu, a ona se manifestira u obliku vremena i truda uloženog u razvoj odgovarajućih procedura, primjerenu edukaciju osoblja, te napor uložen da se tijekom početnog razdoblja osigura dosljedno usvajanje tih procedura do trenutka kada one postaju prirodan dio obavljanja radnih zadaća.

ZAKLJUČAK

Iskustva iz prakse pokazuju da je sigurnost područje koje je često prvo izloženo rezovima kada se poduzeće mora suočiti s ograničenjem financijskih i drugih resursa. Budući da sam doprinos sektora sigurnosti profitabilnosti poduzeća uglavnom nije izravno vidljiv, needuciranom osoblju lako je na segment zaštite početi gledati kao na luksuz ili formalnost. Također, veliki broj načina na koji se sustav zaštite može organizirati, kao i pripadnih tehničkih pomagala, mogu stvoriti dojam da je zaštita nešto što je u svojoj biti nužno vrlo kompleksno, a time i skupo. No pomnije razmatranje sigurnosnih potreba u kontekstu ciljeva koje je potrebno ostvariti, a ne samih procedura ili pomagala koje treba implementirati, može uvelike doprinijeti pojednostavljenju samog sustava, čime mu se smanjuje cijena i olakšava njegova svakodnevna uporaba. Nuđenjem dobro osmišljenih, specifičnih sigurnosnih rješenja, povećava se vjerojatnost da će osobe na odgovornim položajima ta rješenja usvojiti. Prilikom dizajniranja takvih rješenja, nužno je na sigurnost gledati kao na sredstvo koje pomaže uspješnom poslovanju poduzeća, te ju tako i predstavljati. Težnja za predstavljanjem sigurnosnih sustava kao nečeg izuzetno kompleksnog u najvećem broju slučajeva služi samo poticanju sumnjičavosti u osoba koje u konačnici donose odluku o tome hoće li se u sigurnost uložiti odgovarajuća sredstva ili ne. Ako se važnost segmenta zaštite uspije prikazati u svjetlu promicanja ukupne profitabilnosti poslovanja poduzeća, time se povećava vjerojatnost da će mu se posvetiti primjerena pažnja, a prvi korak na tom putu jest njegovo pojednostavljenje na razinu koja zadržava svoju funkcionalnost, ali ga istovremeno čini razumljivim i smislenim i u očima osoba čija primarna djelatnost nije sigurnost.

LITERATURA

[1] Samuelson, P., Nordhaus, W.: **Microeconomics**. - McGraw Hill, 2001.
[2] Bayuk, J. L.: **Enterprise security for the executive: setting the tone from the top.** – ABC-Clio llc, 2010.
[3] Taleb, N.: **The Black Swan.** – Random House, 2007.
[4] Fischer, R. J., Halibozek, E., Green, G.: **Introduction to Security, Eighth Edition.** – Oxford: Elsevier Inc, 2008.
[5] Schneier, B.: **Beyond Fear.** - Springer-Verlag, 2003.
[6] Contos, T. B.: **Enemy at the Water Cooler.** – Syngress Publishing Inc, 2006.