HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Fizička sigurnost informacijskih sustava

CCERT-PUBDOC-2007-11-209

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

U današnjem kompetitivnom poslovnom svijetu negativan publicitet i financijski gubici, koji nastaju kao posljedica sloma fizičke sigurnosti informacijskih tehnologija, mogu biti pogubni. Jedan takav slom fizičke sigurnosti može dovesti (i najčešće dovodi) do prodaje dionica, smanjenja prihoda, korporativnih parnica, nezadovoljnih zaposlenika, sramotnih situacija za tvrtku te ogromne količine vremena i truda potrošenih na istraživanje problema i njihovo uklanjanje. Današnje sigurnosne inicijative, jednako kao što uključuju očuvanje zgrada i opreme, uključuju i čuvanje mreža, bavljenje sigurnosnim problemima i upravljanje rizicima. Donedavno su u većini organizacija sustavi za upravljanje fizičkim i logičkim pristupom bila dva različita, neovisna sustava i njima su se bavili potpuno odvojeni sektori. Primjerice, sustavima za upravljanje logičkim pristupom, koji dodjeljuju prava pristupa informacijskoj infrastrukturi (kao što su intranet/internet, poslužitelji elektroničke pošte, web poslužitelji i aplikacije za pristup bazama podataka), bavio se IT sektor. Sektor za upravljanje resursima bavio se fizičkim pravima pristupa, koja uključuju etiketiranje zaposlenika, pristup ulazima u zgrade, sustav zdravstvenog osiguranja i sl. Danas se ova dva aspekta sigurnosti sve češće objedinjuju pa i fizička sigurnost prelazi u nadležnost IT sektora. Što točno podrazumijeva fizička sigurnost i na koji način je pravilno organizirati pitanja su kojima se bavi ovaj dokument.

2. Općenito o fizičkoj sigurnosti

Sustavi za upravljanje fizičkom sigurnošću služe za kontrolu pristupa resursima (objektima) tvrtke, odnosno određuju tko ima pristup, kada i pod kojim uvjetima. Tipična infrastruktura jednog takvog sustava sastoji se od:

- kontrole fizičkog pristupa - čitači kartica ili biometrijski uređaji (čitači otiska dlana/prsta, prepoznavanje lica i sl.),
- sustava za upravljanje energijom – UPS (eng. *Uninterrupted Power Supplies*) generatori, rezervne baterije, sustavi za distribuciju električne energije i td.,
- sustava za fizičko blokiranje i mehanizama zaključavanja, npr. elektromagnetski uređaji zaključavanja,
- sustava za kontrolu požara – prskalice, detektori dima, detektori ugljičnog monoksida i dr.,
- sustava za poboljšanje uvjeta rada – grijanje i hlađenje, ventilacija, HVAC sustavi (eng. *Heating, Ventilation, and Air Conditioning*), mjerači vlage u zraku, temperature i sl., te
- sustava za video i audio nadzor – npr. CCTV (eng. *Closed-circuit Television*) sustavi te njihova infrastruktura (CSU/DSU, FDDI prstenovi, ATM (eng. *Asynchronous Transfer Mode*) mreža i dr.).

Spomenuti sustavi međusobno komuniciraju koristeći infrastrukturne usluge koje im osigurava IT sektor. Primjerice, čitač kartica na ulazu može na taj način biti povezan sa sustavom za kontrolu požara, koji je povezan sa CCTV sustavom, a kojeg nadzire sustav za upravljanje fizičkom sigurnošću.
Fizička sigurnost usmjerena je na zaštitu imovine, ljudi i strukture. Nadalje, bavi se nadziranjem i upravljanjem tokom ljudi i imovine kroz prostor. Upravo se iz tog razloga, upravljanje metodama pristupa, uočavanje neovlaštenih upada i sl., mora provoditi svakodnevno s ciljem osiguravanja što bolje fizičke zaštite.

2.1. Ljudi su rizik

Kada se spomene sigurnost podataka, prva stvar koja u većini slučajeva padne na pamet jest zaštita od sabotaže, špijunaže ili krađe podataka. Iako je očita potreba za zaštitom od napadača i potencijalne štete koju bi oni mogli prouzročiti, u mnogo slučajeva veći rizik za poslovanje predstavljaju opasnosti koje su posljedica svakodnevnih aktivnosti zaposlenika tvrtke. Ljudi su neophodni za pravilno djelovanje podatkovnih centara, ali, istraživanja pokazuju da su oni sami, preko raznih nesreća i pogrešaka (neodgovarajuće procedure, pogrešno označena oprema, stvari koje ispadaju ili se proliju, pogrešno utipkane naredbe, i sl.), izravno odgovorni za 60% vremena zastoja centara. Upravo zbog ljudskih grešaka i činjenice da su oni ipak neophodni za odgovarajuću funkcionalnost centara, potrebno je maksimalno smanjiti i nadzirati pristup osoblja resursima kompanije, jer je na taj način najlakše upravljati možebitnim rizicima, čak i u slučaju kad postoje male izgledi zloporabe pristupa.
U novije vrijeme, oprema potrebna za identifikaciju zaposlenika i kontrolu pristupa mijenja se jednako brzo kao što se javljaju nove informacije, novi resursi i sl. Zbog tog stalnog pojavljivanja nove opreme i novih tehnologija, često se zaboravlja da problem koji bi sva ta tehnologija trebala riješiti nije složen niti je tehničke prirode, Radi se o sprečavanju neovlaštenog pristupa određenim područjima osobama kojima tamo nije mjesto. I iako prvi korak u tom procesu - označavanje područja koja treba osigurati i definiranje pravila pristupa – može rezultirati slojevitim i složenim planom zaštite, on intuitivno i nije toliko zahtjevan, budući da IT menadžeri već znaju kome se treba dozvoliti pristup kojem području. Problem se javlja kod drugog koraka, tj. odluke kako najbolje primijeniti ne tako savršene tehnologije koje stoje na raspolaganju i koje treba objediniti s ciljem optimalne izvedbe prethodno definiranog plana zaštite.

2.2. Osnovne smjernice – tko i zašto

Iako pojava novih sigurnosnih tehnologija može djelovati egzotično i tajanstveno, postoje tehnologije koje se nisu mijenjale od samih početaka njihove uporabe, a jednostavne su i razumljive svima nama te nam osiguravaju pouzdan odgovor na pitanje "Tko si ti i što radiš ovdje?". To su npr. otisci prstiju, skeniranje očiju, pametne kartice, čitači geometrije lica i dr.

Prvi dio prethodno navedenog pitanja uzrokuje većinu problema kod dizajniranja automatskih sigurnosnih sustava. Sve trenutno postojeće tehnologije trude se ocijeniti identitet osobe na ovaj ili onaj način, s različitim razinama točnosti i samim time, različitim cijenama same opreme. Npr. magnetska kartica je jeftina, ali nikad se ne može sa sigurnošću utvrditi tko ju zaista koristi te to onemogućava sigurnu procjenu identiteta osobe. S druge strane, skener šarenice (eng. *iris*) je vrlo skup, ali omogućava prilično sigurnu provjeru identiteta. Upravo postizanje kompromisa između točnosti i cijene tehnologija, čini osnovu gradnje sigurnosnih sustava.
Odgovor na drugi dio pitanja, "što radiš ovdje?", često se može zaključiti odmah nakon identifikacije osobe (npr. ako se radi o osobi koja je zadužena za rad sa pisačima, očito je da je upravo ispis nekog dokumenta razlog njenog dolaska). Ipak, traženje odgovora na to pitanje može se implementirati i na brojne druge načine, primjerice, kod magnetskih kartica, otkriveni identitet osobe može automatski pozvati niz informacija iz određene datoteke u kojoj su zabilježeni dozvoljeni razlozi pristupa. Također, mogu se implementirati različite pristupne metode za različita područja i različite namjene. Često se odgovori na oba pitanja kombiniraju, a zna se dogoditi i da je kod određivanja prava pristupa dovoljan odgovor na samo jedno od njih.

3. Područje zaštite i prava pristupa

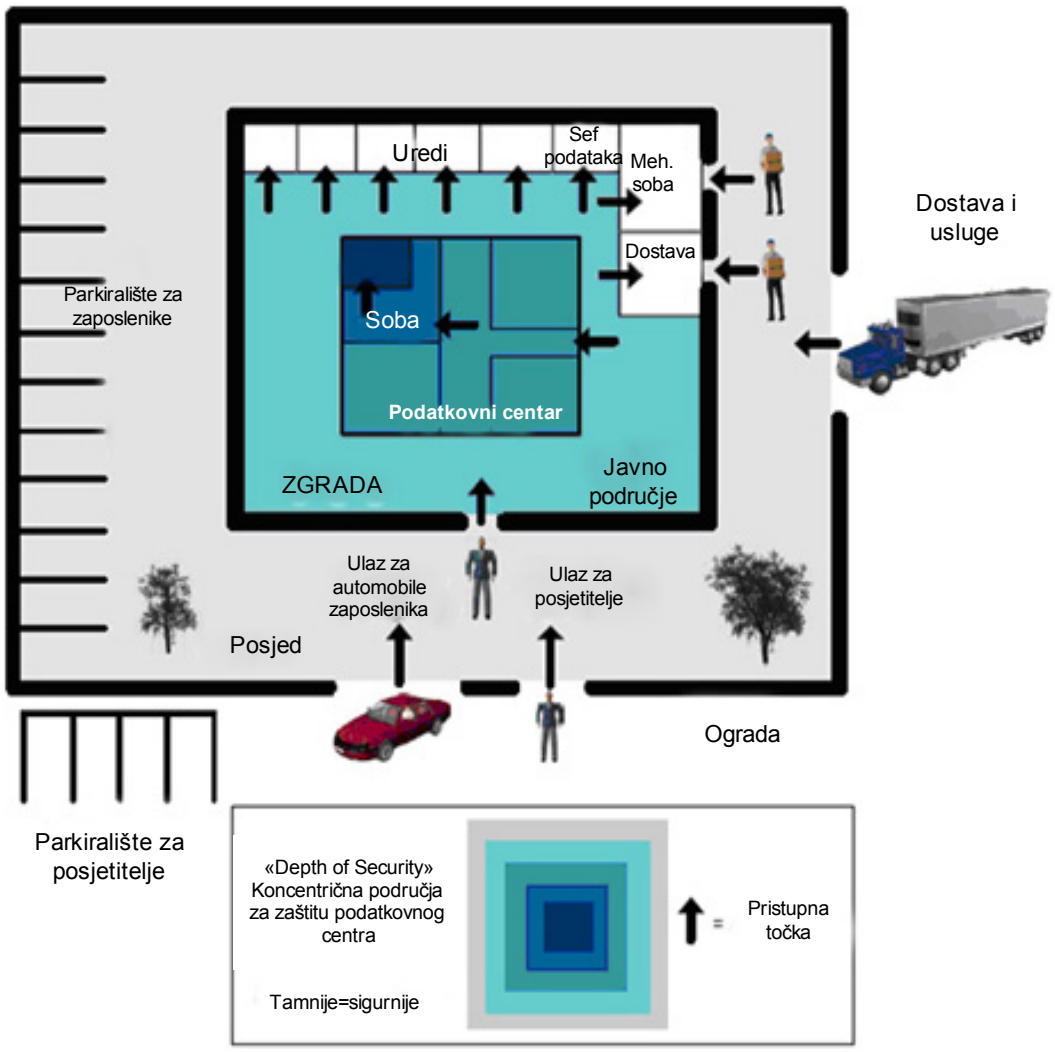
Prvi korak u izradi sigurnosnog plana je upravo izrada plana fizičkih objekata te identificiranje područja i ulaznih točaka koje zahtijevaju različita prava pristupa ili različite razine sigurnosti.
Ta područja mogu imati koncentrične granice:

- opseg područja,
- opseg gradnje,
- računalno područje,
- računalne sobe i
- police za opremu.

Ili bočne, tzv. *side-by-side* granice:

- područja za posjetitelje,
- uredi i
- komunalne sobe.

Koncentrična područja često imaju različite ili vrlo oštre pristupne metode, koje osiguravaju dodatnu zaštitu nazvanu *depth of security.* Na taj je način određeno unutarnje područje zaštićeno vlastitim pristupnim metodama i metodama onih područja koja ga okružuju.



Slika 1. Prikaz definicije razina sigurnosti

Sigurnost na razini ormara *(eng. Rack-Level Security)* – u unutarnjem *"depth of security"* sloju nalazi se ormar (poslužiteljski / mrežni / komunikacijski). Zaključavanje ormara zasad se rijetko koristi, ali u slučaju korištenja, služi kao posljednja obrana od neovlaštenog pristupa kritičnoj opremi. Bilo bi neobično da svi imaju potrebu za pristupom svakom ormaru u sobi punoj ormara – upravo zato zaključavanje ormara omogućava ograničenje pristupa samo na one zaposlenike koji su zaduženi za pojednini resurs. Isto tako, uvode se udaljena zaključavanja ormara, koja omogućuju dopuštanje pristupa osoblju samo u neophodnim situacijama, i to određenim ljudima u određeno vrijeme. Tako se smanjuje rizik od nesreća, sabotaže ili neovlaštene instalacija dodatne opreme, koja bi mogla trošiti previše energije i prouzročiti visoke temperature unutar ormara te na taj način uzrokovati njegovo oštećivanje.

Infrastrukturna sigurnost (eng. *Infrastructure Security)* – važno je u plan zaštite uključiti ne samo ona područja koja sadrže funkcionalnu IT opremu određenog postrojenja, već i područja koja sadrže elemente fizičke infrastrukture, čija kompromitacija može uzrokovati zastoj sustava. Primjerice, može doći do namjernog ili slučajnog isključivanja HVAC opreme, krađe baterija potrebnih za rad generatora ili zbunjivanja upravljačke konzole tako da dođe do aktivacije prskalica protiv požara.

Ovlasti koje osoblje posjeduje za pristup osiguranim područjima mogu se temeljiti na različitim informacijama, kao što su prethodno spomenute - identitet i svrha dolaska, ali i neke dodatne kategorije razloga, kojima se mora posvetiti posebna pažnja. Takva je, primjerice, tzv. *need to know*

kategorija. U nastavku je dan opis dva najčešća i spomenutog dodatnog kriterija za izradu plana pristupa.

Osobni identitet - Određene osobe, koje rade u nekom postrojenju, trebaju pristup područjima bitnim za njihovu poziciju. Npr. direktor sigurnosti imat će pristup gotovo svim postrojenjima, ali ne i svim pohranjenim podacima; vođa računalnih operacija mora imati pristup računalnim sobama i operacijskim sustavima, ali ne i mehaničkim sobama i HVAC postrojenjima; CEO (eng. *chief executive officer*) upravitelj mora imati pristup uredima direktora sigurnosti i IT osoblja te javnim područjima, ali ne i računalnim ili mehaničkim sobama.

Razlog dolaska – Na temelju pozicije određene osobe može se zaključiti možebitni razlog ulaska u određeni sektor. Tako npr. osobe zadužene za popravke u postrojenjima mogu imati pristup samo mehaničkim sobama i javnim područjima. Osoblje zaduženo za čišćenje može imati pristup samo javnim područjima. Stručnjak koji se bavi mrežnim komutatorima može imati pristup samo ormarima koji sadrže opremu potrebnu za njihov rad, ali ne i ormarima u kojima se nalaze poslužitelji ili uređaji za skladištenje podataka. U slučaju postrojenja koje se bavi web poslužiteljima, osobe zadužene za održavanje klijentskih sustava mogu imati pristup samo tzv. *"client access"* prostoriji . Ondje su uspostavljene veze prema njihovim osobnim poslužiteljima koje služe obavljanju administratorskih poslova.

Need to know – pristup posebno osjetljivim područjima može se dodijeliti samo određenim ljudima iz posebnih razloga, odnosno ako oni nešto "moraju znati", i samo onoliko dugo dok postoji ta potreba.

4. Metode zaštite/identifikacije

Metode određivanja identiteta ljudi mogu se svrstati u tri kategorije ovisno o pouzdanosti i cijeni opreme:

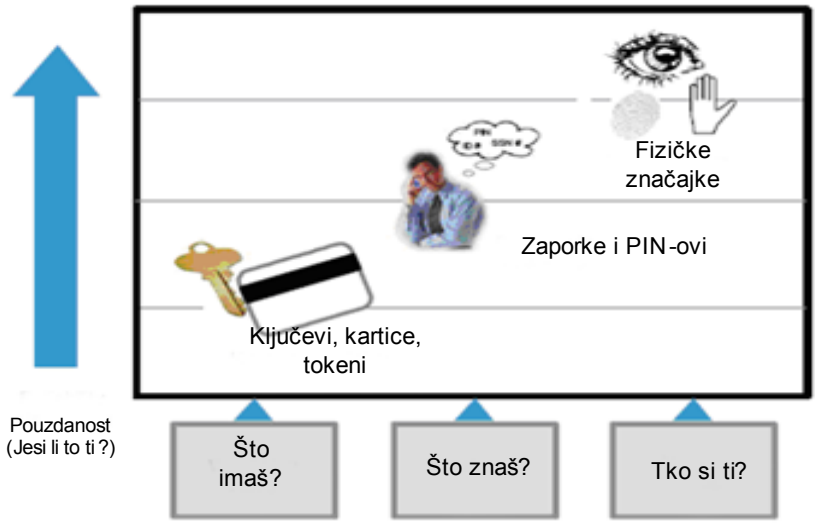
- **što imaš** kategorija,
- **što znaš** kategorija i
- **tko si** kategorija.

Što imaš kategorija je najmanje pouzdana jer se određena sredstva mogu dijeliti ili biti ukradena. U ovu kategoriju uključuju se stvari koje osoblje posjeduje i nosi sa sobom, npr. ključevi, kartice, mali objekti (eng. *token*) koji se mogu pričvrstiti na privjesak ključa. Ključevi su u ovom slučaju "najmanje inteligentna" metoda, dok su kartice s procesorom koji izmjenjuje informacije s čitačem (eng. *smart card)* puno bolja rješenja. To mogu primjerice biti kartice s magnetskom trakom koja sadrži informacije o vlasniku; mogu biti kartice ili tokeni koji sadrže odašiljač i/ili prijemnik, a koji komunicira s čitačem na maloj udaljenosti (eng. *proximity card, proximity token*). Kao što je već spomenuto, ova je kategorija najmanje pouzdana jer nitko ne može jamčiti da određeno sredstvo za identifikaciju koristi upravo njegov vlasnik.

Što znaš kategorija je pouzdanija, ali ipak ne sasvim pouzdana jer, iako sredstvo raspoznavanja ne može biti ukradeno, može se dijeliti ili prepisati. Ovdje se primjerice radi o zaporkama, kodovima ili procedurama koje nešto obavljaju (npr. otvaraju nešto zaključano kodom), verifikaciji čitača kartica ili pristupu računalu preko tipkovnice. U slučaju zaporke ili koda postoji sigurnosna dilema – ako je zaporka lako pamtljiva, lako se može pogoditi. S druge strane, ako je teško pamtljiva, teško će ju biti pogoditi, ali se povećava vjerojatnost njenog prepisivanja, što onda smanjuje sigurnost. Dakle, iako je ovo pouzdanija kategorija, ovdje korištena sredstva se i dalje mogu dijeliti, a u slučaju prepisivanja javlja se rizik od njihovog razotkrivanja.

Tko si kategorija je najpouzdanija jer se odnosi na nešto što je fizički jedinstveno pojedinoj osobi. Dakle ovdje se identifikacija vrši na temelju određenih fizičkih značajki. Kad se ova metoda postigne (ili pokuša postići) tehnološkim načinima, naziva se biometrija (eng. *biometrics*). Neki od razvijenih biometrijskih uzoraka su:

- otisak prsta ili šake (temelji se na obliku prsta i debljini ruke),
- šarenica (uzorak boja),
- pozadina oka (uzorak krvnih žila),
- rukopis (dinamičnost olovke koje se miče) i
- glas .



Slika 2. Prikaz metoda zaštite/identifikacije

Biometrijski uređaji su obično vrlo pouzdani – ako se postigne prepoznavanje, tada je gotovo sigurno da je točno. Glavni razlog sumnje u pouzdanost ovakvih uređaja nije činjenica da dolazi do "krivog" prepoznavanja ili smetnji od strane uljeza, već mogućnost neprepoznavanja korisnika koji ima dodijeljena određena prava pristupa (eng. *false rejection*).

4.1. Uređaji za identifikaciju

Uređaje za identifikaciju također možemo dijeliti u tri gore navedene kategorije:

Što imaš – u ovu kategoriju spada nekoliko vrsta kartica i malih objekata (eng. *Token*) koji se razlikuju po svojim svojstvima:

- mogućnost za preprogramiranje,
- otpornost na krivotvorenje,
- vrsta interakcije s čitačem (provlačenje, umetanje, površinski kontakt, bez kontakta),
- fizičke karakteristike (veličina, lakoća spremanja / nošenja),
- količina pohranjenih podataka,
- sposobnost obavljanja matematičkih operacija,
- cijena kartice / objekta i
- cijena terminala / čitača.

Uzevši u obzir navedena svojstva razlikujemo nekoliko osnovnih kategorija ovih uređaja:

- magnetske kartice na provlačenje (eng. *swipe card*),
- kontaktne magnetske kartice ili barij-feritne kartice – na sebi imaju magnetski uzorak,
- Weigand kartica – sadrži vodič s jedinstvenim magnetskim uzorkom,
- kartica s bar kodom,
- infracrvena kartica – sadrži bar kod sakriven slojem koji je nepropustan za vidljivo svjetlo, ali propustan za infracrveno svjetlo,
- beskontaktna kartica – sadrži jedinstveni identifikator koji se prenosi bežičnim signalom do čitača te
- pametna kartica (eng. *smart card*) – sadrži jedinstveni digitalni potpis koji je kriptiran; ne mora biti u obliku kartice, već može biti i u obliku malog objekta (npr. privjesak za ključeve).

Bez obzira na sigurnost i pouzdanost uređaja iz ove kategorije sigurnost koju oni daju je ograničena činjenicom da nitko ne garantira da je osoba koja ih koristi njihov stvarni vlasnik. Zbog toga je uobičajeno korištenje ovih uređaja zajedno s još nekom od metoda za utvrđivanje identiteta kao što su poznavanje zaporke ili biometrijska potvrda.

Što znaš – u ovu kategoriju ulaze razne tipkovnice za unos zaporke ili kodirane brave. Obje vrste uređaja temelje se na poznavanju zaporke s tim da tipkovnice za unos zaporke prihvaćaju zasebne

zaporke za svakog korisnika dok kodirane brave prihvaćaju samo jednu zaporku za otključavanje brave koju koriste svi. Sigurnost ovih uređaja može se povećati periodičnom izmjenom zaporki, ali to naravno uključuje upotrebu nekog sustava za obavještavanje korisnika o promjeni i distribuciju novih zaporki. Kodirane brave kojima se ne mijenja zaporka moraju biti periodično mijenjane zbog pojave povećanog trošenja tipki koje se koriste kod unosa ispravne zaporke. Naravno i kod ovih uređaja sigurnost se može povećati upotrebom dodatnih biometrijskih provjera.

Tko si – u ovu kategoriju ulaze svi biometrijski uređaji koji sa smanjenjem cijene postaju sve češće korišteni sigurnosni mehanizmi. U kombinaciji s uređajima iz ostale dvije kategorije oni predstavljaju najbolje rješenje za fizičku zaštitu. Biometrijski uređaji se najčešće ne koriste za prepoznavanje korisnika nego za verifikaciju identiteta nakon što je on utvrđen nekom od druge dvije metode. Razlog za to su uglavnom performanse biometrijskih uređaja koje ne dozvoljavaju pretraživanje velikih baza podataka korisnika u kratkom vremenu. Međutim kako se performanse tih uređaja poboljšavaju moguće je i njihovo samostalno korištenje. Međutim postoje dvije vrste problema koji se javljaju kod ovih uređaja:

- Lažno odbijanje – neuspješno prepoznavanje važećeg korisnika. Iako bi se ovo moglo shvatiti kako dodatni element sigurnosti to najčešće predstavlja samo frustraciju za korisnike.
- Lažno prihvaćanje – krivo prepoznavanje, tj. zamjena identiteta nevažećeg korisnika za važećeg. Količina ovakvih grešaka može se reducirati povećanjem praga potrebnog za prihvaćanje, ali time se naravno povećava broj lažnih odbijanja.

Kriterij pri odabiru ovih uređaja stoga mora biti količina lažnih prihvaćanja / odbijanja, cijena opreme i prihvaćanje korisnika, tj. ocjena koliko je korištenje uređaja (ne)lagodno za korisnike. Tako se na primjer uređaji za prepoznavanje uzorka rožnice smatraju uglavnom neprikladnim jer zahtijevaju da korisnik primakne oko na nekoliko centimetara od uređaja koji usmjerava LED diodu izravno u nj .

5. Ostali sigurnosni elementi

Projektiranje sigurnosnih sustava temelji se na uređajima koji će identificirati i prikazati osobe kad ulaze u zaštićenu prostoriju (eng. *"access control"*). To je ujedno sve što bi bilo potrebno za odgovarajuću zaštitu kad bi postojala stopostotna pouzdanost identifikacije, potpuna pouzdanost u namjere ljudi kojima je dozvoljen pristup i fizička savršenost – neslomljivi zidovi, vrata, prozori, ključanice i stropovi. Kako bi se kompenzirale neizbježne slabosti nastale zbog nesavršenosti ili sabotaže, sigurnosni sustavi redovito uključuju dodatne metode zaštite, nadzora i oporavka.

Projektiranje gradnje – u slučaju gradnje novog postrojenja ili nadogradnje postojećeg, fizička se sigurnost može implementirati iz temelja ugradnjom arhitektonskih i konstrukcijskih obilježja koja služe za obeshrabrivanje možebitnih pokušaja neovlaštenog pristupa. Ono što se uglavnom uzima u obzir prilikom gradnje su potencijalni ulazi i mogućnosti bijega, pristup kritičnim infrastrukturnim elementima (kao npr. HVAC i ožičenje) te potencijalne lokacije za skrivanje koje bi uljezi mogli iskoristiti.

Zamke – rješenja koja sprečavaju tzv. *piggybacking* i *tailgating* pokušaje. Radi se o pukušajima iskorištavanja slabosti sustava zaštite zajedničkim ulaskom s ovlaštenom osobom. Kod postupka nazvanog *piggybacking* ovlaštena je osoba sudionik upada i ona, u dobroj namjeri, neovlaštenoj osobi svjesno omogućuje ulazak. *Tailgating*, s druge strane, podrazumijeva neopažen prolazak neovlaštene osobe iza ovlaštene. Zamke, odnosno uobičajena rješenja ovih problema, obično su skučeni prostori u koje može stati samo jedna osoba. Zamke se mogu implementirati s kontrolom pristupa na ulaznim i izlaznim vratima ili samo na izlaznim. U potonjem slučaju neuspjeli pokušaj izlaska iz ograđenog prostora uzrokuje zaključavanje ulaznih vrata i pokretanje alarma koji upozorava na činjenicu da je uljez uhvaćen u zamku. Također, postoji i mogućnost dodatne kontrole – ugradnja detektora koraka u pod, što omogućava provjeru je li samo jedna osoba prošla kroz osigurano područje. Novije tehnologije koje nude rješenje opisanog problema sastoje se od ugradnje kamera koje prate i obilježavaju osobe koje prolaze i pokreću alarm ako detektiraju prolazak više od jedne osobe nakon samo jednog odobrenog ulaza.

Nadzor kamerama – Kamere se i dalje koriste za praćenje oznaka prava pristupa na automobilima koji ulaze u osigurano područje ili u kombinaciji sa senzorima koji detektiraju korake za snimanje prolaska ljudi kroz kritične lokacije. CCTV (eng. *Closed circuit TV*) kamere, bilo da su vidljive ili skrivene, osiguravaju unutarnji ili vanjski nadzor, zastrašivanje možebitnih uljeza i, u krajnjem slučaju, pregled

snimljenih događaja nakon određenog incidenta. Koriste se razni načini snimanja – fiksirani, rotirajući, ili daljinski upravljan.
Ima nekoliko stvari koje se trebaju uzeti u obzir prilikom postavljanja sigurnosnih kamera:

- Je li bitna laka identifikacija snimljenih osoba?
- Je li je dovoljno samo raspoznati prisutnost osoba u prostoriji?
- Snima li se s namjerom otkrivanja otuđivanja određene imovine?
- Služi li kamera samo kao sredstvo zastrašivanja?

U slučaju snimanja CCTV signala, moraju postojati unaprijed određene procedure koje se odnose na sljedeće situacije:

- Kako će se snimljene trake indeksirati i kategorizirati radi lakšeg kasnijeg pronalaska?
- Hoće li se trake spremati na tom području ili izvan njega?
- Tko će imati pristup trakama?
- Kakva je procedura pristupa?
- Koliko će dugo trake biti čuvane prije nego budu uništene?

Nova tehnologija bavi se automatizacijom posla koji su tradicionalno obavljali zaštitari. Jedan od takvih je, primjerice, praćenje TV ekrana. Automatizacija bi se trebala postići uz pomoć programske podrške koja detektira promjene (pokrete) slike na ekranu.
Zaštitari – unatoč velikom broju novih sigurnosnih tehnologija, stručnjaci se slažu da kvalitetno osoblje (zaštitari) još uvijek drži vrh liste metoda za kontrolu pristupa. Zaštitari pružaju mogućnost nadgledanja svim ljudskim osjetilima, a dodatno i mogućnost brze i inteligentne reakcije na sumnjive, neobične ili katastrofalne događaje.
Senzori i alarmi – Svi smo upoznati s tradicionalnim kućnim alarmima i odgovarajućim senzorima koji detektiraju pokrete, promjene temperature, određene kontakte (npr. zatvaranje vrata) i sl. Alarmni sustavi podatkovnih centara osim spomenutih koriste i neke dodatne vrste senzora. Tu se mogu ubrojiti snopovi laserskih zraka koji služe kao barijere kod prolaska, senzori koji detektiraju korake, dodir, vibracije i dr. Također, podatkovni centri često preferiraju tihe alarme na određenim područjima, jer takvi alarmi omogućuju hvatanje uljeza na djelu. Ako su senzori mrežno osposobljeni, njima se može udaljeno upravljati i nadzirati njihov rad uz pomoć različitih nadzornih sustava koji mogu uključivati i podatke o kretanju osoblja dobivene na temelju uređaja za kontrolu pristupa.
Posjetitelji – Rukovanje situacijama s posjetiteljima mora se, dakako, uzeti u obzir kod projektiranja bilo kakvog sigurnosnog sustava. Tipično rješenje je izdavanje privremenih iskaznica ili kartica za područja s manjom potrebom osiguravanja i dodjeljivanje pratnje za jače osigurana područja. Pritom se zbog prethodno spomenutih zamki mora osigurati mogućnost privremenog onesposobljavanja zamke ili dodijeliti posjetitelju ovlasti koje će mu omogućiti pristup.

6. Preporuke

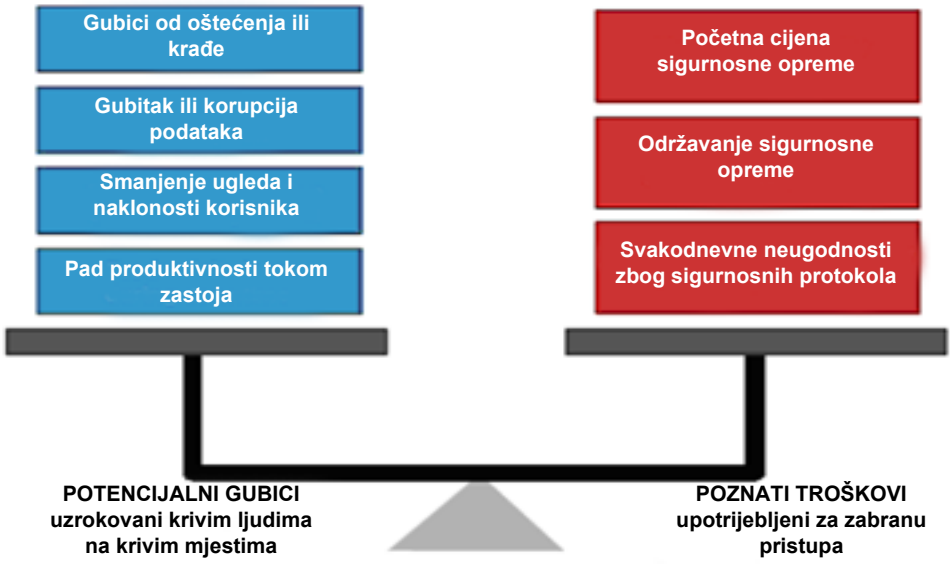
Pravi sigurnosni sustav je onaj sustav koji osigurava najbolji kompromis između rizika i potencijalne štete nastale prilikom neovlaštenog pristupa te cijene samih sigurnosnih mjera, kao i neugodnosti nastalih njihovom primjenom.
Iako svaki podatkovni centar ima svoje jedinstvene značajke pa tako i jedinstvene potencijalne gubitke, postoje neke općenite kategorije gubitaka koje su prisutne u gotovo svakom centru, a to su sljedeće:

- **fizički gubitak** – oštećivanje soba i opreme prilikom nezgoda, sabotaže ili krađe,
- **gubitak IT produktivnosti** – skretanje osoblja s prvobitnih obveza, zbog nadomještanja ili popravka opreme, rekonstruiranja podataka ili čišćenja sustava,
- **gubitak korporativne produktivnosti** – prekid poslovanja zbog određenog zastoja uzrokovanog sigurnosnim problemima,
- **gubitak informacija** – gubitak, zagađenje ili krađa podataka, te
- **gubitak ugleda i naklonosti korisnika** – posljedice težih ili često ponavljanih sigurnosnih problema mogu biti i gubitak posla, pad cijene dionica, parnice i sl.

Prilikom projektiranja sigurnosnog sustava u obzir treba uzeti slijedeće parametre:

- **Cijena opreme** – ograničenja budžeta obično sprečavaju korištenje najpouzdanije identifikacijske opreme. Uobičajen pristup je grupirati različite tehnike ovisno o različitim sigurnosnim razinama.
- **Kombiniranje tehnologija** – pouzdanost identifikacijske opreme na bilo kojoj razini može biti poboljšana kombiniranjem jeftinijih tehnologija sa područjem koje se nalazi najviše u unutrašnjosti te je time zaštićeno vlastitim i svim okolnim sigurnosnim tehnologijama.
- **Prihvatljivost od strane korisnika** – tu dolazi do izražaja čimbenik neugode. Treba odabrati identifikacijske tehnologije koje su jednostavne za korištenje, a s druge strane, nisu izvor frustracija i sl.
- **Nadogradivost** – potrebno je kod projektiranja ostaviti otvorenima mogućnosti nadogradnje u slučaju potrebe, dodatnih financijskih sredstava i dr.
- **Unazadna kompatibilnost** – potrebno je osigurati da novi sustav bude kompatibilan sa elementima prethodno ugrađenog sustava, jer se zadržavanjem određenih elemenata starog sustava mogu znatno smanjiti troškovi implementacije novog.

Slijedeća slika prikazuje ravnotežu koju je potrebno postući prilikom projektiranja sustava zaštite.



Slika 3. Čimbenici koji utječu na dizajn sustava fizičke zaštite

7. Zaključak

S razvojem poslovanja, podatkovni centri i centri za pružanje web usluga moraju, jednako kao mrežnu, osigurati i fizičku sigurnost. Uljezi koji krivotvore svoj identitet ili namjere, mogu uzrokovati katastrofalne štete – od fizičkog onesposobljavanja kritične opreme do izvođenja napada na programsku podršku. Čak i svakodnevne pogreške dobronamjernog osoblja mogu značajno ugroziti poslovanje. Svi spomenuti problemi rješavaju se smanjenjem i kontrolom pristupa kritičnim područjima i opremi.

Razvijaju se brojne tehnologije koje sve više i po sve manjoj cijeni implementiraju široki raspon rješenja temeljenih na tri osnovna identifikacijska principa – **Što imaš? Što znaš?** i **Tko si?** Kombiniranjem procjene rizika sa analizom potrebe pristupa i raspoloživim tehnologijama, može se izgraditi učinkovit sigurnosni sustav koji trošak uravnotežuje s razinom ostvarene zaštite.

8. Reference

[1] Fizička sigurnost, http://www.apcmedia.com/salestools/SADE-5TNRPL_R1_EN.pdf , rujan 2004.

[2] Integracija IT i fizičke sigurnosti, http://www.sans.org/reading_room/whitepapers/authentication/1308.php , lipanj 2004.

[3] Preporuke za ostvarenje fizičke sigurnosti, http://www.sans.org/reading_room/whitepapers/awareness/416.php , kolovoz 2001.