CARNet

HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Fizička zaštita informacijskih sustava

NCERT-PUBDOC-2010-06-304

Nacionalni CERT

u suradnji s

LSS

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

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

Nacionalni 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

Informacijski sustavi često su osnova poslovanja organizacije te sadrže vrlo važne informacije o proizvodima, zaposlenicima, kupcima ili partnerima. Narušavanje njihove sigurnosti može voditi do otkrivanja osjetljivih podataka te materijalnih gubitaka. Jedan od aspekata sigurnosti informacijskog sustava predstavlja i fizička sigurnost, tj. skup mjera koje sprječavaju nedozvoljen fizički pristup informacijama i resursima.

Prijetnje fizičkoj sigurnosti dolaze od prirodnih nepogoda poput poplava i potresa te ljudskih ranjivosti poput neposlušnosti, namjere za sabotažom ili krađom. Također, postoje neke prijetnje koje su rezultat nepredviđenih okolnosti kao što je požar uzrokovan ispuštanjem plina ili neke vrste kvarova na raznim sustavima. Kako bi se smanjila šteta nakon pojavljivanja neke od spomenutih prijetnji potrebno je uvesti adekvatne mjere zaštite. Pod tim se podrazumijeva osiguravanje okoline i prostorija objekata, kao i recepcije te provođenje kontrole pristupa. Također, potrebno je implementirati zaštitu opreme i uređaja putem dostupnih tehnologija. Razni sustavi razvijeni su za uspostavljanje i poboljšanje fizičke sigurnosti. Neki od njih su alarmni sustavi te sustavi za nadzor, kontrolu pristupa ili zaključavanje vrijednih uređaja.

Ovaj dokument daje uvod u načine uspostavljanja i važnost fizičke sigurnosti te opisuje glavne prijetnje koje ju mogu narušiti. Zatim je dan opis potrebnih mjera zaštite za svaki element sustava. Na kraju su predstavljeni uređaji kojima je osnovna namjena ostvarivanje fizičke sigurnosti informacijskih sustava.

2. Fizička sigurnost

Fizička sigurnost opisuje mjere koje sprječavaju neovlašten pristup resursima ili informacijama pohranjenim na fizičkim medijima. Radi se o skupu smjernica za dizajniranje strukture koja je otporna na razne zlonamjerne radnje, a može uključivati jednostavnu primjenu zaključavanja vrata ili zapošljavanje zaštitara.

Fizička sigurnost je najosnovniji aspekt zaštite, a obuhvaća kontrolu zaštite prostorija, postrojenja, zgrada i druge imovine. Primjena fizičke sigurnosti podrazumijeva proces uporabe mjera zaštite kako bi se spriječio neovlašten pristup, oštećenje ili uništenje dobara. U osnovi, fizička sigurnost odnosi se na sprječavanje oštećenja bilo kojeg dijela nekretnina, postrojenja, ureda, objekata ili zgrada.

Također, ona doprinosi zaštiti ljudi i informacija, iako se na te skupine primjenjuju i druge sofisticirane mjere zaštite. Prema tome, fizička sigurnost čini dio sveukupne sigurnosti informacijskog sustava kao osnova na kojoj su sve sigurnosne mjere utemeljene.

Mjere koje uključuje fizička sigurnost, a služe za zaštitu osoblja, opreme i imovine, mogu se podijeliti na:

1. *Pasivne mjere* – efektivna uporaba arhitekture, okoliša i osvjetljenja za postizanje bolje sigurnosti kroz olakšanu detekciju upada ili potencijalnih prijetnji.
2. *Aktivne mjere* – uključuju upotrebu poznatih sustava i tehnika dizajniranih za detekciju i reakciju na prijetnje.

2.1. Aspekti fizičke sigurnosti

Fizička sigurnost može se promatrati preko tri aspekta:

1. *Fizički aspekt* – mjere poduzete da bi se osigurala imovina (npr. zapošljavanje zaštitara).
2. *Tehnički aspekt* – mjere poduzete za osiguravanje usluga i elemenata koji služe kao podrška informacijskim tehnologijama (npr. sigurnost sobe s poslužiteljima).
3. *Operacijski apekt* – općenite sigurnosne mjere koje se provode prije izvođenja neke operacije (npr. analiziranje prijetnji ili aktivnosti).

Bez obzira na gledište, svi aspekti imaju zajedničke ciljeve:

- spriječiti bilo kakav neautorizirani pristup računalnom sustavu,
- spriječiti krađu podataka s računalnih sustava,
- zaštititi integritet podataka pohranjenih na računalu i
- spriječiti gubitak ili oštećenje podataka uslijed bilo kakvih nepogoda ili nesreća.

2.2. Uloga fizičke sigurnosti

Fizička zaštita se koristi kako bi se osiguralo da samo ovlaštene osobe imaju pristup nekretninama i informacijskom sustavu. Primijenjene mjere zaštite moraju biti prilagođene radnom okruženju, a ovise o sljedećim faktorima:

1. Koju imovinu treba zaštititi?
2. Gdje je smještena imovina koju treba zaštititi?
3. Koliku vrijednost ima imovina koju treba zaštititi?
4. Koje ranjivosti, prijetnje ili rizici prijete imovini?

Primjena odgovarajuće razine zaštite u svakom okruženju zahtjeva dizajniranje fizičke sigurnosti u procesu izgradnje i konstrukcije. Kako bi se postigla najbolja razina zaštite, arhitekti i sigurnosni stručnjaci trebali bi zajedno proučiti sve aspekte zaštite primjenjive na neku radnu okolinu. Ovakav oblik planiranja pomaže pri stvaranju optimalne sigurnosti uz najmanje troškove (jer se time zaobilaze brojni sigurnosni problemi).

Sigurnosni problemi koji se jave kao posljedica pogreške u fazi dizajniranja i konstrukcije obično zahtijevaju puno napora za otklanjanje te uzrokuju velike novčane izdatke. Jedno od rješenja u tom slučaju je primjena dodatnih mjera zaštite koje nisu prvotno planirane. Ukoliko se fizička sigurnost ne primjeni u početnoj fazi, potrebno je adresirati sigurnosne probleme prije puštanja postrojenja u rad.

Najbolja praksa primjene fizičke sigurnosti je u slojevitom pristupu, jer ne postoji niti jedna sigurnosna kontrola koja će u potpunosti zadovoljiti sve zahtjeve. Slojevitu primjenu kontrola potrebno je implementirati od unutarnjih do vanjskih granica informacijskog sustava kako je vidljivo na Slika 1.

Vanjski slojevi zaštite ovise o tipu nekretnine i lokaciji. Na primjer, objekt smješten u gradu može imati samo zid ili ogradu oko objekta, dok imovina smještena u industrijskom području može imati velika zelena područja, parkirališta i sl. u svojoj okolini. Kod drugog tipa objekta, okolina stvara dodatnu prepreku za fizički pristup.

Za razliku od vanjskih slojeva, unutarnji slojevi zaštite uključuju mjere primijenjene u uredima, na ulazu u objekt i sl. Usmjeravaju se na zaštitu svih unutarnjih dijelova objekata i imovine.

Slika 1. Slojevita fizička sigurnost

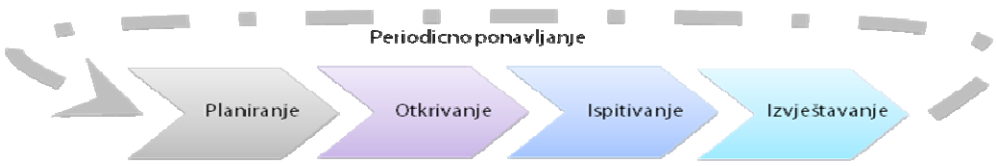
2.3. Procjena fizičke sigurnosti

Procjena fizičke sigurnosti vrlo je važna za svaku organizaciju i to u svakom trenutku. Ona ukazuje na stupanj pripremljenosti na prijetnje fizičkoj sigurnosti te pokazuje kolike bi gubitke mogla pojedina prijetnja uzrokovati.

U procjenu fizičke sigurnosti uključeno je:

- ocjenjivanje stupnja sigurnosti lokacije,
- ispitivanje procedura za zaposlenike i njihove svijesti o problemima,
- procjena sigurnosti sve imovine te
- ocjena sigurnosti zaposlenika.

Postupak procjene fizičke sigurnosti sastoji se od četiri faze prikazane na Slika 2. Prva faza podrazumijeva planiranje i tu se definira raspon procjene, uloge te cilj. Nakon planiranja slijedi faza otkrivanja u kojoj se prikuplja što je više moguće informacija. Treća faza je testiranje, a uključuje provođenje „penetracijskih ispitivanja" izvođenjem neke vrsta napada socijalnim inženjeringom. Nakon provođenja ovih faza slijedi posljednja faza u kojoj se stvaraju izvještaji o razini fizičke sigurnosti. Opisane faze slikovito su prikazane na Slika 2. Postupak procjene fizičke sigurnosti treba obavljati periodično jer se rizici i prijetnje mogu mijenjati tokom vremena. Prema tome, ovaj je postupak vrlo važan jer može pomoći pri otkrivanju novih prijetnji i ranjivosti.



Slika 2. Koraci procjene fizičke sigurnosti

3. Prijetnje fizičkoj sigurnosti

3.1. Prirodne nepogode

Prirodne prijetnje jedne su od najprisutnijih opasnosti za fizičku sigurnost na koje čovjek ne može utjecati. Ipak, postoje određene mjere kojima je moguće smanjiti njihov štetan učinak na sigurnost informacijskog sustava.

U skupinu prirodnih prijetnji spadaju:

- **meteorološke nepogode** – uključuju sve atmosferske nepogode poput raznih padalina (kiša, snijeg), vjetra, oluje, jako visokih i niskih temperatura i sl. Neke od posljedica ovih nepogoda na informacijski sustav su gubitak ili degradacija komunikacija te uništenje uređaja (a samim time i informacija).
- **geofizičke nepogode** – podrazumijevaju potrese i vulkanske aktivnosti, a mogu izazvati niz drugih nepogoda poput požara, poplava, ispuštanja plina ili otrovnih kemikalija, prekida napajanja i sl. Kao osnovni učinci ovih prijetnji javljaju se mogućnosti uništenja ili oštećenja uređaja što može rezultirati gubitkom podataka, prekidom rada sustava i velikim materijalnim gubicima.
- **sezonski fenomeni** – uključuju nepogode vezane uz neko razdoblje poput vremenskih ekstrema, šumskih požara ili uragana, a mogu dovesti do gubitka ili degradacije mrežnih komunikacija te uništenja uređaja.
- **astrofizički fenomeni** – podrazumijevaju sunčane fenomene i meteore koji mogu uzrokovati gubitak ili degradaciju satelitskih veza.
- **biološke prijetnje** – razne bolesti koje mogu uzrokovati smanjenje broja sposobne radne snage.

Prirodne prijetnje mogu dovesti do ogromnih materijalnih gubitaka i prouzročiti veliku štetu kako je vidljivo i na Slika 3. Ne postoje nikakve metode zaštite koje bi spriječile pojavu prirodnih nepogoda. Ipak, moguće je poduzeti mjere koje će omogućiti nastavak neprekidnog rada informacijskog sustava i spriječiti gubitak informacija potrebnih za poslovanje. Takvi postupci umanjuju nepovoljne posljedice koje donose neke od opisanih prirodnih nepogoda.

Slika 3. Prirodne prijetnje

3.2. Ljudske prijetnje

Zaposlenici su jedan od osnovnih rizika svake organizacije jer unose veliki raspon prijetnji sigurnosti informacijskog sustava. Neke od prijetnji, prikazane na Slika 4, koje uzrokuju zaposlenici su:

- **Neposlušnost** – jedna od prijetnji ove skupine javlja se uslijed neposlušnosti zaposlenika što može dovesti do prosvjeda ili štrajka. Posljedice takve situacije mogu biti oštećenje imovine ili uređaja te ozljeđivanje samih zaposlenika.
- **Otkrivanje osjetljivih podataka** – zaposlenici također mogu nanijeti druge oblike šteta poput otkrivanja osjetljivih podataka zbog nepravilnog rukovanja ili nerazumijevanja/nepostojanja sigurnosne politike.
- **Sabotaža** – svaka organizacija trebala bi uvesti i zaštitu od sabotaže ili namjernog narušavanja rada sustava i ispravnosti uređaja.
- **Nenamjerno oštećenje imovine** – nepravilno rukovanje može dovesti do oštećenja uređaja ili drugih dijelova imovine. Kako bi se to spriječilo, zaposlenike treba pravilno educirati i upozoriti na posljedice nepravilnog korištenja.
- **Zlouporaba ovlasti** – zaposlenicima treba jasno definirati uloge te objasniti prava i posljedice njihovog nepridržavanja. Zlouporaba ovlasti može se odraziti u obliku prekomjernog korištenja imovine organizacije ili njenog iznošenja izvan prostora za koji je namijenjena.
- **Neovlašten pristup podacima ili imovini** – zaposlenicima treba pravilno definirati prava pristupa kako ne bi došli do povjerljivih podataka. Ukoliko zaposlenici rade s nekim povjerljivim podacima ili dijelovima sustava potrebno je napraviti ugovore o povjerenju.
- **Krađa** – zaposlenici koji imaju pristup imovini organizacije mogu prisvojiti neke dijelove ili uređaje.

Slika 4. Ljudske prijetnje

Dosta opisanih prijetnji dolazi ne samo od zaposlenika, već od korisnika, klijenata, poslovnih partnera, dostavljača te ostalih osoba koje imaju doticaja s imovinom i podacima organizacije. Svaka osoba koja na neki način dolazi u kontakt s poslovanjem ili imovinom organizacije može uzrokovati nenamjerno oštećenje imovine. Ipak, organizacije često ulažu velike napore i resurse u zaštitu od namjernog uništavanja, krađe dobara i podataka, sabotaže, terorizma, špijunaže i sl. Ljudski faktor čini ključnu ulogu

u postizanju sigurnosti, a kako bi se ostvarila zaštita od navedenih prijetnji potrebno je brojne mjere implementirati i na samoj fizičkoj razini.

3.2.1. Socijalni inženjering

Postoji cijela skupina napada usmjerena na dobivanje pristupa računalnom sustavu iskorištavanjem ljudskih ranjivosti poput nemarnosti ili lakog povjerenja. Cilj tih napada je pridobiti povjerenje žrtve kako bi se ostvarila krađa identiteta ili podataka te izveo upad u mrežu/sustav. Socijalni inženjer može biti bilo tko, od hakera, špijuna, nezadovoljnih zaposlenika do prodavača i vladinih službenika.

Napadi temeljeni na socijalnom inženjeringu, prikazani na Slika 5, mogu se izvesti:

- oponašanjem dostavljača ili nekih službenih osoba kako bi se ostvario pristup sustavu,
- lažnim predstavljanjem u komunikaciji preko telefona (npr. kao osoba zaposlena u tehničkoj podršci),
- uvjeravanjem osoba da će dobiti nagradu ukoliko obave neki zadatak,
- prikupljanjem informacija o navikama zaposlenika kako bi se iste mogle iskoristiti kao njihove slabosti te
- „izvlačenjem“ informacija od zaposlenika (npr. podataka za pristup).

Slika 5. Napadi socijalnog inženjeringa

Općenito, napadi su uspješniji ako ne postoji definirana sigurnosna politika te nije provedena edukacija zaposlenika o opisanim opasnostima. Ukoliko su uspješno izvedeni, mogu uzrokovati velike gubitke za neku organizaciju poput otkrivanja osjetljivih podataka o zaposlenicima, partnerima i kupcima, zatim gubitka nacrta i planova za nova poslovanja i proizvode i sl. Više informacija o metodama i posljedicama socijalnog inženjeringa moguće je pronaći u CERT-ovom dokumentu „Napredne tehnike socijalnog inženjeringa“:

http://www.cert.hr/documents.php?id=408

Napadi socijalnog inženjeringa predstavljaju veliku prijetnju fizičkoj sigurnosti, ali njihov utjecaj može biti smanjen odgovarajućim mjerama.

3.2.2. Definiranje sigurnosnih politika

Temelj sigurnosti svake organizacije je dobro definirana sigurnosna politika koja treba jasno opisati opseg i sadržaj svakog područja na koje se odnosi. Kako bi bila potpuna, sigurnosna politika mora uključivati i područja fizičke sigurnosti. Treba pravilno odrediti svaki aspekt zaštite i sve mjere koje se provode radi postizanja fizičke sigurnosti.

Ukoliko je sigurnosna politika loše definirana ili nepotpuna, ona može stvarati nedoumice kod zaposlenika. Nejasne odredbe teško je primijeniti pa i sami zaposlenici imaju poteškoća s njihovim primjenama. U takvim situacijama veća ja mogućnost narušavanja fizičke sigurnosti. Prijetnju predstavljaju zaposlenici kojima nije adekvatno definirano kako se ponašati u određenim situacijama, ali i korisnici, kupci te partneri prema kojima ne postoji pravilan način ophođenja.

3.3. Odgovornost za fizičku sigurnost

U većini organizacija ne postoji osoba izravno zadužena za fizičku sigurnost, tj. za održavanje i implementaciju svih mjera potrebnih za postizanje odgovarajuće razine sigurnosti. U takvim okolnostima organizacija je više izložena svim prijetnjama jer ne postoji adekvatna briga o uspostavljanju mjera zaštite.

Iako velik broj organizacija zapošljava sigurnosne zaštitare, najčešće nije dovoljno njima prepustiti fizičku zaštitu. Razlog tome je što postoje brojne mogućnosti za narušavanje sigurnosti te je potrebno provoditi stalni nadzor nad brojnim područjima. Sigurnosni zaštitari se obično usmjeravaju na praćenje osoba tj. na osiguravanje kontrole pristupa i sprječavanje krađe.

Još jedna od osoba koja ima određeni dio odgovornosti za fizičku sigurnost je analitičar informacijske sigurnosti. Njegov je zadatak provesti potrebne analize i ispitivanja sigurnosti kako bi se utvrdile moguće kritične točke.

U provođenje fizičke sigurnosti uključen je i voditelj informacijskog sustava, koji ima zadatak nadzirati implementirane mjere te predlagati izmjene koje bi mogle rezultirati poboljšanjem sigurnosti.

Takvo dijeljenje odgovornosti ne pogoduje sustavnom praćenju sigurnosti zbog mogućnosti lošeg razumijevanja uloga i izbjegavanja izvršavanja zadataka koje uloge donose.

3.4. Ostale prijetnje

Postoje i brojne prijetnje koje mogu uzrokovati prekid rada sustava, a nisu uzrokovane prirodnim nepogodama ili ljudskim aspektima. Te prijetnje nisu uzrokovane djelovanjem čovjeka ili prirode, nego su rezultat nekih nesreća:

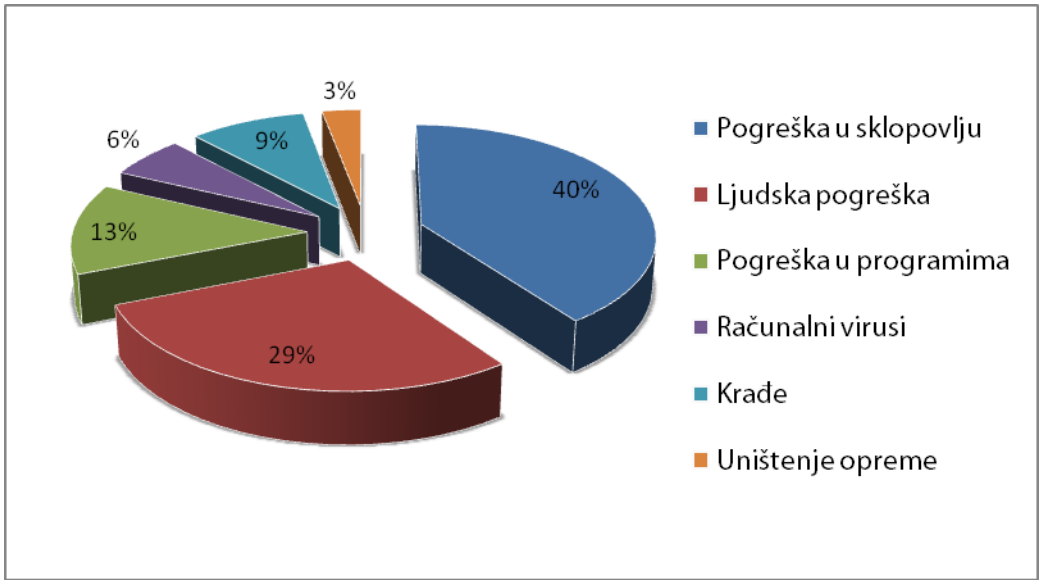
- **Eksplozija** – uzroci eksplozija mogu biti razni, od kvara na uređajima do zapaljenja plina u uređajima za zagrijavanje. Ovaj oblik prijetnji nosi vrlo opasne posljedice za sigurnost sustava i zaposlenika.
- **Prašina** – neodržavanje čistoće poslužitelja ili nekih drugih dijelova sustava može dovesti do kvarova na njima. Posljedice takvih kvarova su mogućnosti gubitka podataka, prekida rada sustava, uzrokovanje dodatnih kvarova i sl.
- **Poplava** – osim poplava uzrokovanih prirodnim nepogodama, velike štete mogu nanijeti i poplave uzrokovane slučajnim kvarovima ili puknućem cijevi. Ukoliko dođe do takvih situacija, može doći do kvarova na svim poslužiteljima ili drugim elektroničkim komponentama sustava.
- **Gubitak električnog napajanja** – gubitak električnog napajanja može biti uzrokovan kvarovima na električnoj infrastrukturi, prekidom rada nekog dijela sustava i sl. Često može imati za posljedicu prekid kontinuiranog poslovanja ukoliko ne postoji adekvatna zaštita (npr. alternativni izvori energije ili napajanja).
- **Elektromagnetska radijacija** – uređaji koji ispuštaju elektromagnetske valove mogu u određenim situacijama i uzrokovati kvarove na drugim uređajima.

Svaka od prijetnji, ukoliko se zanemari njen utjecaj, može prouzročiti velike gubitke. Oni mogu biti u materijalnom obliku zbog fizičkog uništenja opreme ili uzrokovanja kvara, ali mogu se odraziti i u obliku

gubitka informacija potrebnih za poslovanje. Također, neke od prijetnji mogu nanijeti ozbiljne posljedice na zdravlje zaposlenika.

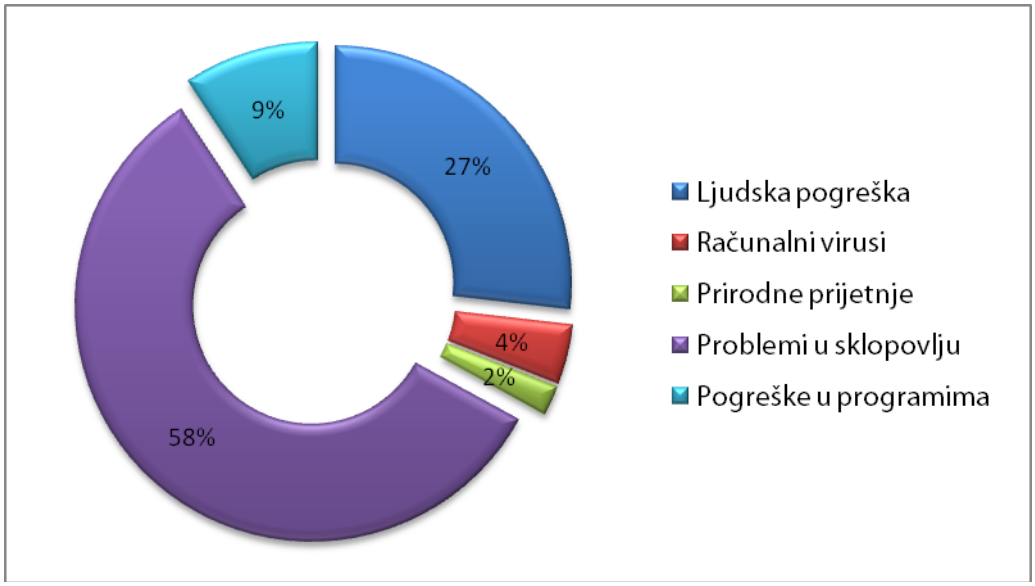
3.5. Učestalost prijetnji fizičkoj sigurnosti

Statistički podaci o uzrocima gubitka podataka organizacije Graziadio Business Report vidljivi su na Slika 6. Može se primijetiti kako se neke od prijetnji fizičkoj sigurnosti nalaze među najčešćim uzrocima gubitka podataka. Ljudske pogreške čine čak 29% uzroka za gubitke podataka. Također, krađa (9%) i uništenje opreme (3%) nalaze se u najčešćim uzrocima gubitaka podataka.



Slika 6. Uzroci gubitaka podataka
Izvor: Graziadio Business Report

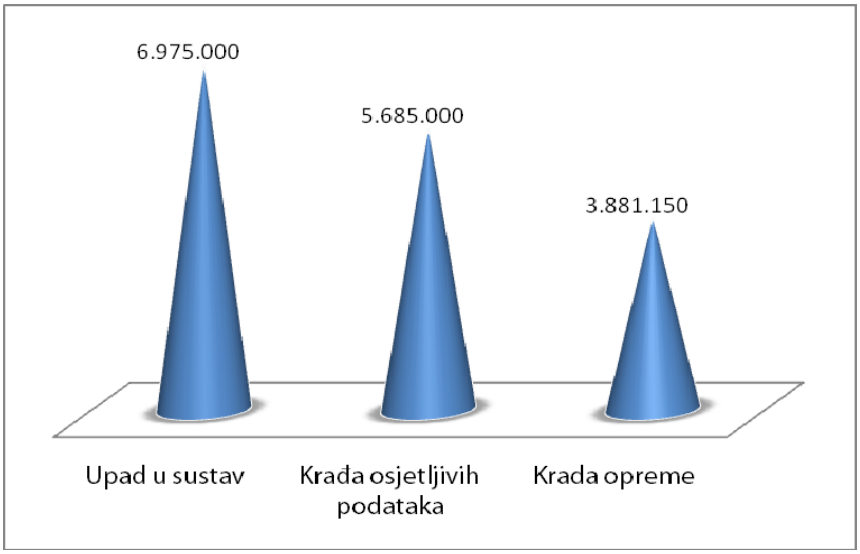
Izvješće organizacije Ontrack, izrađeno prema iskustvu s korisnicima, navodi i prirodne prijetnje kao jedne od čestih uzročnika gubitka podataka. Prema njihovim statističkim podacima (prikazanim na Slika 7), prirodne prijetnje uzrokuju gubitke podataka u čak 2% slučajeva. Veliki postotak, čak 27%, gubitaka podataka rezultat je ljudskih pogrešaka.



Slika 7. Razlozi gubitaka podataka
Izvor: Ontrack

Prikazani podaci ukazuju kako su prijetnje fizičkoj sigurnosti među važnijim razlozima gubitka podataka. Obično ljudske pogreške predstavljaju veću razinu prijetnji jer su dosta češće nego prirodne prijetnje. Iako su gubici uzrokovani prirodnim prijetnjama puno manji nego oni koji su rezultat ljudskih pogrešaka, ne smiju se zanemariti.

Materijalni gubici koje uzrokuje ugrožavanje fizičke sigurnosti vrlo su veliki, kako pokazuju statistike s portala „noticebored" prikazane na Slika 8. Iznos gubitaka koji su rezultat krađe prijenosnih računala ili drugih uređaja iznosili su 2007. godine oko 4 milijuna dolara. Oko 64% organizacija pretrpilo je krađu opreme nekog oblika, a 88% njih izjavljuje kako izgubljenu opremu nisu uspjeli vratiti. Krađa povjerljivih podataka uzrokovala je gubitke od skoro 6 milijuna dolara. Raznim metodama upada u sustav ostvareni su gubici od oko 7 milijuna dolara.



Slika 8. Novčani gubici uzrokovani narušavanjem fizičke sigurnosti
Izvor: Noticebored

3.6. Primjeri narušavanja fizičke sigurnosti

U svibnju 2006. godine ukradeno je računalo vladinog službenika u SAD-u koje je sadržavalo podatke o 26.5 milijuna veterana. Podaci su uključivali identifikacijske brojeve, datume rođenja te još neke osjetljive podatke.

Također, u svibnju 2008. godine ukradena su četiri računala službenika banke *Bank of Ireland* koja su sadržavala osobne podatke o 10.000 korisnika. Osobna računala ukradena su iz prostorija banke, a koristili su ih zaposlenici koji su radi na policama osiguranja. Podaci na računalima uključivali su detalje o osiguranju i korisničkim računima, podatke o mjestu stanovanja te povijest bolesti korisnika.

Jedan od primjera gubitka podataka uslijed sabotaže dogodio se početkom svibnja 2009. godine. Radi se o sabotaži koju je izveo jedan od zaposlenika organizacije koja održava web stranicu JournalSpace.com. Oporavak podataka nije bio moguć jer su, uz uništenje originalnih podataka, uništeni i podaci koji su predstavljali sigurnosne kopije.

Veliki požar zahvatio je vladine urede u Indiji, u svibnju 2009. godine. U požaru su izgubljeni važni dokumenti i oštećena računala, iako je vatra ugašena za samo 30 minuta.

U lipnju 2010. godine IT sustavi u državi Dallas nisu radili tri dana nakon poplave u objektu Dallas County Records Building. Poplava je uzrokovala kvar na sustavima i drugoj elektroničkoj opremi koji služe kao podrška podatkovnim centrima. Najveći problem predstavljala je činjenica kako nisu postojale sigurnosne kopije podataka iz podatkovnih centara.

4. Fizička zaštita informacijskog sustava

4.1. Zaštita okoline

Okolina objekta je prvi element nad kojim treba provesti postupke fizičke zaštite. Pravilna arhitektura može pomoći pri zaštiti objekta od špijunaže i izvođenja nekih drugih oblika napada socijalnog inženjeringa. Ukoliko je područje oko objekta adekvatno uređeno te postoji stalni nadzor, moguće je izbjeći razne prijetnje koje donose sami ljudi.

Jedan od osnovnih načina zaštite objekta je postavljanje ograda oko područja koje je u vlasništvu organizacije. Time se izravno sprječava prilazak osoba do objekta te zahtjeva najava prije ulaska u prostore organizacije. Ponekad se, umjesto postavljanja ograda, organizacije odlučuju za izgradnju zidova oko svog posjeda. Na taj način smanjena je vidljivost u unutrašnjoj organizacije te je time otežano izvođenje napada. Također, ograde mogu štititi i od nekih prirodnih prijetnji poput poplava i sl. Neki od načina zaštite okoline prikazani su na Slika 9.

Ulazi i izlazi su sljedeći element okoline koji se mora osigurati na adekvatan način, a to može uključivati:

- postavljanje lokota kako bi se onemogućio ulazak osobama koje ne posjeduju ključ,
- postavljanje zaštitara kako bi se provodila identifikacija osoba na ulazu te poboljšao nadzor okoline,
- postavljanje nadzornih kamera koje mogu služiti i za identifikaciju osoba,
- postavljenje alarmnih sustava koji bi se oglašavali u slučaju provale, ili nekih drugih prijetnji (npr. požar).

Slika 9. Zaštita okoline

Postizanje adekvatne zaštite okoline definirano je kroz CPTED (eng. *Crime prevention through environmental design*) dizajn. Temelji se na sposobnosti da se utječe na odluke koje prethode počinjenju kaznenih djela. Definira načine prirodnog nadzora i kontrole pristupa koje ograničavaju priliku za kriminal te teritorijalno pojačavanje koje promiče socijalne kontrole kroz razne mjere.

Mjere prirodnog nadzora povećavaju vizualnu percepciju i strah da bi napadač mogao lako biti uočen. Provodei se dizajniranjem prostornih obilježja i aktivnosti na način da se poveća vidljivost i potiču pozitivne društvene interakcije. Na taj način potencijalni prijestupnici imaju osjećaj povećane kontrole i ograničenja na mogućnost bijega.

Mjere prirodnog pristupa kontroliraju granice kako bi se jasno razlikovao prostor javnog i privatnog vlasništva. Selektivnim postavljenjem ulaza i izlaza, ograda, rasvjete i krajobraza ograničava se pristup i pregled područja.

Teritorijalno pojačavanje promiče društveni nadzor kroz definiranje vlasničke zbrinutosti. Stvaranjem razdvojenosti javnog i privatnog prostora, postiže se osjećaj vlasništva nad privatnim. Vlasnici imaju interes zaštititi svoju imovinu, a uljeze je lakše identificirati.

4.2. Zaštita recepcije

U većini organizacija se, odmah nakon ulaska u objekt, dolazi do prostora za informiranje i obavljanje nekih administrativnih poslova - recepcije. Obično je recepcija jedno od „najprometnijih" mjesta kroz koje prolaze brojne osobe. Zbog toga je vrlo važno održavati urednost te paziti na pohranu važnih dokumenata (koji se ne smiju ostavljati na vidljivim i dostupnim mjestima). Ista pravila odnose se na prijenosne uređaje za pohranu podataka.

Većem stupnju zaštite pridonosi i dizajniranje prostora na način da neautorizirane osobe nemaju pristup dijelu za zaposlenike. Postavljanje računala ne smije omogućiti posjetiteljima pregled sadržaja na njima, niti njihovo korištenje.

U područje recepcije moguće je također postaviti alarme, gumbe za slučaj opasnosti i kamere za nadzor. Ipak, svi navedeni postupci mogu biti nedovoljni ukoliko nisu definirana pravila ponašanja osoba zaposlenih na recepciji. Ta pravila uključuju praksu ispravnog ophođenja s posjetiteljima kako ne bi došlo do otkrivanja podataka o organizaciji i zaposlenicima. Osim toga, definira se ophođenje prema računalu kojeg nikad ne treba ostaviti dostupnim i spremnim za uporabu ukoliko se napušta radno mjesto. Nakon radnog vremena, računalo je potrebno ugasiti te pohraniti sve povjerljive dokumente i vrijedne uređaje na sigurno mjesto.

4.3. Zaštita prostorija

U unutrašnjosti objekta nalaze se razne prostorije koje treba zaštititi u skladu s njihovom namjenom. Kod prostorija koje sadrže važne poslužitelje ili skupocjene uređaje potrebno je primijeniti veći stupanj zaštite te uvesti veće mjere sigurnosti.

Neki od načina zaštite unutrašnjih prostorija objekta, dani na Slika 10, su:

- uporaba kamera s nadzornim ekranima kako bi se mogli pratiti postupci zaposlenika i posjetitelja (obično se postavljaju samo na ključna mjesta),
- pohrana snimljenih video zapisa potrebna je radi mogućnosti kasnije kontrole u slučaju nekog nepredviđenog događaja,
- postavljanje gumba za slučaj opasnosti koji mogu aktivirati zaposlenici u slučaju provale, požara ili neke druge opasnosti,
- instalacija protuprovalnog alarma koji bi osiguravao prostorije koje su stalno zaključane te ostale prostorije izvan radnog vremena,
- postavljanje zaštite od požara u obliku alarma za pravodobno obavještavanje osoblja i vatrogasaca te
- implementacija sustava protiv upada kako bi se spriječio neželjeni pristup osjetljivim dijelovima, a može uključivati postavljanje prepreka na prozore i vrata, ugradnju lokota i sl.

Slika 10. Zaštita prostorija

4.4. Zaštita opreme

Najvažniji aspekt kod fizičke zaštite informacijskog sustava predstavlja pravilna zaštita opreme i uređaja. Svakom uređaju treba definirati posebne mjere zaštite s obzirom na njegovu namjenu i vrijednost. Takve mjere trebaju spriječiti sve prijetnje, uključujući prijetnje od prirodnih nepogoda ili ljudske prijetnje.

Većina organizacija provodi samo osnovne mjere zaštite opreme koje često nisu dovoljne, a odnose se na zaštitu poslužitelja i osobnih računala. Razlog tome je što navedeni elementi sadrže najviše osjetljivih podataka pa njihovo oštećenje može dovesti do ozbiljnih posljedica.

Ipak, potrebno je provesti dodatne sigurnosne mjere pri rukovanju s opremom, kao što su:

- zaključavanje uređaja nakon uporabe (npr. fax uređaja),
- smještaj uređaja na osigurana mjesta,
- pohrana prijenosnih medija na sigurna mjesta te
- adekvatno uništavanje starih prijenosnih medija.

4.4.1. Zaštita poslužitelja

Poslužitelji predstavljaju vrlo važan aspekt za poslovanje svake organizacije jer mogu sadržavati vrlo važne informacije , a zaposlenici ih svakodnevno koriste. Zbog takvih namjena, najbolja praksa je razdvajanje svakodnevnih funkcija od poslužitelja. To znači da se jedan poslužitelj ne bi trebao koristiti za obavljanje svakodnevnih zadataka.

Još jedan od važnih elemenata zaštite predstavlja pravilan smještaj poslužitelja. Najbolje bi bilo poslužitelje izdvojiti u posebnu prostoriju koju je moguće dobro nadzirati. Također, smještaj treba implementirati tako da se spriječi pomicanje i premještanje poslužitelja. Time se sprječava oštećenje i uzrokovanje kvarova, ali se može postići i bolja zaštita od nekih prirodnih prijetnji (npr. potres).

Administrator sustava također treba biti uključen u održavanje fizičke sigurnosti poslužitelja. To može učiniti, primjerice, onemogućavanjem pokretanja CD (eng. *Compact Disc*) medija kako bi se spriječilo namjerno oštećenje sustava ili pokretanje nekih napada.

Slika 11 prikazuje neke od načina zaštite poslužitelja od pomicanja te pristupa neovlaštenih osoba.

Slika 11. Zaštita poslužitelja

4.4.2. Zaštita osobnih računala

Najosnovniji način zaštite osobnih računala uključuje dobru edukaciju zaposlenika. Ukoliko su zaposlenici upoznati s pravilnim načinom rukovanja s računalom, rizik od raznih prijetnji znatno je umanjen. Zaposlenicima je potrebno jasno definirati pravila u obliku sigurnosnih politika te ih predstaviti na jednostavan način. U sklopu sigurnosne politike treba navesti pravilno ophođenje prema računalima u slučaju nekog kvara ili prirodne nepogode. Također, treba definirati zaštitu od krađe, špijunaže i drugih prijetnji koje donose ljudi, a odnose se na fizičku sigurnost.

Uporaba nadzora u obliku postavljanja kamera i osiguranja može spriječiti zaposlenike pri pokušaju oštećivanja ili krađe računala. Nadzorne kamere potrebno je postaviti na ključna mjesta, koja su u blizini vrijednih uređaja ili računala.

Kako bi se onemogućilo zlonamjerno rukovanje računalom nekog zaposlenika potrebno je isto zaključati ukoliko nije u upotrebi. Računalo koje ostaje upaljeno posjetitelji mogu zlouporabiti za otkrivanje osjetljivih podataka ili nanošenje druge štete.

Smještaj računala zaposlenika također predstavlja važan aspekt zaštite. Računala je potrebno rasporediti na način da niti jedan zaposlenik nema pristup podacima drugog zaposlenika. Kako bi se dodatno spriječilo otkrivanje osjetljivih podataka treba izbjegavati da svi korisnici upotrebljavaju isti prijenosni uređaj za pohranu podataka.

Sprječavanje krađe može se postići i nekim sofisticiranim uređajima. Neki od njih su lokoti za zaključavanje kabela te sustavi za praćenje i otkrivanje lokacije ukradenih ili izgubljenih stvari. Također, postoje posebni držači za prijenosna računala koji imaju mogućnost zaključavanja. Ukoliko takvi uređaji nisu dostupni, moguće je ugraditi ormariće s lokotima za sigurnu pohranu prijenosnih računala. Prikaz nekoliko načina zaštite osobnih računala nalazi se na Slika 12.

Sigurnost informacijskog sustava dodatno se može povećati implementacijom zaključavanja USB priključaka kako bi se spriječilo preuzimanje podataka ili onemogućilo umetanje zlonamjernih programa.

Slika 12. Zaštita osobnih računala

4.5. Implementacija kontrole pristupa

Kontrola pristupa osigurava mogućnost ograničavanja pristupa određenim područjima i resursima u fizičkom objektu ili računalnom informacijskom sustavu. U području fizičke sigurnosti, obično se predstavlja kao drugi sloj u sigurnosti fizičke infrastrukture koji služi za ograničavanje pristupa imovini, zgradi, prostoriji i sl.

Adekvatna kontrola pristupa jedan je od ključnih faktora koji su uključeni u fizičku zaštitu informacijskog sustava. Treba ju provoditi na ulazu u objekt te u prostorije koje sadrže važne uređaje, poslužitelje ili podatke.

Fizička kontrola pristupa može se postići pomoću drugih osoba (stražara, zaštitara ili recepcionara), putem mehaničkih sredstava (kao što su brave i ključevi) ili kroz tehnološka sredstva.

Kontrolu pristupa potrebno je posebno definirati za korisnike, a posebno za zaposlenike. Korisnici ili posjetitelji moraju se identificirati na ulazu u objekt putem identifikacijskih oznaka (Slika 13). Dodatno, potrebno je zatražiti nošenje posebnih oznaka ili kartica koje označavaju da je neka osoba posjetitelj. Takve identifikacijske oznake za posjetitelje mogu umanjiti mogućnost zlouporabe pristupa unutrašnjosti objekta ili određenim dijelovima informacijskog sustava.

Slika 13. Nošenje identifikacijskih oznaka
Izvor: FPM

Zaposlenicima je moguće definirati sigurnosne mjere nošenja posebnih kartica kojima bi se prijavljivali pri ulazu u objekt te pri napuštanju istog. Takav postupak je vrlo jednostavan i široko raširen upravo zbog lakoće korištenja pametnih kartica. Osim karticama, identifikacija zaposlenika može se provoditi nekim sofisticiranijim načinima, kao što je biometrička kontrola pristupa. Tu spadaju metode skeniranja otiska prsta, prepoznavanja lica, šarenice oka ili glasa te skeniranje rasporeda vena na ruci.

4.6. EPS sigurnost

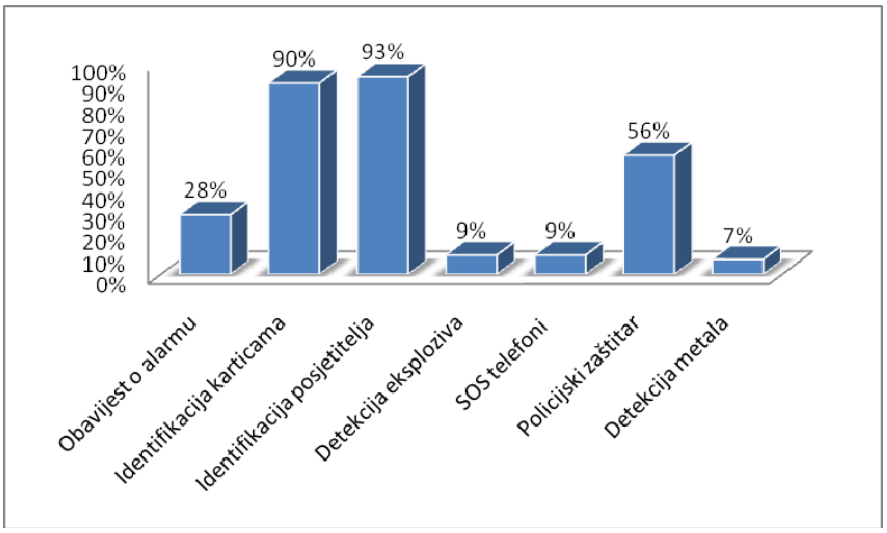
Integrirana primjena brojnih elektroničkih sustava za sigurnost naziva se EPS (eng. *electronic physical security*), te uključuje:

- sustave za detekciju požara,
- automatske sustave za suzbijanje plinova,
- sustave za nadzor (npr. kamere),
- sustave za kontrolu pristupa (pametne kartice, biometrička kontrola i sl.),
- sustave za detekciju upada,
- adekvatnu opremu za zaštitare i
- sustave za opremanje okoline i prostorija (ograde, skenere i sl.).

4.7. Zastupljenost fizičke zaštite

Statistički podaci objavljeni na web stranici organizacije AGA (eng. *American Gas Association*) pokazuju kako je mali broj organizacija primijenio potrebne sigurnosne mjere za zaštitu od fizičkih prijetnji. Spomenute statistike nalaze se na Slika 14.

Oko 28% organizacija prima obavijest ukoliko se aktivira alarmni uređaj, a samo 9% ih ima ugrađene uređaje za detekciju eksploziva. Još manji postotak, oko 7% organizacija, koristi uređaje za detekciju metala kod osoba pri ulasku u objekte organizacije. Nešto više od polovice organizacija (56 %) zapošljava policijskog službenika za održavanje sigurnosti. Ipak, neki aspekti zaštite zastupljeni su vrlo dobro pa tako 93% organizacija provodi identifikaciju posjetitelja putem osobnih isprava.



Slika 14. Implementacija zaštite od prijetnji fizičkoj sigurnosti

5. Elementi za postizanje fizičke sigurnosti

5.1. Alarmni sustavi

Alarmni sustavi služe za davanje zvučnog ili vizualnog upozorenja o problemu ili stanju sustava, a uključuju:

1. alarme protiv provale – dizajnirani za upozoravanje u slučaju provale, često se koriste u obliku tihih alarma za obavještavanje policije bez uzbunjivanja provalnika,
2. vremenske alarme – pokreću aktiviranje alarma u trenutku koji je definirao korisnik, zaposlenik, vlasnik i dr.,
3. DCS (eng. *distributed control manufacturing system*) sustave koji obavještavaju osoblje o važnim događajima, a obično se koriste u kemijskim i nuklearnim laboratorijima.
4. alarme u O&M (eng. *operation and maintenance*) sustavima koji služe za slanje obavijesti o lošem radnom stanju sustava koji se nadzire,
5. alarme za sigurnost - uključuju alarme za dojavu prirodnih nepogoda (tornada, požara, plinova i sl.) te nekih izvanrednih situacija (poput pojave radijacije).

Iako služe u dobre svrhe, alarmi imaju mogućnost uzrokovanja panike kod ljudi. Također, svaka vrsta alarma može proizvesti lažnu dojavu problema, tj. oglasiti se kada problem zapravo ne postoji ili zatajiti pri stvarnom problemu tj. ne oglasiti uzbunu u slučaju problema.

Alarmi protiv provala su posebno važni za fizičku zaštitu informacijskog sustava, a mogu se koristiti na svim ulazima u objekt. Obično funkcioniraju tako da detektiraju otvaranje vrata ili prozora putem PIR (eng. *passive infrared*) zraka. Signali sa senzora prenose se žično ili bežično do jedne ili više kontrolnih jedinca. Razlikuju se po namjeni (kućni, industrijski i sl.) te po mjestu postavljanja (unutrašnjost objekta ili izvan objekta). Primjeri nekih alarma protiv provala prikazani su na Slika 15. Pravovremeno otkrivanje pokušaja provale može onemogućiti krađu uređaja ili podataka.

Alarmni sustavi protiv požara dizajnirani su za detekciju prisutnosti vatre nadzorom promjena u okolini. Mogu biti automatski pa se samostalno pokreću nakon detekcije požara ili ručni pa zahtijevaju djelovanje ljudi za aktivaciju. Koriste se za pokretanje evakuacije, pozivanje pomoći te pripremanje sustava na kontrolu širenja požara. Kao jedan indikator požara često se koriste detektori dima koji generiraju signal za aktivaciju alarma ukoliko detektiraju prisutnost dima. Postavljanje uređaja za detekciju požara vrlo je važno za svaki informacijski sustav jer u slučaju širenja požara može doći do uništenja sve imovine, opreme, poslužitelja, računala i sl. Takvi slučajevi mogu rezultirati gubitkom svih podatka i imovine neke organizacije.

Slika 15. Alarmi protiv provale
Izvor: IST

5.2. Rasvjeta

U području fizičke sigurnosti, rasvjeta se obično koristi kao preventivna mjera protiv upada ili drugih kriminalnih aktivnosti na imovini. Može se koristiti kao dodatak nadzoru kako bi se olakšala detekcija uljeza, ali i za podizanje osjećaja sigurnosti.

Postoji više tipova rasvjete, a odabir odgovarajućeg ovisi o namjeni. Jedan od tipova je rasvjeta koja se aktivira i deaktivira u određeno, prethodno definirano vrijeme. U tom slučaju objekt je stalno osvijetljen pa je moguće provoditi nadzor kamerama. Drugi tip predstavlja rasvjeta koja se aktivira u slučaju detekcije pokreta putem senzora. Prednost ovakve implementacije je u štednji energije.

Ipak, rasvjeta može imati i negativne utjecaje. Jedan od njih je smanjenje vidljivosti u područjima koja ostaju u sjeni. Također, ispitivanja pokazuju kako se uz rasvjetu osobe osjećaju zaštićenijima, uključujući i same kradljivce. Na Slika 16 dan je primjer korištenja rasvjete u svrhu podizanja fizičke sigurnosti.

Slika 16. Primjer rasvjete
Izvor: Mr. Electric

5.3. Zaštitari

Zaštitari su obično zaposlenici čija je dužnost štititi vlasništvo, dobra i osoblje neke organizacije. Često su obučeni u posebne uniforme te nastoje spriječiti ilegalne i nedozvoljene radnje promatrajući okolinu i tražeći znakove kriminala, požara ili neposlušnosti. Ponekad se u funkciji zaštitara mogu naći i policijski službenici.

Uobičajena metodologija koju slijede zaštitari je „otkriti, umanjiti, promatrati i izvijestiti“, a cilj je sprječavanje bilo kakvih kriminalnih radnji i opasnih događaja. Često su sposobni za izvođenje uhićenja, rukovanje opremom za prvu pomoć i opasnost, pisanje detaljnih izvještaja i izvođenje drugih zadataka definiranih ugovorom. Mnogi zaštitari prolaze posebne treninge prije zapošljavanja kako bi mogli obavljati i zahtjevnije i opasnije radnje (poput nošenja oružja te deaktivacije eksplozivnih naprava).

Osim navedenog, zaštitari mogu provoditi kontrolu na ulazu u objekte u obliku osiguravanja da zaposlenici i posjetitelji pokažu identifikacijske iskaznice prije ulaska. Također, često moraju reagirati u slučaju neke opasnosti te usmjeriti osoblje na izlaz ili dokumentirati incident.

Obično, veliki dio dužnosti jednog zaštitara čini i patroliranje, tj. obilaženje prostorija kako bi se uvjerili u odsutnost bilo kakvih prijetnji. Međutim, u zadnje vrijeme elektronički sustavi (poput alarma i detektora pokreta) su postali popularniji pa patroliranje nije više neophodno za održavanje sigurnosti.

Zapošljavanje zaštitara može uvelike povećati fizičku sigurnost informacijskog sustava umanjivanjem opasnosti od ljudskih prijetnji, provođenjem kontrole pristupa te umanjivanjem štete od nekih nezgoda (poput požara).

5.4. Nadzorne kamere

U svrhu fizičke zaštite operacijskog sustava najčešće se koriste CCTV (eng. *Closed-circuit television*) kamere koje prenose signal do određenog mjesta na ograničen broj zaslona. Osnovno obilježje ovih kamera je da se signal ne prenosi kao kod televizijskog sustava, nego se radi o „zatvorenom sustavu“ gdje signal putuje do jednog ili nekoliko zaslona. Moguće ih je koristiti i za nadzor nekog procesa ili koraka u razvoju u okolišima koji nisu prikladni za ljude (npr. zbog radijacije).

Napredniji oblici ovih kamera, DVR (eng. *Digital Video Recorders*) kamere, omogućuju snimanje stanja kroz veća vremenska razdoblja s raznim kvalitetama i opcijama (poput detekcije pokreta).

Nadzorne kamere pomažu u održavanju fizičke sigurnosti tako da:

- sprječavaju zločine,
- omogućavaju praćenje prijevoza opreme,
- pružaju mogućnost kontrole prilaska objektima,
- omogućuju identifikaciju osoba na ulazu i
- omogućuju praćenje aktivnosti zaposlenika i posjetitelja.

U posljednje vrijeme sve se više koriste IP (eng. *Internet protocol*) kamere koje omogućuju stalni pregled stanja preko bilo koje veze na Internet. Slika 17 prikazuje jednu vrstu IP kamera koje rade s bežičnim mrežama uz stalno napajanje.

Prednosti uporabe ovakvih kamera su sljedeće:

- mogućnost dvosmjernog prenošenja audio zapisa,
- veća rezolucija slike,
- fleksibilnost,
- prijenos naredbi za povećavanje slike, okretanje kamera i sl.,
- mogućnost šifriranja sadržaja,
- mogućnost udaljenog pristupa,
- novčana efikasnost kod većih sustava te
- mogućnost uporabe na bežičnim mrežama.

Ipak, postoje određeni nedostaci uporabe IP kamera, a to su:

- nedostatak standarda,
- zahtjev za velikim resursima za prijenos sadržaja,

- tehnički problemi (pravilno postavljanje mrežnih postavki i uređaja),
- mogućnost narušavanja privatnosti.

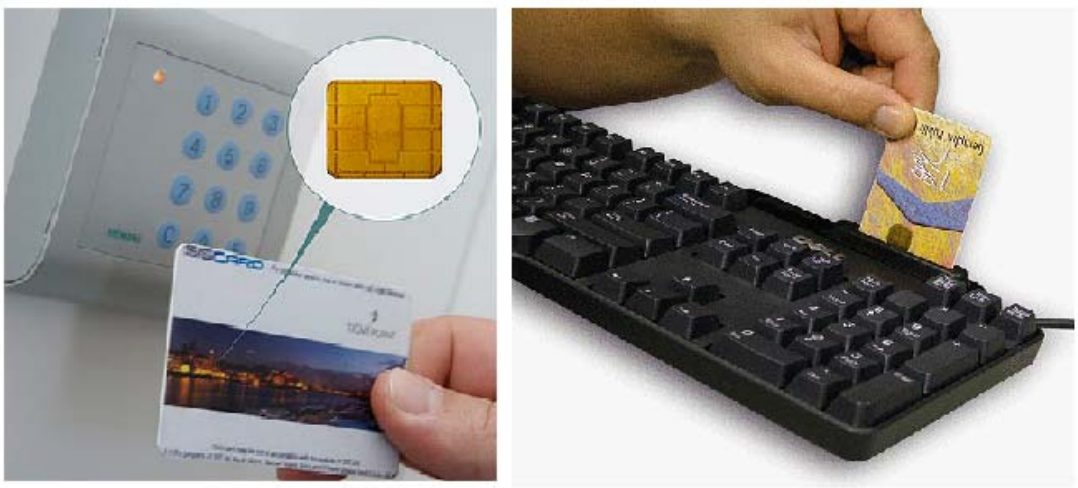
Slika 17. IP kamera
Izvor: wikipedia

5.5. Uređaji za kontrolu pristupa

Fizička kontrola pristupa može se održavati raznim uređajima kako bi se postigla odgovarajuća razina sigurnosti. Jedan od načina je uporaba pametnih kartica, tj. kartica s integriranim sklopovima. Postoje dvije osnovne vrste kartica:

- memorijske kartice - sadrže memorijske komponente za pohranu i određenu logiku.
- mikroprocesorske kartice - sadrže mikroprocesor i memorijske komponente.

Izgrađene su od plastike te često sadržavaju hologram kako bi se spriječilo krivotvorenje. Vrlo su korisne za proces autentikacije i identifikacije. Uvođenjem pametnih kartica može se osigurati kontrola pristupa objektima, ali i određenim uređajima i opremi kako je vidljivo na Slika 18.



Slika 18. Kontrola pristupa putem pametnih kartica

Osim pametnih kartica razvijeni su uređaji koji obavljaju kontrolu pristupa identificiranjem osoba preko određenih bioloških karakteristika. Riječ je o metodama biometrike za jednostavno prepoznavanje ljudi na temelju jedne ili više fizičkih osobina. U računarstvu se koristi kao oblik autorizacije za upravljanje i

kontrolu pristupa opremi. Također, može se koristiti za identifikaciju pojedinaca u skupinama koje trebaju biti pod nadzorom (npr. posjetitelja ili radnika).

Fiziološke karakteristike koje se koriste za identifikaciju mogu se klasificirati u dvije skupine:

1. Fiziološke – odnose se na oblik tijela, a uključuju otisak prsta, prepoznavanje lica, geometrije ruke, šarenice oka i sl.
2. Ponašajne – odnose se na ponašanje osoba, a uključuju ritam, hod ili glas.

Uređaji za kontrolu pristupa zasnovani na biometrici uključuju provjeru jedne ili više fizioloških i ponašajnih osobina. Neki od uređaja koji osiguravaju kontrolu pristupa objektima i opremi preko kontrole biometričkih obilježja dani su na Slika 19.

Slika 19. Kontrola pristupa preko biometrike

5.6. Sustavi za zaključavanje prostorija

Lokoti su mehanički ili elektronički uređaji koji se otvaraju fizičkim objektom (ključ, kartica i sl.), tajnom informacijom (poput lozinke) ili njihovom kombinacijom. Osnovna namjena im je sprječavanje fizičkog pristupa nekom dobru ili imovini, a mogu se koristiti na vratima, prozorima, ormarićima ili uređajima. Ovisno o njihovom dizajnu i implementaciji moguće je pružiti različitu razinu sigurnosti.

Mehanički lokoti imaju pomične dijelove kojima se rukuje bez električnog pogona. Za razliku od njih, elektronički lokoti sadrže skenere koji služe za očitavanje kodova te komponente za provjeru identiteta. Postoje brojne inačice spomenutih vrsta lokota, a primjer jednog mehaničkog i elektroničkog lokota dan je na Slika 20.

Slika 20. Mehanički i električki lokot

Sigurnosni problemi vezani uz lokote javljaju se uslijed „obijanja lokota“ tj. otključavanja pomoću analiziranja i manipuliranja komponentama uređaja bez originalnog ključa. Osnovno obilježje ovakvog načina otvaranja lokota je da ne dolazi do fizičkog oštećenja. Razvijeni su razni uređaji i tehnike za

provođenje opisanog postupka. Međutim, postoje načini sprječavanja upada putem korištenja alarmnih sustava ili elektroničkih lokota.

5.7. Uređaji za zaključavanje opreme

Fizička sigurnost može se postići primjenom uređaja za zaključavanje opreme. Razvijeni su razni načini za zaključavanje uređaja, a jedan od njih je korištenje sustava koji omogućuju fizičko zaključavanje kabela. Sustav „Kensington Security Slot", prikazan na Slika 21, je mali utor na gotovo svim prijenosnim računalima i elektroničkoj opremi (računalnih zaslona, igraćim konzolama, video projektima i sl.). Koristi se za spajanje uređaja za zaključavanje kabela. Obično se primjenjuje ključ ili lokot s kombinacijama pričvršćen na metalni kabel. Jedan kraj kabela sadrži malu petlju koja omogućuje povezivanje oko nekog objekta poput stola.

Opisani kabeli nisu dizajnirani kao neprobojne mjere zaštite jer su obično građeni od plastike ili tankog metala. Ipak prisilno vađenje kabela iz uređaja nije moguće pa ostaje trajna indikacija kako je uređaj ukraden.

Postoje alternativne metode mehanizma zaključavanja koje ne zahtijevaju postojanje posebnog utora na uređaju. Povezuju se na popularne priključke kao što su VGA ili priključak za pisač te imaju posebne vijke za osiguravanje na mjestu. Također, postoje potpuno elektronička rješenja koja sadrže i alarmne sustave.

Slika 21. Kensington Security Slot
Izvor: Kensington Slot

Umjesto zaključavanja kabela moguće je upotrijebiti uređaje za zaključavanje prijenosnog računala. Radi se o držačima koji sadrže neku vrstu lokota. Obično se lokoti postavljaju tako da obuhvaćaju cijelo računalo te se povezuju s nekim nepomičnim objektom. Prijenosno računalo je osigurano bez obzira da li je trenutno u upotrebi. Nedostatak ovih držača je smanjena pokretljivost, ali mogu se primijeniti kod uređaja koji ne sadrže posebne utore za zaključavanje. Primjeri držača s funkcijom zaključavanja prijenosnih računala prikazani su na Slika 22.

Slika 22. Držači za zaključavanje uređaja
Izvor: computer-security

Najjednostavniji način zaključavanja opreme je njena pohrana u odgovarajuće ormariće. Primjeri ormarića za sigurnu pohranu opreme dani su na Slika 23.

Pri odabiru takvih ormarića potrebno je voditi računa o:

- konstrukciji ormarića,
- načinu zaključavanja,
- mogućnosti korištenja kabela za povezivanje s napajanjem i drugim uređajima (npr. pisačima),
- prenosivosti,
- jednostavnosti rukovanja i
- mogućnosti razmještanja polica u unutrašnjosti.

Slika 23. Primjeri ormarića za pohranu opreme
Izvor: datalinksales

5.8. Sustavi za praćenje i otkrivanje lokacije

Sustavi za praćenje i otkrivanje lokacije imaju ulogu detektirati krađu te otkriti položaj ukradenog uređaja ili druge opreme. Vrlo su korisni u slučajevima gubitka neke od važnih komponenata, uređaja za pohranu podataka i sl.

Pri krađi prijenosnih računala, organizaciji se nanosi materijalna šteta puno veća od same vrijednosti uređaja. Razlog tomu je što oni često sadrže razne važne podatke o poslovanju, zaposlenicima, kupcima, partnerima, proizvodima i dr.

„LoJack“ je program koji omogućuje otkrivanje lokacije ukradenih prijenosnih računala njegovim praćenjem preko Internet mreže. Radi se o programu koji obavlja periodičke pozive u centar za kontrolu dojavljujući lokaciju te provjeravajući je li prijavljena krađa.

„Locate Laptop“ je program koji provodi kontinuirano praćenje lokacije prijenosnih računala dok je spojeno na Internet. U slučaju krađe, pri prvom spajanju na Internet obavještava korisnika o lokaciji ukradenog uređaja. Također, provodi i „tajno“ šifriranje svih podataka koje korisnik prethodno označi za tu namjenu.

„GadgetTrak“ je programsko rješenje za praćenje i otkrivanje lokacije ukradenih prijenosnih računala. Rad zasniva na iskorištavanju ugrađenih kamera i veze na Internet. Nakon aktivacije ukradenog uređaja, aktivira se ugrađena kamera te se snimaju fotografije osobe koja koristi računalo. Svakih 30 minuta slike i trenutna lokacija šalju se vlasniku putem poruka elektroničke pošte.

Postoje i sustavi koji omogućuju praćenje lokacije USB medija, kao što je „Track Stick“. Radi se o sustavu koji zapisuje lokaciju, vrijeme, datum te neke dodatne informacije u određenim intervalima. Putem podataka primljenih preko satelitske veze provodi se proračun trenutne lokacije.

Zaključak

Fizička sigurnost predstavlja vrlo važan aspekt sigurnosti svake organizacije i njenog informacijskog sustava. Podrazumijeva uklanjanje ili smanjivanje prijetnji koje dolaze od prirodnih nepogoda i ljudi te nekih nepredviđenih nesretnih događaja (požara, eksplozije i sl.). Spomenute prijetnje mogu nanijeti ozbiljnu štetu informacijskom sustavu u obliku oštećenja opreme i uređaja te gubitka važnih podataka.

Kako bi se umanjila šteta uzrokovana pojavom neke prijetnje, uvode se mjere za fizičku zaštitu informacijskih sustava. One uključuju zaštitu okoline i unutrašnjosti objekta, adekvatno provođenje kontrole pristupa te osiguravanje opreme. Za svaki navedeni element potrebno je uvesti posebne mjere zaštite kako bi se ostvarila željena razina fizičke sigurnosti.

Razvijeni su razni uređaji koji služe za provođenje fizičke sigurnosti poput alarmnih sustava koji služe za upozoravanje na opasnosti i izvanredne situacije. Osim alarma, često se koriste sustavi za detekciju dima, nadzorne kamere, sustavi za kontrolu pristupa te uređaji za zaključavanje opreme. Svaka navedena komponenta može pomoći pri zaštiti informacijskog sustava ako se primjeni na adekvatan način.

Ostvarivanje fizičke sigurnosti zahtjeva analizu stanja sustava te planiranje potrebnih mjera. Kako bi se spriječilo narušavanje fizičke sigurnosti potrebno je osigurati sve ključne elemente i dijelove informacijskog sustava. Ipak, održavanje fizičke sigurnosti nije dovoljno za postizanje sigurnosti informacija ukoliko se ne primjene dodatne mjere za zaštitu računala i sustava.

6. Reference

[1] Fizička sigurnost, http://en.wikipedia.org/wiki/Physical_security, lipanj, 2010.

[2] INFORMATION SYSTEMS SECURITY QUESTIONNAIRE, http://www.bussvc.wisc.edu/intaudit/IS.html#C, lipanj, 2010.

[3] Lawrence J. Fennelly, „Effective Physical Security", Elsevier Inc., 2004.

[4] Physical Security Assessments, http://www.slideshare.net/agent0x0/physical-security-assessments-presentation, lipanj, 2010.

[5] PHYSICAL SECURITY, http://www.infosyssec.org/infosyssec/physical_security.htm, lipanj, 2010.

[6] Access control, http://en.wikipedia.org/wiki/Access_control, lipanj, 2010.

[7] CPTED, http://en.wikipedia.org/wiki/Crime_Prevention_Through_Environmental_Design, lipanj, 2010.

[8] Physical Security (Policy), http://www.t2pa.com/t2pwikis/doku.php?id=it_policies:physical_security_policy, lipanj, 2010.

[9] Ethical Hacking and Countermeasures v6, Module XXI: Physical Security, lipanj, 2010.

[10] The Cost of Lost Data, http://gbr.pepperdine.edu/033/dataloss.html, lipanj, 2010.

[11] Understanding Data Loss, http://www.ontrackdatarecovery.com.au/understanding-data-loss/, lipanj, 2010.

[12] Water Main Break Floods Dallas Dana Center, http://www.datacenterknowledge.com/archives/2010/06/07/water-main-break-floods-dallas-data-center/, lipanj, 2010.

[13] Vital data lost in Intellectual Property office fire, http://www.indianexpress.com/news/vital-data-lost-in-intellectual-property-off/462238/, lipanj, 2010.

[14] Veterans' dana swiped in theft, http://news.cnet.com/Veterans-data-swiped-in-theft/2100-1029_3-6075212.html, svibanj, 2006.

[15] JournalSpace data loss terminal, http://www.bit-tech.net/news/2009/01/07/journalspace-data-loss-terminal/1, siječanj, 2009.

[16] Alarm, http://en.wikipedia.org/wiki/Alarm, lipanj, 2010.

[17] Fire alarm system, http://en.wikipedia.org/wiki/Fire_alarm_system, lipanj, 2010.

[18] Smoke detector, http://en.wikipedia.org/wiki/Smoke_detector, lipanj, 2010.

[19] Security lighting, http://en.wikipedia.org/wiki/Security_lighting, lipanj, 2010.

[20] Security guard, http://en.wikipedia.org/wiki/Security_guard, lipanj, 2010.

[21] CCTV, http://en.wikipedia.org/wiki/Closed-circuit_television, lipanj, 2010.

[22] Lock, http://en.wikipedia.org/wiki/Lock_%28device%29, lipanj, 2010.

[23] LoJack, http://en.wikipedia.org/wiki/LoJack, lipanj, 2010.

[24] Locate Laptop, http://www.locatelaptop.com/, lipanj, 2010.

[25] GadgetTrak,http://www.gadgettrak.com/products/pc/, lipanj, 2010.

[26] Kensington Security Slot, http://en.wikipedia.org/wiki/Kensington_Security_Slot, lipanj, 2010.