FIZIČKA ZAŠTITA DIGITALNIH PODATAKA

Jurišić, Gabrijela

Master's thesis / Specijalistički diplomski stručni

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:860493

FIZIČKA ZAŠTITA DIGITALNIH PODATAKA

Jurišić, Gabrijela

Master's thesis / Specijalistički diplomski stručni

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Karlovac University of Applied Sciences / Veleučilište u Karlovcu**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:128:860493

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Gabrijela Jurišić

FIZIČKA ZAŠTITA DIGITALNIH PODATAKA

ZAVRŠNI RAD

Karlovac, 2022.

Karlovac University of Applied Sciences

Safety and Protection Department

Professional graduate study of Safety and Protection

Gabrijela Jurišić

PHYSICAL PROTECTION OF DIGITAL DATA

Final Paper

Karlovac, 2022

Veleučilište u Karlovcu

Odjel Sigurnosti i zaštite

Specijalistički diplomski stručni studij sigurnosti i zaštite

Gabrijela Jurišić

FIZIČKA ZAŠTITA DIGITALNIH PODATAKA

ZAVRŠNI RAD

Mentor:

Dr. sc. Damir Kralj, prof. v. š.

Karlovac, 2022.

PREDGOVOR

Izjavljujem da sam ovaj rad izradila samostalno koristeći se dostupnom i u radu navedenom literaturom te znanjem koje sam stekla tijekom studija.

Zahvaljujem se mentoru dr. sc. Damiru Kralju, prof. v. š. na pruženoj podršci, stručnoj pomoći, savjetima i razumijevanju tijekom izrade diplomskog rada.

SAŽETAK

Zaštita digitalnih podataka bitna je u domeni evidencija zaštite na radu. Narušavanje sigurnosti digitalnih podataka može dovesti do otkrivanja osjetljivih podataka te materijalnih gubitaka, koji mogu utjecati na zdravlje i život radnika, velike materijalne štete, kao i terorističke napade. Jedan od aspekata sigurnosti digitalnih podataka predstavlja fizička sigurnost, odnosno skup mjera koje sprječavaju nedozvoljen fizički pristup podacima i resursima. Fizičkoj sigurnosti digitalnih podataka prijetnje dolaze od prirodnih nepogoda poput poplava i potresa, te ljudskih ranjivosti poput neposlušnosti, namjere za sabotažom ili krađom. Također, postoje prijetnje koje su rezultat nepredviđenih okolnosti kao što je rat, požar ili neke vrste kvarova na raznim sustavima. Kao prevencija kojom bi se smanjila šteta nakon pojavljivanja gore spomenutih prijetnji uvode se adekvatne mjere zaštite, osiguranje okoline i prostorija objekata, recepcije, te provođenje kontrole pristupa. Također, potrebno je implementirati zaštitu opreme i uređaja putem dostupnih tehnologija. Razvijeni su razni sustavi za uspostavljanje i poboljšanje fizičke sigurnosti digitalnih podataka. Neki od njih su alarmni sustavi te sustavi za nadzor, kontrolu pristupa ili zaključavanje vrijednih uređaja.

Ključne riječi: podaci, fizička zaštita digitalnih podataka, mjere zaštite, sredstva zaštite, mediji za pohranu podataka, informacijska sigurnost, zakonska regulativa.

SUMMARY

The protection of digital data is essential in the domain of occupational safety records. Violation of the security of digital data can lead to the disclosure of sensitive data and material losses, which can affect the health and life of workers, large material damages, as well as terrorist attacks. One of the aspects of digital data security is physical security, that is, a set of measures that prevent unauthorized physical access to data and resources. Threats to the physical security of digital data come from natural disasters such as floods and earthquakes and human vulnerabilities such as disobedience, sabotage or theft. Also, there are threats that are the result of unforeseen circumstances such as fire caused or some kind of malfunctions in various systems. Adequate protection measures, security of the environment and premises of the facilities, reception, and implementation of access control are introduced as a prevention to reduce damage after the appearance of the above-mentioned threats. Also, it is necessary to implement the protection of equipment and devices through available technologies. Various systems have been developed to establish and improve the physical security of digital data. Some of them are alarm systems and systems for monitoring, access control or locking of valuable devices.

Keywords: physical protection of digital data, protection measures, means of protection, data storage media, law regulation.

SADRŽAJ

1.UVOD

Zaštita digitalnih podataka se sastoji od tri osnovne vrste zaštite. Prva od koje sve kreće je fizička zaštita koja onemogućuje neovlašteni pristup podatcima i informacijama. Druga je pravna zaštita, ona postavlja pravni okvir za zaštitu podataka i informacija u slučaju zlouporabe tih podataka i treća koja u pravilu nije osnovna kategorija je kompenzacijska zaštita, odnosno umanjenje štete nastale zloporabom podataka. Prvoj je zadatak sprječavanje neovlaštenog pristupa odnosno fizičko onemogućavanje pristupa podacima. Druga, pravna zaštita djeluje preventivno prije neovlaštenog pristupa i nakon neovlaštenog pristupa djeluje represivno, dok treća kompenzacijska odnosno osiguravajuća zaštita djeluje nakon neovlaštenog pristupa i zlouporabe kompenzirajući štetu. Fizička zaštita podataka i informacija razlikuje se ovisno o tome gdje se podatak ili informacija nalazi, odnosno radi li se o stvarnom mjestu kao prostorija ili otvoreni prostor ili se radi o „virtualnom“ mjestu kao što su sustavi za računalnu pohranu podataka. Također ovisi i na kakvom mediju se podaci nalaze. U slučaju kada se radi o fizičkoj zaštiti medija na kojem se nalaze podaci, a radi se o stvarnom prostoru, a ne o računalnoj mreži tada se provode mjere fizičke zaštite koje uključuju alarmne sustave, rasvjetu, zaštitare, nadzorne kamere, fizičke prepreke, uređaje za kontrolu pristupa, sustave za zaključavanje prostorija, uređaje za zaključavanje opreme te uređaje za praćenje lokacije.

Fizička zaštita podataka je proces u kojem se osiguravaju digitalni podaci od neovlaštenog pristupa, gubitka ili krađe. To je koncept koji obuhvaća fizičku zaštitu osoblja, fizičkih dijelova elektroničkih računala, računalnog sustava ili sličnog elektronskog uređaja, programske podrške, mreža i podataka od fizičkih radnji i događaja koji bi mogli uzrokovati ozbiljan gubitak ili štetu poduzeću, agenciji ili instituciji. To uključuje zaštitu od požara, poplava, prirodnih katastrofa, provala, krađe, vandalizma i terorizma.[1]

Postoji niz sigurnosnih prijetnji, svaka s različitim razinama vjerojatnosti, ozbiljnosti i razmatranja, koje su jedinstvene za svako pojedino dijeljenje podatka i mehanizme pristupa.[2]

Ključ za povećanje mjera sigurnosti je ograničiti i kontrolirati pristup ljudi mjestima, objektima i materijalima, obzirom na to imamo fizički sigurnosni okvir koji se sastoji od tri glavne komponente: kontrole pristupa, nadzora i testiranja. Primjeri barijera koji se često koriste su: ID značke, tipkovnice i zaštitari. Sigurnost pristupa je kategorizirana u tri razine: visoka, srednja i niska sigurnost. Uspjeh programa fizičke zaštite organizacije često se može pripisati tome koliko je dobro svaka od ovih komponenti implementirana, poboljšana i održavana.[1] Stoga dolazimo do zaključka da je jedna od bitnih zadaća zaštite na radu također i zaštita podataka, jer gubitkom istih može doći do gašenja sustava te neočekivanih posljedica u postrojenjima tvrtki.

Cilj ovog rada je na osnovu dostupnih izvora te vlastitih iskustava, stečenih znanja tijekom školovanja i prakse, analizirati važnost fizičke zaštite osjetljivih digitalnih podataka kao vrlo bitnog čimbenika sigurnosti i zaštite života i zdravlja ljudi kao i materijalnih dobara. Osvrnuti se na pravnu regulativu u ovom području, te u eksperimentalnom djelu opisati i analizirati efikasnost fizičke zaštite digitalnih podataka.

Metoda za izradu ovog rada je bila istraživanje i analiza dostupnih pisanih i mrežnih izvora koji sadrže i obrađuju informacije o važnosti fizičke zaštite digitalnih podataka, metodama kojima se štite digitalni podaci, te o primjeni zakonske regulative u ovom području.

2. PODACI I NJIHOVA POHRANA

Podaci objašnjavaju skup entiteta koji sadrže opis nekog događaja, zapažanja ili činjenice, stoga se može reći da element podataka može biti broj, riječ, slika ili neki drugi proizvoljan zapis. Ukoliko podaci predstavljaju neku činjenicu za koju je utvrđeno da neosporno vrijedi, tada ti podaci predstavlja informaciju. Sirovim podacima nazivaju se brojevi, znakovi, slike ili ostali izlazi iz uređaja koji pretvaraju fizičke veličine u simbole, u širem smislu riječi. Izraz „sirovi podaci“ je termin relativnog značenja jer se obrada podataka najčešće događa u nekoliko faza gdje se obrađeni podaci iz jedne faze mogu smatrati sirovim podacima za sljedeću. Mehanički uređaji za računanje klasificirani su prema načinu na koji zapisuju podatke. Analogna računala predstavljaju podatke kao što su: napon, udaljenost, položaj ili neku drugu fizikalnu veličinu. Digitalna računala predstavljaju podatke kao nizove simbola uzete iz konačnog skupa simbola, tzv. abecede simbola. Najčešće se u digitalnim računalima koristi binarna abeceda. Binarna se abeceda sastoji od dva znaka, tipično '0' i '1'. Binarnom se abecedom mogu konstruirati simboli više razine poput slova ili brojeva. [3]

2.1. Pohrana podataka

Pohrana podataka podrazumijeva magnetske, optičke ili mehaničke medije koji bilježe i čuvaju digitalne podatke za tekuće ili buduće operacije. [4]

2.2. Mediji za pohranu digitalnih podataka

Fizički medij je svaki uređaj koji se koristi za pohranu podataka: tvrdi diskovi, SSD diskovi i prijenosni mediji. Izmjenjivi mediji uključuju uređaje poput USB pogona, DVD-ova i vanjskih tvrdih diskova. Uređaji za pohranu podataka moraju zadovoljiti dva osnovna uvjeta. Prvi je da moraju omogućiti pouzdano zapisivanje, a drugi da moraju omogućiti pouzdano čitanje podataka. Valja uočiti da su ta dva uvjeta povezana pojmom pouzdanosti koji je ujedno i najvažnija osobina svakog uređaja ove vrste. Upravo je pouzdanost bila poticaj proizvođačima na razvoj boljih i različitijih uređaja za pohranu podataka. Osim pouzdanosti, vrlo važan čimbenik u razvoju i radu svakog uređaja za masovnu pohranu (engl. *mass storage*) je i njegova brzina. Riječ je o uređajima na koje je

moguće pohraniti velike količine podataka, a uključuju tvrde diskove, USB memorije, diskete, vrpce i sl. Ne uključuju radne memorije budući da one nemaju svojstvo zadržavanja podataka bez utroška energije. Ovisno o načinu pristupa, pohranjeni podaci se dijele u tri kategorije: izvanmrežna pohrana koja nije odmah dostupna *(engl. off-line),* odmah dostupna pohrana *(engl. on-line)* ili nije dostupna odmah, ali se može brzo postati dostupna bez ljudske intervencije *(engl. near-line)*. Standardni tvrdi disk svakog osobnog računala primjer je *on-line* uređaja, uređaja gdje su podaci u svakom trenutku dostupni procesoru. Uređaji koji koriste traku, kasete s trakom (ili nekim drugim medijem), CD-čitači i drugi slični uređaji primjer su *off-line* uređaja. Pristup podacima moguć je tek nakon što se obavi eksterna predradnja kao što je stavljanje odgovarajuće trake u uređaj. [2]

2.2.1. Magnetski mediji

Prvi mediji za pohranu podataka koristili su magnetske valjke i trake. Vrlo brzo došlo se do zaključka da su trake daleko pouzdaniji medij pa su unatoč inicijalnoj sporosti odnijele prevagu. Pouzdanost uređaja za masovnu pohranu koji koriste traku bila je od samog početka toliko velika da se u različitim oblicima javljaju i danas, čineći traku tako jednim od najdugovječnijih medija u korištenju računala. Pouzdanost zapisa im je dobra, no duže arhiviranje zahtjeva ipak skladištenje u odgovarajućim uvjetima. U profesionalnim uvjetima najpopularniji su DLT uređaji, dok su uređaji koji koriste DAT i naročito QIC trake zanimljiviji ostalim korisnicima. Najveća mana svih tih medija je spor pristup podacima koji je prije svega uvjetovan činjenicom da je traka sekvencijalni medij. Unatoč činjenici da moderni uređaji koji koriste trake imaju mehanizam praćenja zapisa te da kvaliteta traka omogućuje njihovo izuzetno brzo premotavanje, još uvijek je potrebno puno vremena (mjeri se u minutama) da bi se došlo do željenih podataka. Usporedno s trakama razvijali su se i ostali mediji za pohranu, a ponajprije se to odnosi na diskove koji su zbog brzine pristupa i pouzdanosti postali nezaobilazan element on-line pohrane podataka. Temeljni princip rada nije se promijenio od njihova nastanka.

U hermetički zatvorenom kućištu nalazi se jedna ili više aluminijskih ploča na koje je s jedne ili obje strane nanesen magnetski sloj. Podaci se čitaju i pišu

pomoću jedne ili više glava (svaka za jednu stranu pojedine ploče). Taj relativno jednostavan sustav u stanju je u modernim diskovima pohraniti zaista velike količine podataka. Osim kapacitetom, diskovi se odlikuju izuzetno brzim pristupom podacima (mjeri se u milisekundama) te velikom brzinom prijenosa podataka (više desetaka pa i do preko stotinu MB), što ih čini idealnim on-line uređajima za pohranu. Ipak nisu bez mana, a tu se prije svega ubrajaju osjetljivost na udare i vibracije. [3]

2.2.2. Optički mediji

Razvoj tehnologije doveo je, naročito u zadnjim desetljećima, do pojave posve novih načina zapisivanja podataka te shodno tome i do pojave posve novih uređaja. Najznačajniji je bio prijelaz na optički zapis koji je omogućio pohranu velikih količina podataka na vrlo malom prostoru kao i bitno duži životni vijek tako zapisanih podataka. Najpoznatiji današnji medij koji koristi optičko zapisivanje podataka je svakako CD/DVD-ROM. Na CD medij može se pohraniti 650 MB podataka (neki mediji dopuštaju i nešto veći kapacitet) kojima se može pristupiti sasvim zadovoljavajućom brzinom uz brzinu prijenosa koja u praksi ne zaostaje puno za diskovima. Potreba za skladištenjem veće količine podataka dovela je do prodora DVD medija na tržište, a time i uređaja za njihovo snimanje odnosno čitanje. Tehnologija je u suštini jednaka, samo se koriste preciznija optika i laserske glave koje rade na kraćim valnim dužinama. Današnji uređaji u okviru jednog CD/DVD pogona obuhvaćaju čitač i pisač CD medija te čitač i pisač DVD medija. [3]

2.2.3. Mješoviti mediji

Tijekom razvoja uređaja za masovno pohranjivanje iskušavane su različite tehnologije pa se tako došlo na ideju da se neke od njih kombiniraju. Jedna takva uspješna kombinacija predstavlja spoj magnetske i optičke tehnologije, a najpoznatiji njeni predstavnici su magnetno-optički diskovi. Osnovni materijal za zapisivanje je magnetski, ali posve drugačiji od onoga koji se nalazi na diskovima. Tijekom zapisivanja optički dio uređaja - laser, pripremit će magnetski sloj za zapisivanje koje će obaviti magnetska glava. Čitanje podataka obavlja optički dio uređaja, odnosno laser s pripadajućim optičkim sustavom. Magnetno-optički

mediji za pohranu podataka predstavljaju vrlo pouzdane sustave jer kombiniraju dobre osobine jedne i druge tehnologije. Visoka koercitivnost magnetno-optičkih diskova odnosno svojstvo feromagneta da se opire demagnetizaciji razlog je gotovo potpunom imunitetu na ″samobrisanje″ koje se javlja kod svakog magnetskog medija, a očituje se u slabljenju magnetskog polja koje definira zapis. Upravo zbog toga će magnetno-optički mediji podatke zadržavati duže od drugih čisto magnetskih tehnologija, pa su pogodni za arhiviranje podataka na duže vrijeme. [3]

2.2.4. Oblak

Usluge u oblaku (eng. *Cloud*) pružaju rješenje za pohranu podataka, koje također služi kao mehanizam za prijenos podataka. Platforme u oblaku omogućuju jednostavan pristup tvrtkinoj infrastrukturi. U isto vrijeme platforme za računalstvo u oblaku pružaju, pouzdanost, visoke performanse i mogućnost konfiguracije. [5] Pohranjivanje podataka na oblak omogućava korisnicima brzo i jednostavno pristupanje podacima, odnosno može im se pristupiti bilo kad i bilo gdje. Privatnost i sigurnost su mu najveća mana, budući da se podaci raznih korisnika i poslovnih organizacija nalaze zajedno u oblaku, kako bi se izbjegla moguća zloupotreba podataka koji se nalaze na oblaku dobro bi bilo šifrirati te podatke prije učitavanja na oblak. Šifriranje podataka osigurava da podaci nisu vidljivi vanjskim korisnicima i administratorima oblaka. Postoje četiri glavne pohrane u oblaku:

1. Osobna pohrana u oblak-poznata je kao mobilna pohrana u oblaku. Podaci pojedinca se pohranjuju u oblak kako bi bili dostupni bilo kad i bilo gdje.

2. Javna pohrana u oblak- poduzeće i davatelj usluge pohrane su odvojeni i ne postoje resursi oblaka pohranjeni u podatkovnom centru poduzeća. ova vrsta oblaka nije preporučljiva tvrtkama, jer ova vrsta institucija zahtijeva višu razinu sigurnosti i superiornu pohranu, što javni oblaci ne mogu ponuditi, zbog čega će spomenuti oblak koristiti ljudi koji žele pohranjivati njihove osobne podatke, bez straha od gubitka njihovih podataka iz bilo kojeg razloga.

3. Privatna pohrana u oblak- poduzeća i oblak pružatelj usluge pohrane su integrirani u podatkovni centar poduzeća. Privatni računalni oblaci najsigurniji su među svim računalnim oblacima, budući da su sve informacije koje se unose i pohranjuju kriptirane i pregledavaju od strane internetskog antivirusa koji ima oblak prema zadanim postavkama, omogućujući korisnicima da pohranjuju svoje podatke bez bilo kakvog štetnog agensa koji ne samo da šteti vašim podacima, nego je i veliki problem za oblak općenito. Raspon pohrane ovog oblaka veći je od javnog tipa, ali za prekoračenje utvrđenog ograničenja potrebno je platiti pretplatu. Još jedna nova kvaliteta ove vrste oblaka je njegova sposobnost prilagođavanja korisničkog ulaznog područja ovom alatu, kao i mogućnost prilagođavanja svega što korisnik želi, Nedostatak ove vrste oblaka je da, da biste uživali u svim njegovim funkcijama, kvalitetama i udobnosti, morate snositi mjesečne troškove za članstva ili pretplate, koji imaju različite iznose ovisno o modalitetima i pogodnostima koje nude korisnicima, ovisno o vrsti platforme koja se koristi.

4. Hibridna pohrana u oblak-kombinacija je javnog i privatnog pohranjivanja u oblak. Osjetljivi podaci se pohranjuju u privatni oblak poduzeća, dok se drugi podaci, manje osjetljivi pohranjeni i dostupni u javnoj pohrani u oblaku. [22]

3. 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. 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. [7]

4. ZAŠTITA PODATAKA U HRVATSKOJ I EUROPSKOJ UNIJI

4.1. Zakonski propisi u području zaštite podataka

U Republici Hrvatskoj informacijsku sigurnost regulira Zakon o informacijskoj sigurnosti (NN79/07), a primjenjuje se na državna tijela, tijela jedinica lokalne i područne (regionalne) samouprave te na pravne osobe s javnim ovlastima koje u svom djelokrugu koriste klasificirane i neklasificirane podatke, na pravne i fizičke osobe koje ostvaruju pristup ili postupaju s klasificiranim i neklasificiranim podacima.

4.2. Mjere i standardi informacijske sigurnosti

Mjerama i standardima informacijske sigurnosti utvrđuju se minimalni kriteriji za zaštitu klasificiranih i neklasificiranih podataka. Mjere i standardi informacijske sigurnosti utvrđuju se za klasificirane i neklasificirane podatke, sukladno stupnju tajnosti, broju, vrsti te ugrozama klasificiranih i neklasificiranih podataka na određenoj lokaciji i stupnju tajnosti „Povjerljivo“, „Tajno“ i „Vrlo tajno“, trajno se provodi sigurnosna prosudba ugroze.

4.3. Fizička sigurnost

Fizička sigurnost je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti za zaštitu objekta, prostora i uređaja u kojem se nalaze klasificirani podaci. Tijela i pravne osobe koji koriste klasificirane podatke stupnja tajnosti „Povjerljivo“, „Tajno“ i „Vrlo tajno“ izvršit će kategorizaciju objekata i prostora na sigurnosne zone, propisane mjerama i standardima informacijske sigurnosti.

4.4. Sigurnost informacijskog sustava

Sigurnost informacijskog sustava je područje informacijske sigurnosti u okviru kojeg se utvrđuju mjere i standardi informacijske sigurnosti klasificiranih i neklasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijski sustav te zaštita cjelovitosti i raspoloživosti informacijskog sustava u procesu planiranja, projektiranja, izgradnje, uporabe, održavanja i prestanka rada informacijskog sustava. Sigurnosna akreditacija informacijskog sustav provodi se za informacijski sustav u kojem se koriste klasificirani podaci stupnja tajnosti

„Povjerljivo“, „Tajno“ i „Vrlo tajno“. Osobe koje sudjeluju u procesu utvrđivanja mjera i standarda informacijske sigurnosti klasificiranih i neklasificiranih podataka trebaju posjedovati certifikat razine „Vrlo tajno“ ili za jedan stupanj više od najviše razine tajnosti klasificiranih podataka koji se obrađuju, pohranjuju ili prenose u informacijskim sustavima pod njihovom nadležnosti. Mjere fizičke zaštite prostora u kojima se nalaze informacijski sustavi poduzet će se sukladno najvišoj razini tajnosti klasificiranih podataka koji se u njima obrađuju, pohranjuju ili prenose. Središnja državan tijela za informacijsku sigurnost ustrojavaju registar certificirane opreme i uređaja koji se koriste u klasificiranom informacijskom sustavu razine „Povjerljivo“, „Tajno“ i „Vrlo tajno“. Registar certificirane opreme i uređaja ustrojava se na temelju preuzimanja odgovarajućih registara međunarodnih organizacija ili vlastitim certificiranjem u skladu s odgovarajućim međunarodnim normama. [23]

4.5. Norme ISO 27000, 27001 i 27002

Najpoznatije međunarodne norme koje se bave informacijskom sigurnošću su ISO 27001 i ISO 27002, odnosno paleta normi ISO 27000. Te se norme stalno mijenjaju i dorađuju kako bi bile dio sustava u kojem su usklađene s drugim normama (primjerice s normom ISO 9001, koja se bavi upravljanjem kvalitetom poslovanja) i međusobno. Norma ISO 27001 bavi se uspostavom sustava upravljanja informacijskom sigurnošću, koji se označava kraticom ISMS *(engl. Information Security Management System)*. U toj normi su određeni ciljevi koje organizacija treba postići kako bi imala učinkovit sustav zaštite svojih podataka. ISO 27002 se bavi načinima, postupcima i najboljim praksama pomoću kojih se ti ciljevi mogu postići. U tom smislu je i tvrtka certificirana za HRN ISO/IEC 27001 usklađena i s hrvatskim propisima informacijske sigurnosti koji vrijede isključivo za neklasificirane podatke. Za zaštitu klasificiranih podataka razine ograničeno primjenjuju se, uz spomenutu normu ISO 27001 dodatno i druge mjere. Za zaštitu klasificiranih podataka povjerljivo i više, primjenjuju se zakonski i podzakonski akti informacijske sigurnosti, a posjedovanje certifikata ISO 27001 nije niti dovoljno niti nužno. Naravno, uspješna provedba norme kao što je ISO 27001, može olakšati provedbu propisanih mjera i standarda

informacijske sigurnosti jer su neki sigurnosni zahtjevi slični te sama realizacija može biti lakše usklađena. [24]

5. PRIJETNJE FIZIČKOJ SIGURNOSTI I GUBITKU DIGITALNIH PODATAKA

5.1. Fizička oštećenja

Širok raspon pogrešaka smože izazvati fizičko oštećenje medija za pohranu. CD/DVD mediji mogu imati izgrebenu podlogu, tvrdi disk može biti oštećen prilikom pada, nedopušteno visoka temperatura može oštetiti tvrde diskove (slika 1), a trake za pohranu mogu jednostavno puknuti. Ipak, kao jedan od najčešćih problema u računalima javlja se oštećenje tvrdog diska glavom za čitanje/pisanje. [7]

Slika 1. Oštećenje tvrdog diska pod utjecajem visoke temperature [9]

5.2. Logičke greške

Osnovni uzroci logičkih pogrešaka su:

• gubitak napajanja koji sprječava zapis struktura datotečnog sustava na medij,

• problemi sa sklopovljem i upravljačkim programima i

• rušenje sustava.

Rezultat bilo koje logičke pogreške je dovođenje sustava u nekonzistentno stanje što može uzrokovati razne probleme, poput:

• neočekivanog ponašanja

• rušenja sustava

• gubitak podataka.

Postoje razni programi za ispravak spomenutih stanja, a svi operacijski sustavi sadrže barem osnovni alat za popravak datotečnog sustava. [7]

5.3. Obrisani podaci

Brisanje podataka je metoda prepisivanja podataka kojom se u potpunosti uklanjanju svi elektronički zapisi podataka na tvrdom disku ili drugom digitalnom mediju. Trajno brisanje podataka nije isto što i osnovno brisanje datoteka. Postoje metode koje omogućuju potpuno uklanjanje podataka poput demagnetiziranja i fizičkog uništavanja diska. Postoje tri razine uklanjanja podataka:

1. Čišćenje osjetljivih informacija – uklanjanje osjetljivih podataka s uređaja za pohranu na takav način da je korisnik siguran kako izbrisane podatke nije moguće rekonstruirati uporabom raznih funkcija sustava ili programa za obnovu podataka. Ipak, podatke je još uvijek moguće obnoviti uporabom nekih specijaliziranih laboratorijskih tehnologija. Obično se koristi kao administrativna zaštita protiv slučajnog otkrivanja podataka u organizacijama.

2. Potpuno čišćenje – uklanjanje osjetljivih podataka sa sustava ili uređaja za pohranu s namjerom da se ne mogu rekonstruirati nikakvim poznatim tehnikama. Obično se obavlja prije otpuštanja medija izvan kontrole firme, kao što je odbacivanje medija ili premještaj u drugo sigurnosno okruženje.

3. Uništavanje – fizičko uništavanje medija spaljivanjem, taljenjem, mljevenjem, bušenjem ili na neki drugi način kako bi se spriječila obnova podataka.

Jedna od metoda brisanja podataka je njihovo prepisivanje novim podacima. Kod najjednostavnijeg oblika prepisivanja pohranjenih podataka zapisuju se neki podaci (obično uzorci nula) po svim sektorima diska, što pruža zaštitu od čitanja podataka s medija uporabom osnovnih funkcija sustava. Kako bi se izbrisali svi tragovi podataka te onemogućila uporaba tehnika obnove podataka, treba se koristiti neki složeniji uzorak (npr. uzorak nula i jedinica). [7]

5.4. 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 digitalnih podataka. Prirodne prijetnje mogu dovesti do ogromnih materijalnih gubitaka i prouzročiti veliku štetu, primjerice poplava kako je prikazano na slici 2 i potres prikazan na slici 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. [6]

Slika 2. Prikaz poplave [10]

Slika 3. Prikaz potresa [10]

5.5. Ljudske prijetnje

Zaposlenici su jedan od osnovnih rizika svake organizacije jer unose veliki raspon prijetnji sigurnosti. Neke od prijetnji prikazane na slici 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 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.

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. [6]

Slika 4. Ljudske prijetnje [6]

5.6. 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 slici 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).

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. [6]

Slika 5. Vrste napada u domeni socijalnog inženjeringa [6]

5.7. Ostale prijetnje

Postoje i brojne prijetnje koje mogu uzrokovati oštećenje podatka, gubitak podatka, odnosno 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. [6]

6. FIZIČKA ZAŠTITA PODATAKA

Sigurnosne postavke se uvelike oslanjaju na fizičko okruženje u kojem se podaci pohranjuju, obrađuju, prenose i pristupaju te iz kojih fizičke osobe mogu pristupiti računalima koja pohranjuju i obrađuju podatke. Fizička sigurnost podataka je samo jedna komponenta zaštite i sigurne uporabe podataka za istraživanje i ne može se razmatrati samostalno. Fizički sigurnosni okvir zaštite podataka sastoji se od tri komponente: kontrole pristupa, nadzora i testiranja. Fizička zaštita može imati mnogo oblika i formi. Strategije, prepreke i tehnike koje organizacije koriste za podršku općoj sigurnosti fizičke informacijske tehnologije, značajno se razlikuju od onih koje se koriste za omogućavanje dosljedne fizičke sigurnosti mreže. Sigurnost pristupa računalima može značajno varirati. Ovaj aspekt obuhvaća i mjesto gdje se nalazi pristupno računalo i vrstu pristupnog računala. Sigurnost pristupa kategorizirana je u tri skupine: visoka srednja i niska sigurnost. U slučajevima kada strana koja nije pružatelj podataka održava lokaciju pristupa, davatelji podataka obično imaju pravo odobriti sigurnosne aranžmane, provesti revizije ili na drugi način izravno provjeriti je li operater u skladu s obveznim sigurnosnim zahtjevima. Visoko sigurnosna pristupna lokacija ima jake specifikacije za fizičku sigurnost, zahtijeva korištenje sigurne sobe, obično zahtjeva dodatno ojačavanje prostorije osim kontrole pristupa, fizičkog nadzora od strane osoblja ili osoblja na lokaciji pristupa, uz bilo kakvo elektroničko praćenje pristupa samog računala. Dodatne zaštite i nadzor štite od neovlaštenog pristupa kao i od uklanjanja neovlaštenih izlaza s mjesta pristupa. Ako već ne postoje na lokaciji pristupa, zahtijevat će stručnost IT i sigurnosnih stručnjaka kako bi pomogli u definiranju specifikacija i implementaciji značajki pristupnih soba visoke sigurnosti. Mjesto za pristup srednje sigurnosti ima definiranu lokaciju s pristupom ograničenim samo za odobrene osobe. To mogu biti sobe osigurane ključnim karticama, biometrijskim podacima ili jednostavnom bravom i ključem ograničenim na odobreno osoblje. Takva ograničenja mogu biti osmišljena kako bi se spriječili pokušaji neovlaštenog pristupa ili kako bi se spriječilo surfanje preko ramena, odnosno čina pribavljanja privatnih ili osobnih podataka izravnim promatranjem. Prostorije s pristupom srednje sigurnosti mogu uzrokovati dodatne troškove za administratora lokacije, zahtijevajući namjenski

prostor i osoblje za održavanje same pristupne lokacije. Pristupna lokacija niske sigurnosti ima malo ili nimalo kontrola pristupa. Jednostavna ograničenja mogu uključivati široka geo-ograničenja ili postupke koje treba slijediti. Davatelji podataka mogu naložiti da se pristupno računalo smjeti u zaključanu sobu ili zahtijevati korištenje ograničenja IP adrese. Kada nisu nametnuta ograničenja pristupa, istraživači mogu slobodno koristiti pristupna računala s bilo kojeg mjesta. Osim gore opisane lokacijske sigurnosti, vrsta pristupnog računala također može varirati od visoke do niske sigurnosti. Vrlo sigurna pristupna računala mogu uključivati potpuno šifrirane operacijske sustave, korištenjem VPN-ova, softvera za udaljenu radnu površinu, sigurne mrežne protokole i šifriranje ili zahtijevanje biometrijske provjere autentičnosti pristupnog računala. To može biti u obliku namjenskih tankih klijenata. Računala s pristupom niske sigurnosti obično su dopuštena za daljinsko podnošenje ili pristup tipa web portala, gdje je dopušteno bilo koje računalo, na bilo kojem mjestu. [2]

6.1. 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 aspekt – općenite sigurnosne mjere koje se provode prije izvođenja neke operacije, primjerice 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. [6]

6.2. Uloga fizičke zaštite

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 primjer slojevite zaštite prikazan na slici 6. Slojevitu primjenu kontrola potrebno je implementirati od unutarnjih do vanjskih granica. 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. [6]

Slika 6. Slojevita fizička sigurnost [6]

6.3. 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. 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. 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. [6]

7. KOMPONENTE FIZIČKOG SIGURNOSNOG OKVIRA

7.1. Kontrola pristupa

Kontrola pristupa obuhvaća mjere poduzete kako bi se ograničila izloženost određene imovine samo ovlaštenom osoblju. Zgrada je često prva linija obrane za većinu fizičkih sigurnosnih sustava. Predmeti kao što su ograde, zidovi, vrata djeluju kao fizičko odvraćanje od ulaska kriminalaca. Dodatne brave, bodljikava žica, vidljive sigurnosne mjere i znakovi smanjuju broj slučajnih pokušaja kibernetičkih kriminalaca. Sofisticiranije kontrole pristupa uključuje pristup podržan tehnologijom. Skeneri osobnih iskaznica i komunikacijske osobne iskaznice. Koristeći taktički postavljene prepreke, organizacije mogu otežati napadačima pristup vrijednoj imovini i informacijama. Ove prepreke povećavaju vrijeme koje je potrebno akterima prijetnji da uspješno realiziraju djela krađe, vandalizma ili terorizma. Što je više prepreka na mjestu, organizacije imaju više vremena da odgovore na fizičke sigurnosne prijetnje i obuzdaju ih. Ako kriminalci nisu jedina prijetnja koju kontrole pristupa mogu minimizirati, prepreke kao što su zidovi i ograde mogu se koristiti za učvršćivanje zgrada protiv ekoloških katastrofa, poput klizišta, poplava, potresa. Ovi rizici izrazito ovise o lokaciji. Organizacije koje usmjeravaju resurse prema takvima mjerama očvršćivanja trebale bi uravnotežiti trošak i koristi od njihove provedbe prije ulaganja. [1]

7.2. Nadzor

Ovo je jedna od najvažnijih komponenti fizičke sigurnosti za prevenciju i oporavak nakon incidenta. Nadzor se u ovom slučaju odnosi na tehnologiju, osoblje resurse koje organizacije koriste za praćenje aktivnosti različitih lokacija i objekata u stvarnom svijetu. Ovi primjeri mogu uključivati patrolne stražare, toplinske senzore i sustave obavijesti. Najčešća vrsta nadzora su televizijske kamere zatvorenog kruga koje bilježe aktivnost kombinacije područja. Prednost ovih kamera je da su jednako vrijedne u bilježenju kriminalnog ponašanja kao u sprječavanju istog. Izvršitelji prijetnji prilikom primjećivanja kamere često su manje skloni provaliti ili vandalizirati zgradu iz straha da će njihov identitet biti snimljen. Slično, ako je određena imovina ili dio opreme ukraden, nadzor može

pružiti vizualne dokaze koji su potrebni za identifikaciju krivaca i njegove taktike. [1]

7.3. Testiranje

Fizička sigurnost je preventivna mjera i alat za odgovor na incidente. Planovi za oporavak od katastrofe, primjerice usredotočenost na kvalitetu nečijih sigurnosnih protokola-koliko dobro tvrtka identificira prijetnju, reagira na nju. Provođenje aktivnog testiranja je jedini način da se osigura da će takve politike oporavka od katastrofa biti učinkovite kada dođe vrijeme. Vatrogasne vježbe nužna su aktivnost za škole i zgrade jer pomažu koordinaciji velikih skupina, kao i njihovom načinu reagiranja. Ovi testovi bi se trebali provoditi redovito kako bi se uvježbalo dodjeljivanje uloga i odgovornosti te smanjila vjerojatnost pogrešaka. [1]

8. MJERE FIZIČKE ZAŠTITE DIGITALNIH PODATAKA

8.1. 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 unutrašnjost organizacije te je time otežano izvođenje napada. Također, ograde mogu štititi i od nekih prirodnih prijetnji poput poplava i sl. 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, primjer nadzorne kamere prikazan na slici 7, koje mogu služiti i za identifikaciju osoba,

- postavljenje alarmnih sustava koji bi se oglašavali u slučaju provale, ili nekih drugih prijetnji (npr. požar). Postizanje adekvatne zaštite okoline definirano je kroz program prevencije kriminala kroz dizajn okoliša, 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. Provodi 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. [6]

Slika 7. Nadzorna kamera [11]

8.2. 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. [6]

8.3. Sigurne sobe

Prostorije u kojima se nalaze računalni sustavi za pohranu i pristup mogu se osigurati od neovlaštenog pristupa. Sobe se mogu izgraditi na načine koji sprječavaju neovlašteni pristup i mogu se opremiti za praćenje korištenja i korisnika. Možda će se zahtijevati da sigurne sobe imaju potpuno zatvorene zidove koji se protežu od poda do stropa, imaju mali broj mogućih ulaza i imaju vrata, prozore, ventilacijske otvore i druge moguće ulaze osigurane rešetkama, mrežom ili drugim metodama. Vrata i zidovi će možda morati zadovoljiti minimalne specifikacije u pogledu materijala, tehnika konstrukcije i debljine kako bi se povećala zaštita od fizičkih napada. Primjerice ojačana vrata i zidovi nude veću zaštitu u odnosu na obične materijale za izgradnju kuća i ureda. Šarke za vrata, pristupne ploče, pregrade, prozori i drugi mogući načini ulaska u prostoriju mogu se ugraditi s unutarnje strane sigurne prostorije kako bi se spriječilo njihovo uklanjanje izvana. Dodatni zahtjevi mogu se proširiti na uređaje za fizičko osiguranje unutar prostorije. Od računala se može zahtijevati da nemaju vanjske mrežne veze ili da uopće nemaju mrežnu vezu. Ova ograničenja se obično koriste samo kada ih nalažu davatelji podataka ili ako ih zakon zahtijeva za dijeljenje podataka. Izgradnja sigurnih prostorija skup je pothvata, jer će malo ureda ispuniti ove specifikacije bez dodatne izgradnje i očvršćivanja. [2]

8.4. Zaštita prostorije

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:

- 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. [6]

8.5. Zaštita opreme

Najvažniji aspekt kod fizičke zaštite digitalnih podataka 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
- smještaj uređaja na osigurana mjesta,
- pohrana prijenosnih medija na sigurna mjesta te
- adekvatno uništavanje starih prijenosnih medija. [6]

8.5.1. Zaštita poslužitelja

Poslužitelji predstavljaju vrlo važan aspekt za poslovanje svake organizacije jer mogu sadržavati vrlo važne podatke, 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, primjer zaštite poslužitelja prikazan na slici 8. Implementacijom smještaja sprječava se 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 medija kako bi se spriječilo namjerno oštećenje sustava ili pokretanje nekih napada. [6]

Slika 8. Zaštita poslužitelja [12]

8.5.2. 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. Sigurnost digitalnih podataka dodatno se može povećati implementacijom zaključavanja USB priključaka, kako bi se spriječilo preuzimanje podataka ili onemogućilo umetanje zlonamjernih programa USB sigurnosni ključ prikazan na slici 9. [6]

Slika 9. USB sigurnosni ključ [13]

8.6. Biometrijska provjera autentičnosti

Biometrija je fizičko biološko obilježje, a ponekad i bihevioralno obilježje jedinstveno za pojedince. Biometrijska autentifikacija je korištenje biometrijskih značajki za provjeru identiteta pojedinačnih korisnika na temelju pohranjenih podataka o ovlaštenim korisnicima. Jedna od najčešćih biometrijskih tehnologija u trenutnoj upotrebi su skeneri otiska prsta za potrošačku elektroniku kao što su prijenosna računala i pametni telefoni. Druge najčešće korištene tehnologije

uključuju prepoznavanje lica, prepoznavanje mrežnice ili šarenice te glasovnu identifikaciju. Biometrija se može koristiti za kontrolu pristupa sigurnim lokacijama, kao i za osiguranje pojedinačnih uređaja, pomažući u sprječavanju neovlaštenog pristupa. Glavne komponente takvog sustava uključuju sam biometrijski senzor koji je povezan s bazom podataka koja sadrži skup provjerenih korisnika, te fizička ili elektronička blokada za određeni sustav, primjerice ulazak u sobu ili prijava na računalo, kojima upravlja biometrijski senzor. Tehnike biometrijske provjere autentičnosti mogu poslužiti i kao primarni oblik identifikacije, kao i slojevite tehnike provjere autentičnosti s dva ili više faktora, kao što je u kombinaciji s lozinkama ili drugim uređajima. Dok neki uređaji dolaze s ugrađenom biometrijskom autentifikacijom, kao što su prethodno spomenuti skeneri, otisak prsta, implementacija dodatne biometrijske provjere autentičnosti zahtjeva značajna sredstva. Konkretno, početni upis biometrijskih podataka korisnika obično zahtjeva fizičku prisutnost pojedinca. [2]

8.7. 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 kao što su stražari, zaštitari ili recepcionari, 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. 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. Zaposlenicima je moguće definirati sigurnosne mjere nošenja posebnih kartica kojima bi se prijavljivali pri ulazu u objekt te pri napuštanju istog. Fizičke

pristupne kartice su elektroničke kartice koje identificiraju nositelja kartice za fizički sustav kontrole pristupa. Pristupni mehanizam za uređaje ili sobe osigurane čitačem kartica provjerava valjanost korisničke kartice u bazi podataka koja ima skup valjanih kartica i nakon toga otvara brave na sustavu ili sobi. Kartice se mogu opremiti magnetnim trakama, crtičnim kodovima, čipovima ili drugim sustavima za povezivanje s čitačem kartica. Fizičke pristupne kartice uglavnom koriste firme organizacije, uključujući sveučilišta i vladine organizacije, a mogu imati prednost korištenja postojeće infrastrukture za podršku stvaranja sigurnih pristupnih soba za istraživače koji primaju administrativne podatke. Za razliku od biometrijske autentifikacije, pristupne kartice se mogu lako izgubiti ili dati drugima pri čemu imaju veći potencijal za zloupotrebu. Stariji sustavi također mogu biti osjetljivi na napade kloniranja u kojima se magnetska traka kopira na neovlaštenu karticu. Zaštita samih pristupnih kartica prvenstveno je pitanje politike i obuke. [2] 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 biometrijska kontrola pristupa. Tu spadaju metode skeniranja otiska prsta, primjer otiska prsta prikazan na slici 10, prepoznavanja lica, šarenice oka ili glasa te skeniranje rasporeda vena na ruci. [6]

Slika 10. Kontrola pristupa autentikacijskom pametnom karticom [14]

8.8. Elektronička fizička 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, biometrijska kontrola i sl.),
- sustave za detekciju upada,
- adekvatnu opremu za zaštitare i
- sustave za opremanje okoline i prostorija (ograde, skenere i sl.). [6]

9. SREDSTVA ZA POSTIZANJE FIZIČKE ZAŠTITE

9.1. 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,

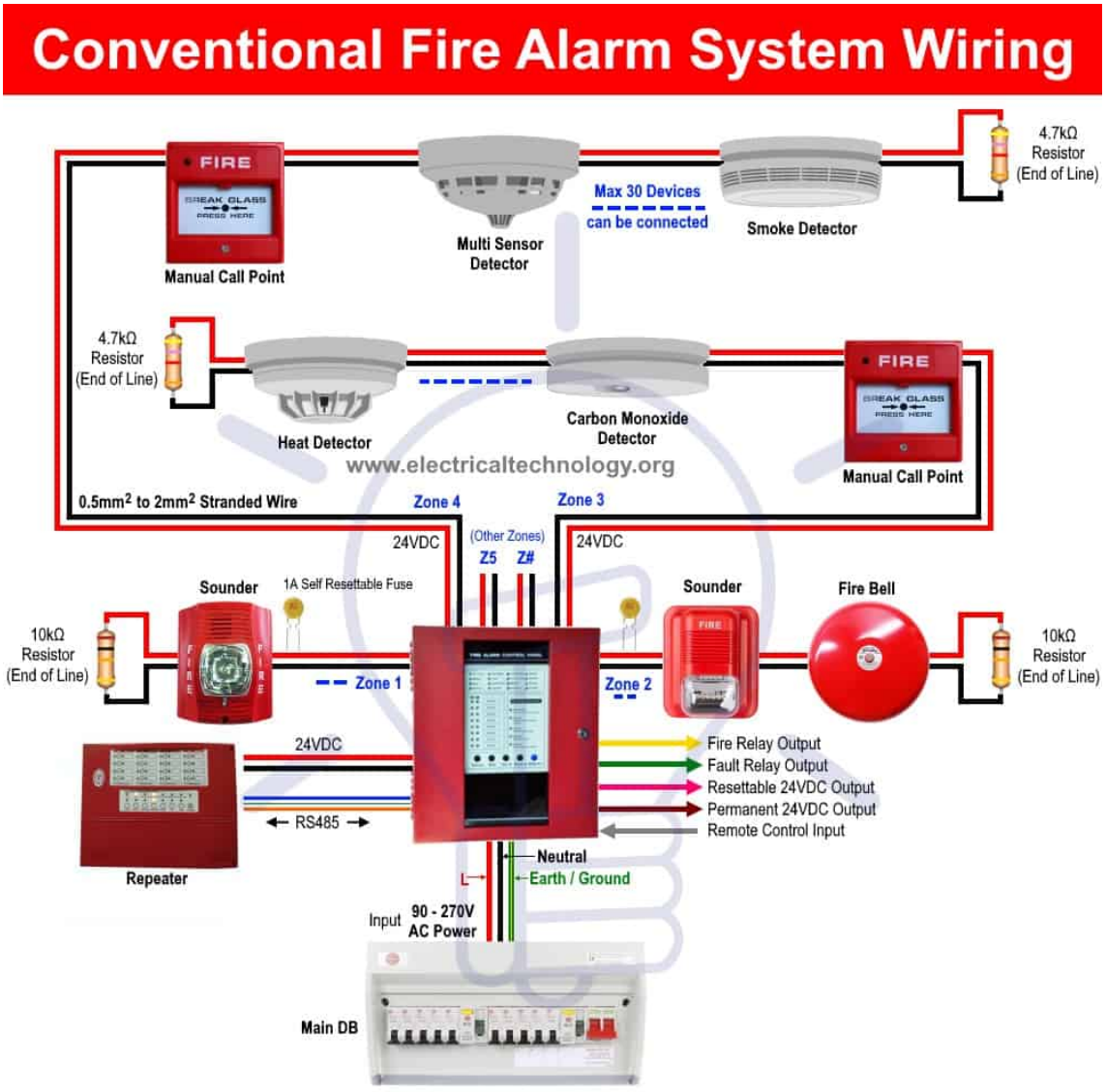
2. vremenske alarme – pokreću aktiviranje alarma u trenutku koji je definirao korisnik, zaposlenik, vlasnik i dr.,

3. distribuirane sustave za upravljanje proizvodnjom, DCS *(eng. distributed control manufacturing system)* koji obavještavaju osoblje o važnim događajima, a obično se koriste u kemijskim i nuklearnim laboratorijima.

4. alarme u operativnim sustavima i sustavima održavanja O&M (eng. *operation and maintenance*) koji služe za slanje obavijesti o lošem radnom stanju sustava koji se nadzire,

5. alarme za sigurnost - uključuju alarme za dojavu prirodnih nepogoda kao što su tornada, požari prikazano na slici 11, plinovi 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 digitalnih podataka, a mogu se koristiti na svim ulazima u objekt. Obično funkcioniraju tako da detektiraju otvaranje vrata ili prozora putem pasivnog infracrvenog detektora PIR *(eng. passive infrared)*. Signali sa senzora prenose se žično ili bežično do jedne ili više kontrolnih jedinca. Razlikuju se po namjeni, mogu biti kućni, industrijski i sl. te po mjestu postavljanja, unutrašnjost objekta ili izvan objekta. 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. [6]



Slika 11. Konvencionalni alarmni sustav za dojavu požara [15]

9.2. 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. [6]

9.3. 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 umanjivanjem opasnosti od ljudskih prijetnji, provođenjem kontrole pristupa te umanjivanjem štete od nekih nezgoda poput požara. [6]

9.4. Nadzorne kamere

U svrhu fizičke zaštite operacijskog sustava najčešće se koriste nadzorne kamere zatvorenog kruga, 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 primjerice zbog radijacije. Napredniji oblici ovih kamera, digitalni video snimač, 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 internet protokolne kamere, IP *(eng. Internet protocol)* kamere koje omogućuju stalni pregled stanja preko bilo koje veze na Internet, primjer Internet protokolne kamere na slici 12. 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. [6]

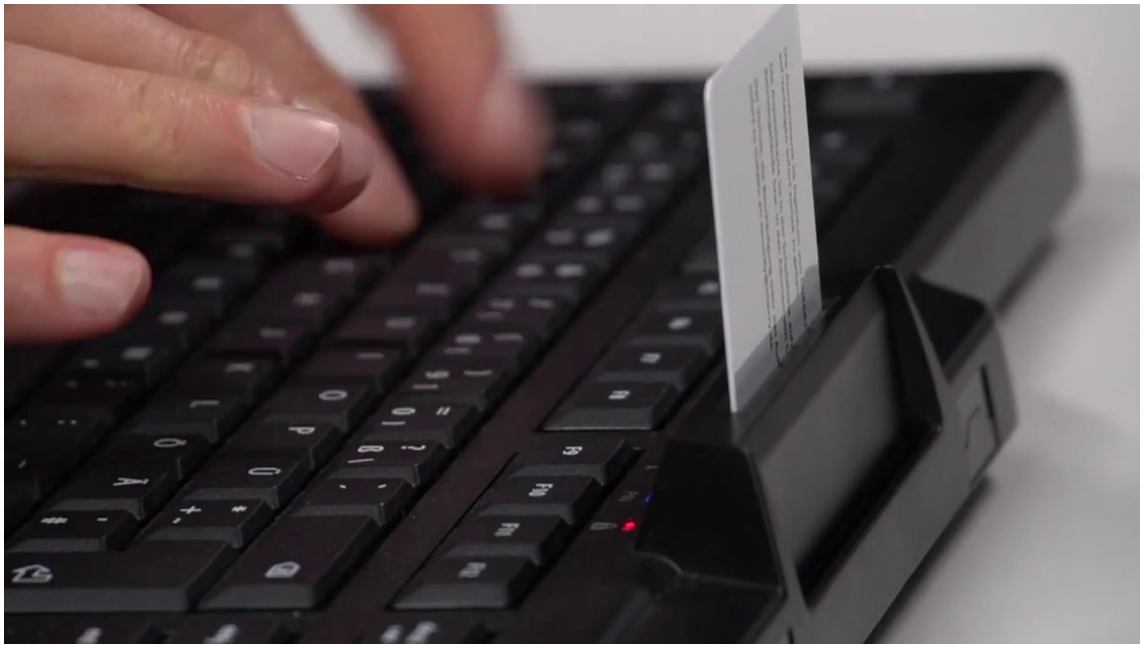
Slika 12. IP nadzorna kamera [16]

9.5. 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, primjer kontrole pristupa računalu s pametnom karticom prikazano na slici 13.



Slika 13. Kontrola pristupa s pametnim karticama [17]

Osim pametnih kartica razvijeni su uređaji koji obavljaju kontrolu pristupa identificiranjem osoba preko određenih bioloških karakteristika. Riječ je o

metodama biometrije 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 na primjer 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., primjer kontrole pristupa preko biometrije prikazan na slici 14.

2. Ponašajne – odnose se na ponašanje osoba, a uključuju ritam, hod ili glas. Uređaji za kontrolu pristupa zasnovani na biometriji uključuju provjeru jedne ili više fizioloških i ponašajnih osobina. [6]

Slika 14. Kontrola pristupa preko biometrije [18]

9.6. Sustavi za zaključavanje prostorija

Lokoti su mehanički ili elektronički uređaji koji se otvaraju fizičkim objektom poput ključa, 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, primjer mehaničkog lokota prikazan na slici 15, imaju pomične dijelove kojima se rukuje bez električnog pogona. Za razliku od njih, elektronički lokoti, primjer elektroničkog lokota prikazan na slici 16, sadrže skenere koji služe za očitavanje kodova te komponente za provjeru identiteta. Postoje brojne inačice spomenutih vrsta lokota.

Slika 15. Mehanički lokot [20]

Slika 16. Električni lokot [19]

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. [6]

9.7. Uređaji za zaključavanje opreme

Fizička sigurnost može se postići primjenom uređaja za zaključavanje opreme, primjer zaštitne sajle za zaključavanje prikazano na slici 17. Razvijeni su razni načini za zaključavanje uređaja, a jedan od njih je korištenje sustava koji omogućuju fizičko zaključavanje kabela. Sustav „*Kensington Security Slot*“, 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 konektor za video izlaz računala ili priključak za pisač te imaju posebne vijke za osiguravanje na mjestu. Također, postoje potpuno elektronička rješenja koja sadrže i alarmne sustave. 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.

Slika 17. Zaštitna sajla za zaključavanje [21]

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. [6]

9.8. 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. [6]

10. EFIKASNOST FIZIČKIH METODA ZAŠTITE DIGITALNIH PODATAKA

Analizirajući fizičke metode od jednostavnih široko primjenjivih metoda zaštite, do sofisticiranih arhitektonskih i fortifikacijskih metoda dolazi se do informacije kako svaka od tih metoda jedna bez druge nije potpuna, odnosno ne pruža visoki stupanj zaštite. Uz jednostavne fizičke metode zaštite do sofisticiranih arhitektonskih i fortifikacijskih metoda bitno je ukazati na sigurnosnu politiku unutar kolektiva, jer često se događa da je nepažnja radnika dovela do zlouporabe podataka, krađe podataka kao i krađe dostupnih uređaja s osjetljivim podacima. Ukoliko postoje dostupna zaštitna sredstva, kao što je to zaštitna sajla za zaključavanje prijenosnog računala, radnika je bitno uputiti u važnost korištenja iste, jer u slučaju probijanja ključanice, primjerice na vratima ureda prijenosno računalo je i dalje zaštićeno od lakog otuđivanja. Kamere često ne pružaju veliku pomoć u zaustavljanju krađe i imaju ograničenu upotrebu u identifikaciji prijestupnika. Arhitektonske metode zaštite su bitna stavka u fizičkoj zaštiti jer onemogućuju jednostavan pristup i ograničavaju osobu u pokušaju upada kako u samo lokaciju tako i do podataka ukoliko se oni nalaze u sigurnosnim sobama. One su izgrađene planski kako bi maksimalno mogle zaštiti podatke. Ukoliko uz njih imamo i fortifikacijsku zaštitu, zaključit ćemo kako se sa svim tim metodama u kombinaciji postiže vro visoki stupanj zaštite i teško je doći do mogućnosti krađe. Naravno ako se uz sve navedeno uzima u obzir da su zaposlenici educirani o sigurnosti što povećava otpornost zaposlenika prema socijalnom inženjeringu i povećava učinkovitost ostalih sigurnosnih mehanizama.

11. ZAKLJUČAK

Zaštita digitalnih podataka u poslovanju još uvijek nije dovoljno ozbiljno shvaćena. Ulaganje u znanje je skupo, ali niska razina znanja zaposlenika predstavlja ozbiljan rizik za imovinu organizacije. Zbog toga je važno u planiranju i razvoju sustava sigurnosti voditi brigu o educiranosti zaposlenika te odgovornostima i dužnostima svakog pojedinca u organizaciji. Također, značajan rizik za sigurnost digitalnih podataka je i neorganizirano implementiranje sigurnosnih kontrola zbog čega je svaku sigurnosnu kontrolu ugrađenu u sustav nužno dokumentirati.

Uloga sigurnosne politike u području informacijske sigurnosti je određivanje prihvatljivog i neprihvatljivog načina ponašanja kako bi zaštitili podatke. Na temelju pravila definiranih u dokumentu Sigurnosna politika organizacije osiguravaju se tri temeljna svojstva podataka: povjerljivost (tajnost), integritet i dostupnost što je za poslovanje organizacije od velike važnosti. Iako se organizacije odlučuju zaštititi svoju digitalnu imovinu raznim dostupnim alatima, mnoge organizacije još nisu dovoljno svjesne ozbiljnosti od krađe i gubitaka podataka. Krajnji troškovi nastali zbog krađe podataka značajno su veći od troškova ulaganja u sustave za zaštitu digitalnih podataka.

Fizička zaštita predstavlja važan aspekt sigurnosti organizacije. Podrazumijeva uklanjanje ili smanjivanje prijetnji koje dolaze od prirodnih nepogoda i ljudi te nekih nepredviđenih događaja kao što su požari, eksplozije, ratovi i pandemije. Kako bi se umanjila šteta uzrokovana pojavom nekih prijetnji, uvode se mjere za fizičku zaštitu digitalnih podataka. One uključuju zaštitu okoline i unutrašnjost 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 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 digitalnih podataka ako se primjenjuje na adekvatan način, a te komponente su: ostvarivanje zahtjeva, analiza stanja,

planiranje potrebnih mjera te uključivanje i educiranje zaposlenika u važnost provođenja svih potrebnih radnji koje bi spriječile narušavanje fizičke sigurnosti.

Otpornost sustava na izvanredne događaje kao što su rat ili pandemija očituje se kroz to koliko je ranjiv u trenutku kad nastupi neki od ovih navedenih događaja. Otpornost sustava zaštite digitalnih podataka postiže se adekvatnim i pravovremenim planiranjem, izvedbom, edukacijom zaposlenika i brzim intervencijama. Kako je u mnogim poslovnim područjima bitno da su podaci dostupni čak i u situacijama gdje je došlo do zastoja zbog rata ili nekih drugih prirodnih katastrofa vrlo je bitno da su provedene sve mjere zaštite i educiranja zaposlenika. Primjerice, neki data centar koji se nalazi trenutno u Ukrajini potrebno je u što kraćem roku preseliti sa svim podacima u sigurno područje. Pretpostavka održivosti kontinuiteta poslovanja i procesa potrebnih za oporavak u slučaju raspada je dobra preventiva i dobro posložen sigurnosni sustav koji je redovno održavan i dograđivan. Nemoguće je predvidjeti sve tehnološke i organizacijske slabosti sustava, zato su planiranje i prevencija temelj. Neophodno je da se napravi procjena rizika svih segmenata poslovanja. Da bi sve radilo kako treba, mora se poraditi na svim segmentima razvoja svjesnosti o mogućim problemima i riziku te prema njima planirati oporavak u slučaju incidenta. Samo višeslojno sigurnosno rješenje daje mir i stabilnost poslovnom sustavu.

12. LITERATURA

[1] Cobb M.: Physical security, Techtarget, https://www.techtarget.com/searchsecurity/definition/physical-security, pristupljeno 1.travnja.2022.

[2] Cole S., Dhaliwal I., Sautmann A., Vilhuber L.: Physically Protecting Sensitive Data, Handbook on using Administrative Data for Research and evidnece-based Policy, https://admindatahandbook.mit.edu/book/v1.0-rc5/security.html, pristupljeno 1.travnja.2022.

[3] CARNet CERT, Životni vijek podataka, https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2008-05-227.pdf, pristupljeno 15.travnja.2022.

[4] IBM, Data Storage Defined, https://www.ibm.com/topics/data-storage, pristupljeno 25.travnja.2022.

[5] Wu J., Ping L., Ge X., Wang Y., Fu J.: Cloud storage as as the Infrastructure of Cloud Computing, https://ieeexplore.ieee.org/abstract/document/5565955, pristupljeno 12.svibnja.2022.

[6] CARNet CERT, Fizička zaštita informacijskih sustava, https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-06-304.pdf pristupljeno 12.svibnja.2022.

[7] CARNet, CERT, Obnavljanje izgubljenih podataka, https://www.cert.hr/wp-content/uploads/2009/04/CCERT-PUBDOC-2009-04-261.pdf, pristupljeno 20.svibnja.2022.

[8] Dimkov T., Pieters W., Hartel P.: Effectiveness of Physical, Social and Digital Mechanisms against Laptop Theft in Organizations, pristupljeno https://www.researchgate.net/publication/47734709_Effectiveness_of_Physical_Social_and_Digital_Mechanisms_against_Laptop_Theft_in_Open_Organizations 15.lipnja.2022.

[9] DATA SECTOR, Oštećenje tvrdog diska pod utjecajem visoke temperature, https://www.datasector.hr/hr/blog/utjecaj-temperature-na-hard-disk/26, pristupljeno 20.lipnja.2022.

[10] RH MUP Ravnateljstvo Civilne zaštite: Smanjenje rizika od katastrofa, https://civilna-zastita.gov.hr/print.aspx?id=160&url=print, pristupljeno 20.lipnja.2022.

[10] RH MUP Ravnateljstvo Civilne zaštite: Smanjenje rizika od katastrofa, https://civilna-z,astita.gov.hr/print.aspx?id=160&url=print, pristupljeno 20.lipnja.2022.

[11] M.Gračanin: Sigurnost nadzornih kamera, https://zastita.info/hr/casopis/clanak/sigurnost-nadzornih-kamera,15592.html pristupljeno 20.lipnja.2022.

[12] Williams C.: What yours Cage Says About Your Company, https://datacenterfrontier.com/what-your-data-center-cages-says/ pristupljeno 20.lipnja.2022.

[13] Humphries S: What is a USB Security Key, and should You Use One?, https://www.reviewgeek.com/63448/what-is-a-usb-security-key-and-should-you-use-one/, pristupljeno 20.lipnja.2022.

[14] bttechseo client: Smart card door acces or Biometrics: Choose the best for your workspace, https://efficientsystem.home.blog/2021/05/11/smart-card-door-access-or-biometrics-choose-the-best-for-your-workspace/, pristupljeno 21.lipnja.2022.

[15] Electrical Tecnology: Types of Fire Alarm Systems and Their Wiring Diagrams, https://www.electricaltechnology.org/2019/12/fire-alarm-system-wiring.html, pristupljeno 21.lipnja.2022.

[16] ROBAXO, ROBAXO IP kamera RC204Z, Wifi, 1080p, https://www.robaxo.com/izdelek/robaxo-rc360z-ip-kamera-1080p-360-smartcam/, pristupljeno 21.lipnja.2022.

[17] 365online, Wireless Keyboard with Smart Card reader, https://www.hjdgvdfds.tk/products.aspx?cname=wireless+keyboard+with+smart+card+reader&cid=31, pristupljeno 21.lipnja.2022.

[18] Belobrajdić K., Je li GDPR „ubio“ biometriju, https://www.spica.hr/blog/je-li-gdpr-ubio-biometriju, pristupljeno 22.lipnja.2022.

[19] Ralph: 5 Best Shed Locks: Finding The Best Shed Door Locks For Your Structure https://unitedlocksmith.net/blog/5-best-shed-locks-finding-the-best-shed-door-locks-for-your-structure, pristupljeno 22.lipnja.2022.

[20] CODELOCKS https://www.codelocks.com/, pristupljeno 22.lipnja.2022.

[21] eet, Gearlab Security lock with keys for Nano security slot https://www.eetgroup.com/en-eu/glb220103-gearlab-security-lock-with-keys-for-kensington-nano-security-slot-wid-w125988757, pristupljeno 22.lipnja.2022.

[22] Biswas R., A Study of Data Storage Security Issues in Cloud Computing, https://tinyurl.com/bdz93zny, pristupljeno 12.srpnja.2022.

[23] Narodne Novine, Zakon o informacijskoj sigurnosti (NN 79/2007), https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html, pristupljeno 13.srpnja.2022.

[24] RH Ured Vijeća za nacionalnu sigurnost, Ako je informacijski sustav usklađen s HRN ISO/IEC 27001/27002 je li usklađen i s Hrvatskim propisima informacijske sigurnosti o informacijskim sigurnostima?, https://www.uvns.hr/hr/ako-je-informacijski-sustav-uskladjen-s-hrn-iso-iec-27001-27002-je-li-uskladjen-i-s-hrvatskim-propisima-informacijske-sigurnosti-o-informacijskim-sustavima, pristupljeno 14.srpnja.2022.

13. PRILOZI

13.1. Popis Slika