Osiguravanje tjelesne, tehničke i informacijske sigurnosti hotela

Rušidi, Leon

SVEUČILIŠTE U RIJECI

Fakultet za menadžment u turizmu i ugostiteljstvu

Sveučilišni prijediplomski studij

LEON RUŠIDI

Osiguravanje tjelesne, tehničke i informacijske sigurnosti hotela

Ensuring hotel's physical, technical and information security

Završni rad

Zabok, 2023.

SVEUČILIŠTE U RIJECI

Fakultet za menadžment u turizmu i ugostiteljstvu

Sveučilišni prijediplomski studij

Poslovna ekonomija u turizmu i ugostiteljstvu

Studijski smjer: Menadžment u turizmu

Osiguravanje tjelesne, tehničke i informacijske sigurnosti hotela

Ensuring hotel's physical, technical and Information security

Završni rad

Kolegij:	**Sigurnost informacijskih sustava**	Student:	**Leon Rušidi**
Mentor:	Prof. dr. sc. **Ljubica Pilepić Stifanich**	Matični broj:	**006622019**

Zabok, rujan 2023.

SVEUČILIŠTE U RIJECI UNIVERSITY OF RIJEKA
FAKULTET ZA MENADŽMENT U TURIZMU I UGOSTITELJSTVU
FACULTY OF TOURISM AND HOSPITALITY MANAGEMENT
OPATIJA, HRVATSKA CROATIA

IZJAVA O AUTORSTVU RADA I

O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Leon Rušidi	**006622019**
(ime i prezime studenta)	(matični broj studenta)

Osiguravanje tjelesne, tehničke i informacijske sigurnosti hotela

(naslov rada)

Izjavljujem da sam ovaj rad samostalno izradila/o, te da su svi dijelovi rada, nalazi ili ideje koje su u radu citirane ili se temelje na drugim izvorima, bilo da su u pitanju knjige, znanstveni ili stručni članci, Internet stranice, zakoni i sl. u radu jasno označeni kao takvi, te navedeni u popisu literature.

Izjavljujem da kao student–autor završnog rada, dozvoljavam Fakultetu za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci da ga trajno javno objavi i besplatno učini dostupnim javnosti u cjelovitom tekstu u mrežnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci.

U svrhu podržavanja otvorenog pristupa završnim radovima trajno objavljenim u javno dostupnom digitalnom repozitoriju Fakulteta za menadžment u turizmu i ugostiteljstvu Sveučilišta u Rijeci, ovom izjavom dajem neisključivo imovinsko pravo iskorištavanja bez sadržajnog, vremenskog i prostornog mog završnog rada kao autorskog djela pod uvjetima *Creative Commons* licencije CC BY Imenovanje, prema opisu dostupnom na http://creativecommons.org/liceses/.

U Opatiji, rujan 2023.

Leon Rušidi

Sadržaj

Sažetak

Ovaj završni rad opisuje kakve sve vrste zaštite i sigurnosti stoje na raspolaganju te kako ih implementirati i nadograditi u hotelijerskoj industriji koja je jedan od krucijalnih elemenata smještaja u sklopu turističkog sektora. Vrsta zaštite i osiguranja koji su objašnjeni daju se naslutiti iz naslova rada, stoga fokus je primarno na tehničku, tjelesnu i informacijsku sigurnost. Opisani su potencijalni negativni čimbenici koji su mogući tokom svakodnevnog poslovanja hotelskog poduzeća a tiču se negativnih efekata do koji može doći zloćudnim agendama kriminalnih organizacija ili individua u sklopu kompromitiranja hotelskih poduzeća ili gosta. Nerijetko sam problem leži i u samom hotelu koji iako u nekim situacijama možda i koristi najmodernije tehnologije namijenjene poboljšavanju svakodnevnih operativnih zadaća kao i sigurnosne sustave i metode koji ih komplementiraju, ujedno i ne posjeduje dovoljno osviješteno te na adekvatan način educirano osoblje. Rezultat toga mogu biti greške samih zaposlenika, te je ta činjenica jedna od primarnih izazova modernih poduzeća koja da bi bila ukorak s vremenom te ostala konkurentna jednostavno moraju ulagati u sve kompleksniju i višeslojnu zaštitu. Nadalje, svakim danom negativni učinci globalizacije koliko god je ona nama donijela dobroga u globalu, postaju evidentniji razvitkom sve kreativnijih i sofisticiranijih načina potencijalne ugroze po integritet poduzeća, poslovnih partnera te gostiju, kao i krađe podataka u svrhu ostvarivanja kriminalnih ciljeva.

Ključne riječi: vrste zaštite; kompromitiranje hotelskog poduzeća i gosta; negativni učinci globalizacije; kreativni načini ugroze.

1 Uvod

Brzina razvoja globalizacije kao fenomena novijeg doba, napredak u sferi tehnološkog razvoja koji sa sobom vuče sve lakšu umreženost i diverzifikaciju komunikacije koji do prije manje od 100 godina nisu bili ni zamislivi stvaraju plodno tlo za razvitak raznih oblika potencijalnih ugroza.

Kao takvi jedni su od najbitnijih razloga zašto dolazi do sve većeg osjećaja nesigurnosti kako individua tako i samih hotelijerskih poduzeća.

1.1 Predmet, ciljevi i metode istraživanja

S obzirom na prirodu i relativnu nasumičnost događaja koji negativno utječu na stabilnost i sigurnost, onaj tko može osigurati visoku razinu iste, posjeduje jednu od danas najbitnijih konkurentskih prednosti te stvara si mogućnost za profit. To se u današnje vrijeme može postići integracijom raznih vrsta zaštite i sigurnosnih sustava ne bi li se postigao što slojevitiji stup obrane od potencijalnih napada.

Neki hotelijeri su prepoznali potencijal u ulaganje u sigurnosne mjere te pomno prate trendove u korporativnoj sigurnosti ne bi li išli u korak sa najsuvremenijom tehnologijom i podigli konkurentnost. Iz tog razloga predmet ovog rada je opis tih sigurnosnih sustava koji su dostupni sa fokusom na hotelijersku industriju te kako ih implementirati ne bi li se osigurala što veća razina sigurnosti. Naravno sama implementacija sve kompleksnijih sigurnosnih sustava je danas nedovoljna. Neophodno je imati i potrebiti tehnički 'know-how' te vještinu kvalitete prenošenja tog iskustvenog znanja na druge, u ovom slučaju zaposlenike, jer nerijetko je slučaj da upravo osoblje slučajno prouzroči problem radi nedovoljne educiranosti o procedurama i tehnologiji koje im stoji na raspolaganju.

Potencijalna ugroza ne dolazi samo preko vanjskih čimbenika, nego kako je navedeno, problemi i izazovi postoje i unutar samog poduzeća. Stoga je cilj ovoga rada identificiranje najčešćih vrsti prijetnji koje vrebaju u današnje vrijeme, te kojim modernim tehnološkim rješenjima i metodama se zaštiti od njih.

Znanstvena metoda koja korištena u ovom teorijskom radu je primarno deskriptivna, a kao izvori informacija korišteni su relevantni domaći i strani članci i istraživanja vezanih uz

materiju koja se ovdje obrađuje, stručna akademska literatura vezana uz sektor zaštite te kredibilne web stranice koje obrađuju navedenu tematiku.

1.2 Struktura rada

Što se same strukture ovog rada tiče, on se sastoji od osam međusobno povezanih poglavlja koji su obrađeni već spomenutom deskriptivnom znanstvenom metodom.

U ovom uvodnom dijelu rada objašnjen je predmet rada, ukratko je opisan cilj i svrha rada, korištene metode, te izvori iz kojih su se crpile informacije.

U drugom poglavlju govori se o samom pojmu sigurnosti, sa kakvim se izazovima današnje društvo i poduzeća susreću te se po prvi puta spominju najbitniji pojmovi vezani za zaštitu od ugroza.

Treće poglavlje govori o tjelesnoj zaštiti, koje su zadaće i ovlasti zaštitara i interventnog zaštitara, redarskoj službi te kako i kada se taj oblik zaštite koristi u hotelskoj industriji.

U četvrtom poglavlju ukratko se daje osvrt na mehaničku zaštitu kao najosnovniji oblik protuprovalne zaštite na koju se nadovezuje onaj sofisticiraniji oblik, tehnička zaštita.

Tehnička zaštita je naslov petog poglavlja te se podrobnije opisuje kompleksnija tematika same tehničke zaštite te izrada, projektiranje i naposljetku njena implementacija.

U šestom poglavlju se pojavljuje termin informacijske zaštite i sigurnosti, koji su najčešći oblici napada u današnje vrijeme te kako ih prevenirati i kojim metodama.

Sedmo poglavlje opisuje pojam kriznih situacija, značenje propisanih postupaka i procedura temeljenih na prethodnim iskustvima kao i praktični primjer postupka po pitanju potencijalne ugroze zaposlenika.

Rad završava zaključkom u kojem su izvučene najbitnije činjenice, izazovi, te rješenja iznesena u cjelokupnom radu te što budućnost potencijalno nosi.

2 Sigurnost

„Sigurnost je sustavno uspostavljena zaštita koja ima cilj zaštiti ljude i njihove aktivnosti, informacije, uređaje i opremu od namjernog i/ili slučajnog neovlaštenog djelovanja koje ima cilj nanošenja štete pojedincima i tvrtkama te njihovom ugledu." – Nick van der Bijl.[1]

Da bi se čovjek osjećao sigurnim u danas podosta kaotičnom okruženju, potrebno je uvesti određena pravila i zakone koji će se primjenjivati i poštivati, zato je recimo za odabir potencijalne turističke destinacije od velike važnosti prvotno se informirati u kakvu sredinu se dolazi, kakva je razina sigurnosti u samoj destinaciji ne bi li se što više minimizirao rizik samog dolaska i boravka u nepoznatoj sredini. Nakon što smo se uvjerili da je razina rizika prihvatljiva, treba se uvjeriti i o kakvom je smještaju riječ u kojem bi potencijalno boravili, koja je razina sigurnosti u hotelu ako ćemo ga izabrati za svoj oblik smještaja, što se to tamo od sigurnosnog sustava pruža ne bi li nama boravak tamo bio što ugodniji i rasterećeniji.

Hotelski sigurnosni sustavi obuhvaćaju najčešće kontrolu pristupa i prisutnosti u hotelskim smještajnim jedinicama, alarmne sustave u kupaonicama, sobama i zajedničkim hotelskim prostorima. To znači da je za instalaciju i implementaciju sustava sigurnosti nužno imati stručne ljude, koji će u određenom organizacijskom obliku operativno i pomoću suvremenih tehničkih dostignuća zaštite obavljati te aktivnosti.

Različitim tehničko-tehnološkim rješenjima sigurnosnih hotelskih sustava pospješuje se provedba sigurnosnih mjera i povećava razina sigurnosti i zaštite u hotelskim objektima. Sve veći jaz između bogatih i razvijenih sa jedne strane i siromašnih i slabije razvijenih s druge strane, stvara prikladan ambijent za razvoj raznih oblika ekstremizma bilo gospodarskog, religijskog, političkog ili etničkog karaktera. Međutim, pokazalo se da najgori oblik ugrožavanja poput terorističkog napada u gospodarski razvijenim i uređenijim zemljama Europe i svijeta je teško predvidiv i gotovo da je nemoguće u potpunosti otkloniti rizik od istog te posljedice terorističkih napada svaki puta na nova iskušenja stavljaju sigurnosne službe te primijenjene zaštitne mjere i sustave.

Nadalje, informatičko doba u kojem živimo stvara prikladan ambijent za razvoj raznoraznih vrsta kriminalnih cyber napada u vidu djelovanja tajnih kriminalnih hakerskih organizacija ili hakera individua koristeći svoje računalne i hakerske vještine razotkrivanjem i korištenjem

[1] Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.

klasificiranih i tajnih podataka, zlouporabe identiteta i dr., a sve s ciljem ostvarivanja svojih agenda. Pitanje sigurnosti svakim danom postaje sve bitnije, kako općenitu u životu tako i u korporativnom svijetu.

Hrvatska kao zemlja, prije svega još uvijek okrenuta primarno ljetnom turizmu, mora moći pružiti adekvatnu razinu osjećaja sigurnosti svojim gostima, stoga je Pravilnikom o razvrstavanju, kategorizaciji i posebnim standardima ugostiteljskih objekata propisan minimum zaštite od požara u vidu vatrodojavnih i protupožarnih sustava. Sustav od dojave požara također služi kao temelj za ostale safety sustave kao npr.; SOS sustavi, evakuacijska i panik rasvjeta, gašenje, odimljavanje, detekcija plina, detekcija ugljičnog monoksida.

Prema podacima Hrvatske turističke zajednice, na prostoru Republike Hrvatske je ukupno 793 raznih turističkih objekata. Ako uzmemo u obzir podatak da je od ova 793 turistička objekta samo 201 objekt u kategoriji s 4 ili 5 zvjezdica (konkretnije, samo 23 hotela su u kategoriji s 5 zvjezdica) i imaju obvezu imati stabilan sustav za dojavu požara, što je samo jedan tehnički sustav zaštite, tada ukupna ocjena sigurnosti (sagledavajući samo tehničke sustave zaštite) svakako nije zadovoljavajuća. Definira li se "sigurnost" kao skup mjera i aktivnosti kojima se štiti prostor, objekti u tom prostoru, osobe, stvari i imovina te podaci (informacije), tada se moramo složiti da je pokrivenost ove problematike zakonskom, odnosno podzakonskom regulativom apsolutno nedovoljna[2].

Problem je u tome što je još uvijek prisutna niska razina svijesti o korporativnoj sigurnosti što umnogome pridonosi potreba za veća ulaganja i stvaranja dodatnog troška hotelskim poduzećima te se nerijetko vlasnici pitaju da li je sve to toliko neophodno, te u mnogim slučajevima implementiraju samo one minimalne sigurnosne mjere koje su zakonom propisane, u ovom slučaju je riječ primarno o vatrodojavnim i protupožarnim sustavima. Stoga je neophodno da hotelijeri uvide važnost u ulaganju u sigurnosne sustave i da se ne drže samo onog zakonom propisanog.

Upravo taj dio je ključan jer predstavlja metode i tehnologiju koja može poslužiti eliminiranju barem onih negativnih faktora koji su u dosegu naše moći u vidu potencijalnih šteta koja mogu nastati negativnim djelovanjem trećih subjekata sa zloćudnim nakanama te nam tako uliti povjerenje za odabir nekog konkretnog smještaja ili destinacije. Taj osjećaj sigurnosti je od velike važnosti tim više što doba u kojem živimo je sklono iznenadnim ponekad

[2] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4, str. 215.

i drastičnim promjenama prouzročenim silama na koje ne možemo previše utjecati kao na primjer prirodne nedaće, teroristički napadi ili državni udari koji u tren oka poremete ravnotežu na ovaj ili onaj način.

Da bi se navedeni osjećaj sigurnosti povećao, te bio efikasan i učinkovit potrebno je integrirati, uskladiti i organizirati sljedeće sigurnosne elemente[3]:

- Tehničke sustave sigurnosti,
- Tjelesnu zaštitu,
- Informacijsku zaštitu,
- Donošenje procedura postupanja u kriznim situacijama i njihov nadzor poštivanja,
- Uvježbavanje radnji i postupaka po donesenim procedurama te konstantna edukacija zaposlenih.

Što se tiče samih mjera zaštite, kako generalno, tako i u hotelijerstvu, teži se ispunjavanju sljedećih pet osnovnih funkcija[4]:

1. Odvraćanje potencijalnih napadača je važna mjera koja se postiže obznanom postojanja kvalitetnih mjera zaštite koje obuhvaćaju sve primijenjene mjere i ponašanja po procedurama vezane uz zaštitu objekta,
2. Usporavanje neovlaštenog pokušaja prodora ili prodora u štićeno područje postiže se prisustvom mehaničkih zapreka poput sefova, kasa, zidova, vrata, prozora, rešetki, ograda i ostalo,
3. Detekcija neovlaštenog pokušaja prodora ili prodora se ostvaruje upotrebom tehničkih sredstava detekcije prisustva neovlaštenih osoba,
4. Uzbunjivanje se postiže sustavom za prijenos alarmnih stanja i sustavom za nadzor kojima se prenosi, identificira i objavljuje alarmna situacija na određenom mjestu štićenog objekta.

Odgovor na alarmnu situaciju obavlja se tjelesnom zaštitom – intervencijom interventnog zaštitarskog tima, što nas dovodi do tjelesne zaštite.

[3] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4.
[4] Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.

3 Tjelesna zaštita

Tjelesna zaštita definira se kao sektor koji pruža temeljnu uslugu koju zaštitarska firma pruža, produkt je osposobljenosti, edukacije i kontinuiranog usavršavanja djelatnika koji mora proći potrebnu obuku i steći licencu za obavljanje zaštitarskog posla. Distinkcije radi, ista se treba izvršiti između dva krucijalna pojma o kojima će biti riječ u ovoj sekciji rada a to su čuvar i zaštitar.

Naoko, dva identična pojma (po nekim osnovnim elementima to i jesu), no ipak se razlikuju u par bitnih točaka. Naime, ovlasti osoba kojima je izdano dopuštenje za obavljanje poslova tjelesne zaštite su[5]:

1. Provjera identiteta osoba,
2. Davanje upozorenja i zapovjedi,
3. Privremeno ograničenje slobode kretanja,
4. Pregled osoba, predmeta i prometnih sredstava,
5. Osiguranje mjesta događaja,
6. Uporaba čuvarskog psa,
7. Uporaba tjelesne snage,
8. Uporaba vatrenog oružja.

Međutim, bitna razlika je u činjenici da čuvari ne mogu koristiti ovlasti iz točaka 3.,6.,7. i 8. Nadalje, čuvari i zaštitari navedene ovlasti smiju primijeniti izričito samo unutar objekata i prostora unutar štićenog objekta i oko štićene osobe do prostorne granice za čije su čuvanje zaduženi, dužni su postupiti po zapovjedi policijskog službenika te primjena ovlasti ne smije izazvati značajnije veće štetne posljedice od onih koje bi nastupile da ih nisu primijenili. U iznimnim situacijama, kada zaštitar obavlja posao neposredne tjelesne zaštite (tjelohranitelj, bodyguard), može primijeniti svoje ovlasti i izvan navedenih granica u sklopu otklanjanja izravnih potencijalnih protupravnih napada prema sebi ili prema osobi za koju je zadužen da štiti.

Što se tiče samog pružanja tjelesne zaštite, ako za to postoje preduvjeti, te ako korisnik usluge zatraži da bi bilo potrebe za neposrednom tjelesnom nazočnošću zaposlenika pružatelja usluge, na štićeni prostor se stavlja određeni broj djelatnika pružatelja usluge ili u slučaju da u

[5] Zakon o privatnoj zaštiti (NN 68/2003)

tom trenutku ne raspolaže sa dovoljno potrebitih ljudi za posao, taj broj ljudi se može outsourceati (no to su logistički problemi te zaštitarske firme, a nerijetko i realan problem pogotovo manjih firmi u sektoru private zaštite koji teže dolaze do potrebne kvalificirane radne snage).

Osnovni poslovi u domeni tjelesne zaštite su[6]:

- Nadzor osoba i robe u štićenom objektu (zaštitari),
- Nadzor kretanja vozila (interventne ekipe, pratitelji vrijednosti),
- Nadzor osoba i robe na ulazu u štićeni objekt (čuvari),
- Ophodnja i nadzor štićenog objekta, te osiguravanje javnih skupova (redarska služba-redari),
- Osiguravanje osoba (bodyguard),
- Vršenje intervencija na zahtjev korisnika ili po alarmnoj dojavi (interventni zaštitar).

Nadzor osoba i robe na ulazu i u štićenom prostoru u vidu zaštite objekta vrše čuvari i zaštitari, ovlašteni, licencirani, moderno opremljeni a po potrebi i naoružani djelatnici (zaštitari) zaštitarske firme koji pružaju zaštitu osoba i imovine svojom osobnom nazočnošću te su u svakom trenutku spremni obavljati i druge poslove kao prijem stranaka, rada na

Što se tiče gotovo nebitnog po hotelski objekt, ali ipak sam po sebi važan aspekt tjelesne zaštite tvrtke koja se bavi privatnom zaštitom, stoga ćemo ga se malo dotaći je nadzor kretanja vozila, prijenosa i pratnje vrijednosti. Posao koji vrše pomno odabrani i specijalno obučeni i educirani zaštitari, tiču se pratnje i osiguranje prijenosa novca, vrijednosnih papira te dragocjenih kovina i metala.

Redarska služba pruža osiguranje događanja, koncerata, festivala i promotivnih evenata sukladno odredbama Zakona o javnom okupljanju i Zakona o sprječavanju nereda na športskim natjecanjima.

Domena redarske službe je[7]:

- Zadržati i predati policiji sudionika okupljanja koji je opasan,

[6] Zakon o privatnoj zaštiti (NN 68/2003)
[7] Zakon o privatnoj zaštiti (NN 68/2003)

- Pregledati osobu koja ulazi u štićeni prostor događanja te privremeno oduzeti predmete koji se ne smiju unositi u navedeni prostor,
- Zabraniti ulazak u prostor osobi za koju se prosudi da bi mogla remetiti red i mir,
- Usmjeravati kretanje sudionika događaja i slično.

Osiguravanje osoba (tjelohranitelj ili bodyguard) pružaju najbolji te posebno opremljeni i uvježbani zaštitari, po potrebi uz naručitelja usluge i 24 sata dnevno. Kao takvi, vrsni su poznavaoci borilačkih vještina te izvrsni strijelci, po potrebi upadljivo/neupadljivo odjeveni, te uz konstantnu podršku operativnog dežurstva i interventne ekipe, spremni su pružiti sigurnu zaštitu od bilo koje potencijalne ugroze korisnika.

Intervencije na zahtjev korisnika ili po alarmnoj dojavi te neovlaštenim ulascima u prostore, vrše interventni zaštitari uz obvezne obavijesti od strane operativnog dežurstva policiji, korisniku a po potrebi i vatrogascima i hitnoj medicinskoj službi. Njihova je zadaća utvrđivanje uzroka uključivanje alarma, sprječavanje moguće štete na štićenim objektima i pripadajućoj imovini te naposljetku i osiguranje mjesta do dolaska policije na mjesto štetnog događaja.

Svi navedeni poslovi u sektoru tjelesne zaštite su manje ili više relevantni po osiguravanje takve vrste zaštite u hotelskoj industriji, konstantno ili povremeno. Najčešće to bude u obliku ophodnje objekta bilo samo tokom noći ili nerijetko i cjelodnevno, ovisno o potrebi hotelskog objekta. Također, održavanje nekih većih događanja u vidu promotivnih evenata, većih domjenaka nerijetko iziskuje potrebu za osiguranjem, te se za taj posao može angažirati redarska služba pružatelja poslova iz branše privatne zaštite.

4 Mehanička zaštita

Najosnovnija protuprovalna i protuprepadna zaštita u hotelskoj industriji dolazi u obliku mehaničke zaštite, koja je u često slučajeva podcijenjena, no zaboravlja se da je upravo ona preteča svih kasnije novopridošlih modernijih vrsta zaštite[8]. Iskusni projektanti sustava zaštite pridaju veliku važnost uporabi elemenata baš ove vrste zaštite, jer mehanička zaštita nisu samo kvalitetni zidovi i visoke ograde nego i najjednostavniji elementi poput sigurnosnih brava i cilindara, zaštićenih prozora, pješačkih i kolnih barijera i slično[9].

Međutim prvi i osnovni element ove vrste zaštite bez obzira radi li se o instalaciji minimalnog ili najvećeg stupnja zaštite su vrata. S obzirom da protuprovalna vrata ponekad dosežu masu i od nekoliko stotina kilograma, postavljati ih se ne može u klasične okvire već je za njih definirano minimalno 5 točaka učvršćenja i to na svakoj strani vrata potpomognuta sa cilindarskom bravom, isti su kriteriji i ja protuprovalne prozore.

Hoteli nekad imaju i sustave protuprovalnih prozora i neprobojna stakla kao i trezora napravljenih od željeznih stjenki koji se prije svega koriste kod pohranjivanja manjih vrijednosti te se otvaraju uz pomoć šifre ili koda ali imaju i dodatnu mehaničku bravu kojom se sef otvara u hitnim slučajevima.

Nadalje, valja spomenuti i sisteme zaključavanja koji čine osnovnu sigurnosnu razinu te u mnogim firmama pa tako i u hotelima su od krucijalne važnosti jer ni daljnja elektronska zaštita nije u potpunosti djelotvorna ako osnovne razine mehaničke zaštite nisu adekvatno napravljene.

U najčešćim slučajevima to uključuje sustav zaključavanja sa cilindričnim uloškima koji sadrže serijski kod ili broj.

[8] http://www.tehnoservis.net/protuprovalni-protuprepadni-sustavi-usluge-2.html
[9] Delišimunović, D., 2002., Suvremeni koncepti i uređaji zaštite, I.T. Graf d.o.o., Zagreb.

5 Tehnička zaštita

5.1 “Safety” sustavi

“Safety” sustavi i sustavi zaštite od požara odnose se na zaštitu ljudi i njihove imovine od elementarne nepogode ili bilo kojeg drugog nesretnog slučaja koji su kao takvi u smještajnim objektima većinom obavezni a tiču se niza posve uobičajenih oblika zaštite osoblja i gostiju[10]. Prije svega, riječ je o SOS pozivnim sustavima u nužnim situacijama koji mora imati svaka kupaonica, evakuacijska i panik rasvjeta koji označavaju predviđene evakuacijske puteve (npr. u slučaju požara, poplave itd.), sustav detekcije plina i ugljičnog monoksida te naposljetku gašenja požara. Safety dio tehničke zaštite strogo je definiran i propisan zakonom[11].

Stručnjaci sigurnosti bi trebali kod same izrade sigurnosnih prosudbi određenog objekta koji nije u kategoriji objekta za koji postoji zakonska obveza implementacije safety sustava tehničke zaštite uvjeriti upravu ili investitora da se investicije isplate, podizanjem sigurnosti taj objekt dobiva na konkurentskoj prednosti jer u slučaju nesreća manji su kako financijski tako i drugi, puno gori i dugoročniji po poduzeće oblici gubitaka. Primjerice negativnim medijskim eksponiranjem te narušavanja ugleda po nastanku nesretnog slučaja ili akcidentne situacije jer se naposljetku postavlja pitanje što se poduzelo i što se moglo poduzeti od strane hotela ne bi li šteta bila manja.

5.2 “Security” sustavi

U rubriku “security” sustava oblika sigurnosti spadaju elektronički sigurnosni sustavi koji omogućuju najučinkovitiju zaštitu objekta, implementiraju se zbog zaštite ljudi i njihove imovine od zlonamjernog djelovanja trećih osoba, te prevenciju rizika od razbojništva, krađa, terorizma, vandalizma i dr.

Hotelijeri to čine ugradnjom različitih sustava tehničke zaštite, a to su[12]:

- Protuprovalni i protuprepadni sustavi s javljačima raznih izvedbi (aktivnim i pasivnim),

[10] Pravilnik o zaštiti od požara ugostiteljskih objekata (NN 100/1999)
[11] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4.
[12] Delišimunović, D., 2002., Suvremeni koncepti i uređaji zaštite, I.T. Graf d.o.o., Zagreb.

- Sustavi kontrole i registracije prolaza,
- Sustavi kojima se obavlja stalni nadzor nad štićenim objektom s jednog mjesta (video nadzorni sustavi),
- Sustavi centralnog prijama i signalizacije alarma - Centralni dojavni sustav i Centralni tehnički nadzor (u daljnjem tekstu: CDS, CTN),
- Integralni sustavi zaštite s najmanje 1 nadzornim mjestom unutar štićenog objekta.
- Sredstva i naprave za neposrednu zaštitu ljudi:
  - protuprepadni alarm.
- Protusabotažni elementi:
  - specijalna ručna ogledala za pregled podvozja vozila.
  -

5.2.1 Videonadzor

Valjalo bi izdvojiti videonadzor koji je kao takav jako vrijedna adicija protuprepadnom i protuprovalnom sustavu jer detektira događaj u stvarnom vremenu, zatim ga verificira te ga se može koristiti kao izvor informacija i dokazni materijal MUP-u. Videonadzor je jedan od najučestalijih i najtraženijih sustava tehničke zaštite, jer najprije detektira događaj, a zatim ga verificira i poslije može dati detaljniju informaciju ili služiti kao dokazni materijal policiji.

Videonadzor omogućava[13]:

- Prostora koji nisu izravno vidljivi sa svih točaka objekta,
- Okoline, prilaza, ulaza i izlaza,
- Prostora s bilo kojeg mjesta na svijetu putem interneta,
- Naknadno pregledavanje snimke ili nadziranje.

Njegova primjena u smještajnim objektima svih veličina umnogome utječe na sigurnost gostiju, jer omogućavaju nadziranje hodnika, stubišta, prostora s većom fluktuacijom gostiju (i onih koji nisu gosti hotela), kao što su npr. restoran i recepcija, pa i okoliša hotela, pri čemu je posebno važan nadzor parkirališta, na kojem prijeti opasnost od oštećivanja vozila gostiju, te nadzor ulaza i izlaza. Sustavi protuprovale i protuprepada najviše su korišteni sustavi tehničke

[13] Delišimunović, D., 2002., *Suvremeni koncepti i uređaji zaštite*, I.T. Graf d.o.o., Zagreb.

zaštite. Prema Zakonu o minimalnim mjerama zaštite u poslovanju gotovim novcem i vrijednostima, obvezno ih je koristiti za zaštitu mjenjačnica, što je usluga koja se uobičajeno nudi gostima u hotelima.

5.2.2 Protuprovalni i protuprepadni sustavi

Cilj bi bio provalu detektirati u najranijoj fazi, pri samom pokušaju obijanja vrata ili prozora stakla. Za to nam služe razni protuprovalni detektori, npr. detektori pokreta, magnetski kontakti te detektori loma stakla, infracrvenim i mikrovalnim senzorima se štiti prostor unutar objekta jer kao takvi detektiraju prisutnost topline kojim zrači ljudsko tijelo. U protuprovalne detektori spadaju i tzv. tehnički detektori u vidu detektora temperature ili vode koji se pale u slučaju iznenadnog povećanja topline i detektiranja istjecanja vode ili poplave[14].

DETEKTORI	CENTRALNI UREĐAJI	ALARMNI IZLAZI
AKTIVNI I PASIVNI: • magnetski kontakti • pasivni infracrveni detektori • dualni (PIR/MW) • detektori loma stakla • zaštitne folije • detektori vibracija • detektori šuma	• mikroprocesorski • žičani i bežični • s rezervnim napajanjem • jedinstvena adresa svakog detektora • digitalnim komunikatorom • u više podstustava	• unutarnje i vanjske sirene s bljeskalicom • govorni i digitalni komunikatori • ostali izlazni uređaji(klima uređaji) • resvjeta, alarmni izlazi i dr.

Tablica 1. Suvremeni elementi protuprovalne zaštite

Izvor: Delišimunović, D., 2002., Suvremeni koncepti i uređaji zaštite, I.T. Graf d.o.o., Zagreb.

Nadalje, za hotelsko poduzeće također bitno, u slučaju neugodnog klijenta ili eventualnog pokušaja napada bilo koje vrste na osoblje ili gosta, postoje detektori u vidu prepadnih

[14] Delišimunović, D., 2002., Suvremeni koncepti i uređaji zaštite, I.T. Graf d.o.o., Zagreb.

detektora kao što su alarmne tipke (najčešće dolaze u bežičnom obliku) koje se u slučaju nužde aktiviraju. Svi detektori su spojeni na centralni uređaj koji prima informacije sa tih detektora i šalje ih prema izlazima na sirene te se vrši dojava na centralni dojavni sustav koji funkcionira u sklopu operativnog dežurstva koji potom ako je potrebno šalje intervenciju ne bi li se novonastali problem uklonio.

5.2.3 Centralni dojavni sustav

Poznat i kao CDS, čini dopunu sustavu tehničke zaštite kojom se podiže razina sigurnosti štićenog objekta na viši nivo te obuhvaća mogućnost nadzora, intervencija te izvješćivanja o potencijalnoj šteti nastaloj na objektu zaštićenim sustavima videonadzora i alarma. Dojava na CDS je spojena telefonskom linijom ili internetskom vezom. Dojavni sustav je dio 24-satnog operativnog dežurstva koji svakodnevno dobiva te obrađuje zaprimljene podatke sa štićenih objekata te postupa propisanom procedurom specifičnom za svakog klijenta utemeljenom sklopljenim ugovorom obiju strana. Sastoji se primarno od alarmnog centra te video centralnog sustava. Na njemu su spojeni svi mogući alarmni sustavi i na kojem se konstantno prate alarmna stanja, tehničke greške na sustavu, uključenja i isključenja alarmnog sustava na štićenim objektima, kao i spomenuti videonadzor preko kojeg se u slučaju uočenih nepravilnosti i kretnje neovlaštenih osoba[15].

5.2.4 Sustavi kontrole i registracije prolaza

Sustavi kontrole pristupa, vrlo specifična i sofisticirana tehnologija koja ima svojih raznih inačica – od sustava zaštite određenih prostora ili prostorija, pa do sustava inteligentnih soba u hotelima. To je svakako tehnički najzahtjevniji i najsloženiji od sustava security zaštite.

Sustav kontrole pristupa u hotelima ima tri glavne primjene: za osoblje, za goste i za vozila. Mnogi ljudi koji češće borave u hotelima, bilo poslovno ili u sklopu odmora, navikli su se na korištenje kartica za otvaranje i zatvaranje hotelskih soba u kojima borave, ali i za pristup

[15] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003)

ostalim hotelskim sadržajima (wellness, bazeni), pa čak i plaćanje računa u barovima. Mogućnost pristupa u sobe putem autonomnih brava koje se otvaraju pomoću kartice isplativa je i vlasnicima hotela, jer smanjuje troškove umnožavanja ključeva, onemogućava neovlašten ulazak u sobe davno odjavljenim gostima, a složeniji sustavi omogućavaju izradu vremenski ograničenih kartica.

Sustav kontrole pristupa mora moći obuhvatiti i pristup parkiralištu, garaži ili drugim objektima u sklopu hotela te može preuzeti i ulogu evidencije potrošnje gostiju (restoran, bar, internet). Osim za goste, sustav se može primijeniti i za evidenciju radnog vremena osoblja, kao i za evidenciju njihovog pristupa prostorima u koje je potrebno spriječiti njihov nehotičan ili zlonamjeran pristup. Kontrola pristupa za vozila te upravljanje rampama za ulaz na parkiralište veoma su često korištene mogućnosti sustava kontrole pristupa u hotelima.

5.3 Projektiranje i implementacija sigurnosnih sustava

5.3.1 Prosudba ugroženosti i izrada projekta

Cilj svakog sustava zaštite je u najvećoj mogućoj mjeri zaštiti osobe i imovinu zbog kojih je projektiran i izveden, te nakon detekcije neke vrste ugroze u najkraćem vremenskom periodu angažirati sva raspoloživa sredstva u svrhu otklanjanja potencijalnih opasnosti i minimiziranja mogućih neželjenih posljedica. Da bi to bilo izvedivo teži se integraciji raznovrsnih sustava tehničke zaštite počevši od tjelesne, tehničke, informacijske i dojavne zaštite sa jednim centralnim nadzornim mjestom. Primjena takvog integralnog koncepta zaštite omogućuje efikasno i optimalno korištenje tehničke i tjelesne zaštite koji djelujući interaktivno i međuovisno tvore najraznovrsniji i najsigurniji sustav zaštite koji se danas može pružiti[16].

Ne bi li sustav kao takav bio funkcionalan, bitne su sigurnosne prosudbe hotela, analiza rizika, projektiranje, implementacija sustava tehničko-tjelesne zaštite, izrada procedura postupanja u kriznim ili akcidentnim situacijama, kao i edukacija osoblja (na svim razinama odgovornosti) u cilju podizanja njihove sigurnosne kulture.

Što se početnog procesa projektiranja sigurnosnih sustava tiče, ono se sastoji od[17]:

[16] Delišimunović, D., 2002., Suvremeni koncepti i uređaji zaštite, I.T. Graf d.o.o., Zagreb.
[17] Delišimunović, D., 2006., *Management zaštite i sigurnosti*, Pragmatekh, Zagreb.

- Snimke postojećeg stanja štićenog prostora i analizu problema s ocjenom,
- Prosudba ugroženosti,
- Sigurnosnog elaborata,
- Projektnog zadatka,
- Projektiranja sustava tehničke zaštite,
- Izvedbu sustava tehničke zaštite,
- Stručni nadzor nad izvedbom radova,
- Obavljanje tehničkog prijama sustava tehničke zaštite,
- Održavanje I servisiranje sustava tehničke zaštite,
- Uporabu sustava tehničke zaštite.

Kvaliteta projekta kao i svega u životu ovisi o pripremi koje je uslijedila prije same implementacije. Od velike je važnosti da se cjelokupan projekt izradi maksimalno poštujući pravila struke po navedenim koracima koji se logički nadovezuju jedan na drugi, ne bi li se u startu preko projekta pa do same ugradnje i instalacije sustava minimizirale prilike za greškama koje potencijalno mogu biti kardinalne, jer je ipak riječ o ugradnji sustava sigurnosti koji služi protekciji nekog korisnika usluge. Tim više što u današnje vrijeme prepuno raznih mogućnosti i sredstava pomoću kojih zlonamjerni pojedinci I organizacije mogu postići svoje loše najmere prema drugima, svaki od navedenih koraka je neophodan.

Počevši od snimke postojećeg stanja kojom se prikupljaju podaci o postojećim mjerama zaštite, broju, tipu i načinu izvršavanja dosadašnjih štetnih događanja te visini šteta izazvanih dosadašnjim štetnim događanjima na budućem štićenom prostoru.

Što se tiče prosudbe ugroženosti, ona se izrađuje na osnovi prikupljenim podacima o:

1. Vrsti, namjeni, veličini i izgledu objekta, lokaciji i okruženju te građevnim i ostalim svojstvima objekta:
    - Osnovni podaci o objektu, lokacija, okruženje objekta, veličina, izgled,
    - Namjena objekta (vrsta poslovanja i osnovni dijelovi štićenog prostora),
    - Građevinska izvedba vrata i prozora, podova i stropova, krovne konstrukcije,
    - Otvori (kanalizacija, ventilacija i drugi otvori koji mogu poslužiti za neovlašten ulazak osoba),
    - Elektroenergetske instalacije i strukturno kabliranje,

- Ostale instalacije s stajališta sigurnosti i moguće sabotaže (spremnici goriva, plin, voda, kanalizacija, ventilacija, klimatizacija),
- Rasvjeta (vanjska, unutarnja rasvjeta).

2. Vrsti i broju stalnih i povremenih korisnika:
    - Broj radnika (u stalnom radnom odnosu, privremenom RO, student servis),
    - Rad sa strankama (način ulaska stranka na objekt i njihova frekvencija),
    - Radno vrijeme (rad u smjenama, radno vrijeme za klijente, za radnike, pauza, način ulaska u objekt).
3. Režimu rada i načinu korištenja objekta:
    - Opis procesa (vrste procesa, proces rada na objektu bitnih za poslovanje i sigurnost objekta),
    - Opis tokova vrijednosti (način rada s novcem, pohrana, dostava i prihvat, zračna pošta, način i vrijeme dopreme novca).
4. Opremi, predmetima i dokumentima koji će se u objektu nalaziti ili se već nalaze te stupnju rizika od njihova oštećenja, otuđenja ili uništenja.

Nadalje, nakon izvršene prosudbe ugroženosti, izrađuje se sigurnosni elaborat kojim se određuje optimalna razina tehničke zaštite, integralne zaštite, kao i povezanost s drugim tehnološkim sustavima na prostoru. Njegova je svrha sprječavanje djelovanja određenih opasnosti ili umanjivanje šteta koje mogu nastati njihovim djelovanjem.

Da bi se koncepcijom mjera zaštite postiglo optimalno rješenje potrebno je zaštitu razbiti na zone detekcije, a za optimalno štićenje nekog objekta potrebno je predvidjeti 5 zona detekcije[18]:

- Ulazak u vanjski perimetar,
- Kretanja unutar perimetra,
- Kretanje u neposrednoj blizini objekta,
- Kretanje u unutrašnjosti objekta,
- Maksimalan pristup štićenom prostoru.

[18] Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.

Nadalje, bitno je raščlaniti i kategorizirati stupnjeve integrirane zaštite koji stoje na raspolaganju subjektima i objektima u sklopu njihove implementacije. Navedeno je shematski prikazano u tablici ispod[19].

1. kategorija Najviši stupanj zaštite koji predviđa:	2. kategorija – visoki stupanj zaštite koji predviđa	3. kategorija – viši stupanj zaštite koji predviđa
• Mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS • Tehničku zaštitu kojom se prati kretanje u štićenom prostoru • Zaštitu pojedinačnih vrijednosti pomoću specijalnih kasa, trezora i sl. • Integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa zaštitarima u štićenom prostoru	• Mehaničku i tehničku zaštitu kojom se signalizira ulazak u štićeni prostor i dojavljuje na CDS • Tehničku zaštitu kojom se prati kretanje u štićenom prostoru (kontrola prolaza i video nadzor) uz video zapis • Integralnu zaštitu s najmanje jednim lokalnim nadzornim mjestom i sustavom veze sa CDS-om	• Mehaničku i tehničku zaštitu kojom se signalizira neovlašten ulazak u štićeni prostor i dojavljuje na CDS • tehničku zaštitu kojom se prati kretanje u štićenom prostoru

[19] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003)

4. kategorija – srednji stupanj zaštite koji predviđa	5. kategorija – niži stupanj zaštite koji predviđa	6. kategorija – minimum zaštite koji predviđa
• Mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štićeni prostor • Video nadzor kojim se prati kretanje u štićenom prostoru uz video zapis	• Mehaničku i tehničku zaštitu kojom se na licu mjesta zvučno ili svjetlosno signalizira neovlašten ulazak u štićeni prostor	• Mehaničku zaštitu bez uporabe elektroničkih naprava • Obične ograde bez tehničkih elemenata

Tablica 2. Kategorije obvezne mjere zaštite

Izvor: Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.

Na temelju izrađenog sigurnosnog elaborata te posebnih zahtjeva korisnika objekta izrađuje se projektni zadatak kojim se utvrđuju svi parametri potrebni za izradu projekta sustava tehničke zaštite[20]:

1. Vrsta tehničke zaštite,
2. Smještaj centra tehničke zaštite,
3. Smještaj uređaja i opreme,
4. Način polaganja instalacija.

Ovo je posljednji korak prije početka procesa projektiranja, ishodišna točka koju kao potvrda o usklađenosti s prethodnim fazama u toku izrade projekta zajednički izrađuju i potpisuju korisnik i predstavnik projektantske zaštitarske tvrtke.

5.3.2 Tijek aktivnosti pri izradi projekta

Projektiranje treba sagledati kao proces te ono poštujući pravilnik struke koji obuhvaća[21]:

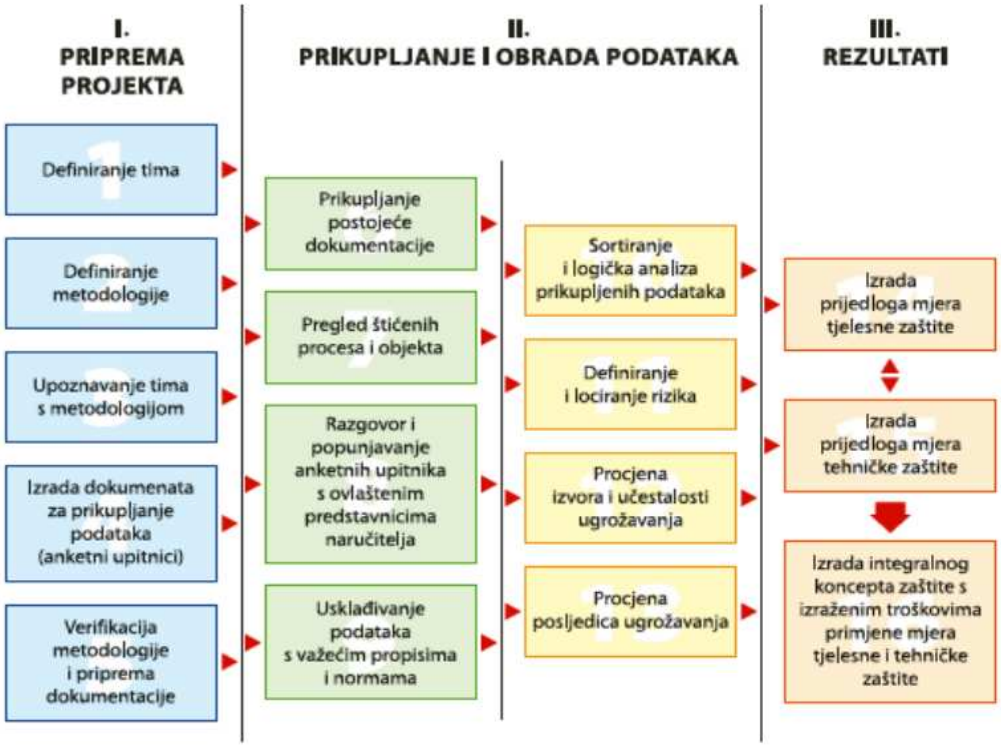
1. Odabir vrste i opsega tehničke zaštite,

[20] Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.
[21] Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003)

2. Odabir uređaja i opreme,
3. Razradu koncepcije tehničke zaštite,
4. Izradu projektne dokumentacije.

Projekt sustava tehničke zaštite mora biti izrađen sukladno propisima koji uređuju poslove projektiranja, te snimka postojećeg stanja štićenog objekta i analiza problema s ocjenom, prosudba ugroženosti, sigurnosni elaborat i projektni zadatak, čine sastavni dio projekta sustava tehničke zaštite. Potrebno je osigurati sigurnu pohranu projekta tehničke zaštite te voditi evidenciju o svim izrađenim kopijama (svaka mora biti brojčano označena) u čiji uvid smiju imati samo osobe koje imaju ovlast za obavljanje poslova tehničke zaštite propisane razine. Navedeni projekt je poslovna tajna i ne može biti dijelom idejnog, glavnog ili izvedbenog građevinskog projekta.

Nakon projekta sustava tehničke zaštite slijedi korak izvedbe i ugradnje sustava tehničke zaštite, te naposljetku, po propisanoj zakonskoj obvezi, održavanje sustava u ispravnom stanju te servisiranje najmanje jednom godišnje.



Slika 1. Prikaz faza izrade prosudbe ugroženosti, sigurnosnog elaborata i projektnog zadatka

Izvor: Delišimunović, D., 2006., Management zaštite i sigurnosti, Pragmatekh, Zagreb.

6 Informacijska zaštita

Turizam i hotelijerstvo vrsta su djelatnosti veoma bogata kolanjem raznih podataka te informacija od generalnog stanja kako tržišta ponude i potražnje tako i privatnih podataka poduzeća i svih ostalih učesnika u turističkom sektoru. Količina podataka koja se obrađuje svakim danom je sve veća, kao i činjenica da je zbog već spomenute globalizacije i lakoće oglašavanja te potrebite transparentnosti, internetska prisutnost koju ovo moderno doba zahtijeva je sve izraženija. Iz navedenih razloga turistički subjekti koji se nalaze na strani ponude (između ostalih i hotelijeri) posežu za što većim stupnjem implementacije modernizacije informacijskih sustava koji pospješuju kvalitetu svakodnevnog poslovanja na relaciji gost – hotelsko poduzeće, uspostavljaju nove oblike marketinga, olakšavaju operativne poslove, personaliziraju usluge te kvalitetno integriraju odjeljenja unutar samog hotelskog poduzeća[22].

Slijedom navedenog, da se zaključiti da su potrebita ulaganja i u informacijsku sigurnost ne bi li sveobuhvatan stupanj sigurnosti koju hotel pruža bio na razini. Stoga je od neophodne važnosti da svi ti privatni podaci koji su u konstantnom opticaju budu na adekvatan način zaštićeni sa što više slojeva zaštite što to u datom trenutku up to date tehnologija dozvoljava. Tim više što sa već navedenom povećanom internetskoj izloženosti, sve učestalije kibernetičke prijetnje (u vidu raznih pokušaja neovlaštenih pristupa, malware napada, povrede podataka, phishing itd.) nisu zaobišle ni sektor turizma i hotelijerstva.

Posebna se pažnja u hotelskim poduzećima posvećuje prije svega zaštiti osobnih podataka, odgovornom i sigurnom kartičnom plaćanju, primjerenom korištenju informacijsko-komunikacijske tehnologije i druge slične tehnološke imovine. Sve to rezultira potrebom za educiranom i tehnološko osviještenom radnom snagom u području turizma do kojeg je sve teže doći uzimajući u obzir činjenicu da je turizam kao djelatnost veoma intenzivna sa velikom fluktuacijom radne snage. Neki hotelijeri prepoznaju potrebu za modernizacijom svojega svakodnevnog poslovanja u vidu informacijske tehnologije te ulože velika količinu sredstva s ciljem podizanja kvalitete i produktivnosti usluge, ali ne posjeduju nužno kvalitetni ljudski resurs koji tu istu tehnologiju može koristi na adekvatan način.

[22] Spremić, M., 2017., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb.

Mnogobrojni su alati kojima se može doći do privatnih, osobnih i kompromitirajućih podataka, na sreću, informacijska sigurnost se generalno razvila u proteklom desetljeću prije svega sa introdukcijom raznih normi i uredbi koje danas služe kao osnovica za zakonodavce i poslodavce u smislu stvaranja povoljne sigurnosne klime.

6.1 Najčešće vrste napada na informacijsku sigurnost

DDoS (distributed denial of service), ili napad uskraćivanjem posluživanja je vrsta napada na informacijski ili računalni sustav s namjerom da se vlasnicima tih sustava privremeno ili trajno onemogući njihovo korištenje a najčešće se provodi slanjem velike količine zahtjeva računalnom sustavu u kratkom vremenskom periodu što isti ne može obraditi[23].

Najpoznatiji i najučestaliji oblici DDoS napada su[24]:

- Teardrop napad koji se oslanja na grešku u funkciji za sastavljanje paketa u raznim operacijskim sustavima tako da šalje pakete sa prevelikim podatkovnim dijelom ili sa podatkovnim dijelovima koji se preklapaju u fragmentima nekog paketa,
- Smurf napadom napadači lažiraju IP adresu izvorišta paketa da odgovara meti napada, tako da sva računala koja dobiju pakete preko adrese za razašiljanje odgovaraju meti napada koja postaje zatrpana,
- Raspodijeljeni napad (eng. DDoS - Distributed Denial of Service) koristi više računala za napad na istu metu. Ta računala su većinom zaražena raznim zlućudnim softverom (npr. virusima, trojancima, crvima) koji služi za koordinaciju tih računala prilikom napada,
- Raspodijeljeni reflektirani napad (eng. DRDoS - Distributed Reflected Denial of Service) je vrsta napada koja se izvodi na način da se više mrežnih odredišta na internetu šalju zahtjevi sa lažiranom izvorišnom adresom koja odgovara adresi mete napada, tako da svi odgovori stižu na jednu metu.

[23] Klarić, I., 2007., Načini zlouporabe ranjivosti računalnog sustava, Seminar, Fakultet elektrotehnike i računarstva, Zagreb.
[24] https://hr.safetydetectives.com/blog/sto-je-ddos-napad-i-kako-ga-sprijeciti/

6.1.1 Zlonamjerni programi

Programi kojima se vrši napad na informacijsku sigurnost su: crvi, virusi, trojanci, spyware, adware.

Virusi su zlonamjerni programi koji iskorištavaju druge dobroćudne programe za svoju ekspanziju tako da na dobroćudni izvršni program legitimne aplikacije prikače zloćudni izvršni program. Nakon što zlonamjerni program obavi svoju zadaću, kontrola izvršavanja se vraća legitimnom programu koji normalno nastavlja svoj rad, a to je primaran razlog zašto korisnici nerijetko nisu ni svjesni da im je računalo zaraženo.

Crvi u usporedbi sa virusima imaju mogućnost samostalnog širenja nakon što su inicijalno pokrenuti od strane napadača, dakle nije im potrebna pomoć korisnika. Za širenje najčešće iskorištavaju jako poznate i neispravljene greške u operacijskim sustavima ili drugim programima. Još jedna učestala metoda širenja je koristeći programe za čitanje elektroničke pošte i to tako da sami sebe pošalju svim kontaktima u adresaru na zaraženom računalu. Crv kao takav ima daleko veći potencijal nanošenja štete od bilo kojeg virusa jer je crv u stanju zaraziti velik broj računala u vrlo kratkom vremenskom periodu. Jednom zaražena računala mogu biti iskorištena od strane napadača na više načina. Najčešće se ta računala koriste za napade protiv nekih drugih računala pretvarajući ih u sudionike raspodijeljenog napada uskraćivanjem usluge.

Trojanci su vrsta zlonamjernih programi koji se predstavljaju kao dobronamjerni programi a zapravo izvršavaju zlonamjernu pozadinsku u računalnom sustavu, dopuštajući hakerima nesmetan pristup resursima tog sustava.

Adware je vrsta programa koji je najčešće besplatan za korištenje zbog činjenice da se unutar programa prikazuju oglasi kojima se proizvođači programa financiraju. Prikazivanje oglasa unutar programa nije sporno, no proizvođači softvera kao sustave za prikazivanje oglasa koriste druge programe koji su napisani tako da ciljano prikazuju oglase koristeći podatke o navikama korisnika koje prikupljaju sa računala na koja su instalirana. Time je narušena privatnost korisnika računalnih sustava.

Spyware je vrsta zlonamjernog programa kojem je jedina zadaća prikupljanje podataka o navikama korisnika na čije se računalo cilja, prikupljene informacije se zatim šalju proizvođačima spyware-a koji iste koriste u marketinške svrhe. Podaci se prikupljaju

praćenjem teksta koji korisnik unosi na računalu ili pohranjivanjem trenutnog sadržaja na display-ju.

6.1.2 Socijalni inženjering

Socijalni inženjering se definira kao skup tehnika koji hakerima služi kao vrsta psihološko-manipulativnih radnji prema korisniku informacijskog sustava ne bi li hakerima omogućio nesmetan pristup tom informacijskom sustavu. Kao takav iskorištava ljudsku neinformiranost i naivnost ne bi li se od legitimnih korisnika računala ili informacijskog sustava izvuklo povjerljive i osobne podatke u sklopu kompromitacije i zlonamjernosti, te se od klasičnog hakiranja sustava razlikuje po tome što uključuje neposrednu ljudsku interakciju. Koliko je efikasan govori statistički podatak da je socijalni inženjering glavni krivac krađe podataka u čak 70% slučajeva, te činjenica da nevjerojatnih 98% cyber napada sadrži određenu razinu socijalnog inženjeringa[25].

Phishing je taktika kojom se od korisnika pokušava izvući povjerljiva informacija o njegovim bankovnim računima i podacima kreditnih kartica i to putem spam-a (nepoželjne e-mail pošte) koji na prvi pogled izgledaju kao legitimni mailovi od strane drugih poduzeća (npr. banke i webshop stranice) preko kojih se traži od korisnika da ostavi svoje osjetljive osobne podatke na posebno kreiranoj web stranici.

Pretexting je tehnika kojom se napadač služi na način da se preko prethodno pomno isplaniranog i uvjerljivog scenarija komunicira sa korisnikom ne bi li ga se prisililo na odavanje osobnih podataka koji dovode do njegove kompromitacije.

Scareware čiji je oblik najčešće pop-up oglas, je tehnika socijalnog injženeringa kojom se nastoji proširiti štetna tehnologija koja je prikazana kao legitimna na način da se korisnika prestraši sa lažnim uzbunama i alarmima o potencijalnoj štetnosti pojedinih programa te ga se natjera da instalira taj maliciozni softver u sklopu zaštite a zapravo se radi o malware-u.

[25] Spremić, M., Šimunic, A., 2018., Cyber security challenges in digital economy, Proceedings of the World Congress on Engineering, International Association of Engineers, Hong Kong.

Kao i kod prethodno navedenih metoda i ovoj je krajnji cilj krađa osjetljivih podataka te nerijetko uključuje i ransomware pomoću kojeg hakeri prijete širenjem tih privatnih informacija ako im se ne isplati određena svota novčanih sredstava.

Ove tehnike su veoma uvjerljive te prosječnim korisnicima upravo iz razloga kako su kreirane djeluju podosta kredibilno.

6.2 Sustavi informacijske zaštite

Informacijska zaštita ili sigurnost je primarno fokusirana na zaštitu privatne imovine i privatnih podataka, te postoje razne uredbe, standardi kao i tehnološka rješenja koje omogućuju hotelskom poduzeću zaštitu vlastitih podataka kao i onih od gostiju. Jedno od primarnih i najjednostavnijih metoda zaštite od modernih kibernetičkih napada je svakako učestalo ažuriranje operativnog sustava i korištenje kredibilnog i legitimnog antivirusnog programa[26].

Međutim, najviše grešaka se dešava kada je u cijelu situaciju uključen faktor čovjek. Nedovoljna informiranost osoblja i klijenata o sigurnosnom postupanju prilikom bilo kakvog oblika međusobne interakcije, bilo uživo a još više preko web-a je najbitniji razlog neautoriziranog curenja osobnih podataka[27].

U nastavku će biti govora o modernim metodama informacijske zaštite.

6.2.1 ISO/IEC 27001

ISO 27001 je međunarodni standard i temeljna norma za upravljanje informacijskom sigurnosti[28]. Osigurava mogućnost poduzeća da se zaštiti interno, tj. od needuciranih i neinformiranih zaposlenika ili neučinkovitih postupaka kao i eksterno u vidu raznih drugih prijetnji koje su moguće u današnje vrijeme temeljenih na tehnologiji te je kao takav temelj današnjeg sigurnog poslovanja.. Propisuje načine na koje se može organizirati informacijska sigurnost u bilo kojoj vrsti poduzeća pa tako I u hotelskim, bilo da se radi o profitnoj ili

[26] Cerović Z., 2010., Hotelski menadžment, Fakultet za turistički i hotelski menadžment, Opatija.
[27] Spremić, M., 2017., Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb.
[28] ISO/IEC 27001:2022

neprofitnoj organizaciji, privatnoj ili državnoj, maloj ili velikoj. S obzirom na značaj norme, mnogim zakonodavstvima kao takva služi kao norma i temelj za pisanje regulative iz područja zaštite i tajnosti osobnih podataka, zaštite informacijskih sustava te upravljanjem operativnim rizicima ne bi li se sveli na minimum.

ISO 27001 se primarno bavi tehničkim ranjivostima ranije navedenima koji potencijalno mogu rezultirati narušavanjem IT sigurnosti poduzeća i organizacije, kao što su:

- Razni oblici socijalnog inženjeringa poput Phishinga i SPAM-a, Pretexting-a, Scareware-a i Ransomware-a koji manipulativnim putem prisile korisnika na odavanje osobnih podataka,
- DDoS/botnetovi koji su u stanju dovesti do narušavanja mogućnosti korištenja sustava pretrpavanjem istog većom količinom podataka no što sustav na koji se napada može to obraditi u kratkom roku,
- Zlonamjerni programi kao npr. Trojanac za daljinski pristup (RAT),
- Državno sponzorirani cyberteroristi, aktivisti, kriminalci kao i unutarnji počinitelji,
- Neadekvatni ili nedostajući procesi.

Prednosti primjene norme ISO/IEC 27001 su sljedeći:

- Smanjivanje rizika vezane uz sve vrste informacija važne za organizaciju,
- Bolje konkurentnost u odnosu na konkurenciju, tj. veliki je značaj samog marketinškog korištenja ISO/IEC 27001 certifikata,
- Efikasnost i optimizacija poslovnih procesa u organizaciji koji su jasni I definirani,
- Smanjenje potencijalnih troškova poslovanja radi prevencije reklamacija I ostalih incidentnih situacija,
- Popunjavanje sve rigoroznijih kriterija i prohtjeva klijenata za imanje ISO/IEC 27001 certifikata ili potvrdom o informacijskoj sigurnosti davatelja usluge,
- Ispunjavanje zakonski propisanih zahtjeva.

Kompromitiranost informacijske sigurnosti se može izbjeći ili u najmanju ruku minimizirati uspješnom procjenom rizika do kojeg se dođe analizom log podataka, poznavanje tehničkih ranjivosti i dubljeg pregleda IT sustava.

6.2.2 GDPR

Jedan od bitnijih elemenata zaštite podataka je Opća uredba o zaštiti podataka (General Data Protection Regulation ili skraćeno GDPR) koja je stupila na snagu 2018. godine i primjenjuje se u svim državama članicama EU. Ključna joj je zadaća da omogući individualnoj osobi veću kontrolu nad zaštitom svojih osobnih podataka. Uredba se primjenjuje na sve institucije koje u sklopu svojih aktivnosti na bilo koji način obrađuju podatke ili ih od drugih pojedinaca trebaju kao recimo u hotelijerskim poduzećima u sklopu evidencija[29].

Vodstvo hotela kao i cjelokupno hotelsko osoblje moraju biti informirani i educirani o osnovnim načelima GDPR-a I pravima ispitanika te moraju biti svjesni odgovornosti koju nosi prikupljanje I obrada podataka. Nerijetko je slučaj da primjerice službenik za zaštitu podataka ne posjeduje potrebite kvalifikacije za kvalitetno obnašanje te funkcije stoga svojim aktivnostima prema ispitanicima ili nadzornom tijelu akcidentno nanosi štetu.

Stoga je od krucijalne važnosti da hotelijerska poduzeća detektiraju manjkavosti u vlastitom kadru na vrijeme ne bi li što je moguće više minimizirali potencijalno narušavanje sigurnosti i integriteta svojih klijenata te poslovnih partnera što se također može negativno odraziti na ugled hotelijerskih poduzeća.

6.2.3 Predautorizacija

Predautorizacija kreditne kartice hotelu omogućuje privremeno "rezerviranje" određenog novčanog iznosa prilikom same rezervacije gosta (najčešće 1-2 noćenja, rijetko cijeli boravak) prije svega u sklopu minimiziranja eventualnih prijevara kreditnom karticom jer vlasnik kartice u tom slučaju zaprima upozorenje da je izvršena predautorizacija. U slučaju dakle da je kreditna kartica ukradena, vlasnik kartice ju može poništiti u banci a hotel u tom slučaju može sobu rezerviranu tom karticom prodati drugom gostu. Također, ako gost recimo rezervira sobu a zatim otkaže rezervaciju tijekom vrhunca sezone, hotel ima jamstvo za unaprijed autorizirani

[29] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ

iznos čime se smanjuje potencijalni gubitak prihoda hotela, tj sprječava nepojavljivanje ili kasno otkazivanje smještaja[30].

Stoga predautorizacija ima višestruke koristi jer štiti i gosta i hotel.

Najsigurnija, najpraktičnija i u moderno vrijeme najprikladnija metoda predautorizacije je ona digitalna koja se vrši jednim klikom od strane vlasnika kartice automatski se pritom povezujući relevantnom bankom.

6.2.4 Dvostruka autentifikacija

U kontekstu online plaćanja a nadovezujući se na proces predautorizacije, bitnu ulogu ima SCA (Strong Customer Authentication), tj. snažna provjera autentičnosti korisnika koju zahtjeva druga Direktiva o platnim uslugama (PSD2).

SCA je naime poznat kao dodatan sloj sigurnosti, odnosno dvostruka ili dvostupanjska autentifikacija, funkcionira po principu dodatnog provjeravanja identiteta gostiju u slučaju njihove fizičke odsutnosti putem jedne od sljedećih metoda provjere:

- Lozinka ili PIN
- Mobilni uređaj
- Biometrijski podaci (otisci prsta).

Dvofaktorska autorizacija naposljetku garantira sigurnost i pristanak, a ako se navedenog procesa gost ne pridržava, hotel naposljetku može odlučiti anulirati rezervaciju.

6.2.5 PMS softver

PMS, poznati kao Property Management System ili sustav upravljanja imovinom je moderno softversko hotelsko rješenje koje pomaže hotelima u svakodnevnim operativnim zadacima koji uključuju razne administrativne i upravne zadatke te je zamišljen kao sustav “sve u jednom”.

[30] Huth, A., Orlando, M., Pesante, L., 2012., Password security, protection, and management, United States Computer Emergency Readiness Team.

Između ostaloga, a u kontekstu ovog rada, omogućava funkcionalnost digitalne prijave koja je novija ponuda na PMS tržištu ali je sve prisutnija automatski sinkronizirajući i ažurirajući podatke o prijavi i popunjenosti. Nadalje, s obzirom da se hotelska industrija sve više usmjerava na podatke, što znači čuvanje podataka o kupcima, jedna od opcija PMS sustava uključuje i sigurno rukovođenje osjetljivim podacima te informacijama o datumima kada su kupci boravili u hotelu, informacije o tome u kojoj se sobi gosti nalaze i dr.

S obzirom na mogućnost pohranjivanja podataka o klijentima na jednom mjestu, PMS softver se može integrirati sa drugim popularnim hotelskim softverom tzv. CRM (Customer Relationship Management) softverom koji hotelu služi kao medij za analizu klijentovih navika i tendencija u sklopu stvaranja što kvalitetnije personalizirane ponude[31].

6.3 Edukacija djelatnika

Slijedom svega navedenog, s obzirom u kojem se smjeru razvija tehnologija te kakvom lakoćom treće osobe mogu u slučaju neadekvatne razine sigurnosti, manjkavosti u protokolima ili u kadru hotela doći do osobnih podataka bilo gostiju ili osoblja, od krucijalne je važnosti uz ulaganje u modernizaciju sustava poslovanja i ulaganje u sigurnost tih sustava kao i u edukaciju vlastitih zaposlenika koji svakodnevno rade i rukovode sa tim istim sigurnosnim sustavima.

Dakle pravilnom i ažurnom edukacijom i informiranošću prije svega djelatnika hotelskog poduzeća može se dosta potencijalne štete eliminirati jer upravo prevencija problema je jedan od najboljih, najjeftinijih i najučinkovitijih metoda zaštite[32].

[31] Baker, S., Bradley, P., Huyton, J., 2001., Principles of Hotel Front Office Operations, Cengage Learning, 2. izdanje.
[32] Cerović Z., 2010., Hotelski menadžment, Fakultet za turistički i hotelski menadžment, Opatija.

7 Postupanja u kriznim situacijama

Od sigurnosnih stručnjaka se očekuje da svojim akcijama i reakcijama, bilo na temelju osobnih iskustvenih spoznaja bilo na osnovi iskustvenih spoznaja drugih, prevenira odnosno spriječi nastanak bilo kojih štetnih radnji i događaja za kompaniju – objekt.

Pravilo "3 P" glasi[33]:

Predviđanje – predvidjeti znači znati,

Planiranje – znati znači imati plan ili proceduru,

Pravilno postupanje – imati plan ili proceduru znači smanjiti ili eliminirati ugrozu ili štetu.

7.1 Protokoli i procedure

Protokoli i procedure su operativni vodič postupanja u kriznim ili akcidentnim situacijama (ali i ne samo u njima), jer opće je poznato da kriza ili akcident je situacija koja započinje potencijalno ozbiljnom prijetnjom ili najavom ugroze, a potom ako se u samom startu ne krene rješavati adekvatno prerasta u događaj koji potencijalno ugrožava živote ljudi i materijalna dobra. Stoga najučinkovitija sredstva za kontrolu i ograničavanje štetnih posljedica su donesene procedure postupanja u kriznim ili akcidentnim situacijama. Naime, mnoge radnje i postupci navedeni u proceduri mogu se učiniti zdravo razumni i logični te kao takvi nepotrebni za unošenje u proceduru, međutim, u kriznoj situaciji zdravi razum i logika nerijetko izostanu.

Procedurom se može potaknuti zaposlene da u takvim kriznim okolnostima postupe prema unaprijed napravljenom planu djelovanja. Nadalje, pojačava se svijest o potrebi učinkovitih reakcija, odnosno omogućava se stvaranje plana postupanja koji će pomoći rukovodećoj grupaciji u rješavanju krizne ili akcidentne situacije i iznalaženju najučinkovitijih odgovora, kao i u stvaranju internih planova i programa koji bi ovu problematiku tretirali na razini dislociranih objekata kompanije, uvažavajući svu specifičnost pojedinog objekta. Procedurom

[33] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4.

se također mogu utvrditi točke uključivanja u rješavanje kriznih ili akcidentnih situacija više razine odlučivanja, odnosno čelnih osoba uprave[34].

Ključ je dakle zaštititi prije svega ljudske živote te materijalna dobra, limitirati štetu, uključiti u postupak rješavanja eventualnog problema koji je nastao nadležne institucije I javne službe, istražiti uroke, izvijestiti o uzrocima, u što kraćem roku vratiti svakodnevne aktivnosti hotelskog poduzeća u normalu te na temelju iskustva koje je stečeno potencijalno prevenirati nastanak sličnih neželjenih situacija.

Upute o postupanju, bez obzira na to sa strane koje razine se izdaju, moraju biti logične i provedive. Upute se uvijek izdaju čelniku tima za postupanje u kriznim ili akcidentnim situacijama, a moraju se izdavati na način da ne djeluju nesigurno i konfuzno i da ne unose pomutnju u djelovanje članova tima. Upute se moraju izdavati autoritativno, ali ne prijeteći i s omalovažavanjem, jer moraju pomoći rješavanju krize, a ne otežati rad na mjestu štetnog događaja.

Veoma je važno redovito izvještavanje o postupanju povodom štetnog događaja, te o činjenicama i uzrocima koje su utvrđene poduzetim radnjama i mjerama. Također je potrebno redovito izvještavati o novonastaloj situaciji na mjestu štetnog događaja, poduzetim mjerama na saniranju nastalih šteta i otklanjanju opasnosti, kao i trenutnom stupnju ugroženosti osoba i materijalnih dobara, a važne su i informacije o reagiranju na štetni događaj od strane zaposlenika, gostiju, medija i lokalne zajednice.[35]

Analiza stanja mora odgovoriti na pitanja što, gdje, kako i zašto se štetni događaj dogodio, mora dati realnu ocjenu uzroka, postupanja i posljedica štetnog događaja, mora poslužiti kao naučena lekcija u preveniraju i rješavanju mogućih sličnih novonastalih situacija i događaja te mora dovesti do poboljšanja u procedurama postupanja, edukacije, opremanja osoba i objekata.

Procedure obuhvaćaju i načine postupanja u situacijama kada dođe do aktivacije vatrodojavnog sustava, tko i koga evakuira, i s kojim prioritetima (invalidi, djeca, starije i nemoćne osobe). Podugačak je niz naizgled suvišnih procedura, no one su produkt iskustvenih spoznaja iz situacija iz prošlosti te služe kao orijentir što i kako u sličnim okolnostima, jer ipak je povijest majka znanja.

[34] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4.
[35] Laušić, M., Petar, S., 2010., Sigurnosne procedure u hotelima, Acta Turistica Nova, Vol. 4.

7.2 Primjer postupka intervencije po alarmnoj dojavi

Postupanje po alarmnoj dojavi može se svrstati u dio postupanja u kriznoj situaciji (reakcije djelatnika hotelskog poduzeća prilikom neugodnog iskustva sa nezadovoljnim gostom ili strankom te postupanja interventne ekipe po alarmnoj dojavi), primjerom djelovanja zaštitarske firme AKD Zaštite kratko će se opisati kako izgleda procedura po primanju alarmne dojave u centralni dojavni sustav (CDS) koji djeluje 24 sata u sklopu operativnog dežurstva.

Recepcionar hotela tijekom dnevne i noćne smjene sa sobom mora obavezno nositi daljinski protupanični odašiljač (bežična panik tipka) a ukoliko dođe do oružanog napada mora na diskretan i neprimjetan način aktivirati jedan od protupaničnih sustava.

Od neophodne je važnosti da djelatnik bude što smireniji i priseban prilikom potencijalne prijetnje, ne bi li uspjeh u (ako je za to potrebno) potencijalnom privođenju ukoliko se radi o prijetnji hladnim ili vatrenim oružjem bio što veći. Dakle, činom pritiska na panik tipku aktivira se tihi panik alarm kojeg zaprima CDS čija firma pruža tehničku i dojavnu zaštitu te vrste hotelskom poduzeću.

Naime, u CDS-u operateri koji obrađuju sve pristigle podatke sa štićenih prostora, po alarmnoj dojavi ili uvidom u videonadzor (kojem je detektirano neautorizirani dolazak na objekt) obavještavaju MUP a po potrebi i vatrogasnu ili hitnu službu, te voditelja smjene operativnog dežurstva po čijem nalogu interventna ekipa izlazi na mjesto sa kojeg je zaprimljena alarma dojava.

Interventna ekipa po dolasku na adresu, obilazi uz policijske službenike objekt sa vanjske a po potrebi i sa unutarnje strane (u slučaju da za to imaju odobrenje od strane korisnika usluge), utvrđuju razlog nastanka alarma, ovisno o situaciji postupaju po svojim propisanim ovlastima te povratno obavještavaju operativno dežurstvo i voditelja smijene koji ih navode što dalje činiti.

Nakon svega, protupanični sustav se treba resetirati ključem koji se nalazi na recepciji nakon čega se na kraju resetira i alarmna centrala ukucavanjem osobnog PIN-a dva puta na panelu protuprovale.

Interventni tim zaštitarske firme koji štiti hotelsko poduzeće piše izvješće koje potpisuje djelatnik hotela kao dokaz o izvršenoj intervenciji koja se na koncu fakturira tom konkretnom hotelu.

Što se tiče hotela, dužan je maksimalno surađivati do kraja sa policijskim službenicima i bilo kojim drugim javnim institucijama koji su uključeni u rješavanje nastalog problema te na temelju tog iskustva naučiti i doći do rješenja kako slične situacija ubuduće eventualno efikasnije rješavati, jer uvijek ima prostora za napredak.

8 Zaključak

Razvoj tehnologije sa sobom donosi modernizaciju kako u poslovanju tako i u osiguravanju sigurnosti u vrijeme u kojem je dostupnost informacija veoma izražena. Globalizacija je podosta doprinijela tome omogućivši lakše potencijalno narušavanje identiteta i krađe osobnih podataka, kao i generalnog osjećaja nesigurnosti. Stoga, da bi hotelsko poduzeće danas moglo biti konkurentno na tržištu, potrebna su ulaganja u inovacije i u modernizaciju sustava koji podiže generalnu efikasnost i produktivnost.

Dakako, to sa sobom povlači neophodnost ulaganja u edukaciju zaposlenika koji tom tehnologijom rukovode te razvoj informiranosti i svijesti o odgovornosti (primjerice o GDPR-u) koja je potrebna ne bi li se na adekvatan i zahvalan način obrađivali podaci koji se svakodnevno obrađuju u svrhu evidencija čija povreda potencijalno rezultira narušavanje privatnosti i integriteta prije svega hotelskog poduzeća, pa zatim I klijenata, gostiju ili poslovnih partnera.

Što se tiče hotelskih sigurnosnih sustava, oni obuhvaćaju najčešće kontrolu pristupa i prisutnosti u hotelskim smještajnim jedinicama, alarmne sustave u kupaonicama, sobama i zajedničkim hotelskim prostorima. To znači da je za instalaciju i implementaciju sustava sigurnosti nužno imati stručne ljude, koji će u određenom organizacijskom obliku operativno i pomoću suvremenih tehničkih dostignuća zaštite obavljati te aktivnosti.

Različitim tehničko-tehnološkim rješenjima sigurnosnih hotelskih sustava pospješuje se provedba sigurnosnih mjera i povećava razina sigurnosti i zaštite u hotelskim objektima.

Nažalost, neka istraživanja su pokazala da unatoč činjenici da je svijest o sigurnosti postepeno u porastu, neki poduzetnici još uvijek u tehničku i informacijsku sigurnost prije svega ulažu onoliko koliko je to zakonom propisano ne bi li se zadovoljila neka norma.

Razvoj tehnologije je uzročno-posljedičnom vezom pridonio i razvoju sve sofisticiranijih i kreativnih metoda i alata kojim se zlonamjerni korisnici danas mogu poslužiti ne bi li postigli svoje maliciozne nakane. Na primjer, stručnjaci za sigurnost upozoravaju da je na porastu korištenje QR koda kojim se navodi na zlonamjernu web stranicu te tako na inovativan način koji pod iluzijom legitimnosti i sigurnosti varaju korisnike, dodajmo tome činjenicu da se QR kod skenira mobilnim uređajem koji ima manji display čime je otežanije iščitavanje ime stranice, dobili smo potencijalno veliki problem.

Daljnjim razvojem umjetne inteligencije također sa sobom nosi mogućnost stvaranja još gramatički točnijih phishing mailova koji stvaraju povećaniji osjećaj kredibilnosti i vjerodostojnosti. Stoga hotelska poduzeća kao jedni od prominentnih pružatelja usluga smještaja u turističkoj sferi, da bi podigli osjećaj sigurnosti svojih djelatnika i gostiju na željeni nivo, moraju biti ažurna po pitanju implementacije sigurnosnih sustava, kao i edukaciju o istima.

Valjalo bi pratiti trendove i razvijati svijest o korporativnoj sigurnosti ne bi li se postigla željena simbioza naprednih sigurnosno-tehnoloških alata, uredbi te sigurnosnih propisa sa faktorom čovjeka. Čovjek kao takav je podložan greškama i nasjedanjima na sve kreativnije i sofisticiranije metode narušavanja privatnosti u sklopu postizanja raznih zlonamjernih agenda.

I za kraj, jačina sigurnosti ovisi o tome koliko je zapravo slaba njezina najslabija i najlabilnija karika.

Bibliografija

1. Baker, S., Bradley, P., Huyton, J., 2001., *Principles of Hotel Front Office Operations*, Cengage Learning, 2. izdanje.
2. Cerović Z., 2010., *Hotelski menadžment,* Fakultet za turistički i hotelski menadžment, Opatija.
3. Delišimunović, D., 2006., *Management zaštite i sigurnosti*, Pragmatekh, Zagreb.
4. Delišimunović, D., 2002., *Suvremeni koncepti i uređaji zaštite*, I.T. Graf d.o.o., Zagreb
5. Garbin Praničević, D., Pivčević, S., Garača, Ž., 2010., *Razvijenost informacijskih sustava velikih hotelskih poduzeća u Hrvatskoj*, Acta Turistica Nova, Vol. 4, str. 175-199, https://hrcak.srce.hr/file/157737 (pristupljeno 24. kolovoza 2023.)
6. http://www.tehnoservis.net/protuprovalni-protuprepadni-sustavi-usluge-2.html (pristupano 02. rujna 2023.)
7. https://hr.safetydetectives.com/blog/sto-je-ddos-napad-i-kako-ga-sprijeciti/ (pristupano 04. rujna 2023.)
8. Huth, A., Orlando, M., Pesante, L., 2012., *Password security, protection, and management*, United States Computer Emergency Readiness Team.
9. ISO/IEC 27001:2022, Information security management systems https://www.iso.org/standard/27001
10. Klarić, I., 2007., *Načini zlouporabe ranjivosti računalnog sustava*, Seminar, Fakultet elektrotehnike i računarstva, Zagreb.
11. Laušić, M., Petar, S., 2010., *Sigurnosne procedure u hotelima*, Acta Turistica Nova, Vol. 4, str. 201-218. https://hrcak.srce.hr/file/157738 (pristupljeno 24. kolovoza 2023.)
12. Petar, S., Perkov, D., 2008*., Utjecaj menadžmenta u stvaranju i rješavanju kriznih situacija u tvrtkama*, zbornik radova s III. znanstveno-stručne konferencije s međunarodnim sudjelovanjem Menadžment i sigurnost, Hrvatsko društvo inženjera sigurnosti, Čakovec, str. 512-517.
13. Pravilnik o uvjetima i načinu provedbe tehničke zaštite (NN 198/2003) https://narodne-novine.nn.hr/clanci/sluzbeni/2003_12_198_3163.html (pristupljeno 20. lipnja 2023.)
14. Pravilnik o zaštiti od požara ugostiteljskih objekata (NN 100/1999) https://narodne-novine.nn.hr/clanci/sluzbeni/1999_10_100_1665.html (pristupljeno 21. kolovoza 2023.)
15. Spremić, M., 2017., *Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije*, Sveučilište u Zagrebu, Ekonomski fakultet, Zagreb

16. Spremić, M., Šimunic, A., 2018., *Cyber security challenges in digital economy*, Proceedings of the World Congress on Engineering, International Association of Engineers, Hong Kong, str. 341-346
17. Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ https://www.zakon.hr/z/3112/Op%C4%87a-uredba-o-za%C5%A1titi-podataka---Uredba-%28EU%29-2016-679- (pristupano 28. kolovoza 2023.)
18. Zakon o privatnoj zaštiti (NN 68/2003) https://narodne-novine.nn.hr/clanci/sluzbeni/2003_04_68_796.html (pristupano 02. rujna 2023.)

Popis slika:

Popis tablica: