Informacijska sigurnost hotelskog poslovanja

Macuka, Nina

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

NINA MACUKA

INFORMACIJSKA SIGURNOST HOTELSKOG POSLOVANJA

Diplomski rad

Pula, 2024.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

NINA MACUKA

INFORMACIJSKA SIGURNOST HOTELSKOG POSLOVANJA

Diplomski rad

JMBAG: 0303057320, redoviti student

Studijski smjer: Informatički menadžment

Predmet: Umjetna Inteligencija

Znanstveno područje: Društvene znanosti
Znanstveno polje: Ekonomija
Znanstvena grana: Poslovna Informatika
Mentor: prof. dr. sc. Branimir Dukić
Sumentor: izv. prof. dr. sc. Danijela Rabar

Pula, rujan 2024.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za magistra ekonomije/poslovne ekonomije ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student

_____

U Puli, _____, _____ godine.

IZJAVA

o korištenju autorskog djela

Ja, _____ dajem odobrenje Sveučilištu Jurja Dobrile

u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom _____

_____

_____ koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, _____ (datum)

Potpis

_____

SAŽETAK

Poslovanje se hotela temelji na točnosti podataka i pravodobnom informiranju. To je u domeni rada hotelskog informacijskog sustava. Zbog toga je od ključnog interesa svakog hotela da njegov informacijski sustav bude točan, pravovremen, ekonomičan i da kontinuirano funkcionira. Da bi se to ostvarilo bitna je informacijska sigurnost hotelskog sustava. Zbog važnosti sigurnosti informacijskog sustava u hotelima, provedeno je istraživanje kojim se željela utvrditi spremnost hrvatskih hotelskih poslovnih sustava da rad vlastitih informacijskih sustava podignu na razinu koja odgovara najvišim standardima informacijske sigurnosti postavljene od strane struke. Desk su istraživanjima utvrđene značajke hotelskih informacijskih sustava, posebice dimenzija sigurnosti. Fokus je bio na vrstama ugroza kao i normama koje se koriste u prevenciji i otklanjanju potencijalnih i stvarnih ugroza. Sagledan je i zakonodavni okvir kao i organizacije koje se u Republici Hrvatskoj bave sigurnošću informacijskih sustava. Empirijsko je istraživanje anketiranjem predstavnika hotela ukazalo kako hotelski sustavi u Republici Hrvatskoj raspolažu informacijskim sustavima, svjesni su značaja informacijskih sustava, stoga vode brigu o sigurnosti vlastitih informacijskih sustava. To podrazumijeva da su implementirani određeni alati za zaštitu od ugroza i protokoli za slučaj ugroza sigurnosti informacijskih sustava. Evidentna je i briga o znanjima zaposlenih. Neki se hoteli s problemom ugroze nose samostalno, dok drugi brigu o sigurnosti informacijskih sustava prepuštaju drugim, specijaliziranim poslovnim subjektima. Istraživanja su pokazala kako su se hoteli susretali s ugrozama informacijske sigurnosti. Generalno se može zaključiti kako stanje u hotelima, vezano za sigurnosni aspekt hotelskih informacijskih sustava nije loše, no postoji i značajan prostor za daljnja poboljšanja.

Ključne riječi: Hotel, informacijski sustav, informacijsko-komunikacijska sigurnost, standardi sigurnosti

ABSTRACT

The operation of a hotel relies on the accuracy of data and timely information, which falls under the domain of the hotels information system. Therefore, it is of critical interest for every hotel that its information system is accurate, timely, economical, and continuously operational. To achieve this, the information security of the hotel system is essential. Due to the importance of information system security in hotels, a study was conducted to assess the readiness of Croatian hotel business systems to elevate the operation of their information systems to a level that meets the highest information security standards set by the industry. Desk research identified the characteristics of hotel information systems, particularly focusing on the security dimension. The study concentrated on the types of threats as well as the standards used in the prevention and mitigation of potential and actual threats. The legislative framework was also examined, along with organizations in the Republic of Croatia that deal with information system security. The empirical research, conducted through surveys of hotel representatives, revealed that hotels in the Republic of Croatia are equipped with information systems and are aware of their significance, thus taking care of their information system security. This includes the implementation of certain tools for threat protection and protocols for handling information system security breaches. There is also a clear focus on the knowledge and skills of employees. Some hotels manage security threats independently, while others delegate the responsibility for information system security to specialized external business entities. The research indicated that hotels have encountered information security threats. In general, it can be concluded that the state of hotel information system security is not bad, but there is significant room for further improvement.

Key words: Hotel, information system, information and communication security, security standards

SADRŽAJ

1 Uvod

U proteklih je tridesetak godina informacijsko-komunikacijska tehnologija znatno napredovala i u pogledu mogućnosti i u pogledu brzina prijenosa podataka te u pogledu količine prenesenih podataka. Podaci su sirovina u procesu kreiranja informacija i znanja. Suvremeni menadžment uspostavlja odnos između kvalitete i pravodobnosti informacija te kvalitete donesenih odluka. Naime, pravodobne i kvalitetne informacije u pravilu rezultiraju pravodobnom i kvalitetnom poslovnom odlukom. Prema tome postoji jasna uzročno posljedična veza između sposobnosti i kvalitete informacijsko-komunikacijske tehnologije s jedne strane te uspješnosti rada menadžmenta, a kroz to i poslovanja s druge strane. Zbog toga poslovni subjekti ulažu u informacijsko-komunikacijsku tehnologiju kako bi osigurali vlastiti opstanak kroz uspješno poslovanje. O važnosti informacija, odnosno informacijsko-komunikacijske tehnologije govori i činjenica da se suvremeno doba uobičajeno naziva i informacijskim dobom. Onaj poslovni subjekt koji je informacijski superioran taj je u boljoj poziciji od onog poslovnog subjekta koji je informacijski inferioran. Stoga u mnogim djelatnostima, osim tržišne utakmice koja se odnosi na cijenu i kvalitetu proizvoda, vodi se i utakmica kojom se pokušava osigurati informacijska superiornost nad konkurencijom. Informacijska superiornost, osim u procesu donošenja odluka, ostvaruje se i u domeni optimalnog pružanja informacija potrošačima o proizvodu i u pogledu kvalitete informacija i u pogledu količine informacija, ali i u pogledu prilagođenosti informacija samom potrošaču. Kako bi se osigurala vrsta informacijske superiornosti nužno je permanentno prikupljati informacije, ne samo o vlastitom poslovanju, već i o potrebama potrošača, stanju konkurencije, zakonodavnom okviru, kao i o drugim bitnim čimbenicima koji pomažu menadžmentu sagledati situaciju i poziciju poslovnog subjekta, kao i mogućnosti optimizacije poslovanja.

Primjerice, kada se radi o hotelskom poslovnom subjektu, temeljem iskustva, svakome je jasno, da bez prenošenja informacija o vlastitoj ponudi, bez znanja o zakonodavnim okvirima poslovanja, kvalitetnog predviđanja kriznih situacija (bolesti, ratova i drugo),

bez saznanja o ciljanim informacijama koje potencijalne goste zanimaju i temeljem kojih se može ostvariti konkurentska prednost i drugog, nije moguće u suvremenim uvjetima optimalno poslovati. Zbog toga su informacijski sustavi, kako svih poslovnih subjekata, tako i hotelskih kuća temelj na kojem se izgrađuje uspješno poslovanje. No, raspad informacijskog sustava, posebice zbog zlonamjernih napada, može imati izuzetno negativne reperkusije na poslovanje, a time i opstanak poslovnog subjekta. Još veći problem može izazvati krađa podataka i javno otkrivanje jalovosti informacijskog sustava hotelskog sustava. Zbog toga je bitno baviti se sustavno problemom informacijske sigurnosti u hotelskim poslovnim subjektima.

Polazeći od ovog problema, načinjeno je istraživanje kako bi se utvrdili aspekti sigurnosti hotelskih poslovnih sustava te sagledali stavovi u hotelskim sustavima koji se odnose na informacijsku sigurnost hotelskih sustava. Rezultati su provedenih istraživanja predstavljeni ovim diplomskim radom.

2 Metodologija istraživanja

S obzirom na pozitivne zakonske propise i obveze formalizacije unutrašnjih tijekova informiranja te poslovnog izvješćivanja države, svaki poslovni subjekt, pa prema tome i svaki hotel, bilo da se radi o malom obiteljskom hotelu ili pak o hotelskom lancu, posjeduje poslovni informacijski sustav. Nekada su, otprilike do prije četrdesetak godina, poslovni informacijski sustavi svoje djelovanje temeljili na manualnoj, ali i mehaničkoj i/ili elektromehaničkoj obradi podataka, dok se danas u obradi podataka poslovni informacijski sustavi koriste suvremenom informacijsko- komunikacijskom tehnologijom. Mnogi laici, koji ne razumiju pojam poslovnih informacijskih sustava, poslovne informacijske sustave ne prepoznaju jer u mnogim poslovnim sustavima nisu funkcijski organizirani i/ili ne nose naziv informacijskog sustava. No, činjenica je da svaki poslovni sustav, koji djeluje u okviru bijele ekonomije, posjeduje poslovni informacijski sustav. Hotelski poslovni informacijski sustavi, osim standardnog računovodstvenog informacijskog podsustava i eventualno drugih informacijskih podsustava koji se susreću i u drugim poslovnim subjektima (marketing-informacijski sustav, informacijski podsustav ljudskih potencijala i drugo) imaju i sustave informiranja koji se odnose na praćenja rezervacija i prijavu gostiju, raspoloživost slobodnih smještajnih kapaciteta i drugo. Kao što je već navedeno, u prošlosti se sustav informiranja u hotelima temeljio na ručnom (manualnom) radu i papirnoj evidenciji, dok se od početka široke primjene računala u poslovnoj praksi, obrada podataka obavlja uz pomoć računala i odgovarajućih programa. Kako se, poput svih poslovnih sustava, poslovanje hotela temelji na točnosti podataka i pravodobnom informiranju, od krucijalnog je interesa svakog poslovnog sustava, tako i hotelskog, da informacijski sustav bude točan, pravovremen, ekonomičan i da kontinuirano funkcionira. Da bi se to ostvarilo bitna je informacijska sigurnost hotelskog sustava. Zbog važnosti aspekta informacijske sigurnosti hotelskog sustava, odnosno zbog važnosti sigurnosti informacijskog sustava u hotelima, provedeno je istraživanje kojim se željela utvrditi spremnost hrvatskih hotelskih poslovnih sustava da rad vlastitih informacijskih sustava

podignu na razinu koja odgovara najvišim standardima informacijske sigurnosti postavljene od strane struke.

Radi donošenja konačnog zaključka o stanju sigurnosti u hrvatskim hotelskim poslovnim sustavim, empirijskim se istraživanjem nastojalo dokazati sljedeću hipotezu:

H0: Sigurnost informacijskih sustava u hrvatskim hotelskim poslovnim subjektima zadovoljava sigurnosne standarde struke.

Temeljem postavljene početne hipoteze definirani su sljedeći ciljevi istraživanja:

1. desk istraživanjem raspoložive literature definirati pojam poslovnog informacijskog sustava,

2. desk istraživanjem raspoložive literature sagledati ulogu poslovnog informacijskog sustava u hotelskim poslovnim subjektima,

3. desk istraživanjima raspoložive literature sagledati pojam informacijske sigurnosti s aspekta hotelskih sustava,

4. empirijskim (primarnim) istraživanjem sagledati stanje informacijske sigurnosti hotelskih sustava te utvrditi spremnost hrvatskih hotelskih poslovnih sustava da rad vlastitih informacijskih sustava podignu na razinu koja odgovara najvišim standardima informacijske sigurnosti,

5. empirijskim (primarnim) istraživanjima sagledati stavove eksperata za informacijsko- komunikacijsku sigurnost glede načina očuvanja sigurnosti hotelskih informacijskih sustava.

Za dokazivanje/odbacivanje je početne hipoteze upotrjebljena metoda dedukcije. Za ostvarivanje prva tri cilja istraživanja korištena je desk metoda, dok je za ostvarenje

četvrtog cilja istraživanja korištena metoda anketiranja, a petog cilja istraživanja dubinski intervju. Podaci su prikupljeni anketiranjem obrađeni statističkim metodama (deskriptivna statistika). Osim navedenih znanstvenih metoda u istraživanju su korištene i metoda apstrakcije, metoda klasifikacije, metoda analize, metoda sinteze, metoda generalizacije, metoda kompozicije, metoda kauzalnog zaključivanja, metoda deskriptivnog modeliranja, povijesna metoda, kao i druge znanstvene metode.

3 Informacijski sustavi: teorijska pozadina

Prema Hrvatskoj enciklopediji informacijski je sustav: „organizirani skup postupaka kojima se prikupljaju, obrađuju, spremaju, pretražuju i prikazuju podatci i informacije značajni za neku organizaciju, ustanovu, društvo ili državu. Sastavni je dio informacijskoga sustava i osoblje obrazovano za rad u sustavu te odgovarajuća oprema. Današnji se informacijski sustavi pretežito ostvaruju uz pomoć suvremene informacijske i komunikacijske tehnologije. Posebno je značajna uporaba informacijskih sustava unutar poslovnih sustava, gdje služe za njihovo upravljanje i kao potpora izvođenju poslovnih procesa. Osnovne su komponente takva informacijskog sustava: sustav za obradbu transakcija, upravljački izvještajni sustav ili upravljački informacijski sustav, sustav za potporu odlučivanju i sustav uredskoga poslovanja. Podatci i informacije unutar informacijskoga sustava danas se najčešće pohranjuju i čuvaju u bazama podataka.“[1] Sličan je pristup u definiranju pojma informacijskog sustava onaj koji smatra da su temeljne funkcije svakog informacijskog sustava prikupljanje, obrada, čuvanje i razdioba informacija svim članovima neke organizacije koji se njima žele koristiti uz odgovarajuću autorizaciju. Prema tome, osnovna je funkcija informacijskog sustava opskrba potrebnim informacijama svih razina upravljanja i odlučivanja u danom tehnološkom, odnosno organizacijskom obliku.[2]

Informacijski su sustavi sastavnica i hotelskih poslovnih sustava. Iskustveno se može konstatirati kako je danas nezamislivo funkcioniranje hotelskih poslovnih informacijskih sustava bez upotrebe suvremene informacijsko-komunikacijske tehnologije.

[1] Informacijski sustav, Hrvatska enciklopedija, mrežno izdanje, Leksikografski zavod Miroslav Krleža, https://www.enciklopedija.hr/clanak/informacijski-sustav [pritupljeno 18.6.2024]

[2] Informacijski sustavi, fpz, https://www.fpz.unizg.hr/ztos/iszp/a2.pdf [pristupljeno 24.4.2023]

Tri su glavna vala tehnološkog razvoja uvodila informacijsko-komunikacijsku tehnologiju u poslovanje hotelskih sustava:[3]

1. kompjutorski rezervacijski sustavi (Computer Reservation Systems - CRS) 70-ih godina,
2. globalni distribucijski sustavi (Global Distribution Systems - GDS) 80-ih godina te
3. internet 90-ih godina proteklog stoljeća

Svaki informacijski sustav treba imati 6 komponenti:[4]

1. hardware – materijalna osnova, sastoji se od: elektroničkog računala, ulazno izlaznih uređaja, dijela uređaja za komuniciranje i prijenos i ostale računalne elektronike namijenjene isključivo ili pretežito obradi podataka,
2. software čini nematerijalne elemente, kao što su npr. programi, uvježbanost i metode vezane uz organizaciju, upravljanje, obrađivanje i korištenje rezultata obrade,
3. netware čini mješovitu materijalno-tehničku i nematerijalnu komponentu koja omogućuje komuniciranje unutar mreže,
4. lifeware je ljudska komponentna koju čine ljudski potencijali,
5. orgware čine organizacijski postupci, metode i načini povezivanja i usklađivanja prethodnih komponentni u cjelinu,
6. dataware je zadužena za organizaciju baze podataka i informacijskih resursa.

[3] V. Galičić i M. Šimunić, Informacijski sustavi i elektroničko poslovanje u turizmu i hotelijerstvu, Sveučilište u Rijeci, Fakultet za turistički i hotelski menadžment u Opatiji, Opatija, 2006., str.110.

[4] V. Strahonja, M. Varga i M. Pavlić, Projektiranje informacijskih sustava, Zavod za informatičku djelatnost Hvatske i INA-INFO, Zagreb, 1992., str.18.

Da bi svaki informacijski sustav bio uspješan u svom radu vrlo je bitno da sve navedene komponente budu podjednake i usklađene u radu. Informacijski sustav je zapravo podsustav poslovnog sustava. Poslovni sustav je taj koji generira podatke te ih dostavlja do unutarnjih i/ili vanjskih jedinica informacijskog sustava koje onda podatke prosljeđuju centralnom dijelu informacijskog sustava koji se bavi obradom prikupljenih podataka. Rezultat obrade podataka su informacije ili znanje. Menadžment upotrebljava njemu korisne podatke kako bi temeljem modela odlučivanja (znanja) generirao informacije koje su mjera u donošenju poslovnih odluka. Složenost je i veličina poslovnog informacijskog sustava proporcionalna veličini poslovne organizacije, no složenost poslovnog informacijskog sustava ovisi i o vrsti poslovanja kojom se određena poslovna organizacija bavi. Informacijski sustav kao cjelina može biti vrlo složen stoga se uobičajeno, radi rješavanja organizacijskih problema, dijeli na podsustave i elemente. Razlikuju se statični i dinamični informacijski sustavi. Statični informacijski sustavi opisuju potrebne entitete i njihova svojstva dok dinamični informacijski sustavi opisuju ponašanja elemenata i podsustava te promjene njihova stanja i međusobnu uvjetovanost. Danas su u pravilu poslovni informacijski sustavi dinamični sustavi. Prilikom modeliranja dinamičnih informacijskih sustava analiziraju se i strukturiraju poslovni procesi. Čimbenici su za modeliranje poslovnih procesa: akteri, izvršitelji (zaposlenici u poslovnim procesima), aktivnosti, entiteti (objekti koji su relevantni za poslovni proces), tijek (međusobna ovisnost) procesa, organizacijske cjeline te način i komunikacija aktera i izvršilaca tijekom procesa.[5]

[5] J. Mesarić, Informacijski sustavi u poslovanju - ciljevi, zadaci i izgradnja informacijskih sustava, prezentacija, Ekonomski fakultet u Osijeku, Osijek, 2015, http://www.efos.unios.hr/informatika/wp-content/uploads/sites/202/2013/04/P11_Info_sustavi.pdf [pristupljeno 24.4.2023]

Model informacijskog sustava sastoji se od:[6]

• modela podataka - definiranje podataka u informacijskom sustavu kojima se opisuju stvarni elementi poslovnog sustava (npr. proizvod se opisuje nazivom, cijenom, jed. mjere, itd.)

• modela procesa (ili modela funkcija) - opisuje procese i funkcije kojima se mijenjaju podaci (npr. ispis računa, izračun prodajne cijene, obračun kamata itd.)

• modela izvršitelja (resursa) - opisuje tehničku opremu (hardware), programsku opremu (software), ljude izvršitelje (lifeware) i organizaciju svih elemenata u cjelinu (orgware)

U današnje vrijeme postoje različiti informacijski sustavi koji su potrebni menadžmentu poduzeća za donošenje novih poslovnih odluka te praćenju same produktivnosti svojih zaposlenika i ostvarivanju postavljenih ciljeva i zadataka, tako razlikujemo:[7]

- izvršni sustavi podrške – zamišljeni su kako bi pomogli menadžmentu donošenju poslovnih odluka,
- upravljački informacijski sustavi – u većini vremena se bavi unutarnjim izvorima informacija,
- sustavi za podršku u odlučivanju – glavni cilj im je pomoći u donošenju odluka u konkretnim situacijama,
- sustavi upravljanja znanjem – glavna zadaća im je stvaranje i razmjena različitih informacija,
- sustavi za obradu transakcija – dizajnirani za učinkovitu i točnu obradu ponavljajućih transakcija,

[6] Ibid

[7] D. Barišić, Poslovni informacijski sustavi kao temelj današnjeg poslovanja, završni rad, Ekonomski fakultet u Osijeku, Osijek, 2021., str. 6., prema: Riley, J.: ICT: types of infomation., 2018, https://www.tutor2u.net/business/reference/ict-types-of-information [pristupljeno 12.8.2020]

- sustavi za automatizaciju rada – poboljšavaju učinkovitost zaposlenika koji trebaju obraditi podatke i informacije.

Iz prethodnih je razmatranja jasno kako poslovni sustavi posjeduju zajednički skup podsustava koji su vezani za praćenje promjena na strukturi poslovnog subjekta te za praćenje događaja koji mijenjaju poslovnu strukturu, a kroz to i poslovnih procesa, ali i skup podsustava poslovnog informacijskog sustava koji su specifični za pojedinu djelatnost, pa čak i za pojedini poslovni subjekt. Prema tome, može se zaključiti da informacijski sustav hotelskog poslovnog subjekta integrira standardne elemente poslovnog informacijskog sustava koji su pojačani onim elementima, odnosno podsustavima informacijskog sustava koji su specifični za hotelske sustave. Hotelski sustavi u Republici Hrvatskoj, zbog specifičnosti hrvatskog zakonodavnog okvira, imaju elemente koji su specifični i koriste se isključivo u poslovanju na teritoriju Republike Hrvatske. Primjerice, jedna je od takvih specifičnosti način i format prijave stranih gostiju Ministarstvu unutarnjih poslova (policiji).

4 Razvijenost hotelskog informacijskog sustava

Primjena suvremene informacijsko-komunikacijske tehnologije u radu hotelskih informacijskih sustava, kao što je vidljivo iz dosadašnjih razmatranja, pojednostavljuje svakodnevne aktivnosti vezane za obradu podataka, ubrzava procedure vezane za evidentiranje promjena na poslovnoj strukturi i poslovnih događaja, smanjuje, pa čak i otklanja mogućnost greške, smanjuje obujam ručne obrade i drugo. Danas se općenito smatra, na što ukazuju iskustva, kako je razvijenost hotelskog informacijskog sustava proporcionalna obujmu i načinu primjene najsuvremenije informacijsko-komunikacijske tehnologije u radu hotelskog informacijskog sustava.

4.1 Karakteristike informatizacije hotelskog poslovanja

Uspješnost je poslovanja hotela u korelaciji s razinom usluga koja pruža svojim gostima. Zaostajanje se u tehnološkom razvitku hotela uobičajeno reflektira na pad konkurentske sposobnosti hotela. No, ne smije se tehnološki razvitak stavljati isključivo u korelaciju s osuvremenjivanjem opreme. Oprema je bitna, no značajno je bitnije od osuvremenjivanja opreme educirati ljudske potencijale, jer su znanja i vještine ljudi temeljni nositelj tehnološkog razvitka. Za racionalnu primjenu i razvoj informacijsko-komunikacijske tehnologije u turističko-hotelskim poslovnim subjektima, neophodno je zadovoljiti više preduvjeta, a prije svega:[8]

- uočiti potrebu za primjenom informacijske tehnologije,
- planirati izgradnju i razvoj poslovnog sustava u cjelini, na osnovama primjene informacijske tehnologije,
- standardizirati opremu, dokumentaciju i metode korištenja informacijske tehnologije,

[8] V.Galičić i M. Šimunić, op. cit., str. 98.

- organizirati proces upravljanja i rukovođenja uvjetima primjene informacijske tehnologije.

Razloge zbog kojih su se turizam i hotelijerstvo nešto kasnije uključili u proces primjene informacijske tehnologije od ostalih djelatnosti, ima više, a najvažniji se mogu pronaći u[9]:

- pasivnosti upravljačkih ljudskih potencijala,
- niskoj razini stručnosti ljudskih potencijala,
- tradicionalnom otporu prema svemu onome što je novo,
- pomanjkanju sredstava za nabavu hardwarea i softwarea,
- izostajanju ponuda domaćih proizvođača elektronske opreme kompatibilne za informacijske sustave u toj izrazito uslužnoj djelatnosti.

Razlozi koji su stimulirali hotelska poduzeća da krenu u proces informatizacije ogledaju se kroz ciljeve poslovanja, koji se mogu svesti pod sljedeće[10]:

- optimalno iskorištenje raspoloživih resursa (materijalnih, financijskih, ljudskih resursa);
- povećanje iskorištenja kapaciteta (smještajnih, konzumnih i ostalih);
- smanjenje rutinskih (repetitivnih) manualnih poslova;
- podizanje kvalitete pruženih usluga;
- omogućavanje uspješnije operativne kontrole;
- uspješnije upravljanje cjelokupnim poslovanjem i
- ostvarenje pozitivnog poslovnog rezultata

Temeljem iskustva može se konstatirati kako suvremeni hoteli za praćenje poslovanja koriste ERP programske sustave (engl. Enterprise Resource Planning). „Upravljanje resursima poduzeća (ERP) odnosi se na vrstu softvera koji organizacije upotrebljavaju za upravljanje svakodnevnim poslovnim aktivnostima kao što su računovodstvo,

[9] Ibid, str. 99.
[10] Ibid, str. 100.

nabava, upravljanje projektima, upravljanje rizikom i usklađenost te operacije opskrbnog lanca. Potpuni paket ERP-a uključuje i upravljanje poslovnim rezultatima, softver koji pomaže pri planiranju, budžetiranju, predviđanju financijskih rezultata organizacije i izvještavanju o njima. Sustavi ERP povezuju mnoštvo poslovnih procesa i omogućuju protok podataka između njih. Prikupljanjem zajedničkih transakcijskih podataka organizacije iz više izvora, sustavi ERP eliminiraju dupliciranje podataka i osiguravaju integritet podataka uz jedinstven izvor informacija. (…) Sustavi ERP dizajnirani su oko jedne definirane strukture podataka (shema) koja obično ima zajedničku bazu podataka. Time se osigurava da se podaci koji se upotrebljavaju u cijelom poduzeću normaliziraju i temelje na zajedničkim definicijama i korisničkim iskustvima. Te osnovne konstrukcije potom se povezuju s poslovnim procesima koje pokreću tijekovi rada u različitim poslovnim odjelima (npr. financije, ljudski potencijali, inženjerstvo, marketing i operacije), povezanim sustavima i korisnicima koji ih upotrebljavaju. ERP je jednostavno rješenje za integraciju korisnika, procesa i tehnologija u cijelom modernom poduzeću.“[11] Kod hotelske djelatnosti, što se može iskustveno dokazati, važan je čimbenik ERP sustava recepcijsko poslovanje. Na recepcijsko poslovanje uobičajeno se oslanja rezervacijski programski sustav. No, rezervacijski se programski sustav uobičajeno kombinira s Web stranicama hotelskog sustava koje omogućavaju komuniciranje s tržištem, kao promocijski alat. Uobičajeno se ERP sustavi nadograđuju s CRM sustavima (engl. Customer Relationship Management). „(…) upravljanje odnosima s klijentima je pristup upravljanju poslovnim subjektom kroz interakciju sa sadašnjim i budućim potrošačima. CRM pristup pokušava analizirati podatke kupaca i njegovu povijest s poslovnim subjektom, kako bi se poboljšali poslovni odnosi s klijentima/kupcima, s naglaskom na njihovo zadržavanje, a kako bi u konačnici ostvarili rast prodaje.“[12]

[11] Upravljanje resursima poduzeća, Oracle, https://www.oracle.com/hr/erp/what-is-erp/ [pristupljeno 5.9.2024]
[12] Što je CRM i što se iza njega krije, Poslovna.hr, https://www.poslovni.hr/lifestyle/sto-je-crm-i-sto-se-iza-njega- krije-307951 [pristupljeno 5.9.2024]

4.2 Definiranje razina razvijenosti hotelskog informacijskog sustava

Razvijenost se informacijskih sustava hotelskog poslovnog subjekta može klasificirati temeljem modela zrelosti koji diferencira tri razine razvijenosti informacijskog sustava:[13]

1. razina razvijenosti - informacijski sustav ima ulogu tehnološkog partnera poslovanja, odnosno podrška je dokumentacijskoj funkciji poslovnog sustava. Komponentne informacijskog sustava najniže razine služe za automatsku obradu podataka. Strojna i programska se komponenta rijetko unaprjeđuju (ciklus unaprjeđenja je veći od 5 godina), podaci su pohranjeni na više mjesta što otežava pristup različitim odjelima unutar samog poslovnog subjekta, a računala su međusobno nepovezana u mrežu. Što se tiče sigurnosti informacijskih sustava nisu poduzete odgovarajuće mjere zaštite podataka, a podatcima se ne može pristupiti kontinuirano. Pouzdanost potrebnih informacija ne omogućava oslanjanje na dobivene informacije bez dodatnih provjera i dopuna, te takve informacije mogu pružiti samo operativnu podršku upravljanju hotelskim poslovnim subjektom.

2. razina razvijenosti - informacijski sustav ima ulogu procesnog i servisnog partnera u poslovanju, te djeluje kao integralni sustav za podršku svim funkcijama poslovnog sustava. Na ovoj razini ostvaruje se veća uključenost mrežne komponentne, te se ova razina može promatrati kao srednja razina razvijenosti gdje se hardverska i softverska komponenta obnavljaju svakih 3 do 5 godina. Podaci se pohranjuju na jednoj zajedničkoj bazi sa serverom na mreži, a koriste se i vanjski podaci s Web servera ili nekog od vanjskih izvora podataka. Pristup informacijama unutar hotela odvija se s umreženih računala povezanih lokalnom mrežom. Sigurnost informacijskih sustava povremeno zadovoljava korisnike sustava, kao i mogućnosti dostupnosti podataka korisnicima sustava. Dobivene informacije iz sustava mogu se smatrati pouzdanima, što

[13] Praničević Garbin, D., S. Pivčević,i Ž. Garača: *Razvijenost informacijskih sustava velikih hotelskih poduzeća u Hrvatskoj*, Acta turistica nova, Vol. 4, No. 2/2010., str. 183.

nižem i srednjem menadžmentu lakše omogućava donošenje novih poslovnih ciljeva dok strateškom menadžmentu ne pomaže u onoj mjeri u kojoj bi to zahtijevalo.

3. razina razvijenosti - informacijski sustav ima ulogu strateškog partnera u poslovanju. Strojna i programska se komponenta unaprjeđuju u razdoblju ispod 3 godine, podaci se pohranjuju na više međusobno povezanih lokalnih mreža. Djelatnici hotelskog poslovnog sustava na ovoj razini razvijenosti trebali bi znati i htjeti primjenjivati kreativna poboljšanja na svom radnom mjestu. Što se tiče same sigurnosti informacijskog sustava, poduzete su sve mjere zaštite podataka od neovlaštenog korištenja, a podaci su prema prethodno određenim ovlastima dostupni kontinuirano, na zahtjev. Integralnost sustava je kompletna, te pouzdanost informacijskih tijekova unutar poslovnog subjekta. Sve su informacije, po svim stupnjevima agregiranosti, u mogućnosti podržati svaku od menadžerskih razina.

4.3 Sigurnost hotelskog poslovanja

Sigurnost hotelskog poslovanja igra važnu ulogu kako bi se osiguralo zadovoljstvo gostiju, zaštita imovine i održavanja ugleda hotela. Ključne točke za sigurnije hotelsko poslovanje:[14]

1. zaštita osobnih podataka – hoteli često prikupljaju osjetljive osobne podatke o svojim gostima, kao što su brojevi kreditnih kartica i osobni dokumenti, stoga je nužno da se pridržavaju stroge politike zaštite osobnih podataka kako bi se izbjegle povrede privatnosti,
2. cyber sigurnost – s obzirom na to da se sve više hotelskog poslovanja obavlja putem Interneta, važno je zaštititi hotelske sustave od kibernetičkih napada i osigurati sigurnost računalnih mrežnih transakcija,

[14] V. Galičić: *Poslovanje hotelskog odjela smještaja*, Sveučilište u Rijeci, Fakultet za menadžment u turizmu i ugostiteljstvu u Opatiji, Opatija, 2017., str. 353 - 390

3. fizička sigurnost – sigurnost informacija nije ograničena na digitalne aspekte, stoga hoteli trebaju imati stroge kontrole pristupa kako bi se osiguralo da samo gosti i ovlašteno osoblje mogu ući u hotelske prostorije, potom video nadzor na ključnim mjestima kako bi se pratila aktivnost i identificirali eventualni problemi kao i sigurnosno osoblje koje čuva imovinu hotela i brine o fizičkoj sigurnosti gostiju,
4. obuka osoblja - osoblje hotela treba biti obučeno za postupanje u hitnim situacijama, prepoznavanje sumnjivih situacija te za pružanje pomoći gostima,
5. sigurnost hrane i pića - hoteli moraju pažljivo pratiti kvalitetu hrane i pića koje služe svojim gostima kako bi se izbjegla trovanja, bolesti i alergijske reakcije,
6. protupožarna sigurnost - hotelima je potrebna dobra protupožarna oprema i planovi evakuacije kako bi se osigurala sigurnost gostiju u slučaju požara,
7. prevencija krađa i prevara - hotelsko osoblje treba biti obučeno za prepoznavanje sumnjivih aktivnosti i ponašanja gostiju za spriječavanje krađe i postupaka prevare,
8. krizni menadžment - hoteli bi trebali imati planove za krizni menadžment kako bi se brzo i efikasno reagiralo na nepredviđene situacije poput prirodnih katastrofa, terorističkih napada ili ozbiljnih zdravstvenih kriza,
9. zaštita imovine - osim sigurnosti gostiju, hotelski objekti također moraju zaštititi svoju imovinu, uključujući inventar, opremu i pomoćne objekte.

Kao što je iz prethodnog nabrajanja vidljivo, sigurnost je u hotelskom poslovanju kompleksno multidisciplinarno područje. Ono zahtijeva pažnju prema detaljima, suradnju s relevantnim eksternim čimbenicima (javna uprava, policija, vatrogasci, zdravstvo i drugo) i kontinuirano unaprjeđenje sigurnosnih protokola kako bi se osigurao siguran rad hotelskog sustava. Velik je broj elemenata sigurnosti, što je također vidljivo iz prethodnog nabrajanja, izravno ili neizravno povezan sa efikasnosti rada i sigurnosti informacijskog sustava hotelskog poslovnog subjekta.

5 Sigurnost informacijskih sustava hotelskih poslovnih subjekata

Da bi se moglo govoriti o sigurnosti informacijskih sustava hotelskih poslovnih subjekata potrebno je sagledati standarde sigurnosti i zakonsku regulativu koja se odnosi na sigurnost informacijskih sustava hotelskih poslovnih subjekata. Nadalje, potrebno je identificirati rizike hotelskog informacijskog sustava te se pozabaviti najčešćim sigurnosnim prijetnjama koje se pojavljuju kod hotelskih informacijskih sustava.

5.1 Standardi i zakonska regulativa

Postoje brojni svjetski standardi koji se primjenjuju u određenom području hotelskog poslovanja. Također, hotelski se poslovni subjekti u Republici Hrvatskoj moraju pridržavati pozitivne zakonske regulative vezane za rad i sigurnost hotelskih poslovnih subjekata.

5.1.1 ISO norme – serija 27000

Prije uvođenja ISO normi, u upotrebi je bila norma Britanska BS 7799 norma koju je definirao Britanski institut za standarde (engl. British Standard Institute - BSI). Ova se norma sastojala od nekoliko dijelova. Prvi je dio ove norme, koji se odnosio na upravljanje informacijskom sigurnošću, revidiran 1998. godine. ISO norma ga preuzela 2000. godine pod oznakom ISO/IEC 17799 te pod nazivom “Informacijska tehnologija: Kodeks prakse upravljanja sigurnošću informacija”. ISO/IEC 17799 norma je zatim revidirana u lipnju 2005. godine i uključena u ISO 27000 seriju normi kao ISO/IEC 27002. Drugi je dio norme, pod oznakom BS 7799, objavljen 1999. godine pod naslovom “Sustav upravljanja informacijskom sigurnošću”. Fokus je norme BS 7799-2 bio na implementaciji sustava upravljanja informacijskom sigurnošću. Kasnije je ta norma ažurirana kako bi pokrila analizu i upravljanje rizikom te je dobila oznaku ISO/IEC 27001:2005. Posljednja je objavljena verzija sustava upravljanja informacijskom sigurnošću (ISMS) norma BS EN ISO/IEC 27001: 2017.[15] Vezano uz informacijsku tehnologiju bitna je norma ISO/IEC 27001 koja se odnosi na informacijsku

[15] https://secureframe.com/hub/iso-27001/history [pristupljeno 23.9.2024]

sigurnost. Mnoga su zakonodavstva uzela taj standard kao temelj za pisanje vlastitih zakona kao što su zakoni o tajnosti podataka, direktive o zaštiti osobnih podataka, zakoni o zaštiti informacijskih sustava, zakoni o upravljanju operativnim rizicima u financijskim ustanovama i slično. Norma ISO 27001 pruža metodologiju za uvođenje informacijske sigurnosti u neku organizaciju. Ova norma prvenstvo služi za zaštitu povjerljivosti, cjelovitosti i integriteta podataka u poslovnim subjektima, a poznata je i kao CIA teorem. Temeljna je zadaća ove norme upravljanje rizicima kroz prepoznavanje i sustavnu obradu svakog rizičnog događaja. Norma predviđa postojanje tima stručnjaka unutar samog poslovnog subjekta koji će se baviti procjenom i identifikacijom sigurnosnih rizika. Nakon sastavljanja tima stručnjaka zaduženih za identifikaciju rizika, norma predviđa izradu plana djelovanja u kriznim situacijama u kojem se definiraju smjernice za procjenu rizika koji nosi pojedini štetni događaj.[16]

Procjena rizika se sastoji od nekoliko komponenti a to su:[17]

- imovina – sve što predstavlja vrijednost za poslovni subjekt,
- prijetnje – potrebna je analiza i identifikacija scenarija koji su nepoželjni ili mogu prouzročiti preveliku štetu poslovnoj organizaciji bez obzira radi li se o štetnim događajima koji su namjerno ili nenamjerno nastali,
- slabosti – otkrivanje događaja koji se mogu pojaviti na strojnom i/ili programskom dijelu sustava, odnosno pronalaženje onih dijelova sustava koji su najviše podložni prijetnjama,
- utjecaji – pronalaženje izvora prijetnji,
- vjerojatnost pojavljivanja – izračun vjerojatnosti pojavljivanja pojedinog štetnog događaja,
- posljedice – pronalaženje načina za optimalno otklanjanje posljedica štetnih događaja.

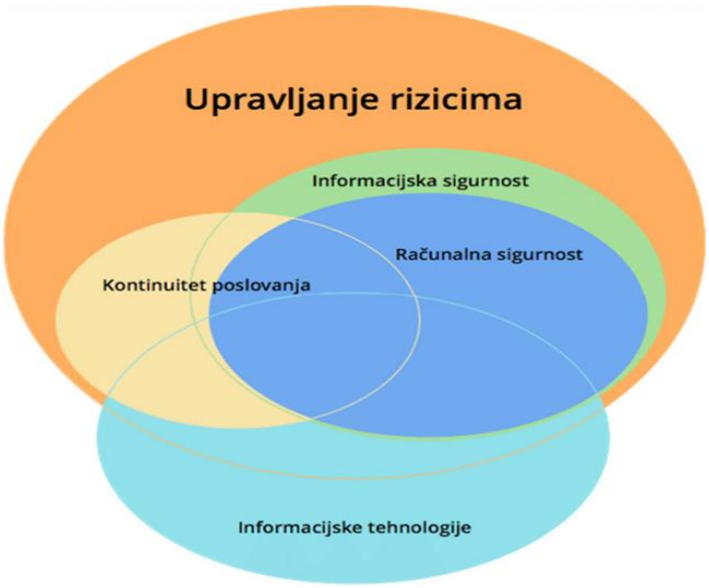
[16] Chopra, A. i M. Chaudhary: *Implementing an Information Security Management System*: Security Management Based on ISO 27001 Guidelines, Apress L.P., New York, 2020., str. 59-60.
[17] Ibid, str. 78.

Postoje četiri ključne poslovne prednosti ukoliko poslovni subjekt postupa po navedenoj normi:[18]

- ostvarivanje marketinške prednosti
- zadovoljavanje pravnih zahtjeva
- niži troškovi poslovanja
- bolja organizacija poslovanja

Ukoliko organizacija svoje poslovanje usklađuje s navedenom normom, veće su šanse za uspješno izbjegavanje mogućih prijetnji, efikasniju borbu s prijetnjama te brži i potpuniji oporavak od štetnih događaja. Slika 1. prikazuje potkategorije upravljanja rizicima u ISO 27001 normi.

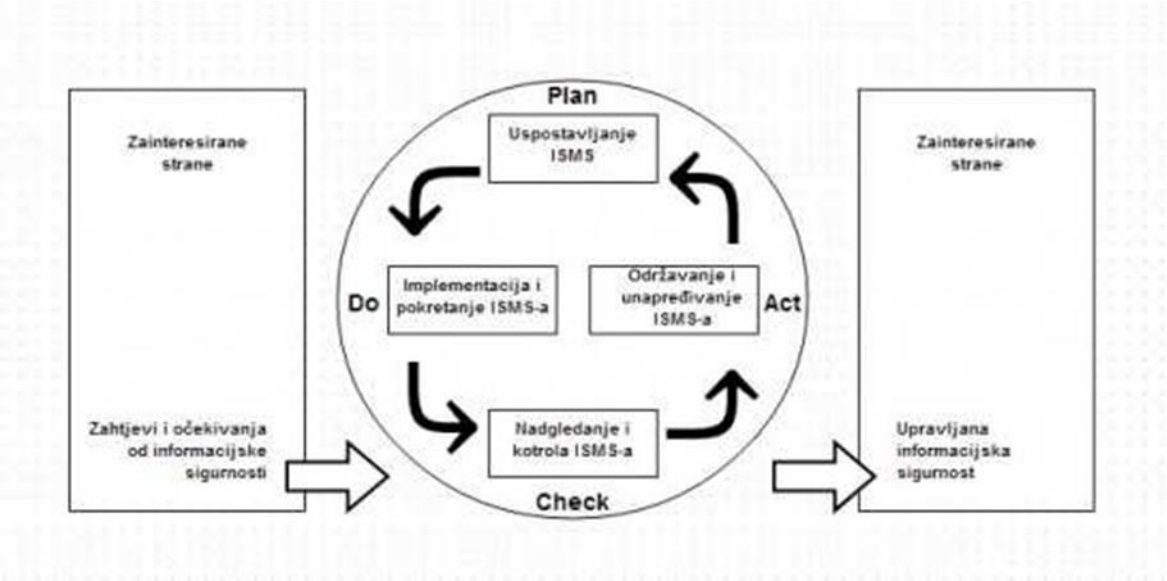
Slika 1. Potkategorije upravljanja rizicima u normi ISO 27001[19]



Međunarodna se norma ISO 27001 temelji na PDCA modelu (engl. Plan – Do – Check – Act). Slika 2. prikazuje PDCA model.

[18] Zašto je ISO 27001 dobar za vašu tvrtku?, Advisera.com, https://advisera.com/27001academy/hr/sto-je-iso- 27001/ [pristupljeno 23.9.2024]
[19] Ibid

Slika 2. PDCA model[20]



Postoje nekoliko normi koji su povezane s ISO/IEC 27001 normom, kao što je norma ISO/IEC 27002. Ova norma služi za davanje smjernica kako implementirati mjere koje se nalaze u normi ISO 27001. Norma ISO/IEC 27004 daje smjernice normi ISO 27001 za mjerenje informacijske sigurnosti, odnosno upućuje kako utvrditi jesu li postavljeni ciljevi u sustavu informacijske sigurnosti ostvareni. Nadalje, norma ISO/IEC 27005 je dodatak normi ISO 27001 jer upućuje kako obaviti procjenu rizika i obradu rizika. Isto tako norme koje nisu dio ISO/IEC 27001 obitelji mogu utjecati na razinu sigurnosti hotelskog informacijskog sustava. Tako će npr. norma ISO 9001, koja se bavi problemima očuvanja kvalitetu, olakšati implementaciju norme ISO 27001 ako je implementirana u poslovnom subjektu prije uvođenja norme ISO 27001.[21]

5.1.2 COBIT5

Norma COBIT (engl. Control Objectives for Information and Related Technologies) propisuje područja i pojedinačne provjere za upravljanje informacijskim sustavima i

[20] PDCA krug, svijet-kvalitete.com, Svijet kvalitete, https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug [pristupljeno 23.9.2024]
[21] Norme za informacijsku sigurnost, Dqsglobal, https://www.dqsglobal.com/hr-hr/edukacija/blog/norme-za-informacijsku-sigurnost-pregled [pristupljeno 23.9.2024]

pripadajućim procesima. Izrađen je od strane neprofitnih organizacija ISACA (engl. Information System Audit and Control Association) i ITGI (engl. Information Technology Governance Institute). Kreirana je kao alat za podršku provedbe revizije financijskih izvještaja, no tijekom svog intenzivnog razvoja ovaj je alat našao svoje mjesto i u području zaštite poslovnih informacijskih sustava. Najnovija se inačica COBIT5 norme sastoji se od 5 područja koja sadrže 37 informacijskih procesa te preko 300 informacijskih kontrola za njihovu primjenu. COBIT5 norma definira radni okvir koji pomaže u definiranju informacijskih ciljeva koji moraju biti usklađeni s poslovnim ciljevima, a sama implementacija ove norme započinje procesom procjene cjelokupne zrelosti informacijskih sustava u organizaciji.[22]

5.1.3 ITIL

ITIL (engl. Information Technology Infrastructure Library) je norma koja se sastoji od postupaka i procesa za upravljanje informacijsko-komunikacijskom tehnologijom i digitalnim uslugama. Upotrebljava ju velik broj poslovnih organizacija kako bi se osiguralo da su usluge informacijsko- komunikacijske tehnologije u potpunosti usklađene s ciljevima poslovne organizacije. Ova je norma prvi put kreirana u osamdesetim godina prošlog stoljeća. Norma je upotrebljavana za standardizaciju procesa u domeni podrške informacijsko-komunikacijske tehnologije te u domeni upravljanja uslugama. U strukturi se norme nalaze skupine procesa orijentiranih na upravljanje uslugama informacijsko-komunikacijske tehnologije. Tijekom je godina ITIL norma pojednostavljivana i prilagođavana promjenama u digitalnoj tehnologiji i uslugama koje je producirao razvitak digitalne tehnologije. Norma ITIL4 (aktualna inačica) pruža poslovnim organizacijama alate potrebne za suočavanje s promjenama u digitalnoj tehnologiji. Poslovne organizacije koriste ITIL normu za procjenu i poboljšanje pružanja digitalnih proizvoda krajnjim korisnicima (engl. End-to-End).[23]

---

[22] Centar Informacijske sigurnosti-COBIT 5 framework, CIS, https://www.cis.hr/dokumenti/5348-cobitframework-5.html [pristupljeno 24.4.2023]
[23] Standardi poslovanja, Storm.hr , https://www.storm.hr/index.php/hr/o-nama/standardi-poslovanja [prstupljeno 23.9.2024]

5.1.4 Zakonska regulativa informacijske sigurnosti i nadležna tijela u Republici Hrvatskoj

U Republici Hrvatskoj postoji nekoliko institucija koje se brinu za informacijsku sigurnost, a to su[24]:

- Nacionalni CERT
- CARNET CERT ili C-CERT
- Zavod za sigurnost informacijskih sustava (ZSIS)
- Ured Vijeća za nacionalnu sigurnost (UVNS)
- Agencija za podršku informacijskim sustavima i informacijskim tehnologijama (APIS IT d.o.o)
- Agencija za zaštitu osobnih podataka (AZOP)
- Središnji državni ured za e-Hrvatsku (SDUeH)

Nacionalni CERT je odjel Hrvatske akademske i istraživačke mreže – CARNET-a. Zadaća je CERT-a prevencija i zaštita od računalnih ugroza javnih informacijskih sustava u Republici Hrvatskoj. Prema tome, CERT se bavi obradom računalno-sigurnosnih incidenata radi očuvanja kibernetike sigurnosti u Republici Hrvatskoj. CERT.hr se aktivira ako se jedna od strana nađe u sigurnosnom incidentu iz Republike Hrvatske, što podrazumijeva da je jedna strana koja sudjeluje u sigurnosnom incidentu ili na .hr domeni ili u hrvatskom IP adresnom prostoru. Ovo se ne odnosi na tijela državne uprave jer je za njih nadležan Zavod za sigurnost informacijskih sustava (ZSIS). CERT se bavi sigurnosnim incidentima koji su prema Zakonu o kibernetičkoj sigurnosti značajni.[25]

Zavod za sigurnost informacijskih sustava (ZSIS) je središnje državno tijelo koje se bavi obavljanjem poslova u domeni tehničke sigurnosti informacijske infrastrukture kod

[24] Zakoni Republike Hrvatske vezani uz informacijsku sigurnost i zaštitu podataka, FOI, https://security.foi.hr/wiki/index.php/Zakoni_Republike_Hrvatske_vezani_uz_informacijsku_sigurnost_i_za%C5%A1titu_podataka.html#Zakonska_regulativa_informacijske_sigurnosti_u_Republici_Hrvatskoj [pristupljeno 9.1.2023]
[25] O nacionalnom CERT-u, CERT.hr, https://www.cert.hr/onama/ [pristupljeno 6.9.2023]

državnih tijela Republike Hrvatske. Poslovi kojima se bavi ZSIS su poslovi vezani za norme sigurnosti informacijskih sustava, kao i za sigurnosnu akreditaciju informacijskih sustava te upravljanje kriptomaterijalima koji se koriste u razmjeni klasificiranih podataka. Također se ZSIS bavi koordinacijom prevencije, kao i odgovorima na sigurnosne ugroze informacijskih sustava. ZSIS je zadužen za reguliranje normi koje se odnose na tehnička područja sigurnosti informacijskih sustava kroz izradu pravilnika koji se permanentno usklađuju s međunarodnim normama i preporukama. Norme s tehničkih područja sigurnosti, koje donosi ZSIS, primjenjuju se na sva državna tijela, jedinice lokalne i područne (regionalne) samouprave kao i na pravne osobe s javnim ovlastima koje se koriste klasificiranim podatcima.[26]

Ured Vijeća za nacionalnu sigurnost središnje je državno tijelo za informacijsku sigurnost – hrvatski NSA (engl. National Security Authority). U njegovom je djelokrugu rada donošenje sljedećih pravilnika:[27]

- Pravilnika o standardima sigurnosne provjere,
- Pravilnik o standardima fizičke sigurnosti,
- Pravilnik o standardima sigurnosti podataka,
- Pravilnik o standardima organizacije i upravljanja područjem sigurnosti informacijskih sustava te
- Pravilnik o standardima sigurnosti poslovne suradnje.

Ured Vijeća za nacionalnu sigurnost koordinira donošenje i nadzire primjenu normi informacijske sigurnosti u okviru:[28]

- sigurnosne provjere,
- fizičke sigurnosti,
- sigurnosti podataka,

[26] Zavod za sigurnost informacijskih sustava, ZNIS, https://www.zsis.hr/default.aspx?id=13 [pristupljeno 6.9.2023]
[27] Zakon o informacijskoj sigurnosti, Narodne Novine 79/2007, https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html [pristupljeno 6.9.2023]
[28] Ibid

- sigurnosti informacijskih sustava i
- sigurnosti poslovne suradnje

Također, Ured Vijeća za nacionalnu sigurnost izdaje certifikate fizičkim i pravnim osobama potrebne za pristup nacionalnim, NATO i EU klasificiranim podacima.[29]

Agencija za podršku informacijskim sustavima i informacijskim tehnologijama d.o.o. - APIS IT d.o.o., pruža strateške, stručne i provedbene usluge javnom sektoru Republike Hrvatske u:[30]

- planiranju,
- razvoju,
- podršci i
- održavanju poslovno-informacijskih sustava.

Navedene se aktivnosti obavljaju po načelu umrežene i korisnički usmjerene uprave. Od 2019. godine je APIS IT partner Središnjem državnom uredu za razvoj digitalnog društva u izgradnji Centra dijeljenih usluga (CDU). Radi se o strateškom projektu Europske unije i hrvatske javne uprave koji je pokrenut s ciljem konsolidacije državne informacijske infrastrukture i kreiranja privatnog oblaka javne uprave. APIS IT djeluje s ciljem kontinuirano osiguranja transparentnijeu, brže, učinkovitije i građanima uslužnije javne uprave te lokalne (regionalne) samouprave u Republici Hrvatskoj.[31]

Temeljem Zakona o zaštiti osobnih podataka, koji je donesen 2003. godine, osnovana je agencija za zaštitu osobnih podataka. Ova je agencija započela s radom 2004. godine. Radi se o neovisnom nadzornom tijelu čiji je glavni zadatak zaštita osobnih podataka što obuhvaća i primjenu mjera informacijske sigurnosti.[32]

[29] Ibid
[30] Digitalna transformacija javne uprave, APIS IT, https://www.apis-it.hr/apisit/index.html#/page?docId=862092FC53B6F468C1257F400043EACF [pristupljeno 6.9.2023]
[31] Ibid
[32] Pravni okvir, Agencija za zaštitu osobnih podataka, https://azop.hr/djelokrug/ [pristupljeno 6.9.2023]

Središnji državni ured za razvoj digitalnog društva ima zadatak praćenja i unaprjeđenja razvoja digitalnog društva te permanentnog usklađivanja sa smjernicama i regulativom Europske Unije na području digitalnog društva i ekonomije, a djelokrug mu je rada:[33]

- upravlja procesom digitalizacije u svim tijelima državne i javne uprave; usuglašava politike i ciljeve procesa digitalizacije s nadležnim tijelima, koordinira i sudjeluje u pripremi i obavlja nadzor provedbe strateški važnih ciljeva procesa digitalizacije
- obavlja poslove koji se odnose na praćenje, međusobnu povezanost i koordinaciju projekata iz područja informacijsko-komunikacijske tehnologije u tijelima državne i javne uprave; razvitak primjene informacijske i komunikacijske tehnologije te sustava elektroničke uprave
- definira smjernice i metodologiju za praćenje napretka i procjenu učinka politika za razvoj digitalnog društva, pruža informacije nadležnim tijelima nužne za poduzimanje aktivnosti usmjerene na poboljšanja,
- obavlja upravne i stručne poslove koji se odnose na standardizaciju, uspostavu, korištenje i održavanje državne informacijske infrastrukture i servisa u tijelima državne i javne uprave; povezivanje informacijskih sustava tijela državne i javne uprave kroz jedinstvenu informacijsko-komunikacijsku mrežu, standardizira i osuvremenjuje mrežu državne informacijske infrastrukture te koordinira povezivanje s drugim mrežama u državnoj i javnoj upravi, unaprjeđuje i upravlja informacijsko-komunikacijskim sustavima temeljenim na načelima interoperabilnosti, razmjene i zajedničkog korištenja podataka iz temeljnih i javnih registara te osigurava preduvjete za njihovu interoperabilnost, predlaže uvođenje novih tehnologija u rad tijela državne i javne uprave,
- obavlja stručne i druge poslove radi ostvarenja uvjeta za informiranje, na temelju službenih informacija izrađuje i vodi baze podataka o tijelima javne vlasti u ulozi

[33] Središnji državni ured za razvoj digitalnog društva, e-Građani, https://rdd.gov.hr/o-sredisnjem-drzavnom- uredu/djelokrug-138/138 [pristupljeno 6.9.2023]

Uz navedene poslove Središnji državni ured preuzima poslove iz djelokruga Ministarstva uprave koji se odnose na razvitak informacijskog sustava državne uprave. U to ulaze:[34]

- uspostava tehnološke i sigurnosne informatičke infrastrukture u tijelima državne uprave,
- povezivanje informacijskih sustava tijela državne uprave kroz jedinstvenu informacijsko- komunikacijsku mrežu,
- praćenje i koordinacija projekata iz područja informacijsko-komunikacijske tehnologije u tijelima državne uprave,
- sudjelovanje u donošenju i praćenju provedbe zakona i drugih propisa u području primjene informacijsko-komunikacijske tehnologije u državnoj upravi,
- razvitak primjene informacijske i komunikacijske tehnologije te sustava elektroničke uprave

Informacijska je sigurnost u Republici Hrvatskoj definirana brojnim zakonima od kojih su najbitniji:[35]

- Zakon o informacijskoj sigurnosti,
- Zakon o zaštiti osobnih podataka,
- Zakon o sigurnosno-obavještajnom sustavu Republike Hrvatske,
- Zakon o tajnosti podataka,
- Zakon o sigurnosnim provjerama te
- Zakon o elektroničkoj ispravi.

[34] Ibid
[35] Zakoni Republike Hrvatske vezani uz informacijsku sigurnost i zaštitu podataka,, ibid.

5.2 Identifikacija rizika hotelskog informacijskog sustava

Rizik obuhvaća opasnost koje prati poslovanje poduzeća te se zavisno o kategoriji u kojoj se nalazi može govoriti o različitim vrstama rizika. Stoga moraju osnovati vlastiti centar za upravljanje rizika koji će im omogućiti da se pripreme za određene rizike i da mogu što lakše ostvariti svoje ciljeve. Tvrtkama je primarni cilj identificirati rizike, te tako predstavljaju podlogu za lakše upravljanje s rizicima. Uz pomoć strategije i implementacije sustava tvrtke će se lakše snalaziti na tržištu. Svaka tvrtka trebala bi identificirati rizike s kojima se susreće. Pregled svih rizika znatno utječe na cjelokupno poslovanje tvrtke.

Rizici se mogu odnositi na[36]:

- sve ono što može naštetiti ugledu organizacije i smanjiti povjerenje dionika
- nepravilno i nezakonito poslovanje
- neučinkovito ili nedjelotvorno upravljanje
- neefikasna organizacija, procesi i aktivnosti
- nepouzdano izvještavanje
- nesposobnost reagiranja na promjene ili nesposobnost djelovanja u promijenjenim okolnostima.

Rizik se može definirati kao vjerojatnost prijetnje da našteti imovini u onom djelu gdje je najslabija. Može se prikazati matematičkom formulom[37]:

*RIZIK = PRIJETNJA*RANJIVOST*VRIJEDNOST IMOVINE*

Prikazana formula se ne koristi za izračunavanje rizika već služi prikazu međuovisnost čimbenika rizika. Odluke vezane za rizik mogu biti[38]:

[36] Upravljanje poslovnim rizicima, http://www.poslovni.hr/poslovni-centar-znanja/upravljanje-poslovnim-rizicima-306103 (pristupljeno 08.01.2023.)
[37] Chopra A.i M. Chaudhary: *Implementing an Information Security Management System*, India, 2020., str. 80
[38] Ibid, str. 81

- Prihvaćanje rizika – prije nego što odlučite da li je potrebno prihvatiti ili ne određeni rizik potrebno je uzeti u obzir nekoliko faktora, kao što su financijski, tehnički, organizacijski, sama okolina, vremenski.
- Ublažavanje rizika - uključuje plan i akciju koji će dovesti do ublažavanja samog rizika.
- Izbjegavanje rizika – moguće je kada se potencijalne prijetnje eliminiraju, rezultat toga je mijenjanje metode izvršavanja rizika.
- Prijenos rizika – najčešće i najbolji način za rješavanje rizika, jer se rizik može prenijeti na treću stranu prema ugovornim uvjetima.

5.3 Najčešće prijetnje sigurnosti hotelskog informacijskog sustava

Prema klasifikaciji Nacionalnog Instituta za norme i tehnologiju (engl. National Institute of Standards and Technology) prijetnje informacijskim sustavima se mogu podijeliti na[39]:

1. Greške i kvarove - ovu se vrstu prijetnji često podcjenjuje, ali mogu nanijeti značajnu štetu informacijskom sustavu. Najčešći uzrok greškama i kvarovima su ljudske radnje. Mogu ih uzrokovati zaposlenici, proizvođači programskih paketa ili administratori informacijskih sustava. Vjeruje se da je gotovo 65% napada uzrokovano greškama i kvarovima.

2. Prijevare i krađe - zlonamjerna aktivnost kojom napadač pokušava steći financijsku ili neki drugi oblik koristi. Prijevare i krađe se mogu dogoditi aktivnostima unutar (zaposlenik) ili izvan (udaljeni napad) organizacije. Međutim, češći su slučajevi aktivnosti prijevare i krađe unutar organizacije koji se događaju u čak 74% slučajeva. Vrlo lako je navesti razloge zbog kojih se prijevare i krađe događaju češće od strane zaposlenika nego udaljenim napadima:

[39] Hrvatska akademska i istraživačka mreža CARNet, Sigurnosna politika CCERT-PUBDOC-2009-05-265, Revizija 1.04, str. 8

• zaposlenici imaju pristup podacima i informacijskom sustavu,

• zaposlenici znaju koje podatke sustav sadrži i koje su sigurnosne provjere i

• zaposlenici znaju koje su prilike za prijevaru i krađu, te kolika je vrijednost mogućeg plijena.

3. Sabotažu od strane zaposlenika - koja je česta prijetnja sigurnosti i podacima informacijskog sustava. Kao što smo već spomenuli, zaposlenici imaju pristup, te znaju u kojim dijelovima sustava je moguće prouzročiti najveću štetu. Ako je u pitanju nezadovoljstvo zaposlenika, sabotaža je vrlo čest slučaj, bilo da se radi o sadašnjem ili bivšem zaposleniku.

Najčešći su primjeri sabotaže u informacijskom sustavu:

• fizičko uništavanje dijelova informacijskog sustava,

• postavljanje logičke bombe (eng. logic bomb), tj. zlonamjernog programskog koda čija je namjena izbrisati, premjestiti ili izmijeniti podatke,

• namjerni unos neispravnih podataka,

• „rušenje“ informacijskih sustava,

• brisanje i uništavanje podataka,

• krađa podataka i ucjena pod prijetnjom otkrivanja tih podataka široj javnosti ili konkurenciji,

• namjerno mijenjanje podataka.

4. Gubitak fizičke i infrastrukturne potpore - vrsta prijetnje koju nije moguće u potpunosti provjeriti, ponekad niti spriječiti, a može nanijeti veliku štetu sustavima. Takvi slučajevi mogu biti npr. prekid u opskrbi električnom energijom, prekid komunikacija, poplava, požar, potresi, itd.

5. Hakerski napadi (engl. Hackers) - relativno nova vrsta prijetnji informacijskim sustavima koja se prepoznaje kao najopasnija, s jedne strane zbog dostupnosti informacijsko- komunikacijske tehnologije posebice uslijed razvoja Interneta i komunikacija, a s druge strane zbog zlonamjernih programa (engl. Malware).

6. Prijetnje privatnosti korisnika - postaje ozbiljna prijetnja jer sve veći broj informacijskih sustava sadrži velik broj osobnih podataka korisnika

5.4 Alati i tehnike Informacijske sigurnosti

Neke od čimbenika informacijske sigurnosti[40]:

1. Digitalni identifikatori (ID) često uključuje korisničko ime i lozinku. U asimetričnoj kriptografiji, korisnik/sustav posjeduje javni ključ i privatni ključ, koji mogu služiti kao digitalni identifikatori. Digitalni certifikati koriste se u asimetričnoj kriptografiji za provjeru autentičnosti javnih ključeva i digitalnih identifikatora. Certifikat povezuje digitalni identifikator korisnika/sustava s njegovim javnim ključem dajući digitalni potpis preko javnog ključa i digitalnog identifikatora korisnika/sustava.
2. Sustav za otkrivanje upada (engl. Intrusion Detection System) je računalni i/ili programski sustav koji analizira događaje koji se događaju u računalnom sustavu ili mreži kako bi otkrio upade ili napade. Upad se može definirati kao pokušaj da se zaobiđu sigurnosne usluge koje koristi sustav. Često su upadi zlonamjernih aktera usmjereni na izvođenje napada uskraćivanjem usluge, što čini računalne sustave organizacije nedostupnima. Upade mogu uzrokovati na različite načine: napadači koji se spajaju na sustave s Interneta ili vanjskih mreža, ovlašteni korisnici sustava koji pokušavaju dobiti dodatne privilegije za koje nisu ovlašteni i ovlašteni korisnici koji krivo koriste i zlorabe privilegije koje su im dane.
3. Fizička sigurnost odnosi se na održavanje mrežne i računalne opreme organizacije u sigurnom fizičkom okruženju.

[40] Shabani, N. I A. Munir: *A review of cyber security issues in hospitality industry*, 2020., https://www.researchgate.net/publication/342683038_A_Review_of_Cyber_Security_Issues_in_Hospitality_Industry [pristupljeno 23.9.2024]

4. Vatrozid (engl. Firewall) može biti strojna, programska ili kombinacija strojne i programske opreme za nadzor prometa između uređaja i/ili dvije ili više računalnih mreža. Strojni je vatrozid fizički uređaj koji je priključen na mrežu, dok je programski vatrozid program koji se instalira na uređaje (npr. računala, tablete, telefone itd.) u mreži za praćenje protoka mrežnog prometa. Vatrozid također može blokirati određene zlonamjerne pakete koji pokušavaju ući ili napustiti računalnu mrežu.
5. Enkripcija je proces skrivanja informacija pretvaranjem informacija na način koji je nemoguć ili vrlo teško razumljiv. Enkripcija uglavnom pruža sigurnosnu uslugu povjerljivosti. Cilj enkripcije je tajnost podataka od svih osim od ovlaštene strane.
6. Biometrija je tehnologija autentifikacije korisnika na temelju fizičkih karakteristika ili karakteristika ponašanja, kao što su otisci prstiju, prepoznavanje glasa, hoda i identifikacija mrežnice ili šarenice. Radi se o učinkovitijoj metodi provjere identiteta. Biometrijski sustavi mjere fizičke karakteristike pojedinca i uspoređuju ih sa snimljenim karakteristikama kako bi potvrdili identitet korisnika.
7. Kontrola pristupa je tehnika ograničavanja korištenja resursa sustava ovlaštenim korisnicima/procesima. Kontrola pristupa obično se sastoji od provjere autentičnosti i autorizacije.
8. Pretraga radi provjere ranjivosti (engl. Vulnerability Assessment Scan) je programsko rješenje koje ispituje informacijski sustav na potencijalne ranjivosti i obavještava administratora sustava o tim ranjivostima kako bi se sustav mogao zaštititi.

Sigurnosna politika informacijskog sustava obuhvaća sljedeće zahtjeve:[41]

- potrebno je poštovati pravila definirana sigurnosnom politikom,
- nepoštivanje pravila može rezultirati sankcijama ili kaznama nadležnih institucija,
- potrebno je usredotočiti se na rezultate, a ne na način provedbe sigurnosne politike i
- određivanje sigurnosne politike se temelji na unaprijed definiranim normama i smjernicama.

[41] Sigurnosna politika CCERT-PUBDOC-2009-05-265, ibid., str. 5

6 Empirijsko istraživanje

Da bi se sagledalo s jedne strane, stanje sigurnosti u hotelskim kućama, a s druge strane, kako bi se dobili stavovi informacijsko-komunikacijskih stručnjaka za sigurnost vezani za optimalne načine osiguranja sigurnosti informacijskih sustava u hotelima, kako danas, tako i u budućnosti, provedena su dva primarna istraživanja. Prvo je primarno istraživanje provedeno anketiranjem djelatnika iz hotelskih kuća, dok je drugo istraživanje provedeno, gdje su ispitivani eksperti za sigurnost informacijsko-komunikacijske tehnologije, dubinskim intervjuom.

6.1 Rezultati istraživanja provedenih anketiranjem ispitanika, djelatnika hotelskih kuća

Provedenim se primarnim (empirijskim) istraživanjem anketiranjem željelo utvrditi sljedeće:

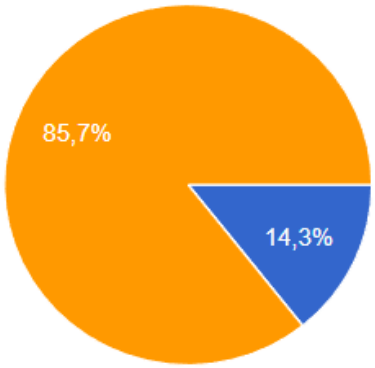
- standard i alati koji se primjenjuju za zaštitu poslovanja u hotelskim sustavima,
- razina znanja zaposlenih na određenim radnim mjestima u hotelskim sustavima i
- programi koji služe za detekciju rizika u poslovanju u hotelskim sustavima.

Primarno je istraživanje vezano za informacijsku sigurnost hotelskog poslovanja provedeno upotrebom upitnika. Ispitivanje je upitnikom provedeno u potpunosti anonimno. Upitnik je kreiran online upotrebom Google Forms obrasca. Hotelskim je kućama poveznica na upitnik dostavljena putem elektroničke pošte uz popratni tekst gdje je pojašnjena svrha prikupljanja podataka. Adrese su elektroničke pošte, na koje su slane poveznice na upitnik, pronađene na službenim Web stranicama hotela. Hoteli koje se pozvalo putem elektroničke pošte da sudjeluju u istraživanju pronađeni su na Web-u. Pozivi za sudjelovanje u istraživanju upućeni su na 100 adresa elektroničke pošte. U većini se slučajeva radilo o hotelskim poslovnim subjektima koji imaju svoje lance hotela. Automatski je odgovor o neuspjeloj isporuci elektroničke pošte dobiven od

poslužitelja 16 hotela. Nadalje, 77 hotela se nije odazvalo na sudjelovanje u istraživanju tako da je upitniku na kraju pristupilo 7 ispitanika što čini stopu odaziva od 8,33%. U distribuciji ispitanika koji su popunili upitnik njih 4 je bilo zaposleno u sektoru informacijskih tehnologija, dok je jedan ispitanik radio na mjestu administratora sustava, jedan na recepciji te jedan kao specijalist u ljudskim resursima. Prikupljeni su podaci upitnikom statistički obrađeni. Rezultati su obrade nadalje prikazani.

Grafikon 1. prikazuje veličinu poslovnih subjekata koji su sudjelovali u istraživanju

Grafikon 1 -Veličina poslovnih subjekata koji su sudjelovali u istraživanju

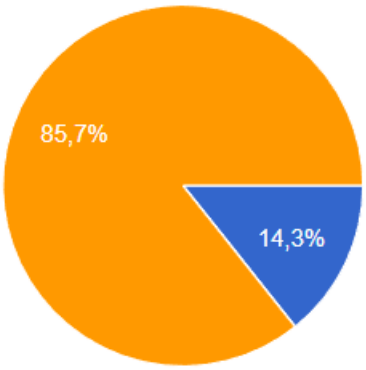


Izvor: obrada autora na temelju ankete

Kao što je iz grafikona 1. vidljivo prema odgovorima ispitanika od ukupno 7 hotelskih kuća čiji su djelatnici sudjelovali u istraživanju njih 6 su veliki poslovni subjekti (85,7%) dok je u istraživanju sudjelovao i jedan mali poslovni subjekt (14,3%).

Grafikon 2. prikazuje aktivne hotelske jedinice u sklopu poslovnog subjekta

Grafikon 2 – Aktivne hotelske jedinice u sklopu poduzeća

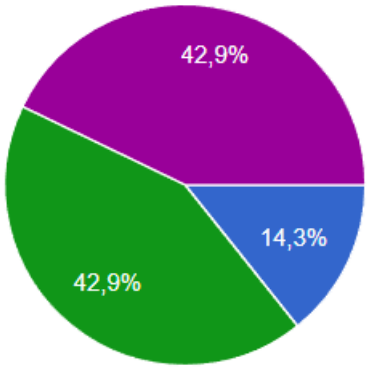


Izvor: obrada autora na temelju ankete

Iz grafikona 2. je vidljivo kako je 85,7% ispitanika odgovorilo kako imaju više od 5 aktivnih hotelskih jedinica, dok je 14,3% odgovorilo da imaju samo jednu aktivnu hotelsku jedinicu.

Grafikon 3. prikazuje strukturu informacijskog sustava u hotelskom poslovnom subjektu

Grafikon 3 – Struktura informacijskog sustava u hotelskom poslovnom subjektu

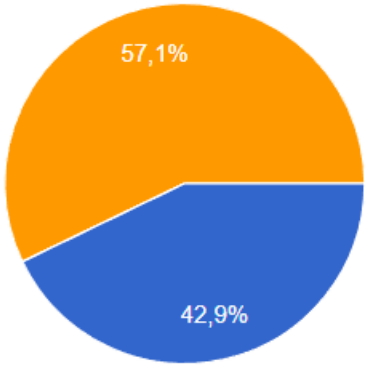


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 3. vidljivo u 14,3% slučajeva se poslovni subjekti koriste samo jednim računalom za potrebe poslovanja, 42,9% ima više korisničkih računala te vlastita poslužiteljska računala, dok 42,9% ima više korisničkih računala te se za poslužiteljsku infrastrukturu koristi računalstvom u oblaku.

Grafikon 4. prikazuje strukturu odgovora ispitanika vezanu uz susret hakerskim napadom unutar poslovnog subjekta

Grafikon 4 – Susret s hakerskim napadom unutar poslovnog subjekta



Izvor: obrada autora na temelju ankete

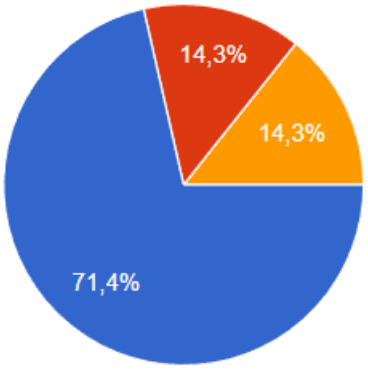
Kako je iz grafikona 4. vidljivo u 57,1% se slučajeva hotelski sustav susreo s hakerskim napadom, dok se u 42,9% slučajeva hotelski sustav nje susreo s hakerskim napadom. Iz ovog je podatka vidljivo koliko je objektivno velika mogućnost ugroze sigurnosti informacijskog sustava kod hotelskih poslovnih subjekata.

Na upit o sustavima za detekciju, odnosno prevenciju hakerskih napada koji se koriste u hotelskom poslovnom sustavu dobiveni su različiti odgovori. U većini slučajeva glavna je stup obrane vatrozid (engl. Firewall) te ostali programi antivirusne zaštite i zaštite

podataka općenito (Windows defender, NAC, DLP, IDR, SIEM, AV BitDefender, e-mail zaštita, 2FA, Backup te Crowdstrike).

Grafikon 5. prikazuje strukturu odgovora ispitanika vezanu za vrijeme ažuriranja sustava za prevenciju hakerskih napada.

Grafikon 5 – Vrijeme ažurnosti sustava za prevenciju hakerskih napada

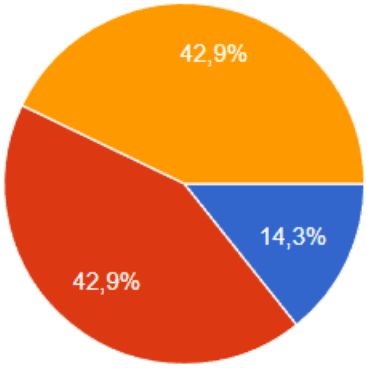


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 5. vidljivo na pitanje vezano za vrijeme kada je posljednji put bio ažuriran sustav za prevenciju hakerskih napada odgovor je bio nedavno kod 71,4% ispitanika, prije mjesec dana kod 14,3% ispitanika te prije šest mjeseci kod 14,3% ispitanika.

Grafikon 6. prikazuje strukturu odgovora ispitanika vezanu uz mjere osiguranja informacijskog sustava od napada.

Grafikon 6 – Mjere osiguranja Iinformacijskog sustava od napada

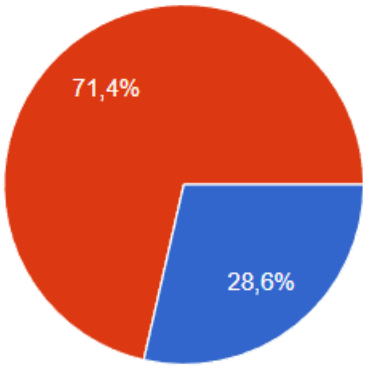


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 6. vidljivo, u 14,3% slučajeva o samoj sigurnosti informacijskog sustava brine se osoba koja je zadužena za sigurnost i koja je ujedno i zaposlenik poslovnog subjekta, u 42,9% slučajeva postoji informatička služba unutar hotelskog sustava koja se sastoji od više stručnjaka koji su zaduženi za sigurnost informacijsko sustava, dok u 42,9% hotelskih sustava postoji potpisan ugovor s vanjskim poslovnim subjektom koji se brine o sigurnosti informacijskog sustava hotelskog poslovnog subjekta.

Grafikon 7. prikazuje strukturu odgovora ispitanika vezanu uz učestalost edukaicje vlastitih zaposlenika vezano uz informacijsku sigurnost

Grafikon 7 – Učestalost edukacije vlastitih zaposlenika vezano uz informacijsku sigurnost

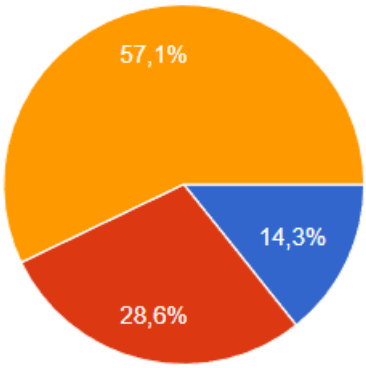


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 7. vidljivo, u 28,6% slučajeva zaposlenici hotelskog sustava, oni koji se brinu o sigurnosti informacijskog sustava, odlaze na dodatne edukacije češće od jednom godišnje, dok u 71,4% slučajeva zaposlenici, oni koji se brinu o sigurnosti informacijskog sustava, odlaze samo jednom godišnje na dodatne edukacije vezano uz sigurnost informacijskog sustava.

Grafikon 8. distribucija odgovora ispitanika o učestalosti pomoći, vezano za informacijsku sigurnost sustava, ukoliko se o održavanju informacijske sigurnosti sustava brine vanjski poslovni subjekt.

Grafikon 8 – Distribucija odgovora ispitanika o učestalosti pomoći, vezano uz informacijsku sigurnost sustava, ukoliko se o održavanju infroamcijske sigurnosti brine vanjski poslovni subjekt



Izvor: obrada autora na temelju ankete

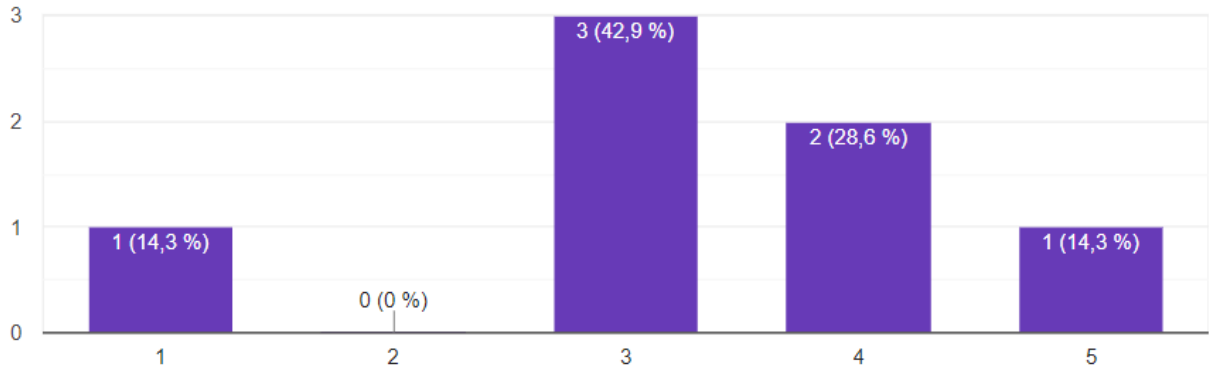
Kako je iz grafikona 8. vidljivo, da je jednom pozvan vanjski poslovni subjekt koji se brine o sigurnosti informacijskog sustava, kad se dogodio kvar ili napad na informacijski sustav, odgovorilo je 14,3% ispitanika. Da se u slučajevima kvara ili napada na informacijski sustav povremeno, ako se to smatra potrebnim, poziva u pomoć vanjski poslovni subjekt koji se brine o sigurnosti informacijskog sustava, odgovorilo je 28,6% ispitanika. Konačno je 57,1% ispitanika dalo odgovor kako u njihovom hotelskom sustavu postoji ugovor o redovitom održavanju informacijskog sustava s vanjskim poslovnim subjektom koji se brine o sigurnosti informacijskog sustava hotela.

Vezano za preduvjete koje treba zadovoljiti osoba koja se zapošljava u hotelskom sustavu, a koja će se koristiti informacijsko-komunikacijskom tehnologijom na svom radnom mjestu, iz distribucije se odgovora ispitanika može vidjeti kako hotelski sustavi nemaju specificirane nikakve preduvjete glede poznavanja budućeg zaposlenik sigurne upotrebe informacijsko-komunikacijske tehnologije. Nadalje se iz distribucije odgovora ispitanika može vidjeti da neki hotelski sustavi ovaj nedostatak vezan za poznavanje

sigurnog rada s informacijsko-komunikacijskom tehnologijom rješavaju edukacijskom. Većina je ispitanika ukazala na to da hotelski sustav u kojem rade traži fokusiranost, odgovornost, pravilnu upotrebu resursa, razumijevanje informacijske sigurnosti te sposobnost rješavanja problema od svojih zaposlenika. To podrazumijeva upoznavanje ili poznavanje sigurnosnih alata koje hotelski sustav upotrebljava za zaštitu svog informacijskog sustava. Ispitanici su također, kroz svoje odgovore, ukazali na važnost, za informacijsku sigurnost, upotrebe vlastitih korisničkih računa i jakih lozinki u svrhu ograničavanja zaposlenika pristupu resursima, posebice podatkovnim, kojima se nema pravo.

Grafikon 9. prikazuje ocjena ispitanika dane zaposlenicima vezano za znanja, kvalitetu i sigurnu upotrebu informacijsko-komunikacijske na svom radnom mjestu u hotelskom sustavu.

Grafikon 9 – Ocjena ispitanika dane zaposlenicima vezano uz znanja, kvalitetu i sigurnu upotrebu informacijsko-komunikacijske na svom radnom mjestu u hotelskom sustavu



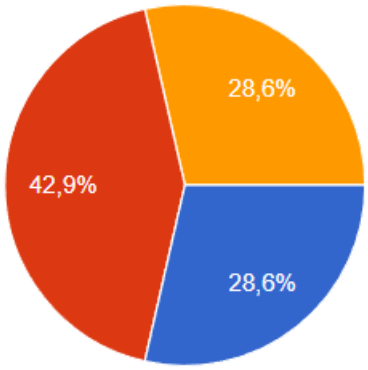
Izvor: obrada autora na temelju ankete

Iz grafikona 9. vidljivo kao su ispitanici ocijenili zaposlenike hotelskog sustava vezano za znanja, kvalitetu i sigurnu upotrebu informacijsko-komunikacijske na svom radnom mjestu, pa tako ocjenu je 1 zaposlenicima hotelskog sustava u kojem rade dalo 14,3%

ispitanika, s ocjenom je 3 zaposlenike hotelskog sustava u kojem rade ocijenilo 42,9% ispitanika, s ocjenom je 4 zaposlenike hotelskog sustava u kojem rade ocijenilo 28,6% ispitanika te s ocjenom je 5 zaposlenike hotelskog sustava u kojem rade ocijenilo 14,3% ispitanika. Kako je iz grafikona 9. vidljivo, niti jedan ispitanik svojim zaposlenicima nije dao ocjenu 2.

Grafikon 10. prikazuje distribuciju odgovora ispitanika vezanu uz provođenje dodatnih edukacija zaposlenih u hotelskom sustavu u kojem radi ispitanik vezano za sigurnost informacijskog sustava hotela.

Grafikon 10 – Distribucija odgovora ispitanika vezana uz provođenje dodatnih edukacija zaposlenih u hotelskom sustavu u kojem radi ispitanik, vezano za sigurnost informacijskog sustava hotela



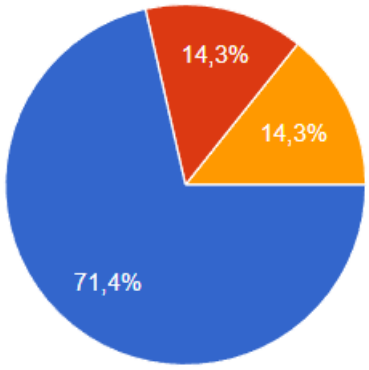
Izvor: obrada autora na temelju ankete

Kako je iz grafikona 10. vidljivo unutar se hotelskih sustava u kojim radi 28,6% ispitanika ne provode dodatne edukacije zaposlenika glede identificiranja prijetnji informacijskom sustavu, unutar hotelskih sustava u kojim radi 42,9% ispitanika svi zaposleni polaze dodatne edukacije glede identificiranja prijetnji, a unutar se hotelskih

sustava u kojim radi 28,6% ispitanika dodatnu edukaciju prolaze samo zaposlenici koji se brinu o sigurnosti informacijskog sustava polaze.

Grafikon 11. prikazuje strukturu odgovora ispitanika vezano za standarde koji se primjenjuju u hotelskom sustavu radi očuvanja sigurnosti informacijskog sustava.

Grafikon 11 – Standardi koji se primjenjuju u poslovnom subjektu

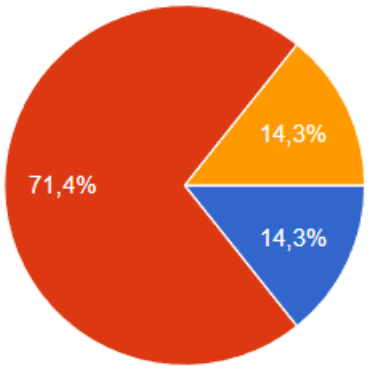


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 11. vidljivo, između 3 svjetski poznata standarda, a sukladno odgovorima ispitanika, najčešće se koristi standard ISO 27001, u 71,4% hotelskih sustava, potom standard COBIT te standard ITIL5 koji se koristi u 14,3% hotelskih kuća.

Grafikon 12. prikazuje distribuciju odgovora ispitanika koja se odnosi na najvrjedniji dio imovine (engl. Asset) informacijskog sustava koju je potrebno zaštiti u hotelskoj kući.

Grafikon 12 – Distribucija odgovora ispitanika koja se odnosi na najvrijedniji dio imovine informacijskog sustava koju j epotrebno zaštititi u hotelskoj kući

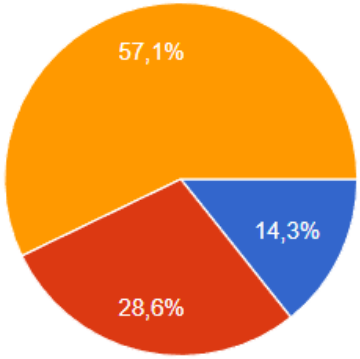


Izvor: obrada autora na temelju ankete

Kako je vidljivo iz grafikona 12. na pitanje koje se odnosi na najvrjedniji dio imovine (engl. Asset) informacijskog sustava koju je potrebno zaštiti u hotelskoj kući, prema 71,4% ispitanika to je informacijsko-komunikacijska tehnologija (računalna oprema, programski sustavi, podatci i drugo), dok je prema 14,3% ispitanika to materijalna imovina (zgrada ili zgrade i sve što je opipljivo), te isto tako prema 14,3% ispitanika to su ljudski potencijali.

Grafikon 13. prikazuje distribuciju odgovora ispitanika vezana za identifikaciju i procjenu rizika informacijskog sustava u hotelskoj kući.

Grafikon 13 – Distribucija odgovora ispitanika vezana za identifikaciju i procjenu rizika informacijskog sustava u hotelskoj kući

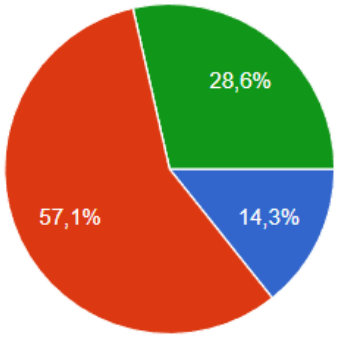


Izvor: obrada autora na temelju ankete

Kako je vidljivo iz grafikona 13., a sukladno odgovorima ispitanika, o identifikaciji se i procijeni rizika informacijskih sustava brinu vlastiti zaposlenici u 14,3% hotelskih sustava, u 28,6% hotelskih sustava postoji poseban tim stručnjaka koji se bave samo identifikacijom rizika (engl. Asset Management), dok u 57,1% hotelskih postoji ugovor s vanjskim partnerima koji brinu o identifikaciji i procijeni rizika informacijskog sustava.

Grafikon 14. prikazuje distribuciju odgovora ispitanika vezana uz učestalost promjene lozinke unutar informacijskog sustava hotelske kuće.

Grafikon 14 – Učestalost promjene lozinke unutar poduzeća

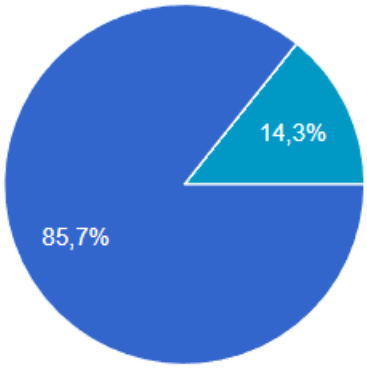


Izvor: obrada autora na temelju ankete

Kako je iz grafikona 14. vidljivo, distribucija je odgovora vezana za učestalost izmjene lozinki unutar hotelske kuće slijedeća: u 14,3% hotelskih sustava učestalost je izmjene lozinki svaka dva tjedna, u 57,1% hotelskih sustava učestalost je izmjene lozinki svakih 90 dana, dok se u 28,6% hotelskih sustava lozinka ne mijenja ako se smatra da nije potrebno. Među ispitanicima nitko nije odgovorio da se lozinka nije mijenjala od osnutka hotelskog sustava.

Grafikon 15. prikazuje distribuciju odgovora ispitanika vezanu uz najčešći izvor prijetnji informacijskom sustavu hotelske kuće putem društvenog inženjeringa.

Grafikon 15 – Distribucija odgovora ispitanika vezana uz najčešći izvor prijetnji infromacijskom sustavu hotelske kuće putem društvenog inženjeringa



Izvor: obrada autora na temelju ankete

Kako je iz grafikona 15. vidljivo ispitanici su svoje odgovore vezanu uz najčešći izvor prijetnji informacijskom sustavu hotelske kuće putem društvenog inženjeringa grupirali u dvije skupine. Tako se 85,7% ispitanika odlučilo za odgovor da ju najčešći izvor prijetnji informacijskom sustavu hotelske kuće putem društvenog inženjeringa pecanje (engl. Phishing), dok se 14,3% ispitanika odlučilo za odgovor ugrožavanje poslovne elektroničke pošte (engl. Business Email Compromise - BEC). Ostale ponuđene odgovore s oblicima društvenog inženjeringa (Pretexting, Baiting, Tailgating i Quid pro quo) ispitanici nisu birali.

6.2 Rezultati istraživanja provedenih dubinskim intervjuom stručnjaka za sigurnost informacijsko-komunikacijskih tehnologija

Evidentno je kako se problemi, koji su vezani uz sigurnost informacijskih sustava, a time i hotelskih informacijskih sustava, rapidno povećavaju. Dinamiku tih promjena teško prate znanstveni i stručni članci, stoga, da bi se dobio uvid u aktualna pitanja i odgovore vezane za sigurnost informacijskih sustava općenito, te posebno hotelskih informacijskih sustava, ispitano je četiri eksperta za informacijsko-komunikacijsku tehnologiju i sigurnost informacijsko- komunikacijske tehnologije s područja Istarske županije koji su iznjeli putem dubinskog intervjua svoje pogled na evolutivne promjene u informacijsko-komunikacijskoj tehnologiji, na probleme sigurnosti i načine osiguranja

sigurnost posebice kod hotelskih informacijskih sustava. Dubinskim su intervjuom ispitani eksperti:

I. Marija Kantolić,

II. Marijela Miličević,

III. Matija Prepušt,

IV. Danijel Grgorović.

I. Dubinski intervju s Marijom Kantolić

Pitanje 1.

Molim Vas da mi se ukratko predstavite, te navedete stručnu spremu, školovanje te poslove koje ste do sada profesionalno obavljali, te radno mjesto na kojem se trenutno nalazite vezano za ICT. Odgovor:

Moje ime je Marija Kantolić, završila sa diplomski studij Informatike na Fakultetu Informatike u Puli te trenutno radim u firmi Infobip d.o.o.

Pitanje 2.

Zbog čega sebe možete smatrati osobom kompetentnom za pitanja sigurnosti informacijskih sustava?

Odgovor:

Infobip kao telekomunikacijska tvrtka surađuje s različitim klijentima i operaterima kako bi im omogućila nesmetano i lakše surađivanje sa svojim krajnjim korisnicima. Stoga, kao zaposlenik Infobipa imam jednim dijelom iskustva koliko je sigurnost informacijskih sustava prisutna i važna.

Pitanje 3.

Kako biste definirali hotelski informacijski sustav i što su po Vama njegove specifičnosti u odnosu npr. na informacijske sustave u trgovini ili proizvodnji?

Odgovor:

Hotelski informacijski sustav je integrirani sustav koji povezuje cjelokupne poslovne procese unutar hotela. Glavni cilj hotelskog informacijskog sustava je optimizirati operativnu efikasnost hotela i iskustvo gosta. Specifičnost hotelskog informacijskog sustava u odnosu na informacijske sustave u trgovini ili proizvodnji su: fokus na usluge, upravljanje rezervacijama, dinamičko upravljanje cijenama, interakcija s gostima (online i recepcija), stanje skladišta, povezanost sa vanjskim sustavima (Tripadvisor).

Pitanje 4.

Koje su po Vama danas najveće prijetnje u pogledu sigurnosti informacijskih sustava, posebice hotelskih informacijskih sustava?

Odgovor:

Hotelski informacijski sustav sadržava određene podatke od svojih gostiju i upravlja određenim podacima o prihodima i troškovima. S tim razlozima, mogućnost napada što vanjskih, što unutarnjih, je veća. Napadi kao malware, phishing mail-ovi, lažni pozivi, nedovoljno kontrolirani sigurnosni sustavi i slično su očekivani.

Pitanje 5.

Što po Vama hoteli trebaju činiti da bi osigurali sigurnost informacijskih sustava?
Odgovor:

Osigurati bolja i adekvatnija tehnološka rješenja za obranu od kibernetičkih napada kao i edukacija svojih zaposlenika kako bi sigurnije upravljala podacima. Svakako i praćenja promjena i usklađivanje sa zakonskim regulativama.

Pitanje 6.

Koje sigurnosne standarde preporučate hotelskim informacijskim sustavima i zašto?
Odgovor:

Svakako kao najbitniji standard bi bio ISO 27001 koji je međunarodno priznati standard informacijske sigurnosti, pomaže prilikom identifikacije i sprječavanja rizika. Dobivanje ovog certifikata uvelike bi povećao povjerenje gostiju i ostalih dionika unutar hotela. Možda bih još i spomenula i GDPR koja je zapravo europska zakonska regulativa koja se bavi zaštitom osobnih podataka.

Pitanje 7.

Koja znanja i koju bi obuku po Vama trebali proći svi djelatnici kako bi se povećao prag sigurnosti hotelskih informacijskih sustava?

Odgovor:

Djelatnici bi trebali proći osnovnu edukaciju o tome kako kreirati sigurne lozinke, kako prepoznati lažne mail-ove, prepoznati na koje stranice i linkove smiju kliknuti a na koje ne smiju. Hoteli bi također trebali imati dedicirani odjel za sigurnost kojeg bi hotelsko osoblje moglo kontaktirati u slučaju sumnjivih mail-ova/poziva.

Pitanje 8.

Koja su po Vama bitna mjerila sigurnosti hotelskih informacijskih sustava, odnosno po kojim biste kriterijima ocijenili je li neki hotelski informacijski sustav siguran ili nije?

Odgovor:

Svakako mislim da ovdje postoje brojni faktori koji mogu utjecati na to od fizičke sigurnosti do tehničkih i organizacijskih faktora. Smatram da bi prvenstveno trebalo imati dobru zaštitu podataka npr. firewall i antivirusne programe, svakodnevni backup podataka (u slučaju da se nešto dogodi podaci su uvijek dostupni). Zaposlenici bi trebali biti educirani na svim razinama poslovanja. Ograničen pristup serverima i informatičkoj opremi te video nadzor cijelog hotela.

Pitanje 9.

Što su danas po Vama važniji problemi kada je u pitanju sigurnost hotelskih informacijskih sustava: potencijalne ugroze od malicioznog koda koje mogu utjecati na rad informacijskog sustava ili pak krađa podataka? Zašto?

Odgovor:

U slučaju da informacijski sustav bude onemogućen na određeno vrijeme, jedino što će se usporiti je obavljanje određenih usluga, kao naplata gostima. U slučaju da nastane krađa podataka, to može dovesti do većih financijskih i reputacijskih posljedica jer se krši niz zakona, kao GDPR.

Pitanje 10.

Danas je prisutan trend eksternalizacije obrade i čuvanja podataka kroz koncept računalstva u oblaku. Kako ocjenjujete sigurnost informacijskih sustava koji su obradu i pohranu podataka eksternalizirali u računalni oblak?

Odgovor:

Sigurnost današnjih informacijskih sustava u oblaku može biti vrlo visoka, što omogućuje veću uštedu troškova i bolju učinkovitost od raznih napada ako se primjenjuju odgovarajuće sigurnosne mjere. Smatram da je danas visoka sigurnost

spremanja podataka u računalni oblak jer takvi sustavi imaju spremno redundantno rješenje. To jest, u slučaju bilo kakvog kvara, uvijek postoji sigurnosna kopija koja smanjuje gubitak podataka. Računalni oblak omogućuje veći prostor za pohranu podataka nego što fizički uređaji to pružaju krajnjem korisniku. Također, ako je potrebno dijeljenje podataka s uređaja na druge uređaje, lakše je isto učiniti s računalnog oblaka nego sa fizičkog uređaja.

Pitanje 11.

Koje bi osobe za sigurnost trebao imati informacijski sustav, koje na rukovodećim mjestima, a koje na izvršnim mjestima? Kako po Vama sigurnosni podsustav informacijskog sustava treba biti organiziran, kao centraliziran odjel (služba) ili decentralizirano?

Odgovor:

Osobe koje bi trebale biti odgovorne za sigurnost informacijskog sustava CISO te osobe koje analiziraju rizike i održavaju sigurnost mreže te osoba koja će implementirati sigurnosne mjere za zaštitu od kibernetičkih napada. Preporuka za organizaciju informacijskog sustava bi bila omogućiti hibridni sustav koji kombinira centraliziranu strategiju s decentraliziranim elementima.

Pitanje 12.

Umjetna je inteligencija nešto novo što će se sigurno koristiti i za potrebe ugroze sigurnosti i za potrebe zaštite od ugroze sigurnosti hotelskih informacijskih sustava. Gdje vidite mogućnosti zloupotrebe s jedne strane i mogućnosti iskorištavanja u svrhu zaštite hotelskih informacijskih sustava s druge strane?

Odgovor:

Mogućnosti zloupotrebe umjetne inteligencije koje bi ugrozile sigurnost hotelskih informacijskih sustava bi mogle biti kroz „phishing“ poruke zaposlenicima, kroz napade na sustav koji bi ukrali sve podatke o osoblju i gostima u tom hotelu te mogućnosti lažnog predstavljanja i rezerviranja smještaja u hotelu. U svrhu zaštite tog istog sustava, umjetna inteligencija bi se mogla koristiti za zaštitu spomenutih napada, za autentifikaciju osoblja i gostiju kako bi se smanjio rizik od neovlaštenog pristupa.

Pitanje 13.

Informacijsko-komunikacijska tehnologija se stalno razvija i mijenja oblike funkcioniranja informacijskih sustava, S obzirom na vaša očekivanja glede informacijsko-komunikacijske tehnologije gdje će u budućnosti biti težište ugroza sigurnosti, a s tim i težište obrane od ugroza sigurnosti hotelskih informacijskih sustava?

Odgovor:

Težište ugroza sigurnosti bi bili kibernetički napadi na sam sustav u pokušaju prikupljanja podataka o gostima hotela. Kako današnja digitalizacija sve više napreduje, hotelski informacijski sustavi moraju biti u toku s trendovima obrane od raznih napada kako bi zaštitili svoje goste, a i svoje osoblje od različitih prijevara.

Pitanje 14.

Ako bi brigu o sigurnosti uprava hotela željela prepustiti specijaliziranoj kući koja bi u outsourceingu održavala hotelski informacijski sustav sigurnim, kojim bi se kriterijima uprava hotela trebala voditi kako bi odabrala optimalnog partnera?

Odgovor:

U slučaju potrage za firmom koja se specijalizira sigurnosnim sustavima potrebno je obratiti pozornost na to s kojim tehnološkim rješenjima to poduzeće upravlja,

zadovoljavaju li sve propisane uvjete od međunarodno priznatih standarda, referencu i reputaciju drugih hotela i klijenata, stručnost i pod kojim uvjetima bi se napravio ugovor.

Pitanje 15.

Nakon svih ovih pitanja, smatrate li da sam Vas zaboravila nešto važno pitati vezano za sigurnost informacijskih sustava općenito te vezano za hotelske informacijske sustave?

Odgovor:

Osobno mišljenje je da ste pokrili cijelu tematiku o sigurnosti u ovih 14 pitanja.

II. Dubinski intervju s Marijelom Miličević

Pitanje 1.

Molim Vas da mi se ukratko predstavite, te navedete stručnu spremu, školovanje te poslove koje ste do sada profesionalno obavljali, te radno mjesto na kojem se trenutno nalazite vezano za ICT. Odgovor:

Moje ime je Marijela Miličević i imam 27 godina. Po struci sam magistra edukacije informatike, završila sam diplomski sveučilišni studij informatike – nastavničkog smjera na Sveučilištu Jurja Dobrile u Puli, a prije toga poslovnu informatiku na prijediplomskom studiju također u Puli, na Fakultetu ekonomije i turizma "Dr. Mijo Mirković". Radim u struci, odnosno učiteljica sam informatike u jednoj osnovnoj školi u Puli te radim kao vanjski suradnik, odnosno naslovni asistent na Fakultetu informatike u Puli.

Pitanje 2.

Zbog čega sebe možete smatrati osobom kompetentnom za pitanja sigurnosti informacijskih sustava?

Odgovor:

Obzirom da sam studirala poslovnu informatiku, a nakon toga i informatiku, smatram da sam dovoljno kompetentna obzirom na različite slušane kolegije o informacijskim, poslovnim sustavima, informatičkom menadžmentu koji također govori o samoj sigurnosti istih, a vodila sam i nekoliko različitih web stranica za vrijeme studiranja u poslovnim organizacijama, pa jedan dio sigurnosti sam odrađivala i u tom području.

Pitanje 3.

Kako biste definirali hotelski informacijski sustav i što su po Vama njegove specifičnosti u odnosu npr. na informacijske sustave u trgovini ili proizvodnji?

Odgovor:

Hotelski informacijski sustav je za razliku od onog u trgovini i proizvodnji specijalizirani sustav koji upravlja različitim aspektima hotelskog poslovanja. Tu bih svakako istaknula rezervacije gostiju, prijavu i odjavu gostiju, upravljanje sobama, obračun usluga, održavanje, ali i kasnije spajanje s drugim hotelskim funkcijama restorana i sl. Dakle, specifičnosti su im upravljanje gostima i sobama u hotelima, rezervacijama, imaju interakciju s drugim odjelima i ono što hotelski sustavi često imaju drugačije od ostalih su vanjski sustavi za online rezervacije poput Bookinga npr. pa se samim time razlikuju od trgovine ili proizvodnje.

Pitanje 4.

Koje su po Vama danas najveće prijetnje u pogledu sigurnosti informacijskih sustava, posebice hotelskih informacijskih sustava?

Odgovor:

Svakako cyber napadi, slabe sigurnosne prakse, napadi koji uključuju šifriranje podataka, phishing i socijalni inženjering u kojem napadači manipuliraju otkrivanjem npr. lozinki i financijskih podataka što nije istina, napadi uskraćivanjem usluga i slično. A

svakako bih spomenula i zastarjeli sustav s lošom infrastrukturom, krađu podataka gostiju sa slabom zaštitom osobnih podataka i insiderske prijetnje gdje zaposlenici mogu slučajno ili namjerno uzrokovati sigurnosne povrede.

Pitanje 5.

Što po Vama hoteli trebaju činiti da bi osigurali sigurnost informacijskih sustava?
Odgovor:

Tehničke mjere, politike i edukacije zaposlenika i stalni nadzor. Dvofaktorsku autentifikaciju, kompleksne lozinke za zaposlenike, redovito ažuriranje sustava, segmentaciju mreže i svakako šifriranje podataka te redovite sigurnosne provjere i nadzor.

Pitanje 6.

Koje sigurnosne standarde preporučate hotelskim informacijskim sustavima i zašto?
Odgovor:

Međunarodni standard za upravljanje informacijskom sigurnošću (Information Security Management System - ISMS), koji pruža okvir za sustavno upravljanje osjetljivim informacijama i njihovu zaštitu. ISO 27001 pomaže hotelima u uspostavljanju procesa za zaštitu osobnih podataka, smanjenje rizika od sigurnosnih incidenata, te održavanje povjerljivosti i integriteta poslovnih informacija. Zakonodavni okvir Europske unije koji regulira privatnost i zaštitu osobnih podataka građana EU-a. Hoteli prikupljaju osjetljive osobne podatke (ime, adresa, podaci o putovnici, kontakt informacije), a kršenje GDPR-a može rezultirati velikim kaznama. Usklađenost s GDPR-om osigurava da hoteli pravilno obrađuju, pohranjuju i dijele osobne podatke gostiju. Proširenje ISO/IEC 27001 koje se fokusira na upravljanje osobnim podacima i usklađenost sa zakonima o zaštiti podataka, poput GDPR-a. Hoteli koji žele osigurati poštivanje privatnosti gostiju i usklađenost sa zakonodavstvom o zaštiti podataka mogu koristiti ISO/IEC 27701 za

postavljanje i održavanje odgovarajućih praksi. Postoji veliki broj standarda, no spomenula bih ove kao najvažnije.

Pitanje 7.

Koja znanja i koju bi obuku po Vama trebali proći svi djelatnici kako bi se povećao prag sigurnosti hotelskih informacijskih sustava?

Odgovor:

Kako bi se povećao prag sigurnosti hotelskih informacijskih sustava, djelatnici hotela trebaju proći temeljnu obuku koja ih educira o ključnim aspektima informacijske sigurnosti. Obuka bi trebala biti usmjerena na prevenciju cyber napada, pravilno rukovanje osjetljivim podacima i prepoznavanje prijetnji. Evo koja znanja i obuke su ključni za sve zaposlenike.

Pitanje 8.

Koja su po Vama bitna mjerila sigurnosti hotelskih informacijskih sustava, odnosno po kojim biste kriterijima ocijenili je li neki hotelski informacijski sustav siguran ili nije?

Odgovor:

Zaštita podataka, integritet podataka, dostupnost potrebnih podataka, autentifikacija i autorizacija i zaštita od vanjskih prijetnji, sigurnosne procedure i politike samog hotelskog sustava i redovito praćenje i nadzor, zakonska usklađenost i na kraju edukacija zaposlenika.

Pitanje 9.

Što su danas po Vama važniji problemi kada je u pitanju sigurnost hotelskih informacijskih sustava: potencijalne ugroze od malicioznog koda koje mogu utjecati na rad informacijskog sustava ili pak krađa podataka? Zašto?

Odgovor:

Danas su i potencijalne ugroze od malicioznog koda i krađa podataka ključni problemi u sigurnosti hotelskih informacijskih sustava, no krađa podataka često predstavlja veći problem zbog direktnih posljedica na povjerenje gostiju i pravne obveze hotela. Zašto? Krađa podataka – financijski i osobni podaci gostiju, maliciozni kod dovodi do operativnog rizika, dovodi do dugoročnih posljedica.

Pitanje 10.

Danas je prisutan trend eksternalizacije obrade i čuvanja podataka kroz koncept računalstva u oblaku. Kako ocjenjujete sigurnost informacijskih sustava koji su obradu i pohranu podataka eksternalizirali u računalni oblak?

Odgovor:

Eksternalizacija obrade i pohrane podataka u računalnom oblaku nudi visoku sigurnost kroz napredne enkripcijske tehnologije i stalni nadzor, no i dalje nosi rizike povezane s povjerenjem trećim stranama i potencijalnim propustima u upravljanju pristupom. Sigurnost ovisi o kvaliteti pružatelja cloud usluga i njihovoj usklađenosti s relevantnim sigurnosnim standardima. Stoga je ključno pažljivo birati provjerene pružatelje i provoditi redovite sigurnosne provjere.

Pitanje 11.

Koje bi osobe za sigurnost trebao imati informacijski sustav, koje na rukovodećim mjestima, a koje na izvršnim mjestima? Kako po Vama sigurnosni podsustav

informacijskog sustava treba biti organiziran, kao centraliziran odjel (služba) ili decentralizirano?

Odgovor:

Informacijski sustav hotela treba imati jasno definiranu strukturu sigurnosnog osoblja na različitim razinama, kako bi se osigurala učinkovita zaštita. Preporučuje se centralizirana struktura za sigurnosni sustav, što omogućuje bolju koordinaciju, standardizaciju politika i učinkovitije upravljanje resursima.

Pitanje 12.

Umjetna je inteligencija nešto novo što će se sigurno koristiti i za potrebe ugroze sigurnosti i za potrebe zaštite od ugroze sigurnosti hotelskih informacijskih sustava. Gdje vidite mogućnosti zloupotrebe s jedne strane i mogućnosti iskorištavanja u svrhu zaštite hotelskih informacijskih sustava s druge strane?

Odgovor:

Umjetna inteligencija ima potencijal za zloupotrebu u hotelskim informacijskim sustavima, primjerice kroz automatizirane cyber napade, poput naprednih phishinga, deepfake prevara ili AI- algoritama koji mogu probiti sigurnosne sustave analizom ranjivosti. S druge strane, AI može značajno poboljšati sigurnost hotelskih sustava kroz proaktivnu detekciju prijetnji, automatizirane odgovore na incidente i analizu ponašanja korisnika kako bi se prepoznale sumnjive aktivnosti prije nego dođe do štete. Uz to, AI može ubrzati praćenje anomalija i rizika, pomažući u realnom vremenu u borbi protiv cyber napada.

Pitanje 13.

Informacijsko-komunikacijska tehnologija se stalno razvija i mijenja oblike funkcioniranja informacijskih sustava, S obzirom na vaša očekivanja glede informacijsko-

komunikacijske tehnologije gdje će u budućnosti biti težište ugroza sigurnosti, a s tim i težište obrane od ugroza sigurnosti hotelskih informacijskih sustava?

Odgovor:

U budućnosti će težište ugroza sigurnosti hotelskih informacijskih sustava biti na naprednim cyber napadima korištenjem AI i IoT uređaja, koji će postati sve češći i sofisticiraniji. Obrana od tih prijetnji zahtijevat će integraciju naprednih analitičkih alata i automatiziranih sigurnosnih rješenja, kako bi se proaktivno detektirali i neutralizirali potencijalni napadi u realnom vremenu.

Pitanje 14.

Ako bi brigu o sigurnosti uprava hotela željela prepustiti specijaliziranoj kući koja bi u outsourceingu održavala hotelski informacijski sustav sigurnim, kojim bi se kriterijima uprava hotela trebala voditi kako bi odabrala optimalnog partnera?

Odgovor:

Uprava hotela trebala bi odabrati partnera temeljem iskustva i stručnosti u industriji, uključujući provjerene reference i uspješne primjere suradnje s drugim hotelima ili sličnim organizacijama. Osim toga, važno je osigurati da partner posjeduje odgovarajuće certifikate i usklađenost s relevantnim sigurnosnim standardima, kao što su ISO 27001 ili ostali koje sam spomenula.

Pitanje 15.

Nakon svih ovih pitanja, smatrate li da sam Vas zaboravila nešto važno pitati vezano za sigurnost informacijskih sustava općenito te vezano za hotelske informacijske sustave?

Odgovor:

Možda biste mogli razmotriti pitanja o novim tehnologijama koje se koriste za poboljšanje sigurnosti, poput blockchain-a ili biometrijske autentifikacije, te o izazovima s kojima se susreću hoteli pri implementaciji sigurnosnih mjera pa bi korisno bilo istražiti kako se hotel može pripremiti za mogućnost sigurnosnih incidenata kroz planiranje oporavka od katastrofa i redovne sigurnosne vježbe.

III. Dubinski intervju s Matijom Prepušt

Pitanje 1.

Molim Vas da mi se ukratko predstavite, te navedete stručnu spremu, školovanje te poslove koje ste do sada profesionalno obavljali, te radno mjesto na kojem se trenutno nalazite vezano za ICT. Odgovor:

Zovem se Matija i u IT-u radim od 2016. godine. Radio sam kao system admin u jednom turističkom poduzeću te kao technical support i routing manager u Messaging-u.

Pitanje 2.

Zbog čega sebe možete smatrati osobom kompetentnom za pitanja sigurnosti informacijskih sustava?

Odgovor:

Kao system admin u turističkom poduzeću, jedan od aspekata je bio i security. U Mesagging-u sam također radio na traženju i blokiranju spamer-a i spoofer-a.

Pitanje 3.

Kako biste definirali hotelski informacijski sustav i što su po Vama njegove specifičnosti u odnosu npr. na informacijske sustave u trgovini ili proizvodnji?

Odgovor:

Današnji hotelski informatički sustavi su slični ako ne i jednaki onima u IT tvrtkama, jer se sastoje od različitih custom, pa čak i in-house made aplikacija koje zadovoljavaju različite potrebe industrije. Od programa za prijave gostiju do različitih sustava za evidenciju i održavanje. Sve više su u upotrebi takozvane pametne sobe koje i same funkcioniraju kao mali zasebni ICT ekosustavi.

Pitanje 4.

Koje su po Vama danas najveće prijetnje u pogledu sigurnosti informacijskih sustava, posebice hotelskih informacijskih sustava?

Odgovor:

Još uvijek različiti hijacker virusi, koji se na različite načine lijepe na servere i domensku mrežu, s ciljem krađe podataka (posebno osobnih podataka), te različiti ransomware-i.

Pitanje 5.

Što po Vama hoteli trebaju činiti da bi osigurali sigurnost informacijskih sustava?
Odgovor:

Educirati osoblje o sigurnom korištenju interneta i štetnosti priključivanja nepoznatog hardware-a na domenu (USB stick-ovi, otvaranje mailova s ransomware virusima, itd). Također uložiti u kvalitetan firewall i backup.

Pitanje 6.

Koje sigurnosne standarde preporučate hotelskim informacijskim sustavima i zašto?
Odgovor:

Nebitno koje standarde, najbitnije je pametno informatičko poslovanje i odgovorna upotreba informatičkih resursa.

Pitanje 7.

Koja znanja i koju bi obuku po Vama trebali proći svi djelatnici kako bi se povećao prag sigurnosti hotelskih informacijskih sustava?

Odgovor:

Osnove internetske sigurnosti - kako prepoznati lažne domene, web stranice i slično, kao tečaj o mogućnostima i limitacijama domenski povezanog sustava. Također neophodan je i tečaj o zaštiti osobnih podataka.

Pitanje 8.

Koja su po Vama bitna mjerila sigurnosti hotelskih informacijskih sustava, odnosno po kojim biste kriterijima ocijenili je li neki hotelski informacijski sustav siguran ili nije?

Odgovor:

Ne postoji u potpunosti siguran sustav, a najbitniji je dobar i redoviti backup.

Pitanje 9.

Što su danas po Vama važniji problemi kada je u pitanju sigurnost hotelskih informacijskih sustava: potencijalne ugroze od malicioznog koda koje mogu utjecati na rad informacijskog sustava ili pak krađa podataka? Zašto?

Odgovor:

Krađa podataka, jer izlaže tvrtku većoj šteti nego što bi je izazvala šteta na informacijskom sustavu. Kao rezultat krađe podataka može doći do potpunog gubljenja povjerenja klijenata.

Pitanje 10.

Danas je prisutan trend eksternalizacije obrade i čuvanja podataka kroz koncept računalstva u oblaku. Kako ocjenjujete sigurnost informacijskih sustava koji su obradu i pohranu podataka eksternalizirali u računalni oblak?

Odgovor:

Ovisno o veličini tvrtke, cloud je praktično i relativno sigurno rješenje (primjer Azure platforme). Za veće tvrtke s centraliziranim sustavom lokalni backup i vatrootporne sobe bi još uvijek trebale biti standard.

Pitanje 11.

Koje bi osobe za sigurnost trebao imati informacijski sustav, koje na rukovodećim mjestima, a koje na izvršnim mjestima? Kako po Vama sigurnosni podsustav informacijskog sustava treba biti organiziran, kao centraliziran odjel (služba) ili decentralizirano?

Odgovor:

Trebao bi sigurno postojati sigurnosni tim koji bi se sastojao od barem jednog domenskog eksperta, DB stručnjaka i nekoga tko bi mogao educirati zaposlenike o digitalnoj sigurnosti.

Pitanje 12.

Umjetna je inteligencija nešto novo što će se sigurno koristiti i za potrebe ugroze sigurnosti i za potrebe zaštite od ugroze sigurnosti hotelskih informacijskih sustava. Gdje vidite mogućnosti zloupotrebe s jedne strane i mogućnosti iskorištavanja u svrhu zaštite hotelskih informacijskih sustava s druge strane?

Odgovor: AI još uvijek nije na razini na kojoj bi mogao biti uspješno korišten u security-u osim za prepoznavanje i filtriranje određenih pattern-a.

Pitanje 13.

Informacijsko-komunikacijska tehnologija se stalno razvija i mijenja oblike funkcioniranja informacijskih sustava, S obzirom na vaša očekivanja glede informacijsko-komunikacijske tehnologije gdje će u budućnosti biti težište ugroza sigurnosti, a s tim i težište obrane od ugroza sigurnosti hotelskih informacijskih sustava?

Odgovor: U budućnosti smatram da će biti još veći naglasak na krađi podataka u svrhu industrijske špijunaže i krađe identiteta.

Pitanje 14.

Ako bi brigu o sigurnosti uprava hotela željela prepustiti specijaliziranoj kući koja bi u outsourcingu održavala hotelski informacijski sustav sigurnim, kojim bi se kriterijima uprava hotela trebala voditi kako bi odabrala optimalnog partnera?

Odgovor: Stabilno poslovanje i dugotrajno iskustvo, prije nego razvikanost i popularnost (primjer Crowdstrike).

Pitanje 15.

Nakon svih ovih pitanja, smatrate li da sam Vas zaboravila nešto važno pitati vezano za sigurnost informacijskih sustava općenito te vezano za hotelske informacijske sustave?

Odgovor:

Važno je napomenuti da je dobra edukacija najbolja prevencija, jer security se još uvijek temelji najviše na sprječavanju ljudske greške u omogućavanju proboja sigurnosne infrastrukture.

IV. Dubinski intervju s Danijelom Gregorovićem

Pitanje 1.

Molim Vas da mi se ukratko predstavite, te navedete stručnu spremu, školovanje te poslove koje ste do sada profesionalno obavljali, te radno mjesto na kojem se trenutno nalazite vezano za ICT. Odgovor:

Ja sam Danijel Grgorović, 27 godina. Po stručnoj spremi sam ekonomist, međutim, uz završene razne tečajeve, zaposlen sam u tvrtki Codx Solutions d.o.o. kao QA Engineer. Moja tvrtka me outsource-ala tvrtki Cora Systems, radi se o jednoj IT kompaniji koja se bavi izgradnjom sustava za vođenje projekata i portfelja. Prije toga, zaposlen sam bio u Cenosco Croatia, također kao QA engineer, gdje sam radio na softverima za sigurnost na naftnim platformama i rafinerijama.

Pitanje 2.

Zbog čega sebe možete smatrati osobom kompetentnom za pitanja sigurnosti informacijskih sustava?

Odgovor:

Cora systems bavi se izradom sustava za vođenje projekata nazvan PMP(project management portfolio). Sa PMP-om klijenti mogu voditi svoje projekte digitalno i vidjeti sve pozadinske procese koji se događaju u stvarnom vremenu, poput troškova, zadataka, aktivnosti, budžeta i raznih reporta. Klijenti dolaze iz svih branši poput medicine, aerospace industrije, željeznica i ostalo.

Pitanje 3.

Kako biste definirali hotelski informacijski sustav i što su po Vama njegove specifičnosti u odnosu npr. na informacijske sustave u trgovini ili proizvodnji?

Odgovor:

Hotelski informacijski sustav po mom mišljenju objedinjuje različite odjele u jedan sustav gdje su uvijek raspoloživi podaci u stvarnom vremenu.

Pitanje 4.

Koje su po Vama danas najveće prijetnje u pogledu sigurnosti informacijskih sustava, posebice hotelskih informacijskih sustava?

Odgovor:

Najveća sigurnosna prijetnja je definitivno krađa podataka (gostiju ili zaposlenika), a tu su onda zlonamjerni virusi, phishing, neovlašteni pristup podacima, loša zaštita Wi-Fi mreže unutar hotela te isto tako i nedovoljna zaštita platnih sustava s kojima gost plaća usluge unutar hotela.

Pitanje 5.

Što po Vama hoteli trebaju činiti da bi osigurali sigurnost informacijskih sustava?
Odgovor:

Prvenstveno smatram da bi trebalo educirati osoblje o prepoznavanju sigurnosnih prijetnji unutar hotela (lopovi) te isto tako edukacija online aktivnosti i kako prepoznati kojim stranicama smiju pristupiti.

Pitanje 6.

Koje sigurnosne standarde preporučate hotelskim informacijskim sustavima i zašto?
Odgovor:

Smatram prvenstveno da, ukoliko hotel ima ISO standard 27001, da zna što radi što se tiče informacijske sigurnosti, iako je u današnje vrijeme teško procijeniti što bi bilo dobro jer je potrebno pratiti trendove i biti u toku sa promjenama.

Pitanje 7.

Koja znanja i koju bi obuku po Vama trebali proći svi djelatnici kako bi se povećao prag sigurnosti hotelskih informacijskih sustava?

Odgovor:

Svi bi trebali proći osnovnu obuku o internetskoj sigurnosti (prepoznavanje lažne domene, lažni mail-ovi, te sumnjivi linkovi).

Pitanje 8.

Koja su po Vama bitna mjerila sigurnosti hotelskih informacijskih sustava, odnosno po kojim biste kriterijima ocijenili je li neki hotelski informacijski sustav siguran ili nije?

Odgovor:

Mislim da danas ne postoji savršeni hotelski informacijski sustav koji je siguran od bilo kakvog napada, ali definitivno, educirani zaposlenici koji znaju prepoznati prijetnje.

Pitanje 9.

Što su danas po Vama važniji problemi kada je u pitanju sigurnost hotelskih informacijskih sustava: potencijalne ugroze od malicioznog koda koje mogu utjecati na rad informacijskog sustava ili pak krađa podataka? Zašto?

Odgovor:

Ako se gleda hotelski informacijski sustav onda definitivno krađa podataka, jer bi napravila veću štetu i uništila ugled samog hotela. A krađa podataka može ugroziti zaposlenike i goste unutar hotela.

Pitanje 10.

Danas je prisutan trend eksternalizacije obrade i čuvanja podataka kroz koncept računalstva u oblaku. Kako ocjenjujete sigurnost informacijskih sustava koji su obradu i pohranu podataka eksternalizirali u računalni oblak?

Odgovor:

Sve više tvrtki je počelo spremati podatke na cloud infrastrukturu, ali ovisno o veličini tvrtke može biti jednostavno rješenje.

Pitanje 11.

Koje bi osobe za sigurnost trebao imati informacijski sustav, koje na rukovodećim mjestima, a koje na izvršnim mjestima? Kako po Vama sigurnosni podsustav informacijskog sustava treba biti organiziran, kao centraliziran odjel (služba) ili decentralizirano?

Odgovor:

Definitivno ako se radi o većim hotelima to jest hotelskim lancima da bi se trebao sastaviti tim stručnjaka koji će se baviti samo sigurnosti hotela i/ili hotelskih lanaca, te bi trebao biti organiziran kao centraliziran odjel.

Pitanje 12.

Umjetna je inteligencija nešto novo što će se sigurno koristiti i za potrebe ugroze sigurnosti i za potrebe zaštite od ugroze sigurnosti hotelskih informacijskih sustava. Gdje vidite mogućnosti zloupotrebe s jedne strane i mogućnosti iskorištavanja u svrhu zaštite hotelskih informacijskih sustava s druge strane?

Odgovor:

To je grana koja je još uvijek u razvoju te smatram da nije pokazala sve svoje prednosti. Ali smatram da bi u odjelu sigurnosti mogla puno pomoći kod ranijeg otkrivanja prijetnji i identifikacije rizika.

Pitanje 13.

Informacijsko-komunikacijska tehnologija se stalno razvija i mijenja oblike funkcioniranja informacijskih sustava, S obzirom na vaša očekivanja glede informacijsko-komunikacijske tehnologije gdje će u budućnosti biti težište ugroza sigurnosti, a s tim i težište obrane od ugroza sigurnosti hotelskih informacijskih sustava?

Odgovor:

Definitivno i dalje će biti veliki problem kod krađe podataka.

Pitanje 14.

Ako bi brigu o sigurnosti uprava hotela željela prepustiti specijaliziranoj kući koja bi u outsourcingu održavala hotelski informacijski sustav sigurnim, kojim bi se kriterijima uprava hotela trebala voditi kako bi odabrala optimalnog partnera?

Odgovor:

Definitivno, dugotrajno iskustvo i stabilno poslovanje.

Pitanje 15.

Nakon svih ovih pitanja, smatrate li da sam Vas zaboravila nešto važno pitati vezano za sigurnost informacijskih sustava općenito te vezano za hotelske informacijske sustave?

Odgovor:

Mislim da za sada su pokrivena sva pitanja što se tiče sigurnosti.

Temeljem dobivenih odgovora može se zaključiti da se svi ispitanici slažu da je najveća sigurnosna prijetnja krađa podataka koja bi mogla ugroziti same zaposlenike te goste. Tri su se ispitanika odredila prema korisnosti certifikata ISO 27001 norme u smislu sigurnosti kroz slijeđenje sigurnosnih protokola dok jedan ispitanik smatra da su norme nebitne, već je bitno pametno informatičko poslovanje i odgovorna upotreba informatičkih resursa. Isto tako, svi ispitanici smatraju da je najvažnija edukacija zaposlenika o sigurnom korištenju informacijsko- komunikacijske tehnologije, osobito interneta. Također, svi ispitanici se slažu da bi trebao biti poseban tim stručnjaka koji su zaduženi za sigurnost hotelskog informacijskog sustava.

7 Zaključak

Evidentno je kako evolucija informacijsko-komunikacijske tehnologije svakodnevno utječe na promjene u načinu poslovanja poslovnih sustava, Ugostiteljstvo, u okviru kojega se nalazi i hotelijerstvo nije pošteđeno utjecaja suvremene informacijsko-komunikacijske tehnologije. Razlozi širokog prihvaćanja novina koje donosi informacijsko-komunikacijska tehnologija su dobrobit koja se ogleda u ubrzanju

poslovnih procesa te njihovom točnijem i ekonomičnijem obavljanju. No, također je evidentno da su sa suvremenom informacijsko-komunikacijskom tehnologijom stigli i negativni izazovi koji nisu postojali u vrijeme manualne obrade podataka. Prije svega treba istaknuti sigurnosne izazove koji ugrožavaju rad informacijsko-komunikacijske tehnologije. Poslovanje se hotela temelji na točnosti podataka i pravodobnom informiranju. To je u domeni rada hotelskog informacijskog sustava. Zbog toga je od ključnog interesa svakog hotela da njegov informacijski sustav bude točan, pravovremen, ekonomičan i da kontinuirano funkcionira. Da bi se to ostvarilo bitna je informacijska sigurnost hotelskog sustava. Zbog važnosti aspekta informacijske sigurnosti hotelskog sustava, odnosno zbog važnosti sigurnosti informacijskog sustava u hotelima, provedeno je istraživanje kojim se željela utvrditi spremnost hrvatskih hotelskih poslovnih sustava da rad vlastitih informacijskih sustava podignu na razinu koja odgovara najvišim standardima informacijske sigurnosti postavljene od strane struke.

Temeljem su disk istraživanja utvrđene značajke informacijskih sustava, a kroz to i hotelskih informacijskih sustava. Također, desk istraživanja su pružila spoznaje o aspektima sigurnosti poslovnih informacijskih sustava, posebice onih u hotelskim poslovnim subjektima. Kroz dobivene rezultate istraživanja utvrđene su vrste ugroza kojima su izloženi hotelski informacijski sustavi, kao i norme koje se koriste u prevenciji i otklanjanju potencijalnih i stvarnih ugroza sigurnosti hotelskog informacijskog sustava. Sagledan je i zakonodavni okvir za osiguranje sigurnosti hotelskih informacijskih sustava, kao i organizacije koje se u Republici Hrvatskoj bave sigurnošću informacijskih sustava i koje mogu biti potpora hotelskim sustavima u osiguranju sigurnosti vlastitih informacijskih sustava. Konačno, provedena su dva empirijska istraživanje, a u okviru prvog su anketirani hoteli kao bi se utvrdilo stanje informacijske sigurnosti u hotelima u Republici Hrvatskoj. Istraživanje je provedeno na malom uzorku, jer se od stotinu poslanih zahtijeva za sudjelovanje u istraživanju, istraživanju odazvalo sedam hotela. Iako se radi o izrazito malom uzorku, rezultati istraživanja se poklapaju s očekivanjima koja su kreirana temeljem iskustva i spoznaja koje su prikupljene kroz neformalne

puteve informiranja. Ovo, probno istraživanje ukazalo je kako hotelski sustavi u Republici Hrvatskoj raspolažu informacijskim sustavima, svjesni su značaja informacijskih sustava, stoga vode brigu o sigurnosti vlastitih informacijskih sustava. Osim što su u radu informacijskih sustava hotela, koji su sudjelovali u istraživanju, implementirane određeni alati za zaštitu od ugroza i protokoli za slučaj ugroza sigurnosti informacijskih sustava, načelno evidentna je i briga o znanjima zaposlenih i prepoznaje se potreba njihovog permanentnog obrazovanja u tom smjeru. Neki se hoteli s problemom ugroze nose samostalno, dok drugi brigu o sigurnosti informacijskih sustava prepuštaju drugim, specijaliziranim poslovnim subjektima. Istraživanja su također pokazala kako je kod većine hotela, koji su sudjelovali u istraživanju, bilo ugroza sigurnosti. Generalno gledano, može se zaključiti kako stanje u hotelima, vezano za sigurnosni aspekt hotelskih informacijskih sustava nije loše, no postoji i značajan prostor za daljnja poboljšanja. Prema tome, generalno gledano, sigurnost informacijskih sustava u hrvatskim hotelskim poslovnim subjektima zadovoljava osnovne sigurnosne standarde struke. Ispitani eksperti, u okviru drugog primarnog istraživanja provedenog dubinskim intervjuom posebno ističu važnost edukacije zaposlenika jer je ljudski čimbenik najčešći uzrok sigurnosnih prijetnji.

Ovo je istraživanje bilo usmjereno na utvrđivanje stanja sigurnosti informacijskih sustava u hotelima u Republici Hrvatskoj te spremnosti hotela za poboljšanjima stanja sigurnosti. Postavljena početna hipoteza zadovoljava dobivene rezultate. Daljnja se istraživanja mogu usmjeriti na pronalaženje modela kojim bi se služili hoteli u ocjenjivanju sigurnosti vlastitih informacijskih sustava te egzaktnih mjerila sigurnosti. Kako se radi o dinamičnom području koje se mijenja iz dana u dan zbog razvitka informacijsko-komunikacijske tehnologije, ovo bi se istraživanje trebalo ponoviti već sljedeće godine, no u značajno većem obujmu.

Literatura

- Barišić, D., *Poslovni informacijski sustavi kao temelj današnjeg poslovanja*, završni rad, Ekonomski fakultet u Osijeku, Osijek, 2021.
- Centar Informacijske sigurnosti-COBIT 5 framework, CIS, Dostupno na: https://www.cis.hr/dokumenti/5348-cobitframework-5.html [pristupljeno 24.4.2023]

- Chopra, A. i M. Chaudhary, *Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines*, Apress L.P., New York, 2020.
- Digitalna transformacija javne uprave, APIS IT, Dostupno na: https://www.apis-it.hr/apisit/index.html#/page?docId=862092FC53B6F468C1257F400043EACF [pristupljeno 6.9.2023]
- Galičić V., *Poslovanje hotelskog odjela smještaja*, Sveučilište u Rijeci, Fakultet za menadžment u turizmu i ugostiteljstvu u Opatiji, Opatija, 2017.
- Informacijski sustav, Hrvatska enciklopedija, mrežno izdanje, Leksikografski zavod Miroslav Krleža, Dostupno na: https://www.enciklopedija.hr/clanak/informacijski-sustav [pristupljeno 18.6.2024]
- Galičić V. i M. Šimunić, *Informacijski sustavi i elektroničko poslovanje*, Sveučilište u Rijeci, Fakultet za turistički i hotelski menadžment u Opatiji, 2006.
- Strahonja, V., M. Varga i M. Pavlić, *Projektiranje informacijskih sustava*, Zavod za informatičku djelatnost Hvatske i INA-INFO, Zagreb, 1992.
- Informacijski sustavi, fpz, Dostupno na: https://www.fpz.unizg.hr/ztos/iszp/a2.pdf [pristupljeno 24.4.2023]
- Mesarić, J.: *Informacijski sustavi u poslovanju - ciljevi, zadaci i izgradnja informacijskih sustava, prezentacija*, Ekonomski fakultet u Osijeku, Osijek, 2015., Dostupno na: http://www.efos.unios.hr/informatika/wp-content/uploads/sites/202/2013/04/P11_Info_sustavi.pdf [pristupljeno 24.4.2023]

- Norme za informacijsku sigurnost, Dqsglobal, Dostupno na: https://www.dqsglobal.com/hr- hr/edukacija/blog/norme-za-informacijsku-sigurnost-pregled [pristupljeno 23.9.2024]
- O nacionalnom CERT-u, CERT.hr,Dostupno na: https://www.cert.hr/onama/ [pristupljeno 6.9.2023]

- PDCA krug, svijet-kvalitete.com, Svijet kvalitete, Dostupno na: https://www.svijet-kvalitete.com/index.php/upravljanje-kvalitetom/948-pdca-krug [pristupljeno 23.9.2024]
- Pravni okvir, Agencija za zaštitu osobnih podataka, Dostupno na: https://azop.hr/djelokrug/ [pristupljeno 6.9.2023]
- Shabani, N. i A. Munir, *A review of cyber security issues in hospitality industry*, srpanj 2020., (PDF) A Review of Cyber Security Issues in Hospitality Industry (researchgate.net) , (pristupljeno 23.09.2024.)
- Praničević Garbin, D., S. Pivčević i Ž. Garača, *Razvijenost informacijskih sustava velikih hotelskih poduzeća u Hrvatskoj*, Acta Turistica Nova, vol.4. No.2, 2010. Dostupno na: https://hrcak.srce.hr/107014 (pristupljeno 01.09.2023.)
- Hrvatska akademska i istraživačka mreža CARNet, Sigurnosna politika CCERT-PUBDOC-2009-05-265, Revizija 1.04, Zagreb, Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2009-05-265.pdf [pristupljeno 23.9.2024]
- Središnji državni ured za razvoj digitalnog društva, e-Građani, Dostupno na: https://rdd.gov.hr/o- sredisnjem-drzavnom-uredu/djelokrug-138/138 [pristupljeno 6.9.2023]
- Standardi poslovanja, Storm.hr , Dostupno na: https://www.storm.hr/index.php/hr/o-nama/standardi-poslovanja [pristupljeno 23.9.2024]
- Što je CRM i što se iza njega krije, Poslovna.hr, Dostupno na: https://www.poslovni.hr/lifestyle/sto-je- crm-i-sto-se-iza-njega-krije-307951 [pristupljeno 5.9.2024]
- The History of ISO 27001, Secureframe.com,Dostupno na: https://secureframe.com/hub/iso-27001/history [pristupljeno 23.9.2024]
- Upravljanje poslovnim rizicima, Poslovni.hr, Dostupno na: http://www.poslovni.hr/poslovni-centar- znanja/upravljanje-poslovnim-rizicima-306103 [pristupljeno 8.1.2023]

- Upravljanje resursima poduzeća, Oracle, Dostupno na: https://www.oracle.com/hr/erp/what-is-erp/ [pristupljeno 5.9.2024]
- Zakon o informacijskoj sigurnosti, Narodne Novine 79/2007, Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2007_07_79_2484.html [pristupljeno 6.9.2023]
- Zakoni Republike Hrvatske vezani uz informacijsku sigurnost i zaštitu podataka, FOI, Dostupno na: https://security.foi.hr/wiki/index.php/Zakoni_Republike_Hrvatske_vezani_uz_informacijsku_sigurnost_i_za%C5%A1titu_podataka.html#Zakonska_regulativa_informacijske_sigurnosti_u_Republici_Hrvatskoj [pritupljeno 9.1.2023]
- Zašto je ISO 27001 dobar za vašu tvrtku?, Advisera.com, Dostupno na: https://advisera.com/27001academy/hr/sto-je-iso-27001/ [pristupljeno 23.9.2024]
- Zavod za sigurnost informacijskih sustava, ZNIS, Dostupno na: https://www.zsis.hr/default.aspx?id=13 [pristupljeno 6.9.2023]

Popis grafikona

Popis slika