Kibernetička sigurnost

Požega, Ivan William

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni prijediplomski studij

IVAN WILLIAM POŽEGA

Kibernetička sigurnost – povrede podataka u hotelima

Cybersecurity – Data breaches in hotels

Završni rad

Opatija, 2024.

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Sveučilišni prijediplomski studij
Poslovna ekonomija u turizmu i ugostiteljstvu
Studijski smjer: Menadžment u hotelijerstvu

Kibernetička sigurnost – povrede podataka u hotelima

Cybersecurity – Data breaches in hotels

Završni rad

Kolegij:	**Sigurnost informatičkih sustava**	Student:	**Ivan William Požega**
Mentor:	**izv. prof. dr. sc Ljubica Pilepić Stifanich**	Matični broj:	**PS25235/20**

Opatija, lipanj 2024.

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

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Ivan William Požega	**PS25235/20**
(ime i prezime studenta)	(matični broj studenta)

Kibernetička sigurnost – povrede podataka u hotelima
(naslov rada)

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

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

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

U Opatiji, lipanj, 2024

Potpis studenta

Sažetak

Kibernetička sigurnost u hotelijerstvu postaje ključna zbog rastućeg utjecaja tehnologije i interneta stvari (IoT). Kibernetika je disciplina koja se bavi upravljanjem složenih sustava te osigurava temelje za zaštitu digitalne infrastrukture hotela. Kako hoteli postaju ranjiviji na napade poput ransomware–a i krađe podataka, kibernetička sigurnost postaje imperativ u današnjem svijetu. Stoga strategije za očuvanje kibernetičke sigurnosti, poput strategije koju provodi Republika Hrvatska, igraju ključnu ulogu u zaštiti osjetljivih podataka i održavanja sigurnosti digitalnog prostora. Svrha rada je ukazati na problem kibernetičkih napada te objasniti njihov utjecaj na poslovanje hotelskih poduzeća. Cilj je pružiti dublji uvid u izazove s kojima se suočavaju hoteli u održavanju sigurnosti svojih digitalnih sustava i podataka gostiju. Prema nalazima može se zaključiti kako će budućnost kibernetičke sigurnosti zahtjevati integraciju naprednih tehnologija koja će istovremeno služiti za održavanje visokih standarda sigurnosti podataka i prevencije napada. Sustavna zaštita podataka i digitalnih sustava postat će sve važnija kako bi se osigurao integritet podataka i stabilnost poslovanja u hotelijerstvu uz rastuće izazove u digitalnom okruženju hotelijerstva.

Ključne riječi: Sigurnost, kibernetika, hotelijerstvo, internet stvari

Sadržaj

UVOD

Predmet, ciljevi i metode istraživanja

U današnjem digitalnom dobu, gdje tehnološki napredak postaje sveprisutan u svim segmentima društva, kibernetička sigurnost postaje imperativ za održavanje integriteta, povjerenja i stabilnosti poslovanja, uključujući i sektor hotelijerstva. S razvojem internetskih povezanosti, digitalnih sustava za rezervaciju, obrade plaćanja i upravljanja gostima, hotelijerstvo je postalo sve ranjivije na širok spektar kibernetičkih prijetnji poput phishinga, socijalnog inženjeringa, malware-a i ransomware-a. Predmet ovog istraživanja je utjecaj kibernetičkih proboja i krađe podataka na poslovanje hotelske industrije. Glavni problem koji će ovaj rad istražiti jest kojim postupkom hotelske kompanije mogu osigurati svoj kibernetički prostor i smanjiti negativne posljedice kibernetičkih proboja.

Svrha rada je pružiti dublji uvid u izazove s kojima se suočavaju hoteli u održavanju sigurnosti svojih digitalnih sustava i podataka gostiju. Ovaj završni rad fokusira se na istraživanje i analizu kibernetičke sigurnosti u kontekstu hotelijerstva.

Osnovni ciljevi rada su sljedeći:

- definirati osnovne kibernetičke prijetnje;
- analizirati osnovne metode kibernetičke zaštite;
- objasniti utjecaj kibernetičkih proboja na poslovanje u hotelskoj industriji;
- identificirati stanje kibernetičke sigurnosti u Republici Hrvatskoj.

Iz tako postavljenog predmeta i ciljeva istraživanja mogu se formulirati sljedeća istraživačka pitanja:

1. Koje su osnovne kibernetičke prijetnje u suvremenom poslovanju?
2. Koje se osnovne metode zaštite primjenjuju u očuvanju kibernetičke sigurnosti?
3. Kakav je utjecaj kibernetičkih napada na poslovanje u hotelskoj industriji?
4. Kakvo je stanje kibernetičke sigurnosti u Republici Hrvatskoj?

U radu su za potrebe istraživanja korišteni sekundarni podaci iz relevantnih izvora. Primjenjuju se sljedeće metode istraživanja: metoda sinteze, metoda analize, metoda dokazivanja, povijesna metoda, te metode dedukcije i indukcije.

Struktura rada

Ovaj završni rad sastoji se od pet poglavlja sa uvodom, zaključkom, popisom bibliografije i ilustracijama. Uvodno poglavlje rada obuhvaća problematiku i predmet istraživanja, svrhu i ciljeve istraživanja, opis znanstvenih metoda te kratak pregled strukture rada.

Prvo poglavlje rada odnosi se na kibernetiku kao pojam, vrste kibernetičkih prijetnji te kibernetičku zaštitu u hotelskim poduzećima.

Drugo poglavlje rada odnosi se na Internet stvari (IoT), novu paradigmu koja je dobila na značaju u modernoj bežičnoj telekomunikaciji. Ovdje se razmatra svrha Interneta stvari u poslovanju hotelske kompanije te sama implementacija IoT-a s ciljem poboljšanja doživljaja gostiju.

Treće poglavlje rada opisuje kibernetičku sigurnost u hotelijerstvu, analizirajući prosječne troškove povrede podataka i statistike kibernetičkih proboja. Razmatraju se četiri najveća i najpoznatija proboja podataka u hotelskoj industriji te njihov utjecaj na buduće poslovanje. Također se istražuju načini zaštite kibernetičkog prostora koji su mogli spriječiti proboje i smanjiti njihov budući utjecaj na poslovanje.

Četvrto poglavlje opisuje trenutno stanje kibernetičke sigurnosti u Republici Hrvatskoj. U njemu se razmatra uloga Nacionalnog CERT-a kao pružatelja godišnjeg izvještaja o stanju kibernetičke sigurnosti u Republici Hrvatskoj, te akcijski plan za provedbu nacionalne strategije kibernetičke sigurnosti.

Peto poglavlje opisuje budućnost kibernetičke zaštite u hotelijerstvu te analizira kako hotelska industrija može osigurati zaštitu podataka klijenata uz pomoć digitalne transformacije i napredne tehnologije.

Nakon toga slijedi zaključak ovog završnog rada, u kojem se sintetizira važnost kibernetičke sigurnosti u hotelijerstvu, s posebnim naglaskom na načine zaštite. Na samom kraju rada nalazi se popis bibliografije i ilustracija.

1. KIBERNETIKA

Kibernetika, skupni naziv niza teorijskih disciplina i praktičnih postupaka koji se primjenjuju pri upravljanju i vođenju složenih sustava[1], također obuhvaća skup mjera, standarda i procesa koji su usmjereni na osiguranje pouzdanosti prilikom korištenja usluga ili proizvoda u kibernetičkom prostoru. Kibernetički sustav sastoji se od triju cjelina koje se dijele na : podsustava za prikupljanje informacija o trenutnom stanju sustava, podsustava koji uspoređuje trenutno stanje s željenim stanjem radi utvrđivanja razlike odnosno pogreške, te podsustava koji djeluje na ponašanje sustava kako bi smanjio te razlike. Zaštita računala, računalnih mreža, informatičke infrastrukture imaju ključnu ulogu u postizanju te pouzdanosti. Za uspješan pristup kibernetičkoj sigurnosti moraju se postaviti višestruki slojevi zaštite raspoređeni po računalima, mrežama, programima ili podacima koje želimo sačuvati od potencijalnih proboja. U organizaciji, ljudi, procesi i tehnologija moraju se međusobno nadopunjavati kako bi se stvorila učinkovita obrana od kibernetičkih napada. Kibernetičke prijetnje također bilježe kontinuirani rast na globalnoj razini,a razne vrste mogućih napada postaju složenije i utječu na svakodnevni život te poslovanje. Postoje različiti oblici zlonamjernih programa, računalnih prijevara te krađa osobnih i financijskih podataka, stoga je iznimno važno biti svjestan mogućih kibernetičkih prijetnji te važnosti kibernetičke sigurnosti. Republika Hrvatska je 2015. godine objavila Nacionalnu strategiju kibernetičke sigurnosti i akcijskog plana za njezinu provedbu kojima nastoji započeti sustavno planiranje aktivnosti koje će imati svrhu zaštite svih korisnika elektroničkih usluga unutar gospodarstva te građanstva. Strategijom se želi postići zaštita svih sektora društva s obzirom na prijetnje u suvremenom kibernetičkom svijetu.

[1] Hrvatska enciklopedija, (2024), mrežno izdanje. Kibernetika https://www.enciklopedija.hr/clanak/kibernetika. (pristupljeno 15.05.2024.)

1.1. Kibernetičke prijetnje

ENISA (European Union Agency for Cybersecurity) je agencija Europske unije koja se bavi kibernetičkom sigurnošću u cijeloj Europskoj uniji te postoji od 2004. godine[2]. Agencija ENISA godišnje izdaje izvještaj o stanju kibernetičkih prijetnji u Europskoj uniji. Izvještaj uključuje glavne prijetnje, ključne trendove uočene u pogledu prijetnji, tehnike koje koriste napadači, te opisuje relevantne mjere kojima se može ublažiti ili spriječiti proboj napadača. Prijetnje su sortirane u osam skupina te su poredane po učestalosti i utjecaju koji imaju na rizik.

Ransomware (Ucjenjivački softver) je vrsta štetnog programa koja korisniku uskraćuje pristup računalnim resursima i traži plaćanje otkupnine za vraćanje pristup datotekama. Ransomware se također još opisuje kao manipulativni program s osvrtom na ljudsku psihologiju jer se dotiče ne samo uzimanja podataka već manipuliranjem pojedinca te iznuđivanjem novca od istog. Prema ENISI 60 posto pogođenih organizacija koje su prijavile problem, platile su zahtjeve za otkupninu koje su napadači zatražili. Ova vrsta napada je učestala u hotelijerstvu baš zbog osjetljivosti podataka koje gosti ostavljaju hotelu prilikom dolaska u hotel.

Malware (zloćudni softver) je vrsta štetnog programa koji radi štetu korisniku. Pokreću se na računalnom sustavu bez pristanka korisnika računala te imaju nepoželjan učinak na računalo i na podatke od korisnika. Krađa osjetljivih i povjerljivih podataka kao što su brojevi kreditnih kartica. Malware se dijeli na računalni virus, trojanski konj, računalni crv, spyware i adware, a svakodnevno se stvaraju nove verzije, koje postaju štetnije za korisnikovo računalo. Jedan od najzloćudnijih programa to jest malwarea koji napadači koriste za napad na hotelske lance jest Keylogger. To je vrsta malicioznog programa koji prati unos preko tipkovnice te tih bilježi u dnevnik (log). Na taj način mogu uhvatiti osjetljive informacije poput korisničkog imena, PIN–ova te omogućiti napadaču informacije koje mu trebaju.[3]

[2] Enisa.europa.eu, (2024); European Union Agency for Cybersecurity, https://www.enisa.europa.eu/ pristupljeno (15.05.2024.)
[3] Rajendra, K.R., Wood, C.A., (2010). Keyloggers in Cybersecurity Education, Rechester Institute of Technology, str. 293.

Socijalni inženjering je niz tehnika koje napadač koristi kako bi iskoristio ljudske pogreške te naveo pojedinca da napravi nešto što nije u njegovom interesu. Napadači koriste ovakve tehnike kada žele dobiti informacije ili resurse do kojih drugačije ne bi mogli doći to jest putem malware–a ili softvera. Socijalni inžinjering dijeli se na tri glavna oblika: phishing, vishing i lažno predstavljanje. Svaki od ta tri oblika vrsta je manipulacije kojom se pokušava prevariti korisnika te napraviti iznudu od njega.

Prijetnje podacima te prijetnje dostupnosti poznatije pod imenom **DDoS napad** je vrsta napada u kojoj napadač koristi računalne mreže putem mrežnih paketa te iskorištava ranjivost pojedinca kako bi mu uskratio pristup na internetu ili preuzeo osjetljive informacije od korisnika. U srpnju 2022. Europu je pogodio najveći DDoS napad u povijesti. Ovaj napad pogodio je korisnike računala te mobilnih uređaja. Europska unija je zbog ovakvih napada počela znatno ulagati u zaštitu pojedinaca unutar Europske unije i u kibernetičku sigurnost.[4]

Dezinformiranje je navedeno kao sedma grupa opasnosti koje vrebaju u kibernetičkom prostoru. Gledajući današnju situaciju u kojoj se koriste metode poput deepfake (umjetnom inteligencijom stvorena lažna slika), te korištenje umjetne inteligencije kako bi se dezinformiralo i prevarilo korisnika te se stvorila dobit nad njime.

Haktivizam je uporaba tehnologije za promoviranje političkih programa i društvenih promjena[5]. Novi val takozvanog političkog haktivizma aktivirao se znatno od Rusko–ukrajinskog rata te stvara određenu prijetnju običnom korisniku, ali i većim kompanijama.

[4] Negreiro M., (2023), Managed security services in Europe, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754556/EPRS_BRI(2023)754556_EN.pdf (pristupljeno 16.05.2024)

[5] Jordana J. G., Leidner D., (2019), From clicktivism to hacktivism: Understanding digital activism; Information and Organization, 29(3), str. 3.

1.2. Kibernetička zaštita

U današnjoj eri digitalizacije i povezanosti, kibernetička sigurnost postaje jedna od ključnih tema za svakog korisnika interneta. Koncept kibernetičke sigurnosti obuhvaća sve mjere koje se poduzimaju radi zaštite računalnih sustava, mreža i podataka od pokušaja proboja, to jest pokušaja krađe i oštećenja. Digitalno doba gdje se infromacije prenose brzinom svjetlosti te gdje se tehnološki napredak odvija svakodnevno, potreba za kibernetičkom sigurnošću je veća nego ikad. Kako raste broj kibernetičkih prijetnji, tako se kibernetička sigurnost svakodnevno nadograđuje i dobiva zakrpe za razne vrste prijetnji i napada koji se stalno pojavljuju.

Prvo i osnovno načelo kibernetičke sigurnosti je prevencija samog zločina odnosno proboja, međutim čak i uz najbolje preventivne mjere, napadi se mogu dogoditi baš zbog učestalosti i napretka koji napadači ostvaruju svakog dana. Kibernetička sigurnosti osim zaštite sustava ima cilj zaštiti aplikacije, računalne uređaje, osjetljive podatke i financijska sredstva pojedinca ili organizacije. Vodeća američka tvrtka za razvoj računala i informacijskih tehnologija IBM (International Business Machines) je u 2023. godini provela istraživanje te je došla do zaključka kako zbog kibernetičkih napada je prosječno u 2023. godini izgubljeno 4,45 milijuna dolara, što je 15 posto više u odnosu na prošle tri godine. Prosječni gubitak zbog ucjenjivačkih softvera (ransomware) iznosio je 5,13 milijuna dolara što je prosječno 20 posto više u odnosu na prošle godine. Prosječna cijena koju su žrtve platile ucjenjivaču iznosila je 1,542,333 dolara, što je 89 posto više nego prošle godine. Prema jednoj procjeni IBM – a, kibernetički kriminal bi svjetsku ekonomiju mogao oštetiti 10,5 milijardi dolara godišnje do 2025. godine.[6]

Osim prevencijom, kibernetička sigurnost se također bavi i detekcijom, koja je vrlo bitna u kibernetičkom svijetu jer, kako je prije napomenuto, svakodnevno se stvaraju novi programi i nove vrste napada, te je samim time sve teže identificirati i detektirati mogući proboj sustava. Najpoznatiji alati za detekciju upada u mrežu su IDS (Intrusion Detection Systems) i IPS (Intrusion Prevention Systems). NIST (Bace i Mell, 2001) opisuju upad u

[6] Ibm.com, (2024), What is cybersecurity?; https://www.ibm.com/topics/cybersecurity (pristupljeno 17.05.2024)

kibernetički prostor uz narušavanje tri ključna aspekta: povjerljivosti, integriteta te dostupnosti. Putem IDS i IPS sustava radi se analiza kako bi se pronašli znakovi upada.

Reakcija na incidente također je ključna komponenta kibernetičke sigurnosti. Nakon odvijanja napada, brza i koordinirana reakcija može znatno smanjiti štetu te u nekim slučajevima identificirati propust i napraviti zakrpu za njega. Takva reakcija uključuje izolaciju zaraženih sustava, analizu štete, povratak na sigurnosne kopije podataka te identifikaciju izvora napada radi sprječavanja budućih napada.

Uz navedene tri komponente moguće zaštite od kibernetičkih prijetnji, obrazovanje korisnika je također važan aspekt kibernetičke sigurnosti. Ljudski faktor, pogotovo u većim kompanijama, predstavlja slabu točku u sigurnosnim sustavima. Edukacija korisnika i zaposlenika kompanija o sigurnosnim praksama, što uključuje snažne lozinke, pravilno korištenje sigurnosnih alata te oprez pri otvaranju mailova i stranica, može pomoći u smanjenju rizika od kibernetičkih napada.

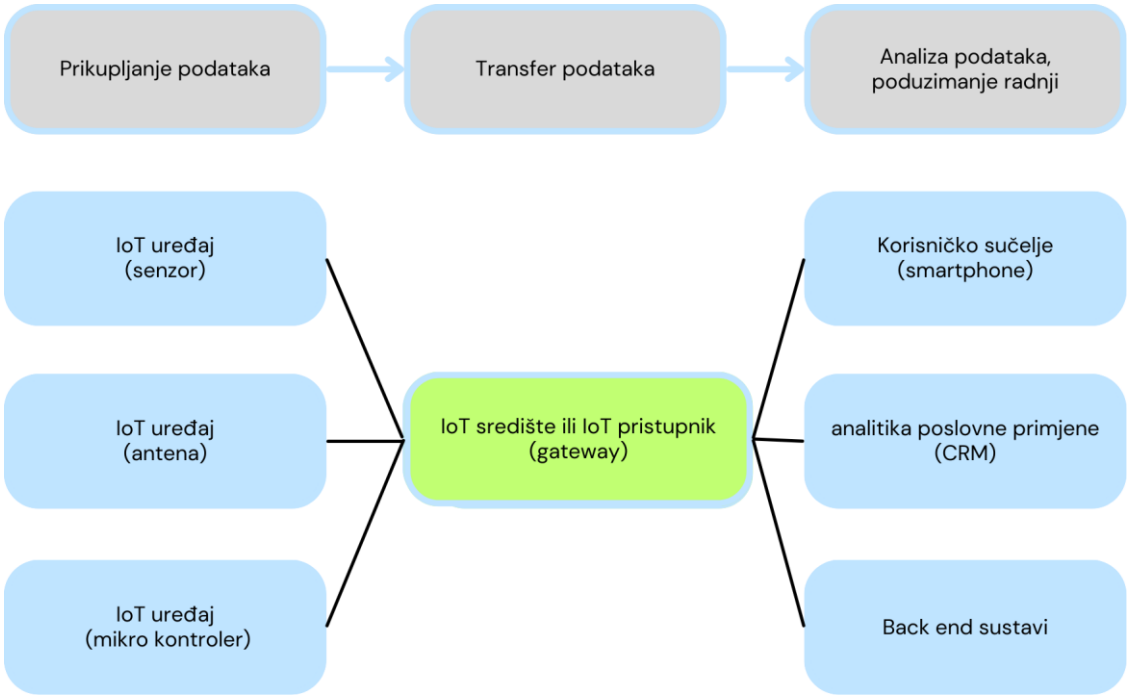
Unatoč svim naporima, kibernetička zaštita je neprestano evoluirajući izazov. Napadači razvijaju nove tehnike i tehnologije kako bi probili sigurnosne barijere. Zbog toga je neophodno da se obrambene strategije kontinuirano prilagođavaju i poboljšavaju.

2. INTERNET OF THINGS (IoT)

Internet of Things je nova paradigma koja je brzo dobila na značaju u modernoj bežičnoj telekomunikaciji. Osnovna ideja je sveprisutnost različitih stvari ili objekata oko nas koji se povezuju na internet. Takve stvari ili objekti poput senzora, mobitela, računala putem jedinstvenih adresnih shema mogu međusobno komunicirati i surađivati kako bi postigli zajedničke ciljeve[7]. Glavna snaga ideje Internet of Things–a je visoki utjecaj koji će imati na svakodnevni život i ponašanje potencijalnog korisnika. Ovakav utjecaj najviše se vidi u pogledu privatnog korisnika jer će utjecaj biti vidljiv i u radnom i u domaćem okruženju. U tom kontekstu stavke poput e–građana, digitalne podrške, e–dnevnika su primjene IoTa koje će imati vodeću ulogu u bliskoj budućnosti. S poslovne perspektive najvidljivije posljedice će biti u automatizaciji i industrijskoj proizvodnji te logistici. IoT sustav radi na principu prikupljanja podataka, zatim prijem i transfer podataka putem prolaza (gateway) te se ti podaci analiziraju i odvija se određena radnja kojom se ti podaci prenose korisniku.

Internet stvari je privukao značajnu pažnju u posljednjih par godina, pogotovo tijekom Covid–19 godina kada je sve bilo online. IoT se smatra internetom budućnosti koji će obuhvatiti milijarde pametnih uređaja koji će moći međusobno komunicirati. Također budućnost interneta ovisi o tim povezanim uređajima koji će dodatno proširiti granice svijeta i povezati se sa fizičkim entitetima i virtualnim komponentama, te osnažiti povezane uređaje novim mogućnostima. Razvoj IoT također je i razvoj turizma i hotelijerstva jer će sve povezane uređaje lakše implementirati određene ideje koje su trenutno nedostupne s obzirom na razvoj tehnologije. [8]

[7] Atzori, L., Iera, A., & Morabito, G. (2010), The Internet of Things: A survey, Computer Networks, 54(15), str. 2787.
[8] Atzori, L., Iera, A., & Morabito, G. (2011), SIoT: giving a social structure to the internet of things. IEEE Communication Letters, 15(11), str. 1193.



Slika 1. Primjer Internet of things sustava

Izvor: Izrada autora prema Gillis, A., (Aug 2023), Internet of Things (IoT), Techtarget, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (pristupljeno 19.05.2024)

Internet stvari funkcionira na način da se određeni uređaj u ovom slučaju senzor, antena, mikro kontroler koji prikupljaju podatke, spoje putem interneta na IoT središte takozvani gateway gdje se odvija transfer podataka, te putem pristupnika podaci se šalju na korisničko sučelje, CRM, Back end sustave gdje se podaci prikupljaju, analiziraju te nakon toga se poduzimaju radnje na temelju prikupljenih podataka. [9]

[9] Gillis, A., (Aug 2023), Internet of Things (IoT), Techtarget, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (pristupljeno 19.05.2024)

2.1. Svrha Internet of Things (IoT) u hotelijerstvu

Uređaju povezani putem Interneta stvari (IoT) došli su do statusa glavne tehnologije u današnje vrijeme, dok su se prije par godina smatrali novom tehnologijom.[10]. Jedna od industrija gdje je ova tehnologija naišla na široku primjenu i razvoj je sektor turizma, ugostiteljstva i hotelijerstva. IoT je donio značajne promjene u turizmu, potencijalno uzrokujući velike promjene, posebno u smislu personaliziranih usluga, sigurnosnih poboljšanja te operativnu optimizaciju. Ovo su četiri najznačajnije promjene koje je IoT omogućio u turizmu:[11]

1. **Personalizacija** – razvoj turizma donio je i nove ključne aspekte od kojih je trenutno najvažnija personalizacija iskustva gosta. Gost može izraziti svoje želje te putem IoT dobiti informacije koje će ga uputiti u sadržaje koji će mu ponuditi iskustvo, proizvode te usluge koje želi, poput restorana, događaja, muzeja itd. Također usluge poput virtualnog asistenta koji će odgovarati na pitanja turista i nuditi im personalizirane usluga poput prevođenja stranih jezika.
2. **Pomoć nadohvat ruke** – Sigurnost turista je postala ozbiljna zabrinutost za turiste i putnike, posebno kada se posjećuju strane zemlje koje imaju drugačiju kulturu te gdje je potreban komunikacijski jezik koji nije materinji turistu. Uz pomoć IoT uređaja može se ojačati sigurnost u turističkim destinacijama, hotelima i transportnim čvorištima te praćenje videozapisa u stvarnom vremenu i ažuriranje lokacija. Ključne informacije poput hitnih kontakata, policije, bolnice te hitne pomoći također se mogu ukomponirati kako bi se pomoć pozvala istog trenutka kada se turistu nešto dogodi.
3. **Kontrola kroz automatizaciju** – Putem IoT–a, turistu se može pružiti veća kontrola nad određenim pogodnostima putem tableta ili vlastitog pametnog telefona. Tu se smatra kako gost u budućnosti može kontrolirati temperaturu i osvjetljenje u svojoj sobi u hotelu ili usluge poput usluge u sobi. Također turist

[10] Kaur, K. & Kaur, R., (2016), Internet of things to promote tourism: An insight into smart tourism, International Journal of Recent Trends in Engineering & Research, 2(4), str. 357.
[11] Smith, A., (Oct 12, 2023), Iot in Travel and Tourism, Medium, https://web-and-mobile-development.medium.com/iot-in-travel-and-tourism-industry-why-it-is-a-game-changer-cf168df4753 (pristupljeno 19.05.2024.)

slične usluge i postavke se mogu koristiti tijekom letova ili u restoranima za rezerviranje stolova, to jest povezati svo iskustvo koje gost dobije na putovanju u jedno.

4. **Pomoć u prirodnom turizmu** – Prirodni turizam je u zadnjih par godina privukao globalnu pozornosti, ljudi ne žele više ići na pretrpane plaže već žele se opustiti i dobiti jedno jedinstveno iskustvo koje svaki turist i zaslužuje. Ekolozi uz pomoć IoT mogu turistima pružiti adekvatne podatke poput vremenskih uvijeta, temperatura, vlaga i sl. Ovi podaci se mogu koristiti kako bi turisti mogli primiti brzo i efikasno informacije te kako bi se spriječile moguće nesreće.

2.2. Implementacija IoT u hotelijerstvu

IoT također nudi mogućnost poboljšanja korisničkih usluga i povećanja povrata investicija. Da bi ostale konkurentne i zadovoljile sve zahtjevnija očekivanja turista, tvrtke u turističkoj industriji trebale bi početi ulagati u sustave temeljene na IoT-u. IoT brzo postaje potreba, a ne luksuz. Turisti i menadžeri u industriji prilagođavaju se ovoj novoj eri, koja će, kako se očekuje, temeljito promijeniti industriju putovanja u skoroj budućnosti. Mnogi hoteli poput Wynn Resorta u Las Vegasu implementirali su IoT u najvišem smislu. Točnije napravili su pametne sobe uz pomoć Amazon Alexe, pametnog pomoćnika koji se može spojiti na internet te putem njega riješavati razne probleme koje mu turist zada. Samim time turisti mogu putem mobitela ili glasovnim komandama mjenjati temperaturu u sobi, pozvati poslugu u sobu ili rezervirati stol u restoranu. Wynn resort je zbog ideje i implementacije pametne sobe osvojio Fores Travel Guide u 2019. godini. Poznati lanac hotela Marriot također je odlučio implementirati IoT u svoj hotel u Singapuru. W Singapore – Sentosa Cove je hotel sa pet zvjezdica na otoku Sentosa u Singapuru koje svojim gostima pruža „futurističke“ usluge za svakog gosta.[12] U sobama u Sentosa Cove hotelu nalazi se LED display preko kojega gost može svaku uslugu ili proizvod iskoristiti i naručiti. Primjer ova

[12] Sbounias, J., (30 Jul, 2019), Smart hotel around the world that highlighted new global trend, Hotelier Academy, https://www.hotelieracademy.org/5-smart-hotels-that-confirm-the-potentials-of-this-new-hotel-trend/ (pristupljeno 20.05.2024)

dva hotela iz poznatih lanaca nam pokazuje kako IoT se razvija vrlo brzo i efektivno ne samo u informatici već i u turizmu i hotelijerstvu.

Moderni pametni objekti poput novih elektroničkih ručnih satova, alarma koji se nalazi u hotelskim sobama koriste se već godinama te ih je lako implementirati u sam hotelski sustav. Predviđa se da će se broj IoT uređaja širom svijeta porasti na gotovo 30 milijardi do 2030. godine. Svi navedeni pametni hoteli imaju isti misiju: pružiti prilagođeno iskustvo i brzo reagirati na sve potrebe svojih gostiju. Neki hoteli osiguravaju svojim gostima pri dolasku u hotel tablete sa kojima je moguće upravljanje svim funkcijama u sobi, dok drugi nude vlastite aplikacije koji se preuzimaju na mobilne telefone. Mnogi hoteli također ulažu u umjetnu inteligenciju te robotsku tehnologiju poput nosača ili batlera te samim time riješavaju kadrovsko pitanje, a pružaju svojim gostima jedinstven osjećaj. Gradski hoteli značajno ulažu u ove vrste tehnologija.

3. KIBERNETIČKA SIGURNOST U HOTELIJERSTVU

Do prije nekoliko godina, turističko tržište se uglavnom smatralo fizičkim prostorom, manji ili veći gdje su se prodavači i kupci različitih turističkih proizvoda i usluga mogli sastajati. Razmjene su se također odvijale kroz fizički kontakt na lokalnoj i međunarodnoj razini, tako da sigurnost u tome smislu označavala zaštitu ljudi od opipljivih prijetnji poput prevara, krađa, otimanja i slično. Današnje vrijeme je donijelo i nove izazove koja se više ne odnose samo na fizički prostor. Tržišta postaju kibernetički prostori gdje se prodavači, trgovci i kupci mogu sastati i odraditi razmjenu usluga i proizvoda bez potrebe za fizičkim kontaktom. Internet prevare, krađe identiteta, krađe podataka od kompanija ili individualaca te korištenje istih podataka u nelegane svrhe. Samim time hotelijerstvo te turizam je doživjelo veliki udar najviše tijekom COVID – 19 pandemije gdje nema hotela i kompanije koja nije doživjela barem jedan pokušaj prevare ili proboja u sustav. [13]

Najveće prijetnje za kibernetičku sigurnost u hotelijerstvu su: Čitači kartica/POS sustavi koje omogućavaju u hotelijerstvu i ostalim popratnim industrijama praktično plaćanje, ali stvaraju povećani potencijalni rizik od krađe podataka. POS uređaji sami po sebi ne obrađuju transakcije već upravljaju inventarom, te kriminalci upravo zbog ovakvih razloga koriste POS aparate kao startnu točku prilikom napada na hotel. Također ukoliko se POS uređaj drži na mreži koja nije zaštićena napadač vrlo lako može doći do bitnih podataka koje mu trebaju kako bi iznudio novac od hotela. Web stranice hotela su vrlo slabo zaštićene te napadači u puno slučajeva ciljaju web stranice kako bi probili sigurnosni sustav hotela i uzrokovali prekid poslovanja. Održavanje PCI DSS to jest Standard za sigurnost podataka industrije platnih kartica je ključno uskladiti sa kibernetičkom sigurnošću u hotelu kako se nebi mogao dogoditi proboj te krađa podataka kartice.

[13] Florido-Benítez, L. (2024), The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities, Smart Cities, 7(1), str. 475.

3.1. Prosječni troškovi povreda podataka u hotelijerstvu

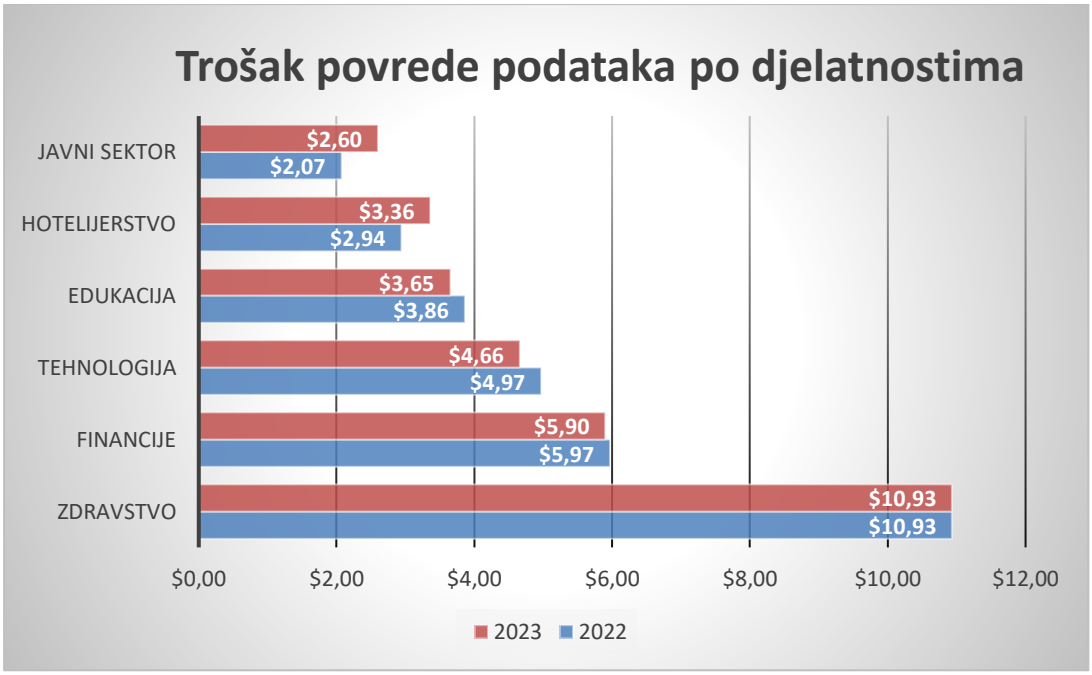
Uslijed mnogim povredama podataka koji se odvijaju u hotelskoj industriji, Trustwave je kompanija koja svake godine objavljuje izvještaj pod imenom : „Hospitality Sector Threat Landscape“ koja istražuje specifične prijetnje i rizike za ugostiteljske i hotelske organizacije, te nudi praktične uvide i savjete kako ojačati obranu od kibernetičkih upada. IBM također svake godine izrađuje izvještaj nazvan „Data breach report“ u kojem iznose ukupne troškove povrede podataka te sve vrste proboja, putem kojeg se može dobiti uvid u troškove povreda podataka te statistiku povreda podataka u kompanijama.

Grafikon 1. Ukupni troškovi povrede podataka u milijunima dolara

Izvor: Izrada autora prema Ibm.com; Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach (pristupljeno 21.05.2024)

Ukupni troškovi povrede podataka u milijunima dolara opadaju od 2020. godine. Veliki skok sa 3.86 milijuna na 4.24 milijuna dolara uzrokovan je Covid-19 pandemijom, koja je zahvatila svijet i prisilila sve kompanije da rade od kuće. Nakon tog negativnog skoka sa 2020. na 2021. godinu također bilježimo pad u zadnje tri godine. Sve više kompanija je odlučilo 2021. koristiti hibridni pristup poslovanja, to jest dio posla se radio od kuće a dio u kompanijama, tako su napadači mogli lako putem ljudske pogreške pristupiti intranetu kompanije te postaviti svoje viruse i zamke od kojih bi stvorili ekonomsku korist nad napadnutim ili iskoristiti upad za krađu podataka. U 2024. godini također se očekuje rast u

ukupnim troškovima povrede podataka jer sve više kompanija se odlučuje za online prodajom te s time omogućavaju napadačima lakši pristup svom kibernetičkom prostoru. [14]



Grafikon 2. Trošak povrede podataka prema djelatnostima u milijunima dolara

Izvor: Izrada autora prema Ibm.com; Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach (pristupljeno 21.05.2024)

Prema prikazanoj tablici, najveći trošak povrede snosi zdravstvo, čak prosječno 10.93 milijuna dolara po povredi podataka. Ovaj podatak je vrlo zabrinjavajuć, s time da se na drugom mjestu nalaze financije sa 5.90 milijuna dolara. Sve navedene djelatnosti su u 2023. godini doživjele pad u prosječnom trošku povrede podataka, osim hotelijerstva. Hotelijerstvo je doživjelo skok sa 2.94 u 2022. godini na 3.36 milijuna dolara što je izrazito loše, s obzirom da sve ostale dijelatnosti rade na zaštiti podataka i smanjenju povrede podataka. Hotelijerstvo je također doživjelo rast prosječnog proboja i samim time povećalo prosječni trošak povrede. Ovakav trend ima negativan utjecaj na potencijalne goste ili kompanije koje planiraju imati poslovne odnose sa drugom kompanijom u hotelijerstvu, također zbog takvih podataka vrlo su ciljane na tržištu hakera.

[14] Ibm.com, (2024); Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach (pristupljeno 21.05.2024)

3.2. Povrede podataka u hotelskoj industriji

Kibernetički proboji u hotelijerstvu su u zadnjih par godina postali sve učestaliji i opasniji. Razvojem interneta i OTA (Online travel agency) internet je postao opasno mjesto za hotelske kompanije. Najveće svjetske kompanije su početkom 2010–ih bile žrtve curenja podataka, poput Yahoo koji je napadnut te su tri milijarde računa kompromitirano, time je počelo doba kibernetičkih napada i krađe podataka. Hoteli su godinama bili ključne mete krađe podataka a glavni razlog napada su plaćanje kreditnim karticama.[15] U hotelu se većinom plaća veća svota novca te većina gostiju odlučuje platiti karticom, podaci od kartice se spremaju te napadači pokušavaju doći do njih. Sigurnosne povrede i proboji se događaju online, jer gosti rezerviraju sobe te usluge online te se time stavlja u ranjiv položaj. Online prostor postao je primaran pri rezervacijama te samim time je prevelik da bi ga se ignoriralo ili povuklo sa njega.[16] Ransomware napadi su najčešća vrsta proboja koja se odvija u hotelijerstvu, ali kako su kompanije postajale bolje u održavanju i korištenju sigurnosnih kompije tako se razvijao i sustav ransomware napada gdje su napadači postali još lukaviji i opasniji. Uz napredne tehnike napada, dodatne prijetnje poput prijetnja napadača objavljivanjem ukradenih podataka ukoliko otkupnina ne bude plaćena. Ciljanje ranjivih sustava koje si ne mogu priuštiti gubitak podataka poput manjih hotelskih kompanija koje nemaju adekvatnu obranu te mogućnost brze reakcije postaju velika meta za kibernetičke napadače. U sljedećem dijelu rada navedeni su najveći i najpoznatiji proboji podataka u hotelskog industriji.

[15] Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., El Koutbi, M., (2019), Digging deeper into Data Breaches: An Exploatory Data Analysis of Hacking Breaches Over Time, Procedia Computer Science 151, str. 1004.
[16] Madnick, S., (Feb 19, 2024). Why data breaches spiked in 2023, Harvard business review, https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (pristupljeno 21.05.2024).

3.2.1. Wyndham Worldwide 2008.

Prvi veliki proboj u bazi podataka dogodio se 2008. godine u Wyndham Worldwide kompaniji iz Delawarea. Wyndham Worldwide je korporacija registrirana u Delawareu sa sjedištem u New Jerseyu te upravlja hotelima i franšizama diljem svijeta preko svojih podružnica. U okviru svojeg redovnog poslovanja, prikupljaju depozite te prihvaćaju uplate, prikupljaju osobne i financijske informacije od svojih klijenata, koje uključuju osobne podatke poput informacije o kreditnim karticama. Tri puta između 2008. i 2010. godine hakeri su provalili u glavnu mrežu jedne od glavnih podružnica Wyndham Worldwide i ukrali informacije o 619 tisuća korisnika Wyndham kompanije. Informacije koje su ukradene, većinom su bile informacije o kreditnim karticama te osobnim podacima korisnika.[17] Nakon što je Wyndham Worldwide objavio kako se dogodio proboj, protiv njih su pokrenute dugotrajne regulatorne istrage te razne građanske tužbe od strane regulatora i privatnih tužitelja. Tek 2015. godine Wyndham Worldwide je dogovorio i zaključio sporazum sa tužiteljima. Wyndham Worldwide je među rijetkim kompanijama koje su osporile vladinu ulogu kao regulatora u ovom području. Dokumenti koje je Wyndham Worldwide dostavio vladi jasno pokazuju koliko je resursa i vremena potrebno kako bi se borilo protiv vladine intervencije. Ovaj sigurnosni proboj u Wyndhamu smatrao se malim, to jest obuhvatio je znatno manje podataka o kupcima u usporedbi sa poznatijim slučajevima, ali krajnji troškovi nakon kazni te regulatornih troškova bi mogli biti i veći. Wyndham je nakon ovog proboja angažirao nezavisnu tvrtku kako bi pregledala njihovu sigurnost. Također je zahtjevao od svojih franšizoprimaca da potpišu dodatak o kibernetičkoj sigurnosti. Ovaj proboj označio je tek početak trenda proboja u hotelsku industriju. U sljedećih 15 godina probijeno je preko tisuću hotela i hotelskih lanaca diljem svijeta te su kompanije i kupci oštećeni za više od 5 milijardi dolara.

[17] Silber, S., Wilson Sonsini G & R, Meal, H, Ropes & Gray Esq (2012), LLP; Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation, str. 2.

3.2.2. Marriot Starwood 2018.

Najveći proboj u hotelskoj industriji dogodio se 8. Rujna 2018. godine, kada je sigurnosni alat kompanije Marriott otkrio sumnjiv pokušaj pristupa internoj bazi podataka. Ovaj pokušaj pristupa uključivao je brendove Starwood kojem pripadaju hoteli Sheraton, W., Westin i St. Regis. Mariott nije objavio mnoge detalje o napadu, tako da se ne može sa sigurnošću potvrditi koja je ranjivost ili greška bila izravan uzrok proboja. Tadašnji izvršni direktor Marriotta Arne Soreson, imao je priliku pojaviti se pred američkim Senatom kako bi govorio o napadu te istaknuo opasnosti i budućnost ovakvih napada u hotelijerstvu. Marriot je prvi put postao svjestan da je žrtva krađe podataka nakon što je njihov sigurnosni alat označio neuobičajen upit baze podataka. Ovaj događaj potakao je internu istragu koja je utvrdila kako je Starwoodu mreža kompromitirana još 2014. godine kada Starwood nije bio u vlasništvu Marriotta ali su napadači ostavili backdoor te kasnije ponovo pristupili bazi. Istražitelji su također pretraživali sustav te su otkrili Trojanac za daljinski pristup koji se sa alatom za njuškanje korisničkih imena te lozinki također bio prisutan u memoriji sustava. Nije nikada javno objavljeno kako su ti alati dospijeli u Marriottov sustav ali se takvi upadi najčešće odvijaju preko e – mailova, i razumno je pretpostaviti kako je ovo također bio slučaj ljudske pogreške. Marriot je 2016. godine kupio Starwood ali su i dalje koristili svoj sustav rezervacija i plaćanja. Prema Marriottovoj istrazi pronašli su podatke koje su napadači šifrirali i ukloniti uz Starwood sustava. Kroz istragu koja je trajala četiri mjeseca došli su do informacije kako je kompromitirano petsto milijuna zapisa gostiju. Marriott je 30. studenog 2018. godine izdao priopćenje u kojemu su obavijestili javnost o proboju u sustav. Napad na Marriott pokazao je snagu i sposobnosti napadača da ukradu osobne podatke korisnika.[18] Marriot je iznio kako je do 2019. godine imala 28 milijuna dolara troškova povezanih sa probojem podataka. Nakon proboja povećali su ulaganja u kibernetičku sigurnost.

[18] Fruhlinger, J., (Feb 12, 2020), Marriot data breach FAQ: How did it happen and what was the impact ?, CSO, https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (pristupljeno 22.05.2024.)

3.2.3. MGM Resort International 2023.

Zadnji veliki napadi na kibernetički prostor u hotelskoj industriji odvijali su se između 2023. i 2024. godine. MGM Resort koji glasi za jednog od najvećih operatera kasnije u svijetu ali također i giganta u hotelskoj industriji, pogođen je kibernetičkim napadom u rujnu 2023. godine. Napad je utjecao na neke od najpoznatijih hotela u MGM kompaniji poput hotela Grand u Las Vegasu, Bellagiom Cosmopolitan i na druge ostale MGM resorte diljem SAD–a. Gosti su kao problem naveli prestanak rada digitalnih ključeva, elektroničkih sustava za plaćanje te online rezervacija. Mjesec dana nakon upada u sustav MGM Resort International priopćio je javnosti kako su pretrpjeli veliki kibernetički napad koji je rezultirao s više od 100 milijuna dolara troškova te krađom osobnih podataka gostiju. Nisu poznati svi detalji o tome kako su napadači izvršili napad na MGM ali istraživači su objavili kako su zaposlenici i servisne službe u MGM – u dobile lažne telefonske pozive te da su putem tih poziva dobili podatke za prijavu. Napadači su prevarili djelatnika korisničke službe te im je dao pristup računu administratora s naprednim privilegijama na MGM – ovim sustavima gdje su ukradeni podaci. Također prema javnom priopćenju MGM Resorta, napadom su ukradeni podaci poput imena klijenata, kontaktnih podataka te brojeva vozačkih dozvola[19]. Ograničenom broju korisnika također su bili pogođeni i brojevi osiguranja te brojevi putovnica što je iznimno opasno jer postoji opasnost od krađe identiteta te prevare sa računima. Nakon napada kompanija MGM morala je isključiti određene sustave te provjeriti sve datoteke kako ne bi dolazilo do novih napada. Istraga o samom proboju i dalje traje od strane FBI–a. MGM Resorts je na konferenciji za novinare također izjavio kako surađuju sa policijom te kako će u budućnosti više ulagati u samu kibernetičku sigurnost.

[19] MGM Resorts International, (Oct 5, 2023), MGM Resorts Update on Recent Cybersecurity Issue, https://investors.mgmresorts.com/investors/news-releases/press-release-details/2023/MGM-RESORTS-UPDATE-ON-RECENT-CYBERSECURITY-ISSUE/default.aspx (pristupljeno 22.05.2024.)

3.2.4. Motel One 2023.

Motel One, njemački lanac niskobudžetnih hotela koji upravlja sa 90 hotela diljem Europe o Sjedinjenih Američkih Država, jedan je od najvećih hotelskih lanaca u Europi te je krajem 2023. godine potvrdio da je bio meta ransomware napada u kojem su hakeri pristupili podacima korisnika. Vijest o ovome napadu na Motel One došla je nekoliko tjedana nakon što je MGM Resort, koji upravlja s nekoliko hotela i kasina na Las Vegas stripu, također bio meta kibernetičkog napada, stoga se smatra kako se kompaniji Hotel One dogodio isti slučaj. Tvrtka je tjedan dana nakon što su javno objavili kako je izvršen kibernetički napad, u kratkoj izjavi tvrdili da je utjecaj napada sveden na „relativni minimum“ zahvaljujući neodređenim mjerama koje je tvrtka poduzela, potvrdila je da su napadači uspijeli pristupiti nekim korisničkim podacima, koje u nastavku nisu htjeli precizirati. Prema Motel Oneu, to uključuje adrese i podatke od oko 150 kartica[20]. Također u izjavi su naveli kako broj i intezitet kibernetičkih napada neizmjerno brzo rastu. U najbržem mogućem roku kompanija Motel One obavijestila je relevantna nadzorna tijela i podnjela kaznene prijave. Policija tijekom istrage nije našla konkretne dokaze kako se dogodio upad te su pod mogućim napadačima naveli grupu Scattered Spider, podgrupu kriminalne grupe ALPHV koji su izvršili napad na MGM Resort kompaniju. Motel One je nakon upada u sustav pokrenuo suradnju sa iskusnim stručnjacima za informatičku i IT sigurnost te su u suradnji sa relevatnim tijelima obavijestili svoje korisnike kako će osigurati najvišu moguću razinu sigurnosti podataka u svojoj kompaniji. Prema policiji koja je vodila slučaj ovog kibernetičkog napada, navela je kako oko 6000 kompanija prijavi hakerske napade svake godine samo u Njemačkoj, dok broj neprijavljenih slučajeva znatno veći. Prilikom kasnije analize ukradene baze podataka uz podršku certificiranog pružatelja IT sigurnostih usluga, ustanovili su kako u sustavu nije pronađen nikakav zlonamjerni softver te da put koji su uljezi pronašli za prodiranje u kibernetički sustav identificiran te je odmah zatvoren.

[20] Motel One Group, (Jan 30, 2024), FAQ About The Data Protection Incident, https://www.motel-one.com/en/services/faqs-hacker-attack-motel-one-group/ (pristupljeno 28.05.2024.)

3.3. Načini zaštite kibernetičkog prostora u hotelijerstvu

Prosječni trošak povrede podataka u hotelijerstvu iznosi 3,3 milijuna dolara prema izvještaju Trustwave Spider Labsa iz 2023. godine[21]. Šanse da se dogode povrede podataka su izrazito velike, tj. 31 % organizacije u hotelijerstvu je prijavilo povredu podataka, a 89 % od tih organizacija pogođeno je više od jednom godišnje. Uzimajući u obzir ove informacije zaštita kibernetičkog prostora je iznimno bitna u hotelijerstvu kako bi se stvorio siguran prostor gdje će potrošači bez razmišljanja kako će im netko krivotvoriti podatke. Osim financijskih posljedica također oštećenje reputacije, pravne posljedice i gubitak kupaca su posljedice s kojima se poduzeće susreće ukoliko dođe do povrede podataka.

Stručnjaci za kibernetičku sigurnost izdvojili su najbitnije strategije za očuvanje sigurnosti hotela:[22]

1. **Enkripcija Wi–Fi mreže** – korištenje jakih protokola šifriranja za Wi–Fi mrežu spriječava potencijalni neovlašteni pristup i potencijalno presretanje podataka. Napadači u većini slučajeva ako napadaju direktno infiltriraju se u mrežu kompanije ili organizacije putem Wi–Fi mreže.
2. **Redovito ažuriranje softvera** – U većini slučajeva kompanije ažuriraju softver samo kada je to potrebno, ili kada nešto prestane efikasno raditi. Samim time si ugrožavaju sigurnost operativnih sustava i sigurnosnih aplikacija. Održavanjem softvera ažurnim može se spriječiti i riješiti ranjivost te poboljšati sigurnost sustava.
3. **Edukacija osoblja** – napadači najčešće naprave proboj u sustav putem ljudske pogreške npr. Netko otvori mail u kojem se nalazi poveznica sa virusom. Redovito provođenje obuka o praksama zaštite sigurnosti podataka te kibernetičke sigurnosti može dovesti do poboljšanja zaštite osjetljivih informacija.

[21] Law, M., (Sept 12, 2023), Trustwave report on hospitality industry security threats, Cybermagazine, https://cybermagazine.com/articles/trustwave-report-on-hospitality-industry-security-threats (pristupljeno 26.05. 2024)
[22] Ludynia, A., (Feb 21, 2024), Analysis of Cybersecurity in the Hospitality industry, Insights, https://insights.shijigroup.com/cybersecurity-in-the-hospitality-industry/ (pristupljeno 22.05.2024)

4. **Šifriranje osjetljivih podataka** – šifriranje osjetljivih podataka gostiju iznimno je važno ukoliko dođe do proboja u sustav, kako napadač nebi mogao iskoristiti podatke koje je ukrao. Šifriranje poput E2EE SSL/TLS protokola za web stranice i šifriranje na razini datoteka.

5. **Ograničavanje pristupa** – ograničavanje pristupa osjetljivim podacima na osnovu potrebe za pristupom. Npr. osigurati kako zaposlenici vide datoteke i podatke koji su potrebni za njihov posao a ostatak sakriti, to jest ograničiti pristup zaposlenika osjetljivim podacima na temelju njihovih poslovnih dužnosti kako bi se smanjio rizik od unutarnjih prijetnji te proboja sustava.

6. **Praćenje i analiza mrežnog prometa** - pratiti i analizirati mrežni promet kako bi se pratile nepravilnosti ili sumnjive aktivnosti u mreži iznimno je važno kako bi se u slučaju proboja ili sumnjivih aktivnosti brzo reagiralo. Kako bi se otkrile moguće prijetnje svakodnevno se moraju pratiti redovne aktivnosti i protokoli u kibernetičkom okruženju.

7. **Izrada sigurnosnih kopija** – sigurnosne kopije služe kako bi se u slučaju povrede ili kvara sustava, sustav na siguran način oporavio i sačuvao datoteke i podatke. Stvaranje sigurnosnih kopija na poseban disk ili u vanjsku pohranu može se također podjeliti prema rasporedu (dnevno, tjedno ili mjesečno) te se automatizirati kako bi podaci redovito bili sigurni i imali svoju kopiju u slučaju kvara. Ovakav način održavanja sustava smatra se iznimno povoljan te moguć u svakoj organizaciji.

8. **Neusklađeni obrasci za autorizaciju** – dosta organizacija i kompanija u Europi te Hrvatskoj i dalje čuvaju papirnate te PDF obrasce za autorizaciju kreditnih kartica. Ovakva praksa je izrazito nesigurna te izlaže organizaciju prijevarama i storniranju provedenih transakcija. Izrada digitalnih obrazaca za autorizaciju smatra se podizanjem stupnja zaštite kibernetičkog prostora.

9. **Informiranost o prijetnjama i trendovima** – iznimno je važno ostati ažuran te informiran o najnovijim prijetnjama i trendovima u kibernetičkom svijetu. Danas postoje razni stručnjaci te razne stranice koje nude iznimno točne i detaljne informacije o trendovima u kibernetičkom prostoru, imati informacije o

najnovijom prijetnjama može stvoriti proaktivne mjere prema nastalim rizicima u poslovanju organizacije.

Postoje mnoge strategije koje hotelska organizacija može iskoristiti kako bi se obranila od povrede podataka ali najvažniji elementi su : enkripcija podataka, stalna analiza te ažurnost te svijest o ugroženosti podataka (slika 2.). Zaštita podataka mora biti prioritet u hotelskoj organizaciji posebice jer vrlo veliki broj gostiju dnevno prođe kroz hotel te ostavi svoje informacije o plaćanju i sl.

Slika 2. Najvažniji elementi zaštite podataka

Izvor: Prilagođeno prema Ibm.com; Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach pristup (21.05.2024)

3.4. Utjecaj kibernetičkih proboja na poslovanje hotelske industrije

Utjecaj kibernetičkih probaja u hotelskoj industriji može se prikazati u više kategorija, ona koja je najveći fokus hotelskih kompanije jest financijska. Hotelska industrija je meta mnogih hakera baš zato što hoteli sadrže veliki broj informacija koje mogu postati korisne hakerima ukoliko ih ukradu. Najveći financijski gubitci uzrokovani probojem u kibernetički prostor dogodili su se u Starwood hotelima gdje se smatra kako je kompanija oštećena za 24 milijuna dolara, dok InterContinental hotel group je izgubio preko 20 milijuna dolara zbog upada u kibernetički prostor te krađe informacija. Kako bi se smanjio negativni utjecaj nakon napada iznimno je važno reagirati odmah, te prikupiti dokaze te sve zabilježiti i obavijestiti nadređene s kojima se treba napraviti plan akcije. Vrlo je bitno također otkriti greške koje su dovele do upada kako se kasnije ne bi ponovo dogodile. Hoteli moraju biti svjesni kako postoji iznimno bliska veza između povrede podataka u hotelima te povjerenja potrošača te kako bi utjecaj postao što blaži moraju redovito i ažurno izvještavati svoje klijente o promjenama koje hotel podnosi kako bi zaštitio podatke gostiju.

Novčane kazne i pravni troškovi su iznimno česti prilikom povrede podataka u hotelskim poduzećima. GDPR u Europi te CCPA u Americi služe za zaštitu podataka kupaca te ukoliko se prekrši kompanije su na riziku od pravne tužbe[23]. Na primjer, Marriott je kažnjen sa 24 milijuna dolara zbog povrede podataka koja je kompromitirala informacije iz Starwood hotelskog lanca. Troškovi obavještavanja i podrške klijentima također smatraju financijskim gubitkom jer kompanije moraju obavijestiti klijente te pružiti usluge nadzora kreditnih kartica ili zaštite identiteta što naravno osim reputacijski i financijski oštećuje kompaniju. Reputacijski gubitci također se mogu smatrati pogubnim za poduzeće jer primjerice ukoliko izgube povjerenje kupca nakon povrede podataka, gosti mogu izgubiti povjerenje u sigurnost hotela i odlučiti se za alternative ili konkurentske lance. Negativni medijski izvještaji nakon povrede podataka će biti javni i oglašavani što naravno negativno utječe na buduće poslovanje hotela. Mediji često javno izvješćuju o velikim povredama podataka te samim time narušavaju reputaciju brenda. Operativni izazovi nakon povrede podataka poput povećanog nadzora i regulacije važni su za spriječavanje budućih proboja.

[23] Johnson, M.S., Kang, Min Jung; Lawson, Tolani; and Singh, A.K., (2018). The Impact of Data Breaches on Hotel and Restaurant Firm Stock Returns, Journal of Hospitality Financial Management, 26(2), Article 3.

Veliki broj hotela nakon povrede podataka su podložniji promjenama te strožijim regulacijama poput InterContinental Hotel Group koji je naglasio javno kako nakon takvog propusta imaju potrebu za jačanjem kibernetičke sigurnosti unutar cijelog lanca hotela. Velik broj hotela i nakon povrede podataka ostaje ranjiv za buduće napade, ciljanje od strane hakera nakon uspješnog napada je vrlo česta praksa kod hakera, te samim probojem napadači vide ranjivost u njihovim sustavima te kasnije mogu ponovo ući u sustav. Probojem u kibernetički sustav također se dodatno oslabljuje IT infrastruktura hotela što otežava sam oporavak i povećava troškove održavanja i poboljšanja sigurnosti.

Regulativne posljedice poput striktnije regulative, revizija i inspekcija čest su način na koji vanjski izvori utječu na oporavak hotelskih industrija nakon proboja. Hoteli su nakon povrede podataka podložni čestim revizijama i inspekcijama kako bi se osiguralo da njihovi sigurnosni protokoli su u skladu sa najnovijim standardima te kako se ne bi ponovio sličan napad. Dodatni troškovi prilikom oporavka i obnove također imaju veliki utjecaj na budućnost poslovanja hotela. Primjerice Wyndham Hotels su između 2008. i 2010. godine doživjeli proboj te su nakon toga hotel potrošio više od 5 milijuna dolara na pravne troškove te buduću zaštitu hotela, taj novac su mogli uložiti u nešto drugo da nije došlo do proboja. Hoteli nakon proboja moraju uložiti novac i vrijeme u dodatne sigurnosne mjere kako bi spriječili buduće napade, što može uključivati obuku zaposlenika, implementaciju nove tehnologije ili revizija postojećih struktura koja je na današnjem tržištu vrlo skupa. Učinkovita zaštita podataka je ključna za hotelsku industriju te za buduće poslovanje hotela, kako bi se izbjegli financijski gubici, zaštitila reputacija samog brenda te osigurala sigurnost gostiju. Implementacija strožih protokola i transparentnost prema klijentima mogu i pomoći u smanjenju rizika od povrede podataka te njihovih negativnih posljedica.

4. KIBERNETIČKA SIGURNOST U REPUBLICI HRVATSKOJ

Kibernetička sigurnost u Republici Hrvatskoj istaknuta je tema u Ministarstvu unutarnjih poslova Republike Hrvatske. Određen je dokument nazvan Nacionalna strategija kibernetičke sigurnosti kojim se nastoji zaštiti građane Republike Hrvatske od mogućih povreda podataka.[24] Strategija identificira ključne vrijednosti za zaštitu, nadležne institucije i mjere za sustavno provođenje zaštite. Ova strategija pokazuje odlučnost svih sudionika kibernetičke sigurnosti da poduzmu mjere u okviru svojih ovlasti, surađuju s ostalim sudionicima, razmjenjuju potrebne informacije, te spremnost na kontinuirani razvoj i prilagodbu. Cilj je osigurati da hrvatski kibernetički prostor bude uređen, dostupan, otvoren i siguran za korištenje. Strategija se temelji na postojećim zakonskim okvirima I odgovornostima, ali prepoznaje potrebu za prilagodbom određenih zakonskih rješenja kroz provedbu mjera Akcijskog plana kako bi se zadovoljile potrebe virtualnog aspekta društva. Strategija se također smatra početnim korakom ka sustavnom i trajnom unaprijeđenju trenutne situacije u kibernetičkoj sigurnosti te istovremeno označava početak trajne i sustavne brige za buduće izazove u virtualnom prostoru, što je od ključne važnosti za zaštitu podataka i za daljnji razvoj društva. Najbitnije stavke u kibernetičkoj sigurnosti Republike Hrvatske smatraju se zaštita podataka (klasificirani podaci, poslovne tajne te osobni podaci), tehnička koordinacija u obradi računalnih sigurnosnih incidenata, međunarodna suradnja te obrazovanje, istraživanje, razvoj i jačanje svijesti o sigurnosti u kibernetičkom prostoru.[25]

[25] Ministarstvo unutarnjih poslova Republike Hrvatske, (2024), Kibernetička sigurnost, https://mup.gov.hr/istaknute-teme/nacionalni-programi-planovi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335 (pristupljeno 23.05.2024)

4.1. Nacionalni CERT

Republika Hrvatska u sklopu Nacionalnog CERT–a koji je dio Hrvatske akademske i istraživačke mreže izdaje godišnji izvještaj u sklopu kibernetičke sigurnosti. Statistika pokazuje kako je u Republici Hrvatskoj blagi pad u broju incidenata to jest 4,63 % ali je porastao broj kompromitiranih web sjedišta što nam pokazuje kako uz manji broj prijavljenih incidenata kompanije koje posluju putem web sjedišta su sve više u opasnosti od mogućih upada.[26] Nacionalni CERT također surađuje i sa brojim Europskim organizacijama za zaštitu podataka te samim time pruža bolju sigurnost i ažurnost u kibernetičkom svijetu. CERT brine o proaktivnim i reaktivnim mjerama te pruža usluge kompanijama i građanima besplatno. Proaktivne mjere su one koje se odnose na djelovanje prije incidenta i spriječavanje događaja koji se mogu negativno odraziti na poslovanje i sigurnost informatičkih sustava. Sa druge strane nalaze se reaktivne mjere, one se odnose i odgovaraju na incidente u Republici Hrvatskoj te pokušavaju umanjiti negativan utjecaj povrede podataka u budućem poslovanju.

VRSTA INCIDENTA	BROJ INCIDENATA U 2023. GODINI
PHISHING	421
SCAM	163
POGAĐANJE ZAPORKI	149
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	142
POSLOVNA PRIJEVARA	31
MALWARE URL	23

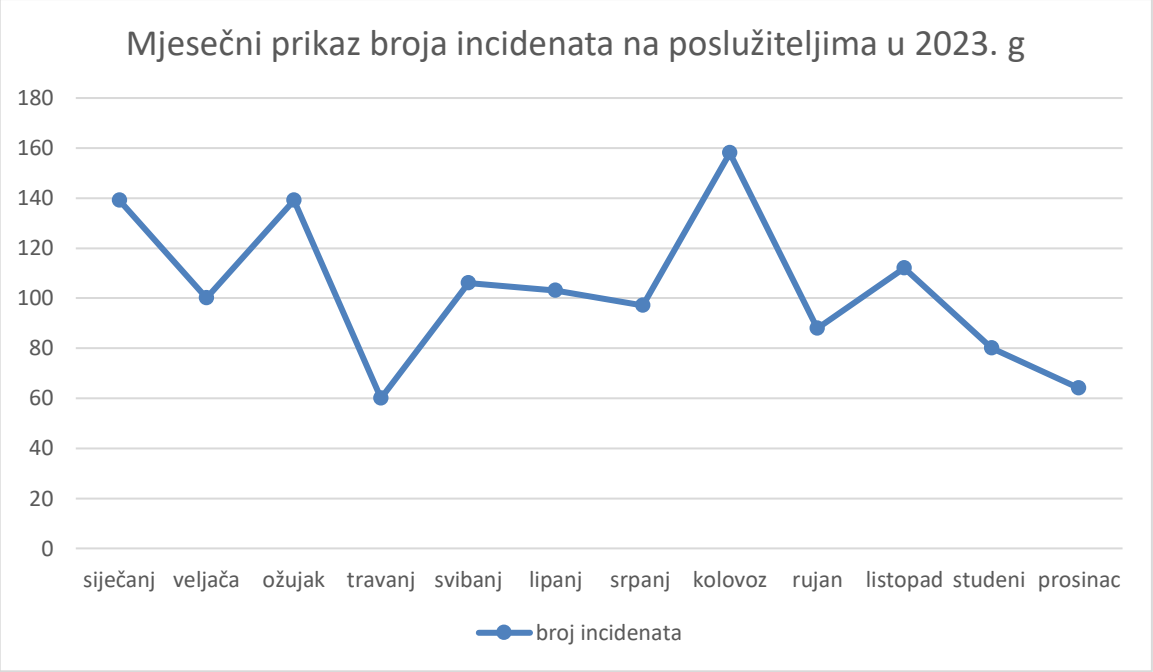
Tablica 1. Prikaz incidenata po tipu u 2023. godini

Izvor: izrada autora prema CERT.HR (2024.) Godišnji izvještaj za 2023. godinu, CARNET, CERT, https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023-godinu/ (pristupljeno 23.05.2024)

Prema tablici zabilježen je porast broja Phishing te Scam incidenata koji su sve učestaliji u hotelskoj industriji. Podaci su anonimni te se ne zna iz koje organizacije podaci

[26] CERT.HR, (2024), godišnji izvještaj za 2023. godinu, CARNET, CERT, https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023-godinu/ (pristupljeno 23.05.2024)

dolaze. Također sve je češći pojam poslovne prijevare koje se također mogu odvijati u hotelijerstvu sa dobavljačima i klijentima.



Grafikon 3. Mjesečni prikaz broja incidenata na poslužiteljima u 2023. godini

Izvor: izrada autora prema CERT.HR (2024.) Godišnji izvještaj za 2023. godinu, CARNET, CERT, https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023-godinu/

Na grafičkom prikazu možemo vidjeti tri velika skoka broja incidenata. Prvi skok se nalazi u prvom mjesecu koji su prema CERT – u opravdali sa uvođenjem eura te povećanjem incidenata iz domene financijskog sektora. Najveći broj incidenata zabilježen je u kolovozu kada je u Republici Hrvatskoj vrhunac sezone. Veliki je broj phishing kampanja te zlonamjernim kodovima. Postoji velika mogućnost s obzirom na izrečene podatke kako su podaci izraženi u kolovozu iz hotelijerskih ustanova. Vrlo je očigledno kako se većina napada odvija u samoj turističkoj sezoni u Hrvatskoj što zbog velikog broja turista i samog sezonskog osoblja u hotelima predstavlja veliki rizik za povredu podataka ili upade u sam kibernetički sustav. Nacionalni CERT sudjeluje također i u projektima koji su sufinancirani sredstvima iz Europske unije kojima pruža obuku i obrazovanje zaposlenicima kompanija u sklopu kibernetičke sigurnosti Hrvatske te same kompanije u kojoj rade zaposlenici.

4.2. Akcijski plan za provedbu nacionalne strategije kibernetičke sigurnosti

Zaštita kibernetičke sigurnosti u Republici Hrvatskoj je uz Nacionalnu strategiju kibernetičke sigurnosti napravila i Akcijski plan za provedbu Nacionalne strategije kibernetičke sigurnosti koji služi primarno za zaštitu podataka te kibernetički kriminalitet koji je u visokom porastu u Hrvatskoj u posljednjih pet godina. Kibernetička sigurnost je izrazito bitna pri samom pristupanju na internet u Republici Hrvatskoj s time se mora osigurati svakom građanu sigurnost.[27] Usvajanjem Strategije i Akcijskog plana te uvođenjem sustavnog i sveobuhvatnog pristupa kibernetičkoj sigurnosti Republika Hrvatska želi postići ključne ciljeve koje su od velike važnosti za razvoj društva te zaštitu kibernetičkog prostora. Integracija novih kibernetičkih dimenzija društva u razvoj i primjenu nacionalnog zakonodavstva, provođenje mjera i aktivnosti za poboljšanje sigurnosti, otpornosti i pouzdanosti kibernetičkog prostora, uspostava učinkovitijih sustava za razmjenu i pristup podacima potrebnim za povećanje opće sigurnosti prilikom stupanja u kibernetički prostor, podizanje svijesti građana te zaposlenika o važnosti sigurnosti među svim korisnicima kibernetičkog prostora, poticanje razvoja obrazovnih programa koji su usklađeni s potrebama kibernetičke sigurnosti u Republici Hrvatskoj, podrška istraživanju i razvoju novih tipova kibernetičkih napada, sustavno pristupanje međunarodnoj suradnji sa organizacijama poput ENISA. Ovakav akcijski plan izrazito je važan za zaštitu kibernetičke sigurnosti jer ukoliko kompanije te pojedinci prihvate plan moguće je postići razvoj društva te zaštitu kibernetičkog prostora u cijeloj Republici Hrvatskoj. Poticanje potencijala u Republici Hrvatskoj u području kibernetičku sigurnost je od iznimne važnosti pri zaštiti državnog proračuna, javnih ustanova i drugih privatnih kompanija.

[27] Ministarstvo unutarnjih poslova Republike Hrvatske, (2015), Nacionalna strategija kibernetičke sigurnosti, https://mup.gov.hr/UserDocsImages/minstarstvo/kibernetika/strategija_kibernetika.pdf (pristupljeno 24.05.2024)

5. BUDUĆNOST KIBERNETIČKE SIGURNOSTI U HOTELIJERSTVU

Sektor hotelijerstva i turizma iznimno brzo raste svake godine te se sve više oslanja na digitalnu tehnologiju kako bi pružio najbolje i najbrže usluge svojim korisnicima. Od rezervacije hotelskih soba i do upravljanja smještajem gostiju te planiranjem cijelokupnog poslovanja hotela, tehnologija je uključena u svaki i najmanji proces. Koristeći nove tehnologije poput Interneta stvari (IoT), umjetne inteligencije (AI), podataka u cloudu (online servis za pohranu podataka), izloženost napadima također raste iznimno brzo. Budućnost kibernetičke sigurnosti u sektoru hotelijerstva i turizma iznimno je kritična tema koja zaslužuje pažljivu analizu i proaktivne mjere koje će doprinjeti zaštiti podataka.[28] U budućnosti kibernetičke sigurnosti u hotelijerstvu bit će iznimno bitno ispuniti nekoliko ključnih koncepata poput zaštite podataka o korisnicima, uključujući osobne i platne informacije, koji su glavna tema kibernetičkih kriminalaca. Budućnost kibernetičke sigurnosti u hotelijerstvu oblikovati će se kroz integraciju naprednih tehnologija te je od iznimne važnosti svaku novinu koja se dodaje u hotelsku industriju implementirati u zaštitu kibernetičkog prostora.

5.1. Zaštita podataka u budućnosti hotelijerstva

Zaštita podataka osigurava povjerljivost, integritet, i dostupnost tih istih podataka. Usklađenost s GDPR-om za europske korisnike je ključan zahtjev koji se mora ispuniti, osobito s obzirom na rastući broj kibernetičkih napada. GDPR postaje sve stroži kako bi se osigurala zaštita osobnih podataka pojedinaca, stoga je iznimno važno poštivati ga kako bi se pokazao znak povjerenja prema kupcima. Sigurnost mreže s obzirom na to da se danas mnoge transakcije odvijaju putem interneta od presudne je važnosti kako bi se spriječili budući proboji podataka. Preko osoblja najčešće kibernetički kriminalci upadaju u sam

[28] Controlaudits, (24 Feb, 2024), What is the Future of Cybersecurity in the Travel and Tourism sector, Controlaudits, https://www.controlaudits.com/blog/what-is-the-future-of-cybersecurity-in-the-travel-and-tourism-sector/ (pristupljeno 24.05.2024)

kibernetički prostor te je iznimno bitna obuka osoblja o najboljim praksama u kibernetičkoj sigurnosti i time se pomaže u smanjenju ljudskih pogrešaka, što je kao i prije napomenuto najveći čimbenik rizika za proboje podataka i krađu podataka. Strategije za održavanje kibernetičke sigurnosti u budućnosti će imati veliku ulogu poput redovite procjene rizika, višefaktorske autentifikacije koja se u zadnje vrijeme značajno povećava u hotelijerstvu, enkripcije podataka da ukoliko dođe do proboja kibernetički kriminalci ne mogu dobiti kvalitetne informacije od ukradenih podataka. Aktivno prikupljanje informacija o prijetnjama te surađivanje sa organizacijama poput CERT – a ili ENISE može preduhitriti potencijalne kibernetičke prijetnje i osigurati gostima i radnicima u hotelijerstvu siguran rad. Fokus na kibernetičku sigurnost donosi svoje brojne prednosti za sektor hotelijerstva to jest samo povjerenje kupaca, ukoliko hotelska kompanija ulaže u kibernetičku sigurnost povećava se povjerenje kod potrošača u brend jer su sigurni sa svojom kupovinom u kompaniji. Stvaranje konkurente prednosti pokazivanjem posvećenosti kibernetičkoj sigurnosti te time pokazati na tržištu kako im je sigurnost klijenta najbitnija stavka poslovanja. Smanjeni troškovi također su jedna od najboljih prednosti koje može donjeti dobra kibernetička sigurnost jer ukoliko dođe do proboja podataka to kompaniji stvara veliki financijski problem. Osim brojnih prednosti također mogući su i nedostaci prilikom prevelikog fokusa na kibernetičku sigurnost, to jest stalna evaluacija koja se mora odvijati za ažurnosti u smislu kibernetičke sigurnosti, svakih par dana se stvara nova prijetnja te to može resursno biti vrlo zahtjevno ako je u pitanju srednja ili manja organizacija. Proračunska ograničenja također za mala i srednja poduzeća mogu biti izrazito problematična jer kompanije koje nemaju dovljno sredstava smatrati će ulaganje u kibernetičku sigurnost prohibitivnim. Kako bi se održala kibernetička sigurnost, kompanije sa najboljim praksama imale su redovite procjene rizika kako bi identificirale i smanjile potencijalne kibernetičke ranjivosti. Kompanije poput IBM–a su istaknule kako najbolje prakse imaju kompanije koje su u prošlosti doživjele kibernetički napad te samim time su stvorili strah od ponovnog mogućeg upada i napravili iznimno siguran kibernetički prostor.

5.2. Digitalna transformacija u hotelijerstvu

Digitalna transformacija je proces korištenja digitalnih tehnologija za stvaranje novih ili prilagođavanje postojećih poslovnih procesa, proizvoda i korisničkih sustava kako bi se zadovoljile promjenjive potrebe na tržištu za samog korisnika[29]. Jedno od ključnih područja gdje se odvija digitalna transformacija u hotelijerstvu jest korištenje tehnologije u sobama, što može poboljšati iskustvo gostiju, njihovu sigurnost i udobnost te stvoriti konkurentsku prednost za poslovanje. Digitalnom transformacijom se sve više pristupa u kibernetičkom svijetu hotelijerstva te također se smatra budućnosti u kibernetičkoj sigurnosti jer ukoliko kriminalci naprave proboj u digitalne podatke u hotelijerstvu mogu ogroziti cijelokupno poslovanje kompanija, stoga je bitno zaštiti kibernetički prostor kako bi se zaštitilo poslovanje i osobni podaci. Također digitalna transformacija donosi nove prilike u poslovanju hotelske industrije, a kako bi maksimizirali prihode i zaštitili svoj tržišni udio od tradicionalnih konkurenata i mnogih novih vrsta konkurenata (Airbnb) hotelska industrija sve više se oslanja na digitalnu transformaciju te korištenje tehnologije u različitim operativnim djelovima poslovanja. Kako bi kompanije ostale konkurente u ugostiteljskoj industriji, operateri hotela, restorana i ostalih sadržaja moraju biti informirani o najnovijim tehnologijama. S povećanjem digitalizacije, hotelska industrija mogla bi se suočiti sa brojnim pitanjima kibernetičke sigurnosti. Mnoge kompanije odlučuju se za servitizaciju, to jest dodavanje usluga poslovanju usmjerenom na proizvode kako bi se kupcima pružio kontinuirano željeni rezultat. Digitalna transformacija i servitizacija predstavljaju značajne mogućnosti za unaprijeđenje hotelske industrije. Usvajanje novih tehnologija može pomoći u stvaranju personaliziranijeg i sigurnijeg kibernetičkog prostora, što dovodi ka povećanju zadovoljstva gostiju i prihoda. Iako postoje izazovi smatra se kako zasad digitalna transformacija djeluje pozitivno na zaštitu kibernetičkog prostora.

[29] Tomičić Furjan, M., Tomičić – Pupek K., Pihir I. (2020), Understanding Digital Transformation Initiatives: Case Studies Analysis, Business System Research, 11(1), str. 125.

ZAKLJUČAK

Kibernetička sigurnost postaje sve važnija tema u hotelijerstvu, kako se industrija sve više oslanja na razvoj tehnologije kako bi unaprijedila svoje usluge i poslovanje. Hotelska industrija je danas sve više izložena raznim kibernetičkim prijetnjama i napadima koji uključuju krađu podataka, phishing kampanje i zlonamjerne napade. Mnogi hoteli su pretrpili napade te su imali negativne utjecaje na poslovanje nakon napada, poput financijskih, reputacijskih i zakonskih utjecaja. S obzirom na sve veći broj incidenata i kompromitiranih web stranica, ključno je za hotelsku industriju usmjeriti pažnju na zaštitu svojih digitalnih sustava i podataka gostiju. Osnovne kibernetičke prijetnje poput ransomware-a, malware-a, te socijalnog inženjeringa predstavljaju veliki problem u kibernetičkoj zaštiti. Osnovne metode zaštite koje se primjenjuju u očuvanju kibernetičke sigurnosti su: prevencija, detekcija te obrazovanje korisnika i zaposlenika. Prosječni troškovi povreda u hotelijerstvu su u rastu zadnjih par godina što je negativan trend, ali se broj povreda podataka koji su javno objavljeni smanjuju u zadnjih četiri godina. Mnogi načini zaštite poput enkripcije Wi-Fi mreže, redovitog ažuriranja softvera te informiranost o prijetnjama i trendovima mogu pomoći za zaštitu kibernetičkog prostora. Mnogi čimbenici utječu na sigurnost kibernetičkog prostora u hotelijerstvu, poput ljudskog čimbenika koji je najčešće prvi uzrok proboja u sustav hotela, stoga je izrazito bitno vršiti redovitu i kvalitetnu edukaciju osoblja kako bi osoblje u slučaju proboja znalo pravilno i brzo reargirati kako bi se smanjio negativan utjecaj proboja. Utjecaj kibernetičkih napada na poslovanje u hotelskoj industriji iznimno je negativan jer osim financijskih gubitaka dolazi do loše reputacije kompanije na tržištu te gubitka povjerenja gostiju. Kibernetička sigurnost u Republici Hrvatskoj je dinamična, ali je pod stalnim unapređenjem uz nacionalnu strategiju, suradnju i edukaciju privatnog te javnog sektora. Hrvatska s obzirom na važnost turizma, ulaže dosta resursa u očuvanje kibernetičke sigurnosti RH. Budućnost kibernetičkog sustava uveliko ovisi o samom ponašanju kompanija te poštivanju smjernica koje izdaju organizacije poput ENISA ili CERT koje brinu o kibernetičkim prostorima na globalnoj razini. Digitalizacija i korištenje umjetne inteligencija kako bi se brže pronašlo mjesto upada može imati velike utjecaje na poduzeća jer će time bez ljudskih resursa moći vrlo brzo i detaljno odrediti kada se dogodio upad te kako je moguće spriječiti taj upad u budućnosti. Pravovremenom i

sigurnom zaštitom podataka hotelske kompanije će ne samo stvoriti dodatan prihod, jer će sve više gostiju odsjedati u sigurnom okruženju već će stvoriti i pozitivnu reputaciju te unaprijediti svoju poziciju na tržištu, stoga je vrlo važno ulagati u kibernetičku sigurnost jer bez kibernetičke sigurnosti nema ni budućnosti. Prema provedenom istraživanju, dolazi se do zaključka kako budućnost uspješne kibernetičke zaštite u hotelskim poduzećima najviše ovisi o tehnologiji (primjeni adekvatnih softverskih rješenja zaštite), ljudima (edukaciji tvrtki i pojedinaca te podizanju razine svijesti o kibernetičkoj sigurnosti) te procesima (jasnom definiranju aktivnosti i mjera zaštite u svrhu očuvanja kibernetičke sigurnosti.

BIBLIOGRAFIJA

Atzori, L., Iera, A., & Morabito, G., (2010) The Internet of Things: A survey, Computer Networks, 54(15), str. 2787.

Atzori, L., Iera, A., & Morabito, G., (2011). SIoT: giving a social structure to the internet of things, IEEE Communication Letters, 15(11), str. 1193.

CERT.HR, (2024), godišnji izvještaj 2023., CARNET, CERT, https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2023-godinu/ (pristupljeno 23.05.2024)

Controlaudits, (24 Feb, 2024), What is the Future of Cybersecurity in the Travel and Tourism sector, Controlaudits, https://www.controlaudits.com/blog/what-is-the-future-of-cybersecurity-in-the-travel-and-tourism-sector/ (pristupljeno 24.05.2024)

Enisa.europa.eu., (2024); European Union Agency for Cybersecurity, https://www.enisa.europa.eu/ pristupljeno (15.05.2024.)

Florido-Benítez, L., (2024). "The Cybersecurity Applied by Online Travel Agencies and Hotels to Protect Users' Private Data in Smart Cities" Smart Cities, 7(1), str. 475.

Fruhlinger, J., (Feb 12, 2020), Marriot data breach FAQ: How did it happen and what was the impact ?, CSO, https://www.csoonline.com/article/567795/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html (pristupljeno 22.05.2024.)

Gillis, A., (Aug 2023), Internet of Things (IoT), Techtarget, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (pristupljeno 19.05.2024)

Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., El Koutbi, M., (2019). Digging deeper into Data Breaches: An Exploatory Data Analysis of Hacking Breaches Over Time, Procedia Computer Science 151, str. 1004.

Hrvatska enciklopedija, (2024), mrežno izdanje. Kibernetika https://www.enciklopedija.hr/clanak/kibernetika. (pristupljeno 15.05.2024.)

Ibm.com, (2024); Cost of Data Breach Report 2023, https://www.ibm.com/reports/data-breach (pristupljeno 21.05.2024)

Ibm.com. (2024); What is cybersecurity ?; https://www.ibm.com/topics/cybersecurity (pristupljeno 17.05.2024)

Johnson, M.S., Kang, Min Jung; Lawson, Tolani; and Singh, A.K., (2018). The Impact of Data Breaches on Hotel and Restaurant Firm Stock Returns, Journal of Hospitality Financial Management, 26(2), Article 3

Jordana J. G., Leidner D., (2019), From clicktivism to hacktivism: Understanding digital activism; Information and Organization, 29(3), str. 3.

Kaur, K. & Kaur, R., (2016), Internet of things to promote tourism: An insight into smart tourism, International Journal of Recent Trends in Engineering & Research, 2(4), str. 357.

Kibernetička sigurnost, (2024), Ministarstvo unutarnjih poslova Republike Hrvatske, https://mup.gov.hr/istaknute-teme/nacionalni-programi-planovi-i-projekti/nacionalne-strategije/kiberneticka-sigurnost/222335 (pristupljeno 23.05.2024)

Law, M., (Sept 12, 2023), Trustwave report on hospitality industry security threats, Cybermagazine, https://cybermagazine.com/articles/trustwave-report-on-hospitality-industry-security-threats (pristupljeno 26.05. 2024)

Ludynia, A., (Feb 21, 2024), Analysis of Cybersecurity in the Hospitality industry, Insights, https://insights.shijigroup.com/cybersecurity-in-the-hospitality-industry/ (pristupljeno 22.05.2024)

Madnick, S., (Feb 19, 2024). Why data breaches spiked in 2023, Harvard business review, https://hbr.org/2024/02/why-data-breaches-spiked-in-2023 (pristupljeno 21.05.2024).

MGM Resorts International, (Oct 5, 2023), MGM Resorts Update on Recent Cybersecurity Issue, https://investors.mgmresorts.com/investors/news-releases/press-release-details/2023/MGM-RESORTS-UPDATE-ON-RECENT-CYBERSECURITY-ISSUE/default.aspx (pristupljeno 22.05.2024.)

Motel One Group, (Jan 30, 2024), FAQ About The Data Protection Incident, https://www.motel-one.com/en/services/faqs-hacker-attack-motel-one-group/ (pristupljeno 28.05.2024.)

Negreiro M., (2023), Managed security services in Europe, European Parliamentary Research Service, https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754556/EPRS_BRI(2023)754556_EN.pdf (pristupljeno 16.05.2024)

Rajendra, K.R., Wood, C.A., (2010). Keyloggers in Cybersecurity Education, Rechester Institute of Technology, str. 293.

Sbounias, J., (30 Jul, 2019), Smart hotel around the world that highlighted new global trend, Hotelier Academy,https://www.hotelieracademy.org/5-smart-hotels-that-confirm-the-potentials-of-this-new-hotel-trend/ (pristupljeno 20.05.2024)

Silber, S., Wilson Sonsini G & R, Meal, H, Gray & Ropes Esq., (2012) LLP; Petition of Wyndham Hotels & Resorts, LLC and Wyndham Worldwide Corporation, str. 2.

Smith, A., (Oct 12, 2023), Iot in Travel and Tourism, Medium, https://web-and-mobile-development.medium.com/iot-in-travel-and-tourism-industry-why-it-is-a-game-changer-cf168df4753 (pristupljeno 19.05.2024.)

Tomičić Furjan, M., Tomičić – Pupek K., Pihir I., (2020) Understanding Digital Transformation Initiatives: Case Studies Analysis, Business System Research, 11(1), str. 125.

POPIS ILUSTRACIJA

Tablice

Grafikoni

Slike