Kibernetička sigurnost pametnih destinacija

Tupi, Ričard

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Preddiplomski sveučilišni studij

Ričard Tupi

Kibernetička sigurnost pametnih destinacija

Cybersecurity of Smart Destination

Završni rad

Opatija, 2023..

SVEUČILIŠTE U RIJECI
Fakultet za menadžment u turizmu i ugostiteljstvu
Preddiplomski sveučilišni studij
Poslovna ekonomija u turizmu i ugostiteljstvu
Studijski smjer: Menadžment u turizmu

Kibernetička sigurnost pametnih destinacija

Cybernetic security of smart destination

Završni rad

Kolegij:	**Sigurnost informacijskih sustava**	Student:	**Ričard Tupi**
Mentor:	**Izv.prof.dr. sc. Ljubica Pilepić Stifanich**	Matični broj:	**0116166836**

Opatija, siječanj, 2023.

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

IZJAVA O AUTORSTVU RADA I O JAVNOJ OBJAVI OBRANJENOG ZAVRŠNOG RADA

Ričard Tupi (ime i prezime studenta)

0116166836 (matični broj studenta)

Kibernetička sigurnost pametnih destinacija (naslov rada)

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

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

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

U Opatiji, rujan, 2023.

Ričard Tupi

Potpis studenta

SAŽETAK

Popularizacijom pametne turističke infrastrukture dolazi i do povećanja učestalosti kibernetičkih napada. Povezanost turista sa pametnim smještajnim objektima povećava količinu podataka koja su dostupna napadaču. Česte su financijske i reputacijske posljedice za destinaciju, a turist je najčešće žrtva gubitka privatnih podataka. Pojava interneta stvari je omogućila razvoj pametnih destinacija, ali istovremeno izazvala i veće rizike radi pojedinih sigurnosnih nedostataka. Uvođenje robotike omogućava nove inovacije u pružanju usluga, ali isto tako predstavlja i prijetnju za spyware napade u hotelima. Potreba za razvijanjem kompleksnih sigurnosnih sustava raste, a od izuzetne je važnosti obrazovanje zaposlenika i turista o sigurnosti u digitalnom svijetu. Svrha ovog rada je čitatelju približiti rastući problem kibernetičkih napada i njihov utjecaj na pametne turističke destinacije i daljnji razvoj pametnog turizma. Cilj rada je istraživanje veza i posljedica kibernetičkih napada na pametne turističke destinacije i informiranje čitatelja o metodama sigurnosti koje je u današnje vrijeme potrebno implementirati radi umanjivanja rizika i više slojevite zaštite. Dolazi se do zaključka da su u današnje vrijeme kibernetički napadi postali kompleksniji i da su posljedice znatno veće za pametne destinacije. Potrebna je implementacija suvremenih zaštitnih sigurnosnih modela te donošenje i provođenje novih strategija radi postizanja maksimalne sigurnosti od rastućeg broja kompleksnih kibernetičkih napada.

Ključne riječi: kibernetički napad, pametne destinacije, sigurnosni sustavi, internet stvari

SADRŽAJ

UVOD....1

1. SMART TURIZAM....3

1.1. Pametna turistička destinacija....4

1.2. Primarni elementi pametne turističke destinacije....5

1.3. Odnos održivog razvoja i pametne turističke destinacije....7

1.4. Pametni hoteli u pametnoj turističkoj destinaciji....9

1.5. Kibernetička sigurnost pametnih hotela....10

1.6. Opasnost Ransomware napada u pametnim turističkim destinacijama....12

2. INTERNET OF THINGS....17

2.1. Opasnosti kibernetičkih napada na pametan prijevoz destinacije....18

2.2. Opasnost Botnet napada na Internet of Things uređaje....20

2.3. Uloga virtualne realnosti u pametnom turizmu....21

2.4. Kibernetičke prijetnje na sustave virtualne realnosti....22

3. ROBOTIKA U PAMETNIM HOTELIMA....25

3.1. Primjena robotike u pametnim hotelima....25

3.2. Nedostaci robotike u turizmu i kibernetičke prijetnje....27

4. ULOGA MOBILNIH UREĐAJA U PAMETNOJ TURISTIČKOJ DESTINACIJI....29

4.1. Utjecaj 5G mreža u pametnoj infrastrukturi....32

4.2. Opasnost Keyloggera i Supply Chain napada....33

5. MJERE ZAŠTITE OD KIBERNITIČKIH NAPADA....35

5.1. Biometrijske sigurnosne tehnike....37

5.2. Zero Trust Model....38

5.3. Defense-in-Depth....40

5.4. Risk Based Security 41

5.5. Compliance Framework 42

5.6. Security by Design 43

ZAKLJUČAK 45

BIBLIOGRAFIJA 47

POPIS ILUSTRACIJA 50

UVOD

U ovome završnom radu govorit će se o utjecajima kibernetičkih napada na pametne turističke destinacije i na implementaciju adekvatnih sigurnosnih sustava zaštite i čuvanja podataka u svrhu postizanja dobrobiti turista. Kroz rad su objašnjene različite vrste kibernetičkih napada koje se mogu odnositi na pametne objekte za smještaj, dobrobit turista ili za pametnu turističku destinaciju općenito. Kibernetički napadi su rastuća prijetnja na koju pametna destinacija uvijek mora biti spremna uvođenjem suvremenih sigurnosnih sustava. Napadi mogu znatno narušiti ugled i negativno utjecati na poslovanje destinacije te jepotrebno informirati i obrazovati sve dionike na određenom turističkom prostoru kako bi se rizik minimizirao.

Svrha rada je čitatelju približiti rastući problem kibernetičkih prijetnji te njihov utjecaj na daljnji razvoj pametnog turizma. Nadalje, analizirane su i sigurnosne metode koje bi se trebale primijeniti od strane pojedinca kako bi se minimizirao sigurnosni rizik. Ciljevi ovog završnog rada su istražiti vezu između kibernetičkih prijetnji i njihovog utjecaja na pametne destinacije, ali isto tako i na smart turizam općenito, odrediti učestalost kibernetičkih prijetnji u pametnim destinacijama, vrste koje se najčešće pojavljuju te najefikasnije načine zaštite. Također će se analizirati podaci i utjecaj sustava virtualne stvarnosti, interneta stvari te uloge mobilnih uređaja u pametnim turističkim destinacijama. Za izvore podataka u ovom završnom radu koristili su se sekundarni podaci odnosno znanstveni i stručni članci na temu pametne turističke destinacije te knjige o pametnom turizmu, pametnim gradovima i njihovim elementima. Metode istraživanja korištene u ovome radu su metoda dekripcije, metoda analize, metoda sinteze, metoda dokazivanja, metoda komparacija te deduktivna metoda. Rad se sastoji od pet glavnih poglavlja. U prvom poglavlju govorit će se o pojmu pametnog turizma i njegovog utjecaja na promjenu modernog turizma, isto tako definirat će se pojam pametne destinacije i njene glavne karakteristike. Tema drugog poglavlja je internet stvari, kakave pogodnosti se postižu korištenjem IoT uređaja te koji su njihovi rizici. Treće poglavlje objašnjava ulogu pametnih hotela u pametnoj destinaciji i povezanosti između hotela i turista. Isto tako dotaknut će se i teme robotike u turizmu i njihovom naglom popularizacijom. U četvrtom poglavlju se objašnjava utjecaj mobilnih uređaja na integraciju s digitalnim uslugama u pametnoj destinaciji isto kao i važnost 5G mreže za daljnji razvoj

sigurnosnih sustava i njegovog utjecaja na konkurentnost destinacije. U posljednjem petom poglavlju govori se o mjerama zaštite protiv kibernetičkih napada. Spominju se najčešće metode zaštite podataka isto kao i informacije o sigurnosnim biometrijskim tehnikama te sigurnosnim modelima kao što su Zero Trust Model, Defense-in-Depth i Security by Design modeli.

1. SMART TURIZAM

Smart turizam je oblik turizma koji se koristi digitalnom tehnologijom kako bi se pojačalo iskustvo putovanja turista, ali i njegovog samog boravka u određenoj destinaciji. Intenzivniji razvoj pametnog turizma započinje ranih 2000.-ih godina kada su se počele razvijati mobilne tehnologije te se tada bilježi i sve veće korištenje interneta. Smart turizam na samom početku nije mogao biti ono što je danas. Tada tehnologija nije bila dovoljna razvijena da pruži turistima sve pogodnosti koje su danas dostupne. Tako da se smart turizam u počecima razvijao sporo, ali je veoma brzo uzeo maha radi sve većeg ubrzanja u razvoju moderne tehnologije. Ranih 2010.-ih se znatno bilježi porast pametnih turističkih destinacija što je sukladno tome potaknuto pojavom sve većeg broja pametnih mobilnih uređaja na tržištu te razvojem interneta stvari.[1] U samim počecima smart turizam znatno je promijenio način na koji turisti planiraju svoje putovanje radi uvođenja online aplikacija i web stranica za rezerviranje boravka, programa i pomagala za organizaciju putovanja te digitalnih marketinških strategija. ICT tehnologija je promijenila dinamiku funkcioniranja mnogih gospodarskih grana pa tako i turizma. Prioritet postaje korištenje informacijske tehnologije kako bi se osigurao jednostavniji način života domicilnog stanovništva u skladu s turistima, ali isto tako i razvijanje modela koji potiče očuvanje prirodnih resursa i kulture. Rezultat kvalitetnog izvođenja ovih ideja je konkurentna pozicioniranost na turističkom tržištu radi porasta interesa u turistima za destinacijama koje se okreću digitalizaciji i održivom razvoju. Porastom prisutnosti informacijske tehnologije u mnogim dijelovima turističkih proporcionalno tome raste i prijetnja od kibernetičkih napada kojima se ta destinacija izlaže. Upravo radi tih rizika koji mogu snažno utjecati a destinaciju, potrebno je raznim sigurnosnim mjerama zadržati stabilnost destinacije i osigravanje budućeg razvoja. Turistički sektor spada među najosjetljivije sektore po pitanju sigurnosti i utjecaja prijetnji poput kibernetičkog terorizma. To je prvenstveno zbog ranjivosti korisnika turističkih usluga, a kibernetički napadi se pojavljuju prvenstveno radi nepažnje individualca. Ovaj oblik turizma promijenio je način razmišljanja turista o njihovom putovanju te njihovim iskustvima te je omogućio daljnji razvoj turističkih destinacija koje su ove digitalne

[1] Gretzel, U., Sigala, M., Xiang, Z., Koo, C.; Smart Tourism: foundations and developments; Electronic Markets, 25, str.180; 2015.

prednosti pravovremeno iskoristile. Radi uvedenih tehnologija moguće je na jednostavniji način imati uvid u osobne preferencije, interese i ponašanja gosta te na temelju tih informacija kreirati posebnu ponudu. Implementiranje digitalne tehnologije pomaže i pri kvaliteti komuniciranja između turista, smještajnih objekata, turističkih zajednica te turističkih destinacija. Visoka kvaliteta komunikacije omogućava brži protok informacija što omogućuje brže pružanje potrebne usluge ili pomoći te isto tako doprinosi jednostavnijem obavljanju transakcija. Smart turizam uključuje integraciju mobilnih aplikacija, online booking sistema, umjetne inteligencije, interneta stvari (Internet of Things) te virtualne stvarnosti (VR) i proširene stvarnosti (AR).[2]

1.1. Pametna turistička destinacija

Pametna turistička destinacija je destinacija koja koristi tehnologiju i inovacije kako bi unaprijedila turističko iskustvo, podigla kvalitetu upravljanja destinacijom i njenom održivošću te potaknulo lokalno gospodarstvo. Pametna turistička destinacija integrira tehnologije poput mobilnih aplikacija, umjetne inteligencije, analize velikih podataka, interneta stvari (IoT) i drugih kako bi turistima pružila personalizirane i efikasnije usluge tijekom cijelog njihovog boravka.[3] Razvoj mjera za smanjenje rizika od kibernetičkih napada posebno je važan za zemlje u kojima je turizam dominantna grana i u kojoj prevladava koncept pametnog turizma u velikoj mjeri. Nedovoljna razina sigurnosti vrlo brzo može stvoriti reputaciju nesigurne zemlje što će u dugoročnom pogledu naštetiti brojevima turističkih dolazaka. Pametne turističke destinacije također imaju mogućnost ostvarivanja bolje sinergije između gospodarskih grana unutar svojeg djelovanja radi rasprostranjenosti digitalne tehnologije. Osim što pomaže gospodarskim granama koje funkcioniraju unutar destinacije, pomažu i svim dionicima; domicilnom stanovništvu, turistima, menadžerima, turističkim zajednicama te smještajnim objektima.[4] Korištenje tehnologije u turizmu također podiže i razinu efikasnosti obavljanja procesa koji su vezani za rezerviranje smještaja, osiguravanja gostu željenog turističkog sadržaja te bržu i

[2] Ijaz, S., Shah, A., Khan A., Mansoor, A.,: Smart Cities: A Survey on Security Concerns; International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 7, No. 2; 2016.
[3] Xiang, Z., Fesenmaier, D. R.; Smart Tourism Destinations; str. 299.,300.; Švicarska, 2017.
[4] Gretzel, U., Sigala, M., Xiang Z., Koo, C.; Smart Tourism: Foundations and Developments; Electronic Markets, 25; 181 str; 2015.

jednostavniju dostupnost informacija koja omogućava turistu da svoje vrijeme provodi na kvalitetniji način što na kraju putovanja rezultira i povećanim krajnjim zadovoljstvom. Potrebno je konstantno ulaganje u aktualne mehanizme i adekvatno obrazovanje radnika na raznim pozicijama u turističkom sektoru, pogotovo na mjestima gdje se nalazi veliki broj turista. Digitalne usluge mogu se koristiti putem mobilnih aplikacija, web stranica i društvenih medija kako bi se turistima pružile informacije o vremenskim uvjetima, prometnim gužvama i rasporedu događaja u određenoj destinaciji.

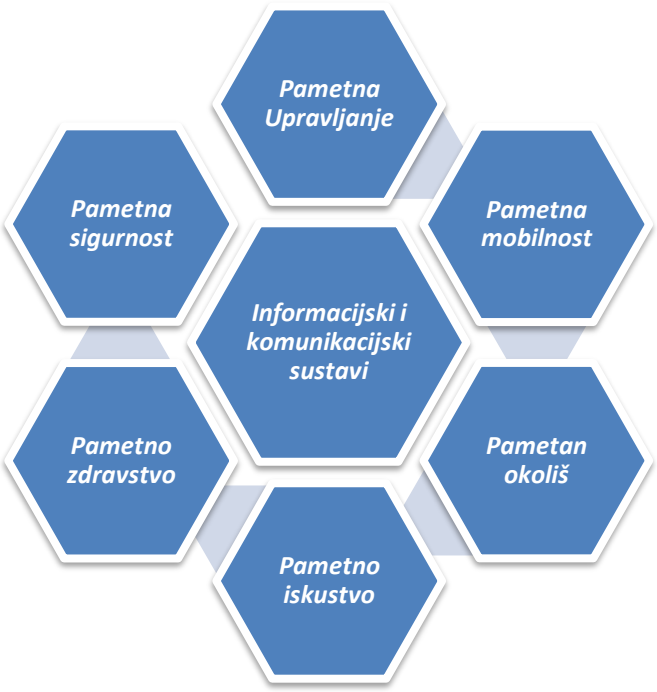
1.2. Primarni elementi pametne turističke destinacije

Pametna turistička destinacija sastoji se od sedam primarnih elemenata. Pametna mobilnost, pametan okoliš, pametno iskustvo, pametno zdravstvo, pametna sigurnost i pametna vlada tj. upravljanje. Pametna mobilnost predstavlja mogućnost kretanja unutar destinacije putem pametne infrastrukture. Postoje mnoge pogodnosti implementacija ovakvoga sustava, ali upravo u njemu se kriju i najveće opasnosti koje se mogu dogoditi prilikom većeg kibernetičkog napada. Pametna prijevozna sredstva omogućuju turistima jednostavan dolazak do željene destinacije primjerice s autonomnim autobusima. Pametan okoliš se odnosi na razvoj održivog razvoja u pametnoj destinaciji. Turisti nakon pandemije preferiraju posjetiti destinacije koje se fokusiraju na dugoročnom održivom razvoju te očuvanju prostora na kojem se zbivaju velika turistička kretanja.[5] Radi razvoja Internet of Things tehnologije danas postoje i uređaji za reguliranje potrošnje energije, osvjetljenja i zagađenosti prostora, koristeći takve uređaje lakše se kontrolira potrošnja. Element pametnog iskustva se fokusira na podizanje zadovoljstva i iskustva gosta na veću razinu primjenom pametne tehnologije. Primjerice u ove svrhe se mogu koristiti nove inovacije izazvane pojavom 5G mreže te sve češćom prisutnošću VR i AR sadržaja u turizmu. Mogućnost veće personalizacije usluge jedna je od bitnijih karakteristika usluga koja se promijenila na bolje od uvođenja pametne tehnologije Pametni sigurnosni sustavi predstavljaju sve sigurnosne sustave u pametnoj destinaciji kojima je cilj sprječavanje kibernetičkih napada na uređaje koji se koriste za pružanje određene usluge turistima ili koje

[5] Florencio-Palacios B. Roldan-Santos L., Pineda-Berbel Manuel J., ,Canalejo-Castillo A.: Sustainable Tourism as a Driving force of the Tourism Industry in a Post-Covid-19 Scenario; Social Indicators Research 158; str. 996; 2021.

služe za pojednostavljivanje procesnih funkcija u hotelu. Prilikom izvršenja takvih napada gosti mogu izgubiti svoje privatne podatke, imovinu, kartične podatke ili ih se može tražiti otkupnina ako se dogodi kriptiranje njihovih podataka ili takozvani Ransomware napad. Važnost pametne zdravstvene skrbi u pametnim gradovima je od ključne važnosti. Kako se gradovi povezuju i postaju sve više usmjereni na tehnologiju, uključivanje pametnih zdravstvenih sustava postaje neophodno. Pametni zdravstveni sustavi mogu optimizirati isporuku zdravstvenih usluga usmjeravanjem procesa, smanjenjem vremena čekanja i osiguravanjem pravovremene i točne medicinske skrbi. Udaljene zdravstvene usluge omogućavaju pacijentima da se konzultiraju s liječnicima iz udobnosti vlastitih domova. Ova opcija ne samo da štedi vrijeme i resurse, nego povećava pristup zdravstvenoj skrbi, posebno za ljude u udaljenim područjima ili s poteškoćama u mobilnosti. Napredno upravljanje igra ključnu ulogu u izgradnji i održavanju pametnih gradova. Kroz korištenje tehnologije i analitike podataka, omogućuje učinkovitu isporuku usluga utemeljenih na podacima, transparentnost, sudjelovanje građana, održivo urbanističko planiranje, javnu sigurnost i integraciju gradskih usluga. Pametnim upravljanjem se potiče ekonomski rast, inovacije, digitalna infrastruktura i otpornost gradova na nepredviđene izazova. Koncept pametne turističke destinacije proizlazi iz razvoja pametnih gradova. Pristup koncipiranju pametnih gradova se usredotočuje na građane, a pametna destinacija uključuje građane zajedno s turistima i putnicima.[6]

[6] Demertzi V., Demertzis S., Demertzis K.: An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities; Applied Sciences, Vol.13, No.2: 2022.



Slika 1: Primarni elementi pametne destinacije
Izvor: Demertzi V., Demertzis S., Demertzis K.: An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities; Applied Sciences, Vol. 13, No. 2, 2022.

1.3. Odnos održivog razvoja i pametne turističke destinacije

Usmjerenje pažnje na održivi turizam u zadnjih je nekoliko godina uhvatio pažnju raznih institucija kojima je cilj smanjiti štetne posljedice masovnog turizma i turističkih kretanja na ugroženim mjestima. Potrebne mjere za sprječavanje budućeg nekvalitetnog temelja za turizam se poduzimaju u sve intenzivnijim pokušajima, a smart turizam također pridonosi tim ciljevima. Korištenjem digitalne tehnologije smanjuje se štetnost prekomjernog papirnatog otpada radi digitalnih obrazaca i platformi, smanjuje se sveukupna potrošnja energije te nepoželjne emisije ispušnih plinova u atmosferu. Smanjenje emisije ispušnih plinova u okolinu povezuje se s implementacijom online sustava za rezervaciju smještaja koji smanjuju potrebu za fizičkim putovanjima i upotrebom prijevoznih sredstava, ali isto tako i s virtualnim turama koje su u zadnjih nekoliko godina postale poznatije među turistima.. Pametnim turističkim destinacijama pogoduje razvoj tehnologija za reguliranje i uvid u potrošnju energije i prikaz kvantitativnih podataka iz kojih pametna turistička destinacija u budućnosti može eliminirati određene probleme. Tako na primjer u hotelima

danas postoje pametni uređaji koji reguliraju potrošnju vode i energije. Primjerice Adeunis Temperature Monitor je Internet of Things uređaj koji pomaže pri pravilnom održavanju hotelskih sanitarnih čvorova reguliranjem potrošnje vode i njezinim filtriranjem radi zdravstvene ispravnosti. Uređaj koristi Temp 2S senzore koji se koriste za mjerenje temperature vode i preko uređaja izdaju obavijesti kada temperatura padne ispod 55°C. Korisnici također imaju pristup podacima preko Energisme platforme gdje su dostupni svi potrebni podaci za željena razdoblja. U današnje vrijeme se koriste digitalni IoT uređaji za regulaciju potrošnje energije, nadogradnju ekoloških monitoring sustava, smanjenje sveukupnog troška te povećanje produktivnosti.[7] Pravilnom zaštitom ovakvih sustava indirektno se utječe i na napredak održivog. ICT tehnologija je postala jednim od glavnih elemenata za postizanje ekonomskog razvoja dvadeset prvog stoljeća. Mnogi pametni digitalni sustavi pozitivno utječu na održivi razvoj u turizmu. Primjerice pametna infrastruktura, programi za prikupljanje velike količine podataka, upravljanje na daljinu i slično. Međutim, bez adekvatne elektroničke zaštite ti sustavi postaju nepouzdani i predstavljaju veliki rizik. Za sprječavanje negativnih učinaka smart turizma na okoliš potreban je adekvatan menadžment destinacije i poznavanje granice posjećenosti kako bi se spriječila dugoročna ekološka degradacija turističkog prostora. Pretjerano korištenje moderne digitalne tehnologije može čak uzrokovati i veću nepotrebnu potrošnju energije nego što je potrebno i povećanje nakupljanja nerecikliranog e-otpada. Razvoj pametnog turizma u destinaciji može imati pozitivne utjecaje na održivi razvoj, ali samo uz adekvatnu opremljenost informatičkim zaštitnim sustavima. Digitalizacija pojednostavljuje reguliranje potrošnje i brže se prikupljaju potrebni podaci za daljnju analizu, ali isto tako porastom digitalizacije se povećava rizik od prekomjernog posjećivanja destinacije, zagađenja, sakupljanja elektroničkog otpada te od kibernetičkih napada koji mogu ostaviti dugoročne posljedice kada je u pitanju održivi razvoj. Primjer kvalitetnog provođenja plana održivog razvoja je otok El Hierro, ujedno i prvi pametni otok na svijetu. U mnogim europskim otocima turizam je u zadnjih nekoliko desetljeća postao glavni izvor prihoda. Sukladno tome, potreba za smanjenjem dugoročne ovisnosti, optimizacijom uporabe resursa i osiguravanjem kvalitete života ljudi potaknule je primjenu pametnih rješenja u turizmu. Projekt otoka je učiniti ga 100% energetski samodostatnim. Trenutno omogućuje svima

[7] Hertzfeld, E.: How IoT can help with energy management; https://www.hotelmanagement.net/tech/how-iot-can-help-energy-management (2020.) (pristupljeno 10.4.2023.)

besplatni Wi-Fi. Kroz Wi-Fi mreže otokom se upravljaju sustavi za nadzor prometa, sustavi za reguliranje požara, reguliranje vode, otpada i slično. Otok je također razvio aplikaciju koja omogućuje turistima iščitavanje QR kodova preko kojih mogu saznati informacije o turističkim atrakcijama na četiri različita jezika. Mjestima kao El Hierro, koji ovise o održivom razvoju i prirodnim izvorima energije, sigurnost informacijskih sustava treba biti prioritet. Takvim destinacijama od izrazite je važnosti sačuvati dobru reputaciju i slati poruku sigurne destinacije.[8] U izvješću iz 2021. godine o održivom putovanju stranice Booking.com, 61% putnika je izjavilo da ih je pandemija potaknula da putuju na održiviji način. Također, 81% putnika je izjavilo da želi boraviti u održivim smještajnim objektima u sljedećoj godini.[9]

1.4. Pametni hoteli u pametnoj turističkoj destinaciji

Pojava pametnih hotela promijenila je način funkcioniranja pametnog turizma u pojedinim destinacijama. Pametni hoteli su vrsta smještajnog objekta koji nudi gostima usluge doručka i smještaja, ali glavna karakteristika im je korištenje napredne digitalne tehnologije kako bi gostima omogućili jednostavniji boravak i postigli veću tečnost poslovnih procesa u hotelu. Prema istraživanju provedenom od strane Expedie. Prema studiji Exepedia-e, u 72% slučajeva putnici će odabrati hotel s višim ocjenama gostiju umjesto hotela poznatog brenda ili s nižom cijenom.[10] Za jednostavnije praćenje stanja hotela i protok gostiju koriste se Big Data software-i za analizu podataka. Hoteli koriste različite vrste tehnologije kao primjerice već spomenuti Internet of Things, automatizaciju te umjetnu inteligenciju kako bi postigli što personaliziraniji pristup gostu. Implementacijom pametne tehnologiju u velikom dijelu hotela raste i vjerojatnost kibernetičkih napada na informacije gosta, a u nekim slučajevima u opasnost dolazi i njihova fizička imovina koju su donijeli u hotel.

[8] Lopez Cappa, R.: The Sustainable Development Plan of El Hierro and its Impact on the Tourism Industry: Desarrollo sostenible; Repositorio institucional de la Universidad de La Laguna; 2018.
[9] Booking.com; Sustainable Travel Report 2022.: https://www.ukinbound.org/wp-content/uploads/2023/01/Booking.com-Sustainable-Tourism-Report-2022.pdf (pristupljeno 15.6.2023.)
[10] Study Shows Hotel Price and Ratings More Important Than Brand Name - https://www.travelpulse.com/News/Hotels-and-Resorts/Study-Shows-Hotel-Price-and-Ratings-More-Important-Than-Brand-Name (Pristupljeno 15.6.2023)

1.5. Kibernetička sigurnost pametnih hotela

Kada se govori o kibernetičkoj sigurnosti u hotelima, nedovoljno zaštićeni hotelski informacijski sustavi također mogu predstavljati izvor rizika za identitet turista, kao i informacije o bankovnim karticama, jer turisti u većini slučajeva koriste kreditne ili debitne kartice za plaćanje hotelskih usluga te tako ostavljaju svoje podatke na web stranicama koji su tada podložni aplikacijama za phishing napade. Stoga je potrebno implementirati sigurnosne certifikate na web stranici hotela kako bi se smanjio rizik od krađe. Rizik tada i dalje postoji, ali u znatno manjoj mjeri. Budući da danas svi smještajni objekti nude mogućnost spajanja na hotelski Wi-Fi, postoji opasnost od napada na pametne telefone ili računala gosta upravo preko njega. Svaki gost u hotelu, ali i u pojedinim destinacijama može koristiti isti Wi-Fi, a kada je mnogo ljudi spojeno na istu mrežu, tada raste rizik izvršenja višestrukog napada. Još je veća vjerojatnost od kibernetičkog napada ako je gost spojen na nezaštićeni javni Wi-Fi.[11]

Neki od primjera pametne tehnologije koje se uvode u hotelima su tableti u sobama za kontroliranje temperature i osvjetljenja, digitalne usluge koje se aktiviraju glasovnim naredbama gosta, check-in i check-out na daljinu i regulacija energije. Jedna od važnijih inovacija u pametnim hotelima je Smart Lock tehnologija. To su elektroničke brave koje gostima dopuštaju ulazak u njihove sobe korištenjem njihovih mobitela, osobnih iskaznica, otisaka prstiju ostalih biometrijskih čimbenika. Gosti hotela ne trebaju više nositi ključeve stalno sa sobom već sve potrebne podatke imaju na njihovim pametnim uređajima. Unatoč tome što pružaju veću razinu sigurnosti nego standardne hotelske brave u posljednjih nekoliko godina zabilježeni su napadi upravo na Smart Lock sustave u hotelima. Moguću opasnost predstavlja i kibernetički napad i na sami pametni uređaj gosta na kojemu se nalaze sve potrebne informacije za ulazak u sobu. Kibernetičkim napadom na Smart Lock sustave napadač može doći do osobnih informacija gosta, ali isto tako i do informacija koje govore gdje se gost nalazi. Provaljivanjem u Smart Lock sustav napadač može upasti gostu u sobu i ukrasti vrijednu imovinu. Potencijalnu opasnost predstavlja i mogućnost nastanka tehničkog kvara ili pojave „glitcheva“ u sustavu Smart Locka što bi spriječilo gosta da uđe u sobu na određeno vrijeme. Potrebna sigurnosna mjera je informiranje gosta o opasnostima

[11] WGU.edu: The Top 7 Dangers of Public Wi-Fi for Businesses - https://www.wgu.edu/blog/7-dangers-public-wifi-businesses2112.html#close (pristupljeno 15.6.2023.)

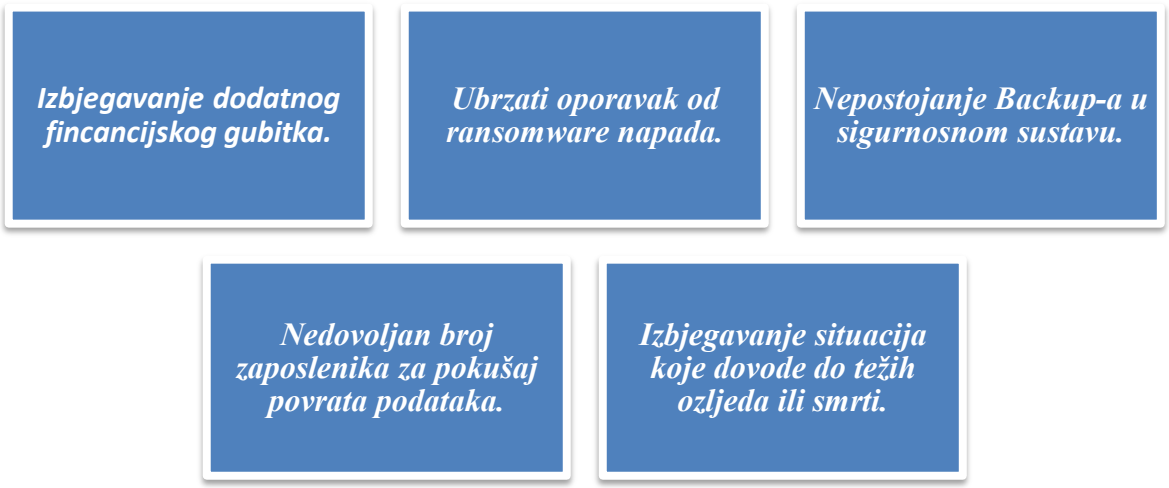
kibernetičkim napadima te o svim mogućim rizicima koji se potencijalno mogu dogoditi. Uzimajući u obzir da se većina kibernetičkih napada dogodi zbog nepažnje individualca, potrebno je gostu pomno objasniti na koje načine treba čuvati svoje podatke i da bilo koju sumnju treba odmah prijaviti. Provaljivanje u Smart Lock sustav također šteti i hotelu jer uzrokuje stagniranje hotelskih procesa te potencijalno može naštetiti ugledu hotela što može rezultirati time da će izgubiti a povjerenju gostiju. 2019. godine je otkrivena ranjivost u Smart Lock sustavu Vision by VingCard koji je razvijen od strane poduzeća Assa Abloy. Ovaj sustav Smart Lock tehnologije se koristi u više od 40,000 hotela diljem svijeta pa je odstranjivanje ove ranjivosti u sustavu bilo od izrazite važnosti radi smanjenja rizika od višestrukog napada. Istraživači iz F-Secure institucije su dijagnosticirali su problem u sustavu te su došli do zaključka da je problem neredovito ažuriranje sustava i da je potrebno dodatno razviti enkripcijski sustav podataka pošto je zastario. Na početku se pretpostavljalo kako bi napadač trebao biti fizički prisutan kako bi ostvario napad, ali se ispostavilo da je moguće to učiniti i pomoću mikrokontrolera te modificiranog hotelskog ključa. Mikrokontroler predstavlja kompaktni integrirani krug koji je dizajniran za upravljanje određenom operacijom u ugrađenom sustavu. Posljedice izvođenja ovakvog napada imale bi velike posljedice jer bi omogućile izradu digitalnog master ključa koji bi imao pristup svakoj hotelskoj sobi. Smart Lock sustave ne koriste samo hoteli, već i ustanove u kojoj je potrebna veća razina sigurnosti, pa su potencijalne prijetnje ovakvog napada sveobuhvatne. Ovaj slučaj služi kao primjer važnosti ažuriranja sigurnosnih sustava te penetracijskog ispitivanja sigurnosnog sustava kako bi se ranjivosti utvrdile od strane korisnika prije nego što problem u sustavu uoče napadači.[12]

Još jedan primjer provaljivanja u Smart Lock sustav se veže uz poduzeće LockState koje je zbog loše izvedenog firmware ažuriranja omogućilo brojne prijetnje na njihov sustav. Napadači mogli ukrasti tokene za ulazak gosta u sobu uz pomoć samo MAC adrese. MAC je Media Access Control Adresa. MAC adresa je trajna adresa koja služi kao identifikator hardverskog proizvoda te je obično otisnuta na procesoru uređaja. [13]

[12] Schneier.com: Security Vulnerabilities in VingCard Electronic Locks - https://www.schneier.com/blog/archives/2018/04/security_vulner_14.html (pristupljeno 30.5.2023.)
[13] Eenewseurope.com: IoT's Smart Lock bricked by software update - https://www.eenewseurope.com/en/iot-smart-lock-bricked-by-software-update/ (pristupljeno 30.5.2023)

1.6. Opasnost Ransomware napada u pametnim turističkim destinacijama

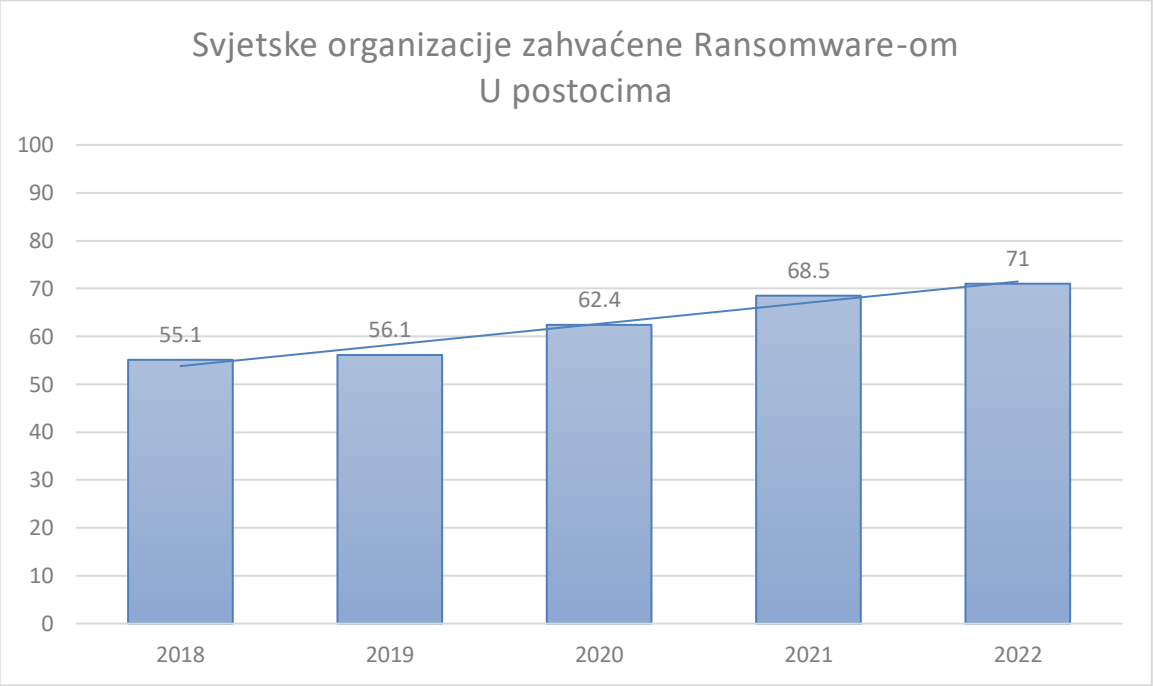
Ransomware je vrsta zlonamjernog softvera koji je dizajniran da blokira pristup računalnom sustavu, mobilnom sustavu ili određenim datotekama dok se ne plati otkupnina. Ovaj softver djeluje tako da kriptira datoteke na sustavu žrtve i čini ih nepristupačnima sve dok se za njih ne uplati zadana otkupnina (ransom). Računalo se može zaraziti Ransomware-om na razne načine, od phishing prijevara, preuzimanja zaražene datoteke ili ranjivosti u operativnom sustavu. Nakon što je Ransomware zarazio operativni sustav, korisniku se obično na ekranu pokaže prozor na kojemu su izdvojeni detalji za uplatu novca i posljedice ako se to ne uradi na vrijeme. Plaćanje se vrši obično u Bitcoinu jer je takvome načinu plaćanja teže uči u trag. Ransomware napadi sa sobom nose više od jednog rizika. Primjerice u pametnim destinacijama Ransomware ima veliki opseg uređaja koje može obuhvatiti. Od gradskih digitalnih platformi do pametnih hotelskih uređaja.



Slika 2: Najčešći razlozi plaćanja otkupnine u poduzećima[14]

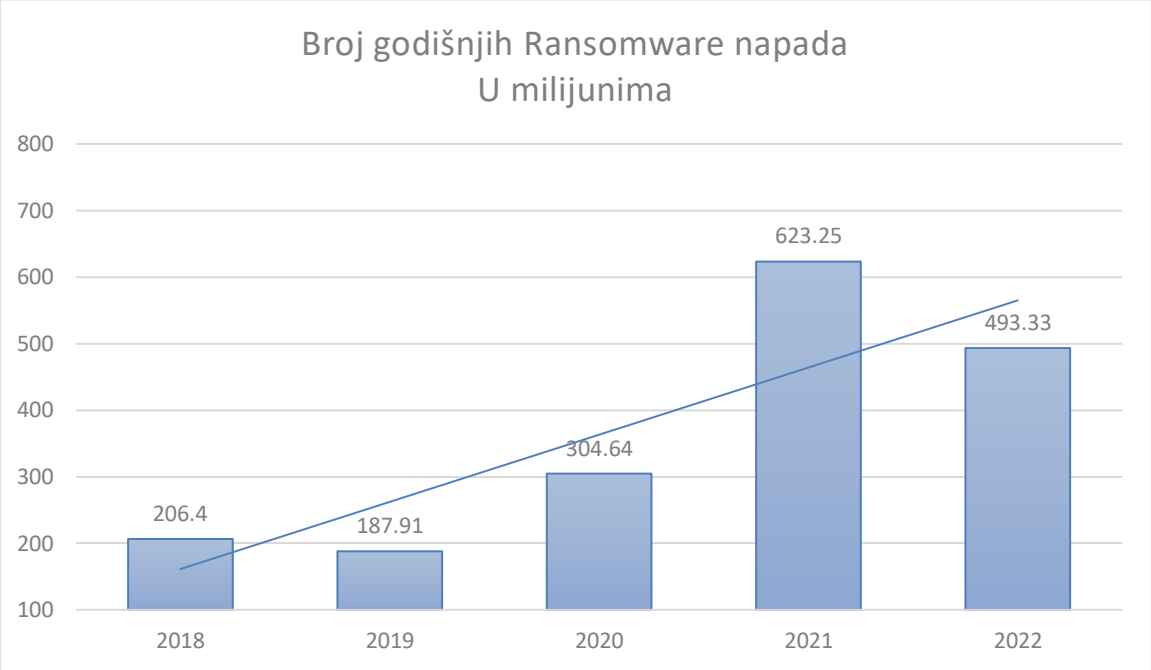
[14] AntivirusGuide: Ransomware Statistics: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=CjwKCAjwuqiiBhBtEiwATgvixCbUk1QwOxx_ZIY8sX227TrEYhmzF_Q57NMAp7goftqtYLwNF1Jf1RoC8DYQAvD_BwE (pristuljeno 30.4.2023.)

Takav napad ima više štetnih i rizičnih posljedica za objekt radi toga jer je napada indirektno vezan i sa gostima hotela. Napad na pametne objekte može indirektno uzrokovati krađu gostovih informacija, uzrokovati paniku i daljnje nepovjerenje prema tome objektu, radi čega može dobiti negativnu reputaciju. S druge strane objekt trpi stagnaciju poslovnih procesa za vrijeme Ransomware napada, dodatne financijske gubitke, trošenje vremena radi uočavanja ranjivosti u sigurnosnom sustavu i nemogućnost daljnjeg poslovanja i funkcioniranja pametne tehnologije.Statistički podaci da Ransomware napada sve više organizacija diljem svijeta, a broj je konstantno u porastu od 2018. godine do danas, što predstavlja idući grafikom.



Grafikon 1 : Svjetske organizacije zahvaćene Ransomware-om
Izvor: Obrada podataka prema "AntivirusGuide; Ransomware Statistics: 2022."

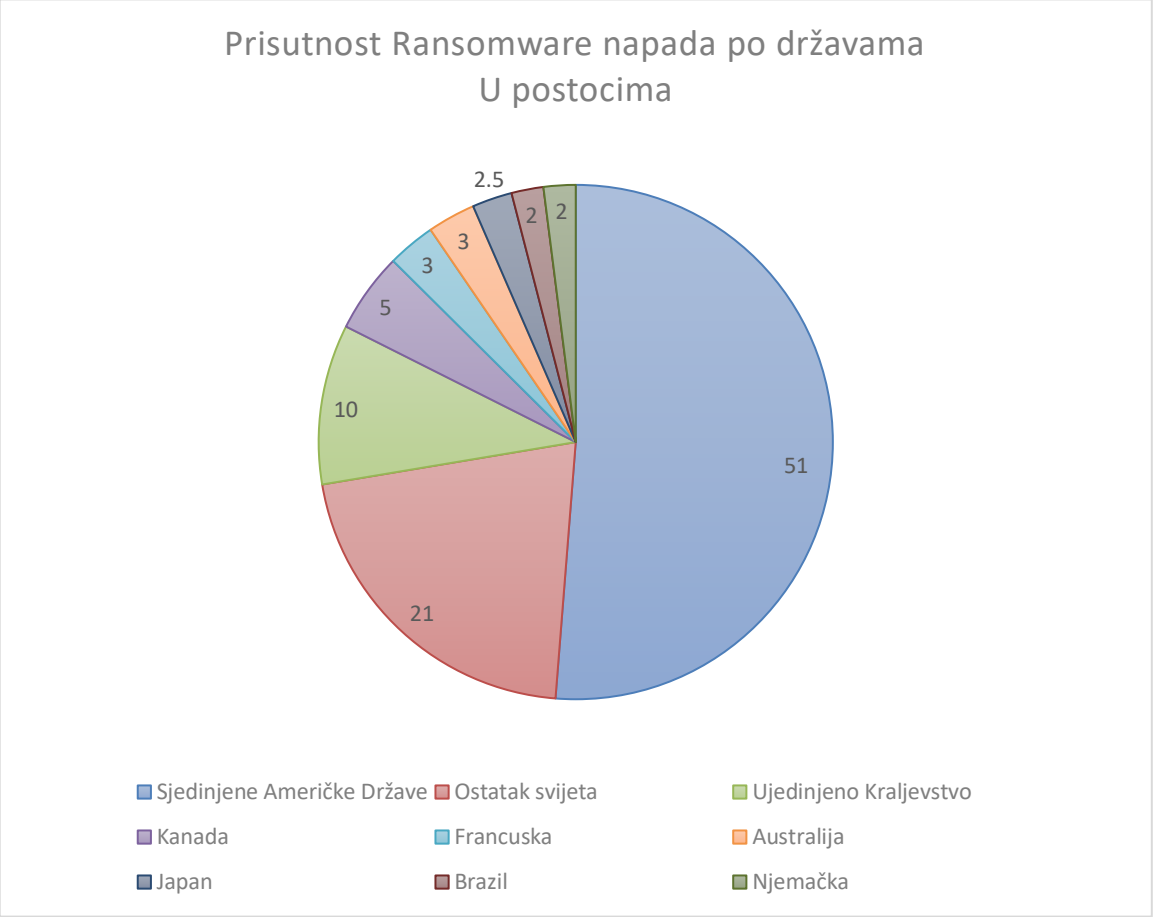
Međutim, sveukupni broj ransomware napada u svijetu bilježi smanjenje nakon drastičnog porasta zabilježenog 2021. godine. To može biti posljedica pojačavanja sigurnosnih sustava nakon povećanja broja napada, a isto tako i radi smanjenja intenziteta pandemije COVID-19 koja je dovela do toga da veliki broj ljudi i poduzeća pređe na online okruženje i rad na daljinu.



Grafikon 2: Broj godišnjih Ransomware napada
Izvor: Obrada podataka prema "AntivirusGuide; Ransomware Statistics: 2022."

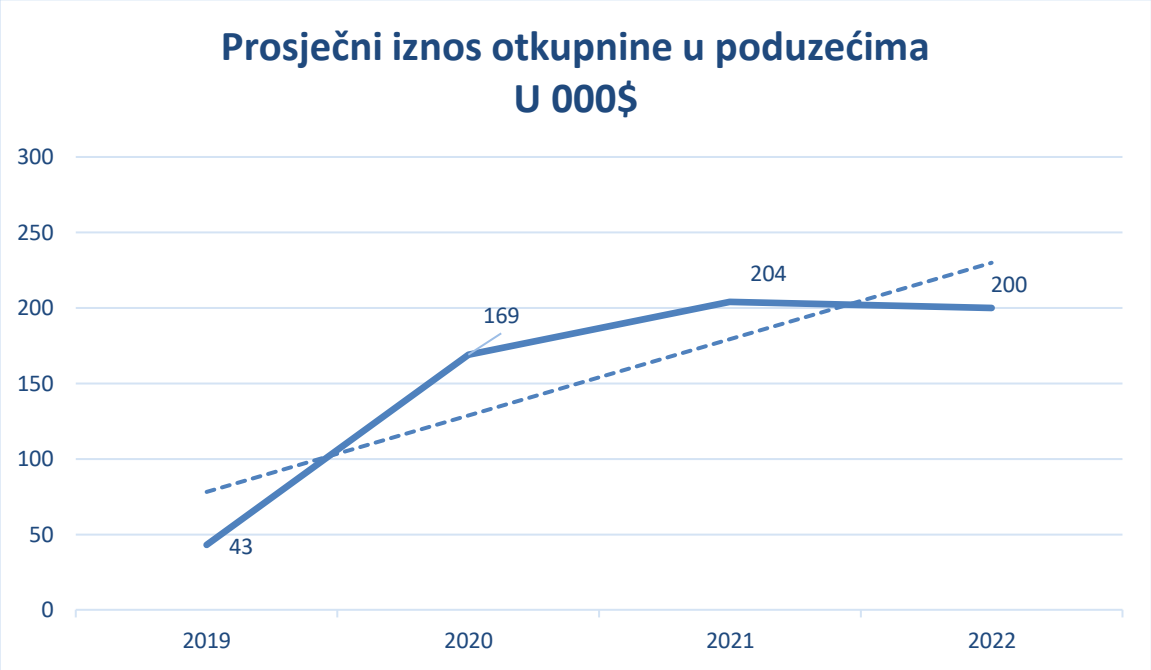
Iz idućeg priloženog grafikona može se iščitati učestalost Ransomware napada po državama diljem svijeta. Iz navedenog grafikona vidljivo je da Ransomware napadi najveću prijetnju predstavljaju Sjedinjenim Američkim Državama, s čak 51% napada usmjerenim upravo tamo. Ovakav postotak predstavlja izrazito veliku broju i na jedan način usporava razvoj pametnog turizma na tim mjestima. Uvođenje pametne tehnologije i pametnih hotelskih objekata u Sjedinjenim Američkim Državama bi isto tako značio i veći rizik od povećanja kibernetičkih napada. U Sjedinjenim Američkim Državama se također često događaju ransomware napadi na veći broj računala, što kao rezultat ima gubitak većeg broja podataka. Ransomware napadom na turistička središta u Sjedinjenim Američkim Državama oštetio bi se veliki opseg hotelskih objekata i turista koji su povezani s njima. Primjerice 2020. godine zabilježen je ransomware napad na Key West u Floridi koji je uzrokovao prestanak izvođenja gradskih usluga i operacija. Ransomware je bio višestruki i napao je glavne računalne sisteme. [15]

[15] MiamiHerald.com: Key West City Hall computers have been shut down for a week: https://www.miamiherald.com/news/local/community/florida-keys/article245467410.html (pristupljeno 30.4.2023.)



Grafikon 3: Prisutnost Ransomware napada po državama
Izvor: Obrada podataka prema "AntivirusGuide; Ransomware Statistics: 2022."

Nakon naglog porasta u povećanju prosječne cijene za povrat podataka, bilježi se minimalan pad u 2022. godini. Nakon naglog porasta za više od 150.000$ 2020. godine trend povećanja cijene je nastavio rast i u 2021. godini rastući tako na 204.000$, te je počeo 2022. bilježiti pad na 200.000$ prosječne tražene otkupnine. To je količina novca koja znatno može utjecati na poslovanje hotela i na funkcioniranje pametne destinacije u budućnosti. Ako se dogode više ransomware napada u kratkom vremenu pametna destinacija se vrlo brzo naći u financijski problematičnoj situaciji radi neočekivanog troška povrata podataka. Pojava Locker ransomware predstavlja prijetnju za turiste. To je vrsta ransomware-a koja napada isključivo mobilne uređaje. Turisti koji nisu dovoljno upoznati sa jezikom destinacije u kojoj se nalaze su izrazito podložni ovakvim napadima. Takav napad utječe na privatnost turista, njegovo sveukupno zadovoljstvo sa destinacijom, osjećaj bespomoćnosti i dodatni trošak povrata podataka.



Grafikon 4: Prosječni iznos otkupnine u poduzećima
Izvor: Obrada podataka prema "AntivirusGuide; Ransomware Statistics: 2022."

2. INTERNET OF THINGS

Internet stvari (IoT) je sustav povezanih računalnih uređaja, mehaničkih i digitalnih strojeva i objekata kojima su dodijeljeni UID indikatori i sposobnost prijenosa podataka putem mreže bez potrebe za interakcijom između ljudi ili računala.[16] Primjeri Internet of Things uređaja koji se često koriste u turizmu su smart lock sistemi u hotelskim sobama, sustavi za regulaciju temperature i potrošnje energije, pametne naočale, pametni mobilni uređaji te pametni sustavi prijevoza. Sam internet stvari postoji već desetljećima, ali je tek krajem devedesetih godina stekao prepoznatljivost u svijetu digitalne tehnologije. Zbog ubrzanog razvoja tehnologije povećala se i efikasnost djelovanja interneta stvari. Pojavile su se nove mogućnosti spajanja na veći broj uređaja, a danas služi kao osnova funkcioniranja pametnih turističkih destinacija. Internet stvari nudi mogućnosti poboljšanja svakodnevnog života te ima sposobnost transformacije turističkih destinacija u destinacije koje se fokusiraju na digitalnu tehnologiju.[17]

Iako imaju mnogo pozitivnih utjecaja, radi široke uporabe interneta stvari raste i mogućnost za kibernetičke napade na uređaje koji ga koriste. Jedna od mana je da je internet of things ovisan o dostupnosti internetske povezanosti kako bi svi predmeti funkcionirali. Povremeni nestanak električne energije ili interneta može u potpunosti zaustaviti rad nekih uređaja koji mogu biti od iznimne važnosti za poduzeće ili turističku destinaciju. Internet stvari ne koriste samo najpouzdaniji i najpoznatiji svjetski proizvođači, nego su prisutni i kod manje vjerodostojnih proizvođača pa je i samim tim njihova kibernetička sigurnost upitna. Vezano uz to, mnogi internet of things uređaji u sebi sadržavaju komponente od različitih proizvođača što otežava jamčenje sigurnosti uređaja u cijelosti.[18] Kada se govori o komponentama koji pripadaju različitim proizvođačima, valja napomenuti da kod internet of things uređaja postoji također opasnost od dijeljenja osobnih podataka s takozvanim „Third-party“ kompanijama bez znanja korisnika. Unatoč tome što je ova vrsta uređaja

[16] Azrour, M., Mabrouki, J., Guezzaz, A., Kanwal, A.; Internet of Things Security: Challenges and Key Issues; Security and Communication Networks, vol. 2021.
[17] Researcgate.net; Wise, N., Heidari H.; Developing Smart Tourism Destinations with the Internet of Things: Managerial Approaches, Techniques, and Applications; Big Data and Innovation in Tourism, Travel and Hospitality (2019.)
[18] Analyticsinsight.net; IoT Standardization: Why IoT has not set standards yet?; https://www.analyticsinsight.net/iot-standardization-why-iot-has-not-set-standards-yet/ (pristupljeno 14.4.2023.)

veoma rasprostranjena i vremenski efikasna, korisnik uređaja će teže biti svjestan da je špijuniran ili da su mu ukradeni osobni podaci ako se radi o IOT uređajima. U većini slučajeva ne pokazuju nikakve signale ili obavijesti koje bi mogle pravovremeno upozoriti korisnika. Opasnost kod mnogih IOT uređaja je upravo nedostatak adekvatnih i pravovremeno ažuriranih sigurnosnih sustava, a u velikom broju slučajeva nedostaju i oni najosnovniji sustavi kao što su firewall ili enkripcija podataka. Isto tako javljaju se i nedostaci kod sigurnosnih standarda kod IoT uređaja u smislu da nemaju svi jednako razvijenu sigurnosnu razinu što može dovesti do nejednakih mjera sigurnosti od uređaja do uređaja. IOT uređaji mogu se koristiti i za videonadzor. To je veoma korisna opcija u većim turističkim poduzećima koja omogućava efikasniju mogućnost praćenja gostiju, zaposlenika i većih prostora. S pojavom takvih uređaja posebno je izražena opasnost od preuzimanja kontrole napadača nad funkcijama kamere čime se narušava privatnost svih prisutnih te može uzrokovati krađu osobnih podataka isto kao i onemogućavanje funkcioniranja sustava za videonadzor što može potencijalno rezultirati i nekom drugom vrstom napada na objekt ili destinaciju.

2.1. Opasnosti kibernetičkih napada na pametan prijevoz destinacije

Pametni prijevoz u pametnim turističkim destinacijama obuhvaća široki spektar uređaja i tehnologija koji međusobnim djelovanjem osiguravaju veću sigurnost i preciznost kod prijevoza putnika ali isto tako i smanjuju zagađenje destinacije. Suvremeni automobili postaju sve više povezani internetom, a neke od njihovih funkcija ovise isključivo o internetskoj povezanosti za njihovo funkcioniranje. U pametnim turističkim destinacijama od izrazite je važnosti razvoj i uvođenje Pametnih transportnih sistema (Eng. Intelligent Transportation Systems). ITS predstavlja sustav aplikacija, vozila i tehnologije kojom se jednostavnije upravlja prometom u destinaciji. Predstavlja ključnu ulogu u kvaliteti prijevoza gostiju u destinaciji.[19] Mogućnost putovanja destinacijom dostupna je na jednostavniji i precizniji način što rezultira i povećanim zadovoljstvom turista. Isto tako, radi mogućnosti Pametnih parking sustava smanjuju se gužve na cestama i sprječava gubljenje vremena turista na odmoru. Smart Traffic Management Systems uvode se u prometni sustav

[19] Oladimeji D., Gupta K., Kose Alperen, N., Gundogan K.: Smart Transportation: An Overview of Technologies and Applications; Sensors Vol.23, No.8; 2023.

turističke destinacije radi lakše organizacije i bržeg protoka osobnih automobila u destinaciji.[20] Hakiranjem ovakve vrste sustava napadač ima mogućnost zamjeniti signale i znakove koji se pojavljuju u prometu i tako uzrokovati potencijalne opasnosti za turiste u destinaciji. Još jedan primjer je da napadač može prouzročiti gašenje rasvjete u kasnim satima što može uzrokovati prometne nesreće ili pojačane gužve na cestama. U Smart Traffic Management System-ima je također prisutan problem u neadekvatnoj standardizaciji tehnologije. Opasnosti u pametnim prijevoznim sustavima ne razlikuju se od opasnosti koje vrijede za ostale IoT uređaje. Međutim, opseg turista koje obuhvaća jedan napad na pametni prometni sustav je mnogo veći pa je od velike važnosti što preciznije definirati standarde i najaktualnije sigurnosne sisteme kako bi se minimalizirao rizik od nesretnih slučajeva. Kibernetički napadi na pametni prometni sustav stvaraju štetu za turista, ali potencijalno i za infrastrukturu same destinacija za čiju se obnovu u težim situacijama trebaju izdvojiti dodatna financijska sredstva od predviđenog. U pametnim destinacijama sve popularnija postaju autonomna prijevozna sredstva poput samovozećih autobusa. Isto tako u većem broju se pojavljuju i električna vozila kao što su skuteri, bicikli ili romobili koji omogućuju turistima upravljanje i navigiranje pomoću aplikacije. Međutim, sigurnosni rizici kod takvih oblika prijevoza su iznimno visoki zato što jedan kibernetički napad usmjeren na javni prijevoz može ugroziti veći broj putnika odjednom. Upravo radi međusobne povezanosti prijevoznih sredstava internetskom konekcijom napadi na vozila mogu imati posljedice koje potencijalno ugrožavaju život putnika. Kibernetičkim napadom moguće je upasti u sustav prijevoznih sredstava preko primjerice GPS sustava i promijeniti rutu putovanja. Stanice za punjenje električnih automobila u pametnim destinacijama također predstavljaju metu kibernetičkog napada. Pošto se bilježi rast popularnosti električnih automobila potaknuta je i češća izgradnja stanica za punjenje električnih automobila. 2016. godine zabilježen je ransomware napada na stanicu za punjenje električnih automobila u Austriji. Ransomware se zvao TeslaCrypt te je uzrokovao gašenje stanice i nemogućnost njenog korištenja sve dok se određena količina novca nije isplatila napadaču.

[20] Haiston, J.: What is a Smart Traffic Management System? : https://www.symmetryelectronics.com/blog/what-is-a-smart-traffic-management-system/ (pristupljeno 15.4.2023.)

2.2. Opasnost Botnet napada na Internet of Things uređaje

Botnet napadi predstavljaju visoku opasnost kada su meta napada IoT uređaji u pametnim turističkim destinacijama. To su napadi u kojoj je veći broj računala ili uređaja zahvaćen s malware-om koji omogućava napadaču kontrolu na daljinu.[21] Ako se uzme za primjer smještajni objekt, napadač prvo napada jedno računalo. Ako to računalo nije adekvatno zaštićeno „Intrusion Detection" alatima, napadač dobiva kontrolu i preko toga prvog zombie računala pokreće napada na sva ostala u tome poduzeću. Ako su sva računala spojena na isti Wi-Fi, opasnost od višestrukog napada postaje veća. Uređaji ili računala koja su zahvaćena s botnet napadom se nazivaju „bot" ili „zombie" uređaji, dok je osoba koja kontrolira tim uređajima „botmaster". Botnet napad karakterizira činjenica da se on izvodi na veliki broj uređaja istovremeno što može uzrokovati potpune zastoje u funkcioniranju određenih sustava od izrazite važnosti u pametnim turističkim destinacijama. Pametne destinacije su česta meta Botnet napada upravo radi njihovog kontinuiranog uvođenja novih IoT uređaja. Primjerice bilježi se povećano uvođenje IoT kamera i senzora za videonadzor i kontrolu prometnog stanja u destinaciji, što potencijalno privlači sve više Botnet napada radi njihove mogućnosti višestrukih napada. Za uspješno izvršavanje botnet napada potrebna je konstantna internetska povezanost sa zaraženim uređajima. Stoga su IoT uređaji jedna od najčešćih meta botnet napada. Ako se pravovremeno ne uoči botnet napad, a IoT uređaji ostanu spojeni na internet raste i količina podataka koju napadač može ukrasti od turista i od poduzeća kojeg napada. Botnet napadi se najčešće koriste za izvršavanje DDoS ili Denial of Service napada koji u potpunosti zaustavljaju funkcioniranje digitalnih uređaja. Botmasteri također imaju mogućnost izvršavanja ostalih vrsta kibernetičkih napada kao što su spamming, phishing, ransomware ili korištenje zombie uređaja za dobivanje kriptovaluti bez znanja korisnika. Ovakvi napadi mogu imati katastrofalne posljedice ako je meta napada prethodno spomenuti pametni prometni sustav u turističkoj destinaciji. Financijska sredstva i daljnje poslovanje poduzeća je u velikoj opasnosti ako se ovaj napad dogodi u većim razmjerima. Radi Bot Fraud vrste napada moguće je iz daljine generirati lažne klikove, mijenjati preferencije, preglede i ostale funkcije koje mogu uzrokovati loš ugled poduzeća te udaljiti investitore i poslovne suradnike.

[21] Kaspersky.com; What is a Botnet?: https://usa.kaspersky.com/resource-center/threats/botnet-attacks (pristupljeno 25.4.2023.)

2.3. Uloga virtualne realnosti u pametnom turizmu

Virtualna stvarnost se također definira i pod nazivom računalno-simulirana stvarnost (Eng. Computer Simulated Reality). Ova vrsta se oslanja na korištenje modernih tehnoloških uređaja koje spajaju svih pet ljudskih osjetila kako bi se postigla što veća razina realnosti kod korisnika. Pružanje svih pet osjetila nekada nije moguće pa se veliki broj ovakvih tehnologija oslanja na vizualna i auditivna osjetila kako bi se uspješno prenijelo iskustvo. Najčešće se za korištenje ove vrste stvarnosti koristi „Headset“ ili kaciga s posebnim zaslonom koja generira realistične slike i doživljaje. VR Headset se sastoji od više ekrana, leća i senzora koji registriraju korisnikove pokrete. Prema registriranim pokretima VR Headset optimizira sliku kako bi se postigao doživljaj boravka u virtualnom svijetu. Proširena stvarnost (Eng. Augmented Reality) se koristi uživo, što znači da ova vrsta proširuje našu postojeću stvarnost i na nju nadodaje iskustva pomoću raznih elektroničkih uređaja koji su za to kompatibilni kao što su primjerice mobiteli i tableti, koji su ujedno i najpopularniji. ARSG ili Augmented Reality Smart Glasses još je jedan od uređaja koji služi za uvođenje virtualnih informacija u realnome životu. Funkcioniraju kao ekrani koji se ugrade u naočale te se ističu po tome da ne zahtijevaju nikakav poseban trud da se nose na duži vremenski period, a korisnicima pružaju razne korisne informacije koje i u tome trenutku zanimaju. Ovakve inovacije i ujedno i implementacija AR tehnologije u tehnološke izume može utjecati na razvoj pametnih turističkih destinacija koje ovakve izume mogu ukomponirati u svoju ponudu te pojačati doživljaj turista. ARSG omogućuje turistu uživanje u željenim digitalnim opcijama primjerice pružanjem određene glazbe, dok istovremeno turist može uživati u stvarnome pogledu na svoju okolinu.

U posljednjih nekoliko godina se ova tehnologija proširila i na druge segmente tržišta pa tako i na turizam, naročito nakon restrikcija i stagnacije turizma uzrokovane pandemijom COVID-19.. AR i VR tehnologija su se počele uvoditi u digitalne ture koje postaju sve popularnije.[22] Počinju se koristiti u pametnim turističkim destinacijama kao vrsta pružanja uvida turistu kakva je destinacija koju želi posjetiti u stvarnome vremenu. Razvijaju se aplikacije koje mogu turista odvesti na željenu destinaciju u virtualnom svijetu kako bi

[22] Harvard.edu: The Rise of Virtual Reality Tourism; https://hir.harvard.edu/the-rise-of-virtual-reality-tourism-digitization-of-culture-in-the-time-of-covid-19/ (pristupljeno 25.4.2023.)

mogao brže i sigurnije donijeti odluku o želji posjećivanja te destinacije. Uvođenje ovakvih mogućnosti turistima može poslužiti i kao kvalitetni marketinški alat koji omogućava promoviranje destinacije turistima koji ne mogu osobno biti tamo. Edukacijski aspekt je također jedan od pozitivnih strana za uvođenje VR i AR sistema u pametne turističke destinacije jer može služiti kao sredstvo informiranja o povijesti i tradicijama nekih mjesta zajedno s dostupnim vizualnim pomagalima koji pojednostavljuju učenje. Primjer ovakve ponude je mjesto Cite Memoire u Montrealu koji na interaktivan način nudi putovanje kroz povijest grada uz komponiranje zvuka, slike i mogućnost pričanja priče o povijesti toga mjesta. Turisti koji imaju zdravstvenih poteškoća ili problema s kretanjem mogu pomoću AR uređaja upoznati destinacije koje bi im inače bile teško pristupačne. U većim pametnim turističkim destinacijama poput Tokya sustavi za virtualnu realnost se koriste za vođenje turista kroz puteve podzemnih željeznica, koje se tamo često koriste kao glavna vrsta prijevoza. Implementacija sustava virtualne realnosti u takvim pametnim destinacijama ima višestruke koristi za turizam. Turisti budu u kraćem vremenu pronašli put do lokacije koja ih zanima što znači da gube manje dragocjenog vremena. VR sustavi u takvim lokacijama obično imaju ugrađenu opciju za preporuke poznatih turističkih atrakcija sukladne s preferencijama turista, pa tako turisti na jednostavan način mogu pronaći mjesta koja ih zanimaju. U nekim pametnim destinacijama nema potrebe ni za posjedovanjem VR headseta za korištenje usluga virtualne stvarnosti. Pametne destinacije poput Helsinkija u Finskoj nude mogućnost pronalaska željenih atrakcija putem pametnih uređaja i tableta u skladu s GPS-om. Uvođenjem ovakve tehnologije pametne destinacije omogućavaju jednostavniju pristupačnost i mogućnosti učenja zainteresiranih posjetitelja, ali si isto tako podižu i kvalitetu marketinške strategije, ali i cjelokupnog doživljaja općenito

2.4. Kibernetičke prijetnje na sustave virtualne realnosti

Upravo s porastom popularnosti AR i VR tehnologije, raste i broj kibernetičkih napada na ovu vrstu uređaja. Pošto se AR i VR sistemi koriste i u pametnim turističkim destinacijama, opasnost takvih kibernetičkih napada postala je sve veća radi mogućnosti krađe ili neovlaštenog ulaska u veću količinu osjetljivih podataka. Takvi napadi sada imaju i veće posljedice, uz krađu osjetljivih podataka, radi integriranja VR i AR uređaja u turizam, oni mogu imati sada i ozbiljne štetne posljedice za poslovanje hotelskih objekata i same destinacije. Poduzeća u pametnim turističkim destinacijama koji intenzivno koriste AR i VR

tehnologije u pružanju ugostiteljskih usluga moraju imati dobro razrađene sigurnosne sustave protiv krađe osobnih podataka osobito radi razloga jer su u zadnjih nekoliko godina bili zabilježeni slučajevi gdje su kibernetički napadi na AR i VR uređaje, radi njihove povezanosti sa stvarnosti imali kao posljedice i fizičke ozljede korisnika. Primjer za kibernetički napad koji je za posljedice imao fizičke ozljede korisnika VR headseta pojavio se u 2018. godini prema podacima iz „Check Point Researcha". Napad je izvršen preko SteamVR software-a. Steam je najpoznatija platforma za kupovanje i igranje videoigara i među svojim brojnim uslugama nudi i usluge VR igranja. Prema podacima iz 2018. godine napad se odvijao preko HTC Vive headseta, a napadači su uspjeli izvršiti napad u kojemu su mogli izmijeniti slike koje se korisniku pojavljuju na headsetu i tako ga dovesti u potencijalno opasnu situaciju pošto to utječe na pokrete koje izvršava. Iako ovaj napad nije izvršen u turizmu i nije povezan, služi kao poveznica i usporedba za to što je sve moguće izvesti napadima na VR sisteme. Primjerice u turizmu kada bi napadači uspjeli ugroziti headset koji je namijenjen virtualnim razgledavanjima, turista bi se moglo dovesti u velike opasnosti što se tiče fizičkih ozljeda, tada odgovornost pada i na poduzeće koje je odgovorno za sigurnost gosta, ali i utječe se na ugled same turističke destinacije. Hakeri mogu također ubacivati određene elemente u kamere od headseta kao na primjer znakove koji bi mogli navesti korisnike da čini radnje koje odgovaraju napadačima. Pošto je u velikom broju slučajeva korisnik povezan s VR Headsetom sa svojim osobnim računom, moguće je putem napada ugroziti sigurnost osobnih podataka gosta što može dovesti do krađe kartičnih podataka ili krađe identiteta.[23] Prilikom napada na VR uređaje napadači imaju mogućnost krađe glasa gosta radi mikrofona koji je dio većine takvih uređaja što može rezultirati nastankom „Deepfake" profila. Deepfake profili su vrsta cyber prijetnje koja uključuje stvaranje lažnih online osoba korištenjem umjetne inteligencije i tehnika strojnog učenja. Ovi profili su dizajnirani da oponašaju stvarne ljude i mogu se koristiti za širenje lažnih informacija, lansiranje phishing napada ili provođenje drugih vrsta kibernetičkih napada. Deepfake profili se stvaraju korištenjem sofisticiranih algoritama koji mogu generirati slike, videozapise i tekst koji su neodvojivi od onih koji stvaraju stvarni ljudi. Za zaštitu od deepfake profila preporučuje se korištenje kombinacija tehnologije i ljudske inteligencije. Primjerice korištenje umjetne inteligencije i algoritama za otkivanje sumnjivih aktivnosti.

[23] Rutgers.edu: Security Vulnerabilites in Virtual Reality Headsets: https://www.rutgers.edu/news/rutgers-researchers-discover-security-vulnerabilities-virtual-reality-headsets (pristupljeno 27.4.2023.)

Još jedna vrsta opasnosti za korisnika javlja se iz činjenice da je headset povezan s kamerom, i ako bi se dogodio kibernetički napad na VR headset moguće je i otkrivanje lokacije gosta i ugrožavanje njihova privatnog života.

3. ROBOTIKA U PAMETNIM HOTELIMA

Uvođenje robotike u pametne hotele može imati snažan utjecaj na prepoznatljivost pametne turističke destinacije radi poboljšavanja personalizacije pružanja usluge i radi efikasnijeg obavljanja procesa u hotelima. Prvobitni roboti u hotelima nisu imali mogućnost pružanja zadovoljavajuće razine personalizacije usluge gostima, ali moderniji roboti u vrhunskim hotelskim lancima danas veoma detaljno funkcioniraju u tome pogledu. Unaprijed znaju identitet gosta i prema njegovim preferencijama roboti komuniciraju s drugim uređajima u hotelu kako bi stvorili što ugodniju atmosferu. Roboti u hotelu mogu obnašati razne funkcije koje pomažu gostima u svakodnevnim upitima u zahtjevima. U samim počecima uvođenja robotske tehnologije u hotele 2010.-ih godina oni su bili jednostavniji nego danas i mogli su obavljati samo nekoliko aktivnosti. Danas je robotika znatno naprednija i postaje sve češće pojava u pametnim hotelima. Roboti su se prvobitno koristili kao Customer Service usluge, pružali bi gostima informacije o obližnjim turističkim atrakcijama, hotelima i restoranima te gostima u više jezika mogu odgovoriti i na specifična pitanja koja imaju vezana za hotel ili destinaciju.[24]

3.1. Primjena robotike u pametnim hotelima

Primjer robota koji je programiran da u hotelu obavlja usluge room service-a je „Roomy“, autonomni mobilni robot u BW hotelu u Bugarskoj. Roboti se u hotelima mogu koristiti za održavanja i čišćenje prostora. Roboti današnje kvalitete mogu obaviti radove čistoće na efikasniji način nego čovjek, a istovremeno smanjuju financijski trošak hotela. Roboti u hotelima služe i kao zaštitni sustavi primjerice imaju mogućnost kontroliranja i evidencije određenih javnih površina, detektiraju sumnjiva ponašanja, također imaju mogućnost intervenirati u hitnim medicinskim slučajevima i pružanja prve pomoći. Animiranje gostiju je također jedna od mogućnosti korištenja robota u hotelima, uvedeni su roboti koji nastupaju u zabavnim parkovima, popularnim mjestima i turističkim atrakcijama. Primjerice 2016. godine Hilton McLean hotel je uveo robota vratara Connie. Nazvan prema osnivaču Conrad

[24] Samala, N., Katkam B., Shekhar R., Rodriguez R.: Impact of AI and robotics in the tourism sector: a critical insight; Journal of Tourism Futures, Vol 8; Issue 1; 2022.

Hiltonu. Njegova funkcija je pomaganje gostima u pronalasku željenog mjesta u destinaciji i pomoć oko orijentacije u hotelu. U sebi ima programiran GPS i mapu koja pretrage gosta sinkronizira s recenzijama i preporukama drugih ljudi, na temelju toga Connie preporučuje mjesto koje se najviše podudara sa zahtjevom gosta. Još jedan primjer su roboti Lexi, Micah i Ariel koji su uvedeni u hotelu Sky Sandton u Johannesburgu.[25] Oni su uvedeni kao odgovor na želju za distanciranjem za vrijeme pandemije COVID-19. Programirani su za usluge room service-a, pružanja informacija o putovanjima, orijentiranju gosta, a imaju i mogućnost nošenja prtljage do 300 kilograma težine. Pepper Robot je još jedan od poznatijih robota koji turistima nudi pomoć pri raznim zahtjevima. Takozvani „The Robot Built For People" ima mogućnost raditi personalizirane preporuke turistima i pomoći im pri odabiru točno onih aktivnosti koje ih zanimaju. Također služi i za prodaju, upselling i cross-selling čime se povećava prodajna efikasnost poduzeća te potencijalno uspješniji financijski rezultat. Pepper je prvi robot koji ima mogućnosti prepoznavanja lica i osnovnih ljudskih emocija, stoga se koristi iza razgovore sa turistima, ali i za pomoć radnom osoblju poduzeća. Roboti su također u manjoj mjeri počeli zamijenjivati vodiče na nekim turističkim destinacijama. Primjerice robot Artron služi kao vodić u muzeju „The Hiroshima Museum of Art" u Japanu, gdje vodi turiste kroz muzej, pruža detaljno sve potrebne informacije o događajima i činjenicama iz toga razdoblja te ima i mogućnost vođenja razgovora sa turistima i odgovaranja na postavljena pitanja vezana za muzej i povijesne događaje. Autonomni roboti za dostavu hrane i pića također postaju sve popularniji i tako u velikoj mjeri zamijenjuju ljudsku radnu snagu, a isto tako i sveukupne troškove poslovanja. To ima svoje pozitivne i negativne strane. Gubi se na personalizaciji usluge i prisutnosti ljudske komunikacije, ali istovremeno je financijski isplativije. U Yokohami postoje „DeliRo" roboti kojima je zadatak prvenstveno dostava hrane iz restorana na određeno mjesto. Postoje više ovakvih robota u tome gradu, a svaki pokriva svoje označeno područje dostave kako bi se dostava izvršavala što brže i točnije.

[25] Reinstein, D.: Hotel Sky Sandton introduces robot staff - https://www.travelweekly.com/Middle-East-Africa-Travel/Hotel-Sky-Sandton-introduces-robot-staff (pristupljeno 30.4.2023.)

3.2. Nedostaci robotike u turizmu i kibernetičke prijetnje

Jedan od najpoznatijih primjera uvođenja robota u hotel je Henn na Hotel u Japanu osnovan 2015. godine. Ovaj hotel se ističe po tome što je skoro cijela radna snaga bila sačinjena od robota. Počevši od recepcije, domaćinstva do robotskih batlera. Ulazak u sobe je također bio digitaliziran a koristi se biometrijski sustav sigurnosti prepoznavanja lica ili otiska prstiju.[26] Nakon nekog vremena ideja o potpunoj robotizaciji hotela se nije ispostavila kao najbolja. Roboti nisu bili dovoljno kvalitetno programirani te su se često kvarili i izazivali nezadovoljstvo kod gostiju. Primjerice hrkanje gostiju u sobama jer moglo slučajno aktivirati sustav za glasovne naredbe u određenim robotima što bi izazvalo buđenje gostiju usred noći. Hotel nije doživio veliki uspjeh i morao je zamijeniti gotovo pola svojih robota s ljudskom radnom snagom radi financijske neisplativosti.[27] U istome hotelu je 2019. zabilježen spyware napad na njihove robote koji su se nalazili u hotelskim sobama. Roboti se nazivaju Tapia roboti, a služili su za pružanje usluga informiranja gosta, navigiranja, vremenske prognoze i slično. Kako bi gost koristio sluge Tapia robota, morao se spojiti s njime na pametni uređaj, što predstavlja dodatnu opasnost za privatne podatke gosta. Radi ranjivosti u sustavu bilo je moguće svakome upasti u sustav i preko kamere na robotu iz daljine imati pogled u unutrašnjost sobe, a isto tako i prisluškivati radi ugrađenog mikrofona. Hotel je na kraju ažurirao sustav i potrebnim zakrpama odstranio ranjivost iz sustava.[28] „The Robot Restaurant“ u Tokyu sadrži robotske batlere koji uz posluživanje hrane i pića gostima prirede određene predstave.

Roboti također zahtijevaju konstantnu povezanost s internetskom vezom kako bi funkcionirali. Stoga nisu sigurni od kibernetičkih napada. Roboti u sustavima spremaju podatke o turistima i radnjama koje obavljanju u određenom vremenu. Pristupom tip podacima mogu se otkriti privatne informacije te izvršiti napadi na ostale robote u hotelu.

[26] Osawa, H., Arisa, E., Hattori, H.,: Analysis of robot hotel: Reconstruction of works with robots; 26th IEEE International Symposium on Robot an Human Interactive Communication (2017.)
[27] Ertzfeld, E.: Japan's Henn na Hotel fires half its robot workforce - https://www.hotelmanagement.net/tech/japan-s-henn-na-hotel-fires-half-its-robot-workforce (pristupljeno 30.4.2023.)
[28] Doctorow, C.: Japanese robot hotel chain ignored repeated warnings that its in-room „bed-facing“ robots could be turned nto spy devices - https://boingboing.net/2019/10/23/sorry-for-uneasiness.html (pristupljeno 13.4.2023.)

Napad na sustav u robotima može biti izvršen i od strane radnika koji je prošao izobrazbu ili je adekvatno informiran. Primjerice radnik nezadovoljan poslom može ući u sustav robota koji mu je svakodnevno pri ruci i počiniti kibernetički napad u vlastitom objektu. Man-In-The-Middle (MitM) napadi su vrsta kibernetičkih prijetnji koje najčešće ciljaju robote. Dokazano je da veliki broj robota danas ima slabiji sustav autentifikacije i autorizacije korisnika te koriste slabije metode sigurnosne enkripcije podataka. Roboti se u većini slučajeva ažuriraju preko Cloud Computing sustava, desktop programa ili aplikacije sa kojom komuniciraju. Man-in-The-Middle napadi omogućavaju napadaču prekidanje veze kod slanja podataka između aplikacije i robota i umetanje svojeg softverskog paketa koji mijenja načina rada robota. To se može dogoditi i na način bez da korisnik robota to primijeti.[29] Primjerice najčešći oblik ovoga napada je takozvani Eavesdropping ili prisluškivanje. Napadač tada ima pristup svim podacima koje prihvaća robot i ima opciju umetnuti svoje poruke, bez da gost ili korisnik robota to saznaju. U turizmu to može izazvati pogrešno navigiranje gosta, navođenje na pristup osobnim podacima, lozinkama, korisničkim imenima, dok u drugim granama kao medicini može imati posljedice opasne po život. Mana korištenja robota u hotelima je i nedostatak emocionalne povezanosti sa turistima, na što su se mnogi žalili u hotelima gdje je pretežito robotska radna snaga. Ne postoje spontane situacije sa robotima i svaka usluga će izgledati isto svaki put i u velikom broju slučajeva roboti neće biti u mogućnosti izvršiti određene posebne želje. Još jedan od popularnih napada na robote su Spoofing napadi. U ovoj vrsti kibernetičkog napada napadač se na mreži predstavlja kao drugi uređaj ili korisnik. Ova tehnika se koristi kako bi napadač krao podatke, zaobišao autorizacijske kontrole ili širio malware. U pametnoj turističkoj destinaciji veliku prijetnju predstavlja GPS spoofing robota, taj napad se izvodi tako da napadač šalje lažne GPS koordinate upravljačkom sustavu robota kako bi se promijenio njegov smjer kretanja te ga je tada moguće navoditi na napadačevu željenu lokaciju.

[29] Javeed D.: Man in the Middle Attacks: Analysis, Motivation and Prevention; International Journal of Computer Networks and Communication Security, Vol.8, No.7; (2020.)

4. ULOGA MOBILNIH UREĐAJA U PAMETNOJ TURISTIČKOJ DESTINACIJI

Od početka popularizacije mobilnih uređaja ranih 2010.-ih godina brzo se ispostavilo da oni svojim svestranim funkcijama budu imali značajan utjecaj na razvoj pojedinih gospodarskih grana pa tako i turizma. U kontekstu kibernetičke sigurnosti, posebno velik rizik predstavlja rezerviranje smještaja putem različitih internetskih usluga ili mobilnih aplikacija u kojima korisnik mora unijeti podatke poput broja bankovne kartice. U praksi se događaju slučajevi u kojima se navedeno koristi za bankovne transakcije s ukradenim karticama kroz fiktivne rezervacije u fiktivnom smještaju, zbog čega je potrebno zapošljavanje posebno osposobljenog osoblja u tim poduzećima koji će nadzirati takve transakcije i po potrebama poduzimati mjere zaustavljanja. Pametni uređaji su najzastupljeniji uređaji kod turista koji se spajaju na internet, a radi brojnih mogućnosti dopuštaju korištenje raznih aplikacija koje su povezane s mnoštvom digitalnih sustava te tako omogućavaju brži pristup potrebnim informacijama i jednostavnijem navigiranju. U današnje vrijeme svi mobilni uređaji imaju ugrađene senzore za korištenje usluge GPS-a, što je prva usluga na mobitelu koju turisti koriste kada odlaze na putovanje. GPS također pravovremeno informira turiste ukoliko je na određenim cestama nepogodna prometna situacija ili da li se približava loše vrijeme. RFID senzori su još jedna od opcija na mobilnim uređajima. RFID je skraćeno od Radio Frequency Identification. Ovi senzori koriste radiovalove u svrhu prijenosa podataka. Primjerice NFC opcija omogućava beskontaktna plaćanja kreditnim karticama. LBS ili Location Based Services predstavljaju na mobitelima korisnu opciju koja turistima omogućava pregled objekata ili obližnjih mjesta. Na taj način turisti imaju mogućnost sortirati dio turističke ponude koji ih zanima i radi kojih su došli. Kina je dobar primjer kada je u pitanju korištenje pametnih mobilnih uređaja za pružanje svih potrebnih usluga u turizmu. Kina je razvila mnoštvo aplikacija koje služe isključivo olakšavanju putovanja turista. Neke od tih aplikacija su Smart Lushan, I Xiangshan Travels te Nanjing Tourist Assistant. Pametni uređaji su u Kini stekli veliku popularnost jer se veliki broj stanovnika spaja isključivo kroz mobilni uređaj na internet.[30] Radi mnogobrojnosti lokalnog stanovništva i stranih turista na tome području pojavila se potreba za razvojem

[30] Liu, P., Liu, Y.: Smart Tourism via Smart Phone; Proceedings of the 2016 International Conference of Communications, Information Management and Network Security, 2016.

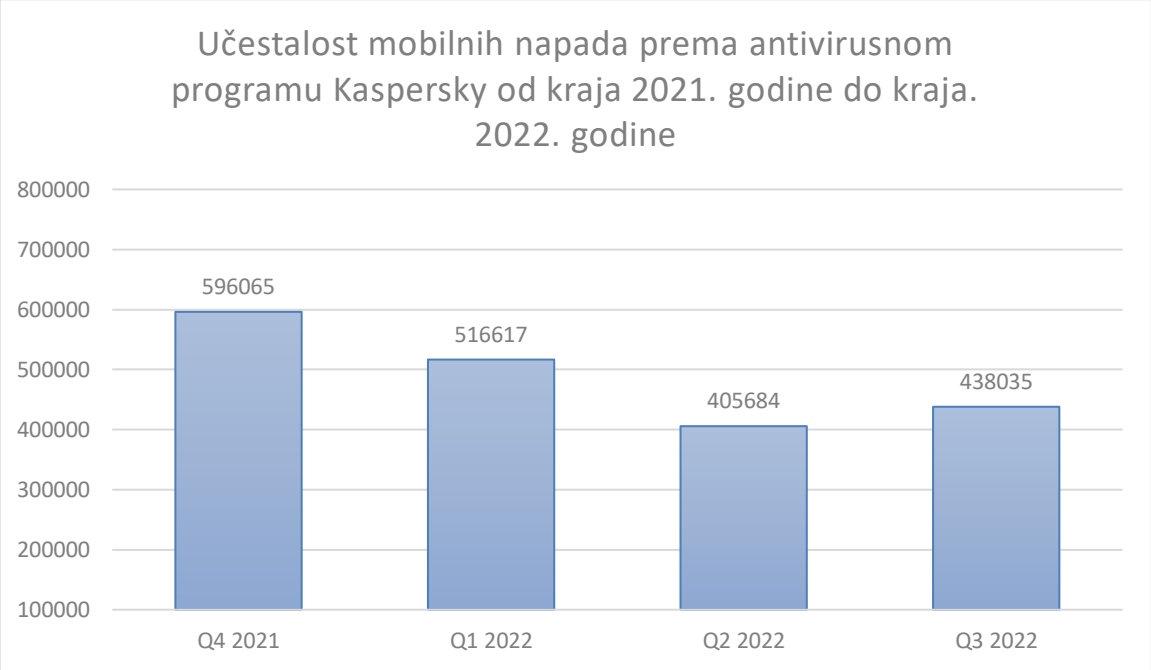
aplikacija koje bi pojednostavile kretanje te minimizirale nastanak prometnih gužvi i lakši protok turista u destinacijama. Postoje također aplikacije koje pomažu turistima pri pronalasku najekonomičnijeg putovanja u tome razdoblju. Primjerice aplikacija Hopper analizira cijene letova svakodnevno kako bi mogla dati izvještaj o tome kada je najbolje vrijeme za rezervaciju leta.

Mobilni uređaji ističu se i mogućnosti korištenja takozvanog Cloud Computinga. Cloud Computing koriste većina Internet of Things uređaja. Cloud dopušta spremanje potrebnih dokumenata i ostalih datoteka na za to predviđene internetske stranice koje su korisniku dostupne u bilo koje doba dok god je uređaj spojen na internetsku vezu. Služe i kao backup za potrebne podatke. Najpoznatije usluge za spremanje datoteka na cloud su Dropbox, Google Drive, TencentCloud, AWS, Alibaba Cloud, ali i mnogi drugi. Korisnik se na cloud spaja sa svojim korisničkim imenom i lozinkom. Problem kod Cloud computinga je centralizacija datoteka koje korisnici prilažu. Korištenjem Cloud usluga riskira se gubljenje velike količine privatnih informacija. Najveći mana cloud computinga na mobilnim uređajima je upravo umanjeno osiguranje autentifikacije i zaštita privatnih podataka od neovlaštenog pristupa.[31] Mobilni uređaji su u većini slučajeva sigurnija alternativa kada se govori o kibernetičkim napadima nego što su to desktop računala. Na računalima postoji mnogo veća vjerojatnost da će korisnik instalirati zaraženu datoteku ili program na računalo, dok je mobitel u tim segmentima limitiran.

Kvaliteta mobilnih aplikacija ovisi i o razini informatičke razvijenosti okoline. Kako bi se određene turističke aplikacije koristile uspješno potrebna je analiza i obrada real time podataka iz okoline velikom brzinom kako bi se sve potrebne informacije bile pravovremeno dostupne turistu. Uz aplikacije koje se razvijaju kako bi omogućili turistima da dobiju informacije o znamenitostima primjerice skeniranjem QR kodova, pojavljuju se i one koje predstavljaju veći rizik za dobrobit turista. Veći rizik predstavlja krađa identiteta pomoću aplikacija za phishing koje se mogu ugraditi u različite turističke aplikacije te se može ukrasti identitet turista. To je posebno rizično u turizmu jer turisti obično postanu svjesni krađe tek nakon što se je već dogodila, a činjenica da se nalaze u drugoj državi čini situaciju još težom. U nekim slučajevima su turisti bili primorani platiti određeni postotak kao depozit za smještaj, koji bi im bio otkazan u zadnjim trenucima bez ikakvog objašnjenja. 2019. godine

[31] Rewind.com: Cybersecurity and cloud computing: Risks and Benefits: https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/ (pristupljeno 15.4.2023.)

je bio zabilježen slučaj malware-a Agent Smith, koji je većinom zahvatio područja Indije, Saudijske Arabije, Pakistana, Sjeverne Amerike i Australije. Ovaj malware je na mobilne uređaje širio adware te je pronalaskom ranjivosti u sustavu zamjenjivao aplikacije na mobitelu bez znanja korisnika.[32] Prevare na aplikacijama se mogu skrivati i u uvjetima i odredbama koje korisnici ne čitaju detaljno. Aplikacija se može činiti legitimna i sigurna, ali prilikom instalacije postoji mogućnost da korisnik aplikaciji daje dozvolu za primjerice skupljanje podataka, snimanje ekrana ili zvuka. Preko mobilnih uređaja se često pojavljuju i takozvane Rogue aplikacije. To su aplikacije koje izgledom i funkcijama izgledaju gotovo identično poznatim aplikacijama. Primjerice moguće je lažirati aplikacije kao što su Booking.com ili Expedia i postaviti ih na Google Play Store na besplatno preuzimanje. Ovakve aplikacije su dizajnirane sa namjerom da ukradu korisnikove podatke za prijavu i kartične podatke.



Grafikon 5: Učestalost napada na mobilne uređaje
Izvor: Obrada podataka prema "Securelist.com: IT Threat evolution in Q3 2022. Mobile Statistics (2022.)"

[32] Checkpoint.com: Agent Smith, The New Virus To Hit Mobile Phones https://blog.checkpoint.com/security/agent-smith-android-malware-mobile-phone-hack-virus-google/ (pristupljeno 15.4.2023.)

Grafikon 6: Prisutnost napada na mobilne uređaje kod ukupnog stanovništva
Izvor: Obrada podataka prema "Securelist.com: IT Threat evolution in Q3 2022. Mobile Statistics (2022.)"

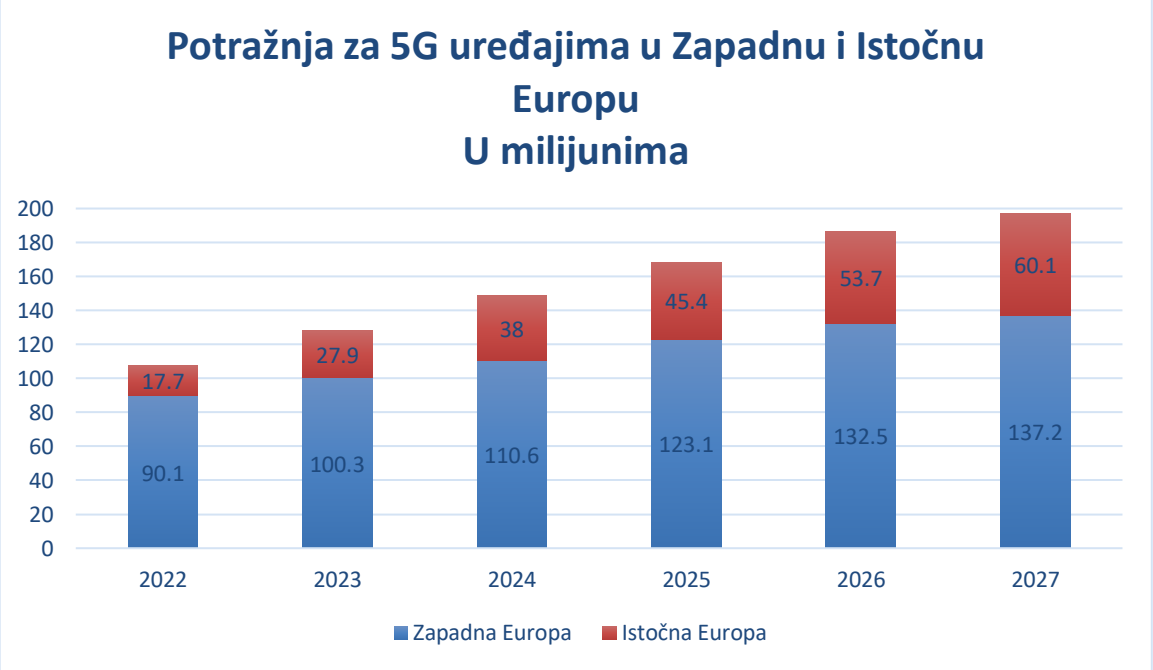
4.1. Utjecaj 5G mreža u pametnoj infrastrukturi

Uvođenje 5G mreže daljnje pomaže razvoju pametnog turizma. Služi kao nadogradnja na već postojeću 4G mrežu. Nova mreža omogućava spajanje više mobilnih uređaja na jednu mrežu, što omogućava osobama bržu internetsku konekciju i pristup podacima. Kvaliteta internetske veze od izrazite je važnosti turistima i može čak uvjetovati i njihov povratak. Istraživanje pokazuje da preko 90% turista s poslovnim motivom želi Wi-Fi u svojim sobama, dok 30% turista ne bi ponovno posjetili hotel s lošom internetskom konekcijom.[33] Od uvođenje 5G mreže nemaju koristi samo gosti. S većom brzinom interneta moguće je uvođenje digitalnih opcija koje olakšavaju poslove check-ina na daljinu, poslova domaćinstva, ugođaja, organiziranije prenošenje prtljage putnika i slično. Uvođenje 5G mreže ima brojne pozitivne utjecaje i na Internet of Things uređaje u drugim granama. Primjerice u medicini 5G mreže utječu i na jačanje digitalnih sigurnosnih sustava radi

[33] Cook, D.: How Wi-Fi Impacts Traveler Experience; https://www.linkedin.com/pulse/how-wi-fi-impacts-traveler-experience-don-cook?trk=pulse-article_more-articles_related-content-card (pristupljeno 23.4.2023.)

sofisticiranije autentifikacije i enkripcije podataka, ali omogućava i kvalitetniju izobrazbu korištenjem efektivnijih sustava virtualne stvarnosti.

Veća cijena 5G hardware-a je nedostatak ove mreže. Povećana cijena dovodi do situacije da nisu sve destinacije mogle u potpunosti implementirati sustav istovremeno. U pametnim destinacijama je od izrazite važnosti držanje koraka sa brzinom interneta. Ovo kratkoročnom pogledu nije problem od presudne važnosti, ali ako pametna destinacija duže vrijeme ne drži korak sa brzinom interneta ona će potencijalno izgubiti na konkurentnosti. Sukladno ovome, primjer neravnomjerne potražnje za 5G uređajima može se uočiti na slučaju Zapadne i Istočne Europe, u kojem se Zapadna Europa značajno izdvaja po kvaliteti razvoja informatičke infrastrukture. Dolje navedeni graf predstavlja potražnju za 5G uređajima te predviđanja do 2027. godine.



Grafikon 7: Potražnja za 5G uređajima u Zapadnoj i Istočnoj Europi
Izvor: Obrada podataka prema: „Abiresearch.com: 5G in Europe: 2022."

4.2. Opasnost Keyloggera i Supply Chain napada

Radi većeg protoka informacija veća je opasnost i od Supply Chain Napada, gdje treća osoba može ugroziti funkcioniranje uređaja spojenih na 5G. Primjerice napad može biti fizički gdje napadač ubacuje USB stick sa Keyloggerom u sustav. Keylogger je naziv za program koji, jednom kada je instaliran, registrira svaki input na tipkovnici toga računalu i sprema te

podatke na svoj hard drive koji je obično kapaciteta nekoliko gigabajta. Međutim, Keyloggeri ne postoje samo u obliku software-a, pojavljuju se i u obliku hardware-a kao mali uređaji koji služe kao konektor između tipkovnice i računala. Uređaji se spajaju se putem PS/2 porta, a to je isti priključak na koji se priključuju tipkovnica i miš. Radi njegove veličine može se lako sakriti od korisnika. Prijetnja koju predstavljaju keyloggeri je upravo neznanje korisnika da se njegovi inputi prate. Keyloggeri mogu biti već ugrađeni u tipkovnicu bez ičijeg znanja. Kako bi se pristupilo podacima hardware keyloggera, uređaj se mora ukloniti iz tipkovnice. Kod software programa input korisnika na tipkovnici se prenosi izravno putem software-a. Keyloggeri su također velika prijetnja za smartphone uređaje, a služe kao sredstvo za spyware napada kojima je najčešći cilj krađa PII (Personally Identifiable Information) informacija, podataka za autentifikaciju u određene programe ili kao krađa podataka poduzeća. Korištenje Keyloggera može imati i pozitivnu stranu. Primjerice može se koristiti i kao sredstvo zaštite od kibernetičkog napada jer korisnici preko programa mogu pratiti neovlaštene aktivnosti njihovih mobilnih uređaja. Isto tako može pomoći i kod nadziranja zaposlenika u poduzeću. Danas postoje više vrste Keyloggera s različitim načinima registriranja inputa, tako da niti jedan individualni sigurnosni sustav neće pružiti stopostotnu zaštitu od ovoga. Antivirusni programi u nekim slučajevima znaju Keylogger software prepoznati kao bezopasan program pa je stoga potrebno korištenje više programa za sigurnost. Primjerice korištenje Anti-Keylogger software-a i antivirusnog programa. Upotreba Firewalla također pomaže pri identificiranju Keylogger programa na računalu. Firewall je također dobra opcija zaštitu od Keyloggera radi mogućnosti prepoznavanja i sprječavanja konstantnog prijenosa podataka.[34]

[34] Crowdstrike.com: Keyloggers: How They Work and How to Detect Them: https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/ (pristupljeno 29.4.2023.)

5. MJERE ZAŠTITE OD KIBERNITIČKIH NAPADA

Zaštita od računalnih prijetnji može se definirati kao skup mehanizama koji se temelje na pokušaju smanjenja rizika neovlaštenog pristupa ili neovlaštene upotrebe podataka i informacija pohranjenih u bazi podataka. To se također odnosi i na zaštitu fizičkih Internet of Things uređaja kako bi se spriječilo moguće preuzimanje kontrole nad njima. Firewall je od izrazite važnosti kada se govori o kontroliranju i uvidu u internetskim aktivnostima koje bi mogle biti prijetnja.. Iako Firewall može poslužiti kao dodatno mjerilo zaštite, mnogi napadači će pronaći način kako da ga zaobiđu pa je potrebno uvođenje većeg broja sofisticiranijih sigurnosnih sustava kako bi se korisnici i destinacije mogle boriti sa modernim kibernetičkim napadima. Kriptiranjem podataka na VR uređajima oni postaju nečitljivi napadačima te se samim time smanjuje razina prijetnje. Velika pažnja se treba također pridodati sigurnosti autentifikacije na uređaje. Potrebno je uvesti „2-factor authentication“ procese u kojima se od korisnika traži više od samo jedne potvrde za pristup podacima. Primjerice korisnik za određene podatke ima postavljenu lozinku, no kako bi se spriječilo neovlašteno korištenje podataka i potvrda identiteta korisnika koriste se dodatne mjere autentifikacije korisnika. To mogu biti postavljanje dodatnih pitanja, potvrda iz osobnih dokumenata ili slanje određenog koda na mobilni telefon uređaja, koji se tada identificira po broju telefona. Redovito ažuriranje sigurnosnih i operacijskih sustava od izrazite je važnosti za održavanje osobne sigurnosti na internetu. Zanemarivanje ažuriranja uređaja na dulje vrijeme može imati ozbiljne posljedice. Tijekom ažuriranja sustavi instaliraju određene „zakrpe“ ili „patches“. Zakrpe predstavljaju sigurnosna rješenja za određene internetske probleme koji su aktualni. Ako se sustav na ažurira duže vrijeme on postaje podložan tim problemima i moguća meta za jednostavnije izvršavanje kibernetičkog napada. Tijekom samog razvoja aplikacije ili uređaja potrebno je pridonijeti pažnje security testing metodama. To su metode kojima se pokušava pristupiti podacima u svrhu uočavanja slabijih sigurnosnih dijelova u sustavu te sprječavanja takvih situacija kada uređaj ili sustav izađu na tržište. Ove sigurnosne mjere je teško izvesti sa potpunom sigurnošću radi ubrzanog razvoja tehnologije i radi toga što su sustavi najranjiviji prvih nekoliko dana od puštanja na tržište. Potrebna je konstantna i pravovremena informiranost o trendovima u svijetu tehnologije kako bi se moguće prijetnje mogle prepoznati i spriječiti prije nego što postanu

ozbiljniji problem sa posljedicama koje mogu rasti eksponencijalno. Neispravno rukovanje radnika sa operacijskim sustavom ili neprovjereno povjerivanje podataka nepouzdanim izvorima može izazvati visoke prijetnje čak iako je sigurnosni sustav dobro razvijen. Turizam je radno intenzivna gospodarska grana i ljudski faktor i pogreške bi se uvijek trebale uzimati u obzir te nikada neće prestati postojati, ali je potrebno minimalizirati rizik od pojavljivanje takve neželjene situacije.

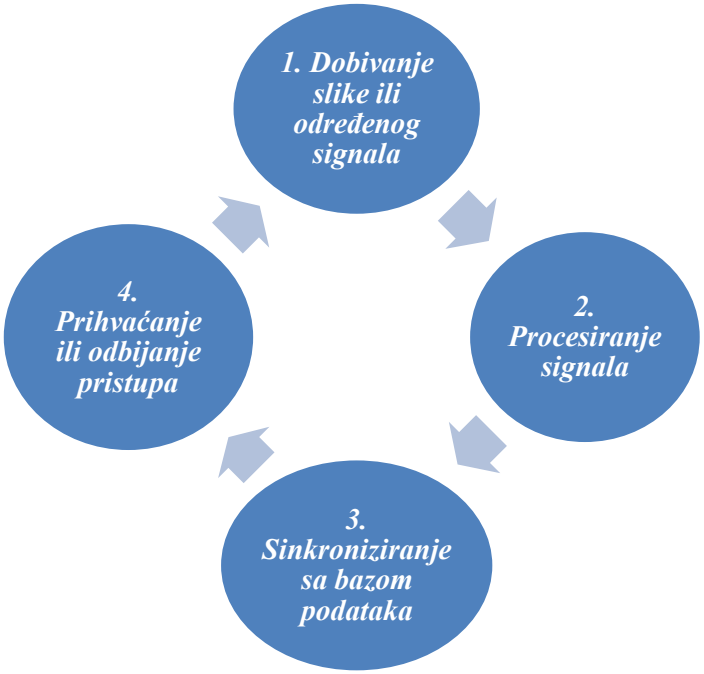
Prije implementacije bilo kojih sigurnosnih mjera, pametne turističke destinacije bi trebale provesti opću procjenu rizik akako bi identificirale sve moguće ranjivosti i prijetnje. Potrebno je sustavno procjenjivanje informatičke infrastrukture destinacije, uključujući pri tome sigurnost mreže, sigurnost velike količine podataka koje se prikupljaju i aplikacije koje su povezane sa uslugama u destinaciji. Kontinuirano praćenje informatičkih sustava omogućuje pametnim destnacijama da na vrijeme reagiraju na potencijalne kibernetičke napade i tako smanje nastanak većih štetnih posljedica. Sukladno tome, destinacije bi trebale imati Incident Response Plan ili Plan odgovora na kibernetički napad. Cilj ovog plana je u kratko vremenu izolirati segment destinacije ili objekta koji je napadnut i na što brži način ga vratiti u pravilno funkcioniranje. Implementacija ovakvog programa spriječava širenje napada na ostale sektore i smanjuje sveukupnu štetu. Organizirana izobrazba dionika u pametnoj turističkoj destinaciji je od iznimne važnosti. Ne samo zaposlenika, već i turista. Turisti su u stranim državama najranjiviji radi nepoznavanja jezika i većih mogućnosti prijevara na internetu. Pravovremenom izobrazbom smanjio bi se rizik ljudske greške, a samim time i učestalost napada. Sustavi za Backup ili očuvanje podataka su od iznimne važnosti. Oni spriječavaju trajni gubitak podataka radi koji mogu nastati organizacijske i poslovne nepogode u hotelu te može izazvati pad kvalitete pružanja usluga. U većini slučajeva se koriste sustavi koji pohranjuju informacije na lokaciju koja je izvan mjesta operiranja objekta ili destinacije, tako da nije zahvaćena napadom. Također se koriste visoko razvijenim cloud sustavima. Enkripcija ili šifriranje podataka je još jedan način za zaštitu od neželjenih napada na sustav. Ova sigurnosna mjera se bazira na pretvaranju podataka u kod koji sprječava neautorizirani pristup. Kada se govori o sigurnosti turista kao pojedinca potrebno je pružiti mogućnost korištenja osobnih sigurnosnih uređaja. Postoje uređaji koji su spojeni na GPS i prate lokacije određenih turista kako bi se znala njihova lokacija ako se

dogodi hitan slučaj. Isto tako uvode se i „Panic Button“ uređaji koji automatski signaliziraju policiju ili hitnu pomoć.[35]

5.1. Biometrijske sigurnosne tehnike

Potrebno je napomenuti i važnosti biometrijske zaštite u pametnim turističkim destinacijama. Biometrijska zaštita izrazito je važna za zaštitu pametnog prijevoznog sustava pametne destinacije. Primjena biometrijske tehnologije u transportnom sustavu ima za cilj stvaranje neometanog iskustva putovanja, u kojem zračne luke, prijevozna čvorišta i agencije za kontrolu granica zajednički sudjeluju u inovacijama i olakšavanju putnog procesa te povećanju efikasnosti sigurnosnih praksi koje se temelje na procjeni rizika. Biometrijske tehnike sigurnosti spadaju pod pametne sustave nadziranja turista kojima je glavni cilj vođenje kontrole o turističkim aktivnostima i spriječiti kriminalne aktivnosti. Prepoznavanje lica je vrsta biometrijske zaštite kojom se autentificiraju putnici na check-inu, mjestima pojačanog osiguranja i na mjestima ulaska na zračnim lukama. Prepoznavanja glasa se može koristiti kao glasovna naredba za korištenje pojedinih pametnih uređaja s tom opcijom, ali se primjenjuje zajedno sa ostalim biometrijskim tehnikama za bolju autentifikaciju putnika. Biometric eGates ili prolazi sa pojačanom biometrijskom sigurnosti koriste više biometrijskih sigurnosnih tehnika za prepoznavanje putnika, primjerice otisak prsta, prepoznavanje lica i skeniranje šarenice ili mrežnice oka. U zadnjih nekoliko godina pojavile su se i mobilne biometrijske tehnike. One se odnose na korištenje mobitela i ostalih pametnih uređaja. Biometrijski autentifikatori su ugrađeni u mobilne uređaje kako bi se ostvario sigurniji pristup. Radi bržeg prepoznavanja identiteta putnika uvedene su i pametne putovnice. To su putovnice koje su čipirane i sadrže sve potrebne podatke o putniku. Bihevioralne biometrijske tehnike se koriste kod prepoznavanja specifičnih pokreta osoba koje mogu koristiti radi njihovog lakšeg prepoznavanja ili pristup personaliziranim podacima. [36]

[35] Ma, C.: Smart City and cyber security; technologies used, leading challenges and future recommendations; Energy Reports, Vol. 7, 2021.
[36] Neo, H., Teo, C.: Biometrics in Tourism: Issues and Challanges; Handbook of e-Tourism, 2021.



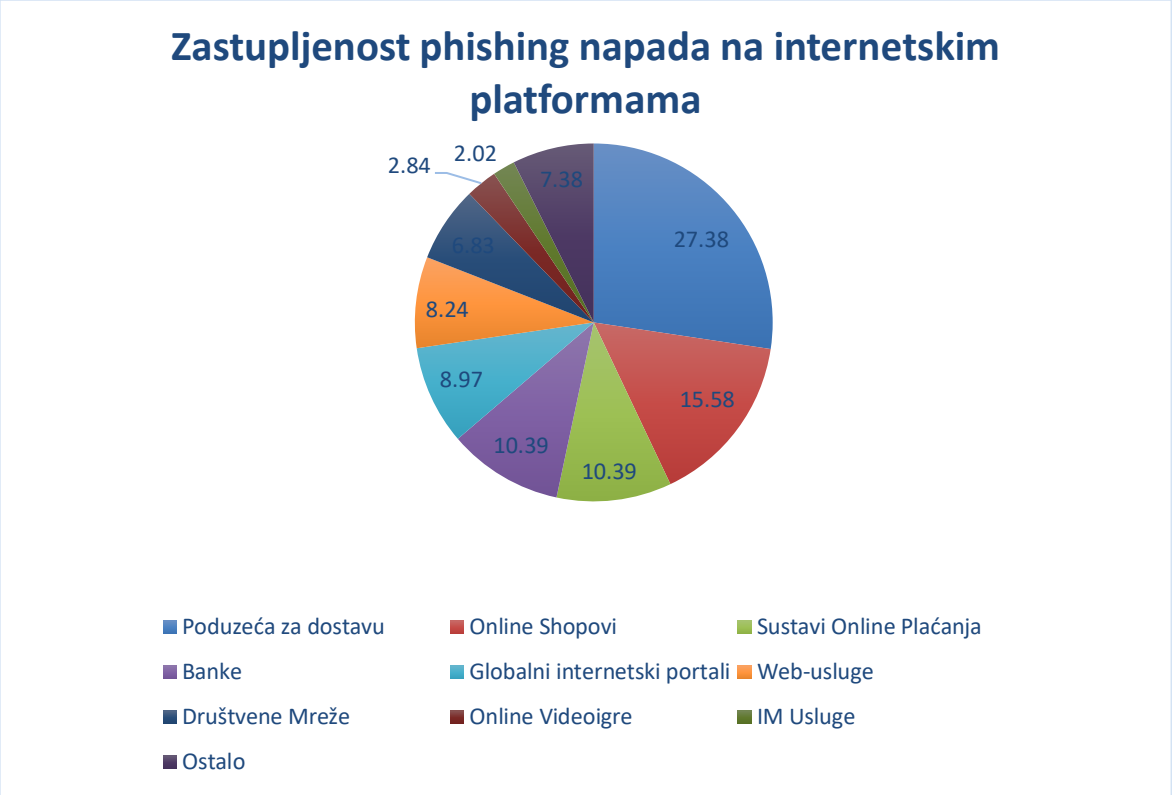
Slika 3: Biometrijska sigurnost
Izvor: M. Boban, M. Perišić: Biometrija u sustavu sigurnosti, zaštite i nadzora informacijskih sustava; str. 125.-126.; 2015.

5.2. Zero Trust Model

Zero Trust Model predstavlja sigurnosni model koji funkcionira pod pretpostavkom da se niti jednom korisniku ili uređaju vjeruje po defaultu. U pametnoj turističkoj destinaciji to znači da se svi dionici i njihovi uređaji smatraju rizičnima dok ne prođu za to prigodnu autentifikaciju i autorizaciju za ulazak u mrežu. Ključni dio Zero Trust Modela je korištenje takozvane mikrosegmentacije, to jest podjela mreže na manje dijelove od koje svaka zahtjeva poseban način pristupa i dostupna je određenim korisnicima. Ovaj model sigurnosnog sustava sadrži slojevite sigurnosne tehnike kao primjerice enkripciju podataka, multi-faktor autentifikaciju, kontinuirano praćenje... Vezano za to, u pametnim destinacijama pojavljuje se sigurnosna strategija podnazivom Defense-In-Depth model. To je strategija koja se zasniva na implementaciji višestrukog osiguranja od kibernetičkih napada kombiniranjem različitih sigurnosnih tehnika. Koristi se za osiguranje informatičke insfrastrukture od neautoriziranog pristupa kao primjerice osigurava pametne kamere, robote te smart lock sisteme u hotelima. Pruža zaštitu internetskim sustavima povezanim sa turističkom destinacijom uvođenjem firewalla, antivirusnih programa, intrusion detection

sistema i slično kao i za zaštitu od neautoriziranog provaljivanja u aplikacije vezane za usluge pametne destinacije. Enkripcijom podataka štiti ulazak u baze podataka, a višestrukim provjeravanjem, provjeravanjem pozadine korisnika i provođenjem adekvatnog treninga se osigurava korektno rukovanje zaposlenika sa sigurnosnim sustavima. Turizam je grana u kojoj dolazi do izrazite važnosti podizanje kvalitete sigurnosnih sustava turista i poduzeća radi toga jer poduzeća raspolažu informacijama turista. Stoga nekvalitetan sigurnosni sustav poduzeća ima višestruke posljedice. Isto tako potrebno je razvijati sigurnosne mjere za različite pametne i poslovne sustave jer sigurnosni propusti kod jednog sektora se mogu proširiti i na druge. Prema podacima iz antivirusnog software-a Kaspersky, 2022. godine 62% napada su bili usmjereni na potrošače, dok su 38% bili usmjereni na poduzeća. Najčešća vrsta napada su phishing napadi radi velike rasprostranjenosti mnogih vrsta internetskih platformi gdje se napadači mogu jednostavno povezati sa korisnicima. Dolje priloženi graf predstavlja prisutnost kibernetičkih napada po internetskim platformama.[37]

[37] Iiot.com: Use a Zero Trust Approach to Protect Your Smart Cities from Hackers: https://www.iiot-world.com/ics-security/cybersecurity/use-a-zero-trust-approach-to-protect-your-smart-cities-projects-from-hackers/ (pristupljeno 29.4.2023.)



Grafikon 8: Zastupljenost phishing napada na internetskim platformama
Izvor: Obrada podataka prema "Kaspersky.com: The number of phishing attacks doubled to reach over 500 million in 2022."

5.3. Defense-in-Depth

Defense-in-Depth model je sveobuhvatni sigurnosni model koji uključuje implementaciju višestrukih slojeva zaštite u pametnoj turističkoj destinaciji. Cilj ovog sigurnosnog modela je preklapanje većeg broje sigurnosnih slojeva kako bi se smanjio rizik od potencijalnih sigurnosnih prijetnji ili incidenata. Radi konstantnog razvijanja kompleksnosti kibernetičkih napada, prepoznato je da oslanjanje na pojedinačnu sigurnosnu mjeru nije dovoljno. Kombiniranjem više slojeva sigurnosti, ovaj model ima za cilj stvoriti snažniju i otporniju sigurnosnu strategiju. Sigurnosni slojevi u ovome modelu su podijeljeni na segmente nad kojima vrše sigurnosnuu zaštitu. Sloj za prostornu sigurnost usredotočuje se na osiguranje turističkog prostora u destinaciji. Uključuje sustave za kontrolu pristupa, nadzorne kamere i sustave za otkrivanje provale kako bi se spriječio neovlašteni pristup. Prostorne sigurnosne mjere pomažu u kontroliranju ulaza u turistički prostor i stvaraju granice između javnih i

ograničenih područja. Sigurnosni sloj mreže uključuje zaštitu mrežne infrastrukture pametne turističke destinacije, što uključuje žičane i bežične mreže, rutere, prekidače i vatrozide. Mjere sigurnosti mreže pomažu u kontroli mrežnog prometa, praćenju sumnjivih aktivnosti i spriječavanju neovlaštenog pristupa. Sigurnosni sloj zaštite sustava i aplikacija usredotočuje se na osiguravanje pojedinačnih sustava i aplikacija unutar pametnog turističkog odredišta. Uključuje implementaciju mjera poput snažnih kontrolnih pristupa, redovitih zakrpi i ažuriranja, antivirusnih sustava i testiranja sigurnosti aplikacija. Sigurnosni sloj podataka usredotočuje se na zaštitu osjetljivih podataka. To može uključivati tehnike kriptiranja podataka, mehanizme za spriječavanje gubitka podataka, kontrole pristupa i sigurnosne kopije podataka. Mjere sigurnosti podataka osiguravaju zaštitu podataka kako u mirovanju tako i prilikom prijenosa, smanjujući utjecaj povrede podataka ili neovlaštenog pristupa. Pod posljednjim slojem se prepoznaje važnost obuke i svijesti korisnika. Pravilna obuka zaposlenika može biti značajan faktor u sigurnosnim ranjivostima. Programi svijesti i obuke korisnika pomažu educirati zaposlenike, osoblje i posjetitelje o najboljim praksama sigurnosti, prijetnjama socijalnog injženjeringa i načinima reagiranja na potencijalne incidente. Promicanjem kulture svjesnosti o sigurnosti, ovaj sloj jača cjelokupnu sigurnosnu strategiju.[38]

5.4. Risk Based Security

Risk Based Security ili model sigurnosti temeljen na riziku u pametnim turističkim destinacijama usredotočuje se na procjenu, prioritizaciju i upravljanje sigurnosnim rizicima kako bi se zaštitili resursi, infrastruktura i posjetitelji destinacije. Ovaj model uključuje sustavan pristup za identifikaciju, analizu i umanjivanje rizika temeljenih na njihovom potencijelnom utjecaju i vjerojatnosti. Razumijevanjem i rješavanjem najznačajnijih rizika, pametna turistička destinacija može učinkovito rasporediti resurse i implementirati ciljane sigurnosne mjere. Procjenom rizika uključuje identifikaciju i procjenu potencijalnih sigurnosnih rizika s kojima se pametna turistička destinacija može suočiti. U to spada provođenje sveobuhvatne analize resursa odredišta, sustava, procesa i ranjivosti. Rizici mogu proizaći iz različitih izvora kao što su fizičke prijetnje, kibernetički napadi, prirode

[38] Fortinet.com: What Is Defense-In-Depth?; https://www.fortinet.com/resources/cyberglossary/defense-in-depth (pristupljeno 1.7.2023.)

katastrofe ili operativne slabosti. Nakon što su rizici identificirani, oni se prioritiziraju na temelju njihovog potencijalnog utjecaja i vjerojatnosti. Ovaj korak podrazumijeva dodjeljivanje razine rizika svakom identificiranom riziku. Proces prioritizacije uzima u obzir faktore kao što su vrijednosti ugroženih resursa, potencijalne posljedice incidenta i vjerojatnost njihovog nastanka. Prioritiziranjem resursa pametne turistička destinacija može usmjeriti resurse na umanjivanje najkritičnijih i najrizičnijih područja. Nakon prioritizacije rizika, pametna destinacija razvija i implementira određene strategije umanjivanja rizika. Strategije umanjivanja rizika mogu uključivati fizičke sigurnosne mjere, kibernetičke kontrole, planove za hitne situacije, obuku osoblja i programe podizanja svijesti. U Risk Based Security modelu naglašena je i funkcija kontinuiranog praćenja i pregleda implementiranih sigurnosnih mjera. Kontinuirano praćenje pomaže u identifikaciji novih rizika, pricjeni učinkovitosti postojećih mjera i potrebnim prilagodbama sigurnosne strategije prema potrebi. Ključna je i komunikacija i uključivanje ključnih dionika u turističkoj destinaciji. Redovita i učinkovita komunikacija osigurava da svi razumiju svoje uloge i odgovornosti u održavanju sigurnosti te potiče suradnički pristup upravljanja rizicima.[39]

5.5. Compliance Framework

Compliance Framework ili model u skladu sa postavljenim okvirima usredotočuje se na poštivanje primjenjivih propisa, standarda i najboljih praksi kako bi se osigurala sigurnost, privatnost i integritet sustava i podataka unutar pametnih destinacija. Postavljeni okviri sigurnosti predstavljaju smjernice i zahtjeve za određena sigurnosna područja te pomažu u postavljanju osnovnih sigurnosnih kontrola i praksi. Pametne turističke destinacije moraju se pridržavati različitih zakona i propisa koji se odnose na zaštitu podataka, privatnost i sigurnost. Industrijski standardi pružaju pružaju smjernice i najbolje prakse za sigurnost i privatnost u određenim sektorima. Neki od propisa koji se odnose na zaštitu podataka na internetu su Opća uredba o zaštiti podataka (GDPR) i Standard sigurnosti podataka kod kartičnog plaćanja. Na primjer ISO standardi poput standarda ISO 27001 za upravljanje

[39] Calvo, M., Beltran, M.: A Model For risk-Bases adaptive security controls; Computers and Security, Vol. 115; 2022.

informacijskom sigurnošću, nude sveobuhvatne okvire za implementaciju sigurnosnih kontrola i upravljanje rizicima. Pridržavanjem ISO standarda pametne turistička destinacije pokazuju predanost ka pružanju adekvatne sigurnosti i smanjivanju rizika kod modernih kibernetičkih napada. Ovaj model mora definirati osnovne razine sigurnosti ili skupove kontrola koji opisuju minimalni skupp sigurnosnih kontrola i zahtjeva. Ove osnovne razine pomažu u uspostavi temelja za sigurnost unutar pametne destinacije. Obično obuhvaćaju područja poput kontrole pristupa, sigurnostni mreže, odgovora na incidente, upravljanje ranjivostima i osviještenosti o sigurnosti. Potrebno je i redovito provođenja revizija sigurnosti i procjene kako bi se ocjenila usklađenost pametnog odredišta s definiranim zahtjevima. Neovisni revizori ili interni sigurnosni timovi toga odredišta procjenjuju provedebu sigurnosnih kontrola, pregledavaju politike i postupke te identificiraju eventualne nedostatke ili slabosti. Pravilno identificiranje sigurnosnih nedostataka putem revizije pomaže pri identificiranju područja za poboljšanje i osiguravanje kontinuirane usklađenosti sigurnosnog sustava. Od velike je važnosti kontinuiranost kod praćenja i nastrojenost ka stalnom poboljšanju. Stoga je za pametne destinacije od izrazite važnosti uspostavljanje mehanizama za praćenje sigurnosnih kontrola, otkrivanje odstupanja od zahtjeva i na temelju toga provedbu ispravnih strategija.[40]

5.6. Security by Design

Security by Design ili model sigurnosti temeljen na dizajnu naglašava integraciju sigurnosnih razmatranja kroz cijeli životni ciklus razvoja i implementacije pametnih turističkih destinacija. Uključuje uvođenje sigurnosnih načela, najboljih praksi i kontrola od samog početka dizajna, umjesto naknadnog dodavanja sigurnosti. Cilj ovog sigurnosnog modela je izgradnja sigurnog i otpornog okruženja za infrastrukturu, sustave i aplikacije odredišta. Pristup sigurnosti temeljen na dizajnu započinje modeliranjem prijetnji, pri čemu se identificiraju i analiziraju potencijalne prijetnje, ranjivosti i rizici. To uključuje razmatranje različitih vrsta napada s kojima se pametna destinacija može susresti. Razuijevanjem potencijalnih prijetnji dizajneri mogu proaktivno implemenirati

[40] Comptia.org: What is Cybersecurity Compliance?: https://www.comptia.org/content/articles/what-is-cybersecurity-compliance (pristupljeno 1.7.2023.)

odgovarajuće sigurnosne mjere radi umanjivanja tih rizika. Model se usredotočuje na dizajniranje sigurne arhitekture i infrastrukture pametnog turističkog odredišta. To podrazumijeva definiranje sigurnosnih zahtjeva, implementaciju segmentacije mreže i dizajniranje otpornih sustava koji mogu izdržati napade i kvarove. Razvoj sigurnosti potrebnih softvera je također jedan od zadataka ovog modela. Promiče se uključivanje sigurnosti u životni ciklus softvera koji se koristi u pametnoj turističkoj destinaciji. Radi toga se poduzimaju sigurne prakse kriptiranja, redovite preglede koda i testiranje sigurnosti radi identifikacije i rješavanja ranjivosti. Razvojni timovi slijede smjerniceza sigurno kodiranje i integriraju sigurnosne kontrole, poput provjere valjanosti unosa, sigurne autentifikacije i upravljanja sigurnim sesijama, u proces razvoja aplikacija. Ističu se snažni mehanizmi kontrole pristupa i mjere autentifikacije kako bi se osiguralo da samo ovlaštene osobe imaju pristup sustavima i resursima odredišta. U to spada implementacija snažnih metoda autentifikacije poput višestupanjske autentifikacije te upravljanje pristupom temeljeno na ulogama radi provedbe načela najmanjih privilegija. Potiče se kontinuirano testiranje valjanosti. Sigurnost temeljena na dizajnu uključuje redovito testiranje sigurnosti i provjeru valjanosti kako bi se osiguralo da implementirane sigurnosne mjere budu učinkovite. To uključuje provođenje procjene ranjivosti, testiranje probijanja i sigurnosnih revizija radi bilo kakvih slabosti i ranjivosti.[41]

[41] Carter, B., Adams, S., Bakirtzis, G., Sherbourne T., Beling, P., Horowitz, B., Fleming C.: A Preliminary Design-Phase Security Methodology for Cyber-Physical Systems; Systems Vol. 7, No. 2.; 2019.

Zaključak

Na temelju iznesenih podataka o vrstama kibernetičkih napada i njihovim utjecajima na pametne turističke destinacije može se zaključiti da su kibernetički napadi danas sve češći i opasniji u pametnom turizmu. U planovima i strategijama razvoja pametnih turističkih destinacija posebna pažnja bi se trebala obratiti na uvođenje suvremenih i ispitanih sigurnosnih sustava kako bi se minimizirao rizik od štetnih posljedica. Razlog tome je što uvođenje pametne tehnologije u pametne turističke destinacije povećava mogućnost za kibernetički napada te su isto tako veće i posljedice radi mogućnosti krađe većeg broja podataka. Suvremenim inovacijama i novim uvođenjem digitalnih sustava u pametne turističke destinacije pojavljuju se nove vrste štetnih posljedica koje napadi mogu izazvati. Vrsta malware-a koja je odgovorna za najveće novčane gubitke je svakako Ransomware. Jednom greškom korisnik ili poduzeće se može naći u neočekivanoj situaciji koja izaziva velike novčane uplate kako bi se informacije vratile u prvobitno stanje. Sve većom popularizacijom mobilnih ransomware softvera raste i opasnost za turiste u destinaciji. Pametni hoteli bi u ovome slučaju svakako trebali osigurati najsuvremenije sigurnosne sustave u svoju informatičku tehnologiju te obavezno izvršavati što kvalitetnije informiranje i treniranje radnika, ali i turista o načinima izbjegavanja suvremenih kibernetičkih napada.
Primjerice uvođenje virtualne realnosti može izazvati do sada neviđene fizičke posljedice za korisnika koje do sada nisu bile toliko česte. Stoga je potrebno analizirati nove sustave koje se uvode u pametne destinacije i raznim testiranjima ukloniti sve potencijalne ranjivosti u njihovom sustavu, naročito ako se radi o novim tehnologijama. Potrebno je staviti naglasak i na korištenje pametne tehnologije u svrhu kvalitetnog provođenja strategije održivog razvoja u pametnoj destinaciji. Turisti nakon pandemije preferiraju pametne destinacije koje naglasak stavljaju na očuvanju prirodnog prostora i održavanju postojeće turističke infrastrukture. Unatoč mogućnosti kibernetičkog napada na sustave održivog razvoja kao primjerice spomenutog sustava za reguliranje potrošnje energije, pametni gradovi raspolažu sa potrebnom digitalnom opremom da podignu kvalitetu održivog razvoja na novu razinu, a samim time i sigurniji razvoj u budućnosti.
Internet stvari predstavlja dodatnu prijetnju za sigurnosti uređaja u pametnim destinacijama. Unatoč tome što znatno poboljšava pružanje usluga i odvijanje poslovnih procesa unutar

destinacije i hotelskih objekata pouzdani sigurnosni sustavi za ovakve uređaje još nisu u potpunosti razvijeni radi nedovoljne standardizacije i nemogućnosti provjere autentičnosti materijala od kojih su ti sustavi izgrađeni. Uvođenjem interneta stvari u svakodnevno poslovanje pametnog hotela ili destinacije potrebno je uvesti kvalitetan cloud sustav te omogućiti decentralizaciju podataka na segmentirane sigurnosne dijelove kako napad na jedan dio podataka ne bi uzrokovao gubitak ostalih. Od pojave pametnih hotela mnogo se destinacija okrenulo robotizaciji turističke usluge. Ovakav oblik pružanja usluge nudi određene pogodnosti, ali bi se trebalo paziti u kojim mjerama se uvodi. Prekomjerno uvođenje robotske radne snage u hotelske sustave može izazvati nezadovoljstvo gosta radi nedostatka ljudskog elementa u pružanju usluge. Potrebno je paziti i na pozicioniranje robota u pametnom hotel, ali isto tako i u destinaciji jer služe kao jednostavan način napadaču za izvođenje spyware napada kojima se laku mogu pratiti lokacija i privatni podaci gosta. Današnja sveprisutnost mobilnih uređaja pojednostavljuje pružanje usluga u pametnoj turističkoj destinaciji. Moguće se integrirati na digitalne platforme destinacije i na jednostavniji i brži način pronaći informacije koje su potrebne. Sve veća dostupnost 5G mreže uvelike pomaže korisnicima mobilnih uređaja, ali isto tako i kvalitetnijem i čvršćem funkcioniranju pametne turističke infrastrukture određene destinacije radi bržeg prenošenja podataka. U današnje vrijeme svaka bi pametna destinacija trebala prioritizirati implementaciju sigurnosnih modela kako bi se osigurao opstanak destinacije na tržištu, smanjio rizik od stagnacije poslovanja i krađe osobnih podataka turista, mogućnost daljnjeg razvoja te dobrobiti zaposlenih u destinaciji.

Bibliografija

Azrour, M., Mabrouki, J., Guezzaz, A., Kanwal, A., ; Internet of Things Security: Challenges and Key Issues; Security and Communication Networks 2021.

Calvo, M., Beltran, M.: A Model For risk-Bases adaptive security controls; Computers and Security, Vol. 115; 2022.

Carter, B., Adams, S., Bakirtzis, G., Sherbourne T., Beling, P., Horowitz, B., Fleming C.: A Preliminary Design-Phase Security Methodology for Cyber-Physical Systems; Systems Vol. 7, No. 2.; 2019.

Demertzi V., Demertzis S., Demertzis K.: An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities; Applied Sciences, Vol.13, No.2: 2022

Buhalis, D., Amaranggana, A.; Smart tourism destinations enchancing tourism experience through personalisation of services; 377-389, (2015.)

Florencio-Palacios B. Roldan-Santos L., Pineda-Berbel Manuel J., ,Canalejo-Castillo A.: Sustainable Tourism as a Driving force of the Tourism Industry in a Post-Covid-19 Scenario; Social Indicators Research 158; 2021.

Gretzel, U., Sigala, M., Xiang, Z., Koo, C.; Smart Tourism: foundations and developments; Electronic Markets, 25, 179-188, 2015.

Ijaz, S., Shah, A., Khan A., Mansoor, A.,: Smart Cities: Asurvey on Security Concerns; International Journal of Advanced Computer Science and Applications(IJACSA), Vol. 7, No. 2; 2016.

Liu, P., Liu, Y.: Smart Tourism via Smart Phone: Proceedings of the 2016 International Conference of Communications, Information Management and Network Security, 2016.

Lopez Cappa, R.: The Sustainable Development Plan of El Hierro and its Impact on the Tourism Industry: 2018.

Javeed D.: Man iin the Middle Attacks: Analysis, Motivation and Prevention; International Journal of Computer Networks and Communication Security, Vol.8, No.7; (2020.)

Neo, H., Teo, C.: Biometrics in Tourism: Issues and Challanges; Handbook of e-Tourism, 2021.

Ma, C.: Smart City and cyber security; technologies used, leading challenges and future recommendations; Energy Reports, Vol 7, 2021.

Oladimeji D., Gupta K., Kose Alperen, N., Gundogan K.: Smart Transportation: An Overview of Technologies and Applications; Sensors Vol.23, No.8; 2023.

Osawa, H., Arisa, E., Hattori, H.,: Analysis of robot hotel: Reconstruction of works with robots; 26th IEEE International Symposium on Robot and Human Interactive Communication (2017.)

Samala, N., Katkam B., Shekhar R., Rodriguez R.: Impact of AI and robotics in the tourism sector: a critical insight; Journal of Tourism Futures, Vol 8; Issue 1; 2022.

Wise, N., Heidari H.; Developing Smart Tourism Destinations with the Internet of Things: Managerial Approaches, Techniques, and Applications; Big Data and Innovation in Tourism, Travel and Hospitality (2019.)

Xiang, Z., Fesenmaier, D. R.; Smart Tourism Destinations; str. 299.-300. 1-13; Švicarska; 2017.

Web Izvori

Analyticsinsight.net; IoT Standardization: Why IoT has not set standards yet?, (2021.) (pristupljeno 14.4.2023.)

AntivirusGuide: Ransomware Statistics: https://www.antivirusguide.com/cybersecurity/ransomware-statistics/?gclid=CjwKCAjwuqiiBhBtEiwATgvixCbUk1QwOxx_ZIY8sX227TrEYhmzF_Q57NMAp7goftqtYLwNF1Jf1RoC8DYQAvD_BwE (pristupljeno 30.4.2023.)

Booking.com; Sustainable Travel Report 2022.: https://www.ukinbound.org/wp-content/uploads/2023/01/Booking.com-Sustainable-Tourism-Report-2022.pdf (pristupljeno 15.6.2023.)

Checkpoint.com: Agent Smith, The New Virus To Hit Mobile Phones https://blog.checkpoint.com/security/agent-smith-android-malware-mobile-phone-hack-virus-google/ (15.4.2023.)

Cook, D.: How Wi-Fi Impacts Traveler Experience: https://www.linkedin.com/pulse/how-wi-fi-impacts-traveler-experience-don-cook?trk=pulse-article_more-articles_related-content-card (23.4.2023.)

Comptia.org: What is Cybersecurity Compliance?: https://www.comptia.org/content/articles/what-is-cybersecurity-compliance (pristupljeno 1.7.2023.)

Crowdstrike.com: Keyloggers: How They Work and How to Detect Them: https://www.crowdstrike.com/cybersecurity-101/attack-types/keylogger/ (pristupljeno 29.4.2023.)

Doctorow, C.: Japanese robot hotel chain ignored repeated warnings that its in-room „bed-facing“ robots could be turned nto spy devices - https://boingboing.net/2019/10/23/sorry-for-uneasiness.html (pristupljeno 13.4.2023.)

Eenewseurope.com: IoT's Smart Lock bricked by software update - https://www.eenewseurope.com/en/iot-smart-lock-bricked-by-software-update/ (pristupljeno 30.5.2023.)

Fortinet.com: What Is Defense-In-Depth?; https://www.fortinet.com/resources/cyberglossary/defense-in-depth (pristupljeno 1.7.2023.)

Harvard.edu: The Rise of Virtual Reality Tourism (pristupljeno 25.4.2023.)

Herrtzfeld, E.: Japan's Henn na Hotel fires half its robots workforce - https://www.hotelmanagement.net/tech/japan-s-henn-na-hotel-fires-half-its-robot-workforce (pristupljeno 10.4.2023.)

Hertzfeld, E.: How IoT can help with energy management; https://www.hotelmanagement.net/tech/how-iot-can-help-energy-management (pristupljeno 10.4.2023.)

Rutgers.edu: Security Vulnerabilites in Virtual Reality Headsets: https://www.rutgers.edu/news/rutgers-researchers-discover-security-vulnerabilities-virtual-reality-headsets (pristupljeno 27.4.2023.)

Haiston, J.: What is a Smart Traffic Management System? : https://www.symmetryelectronics.com/blog/what-is-a-smart-traffic-management-system/ (pristupljeno 15.4.2023.)

Iiot.com: Use a Zero Trust Approack to Protect Your Smart Cities from Hackers; https://www.iiot-world.com/ics-security/cybersecurity/use-a-zero-trust-approach-to-protect-your-smart-cities-projects-from-hackers/ (pristupljeno 29.4.2023.)

Kaspersky.com; What is a Botnet?: https://usa.kaspersky.com/resource-center/threats/botnet-attacks (pristupljeno 25.4.2023.)

MiamiHerald.com: Key West City Hall computers have been shut down for a week: https://www.miamiherald.com/news/local/community/florida-keys/article245467410.html (pristupljeno 30.4.2023.)

Reinstein, D.: Hotel Sky Sandton introduces robot staff - https://www.travelweekly.com/Middle-East-Africa-Travel/Hotel-Sky-Sandton-introduces-robot-staff (pristupljeno 30.4.2023.)

Rewind.com: Cybersecurity and cloud computing: Risks and Benefits: https://rewind.com/blog/cybersecurity-and-cloud-computing-risks-and-benefits/ (15.4.2023.)

Study Shows Hotel Price and Ratings More Important Than Brand Name - https://www.travelpulse.com/News/Hotels-and-Resorts/Study-Shows-Hotel-Price-and-Ratings-More-Important-Than-Brand-Name (pristupljeno 15.6.2023.)

Schneier.com: Security Vulnerabilities in VingCard Electronic Locks - https://www.schneier.com/blog/archives/2018/04/security_vulner_14.html (pristupljeno 30.5.2023.)

WGU.edu: The Top 7 Dangers of Public Wi-Fi for Businesses - https://www.wgu.edu/blog/7-dangers-public-wifi-businesses2112.html#close (pristupljeno 15.6.2023)

Popis ilustracija

Slika 1: Primarni elementi pametne destinacije 7
Slika 2: Najčešći razlozi plaćanja otkupnine u poduzećima 12
Slika 3: Biometrijska sigurnost 38

Grafikon 1 : Svjetske organizacije zahvaćene Ransomware-om 13
Grafikon 2: Broj godišnjih Ransomware napada 14
Grafikon 3: Prisutnost Ransomware napada po državama 15
Grafikon 4: Prosječni iznos otkupnine u poduzećima 16
Grafikon 5: Učestalost napada na mobilne uređaje 31
Grafikon 6: Prisutnost napada na mobilne uređaje kod ukupnog stanovništva 32
Grafikon 7: Potražnja za 5G uređajima u Zapadnoj i Istočnoj Europi 33
Grafikon 8: Zastupljenost phishing napada na internetskim platformama 40