UPRAVLJANJE RIZIKOM IOT- A

Doljanin, Iva

SVEUČILIŠTE U SPLITU
EKONOMSKI FAKULTET

ZAVŠNI RAD

UPRAVLJANJE RIZIKOM IOT-A

Mentor: **Studentica:**

Prof. dr. sc. Željko Garača **Iva Doljanin**

Split, srpanj, 2022.

SADRŽAJ

1. UVOD 1

2. NEKI ASPEKTI UGROZA, PRINCIPI I PREPORUKE U ZAŠTITI IOT-A 3

2.1 SIGURNOSNI ASPEKTI 4

2.1.1 Sigurnosna politika 5

2.1.2 Procjena i umanjivanje sigurnosnog rizika 5

2.2 STRATEŠKI PRINCIPI SMANJENJA RIZIKA NAPADA INFORMACIJSKIH SUSTAVA 10

2.3 ODRŽAVANJE SIGURNOSTI UREĐAJA 11

2.4 METODE ZAŠTITE 12

2.4.1 Organizacijske mjere 12

2.4.2 Fizičke mjere 14

2.4.3 Programske mjere 15

2.5 INDUSTRIJE KOJE SU RANJIVE NA SIGURNOSNE PRIJETNJE IOT-A 15

3. IOT - UPRAVLJANJE RIZIKOM 17

3.1 PROCJENA RIZIKA 17

3.2 SLOJEVI NAMIJENJENI UPRAVLJANJU KIBERNETIČKIM RIZIKOM INTERNETA STVARI 18

3.3 UPRAVLJANJE RIZIKOM- PRIMJERI 19

3.3.1 Pametna soba s primjenom IoT tehnologije 19

3.3.2 „Pametna“ kuća 20

3.3.3 Zdravstvo 22

3.3.4 Autoindustrija 26

4. ZAKLJUČAK 28

LITERATURA 29

SAŽETAK 31

SUMMARY 32

1. UVOD

Internet stvari (*eng. Internet of Things* ili skraćeno IoT) stvorio je novu paradigmu u kojoj mreža strojeva i uređaja pokreću nove procesne inovacije te omogućuje međusobno komuniciranje i surađivanje u poduzećima.[1] Ideja Internet of Things seže iz 80-ih i 90-ih godina prošlog stoljeća kada se raspravljao o povezivanju uređaja s internetom te dodavanju senzora i inteligencije u osnovne objekte.[2] U današnje vrijeme „Internet stvari" na temelju protokola IP adrese povezuje objekte iz okolne u globalnu mrežu, takva mreža stvara preduvjet za pametne okoline velikih razmjera. Koncept Internet objekata, kojeg ostvaruju pojedina područja tehničkih znanosti, ostvaruje se pomoću tehnologije dodavanjem posredničkog sloja, bežičnom senzorskom mrežom za povezivanje uređaja i drugim načinima.

O utjecaju IoT govori podatak da će do 2030 godine biti povezano 500 milijardi uređaja na internet. Svaki uređaj uključuje senzore koji prikupljaju podatke interakcijom s okolinom i komunikacijom putem mreže. Internet stvari (IoT) mreža je ovih povezanih uređaja. Ti pametni, povezani uređaji generiraju podatke koje IoT aplikacije koristiti za prikupljanje, analizu i isporuku uvida, što pomaže u poticanju više informirane odluke i radnje.[3]

Može se reći da je jedna od prednost Internet stvari brzo i jednostavno prikupljanje podataka te kvalitetnija komunikacija preko mreže međusobno povezanih uređaja. Međutim, sve informacije koje se prenose i nalaze unutar IoT su izložene stalnim rizikom i opasnostima. Zbog velike brzine, volumena i raznolikosti informacija koje se generiraju putem Interneta stvari, povjerljivost, integritet i dostupnost tih podataka je ugrožena. Zbog toga se postavlja pitanje o sigurnosti uređaja s IoT tehnologijom, pa i sigurnosti cijelog ekosustav IoT-a. Učestaliji i sve veći napadi kibernetičke sigurnosti (*eng. Cybersecurity*) na IoT sustave uzrokovali su ljudima i organizacijama širok raspon problema u pogledu reputacije, usklađenosti, financija i poslovnih operacija. Brzi porast kibernetičkih napada dijelom je posljedica fenomenalnog rasta IoT uređaja u područjima kao što su pametne mreže, nadzor okoliša, sustavi za praćenje pacijenata, pametna proizvodnja i logistika. Internet stvari popraćen je mnogim pozitivnim čimbenicima koji doprinose kvaliteti života. Međutim,

[1] Lee, I. The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model. Internet Things Eng. Cyber Phys. Hum. Syst. **2019**, 7, 100078. [Google Scholar] [CrossRef]
[2] https://www.ofir.hr/iot-ili-internet-stvari-2/
[3] https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf

potrebno je smanjiti rizik kibernetičke sigurnosti za organizacije i korisnike kroz zaštitu IoT imovine i privatnosti. Sigurnost i privatnost se može promatrati kao osnovno ljudsko pravo ili osobno pravo, u čijim poslovima je potrebna visoka razina pouzdanosti. U poslovima u kojima dolazi do korištenja Internet stvari potrebna je primjena u upravljanju rizikom. Svrha upravljanja IoT- om jest minimalizirati rizik napada. U nastavku će biti više govora o načinu zaštite te rizikom koja Iot tehnologija nosi.

2. NEKI ASPEKTI UGROZA, PRINCIPI I PREPORUKE U ZAŠTITI IOT-A

Digitalno povezani uređaji koji dijele velike količine podataka prožimaju nekoliko pitanja sigurnosti i privatnosti. Kako razne bežične tehnologije rastu, tako raste i korištenje IoT uređaja. Revolucija minijaturizacije rezultirala je erom „pametnih objekata". IoT uređaji ograničeni su resursima koji prate mnoge izazove sigurnosti podataka. IoT tehnologija koristi ugrađene senzore za prikupljanje osobnih podataka, što može dovesti do neželjenog zadiranja u privatnost. Može se reći da svako pojam koji ima uz sebe pridjev „ pametni", jest dio Interneta stvari. Stoga, pametne kuće sa svojim pametnim uređajima, žaruljama su povezani na istu IP adresu. Povezani i digitalizirani uređaji olakšavaju svakodnevni život i štede energiju. Pri kupovini „pametne" kuće pitamo li se: „Tko je ugradio pametne brave?". Uvijek je naglasak na sigurnosti i zaštiti podataka, ali dovodi se u pitanje koliki je rizik izloženosti informacija, računa, kuće od hakerskih napada koji rezultiraju krađom?

Internet je postao dio privatnog i poslovnog života te informacije prikupljene iz okoline se pohranjuju na „ Oblak" *eng. Cloud.* „ Oblak" se odnosi na poslužitelje kojima se pristupa putem interneta, te softver i baze podataka koji rade na tim poslužiteljima.[4]

Dok IoT uređaji mogu uvelike povećati produktivnost poslovanja, oni isto tako dolaze sa rizikom. Budući da su takvi uređaji povezani na Internet mogu biti hakirani kao bili koji drugi uređaj povezan s Internetom. Jedan od ključnih sigurnosnih problema IoT-a je širenje površina napada zbog povećanog broja krajnjih točki. U mreži, krajnje točke su uređaji koji su povezani na internet u cjelini, što znači da svaki nudi točku ulaska lošim akterima izlažući mrežu vanjskim rizicima. Površina napada mreže sastoji se od svih mogućih mjesta koji mogu biti napadnuti, a širi se sa svakim novim uređajem spojenim na internet. Čak i ako je vjerojatnost da počinitelj pristupi jednom uređaju mala, veliki je broj IoT uređaja koji se unose u tvrtke može stvoriti značajan sigurnosni rizik.

[4] https://www.cloudflare.com/learning/cloud/what-is-the-cloud/

2.1 Sigurnosni aspekti

Tehnologija se razvija eksponencijalno te paralelno raste broj direktiva, regulativa i standarda iz domene sigurnosti. „European Union Agency for Network and Information Security (ENISA) je centar za ekspertizu mreža i informacijske sigurnosti unutar EU koji u svojim zadacima IoT-a i sigurnosti ističe:

- Promicanje usklađivanja IoT sigurnosnih inicijativa i propisa
- Podizanje svijesti o potrebi kibernetičke sigurnosti u IoT
- Definiranje sigurnosnih smjernica životnog ciklusa razvoja softvera i hardvera za IoT
- Postizanje konsenzusa za interoperabilnost u IoT ekosustavu
- Poticanje ekonomskih i administrativnih poticaja za sigurnost IoT-a
- Uspostavljanje sigurnog upravljanja životnim ciklusom IoT proizvoda / usluga
- Razjašnjenje odgovornosti među dionicima IoT-a.“[5]

U današnjem poslovanju bilo da je riječ o medicini, autoindustriji ili nekoj drugoj industrije potrebno je uspostaviti kvalitetan i pouzdan sustav upravljanja sigurnošću u poslovnom sustavu. Posebice sigurnost upravljanja informacijskim sustavom kao njegovim važnim podsustavom.

Dobro planiranje, sustavna analiza, procjena rizika, kontinuirani pregled i procjena sigurnosnog položaja vrlo su važne stavke razine sigurnosti poduzeća. „Upravljanje sigurnosnim rizikom je trajan poslovni proces čiji je cilj osiguravanje pune dostupnosti informacijskog sustava. Smatra da se taj cilj ostvaruje kroz četiri osnovne funkcije upravljanja sigurnosnim rizikom:

- Utvrđivanje sigurnosne politike
- Procjena sigurnosnog rizika
- Umanjivanje sigurnosnog rizika
- Evaluacija sigurnosnog rizika“[6]

[5] https://www.versoaltima.com/wp-content/uploads/2019/11/IOT-IGOR-GREGUREC.pdf
[6] Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 190.

2.1.1 Sigurnosna politika

Sigurnosna politika se sastoji od niza pravila, smjernica i postupaka koja učinkovito i djelotvorno upravlja sa sigurnošću poslovnih sustava. Ona bi se trebala formalizirati kroz odgovarajući dokument, upućivati korisnike na pravilno korištenje poslovnih sustava, te ukoliko se korisnik ne pridržava određenih sigurnosnih politika slijede sankcije. Politikom se isključivo štiti informacijski sustav. Sigurnosne politike trebaju biti prilagođene cjelokupnom poslovnom subjektu, ali i podijeljene po organizacijskoj strukturi zbog različitih znanja i obveza. Sigurnosne politike trebaju biti prilagođene cjelokupnom poslovnom subjektu, ali i podijeljene po organizacijskoj strukturi zbog različitih znanja i obveza. Postoji sveobuhvatna sigurnosna politika, opća organizacijska politika i funkcionalna politika. One bi trebale biti opisane standardima, postupcima i preporukama ponašanja za različita pitanja. Zbog neprekidnih novih sigurnosnih prijetnji napisana politika mora se redovito regulirati i nadopunjavati kada je to potrebno.

Sigurnosnom politikom definirane su norme koje se odnose na:

- sve korisnike i zaposlenike sustava, tj. osobe koje imaju pravo pristupa
- vanjski suradnici
- osobe koje su odgovorne za administraciju informacijskog sustava
- sva računalna oprema institucije (hardver i softver)

2.1.2 Procjena i umanjivanje sigurnosnog rizika

Proces upravljanja sigurnosnim rizikom obuhvaća identifikaciju, analizu i uklanjanje rizika. Navedene funkcije su zavisne te postoji određena povezanost među njima. Zbroj niza pojedinačnih rizika čini ukupni sigurnosni rizik zbog toga se ne mogu gledati kao cjelina jer se mjere umanjivanja rizika postavljaju pojedinačno za svaki rizik.

Slika 1: Sigurnosni rizik

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

Proces procjene rizika zahtjevna je i složena metoda koja se provodi profesionalno i iz korijena, kako bi se dobili precizniji podatci. Iskusni sigurnosni stručnjaci zaduženi su za proces analize i procjene sigurnosti informacijskih sustava, a rezultate njihove procjene šalju se menadžmentu za daljnje potrebne odluke.

Proces procjene rizika složena je i zahtjevna metoda, stoga se provodi stručno i iz korijena kako bi se dobili što precizniji podatci. Osobe koje su zadužene za sam proces analize i procjene sigurnosti informacijskih sustava provode iskusni sigurnosni stručnjaci, a procjene rezultata šalju se menadžmentu na temelju kojih će se donositi potrebne odluke. [7]

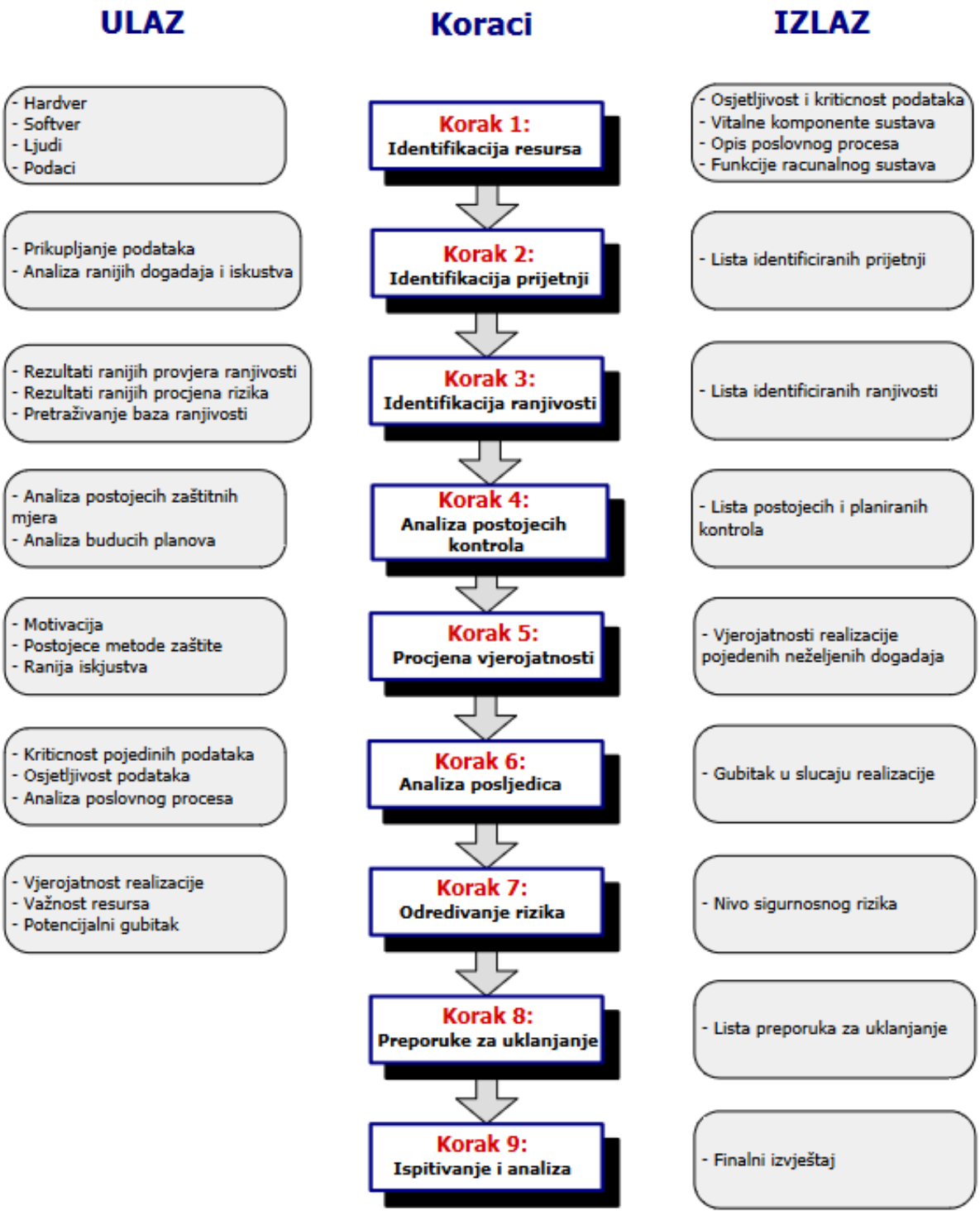
„Proces procjene rizika sastoji se od devet koraka:

1. Korak: Identifikacija i klasifikacija resursa (engl. Asset Identification);
2. Korak: Identifikacija prijetnji (engl. Threat identification);
3. Korak: Identifikacija ranjivosti (engl. Vulnerability Identification);
4. Korak: Analiza postojećih kontrola (engl. Control Analysis);
5. Korak: Vjerojatnost pojave neželjenih događaja (engl. Likelihood Determination);
6. Korak: Analiza posljedica (engl. Impact Analysis);
7. Korak: Određivanje rizika (engl. Risk Determination);
8. Korak: Preporuke za umanjivanje (engl. Control Recommendation);

[7] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

9. Korak Dokumentacija (engl. Result Documentation)“[8]

Navedeni koraci su prikazani dijagramom na sljedećoj Slika 2:



Slika 2: Proces procjene rizika

[8] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

Analiziranjem, evoluiranjem i implementacijom odgovarajućih sigurnosnih koraka umanjuje se sigurnosni rizik. Za umanjivanje sigurnosnih rizika primjenjuju se četiri pristupa.

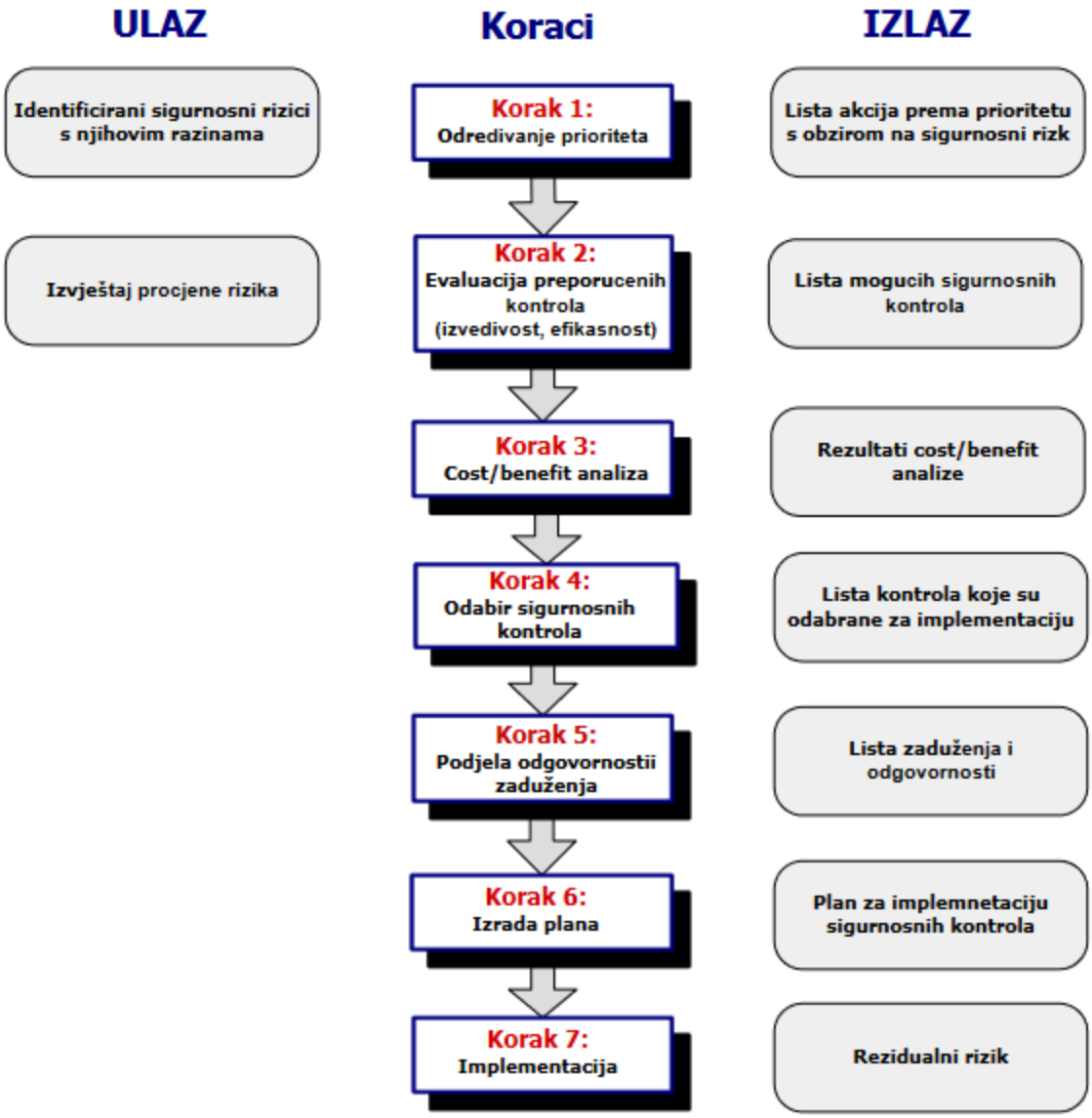
Prvi jest umanjivanje rizika, taj pristup podrazumijeva provedbu i izgradnju zaštitnih mehanizama koji smanjuju izloženost informacija resursa jer na vjerojatnost određenih resursa ne možemo utjecati.

Drugi pristup je transfer rizika čiji se rizik uz odgovarajuću naknadu prenosi na drugog, odnosno rizik i troškovi će u slučaju njegovog provođenja prebaciti drugoj organizaciji.

Treći po redu pristup je prihvaćanje rizika. To je pristup koji bez provođenja mjera transfera ili umanjivanja rizika prihvaća procijenjene rizike. Cost- benefit analizom se odlučuje o isplativosti djelovanja sigurnosnih mehanizama.

Zadnji, četvrti, pristup odnosi se na odbacivanje rizika. Zanemarivanje rizika u nadi da nikada neće doći do njegove realizacije. Takav pristup se smatra neprihvatljivim te se ne smije provoditi u niti jednom slučaju.

Na sljedećoj slici Slika 3 biti će prikazan dijagram procesa umanjivanja rizika:



Slika 3: Proces umanjivanja rizika

Izvor: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

Implementacijom koraka sa slike 3 sigurnosni rizik se umanjuje na kontroliranu razinu, uzimajući u obzir stalni rezidualni rizik kojeg prema analizama nije isplativo uklanjati.

Također, ponovnom analizom utjecaja ranjivosti i prijetnji, ujedino i glavnih čimbenika moguće je procijeniti sigurnosni rizik koji je reduciran implementacijom novih ili nadogradnjom postojećih kontrola Rizik može biti umanjen implementacijom sljedećih kontrola:

– eliminacija ranjivosti u sustavu,

– smanjivanje motivacije za provođenja napada, odnosno iskorištavanja ranjivosti,

– smanjivanje potencijalnih gubitaka u slučaju realizacije rizika[9]

2.2 Strateški principi smanjenja rizika napada informacijskih sustava

Krajem 2016. godine Ministarstvo Domovinske sigurnosti SAD- a izdalo je dokument pod nazivom „ Strategic Principles for Securing the Internet of things IoT“[10]. Navedeni dokument govori kako strateški osigurati IoT ekosustav, odnosno smanjiti rizik napada. Smatra se da razne ranjivosti u IoT-u bi se mogle ublažiti kroz priznate najbolje sigurnosne prakse. Međutim, u današnjici mnogo proizvoda ni ne sadrži najosnovnije sigurnosne mjere. Veliki je broj čimbenika koji doprinose manjku sigurnosti. Jedan od čimbenika odnosi se na odgovornost sigurnosne odluke, no postoje pitanja: „Tko je odgovoran za sigurnosne odluke u svijetu u kojem jedna tvrtka dizajnira uređaj?“, „Tko opskrbljuje komponentni softver?“, „Tko upravlja mrežom u koju je uređaj ugrađen?“, „Tko razvija uređaj?“ i ostala pitanja.

Također, problem je nedostatak poticaja za programere da adekvatno osiguraju proizvode. Tvrtke ne moraju nužno snositi troškove propuštanja te imaju neujednačenu svijest o tome kako procijeniti sigurnosti značajke konkurentskih opcija.

U dokumentu Ministarstvo Domovinske sigurnosti SAD-a navodi načela za bolju organizaciju u rješavanju navedenih IoT sigurnosnih rizika, a to su:

- uključivanje sigurnosti u fazi dizajniranja,
- unaprjeđivanje sigurnosne nadogradnje i upravljanje ranjivostima,
- korištenje nadogradnje dokazanim sigurnosnim praksama,
- određivanje prioriteta sigurnosnih mjera prema potencijalnim učincima prijetnje,
- promoviranje transparentnosti u cijelom IoT- u,
- pažljivo povezivanje s namjerom[11].

[9] https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf

[10] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

[11] https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf

2.3 Održavanje sigurnosti uređaja

Iako će osiguranje krajnjih točaka i mreže ovisiti o vrsti uređaja, postoje određene mjere opreza koje će pomoći pri zaštiti bilo koje vrste Internet stvari *eng.*"*gadget*" ili uređaja.

Korištenje „snažnih" lozinki

Posjedovanje „snažnih" lozinki uvijek je važno, ali posebno za IoT uređaje. Preuzimanje kontrole nad IoT uređajem putem vlastitog sučelja ili web portala je trivijalno ukoliko se koriste „slabe" lozinke. Još više zabrinjava činjenica to što mnogi IoT uređaji dolaze sa zadanim lozinkama koje mnogi korisnici ne mijenjaju- što znači da napadač možda već zna lozinku uređaja.

„Snažne" lozinke na ostatku mreže dodati će drugu razinu obrane u slučaju da haker ipak dobije pristup putem uređaja, a to su: zaustavljanje ili ometanje pokušaja pristupa datotekama, bazama podataka i drugim uređajima. Promjena lozinke na usmjerivaču u dugu i „snažnu" je posebno važna jer kompromitirani usmjerivač brzo ostavlja cijelu mrežu ranjivom.

Mrežna sigurnost

Potrebno je provjeriti je li ažuran i siguran usmjerivač *eng. router* s uključenim firewall-om. Usmjerivač može biti prva točka napada, a ako je usmjerivač kompromitiran, cijela mreža će postati ranjiva. Instaliranje sigurnosnog rješenja krajnje točke koje omogućuje otkrivanje ranjivosti u pojedinoj mreži, primjerice sigurnosna rješenja sa značajkom skeniranja kao što je Avastov Wi-Fi Inspector jest ključno.

Nadogradnja

Odgovorni proizvođači će dopustiti sigurnosna ažuriranja za svoje IoT uređaje kada se otkriju ranjivosti. Važno je osigurati da se uređaji redovito nadograđuju s najnovijim ažuriranjem. U slučaju posjedovanja uređaja koji ne prima ažuriranja, potrebno je razlučiti prednosti uređaja u odnosu na potencijalni utjecaj na poslovanje u slučaju napada. Za uređaje koji primaju ažuriranja, preporuča se ulaganje u softver za upravljanje nadogradnjom radi potvrde o ažurnosti.

Nužnost

Kako postoji rastuće tržište za IoT uređaje, proizvođači su željni izbaciti veliki broj istih i dovodi se u pitanje potrošnja vremena koja je potrebna za razvoj sigurnosti proizvoda. Iako IoT uređaji mogu biti vrlo korisni, potrebno je razmisliti:“ je li potreban toster ili kuhalo za vodu spojeno na Internet?“. Naime, ako bilo koji kućanski aparat spojen na Wi- fi mrežu koja nije zaštićena, napadač može preko tih uređaja ući u mrežu te doći do bankovnih ili nekih drugih osobnih podataka.

Međutim, prednosti nove tehnologije uvijek su primamljive vlasnicima malih poduzeća koji žele uštedjeti novac i povećati produktivnost. Prvenstveno je važno osvijestiti se i educirati o rizicima koje nova tehnologija donosi. Pametni uređaji imaju potencijal poboljšanja učinkovitosti u mnogim industrijama, ali također treba poduzeti korake sigurnosti kako mreža ne bi bila izložena zlonamjernim akterima.

2.4 Metode zaštite

„Metode zaštite u oblaku dijele se na:

1. **Organizacijske mjer**e – opće mjere zaštite informacijskih resursa koje se ne bave specifičnostima zaštite sustava već osiguravaju okvir za provođenje specifičnih mjera
2. **Fizičke mjere** – odnose se na onemogućavanje pristupa neovlaštenim osobama, uzimaju u obzir sve pristupne putove informacijskim resursima
3. **Programske mjere** – specifične za sigurnosne rizike informacijskih sustava, odnose se na podatke te se provode pomoću softvera i odnose se na sam softver“[12]

2.4.1 Organizacijske mjere

Organizacijske mjere poduzima sam poslovni sustav u svrhu osiguranja željene razine funkcionalnosti sustava te integriteta podataka u uvjetima djelovanja pretpostavljenih oblika prijetnji. Organizacijskim mjerama smatra se sveukupni sadržaj mjera i postupaka iz oblasti

[12] Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 200.

sigurnosti, izrada potrebne dokumentacije koja je potrebna za njihovu primjenu te donošenje i izrada organizacijskih uputa kojima se one provode na radnom mjestu. [13]

Dijelimo ih na tri razine, a to su: infrastruktura informacijske sigurnosti, sigurnost pristupa treće osobe te outsorcing.

Infrastruktura informacijske sigurnosti ima za cilj upravljati sigurnošću unutar organizacije kako bi funkcionirala te štitila povjerljive informacije. Može se podijeliti na:

1. Tim za upravljanje informacijskom sigurnošću
2. Koordinacija rada informacijske sigurnosti
3. Dodjela odgovornosti za informacijsku sigurnost
4. Proces autorizacije organizacijskih cjelina koje sudjeluju u obradi
5. Savjeti specijalista o informacijskoj sigurnosti
6. Suradnja između organizacija
7. Neovisni pregledi efikasnosti informacijske sigurnosti[14]

Naime, politika informacijske sigurnosti trebala bi doprinijeti općenitom vodstvu za sigurnost i odgovornost uloga unutar organizacije. Glavni cilj politike informacijske sigurnosti je specificiranost svih njezinih odgovornosti, koje se odnose na odgovornost korisnika. Upravo zbog toga najveća pažnja bazira se na identifikaciji i jasnom definiranju dijelova imovine i sigurnosnih procesa pridruženih svakom pojedinačnom sustavu. Na kraju svega potrebno je definirati razine ovlasti i iste dokumentirati.

Kako bi organizacija što bolje funkcionirala dolazi do potrebe zaposlenja i treće strane. Prilikom pristupa treće zaineresirane strane postoj dvije vrste pristupa, a to su fizički i logički pristup. Kod fizičkog pristupa dolazi do mogućnosti pristupa prostorijama s ormarima za pohranu i računalnom opremom, a kod logičkog pristupa omogućen je ulazak u baze podataka određene organizacije i njezinim informacijskim sustavima.

Outsourcing je pojam koji se koristi kod vanjskih poduzeća i pojedinih osoba za obavljanje zadanog posla. Glavni zadatak polsovnig subjekta je održavanje sigurnosnih informacija čija j provjera izvršena u nekoj drugoj organizaciji. Prilikom ugovaranja poslova outsourcing-a potrebno je sklopiti ugovor s trećom stranom. Njime se kotroliraju mehanizmi, procjenjuje rizik

[13] Šehanović, Hutinski, Žugaj 2002.
[14] http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf

i provode se sigurnosni postupci kako ne bi došlo do zlonamjernih korištenja informacija unutar organizacije.

2.4.2 Fizičke mjere

Fizičke mjere se koriste prilikom očuvanja sustava informacija u slučajevima poput elementarnih nepogoda, ali i ljudskih slabosti kao što je krađa, sabotaža i neposlušnost. Cilj je spriječiti neautorizirani pristup računalnom sustavu, zaštititi integritet podataka koje se pohranjuju na uređaj. Primjena fizičke sigurnosti jest proces koji koristi mjere zaštite kako bi se spriječilo oštećenje, neovlašten pristup ili uništenje dobara.[15]

Fizičke prijetnje mogu se podijeliti na prijetnje uzrokovane ljudskim utjecajem te na prirodne nepogode.

Do ljudske prijetnje dolazi izravnim ili neizravnim potezima korisnika, a dijele se na:

1. Krađu
2. Nenamjerno oštećenje imovine
3. Sabotaža
4. Zloupotreba ovlasti
5. Otkrivanje osjetljivih podataka
6. Neposlušnost
7. Neovlašten pristup podatcima ili imovini

Prijetnje nastale zbog prirodnih nepogoda smatraju se onima na koje čovjek nikako ne može djelovati te se dijele na:

1. Geofizičke nepogode
2. Sezonski fenomeni
3. Metodološke nepogode
4. Biološke snage
5. Astrofizički fenomen

[15] https://www.cert.hr/wp-content/uploads/2019/04/NCERT-PUBDOC-2010-06-304.pdf

Fizičkom zaštitom štiti se cijela okolina kako bi bilo što teže doprijeti do traženih informacija. Stoga, postoji zaštita okoline, zaštita prostorija, zaštita opreme te kontrola pristupa.

2.4.3 Programske mjere

Programske mjere se dijele na dvije razine, prva je razina operativnog sustava, a druga je razina programa koja se tiče korisnika. Kod organizacija većinom se koriste mnogobrojni operativni sustavi. Prilikom upotrebe za svakog pojedinog korisnika je potrebno postaviti dozvoljeno područje ovlaštenog djelovanja te mogućnost razine pristupa potrebnim djelovanja i razinu pristupa informacijama, što se čini postavljanjem lozinki kao za povećanje zaštite.

U svrhu zašite informacije, ovlaštenim informacijama isključivo administrator ima pristup, a korisnik ima samo pristup ovlaštenim informacijama koje mu dopusti administrator sukladno s korisnikovim ovlastima. Sukladno tome svaki korisnik dobije korisničko im i lozinku kojima se koristi za nesmetani pristup bitnim informacijama.

Sljedeća je razina sigurnosti podataka razina korisničkih podataka. Provedba zaštite korisničkih programa provodi se kroz tri razine:

1. Čitanje podataka iz baze
2. Omogućuje unos i promjenu u bazi
3. Omogućuje prethodne dvije razine te eliminaciju podataka

Uloga administratora u zaštiti informacija jest od izrazite važnosti. O tome govori činjenica da se obrisani podaci ne uklanjaju na izravan način, nego se spremaju u datoteke čiji pristup ima samo administrator. Nakon toga administrator provjerava podatke te odlučuje hoće li ih ukloniti ili ne.

2.5 Industrije koje su ranjive na sigurnosne prijetnje IoT-a

Dok IoT uređaji mogu predstavljati sigurnosni rizik za sve tvrtke koje ne poduzimaju potrebne korake u osiguravanju svoje mreže, postoje određene industrije su posebno osjetljive na napade.

Industrije koje će se suočiti s najvećim rizicima su one u kojima se IoT uređaji ne koriste samo kao alati za povećanje produktivnosti, već se integriraju u samu srž poslovanja. Na primjer,

korištenje IoT uređaja u proizvodnji može pružiti ogromne prednosti učinkovitosti, ali kada proizvodni procesi postanu potpuno oslonjeni na pametnu tehnologiju, jedan napad može dovesti do prestanka rada tvornice.

Virus Stuxnet, 2010. godine, zarazio je tvornicu za obogaćivanje urana u Iranu i prouzročio trajna oštećenja centrifuga.[16] Iako je vjerojatno da nitko neće upotrijebiti tako sofisticirani napad na malu tvrtku, IoT- ov zlonamjerni softver se razvija brzim tempom. Naime, svaka tvrtka koja koristi nezaštićene IoT uređaje u svom proizvodnom procesu mogla bi jednog dana pronaći svoju operaciju kao taoca hakera.

Zatim, vlasnici bilo koje male tvrtke koja bilježi povjerljive podatke o klijentima također bi trebali biti zabrinuti zbog rizika. Web kamere, pisači, sigurnosne kamere i digitalna zvona na vratima samo su neki od uređaja koji se potencijalno mogu „hakirati“ i putem svojih kamera i mikrofona otkriti povjerljive informacije napadačima. To je samo jedna od pet ključnih prijetnji krajnje točke koje predstavljaju rizik za mala poduzeća.

U sljedećem poglavlju biti će detaljnije opisano kako upravljati s takvom vrstom rizika.

[16] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

3. IOT - UPRAVLJANJE RIZIKOM

Upravljanje rizikom *eng. Internet of things* skup je procesa i praksi koji se koriste za prepoznavanje i pomoć u uklanjanju potencijalnih opasnosti i negativnih posljedica ranjivosti IoT-a. Upravljanje rizikom primjenjuje prakse upravljanja rizicima i upravlja uključenim poslovnim rizikom na temelju svih aspekata, načina na koje to poslovanje koristi tehnologiju. Konkretno, značajan rast Interneta stvari dramatično je povećao broj izazova upravljanja rizicima i sigurnosnih izazova s kojima se poduzeća suočavaju. Cyber kriminalci pokreću sofisticiranije i potencijalno štetne napade, a broj uređaja kojima je potrebno osiguranje nastavlja rasti kako se IoT širi.

Rizik je vjerojatnost da se dogodi prijetnja koja može rezultirati negativnim utjecajem ili oštećenjem imovine. Primjer koji se temelji na IoT-u je vjerojatnost da se dogodi napad krađe identiteta na povezani poslovni uređaj, poput prijenosnog računala tvrtke ili pametnog telefona. To uzrokuje nekoliko zaraženih IoT senzora zlonamjernim softverom i dovodi do posljedičnog narušavanja proizvodnog pogona proizvodnih linija. Iako postoje mnoge aplikacijske domene za IoT, kao npr.: Povezana i autonomna vozila, Zdravlje i dobrobit, Industrija 4.0 i Smart Grid.

3.1 Procjena rizika

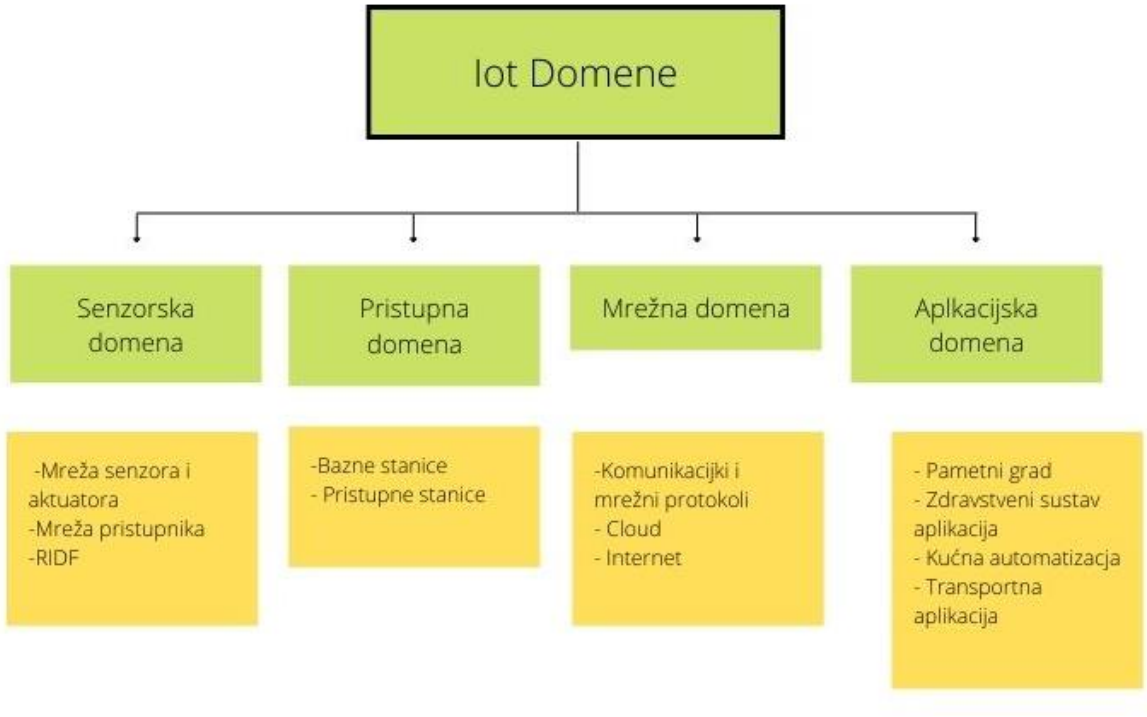
Kada je riječ o potencijalnom riziku u IoT- u prvo se procjenjuje rizik. Sljedeći korak je mogućnost sposobnosti procjene što uključuje; definiranje rizika koja vodi do jasnog razumijevanja koja su organizacijska sredstva na meti, što se može oštetiti i kakva bi se šteta mogla dogoditi da su napadi uspješni.

Zatim slijedi procjena rizika. Ovaj korak ima za cilj izmjeriti rizik na temelju vjerojatnosti pojava prijetnji i utjecaj na infrastrukturu IoT organizacije. Te mjere mogu biti kvalitativne (npr. ocjene prema razinama; visoka, srednja i niska) ili kvantitativne (temeljene na matematičkim procjenama i izračunima).

Nakon što je napravljen popis rizika te je svaki od njih procijenjen, sljedeći korak je određivanje prioriteta rizika. To u biti pruža rangiranje rizika na temelju već procijenjenih razina kao što je navedeno u prethodnom paragrafu.

Navedena tri koraka smatraju se najboljim procesom procjene rizika.[17]

IoT sustav obično se dijeli na četiri domene (Slika 4), a to su: senzorska domena, pristupna domena, mrežna i aplikacijska domena. Za svaku od navedenih domena potrebno je odrediti izvore kako bi se procijenio rizik, utvrditi resurse koje je potrebno zaštititi i kako se rizik može ublažiti. Zato je potrebno dobro poznavati i razumjeti IoT arhitekturu sustava za vrijeme analitičkog postupaka u procjeni rizika.



Slika 4: IoT domene

Izvor: https://zir.nsk.hr/islandora/object/algebra%3A428/datastream/PDF/view

3.2 Slojevi namijenjeni upravljanju kibernetičkim rizikom interneta stvari

Okvir za upravljanje rizikom počinje slojem kibernetičkog ekosustava Interneta stvari. Procjenom iz elemenata ekosustava, organizacija identificira i razumije dinamiku i uloge svojih dionika. Sloj kibernetičkog ekosustava povremeno i/ili stalno nadzire, ocjenjuje okolinu i priopćava zaključke drugim relevantnim slojevima.

[17] https://www.preprints.org/manuscript/201903.0104/v1

Organizacija, na sloju cyber infrastrukture, analizira trenutno stanje kibernetičke sigurnosne infrastrukture analizirajući uloge i odgovornosti ljudi, organizacijske politike te implementaciju tehnologija istih sigurnosti.

Sloj procjene cyber rizika identificira IoT sredstva i usluge, ranjivosti i kibernetičke prijetnje. Kvantificira i daje prioritet kibernetičkim prijetnjama i učincima te vrši raspodjelu resursa različitim IoT projektima kibernetičke sigurnosti. Na sloju cyber izvedbe IoT-a razvijaju se kibernetičke tehnologije. Provode se aktivnosti nadzora i kontrole te se provode aktivnosti kontinuiranog poboljšanja.[18]

Tablica 1: Prikaz arhitektura IoT slojeva

Sloj kibernetički ekosustav IoT-a
Sloj kibernetičke infrastrukture
Sloj procjene kibernetičkog rizika
Sloj kibernetičke izvedbe IoT-a

Izvor: https://www.mdpi.com/1999-5903/12/9/157/htm

3.3 Upravljanje rizikom- primjeri

3.3.1 Pametna soba s primjenom IoT tehnologije

Pametne sobe temeljene na IoT tehnologiji postale su vrlo popularne u hotelima, bolnicama, individualnim kućama i raznim vrstama zgrada. Pametna soba prikladna je za ilustraciju procjene rizika. Budući da u pametnim sobama postoji više složenih IoT – ranjivosti – prijetnji u kojima više heterogenih uređaja i tehnoloških platformi međusobno komuniciraju. U hotelskoj industriji pametna hotelska soba postala je regulativa zbog pada cijene IoT sustava i konkurencije u hotelskoj industriji. Neke od očekivanih prednosti pametne hotelske sobe uključuju integrirano iskustvo korisnika s pristupom vlastitim podacima i informacijama,

[18] https://www.mdpi.com/1999-5903/12/9/157/htm

pristupačne glasovne i mobilno optimizirane kontrole te poboljšanu personaliziranu uslugu. Međutim, zadiranje u privatnost još uvijek zabrinjava korisnike pametnih hotelskih soba. Kao dokaz koncepta, LP model se primjenjuje na scenarij hipotetske pametne sobe. LP model ima tri glavne komponente:

1. varijable odluke, koje predstavljaju obrambene vjerojatnosti IT imovine, ranjivosti i prijetnji
2. ciljanu funkciju, koja je matematička funkcija varijabli odlučivanja za minimiziranje ukupnog cyber troška
3. ograničenja, koja se odnose na skup funkcionalnih jednakosti ili nejednakosti koje predstavljaju financijska, tehnološka i operativna ograničenja o tome koje se numeričke vrijednosti mogu dodijeliti varijablama odluke.

Iako je ovaj scenarij ostvariv te će se vjerojatno pojaviti u svakoj pametnoj hotelskoj sobi, ne implicira da je bilo koja hotelska organizacija uključena u razvoj takve mogućnosti. Glavni cilj takve informatičke transformacije jest: ubrzati isporuku novih usluga putem digitalnog kanala, poboljšati korisničko iskustvo s mobilnim tehnologijama, maksimizirati prihod potencijal i smanjiti ukupne troškove vlasništva IT-a. Uz revitalizaciju tvrtke digitalne platforme može se poboljšati iskustvo gostiju u svakoj fazi njihovog boravljenja. Doprinosi boljem iskustvu samog putovanja, te time jača lojalnost te povećava svoju konkurentnost na tržištu.[19]

3.3.2 „Pametna" kuća

Pametna kuća se sastoji od računala, pametnog telefona i drugih uređaja koji su opremljeni vezom za povezivanjem s Internet stvari i „pametnim" senzorom. Primjerice, korisnik može daljinski upravljati putem internetske veze, također može „motriti" kuću u stvarnom vremenu putem IP kamere. Razvijaju se čak i brave za vrata koje uključuju opcije povezivanja koje omogućuju daljinsko upravljanje. U IoT okruženjima poput „pametne" kuće daljinski su upravljane mobilnim uređajima kao što su pametni telefoni.

Sa stajališta slojeva IoT arhitekture senzori pametnih telefona mogu uzrokovati sekundarnu štetu kao što je curenje osobnih podataka. U slučaju da je na takvom uređaju instalirana aplikacija šteta može biti još veća. Ovaj fenomen povećava mogućnost prijetnji „stvarnom prostoru", za razliku od kibernetičkih napada (DDoS, APT napadi i sl.), koji nanose štetu cyber

[19] https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/customers/vmware-marriott-17q1-casestudy.pdf

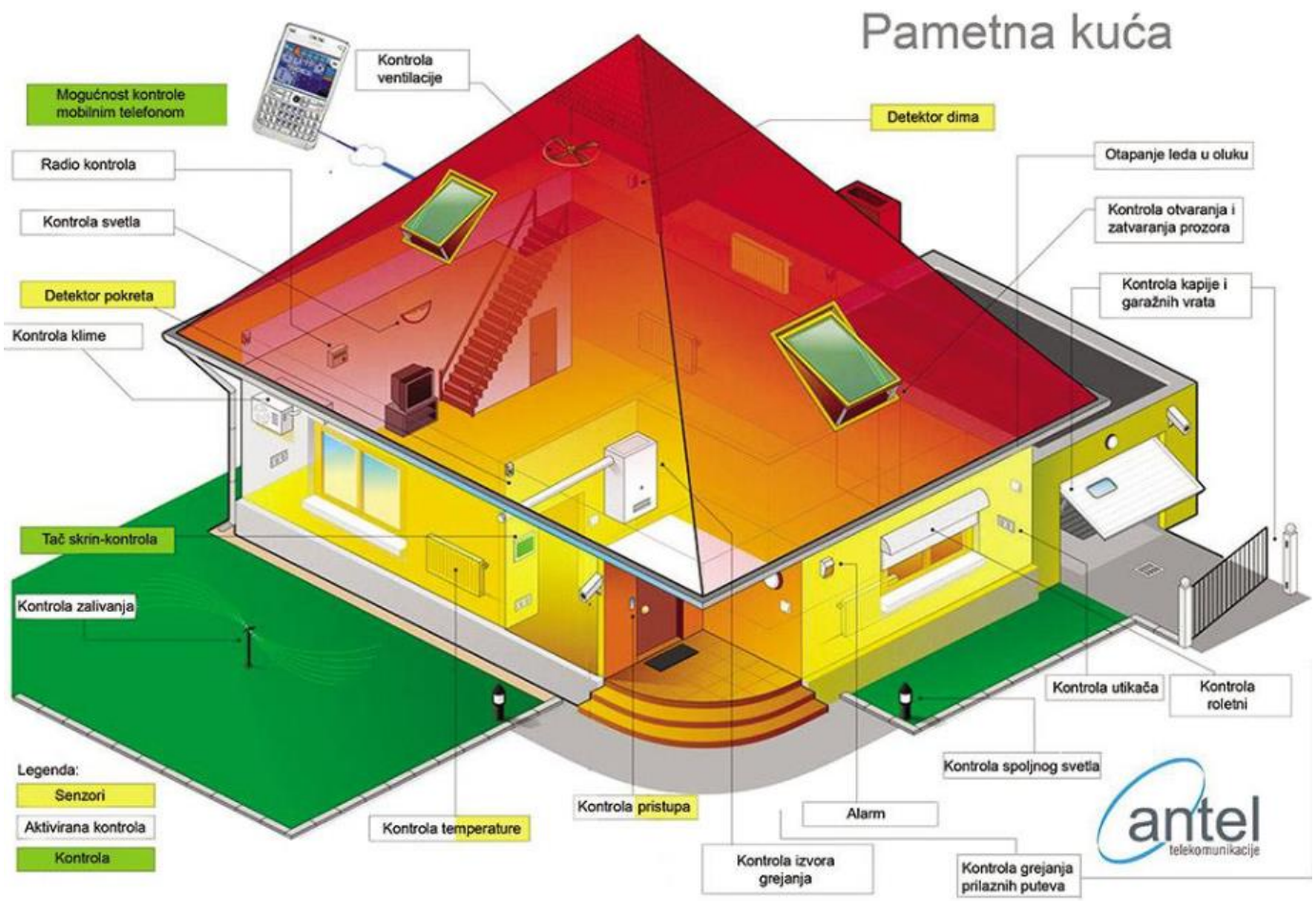
prostoru *eng. cyberspace*. „Pametna“ kuća je ranjiva na sigurnosne prijetnje jer koristi internet koji koristi Radio frekvencijsku identifikaciju *eng. Radio Frequency Identification* (RFID), bežičnu senzorsku mrežu kao što je: (WSN), Wi-Fi, 3G i 4G. Zbog njihove ranjivosti, prikupljene informacije sa senzora na IoT uređajima napadaču lako mogu „procuriti“ osobni podatci članova kućanstva. Recimo, napadač ima namjeru uzeti podatke prikupljene sa senzora IoT uređaja koristeći zlonamjerne aplikacije. Ova zlonamjerna aplikacija podijeljena je u dvije vrste. Prvi je tip koji zamjenjuje često korištene aplikacije pravom aplikacijom, a drugi je tip koji radi u pozadini uređaja za krađu internih podataka.[20]

Nakon što se zlonamjerna aplikacija instalira u IoT uređaje dobiva pristup raznim senzorima. To omogućuje neovlašteno prikupljanje informacija i praćenje privatnosti. Kako bi se koristio pristup procjeni rizika, potrebno je postaviti niz informacijskih sredstava te ih profilirati. U ovom procesu profiliranja identificiraju se sigurnosni zahtjevi sredstva, to određuje gdje se sva imovina pohranjuje, transportira i obrađuje. Korisnik ili sustav u pametnom domu identificira ranjive točke koje mogu ugroziti sigurnosne zahtjeve za povjerljivost, integritet i dostupnost, ovisno o tome kako se pristupa imovini. Ta identificirana informacijska sredstva omogućuju prepoznavanje sigurnosnih prijetnji. Sigurnosne ranjivosti koje izazivaju zabrinutost stvaraju se kao scenariji u vezi s atributima prijetnje. Ono može identificirati specifične prijetnje koje bi mogle imati negativan utjecaj na imovinu. Kroz tri scenarija biti će opisan rizik s kojim se korisnik može susresti.

U prvom scenariju napadač oponaša napad kao korisnik s legitimnim pravima. Da bi napadač postigao cilj potrebne su akreditacije korisnika „pametnog“ doma, potrebno je steći korisnički ID i lozinku. Pristup vjerodajnicama može se izvesti pomoću tehnika društvenog inženjeringa ili presretanja generičkih podataka prikupljenih putem IoT senzora. Budući da opći podaci koriste senzore pokreta i audio senzore, sami prikupljeni podaci mogu biti slaba točka jer omogućuju izravnu analizu podataka. U trećem scenariju napadač može „ubaciti“ zlonamjerni kod u aplikaciju. Ubacivanjem zlonamjernog koda u mobilnu aplikaciju povezanu s IoT sustavom napadaču se omogućuje vođenje štetnih operacija. Takva prijetnja umetanjem zlonamjernog koda može uzrokovati štetu zbog curenja općih podataka kroz GPS senzore, senzore pokreta, audio senzore i senzore kamere postavljene na mobilni uređaj. Konkretno, takva bi se prijetnja mogla iskoristiti kao put napada za stjecanje akreditacija korisnika. Kod trećeg scenarija može doći do otkrivanja fizičke prijetnje preko „pametnih“ senzora okoliša

[20] https://www.mdpi.com/1424-8220/19/9/2148/htm#B1-sensors-19-02148

kao što je abnormalnost u domu i upozoravanja korisnika na opasnost. Napadač može ukrasti informacije prikupljene s instaliranih senzora oslobađanjem zlonamjernog koda korištenog u scenariju 2 na uređaje. Takvo ponašanje može se koristiti kao neovlašteni alat za nadzor kako bi se utvrdilo gdje se korisnik nalazi u domu. Na sljedećoj slici Slika 5 prikazano koje elemente sadrži pametna kuća.



Slika 5: Prikaz sheme pametne kuće

Izvor:https://repozitorij.fpz.unizg.hr/islandora/object/fpz%3A179/datastream/PDF/viw

3.3.3 Zdravstvo

Sigurnosne ranjivosti IoT tehnologije u zdravstvu predstavljaju značajniju prijetnju od ranjivosti u potrošačkim uređajima jer mogu dovesti do fizičkih ozljeda. Zdravstveni djelatnici

i pacijenti oslanjaju se na točne podatke kako bi donosili odluke o skrbi i provođenju liječenja. Zdravstvo je među brzorastućim industrijama u IoT-u s postojećim različitim aplikacijama u rasponu od daljinskog nadzora do integriranih mobilnih uređaja za lijekove. Proizvodi za praćenje zdravstvenog stanja omogućuju pacijentu da prati svoju prehranu, krvni tlak, puls, kondiciju ili druge vitalne znakove te prima povratne informacije u stvarnom vremenu od bolnica, rehabilitacijskih centara, liječnika, medicinskih sestara, vozila hitne pomoći, pomoćnih uređaja itd. Uređaji za identifikaciju su ugrađeni s pametnim zdravstvenim rješenjima i povezani su s mrežom za prikupljanje i prijenos podataka o pacijentima putem interneta. Što omogućuje ovlaštenom zdravstvenom osoblju lakše i brže prikupljanje podataka. Slika 6 prikazuje ideju kako IoT platforma može spojiti navedene elemente u zdravstveni sustav.

Slika 6: Zdravstveni sustav povezan IoT tehnologijom

Izvor:https://ejournal.um.edu.my/index.php/MJCS/article/download/21469/10998/4627

Budući da se podaci prenose putem interneta zaštita povjerljivosti i integriteta kartona pacijenata ključna je kako bi se osiguralo postavljanje pravih tretmana za pacijente. Stoga postoje pet glavnih rizika implementacije IoT-a u zdravstvu, a to su:

1) Rizik izlaganja privatnosti pacijenata,
2) Prijetnje narušavanja privatnosti zbog cyber napada,
3) Prisluškivanje podataka i povjerljivost podataka,

4) Prijetnje krađi identiteta i privatnosti pohranjenih podataka,
5) Privatnost lokacije.[21]

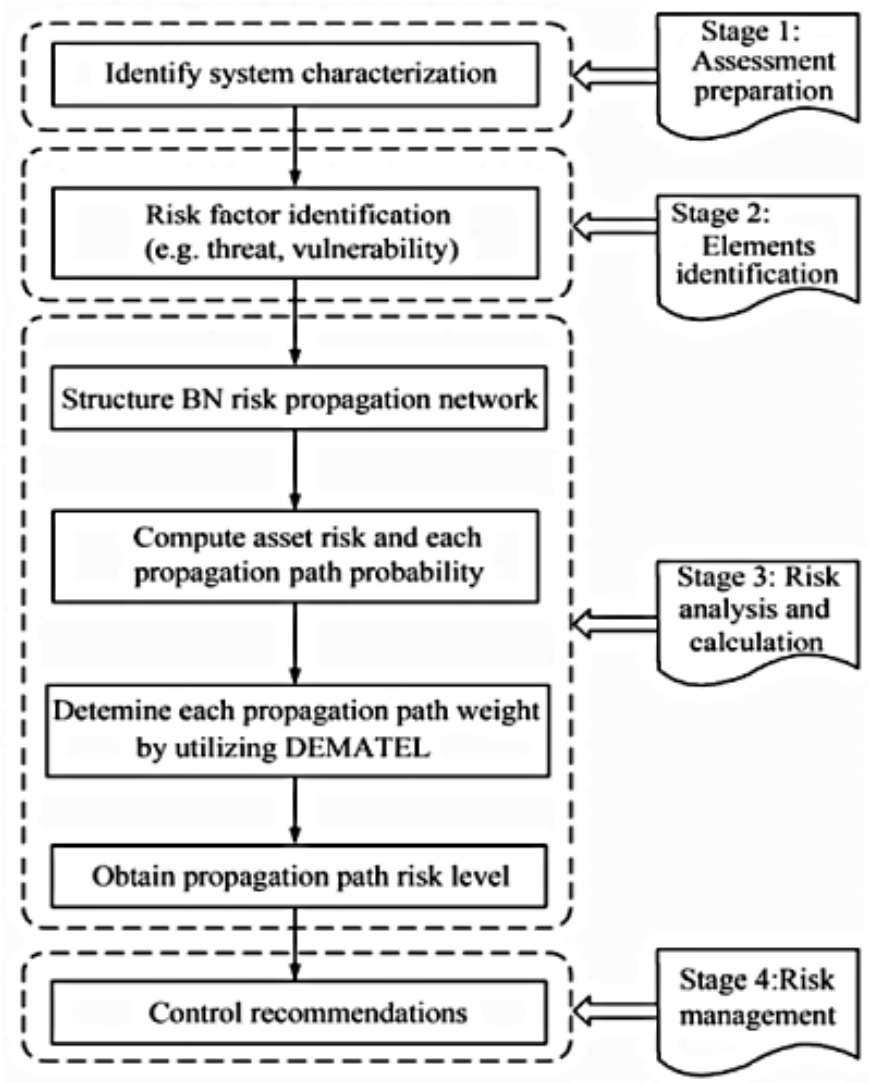
Međutim, dolaskom novih značajki i mogućnosti IoT-a zanemareni su zahtjevi za sigurnosti i privatnosti podataka. Ovaj problem može biti povezan s hardverom, softverom, aplikacijom, udaljenom vezom i drugim tehnologijama u upotrebi. Primjerice, prilagodba hardvera za IoT dizajn zadovoljit će potrebu za ispunjavanjem predviđenog dizajna ugrađenih sustava. Stoga bilo bi pogrešno implementirati uređaje koristeći unaprijed određene funkcije i platforme koje nisu namijenjene za sigurnosne svrhe.

Hakere interesiraju zaštićenije medicinske informacije za cyber napad te provaljuju u informacijske sustave temeljene na IoT-u. U slučaju da se podatci otkriju, tvrtke bi se potencijalno mogle suočiti s financijskim gubicima, prekidom poslovanja ili oštećenjem ugleda zbog neuspjeha u osiguravanju podataka koji se drže u njihovim informacijskim sustavima. Primjerice, tvrtka koja proizvodi nosive srčane monitore mogla bi imati medicinska očitanja učitana u oblaku. U slučaju da inženjeri koji su odgovorni za sigurnost u oblaku ne uspiju ispravno konfigurirati sigurnosnu zakrpu, to bi moglo stvoriti ranjivost. Ako hakeri doprije unutar sustava mogli bi prodati osjetljive zdravstvene podatke pacijenta. Tvrtke se mogu smatrati odgovornim za tjelesne ozljede, ekonomske gubitke trećim stranama i neuspjeh u propisnom osiguranju podataka. No tehnološke tvrtke mogu poduzeti korake kako bi se zaštitile od mogućeg rizika. Drugi primjer su medicinski IoT uređaji koji su dizajnirani prvenstveno za jednostavnu upotrebu, ali s takvom jednostavnošću dizajna, većina ne podržava enkripciju. To znači da svaki put kada se medicinski uređaj povezan na internet koristi za povezivanje s bolničkom mrežom ili zdravstvenom bazom podataka, postoji rizik od presretanja ili infiltracije. Takav scenarij bi se mogao dogoditi kada vozači hitne pomoći koriste mobilne uređaje za prijenos podataka o pacijentima u hitnu, kada mobilne zdravstvene klinike *eng. mobile health clinics* (MHC) prenose podatke o pacijentima u svoju bazu podataka ili kada kućni uređaji za telemedicinu prenose podatke pružateljima zdravstvenih usluga.

Nekoliko radnji koje treba razmotriti radi smanjenja izloženosti navedenim rizicima:

- Procijeniti i implementirati odgovarajuće sustave upravljanja kvalitetom i rizicima
- Ugraditi kibernetičku sigurnost.
- Procijeniti ugovorne prakse poduzeća

[21] https://ejournal.um.edu.my/index.php/MJCS/article/download/21469/10998/46267



Slika 7: Postupak procjene rizika IoT-a

Izvor: https://ejournal.um.edu.my/index.php/MJCS/article/download/21469/10998/46267

Za kraj, može biti korisno razgovarati o relevantnom osiguranju s agentom ili brokerom. Prednosti pokrivenosti odgovornosti za proizvod nudi pokriće odgovornosti za pogreške, propuste, kibernetičku odgovornost i pokriće prve strane povezane s internetom mogu pomoći u zaštiti od potencijalne odgovornosti.[22]

[22] https://ejournal.um.edu.my/index.php/MJCS/article/download/21469/10998/46267

3.3.4 Autoindustrija

Automobilska industrija po svojoj prirodi je inovativna. Od početaka proizvodnje automobila na parni pogon do današnjih električnih vozila automobili su promijenili način na koji radimo i živimo. Inovacija se nastavlja i danas velikim dijelom zahvaljujući Internetu stvari. Može se reći da je IoT otvorio novi svijet za korisničko iskustvo u automobilskoj industriji; od povezanih automobila do samovozećih vozila, to su stvarnost današnjice i više ne znanstvena fantastika.

U 2020. godini 91% novih prodanih automobila u SAD-u bilo je povezano s Internetom stvari. Znači to je više od 13 milijuna povezanih vozila prodanih samo u SAD-u te se očekuje da će taj broj samo rasti. Dalje, procjenjuje se da će do 2025. godine biti prodano 115 milijuna povezanih automobila. Gotovo je nemoguće zamisliti vožnju automobila koji nije povezan s pametnim telefonom ili pruža mogućnost prometnih upozorenja u stvarnom vremenu.[23]

Međutim, kao i kod svakog drugog uređaja povezanim s internetom, postoji potencijalni rizik za sigurnost automobila od cyber kriminalaca. Kršenje sigurnosti može rezultirati „curenjem" osobnih podataka, prijetnjama osnovnim sigurnosnim mehanizmima vozila u ekstremnim slučajevima te potpunim daljinskim upravljanjem automobilom. Kao što je već prije rečeno, kako se industrija kreće prema autonomnijim vozilima, ovi rizici će se samo povećati zbog oslanjanja na aplikacije, povezanost na složenije i integrirane elektroničke komponente. Neuspjeh u rješavanju navedenih rizika može imati katastrofalan učinak na povjerenje potrošača, privatnost, reputaciji robne marke te najvažnije sigurnost kupca/korisnika.

Ključni rizici povezani s industrijskim IoT-om, uključujući:

- Otmica uređaja
- Sifoniranje podataka
- Napadi uskraćivanja usluge
- Kršenje podataka
- Krađa uređaja
- Čovjek u sredini ili zavaravanje uređaja[24]

U nastavku će biti objašnjena dva rizika;

[23] https://blogs.oracle.com/cx/post/iot-impacting-the-automotive-industry
[24] https://www.archonsecure.com/blog/what-are-the-risks-associated-with-industrial-iot

Otmica uređaja

Otmica uređaja događa se kada zlonamjerni akter preuzme kontrolu nad senzorom uređaja IoT krajnje točke, pritom često vlasnik nije svjestan da je došlo do napada. Ovisno o tome koliko su "pametni" krajnji uređaji otmica uređaja može varirati u glede toga koliko velik je rizik ili koliku predstavlja zabrinutost. U slučaju ako je krajnja točka ili IIoT(*eng. Industrial internet of things*) senzor ugrožen zlonamjernim softverom, napadač možda može kontrolirati aktivnost samog uređaja krajnje točke. Posebno je zabrinjavajuće ako ta krajnja točka ili uređaj imaju automatiziranu funkcionalnost, kontroliraju proizvodnju ili funkciju proizvoda povezanog s internetom na terenu. Može se često dogoditi ako korisnik ne uspije pravilno ažurirati svoje industrijske uređaje (IIoT). Također, početna točka može biti izložena napadu koji prati cijelu mrežu tako što počinje na krajnjoj točki i koristi taj uređaj za pristup centraliziranoj mreži. Mnogi se uređaji u proizvodnim pogonima ili unutar skladišta oslanjaju na stariju ili naslijeđenu tehnologiju koja se vrlo vjerojatno uopće neće moći ažurirati i zato njihovo povezivanje na mrežu otvara mnoga vrata na razini uređaja. Korištenje VPN rješenja temeljenog na hardveru često je jedini način da se osigura sigurnost i samom IoT uređaju, podacima ili informacijama koje prenosi što je isto tako kompatibilno sa starijom ili naslijeđenom tehnologijom.

Čovjek u sredini ili zavaravanje uređaja

Ovaj rizik uključuje mogućnost da se napadač smjesti između industrijskog IoT krajnjeg uređaja i oblaka ili centralizirane mreže pa se pretvara da šalje podatke kao uređaj. To povećava zabrinutost jer se promet koji dolazi iz uređaja krajnje točke može koristiti za promjenu informacija o proizvodnji ili kontroli uređaja na terenu. Primjerice proizvodnja vijaka, u slučaju da je napadač, koji se pretvarao da je IoT, poslao lažne informacije koje su uzrokovale da proizvodna oprema ili strojevi promijene kalibraciju ili proizvodne procese, to bi moglo rezultirati proizvodnjom neispravnih vijaka. U ovom slučaju, korištenje sigurnosnog rješenja temeljenog na hardveru može stvoriti korijen povjerenja, omogućujući središnjoj mreži da bez sumnje zna dolaze li informacije od stvarnog krajnjeg uređaja ili nekog drugog.

4. ZAKLJUČAK

Zbog brzog napretka razvoja tehnologije Interneta stvari nalazimo se u 4. industrijskoj revoluciji. Ona nam donosi razne benefite koje nam olakšavaju svakodnevan život. Međutim, zbog svoje prevelike uključenosti u naše živote izloženi smo cyber napadima. Što većim razvojem mreže pod većom smo izloženosti zato je potrebno konstantno razvijati mjere zaštite. Potrebno je osvijestiti poduzeća i privatne subjekte o riziku koja nam nosi primjena nove tehnologije. Razna poduzeća koriste zastarjele sustave pri čemu olakšavaju pristup neovlaštenim osobama u informacijski sustav. Posljedično, kao što je već navedeno, može doći do curenja podataka, krađe identiteta i raznih drugih podataka. Zbog loše zaštićenosti narušava se povjerenje korisnika, a time i reputacija poduzeća. Dakle, potrebno je izvršiti procjenu rizika, odrediti ranjivost, moguće prijetnje koje se mogu zloupotrijebiti u slučaju napada. U slučaju da dođe do na pada potrebno je procijeniti posljedice koje bi mogle nastati. Tvrtke koje nude i prodaju sigurnost odnosno *eng. Firewall* imaju za glavnu zadaću stalno testirati sigurnosni sustav. Problem je jer zaštita nije na zadovoljavajućem nivou te se nikad sa 100% sigurnošću ne može reći da je neki informacijski sustav siguran. Zbog toga napadima je najizloženiji zdravstveni sustav preko kojeg se može utjecati na zdravlje korisnika i može se doći do zdravstvenih podataka u kratkom roku.

Zaključno, potrebno je uložiti više novčanih sredstava, znanja i testiranja da bi se bolje zaštitili jer čemu nam ta napredna tehnologija ako to podrazumijeva život u nezaštićenom okruženju?

LITERATURA

1. Archon(2020), What are the Risks Associated with Industrial IoT (Industrial Internet of Things)?, [Internet], raspoloživo na: https://www.archonsecure.com/blog/what-are-the-risks-associated-with-industrial-iot (2.0702022.)
2. Carnet (2003.) : Upravljanje sigurnosnim rizicima [Internet], raspoloživo na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2003-10-44.pdf
3. Carnet(2019): Fizička zaštita informacijskih sustava, [Internet], raspoloživo na: http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf
4. Cisco(2016): Internet of Things, [Internet], raspoloživo na: https://emarsonindia.com/wp-content/uploads/2020/02/Internet-of-Things.pdf (1.06.2022.)
5. Cloudflare, Inc.(2022) : What is the cloud? | Cloud definition , [Internet], raspoloživo na: https://www.cloudflare.com/learning/cloud/what-is-the-cloud/ (2.06.2022.)
6. Fathi Ibrahim Salih1, Nur Azaliah Abu Bakar, Noor Hafizah Hassan, Farashazillah Yahya, Nazri Kama, Jalal Shah: IOT Security Risk Management Model for Healthcare Industry (Special Issue 2019), [Internet], raspoloživo na: https://ejournal.um.edu.my/index.php/MJCS/article/download/21469/10998/46267 (26.06.2022.)
7. Garača, Ž. (2009.): ERP sustavi, Sveučilište u Splitu Ekonomski fakultet, Split, str. 190. i 200.
8. Jessica Kaufman, Costumer Experience Blog(2021): Five ways IoT is impacting customer experience in the automotive industry, [Internet], raspoloživo na: https://blogs.oracle.com/cx/post/iot-impacting-the-automotive-industry (30.06.2022.)
9. Jusuf Šehanović, Željko Hutinski, Miroslav Žugaj(2002): Informatika za ekonomiste
10. Kim Zetteer(2014): An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Wired, [Internet], raspoloživo na: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
11. Lee, I. The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model. Internet Things Eng. Cyber Phys. Hum. Syst. Raspoloživo na: [Google Scholar] [CrossRef] (1.06.2022.)

12. Marriott International(2017): Marriott's agile, modern dana center environment elevates operations and guest experiences, [Internet]: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/customers/vmware-marriott-17q1-casestudy.pdf (15.06.2022.)
13. Mookyu Park, Haengrok Oh, Kyugho Lee, , MDPI open Access Journals (2014):
14. Ofir(2019): IoT ili Internet stvari, [Internet], raspoloživo na: https://www.ofir.hr/iot-ili-internet-stvari-2/ (1.06.2022.)
15. Prof. In Lee, MDPI open Access Journals(2020): Internet of Things (IoT) Cybersecurity, [Internet], raspoloživo na: https://www.mdpi.com/1999-5903/12/9/157/htm (11.06.2022.)
16. Radanliev, P.; De Roure, D.C.; Maple, C.; Nurse, J.R.; Nicolescu, R.; Ani, U. Cyber Risk in IoT Systems . Preprints (2019), [Internet], raspoloživo na: https://www.preprints.org/manuscript/201903.0104/v1 (7.06.2022.)
Security Risk Measurement for Information Leakage in IoT-Based Smart Homes from a Situational Awareness Perspective, [Internet], raspoloživno na: https://www.mdpi.com/1424-8220/19/9/2148/htm#B1-sensors-19-02148 (21.06.2022.)
17. Tomislav Bukavac(2016): Sigurnost informacijskih sustava, [Internet]. Zagreb: Sveučilište u Zagrebu, Filozofski fakultet. Raspoloživo na: http://darhiv.ffzg.unizg.hr/id/eprint/9366/1/Tomislav%20Bukovac_diplomski.pdf
18. U.S. Department of Homeland Security(2016): Strategic principles for securingthe Internet of things (IoT), [Internet], raspoloživo na: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL_v2-dg11.pdf
19. Versoaltima(2019): IoT i izazovi kibernetičke sigurnosti, [Inetnet], raspoloživo na: https://www.versoaltima.com/wp-content/uploads/2019/11/IOT-IGOR-GREGUREC.pdf (2.06.2022.)

SAŽETAK

U uvodnom dijelu rada govori se o samoj ideji IoT tehnologije i kako je razvoj tehnologije utjecao na digitalizaciju svakodnevnice pa tako i na produktivnost poslovanja. Definiran je i sam pojam pohranjivanja podataka u oblak. U glavnom dijelu detaljnije su opisani sigurnosni aspekti i pouzdanost IoT komunikacije. Zatim - način na koji mogu utjecati na bilo koju vrstu poslovanja i sigurnosnu politiku da bi se, u konačnici, što više smanjio sigurnosni rizik ili lakše upravljalo s njim. Razrađuje se i sam pojam sigurnosnog rizika, mogućnost smanjenja napada informacijskih sustava kao i eventualna sprječavanja zloupotrebe podataka preko snažnih lozinki ili nadogradnje uređaja. Dalje, govori se o industrijama koje su najranjivije na sigurnosne prijetnje i potencijalnoj procijeni rizika te koracima kroz koje se upravlja istim. U završnom dijelu je sve navedeno potkrijepljeno primjerima poput „pametnih“ soba s primjenom IoT tehnologije, „pametnih“ kuća, medicine i autoindustrije.

Ključne riječi: IoT tehnologija, sigurnost, rizik

SUMMARY

In the beginning, the idea of IoT technology was considered and how the development of technology has affected the digitization of everyday life, as well as productivity of business. Also, is defined the very concept of storage data in the Cloud. In the main part is explained more about security aspects and reliability of IoT communication. Then - the way in which they can influence any type of business and security policy to ultimately reduce the security risk as much as possible or manage it more easily. The very concept of security risk is being elaborated. Possibility of reducing attacks on information systems, as well as possible prevention of misuse of data through strong passwords or device upgrades. Next, it is alleged the industries that are most vulnerable to security threats, protentional risk assessment and the steps through which the same are managed. At the end, all of the above is supported by examples such as “smart” rooms with the application of IoT technology, "smart" houses, medicine and the auto industry.

Key words: IoT technology, safety, risk