Implementacija i upravljanje sigurnosnim protokolima u platformi e-Građani

Matošević, Antonio

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Economics and Business / Sveučilište u Zagrebu, Ekonomski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:148:733490

Rights / Prava: Attribution-NonCommercial-ShareAlike 3.0 Unported/Imenovanje-Nekomercijalno-Dijeli pod istim uvjetima 3.0

Download date / Datum preuzimanja: **2024-05-19**

Repository / Repozitorij:

REPEFZG - Digital Repository - Faculty of Economcs & Business Zagreb

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski studij poslovne ekonomije – smjer Menadžerska informatika

IMPLEMENTACIJA I UPRAVLJANJE SIGURNOSNIM PROTOKOLIMA U PLATFORMI E-GRAĐANI

Diplomski rad

Antonio Matošević

Zagreb, ožujak 2024.

Sveučilište u Zagrebu

Ekonomski fakultet

Integrirani preddiplomski i diplomski studij poslovne ekonomije –
smjer Menadžerska informatika

IMPLEMENTACIJA I UPRAVLJANJE SIGURNOSNIM PROTOKOLIMA U PLATFORMI E-GRAĐANI

IMPLEMENTATION AND MANAGEMENT OF SECURITY PROTOCOLS IN THE E-GRAĐANI PLATFORM

Diplomski rad

Student: Antonio Matošević

JMBAG studenta: 0067570174

Mentor: Prof. Dr. Sc. Mario Spremić

Zagreb, ožujak 2024.

SAŽETAK

Ovaj diplomski rad se bavi javnim središnjim državnim portalom e-Građani te sigurnosnim aspektima . Također, naglašava se važnost digitalizacije kao procesa uslijed koje je došlo do razvijanja digitalnih rješenja poput ove platforme. Cilj rada je opisati na koji način sama platforma djeluje, kako je moguće prijaviti se na istu te sve opasnosti i mjere zaštite koje bi pomogle pri radnjama koje su opasne i štetne za njezine korisnike. Obrađena je digitalizacija kao preduvjet za razvijanje modernih tehnologija i uvođenje u svakodnevni život građana. Napadi na informacijsku infrastrukturu i zaštitne mjere su detaljno objašnjene kako bi se rizik od nezakonitih radnji svela na najmanju moguću razinu. U drugom dijelu rada nalazi se intervju s tri stručne osobe koje imaju višegodišnje iskustvo rada s informacijskim sustavima i odlično su upoznati s mogućim ugrozama i zaštitnim mjerama koje se mogu provesti. Rad se zaključuje činjenicom da niti jedan informacijski sustav, pa tako ni platforma e-Građani, nije posve siguran. Provedbom zaštitnih mjera i podizanjem kolektivne svijesti korisnika, taj sigurnosni rizik bi se mogao svesti na najmanji mogući.

Ključne riječi: Platforma e-Građani, digitalizacija, vjerodajnica, mjere zaštite informacijskog sustava

SUMMARY

This master's thesis deals with the public central state portal e-Građani and its security aspects. It also emphasizes the importance of digitalization as a process that has led to the development of digital solutions such as this platform. The aim of the thesis is to describe how the platform itself operates, how it is possible to register on it, and all the dangers and protective measures that could help in actions that are dangerous and harmful to its users. Digitalization has been discussed as a prerequisite for the development of modern technologies and their introduction into citizens' everyday lives. Attacks on information infrastructure and protective measures are explained in detail to minimize the risk of unlawful actions. The second part of the thesis includes interviews with three experts who have years of experience working with information systems and are well-acquainted with potential threats and protective measures that can be implemented. The thesis concludes with the fact that no information system, including the e-

Citizens platform, is entirely secure. By implementing protective measures and raising the collective awareness of users, this security risk could be minimized as much as possible.

Keywords: e-Građani platform, digitalization, authentication, information system security measures

IZJAVA O AKADEMSKOJ ČESTITOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad isključivo rezultat mog vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju korištene bilješke i bibliografija.

Izjavljujem da nijedan dio diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog izvora te da nijedan dio rada ne krši bilo čija autorska prava.

Izjavljujem, također, da nijedan dio diplomskog rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(vlastoručni potpis studenta)

_____

(mjesto i datum)

STATEMENT ON THE ACADEMIC INTEGRITY

I hereby declare and confirm by my signature that the master's thesis is the sole result of my own work based on my research and relies on the published literature, as shown in the listed notes and bibliography.

I declare that no part of the master's thesis has been written in an unathorized manner, i.e., it is not transcribed from any non-cited work, and that no part of the thesis infringes any of the copyrights.

I also declare that no part of the thesis has been used for any other work in any other higher education, scientific or educational institution.

_____

(personal signature of the student)

_____

(place and date)

SADRŽAJ

1. UVOD

1.1. Predmet i cilj rada

Predmet rada *Implementacija i upravljanje sigurnosnim protokolima u platformi e-Građani* je prikazati način na koji općenito radi platforma e-Građani te postupak same prijave u nju. Tijekom postupka prijave i samog korištenja sustava diplomski rad donosi popis i objašnjenje sigurnosnih protokola koji su korišteni, od samog početka i odluke o pridruživanju platformi do internetske prijave i korištenja sustava i njegovih značajki. Sama platforma je nastala kao korak u modernizaciji društva, ali i potreba za objedinjavanjem svih usluga koji su potrebni građanima. Kako je riječ o vrlo povjerljivim i osobnim podacima, vrlo veliki naglasak kako u samoj platformi tako i u ovom radu je na sigurnosti. Sigurnost, kao jedan od kompleksnijih aspekata internetskog poslovanja je prikazano kroz sigurnosne provjere korisnika, identifikaciju korisnika te načine skladištenja i čuvanja korisnikovih podataka. Sekundarnim podacima iz stručnih i znanstvenih istraživanja, knjiga, članaka i drugih izvora prikazuju se vrste sigurnosnih protokola te kako se ti protokoli implementiraju i konkretno koriste u platformi e-Građani. Diplomski rad čitatelju približava i dodatno pojašnjava kako sami sustav funkcionira, sve njegove prednosti koje su zaista velike, te moguće nedostatke na koje isto tako treba obratiti pozornost. Treba naglasiti da su podaci vidljivi samo korisniku i pružatelju usluga te nikakve treće strane nisu uključene u njihov interaktivni proces.

Naposlijetku će se provesti istraživanje pomoću intervjua u kojem će svoj sud dati troje iskusnih sigurnosnih stručnjaka o samoj platformi e-Građani te njenoj sigurnosti. Također, reći će nešto općenito o stanju u svijetu na tu temu i svoje stavove vezane uz to.

Cilj ovog rada je analizirati, komentirati i diskutirati o sigurnosnim protokolima koji se primjenjuju unutar platforme e-Građani kako bi se osigurala zaštita korisničkih podataka, privatnosti i integriteta sustava. Neki od specifičnih ciljeva su pregledati sigurnosne protokole koji se primjenjuju te identificirati njihove prednosti i nedostatke, istaknuti primjere konkretnih sigurnosnih protokola koji se primjenjuju na platformi e-Građani. Također, cilj je olakšati sugrađanima korištenje platforme i prikazati sve njene dobre i loše strane, ako ih ima.

1.2. Metode istraživanja i izvori podataka

Metode kojima su dokazani ciljevi su različite. Pregledom literature je proveden opsežan pregled relevantne literature i njime je usvojeno dublje znanje i razumijevanje sigurnosnih protokola na platformi e-građani. Dubljom analizom su identificirani sigurnosni protokoli i njihove snage, slabosti te mogućnost nekakvog poboljšanja koje bi imao utjecaj na sigurnost podataka građana i zaštitu korisničkih računa i povjerljivih dokumenata. Sintezom podataka i informacija se dobila cjelovita slika o trenutnom stanju te bi se definirale smjernice za daljnji razvoj iste. Kroz istraživanje je napravljen intervju sa tri stručne osobe za informacijsku sigurnost koje su odgovarale na postavljena pitanja u vezi platforme i njezine sigurnosti. Kombinacija ovih metoda omogućila je provedbu sveobuhvatnog istraživanja sigurnosnih protokola unutar platforme e-Građani te dokazivanje ciljeva istraživanja postavljenih u radu.

Za potrebe rada su korišteni sekundarni podaci koji su prikupljeni iz različitih znanstvenih i stručnih istraživanja, knjiga, publikacija, znanstvenih članaka, internetskih baza podataka te internetskih stranica. Kao jedan od ključnih izvora podataka je naravno i sama platforma e-Građani.

1.3. Sadržaj i struktura rada

Ovaj diplomski rad sadrži sljedeće komponente:

U prvom poglavlju donosi se kratki uvod u temu i ciljevi rada, te nakon toga drugo poglavlje započinje definiranjem digitalizacije općenito s opisima digitalizacije u Hrvatskoj i prikaz portala e-Građani u okviru digitalizacije. Nadalje, treće poglavlje donosi pregled platforme e-Građani, korisnike i katalog usluga, te razine sigurnosti platforme i vrste vjerodajnica kojima se korisnici mogu prijavljivati u sustav. U četvrtom poglavlju se govori općenito o informacijskim sustavima te mogućim prijetnjama unutar njih. Nacionalni centri poput CERT-a i SK@UT-a su okosnica cyber sigurnosti u RH. Također, objašnjavaju se pojmovi poput vektora napada, učinka napada na informacije, objekta napada i dosegnute faze napada. U petom poglavlju je naglasak na mjerama zaštite informacijskog sustava i načinima identifikacije informacijskom sustavu. Šesto poglavlje donosi SWOT analizu, a posljednje poglavlje donosi intervju s tri stručne osobe za informacijsku sigurnost koji pomažu približiti materiju čitatelju i razjasniti određene nejasnoće, te svojim stručnim mišljenjem pridonijeti boljem razumijevanju teme čitateljima.

U završnom dijelu rada, u Zaključku, se donosi pregled rada i izvode se zaključci iz svih navedenih poglavlja.

2. DIGITALIZACIJA

2.1. Digitalizacija društva

Preduvjet digitalnim tehnologijama je internet. Internet je pokretač novih tehnologija koje mijenjaju svijet koji poznajemo iz dana u dan. Razvoj novih tehnologija eksponencijalno raste i tome se ne nazire kraj. Pristup internetu i novim tehnologijama je danas potreba, a ne luksuz kao u neka prošla vremena.

Koliko je digitalizacija važan i neizbježan proces objašnjava Spremić (2017.a) u svojoj knjizi „*Digitalna transformacija poslovanja"* gdje navodi krilaticu „digital or die" te na taj način stavlja veliki naglasak na imperativnu digitalizaciju poslovanja da bi poslovanje bilo održivo i konkurentno. Naravno, nije samo naglasak na poslovanju kada govorimo o digitalizaciji, već o općoj promjeni pristupa na koje smo navikli. Prije tridesetak godine je bilo potpuno nezamislivo iz udobnosti svoga doma pohađati nastavu, naručivati lijekove, prijaviti fakultetski ispit ili pak predati zahtjev za novom osobnom iskaznicom. Danas zahvaljujući tehnološkom napretku je sve to moguće i društvo se polako, ali sigurno adaptira i prihvaća u svoj život nove tehnologije koje čine život jednostavnijim. Međutim, postoje oni koji se pitaju koliko uistinu je digitalizacija statistički važna za razvoj gospodarstva (Mammadli, Klivak, 2020.).

U Republici Hrvatskoj prema nacionalnoj razvojnoj strategiji (2024.) u digitalnoj tranziciji društva i gospodarstva postoje prioritetna područja javnih politika:

1. Digitalna tranzicija gospodarstva
2. Digitalizacija javne uprave i pravosuđa
3. Razvoj širokopojasnih elektroničkih komunikacijskih mreža
4. Razvoj digitalnih kompetencija i digitalnih radnih mjesta

Prema DESI indeksu gospodarske i društvene digitalizacije ciljana vrijednost je dostići prosjek zemalja članica Europske Unije do 2030. godine. Početna vrijednost Republike Hrvatske je iznosila 47,6 (2020.), a ciljani prosjek EU iznosi 50,7 (Nacionalna razvojna strategija, 2024.)

Proces stvaranja e-uprave bi se trebao provoditi prema nekoliko faza. U prvoj fazi je uspostavljena službena vladina online prisutnost. U drugoj fazi informacije postaju dinamičnije i redovito se ažuriraju te postoje obrasci, dokumenti i značajke koje se mogu preuzeti na web stranicama. U trećoj fazi korisnici mogu slati obrasce na e-mail službenicima, komunicirati putem weba, također se pojavljuju specijalizirane baze podataka. Četvrta faza donosi plaćanje usluga i drugih transakcija na siguran način online putem. Zadnja faza je potpuna integracija e-usluga. Pristup i povezivanje se obavlja putem središnjeg državnog portala i sve transakcije se nude putem središnje integrirane stranice (Spremić, Šimurina, Jaković & Ivanov, 2009.).

2.2. Digitalna ekonomija

Pojam digitalne ekonomije služi kao krovni pojam za označavanje novih modela poslovanja, proizvoda, usluga, tržišta i brzorastućih sektora ekonomije, posebice onih koji se temelje na digitalnim tehnologijama kao osnovnoj infrastrukturi poslovanja (Spremić, 2017.a). Temelj digitalne ekonomije su praćenje novih trendova i implementacija novih tehnologija koje omogućuju veću efikasnost i bolje rezultate sa sve manje uložene ljudske radne snage. Digitalna transformacija je postala prioritet u svim razvijenim zemljama. Jedno od istraživanja utvrđuje kako 90% poslovnih lidera iz SAD-a i UK-a smatra da će IT i digitalne tehnologije imati veći strateški doprinos u ukupnom poslovanju (Spremić & Šimunic, 2018.). Smanjenje mogućnosti operativnih pogrešaka i usmjeravanje radne snage prema kreativnim zadacima može povećati njenu učinkovitost, a sve zbog rasta produktivnosti rada uoči smanjivanja potrebe za ljudskom radnom snagom u obavljanju rutinskih poslova (Franc, Bilas & Bošnjak, 2021.). Cijeli koncept digitalne ekonomije se prema Spremiću (2017.a) zasniva na idućim principima:

1. Integraciji i istodobnoj primjeni neovisno razvijenih tehnologija i mogućnosti koje one pružaju - komunikacija i informacijska tehnologija (softver, hardver, društvene mreže, robotika, virtualna stvarnost itd.)
2. Integraciji progresivnih koncepcija poslovanja
3. Korištenju digitalnih platformi poslovanja - procesi koji su digitalizirani i povezani te omogućuju brzu i efikasnu provedbu poslovnih transakcija
4. Uspješnim i “neodoljivim” digitalnim poslovnim modelima
5. Vođenju temeljenom na poduzetničkoj organizacijskoj kulturi, inovativnosti i stvaranju nove vrijednosti (digitalno vođenje).

2.3. Digitalizacija u Hrvatskoj

Digitalizacija društva je jedan od temeljnih ciljeva dugogodišnje kampanje Nacionalne razvojne strategije do 2030. godine Vlade Republike Hrvatske. Vodeći ljudi u Hrvatskoj svakodnevno naglašavaju važnost digitalizacije i promicanje zapadnih stavova i vrijednosti. „Naši mladi prvi su u Europskoj uniji po osnovnim digitalnim vještinama, to je dosta bitna prednost“ (Vlada Republike Hrvatske, 2023.). Perspektiva je velika, pogotovo što se tiče mladih ljudi, samo je bitno dodatno i konstantno pratiti svjetske trendove i biti u korak koliko je moguće s najrazvijenijim svjetskim zemljama.

Hrvatska je jedna od prvih članica Europske Unije koja je uvela elektroničku osobnu iskaznicu (eOI) novije generacije sa značajnim zaštitama i elektroničkom komponentom digitalnih certifikata koja ujedno služi kao zdravstvena iskaznica (Vlada Republike Hrvatske, 2023.).

Svjetska ljestvica digitalne konkurentnosti koja u obzir uzima tri faktora: znanje, tehnologiju i spremnost za budućnost koju provodi IMD (Institute of Management Development) svrstala je Hrvatsku na 43. mjesto od ukupno 63 vodeće svjetske ekonomije. Po znanju smo na 40. mjestu ljestvice, u tehnologiji na 42. mjestu, a u spremnosti za budućnost na 48. mjestu.

Također jedna od prednosti ulaska Hrvatske u Europsku Uniju 2013. godine je pristup i iskorištavanje europskih fondova koji su uvelike ubrzali i potpomogli digitalizaciji Hrvatske, a ta sredstva mogu povući i mali poduzetnici putem “vaučera za digitalizaciju”.

2.4. Portal e-Građani u okviru digitalizacije

Prema podacima Vlade Republike Hrvatske (2023.) portal koji je namijenjen građanima i poduzetnicima koristi gotovo 1,8 milijuna hrvatskih građana, a sustav koji nudi više od 100 različitih usluga putem interneta je korišten 140 milijuna puta.

„Pandemijske“ godine koje su iza nas nisu imale previše dobrih strana, ali jedna od njih je svakako osjetno povećanje prometa i korisnika platforme e-Građani. Izolacija i zatvorenost u svojim domovima je za posljedicu imala da se građani moraju snaći na neki način te su možda bili primorani koristiti usluge platforme i na taj način uštedjeli vrijeme u budućnosti jer su uvidjeli da je digitalizacija uistinu korisna.

3. PREGLED PLATFORME E-GRAĐANI

3.1. Opis i mogućnosti platforme

Platforma e-Građani je digitalna platforma koju je razvila Vlada Republike Hrvatske i koja je implementirana u lipnju 2014. godine. Platforma zadire u sve aspekte građana Republike Hrvatske i kao takva je korak naprijed u modernizaciji i digitalizaciji društva kojoj Hrvatska teži. Spremić (2017.a) nam opisuje kako digitalna transformacija poslovanja donosi intenzivnu primjenu digitalnih tehnologija i digitalnih resursa u svrhu stvaranja novih prihoda, novih modela i općenito novih načina poslovanja. Upravo ta digitalna transformacija je bila ključna za početak rada ove platforme.

Platforma je skup različitih usluga koje su prije modernizacije građani morali osobno, fizički podnositi u različitim institucijama i uredima. Sada sve te usluge su dostupne na jednom mjestu, bez čekanja u redovima i gubljenju vremena. Jedan od glavnih ciljeva je pojednostaviti građanima pristup javnim uslugama na način da svaki građanin ima svoje korisničke podatke koji su samo njemu poznati i pomoću njih dolazi do željenih sadržaja, dokumenata, potvrda itd.

Mogućnosti platforme su skoro pa neograničene. Tu tvrdnju potkrjepljuje činjenica da je na samom početku bilo nekoliko ponuđenih usluga, a danas se dijele u čak 12 velikih područja (obitelj i život, pravna država i sigurnost, odgoj i obrazovanje, promet i vozila, aktivno građanstvo, prava potrošača, financije i porezi, zdravlje, rad, poslovanje, stanovanje i okoliš te hrvatski branitelji).[1]

3.2. Usluge platforme

3.2.1. Korisnici usluga

Usluge platforme e-Građani mogu koristiti svi hrvatski državljani, državljani EU/EEA s boravištem u Hrvatskoj, državljani zemalja izvan EU s boravištem u Hrvatskoj, digitalni nomadi (državljanin treće zemlje to jest osoba koja nema državljanstvo EPG-a ili Švicarske Konfederacije, koji je zaposlen ili obavlja poslove putem komunikacijske tehnologije za tvrtku ili vlastitu tvrtku koja nije registrirana u Republici Hrvatskoj i ne obavlja poslove ili pruža

[1] Središnji državni portal (b.d.), Katalog usluga, preuzeto 19. ožujka 2024. s https://gov.hr/hr/katalog-usluga/10

usluge poslodavcima na području Republike Hrvatske (Ministarstvo unutarnjih poslova, 2024.) i državljani EU preko čvora za prekograničnu suradnju.

3.2.2. Struktura platforme

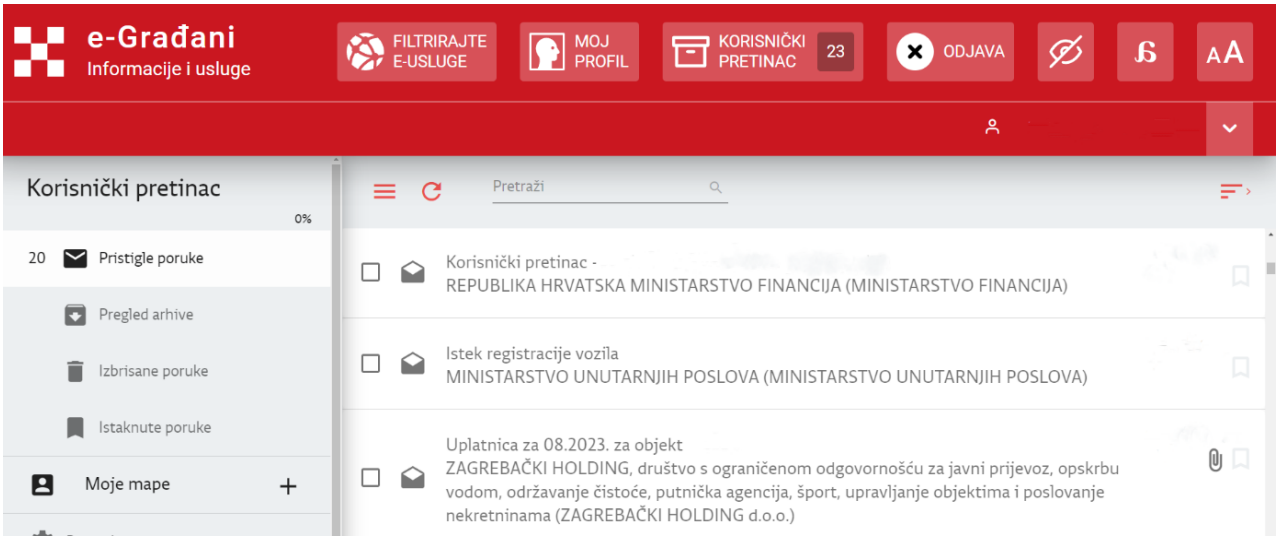
Problem koji je riješen pojavom platforme e-Građani 2014. godine je raspršenost usluga koje nisu bile objedinjene na jednom mjestu te su doprinosile i bile korisne građanima u puno manjoj mjeri nego što je to slučaj danas.

Danas se sustav dijeli na tri područja:

1. **Osobni korisnički pretinac**

   Korisnički pretinac je jedna od usluga portala e-Građani koja omogućava primanje službenih poruka vezanih uz javne usluge, dobivanje računa, podsjetnika za razne stvari koje su nam bitne (istek registracije automobila), obavijesti raznih ministarstava, HZMO-a, REGOS-a, HZZ-a, HZJZ-a itd.

Slika 1. Osobni korisnički pretinac



Izvor: Središnji državni portal, 2024.

2. **Nacionalni identifikacijski i autentifikacijski sustav (NIAS)**

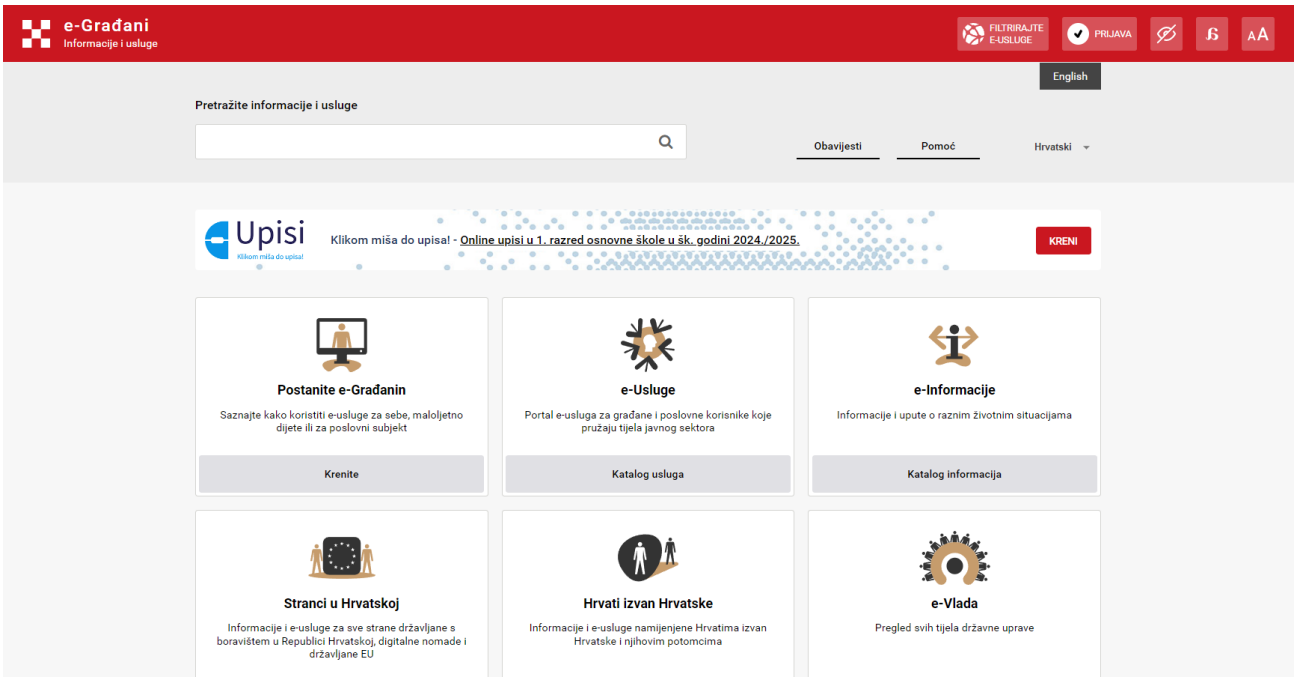
   NIAS je sustav koji predstavlja središnje mjesto identifikacije i autentifikacije korisnika prilikom prijave na e-uslugu. Temeljna mu je funkcija sigurno i pouzdano pružanje usluge elektroničke identifikacije i autentifikacije korištenjem vjerodajnice. Vjerodajnica je sredstvo dokazivanja (prepoznavanja) elektroničkog identiteta (npr.

korisničko ime/lozinka, token na mobilnom telefonu, digitalni certifikat i sl.). Vjerodajnica služi kao sredstvo prijave na elektroničku uslugu.[2]

3. Središnji državni portal

Na središnjem državnom portalu se nalaze sve usluge koje platforma nudi na jednom mjestu. Na taj način je Vlada Republike Hrvatske riješila problem građana koji nisu mogli pronaći određene usluge, a sada je sve spojeno na jednom mjestu. Osim jednostavnijeg korištenja za građane, jednostavnije je održavanje usluga u sigurnosnom i informatičkom smislu.

Slika 2. Sučelje središnjeg državnog portala



Izvor: Središnji državni portal, 2024.

3.2.3. Katalog usluga

U katalogu usluga na stranici Središnjeg državnog portala se nalaze sve usluge koje e-Građani nude te su podijeljene u 12 kategorija.

[2] Središnji državni portal (b.d.), Katalog usluga, preuzeto 19. ožujka 2024. s https://gov.hr/hr/katalog-usluga/10

Tablica 1. Popis usluga platforme e-Građani

Područje	
Obitelj i život	- e-Novorođenče (3.) - e-Dječja kartica (2.) - e-Prijava vjenčanja (2.) - e-Prijava životnog partnerstva (2.) - Potvrde iz registra osoba s invaliditetom (2.) - e-Matične knjige (1.) - e-usluge grada Bjelovara (1.) - e-Usluge socijalna skrb (1.) - Kalkulator doplatka za djecu (1.)
Pravna država i sigurnost	- e-prijava boravišta hrvatskih državljana (3.) - e-Zahtjev za izdavanje putovnice (3.) - Suglasnosti i punomoći u postupcima djelokruga MUP-a (3.) - e-Ovrhe (2.) - e-Upravni postupak (2.) - Izdavanje elektroničke isprave Grada Zagreba (2.) - e-Birači (1.) - e-Usluge MUP-a (1.) - Korisnički pretinac (1.) - Moj profil (1.) - Registar birača (1.) - Uvjerenje da se ne vodi kazneni postupak (1.) - Uvjerenje iz kaznene evidencije (1.)
Odgoj i obrazovanje	- e-Dnevnik za roditelje (1.) - ePodnesak Ministarstva znanosti i obrazovanja (1.) - e-Razmjena studentskih ocjena (1.) - e-Upisi u odgojno-obrazovne ustanove (1.) - e-Zapis o statusu studenta (1.) - Home for Homeless servis sustava AAI@EduHr (1.) - Online Tečajevi Srca (1.)

	- Prijava na diplomske studijske programe (1.)
Promet i vozila	- eTahograf (3.) - e-Zahtjev za izdavanje vozačke dozvole (3.) - Dostava elektroničkih isprava za registraciju vozila u Republici Hrvatskoj (2.) - Obavijest o prekršaju u prometu (2.) - Otočna iskaznica (2.) - Porezna prijava za obračun i plaćanje posebnog poreza na motorna vozila (2.) - e-Nautika (1.) - ePlovilo (1.) - Registracija operatora bespilotnih zrakoplova (1.)
Aktivno građanstvo	- Moja e-Kultura (2.) - e-Prijavnice Ministarstva kulture i medija (1.) - e-Savjetovanja (1.) - MojZagreb (1.) - Registri neprofitnih pravnih osoba (1.)
Prava potrošača	- Prava potrošača
Financije i porezi	- SKDD e-Ulagatelj (2.) - e-Dugovanja (e-Blokade) (1.) - ePorezna (1.) - e-Pristojbe (1.) - Moj OIB (1.)
Zdravlje	- EU digitalna COVID potvrda (2.) - Portal zdravlja (2.) - eHZZO (1.)
	- Mirovinsko osiguravajuće društvo (3.) - Obvezni mirovinski fond (3.) - Odabir mirovine (mirovina samo iz I. stupa ili mirovina iz I. i II. stupa) (3.)

Rad	- e-Osiguranje radničkih tražbina (2.) - e-Usluge HZMO-a (2.) - Burza rada (1.) - Elektronički zapis o radno pravnom sustavu (e-radna knjižica) (1.) - e-Pomorac (1.) - e-Usluge Središnjeg registra osiguranika – REGOS (1.) - Korisničke stranice HZMO-a (1.) - Moj račun - REGOS (1.) - Moja mirovina (1.) - Ostvarivanje prava u sustavu sporta (1.) - Postupci vezani uz članstvo Hrvatske komore psihoterapeuta (1.)
Poslovanje	- e-Ovlaštenja (3.) - Prijava patenata i uporabnog modela (3.) - Registar revizora (3.) - Registar stvarnih vlasnika (3.) - Registracija žiga i industrijskog dizajna (3.) - e-Autoškole (2.) - eTurizam (2.) - e-Visitor (2.) - Kalendar plaćanja obveznih naknada (2.) - Postupci vezani uz članstvo Hrvatske komore arhitekata (2.) - Postupci vezani uz članstvo u Hrvatskoj komori inženjera elektrotehnike (2.) - Postupci vezani uz članstvo u Hrvatskoj komori inženjera građevinarstva (2.) - Postupci vezani uz članstvo u Hrvatskoj komori inženjera strojarstva (2.) - Postupci vezani uz članstvo u Hrvatskoj komori ovlaštenih inženjera geodezije (2.)

	- Registar poreznih savjetnika (2.) - Registar profesije iz nadležnosti Ravnateljstva civilne zaštite (2.) - START Plus (2.) - e-Obrt (1.) - e-Zahtjev za izdavanje vodopravnih akata (1.) - Prijava polaganja stručnog ispita za obavljanje stručnih geodetskih poslova (1.) - Priznavanje inozemnih stručnih kvalifikacija (1.) - Registracija objekata koji pružaju uslugu smještaja strancima (1.) - Uvid u registar stvarnih vlasnika (1.) - Zastupanje i kolektivno ostvarivanje prava intelektualnog vlasništva (1.)
Stanovanje i okoliš	- eGrađevinska dozvola i druge usluge u gradnji (3.) - e-Konzervatorska lokacijska informacija (2.) - eObnova (2.) - Moja mreža – HEP Operatora distribucijskog sustava (2.) - Geoportal Jaska (1.) - Jedinstvena informacijska točka – Sustava katastra infrastrukture (1.) - Komunalne usluge i naknade (1.) - Moj račun – Gradska plinara Zagreb - Opskrba (1.) - Vodne usluge Međimurskih voda (1.) - Zajednički informacijski sustav zemljišnih knjiga i katastra – ZIS OSS (1.)
Hrvatski branitelji	- Predaja zahtjeva hrvatskih branitelja i članova obitelji (1.)

Izvor: Obrada autora prema Središnji državni portal, 2024.

3.3. Vrste sigurnosti i vjerodajnice

Nacionalni identifikacijski i autentifikacijski sustav (NIAS) je središnji sustav za prijavu korisnika koji mora zadovoljiti sigurnosne standarde zbog sigurnosti samih korisnika sustava koja je na prvom mjestu.

3.3.1. Razine sigurnosti

Prema kriterijima koje su odredili informatički stručnjaci koji su radili na sigurnosti portala i u skladu s europskim direktivama i , određene su tri razine sigurnosti[3]:

- **Niska razina sigurnosti**
- **Značajna razina sigurnosti**
- **Visoka razina sigurnosti**

3.3.2. Način prijave u sustav

Odabirom web adrese Središnjeg državnog portala, korisnik dolazi na naslovnu stranicu. Ako se korisnik želi prijaviti u sustav, odabire „Prijava“. Nakon toga odlučuje koju razinu sigurnosti će odabrati s obzirom na to koju uslugu portala e-Građani želi koristiti. Ako odabire Nisku razinu sigurnosti, jedna od opcija je **ePASS** koji omogućuje prijavu u sustav starijima od 15 godina pomoću korisničkog imena i lozinke. Ako se korisnik odluči prijaviti u sustav Značajnom razinom sigurnosti, **mToken** je jedna od opcija. To je vjerodajnica koja omogućuje pristup portalu pomoću mobilne aplikacije koja služi za generiranje jednokratnih lozinki. Ako je korisniku potrebna Visoka razina sigurnosti, odabire **eOsobnu iskaznicu** (eOI) i umetanjem osobne iskaznice u čitač pristupa sustavu i usluzi koju je odlučio koristiti.

[3] Središnji državni portal (b.d.), Katalog usluga, preuzeto 19. ožujka 2024. s https://gov.hr/hr/katalog-usluga/10

3.3.3. Vjerodajnice

Tablica 2. Popis vjerodajnica i razina sigurnosti

Niska razina sigurnosti (1.)	Značajna razina sigurnosti (2.)	Visoka razina sigurnosti (3.)
▪ ePASS ▪ AAI@EduHr ▪ ePošta ▪ HT Telekom ID	▪ HZZO pametna kartica ▪ mToken ▪ HPB token ▪ FINA soft certifikat ▪ ZABA token ▪ PBZ token ▪ RBA token ▪ KentBank token ▪ OTP banka d.d. token ▪ Erste token ▪ Addiko Bank token ▪ Istarska kreditna banka Umag d.d. token ▪ Certilia osobni sms.ID ▪ Certilia poslovni sms.ID ▪ Agram banka token	▪ eOsobna iskaznica ▪ Mobile ID osobne iskaznice ▪ FINA RDC osobni certifikat ▪ FINA RDC poslovni certifikat ▪ Certilia osobni certifikat ▪ Certilia poslovni certifikat

Izvor: Obrada autora prema Središnji državni portal, 2024.

4. INFORMACIJSKI SUSTAV I PRIJETNJE

„Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tada, ne bih se baš kladio na njega.“ (Spremić, 2017.b prema Eugene Spafford, director Computer Operations, Audit and Security Technology, COAST)

Ovaj citat nam najbolje govori da jednostavno nije moguće u potpunosti zaštiti informacijski sustav toliko dobro da on ne može biti kompromitiran. Razvojem interneta, informacijskih sustava i ostalih digitalnih tehnologija, sigurnost ima vrlo bitnu ulogu u provedbi svih zamišljenih radnji. Kako su se razvijale nove tehnologije koje pozitivno utječu na naš životni standard, tako su se usporedno razvijali sustavi koji za cilj imaju kompromitirati sustave, krađu osobnih podataka, kartičnih informacija, povjerljivih podataka, stručnih analiza, poslovnih modela i tako dalje. Širenjem mreža i galopirajućom digitalizacijom, informacije organizacija su ranjivije nego ikad prije i izložene sve većim prijetnjama. Prema mnogim istraživanjima ljudski je faktor “najslabija karika” informacijske sigurnosti (Arbanas, Spremić & Žajdela Hrustek, 2021.).

Spremić (2017.b) cyber rizike definira na sljedeći način: “poslovni rizici koji proizlaze iz intenzivne uporabe informacijskih sustava i tehnologije u okruženju digitalne ekonomije kao važne podrške odvijanju i unapređenju poslovnih procesa i poslovanja uopće.” Ti rizici se odnese na to da intenzivna primjena informacijske tehnologije može dovesti do neželjenih ili neočekivanih posljedica te tako može nastati financijska ili materijalna šteta. Šteta može biti izravna ili neizravna. Informatički rizici su uvijek prisutni, bez obzira je li ih kompanija svojim mehanizmima korporativnog upravljanja informatikom otkrila i prihvatila ili nije, a ovladavanje tim rizicima predstavlja prilične izazove u dostizanju strateških ciljeva poslovanja (Spremić, 2017.b).

Autor Roman V. Veresha (2018.) u svom radu: ”Preventive measures against computer related crimes: approaching an individual” uspoređuje zemlje s najviše “zaraženih” računala različitim kompromitirajućim sadržajima u svijetu. Kina predvodi ljestvicu, ali u negativnom smislu jer ima najviše takvih računala, čak 57,2 %, što nam govori kako je svako drugo računalo na neki način kompromitirano. Na drugom mjestu je Tajvan s 49,15 %, a treće mjesto je zauzela Turska s 42,52 %. Listu najsigurnijih zemalja čine skandinavske zemlje Finska s

20,32 %, Norveška s 20,51% i Švedska (20,8 %). Ovako dobre rezultate, ove zemlje mogu pripisati učinkovitijim mjerama zaštite računala općenito i podataka na njima, blokiranje određenih stranica koje mogu uzrokovati probleme od strane vlasti te većom informiranošću samih korisnika računala, na koji način pristupiti određenim sadržajima. Također, Spremić (2013.) opisuje kako informacijski sustav može utjecati na konkurentnost na dva različita načina, prvi je podržavanje operativne učinkovitosti, a drugi diferenciranje poslovanja kroz inovaciju poslovnog modela i primjenu poslovnih procesa. Ekonomska vrijednost od informacijskih sustava nastaje kada se kreiraju stvari koje prije nisu postojale.

4.1. Nacionalni CERT

CERT (eng. Computer Emergency Response Team) je organizacija koja reagira na računalno-sigurnosne incidente i pokušava ih pravovremenim djelovanjem prevenirati te radi na poboljšanju računalne sigurnosti informacijskih sustava. Osnovan je 2007. godine temeljem *Zakona o informacijskoj sigurnosti Republike Hrvatske* kao nacionalno tijelo za prevenciju i zaštitu od sigurnosnih ugroza. Nacionalni CERT je nadležan za pet sektora temeljem *Zakona o kibernetičkoj sigurnosti (NN 14/24)*. Sektori su: bankarstvo, infrastruktura financijskog tržišta, digitalna infrastruktura, istraživanja te sustav obrazovanja[4].

Proaktivne mjere koje provodi CERT su[5]:

- sigurnosne preporuke
- praćenje računalno-sigurnosnih tehnologija
- diseminacija informacija iz područja nacionalne sigurnosti
- unapređenje svijesti o značaju računalne sigurnosti
- edukacija i obuka o računalnoj sigurnosti
- provjera ranjivosti za ustanove članice CARNET-a
- izdavanje elektroničkih certifikata za ustanove članice CARNET-a

[4] Središnji državni portal (b.d.), Katalog usluga, preuzeto 20. ožujka 2024. s https://gov.hr/hr/nacionalni-cert/1230?lang=hr

[5] Središnji državni portal (b.d.), Katalog usluga, preuzeto 20. ožujka 2024. s https://gov.hr/hr/nacionalni-cert/1230?lang=hr

- sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacije koje pristupaju sustavu eMatica

Reaktivne mjere su:

- sigurnosna upozorenja
- postupanje s računalno-sigurnosnim incidentima
- koordinacija rješavanja značajnih incidenata

4.2. Sustav SK@UT

Nacionalni kibernetički prostor je u modernim vremenima jedan od najosjetljivijih sektora neke države. Sustav SK@UT je projekt zaštite kibernetskog prostora kojeg su izgradili Sigurnosno-obavještajna agencija i Zavod za sigurnost informacijskih sustava. Cilj sustava je otkrivanje, rano upozorenje i zaštita od sponzoriranih kibernetičkih napada, naprednih ustrajnih kampanja i drugih kibernetičkih ugroza. Ove odluke su definirane odlukom Vlade Republike Hrvatske 2021. godine. Ovaj sustav predstavlja nacionalni „kibernetički kišobran“ koji trenutno pokriva više od 60 % državnih tijela, operatora ključnih usluga i pravnih osoba od posebnog interesa za Republiku Hrvatsku (SKAUT, Zaštita nacionalnog kibernetičkog prostora, 2024.)

4.3. Nacionalna taksonomija Republike Hrvatske

Nacionalna taksonomija je izrađena korištenjem javno dostupne taksonomije razvijene u SAD-u. Prilikom obrade u obzir su uzeta iskustva i specifičnosti računalno-sigurnosnih incidenata u Hrvatskoj (Nacionalna taksonomija računalno-sigurnosnih incidenata, 2021.).

Akronim **VOUND** dobiven je korištenjem početnih slova ključnih atributa predloženih za opis računalno- sigurnosnih incidenata u Republici Hrvatskoj:

- **V**ektor napada
- **O**perativni učinak napada
- **U**činak napada na informacije
- Objekt **N**apada
- **D**osegnuta faza napada (Nacionalna taksonomija računalno-sigurnosnih incidenata, 2021.)

4.3.1. Vektor napada

Vektor napada opisuje način na koji napadač ostvaruje inicijalni pristup računalu odnosnu sustavu. Nekada identifikacija atributa Vektor napada može predstavljati izazov kod napada

visokog stupnja kompleksnosti jer napadači prikrivaju korake napada (Nacionalna taksonomija računalno-sigurnosnih incidenata, 2021.).

Napadi i načini izvođenja prema Nacionalna taksonomija računalno-sigurnosnih incidenata, (2021.) mogu biti sljedeći:

- **Prijenosni mediji/uređaji**

Širenje zlonamjernog koda putem zaraženog USB-a ili CD/DVD-a

- **Napad na web tehnologije**

XSS

Napad gdje napadač umetne u ranjivu web stranicu ili aplikaciju skript koji preusmjeri korisnika na zlonamjerne web stranice i prikupi osjetljive informacije.

SQL Injection

Umetanje zlonamjernog SQL koda pomoću SQL upita i kada se taj kod izvrši, može doći do brisanja, krađe ili izmjene sadržaja u bazama podataka ili čak preuzimanja kontrole nad aplikacijom. Jedno od mogućih rješenja je poboljšanje tehnike programiranja (Boyd & Keromytis, 2004.).

DNS Hijacking

Napadač manipulira DNS postavkama kako bi preusmjerio promet s legitimnih web stranica na zlonamjerne web stranice. Budući da je odgovornost domene dodijeljena vlasnicima, nitko ne može vidjeti promjene DNS zapisa i na taj način se teže detektira ova vrsta napada (Houser, Hao, Li, Liu, Cotton & Wang, 2021.).

Brute force napadi

Različitim metodama napadači pokušavaju dešifrirati podatke poput lozinki ili ključeva enkripcije. Isprobavaju sve moguće kombinacije dok ne nađu ispravnu.

Spremić (2017.) utvrđuje da su napadi grubom silom nasumice isprobavanje različitih lozinki, sve dok ne pronađu pravu, a napad pomoću rječnika (eng. dictionary attack) za neovlašteni ulaz koristi algoritam rječnika često korištenih izraza.

- **Napad na dostupnu mrežnu i računalnu opremu**

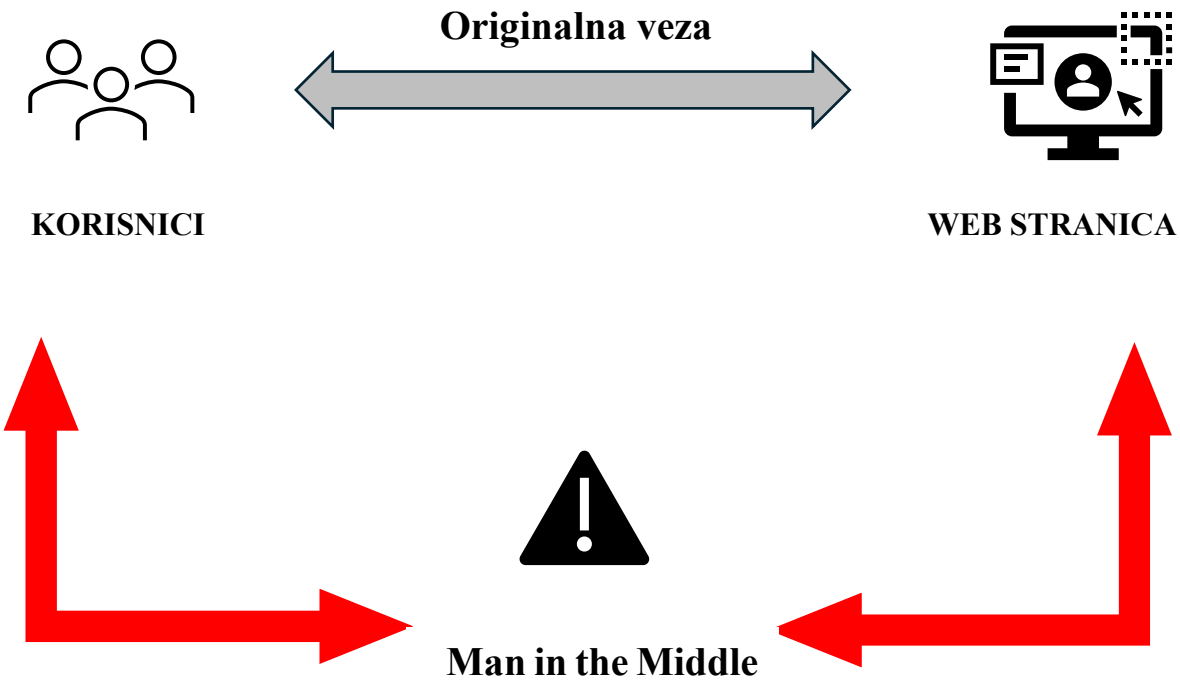
(D)DoS

DoS se odnosi na nedopuštene aktivnosti sprječavanja ili onemogućavanja ovlaštene uporabe računalne mreže, sustava ili programa iskorištavanjem njihovih resursa (procesor, memorija, propusnost mreže, prostor za smještaj podataka) (Spremić, 2017.b).

DDoS se odnosi na koordinirani napad, upotrebom više računala, ponekad i botneta, napadaju određeni resursi sustava i cilj im je onemogućiti njihov rad (Spremić, 2017.b).

Man-In-The-Middle

Spremić (2017.b) opisuje kako napadač se nalazi između tražitelja resursa i samog resursa te iskorištava ranjivost same mreže i zaobilazi komunikacijske protokole što mu omogućuje nadgledanje sadržaja, pohranjivanje datoteka i izmjenu same komunikacije. Računalni program probije zaštitu i neprimjetno stoji, dok korisnik ne sumnja u povjerljivost komunikacije. Obično su ciljevi aplikacije s financijskim podacima i druge web stranice na kojima je potrebna prijava. Dobivene informacije napadači koriste u mnoge svrhe, nezakonitu promjenu lozinke, krađu postojeće lozinke, prijevaru, itd. (Mallik, 2018.).



Izvor: Izrada autora

Skeniranje javno dostupnih resursa

Skeniranje javno dostupnih resursa može služiti kao neka podloga ili početna faza napada u smjeru pronalaženja ranjivosti ili ciljeva za napad.

Lažne bežične pristupne točke

Utjecaj na otvorene portove javno izloženih poslužitelja

Malware

Malware je postao jedan od najkorištenijih alata za napade. Prema istraživanju koje je proveo Microsoft, svako treće računalo je zaraženo nekom vrstom malware zlonamjernog softvera (Rieck, Holz, Willems, Dussel & Laskov, 2008.). Napadači koriste zlonamjerne računalne kodove i distribuiraju ih s namjerom da učine štetu nad računalom ili ostalim resursima. Velik je broj računalnih zlonamjernih kodova, a među često korištenima su oglašivački program (eng. adware) i računalna ucjena (eng. ransomware) kojim se usred neovlaštenog upada u računalo, najčešće djelovanjem virusa se šifriraju podaci koji su u njemu pohranjeni. Napadači vrlo često traže odštetu za dešifriranje podataka.

Primjer malware napada - Jedan od poznatijih napada na informacijski sustav opisuje Spremić (2017.b) gdje je napadnut jedan od najvećih maloprodajnih lanaca u SAD-u - Target. 2013. godine je provaljeno u informacijski sustav Targeta pri čemu je ukradeno 40 milijuna brojeva kreditnih kartica, 70 milijuna adresa, brojeva telefona i ostalih osobnih informacija. Hakeri su pristupili svim podacima na način da su hakirali kompaniju koja je održavala rashladne sustave u Targetovim prodavaonicama. Hakeri su pristupili podacima preko POS terminala gdje su instalirali malware (zloćudni software) koji im je omogućio čitanje i krađu podataka s magnetnih traka kreditnih kartica. Target je shvatio da je pod napadom hakera tek nakon 18 dana od početka napada. Napad je primijetila kompanija koja je kasnije instalirala anti-malware softver.

Zaključak je da je kompanija poput Targeta imala vrlo loše sigurnosne protokole u svom informacijskom sustavu, samim time je dovela u opasnost milijune građana. To je očigledan primjer poslovanja tvrtke koje bi se trebalo izbjegavati. Preventivne mjere kako se slučaj ne bi ponovio bile su promjena POS terminala, uvođenje kartica s PIN-om i čipom koje znatno otežavaju krađu podataka i ograničili su pristup informacijskom sustavu na manji broj ljudi.

- **Fizički napad**

Gubitak ili krađa računalne opreme, računala ili medija za pohranu podataka. Otuđenje i instalacija zlonamjernog koda na uređaje, instalacija zlonamjernog koda na fizičke uređaje (bankomati, POS uređaji, itd.), instalacija zlonamjernih dijelova prilikom proizvodnje ili isporuke računalne opreme.

- **Socijalni inženjering** - Vrsta napada na ljudsku interakciju i navođenje na kršenje sigurnosnih normi i standarda s ciljem zlonamjernog postupanja.

Pokušaj otkrivanja povjerljivih informacija lažnim predstavljanjem

Pomoću lažnog predstavljanja, napadači pokušavaju zadobiti povjerenje korisnika usluga, uglavnom osoba starije životne dobi i na taj način zlonamjerno preuzeti povjerljive podatke poput broja osobne iskaznice, raznih kartičnih podataka, korisničkih imena i lozinka kako bi pristupili drugim osobnim i osjetljivim sadržajima napadnutih osoba.

Phishing

Phishing je prvi put detektiran 1996. godine, a danas je jedan od najučestalijih i najtežih vrsta cyber kriminala (Varshney, Misra & Atrey, 2016.). Vrsta računalne prijevare s ciljem krađe identiteta. Napadači šalju lažne e-mail ili SMS poruke koje izgledaju da su poslane iz izvornih institucija. Na taj način dobivaju pristup povjerljivim korisničkim podacima kao što su brojevi i autorizacijske šifre kreditnih kartica i bankovnih računa. najčešća metoda su razni skočni prozori (eng. pop-up) (Spremić, 2017.b). Također se u e-mailovima mogu pojaviti zlonamjerni dokumenti, poveznice zlonamjernih web sadržaja, zlonamjerni računalni program (eng. malware) koji me se šifriraju korisnikovi podaci. Primjer phishinga su lažne e-mail poruke. Napadači su pokušali pomoću prijevare izvući novac od hrvatskih građana. Naime, predstavili su se kao zaposlenici Hrvatske agencije za nadzor financijskih usluga (HANFA) te su poslali e-mailove građanima s kompromitirajućim sadržajem. Kako bi zadržali kredibilitet i zadobili povjerenje građana, pozivali se se na HANFA-u, američki SEC, Europsku središnju banku (ECB) te lažno upozoravali žrtve napada i zastrašivali protuzakonitim radnjama poput pranja novca. Način na koji bi napadači dobili novce od građana je uplata građana za aktivaciju fiktivnog računa na kojem su izdvojena određena novčana sredstva. HANFA se povodom ovog

službeno obratila i dala do znanja građanima da oni nikada ne šalju e-mailove nalik tome i da budu oprezni.

Zaključno, napadači su se u ovom slučaju služili socijalnim inženjeringom to jest phishingom kako bi pokušali navesti građane na uplatu novca na nezakonit način. Opreznost, logičko zaključivanje, pravovremeno reagiranje nadležnih institucija, neki su od načina prevencije i sprječavanja ovakvih napada.

Vishing

Sličan napad phishingu, ali se odnosi na telefonske pozive kojima se napadači lažno predstavljaju kao zaposlenici banaka, internetskih trgovina ili nekih drugih organizacija. Na taj način žele doći do povjerljivih podataka korisnika ili čak navesti korisnika na prijenos novca (Spremić, 2017.b).

Navođenje na preuzimanje zlonamjernog sadržaja, zlonamjernih mobilni aplikacija i slično

U gore navedenim stavkama, vidljivo je da je raznovrsnost načina prijevara uistinu velika. Prijetnje za sigurnost sustava i korisnika mogu doći u različitim pravcima i na različite načine. Cyber kriminal, kao novija vrsta kriminala je još u svom razvoju i napadači svakim danom su sve maštovitiji i vještiji te nalaze nove načine kako ugroziti sigurnost. Daljnjim razvojem tehnologije se razvijaju i mogućnosti za još veće i učinkovitije cyber napade s dalekosežnim posljedicama. U današnje doba informacijski sustavi su zaokupili sve sfere života. To ima naravno puno pozitivnih strana, ali ima i dosta negativnih strana. Sigurnost je svakako jedna od najvećih pitanja modernog doba i nešto na čemu bi sve države trebale pristupiti vrlo oprezno i s velikom pažnjom. Danas „hakirati“ nekog ne znači samo ukrasti na primjer novce s računa i slično, danas je moguće ugroziti u ozbiljnom smislu nacionalnu sigurnost. Na povećanje zaštite i prevenciju napadan se svakako može utjecati. U gore navedenom istraživanju je vidljivo da visoko razvijena društva poput skandinavskih zemalja imaju nižu stopu zaraženih računala. To proizlazi iz više aspekata kao što su obrazovanje korisnika, svijest korisnika o potencijalnoj opasnosti, povećanja pažnja pri otvaranju “sumnjivih” web stranica, uloga države koja regulira dostupnost štetnih stranica te onemogućuje pristup istima ili upozorava na vrijeme svoje građane.

4.4. Učinak napada na informacije

Autor Spremić (2017.b) navodi kako je sigurnost informacija i sigurnost informacijskih sustava skup zaštitnih mjera i metoda kojima se informacijski sustavi štite od različitih vrsta kriminalnih radnji poput neovlaštenog pristupa, uporabe, otkrivanja, prekida rada, promjena ili uništenja.

Postoje tri temeljna parametra informacijske sigurnosti:

- Povjerljivost
- Integritet (cjelovitost)
- Raspoloživost (dostupnost)

1. **Povjerljivost**

Svojstvo informacije da je raspoloživa isključivo osobama koje imaju valjano ovlaštenje. Posljedice gubitka povjerljivosti informacija mogu biti različiti. Neke od njih su gubitak povjerenja klijenata, nepoštovanje mjerodavnih propisa, financijski gubici itd. (Spremić, 2017.b).

2. **Integritet (cjelovitost)**

Svojstvo informacije kod koje postoji uvjerenje u njezinu točnost i da nije naknadno izmijenjena. Posljedice narušavanja cjelovitosti mogu biti pogrešne poslovne odluke, gubitak povjerenja klijenata, nepoštivanje mjerodavnih propisa i drugo (Spremić, 2017.b).

3. **Raspoloživost (dostupnost)**

Svojstvo koje zahtijeva da informacija bude u prihvatljivom roku dostupna ovlaštenim osobama. Posljedice narušavanja dostupnosti mogu biti nemogućnost isporuke proizvoda i usluge klijentima (Spremić, 2017.b).

Ako informacije budu ugrožene, što je i cilj napada na informacijski sustav, ti napadi se klasificiraju po različitim kriterijima kao što su krajnji cilj napada i njegove posljedice. Učinci se prema Nacionalnoj taksonomiji računalno-sigurnosnih incidenata, 2021. dijele na:

Izmjena ili iskrivljavanje - Podaci se izmjenjuju ili "iskrivljuju u cilju narušavanja cjelovitosti informacije.

Nedostupnost - Najčešće se uskraćuje dostupnost servisa koji ima pristup informaciji. Većinom je posljedica (D)DoS napada.

Uništenje - Uobičajeno dolazi do uništenja kada je brisanje podataka ili uklanjanje pristupnih prava jedan od ciljeva napada.

Otkrivanje - Vrsta učinka gdje napadač ima uvid u informacije u koje inače ne bi imao te se na taj način može protuzakonito okoristiti.

Nepoznato - Rana faza otkrivanja napada gdje učinak napada na informacije nije još poznat.

Bez utjecaja - nije bilo utjecaja na osnovna načela informacijske sigurnosti.

4.5. Objekt napada

Kroz atribut Objekt napada se precizira koja je vrsta informacijske infrastrukture meta napadača. Ovaj atribut se mijenja s obzirom na fazu napada i ovisno o tome što je krajnji cilj napadača. Prema Nacionalnoj taksonomiji računalno-sigurnosnih incidenata (2021.) objekti napada se dijele na:

Upravljačka infrastruktura - napad na kritične dijelove informacijskog sustava koji upravljaju resursima.

Računalna mreža - Napad na mrežnu infrastrukturu.

Lokalno računalo - Cilj napada je kompromitacija lokalnog računala.

Korisnik - Napad na korisnika u cilju prikupljanja povjerljivih informacija od strane napadača koje bi kasnije nezakonito upotrijebio.

Aplikacijski sustav - Napad na aplikacijsku infrastrukturu je ustvari napad na određenu aplikaciju ili njen dio.

4.6. Dosegnuta faza napada

Ovaj atribut nam govori koliko je kibernetički napad napredovao i u kojoj je fazi. Nekada je vrlo teško odrediti taj stadij kibernetičkog napada, ali je moguće. Cilj identifikacije dosegnute faze napada je prevencija i zaštita informacijskog sustava. Dosegnute faze napada kronološki poredane prema Nacionalnoj taksonomiji računalno-sigurnosnih incidenata (2021.) su:

Izviđanje - Prikupljanje informacija o potencijalnoj meti i priprema daljnjih strategija za cjeloviti napad.

Isporuka - Aktiviranje mehanizama od strane napadača gdje se na primjer šalju e-mailovi s kompromitiranim sadržajem.

Ostvarivanje pristupa - Ranije ostvarenim radnjama, napadač je identificirao ranjivosti sustava te ih iskorištava i ostvaruje pristup ciljnom informacijskom sustavu. Napadač instalira zlonamjerni kod te se širi djelokrug napada.

Potpuna kompromitacija - Faza napada u kojoj napadač ostvaruje svoje ciljeve i motivaciju za napad. Ova faza podrazumijeva eksfiltraciju, uništenje ili izmjenu podataka.

Perzistencija - Napadač ostvaruje trajnu prisutnost u kompromitiranom sustavu.

5. MJERE ZAŠTITE INFORMACIJSKOG SUSTAVA

Kako bi zaštitila svoj informacijski sustav od mogućih zlouporaba, organizacija treba razviti kontrole i tehnike za kontrolu IT incidenata. Plan za upravljanje IT rizikom ima nekoliko važnih koraka: identifikaciju i klasifikaciju IT rizika, procjenu IT rizika, strategije odgovora na IT rizik, provedba i dokumentiranje odabranih protumjera, portfeljski pristup IT rizicima i stalno praćenje razine IT rizika (Spremić, 2012.). Zaštiti informacijski sustav je u današnjem digitalnom dobu jedan od najvažnijih zadataka, kako države, tako i svakog pojedinca osobno. To je zadatak koji je vrlo težak s obzirom na razvoj tehnologije, ali s dobrim pristupom i svjesnošću koliko je to uistinu važno, možemo kao društvo doprinijeti sigurnijoj uporabi internet usluga i servisa. Harkins (2016.) utvrđuje kako je IT integriran u gotovo sve i da nije moguće kako bi zaštitili sustav, zaključati informacijsku imovinu jer na taj način se ograničava njezin rad. Mjere zaštite mogu obuhvaćati različite tehnike, prakse, politike u svrhu osiguravanja povjerljivosti i dostupnosti informacija. Kontrola pristupa ubraja se među najvažnije mehanizme zbog ograničavanja i kontrole pristupa svim resursima informacijskog sustava. Kontrolom pristupa se sprječava neovlaštena uporaba podataka, aplikacija, poslovnih procesa, opreme i infrastrukture (Spremić, 2017.b)

5.1. Identifikacija korisnika

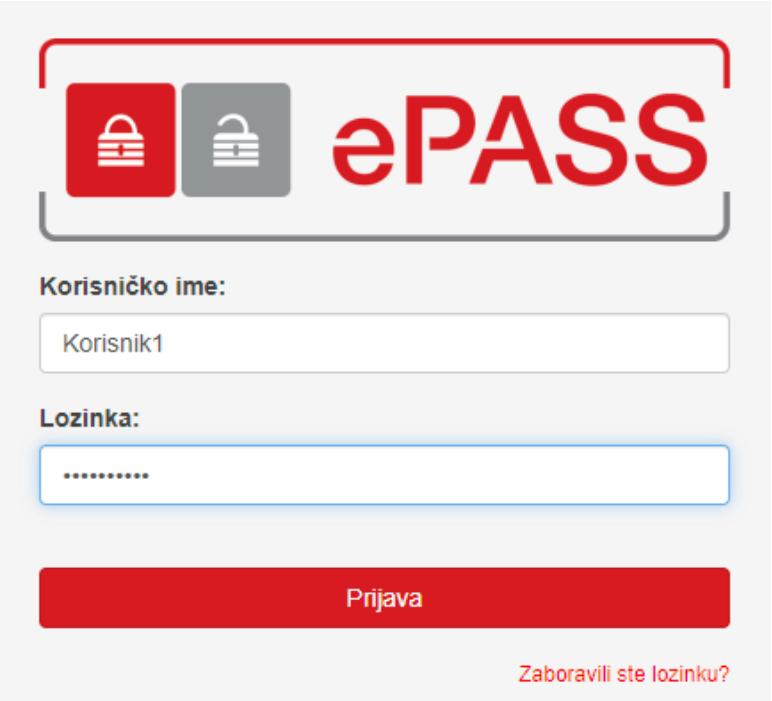
Identifikacija korisnika se definira kao postupak prijave korisnika u sustav korištenjem fizičkih, logičkih ili biometrijskih identifikacija. Na taj način se korisnici "predstavljaju" informacijskom sustavu, a informacijski sustav provjerava točnost unesenih podataka i na temelju toga daje pristup korisniku ili odbija korisnika (Spremić, 2017.b). Siguran pristup korištenjem vjerodajnica je cilj identifikacije korisnika, a sve to u cilju zaštite privatnosti, pouzdanosti i integriteta sustava.

5.1.1. Logička identifikacija

Logička identifikacija se temelji na provjeri zna li korisnik nešto što bi trebao znati odnosno može saznati bez činjenja prekršaja. To je podatak koji bi korisnik trebao znati (lozinka, identifikacijski ključ, korisničko ime, ključna riječ itd.)(Spremić, 2017.b).

Na platformi e-građani, logička identifikacija se koristi za nisku razinu sigurnosti. Ovisno o vjerodajnici potrebno je upisati korisničko ime ili Telekom ID i lozinku.

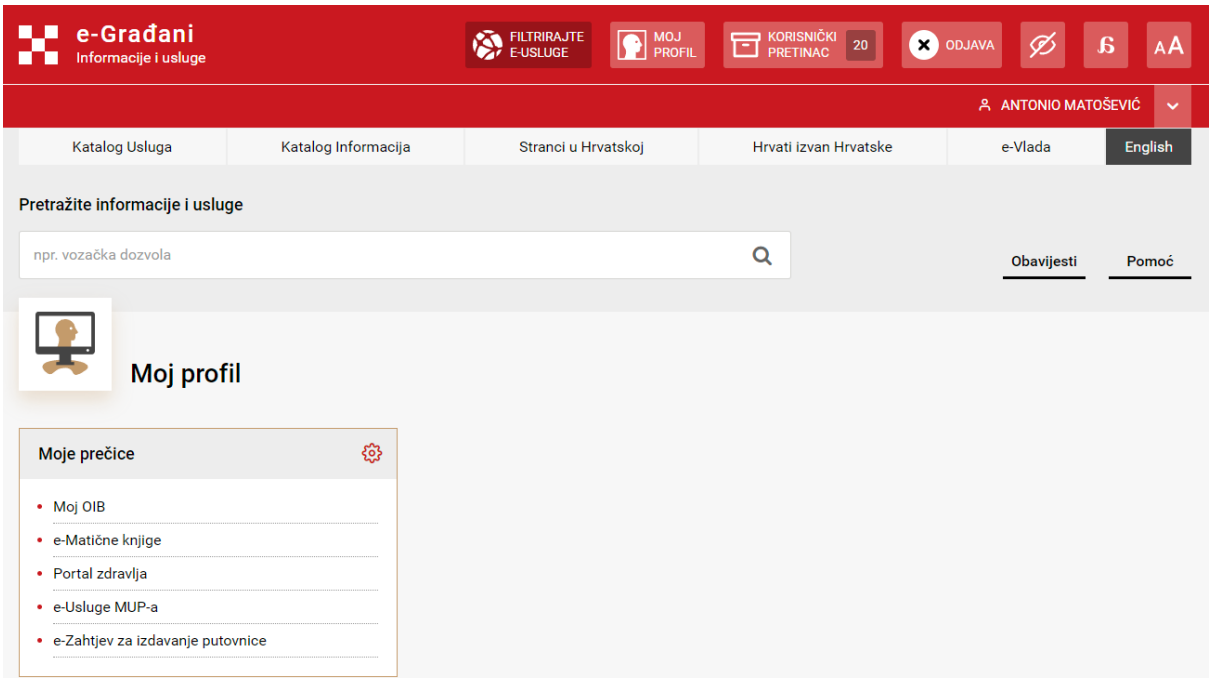
Slika 3. Prijava u sustav putem ePASS-a



Izvor: Središnji državni portal, 2024.

Upisivanjem točnog korisničkom imena i točne lozinke, portal prepoznaje korisnika i dozvoljava mu pristup svim uslugama za koje je potrebna niska razina sigurnosti. Neke od njih su korisnički pretinac, Moj OIB, REGOS, Burza rada, ePorezna itd.

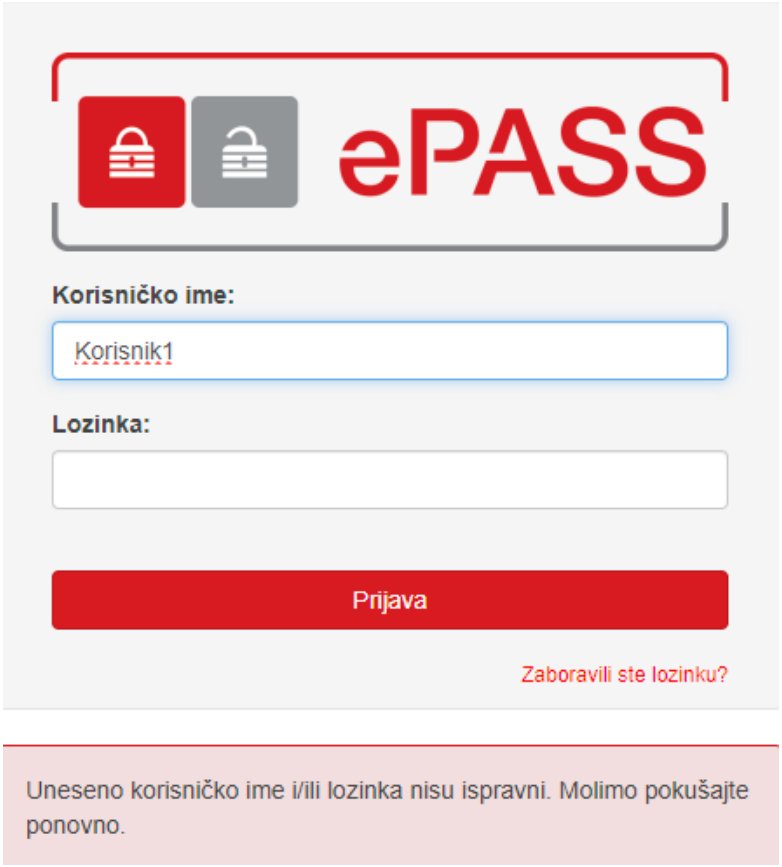
Slika 4. Uspješna prijava i naslovna stranica



Izvor: Središnji državni portal, 2024.

U slučaju upisivanja netočnog korisničkog imena ili lozinke, sustav automatski ne dozvoljava prijavu te šalje obavijest korisniku da podaci nisu ispravni i da može pokušati ponovno.

Slika 5. Neuspješna prijava u sustav



Izvor: Središnji državni portal, 2024.

Nekoliko potencijalnih problema kod ove vrste prijave u sustav su slaba autentifikacija (vrlo slabe i predvidljive lozinke te nedovoljno pouzdan način provjere identiteta), rizik od krađe identiteta (nepažljivi korisnici, najčešće osobe starije životne dobi, zapisuju svoje korisničke podatke kako ih ne bi zaboravili na mjesta gdje bi vrlo lako mogli biti zlouporabljeni te na taj način dolazi do krađe identiteta), slaba osviještenost građana o stvarnoj osjetljivosti osobnih podataka.

Kako bi lozinka bila što bolje postavljena postoje nekoliko jednostavnih pravila za postavljanje iste. Lozinka bi trebala u pravilu biti što dulja, a minimalno bi se trebala sastojati od 8 znakova. Kako bi bila što bolja, trebala bi sadržavati kombinaciju velikih i malih slova,

brojeva te posebnog simbola (.,!-*+). Također, lozinka ne bi trebala sadržavati osobne podatke poput imena, prezimena, datuma rođenja ili nečeg što bi moglo biti lako predvidljivo. Popis najlošijih lozinki već je godinama praktički nepromijenjeno. Na samom vrhu je niz znamenki "12345678", niz slova "qwertz(y)" također je jedan od najlošijih odabira. Još su tu lozinke poput "password", "football", "username" i slično.

Vrlo je važno naglasiti kako je snažna lozinka preduvjet za sigurnost osobnih podataka. To je najmanje što građani mogu učiniti za svoju sigurnost. Isto tako građani ne bi trebali zapisivati svoje lozinke i na primjer staviti je u novčanik jer gubitkom tog novčanika, osim osobnih dokumenata će im biti izloženi svi povjerljivi osobni podaci koji su dostupni na stranicama portala.

Prema Spremiću (2017.b) najčešće mjere logičkog pristupa su: osiguranje postajanja primjerenih logičkih kontrola pristupa, provjera pravila identifikacije i autorizacije korisnika, provjera pravila vezana za dodjelu, izmjenu i ukidanje korisničkih računa, određivanje i primjene minimalnih standarda svojstava lozinki, lozinke pamtiti, nikada ih zapisivati na papir, kriptirati lozinke pohranjene u elektroničkim evidencijama (baze podataka i datoteke).

5.2. Sigurnosni token

Sigurnosni tokeni u sebi sadrže pristupne podatke o korisniku usluge. Sustav je programiran tako da se kreiraju jednokratni pristupni podaci što je zapravo vrsta provjere autentičnosti s dva faktora (2FA - eng. two factor authentication). Pristupni podaci obuhvaćaju serijski broj tokena koji se ne mijenja i jednokratnu lozinku koja je dostupna 30 sekundi i nakon toga više nije aktivna, to jest mora se generirati nova. Sustav tokena osim funkcije potvrde identiteta, ima i ulogu u autoriziranju provođenja različitih transakcija. U istraživanju koje je provedeno na 100.000 Google računa, uočeno je da samo nešto više od 6% koristi 2FA, što svakako nije dobar podatak jer su računi manje sigurni (Petsas, Tsirantonakis, Athanasopoulos & Ioannidis 2015.).

Na portalu e-Građani se sigurnosni tokeni koriste kao značajna razina sigurnosti, a izdavači tokena su većinom banke (HPB, ZABA, Kent, RBA, PBZ, OTP, itd.) i Financijska agencija (FINA).

Postupak izdavanja i prijave putem mToken-a

Ispunjavanje pristupnice s najvažnijim podacima (Ime i prezime, OIB, Adresa, Adresa e-pošte, broj mobitela).

Odlazak u poslovnicu FINA-e i predaja pristupnice

Službenik/ica provjerava vjerodostojnost unesenih podataka. Ako je sve u redu, korisniku se predaje papir s korisničkim podacima potrebnima za aktivaciju mToken-a.

Slika 6. Pristupnica za mToken

1. Podaci o korisniku (obavezni podaci)

Molimo Vas da sve podatke unesete čitko.

Ime

Prezime

OIB korisnika

Vrsta identifikacijske isprave ☐ Osobna iskaznica ☐ Putovnica

Broj identifikacijske isprave

Adresa e-pošte

Broj mobitela ili telefona

2. Tražena vjerodajnica:

Označite znakom **X** određenu vjerodajnicu i vrstu postupka vezanog uz označenu vjerodajnicu.

ePASS

☐ ePASS – Korisničko ime i lozinka

☐ Izdavanje ☐ Reizdavanje ☐ Deaktivacija

mTOKEN

☐ mToken – Mobilna aplikacija za e-Građane

☐ Izdavanje ☐ Reaktivacija ☐ Deaktivacija

3. Izjava korisnika

Izjavljujem da su svi podaci navedeni u ovoj Pristupnici točni i istiniti te da su dobrovoljno stavljeni na raspolaganje Fini koja će ih koristiti u svrhu navedenu u Pristupnici. Osobni podaci prikupljeni u svrhu izdavanja /reaktivacije /deaktivacije za mToken se dostavljaju i CARNet-u.
Upoznat/a sam s Općim uvjetima zatražene vjerodajnice te su mi isti stavljeni na raspolaganje na šalteru Fine i u elektroničkom obliku na internet stranici izdavatelja vjerodajnice (za ePASS https://epass.gov.hr, a za mToken https://mToken.gov.hr).

Potpis korisnika Datum

4. Potvrda o preuzimanju aktivacijskog koda za ePASS / inicijalne lozinke za mToken

Izjavljujem da sam u poslovnici Fine osobno preuzeo/la aktivacijski kod (za ePASS) / inicijalnu lozinku (za mToken) za vjerodajnicu zatraženu u Pristupnici i da preuzimam odgovornost u slučaju gubitka ili otkrivanja ovog podatka trećim stranama. Upoznat/a sam da aktivacijski kod (za ePASS) / inicijalna lozinka (za mToken) vrijede 14 dana od dana izdavanja.

Potpis korisnika Datum

Izvor: Središnji državni portal, 2024.

Slika 7. Prikaz inicijalne lozinke

mTOKEN CARNet

mToken - korisnički podaci

Poštovani,

Vaš e-Građani mToken je uspješno kreiran. Za aktivaciju mToken aplikacije potrebni su:

- korisnički identifikator - dostavlja se na e-mail adresu navedenu u pristupnici
- inicijalna lozinka

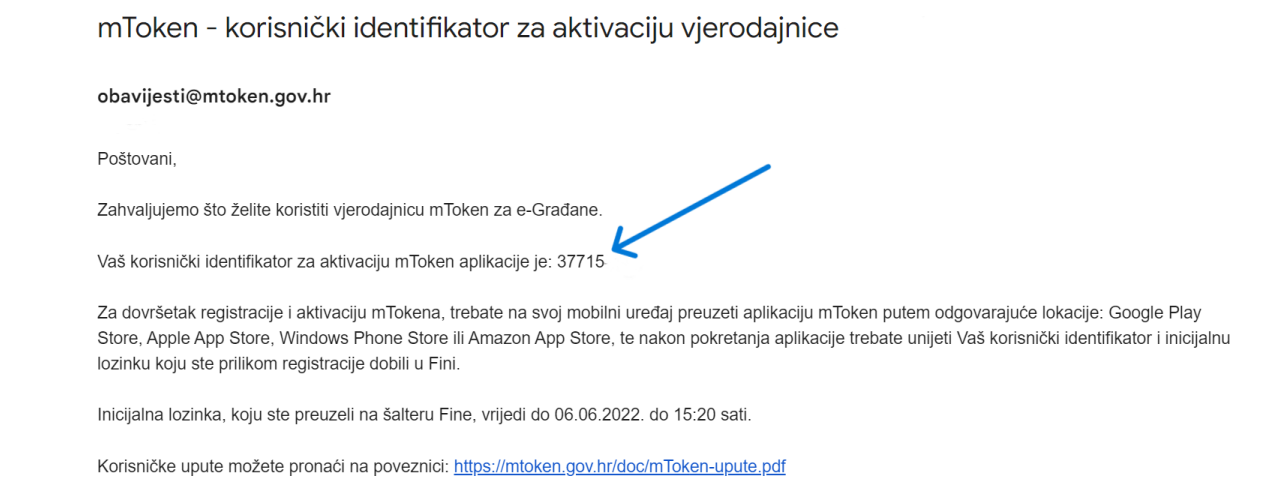
Podaci o mTokenu	
Inicijalna lozinka	12345678
Vrijeme izdavanja inicijalne lozinke	20.02.2015. (18:00:00)
Zadnji dan validnosti aktivacije mTokena	06.03.2015. (18:00:00)
Kontrolni broj:	1234

Podaci o korisniku	
Ime	
Prezime	

Izvor: Središnji državni portal, 2024.

Kombinacijom inicijalne lozinke koja je dobivena na papiru u poslovnici i korisničkog identifikatora koji je poslan na odabranu e-poštu vrši se aktivacija tokena

Slika 8. Prikaz korisničkog identifikatora



Izvor: Izrada autora

Upisivanje dobivenih podataka u aplikaciju

Slika 9. Aktivacija mTokena

Izvor: Središnji državni portal, 2024.

Nakon uspješne aktivacije se odabire PIN koji se unosi prilikom svakog ulaska u aplikaciju

Slika 10. Odabir PIN-a

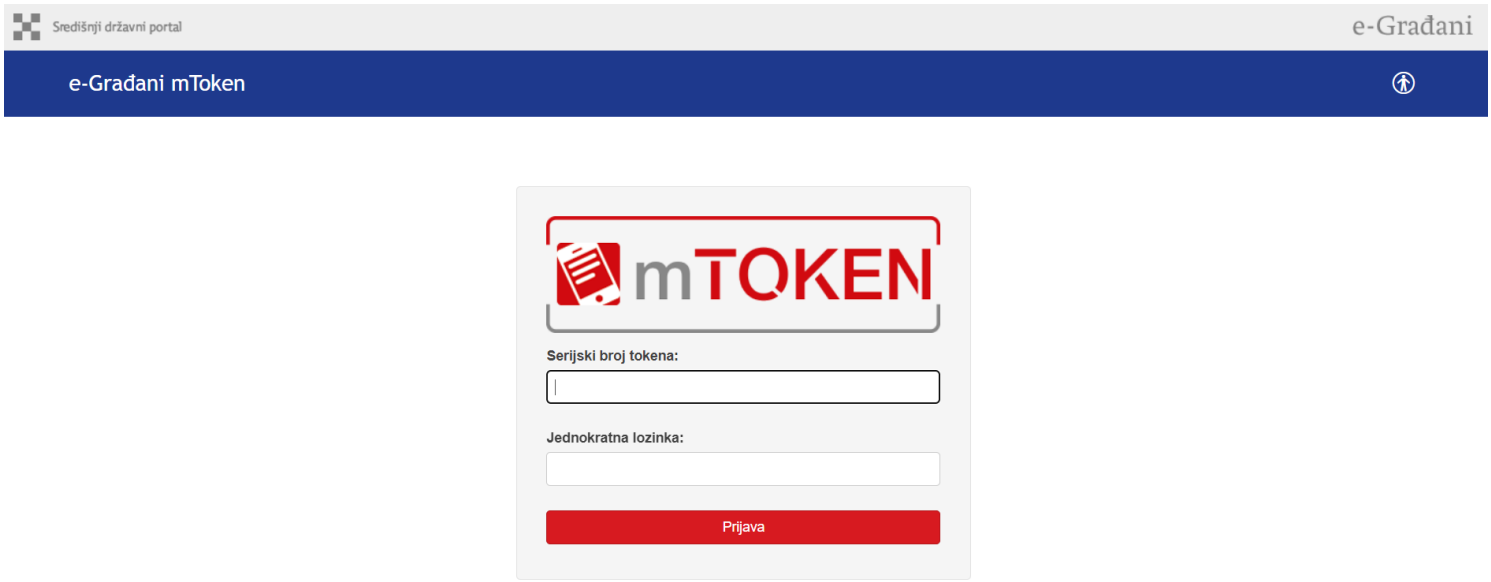
Izvor: Središnji državni portal, 2024.

Slika 11. Podaci za prijavu u sustav

Otvaranjem aplikacije i unosom PIN-a na mobilnom uređaju, otvara se novi prozor s podacima potrebnim za prijavu u sustav (Jednokratna lozinka se mijenja nakon 30 sekundi)

Izvor: Središnji državni portal, 2024.

Slika 12. Mjesto za upis podataka na računalu



Izvor: Središnji državni portal, 2024.

Od svih drugih načina prijave u sustav, mToken je izabran za detaljnu analizu zbog učestalosti korištenja u portalu. Prednost mu je što je najjednostavniji i vrlo efikasni način za pristupiti aplikaciji, a obuhvaća nisku razinu sigurnosti i značajnu razinu sigurnosti, tako da je obuhvaćena većina usluga koja je potrebna građanima. Nedostatak je što na primjer gubitkom mobilnog telefona, napadač može pristupiti velikom opsegu osobnih podataka i iskoristiti ih kako bi izvukao novac ili neke druge nezakonite koristi.

5.3. Pametne kartice

Pametne kartice se ubacuju u fizičke uređaje (čitače) s elektroničkim sklopovima te su u njima pohranjeni korisnički pristupni podaci. Ubacivanjem pametne kartice u čitač se provjeravaju pristupni podaci i odobrava ili uskraćuje pristup željenom sadržaju (Spremić, 2017.b). Primjena pametnih kartica je širokog spektra. Mogu se koristiti za financijske usluge, telekomunikacijske usluge, zdravstvo, e-usluge itd (Dhem & Feyt, 2001.).

Ovom metodom se na platformi e-Građani mogu pomoću pametne kartice Hrvatskog zavoda za zdravstveno osiguranje (HZZO) otvarati usluge koje zahtijevaju značajnu razinu sigurnosti i elektroničkom osobnom iskaznicom Republike Hrvatske (eOI) mogu otvarati usluge koje zahtijevaju visoku razinu sigurnosti.

5.4. Certifikati

Identifikacija korisnika pomoću certifikata je jedan od načina pristupanja podacima u sustavu koji su opisani kao visoka razina sigurnosti. Fizičke uređaje ili elektroničke sustave koji služe za identifikaciju korisnika izdaje posebno tijelo ili institucija. U Hrvatskoj su te institucije Financijska agencija (FINA), Hrvatska gospodarska komora (HGK), banke i slično (Spremić, 2017.b).

FINA (2024.) dijeli certifikate prema vrstama namjene:

- Kvalificirani certifikat za elektronički potpis - Nedvojbeno su vezani za potpisnika i omogućuju njegovu identifikaciju.
- Certifikati za autentikaciju - Koriste se za izradu elektroničkog potpisa, za jaku autentikaciju i za enkripciju ključa.
- Certifikati za aplikacije, odnosno poslovni certifikati za IT opremu - Ima istu namjenu kao i Certifikat za autentikaciju, ali se izdaje u poslovne svrhe.
- Certifikat za elektronički pečat - povezuje pravnu osobu i podatke za validaciju elektroničkog pečata te osigurava cjelovitost dokumenta.
- Certifikat za autentikaciju mrežnih stranica - Koristi se za autentikaciju web poslužitelja kojima se pristupa putem TLS ili SSL protokola.

5.5. Infrastruktura javnog ključa

Infrastruktura javnog ključa (eng. PKI - Public Key Infrastructure) je ustvari sustav digitalnih certifikata, certifikacijskih autoriteta i registracijskih autoriteta koji obavljaju provjeru identiteta svi strana uključenih u internetsku transakciju upotrebom para ključeva - javni i tajni/privatni ključ (FINA, 2024.).

Tehnologija kao što je PKI omogućuje tajnost elektroničkih transakcija, provjeru identiteta, integritet informacija, sigurnije procese razmjene podataka, pristup javnosti državnim i e-servisima, prihvat različitih elektroničkih ispunjenih dokumenata, sigurnu komunikaciju sa zaposlenicima na udaljenim lokacijama, razmjenu tajnih podataka, smanjenje operativnih troškova uvođenjem elektroničkog poslovnog procesa (FINA, 2024.).

Transakcije štićene PKI tehnologijom zadovoljavaju osnovne zahtjeve:

- Autentikacija
- Integritet
- Tajnost
- Neporecivost (FINA, 2024.)

5.5.1. Autentikacija

Autentikacija se koristi kako bi se potvrdio identitet nekog subjekta, bio on poslovni subjekt, pravna ili fizička osoba. Proces provjere korisničkog identiteta kojim korisnik dokazuje da je zaista onaj za kojeg se predstavlja (prilikom prijavljivanja u neki sustav i sl.) (FINA, 2024.). Primarni cilj autentikacije u infrastrukturi javnog ključa je podržati udaljenu i nedvosmislenu autentikaciju između entiteta koji su jedan drugome nepoznati. Autentikacija u PKI okruženju se oslanja na matematički odnos između javnog i privatnog ključa. Poruke koje je potpisao jedan entitet može testirati bilo koji subjekta, a samo vlasnik ima pristup privatnom ključu te je u tom slučaju sigurno vlasnik ključa pokrenuo poruku (Weise, 2001.).

5.5.2. Integritet

Jamstvo za podaci u prijenosu nisu promijenjeni ili uništeni. Cjelovitost i izvornost podataka osigurava elektronički potpis. Provjerom se može utvrditi jesu li podaci nelegalno naknadno mijenjani (FINA, 2024.). Primjer su certifikati javnih ključeva i omotnice s digitalnim potpisom

koje moraju imati jamstvo integriteta. Integritet se unutar PKI-ja osigurava korištenjem javne ili tajne kriptografije (Weise, 2001.).

5.5.3. Tajnost

Enkripcija (šifriranje) podataka koji su pohranjeni ili poslani mrežom sprječavanja čitanja sadržaja od strane neovlaštenih osoba (FINA, 2024.). Šifriranje podataka moguće je korištenjem javne (asimetrične) ili tajne (simetrične) kriptografije. Za pružanje povjerljivosti se koriste tajni ključevi jer je kriptografija učinkovitija od javnih ključeva. tajni ključevi su ugrađeni u PKI sustave za skupno šifriranje podataka (Weise, 2001.).

5.5.4. Neporecivost

Napredan elektronički potpis pruža neupitan dokaz o akciji koju je osoba poduzela ili autorizirala (FINA, 2024.). Ta radnja se osigurava kriptografijom s javnim ključem digitalnim potpisivanjem. Vrlo je važno da korisnici zaštite svoje privatne ključeve kako ne bi došlo u pitanje identitet osobe koja upravlja ključevima (Weise, 2001.).

5.6. Autorizacija

Svakom korisniku se dodjeljuju određene ovlasti nad resursima rada informacijskog sustava koja ovisi o potrebama posla (Spremić, 2017.b). Primjer neka bude e-Dnevnik koji je postao „novo normalno“ i zamijenio klasični imenik i sve njegove funkcije. U sustavu e-Dnevnika svaki pojedinac ima svoje ovlasti i način na koji može koristiti aplikaciju. Primjerice, učenik u sustavu može pregledavati svoje ocjene, pregledati dane kada je izostao s nastave, pregledati datume svojih ispita itd. Roditelj ima drugačiju ulogu u ustavu, on na primjer može opravdati učenikove izostanke odgovarajućom liječničkom ispričnicom ili samostalnim objašnjenjem zašto učenik nije bio na nastavi, ali naravno samo određen broj sati. Učitelj ili profesor u sustav ima mogućnost upisivati ocjene, određivati datume ispita, upisivati izostanke učenika i ostalo. Na ovom primjeru možemo vidjeti koliko zapravo je autorizacija bitna u ovom sustavu i koliko bi bilo pogrešno da na primjer učenik sebi može upisivati ocjene. Na istom principu autorizacija djeluje i u drugim područjima i poduzećima općenito. Vrlo je važno odrediti uloge koje ima svaki član u lancu kako bi krajnji rezultat bio što povoljniji.

6. SWOT ANALIZA

SWOT analizom će se sagledati čimbenici koji su vezani za platformu e-Građani i njenu sigurnost. U analizi će se obuhvatiti 4 čimbenika: snage, slabost, prilike i prijetnje. Snage i slabosti predstavljaju sadašnjost, a prilike i prijetnje budućnost.

Tablica 3. SWOT analiza

SNAGE	SLABOSTI
- Velika ulaganja u postojeći sustav i konstantna nadogradnja istog novim uslugama - Veliki izbor raznovrsnih usluga (više od 100) - Konstantni rast platforme u okviru digitalizacije društva - Jedinstven sustav u Hrvatskoj - Prijava u sustav omogućena različitim računima i vjerodajnicama - Uspješno provođenje popisa stanovništva - Dobro razvijeni sigurnosni aspekt	- Ne koristi je više od polovice stanovništva Republike Hrvatske - Građani u starijoj životnoj dobi su nezainteresirani za usluge koje platforma nudi - Marketing koji nije dovoljno uključen u promoviranje korisnih sadržaja - Mogućnost lagane krađe identiteta kod lakovjernih građana - Komplicirana prijava u sustav mToken za informatički nepismene građane
PRILIKE	**PRIJETNJE**
- Razvojem tehnologije se javljaju još veće i bolje mogućnosti - Proširivanje palete usluga - Pojačavanje kampanje uključenosti starijih sugrađana u rad platforme - Jačanje sigurnosnih standarda i revizije sustava - Približiti usluge mlađim generacijama	- Razvoj tehnologije koji pomaže napadačima da lakše nezakonito koriste tuđe podatke i ovlasti - Sve učestaliji napadi na informacijsku infrastrukturu - Što je više usluga i povjerljivih informacija na platformi, više toga može doći u opasnost - Utjecaj društvenih mreža na odavanje osobnih podataka - socijalni inženjering

Izvor: Izrada autora

7. INTERVJU SA STRUČNJACIMA ZA INFORMACIJSKU SIGURNOST

Jedan od najboljih načina kako uistinu približiti stručnu materiju čitatelju je svakako intervju sa stručnom osobom za to područje. Područje za koje su postavljena različita pitanja troje stručnih osoba je informacijska sigurnost i sama platforma e-Građani. Intervju je kreiran u obliku pitanja i odgovora. Svakoj stručnoj osobi su postavljena ista pitanja. Pitanja su kreirana kako bi svi čitatelji ovog rada mogli razumjeti o čemu se priča i bez prethodnog znanja vezanog za sigurnost informacijskog sustava. Cilj intervjua je da se svaki čitatelj se mogao poistovjetiti sa stručnom osobom i imati svoje mišljenje u vezi pitanja te ga na kraju komparirati sagledavajući sva tri odgovora. Pitanja su jednostavnijeg i otvorenog tipa jer je taj način puno prihvatljiviji široj populaciji te je puno zanimljivije i interaktivnije.

Stručna osoba 1: U svojoj kompaniji zaposlena je na mjestu voditeljice odjela. U IT sektoru ima više od 6 godina iskustva.

Stručna osoba 2: U svojoj kompaniji je zaposlen kao savjetnik za poslovna rješenja. U IT sektoru ima više od 5 godina iskustva.

Stručna osoba 3: U svojoj kompaniji je zaposlen kao specijalist za sigurnost u Security odjelu. U IT sektoru ima više od 17 godina iskustva.

Pitanja i odgovori:

1. **Kako gledate općenito na sigurnost informacijske tehnologije u svijetu? Koje su po Vama najveće prijetnje i koje bi preventivne mjere trebalo poduzeti kako bi se spriječile?**

Stručna osoba 1:

Kao preventivnu mjeru istaknula bih osviještenost, ako govorimo o svakom zasebnom djelatniku zaposlenom u velikoj instituciji, a ista se postiže čestim edukacijama o IT sigurnosti. Dovoljan je jedan phishing, kao vrlo čest primjer socijalnog inženjeringa kojem sam i sama bila često izložena, da se pokupe podaci zaposlenika i potencijalno nastane velika šteta za tvrtku.

Najveće prijetnje, a neke sam i navela u ovom upitniku, smatram da su svi oblici malware-a, phishing, DDoS napadi. Osim navedenih, a obzirom na situaciju u svijetu mogu reći da tu spadaju i prirodne katastrofe. Preventivna mjera za prirodne katastrofe je DR lokacija (kao i redovite provjere prijenosa podataka na istu).

Stručna osoba 2:

Sigurnost informacijske tehnologije je dosta snažna. Svakim danom tehnološki razvitak je sve više vidljiv i samim time su i informacijski sustavi kao takvi puno sigurniji. Tehnološka grana je definitivno budućnost te se već sada sve velike kompanije okreću kao sigurnosti u tehnologiji umjesto klasičnom staromodnom načinu zaštite informacija. Uspostavljanje ureda za informacijsku sigurnost unutar tvrtke je jako važan korak prema zaštiti podataka. Kontrolirano vođenje sigurnosti je svakako nužno u moderno doba. Takav ured treba voditi brigu o sigurnosti te prilagoditi sigurnost standardima. Prijetnja će naravno uvijek biti, ali educiranje zaposlenika kao i kontrola korištenja sustava može riješiti većinu problema. Najveće prijetnje i u najvećoj količini svakako dolaze mailovima kojima se pokušava na jednostavan način dobiti pristup podatcima firme, računajući da će zaposlenici napraviti grešku jednostavnom nepažnjom.

Stručna osoba 3:

Općenito, sigurnost informacijske tehnologije je vrlo bitna u ovo vrijeme. Najveće prijetnje su phishing napadi, napadi na infrastrukturu i nedovoljno osviješteni korisnici. Treba imati preventivne mjere: redovite sigurnosne revizije, edukaciju zaposlenika, upotrebu jakih lozinki, vise faktorsku autentifikaciju te implementaciju naprednih sigurnosnih alata poput firewalla.

2. **Opišite svoja iskustva s najvećim cyber napadom u Vašoj karijeri. Navedite kako je do problema došlo i kako se problem riješio. Također navedite je li se napad mogao spriječiti, ako da, na koji način?**

Stručna osoba 1:

Moram priznati da tijekom svoje karijere nisam svjedočila nekim značajnim cyber napadima. Kao primjer mogu navesti DDoS napad na platformu koja je u tom periodu imala velik broj

korisnika, a još više osjetljivih podataka korisnika i napad se nije slučajno dogodio baš na toj platformi. Riješen je vrlo brzo standardnim procedurama odjela za sigurnost. Napad se zapravo spriječio pri samom pokušaju tako da nije bilo potencijalno velike ugroze.

Stručna osoba 2:

U našoj tvrtki nisam upoznat da je bilo cyber napada jer je sigurnost odlično vođenja. Ipak, u karijeri susreo sam se sa slučajem u stranoj tvrtki koja je imala problem s napadom na bazu podataka koji je uzrokovao ogromne gubitke tvrtke. Cijela produkcijska okolina tvrtke morala se ugasiti na 2 tjedna te su time gubitci bili jako veliki za navedenu tvrtku. Sve je moglo biti spriječeno da je navedena tvrtka puno bolje organizirala sigurnost podataka na produkcijskoj okolini te imala odgovornu osobu za kontrolu sigurnosti, pogotovo za sustave koji su bitni za opće poslovanje tvrtke, jer je ovim napadom cijelo korisničko sučelje bilo nedostupno. Nakon toga, tvrtka je u strahu od ponavljanja uvela mjere koje su otežavale rad zaposlenicima i vjerojatno nisu bile ni nužne, no strah od ponovnog probijanja u podatke je presudila.

Stručna osoba 3:

U svojoj karijeri nisam doživio veliki cyber napad, ali sam se susreo s pokušajima phishing napada i malware infekcija. U jednom slučaju, zaposlenik je otvorio phishing e-mail i uveo malware u sustav. Problem je brzo identificiran zahvaljujući našem sustavu, a zatim je zaraženi sustav izoliran i očišćen. Dodatna edukacija zaposlenika o prepoznavanju phishing e-mailova i korištenje sandboxing tehnologija za testiranje sumnjivih datoteka mogli bi pomoći u sprječavanju takvih problema u budućnosti.

3. **Kako gledate na platformu e-Građani u smislu informatičke i korisnikove sigurnosti? Smatrate li da su podaci dovoljno zaštićeni? Koje metode zaštite smatrate dobrima, a koje bi možda Vi nadogradili ili koristili?**

Stručna osoba 1:

Na platformu e-Građani gledam kao na sigurnu obzirom na sustav koji se koristi za autentifikaciju. U NIAS-u se cjelokupna komunikacija odvija razmjenom SAML poruka, a

komunikacija ima svojstvo očuvanja povjerljivosti i integriteta primjenom mehanizama elektroničkog potpisivanja i uspostave SSL kanala.

Stručna osoba 2:

Platforma e-Građani po meni je dosta sigurna. Načini pristupa su dosta sigurni te su samim time podatci dobro zaštićeni. Metode zaštite u kojima se prilikom prijave koriste npr. tokeni zasigurno su dobra zaštita. Uobičajena lozinka s bilo koje mreže nije najbolji način te se može jednostavno provaliti u takve sustave. Za osjetljive sustave svakako bi se trebala dodati višestruka autentifikacija (MFA), ako se sustav već ne može sakriti iza VPN-a.

Stručna osoba 3:

Platforma e-Građani je korisna inicijativa koja olakšava pristup različitim uslugama građanima, ali je također važno osigurati visoku razinu sigurnosti podataka. Metode kao što su više faktorska autentifikacija i enkripcija podataka su dobre prakse koje se već koriste. Nadogradnje bi mogle uključivati implementaciju biometrijske autentifikacije.

4. **Koje su po Vama najveće prednosti platforme, a koji najveći nedostaci? Na koji način bi Vi riješili eventualne probleme?**

Stručna osoba 1:

Najveća prednost sustava e-Građani je digitalizacija javne uprave. Digitalizacija u ovom slučaju korisnicima sustava donosi značajnu uštedu vremena i novca pri obavljanju administrativnih poslova. Dakle zaista vidim veliku korist i drago mi je da imamo ovakav sustav u Hrvatskoj. Od nedostataka imam jedan primjer iz osobnog iskustva, ali nije direktno povezan sa samom uslugom e-Građani. Vezano je uz neinformiranost određenih institucija da se određene aktivnosti mogu obaviti putem sustava e-Građani. Ne bih isticala o kojoj ustanovi je riječ, ali nakon duže vremena ipak smo došli do rješenja i izvršavanja usluge putem platforme. Središnjice svih sustava su jako dobro upoznate s uslugama koje njihova institucija pruža putem sustava e-Građani, ali poslovnice u manjim mjestima iz nekog razloga nisu toliko informirane. Razlog tome možda je manje korištenje takvog oblika komunikacije i rada. To bih navela kao

nedostatak, ali kao što sam rekla nije povezano s uslugom e-Građani već samo korisničko iskustvo.

Stručna osoba 2:

Prednosti su svakako mogućnost obavljanja raznih akcija kroz sustav i digitalnim putem. To uvelike olakšava svakodnevne aktivnosti građanima. Problem je navigacija kroz platformu koja svakako nije najbolje osmišljena te nije dovoljno intuitivna. Mislim da bi se ljude moglo motivirati više da je sustav bolje logički prilagođen korisniku.

Stručna osoba 3:

Najveće prednosti platforme e-Građani su jednostavan pristup raznim javnim uslugama, smanjenje administrativnih postupaka i olakšavanje komunikacije s državnim institucijama. Također, platforma može pomoći u digitalizaciji i modernizaciji javne uprave. Naravno, neki od nedostataka mogu uključivati potencijalne sigurnosne ranjivosti i moguće tehničke poteškoće prilikom integracije s različitim sustavima. Za rješavanje tih problema, predlažem kontinuirano ažuriranje i poboljšanje sigurnosnih protokola te suradnju s stručnjacima iz područja informacijske sigurnosti kako bi se identificirale i otklonile potencijalni problemi.

5. **Smatrate li da je Nacionalni identifikacijski i autentifikacijski sustav (NIAS) dovoljno siguran za ulogu koju ima na portalu e-Građani? Koji su potencijalni problemi sustava i na koji način bi mogli biti riješeni?**

Stručna osoba 1:

Sve vjerodajnice koje su uključene u NIAS su ujedno i nacionalno priznate vjerodajnice te služe kao sredstvo elektroničke identifikacije na pristupu e-uslugama. Na ovaj način se vjerodajnicama koje se koriste u druge svrhe povećava uporabna vrijednost. Izdavatelj vjerodajnice i dalje nastavlja brinuti o izdavanju vjerodajnice kao i provjeri njezine autentičnosti putem svojeg autentifikacijskog poslužitelja dok sustav NIAS brine o prihvaćanju tako izdane vjerodajnice. Zadatak pružatelja usluga identifikacije i autentifikacije poput sustava NIAS je sigurna i pouzdana autentifikacija korisnika koji putem odgovarajuće vjerodajnice pristupa elektroničkim uslugama. Ne vidim potencijalne probleme.

Stručna osoba 2:

Smatram da je te ne vidim konkretne probleme.

Stručna osoba 3:

Smatram da NIAS ima solidne sigurnosne mjere, ali kao i svaki sustav, postoji potencijal za ranjivosti. Mogući problemi uključuju potencijalne slabosti u autentifikacijskim metodama, ranjivosti u softveru i hardveru te izloženost phishing i brute force napadima. Za rješavanje ovih problema, trebalo bi ulagati u redovito ažuriranje i nadogradnju autentifikacijskih metoda, implementaciju dodatnih sigurnosnih slojeva kao što je biometrijska verifikacija, te provođenje kontinuiranih sigurnosnih revizija i testiranja.

6. **Smatrate li da je raspršenost vjerodajnica dobra u sigurnosnom smislu (1. i 2. sigurnosna razina podataka dostupna)? Vjerujete li da svi pružatelji token usluga (pretežito banke) mogu odgovoriti dovoljno brzo i kvalitetno na moguće ugroze i napade na podatke korisnika?**

Stručna osoba 1:

Mislim da je dobra raspršenost vjerodajnica po razinama, obzirom da kriteriji za određivanje razine osiguranja kvalitete autentifikacije dolaze iz smjernica koje se koriste u NIAS-u, a one su koncipirane na načelima EU projekta STORK. Glavna zadaća definicije kriterija je ocjena i rangiranje vjerodajnica te služe i kao pomoć pružateljima servisa kako bi znali ispravno procijeniti koju razinu sigurnosti vjerodajnice odabrati kao odgovarajuću za pristup njihovom servisu. Na ovaj način je značajno lakše procijeniti stupanj prihvatljivog rizika kojeg primjena nekog autentifikacijskog procesa unosi u poslovanje.

Stručna osoba 2:

Svakako je korisna u obliku dodatne sigurnosti te ju koristim na raznim sustavima. Smatram kako se na taj način otkloni dosta potencijalnih opasnosti. Obično se druga razina sigurnosti provodi putem aplikacija na mobilnom uređaju. Najpoznatiji način je generiranje nove lozinke

u vremenskom razmaku te se na taj način onemogućava učestalo pokušavanje probijanja u sustav. Smatram kako su ti sustavi vrlo korisni. Kod banaka se putem tokena generira određeni broj za transakciju te je također dosta siguran način kontrole pristupa.

Stručna osoba 3:

Raspršenost vjerodajnica može dodatno otežati neovlašten pristup računima i podacima, što može povećati sigurnost, najviše kada su u pitanju visoke razine sigurnosnih razina. Da, banke imaju dosta stabilna i dobra rješenja.

7. **„Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, okružen nervnim plinom i dobro plaćenim naoružanim čuvarima. Čak ni tada, ne bih se baš kladio na njega.“ Slažete li se s ovim citatom ili se ne slažete? Obrazložite odgovor.**

Stručna osoba 1:

U potpunosti razumijem citat i mogu se složiti. Ali usudit ću se povući paralelu s činjenicom da ako nikada ne napustite svoja 4 zida nećete iskusiti život kakav je zamišljen; uključujući njegove i pozitivne i negative strane.

Stručna osoba 2:

Svakako se ne slažem s navedenom tvrdnjom te smatram kako se u moderno doba moramo prilagoditi i vjerovati informacijskoj sigurnosti. Dobrom kontrolom rizika i nadzorom sigurnosti možemo postići iznimno sigurne platforme. Rizik će uvijek postojati, ali ga možemo svakako svesti na minimum.

Stručna osoba 3:

Slažem se s osnovnom porukom citata jer je potpuna sigurnost nemoguća. Uvijek će postojati potencijalne ranjivosti koje mogu biti iskorištene, bilo da su to tehničke greške, ljudske pogreške ili napadi. To ne znači da ne bismo trebali ulagati u sigurnosne mjere i prakse. Važno

je kontinuirano poboljšavati sigurnosne protokole, educirati korisnike i pratiti najnovije sigurnosne trendove kako bismo smanjili rizike i zaštitili informacijske sustave koliko je to moguće.

Odgovori koje su ponudili stručnjaci su međusobno slični, ali naravno postoje određene različitosti. Svi se slažu kako je digitalizacija jedna od najvažnijih stvari današnjice te kako je sigurnost u toj digitalizaciji gotovo najvažniji faktor i preduvjet daljnjeg razvoja. Svi su se složili kako je edukacija i osviještenost ljudi faktor koji je najvažniji i kod kojeg je najveća mogućnost za napretkom. Razlog tome je što je dovoljan jedan e-mail koji može nanijeti veliku štetu cijelom sustavu. Također je važno u svim razvijenijim kompanijama imati zaseban ured koji bi se bavio informacijskom sigurnošću. U svom radu, stručnjaci su se susreli s DDoS napadom, napadom na bazu podataka i uvođenje malware zloćudnog softvera putem e-mail poruke (socijalnog inženjeringa). Svi ovi napadi su mogli biti izbjegnuti prepoznavanjem prijetnje na vrijeme ili pažljivijim radnjama zaposlenika. Svi se slažu kako je platforma e-Građani vrlo korisna i veliki napredak u digitalizaciji hrvatskog društva. Najniža razina je svakako najranjivija jer se obične lozinke mogu vrlo lako manipulirati. Token tu igra ključnu ulogu i odlično je rješenje za povjerljivije informacije građana jer se koristi dvo-faktorska zaštita (2FA). Svo troje smatraju kako je digitalizacije javne u prave i objedinjivanje svih usluga na jednom mjestu najveća prednost platforme i njezina snaga. Jedan stručnjak kao slabost navodi neinformiranje određenih državnih institucija o uslugama koje se mogu obaviti putem platforme, drugi navodi kako misli da se može bolje posložiti navigacija kroz platformu, dok treći preporučuje preventivno kontinuirano ažuriranje i poboljšanje sigurnosnih protokola. Svi stručnjaci se slažu kako je NIAS stabilno i dobro rješenje po pitanju provođenja sigurnosti na platformi. Na citat koji govori kako ne postoji informacijski sustav koji nije ranjiv, dvoje od tri stručnjaka se slaže s tim, no ipak misli kako se stvari ne mogu baš gledati na takav način jer onda inače u svom životu ne bi ništa radili jer svugdje postoji nekakav rizik. Treći stručnjak ima mišljenje da trebamo vjerovati informacijskoj sigurnosti i da dobrom kontrolom rizika i nadzorom nad sigurnosti možemo svesti rizik na minimum.

8. ZAKLJUČAK

Kroz ovaj diplomski rad analizirane su najbitnije promjene u novom dobu, a to su digitalizacije kompletnog sustava i platforma koja tu digitalizaciju najbolje prikazuje u nama poznatom i bliskom okruženju, platforma e-Građani.

Digitalno društvo, jedan je od preduvjeta moderne i napredne gospodarske politike, politike koja teži modernim principima i rješenjima. Tome teži i Republika Hrvatska koja je 2013. objedinila većinu javno dostupnih e-usluga i napravila jedinstveni središnji državni portal i aplikaciju e-Građani. Glavni cilj je tada bio zadobiti povjerenje građana i privući ih da počnu koristiti platformu. Danas platforma broji više od 1.8 milijuna prijava sa zasebnim OIB-om i možemo reći da je Vlada Republike Hrvatske uspjela u svom naumu.

Naravno, kroz proces i razvoj digitalizacije su se javile i loše strane. To je pitanje informacijske sigurnosti koja danas igra vrlo veliku ulogu u svim razvijenim gospodarstvima. Informacijska sigurnost započinje ponajprije edukacijom svih građana ili zaposlenika neke tvrtke. Važna je kako bi se informirali kako se treba ponašati na internetu, kako pravilno koristiti stvari na internetu, ponajprije zaštiti svoje osobne podatke. Najčešće su građani meta socijalnog inženjeringa i na taj način napadači dolaze nezakonito do željenih povjerljivih informacija i njima se služe kako bi izvukli određenu korist. Različitim metodama napada poput phisihinga, malware-a, man in the middle napada, itd., napadači pokušavaju nanijeti štetu žrtvama. Zato su tu uz osviještenost građana, i mjere zaštite informacijskih sustava koje pomažu da povjerljivi podaci budu zaštićeni i sigurnost korisnika što veća. U platformi e-Građani se najviše koriste tokeni koji identifikacijski alat za ulaz na samu platformu. Pomoću njih se ostvaruje dvo-faktorska autentikacija korisnika i puno je manja vjerojatnost za uspješan napad na privatnost korisnika. Uz dvo-faktorsku autentikaciju još su tu i alati poput autorizacije, kriptografskih protokola itd. U istraživačkom dijelu rada su intervjuirane tri osobe koje se bave pitanjem informacijske sigurnosti i oni su u svojim odgovorima na postavljena pitanja dali svoje viđenje općenito o sigurnosti, ali i konkretno ocijenili platformu e-Građani i dali svoj stručni sud o njenoj sigurnosti.

Konačno, smatramo da će kontinuirana pažnja prema sigurnosti u platformi e-građani biti ključna za održavanje povjerenja korisnika te za uspješno ostvarivanje ciljeva ove važne digitalne platforme u kontekstu modernog društva.

Popis literature

1. Arbanas, K., Spremić, M., Žajdela Hrustek, N. (2021.), Holistic framework for evaluating and improving information security culture [e-publikacija]
2. Bosilj Vukšić, V., Ćurko, K. Jaković, B., Milanović Glavan, Lj., Pejić Bach, M., Pivar J., Spremić, M., Stjepić, A., Strugar, I., Varga, M., Vlahović, N., Srića, V., Suša Vugec, D. i Zoroja, J. (2020.), Osnove poslovne informatike, Zagreb: Ekonomski fakultet - Zagreb
3. Boyd, S., Keromytis, D. (2004.), SQLrand: Preventing SQL Injection Attacks [e-publikacija], preuzeto s https://link.springer.com/chapter/10.1007/978-3-540-24852-1_21
4. Dhem, J.-F., Feyt, N. (2001.), Present and future of smart cards [e-publikacija], preuzeto s https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=a1fa80e980169fb461cc3
5. Financijska agencija (b.d.), Digitalni certifikati i vremenski žig, preuzeto 25. ožujka 2024. s https://www.fina.hr/finadigicert
6. Franc S., Bilas V., Bošnjak M. (2021.), Konkurentnost i komparativne prednosti u globalnoj digitalnoj ekonomiji, Zagreb, Ekonomski fakultet - Zagreb
7. Hajdarević, K., Allen, P., Spremić, M. (2016.), Proactive Security Metrics for Bring Your Own Device (BYOD) in ISO 27001 Supported Enviroments [e-pbulikacija]
8. Harkins M. W. (2016.), Managing Risk and Information Security, 2nd Edition, California, USA, Library of Congress
9. Houser R., Hao S., Li, Z., Liu, D., Cotton, C & Wang H. (2021.), A comprehensive Measurement-based Investigation of DNS Hijacking [e-publikacija], preuzeto s https://ieeexplore.ieee.org/abstract/document/9603621
10. Mallik, A. (2018.), Man-In-The-Middle attack: Understanding in simple words [e-publikacija], preuzeto s https://jurnal.ar-raniry.ac.id/index.php/cyberspace/article/view/3453
11. Mammadli E, Klivak V. (2020.), Measuring the effect of the Digitalization [e-publikacija], preuzeto s https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3524823

12. Nacionalna razvojna strategija Republike Hrvatske do 2030. godine (b.d.), Digitalna tranzicija društva i gospodarstva, preuzeto 17. ožujka 2024. s https://hrvatska2030.hr/rs3/sc11/
13. Petsas, T., Tsirantonakis G., Athanasopoulos E. & Ioannidis S. (2015.), Two-factor Authentication: Is the World Ready? Quantifying 2FA Adoption [e-publikacija], preuzeto s https://dl.acm.org/doi/abs/10.1145/2751323.2751327
14. Rieck, K., Holz, T., Willems, C., Duseel, P., Laskov, P. (2008.), Learning and Classification of Malware Behavior [e-publikacija], preuzeto s Learning and Classification of Malware Behavior | SpringerLink
15. SK@UT Zaštita nacionalnog kibernetičkog prostora (b.d.), O sustavu SK@UT, preuzeto 23. ožujka 2024. s https://www.skaut.hr/#odluka
16. Spremić, M. (2012.), Corporate IT Risk Management Model: a Holistic view at Managing Information System Security Risks [e-publikacija]
17. Spremić, M. (2017.a), Digitalna transformacija poslovanja, Zagreb: Ekonomski fakultet - Zagreb
18. Spremić, M. (2017.b), Sigurnost i revizija informacijskih sustava u okruženju digitalne ekonomije, Zagreb: Ekonomski fakultet - Zagreb
19. Spremić, M. (2013.), Holistic Approach for Govering Information System Security [e-publikacija]
20. Spremić, M., Šimunc, A. (2018.), Cyber Security Challenges in Digital Economy [e-publikacija]
21. Spremić, M., Šimurina, J., Jaković, B., Ivanov, M. (2009.), E-Government in Transition Economies [e-publikacija]
22. Varshney, G., Misra, M., Atrey, K. (2016.), A survey and classification of web phishing detection schemes [e-publikacija], preuzeto s https://onlinelibrary.wiley.com/doi/abs/10.1002/sec
23. Veresha, R. (2018.), Preventive measures against computer related crimes: approaching an individual [e-publikacija], preuzeto s https://doi.org/10.32914/i.51.3-4.7
24. Vlada Republike Hrvatske (06.06.2023.), Sjednica Vijeća za digitalnu transformaciju, preuzeto 17. ožujka 2024. s https://vlada.gov.hr/vijesti/sjednica-vijeca-za-digitalnu-transformaciju-za-ubrzanu-digitalizaciju-hrvatske-koristimo-znacajna-europska-sredstva/38458?lang=hr
25. Zakon o informacijskoj sigurnosti, Narodne novine br. 79/07 (2007.)
26. Zakon o kibernetičkoj sigurnosti, Narodne novine br. 14/24 (2024.)

27. Zavod za sigurnost informacijskih sustava i nacionalni CERT (2021.), Nacionalna taksonomija računalno-sigurnosnih incidenata [e-publikacija], preuzeto s https://www.cert.hr/wp-content/uploads/2021/12/Nacionalna-taksonomija-racunalno-sigurnosnih-incidenata.pdf
28. Weise J. (2001.), Public Key Infrastructure Overview [e-publikacija], preuzeto s http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf

POPIS SLIKA

POPIS TABLICA

ŽIVOTOPIS

Osobni podaci

Ime i prezime: Antonio Matošević
Datum rođenja: 07.04.1998.
Mjesto rođenja: Zagreb, Republika Hrvatska
E-mail: antonio.matosevic11@gmail.com
Mobilni telefon: +385992987515

Obrazovanje

2017. - 2024. Ekonomski fakultet Sveučilišta u Zagrebu, smjer Menadžerska informatika
2013. - 2017. I. gimnazija, Zagreb
2005. - 2013. Osnovna škola Gustava Krkleca, Zagreb

Radno iskustvo

2017. Financijska agencija - unos podataka u sustav
2018. Sustenta azvoj i upravljanje - Radovi na održavanju West Gate-a
2019. PRO MP - rad na visokonaponskim sustavima
2019 - 2022. General Logistics Systems - logistika
2022. - danas Winners sports hub - Gaming, rad u e-sportu

Strani jezici

Hrvatski jezik - materinji jezik (C2)
Engleski jezik (B2)
Njemački jezik (A2)

Osobne vještine i interesi

Izvrsno korištenje MS Office alata (Excel, Word, Outlook, PowerPoint)

Iskustvo rada u timu

Bizagi Modeler

Visual studio

OBS studio

Vozačka dozvola za automobil (B kategorija)

Nogomet

Gaming

Padel

Stolni tenis