UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA KIBERNETSKE VARNOSTI IZBRANE SPLETNE REŠITVE V TRANSPORTNI PANOGI

Ljubljana, oktober 2025 KRISTJAN MIHIN

IZJAVA O AVTORSTVU

Podpisani Kristjan Mihin, študent Ekonomske fakultete Univerze v Ljubljani, avtor predloženega dela z naslovom Analiza kibernetske varnosti izbrane spletne rešitve v transportni panogi, pripravljenega v sodelovanju s mentorjem doc. dr. Luko Tomatom

I Z J A V L J A M

1. da sem predloženo delo pripravil samostojno;

2. da je tiskana oblika predloženega dela istovetna njegovi elektronski obliki;

3. da je besedilo predloženega dela jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam oziroma navajam v besedilu, citirana oziroma povzeta v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani;

4. da se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Kazenskem zakoniku Republike Slovenije;

5. da se zavedam posledic, ki bi jih na osnovi predloženega dela dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom;

6. da sem pridobil vsa potrebna dovoljenja za uporabo podatkov in avtorskih del v predloženem delu in jih v njem jasno označil;

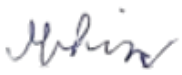
7. da sem pri pripravi predloženega dela ravnal v skladu z etičnimi načeli in, kjer je to potrebno, za raziskavo pridobil soglasje etične komisije;

8. da soglašam, da se elektronska oblika predloženega dela uporabi za preverjanje podobnosti vsebine z drugimi deli s programsko opremo za preverjanje podobnosti vsebine, ki je povezana s študijskim informacijskim sistemom članice;

9. da na Univerzo v Ljubljani neodplačno, neizključno, prostorsko in časovno neomejeno prenašam pravico shranitve predloženega dela v elektronski obliki, pravico reproduciranja ter pravico dajanja predloženega dela na voljo javnosti na svetovnem spletu preko Repozitorija Univerze v Ljubljani;

10. da hkrati z objavo predloženega dela dovoljujem objavo svojih osebnih podatkov, ki so navedeni v njem in v tej izjavi;

11. da sem preveril verodostojnost informacij, ki izhajajo iz zapisov na podlagi uporabe orodij umetne inteligence.

V Ljubljani, dne 16.10.2025 Podpis študenta: 

POVZETEK

Kibernetska varnost je področje, ki se ukvarja z zaščito računalniških sistemov, omrežij in podatkov pred nepooblaščenim dostopom, napadi ali škodljivo programsko opremo. Z naraščajočo digitalizacijo je pomen varovanja informacij še večji, saj grožnje postajajo vse bolj napredne in ciljno usmerjene. Ključni elementi kibernetske varnosti vključujejo močna gesla, redne varnostne posodobitve, uporabo požarnih zidov ter ozaveščanje uporabnikov o varni rabi tehnologije. Namen kibernetske varnosti je zagotoviti zaupnost, celovitost in razpoložljivost podatkov ter s tem varno digitalno okolje za posameznike in organizacije.

Magistrsko delo se osredotoča na kibernetsko varnost v izbranem podjetju. Cilji naloge so bili, primerjava različnih metod testiranja kibernetske varnosti, preverjanje stopnje varnosti izbrane spletne rešitve v transportni panogi, predlaganje izboljšav varnosti izbrane spletne rešitve in pa ocena ekonomske koristi implementacije ukrepov za izboljšanje kibernetske varnosti izbrane spletne rešitve. Naloga je bila sestavljena iz 2 delov, teoretičnega in praktičnega. V teoretičnem delu sem pregledal relevantno literaturo ter raziskal različne vrste testiranj kibernetske varnosti in prepoznavanja spletnih groženj ter strategij za zaščito pred njimi. V empiričnem delu pa sem se osredotočil na varnostno testiranje izbrane spletne rešitve v transportni panogi. Najprej sem predstavil izbrano rešitev, nato pa sem na primeru izbranega podjetja uporabil metode in pristope, obravnavane v teoretičnem delu. Na podlagi analize podatkov, pridobljenih z izvedenim varnostnim testiranjem sem ocenil, ali izbrana spletna rešitev izpolnjuje zahteve kibernetske varnosti.

Rezultati varnostnega preizkusa so pokazali, da je aplikacija tehnično razmeroma dobro zaščitena pred klasičnimi napadi, vendar vsebuje ranljivosti, kot sta nezaupanja vredni certifikat TLS in manjkajoča glava. Še večje tveganje pa predstavlja človeški dejavnik, polovica uporabnikov je kliknila na lažno povezavo, trije pa celo vnesli gesla, kar kaže na visoko ranljivost za socialni inženiring. Na podlagi ugotovitev so bila oblikovana priporočila za ureditev certifikata TLS, vključitev varnostne glave, uvedba večstopenjske avtentikacije, redna izobraževanja zaposlenih ter dodatni ukrepi, kot so opozorila o sumljivih prijavah in redna varnostna testiranja. Ti ukrepi bi namreč lahko bistveno izboljšali odpornost sistema in zmanjšali tveganja.

KLJUČNE BESEDE: kibernetska varnost, socialni inženiring, testiranje varnosti, TLS certifikat, večstopenjska avtentikacija, transportna panoga

CILJI TRAJNOSTNEGA RAZVOJA



ABSTRACT

Cybersecurity is a field of which the main function is protecting computer systems, networks, and data from unauthorized access, attacks, or malicious software. With increasing digitization, the importance of safeguarding information is even greater, as threats are becoming more advanced and targeted. Key elements of cybersecurity include strong passwords, regular security updates, the use of firewalls, and raising users' awareness about the safe use of technology. The purpose of cybersecurity is to ensure the confidentiality, integrity, and availability of data, thereby providing a secure digital environment for individuals and organizations.

My master's thesis focuses on cybersecurity in a selected company. The objectives were to compare different methods of cybersecurity testing, to verify the security level of a selected web solution in the transport sector, to propose improvements to the security of that web solution, and to assess the economic benefits of implementing measures to enhance its cybersecurity. The thesis consists of two parts theoretical and practical. In the theoretical part, I reviewed relevant literature and examined various types of cybersecurity testing and the identification of online threats, as well as strategies for protection against them. In the empirical part, I focused on security testing of the selected web solution in the transport sector. I first presented the chosen solution and then, using the example of the selected company, applied the methods and approaches discussed in the theoretical part. Based on analysis of the data obtained from the security testing, I assessed whether the selected web solution meets cybersecurity requirements.

The results of the security test showed that the application is technically relatively well protected against classic attacks, but it contains vulnerabilities such as an untrusted TLS certificate and a missing security header. An even greater risk is the human factor, half of the users clicked on a phishing link, and three even entered their passwords, indicating a high susceptibility to social engineering. Based on these findings, recommendations were formulated to fix the TLS certificate, include the security header, introduce multi-factor authentication, provide regular employee training, and adopt additional measures such as alerts about suspicious logins and regular security testing. These measures could significantly improve the system's resilience and reduce risks.

KEY WORDS: cybersecurity, social engineering, security testing, TLS certificate, multi-factor authentication, transport sector

SUSTAINABLE DEVELOPMENT GOALS



KAZALO

1 UVOD 1

2 KIBERNETSKA VARNOST PODJETJA 3

2.1 Opredelitev kibernetske varnosti 3

2.2 Različne vrste ter najpogostejše grožnje 4

2.2.1 Začetni kompromisi organizacij 4

2.2.2 Zlonamerna programska oprema 5

2.2.3 Zvabljanje 6

2.2.4 DDoS napadi 7

2.2.5 Izsiljevalska programska oprema 9

2.2.6 Grožnje, povezane z nastajajočimi tehnologijami 10

2.3 Zaščita pred grožnjami 10

2.3.1 Izobraževanje 11

2.3.2 Antivirusni programi 12

2.3.3 Požarni zid 12

2.3.4 Šifriranje podatkov 13

2.3.5 Dvofaktorska avtentikacija 13

2.3.6 Zaščita pred DDoS napadi 14

2.3.7 Umetna inteligenca kot zaščita pred grožnjami 14

2.4 Standardi 15

2.4.1 Nacionalni inštitut za standarde in tehnologijo 15

2.4.2 ISO 16

2.4.3 CIS 18

2.4.4 COBIT 19

3 STRATEGIJE KIBERNETSKE VARNOSTI 20

3.1 Strategija kibernetske varnosti 20

3.2 Vrste obstoječih strategij kibernetske varnosti 20

3.2.1 Strategija zaščite in obnove 20

3.2.2 Strategija zaščite končnih točk 21

3.2.3 Fizična kontrola in varnostna dovoljenja kot strategija kibernetske varnosti 21

3.2.4 Skladnost kot varnostna strategija 21

3.2.5 Strategija osredotočena na aplikacije 22
3.2.6 Strategija osredotočena na identiteto 22
3.2.7 Strategija osredotočena na podatke 22
3.2.8 Strategija osredotočena na napadalca 23
3.2.9 Strategija ničelnega zaupanja 23
4 METODE IN PRISTOPI TESTIRANJA KIBERNETSKE VARNOSTI 24
4.1 Penetracijski testi 24
4.1.1 Penetracijsko testiranje omrežij 25
4.1.2 Penetracijsko testiranje spletnih aplikacij 26
4.1.3 Penetracijsko testiranje s področja socialnega inženiringa 26
4.1.4 Penetracijsko testiranje odjemalcev 27
4.2 Identifikacija ranljivosti 27
4.3 SQL injekcije 28
4.4 Orodja za skeniranje ranljivosti sistema 29
4.4.1 Spletna orodja 30
4.4.2 Lokalna orodja 30
5 ANALIZA KIBERNETSKE VARNOSTI IZBRANE SPLETNE REŠITVE 31
5.1 Predstavitev izbrane spletne rešitve 31
5.2 Uporabljena metodologija 34
5.3 Izvedba preizkusa varnosti spletne rešitve 34
5.3.1 Testiranje varnosti z aplikacijo OWASP ZAP in intruder.io 35
5.3.2 Testiranje varnosti s pomočjo socialnega inženiringa 36
5.4 Analiza rezultatov 37
5.5 Predlogi za omilitev groženj 38
5.5.1 Ureditev certifikata TLS 38
5.5.2 Vključitev glave »Strict-Transport-Security« 39
5.5.3 Uvedba večstopenjske avtentikacije (MFA) 39
5.5.4 Redna ozaveščevalna izobraževanja uporabnikov 39
5.5.5 Dodatna priporočila 40
6 DISKUSIJA 40
6.1 Predstavitev ključnih ugotovitev 40
6.2 Primerjava ugotovitev iz literature in ugotovitve empiričnega dela 41

6.3 Omejitve raziskave....42
6.4 Smernice za nadaljnje delo....43
7 SKLEP....43
SEZNAM KLJUČNE LITERATURE....44
LITERATURA IN VIRI....44
PRILOGA....1

KAZALO SLIK

Slika 1: Primer vmesnika začetne strani....32
Slika 2: Primer obrazca za dodajanje dokumentov....32
Slika 3: Mobilna aplikacija....33
Slika 4: Primer elektronske pošte....37

KAZALO PRILOG

Priloga 1: Poročilo OWASP ZAP testa....1

SEZNAM KRATIC

angl. - angleško
2FA - (angl. Two-Factor Authentication); dvostopenjska avtentikacija
AI - (angl. Artificial Intelligence); umetna inteligenca
CCPA - (angl. California Consumer Privacy Act); kalifornijski zakon o varstvu zasebnosti potrošnikov
COBIT - (angl. Control Objectives for Information and Related Technologies); okvir za upravljanje informacijske tehnologije
CSRF - (angl. Cross-site Request Forgery); ponarejena zahteva iz druge strani
DDoS - (angl. Distributed Denial of Service); porazdeljeni napad onemogočanja storitve
DNS - (angl. Domain Name System); sistem domenskih imen
DLP - (angl. Data Loss Prevention); preprečevanje izgube podatkov
FBI – (angl. Federal Bureau of Investigation); Zvezni preiskovalni urad
GDPR - (angl. General Data Protection Regulation); splošna uredba o varstvu osebnih podatkov
HIPAA - (angl. Health Insurance Portability and Accountability Act); zakon o prenosljivosti in odgovornosti zdravstvenega zavarovanja
HTTP - (angl. HyperText Transfer Protocol); spletni komunikacijski protokol
HTTPS - (angl. HyperText Transfer Protocol Secure); varni HTTP-protokol

HSTS - (angl. HTTP Strict Transport Security); mehanizem za uveljavljanje uporabe HTTPS povezave
ICMP - (angl. Internet Control Message Protocol); internetni protokol za nadzorna sporočila
IEC - (angl. International Electrotechnical Commissio); Mednarodna elektrotehnična komisija
IoT - (angl. Internet of Things); internet stvari
IP - (angl. Internet Protocol); protokol za naslavljanje in prenos podatkov
IRC - (angl. Internet Relay Chat); protokol za spletno klepetanje
ISO - (angl. International Organization for Standardization); Mednarodna organizacija za standardizacijo
IT - (angl. Information Technology); informacijska tehnologija
MFA - (angl. Multi-Factor Authentication); večfaktorska avtentikacija
MBSA - (angl. Microsoft Baseline Security Analyzer); orodje za preverjanje osnovne varnosti sistemov Windows
MMS - (angl. Multimedia Messaging System); večpredstavnostni sporočilni sistem
NIST - (angl. National Institute of Standards and Technology); Nacionalni inštitut za standarde in tehnologijo
OWASP ZAP - (angl. Open Web Application Security Project - Zed Attack Proxy); odprtokodno orodje za testiranje spletnih aplikacij
SaaS - (angl. Software as a Service); programska oprema kot storitev
SMS - (angl. Short Message Service); sistem kratkih sporočil
SQL - (angl. Structured Query Language); jezik za upravljanje relacijskih baz
SSL - (angl. Secure Sockets Layer); protokol za varno komunikacijo
TCP - (angl. Transmission Control Protocol); zanesljiv protokol za prenos podatkov
TLS - (angl. Transport Layer Security); protokol za šifriranje in varno komunikacijo
UDP - (angl. User Datagram Protocol); protokol za hiter prenos podatkov
URL - (angl. Uniform Resource Locator); enotni naslov vira na spletu
USD - (angl. United States dollar); Ameriški dolar
WEP - (angl. Wired Equivalent Privacy); varnostni protokol za brezžična omrežja
WPA/WPA2 - (angl. Wi-Fi Protected Access); protokola za zaščito brezžičnih omrežij
XSS - (angl. Cross-site Scripting); vnos zlonamerne skripte v spletno stran

1 UVOD

Kibernetska varnost namreč še nikoli ni bila tako pomembna za komercialne družbe in javne organizacije. V času, ko svet vse bolj postaja odvisen od tehnologije in interneta, se kibernetski napadi krepijo. Svetovna gospodarstva slonijo na neprekinjenem delovanju tehnologije, nobena panoga ali geografska pokrajina pa ni imuna na kibernetske napade.

Vedno večja digitalizacija podjetij je močno vplivala na razvoj in delovanje vseh panog, še posebej pa je zelo spremenila razvoj v transportni panogi, kjer so spletne rešitve postale ključne za učinkovito delovanje sistemov in procesov. Ravno zaradi tega pa se je povečala odvisnost od spletnih tehnologij, ki pa posledično prinašajo tudi večje tveganje za kibernetske napade, ki lahko povzročijo gospodarsko ali družbeno škodo.

V letu 2021 je bila vrednost globalne industrije kibernetske varnosti ocenjena na približno 220 milijard dolarjev. Ob upoštevanju letne stopnje rasti 12 % bi do konca desetletja lahko dosegla približno 500 milijard dolarjev. Vse več ponudnikov kibernetske varnosti uporablja frazo »nenehno spreminjajoča se grožnja« za trženje svojih rešitev zaskrbljenim organizacijam (Spherical Insights, 2023).

Zaradi hitrega razvoja tehnologij v zadnjih nekaj letih so napadalci začeli uporabljati nove tehnike ter nova zmogljiva orodja za zlorabljanje varnosti sistemov, ki pa posledično ogrožajo zaščito zasebnih podatkov. Prav zaradi tega je nenehno izobraževanje novih in trenutnih uporabnikov sistemov, o pomenu kibernetske varnosti vse bolj pomembno. Najpogostejše napake se pogosto zgodijo prav zaradi tega, ker so zaposleni v podjetjih premalo ozaveščeni o grožnjah, na katere bi morali biti vedno pozorni (Kaur in Ramkumar, 2022).

V akademski in strokovni literaturi so na voljo številne smernice za zaščito informacij, med katerimi izstopajo tehnike odvračanja groženj ter zaznavanje in odzivanje na grožnje. Kljub temu se večina podjetij osredotoča predvsem na odvračanje groženj z uporabo trenutno dostopnih tehnoloških ukrepov (Ghelani, 2022).

Mednarodna telekomunikacijska zveza kibernetsko varnost opredeljuje kot zbirko orodij, politik, varnostnih zasnov, varnostnih zaščitnih ukrepov, smernic, pristopov k upravljanju tveganj, dejanj, usposabljanj, najboljših praks, zagotovil in tehnologij, ki se lahko uporabijo za zaščito kibernetskega okolja, ter sredstev organizacij in uporabnikov (Solms in Niekerk, 2013).

Ker živimo v dobi digitalizacije, je kibernetska varnost vedno bolj pomembna oziroma nujna. Zlorabe in napadi na kibernetske sisteme lahko povzročijo hude gospodarske, pravne in družbene posledice, vključno s krajo identitete, finančnimi izgubami ter okvaro kritične infrastrukture (Kamiya in drugi, 2018).

Organizacije v transportni panogi, ki stremijo k optimiziranju dobavnih verig in logističnih procesov, pa se soočajo z dodatnimi izzivi. Zaradi potrebe po hitri izmenjavi podatkov in zanesljivosti sistemov za sledenje pošiljk, so te organizacije izpostavljena napadom, ki lahko

ogrozijo učinkovitost njihovih sistemov. Spletne rešitve v transportni panogi so narejene za pomoč pri optimizaciji dobavnih verig in logističnih procesov, vendar pa lahko podjetja le ob ustrezni kibernetski zaščiti sistemov zagotovijo varno in učinkovito delovanje. Zato je ključnega pomena, da podjetja, ki uporabljajo, ali se odločajo za spletne rešitve v oblaku, razumejo prednosti in slabosti, ki jih le te prinašajo. Integracija sodobnih spletnih rešitev v transportni panogi organizacijam omogoča večjo učinkovitost, a obenem zahteva višjo stopnjo varnosti, ki je potrebna za preprečevanje vedno bolj naprednih kibernetskih groženj.

Namen magistrskega dela je razumeti, kakšne kibernetske grožnje so danes prisotne ob uporabi spletnih rešitev v transportni panogi in kako se pred njimi organizacije lahko učinkovito zaščitijo. V magistrskem delu sem proučil tudi metode, s katerimi lahko napadalci pridobijo zaupne podatke in grožnje kibernetske varnosti oblačnih sistemov ter analizo načinov prepoznavanja teh groženj in ukrepov za njihovo preprečevanje. Za dosego namena sem v svoji raziskavi zasledoval naslednje cilje:

- primerjati različne metode testiranja kibernetske varnosti,
- preverjati stopnjo varnosti izbrane spletne rešitve v transportni panogi,
- predlagati izboljšanje varnosti izbrane spletne rešitve in
- oceniti koristi implementacije ukrepov za izboljšanje kibernetske varnosti izbrane spletne rešitve.

Magistrsko delo je razdeljeno na 2 dela, teoretični in praktični. V teoretičnem delu sem pregledal relevantno literaturo ter raziskal različne vrste testiranj kibernetske varnosti, prepoznavanje spletnih groženj in strategije za zaščito pred njimi. Posebno pozornost sem namenil metodam in pristopom za testiranje kibernetske varnosti, ki bodo kasneje uporabljeni v praktičnem delu. Zaradi pojava novih oblik prevar sem se v teoretičnem delu tako spoznal z različnimi vrstami vdorov v sisteme in drugimi načini za zlorabo tehnologije za pridobivanje osebnih ali občutljivih podatkov. Prav tako sem predstavil, kaj narediti v primeru človeške napake, kako se lahko najbolje zavarujemo in pa tudi, kaj lahko stori podjetje, da zmanjša možnost uspešnih napadov, napak ljudi ali pomanjkljivosti informacijskih sistemov.

V empiričnem delu sem se osredotočil na varnostno testiranje izbrane spletne rešitve v transportni panogi. Najprej sem predstavil izbrano rešitev, nato pa sem na primeru izbranega podjetja uporabil metode in pristope, obravnavane v teoretičnem delu. Na podlagi analize podatkov, pridobljenih z izvedenim varnostnim testiranjem sem ocenil, ali izbrana spletna rešitev izpolnjuje zahteve kibernetske varnosti.

Po zaključku obeh delov sem kritično analiziral zbrane podatke ter predstavil dosežene rezultate. Na podlagi analize sem opredelil ključne pomanjkljivosti izbrane spletne rešitve in predlagal ustrezne ukrepe za njihovo odpravo. Izsledki te naloge lahko služijo kot smernice za izboljšanje kibernetske varnosti tudi pri drugih podobnih spletnih rešitvah, s čimer bi bilo mogoče učinkoviteje preprečiti potencialno ekonomsko škodo v transportni panogi, ki nastaja zaradi kibernetskih napadov oziroma neučinkovitega zagotavljanja varnosti spletnih rešitev.

Struktura magistrskega dela je zasnovana tako, da bralcu omogoča celovit vpogled v področje kibernetske varnosti s poudarkom na spletnih rešitvah v transportni panogi. Prvo poglavje opredeljuje temeljne pojme kibernetske varnosti in vrste najpogostejših groženj, skupaj z obstoječimi zaščitnimi ukrepi in mednarodnimi standardi. V drugem poglavju pa so obravnavane različne strategije kibernetske varnosti, ki jih organizacije uporabljajo za obrambo pred digitalnimi grožnjami. Tretje poglavje se osredotoča na metode in pristope testiranja varnosti, ki predstavljajo teoretično osnovo za empirični del naloge. Četrto poglavje pa vključuje podrobno analizo kibernetske varnosti izbrane spletne rešitve, izvedbo testiranj ter predstavitev rezultatov in predlogov za izboljšave le-teh. V petem poglavju sledi diskusija ključnih ugotovitev, medtem ko sklep povzame dosežene cilje in možnosti za nadaljnje raziskave.

2 KIBERNETSKA VARNOST PODJETJA

2.1 Opredelitev kibernetske varnosti

Kibernetska varnost označuje celovit sistem ukrepov za zaščito informacijskih sistemov, omrežij in podatkov pred kibernetskimi grožnjami. V sodobni digitalni dobi se kibernetska varnost obravnava kot ključni element nacionalne varnosti, varstva osebnih podatkov in zaščite poslovnih informacijskih struktur.

Kibernetska varnost presega zgolj zaščito informacij, ki vključuje tudi zaščito strojne opreme, programske opreme, omrežij in procesov, ki omogočajo digitalno delovanje sistemov. Ta celoviti pristop je ključen za zanesljivo delovanje informacijske družbe. Arina in Anatolie Alexei izpostavljata, da je kibernetska varnost usmerjena predvsem proti zunanjim napadom, pri čemer vključuje mehanizme za preprečevanje, zaznavanje in odzivanje na kibernetske incidente, ki lahko ogrozijo delovanje sistemov ali krajo podatkov (Alexei in Alexei, 2022).

V praktičnem smislu je kibernetska varnost, usmerjena v zagotavljanje preprečevanja, zaščite in odpornosti sistemov pred naslednjimi vrstami groženj: nepooblaščen dostop, virusi, izsiljevalska programska oprema, napadi z zavrnitvijo storitve (angl. Distributed denial of service - v nadaljevanju DDoS) in manipulacije z informacijami. Članek Patel podaja klasifikacijo kibernetskih groženj ter poudarja pomembnost stalnega spremljanja in izobraževanja uporabnikov kot ključen obrambni mehanizem (Patel, 2017).

Nazadnje, Althonayan in Andronache v svoji raziskavi predlagata prehod iz tradicionalnega pogleda na informacijsko varnost v bolj holistični okvir kibernetske varnosti. Poudarjata, da je zaradi porasta medsebojno povezanih naprav oz. interneta stvari (angl. Internet of things – v nadaljevanju IoT), mobilnih tehnologij in globalne digitalizacije nujno, da se kibernetska varnost obravnava kot strateška in vseobsegajoča sistemska zasnova (Andronache in Althonayan, 2018).

2.2 Različne vrste ter najpogostejše grožnje

Kibernetske grožnje so raznolike in nenehno spreminjajoče se nevarnosti, ki ciljajo na informacijske sisteme, infrastrukture in uporabnike. Te grožnje lahko povzročijo izgubo podatkov, finančno škodo, ohromitev sistemov in kršitev zasebnosti. Razvrščamo jih glede na naravo napada, cilje ter uporabljena orodja in tehnike.

Eksponentna rast internetne povezanosti je pripeljala do znatnega povečanja incidentov kibernetskih napadov, ki imajo pogosto katastrofalne in resne posledice. Glavno orožje za izvedbo zlonamernih namenov v kibernetskem prostoru ostaja zlonamerna programska oprema. Številne spletne aplikacije še vedno vsebujejo osnovne varnostne napake, kot so pomanjkanje preverjanja vhodnih podatkov in neustrezno šifriranje. Napake pogosto izvirajo iz nepodučene rabe spletnih ogrodij ter pomanjkanja zavedanja razvijalcev o varnostnih praksah, kar vodi do ponavljajočih se ranljivosti. To še posebej velja za aplikacije v hitro rastočih sektorjih, kot je transport, kjer se funkcionalnost pogosto postavlja pred varnost (Jang-Jaccard in Nepal, 2014).

2.2.1 Začetni kompromisi organizacij

Čeprav so kibernetske grožnje raznolike in kompleksne, številne strokovne raziskave in praktične izkušnje iz odzivov na incidente kažejo, da so le-ti vedno znova rezultat petih ključnih vektorjev začetnega kompromisa. Ta temeljna resnica, ki jo poudarja tudi sodobna Microsoftova in neodvisna varnostna stroka, je osnova vsake učinkovite strategije kibernetske varnosti (Rains, 2023).

Ranljivosti v programski in strojni opremi so ena najpogostejših vstopnih točk za napadalce. Številni zgodovinski incidenti so namreč bili posledica nepravočasnega popravila znanih ranljivosti. Danes je namreč nadzor in sprotno posodabljanje vseh naprav v organizaciji absolutni minimum varnostne higiene (Rains, 2023).

Privzete ali nepravilne nastavitve npr. gesla, nepotrebne odprte storitve, napačne pravice so redna tarča napadalcev. Pogosto se pojavljajo pri spletnih strežnikih, požarnih zidovih, oblačnih storitvah in IoT napravah. Skoraj polovica varnostnih incidentov je neposredno povezanih s slabo konfiguracijo, ki omogoči stopnjevanje dostopa ali “pivotiranje” v notranje omrežje (Rains, 2023).

Ponavljajoča se uporaba gesel, preprosta gesla, ali pa gesla, ki so že bila kompromitirana v prejšnjih napadih, so izjemno nevarna. Z napredkom orodij za “napad z grobo silo” (angl. Brute force) in avtomatizirano testiranje, ter javno objavljenimi bazami ukradenih gesel, je geslo kot edina zaščita danes neustrezno. Implementacija večfaktorske avtentikacije (angl. Multifactor authentication - v nadaljevanju MFA) in nadzor nad privilegiranimi računi je postal nujen (Rains, 2023).

Najpogostejša vstopna točka, kjer napadalec žrtev zavede, da sama omogoči dostop npr. zvabljanje (angl. Phishing), lažne povezave, telefonske prevare. Statistično večina “uspešnih” vdorov v organizacije vključuje element socialnega inženiringa. Usposabljanje uporabnikov in stalno simuliranje napadov je ključno za zmanjšanje uspešnosti teh vektorjev (Rains, 2023).

Napake ali zlonamerno delovanje zaposlenih, administratorjev ali partnerjev lahko povzročijo hujše varnostne incidente kot zunanji napadi. Ločimo nenačrtovane napake, npr. napačno posredovane podatke ter zavestno zlonamerna dejanja. Temeljno je omejevanje pravic, spremljanje in revizija dostopov ter ločitev nalog (Rains, 2023).

2.2.2 Zlonamerna programska oprema

Zlonamerna koda (angl. malware), je skupno ime za različne oblike sovražne ali vsiljive programske opreme. Kibernetski kriminalci jo razvijajo z namenom kraje podatkov, obhoda varnostnih mehanizmov in pridobivanja nepooblaščenega dostopa do osebnih računalnikov, pogosto pa tudi za poškodovanje ciljanega sistema, njegovih podatkov ali aplikacij (Alenezi in drugi, 2020).

Razvoj bolj inovativnih in učinkovitih obrambnih mehanizmov proti zlonamerni programski opremi je prepoznan kot nujna potreba v skupnosti kibernetske varnosti. Napadalci izkoriščajo tako znane ranljivosti obstoječe strojne in programske opreme kot tudi specifične lastnosti nastajajočih tehnologij (Jang-Jaccard in Nepal, 2014).

Danes je industrija zlonamerne programske opreme postala izjemno dobičkonosna, kar je spodbudilo dodatna prizadevanja kibernetskih napadalcev ter povzročilo eksponentno rast števila, vrst in kompleksnosti ustvarjene zlonamerne kode. Poleg tega običajna protivirusna programska oprema pogosto ne zazna mutacij ali različic zlonamerne programske opreme, zaradi česar so uporabniki in sistemi ranljivi ves čas. Zlonamerna programska oprema se v osnovi deli na dve glavni kategoriji prvo generacijo in drugo generacijo. Prva generacija ostaja nespremenjena po okužbi sistema, medtem ko druga generacija prilagaja svojo strukturo pri vsaki novi okužbi in ustvarja nove različice. Dinamična zlonamerna koda se dodatno razvršča na metamorfno, šifrirano, polimorfno in oligomorfno zlonamerno programsko opremo. Poleg tehničnega vidika jo lahko razvrstimo tudi glede na cilje, ki jih dosega denimo izsiljevalska programska oprema (angl. Ransomware), ki cilja na finančne podatke, vohunska programska oprema (angl. spyware), ki cilja na krajo zaupnih informacij, medtem ko beležilci pritiskov tipk (angl. keyloggers) zajemajo uporabniška imena in gesla. Razvoj zlonamerne programske opreme je razdeljen na pet časovnih faz. V prvi fazi so se pojavile najzgodnejše oblike zlonamerne kode, v drugi so prišli prvi črvi za Windows in elektronsko pošto. Tretja faza sovpada z razmahom interneta, ko so postali razširjeni mrežni črvi. V četrti fazi so se pojavili "rootkit-i" in izsiljevalska programska oprema najnevarnejše oblike do tedaj. Peta, torej trenutna faza, pa vključuje prefinjeno zlonamerno programsko opremo, ki jo ustvarjajo celo tajne službe nekaterih držav za namene vohunjenja (Alenezi in drugi, 2020).

2.2.3 Zvabljanje

Zvabljanje je tehnika socialnega inženiringa, ki uporablja različne metode za vplivanje na ciljno žrtev, da ta nehote razkrije osebne podatke, kot so elektronski naslov, uporabniško ime, geslo ali finančne informacije. Napadalci nato te informacije uporabijo v škodo žrtve. Ime zvabljanje izvira iz angleške besede »fishing« (ribolov). Logika izraza je preprosta, napadalec uporabi »vabo« (angl. bait), da privabi žrtev, nato pa »ulovi« želene občutljive podatke. To je eno najpogostejših in najbolj razširjenih metod kibernetskih napadov, pri čemer napadalci nenehno iščejo nove pristope in uporabljajo različne komunikacijske kanale (Alabdan, 2020).

Nove tehnološke platforme, kot so družbena omrežja, računalništvo v oblaku in pametni telefoni, so postale tarče napadalcev, ki uporabljajo prefinjene napade zvabljanja. To pogosto vključuje prilagojene napade (usmerjeno zvabljanje ali angl. Spear phishing), ki izkoriščajo specifične ranljivosti teh tehnologij in uporabniško neozaveščenost (Jang-Jaccard in Nepal, 2014).

Posebna oblika napadov zvabljanja, t. i. ciljno usmerjeno zvabljanje, ostaja najbolj pogost način širjenja zlonamerne programske opreme, v letu 2018 ga je uporabilo kar 71 % napadalnih skupin, v letu 2019 pa 65 %. Prav tako se je med letoma 2017 in 2018 število »zvabljajoč« enotni naslovov vira na spletu (angl. Uniform Resource Locator - v nadaljevanju URL) povečalo za 20 %, pri čemer je dve tretjini teh strani uporabljalo protokol za varno komunikacijo (angl. Secure Sockets Layer - v nadaljevanju SSL). Ta podatek je vznemirljiv, saj pomeni, da uporaba varnega spletnega komunikacijskega protokola (angl. HyperText Transfer Protocol Secure - v nadaljevanju HTTPS) ni več zanesljiv kazalnik varnosti spletnega mesta, kar dodatno otežuje razlikovanje med legitimnimi in zlonamernimi spletnimi stranmi (Alabdan, 2020).

V zadnjih letih so se napadalci s pomočjo tehnik zvabljanja osredotočili predvsem na storitve programske opreme kot storitev (angl. Software as a Service - v nadaljevanju SaaS) in spletno pošto, ki skupaj predstavljajo kar 33 % vseh napadov zvabljanja, usmerjenih proti različnim industrijam. Podjetje IBM je ugotovilo, da se je leta 2018 kar 27 % napadov zvabljanja osredotočalo na storitve spletne pošte. Poleg tega je analiza IBM-ove skupine X-Force pokazala, da je bil pri 29 % kibernetskih vdorov v podjetja glavni vzrok »zvabljajoča« e-pošta, kar potrjuje razširjenost in učinkovitost te oblike napada. Leta 2018 je FBI prejel okoli 100 prijav, povezanih z napadi, pri čemer so bile najpogosteje tarče sektorji zdravstva, izobraževanja in letalskega prometa. Kombinirana škoda v teh sektorjih je znašala okoli 100 milijonov ameriških dolarjev (angl. United States dollar - v nadaljevanju USD). Napadalci so s pomočjo »zvabljajoče« e-pošte pridobili prijavne podatke zaposlenih in nato dostopali do plačilnih sistemov podjetij. Po vdoru so uvedli spremembe pravil, da zaposleni niso več prejemali obvestil o spremembah na svojih računih. Na ta način so napadalci lahko spremenili podatke za neposredno nakazilo plač, sredstva pa so bila preusmerjena na njihove račune, pogosto v obliki predplačniških kartic. Zvabljanje je odigralo ključno vlogo tudi pri prvem uspešnem kibernetskem napadu na elektroenergetsko omrežje, ki se je zgodil v Ukrajini

decembra 2015. Osebje informacijske tehnologije (angl. Information technology - v nadaljevanju IT) in sistemski administratorji več podjetij, ki so bila odgovorna za distribucijo električne energije, so postali tarče ciljanih napadov usmerjenega zvabljanja. Napad je vključeval zlonameren dokument Microsoftov Word, ki je uporabnika pozval k omogočanju makrov. Ko je ta zahtevek potrdil, se je na računalnik namestila zlonamerna programska oprema BlackEnergy3, ki je napadalcem omogočila prikrit dostop do sistema. Končna posledica tega napada je bil uspešen izpad 30 transformatorskih postaj, kar je približno 230.000 prebivalcev pustilo brez električne energije do šest ur (Alabdan, 2020).

Tehnike zvabljanja lahko v osnovi razdelimo na tri temeljne komponente:

- Medij, komunikacijski kanal, prek katerega napadalec komunicira z žrtvijo.
- Vektor, pot napada, torej konkretni način izvedbe.
- Tehnični pristop, tehnologije in metode, ki se uporabljajo za izvedbo napada.

Zvabljanje preko glasu (angl. Vishing) je metoda zvabljanja, pri kateri napadalec uporablja glasovno komunikacijo, običajno telefonijo s pomočjo interneta. Z lažnim prikazom številke t. i. spoofing klic deluje, kot da prihaja iz legitimnega vira. Z avtomatiziranimi sistemi in nizkimi stroški komunikacije napadalci učinkovito manipulirajo z žrtvami, pogosto starejšimi osebami, ki so nagnjene k zaupanju telefonskim klicem, še posebej če je v igri lažno predstavljanje uradne institucije (Alabdan, 2020).

Zvabljanje preko sistema kratkih sporočil (angl. Short Message Service - v nadaljevanju SMS) in večpredstavnostnega sporočilnega sistema (angl. Multimedia Messaging System - v nadaljevanju MMS) (angl. Smishing), ki predstavlja zlorabo storitev kratkih sporočil, kjer napadalec žrtvi pošlje sporočilo z nujno vsebino, ki naj bi prihajala iz banke ali druge institucije. Sporočilo vsebuje povezavo ali številko, kjer mora žrtev vnesti osebne podatke. Alternativno pa vsebuje neposredno povezavo do zlonamerne programske opreme, ki se namesti na napravo in omogoča nadaljnjo eksfiltracijo podatkov (Alabdan, 2020).

Zvabljanje preko spleta, najširše uporabljen medij za zvabljanje ostaja internet, predvsem v obliki e-poštnih sporočil. Ta lahko vsebujejo lažne povezave, ponarejene prijavne obrazce ali zlonamerne priponke. Podobno so ranljiva tudi družbena omrežja, kjer napadalci uporabljajo lažne profile za izvedbo psihološke manipulacije npr. romantika, nagradne igre, medtem ko spletne strani pogosto posnemajo videz legitimnih portalov (Alabdan, 2020).

Druge pogosto zlorabljene poti so takojšnje sporočilne platforme npr. WhatsApp, Telegram, eFax storitve, lažne spletne strani ter lažne Wi-Fi dostopne točke, ki prestrezajo podatke uporabnikov na javnih omrežjih (Alabdan, 2020).

2.2.4 DDoS napadi

DDoS predstavljajo eno izmed najresnejših in najpogosteje uporabljenih oblik kibernetskih napadov današnjega časa. Cilj takšnih napadov je preobremeniti omrežje, spletno storitev ali

aplikacijo z izjemno količino prometa oziroma zlonamernih zahtev, kar ima za posledico nedostopnost storitve za legitimne uporabnike (Mahmood in Avcı, 2024).

Kritična infrastruktura, kot so energetski, transportni in komunikacijski sistemi, je vse bolj pogosta tarča DDoS napadov, ki lahko povzročijo dolgotrajne izpade in resne posledice za varnost držav in regij (Jang-Jaccard in Nepal, 2014).

Motivacija napadalcev se razlikuje od izsiljevanja in politične motivacije, do prikrivanja drugih kibernetskih dejanj, kot so vdori ali kraje podatkov. Med najbolj odmevnimi primeri napadov sodijo napad na podjetje Dyn leta 2016, največji zabeležen DDoS napad na GitHub leta 2018 ter napad na blog KrebsOnSecurity. Ključno vlogo pri izvajanju DDoS napadov igrajo botneti, sestavljeni iz okuženih naprav, ki pošiljajo sinhronizirane zahteve in tako izčrpavajo ključne vire, kot so pasovna širina, pomnilnik in procesorska moč. Obstajajo različne vrste DDoS napadov glede na omrežno plast, na katero ciljajo:

- volumetrični napadi, ki z obsegom prometa izčrpajo pasovno širino,
- napadi na protokole, ki izrabljajo ranljivosti v skladu zanesljivega protokola za prenos podatkov (angl. Transmission Control Protocol - v nadaljevanju TCP) in protokola za naslavljanje in prenos podatkov (angl. Internet Protocol - v nadaljevanju IP),
- napadi na aplikacijski plasti, ki ciljata na funkcionalnosti, kot so spletni komunikacijski protokol (angl. HyperText Transfer Protocol - v nadaljevanju HTTP) ali poizvedbe sistema domenskih imen (angl. Domain Name System – v nadaljevanju DNS), in tako simulirajo običajno uporabniško vedenje.

Posebej nevarni so slednji, saj zaradi svoje podobnosti legitimnemu prometu močno otežujejo zaznavo (Mahmood in Avcı, 2024).

DDoS napad je sestavljen iz štirih osnovnih komponent napadalca, nadzornikov, agentov in končne žrtve. Napadalec izkoristi ranljivosti sistemov in nanje namesti zlonamerno programsko opremo, ki omogoča oddaljeno nadzorovanje prek handlerjev. Ti nadzorujejo agente, ki usmerjajo škodljiv promet proti cilju. Celoten napad se začne z izbiro primernih agentov, kar vključuje ranljive sisteme z zadostnimi viri, ki se kompromitirajo ročno ali z uporabo avtomatiziranih orodij, kot so črv Ramen ali Code Red. Za komunikacijo med napadalcem, handlerji in agenti se uporabljajo protokoli TCP, protokol za hiter prenos podatkov (angl. User Datagram Protocol - v nadaljevanju UDP) ali internetni protokol za nadzorna sporočila (angl. Internet Control Message Protocol - v nadaljevanju ICMP), in pa tudi kanali protokola za spletno klepetanje (angl. Internet Relay Chat - v nadaljevanju IRC), ki omogočajo ustvarjanje tajnih komunikacijskih poti. Agenti, imenovani tudi »zombie bots«, so pogosto programirani, da delujejo prikrito in uporabljajo le minimalne sistemske vire, kar omogoča, da ostanejo neodkriti (Douligeris in Mitrokotsa, 2004).

Posebej nevaren je model IRC »temelječih napadov«, saj ponuja visoko stopnjo anonimnosti, če je komunikacija pravilno izvedena. IRC omrežja omogočajo ustvarjanje zasebnih kanalov,

kjer napadalec ni potreben kot stalen nadzornik, saj agenti samodejno poročajo o svoji prisotnosti. Med najbolj znanimi orodji, ki omogočajo izvedbo DDoS napadov, so Trinoo (prvi široko uporabljen UDP flood napadni sistem), Tribe Flood Network (TFN), TFN2K (nadgradnja TFN s šifrirano komunikacijo in prikritimi ukazi), Stacheldraht (zmožnost samodejnih posodobitev agentov), Shaft (dinamična menjava naslovov handlerjev med napadom) in mstream (ACK flooding orodje). Orodja IRC, kot so Trinity, Knight in Kaiten, dodatno uvajajo napade s TCP fragmenti, TCP RST in TCP z naključnimi zastavicami, kar povečuje variabilnost in možnost prikrivanja napada (Douligeris in Mitrokotsa, 2004).

Klasifikacija DDoS napadov je večdimenzionalna. Po stopnji avtomatizacije ločimo ročne, polavtomatske in avtomatske napade. Polavtomatski napadi omogočajo posredno komunikacijo prek handlerjev, medtem ko avtomatski napadi omogočajo minimalen stik napadalca z agenti, saj so vsi parametri napada (cilj, čas, trajanje) že programirani. Glede na vrsto izkoriščene ranljivosti ločimo poplavne napade, amplifikacijske napade, protokolne napade ter napade z napačnimi paketi (napadi z istimi IP-naslovi ali z naključnimi opcijami v IP paketih). Po dinamiki se napadi ločijo na stalne in spremenljive, kar napadalcem omogoča izogibanje zaznavanju. Po učinku pa ločimo disruptivne (popolna prekinitev storitve) in degradacijske napade (upočasnitev delovanja brez takojšnje zaznave). Amplifikacijski napadi izkoriščajo reflektorje (npr. DNS strežnike, usmerjevalnike), ki pošiljajo škodljiv promet žrtvi z lažno navedenimi naslovi pošiljateljev. DDoS napadi so nevarni zaradi svoje decentralizirane narave, visoke stopnje anonimnosti in težavnosti zaznavanja. Tradicionalni varnostni mehanizmi niso več dovolj. Za uspešno obrambo so potrebne napredne metode, kot so sistemi za zaznavanje anomalij, filtriranje prometa in uporaba umetne inteligence za identifikacijo nenavadnega vedenja v omrežju. Z razvojem tehnologij in povečano uporabo IoT naprav se bo kompleksnost teh napadov še povečevala, kar zahteva sistematičen in multidisciplinaren pristop k varovanju informacijske infrastrukture (Douligeris in Mitrokotsa, 2004).

2.2.5 Izsiljevalska programska oprema

Eden najuspešnejših modelov kibernetskega izsiljevanja je nedvomno izsiljevalska programska oprema, torej škodljiva programska oprema, ki zaklene podatke ali sisteme žrtve in nato zahteva odkupnino za njihovo odklepanje.

Napadi z izsiljevalno programsko opremo so se iz preprostih začetkov razvili v globalne, avtomatizirane in zelo prefinjene operacije. Uporaba novih tehnologij, kot so kriptovalute in anonimni komunikacijski kanali, omogoča napadalcem še večjo anonimnost in učinkovitost pri zbiranju odkupnin (Jang-Jaccard in Nepal, 2014).

Ta metoda je iz preprostih in tehnično pomanjkljivih začetkov prerasla v globalni posel, ki letno povzroča škodo v višini več milijard dolarjev. Danes so napadi prefinjeni, globalni in avtomatizirani. Zlonamerna koda se prenaša prek spletnih protokolov, pogosto v obliki prilog v lažnih elektronskih sporočilih, preko okuženih spletnih strani ali ranljivosti v programski

opremi. Glavna orodja napadalcev so Exploit Kiti, družbeni inženiring, prefinjeni kriptografski algoritmi ter kriptovalute, ki omogočajo anonimna plačila (O'Kane in drugi, 2018).

Uspešna izvedba napada z izsiljevalno programsko opremo pa temelji na naslednjih pogojih:

- Enkripcija, prehod s simetričnih ključev na asimetrične algoritme pomeni, da dešifriranje podatkov brez zasebnega ključa, ki ga ima le napadalec, postane skoraj nemogoče.
- Plačila z Bitcoini, izsiljevalska programska oprema je izkoristila popularnost kripto valut, saj omogočajo visoko stopnjo anonimnosti. Transakcije se beležijo v blockchainu, identitete pa ostajajo skrite za psevdonimi.
- Razvoj izsiljevalske programske opreme kot dejavnost (angl. Ransomware-as-a-Service - v nadaljevanju RaaS), kriminalci, ki nimajo tehničnega znanja, lahko zdaj najamejo že pripravljena orodja in infrastrukturo za napade, s čimer je vstopna ovira močno znižana.
- Družbeni inženiring, zlonamerna programska oprema je pogosto skrita v legitimno videnih dokumentih, lažnih obvestilih o dostavi ali opozorilih varnostnih služb.

Ti napadi pogosto sledijo postopku, da v prvem koraku žrtev prejme lažno elektronsko sporočilo z okuženo prilogo ali povezavo, nato s klikom sproži prenos izsiljevalne programske opreme, program kontaktira z t. i. Command-and-Control (C&C) strežnik, pridobi javni ključ in začne šifrirati podatke na disku in povezanih omrežjih. Po zaključku se na zaslonu prikaže opozorilo z navodili za plačilo, ali plačilo ni izvedeno pravočasno, napadalci pogosto grozijo z dodatno škodo (brisanje datotek, objava občutljivih podatkov itd.).

Zaradi množične okužbe potencialno milijonov uporabnikov po vsem svetu, imajo kriminalci izjemno razmerje med vloženim trudom in izkupičkom. Ocenjeno je, da zgolj 1-3 % žrtev plača odkupnino, vendar ta odstotek zaradi velike baze tarč vseeno pomeni milijonske prihodke. Izsiljevalska programska oprema danes ni več domena posameznikov, temveč organiziranega kriminala z razdeljenimi vlogami razvijalci, posredniki, »podjetniki«, ki tržijo RaaS storitve in tudi mešalci Bitcoin transakcij za pranje denarja (O'Kane in drugi, 2018).

2.2.6 Grožnje, povezane z nastajajočimi tehnologijami

Nastajajoče tehnologije, kot so družbena omrežja, računalništvo v oblaku, pametni telefoni in IoT naprave, prinašajo nove ranljivosti, ki jih kibernetski napadalci izkoriščajo za izvajanje napadov. Družbena omrežja omogočajo hitro širjenje zlonamerne kode, računalništvo v oblaku prinaša tveganja za izgubo podatkov in krajo identitete, IoT naprave pa so pogosto slabo zavarovane in predstavljajo enostavne tarče za vključitev v botnete in izvajanje DDoS napadov (Jang-Jaccard in Nepal, 2014).

2.3 Zaščita pred grožnjami

Pred grožnjami se lahko zaščitimo na več različnih načinov. Učinkovita zaščita vključuje kombinacijo tehničnih in organizacijskih ukrepov, ki zmanjšujejo verjetnost kibernetskih incidentov ter omejujejo njihov vpliv. Ključno je, da organizacije razvijejo celostno varnostno

strategijo, ki zajema tako ozaveščanje zaposlenih kot uporabo naprednih varnostnih tehnologij. Med najpomembnejše elemente zaščite sodijo stalno izobraževanje uporabnikov, uporaba zanesljivih antivirusnih programov, postavitev požarnih zidov, šifriranje občutljivih podatkov ter uporaba večfaktorske avtentikacije za preverjanje pristnosti. Požarni zidovi delujejo kot primarna obrambna plast, ki preverja nepooblaščen dostop do omrežja. Protivirusna programska oprema, ki pregleduje in odstranjuje škodljivo programsko opremo. Šifriranje deluje kot zaščitni ščit, ki podatke pretvori v neberljivo obliko in tako zagotovi njihovo varnost med prestrezanjem. Na koncu pa dvostopenjska avtentikacija izboljša varnost s tem, da zahteva dodatni korak preverjanja poleg samega gesla. Vsak od teh pristopov predstavlja pomemben steber v obrambi pred kibernetskimi grožnjami, zato bodo v nadaljevanju podrobneje predstavljeni (George in drugi, 2023).

2.3.1 Izobraževanje

Izobraževanje zaposlenih in uporabnikov informacijskih sistemov predstavlja enega izmed najpomembnejših elementov zaščite pred kibernetskimi grožnjami. Četudi so implementirani najnaprednejši varnostni mehanizmi, ostajajo človeški dejavniki in napake uporabnikov pogosto najšibkejši člen informacijske varnosti. Uporabniki, ki ne razumejo groženj, kot so napadi zvabljanja, socialni inženiring ali uporaba šibkih gesel, so pogosto tarče napadalcev, ki izkoriščajo ravno neozaveščenost. Redna varnostna izobraževanja povečajo odpornost organizacije na napade, saj uporabniki pridobijo znanje o prepoznavanju sumljivih dejavnosti, varni rabi interneta, pravilnem ravnanju z občutljivimi informacijami in postopkih ob zaznavi incidenta. Poleg tega izobraževanje spodbuja kulturo varnosti, kjer se varnostne prakse obravnavajo kot del vsakodnevnega delovanja.

Zakaj je to izobraževanje tako pomembno? Prvič, pripravi posameznike na prepoznavanje in ustrezen odziv. Naučijo se razlikovati med resničnimi in lažnimi e-poštnimi sporočili, razumejo tveganja priponk iz neznanih virov in se zavedajo pasti na videz nedolžnih povezav. Tako se zmanjšuje možnost uspešnega napada. V podjetjih, kjer imajo zaposleni dostop do občutljivih podatkov, je takšno usposabljanje nujno potrebno. Poročilo podjetja Verizon iz leta 2020 navaja, da je bilo kar 28 % varnostnih incidentov posledica zaposlenih. Njihove napake pa lahko vodijo do izgub podatkov, finančnih izgub in izgub ugleda. Z ustreznim izobraževanjem se te nevarnosti bistveno zmanjšajo. Učinkovit pristop k izobraževanju so simulacije resničnih položajev, npr. lažna »zvabljajoča sporočila« ali navidezni napadi z izsiljevalsko programsko opremo. To spodbuja izkustveno učenje, ki je pogosto učinkovitejše od teorije, saj omogoča praktične izkušnje v varnem okolju (George in drugi, 2023).

Kibernetske grožnje se nenehno spreminjajo, zato letni seminar ni več dovolj. Potrebni so pogosti osvežitveni tečaji, sledenje vedenju uporabnikov in redne nadgradnje znanja. Pomembno je tudi, da organizacije gojijo kulturo kibernetske varnosti. Vodstvo mora s svojim zgledom pokazati zavezanost varnosti in poudarjati njen pomen na vseh ravneh podjetja. Cilj je, da vsi razumejo svojo vlogo pri zaščiti digitalnega okolja. Tehnologija je sicer ključno

orodje pri vzpostavljanju digitalne imunosti, a ljudje so tisti, ki odločajo, ali bodo ta orodja pravilno uporabljali (George in drugi, 2023).

2.3.2 Antivirusni programi

Antivirusni oziroma protivirusni programi so ena izmed glavnih komponent pri preprečevanju groženj. Osnovna naloga je prepoznavanje in odstranjevanje zlonamerne programske opreme (malware), s čimer preprečuje škodo v digitalnem okolju. Zlonamerna programska oprema se pojavlja v različnih oblikah, kot so virusi, črvi, trojanski konji, izsiljevalska programska oprema, vohunski programi (spyware), pri čemer ima vsaka svoje posebnosti, a skupni cilj je motenje, poškodovanje ali nepooblaščen dostop do sistemov. Protivirusna programska oprema je tako prva linija obrambe pred temi nevarnostmi (George in drugi, 2023).

Antivirusni programi delujejo na 2 glavni metodi zaznavanja groženj (George in drugi, 2023):

- Zaznava na podlagi podpisov uporablja podatkovno bazo znanih vzorcev t. i. podpisov zlonamerne kode. Program primerja datoteke s temi vzorci in ob ujemanju zazna grožnjo,
- Vedenjska analiza, uporablja analizo vedenja programov. Če program izvaja sumljive dejavnosti, kot je spreminjanje sistemskih nastavitev ali dostop do zaščitenih datotek, ga antivirus označi kot potencialno grožnjo.

Ko antivirusni program zazna grožnjo, jo odstrani, izolira v karanteno, ali trajno izbriše. Sodobni protivirusni programi vključujejo še dodatne varnostne funkcije zaščito e-pošte, nadzor prenosa datotek, zaščito pred lažnimi spletnimi stranmi in funkcije za zaščito zasebnosti na spletu. Pomembna značilnost teh programov je zaščita v realnem času, kjer se datoteke preverjajo že med samim dejanjem, kar pomeni, da lahko program zazna in nevtralizira grožnjo, še preden le-ta povzroči škodo. Večina protivirusnih rešitev omogoča samodejno posodabljanje, kar je ključnega pomena za obrambo pred najnovejšimi grožnjami. V hitro spreminjajočem se kibernetskem okolju je prilagajanje oziroma posodabljanje nujno, ne le priporočeno (George in drugi, 2023).

2.3.3 Požarni zid

Požarni zid učinkovito nadzoruje in blokira nepooblaščen dostop. Poznamo več različnih vrst požarnih zidov od enostavnih filtrov paketov, ki pregledujejo podatke na podlagi vnaprej določenih pravil, do naprednih požarnih zidov na aplikacijski ravni, ki preverjajo podatke glede vsebine in vedenja. Ne glede na kompleksnost imajo vsi enoten cilj, dopustiti zakonit promet in preprečiti sumljive ali škodljive dejavnosti. Požarni zid deluje kot nadzorna točka med notranjim omrežjem npr. osebnim računalnikom ali omrežjem podjetja in zunanjim svetom, običajno internetom. Pregleduje vsak podatkovni paket, ki želi prestopiti to mejo, in na podlagi nastavljenih pravil odloča, kateri promet dovoli in kateri zavrne. Vsak paket se pregleda glede na vire, cilje in druge parametre, preden se sprejme odločitev o njegovem prehodu (George in drugi, 2023).

Tradicionalni požarni zidovi so bili osredotočeni predvsem na zaščito omrežnega perimetra. Vendar pa so mobilne naprave, računalništvo v oblaku in delo na daljavo povzročili premik k distribuirani zaščiti, kar je privedlo do razvoja požarnih zidov naslednje generacije. Ti vključujejo napredne funkcije, kot so sistemi za preprečevanje vdorov, nadzor nad aplikacijami in sledenje uporabnikom, kar omogoča globljo in bolj kontekstualno analizo. Nadzor nad aplikacijami omogoča, da požarni zid prepozna in nadzira uporabo posameznih aplikacij v omrežju, kar preprečuje morebitne zlorabe. Sledenje identiteti uporabnikov omogoča povezavo dejavnosti v omrežju s posameznimi uporabniki, kar vzpostavlja odgovornost in hitrejše zaznavanje tveganega vedenja. Poleg tega požarni zidovi, vse pogosteje uporabljajo umetno inteligenco in strojno učenje za izboljšano zaznavanje groženj in odzivanje nanje. Te tehnologije jim omogočajo učenje na podlagi preteklih interakcij in s tem izboljšanje časovne odzivnosti (George in drugi, 2023).

2.3.4 Šifriranje podatkov

Za zaščito občutljivih podatkov je šifriranje najbolj pomemben korak. Osnovno načelo šifriranja je pretvorba običajnega besedila (angl. plaintext) v nerazumljivo obliko, imenovano šifrirano besedilo (angl. ciphertext). Za pretvorbo šifriranega besedila nazaj v prvotno obliko je potreben šifrirni ključ, ki mora ostati v varstvu nameravanega prejemnika. Ključ sproži obratni proces šifriranja, s katerim se podatki ponovno pretvorijo v razumljivo obliko. Ta proces omogočajo matematični algoritmi, ločimo 2 vrsti šifriranje, in sicer simetrično in asimetrično šifriranje. Pri simetričnem se uporablja isti ključ za šifriranje in dešifriranje, pri asimetričnem pa se uporablja par ključev, javni ključ za šifriranje in zasebni ključ za dešifriranje. Šifriranje ni univerzalna rešitev. Različni podatki zahtevajo različne algoritme, močnejše metode pa zahtevajo več računalniških virov. Tu nastopi ravnovesje med varnostjo in zmogljivostjo (George in drugi, 2023).

2.3.5 Dvofaktorska avtentikacija

Dvofaktorska avtentikacija (angl. Two factor authentication – v nadaljevanju 2FA) zagotavlja dodatno varovalo potrditve identitete uporabnika, ki presega zgolj uporabniško ime in geslo. Temelji na načelu »nekaj, kar veš, nekaj, kar imaš ali nekaj, kar si«. Prvi dejavnik je običajno geslo ali PIN-koda. Drugi dejavnik pa je nekaj, kar uporabnik fizično ima npr. pametni telefon za prejem enkratnega gesla, varnostni USB ključek ali biometrični podatek, npr. prstni odtis ali prepoznavanje obraza. Z združevanjem različnih razredov preverjanja pristnosti 2FA tvori večplastno obrambo, ki bistveno izboljša varnost. 2FA ščiti pred pogostimi grožnjami, kot so napadi zvabljanja, prestrezanje gesel in napadi z ugibanjem gesel (brute-force). V napadu zvabljanja lahko napadalec pridobi tvoje geslo, a brez drugega dejavnika nima dostopa do računa. Ima pomembno vlogo zlasti na področjih spletnega bančništva, e-trgovine in storitev v oblaku, kjer je pogosto ogrožena občutljiva osebna ali finančna vsebina. V zadnjih letih postaja standardna varnostna praksa, prisotna že v družbenih omrežjih, poslovnih orodjih in storitvah. Tudi 2FA ni brezhibna. Obstajajo načini, kako jo napadalci obidejo z uporabo socialnega inženiringa, zlonamerne programske opreme ali zamenjave SIM kartic. Zato mora biti 2FA del

širše varnostne strategije, ki vključuje močna gesla, redne posodobitve, varna omrežja in ozaveščenost uporabnikov. Pomembno je tudi, katero vrsto 2FA uporabljamo. Potrditve prek SMS so sicer udobne, a manj varne zaradi ranljivosti mobilnih omrežij. Fizični varnostni ključi in aplikacije za preverjanje pristnosti npr. Google Authenticator, pa veljajo za bolj zanesljive (George in drugi, 2023).

2.3.6 Zaščita pred DDoS napadi

Za zaščito pred DDoS napadi, ki predstavljajo eno najpogostejših in najnevarnejših oblik kibernetskih napadov, je ključno uvesti večslojni pristop. Prvi korak je načrtovanje zadostne pasovne širine, ki omogoča absorbiranje večjih količin prometa brez prekinitve delovanja storitev. Pomembno vlogo ima tudi uporaba sistemov za zaznavanje anomalij, ki spremljajo promet v realnem času in samodejno prepoznajo nenavadne vzorce, značilne za DDoS napade, ter sprožijo opozorila ali avtomatizirane odzive. Poleg tega je priporočljiva uporaba sistemov CAPTCHA, ki omejujejo avtomatizirane zahteve z omogočanjem le človeških interakcij. Ena izmed naprednejših praks je uporaba rezervnih IP-naslovov oziroma t. i. IP poolov, ki omogočajo hitro preklopitev na varno povezavo v primeru napada. Prav tako je učinkovita implementacija geografske ali vsebinske filtracije prometa, kjer se promet iz sumljivih regij ali IP-naslovov blokira ali omeji. Uporaba oblačnih storitev za razpršitev prometa in vsebinskih dostavnih omrežij lahko znatno zmanjša vpliv napada s preusmeritvijo obremenitve. Vse te rešitve je treba podpreti s stalnim spremljanjem omrežja, nadgradnjami sistemov in vajami odziva na incidente, saj se taktike napadalcev nenehno razvijajo (Jain in drugi, 2022).

2.3.7 Umetna inteligenca kot zaščita pred grožnjami

Umetna inteligenca (angl. Artificial intelligence – v nadaljevanju AI) postaja ključni element v boju proti kibernetskim grožnjam, saj omogoča sprotno zaznavanje tveganj in avtomatizirano odzivanje. AI ima ključno vlogo pri identifikaciji vzorcev in anomalij v omrežnem prometu in vedenju uporabnikov, kar omogoča zgodnje prepoznavanje potencialnih napadov. S pomočjo algoritmov strojnega učenja lahko sistemi prepoznajo znake napadov, še preden se ti zgodijo, in tako organizacijam omogočijo pravočasno zaščito.

Sistemi, ki temeljijo na umetni inteligenci, omogočajo tudi zaznavanje zlonamerne programske opreme, preprečevanje ribarskih napadov in izolacijo okuženih naprav z omrežja. AI omogoča neprekinjeno obdelavo velikih količin podatkov v realnem času, kar znatno presega zmogljivosti ročnega dela analitikov. Glavne metode, ki jih umetna inteligenca uporablja so: strojno učenje oziroma angleško »Machine learning«, s pomočjo te metode lahko zaznava nevarno opremo ali malware in nenavadnega prometa, globoko učenje oziroma angleško »Deep learning«, ki pripomore k prepoznavanju kompleksnih vzorcev v zlonamerni kodi, Obdelava naravnega jezika, ki analizira nevarnosti v družbenih omrežjih in forumih. Uporaba AI v kibernetski varnosti ima prednosti in pomanjkljivosti. Najpomembnejša aplikacija AI je na področju obveščevalnih podatkov o grožnjah. AI lahko analizira ogromne količine podatkov

iz različnih virov in tako prepozna vzorce in trende, ki nakazujejo na morebitne kibernetske grožnje. Na ta način lahko organizacije z uporabo AI napovedujejo in preprečujejo prihodnje napade. Največji izziv je pomanjkanje preglednosti algoritmov AI, kar otežuje razumevanje odločitev in zmanjšuje zaupanje v sistem. Poleg tega lahko pride do lažnih pozitivnih zaznav, kar povečuje število nepotrebnih alarmov in dodatno obremenjuje analitike (Rizvi, 2023).

2.4 Standardi

Zadostna zaščita kibernetske varnosti, ki zajema vse rešitve za varnost podatkov, je mogoča le z uporabo okvira za kibernetsko varnost, ki zagotavlja strukturo in metodologijo za zaščito kritičnih digitalnih sredstev. Strokovnjaki za varnost priporočajo uporabo kibernetskih standardov, ki vključujejo zbirko najboljših praks za zaščito organizacij pred kibernetskimi grožnjami. Standard je idealno stanje oziroma najnižja meja dosežka, pogosto pa tudi najvišja ali popolna izvedba. Standard pomeni tudi tehnične specifikacije, ki jih mora izpolnjevati storitvena dejavnost, da lahko uporabniki storitev dosežejo največjo funkcionalnost ali koristi. Po podatkih www.standards.org.au so standardi prostovoljni dokumenti, ki določajo specifikacije, postopke in smernice, katerih cilj je zagotoviti varnost, doslednost in zanesljivost proizvodov, storitev ali sistemov. Mednarodna organizacija za standardizacijo (angl. International Organization for Standardization - v nadaljevanju ISO) in mednarodna elektrotehnična komisija (angl. International Electrotechnical Commissio - v nadaljevanju IEC) opredeljujejo kot pravila ali dokumente, sprejete na podlagi splošnega soglasja in potrjene s strani pravnega subjekta, ki določajo uporabo, regulacijo ali kakovost določene dejavnosti z namenom doseganja optimalnih rezultatov v določenem kontekstu kot smernice, model ali vzorec. Standard lahko razvije podjetje ali država, kot lasten standard ali lokalno regulativo, obstajajo pa tudi specifični industrijski standardi ali standardi za ustreznost storitev oziroma izdelkov. Večina mednarodnih standardov je prostovoljnih, zato je njihova uporaba neobvezna. Nekateri standardi pa so lahko obvezni na podlagi zakonskih ali regulativnih zahtev (Syafrizal in drugi, 2020).

2.4.1 Nacionalni inštitut za standarde in tehnologijo

Nacionalni inštitut za standarde in tehnologijo (angl. National Institute of Standards and Technology - v nadaljevanju NIST) je izdal okvir za kibernetsko varnost, namenjen zagotavljanju usmeritev organizacijam v kritični infrastrukturi za zmanjšanje tveganj, povezanih s kibernetsko varnostjo. Ta okvir, poznan kot NIST Cybersecurity Framework (CSF), je v zadnjih letih postal pomembno priporočilo za številne organizacije, ki že izvajajo ali so usklajene z različnimi standardi informacijske varnosti. Pri implementaciji NIST CSF je ključno, da je le-ta usklajena in dopolnjuje obstoječe okvire, kot so ISO/IEC 27001, COBIT in ISF Standard of Good Practice (SoGP). Ker NIST CSF ni zasnovan kot model zrelosti, organizacije pogosto potrebujejo lasten model zrelosti ali prilagoditev obstoječih modelov za dosledno merjenje napredka pri izvajanju okvira. Glavni cilj NIST CSF je upravljanje kibernetskih tveganj v organizacijah, ne pa celovito pokrivanje vseh procesov informacijske varnosti. Del okvira, imenovan »Implementation Tiers«, sicer omogoča

organizacijam vpogled v njihov pristop k upravljanju tveganj, ne zagotavlja pa mehanizma za merjenje zrelosti varnostnih procesov ali napredka implementacije (Almuhammadi in Alsaleh, 2017).

NIST Cyber Security Framework (CSF) je zasnovan kot tveganjsko usmerjen okvir, kjer se kibernetska varnost obravnava kot tveganje, ki ga je treba obvladovati v okviru celovitega upravljanja tveganj v organizaciji. Okvir NIST CSF je sestavljen iz treh glavnih delov (Almuhammadi in Alsaleh, 2017):

- jedro okvira (framework core), vključuje niz kibernetskovarstvenih dejavnosti, ki so organizirane v podkategorije, te pa v kategorije in končno v pet ključnih funkcij, ki so zasnovane kot sočasne in neprekinjene ter skupaj tvorijo strateški pristop k upravljanju kibernetskih tveganj. Poleg tega jedro okvira vsebuje tudi cilje kontrol in informativna priporočila, ki povezujejo dejavnosti z drugimi standardi, kot so COBIT, ISO/IEC 27001 in ISF SoGP.
- ravni tveganja (risk tiers), predstavljajo vizionarsko orodje, ki organizacijam omogoča vpogled v njihov pristop k upravljanju kibernetskih tveganj.
- profil okvira (framework profile), služi kot orodje za dokumentiranje in sledenje trenutnih ter načrtovanih dejavnosti informacijske varnosti v organizaciji. Profil omogoča prepoznavanje vrzeli med trenutnim in želenim stanjem ter določa potrebne dejavnosti za izboljšanje varnostne drže glede na izvedeno oceno tveganj.

2.4.2 ISO

Mednarodna organizacija za standardizacijo (angl. International Organization for Standardization - ISO) je globalna organizacija, ki razvija in objavlja mednarodne standarde za različne industrije. Na področju kibernetske varnosti je ISO razvil vrsto varnostnih standardov, ki organizacijam zagotavljajo smernice in najboljše prakse za upravljanje kibernetskih tveganj. Ti standardi pomagajo organizacijam vzpostaviti trdne varnostne politike in okvire, izboljšati upravljanje tveganj ter zagotoviti skladnost z regulativnimi zahtevami (Folorunso in drugi, 2024).

Naraščajoča pogostost in kompleksnost kibernetskih groženj organizacijam narekuje sprejetje robustnih okvirov kibernetske varnosti. Standardi varnosti ISO, zlasti serija ISO/IEC 27000, imajo ključno vlogo pri izboljšanju kibernetske varnosti organizacij po vsem svetu. Ti standardi zagotavljajo sistematičen pristop k upravljanju občutljivih informacij ter skrbijo za njihovo zaupnost, celovitost in razpoložljivost. ISO/IEC 27001, ki je osredotočen na vzpostavitev sistema za upravljanje informacijske varnosti, je splošno priznan zaradi svoje sposobnosti pomagati organizacijam pri prepoznavanju, upravljanju in ublažitvi kibernetskih tveganj. Z uporabo ISO standardov organizacije pridobijo boljše upravljanje tveganj, izboljšane zmogljivosti odzivanja na incidente ter močnejše usklajevanje z zahtevami regulatorne skladnosti, kot sta splošna uredba o varstvu podatkov (angl. General Data Protection Regulation - v nadaljevanju GDPR) in zakon zdravstvenega zavarovanja, prenosljivosti in

odgovornosti (angl. Health Insurance Portability and Accountability Act - v nadaljevanju HIPAA). Poleg tega ISO varnostni standardi spodbujajo kulturo varnosti v organizacijah, povečujejo ozaveščenost zaposlenih ter zagotavljajo dosledno izvajanje najboljših praks v različnih oddelkih in regijah. Uvedba standardov, kot so ISO/IEC 27001 (Informacijska varnost, kibernetska varnost in varstvo zasebnosti), ISO/IEC 27018 (Kodeks ravnanja za zaščito osebnih podatkov v javnih oblakih, ki delujejo kot obdelovalci podatkov), ISO/IEC 27017 (Kodeks ravnanja za varnostne kontrole informacij na osnovi ISO/IEC 27002 za storitve v oblaku), ISO/IEC 27015 (Smernice za upravljanje informacijske varnosti v finančnih storitvah), ISO/IEC 27002 (Informacijska varnost, kibernetska varnost in varstvo zasebnosti kontrole informacijske varnosti) ter ISO/IEC 27701 (Tehnike varnosti razširitev na ISO/IEC 27001 in ISO/IEC 27002 za upravljanje zasebnih informacij, zahteve in smernice) je pokazala pomembne izboljšave pri varstvu podatkov, še posebej v panogah, ki obdelujejo občutljive osebne ali finančne podatke. Kljub prednostim pa implementacija ISO standardov prinaša izzive, kot so omejitve virov, razširljivost in potreba po stalnem posodabljanju. Z razvojem groženj bodo ISO varnostni standardi ostali sestavni del proaktivne strategije kibernetske varnosti in se bodo povezovali z novimi tehnologijami, kot sta umetna inteligenca in internet stvari (IoT). Globalno sprejetje teh standardov odraža njihovo ključno vlogo pri zagotavljanju digitalne infrastrukture sodobnih organizacij. V nadaljevanju bom podrobneje predstavil te standarde (Folorunso in drugi 2024).

ISO 27001 je sistem za upravljanje informacijske varnosti. Ta mednarodni standard pomaga podjetjem in organizacijam po vsem svetu vzpostaviti in vzdrževati najboljši sistem upravljanja informacijske varnosti (ISMS) (Standardi.si, 2025). ISO 27001:2022 se brezhibno integrira z drugimi standardi, kot so ISO 9001 za upravljanje kakovosti, ISO 27002, kot kodeks dobre prakse za varnostne kontrole informacij, in predpisi, kot je GDPR, s čimer izboljšuje skladnost ter operativno učinkovitost. Ta integracija organizacijam omogoča poenostavitev prizadevanj za regulativno skladnost ter uskladitev varnostnih praks s širšimi poslovnimi cilji. ISO 27001 ima ključno vlogo pri krepitvi strategij zaščite podatkov v organizaciji. Ponuja celovit okvir za upravljanje občutljivih informacij ter se s pristopom, temelječim na tveganju, usklajuje s sodobnimi zahtevami kibernetske varnosti. Ta uskladitev, ne le krepi obrambe, ampak zagotavlja tudi spoštovanje predpisov, kot je GDPR, in zmanjšuje morebitna pravna tveganja. ISO 27001 je del širše družine ISO standardov sistemov vodenja, kar omogoča njegovo enostavno integracijo z drugimi standardi, kot so ISO 9001, ISO 22301, ISO 27701 (Starkova in Nazarov, 2025).

Za certifikacijo ISO/IEC 27001 mora organizacija opraviti zunanjo presojo s strani akreditiranega certifikacijskega organa. Postopek vključuje dva ključna koraka: pregled dokumentacije ISMS ter pregled na lokaciji za oceno implementacije in učinkovitosti varnostnih kontrol. Certifikat ISO/IEC 27001:2022 velja za dokaz zavezanosti organizacije robustnim praksam informacijske varnosti (Folorunso in drugi, 2024).

ISO/IEC 27018:2019 je prvi mednarodni standard, ki je v celoti osredotočen na zaščito osebnih podatkov v javnih oblačnih okoljih. Posebej je pomemben za ponudnike SaaS in IaaS, ki

obdelujejo osebne podatke v imenu svojih strank (upravljavcev podatkov) in morajo dokazati, da ustrezno obvladujejo tveganja glede zasebnosti. Oblačne platforme obdelujejo ogromne količine osebnih in občutljivih podatkov, a pogosto nimajo ustreznih kontrol za upravljanje dostopov, obdobja hranjenja ali obdelave zahtev za izbris. ISO/IEC 27018 zagotavlja natančen, preverljiv okvir za zagotavljanje skladnosti z zakonodajo o zasebnosti v oblaku. Pomemben je zaradi tega, ker povezuje varnost in zasebnost z usklajevanjem ISO/IEC 27001 varnostnih kontrol in specifičnih tveganj zasebnosti, ponudnikom omogoča izpolnjevanje pogodbenih in zakonskih obveznosti, ustvarja zaupanje pri strankah s preglednostjo glede obdelave, shranjevanja in prenosa podatkov, zmanjšuje pravno tveganje ob morebitnih kršitvah zasebnosti ali neskladnosti z GDPR, CCPA ipd., certifikat presega zgolj trženjske trditve o »varnem oblaku« (Pacific certifications, 2025).

ISO/IEC 27002:2022 je mednarodni standard, ki organizacijam zagotavlja celovit nabor kontrol za varovanje informacij, še posebej pri vzpostavljanju, vzdrževanju ali izboljševanju sistema upravljanja informacijske varnosti, v skladu z ISO/IEC 27001. Standard razvršča kontrole na organizacijske, kadrovske, fizične in tehnološke domene ter služi kot priporočilo za dobre prakse, obvladovanje tveganj ter skladnost z zakonskimi in regulativnimi zahtevami. ISO/IEC 27002:2022 poudarja pomen prilagajanja kontrol specifičnemu kontekstu, poslovnim ciljem in tveganjem posamezne organizacije. Zadnja revizija uvaja novo strukturo in sistem atributov za kontrole, kar omogoča večjo prilagodljivost, jasnost in odzivnost na sodobne varnostne izzive v medsebojno povezanem digitalnem okolju (ISO Standards, 2022).

ISO/IEC 27001:2022 je najnovejša izdaja mednarodnega standarda za vzpostavitev, izvajanje, vzdrževanje in nenehno izboljševanje sistema upravljanja informacijske varnosti (ISMS). Ta standard zagotavlja celovit okvir, ki organizacijam pomaga identificirati, oceniti in obvladovati tveganja za informacijsko varnost ter tako ščiti zaupnost, celovitost in razpoložljivost informacij. Ključna novost izdaje iz leta 2022 je boljša uskladitev s strukturo drugih vodilnih standardov vodenja (Annex SL) kot tudi popolno uskladitev s posodobljenim standardom ISO/IEC 27002:2022, ki določa varnostne kontrole. Standard pokriva vse od določanja konteksta organizacije, vključno z analizo notranjih in zunanjih dejavnikov ter potreb zainteresiranih strani, do opredelitve vodstva, načrtovanja, podpore, izvajanja operacij, evalvacije učinkovitosti in nenehnega izboljševanja sistema. Pomemben del je tudi dodatek A, ki vsebuje nabor 93 varnostnih kontrol, razdeljenih na organizacijske, kadrovske, fizične in tehnološke kontrole, ki omogočajo celovit pristop k obvladovanju informacijskih tveganj. S tem standardom organizacije izkazujejo zavezanost mednarodno priznanemu pristopu k varovanju informacij, povečujejo skladnost z zakonodajo ter izboljšujejo zaupanje strank in partnerjev v poslovnem okolju (ISO Standards, 2022).

2.4.3 CIS

CIS Controls v8 predstavljajo nadgradnjo temeljnih varnostnih ukrepov, ki jih je razvila globalna skupnost strokovnjakov pod okriljem Centra za internetno varnost (CIS). Glavni cilj CIS Controls je organizacijam ponuditi prednostni, izvedljiv in merljiv nabor varnostnih praks,

ki temeljijo na dejanskih podatkih o napadih in preizkušenih obrambnih ukrepih. CIS Controls temeljijo na naslednjih načelih, napad informira obrambo, osredotočenost na najpomembnejše grožnje, izvedljivost ukrepov, merljivost napredka ter poravnava z drugimi standardi in regulatornimi okviri (npr. NIST, ISO ...) (Center for Internet Security, 2021).

Struktura CIS Controls v8 je razdeljena na 18 nadzornih točk, ki pokrivajo celoten spekter varnosti od inventarja naprav in programske opreme, zaščite podatkov, upravljanja računov in dostopa, do stalnega upravljanja ranljivosti, varnosti omrežij, odzivanja na incidente, preverjanja zmožnosti in ozaveščanja zaposlenih. Vsak ukrep vsebuje jasen opis, razlago njegove kritičnosti, praktične postopke ter tabele s t. i. »Safeguards« (prej znani kot podkontrole), ki so razdeljene glede na stopnjo zahtevnosti in tip organizacije. Posebnost CIS Controls je v tem, da niso zgolj »seznam dobrih praks«, temveč predstavljajo celovito podprt, prednostni in osredotočen nabor dejansko izvedljivih ukrepov, ki so usklajeni s potrebami različnih organizacij od manjših do največjih. Razvoj kontrol temelji na realnih podatkih, vključuje pa tudi model kolektivne obrambe Community Defense Model (CDM), ki povezuje najpogostejše tipe napadov s konkretno uporabnimi obrambnimi ukrepi. Skupnost CIS nenehno razvija in posodablja podporne materiale, kot so povezave z regulativnimi okvirji, praktične študije primerov, priporočila za mala podjetja ter smernice za merjenje zrelosti in napredka. CIS Controls tako predstavljajo osnovo za sistematično izboljševanje kibernetske odpornosti, saj omogočajo prilagoditev varnostnih ukrepov glede na velikost, tveganja in zrelost organizacije. Poleg tega ustvarjajo skupnost in ekosistem, kjer si uporabniki izmenjujejo orodja, rešitve, praktične izkušnje in gradijo skupne standarde sodobne kibernetske obrambe (Center for Internet Security, 2021).

2.4.4 COBIT

COBIT 2019 se je v zadnjih letih uveljavil kot ena izmed osrednjih metodologij za upravljanje informacijske tehnologije (IT) v organizacijah različnih sektorjev. COBIT 2019 je celovit okvir, ki organizacijam pomaga doseči poslovne cilje preko strukturiranega in standardiziranega upravljanja IT. Na primer, v sektorju rudarske industrije je implementacija COBIT 2019 izboljšala obvladovanje tveganj informacijske varnosti ter skladnosti s predpisi, medtem ko v sektorju zunanjega izvajanja poslovnih procesov prispeva k merjenju uspešnosti in lažjemu dostopu do znanja znotraj organizacije (Antariksa in drugi, 2025).

Pomembni prispevek COBIT 2019 je tudi okrepitev notranjih kontrolnih postopkov ter zapolnitev vrzeli v ekonomskih enotah, kjer se IT aktivno uporablja za izboljšanje operativne učinkovitosti in dolgoročne trajnosti organizacije. Okvir prinaša nove cilje upravljanja, kot so upravljanje podatkov, upravljanje projektov in upravljanje zagotavljanja kakovosti, ter uvajanje zasnov fokusnih področij in oblikovnih dejavnikov. Z modelom kaskade ciljev (goals cascade) COBIT 2019 omogoča doseganje IT ciljev, ki so neposredno usklajeni s poslovnimi strategijami organizacije. Osrednja načela COBIT 2019 vključujejo ustvarjanje vrednosti za deležnike, celosten pristop, prilagodljivost spremembam, razlikovanje med upravljanjem in menedžmentom, prilagodljivost potrebam posamezne organizacije ter celovitost, ki pokriva vse

funkcije podjetja. COBIT 2019 prinaša številne koristi pri upravljanju IT, saj omogoča strateško uskladitev IT s poslovnimi cilji, zagotavlja, da IT-storitve in novi projekti ustvarjajo dodano vrednost, ter učinkovito upravlja tveganja in varuje organizacijo pred morebitnimi motnjami ali grožnjami. Poleg tega okvir podpira optimizacijo upravljanja Zvirov IT (ljudje, tehnologija, proračun) in omogoča strukturirano merjenje uspešnosti IT, kar prispeva k doseganju strateških in operativnih ciljev na podlagi globalno priznanih standardov (Antariksa in drugi , 2025).

3 STRATEGIJE KIBERNETSKE VARNOSTI

To poglavje podrobneje opiše, kako je videti strategija kibernetske varnosti in katere sestavine so za njen uspeh nujne. Najprej pojasnim, kaj sploh pomeni strategija kibernetske varnosti in kakšno vlogo ima v sodobnih organizacijah. Nato predstavim različne vrste strategij, ki jih srečujemo v praksi, ter za vsako vrsto izpostavim njene posebnosti in cilje. S tem poglavje ponudi celovit vpogled v to, kako lahko dobro zasnovana strategija pripomore k učinkovitemu obvladovanju tveganj in zaščiti informacijskih sistemov.

3.1 Strategija kibernetske varnosti

Organizacije, ki imajo izredno močno varnostno kulturo, imajo varnost tako rekoč vtkano v vse procese. Za vse druge pa je nujna strategija. Izkušnje kažejo, da sta pojma »strategija« in »taktika« v poslovnem svetu pogosto napačno razumljena. Kar je za nekoga strategija, je za drugega lahko le taktika. Poleg tega strokovnjaki za varnost in skladnost pogosto uporabljajo izraz »strategija«, ko v resnici mislijo na ogrodja, modele ali standarde. Teh je v industriji ogromno in jih organizacije pogosto uporabljajo na primer ISO standarde, NIST standarde, OWASP Top 10, CIS Benchmarks, STRIDE, ogrodja za upravljanje tveganj in številne druge (Rains, 2023).

Prava strategija za organizacijo je tista, ki najbolj učinkovito zmanjšuje najpomembnejša tveganja za poslovanje. Tveganje je relativno, zato nobena strategija ni univerzalno najboljša izbira za vse. Čeprav imamo na voljo vedno več odličnih ogrodij in standardov, se število varnostnih incidentov ne zmanjšuje.

3.2 Vrste obstoječih strategij kibernetske varnosti

3.2.1 Strategija zaščite in obnove

Poznana je tudi kot strategija perimetra (angl. perimeter security strategy). Pogosto jo slikovito opisujejo kot »trda lupina z mehko sredico« kar pomeni, da če napadalcu uspe prebiti obodno zaščito, ga v notranjosti skoraj nič več ne ovira pri lateralnem gibanju in vzdrževanju prisotnosti. Organizaciji ne preostane drugega, kot da skuša obnoviti izvorne podatke in okolje. Po današnjih standardih velja ta pristop za zastarelega, a presenetljivo veliko organizacij se ga še vedno oklepa. Kot že ime pove, je bistvo strategije v preprečevanju uspešnosti napadalcev s tehnologijami, kot so požarni zidovi, DMZ-ji, proxy strežniki in mikrosegmentacija. Osnovna predpostavka te strategije je, da bo organizacija lahko vzpostavila in upravljala ustrezno

zaščitno tehnologijo in procese. Če to ne uspe, sledi načrt obnove. Ker bodo tako dobri v zaščiti, jim ne bo treba vlagati v odkrivanje in odzivanje. Večina podjetij, ki je sprejela ta pristop, je vlagala tudi v varnostno kopiranje in obnovo podatkov, a pogosto ne primarno zaradi varnosti, temveč zaradi tveganja izgube podatkov. Če torej zaščita odpove, je njihova zadnja linija varnostna kopija. Ta strategija temelji na domnevi, da administratorji, partnerji in uporabniki ne bodo nikoli naredili napake ali slabe odločitve. Kot pa smo videli čez desetletja, uporabniki pogosto sami predstavljajo grožnje skozi vse plasti obrambe. Brez sposobnosti odkrivanja in odziva lahko napadalci vdrejo in ostanejo v okolju zelo dolgo, kar obnovo podatkov naredi le še dražjo in bolj negotovo (Rains, 2023).

3.2.2 Strategija zaščite končnih točk

Naslednja strategija je strategija zaščite končnih točk (angl. Endpoint Protection Strategy). To imenujem tudi »proxy strategija«. Ideja je, da so končne točke osebni računalniki, mobilne naprave, določene vrste IoT naprav ipd. tiste, ki obdelujejo, shranjujejo in prenašajo podatke. Če torej zaščitimo končne točke, s tem posredno zaščitimo podatke, kar je v bistvu tudi glavni cilj zaščite podatkov. Grožnje so lahko datotečne, makroji, skripte, polimorfni virusi, boot virusi, rootkiti ipd. in se pojavljajo v različnih operacijskih sistemih ter datotečnih sistemih (Rains, 2023).

3.2.3 Fizična kontrola in varnostna dovoljenja kot strategija kibernetske varnosti

Kot pove že ime, strategija fizične kontrole in varnostnih dovoljenj (angl. Physical Control and Security Clearances Strategy) temelji na fizičnem nadzoru infrastrukture, ki se uporablja za prenos, shranjevanje in obdelavo podatkov, ter na klasifikaciji podatkov in z njo povezanih varnostnih dovoljenjih. Osnovna ideja te strategije je, da vsi podatki nimajo enake vrednosti za organizacijo, ki jih nadzoruje. S klasifikacijo podatkov v različne kategorije, glede na njihovo vrednost, lahko zagotovimo, da so najbolj dragoceni podatki zaščiteni v skladu z njihovo pomembnostjo. Takšne politike klasifikacije podatkov določajo, kateri ljudje, procesi in tehnologije morajo biti uporabljeni pri obdelavi posamezne kategorije podatkov. Število in narava kategorij močno vplivata na kulturo organizacije, zaposlovanje, naložbe v IT in proračune. Tu postanejo pomembna tudi varnostna dovoljenja. Za dostop do podatkov v določeni kategoriji mora imeti posameznik veljavno dovoljenje za to stopnjo zaupnosti (Rains, 2023).

3.2.4 Skladnost kot varnostna strategija

Skladnost (angl. Compliance) in kibernetska varnost sta dva različna, delno prekrivajoča se področja. Skladnost se osredotoča predvsem na dokazovanje, da organizacija izpolnjuje zahteve, ki so opredeljene v regulativnih, industrijskih ali notranjih standardih. Skladnost je lahko zelo koristna, zlasti z vidika pridobivanja kibernetskega zavarovanja in dokazovanja skrbnosti ter omejevanja odgovornosti. To je drugače kot kibernetska varnost, ki se osredotoča na zaznavanje, zaščito, odkrivanje, odzivanje in obnovo. Osnovna predpostavka te strategije je, da je izpolnjevanje obveznosti skladnosti dovolj za zaščito podatkov organizacije. Fokus je

tako na izpolnjevanju vseh zahtev (regulativnih, industrijskih in notranjih) in dokazovanju tega na revizijah. Primeri so standardi kot PCI DSS, HIPAA, GDPR, NIST, ISO/IEC 27001 ali interni IT standardi organizacije. Strategija zahteva vlaganja v ljudi, procese in tehnologije, ki pomagajo dosegati in dokazovati skladnost. To se običajno kaže kot natančno definirani kontrolni sklopi in ponovljivi procesi, ki jih periodično preverjajo z revizijami. Strategija je lahko zelo pozitivna za organizacije, ki nimajo razvite kibernetske varnostne strategije ali upravljanja. Večina varnostnih regulativnih standardov v posamezni panogi določa minimalne zahteve, ki jih mora podjetje izpolniti (Rains, 2023).

3.2.5 Strategija osredotočena na aplikacije

Aplikacije so tiste, ki obdelujejo, shranjujejo in prenašajo podatke. Če zaščitimo aplikacijo, torej posredno ščitimo tudi podatke. Pristop se osredotoča na zaščito aplikacij s tem, da zmanjšuje število njihove ranljivosti in resnost teh ranljivosti. Poleg tega si prizadeva, da bi morebitne ostale ranljivosti v aplikacijah postale zelo težko, če ne že nemogoče izkoriščene. Osnovna predpostavka tega pristopa je, da je bistveno ceneje odpraviti napake in ranljivosti še pred izidom aplikacije v produkcijo. To vključuje vlaganja v ljudi, procese in tehnologije, kot so modeliranje groženj, varnostno razvojni življenjski cikel, orodja za statično in dinamično analizo kode, penetracijsko testiranje, upravljanje mobilnih naprav in aplikacij, nagradne sheme za lov na napake ipd. (Rains, 2023).

3.2.6 Strategija osredotočena na identiteto

Šibke, izpostavljene ali ukradene identitete so ena izmed glavnih šibkih točk v kibernetski varnosti. Mnogi ljudje uporabljajo ista gesla na različnih aplikacijah, sistemih in storitvah. Ko pride do kraje le-teh, napadalci takoj poskusijo iste podatke uporabiti še drugod na bančnih portalih, spletnih trgovinah, družbenih omrežjih in podobno. Čeprav je zasnova identitete in dokazovanja le-te zelo stara, je ta strategija razmeroma nova in je v zadnjih letih hitro pridobila veljavo. Osnovna ideja je, da napadalci pri večini uspešnih vdorov prej ali slej uporabijo legitimne podatke. Procesi avtentikacije in avtorizacije lahko ustvarjajo koristne metapodatke. Na primer, če ugotovimo, iz katere lokacije prihaja zahteva za prijavo, lahko ocenimo, kako verjetno je, da je zahteva legitimna. Če primerjamo določene lastnosti prijave z zgodovino istega uporabnika, lahko to dodatno zviša našo stopnjo zaupanja. Temeljna predpostavka strategije je, da lahko organizacije bolje zaščitijo podatke, hitreje zaznajo ukradene podatke in se nanje učinkoviteje odzovejo z boljšo zaščito identitet ter z uporabo metapodatkov identitete za iskanje znakov kompromisa (Rains, 2023).

3.2.7 Strategija osredotočena na podatke

Strategija, osredotočena na podatke v zadnjih letih, postaja vse bolj priljubljena, predvsem zaradi številnih odmevnih incidentov uhajanja podatkov, razkritij o državnih programih zbiranja podatkov, vse večjega števila izsiljevalskih napadov in povečanja tveganja kraje intelektualne lastnine. Hkrati je tudi vse več regulativnih zahtev, ki varujejo zasebnost potrošnikov in so povezane z visokimi globami za neskladnost (npr. GDPR). Namesto da bi

zaupale zaščiti, ki jo nudijo požarni zidovi, končne naprave ali aplikacije, želijo zagotoviti, da so podatki zaščiteni, ne glede na to, kje so in tudi ne glede na to, ali so podatki v notranjosti perimetra, dostopni s službene naprave ali procesirani z aplikacijo, ki ustreza varnostnim zahtevam, je cilj, da so podatki vedno zaščiteni (Rains, 2023).

Glavne predpostavke pri strategiji, ki je osredotočena na podatke, so (Rains, 2023):

- Podatki so tista ključna vrednost, ki jo je treba zaščititi.
- Podatki bodo prehajali izven organizacije, ne glede na dovoljenja, zato jih je treba zaščititi vedno in povsod.
- Nekatere sisteme, ki obdelujejo podatke, je treba obravnavati kot potencialno nevarne, zato mora zaščita podatkov delovati tudi v takšnih okoljih.
- Podatke je še vedno treba varno deliti znotraj podjetja in z zunanjimi partnerji (proizvodnja, marketing, PR, pravne službe). Podatki morajo biti varni, a hkrati dostopni in uporabni.

Osrednji cilj strategije je zaščititi podatke povsod, kjer se prenašajo, obdelujejo ali shranjujejo, in to za čim daljše obdobje. To običajno vključuje vlaganja v tehnologije za šifriranje in upravljanje ključev, preprečevanju izgube podatkov (angl. Data Loss Prevention - v nadaljevanju DLP) ter po možnosti klasifikacijo podatkov. Glavne značilnosti te strategije so šifriranje in upravljanje ključev. Če so podatki ves čas in povsod šifrirani, se napadalna površina občutno zmanjša (Rains, 2023).

3.2.8 Strategija osredotočena na napadalca

Ideja strategije, osredotočene na napadalca, je, da morajo varnostne ekipe svoje zaščitne ukrepe, zaznavanje kompromitacij in odzivanje na napadalce prilagajati realnim taktikam, tehnikam in postopkom, ki jih napadalci dejansko uporabljajo. Drugače povedano, razumevanje načinov delovanja napadalcev in načrtovanje obrambe glede na te metode povečuje učinkovitost zaščite. Osnovna predpostavka tega pristopa je, da če napadalce prisilimo, da morajo biti pri vdiranju uspešni večkrat, jim tako bistveno otežimo delo in hkrati zmanjšamo čas do zaznave in okrevanja po incidentu. Fokus tega pristopa je razumeti, kako napadalci delujejo, ter vsak njihov korak in taktiko narediti neučinkovito. Ta pristop zahteva vlaganja v številna področja in uvajanje večslojnih zaščitnih ukrepov na vsakem koraku napadalnega cikla (Rains, 2023).

3.2.9 Strategija ničelnega zaupanja

Eden izmed temeljnih predpostavk klasičnih varnostnih strategij je, da je uporabnik ali sistem, ki uspešno opravi avtentikacijo v IT okolje, avtomatsko vreden zaupanja. Osnovno načelo strategije ničelnega zaupanja (angl. Zero Trust) je: »Nikoli ne zaupaj, vedno preveri!«. Vsaka zahteva za dostop do katerekoli organizacijske resurse je obravnavana kot potencialna grožnja, zato je treba vsakič znova izvesti preverjanje identitete, stanja naprave in pravic. Pristop ničelnega zaupanja je še posebej smiseln v času množične uporabe mobilnih naprav, IoT, dela na daljavo in oblačnih storitev, kjer je jasno, da tradicionalni perimetri ne obstajajo več. Vse

večji pomen ima upravljanje identitet, varnost naprav in nadzor dostopa do podatkov, ne glede na fizično lokacijo. Vendar pa ničelno zaupanje samo po sebi ne rešuje vseh kibernetskih tveganj, saj ne odpravlja ranljivosti, napačnih nastavitev, socialnega inženiringa ali nenamernih notranjih groženj (Rains, 2023).

4 METODE IN PRISTOPI TESTIRANJA KIBERNETSKE VARNOSTI

Kibernetska varnost se nanaša na sposobnost zaščite in upravljanja dostopa do omrežnih sistemov ter podatkov, ki jih ti vsebujejo, s ciljem zagotavljanja zaupnosti, razpoložljivosti in celovitosti informacij za organizacije in posameznike. Pomembnost kibernetske varnosti se z razvojem tehnologije še povečuje, saj so podatki postali ena ključnih vrednot sodobnih družb in držav. Kibernetski napadi lahko močno prizadenejo posameznike, organizacije in celotne države, kar se odraža v finančnih izgubah, izgubi ugleda, pravnih posledicah in celo psiholoških posledicah za žrtve. Osnovne komponente učinkovitega sistema kibernetske varnosti vključujejo šest ključnih korakov analizo in prepoznavo tveganj, obrambne ukrepe, zaznavanje napadov, obnovo po incidentu, raziskovanje napadov in stalni nadzor ter razvoj (Aboelfotoh in Hikal, 2019).

Ocena kibernetske varnosti ima pomembno vlogo pri odkrivanju in odpravljanju ranljivosti v omrežjih, sistemih, aplikacijah in politikah organizacije. Ocenjevanje vključuje tehnične metode, ki so analiza ranljivosti, analiza omrežja, penetracijsko testiranje, ocenjevanje avtentikacije in odkrivanje virusov ter fizične metode, ki pa so ocena socialnih groženj, groženj strojne opreme, pregled politik in ukrepov ter naravnih groženj. S celovitimi ocenami je mogoče odkriti ranljivosti, zagotoviti ustrezne popravke ter izboljšati odpornost organizacije na kibernetske grožnje (Aboelfotoh in Hikal, 2019).

4.1 Penetracijski testi

Penetracijsko testiranje je simulacija dejanskega kibernetskega napada na ciljne sisteme, s katerim preverimo učinkovitost in stabilnost sistemov ob morebitnih resničnih napadih ter odkrijemo ranljivosti, ki bi jih lahko napadalci izkoristili. Takšno testiranje pogosto imenujemo tudi "etični heking", saj se izvaja na podlagi predhodnega dovoljenja lastnika sistema in z namenom izboljšanja kibernetske varnosti organizacije. Poznamo več vrst penetracijskih testov, in sicer testiranje omrežij, spletnih aplikacij, socialnega inženiringa in pa testiranje odjemalcev. Penetracijsko testiranje lahko glede na področje izvajanja razdelimo v pet osnovnih vrst, ki vsaka naslavlja specifične vidike informacijske varnosti v organizaciji (Aboelfotoh in Hikal, 2019).

Glede na dostopnost informacij delimo penetracijske teste na 3 tipe. Prvi je Black Box, kjer izvajalec nima nobenih predhodnih informacij o omrežju ali sistemu. Pridobivanje informacij temelji izključno na lastnem raziskovanju, orodjih in tehnikah. Namen je posnemati napadalca iz resničnega sveta, ki nima notranjih informacij. Drugi način je White Box, kjer ima izvajalec popoln dostop do informacij o sistemu (npr. IP-naslovi, domene, omrežne sheme, verzije aplikacij, konfiguracije požarnih zidov). Ta pristop prikazuje najslabši scenarij, ki prikaže, kaj

lahko napadalec doseže, če ima vse podatke o sistemu. Tretji način pa je Grey Box, kjer ima izvajalec delne informacije ali omejen dostop, podobno kot običajen zaposleni v organizaciji. Pogosto se uporablja za simulacijo internega napada ali preizkušanje specifičnih segmentov sistema (Singh in Singh, 2017).

Penetracijsko testiranje sestoji iz niza zaporednih faz, ki jih je treba dosledno upoštevati za učinkovito izvedbo testa in pridobitev uporabnih rezultatov (Singh in Singh, 2017):

- Načrtovanje je faza, v kateri izvajalec testa zbira čim več informacij o ciljni tarči. To lahko vključuje podatke o spletni strani, domeni, IP-naslovih, poštnih strežnikih in drugih relevantnih informacijah. Pri "black box" testiranju je ta faza običajno najzahtevnejša in najbolj časovno potratna, vendar bistveno pripomore k uspehu nadaljnjih faz testa.
- Skeniranje je faza, v kateri izvajalec z uporabo različnih orodij pregleduje tarčo z namenom odkrivanja ranljivosti in varnostnih vrzeli. Pošilja različne zahteve omrežju ali spletnim aplikacijam in beleži odzive, da ugotovi odprte porte, storitve, dostopne skupne diske, ranljive knjižnice, funkcije v kodi ipd. Tu se pogosto uporablja avtomatizirano orodje za varnostno skeniranje.
- Pridobivanje dostopa, po identificiranju ranljivosti v prejšnji fazi se izvajalec loti njihovega izkoriščanja, da pridobi dostop do ciljne tarče oziroma sistema.
- Ohranjanje dostopa, ko je dostop enkrat pridobljen, je cilj v tej fazi zagotoviti vztrajnost oziroma trajnost dostopa.
- Izkoriščanje je faza, v kateri izvajalec izvede dejanske vdore, na primer pridobiva podatke, izvaja DoS napade ali preizkusi druge vrste napadov znotraj sistema. Ta faza je posebej občutljiva, zato mora biti nadzorovana, da ne pride do večje škode na tarčnem sistemu.
- Zbiranje dokazov in priprava poročila, na koncu se zberejo vsi dokazi o izkoriščenih ranljivostih ter pripravi podrobno poročilo, ki vključuje opis odkrite varnostne vrzeli, način izkoriščanja ter priporočila za odpravo. Poročilo se nato preda vodstvu oziroma odgovorni osebi za nadaljnje ukrepanje.

4.1.1 Penetracijsko testiranje omrežij

Gre za najpogostejšo in osnovno vrsto penetracijskega testiranja, katere glavni cilj je odkrivanje ranljivosti v infrastrukturi omrežja pod testom. S tem testiranjem se preverja, ali obstajajo vrzeli ali varnostne pomanjkljivosti, ki bi jih lahko napadalci izkoristili za dostop do notranjih virov organizacije. Računalniška omrežja so vse bolj izpostavljena kibernetskim grožnjam, ki postajajo pogostejše, kompleksnejše in prefinjene. Penetracijski testi posnamejo postopke, ki jih v resničnih napadih uporabljajo hekerji, in je postala ključna ter pogosto tudi zakonsko zahtevana komponenta kibernetskih revizij (Ghanem in Chen, 2019).

Glavna zaščita brezžičnih omrežij temelji na šifrirnih protokolih, kot sta varnostni protokol za brezžična omrežja (angl. Wired Equivalent Privacy - v nadaljevanju WEP) in protokola za zaščito brezžičnih omrežij (angl. Wi-Fi Protected Access - v nadaljevanju WPA/WPA2). Za testiranje teh protokolov se postavi okolje, ki je sestavljeno iz strojne opreme, to so

usmerjevalniki, odjemalske naprave, telefoni, tablice, prenosniki in programske opreme, kot je linux, Aircrack paket, orodja za spremljanje naslovov in še drugi. Takšna postavitev omogoča izvajanje širokega nabora napadov, vključno s prisluškovanjem brezžičnim komunikacijam, zajemanjem paketov, replay ali »brute-force« napadi na šifrirne protokole ipd. (Alhamed in Rahman, 2023).

4.1.2 Penetracijsko testiranje spletnih aplikacij

Ta vrsta testiranja se osredotoča na končne točke spletnih aplikacij, s katerimi uporabniki redno komunicirajo. Zaradi naraščajočih groženj v spletnem okolju je potrebno skrbno načrtovanje in več časa, saj so napadi na spletne aplikacije vedno bolj prefinjeni in raznoliki. Ker je vse več storitev spletno podprtih, so spletne aplikacije tarča različnih napadov, zato je nujna uporaba varnostnih pristopov »obramba v globino«. Preden gre katerakoli spletna aplikacija v produkcijo, je nujno izvesti penetracijsko testiranje, saj napadalci stalno iščejo ranljivosti. Poznamo več vrst napadov na spletne aplikacije, v osnovi jih delimo na napade na strani odjemalca in pa napade na strani strežnika. Pri penetracijskem testiranju gre za preizkušanje ranljivosti, ali jih lahko izkoristimo. Penetracijsko testiranje spletnih aplikacij, tako kot vsako penetracijsko testiranje temelji na pristopu, kot smo ga že navedli, sledimo fazam, ki so navedene zgoraj, načrtovanje, skeniranje, izkoriščanje (Nagendran in drugi,2019).

4.1.3 Penetracijsko testiranje s področja socialnega inženiringa

Ta oblika testiranja je ključna za preverjanje t. i. človeškega dejavnika v podjetju in spada pod fizično varnost. Preverja, kako ranljivi so zaposleni na prevare in manipulacije. Pri fizičnih penetracijskih testih, kjer je socialni inženiring dovoljen, penetracijski tester neposredno komunicira z zaposlenimi. Te interakcije običajno temeljijo na prevari, in če niso izvedene pravilno, lahko vznemirijo zaposlene, kršijo njihovo zasebnost ali omajejo zaupanje v organizacijo, kar lahko vodi v tožbe in zmanjšanje produktivnosti. Pri digitalnih penetracijskih testih se odpornost zaposlenega meri posredno, na primer s telefonskimi poizvedbami ali pošiljanjem lažnih elektronskih sporočil, ki naj zaposlenega pripravijo do razkritja zaupnih informacij. Ti testi so lahko oblikovani na etičen način in v zakonskih okvirih (Dimkov in drugi , 2010).

Zahteve za uspešno izveden penetracijski test so (Dimkov in drugi, 2010):

- Realističnost, test mora biti realističen, saj simulira napad, ki bi ga izvedel pravi nasprotnik.
- Spoštovanje, zaposleni morajo biti med testom obravnavani s spoštovanjem. Zaposleni ne smejo biti pod stresom, se počutiti nelagodno ali biti ogroženi, saj bi to lahko povzročilo nezadovoljstvo, jezo ali celo pravne postopke proti organizaciji.
- Zanesljivost, test ne sme povzročiti izgube produktivnosti zaposlenih.
- Ponovljivost, test mora biti izvedljiv večkrat, in če se okolje ne spremeni, morajo biti rezultati enaki.
- Poročljivost, dejanja med testom morajo biti beležena, izid testa pa mora biti predstavljen v obliki, ki omogoča smiselno in uporabno dokumentacijo ugotovitev ter priporočil.

Pri realističnem testu velikokrat pride do dejstva, da si te zahteve med sabo nasprotujejo. Pri realističnem testu je velikokrat potrebno zavajanje zaposlenega, kar ni spoštljivo, realističen test lahko cilja na poljubne zaposlene prek socialnega inženiringa, kar ni zanesljivo, pri poročljivem testu je treba beležiti vsa dejanja penetracijskega testerja, kar ni realno. Izvedba penetracijskega testa pomeni iskanje optimalnega ravnovesja med temi nasprotujočimi zahtevami. Če ravnovesja ni, bodisi test ne bo ustrezno ocenil varnosti organizacije, bodisi bo škodoval zaposlenim (Dimkov in drugi, 2010).

4.1.4 Penetracijsko testiranje odjemalcev

Namen teh testov je odkrivanje varnostnih groženj na uporabniških delovnih postajah, kot so napake ali ranljivosti v programski opremi. Testiranje je ključno tudi za interne aplikacije, razvite v podjetju, saj morajo biti pred uporabo ustrezno preverjene z vidika varnosti. Delovne postaje imajo običajno nameščenih veliko različnih orodij, kar povečuje tveganje za ranljivosti, še posebej, če niso redno posodobljene od operacijskih sistemov, gonilnikov do različnih aplikacij in tudi AI orodij. Med testiranji pogosto najdejo tudi programsko opremo, ki omogoča povišanje privilegijev npr. običajni uporabnik lahko postane administrator. Če je naprava član Active Directory domene, je tveganje še večje, saj lahko napadalec pridobi podatke drugih uporabnikov. Ob testiranju se velikokrat odkrije, da imajo uporabniki nepravilno nastavljene pravice za datoteke in mape. Običajni uporabniki lahko npr. spreminjajo datoteke ali nastavitve v mapah, kjer bi morali imeti le bralni dostop, ali celo nimajo pravice dostopa. To omogoča napadalcem, da zamenjajo, ali okužijo izvršljive datoteke ali konfiguracije, ki jih nato preberejo, ali se izvedejo procesi z višjimi privilegiji (Usd more security, 2025).

4.2 Identifikacija ranljivosti

Ranljivost je napaka v izdelku ali sistemu, ki lahko napadalcu omogoči ogrožanje zaupnosti, celovitosti ali razpoložljivosti tega izdelka ali sistema. Poznamo več vrst ranljivosti (Aslan in drugi, 2023):

- Programske ranljivosti, ki nastanejo zaradi napak ali hroščev v aplikacijah, kar napadalci izkoristijo za kompromitiranje sistema.
- Ranljivosti požarnih zidov so napake pri zasnovi, implementaciji ali konfiguraciji požarnega zidu, ki omogočajo napade na zaščiteno omrežje.
- Ranljivosti TCP/IP so pomanjkljivosti v različnih plasteh omrežnih protokolov, kot so ARP napadi in fragmentacijski napadi.
- Ranljivosti brezžičnih omrežij so napadi na brezžične dostopne točke in protokole, npr. težave s SSID ali WEP.
- Ranljivosti operacijskih sistemov so varnostne pomanjkljivosti v operacijskih sistemih, kjer že manjša nepazljivost skrbnika lahko odpre možnosti za napade.
- Ranljivosti spletnih strežnikov pa so napake v zasnovi ali napačna uporaba, ki omogoča napade, kot sta sniffing in spoofing.

Hitra identifikacija zgoraj opredeljenih ranljivosti je zelo pomembna, da ne nastane prevelika škoda, če se ranljivosti ne odkrijejo dovolj hitro, jih napadalci izkoristijo in zaradi tega lahko nastane velika škoda. Zato pri identifikaciji uporabljamo orodja za skeniranje ranljivosti, ki so namenjena odkrivanju varnostnih lukenj v napravah in programski opremi. Večina teh orodij temelji na bazah znanih ranljivosti. Pri izboru orodja so zelo pomembne lastnosti, kot so podprt nabor naprav, metode skeniranja ter zmožnosti opozarjanja in poročanja. Najbolj razširjena orodja pa so (Aslan in drugi, 2023):

- WireShark je odprtokodni analizator omrežnih protokolov za poglobljeno preiskavo in zaznavanje omrežnih težav v realnem času.
- Netsparker je samodejni optični čitalnik, ki odkriva ranljivosti v spletnih aplikacijah in API-jih, pri čemer potrjuje pristnost ranljivosti, da zmanjša lažne pozitivne rezultate.
- Acunetix je avtomatizirani spletni optični čitalnik, ki zazna več kot 4500 ranljivosti in vključno s injekcijam jezika za upravljanje relacijskih baz (angl. Structured Query Language - v nadaljevanju SQL) in vnosa zlonamerne skripte v spletno stran (angl. Cross-site Scripting - v nadaljevanju XSS), ter omogoča napredne funkcije upravljanja tveganj.
- Intruder je optični čitalnik, ki izvaja proaktivne preglede za nove ranljivosti, integriran s Slack, Jira in AWS za obveščanje in usklajevanje naslovov.
- Apptrana je program za zaznavanje in poročanje spletnih ranljivosti, omogoča pa validacijo in integracijo z WAF za takojšnje virtualno odpravljanje ranljivosti.
- MBSA je Microsoftovo orodje za preverjanje varnosti sistemov Windows in ustreznosti nameščenih popravkov. To je samo nekaj od orodij, ki pripomorejo pri skeniranju in identifikaciji ranljivosti (Aslan in drugi, 2023).

4.3 SQL injekcije

Velika količina občutljivih podatkov podjetij in organizacij je shranjena v specializiranih podatkovnih bazah na strežnikih v organizaciji ali v tujini. Varovanje teh podatkov pred nepooblaščenim dostopom je ključno za organizacije v različnih sektorjih, saj lahko vsakršno razkritje podatkov povzroči veliko škodo za zasebnost uporabnikov, ugled in finančno stabilnost organizacije. Podatki tako predstavljajo eno najpomembnejših sredstev, ki jih je treba skrbno zaščititi, zaradi česar so baze podatkov postale stebri sodobnih organizacij. Za dostop in upravljanje teh baz se najpogosteje uporablja standardni jezik SQL, ki administratorjem omogoča izvajanje različnih operacij nad podatki, kot so shranjevanje, iskanje, ustvarjanje, posodabljanje in brisanje. Napadalci pogosto izkoriščajo ranljivosti v spletnem programu in napadajo podatkovne baze, pri čemer je najpogostejši napad prav napad s SQL injekcijami, kjer z vnosom zlonamernih znakov SQL spremenijo logiko poizvedbe in pridobijo dostop do podatkov (Nasereddin in drugi, 2021).

Napade s SQL injekcijami lahko razvrstimo v različne kategorije glede na več dejavnikov, najcelovitejša in najpogostejša pa sta namen napadalca in način izvedbe. Namen se nanaša na cilj, ki ga želi napadalec doseči z napadom, na primer spreminjanje ali brisanje podatkov oziroma pridobivanje informacij o shemi podatkovne baze. Glede na to, kako to SQL stavek

pošljemo ali vstavimo pa je določen glede na klasifikacijo ranljivosti v spletni aplikaciji in pot, ki jo napadalec izbere. Poznamo 2 najpogostejši vrsti, in sicer po kakšnem vrstnem redu vstavimo SQL stavke in po odzivu strežnika (Nasereddin in drugi2021).

Glede na vrstni red izvedbe napada lahko SQL injekcije razdelimo na dve glavni vrsti. Pri napadu prvega reda gre za način napada, kjer napadalec neposredno vnaša zlonamerno kodo v ranljivo polje aplikacije. Pri napadu drugega reda pa napadalec vstavi del zlonamerne poizvedbe v zahtevek, ki sicer ni neposredno ranljiv, ta koda pa se izvede šele ob kasnejši poizvedbi, ki je dovzetna za SQL injekcije (Nasereddin in drugi, 2021).

Pri tej vrsti napada je odločilno, kako strežnik odgovori na spremembo in kaj razkrije. Tudi tukaj se deli na 2 dela, prvi je vnos neveljavnih/napačnih poizvedb, tukaj napadalec izkoristi odziv baze na napako, ki pogosto razkrije informacije o shemi podatkovne baze. To mu omogoča izvajanje nadaljnjih napadov, saj napake razkrijejo ranljivosti baze. Drugi pristop pa je časovno pogojeni slepi napad, tukaj pa napadalec pošilja bazi zaporedje vprašanj, na katera baza odgovarja posredno, napadalec pa glede na odziv sklepa o vsebini podatkov. Ta napad je zahtevnejši, saj podatki niso neposredno prikazani na spletni strani (Nasereddin in drugi, 2021).

Zaznavanje napadov s SQL injekcijami je zelo pomembno, zato so se razvile različne tehnike in metode, kako jih prepoznamo (Nasereddin in drugi, 2021):

- Statična analiza je pristop, ki zaznava slovnične in sintaktične napake v uporabniškem vnosu. Osredotoča se le na preverjanje veljavnosti uporabniškega vnosa, zato ne more zaznati zlonamernih vnosov, ki so po sintaksi pravilni.
- Pri randomizaciji naborov navodil gre za podvrsto statične analize, kjer se v SQL poizvedbe spletne aplikacije vstavljajo naključne vrednosti, nato pa se preverja odzivnost le-teh na spremembe za zaznavo napadov SQL injekcij.
- Dinamična analiza je metoda, ki preverja odziv spletne aplikacije tako, da vsak vhod posreduje cilju in analizira povratni odziv aplikacije.
- Kombinirana analiza je hibrid statične in dinamične metode, ki združuje prednosti obeh tehnik za učinkovitejše zaznavanje injekcijskih SQL napadov.
- Strojno učenje se uporablja za generiranje SQL poizvedb v spletnih aplikacijah in za učenje parametrov modela zaznavanja. Ta model se nato primerja z dinamičnimi poizvedbami SQL za odkrivanje nepravilnosti in morebitnih napadov.

4.4 Orodja za skeniranje ranljivosti sistema

Orodja za skeniranje ranljivosti IT osebju v sodobnih podjetjih omogočajo hitro prepoznavanje šibkih točk v omrežju, kot so odprta vrata, ki jih lahko izkoristijo nepooblaščeni uporabniki, ali aplikacije, ki nimajo nameščenih najnovejših varnostnih popravkov. S tem organizacije zagotovijo, da njihova omrežja sledijo interni varnostni politiki in zmanjšajo možnost zlorabe ranljivosti. Orodja za skeniranje ranljivosti lahko v grobem razdelimo na dve glavni skupini, in sicer spletna orodja in lokalna orodja. Prva so namenjena prepoznavanju ranljivosti, ki so

izpostavljene na javnem internetu in jih lahko izkoristijo napadalci, druga pa nadzorujejo notranji promet znotraj organizacijskega omrežja in pomagajo pri odkrivanju šibkih točk, ki bi jih sicer težje zaznali. Pomembno je, da se ti dve skupini orodij med seboj dopolnjujeta in lahko delujeta skupaj v omrežju, da dosežemo najbolj celovite rezultate. Orodja za skeniranje lahko delujejo tudi kot specializirani iskalniki, ki so usmerjeni bodisi na splošne cilje, kot je Google z naprednimi poizvedbami, ali na specifične ranljivosti, kot so odprta vrata, SSL/TLS pomanjkljivosti ali ranljivosti posameznih protokolov na primer SQL Injection ali XSS. Tako so ta orodja nujna za proaktivno zagotavljanje varnosti, saj omogočajo redno preverjanje in utrjevanje informacijskega okolja podjetja (Aboelfotoh in Hikal, 2019).

4.4.1 Spletna orodja

Spletna orodja za skeniranje ranljivosti so ključna za odkrivanje varnostnih pomanjkljivosti v omrežjih in sistemih sodobnih podjetij. Razdelimo jih lahko v dve glavni skupini specifična orodja in splošna orodja. Specifična orodja so usmerjena v zaznavanje točno določenih vrst ranljivosti ali pregled izpostavljenih storitev, medtem ko splošna orodja omogočajo širše iskanje občutljivih podatkov v javno dostopnih virih (Aboelfotoh in Hikal, 2019).

Nekatera specifična orodja so OWASP Zap, Shodan, Censys, ZoomEye in Pentest-tools. Vsako izmed teh orodij ima svoje prednosti in slabosti, in sicer enostavna uporaba, avtomatizacija, plačljivost, omejitve pri posodobitvah podatkov ipd., zato je priporočljivo kombinirati njihovo uporabo glede na varnostne cilje in potrebe organizacije (Aboelfotoh in Hikal, 2019).

Splošna orodja pa so iskalniki, kot je Google, kjer se varnostni strokovnjaki in napadalci uporabljajo posebne poizvedbe, imenovane Google Dorks. Gre za uporabo naprednih iskalnih operatorjev, s katerimi je mogoče najti občutljive datoteke, konfiguracije, prijavne strani, napake v aplikacijah, izpostavljene uporabniške podatke in drugo. Google Dorks so razdeljeni v več kategorij, npr. iskanje ranljivih strežnikov, napak, datotek z gesli ali uporabniškimi imeni, prijavnih strani, izpostavljenih naprav ipd. Iskalne poizvedbe so lahko sestavljene iz različnih dejavnikov, s čimer se omeji obseg rezultatov in lažje najde specifične informacije (Aboelfotoh in Hikal, 2019).

4.4.2 Lokalna orodja

Orodja za lokalno skeniranje ranljivosti lahko razdelimo na omrežno usmerjene optične čitalnike (network-based scanners) in optične čitalnike na gostitelju (host-based scanners). Vsaka izmed teh skupin ima svoje prednosti in slabosti ter posebna orodja, ki so standard v praksi (Aboelfotoh in Hikal, 2019).

Omrežno usmerjeni optični čitalniki so običajno nameščeni na osrednji napravi (npr. strežniku), s katere pregledujejo druge naprave v omrežju. Omogočajo odkrivanje kritičnih ranljivosti, kot so slabe konfiguracije požarnih zidov, nezaščiteni strežniki, zastarela programska oprema ali težave pri avtentikaciji znotraj omrežja. Poznamo več vrst teh optičnih čitalnikov, in sicer port

optične čitalnike, omrežne optične čitalnike ranljivosti, optične čitalnike za spletne strežnike, optične čitalnike za aplikacija ipd. (Aboelfotoh in Hikal, 2019).

Optični čitalniki na gostitelju pa so nameščeni neposredno na napravi, ki jo pregledujejo, in imajo s tem dostop do nizkonivojskih datotek operacijskega sistema, registrov, nameščenih aplikacij in konfiguracijskih datotek. Omogočajo poglobljeno analizo, spremljanje sumljivih dejavnosti, zaznavanje nepričakovanih programov ali sumljivih imen datotek ter preverjanje sistemske integritete (Aboelfotoh in Hikal, 2019).

5 ANALIZA KIBERNETSKE VARNOSTI IZBRANE SPLETNE REŠITVE

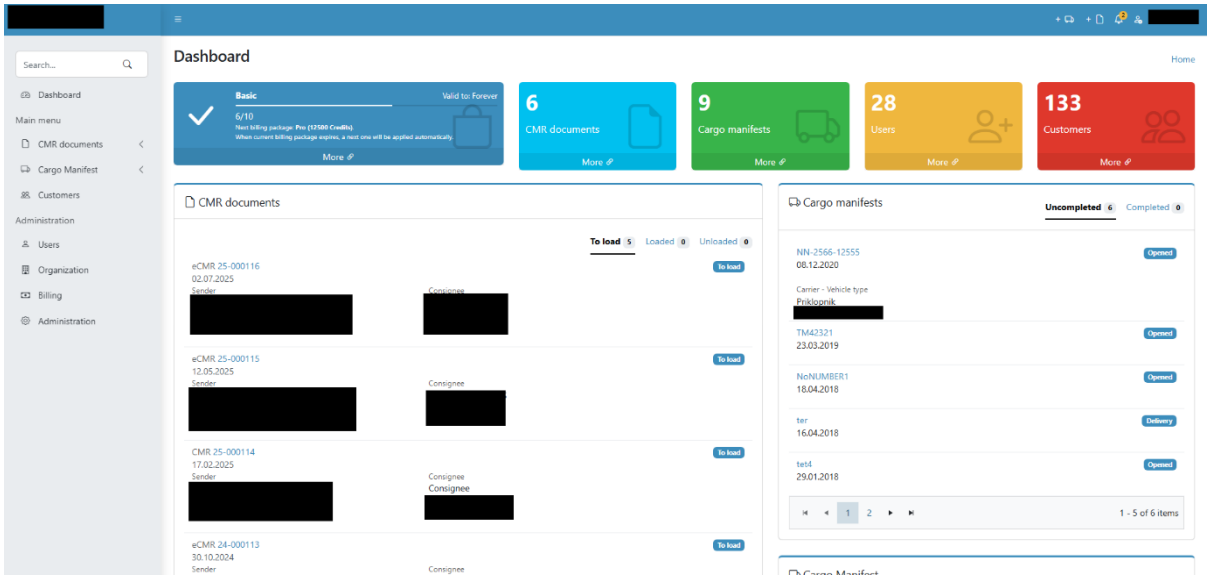
5.1 Predstavitev izbrane spletne rešitve

Preučevano podjetje je manjše slovensko IT-podjetje, ustanovljeno julija 1992, s sedežem v Ljubljani. Specializirano je za razvoj programske opreme za avtomatizacijo carinskih in logističnih postopkov. Podjetje predvsem podpira špedicijska, proizvodna in trgovska podjetja, za katera razvija rešitve za carinske in tranzitne postopke, pripravo transportne dokumentacije ter finančno poslovanje. Podjetje zaposluje približno 15 oseb, v letu 2024 pa je doseglo približno 2,18 milijona evrov letnih prihodkov ter okrog 285.000 evrov čistega dobička, kar kaže na stabilno poslovanje. Podjetje ima visok bonitetni razred AA+.

V okviru preverjanja kibernetske varnosti je bila za testiranje izbrana sodobna spletna spletna rešitev izbranega podjetja, ki omogoča digitalno upravljanje prevoznih dokumentov v logistiki. Gre za sistem, katerega jedro predstavlja elektronska verzija Sporazuma o pogodbi za mednarodni prevoz tovora po cesti (angl. Convention on the Contract for the International Carriage of Goods by Road - CMR) dokumentov, ki je digitaliziran obrazec, ki se uporablja v cestnem tovornem prometu za mednarodne pošiljke. Rešitev omogoča podjetjem, prevoznikom in njihovim partnerjem, da brezpapirno in učinkovito izdajajo, upravljajo ter arhivirajo tovorne dokumente, s čimer lahko izboljšajo poslovne procese.

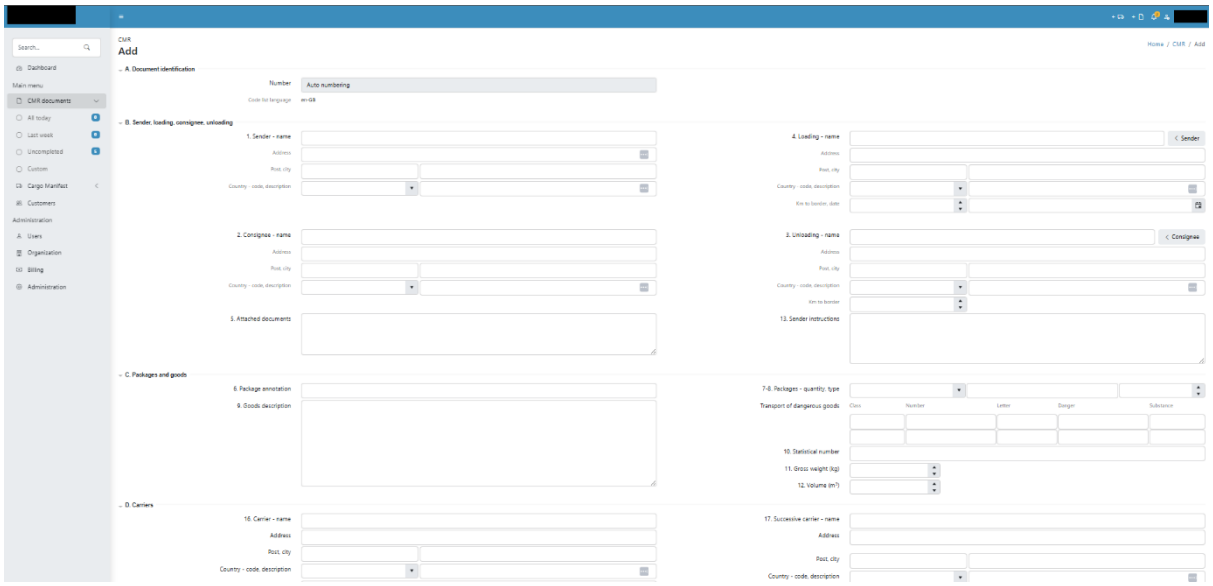
Uporabniški vmesnik spletne aplikacije temelji na enostavnosti in preglednosti, kar omogoča intuitivno uporabo tudi manj veščim uporabnikom. Na začetni strani ob prijavi so prikazani ključni podatki za uporabnika, kar je razvidno na sliki 1. V osrednjem delu rešitve je obrazec za vnos ključnih podatkov, kot so informacije o pošiljatelju, prejemniku, vozniku, vrsti tovora in tranzitnih točkah, kar je tudi razvidno na sliki 2. Obrazec je sestavljen iz preglednih polj in spustnih seznamov, ki vodijo uporabnika skozi postopek izpolnjevanja dokumenta.

Slika 1: Primer vmesnika začetne strani



Vir: Lastno delo (2025).

Slika 2: Primer obrazca za dodajanje dokumentov



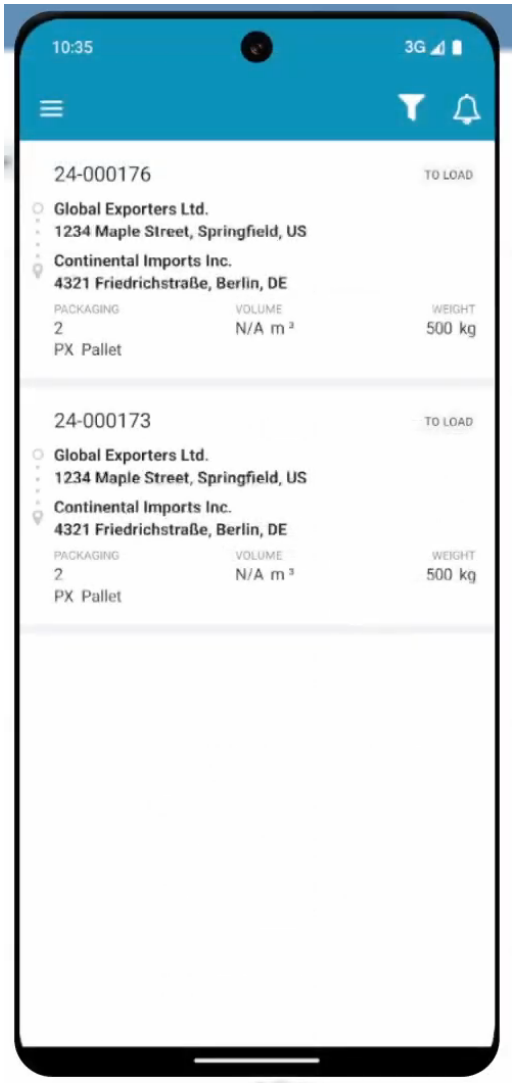
Vir: lastno delo (2025).

Sistem dodatno vključuje funkcije, kot so samodejno shranjevanje vnesenih podatkov in predlogi pogosto uporabljenih strank, kar bistveno pospeši izpolnjevanje in zmanjšuje napake. Posebna pozornost je namenjena večjezičnosti, saj rešitev podpira delo v različnih jezikih, kar je še posebej pomembno za mednarodne prevoze.

Arhitektura rešitve je zasnovana tako, da omogoča uporabo tako prek namiznih računalnikov kot tudi prek mobilnih naprav z mobilno aplikacijo (Slika 3). To pomeni, da lahko vozniki dostopajo do dokumentacije tudi na terenu, kar dodatno povečuje prilagodljivost in odzivnost prevoznih ekip. Integracija z drugimi sistemi je omogočena preko API-jev, kar omogoča

povezovanje s poslovnimi informacijskimi sistemi ali drugimi aplikacijami znotraj podjetja. Dokumenti se hranijo v oblaku, kar zagotavlja neprekinjen dostop in varnostno kopiranje, hkrati pa izpostavlja potrebo po premišljenem nadzoru dostopa in zaščiti podatkov.

Slika 3: Mobilna aplikacija



Vir: Lastno delo (2025).

Z vidika varnosti rešitev vključuje osnovne mehanizme za avtentikacijo uporabnikov in upravljanje pravic glede na dodeljene vloge. Določeni uporabniki lahko ustvarjajo dokumente, drugi pa jih le pregledajo ali potrjujejo, kar zmanjšuje možnost notranjih zlorab. V sistem je vključeno tudi revizijsko sledenje, kar pomeni, da so vse spremembe dokumentov zabeležene in sledljive, kar je ključno za preglednost poslovanja in kasnejše preverjanje dogodkov. Aplikacija vključuje tudi orodja za komunikacijo med udeleženci prevoznega procesa, na primer med pošiljateljem, prevoznikom in prejemnikom. Čeprav to omogoča hitrejše usklajevanje in reševanje morebitnih težav, predstavlja tudi dodatno površino napada, ki zahteva ustrezno šifriranje in nadzor. Rešitev je zanimiva tako s tehnološkega kot tudi z varnostnega vidika. Ponuja učinkovito digitalno alternativo papirni dokumentaciji in s tem

odpira pomembna vprašanja, povezana z varnostjo podatkov, nadzorom dostopa ter zagotavljanjem integritete elektronskih dokumentov v mednarodnem prometu. Njen razvoj kaže na vse večje potrebe po avtomatizaciji in digitalizaciji znotraj transportne panoge, hkrati pa izpostavlja kompleksnost zagotavljanja varnosti v okolju, ki vključuje več uporabniških vlog, dinamične podatke in različne komunikacijske kanale.

5.2 Uporabljena metodologija

Pri izvedbi varnostnega preizkusa izbrane spletne rešitve je bila uporabljena večnivojska metodologija, ki je združevala tako tehnične kot psihološke pristope k ugotavljanju ranljivosti. Preverjanje je bilo razdeljeno v dve ključni fazi, ki se medsebojno dopolnjujeta in skupaj zagotavljata celostno sliko o varnostni zrelosti testirane aplikacije. Prva faza metodologije je temeljila na pristopu testiranja aplikacije s pomočjo specializiranih orodij, pri čemer sta bila osrednji orodji OWASP ZAP in platforma Intruder.io. Uporabljena je bila metoda t. i. "black-box" testiranja, kjer preizkuševalec nima neposrednega dostopa do izvorne kode ali notranjih mehanizmov sistema. Ta pristop simulira napad zunanjega napadalca, ki do aplikacije dostopa le kot običajen uporabnik prek spletnega vmesnika. Z OWASP ZAP sem analiziral promet med odjemalcem in strežnikom, identificiral aktivne vhodne točke ter preizkušal odpornost aplikacije na standardne spletne napade, kot so XSS, manipulacije s parametri URL, ranljivosti v HTTP glavah in vnosnih poljih. Platforma Intruder.io je dopolnila pregled s podrobno avtomatizirano analizo strežniške konfiguracije, odprtih storitev ter potencialno znanih ranljivosti v uporabljenih tehnologijah. Skupaj sta orodji omogočili tako širok kot poglobljen vpogled v varnostno stanje aplikacije.

Druga faza metodologije je vključevala preizkus socialnega inženiringa, kjer so bili cilji usmerjeni v analizo vedenja uporabnikov in njihove zmožnosti prepoznave zavajajočih komunikacij. Ta del je bil ključen za razumevanje, kako človeški dejavnik vpliva na splošno varnost informacijskega sistema. Z uporabo javno dostopnih informacij smo identificirali ključne osebe v podjetju in oblikovali lažno komunikacijo, ki je temeljila na realističnem scenariju varnostnega incidenta. Sporočilo, poslano v zgodnjih jutranjih urah, je uporabnike pozivalo k takojšnji spremembi gesla prek povezave, ki je vodila na ponarejeno spletno stran. Znotraj testnega okolja smo spremljali, ali bi uporabniki nasedli takšni taktiki in dejansko sledili navodilom. Izbrana metodologija je bila načrtno večplastna. Tehnični del je pokazal odpornost aplikacije na standardizirane kibernetske napade, medtem ko je psihološki vidik razkril, kako pomembna je ustrezna varnostna kultura in ozaveščenost zaposlenih. Poudarek je bil na uporabi realnih scenarijev, ki odražajo sodobne prakse napadalcev v resničnem svetu. Tak pristop omogoča realno oceno varnostnega tveganja ter zagotavlja bolj relevantna priporočila za izboljšave.

5.3 Izvedba preizkusa varnosti spletne rešitve

Preizkus varnosti spletne rešitve je bil izveden v več fazah, s poudarkom na preverjanju delovanja aplikacije z uporabo testnih orodij, na simulaciji zunanjega napadalca in vključitvi izbranih elementov socialnega inženiringa. Namen testa je bil preveriti, kako učinkovito

aplikacija varuje podatke pred nepooblaščenim dostopom ter kako se odziva na različne vrste manipulacij s strani uporabnika ali napadalca.

5.3.1 Testiranje varnosti z aplikacijo OWASP ZAP in intruder.io

V prvi fazi varnostnega preizkusa je bila izvedena analiza neposredne komunikacije med uporabnikom in strežnikom z uporabo orodij OWASP ZAP in Intruder.io. Namen te faze je bil odkriti morebitne ranljivosti, napačne konfiguracije ter izpostavljene storitve, ki bi jih lahko zlonamerni uporabniki izkoristili za dostop do sistema ali podatkov.

Z uporabo OWASP ZAP je bil najprej izveden pasivni pregled, kjer so se beležili piškotki, HTTP glave, preusmeritve in druge informacije, ki se izmenjujejo med odjemalcem in strežnikom. Tako je bilo mogoče preveriti, ali se uporabljajo ustrezne varnostne nastavitve npr. Secure in HttpOnly za piškotke in ali so morebitni odzivi strežnika preveč informativni. V nadaljevanju je bila aktivna faza testiranja usmerjena v pošiljanje manipuliranih HTTP zahtevkov, s katerimi se je testirala odpornost aplikacije na najpogostejše spletne ranljivosti, kot so XSS, SQL Injection, CSRF in path traversal. OWASP ZAP ni zaznal kritičnih ranljivosti, vendar je pokazal, da določeni odgovori strežnika ne vključujejo vseh varnostnih HTTP glav, kar pomeni potencialno izpostavljenost v primeru bolj ciljanih napadov.

Za dopolnitev testiranja je bila uporabljena tudi platforma Intruder.io, ki omogoča avtomatizirano skeniranje ranljivosti za spletne aplikacije in infrastrukturo. Skeniranje je zajelo 71.773 posameznih preverjanj, ki so bila usmerjena na:

- znane ranljivostih v programski in strežniški opremi,
- napačne konfiguracije SSL/TLS protokolov,
- nepravilno nastavljene HTTP glav,
- prisotnost občutljivih informacij in
- preverjanje zaščite pred napadi.

Poročilo je razkrilo 2 varnostni težavi eno srednje in eno nizke stopnje. Težava srednje resnosti je bila nezaupanja vreden certifikat TLS. Sistem uporablja certifikat TLS, ki ni zaupanja vreden oziroma ni izdan s strani priznane overiteljske organizacije. To pomeni, da bo večina brskalnikov ob povezavi prikazala opozorilo, saj povezave ne morejo potrditi kot varne. Takšen položaj odpira možnost napada tipa »Man in the middle«, kjer bi napadalec lahko prestregel ali manipuliral s komunikacijo med uporabnikom in strežnikom, zlasti v javnih omrežjih. To napako bi odpravili s tem, da se namesti veljaven, zaupanja vreden certifikat TLS, preveri ujemanje z domeno ter zagotovi, da certifikat ne poteče in ne presega priporočene dolžine veljavnosti.

Druga napaka nizke resnosti pa je bila manjkajoča HTTP glava »Strict-Transport-Security«. To pomeni, da strežnik ne pošilja HTTP glave »Strict-Transport-Security«, ki brskalniku narekuje, naj se s to spletno stranjo povezuje izključno prek varne HTTPS povezave. Brez te glave lahko napadalec v vmesnem položaju poskuša uporabnika preusmeriti na nezavarovano različico

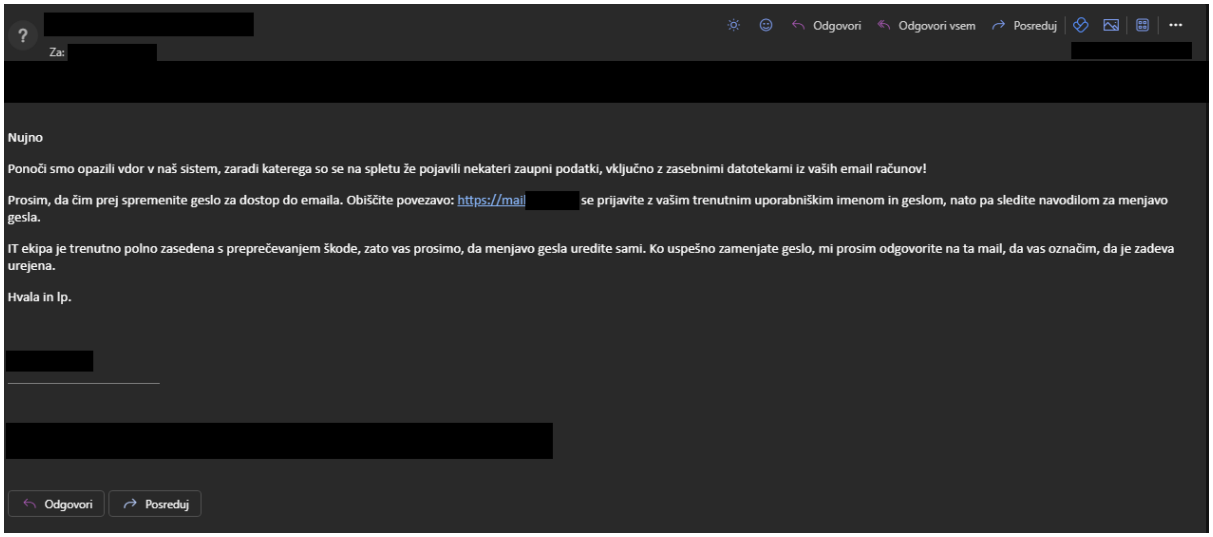
strani. To bi rešili s tem, da bi umestili v konfiguracijo strežnika ustrezno glavo »Strict-Transport-Security: max-age=7776000; includeSubDomains«. S tem se brskalniku določi, da mora naslednjih 90 dni ali več komunicirati izključno prek HTTPS in velja tudi za vse poddomene. Podrobnejše informacije so navedene tudi v poročilu, ki pa je pod prilogami. Skupna ocena ogroženosti sistema, podana v poročilu, je bila srednja. Čeprav v trenutku testiranja ni bilo zaznanih visoko kritičnih ranljivosti, bi naprednejši napadalci lahko izkoristili opisane pomanjkljivosti v primeru ciljanega napada. Zato je priporočljivo, da se popravki izvedejo v roku 90 dni, še posebej v primeru javno dostopnih sistemov.

5.3.2 Testiranje varnosti s pomočjo socialnega inženiringa

V drugi fazi varnostnega preizkusa je testiranje vključevalo elemente socialnega inženiringa, saj je v realnem okolju pogosto prav človeški dejavnik tisti, ki odpira vrata posameznemu napadu. Izvedena je bila simulacija napada z uporabo »zvabljalskega« e-poštnega sporočila, v katerem je bila uporabnikom poslana povezava do ponarejene strani, ki je na videz posnemala legitimno stran za menjavo gesla znotraj testirane aplikacije. Stran je bila oblikovana tako, da je vizualno čim bolj prepričljivo posnemala original, vključno z logotipom, grafično podobo in postavitvijo vnosnih polj. Glavni cilj testa ni bil dejansko zbiranje poverilnic, temveč spremljanje interakcije uporabnikov ali bodo kliknili na povezavo, ali bodo opazili sumljiv URL in ali bodo vpisali občutljive podatke. Poskusi so bili izvedeni pod kontroliranimi pogoji, brez ogrožanja resničnih uporabniških podatkov.

Najprej je bila izvedena osnovna analiza, pri kateri smo z uporabo javno dostopnih virov poiskali vodilne osebe oziroma lastnike podjetja, povezane z uporabo testirane aplikacije. Preko spletnih strani podjetja, družbenih omrežij in poslovnih imenikov smo zbrali informacije, ki so nam omogočile oblikovanje prepričljivega konteksta. Nato smo oblikovali lažni e-poštni naslov, ki je na prvi pogled skoraj identičen originalnemu. Zamenjali smo črko »i« s črko »l« v domeni elektronske pošte na primer »ime.priimek@siol.net« se spremeni v »ime.priimek@slol.net«, kar je ob hitrem branju videti skoraj enako. E-poštno sporočilo je bilo poslano zgodaj zjutraj, okoli 6. ure, kar je bil nameren taktičen element. Zgodnji čas sporočila je ustvaril občutek nujnosti in nepredvidenega dogodka, kar poveča verjetnost impulzivnega odziva. V vsebini je bilo zapisano, da je sistem podjetja čez noč doživel varnostni incident, pri čemer je domnevni napadalec pridobil dostop do uporabniških računov. Sporočilo je bilo oblikovano, kot urgentno obvestilo IT oddelka, ki poziva uporabnike, naj nemudoma spremenijo gesla, da bi zaščitili svoj račun pred nadaljnjo zlorabo (slika 4). Za večjo prepričljivost je bilo sporočilo oblikovano v tonu, ki odraža formalnost in skrb, vključeni so bili običajni podpisi in kontaktna številka, poleg tega pa tudi neposredna povezava za spremembo gesla. Ta povezava je vodila na lažno spletno stran, ki je vizualno popolnoma posnemala uradno stran za prijavo vključno z logotipom, grafičnimi elementi in obrazcem.

Slika 4: Primer elektronske pošte



Vir: lastno delo (2025).

Ključen namen testa ni bil zbiranje podatkov, temveč ocena, ali bi povprečen uporabnik kliknil na povezavo in začel vnašati podatke, kar smo spremljali prek nadzorovanega sistema. Opažanja so pokazala, da bi manj pozoren ali zaspani uporabnik, zlasti v zgodnjih jutranjih urah, brez dodatnega preverjanja verodostojnosti e-sporočila kliknil na povezavo in začel proces vnosa. To jasno kaže, kako učinkovit je socialni inženiring, kadar temelji na realističnem scenariju in čustvenem pritisku. Simulacija je potrdila, da je tudi tehnično dobro zaščitena aplikacija lahko ranljiva, če uporabniki niso ustrezno izobraženi za prepoznavanje poskusov zlorab.

5.4 Analiza rezultatov

Rezultati varnostnega preizkusa izbrane spletne rešitve so pokazali, da aplikacija kljub osnovni zaščiti pred pogostimi tehničnimi napadi še vedno vsebuje določene ranljivosti, ki bi jih bilo mogoče izkoristiti v primeru ciljanega napada. Poleg tega je bila v drugem delu testa jasno potrjena tudi ranljivost človeškega dejavnika, kar dodatno potrjuje potrebo po celovitem pristopu k informacijski varnosti, ki vključuje tako tehnične kot organizacijske ukrepe.

V okviru tehničnega testiranja, izvedenega z uporabo OWASP ZAP in platforme Intruder.io, niso bile odkrite kritične sistemske pomanjkljivosti. Aplikacija se je izkazala za odpornejšo proti klasičnim napadom, kot so SQL Injection, XSS in CSRF, kar kaže na osnovno implementacijo varnostnih mehanizmov pri ravnanju z uporabniškimi vhodi. Kljub temu pa sta bila zaznana dva pomembna varnostna izziva. Nezaupanja vreden TLS certifikat kar pomeni neposredno izpostavljenost napadom tipa »Man in the Middle«, zlasti v javnih omrežjih. To izpostavlja dejstvo, da tudi minimalni tehnični nadzor lahko prepreči verodostojno šifriranje komunikacije in pa manjkajoča HTTP glava »Strict-Transport-Security« kljub temu, da gre za napako nizke stopnje, pomeni zmanjšano zaščito uporabnikov pred manipulacijo z nezavarovanimi povezavami. Obe pomanjkljivosti sta odpravljivi z ustrezno konfiguracijo

strežnika in implementacijo zaupanja vrednega certifikata. Skupna ocena ogroženosti sistema je bila s strani orodja Intruder.io ocenjena kot srednja, kar pomeni, da sicer ni neposredne nevarnosti, vendar bi lahko bolj napreden napadalec uspešno izkoristil prisotne šibkosti. Celotno poročilo je pripeto kot priloga 1.

V okviru socialnega inženiringa pa se je izkazalo, da je tukaj višja stopnja tveganja. Uporabniki so bili postavljeni v položaj, ki je temeljil na realistično zasnovani »zvabljajoči« taktiki, podprti z vizualno prepričljivim e-poštnim sporočilom in lažno spletno stranjo za ponastavitev gesla. Ključni dejavniki za kar se da uspešno izvedbo napada so bili: psihološki pritisk s časovno omejenim odzivom, zgodnje jutranje ure, sporočilo o varnostnem incidentu, vizualna podobnost domene in spletnega vmesnika in pa uporaba prepričljivega tona ter vključitev znanih podatkov o podjetju, kot je npr. e-naslov osebe na visokem položaju.

Rezultati so pokazali, da je približno polovica uporabnikov kliknila na lažno povezavo, ki je bila vključena v elektronski pošti, od teh pa so trije uporabniki celo vnesli staro in novo geslo in smo s tem pridobili tudi podatke, ki smo jih iskali. Gre za pomembno ugotovitev, saj to pomeni, da bi v realnem scenariju lahko napadalec pridobil dostop do občutljivih računov brez uporabe tehničnih napadov. Uporabniki so v tem primeru sami posredovali vse dostopne podatke. Ta oblika pomeni, da je napad skoraj nemogoče zaznati, če ni dodatnih zaščitnih mehanizmov npr. MFA ali opozoril o sumljivih prijavah.

Čeprav je aplikacija tehnično zmerno varna, rezultati testiranja jasno kažejo, da je glavni varnostni izziv pomanjkanje ozaveščenosti uporabnikov. Dejstvo, da je polovica ciljnih uporabnikov kliknila povezavo in da so trije dejansko vnesli gesla, nakazuje visoko stopnjo ranljivosti na socialni inženiring. To predstavlja realno tveganje, saj bi lahko napadalec že z enim uspešnim poskusom pridobil dostop do internih sistemov, elektronske pošte ali drugih občutljivih virov. Zato je bistveno, da se poleg tehničnih ukrepov uvedejo tudi mehki varnostni ukrepi, kot so redna izobraževanja, simulacije »zvabljajočih« napadov in obvezna večstopenjska avtentikacija.

5.5 Predlogi za omilitev groženj

Na podlagi izvedenih testiranj in pridobljenih rezultatov je mogoče oblikovati nabor priporočil, ki bistveno pripomorejo k izboljšanju varnosti spletne rešitve. Priporočila so usmerjena tako v odpravo konkretno zaznanih ranljivosti kot tudi v dvig splošne odpornosti sistema proti prihodnjim napadom. Predlagani ukrepi vključujejo tehnične izboljšave, prilagoditve strežniške konfiguracije in organizacijske spremembe, povezane z uporabniki.

5.5.1 Ureditev certifikata TLS

Zaradi zaznane pomanjkljivosti, kjer sistem uporablja nezaupanja vreden TLS certifikat, je priporočljivo, da se namestiti veljaven in zaupanja vreden certifikat TLS, izdan s strani akreditirane overiteljske organizacije, preveri se, če se commonName oziroma subjectAltName certifikata ujema z domeno aplikacije in zagotoviti je treba redno podaljševanje certifikata, da

se prepreči njegovo nedelovanje. S tem se bo bistveno izboljšala zaupnost in celovitost prenosa podatkov med strežnikom in uporabnikom.

5.5.2 Vključitev glave »Strict-Transport-Security«

Za dodatno zaščito komunikacije in preprečitev napadov z vmesnim prestrezanjem npr. preusmeritev na HTTP je priporočljivo, da strežnik pri vsaki HTTPS povezavi pošlje tudi glava »Strict-Transport-Security« s tem brskalnik zapomni, da mora z aplikacijo komunicirati izključno prek HTTPS, kar znatno zmanjša možnosti napada v nešifriranem okolju.

5.5.3 Uvedba večstopenjske avtentikacije (MFA)

Ker je bil v simulaciji socialnega inženiringa zabeležen dejanski vnos gesel na lažni strani, se priporoča uvedba obvezne dvostopenjske avtentikacije (MFA) za vse uporabnike, uporaba mobilnih aplikacij za generacijo enkratnih kod npr. Google Authenticator ali SMS-sporočil, možnost prijave samo iz odobrenih naprav ali IP-naslovov. S temi zaščitami, tudi če pride do kraje gesla, bo napadalec brez drugega dejavnika še vedno onemogočen pri dostopu.

5.5.4 Redna ozaveščevalna izobraževanja uporabnikov

Socialni inženiring je pokazal visoko uspešnost, zato je ključno, da uporabniki znajo prepoznati znake zlorabe. Prav zaradi tega je zelo pomembno izvajanje rednih izobraževanj in usposabljanj, vsaj 1x letno. Poleg izobraževanj pa naj se uporabijo tudi interaktivne simulacije napadov zvabljanja.

Izobraževanja in usposabljanja zaposlenih predstavljajo enega izmed ključnih stebrov informacijske varnosti. Tehnično zaščitena infrastruktura lahko zelo hitro postane neučinkovita, če uporabniki niso dovolj usposobljeni za prepoznavanje nevarnosti, ki jih prinašajo sodobne oblike napadov, kot so zvabljanje, usmerjeno zvabljanje, zlonamerne povezave ali socialni inženiring.

Redno izvajanje predavanj oziroma izobraževanj bo pripomoglo k temu, da bodo zaposleni zmanjšali človeške napake, ki so eden najpogostejših vzrokov za varnostne incidente, pripomoglo bo tudi k temu, da bodo zaposleni prepoznali sumljiva elektronska sporočila, povezave in priloge ter se bodo pravilno odzivali nanje. Poleg tega to krepi varnostno kulturo znotraj podjetja, kjer vsak posameznik razume svojo vlogo pri zaščiti informacijskih sredstev. Simulacije napadov pripomorejo tudi k praktični pripravi na realne scenarije s tem, saj zaposleni spoznajo, kako prepričljive so lahko zlonamerne taktike. Poleg tega pa je pomembno, da so zaposleni ozaveščeni o pravnih in poslovnih posledicah napak, ki vodijo v uhajanje podatkov ali motnje v poslovanju.

Usposabljanja lahko vključujejo različne oblike: spletne module, delavnice v živo, predstavitve primerov napadov iz prakse, kvize z motivacijskimi nagradami, ali celo vnaprej neznane testne napade z lažnimi sporočili, ki merijo odzivnost uporabnikov. Pomembno je tudi, da se vsebine redno posodabljajo, saj se taktike napadalcev hitro razvijajo. Prav tako naj bodo usposabljanja,

prilagojena različnim vlogam v organizaciji, vodilno osebje, IT osebje in končni uporabniki se namreč soočajo z različnimi tveganji in potrebujejo različno poglobljeno znanje. Z uvedbo strukturiranih in ponavljajočih se izobraževanj lahko podjetje doseže, da uporabniki postanejo »človeški požarni zid«, ki aktivno preprečuje vdor, še preden pride do interakcije s samim sistemom.

5.5.5 Dodatna priporočila

Dodatna priporočila, ki bi pripomogla k varnosti, so tudi implementacija opozoril za sumljive prijave, zlasti če se uporabnik prijavi z nenavadne lokacije ali naprave, redna varnostna testiranja, vsaj dvakrat letno ali ob večjih nadgradnjah sistema, vpeljava revizijskih dnevnikov, ki omogočajo sledenje pomembnim dogodkom, spremembam in prijavam. Z implementacijo teh priporočil bo aplikacija bistveno bolj odporna proti tehničnim napadom, hkrati pa bodo uporabniki bolje opremljeni za prepoznavanje manipulativnih poskusov zlorabe.

6 DISKUSIJA

6.1 Predstavitev ključnih ugotovitev

Izvedeni preizkus varnosti spletne rešitve je pokazal, da učinkovita zaščita informacijskih sistemov zahteva večplastni pristop, ki vključuje tako tehnične kot organizacijske vidike. Rezultati testiranja potrjujejo, da osnovni varnostni mehanizmi v aplikaciji obstajajo, vendar so prisotne pomanjkljivosti, ki bi lahko bile izkoriščene ob ciljanem napadu. Poleg tega je bilo skozi simulacijo socialnega inženiringa razvidno, da je človeški dejavnik še vedno ena največjih šibkosti v varnostnem sistemu.

Ključne ugotovitve pri tehničnem testiranju kažejo, da je aplikacija odporna proti večini osnovnih napadov, kot je SQL Injection, kar kaže na ustrezno obravnavo uporabniških vhodov in osnovno zaščito logike aplikacije. Z uporabo orodij Intruder.io in OWASP ZAP sta bili zaznani dve tehnični pomanjkljivosti, uporaba nezaupanja vrednega certifikata TLS ter manjkajoča HTTP glava »Strict-Transport-Security«. Obe pomanjkljivosti namreč zmanjšujeta varnost komunikacije med odjemalcem in strežnikom ter povečujeta možnost prestrezanja podatkov v primeru napada. Varnostno poročilo je ocenilo skupno stopnjo ogroženosti kot srednjo, kar pomeni, da trenutno ni neposredne izpostavljenosti najnevarnejšim grožnjam, vendar ob odsotnosti dodatnih ukrepov ostajajo določena tveganja realna.

Drugi del testiranja, ki je temeljil na socialnem inženiringu, je prinesel bolj skrb vzbujajoče ugotovitve. Preko simuliranega napada smo ugotovili, da je približno polovica uporabnikov kliknila na povezavo, vključeno v lažno e-poštno sporočilo, trije pa so celo vnesli gesla na ponarejeni strani. Takšen položaj bi v realnem okolju zadostoval za uspešno prevzemanje uporabniških računov in s tem dostop do podatkov znotraj sistema. Rezultati potrjujejo, da tudi pri aplikaciji z razmeroma dobrim tehničnim varnostnim okvirom uspeh napadalca pogosto temelji na psihološkem manipuliranju z zaposlenimi, kar je še posebej nevarno v panogah, kjer informacije krožijo hitro, v realnem času in pogosto pod pritiskom.

Če tak scenarij preslikamo v specifični kontekst transportne panoge, kjer se uporablja testirana rešitev, so lahko posledice varnostnega incidenta veliko širše. Elektronski tovorni listi e-CMR, logistične poti, podatki o pošiljkah in identitetah strank so informacije, ki so ključne za vsakdanje operacije. Neavtoriziran dostop do teh podatkov lahko privede do sprememb v dostavnih podatkih, kraje blaga, preusmeritev tovorov ali manipulacije s carinskimi informacijami. V primeru uhajanja podatkov bi podjetje lahko utrpelo škodo v obliki izgube poslovnih partnerjev, zamud v dobavnih verigah, pogodbene odgovornosti in kazenskih sankcij, še posebej v čezmejnem prometu, kjer veljajo strožja pravila. Stroški, povezani s takimi incidenti, pa ne obsegajo zgolj odprave posledic, temveč tudi povračila strankam, pravnih postopkov, izgube zaupanja in morebitnega izpada prihodkov. Zaradi tesne časovne občutljivosti v transportni dejavnosti je vsaka prekinitev ali zloraba podatkov lahko neposredno povezana s finančnimi izgubami. Zamude pri dostavah, zamenjave prevoznih poti ali dostop do informacij o dragocenem tovoru s strani tretjih oseb pomenijo namreč konkretna tveganja. Poleg tega je treba upoštevati dejstvo, da se številni procesi v tej panogi že izvajajo avtomatizirano in so integrirani z zunanjimi sistemi, kar še dodatno povečuje površino napada in posledično zahteve po robustni zaščiti.

Preizkus je jasno pokazal, da je za učinkovito kibernetsko varnost treba obvladovati tako tehnične konfiguracije kot tudi vedenjske dejavnike uporabnikov. Ranljivosti niso bile le posledica pomanjkljive tehnične zaščite, temveč predvsem posledica človeških napak in neprepoznavanja varnostnih tveganj v praksi. Zato je izboljšanje varnosti mogoče doseči le z usklajenim delovanjem na obeh področjih s tehnično nadgradnjo in z vlaganjem v varnostno kulturo. Zlasti v sektorjih, kot je transport, kjer motnje v delovanju pomenijo realno poslovno škodo.

6.2 Primerjava ugotovitev iz literature in ugotovitve empiričnega dela

Teoretični okvir informacijske varnosti temelji na predpostavki, da celovit pristop vključuje tehnično zaščito in zavedanje uporabnikov o varnostnih tveganjih. V sodobnih smernicah in literaturi, zlasti v dokumentih, kot so OWASP Top 10 in smernice ISO/IEC 27001, je jasno poudarjeno, da učinkovita zaščita ni zgolj rezultat tehničnih rešitev, temveč kombinacija tehnologije, procesov in ljudi (Paule, 2023). V empiričnem delu naloge so bile te trditve neposredno preverjene z dejanskim varnostnim preizkusom izbrane spletne aplikacije, ki se uporablja v transportni panogi. V skladu s teoretičnimi pričakovanji je bilo v prvi fazi testiranja uporabljeno orodje OWASP ZAP, ki je omogočilo preverjanje aplikacije z vidika najpogostejših spletnih ranljivosti. Rezultati so pokazali, da je aplikacija razmeroma dobro zaščitena pred osnovnimi napadi, kot so XSS in SQL Injection, kar sovpada s pričakovanjem, da sodobne aplikacije vsebujejo osnovne mehanizme validacije in sanacije uporabniških vhodov. Po drugi strani pa sta bili v skladu z literaturo zaznani ranljivosti v konfiguraciji TLS in manjkajoči glavi HSTS, kar potrjuje, da tudi pri tehnično stabilnih rešitvah pogosto prihaja do napak v strežniški ali omrežni konfiguraciji.

V drugem delu pa je ujemanje med teorijo in prakso pokazalo testiranje, kjer je bil uporabljen pristop socialnega inženiringa. V literaturi je človeški dejavnik opisan kot najbolj nepredvidljiv in najpogosteje izkoriščen element v napadih na informacijske sisteme (KeepNet, 2025). Empirični del je to potrdil. Kljub temu da aplikacija ni imela kritičnih varnostnih pomanjkljivosti, je bil simuliran napad z lažno e-pošto zelo uspešen. Dejstvo, da je več uporabnikov kliknilo na povezavo in celo vneslo geslo, dokazuje, da so občutek nujnosti, avtoriteta in zgodnji čas pošiljanja sporočila, v praksi še vedno zelo učinkoviti.

Dodatno primerjavo je mogoče zaznati tudi pri priporočilih. Teorija jasno priporoča večstopenjsko avtentikacijo, redna varnostna testiranja, šifrirano komunikacijo in izobraževanje uporabnikov kot bistvene gradnike varnostne arhitekture (Samociuk, 2023). V empiričnem delu so bila ta priporočila potrjena in konkretizirana skozi rezultate testiranja. Pokazalo se je, da je večino ranljivosti mogoče odpraviti z znanimi ukrepi, vendar so ti ukrepi učinkoviti le, če so tudi implementirani in razumljeni v vsakdanji uporabi sistema. Primerjava torej kaže visoko stopnjo skladnosti med teoretičnimi zasnovami kibernetske varnosti in empirično izvedenim testiranjem. Ugotovitve potrjujejo, da teoretični modeli, čeprav pogosto oblikovani v univerzalnem kontekstu, zelo dobro opišejo dejanske nevarnosti in šibkosti, s katerimi se soočajo organizacije, tudi v specializiranih panogah, kot je transport. Empirična izvedba ne le potrjuje teorijo, temveč jo tudi dopolnjuje z vpogledom v konkretne odzive uporabnikov, kar dodatno poudarja potrebo po praktičnem testiranju kot dopolnilu k varnostnim načrtom.

6.3 Omejitve raziskave

Kljub načrtovani izvedbi in večplastnemu pristopu k varnostnemu preizkusu ima raziskava določene omejitve, ki jih je treba upoštevati pri rezultatih. Ena izmed pomembnejših omejitev je dejstvo, da je bila aplikacija testirana v specifičnem časovnem okvirju, kar pomeni, da rezultati odražajo stanje v času testiranja. Programska oprema se redno posodablja, s tem pa se spreminja tudi njen varnostni profil, zato bi bil ponovni test ob kasnejših različicah lahko bistveno drugačen.

Testiranje je bilo izvedeno iz perspektive zunanjega napadalca, brez dostopa do izvorne kode aplikacije in notranjih strežniških nastavitev, kar pomeni, da analiza ni zajela morebitnih napak v poslovni logiki, ki bi jih lahko odkril le napadalec z več notranjega znanja ali z drugačnim pristopom. Prav tako ni bilo mogoče opraviti obremenitvenih testov ali preverjanja odzivnosti sistema pod večjim pritiskom, saj bi to lahko ogrozilo realno delovanje aplikacije in povzročilo prekinitev storitve. Tudi simulacija socialnega inženiringa, čeprav zasnovana realistično, je bila izvedena v omejenem okolju. Uporabniki niso bili obveščeni, vendar v testnem scenariju niso doživeli dejanskih posledic svojega ravnanja, zato njihovo vedenje morda ne povsem odraža reakcij v realnih okoliščinah, kjer bi bile posledice klikov ali vnosa podatkov občutno večje. Poleg teh omejitev velja omeniti še dejstvo, da raziskava temelji na eni konkretni spletni rešitvi znotraj transportne panoge. Čeprav aplikacija predstavlja tipičen primer digitalnega upravljanja

dokumentacije, njene specifične lastnosti ne omogočajo popolne posplošitve na vse druge informacijske sisteme v panogi.

6.4 Smernice za nadaljnje delo

Rezultati raziskave so jasno pokazali, da je preverjanje kibernetske varnosti spletnih rešitev ključnega pomena, še posebej v panogah, kjer se digitalizacija poslovnih procesov hitro širi. V prihodnosti bi bilo smiselno izpeljati dodatne raziskave, ki bi presegale okvire ene same aplikacije in omogočale primerjalno analizo več različnih sistemov, ki se uporabljajo v logistiki, transportu in širše v industriji oskrbovalnih verig. S tem bi bilo mogoče pridobiti bolj celovit vpogled v splošne trende, ranljivosti in skupne točke, ki ogrožajo digitalno varnost v tej panogi. Raziskavo bi bilo mogoče nadgraditi tudi z metodološkega vidika. Tokratni pristop je temeljil predvsem na orodjih za avtomatizirano testiranje in eni simulaciji socialnega inženiringa. Lahko bi tudi spremljali dolgoročno, kako se vedejo uporabniki po izvedenih izobraževanjih in simulacijah.

7 SKLEP

Kibernetska varnost postaja ena ključnih strateških prioritet sodobnih organizacij, saj so informacijski sistemi danes temelj poslovanja v skoraj vseh panogah. Zaradi vedno večje digitalne povezanosti, obdelave občutljivih podatkov in odvisnosti od spletnih rešitev, se posledice kibernetskih napadov ne kažejo več zgolj kot tehnične motnje, temveč povzročajo resne poslovne, pravne in družbene posledice. Napadalci uporabljajo vedno bolj prefinjena metode, hkrati pa človeški dejavnik ostaja ena najpogostejših točk zlorabe.

Namen magistrskega dela je bil razumeti, kakšne kibernetske grožnje so danes prisotne ob uporabi spletnih rešitev v transportni panogi in prepoznati, kako se pred njimi organizacije lahko učinkovito zaščitijo. V magistrskem delu je bil zato izveden celovit preizkus kibernetske varnosti izbrane spletne rešitve, ki se uporablja v transportni panogi za digitalno upravljanje prevoznih dokumentov, s katerim sem želel preveriti, kako dobro je izbrana aplikacija pripravljena na zunanje in notranje varnostne grožnje, ter hkrati oceniti vpliv človeškega dejavnika na celotno varnostno sliko. Z združitvijo tehničnega testiranja z uporabo specializiranih orodij ter izvedbo simuliranega napada socialnega inženiringa je bila pridobljena celovita ocena ogroženosti in odpornosti sistema.

Na začetku magistrsko delo predstavi dobre prakse ter sisteme, ki so dandanes nujni v podjetjih za kibernetsko varnost, nato v drugem delu pa smo uporabili primere iz literature tudi v praksi. V empiričnem delu je bil izveden preizkus z orodjema OWASP ZAP in Intruder.io, kjer je bilo ugotovljeno, da aplikacija nima kritičnih ranljivosti, vendar kaže pomanjkljivosti v konfiguraciji varnih povezav in določenih strežniških nastavitev. Poleg tega je bilo s pomočjo nadzorovane simulacije socialnega inženiringa pokazano, da človeški dejavnik predstavlja enega ključnih elementov tveganja, saj so uporabniki kljub navideznemu zaupanju v sistem padli na zavajajočo e-pošto in s tem odprli vrata potencialnemu napadalcu. Rezultati so pokazali, da varnost informacijskih sistemov ne temelji zgolj na tehnologiji, temveč tudi na

varnostni kulturi, ozaveščenosti zaposlenih in zmožnosti organizacije, da se prilagaja razvijajočim se grožnjam.

Kljub določenim omejitvam raziskave, kot so omejen testni vzorec, simulacijski pogoji ter nepopoln dostop do vseh tehničnih plasti aplikacije, je bila raziskava uspešna pri prikazu ključnih ranljivosti in ponujanju konkretnih priporočil za njihovo omilitev. S tem delo ne prispeva le k razumevanju stanja izbrane rešitve, temveč tudi k širšemu razumevanju pomena celostnega pristopa k informacijski varnosti. Magistrsko delo tako ne zaključi samo ene raziskovalne poti, temveč odpira prostor za nadaljnje poglobitve, bodisi v smeri primerjav več različnih sistemov v panogi bodisi v nadgradnji metod testiranja z dodatnimi tehnikami in analizami odzivov uporabnikov skozi daljše časovno obdobje. Varnost ostaja nenehen proces, ne enkratna naloga, zato je ključnega pomena, da organizacije vzpostavijo mehanizme za sprotno zaznavanje, učenje in odzivanje na nove izzive.

SEZNAM KLJUČNE LITERATURE

1. Aboelfotoh, S. F., in Hikal, N. A. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. *JOIV : International Journal on Informatics Visualization*, *3(2),* 157–176. https://doi.org/10.30630/joiv.3.2.239

2. Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, 12(10), 168. https://doi.org/10.3390/fi12100168

3. George, A., George, A. in Baskar, T. (2023). Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats. *Partners Universal International Innovation Journal (PUIIJ)*, 01(04), 155–172. https://doi.org/10.5281/zenodo.8274514

4. Jang-Jaccard, J. in Nepal , S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80(5),* 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

5. Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., in Al-Qassas, R. (2021). A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal: A Global Perspective*, *32(4),* 252–265. https://doi.org/10.1080/19393555.2021.1995537

6. Rains, T. (2023). *Cybersecurity Threats, Malware Trends, and Strategies.* Packt Publishing.

LITERATURA IN VIRI

1. Aboelfotoh, S. F., in Hikal, N. A. (2019). A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises. *JOIV : International Journal on Informatics Visualization*, *3(2)*, 157–176. https://doi.org/10.30630/joiv.3.2.239

2. Alabdan, R. (2020). Phishing Attacks Survey: Types, Vectors, and Technical Approaches. *Future Internet*, *12(10)*, 168. https://doi.org/10.3390/fi12100168

3. Alenezi, M., Alabdulrazzaq, H., Alshaher, A. A. in Alkharang, M. M. (2020). Evolution of Malware Threats and Techniques: A Review. *International Journal of Communication Networks and Information Security (IJCNIS)*, *12(13)*, 326-337. http://dx.doi.org/10.17762/ijcnis.v12i3.4723

4. Alexei, A. in Alexei, A. (2022). THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY. *Journal of Engineering Science*, *29(4),* 72-83. https://doi.org/10.52326/jes.utm.2022.29(4).08

5. Alhamed, M. in Rahman, M. (2023). A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences, 13(12)*, 69-86. https://doi.org/10.3390/app13126986

6. Almuhammadi, S. in Alsaleh, M. (2017). *Information Security Maturity Model for Nist Cyber Security Framework.* 51-62. https://doi.org/10.5121/csit.2017.70305

7. Andronache, A. in Althonayan, A. (2018). Shifting From Information Security Towards A Cybersecurity Paradigm. *ACM International Conference Proceeding Series, 68–79.* https://doi.org/10.1145/3285957.3285971

8. Antariksa, M. D., Angin, M. P. in Widodo, A. P. (2025). COBIT 2019 Framework in IT Governance: A Systematic Literature Review of Implementation Challenges and Benefits Across Various Industry Sectors. *Journal of Renewable Energy, Electrical, and Computer Engineering*, *5(1)*, 99–105. https://doi.org/10.29103/jreece.v5i1.19501

9. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A. in Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics, 12(6)*, 1333. https://doi.org/10.3390/electronics12061333

10. Center for Internet Security. (2021). *CIS Controls Version 8. Center for Internet Security*. https://learn.cisecurity.org/cis-controls-download-v8

11. Dimkov, T., Pieters, W. in Hartel, P. (2010). Two methodologies for physical penetration testing using social engineering. *Proceedings - Annual Computer Security Applications Conference, ACSAC, 399–408. https://doi.org/10.1145/1920261.1920319*

12. Douligeris, C. in Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks, 44(5)*, 643–666. https://doi.org/10.1016/j.comnet.2003.10.003

13. Folorunso, A., Mohammed , V., Wada, I. in Samuel, B. (2024). The impact of ISO security standards on enhancing cybersecurity posture in organizations. *World Journal of Advanced Research and Reviews*. https://doi.org/10.30574/wjarr.2024.24.1.3169

14. George, A., George, A. in Baskar, T. (2023). Digitally Immune Systems: Building Robust Defences in the Age of Cyber Threats. *Partners Universal International Innovation Journal (PUIIJ)*, *01(04)*, 155–172. https://doi.org/10.5281/zenodo.8274514

15. Ghanem, M. in Chen, T. M. (2019). Reinforcement Learning for Efficient Network Penetration Testing. *Information, 11(1)*, 6. https://doi.org/10.3390/info11010006

16. Ghelani, D. (2022). Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. *Authorea Preprints. 3(6), 12–19.* https://doi.org/10.22541/au.166385207.73483369/v1

17. ISO Standards. (2022). *Information security, cybersecurity and privacy protection — Information security controls*. https://itref.ir/uploads/editor/d3d149.pdf

18. ISO Standards. (2022). *Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* https://itref.ir/uploads/editor/2ef522.pdf

19. Jain, M., Sinha, A., Agrawal, A. in Yadav, N. (2022). Cyber security: Current threats, challenges, and prevention methods. *International Conference on Advances in Computing, Communication and Materials, ICACCM.* https://doi.org/10.1109/icaccm56405.2022.10009154

20. Jang-Jaccard, J. in Nepal , S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, *80(5)*, 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

21. Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., in Stulz, R. M. (2018). What is the Impact of Successful Cyberattacks on Target Firms? *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3135514

22. Kaur, J. in Ramkumar, K. R. (2022). The recent trends in cyber security: A review. Journal of King Saud University. *Computer and Information Sciences, 34(8)*, 5766–5781. https://doi.org/10.1016/J.JKSUCI.2021.01.018

23. KeepNet. (2025, 10. februar). 6 Human Risk Indicators That Could Compromise Your Cybersecurity. [objava na blogu]. Pridobljeno 22. julija 2025 s https://keepnetlabs.com/blog/6-human-risk-indicators-that-could-compromise-your-cybersecurity

24. Mahmood, A. M. in Avcı, İ. (2024). Cybersecurity Defence Mechanism Against DDoS Attack with Explainability. *Mesopotamian Journal of CyberSecurity*, *4(3)*, 278–290. https://doi.org/10.58496/mjcs/2024/027

25. Nagendran, K., Adithyan, A., Chethana, R., Camillus, P. in Varshini, B. S. (2019). Web Application Penetration Testing. *International Journal of Innovative Technology and Exploring Engineering*, *8(10)*, 1029–1035. https://doi.org/10.35940/ijitee.j9173.0881019

26. Nasereddin, M., ALKhamaiseh, A., Qasaimeh, M., in Al-Qassas, R. (2021). A systematic review of detection and prevention techniques of SQL injection attacks. *Information Security Journal: A Global Perspective*, *32(4)*, 252–265. https://doi.org/10.1080/19393555.2021.1995537

27. O'Kane, P., Sezer, S. in Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7(5)*, 321–327. https://doi.org/10.1049/iet-net.2017.0207

28. Pacific certifications. (2025, 21. maj). *ISO/IEC 27018:2019 - Protection of Personal Data in the Cloud*. [objava na blogu]. Pridobljeno 16. julij 2025 s https://blog.pacificcert.com/iso-iec-27018-2019-protection-of-personal-data-in-the-cloud/

29. Patel, D. (2024). Cyber security: Study on Attack, Threat, Vulnerability. *International Journal for Research in Applied Science and Engineering Technology*. *2(2)*, 1074–1078. https://doi.org/10.22214/ijraset.2024.58472

30. Paule, L. G. (2023). *ISO/IEC 27001 - The international standard for information security. Digital Skills & Jobs Platform*. https://digital-skills-jobs.europa.eu/en/inspiration/resources/isoiec-27001-international-standard-information-security

31. Rains, T. (2023). *Cybersecurity Threats, Malware Trends, and Strategies.* Packt Publishing.

32. Rizvi, M. (2023). Enhancing cybersecurity: The power of artificial intelligence in threat detection and prevention. *International Journal of Advanced Engineering Research and Science*, *10(5)*, 055–060. https://doi.org/10.22161/ijaers.105.8

33. Samociuk, D. (2023, 21. september). *Security architecture 101: understanding the basics*. [objava na blogu]. Pridobljeno 5. julija 2025 s https://www.future-processing.com/blog/security-architecture-101-understanding-the-basics/

34. Singh, H., in Singh, J. (2017). Penetration Testing in Wireless Networks. *International Journal of Advanced Research in Computer Science, 8(5),* 2213–2216 https://doi.org/10.26483/IJARCS.V8I5.4012

35. Solms, R. v. in Niekerk, J. v. (2013). From information security to cyber security. Computers & *Security, 38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

36. Spherical Insights. (2023). *Global Cybersecurity Market.* https://www.sphericalinsights.com/reports/cybersecurity-market

37. Standardi.si. *Učinkovita in varna praksa upravljanja z informacijami*. https://standardi.si/iso-27001/

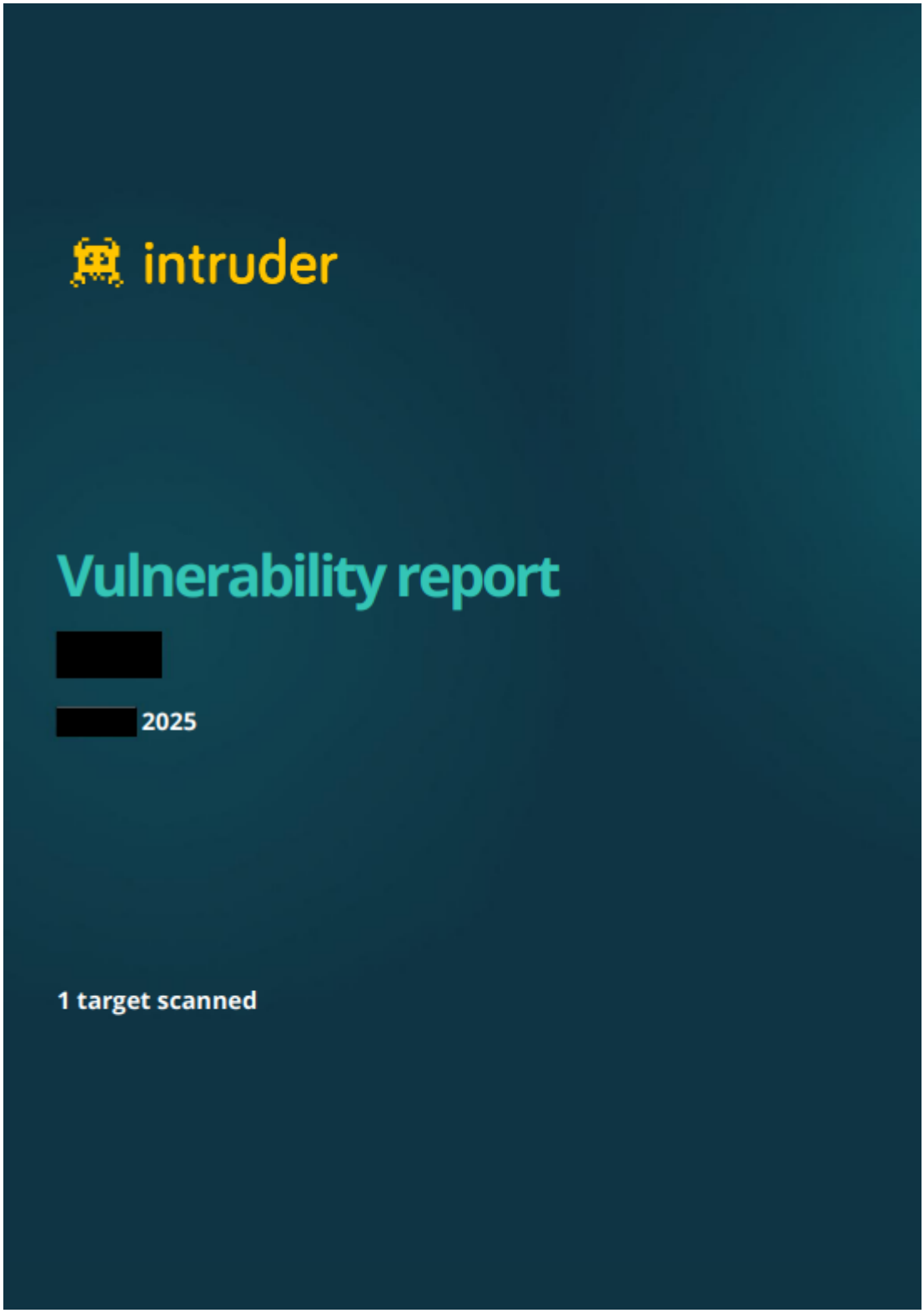
38. Starkova, O., in Nazarov, D. (2025). Integration of ISO 27001:2022 with other information security standards. *Materials of the International scientific-practical conference "Modern information systems and technologies in the digital society": abstracts of reports* (str. 77).

39. Syafrizal, M., Selamat, S. R. in Zakaria, N. A. (2020). Analysis of Cybersecurity Standard and Framework Components. *International Journal of Communication Networks and Information Security (IJCNIS)*, *12(3), 417–432.* https://doi.org/10.17762/ijcnis.v12i3.4817

40. Usd more security. (2025, 20 februar). *Top 3 Vulnerabilities in Pentests of Workstations and Company Notebooks*. More Security. [objava na blogu]. Pridobljeno 22. julija 2025 s https://www.usd.de/en/top-3-vulnerabilities-workstation-pentests/

PRILOGA

Priloga 1: Poročilo OWASP ZAP testa



Executive summary

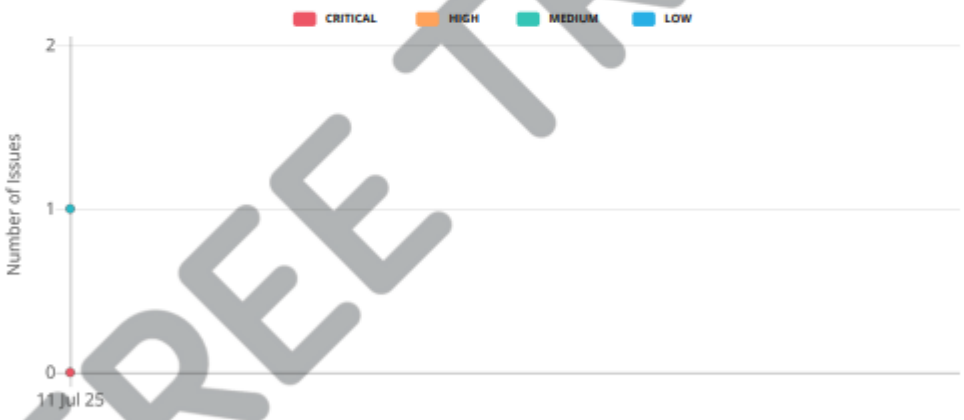
Threat Level

Medium

Target	Issues
1	2
Critical	High
0	0
Medium	Low
1	1

Medium severity issues are unlikely to lead to a breach, as they generally require a level of skill or resource available to only the most highly capable attackers, such as nation states or organised cyber crime groups. Medium severity issues should be fixed if the business faces a significant threat from being targeted by such skilled attackers, ideally within 90 days.

Exposure over time



FREE TRIAL

What we checked

Total checks
71,773

The types of areas we cover when reviewing your targets and their accessible web pages:

Vulnerable software & hardware

- Web servers, e.g. Apache, Nginx
- Mail servers, e.g. Exim
- Development software, e.g. PHP
- Network monitoring software, e.g. Zabbix, Nagios
- Networking systems, e.g. Cisco ASA
- Content management systems, e.g. Drupal, Wordpress
- Other well-known weaknesses, e.g. 'Log4Shell' and 'Shellshock'

Web Application Vulnerabilities

- Checks for multiple OWASP Top Ten issues
- SQL injection
- Cross-site scripting (XSS)
- XML external entity (XXE) injection
- Local/remote file inclusion
- Web server misconfigurations
- Directory/path traversal, directory listing & unintentionally exposed content

Attack Surface Reduction

Our service is designed to help you reduce your attack surface and identify systems and software which do not need to be exposed to the Internet, such as:

- Publicly exposed databases
- Administrative interfaces
- Sensitive services, e.g. SMB
- Network monitoring software

Information Leakage

Checks for information which your systems are reporting to end-users which should remain private. This information includes data which could be used to assist in the mounting of further attacks, such as:

- Local directory path information
- Internal IP Addresses

FREE TRIAL

What we checked

Encryption weaknesses

Weaknesses in SSL/TLS implementations, such as:

- 'Heartbleed', 'CRIME', 'BEAST' and 'ROBOT'
- Weak encryption ciphers & protocols
- SSL certificate misconfigurations
- Unencrypted services such as FTP

Common mistakes & misconfigurations

- VPN configuration weaknesses
- Exposed SVN/git repositories
- Unsupported operating systems
- Open mail relays
- DNS servers allowing zone transfer

FREE TRIAL

Cloud plan

As a Cloud plan customer, you also have access to:

Emerging threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organizations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check.

Internal checks

Your internal systems can also be hacked with a little extra effort, e.g. by an email or web page link that exploits known unpatched software or an employee's device. Our agent-based scanner can be installed on each machine you want to protect.

REE TRIAL

Issue summary

Untrusted TLS Certificate

Medium 2 occurrences

Strict Transport Security HTTP Header Not Set

Low 1 occurrence

Severity Threshold

DEE TRIAL

Issues

Untrusted TLS Certificate

Medium 2 occurrences

Description

The TLS certificate installed on the host is not valid/trusted. This means that a user will be presented with a certificate error when connecting to the service and will be unable to verify the authenticity of the connection.
An attacker in a position to intercept network traffic (e.g. over a shared wireless network), could use this weakness to carry out a Man-in-the-Middle attack against the service, which would allow them to gain access to any data transferred between the user and the server.

Remediation Advice

Ensure the certificate installed on the host:
Is signed by a trusted Certification Authority (CA).
Has a "commonName", which matches the host name.
Has not expired.
Has a validity period of less than 825 days
There are a number of other reasons why a certificate may not be trusted. Please see the scanner output for further information.

Occurrences	First seen
www.[redacted] 443 (tcp)	[redacted]025 03:00:58
www[redacted] : 8172 (tcp)	[redacted] 2025 03:00:58

F TRIAL

Issues

Strict Transport Security HTTP Header Not Set

Low 1 occurrence

Description

The server does not set a "Strict Transport Security" HTTP header in its response.

The HTTP Strict Transport Security policy defines a timeframe within which a browser must connect to the web server via HTTPS. The header adds additional protection against MitM (Man-in-the-Middle) attacks by instructing the user's web browser not to connect to the server unless it is done so over HTTPS with a valid certificate. This helps prevent an attacker in a MitM position from tricking the user into connecting to an attacker controlled server which is impersonating the targeted site.

Remediation Advice

Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows:

Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]

The parameter max-age gives the time frame for requirement of HTTPS in seconds and is recommended to be set for at least several months, with 90 days being a minimum (ie. 7776000 seconds). The flag includeSubDomains defines that the policy should also apply for sub domains of the sender of the response.

For example, the following lines can be added to an Apache configuration file:

Header set Strict-Transport-Security "max-age=7776000"

Header append Strict-Transport-Security includeSubDomains

Occurrences	First seen
www.[redacted] : 8172 (tcp)	[redacted] 2025 03:00:58

TRIAL

Scan info

Target included in this scan

www[redacted]

Scan timings

This report includes last known scan data for your selected targets.

FREE TRIAL

About Intruder

Company

Intruder Systems Ltd is an independent security advisory company, specialising in providing continuous security monitoring for internet-facing web applications and infrastructure.

Security team

Our consultants have delivered work for government agencies, international financial institutions, and global retail giants.

PREF
IAL

Credentials

CREST

Intruder is a member of CREST

SOC 2

Monitored by Drata for SOC 2 compliance

VA

Intruder is a CREST accredited Vulnerability Assessment service

National Cyber Security Centre CSP

Intruder is a member of the Cyber-security Information Sharing Partnership

CYBER ESSENTIALS

Intruder is Cyber Essentials certified

GCHQ Cyber Accelerator Alumni

Compliance

Our reports are ISO 27001 and SOC 2 compliance ready.

FREE TRIAL


contact@intruder.io
intruder
© 2025 Intruder Systems Ltd. Registered in England, VAT Number GB228985360.
Intruder is a trading name of Intruder Systems Ltd., Company Registration Number 09529503.