POROČILO ZUNANJEGA VARNOSTNEGA KIBERNETSKEGA PREGLEDA

14. januar 2026

Organizacija: Ramar d.o.o.

Vrsta pregleda: zunanji varnostni pregled

Datum pregleda: 10. januar 2026 - 14. januar 2026

Datum priprave poročila: 14. januar 2026

KAZALO

SLEDLJIVOST SPREMEMB IN POŠILJANJA DOKUMENTA

Različica dokumenta

Verzija	Datum	Avtor	Opis
0.1	10. januar 2026	Tinkara Grum	Prva različica dokumenta
0.2	10. januar 2026	Tinkara Grum	Izvedba testov
0.3	12. januar 2026	Tinkara Grum	Izvedba analize
0.9	13. januar 2026	Tinkara Grum	Priprava osnutka poročila
1.0	14. januar 2026	Tinkara Grum	Priprava poročila

Pregled sledljivosti pošiljanja dokumenta

Verzija	Datum	Pošiljatelj	Prejemnik	Metoda
1.0	14. januar 2026	Tinkara Grum	Ramar d.o.o.	E-pošta

1. POVZETEK

Zapišite kratek povzetek o tem kakšen je namen izvedbe kibernetskega testa ter predstavite osnovne elemente.

2. CILJI

Glavni cilj projektne naloge je izvesti zunanji varnostni kibernetski pregled podjetja Ramar d.o.o. ter na podlagi ugotovitev oceniti stopnjo izpostavljenosti sistema varnostnim tveganjem. Pregled je usmerjen v identifikacijo morebitnih pomanjkljivosti, ki bi jih lahko zunanji napadalci izkoristili brez predhodnega dostopa do notranjega omrežja.

Posamezni cilji varnostnega pregleda so:

- identificirati ključna informacijska sredstva, ki so javno dostopna ali posredno izpostavljena prek spletne infrastrukture;
- prepoznati potencialne grožnje, ki vplivajo na zaupnost, celovitost in razpoložljivost informacijskega sistema;
- ugotoviti tehnične in konfiguracijske ranljivosti na ravni domene, strežniške infrastrukture in spletne aplikacije;
- izvesti osnovne varnostne teste z uporabo javno dostopnih orodij v skladu z dobrimi praksami informacijske varnosti;
- analizirati rezultate testiranj ter oceniti stopnjo tveganja posameznih ugotovitev;
- pripraviti priporočila za izboljšanje varnostnega stanja sistema, ki vključujejo tehnične in organizacijske ukrepe.

3. SODELUJOČI

Ime in priimek	Funkcija	Podjetje
Tinkara Grum	Izvajalka zunanjega varnostnega kibernetskega pregleda	CGT d.o.o.

4. IZJAVA O AVTORSTVU IN POOBLASTILO O VARNOSTNEM TESTIRANJU

IZJAVLJAMO:

1. Da imamo vse pravice za izvajanje varnostnega testiranja aplikacij ali sistema, ki bodo vključene v test,
2. Da imamo vsa pooblastila in dovoljenja za upravljanje in izvajanje del nad aplikacijo ali sistemom,
3. Da imamo vsa dovoljenja za uporabo podatkov in avtorskih del, ki so del aplikacije ali sistema,
4. Da pooblaščamo podjetje CGT d.o.o., da v skladu z etičnimi načeli izvaja dogovorjeno varnostno testiranje za našo aplikacijo,
5. Dovoljujemo obdelavo podatkov, ki so dostopni ali pridobljeni v sklopu izvajanja penetracijskega testiranja spletne aplikacije.

Datum: 15.12.2025

Podpis:

5. METODOLOGIJA

Varnostni pregled je bil izveden po strukturirani metodologiji zunanjega varnostnega pregleda, ki temelji na dobrih praksah informacijske varnosti in splošno uveljavljenih okvirjih, kot je OWASP. Metodologija je prilagojena obsegu projektne naloge ter omejena izključno na javno dostopne komponente sistema.

Pregled je potekal po naslednjih zaporednih korakih:

- predhodna opredelitev obsega pregleda in ciljev testiranja;
- zbiranje javno dostopnih informacij o domeni in infrastrukturi (OSINT);
- identifikacija informacijskih sredstev, ki so izpostavljena zunanjemu okolju;
- analiza potencialnih groženj in možnih scenarijev zlorab;
- izvajanje osnovnih varnostnih testov z uporabo izbranih orodij (npr. DNS, SSL/TLS, omrežna vrata);
- analiza pridobljenih rezultatov in identifikacija ranljivosti;
- ocena tveganj na podlagi verjetnosti izkoriščanja in vpliva na sistem;
- priprava poročila z ugotovitvami in priporočili za izboljšanje varnosti.

Priporočila in poročilo

Na podlagi stopnje tveganja bomo določili ukrepe, potrebne za ublažitev tveganja. Nekaj splošnih smernic za vsako stopnjo tveganja predstavljajo tveganja:

- **Visoko tveganje** - ki predstavlja resno grožnjo sistemu in ga je mogoče relativno enostavno izkoristiti. Za to stopnjo tveganja je treba čim prej razviti in uvesti načrt korektivnih ukrepov.
- **Srednje tveganje** - z zmernim vplivom ali manjšo verjetnostjo izkoriščanja. Načrt korektivnih ukrepov je treba razviti in izvesti v razumnem časovnem okviru.
- **Nizko tveganje** - z majhnim vplivom ali nizko verjetnostjo zlorabe. Ekipa se mora odločiti, ali bo tveganje sprejela ali pa izvedla dodatne korektivne ukrepe.

6. ČASOVNICA

Izvajanje testa se je izvajalo v naslednjih fazah.

Faza	Datum izvedbe
Identifikacija IT virov in sredstev	10. januar 2026
Ugotovitev groženj	11. januar 2026
Identifikacija ranljivosti	12. januar 2026
Identifikacija nadzora	13. januar 2026
Priporočila in poročilo	14. januar 2026

7. IDENTIFIKACIJA SREDSTEV INFORMACIJSKE TEHNOLOGIJE

Namen identifikacije sredstev je nadaljnji pregled in izvedba testov ter identifikacija s sredstvi povezanimi tveganji. V organizaciji identificiramo različna sredstva, ki jih navajamo spodaj ter prilagamo identificirana tveganja.

Sredstva in viri

- Programska oprema (spletna trgovina, e-poštni sistem, administrativna orodja)
- Strojna oprema (strežniška infrastruktura pri ponudniku gostovanja, delovne postaje, blagajniška oprema)
- Podatki (osebni podatki kupcev, podatki o naročilih, poslovni in kontaktni podatki)
- Vmesniki (spletni obrazci, administrativni vmesniki, integracije s tretjimi sistemi)
- Uporabniki (kupci spletne trgovine)
- Zaposleni (prodajno in administrativno osebje)
- Arhitektura informacijske varnosti
- Omrežje in komunikacijske povezave
- Varnostne politike in postopki IT
- Pretok informacij znotraj in zunaj organizacije
- Tehnični varnostni nadzor
- Varnost fizičnega in IT okolja

Sredstvo ali vir	Tip pregleda	Identifikacija	Tveganje
Programska oprema	IT revizija	Posodobitve, varnostne nastavitve, ranljivosti	**Visoko**
Strojna oprema	IT revizija	Razpoložljivost in zaščita infrastrukture	**Srednje**
Podatki	IT revizija	Obdelava in hramba osebnih podatkov	**Visoko**

Uporabniki	IT revizija	Nepravilna uporaba ali zloraba dostopov	**Srednje**
Zaposleni	IT revizija	Človeški faktor in napake pri delu	**Srednje**
Omrežje	IT revizija	Izpostavljenost omrežnih storitev	**Srednje**
Arhitektura IT	IT revizija	Centralizacija in odvisnost od izvajalcev	**Srednje**

Mnenje in priporočilo

Na podlagi identifikacije sredstev informacijske tehnologije in ocene njihovih tveganj ugotavljamo, da poslovanje podjetja Ramar d.o.o. zaradi narave dejavnosti (spletna trgovina) spada v kategorijo zmerno do visokega tveganja na področju informacijske varnosti.

Identificirali smo dve kategoriji sredstev z visokim inherentnim tveganjem:

1. Podatki - zaradi obveznosti GDPR in obdelave osebnih podatkov strank
2. Programska oprema - predvsem spletna trgovina kot primarni poslovni kanal

Zaposleni, omrežje in arhitektura IT so ocenjeni kot srednje tveganje, kar je značilno za manjša podjetja, ki se zanašajo na zunanje IT izvajalce.

V tej fazi pregleda priporočamo:
• Jasno opredelitev odgovornosti za obdelavo osebnih podatkov,
• Redno vzdrževanje in posodabljanje programske opreme spletne trgovine,
• Ureditev osnovnih varnostnih pravil za zaposlene.

Splošna ocena identifikacijske faze je srednje tvegana, kar pomeni, da so nadaljnje varnostne analize in testiranja potrebne in upravičene glede na naravo poslovanja.

8. IDENTIFIKACIJA IT GROŽENJ

Splošne grožnje za informacijske sisteme in podatke vključujejo okvaro strojne in programske opreme - na primer izgubo električne energije ali poškodbe podatkov. zlonamerna programska oprema - zlonamerna programska oprema, namenjena motenju delovanja računalnika. virusi - računalniška koda, ki se lahko kopira in širi iz enega računalnika v drugega, kar pogosto moti delovanje računalnika.

Grožnja je vse, kar bi lahko škodilo vaši organizaciji. Poleg hekerjev in zlonamerne programske opreme, obstaja še veliko drugih vrst groženj.

Grožnja	Identifikacija	Tveganje
Naravna katastrofa	Analiza	**Nizko**
Odpoved opreme	Analiza	**Srednje**
Zlonamerno delovanje	Pregled	**Visoko**
Motnje storitev	Analiza	**Srednje**
Vdori	Testiranje	**Visoko**
Zloraba podatkov	Pregled	**Visoko**

Mnenje in priporočilo
Na podlagi identifikacije IT groženj ugotavljamo, da podjetje Ramar d.o.o. deluje v okolju z zmernim do visokim kibernetskim tveganjem, kar je posledica spletne prisotnosti in obdelave osebnih podatkov. Tri grožnje so ocenjene kot visoko tvegane: 1. Zlonamerno delovanje - zaradi potenciala za motnje v delovanju spletne trgovine 2. Vdori v informacijske sisteme - zaradi dostopa do podatkov strank 3. Zloraba podatkov - zaradi regulatornih in uglednih posledic Grožnji odpoved opreme in motnje storitev sta ocenjeni kot srednje tveganje, saj lahko vplivata na razpoložljivost spletne trgovine. Naravne katastrofe so ocenjene kot nizko tveganje zaradi zunanjega gostovanja.

V fazi identifikacije priporočamo:
• Osredotočenost na zaščito pred zlonamerno programsko opremo in vdori,
• Redno varnostno kopiranje podatkov,
• Uvedbo osnovnih nadzorov za preprečevanje zlorabe podatkov.

Splošna ocena področja identifikacije IT groženj je srednje do visoko tvegana, kar utemeljuje nadaljnjo, podrobnejšo analizo tveganj.

9. IDENTIFIKACIJA IT RANLJIVOSTI

Grožnja in ranljivost nista eno in isto. Grožnja je oseba ali dogodek, ki lahko negativno vpliva na dragocen vir. Ranljivost je tista kakovost vira ali njegovega okolja, ki omogoča uresničitev grožnje. Oboroženi ropar banke je primer grožnje. Bančni blagajnik je primer dragocenega vira, ki je lahko ranljiv med ropom banke. Neprebojno steklo med roparjem in blagajnikom zavrne roparju možnost, da bi ustrelil blagajnika. Nevarnost ostaja prisotna, vendar je eden od njenih škodljivih učinkov (strel iz pištole) omiljen z zaščitnim mehanizmom (steklo).

Ranljivost	Identifikacija	Tveganje
Zunanji faktor	Analiza	**Srednje**
Zastarela oprema	Analiza	**Srednje**
Nezaželena programska oprema	Pregled	**Srednje**
Preobremenitev sistema	Pregled	**Nizko**
Neprimerna zaščita	Testiranje	**Visoko**
Osebni podatki	Pregled	**Visoko**

Mnenje in priporočilo
Na podlagi identifikacije IT ranljivosti ugotavljamo, da so ranljivosti v informacijskem okolju podjetja Ramar d.o.o. zmerno izražene, z nekaj kritičnimi področji, ki zahtevajo pozornost. Dve ranljivosti sta ocenjeni kot visoko tvegani: 1. Neprimerna zaščita - potencialna odsotnost ustreznih tehničnih zaščit 2. Osebni podatki - tveganje nedoslednega upravljanja z občutljivimi podatki Ranljivosti zunanji faktor, zastarela oprema in nezaželena programska oprema so ocenjene kot srednje tveganje, kar je tipično za podjetja z zunanjimi IT izvajalci. Preobremenitev sistema je ocenjena kot nizko tveganje. V fazi identifikacije ranljivosti priporočamo: • Oceno obstoječih mehanizmov zaščite informacijskih sistemov, • Pregled upravljanja osebnih podatkov v luči GDPR zahtev, • Redno posodabljanje programske in strojne opreme. Splošna ocena področja identifikacije IT ranljivosti je srednje tvegana, kar pomeni, da so nadaljnje faze pregleda potrebne za celovito obravnavo tveganj.

10. IDENTIFIKACIJA IT NADZORA

Namen nadzora je zmanjšanje ali odprava verjetnosti, da se bo določena nevarnost izkoristila ranljivost. Tehnični nadzor vključuje šifriranje, mehanizme za odkrivanje vdorov ter rešitve za identifikacijo in preverjanje pristnosti. Netehnični nadzor vključuje varnostne politike, upravne ukrepe ter fizične in okoljske mehanizme.

Nadzor	Identifikacija	Tveganje
Širfiranje in uporaba SSL	Pregled in testiranje	**Srednje**
Mehanizmi za zaščito	Pregled in testiranje	**Visoko**
Varnost osebnih podatkov	Pregled in analiza	**Visoko**
Varnost IS	Pregled in testiranje	**Srednje**
Uporaba varnostne politike	Analiza	**Visoko**

Mnenje in priporočilo
Na podlagi identifikacije IT nadzorov ugotavljamo, da podjetje Ramar d.o.o. potrebuje okrepitev nadzornih mehanizmov na nekaterih kritičnih področjih, kar je značilno za manjša podjetja brez notranjega IT oddelka. Tri nadzorna področja so ocenjena kot visoko tvegana: 1. Mehanizmi za zaščito - potrebna ocena in morebitna okrepitev 2. Varnost osebnih podatkov - zaradi zahtev GDPR in zaupanja strank 3. Uporaba varnostne politike - verjetno pomanjkanje formaliziranih pravil Področji šifriranja in varnosti informacijskih sistemov sta ocenjeni kot srednje tveganje, saj je osnovna zaščita verjetno prisotna, vendar zahteva redno vzdrževanje. V fazi identifikacije nadzora priporočamo: • Izdelavo osnovne varnostne politike in postopkov, • Oceno in morebitno okrepitev mehanizmov za zaščito, • Ureditev nadzora nad obdelavo osebnih podatkov, • Redno izobraževanje zaposlenih o varnostnih praksah. Splošna ocena področja identifikacije IT nadzora je srednje do visoko tvegana, kar nakazuje potrebo po dodatni pozornosti in morebitni krepitvi nadzornih ukrepov.

11. POROČILO O VARNOSTI INFORMACIJSKE TEHNOLOGIJE

Na podlagi stopnje tveganja določimo ukrepe, potrebne za ublažitev tveganja. Tu je nekaj splošnih smernic za vsako stopnjo tveganja:

- **Visoka** - Čim prej je treba razviti načrt korektivnih ukrepov.
- **Srednja** - Načrt korektivnih ukrepov je treba razviti v razumnem roku.
- **Nizka** - Ekipa se mora odločiti, ali bo sprejela tveganje ali izvedla korektivne ukrepe.

Med ocenjevanjem kontrol za ublažitev vsakega tveganja upoštevamo:

- Organizacijske politike
- Analiza stroškov in koristi

- Operativni vpliv
- Izvedljivost
- Veljavni predpisi
- Splošna učinkovitost priporočenih kontrol ter Varnost in zanesljivost

Grožnja	Ranljivost	Vir	Vpliv	Verjetnost	Tveganje	Predlog nadzora
Naravna katastrofa	Zunanji faktor	Strojna oprema Podatki	Izguba dostopa do spletne trgovine (ur/dni)	Nizka	Nizko	Preverjanje SLA pogodbe z gostiteljem, redno varnostno kopiranje podatkov na ločeno lokacijo
Odpoved opreme	Zastarela oprema	Programska oprema Strojna oprema Podatki	Zaustavite v spletne trgovine, izguba prodaje	Srednja	Srednje	Redno vzdrževanje in posodabljanje, pregled logov opreme, dogovor o hitri podpori z izvajalcem
Zlonamerno delovanje	Nezaželena programska oprema	Programska oprema Podatki	Šifriranje/izguba podatkov, izpad sistema, zaustavite v prodaje	Visoka	Visoko	Namestitev antivirusne zaščite na vse naprave, redne posodobitve, izobraževanje zaposlenih, segmentacija omrežja
Motnje	Preobremenitev sistema	Omrežje Podatki	Počasen/ nedostopen spletni portal, izguba kupcev	Nizka	Nizko	Monitoring obremenitve sistema, plan za povečanje zmogljivosti ob rasti
Vdori	Neprimerna zaščita	Podatki Arhitektura	Kraja podatkov strank, dostop do računov, finančna škoda	Srednja	Visoko	Uvedba dvofaktorske avtentikacije (2FA) za admine, redna zamenjava gesel, revizija dostopov
Zloraba podatkov	Osebni podatki	Podatki Uporabniki	Kazni GDPR (do 4% prometa), izguba zaupanja strank, pravni postopki	Srednja	Visoko	Ureditev GDPR registra, politika ravnanja s podatki, omejitev dostopov, šifriranje občutljivih podatkov

12. PRILOGE: POROČILA TESTIRANJA S POMOČJO PROGRAMSKIH ORODIJ

Pregled zaupnih podatkov

Puščanje sledi zaupnih in osebnih podatkov lahko predstavljajo ranljivost posameznih segmentov uporabe IT sistemov. Grožnjo predstavljajo sledi osebnih podatkov predstavljajo

Metodologija

- Pridobivanje podatkov iz spletne strani
- Varnostni pregled možnih vdorov na podlagi pridobljenih podatkov
- Priprava priporočila

Iz spletne strani www.ramartrgovina.com pridobimo naslednje osebne podatke:

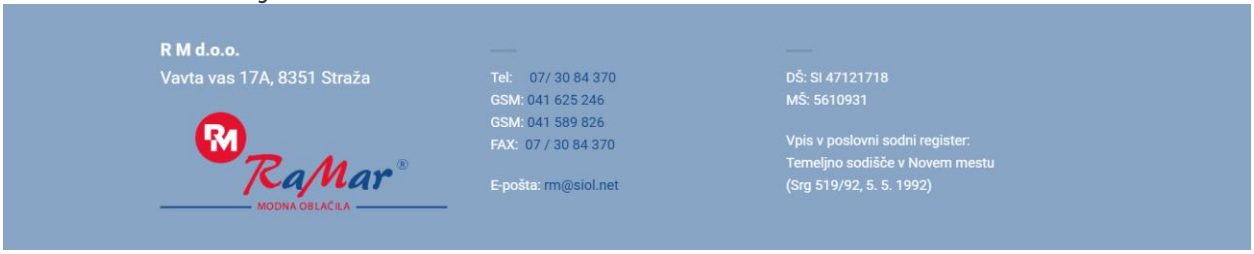
Kontakti zaposlenih

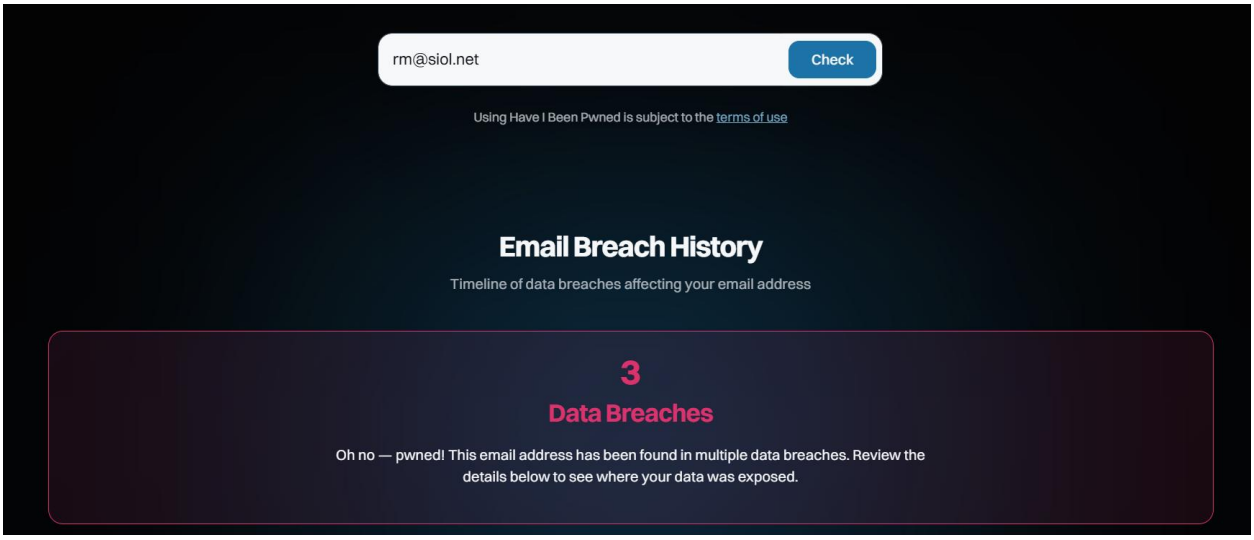
- 07/ 30 84 370
- 041 625 246 - Marjan Ravbar
- 041 589 826 - Irena Ravbar
- rm@siol.net

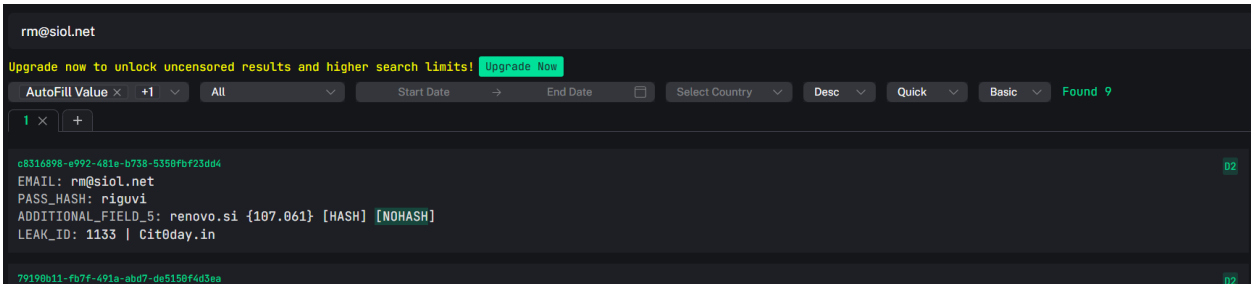
Poročilo testiranja

V poročilu testiranja vključite zaslonske slike s katerimi dokazujete pridobljene podatke.

Rezultat testiranja







Mnenje in priporočilo

Na podlagi pregleda zaupnih podatkov ugotavljamo, da je poslovni e-poštni račun podjetja izpostavljen v več znanih uhajanjih podatkov, kar vključuje tudi izgubo gesel. To pomeni, da so poverilnice potencialno v rokah napadalcev. Javno dostopne osebne telefonske številke lastnikov povečujejo tveganje za ciljne prevare prek telefona ali spleta.

Posledice te izpostavljenosti so resne. Napadalci bi lahko zlorabili e-poštni račun za dostop do poslovnih informacij, ponaredili identiteto za prevare (kot so lažna naročila ali spremembe plačil) ali izvedli napade na zaposlene. To bi lahko povzročilo finančne izgube, kršitve zasebnosti strank in resno škodilo ugledu podjetja.

Ukrepati je treba takoj. Najprej je nujno zamenjati geslo ogroženega e-poštnega računa z zelo močnim in edinstvenim ter takoj vključiti dvofaktorsko avtentikacijo. V kratkem roku je smiselno uvesti ločene, poslovne kontaktne podatke za javno uporabo in izobraziti zaposlene o novih varnostnih tveganjih. Dolgoročno priporočamo vzpostavitev rednega monitoringa in jasnejših pravil za ravnanje s podatki.

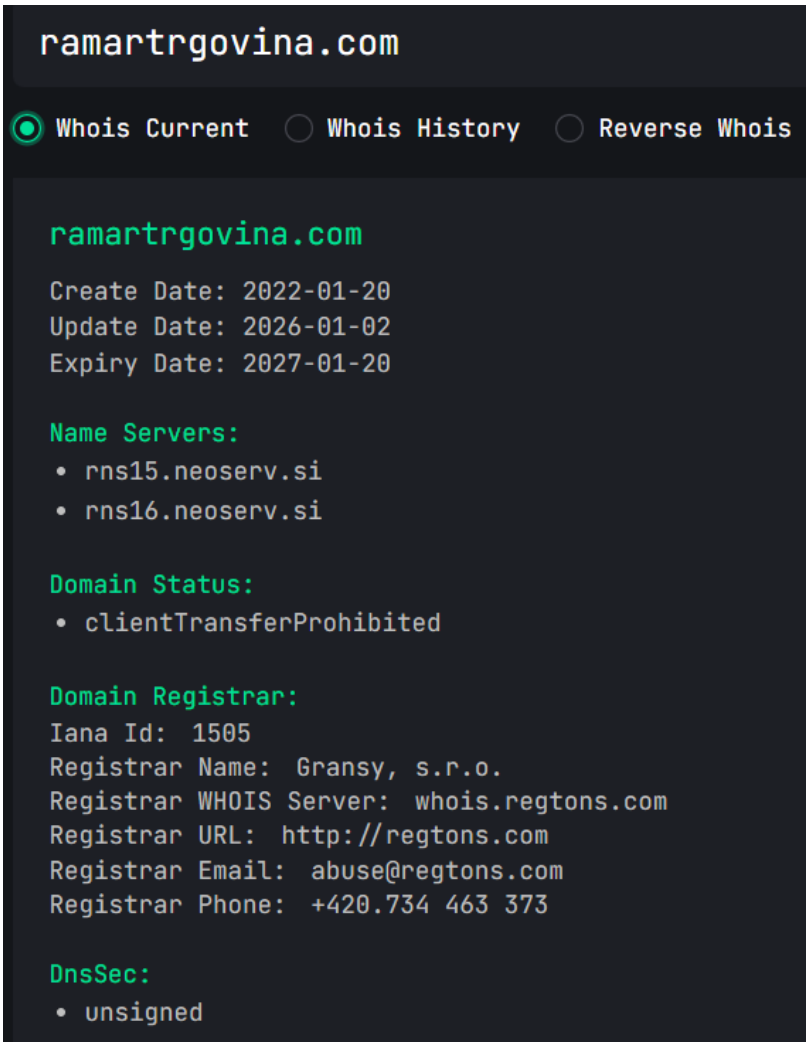
Pregled DNS zapisov

Metodologija

- Pridobivanje podatkov od DNS zapisih
- Varnostni pregled možnih vdorov na podlagi pridobljenih podatkov
- Priprava priporočila

Poročilo testiranja

WHOIS pozivedba po domeni



DNS zapisi na domeni

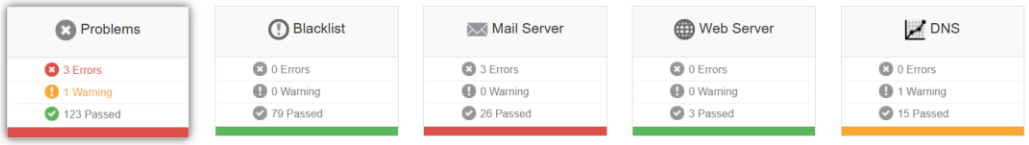
DNS Records for ramartrgovina.com

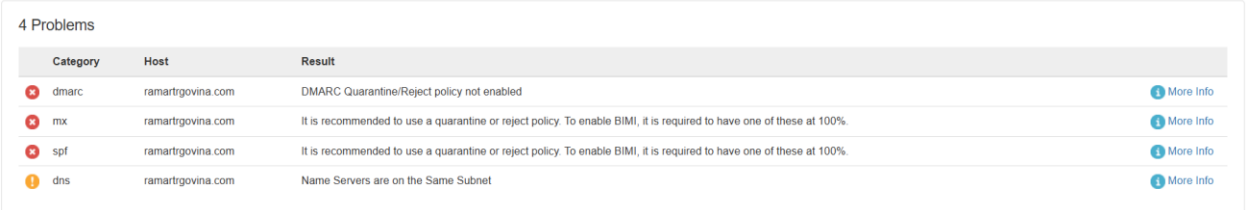
Hostname	Type	TTL	Priority	Content
ramartrgovina.com	SOA	86400		rns15.neoserv.si cpanel.neoserv.si 2026011300 3600 7200 1209600 86400
ramartrgovina.com	NS	0		rns16.neoserv.si
ramartrgovina.com	NS	0		rns15.neoserv.si
ramartrgovina.com	MX	0		mail.ramartrgovina.com
ramartrgovina.com	A	0		152.89.234.125
www.ramartrgovina.com	SOA	86400		rns15.neoserv.si cpanel.neoserv.si 2026011300 3600 7200 1209600 86400
www.ramartrgovina.com	MX	0		mail.ramartrgovina.com
www.ramartrgovina.com	A	0		152.89.234.125
www.ramartrgovina.com	NS	0		rns15.neoserv.si
www.ramartrgovina.com	NS	0		rns16.neoserv.si
www.ramartrgovina.com	CNAME	0		ramartrgovina.com

Pridobljeni IP naslovi

- 152.89.234.125

MAIL Test





Mnenje in priporočilo
Pregled DNS konfiguracije razkrja več varnostnih pomanjkljivosti, ki jih ocenjujemo kot srednje tveganje. Najbolj kritično je odsotnost DMARC zaščite, kar pomeni, da lahko napadalci relativno enostavno pošiljajo lažno e-pošto, ki se pretvarja, da prihaja iz vašega podjetja. Poleg tega so vsi DNS strežniki na istem omrežju, kar poveča tveganje za celoten izpad, če pride do težav pri tem ponudniku. DNSSEC tudi ni omogočen, kar odpira možnost za napade, kjer bi se stranke lahko preusmerile na lažno spletno stran. Posledice teh pomanjkljivosti so resne. Brez DMARC bi lahko stranke prejele prevarantska e-poštna sporočila, ki bi jih napeljevala k izdaji osebnih podatkov ali plačilu na napačne račune, kar bi močno škodilo ugledu podjetja. Izpad DNS strežnikov bi povzročil, da spletna stran ne bi bila dostopna, kar bi zaustavilo celotno spletno prodajo. Pomanjkanje DNSSEC zaščite pa bi omogočilo napadalcem, da stranke preusmerijo na ponarejeno kopijo vaše spletne trgovine. Takoj je treba vzpostaviti DMARC politiko, da se prepreči zloraba domene za phishing. V kratkem roku je potrebno urediti DNS konfiguracijo, odstraniti odvečne zapise in omogočiti DNSSEC zaščito. Dolgoročno pa je smiselno razmisliti o dodajanju DNS strežnikov pri drugem ponudniku za večjo odpornost in vzpostaviti redno spremljanje teh nastavitev.

Pregled odprtih vrat

Metodologija

- Pridobivanje podatkov o odprtih vratih na IP naslovih
- Varnostni pregled možnih vdorov na podlagi pridobljenih podatkov
- Priprava priporočila

Poročilo testiranja

Izpišite podatke o odprtih vratih na zaznanih IP naslovih.

Rezultat testiranja

Uporabite in izpišite rezultat nmap testa.

Odkrita odprta vrata

Vrata	IP	Protokol	Opomba
21	152.89.234.125	tcp/ftp	Prenos datotek – povečano varnostno tveganje
26	152.89.234.125	tcp/rsftp	Alternativna FTP storitev
53	152.89.234.125	tcp/dns	DNS storitev
80	152.89.234.125	tcp/http	Spletna storitev (nešifriran dostop)
110	152.89.234.125	tcp/pop3	E-poštna storitev (nešifriran prenos)
143	152.89.234.125	tcp/imap	E-poštna storitev (nešifriran prenos)
443	152.89.234.125	tcp/https	Spletna storitev (šifriran dostop)
465	152.89.234.125	tcp/smtps	Šifrirano pošiljanje e-pošte
587	152.89.234.125	tcp/submission	SMTP submission
993	152.89.234.125	tcp/imaps	Šifriran dostop do e-pošte
995	152.89.234.125	tcp/pop3s	Šifriran dostop do e-pošte
3306	152.89.234.125	tcp/mysql	Podatkovna baza – omejiti dostop
5050	152.89.234.125	tcp/mmcc	Nestandardna storitev – preveriti namen
8888	152.89.234.125	tcp/sun-answerbook	Nestandardna storitev – priporočena zapora

Mnenje in priporočilo
Pregled odprtih vrat razkriva kritično stanje z visokim tveganjem. Najbolj nevarna so neposredno izpostavljena vrata za FTP (21, 26) in podatkovno bazo MySQL (3306), ki omogočajo neposreden dostop do strežnika in vseh podatkov strank. Tudi nešifrirana e-poštna vrata (110, 143) in nestandardne storitve (5050, 8888) predstavljajo veliko varnostno tveganje. Posledice so lahko hude. Če napadalec izkoristi odprta FTP vrata ali podatkovno bazo, lahko ukrade vse podatke strank, vključno z osebnimi podatki in morebitnimi plačilnimi informacijami. To bi pomenilo hudo kršitev GDPR, velike kazni in popolno izgubo zaupanja strank. Dostop do strežnika bi lahko povzročil tudi njegovo popolno ogrozitev ali uničenje podatkov. Ukrepati je treba takoj. Nemudoma je treba zapreti vrata 21, 26 in 3306 za dostop z interneta. V enem tednu je treba onemogočiti nešifrirano e-pošto (110, 143) in odstraniti nepotrebne storitve (5050, 8888), ter vsiliti uporabo šifrirane spletne strani. Dolgoročno pa je potrebno vzpostaviti strožja pravila dostopa in redno preverjati odprta vrata.

Skeniranje spletne strani

Metodologija

- Razkrivanje podatkov o uporabljeni arhitekturi in tehnologiji spletne strani
- Varnostni pregled možnih vdorov na podlagi pridobljenih podatkov
- Priprava priporočila

Poročilo testiranja

Sken spletne strani

Identificirajte CMS sistem in uporabljene tehnologije spletne strani.

Your final score:

Tested on: Jan 12th, 2026 19:32:28 GMT+1
Server IP: 152.89.234.125
Reverse DNS: rh8.neoserv.si
Location: Slovenia
Client: Desktop version

A
B
C
F

C+ B

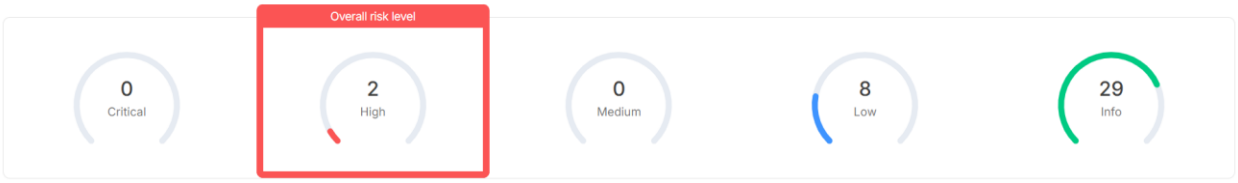
Refresh Test

Download Report

Web Software Security Test	GDPR Compliance Test	PCI DSS Compliance Test	Content Security Policy Test	HTTP Headers Security Test
NOT APPLICABLE	NOT APPLICABLE	1 ISSUE FOUND	NOT APPLICABLE	NOT APPLICABLE

CMS	WordPress 6.9
Programming languages	PHP
Databases	MySQL
Web server	LiteSpeed
Analytics	Google Analytics
Widgets	N/A
Plugins	WooCommerce PayPal Payments 3.3.1, Contact Form 7 6.1.4, Yoast SEO 26.5, WooCommerce 10.4.0, Ultimate GDPR & CCPA, WP Fastest Cache

Summary



H Vulnerabilities found for woocommerce 3.3.2

443 / TCP | CVSS v3: 8.8 | EPSS: 0.01392 | Confidence: Uncertain

H Vulnerabilities found for php 8.3.28

443 / TCP | CVSS v3: 8.2 | EPSS: 0.00056 | Confidence: Uncertain

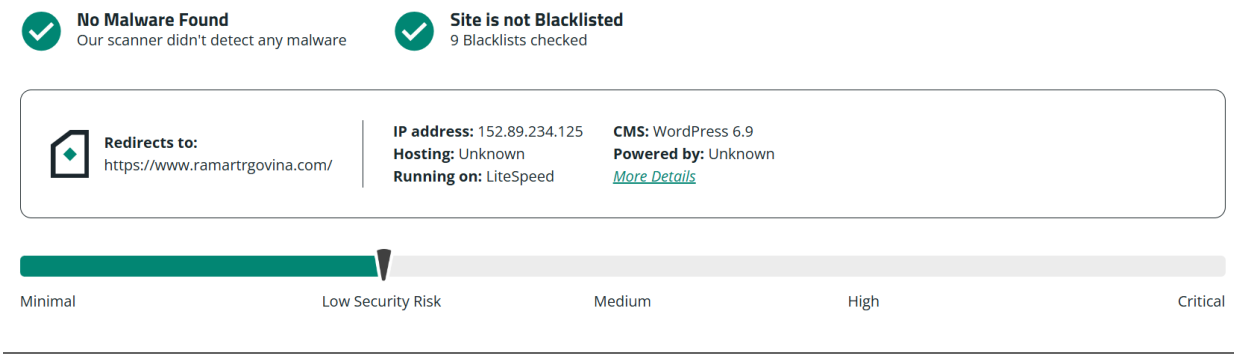
Mnenje in priporočilo

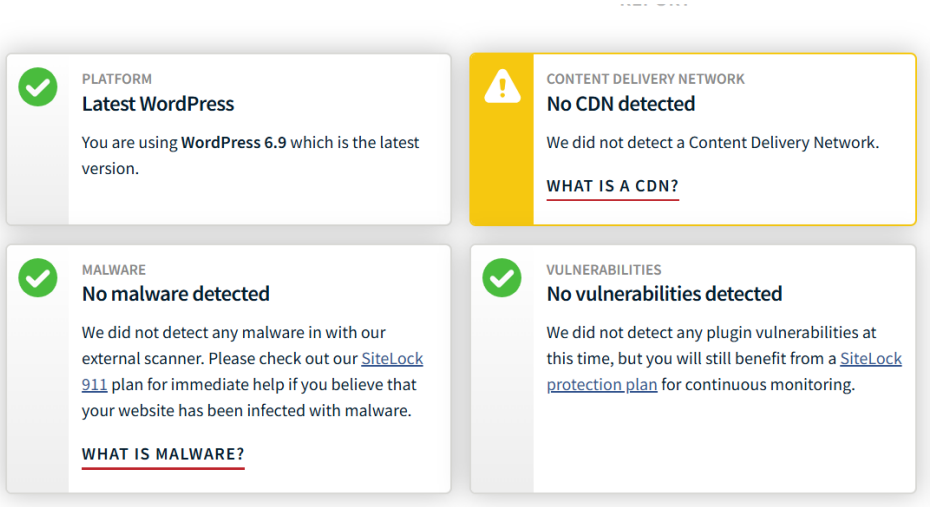
Pregled spletne strani razkriva kritično stanje z visokim tveganjem. Spletna trgovina temelji na skrajno zastareli in znano ranljivi različici WooCommerce (3.3.2), ki je več let stara. Ta vsebuje resne varnostne luknje, ki napadalcem omogočajo dostop do strežnika, podatkov strank in finančnih transakcij. Tudi različica PHP je zastarela in ranljiva.

Posledice so lahko katastrofalne. Zloraba teh ranljivosti bi lahko povzročila popolno prevzemanje spletne trgovine, krajo vseh podatkov strank (vključno z osebnimi in plačilnimi podatki) in neposredno finančno škodo. GDPR kazni bi bile znatne, ugled podjetja pa bi bil trajno okrnjen.

Ukrepati je treba nemudoma. Najnujnejši ukrep je takojšnja posodobitev WooCommerce na najnovejšo različico. V enem tednu je potrebno posodobiti vse vtičnike in PHP okolje. Dolgoročno pa vzpostaviti mesečni cikel posodabljanja in redno testiranje varnosti. Nadaljevanje poslovanja s trenutno zastarelo programsko opremo je neposredno nevarno.

Varnostni pregled spletnega strežnika



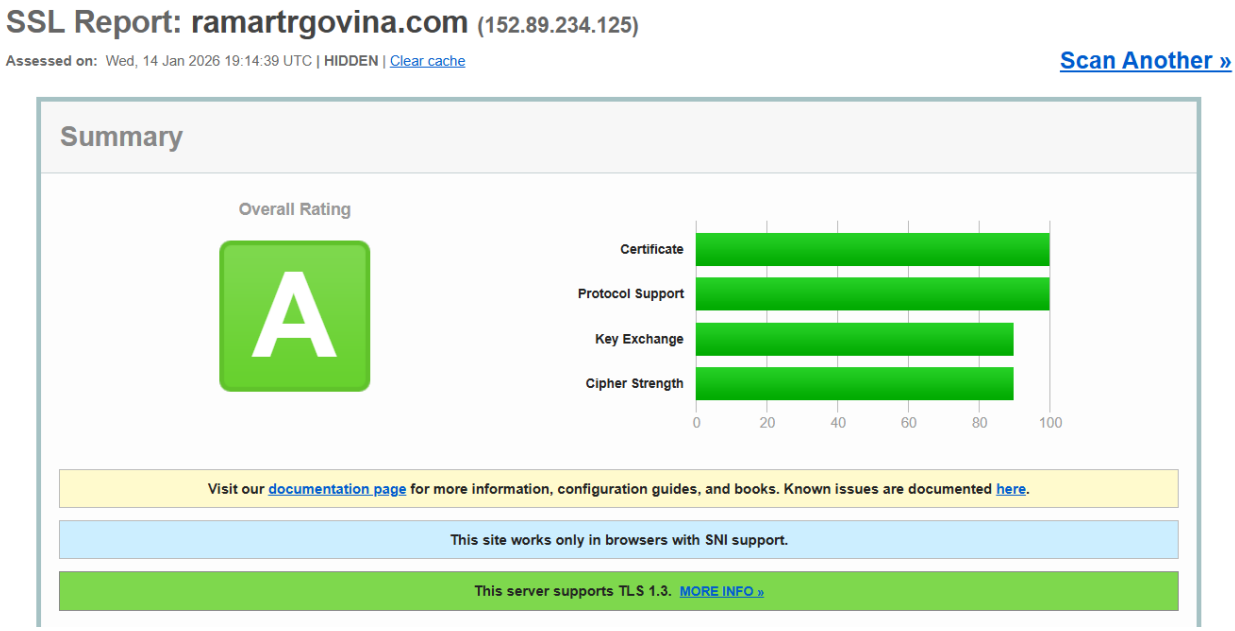


Izvedite in opredelite se glede varnostnega pregleda spletnega strežnika

Mnenje in priporočilo
Zunanji pregled strežnika ne odkrije zlonamerne programske opreme ali črnih list, kar je dobro. WordPress je posodobljen in povezava je šifrirana. Vendar je ta pregled površen in ne zazna notranjih težav, kot so kritično zastareli vtičniki (npr. WooCommerce), ki so bili ugotovljeni drugje. Brez CDN je strežnik tudi bolj izpostavljen napadom. Posledice so, da se lahko podjetje zavarjeno počuti zaradi tega površnega pregleda, medtem ko dejanske in resne ranljivosti ostajajo neodpravljene. To vodi v lažno varnost in večje tveganje za incident. Takoj je treba izvesti poglobljen tehnični pregled vseh vtičnikov in konfiguracije, da se potrdijo ali ovržejo prejšnje ugotovitve o zastareli programski opremi. V kratkem roku je priporočljivo razmisliti o uvedbi CDN za dodatno zaščito in hitrost. Ne smemo se zanašati samo na ta osnovni pregled.

SSL varnostni pregled

Izvedite in opredelite se glede uporabe SSL na spletni strani.



Mnenje in priporočilo
SSL konfiguracija spletne strani je odlična z oceno A. Podpira najnovejši protokol TLS 1.3 in uporablja močno šifriranje, kar učinkovito ščiti podatke strank med prenosom. Ker je to področje dobro konfigurirano, ne predstavlja neposrednega varnostnega tveganja. To je pozitivna izjema v celotnem pregledu. Edino priporočilo je, da spremljate datum veljavnosti SSL certifikata in ga podaljšate pravočasno, da preprečite izpade strani. Konfiguracijo je dobro redno preverjati, da ostane na tej visoki ravni.

Varnostni pregled spletne strani

Izvedite varnostni pregled spletne strani

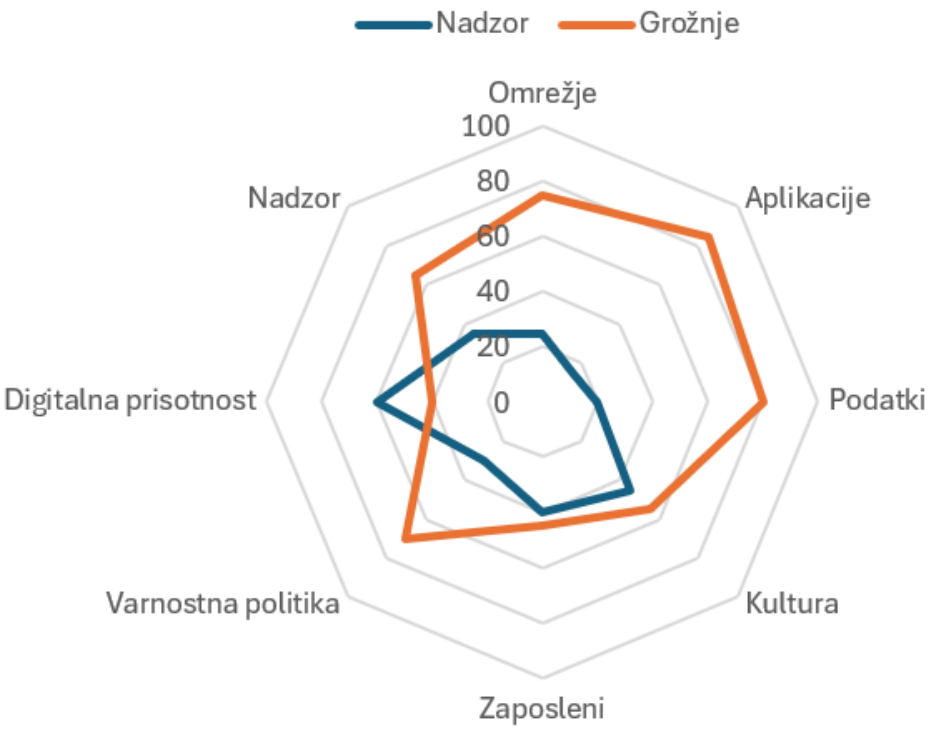
Mnenje in priporočilo
Zunanji pregled ni odkril varnostnih tveganj, kar je dobro. Vendar ta test zajema le površno analizo in ne najde vseh vrst ranljivosti, kot so napake v aplikaciji ali zastarele komponente, ki so bile ugotovljene drugje. Kljub temu, da ni bilo odkritih alarmov, to ni popolna zagotovila varnosti. Potrebno je izvesti poglobljeno testiranje, ki oceni notranjo kodo in konfiguracijo. Vzdrževati je treba redno posodabljanje vseh komponent in spremljati stanje.

13. PRIPOROČILA IN POVRATNE INFORMACIJE

Rezultat varnostnega preverjanja

Vključite graf, ki predstavlja stopnje tveganja na 8ih različnih področjih po vaši lastni oceni.:

- Omrežje - stopnja tveganja zaradi uporabe IT na omrežni ravni
- Aplikacije - stopnja tveganja zaradi uporabe aplikacij
- Podatki - stopnja tveganja zaradi zlorabe podatkov in informacij
- Kultura - stopnja tveganja zaradi slabše kulture organizacije
- Zaposleni - stopnja tveganja zaradi naivnosti uporabnikov IS
- Varnostna politika - stopnja tveganja zaradi neuporabe politike
- Digitalna prisotnost - stopnja tveganja zaradi zunanjih IT sistemov
- Nadzor - stopnja tveganja zaradi neizvajanja nadzora na IT



Poročilo varnostnega testiranja in analiza tveganja organizacije

1. Opis testiranega sistema ali okolja

Varnostni pregled je bil izveden nad informacijskim okoljem podjetja Ramar d.o.o., katerega primarna dejavnost je spletna prodaja prek javno dostopne spletne trgovine. Testirano okolje je vključevalo zunanje izpostavljene komponente informacijskega sistema, do katerih ima dostop splošna javnost oziroma potencialni napadalci z interneta.

V obseg pregleda so bili vključeni:

- spletna trgovina (WordPress/WooCommerce),
- spletni in poštni strežnik pri zunanjem ponudniku gostovanja,
- DNS infrastruktura domene,
- javno dostopni kontaktni in poslovni podatki,
- osnovna omrežna izpostavljenost (odprta vrata in storitve).

Namen sistema je zagotavljanje neprekinjenega delovanja spletne trgovine, obdelava naročil in upravljanje osebnih podatkov kupcev. Ključne informacijske storitve vključujejo spletni portal za prodajo, elektronsko pošto ter podporne strežniške storitve.

2. Uporabljene metode in orodja za varnostno testiranje

Varnostno testiranje je bilo izvedeno po metodologiji zunanjega (black-box) pregleda, brez predhodnega dostopa ali notranjih poverilnic. Uporabljene so bile naslednje metode in orodja:

Metode:

- OSINT analiza (zbiranje javno dostopnih informacij),
- pregled konfiguracij (DNS, SSL/TLS),
- skeniranje omrežnih vrat,

- osnovno testiranje spletne aplikacije,
- analiza izpostavljenosti osebnih in poslovnih podatkov.

Orodja:

- Nmap – za identifikacijo odprtih vrat in storitev,
- WHOIS in DNS orodja – za pregled domenskih zapisov,
- SSL Labs – za preverjanje SSL/TLS konfiguracije,
- javne baze uhajanj podatkov (npr. HaveIBeenPwned),
- spletni skenerji tehnologij (CMS, vtičniki, PHP različice).

3. Rezultati varnostnega testiranja

Varnostno testiranje je razkrilo več pomembnih ugotovitev:

- zaznana so bila kritično izpostavljena omrežna vrata (FTP, MySQL, nestandardne storitve),
- spletna trgovina uporablja zastarelo in znano ranljivo različico WooCommerce,
- poslovni e-poštni račun je bil zaznan v preteklih uhajanjih podatkov,
- DNS infrastruktura nima omogočenih zaščitnih mehanizmov (DMARC, DNSSEC),
- osebni in kontaktni podatki lastnikov so javno dostopni,
- SSL/TLS konfiguracija je ustrezna in predstavlja pozitiven primer dobre prakse.

Ugotovitve kažejo na kombinacijo tehničnih in organizacijskih pomanjkljivosti, ki skupaj bistveno povečujejo tveganje za varnostni incident.

4. Analiza tveganj

Analiza tveganj je bila izvedena na podlagi ocene verjetnosti izkoriščanja in vpliva na poslovanje.

Področje	Opis tveganja	Verjetnost	Vpliv	Stopnja tveganja	Predlagani ukrep
Spletna aplikacija	Zastarela programska oprema (WooCommerce, PHP)	Visoka	Zelo visok	Visoko	Takojšnja posodobitev in redno vzdrževanje
Omrežje	Izpostavljena kritična vrata (FTP, MySQL)	Srednja	Zelo visok	Visoko	Zapora vrat, omejitev dostopa
Podatki	Uhajanje poverilnic in osebnih podatkov	Srednja	Zelo visok	Visoko	Menjava gesel, 2FA, politika dostopov
E-pošta	Odsotnost DMARC zaščite	Srednja	Visok	Srednje–visoko	Uvedba DMARC, SPF in DKIM
Organizacija	Pomanjkanje formalne varnostne politike	Visoka	Srednji	Srednje	Sprejem osnovnih varnostnih pravil

Skupna ocena tveganja za organizacijo je srednje do visoko, predvsem zaradi kombinacije tehničnih ranljivosti in pomanjkanja formaliziranih varnostnih postopkov.

5. Zaključek in priporočila

Zunanji varnostni pregled je pokazal, da ima podjetje Ramar d.o.o. več resnih varnostnih pomanjkljivosti, ki lahko v primeru zlorabe povzročijo:

- izgubo osebnih podatkov strank,
- finančno škodo in izpad poslovanja,
- kršitve GDPR zakonodaje,
- dolgoročno škodo ugledu podjetja.

Najbolj kritična področja so zastarela programska oprema spletne trgovine, izpostavljene omrežne storitve in nezadostno upravljanje z dostopi in podatki.

Ključna priporočila:

- takojšnja posodobitev vseh komponent spletne trgovine,
- zaprtje ali omejitev vseh nepotrebnih odprtih vrat,
- uvedba dvofaktorske avtentikacije in menjave gesel,
- vzpostavitev osnovne varnostne in GDPR politike,
- redno izvajanje varnostnih pregledov (vsaj letno).

Ob upoštevanju predlaganih ukrepov se lahko raven tveganja bistveno zmanjša, podjetje pa pridobi stabilnejše in varnejše okolje za nadaljnje poslovanje.

14. INFORMACIJE IN POTRDILA O STROKOVNI USPOSOBLJENOSTI IT STROKOVNJAKA

Tu se ponavadi vključujo potrdila in povezave do certifikatov, ki jih ima izvajalec pregleda.

/

15. KONTAKTNI PODATKI IZVAJALCA

Izvajalec zunanjega varnostnega pregleda

Tinkara Grum