Balkan Cyber Risk Report 2026

Praktičan izveštaj za vlasnike firmi, direktore, HR i IT timove

Autor: Stefan Spasov BloodCode / ElmConstruct / BloodCode Security

Web: https://elmconstruct.com

Kontakt: bloodcodehack@gmail.com | +381 63 146 0616

Uvod

Većina firmi na Balkanu ne gubi cyber bitku zato što nema najskuplji alat. Gubi je zato što nema osnovnu disciplinu: MFA, dobar backup, phishing trening, jasna pravila incidenta, email zaštitu i pregled javne izloženosti.

Ovaj izveštaj nije akademski papir i ne tvrdi da predstavlja statističko istraživanje celog tržišta. Ovo je praktičan security briefing za firme koje žele da smanje realan rizik pre incidenta.

Glavna poruka

Ako firma ima email, fakture, zaposlene, klijente i web prisustvo, ona već ima cyber rizik.

Pitanje nije da li je firma "dovoljno velika" za napad. Pitanje je da li je dovoljno laka meta.

Top 10 rizika za firme u Srbiji i regionu

1. Email bez MFA

Jedan kompromitovan email može otvoriti fakture, dokumente, komunikaciju sa klijentima i interne odluke.

Prvi korak:

- Uključiti MFA za sve ključne naloge.
- Prioritet: direktor, finansije, HR, IT, administracija.

2. Phishing i lažne fakture

Napadač često ne mora da probije server. Dovoljno je da pošalje ubedljivu lažnu fakturu ili poruku koja izgleda kao da dolazi od direktora, banke, dobavljača ili kurira.

Prvi korak:

- Uvesti proceduru provere promena računa za uplatu.
- Trenirati zaposlene da prijave sumnjive poruke.

3. Backup koji nije testiran

Backup koji nikada nije vraćen možda ne postoji. U incidentu se ne računa šta piše u politici, nego koliko brzo firma može da se vrati u rad.

Prvi korak:

- Testirati restore.
- Definisati RTO/RPO: koliko dugo firma može da stoji i koliko podataka sme da izgubi.

4. Slabe i ponovljene lozinke

Ako zaposleni koristi istu lozinku na više platformi, curenje jedne platforme može ugroziti firmu.

Prvi korak:

- Password manager.
- Zabrana deljenja lozinki preko chata/emaila.
- MFA na ključnim servisima.

5. Nejasan incident response

Kada se desi incident, najskuplji haos nastaje jer niko ne zna ko odlučuje, koga zove, šta gasi i šta čuva kao dokaz.

Prvi korak:

- Napraviti incident contact listu.
- Definisati prvih 30 minuta incidenta.
- Održati tabletop vežbu sa menadžmentom.

6. Javno izloženi paneli i stari sistemi

Admin paneli, staging okruženja, stari subdomeni i zaboravljene aplikacije često ostaju javno dostupni.

Prvi korak:

- Napraviti external attack surface review.
- Ukloniti ili ograničiti nepotrebne javne servise.

7. Loša email konfiguracija

SPF, DKIM i DMARC nisu magija, ali su osnovna higijena. Bez njih je lakše zloupotrebiti identitet domena.

Prvi korak:

- Proveriti SPF/DKIM/DMARC.
- Postepeno pooštriti DMARC politiku.

8. Nema treninga za zaposlene

Zaposleni nisu problem. Problem je firma koja očekuje da zaposleni prepoznaju napad bez treninga.

Prvi korak:

- Kratak awareness trening.
- Phishing simulacija bez prikupljanja realnih lozinki.
- Jasna procedura prijave.

9. Nema executive security izveštaja

Tehnički nalaz bez poslovnog prevoda ne vodi do odluke. Direktor mora da vidi rizik, prioritet, trošak i sledeći korak.

Prvi korak:

- Prevesti security nalaze u poslovni jezik.
- Napraviti 7/30/90 plan.

10. Security se radi tek posle incidenta

Najskuplji security je onaj koji se kupuje u panici. Preventivna dijagnoza je jeftinija od gašenja požara.

Prvi korak:

- 15-min security dijagnoza.
- Starter audit ili corporate trening.

Brza checklist za direktore

☐ Imamo MFA na emailu i ključnim nalozima.
☐ Znamo ko reaguje u prvih 30 minuta incidenta.
☐ Backup restore je testiran u poslednjih 90 dana.
☐ Zaposleni znaju kome prijavljuju sumnjivu poruku.
☐ Finansije proveravaju promenu računa za uplatu drugim kanalom.
☐ Imamo osnovni SPF/DKIM/DMARC.
☐ Znamo koji su naši javno dostupni sistemi.
☐ Imamo listu kritičnih sistema i vlasnika.
☐ Imamo plan za komunikaciju sa klijentima ako se desi incident.
☐ Menadžment je prošao bar jednu tabletop vežbu.

Preporučeni 7/30/90 plan

Prvih 7 dana

- Uključiti MFA na najvažnijim nalozima.
- Proveriti email security konfiguraciju.

- Identifikovati najkritičnije sisteme.
- Definisati incident contact listu.

Prvih 30 dana

- Održati awareness trening.
- Uraditi phishing simulaciju bez prikupljanja lozinki.
- Testirati backup restore.
- Uraditi external attack surface review.

Prvih 90 dana

- Napraviti executive security roadmap.
- Uvesti mesečnu ili kvartalnu phishing simulaciju.
- Održati executive tabletop vežbu.
- Retestirati popravljene rizike.

BloodCode ponude

Security Growth Package

- Starter Audit: 1.500 EUR.
- Pro Security: 3.500 EUR.
- Business Red Team: 7.500 EUR+.
- Corporate: 15.000 EUR+.

Corporate Cyber Training

- Awareness Sprint: 2.500 EUR.
- Phishing + Tabletop: 5.000 EUR.
- Corporate Red Team Workshop: 7.500 EUR+.

Phishing Simulation as a Service

- Starter: 299 EUR mesečno.
- Professional: 599 EUR mesečno.
- Enterprise: 1.499 EUR mesečno.

Sledeći korak

Ako želite da proverite gde je vaša firma najviše izložena, pošaljite:

`SECURITY`

WhatsApp: +381 63 146 0616

Lead forma: https://elmconstruct.com/lead.html

Security landing: https://elmconstruct.com/security.html

Corporate training: https://elmconstruct.com/corporate-training.html