BloodCode Security Growth Package

Security audit, pentest, phishing simulacija i executive izveštaj za firme

Autor: Stefan Spasov BloodCode, osnivač ElmConstruct i BloodCode Security.

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

Kratka poruka

Većina firmi ne pada zato što nema skupe alate. Pada zato što ne zna šta joj je javno izloženo, zaposleni ne prepoznaju phishing, lozinke se ponavljaju, backup nije proveren, a direktor dobija tehničke izveštaje koje ne može da pretvori u odluku.

BloodCode Security Growth Package daje vlasniku firme jasan odgovor:

1. Gde smo ranjivi?
2. Koliko je rizik realan?
3. Šta popravljamo prvo?
4. Koliko nas incident može koštati?
5. Koji sledeći korak štiti novac, reputaciju i operacije?

Sve se radi isključivo u dogovorenom i pisanom scope-u. Nema neovlašćenog testiranja, nema prikupljanja realnih lozinki, nema destruktivnih akcija.

Za koga je paket

- IT firme i web agencije koje žele jači security kredibilitet.
- Klinike, poliklinike, stomatološke ordinacije i optike.
- Advokatske kancelarije, notari i računovodstvene agencije.
- E-commerce, proizvodnja, transport i firme sa 20-300 zaposlenih.
- Direktori koji žele executive izveštaj, ne 80 strana tehničkog haosa.

Šta radimo

1. External Attack Surface Review

Pregled javno dostupnih domena, aplikacija, mail security signala, izloženih servisa i osnovnih rizika koji se mogu videti spolja bez invazivnog testiranja.

Ishod: lista prioriteta i mapa javnog rizika.

2. Web/App Security Audit

Osnovni ručni audit dogovorenih web aplikacija ili landing stranica u legalnom scope-u.

Fokus:

- Autentikacija i autorizacija.
- Slabe forme i logika procesa.
- XSS rizici sa realnim uticajem.
- CORS, headers, session i cookie higijena.
- Sensitive data exposure.
- Loša konfiguracija servera ili aplikacije.

3. Phishing Simulation

Bezbedna phishing simulacija za zaposlene, bez krađe realnih lozinki.

Merimo:

- Ko je kliknuo.
- Ko je prijavio sumnjivu poruku.
- Koliko brzo je tim reagovao.
- Koji tip poruke najviše prolazi.

4. Awareness Mini Trening

Kratak trening za zaposlene i menadžment:

- Kako prepoznati phishing.
- Kako prijaviti sumnjivu poruku.
- Kako koristiti MFA i password manager.
- Šta raditi ako se desi incident.

5. Executive PDF Report

Izveštaj pisan za direktora:

- Rizik.
- Uticaj na novac i reputaciju.
- Prioriteti.
- Brze pobede.
- Plan 7, 30 i 90 dana.

6. Debrief Call

60 minuta sa direktorom, vlasnikom ili IT timom. Prolazimo nalaze i biramo sledeći korak.

Paketi i cene

Starter Audit: 1.500 EUR

Za manje firme koje žele prvi realan security pregled.

Uključuje:

- External attack surface review.
- Osnovni web/app pregled za 1 asset.
- Mail security check.
- Executive PDF report.
- 30-min debrief.

Pro Security: 3.500 EUR

Za firme koje žele ozbiljniji pregled i edukaciju zaposlenih.

Uključuje:

- Sve iz Starter paketa.
- Web/app audit za do 3 asseta.
- Phishing simulation do 50 zaposlenih.
- Awareness mini trening.
- 60-min debrief.

Business Red Team: 7.500 EUR

Za firme koje žele simulaciju realnog poslovnog rizika u kontrolisanom scope-u.

Uključuje:

- Sve iz Pro paketa.
- Scenario-based red-team workshop.
- Phishing simulation do 150 zaposlenih.
- Executive tabletop incident vežba.
- 7/30/90 remediation roadmap.

Corporate: 15.000 EUR+

Za veće firme, compliance, više timova ili više lokacija.

Uključuje:

- Custom scope.
- Multi-team engagement.
- Management workshop.
- Retest.
- Mesečni security advisory opcionalno.

Mesečni nastavak: Phishing Simulation as a Service

Starter: 299 EUR mesečno

- Do 25 zaposlenih.
- 1 kampanja mesečno.
- 3 template-a.
- Kratak PDF izveštaj.

Professional: 599 EUR mesečno

- 26-100 zaposlenih.
- 2 kampanje mesečno.
- 10 template-a i 2 custom template-a.
- Edukativna landing strana.
- Kvartalni trening.

Enterprise: 1.499 EUR mesečno

- 100+ zaposlenih.
- Multi-vector simulacije.
- Compliance izveštaji.
- Dashboard i management reporting.

Legalni okvir

Pre početka rada potpisuju se:

- Scope of Work.
- Pisano ovlašćenje.
- NDA.
- Pravila angažovanja.
- Data handling pravila.
- Stop conditions.

Ne radimo:

- Testiranje van scope-a.
- Krađu ili čuvanje realnih lozinki.
- Destruktivne akcije.
- Brute force, DoS ili opterećenje sistema.
- Neovlašćeno testiranje trećih lica.

Proces

1. Besplatna 15-min dijagnoza.
2. Dogovor scope-a i cilja.
3. Potpisivanje ovlašćenja i pravila.
4. Testiranje i simulacija.
5. Executive report.
6. Debrief.
7. Remediation plan i opcioni retest.

Sledeći korak

Pošaljite poruku:

`SECURITY DIJAGNOZA`

WhatsApp: +381 63 146 0616
Email: bloodcodehack@gmail.com
Web: https://elmconstruct.com