CYBER SECURITY TEAM @ANNI

TESTIRANJE KIBERNETSKE VARNOSTI

s sistemskim varnostnim pregledom

varnost.anni.si

SISTEMSKI VARNOSTNI PREGLED

1. **Pregled in analiza zunanjih informacijskih ranljivosti IKT sistema podjetja**, ki zajema:
   - Pregled zunanjih informacijskih ranljivosti
   - Pregled potencialnih ranljivosti e-poštnega sistema
   - Pregled potencialnih ranljivosti e-poštnih računov, če so bili vpleteni v kakršno koli krajo poverilnic

2. **Interno preverjanje sistema zajema avtomatski in ročni pregled vašega IKT sistema**, pri katerem točno določimo obseg naprav katere pregledujemo:
   - Pregled strežnikov
   - Pregled delovnih postaj
   - Analiza lokalnih delovnih postaj (pravice uporabnikov, ustrezno nameščeni protivirusni produkti, pravilno nastavljeni in redno posodabljani programi)
   - Pregled omrežja

3. **Avtomatsko preverjanje ranljivosti IKT sistema**
   - Avtomatsko preverjanje ranljivosti IKT Sistema z licenčnim orodjem
   - Avtomatsko testiranje ranljivosti spletnih aplikacij po priporočilih OWASP

4. **Analiza aktivnega direktorija podjetja (Active Directory)**
   - Tehnične podrobnosti aktivnega direktorija / Informacije o domeni

5. **Simulacija napada na organizacijo**
   - Izvedba napada na organizacijo preko lažnive e-pošte (Phishing)

6. **Izdelava poročila** s priporočili ter predlaganimi sestemskimi ukrepi

DODATNE STORITVE

- Izobraževanje zaposlenih,
- pregled aktivnega direktorija podjetja (Microsoft Active directory),
- pregled informacijske varnosti domenskega krmilnika (domain controller security hardening),
- analiza informacijske varnosti operacijskih sistemov (windows/linux security hardening),
- analiza zlonamerne programske opreme (malware) in forenzika ob incidentih,
- posodobitev aplikacij delovnih postaj (patch management clients/servers),
- pregled varnostnega kopiranja (backup policy),
- pregled požarnih pregrad in nastavljenih pravil,
- priprava unikatnih zlonamernih programov, ki zaobidejo tradicionalne varnostne rešitve in večino naprednih, predvsem za namene ribarjenja (Phishing test),
- izdelava poročila s priporočili za odpravo najdenih varnostnih pomanjkljivosti,
- ELK Stack in definiranje, priprava in konfiguracija rešitve za centralno zajemanje dnevniških datotek
- pregled informacijske zrelosti podjetja ter vpeljanih tehnoloških rešitev (password policies, granular password policies in AD, MFA,
- več nivojski phishing,
- penetracijski test po meri (več različnih opcija napada ...),
- Onemogočanje storitev, opozori se na potencialno varnostno luknjo katero se lahko izkoristi za onemogočanje storitev (Denial-of-Service), izvede se napad onemogočanja storitev (Denial-of-Service).

PRIDOBLJENI CERTIFIKATI

ITIL (IT Service Management), MS Security Fundamentals, CompTIA Security+, CompTIA Network+ , CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional)

CERTIFICIRANJA V TEKU

-2x , CEH (Certified Ethical Hacker) ter CompTIA Pentest+

ZNANJA, CERTIFICIRANJA TER IZOBRAŽEVANJA

Notranja presoja ISO 27001 ter ISO 9001, MS server, WatchGuard prodajna in tehnična certificiranja, DELL EMC, prodajna in tehnična certificiranja, Bitdefender prodajna in tehnična certificiranja

CYBER SECURITY TEAM @ANNI

Toni JERŠIN
M 041 820 577

Matej PERNEK
M 051 323 343

kibernetska-varnost.anni.si

NOVO!
Prva pomoč pri spletnih napadih
MODRA ŠTEVILKA 080 25 52

anni Že od 1990!

Anni d.o.o., Motnica 7a, Trzin
T 01/ 5800 800, info@anni.si, www.anni.si