

Kiberdrošības apmācība

Apmācību mērķis ir iepazīstināt ar dažādām potenciālajām kiberuzbrukumu metodēm. Tās apzinoties, uzņēmums var savlaicīgi novērst nopietnus draudus, kā piemēram, e-pastu, personas datu un komercnoslēpumu zādzību vai pat ļaunprātīgas kontroles pārņemšanu pār visa uzņēmuma infrastruktūru un biznesa procesiem.

☀ **Krāpnieciskas e-pasta vēstules (pikšķerēšana/viltošana)**

- E-pasts ir viltots, ar mērķi radīt priekšstatu, ka tas tiek sūtīts no uzņēmuma vadības.
- Krāpnieciskais e-pasts satur ziņojumu, ka radusies problēma ar lietotāja kontu, kuru varatrisināt, ievadot savu pieejas paroli.

☀ **Paroļu uzbrukumi**

- Uzbrukumi ar paroļu minēšanu (Password spray)
- Paroļu uzbrukumi, izmantojot vārdnīcu datubāzes (Password dictionary attacks)
- Visbiežāk lietotās paroles
- Rekomendējamās paroles
- Paroļu datu noplūde (haveibeenpwned.com – vietne, kurā iespējams pārbaudīt konkrētu e-pastu un paroļu noplūdes apdraudējuma risku)
- Viltus e-pastu piemēri

☀ **Spieģprogrammatūras un reklāmprogrammatūras (Spyware and adware)**

- Dažādas programmatūras, kas apkopo lietotāja datorā esošus datus, uzrauga lietotāja aktivitātes un reģistrē visu ievadīto informāciju (piemēram, paroles). Traucējošas reklāmas, uz kurām noklikšķinot, tiek atvērta krāpnieciska satura vietne.

☀ **Publiskais Wi-Fi tīkls bez paroles**

- Tā kā aizdomīgas ierīces var izveidot savienojumu ar publisku Wi-Fi tīklu, kas pieejams bez paroles, tas var tikt izmantots ļaunprātīgiem nolūkiem.
- Hakeris izveido Wi-Fi tīklu ar ticamu uzņēmuma nosaukumu. Lietotājs, nesaskatot neko aizdomīgu, izveido savienojumu ar attiecīgo Wi-Fi un tiek novirzīts uz krāpniecisku tīklu.

☀ **Mēstules**

- Reklāmas vai jaunumu vēstkopas par produktiem/pakalpojumiem
- Ļaunprātīgas e-pasta vēstules

☀ Sociālā inženierija (Social Engineering)

- ☉ Māksla manipulēt ar cilvēkiem, lai tie brīvprātīgi sniegtu hakeriem piekļuvi saviem datiem.
- ☉ Tādējādi ļaunprātīgi tiek izmantots cilvēku:
 - ☉ slinkums
 - ☉ neuzmanība
 - ☉ pārmērīga uzticēšanās (hakerim izliekoties par IT speciālistu)
 - ☉ entuziasms (krāpnieks apsola kādu labumu, ja uzreiz tiks veikta konkrēta darbība)
 - ☉ patiesa vēlme palīdzēt
 - ☉ uzticēšanās (lietotājam šķiet, ka viņš izpilda priekšnieka pavēli)
- ☉ Nolietotas iekārtas, kas tiek izmestas atkritumos, neveicot pienācīgu apkopi, t.i., datu dzēšanu.
- ☉ Paroles ievadīšanas procesa noklausīšanās vai novērošana.

☀ Drošības risinājumi

- ☉ Paroles vietā tiek lietots PIN kods
- ☉ Daudzpakāpju autentifikācija (Multi-factor authentication jeb MFA)
- ☉ Bezparoles autentifikācija
- ☉ Bitlocker šifrēšana
- ☉ Par Office365 aizsardzības rīku tiek izmantots Microsoft Defender, nevis ATP

Apmācību laiks: saskaņojot ar klientu

Apmācību vadītājs: Mārtiņš Jurjāns

Apmācību ilgums: 2 stundas

Apmācību vieta: tiešsaistē

Dalībnieku skaits: līdz 20 cilvēkiem vienā grupā vai pēc vienošanās ar klientu

Investīcijas:

Pakalpojuma izveide un rezultātu pārskats: 600€

