# Skats no uzbrucēja puses

Artūrs Daņiļevičs

09.12.2025.

CERT.LV
Kiberincidentu novēršanas institūcija

# Pikšķerēšana

**Atvērta saite**

1. Epasts ir aktīvs
2. Kāda OS
3. Kāda pārlukprogramma
4. No kurienes “nāk” lietotājs
5. Mērķa marķēšana

**Piekļuve epastam**

1. Kontaktu saraksts
2. Iekšējā sarakste
3. Piekļuve citām sistēmām
4. Privilēģiju eskalācija

# Vietnes “uzlaušana”

- **Administratora piekļuves dati** (CMS, hosting, intranet)
- **Datubāzes**: lietotāju e-pasti, paroles (hash), personas dati, API inegrāciju atslēgas
- **Failu augšupielādes iespējas** → ļaunatūra, webshell / backdoor
- **Servera resursi** (CPU/RAM, tīkla trafiks)
- **SEO un reklāmas kanāli** (bot trafiks, redirecti)

# Uzbrukuma simulācija (RedTeam engagement)

**Pasīvā fāze**

1. Publiski pieejamā info
2. “DarkNet” info
3. Izmantoto rīku analīze

**Aktīvā fāze**

1. Pikšķerēšanas kampaņas
2. Eksploitošana
3. Privilēģiju eskalācija

# Ko darīt?

- Nav viens maģisks risinājums
- Drošas izstrādes ietvars (SSDLC/SDLC – (Software)Secure Development life cycle)
- Pārzināt pārvaldīt savu infrastuktūru
- Tīkla segmentācija
- MFA + FIDO2
- Monitorings un darbinieku apmācība
- CVD.CERT.LV

# Interesanti fakti no ikdienas

- 7 dažādas paroles
- Tiek ievadīti kolēģu dati
- Publiski pieejami vietnes dati
- Izstrādātāju monitorings

# Beigas