# Kiberuzbrukumu veidi

Kiberuzbrukumi ir mēģinājumi iegūt datus, piekļuvi sistēmām vai traucēt iestādes darbu. Tie var būt vērsti gan pret organizāciju, gan pret konkrētu darbinieku.
Pašvaldības iestādēs īpaši svarīgi ir sargāt **personas datus, dokumentus, e-pastu un piekļuves kontus**.

# Biežākie kiberuzbrukumu veidi

## 1. Pikšķerēšana (Phishing)

Pikšķerēšana ir mēģinājums izkrāpt sensitīvu informāciju, izliekoties par uzticamu personu vai organizāciju.

**Pazīmes:**

- aizdomīgs sūtītāja e-pasts;
- steidzinošs tonis (“nekavējoties rīkojieties”);
- saites uz nepazīstamām vai viltotām vietnēm;
- pielikumi, kurus negaidījāt;
- lūgums ievadīt paroli vai citus datus.

**Piemērs:**
Saņemat e-pastu, kas izskatās kā no Microsoft vai kolēģa, ar aicinājumu “atjaunot paroli”.

**Ko darīt:**

- neatvērt aizdomīgas saites vai pielikumus;
- pārbaudīt sūtītāja adresi;
- neievadīt paroli, ja neesat pārliecināts par vietnes īstumu;
- ziņot IT atbalstam.

---

## 2. Mērķēta pikšķerēšana (Spear phishing)

Tas ir personalizēts uzbrukums, kas pielāgots konkrētam darbiniekam, nodaļai vai amatpersonai.

**Pazīmes:**

- ziņā minēts jūsu vārds, amats vai iestāde;
- izmantota informācija no publiskiem avotiem;
- ziņa šķiet ticama un saistīta ar darbu.

**Piemērs:**
Darbinieks saņem e-pastu it kā no vadītāja ar lūgumu steidzami atvērt dokumentu vai veikt maksājumu.

**Ko darīt:**

- pārbaudīt pieprasījumu citā saziņas kanālā;
- nesteigties ar darbībām;
- īpaši uzmanīties, ja tiek prasīti dati, faili vai maksājumi.

---

# 3. Ļaunprogrammatūra (Malware)

Ļaunprogrammatūra ir kaitīga programmatūra, kas var bojāt ierīci, vākt datus vai dot uzbrucējam piekļuvi sistēmai.

**Izplatītākie veidi:**

- vīrusi;
- trojāņi;
- spiegprogrammas;
- taustiņspiedienu reģistrētāji;
- izspiedējprogrammatūra.

**Kā izplatās:**

- caur e-pasta pielikumiem;
- lejupielādējot failus no nedrošām vietnēm;
- izmantojot inficētas USB ierīces;
- atverot viltotas saites.

**Ko darīt:**

- atvērt tikai zināmus failus;
- neinstalēt nepārbaudītas programmas;
- izmantot tikai iestādes apstiprinātus risinājumus;
- ziņot IT atbalstam, ja dators sāk darboties neparasti.

---

# 4. Izspiedējprogrammatūra (Ransomware)

Izspiedējprogrammatūra bloķē piekļuvi failiem vai sistēmām un pieprasa samaksu par to atjaunošanu.

**Pazīmes:**

- faili pēkšņi nav atverami;
- parādās paziņojums par šifrēšanu;
- sistēma darbojas neparasti vai tiek bloķēta.

**Sekas:**

- dokumentu nepieejamība;
- darba pārtraukumi;
- datu zudums;
- iestādes pakalpojumu traucējumi.

**Ko darīt:**

- nekavējoties atvienot ierīci no tīkla, ja iespējams;
- nekādā gadījumā nemēģināt risināt vienatnē;
- nekavējoties ziņot IT atbalstam.

---

# 5. Paroļu uzbrukumi

Uzbrucēji mēģina iegūt paroles, lai piekļūtu e-pastam, sistēmām vai dokumentiem.

**Biežākie paņēmieni:**

- paroles minēšana;
- atkārtoti mēģinājumi pieslēgties;
- noplūdušu paroļu izmantošana;
- pikšķerēšanas ceļā iegūtas paroles.

**Riski palielinās, ja:**

- viena parole tiek lietota vairākās vietās;
- parole ir pārāk vienkārša;
- netiek izmantota daudzfaktoru autentifikācija.

**Ko darīt:**

- lietot spēcīgas un unikālas paroles;
- neizpaust paroles citiem;
- izmantot daudzfaktoru autentifikāciju;
- nekavējoties nomainīt paroli, ja ir aizdomas par noplūdi.

---

# 6. Sociālā inženierija

Sociālā inženierija ir cilvēku ietekmēšana, lai panāktu piekļuvi informācijai vai sistēmām.

**Piemēri:**

- zvans no “IT speciālista”, kurš prasa paroli;
- e-pasts no “vadītāja” ar steidzamu uzdevumu;
- persona, kas mēģina iegūt informāciju sarunā vai klātienē.

**Ko darīt:**

- neizpaust paroles pa telefonu vai e-pastā;
- pārbaudīt personas identitāti;
- uzmanīties no steidzinošiem vai neierastiem lūgumiem.

---

# 7. Viltotas mājaslapas

Uzbrucēji izveido lapas, kas izskatās līdzīgas īstām pieteikšanās vietnēm, lai iegūtu lietotājvārdu un paroli.

**Pazīmes:**

- adrese nedaudz atšķiras no īstās;
- vietne izskatās pazīstama, bet darbojas neierasti;
- pieteikšanās lapa atvērta caur saiti no e-pasta.

**Ko darīt:**

- adresei pārlūkā jāpievērš īpaša uzmanība;
- pieteikšanās lapas atvērt pašam, nevis caur aizdomīgu saiti;
- neievadīt datus, ja ir šaubas.

---

# 8. Datu noplūde

Datu noplūde var notikt gan ļaunprātīga uzbrukuma, gan nejaušas kļūdas dēļ.

**Piemēri:**

- dokuments nosūtīts nepareizam adresātam;
- publiski koplietota datne ar ierobežotas pieejamības informāciju;
- paroles glabāšana nedrošā vietā;
- piekļuve datiem neatļautām personām.

**Ko darīt:**

- vienmēr pārbaudīt adresātu pirms nosūtīšanas;
- nekoplietot piekļuves datus;
- dokumentus glabāt tikai apstiprinātās sistēmās;
- par incidentiem nekavējoties ziņot.

---

# Kā sevi pasargāt ikdienā

Lai mazinātu riskus:

- neatver aizdomīgus e-pastus, saites un pielikumus;
- lieto spēcīgas, unikālas paroles;
- izmanto daudzfaktoru autentifikāciju;
- strādā tikai ar apstiprinātām sistēmām un programmām;
- bloķē datoru, aizejot no darba vietas;
- neizmanto nezināmas USB ierīces;
- regulāri pievērs uzmanību sistēmas paziņojumiem;
- aizdomu gadījumā nekavējoties sazinies ar IT atbalstu.

---

# Ja ir aizdomas par kiberuzbrukumu

Nekavējoties:

1. pārtrauc darbību ar aizdomīgo e-pastu, saiti vai failu;
2. ja iespējams, atvieno ierīci no tīkla;
3. neizdzēs pierādījumus;
4. sazinies ar IT atbalstu;
5. īsi apraksti, kas notika un ko esi atvēris.

---

Kristine Majore izveidojis pirms 2026-07-15 14:56:20 EEST
Kristine Majore atjauninājis pirms 2026-08-11 09:42:03 EEST