Datu valsts inspekcija

Kā rīkoties kiberincidenta gadījumā

Prevencijas nodaļas
Informācijas sistēmu drošības pārvaldnieks
Jānis Kravcovs

Datu valsts inspekcija

Semināra mērķis un temati

- **Izprast, kas ir kiberincidents**
- **Uzzināt, kā to ātri atpazīt**
- **Pirmās rīcības veicamie soļi**
- **Rokasgrāmata kiberincidentu gadījumiem**

Datu valsts inspekcija

Kas ir kiberincidents?

Kiberincidents ir jebkurš notikums, kas apdraud informācijas sistēmas konfidencialitāti, integritāti vai pieejamību.

Tipiskākie piemēri:

- Uzbrukumi mājaslapām vai serveriem
- Pikšķerēšana (phishing)
- Uzlauzts e-pasts
- Šifrējošie (izspiedēj) vīrusi
- Datu noplūdes

Datu valsts inspekcija

Kāpēc kiberincidents rada augstu risku maziem un vidējiem uzņēmumiem?

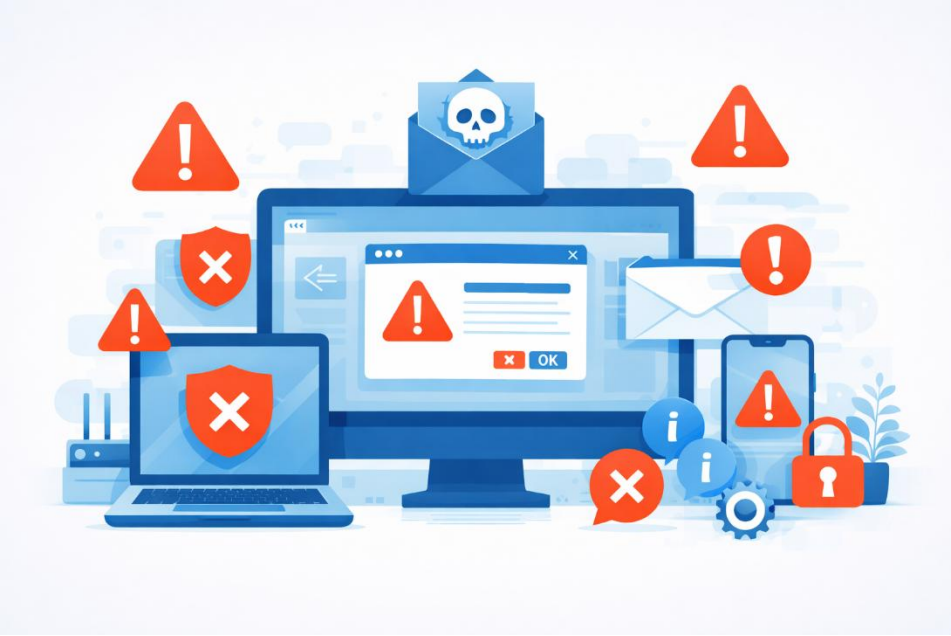
- **Reti ir iekšējie IT drošības speciālisti**
- **Incidenti var paralizēt uzņēmuma darbību**
- **Klientu uzticība un reputācija tiek apdraudēta**
- **Augsts datu zaudēšanas risks**

Datu valsts inspekcija

Kā atpazīt kiberincidentu?

Biežākās pazīmes:

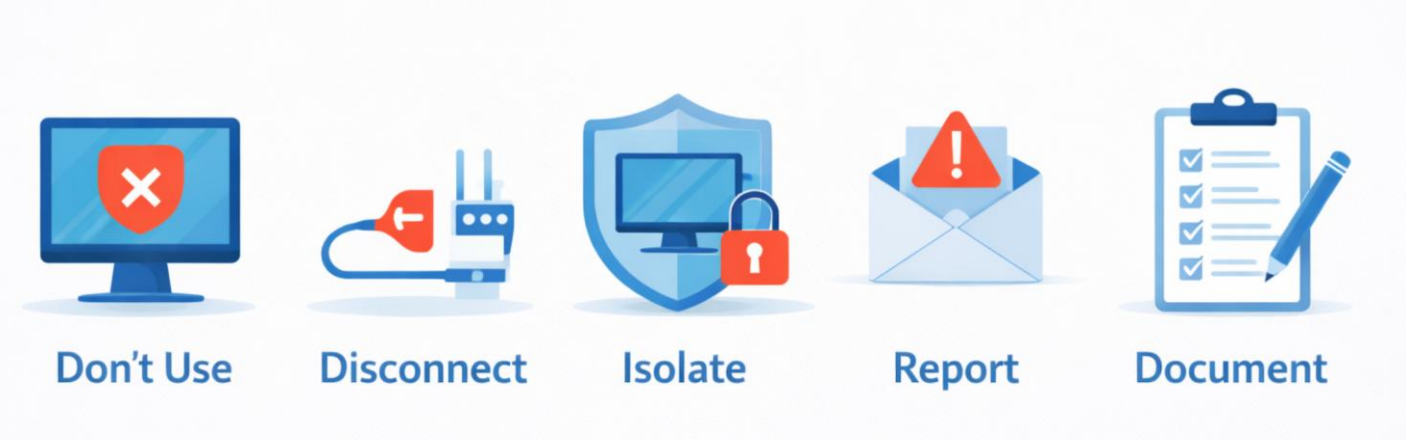
- Nepieejama uzņēmuma tīmekļvietne vai nav pieejas pie uzņēmuma tīkla resursiem
- Netipiska datora uzvedība (lēndarbība, dīvaini vai nesaprotami paziņojumi, antivīrusa programmatūra izdod dažādus brīdinājumus)
- Faili datorā ir nepieejami, vai arī tie neizskatās kā parasti
- Aizdomīgi e-pasti



Datu valsts inspekcija

Pirmās rīcības darbības datora incidenta gadījumā

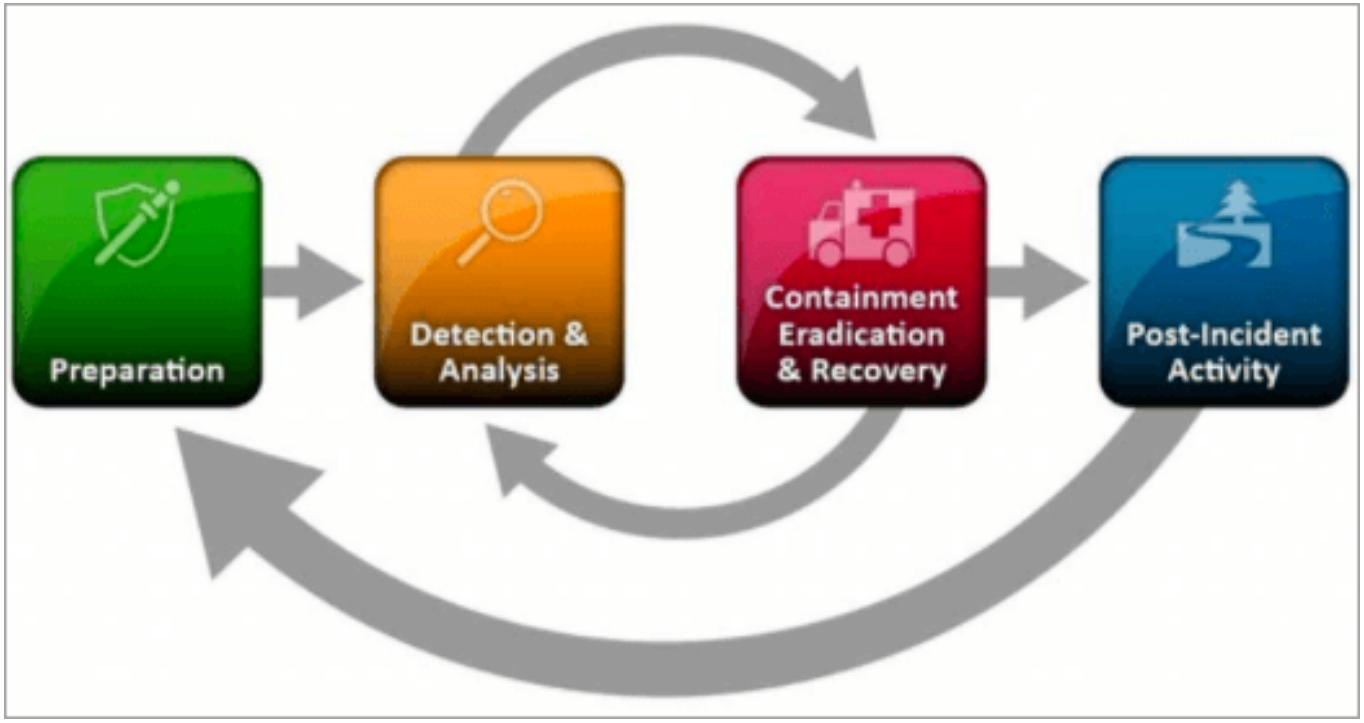
1. **Pārtraukt lietot inficēto ierīci**
2. **Atvienot no interneta / tīkliem**
3. **Neizslēgt ierīci (pierādījumi var pazust)**
4. **Ziņot atbildīgajam personālam**
5. **Fiksēt novēroto (laiks, ekrānuzņēmumi)**



Datu valsts inspekcija

Incidentu pārvaldība

Incidentu pārvaldība – Process, kas palīdz organizācijām identificēt, analizēt un ātri reaģēt uz drošības incidentiem, kas apdraud uzņēmuma informāciju un sistēmas. Tiek sekots līdzi iekšējo noteikumu ievērošanai.



Datu valsts inspekcija

Rokasgrāmata kiberincidentu gadījumiem

Rokasgrāmatā iekļauj šādas sadaļas:

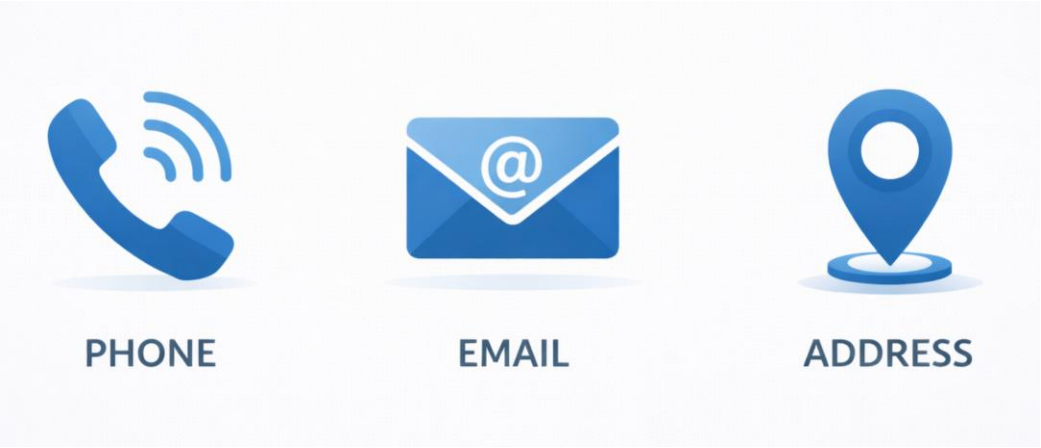
- Kontaktinformācija
- Paziņošanas kārtība
- Rīcības soļi incidentā
- Scenāriju apraksti (piem., nošifrēti dati)
- Datu dublējumu plāns
- Darbības pēc incidenta

Datu valsts inspekcija

Kontaktinformācija

Rokasgrāmatas sākumā definē:

- Atbildīgais uzņēmumā
- IT uzturētājs / pakalpojumu sniedzējs
- Vadība
- Uzraudzības iestādes (piem., DVI, CERT.LV u.c.)
- Ziņošanas kanāli (telefons, e-pasts)

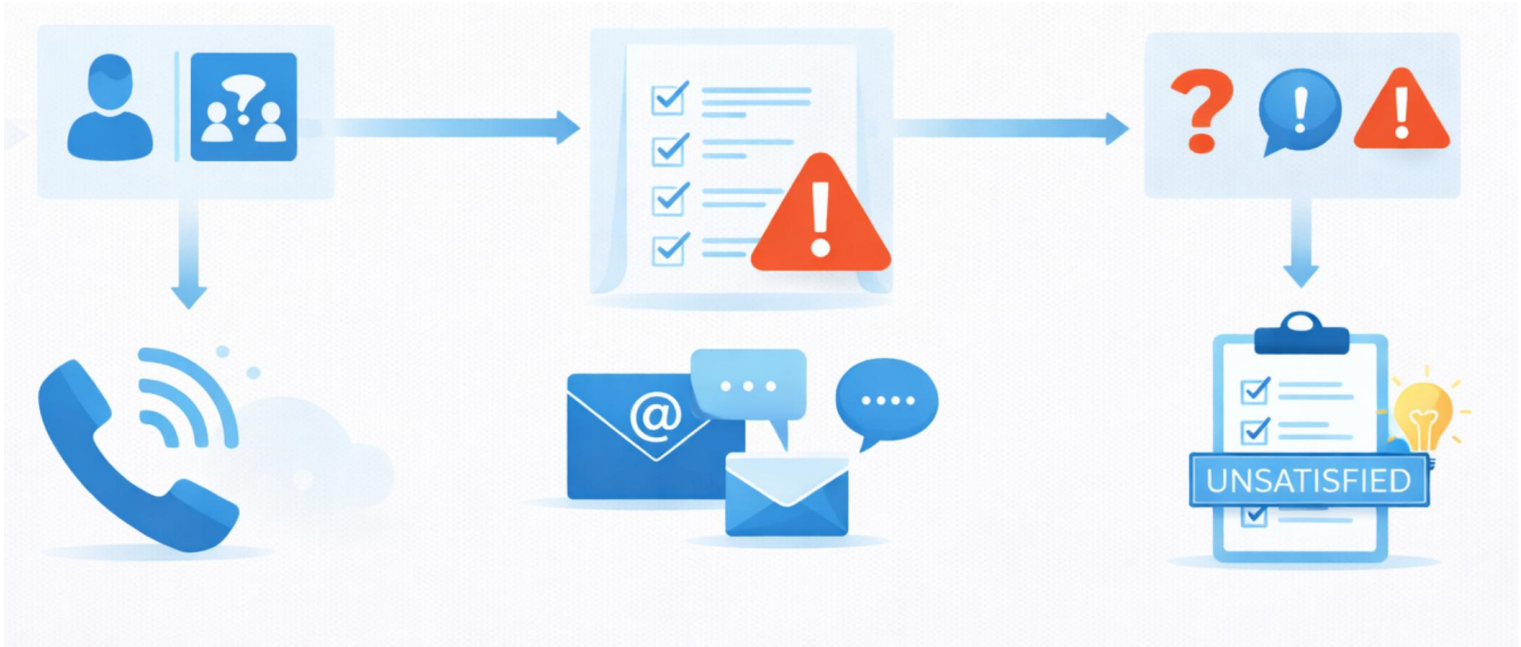


Datu valsts inspekcija

Paziņošanas kārtība

Rokasgrāmatā jābūt skaidram:

- Kam ziņo vispirms?
- Kāda informācija jāsniedz?
- Kādu kanālu lietot (tālr., e-pasts)?
- Kā rīkoties, ja atbildīgais nav sazvanāms?



Datu valsts inspekcija

Scenārijs A: Inficēts dators / izspiedējvīruss

Rīcība:

- Atvienot ierīci
- Informēt atbildīgo
- IT veic izolāciju
- Saglabā log failus
- Atjauno datus no dublējuma kopijām

Datu valsts inspekcija

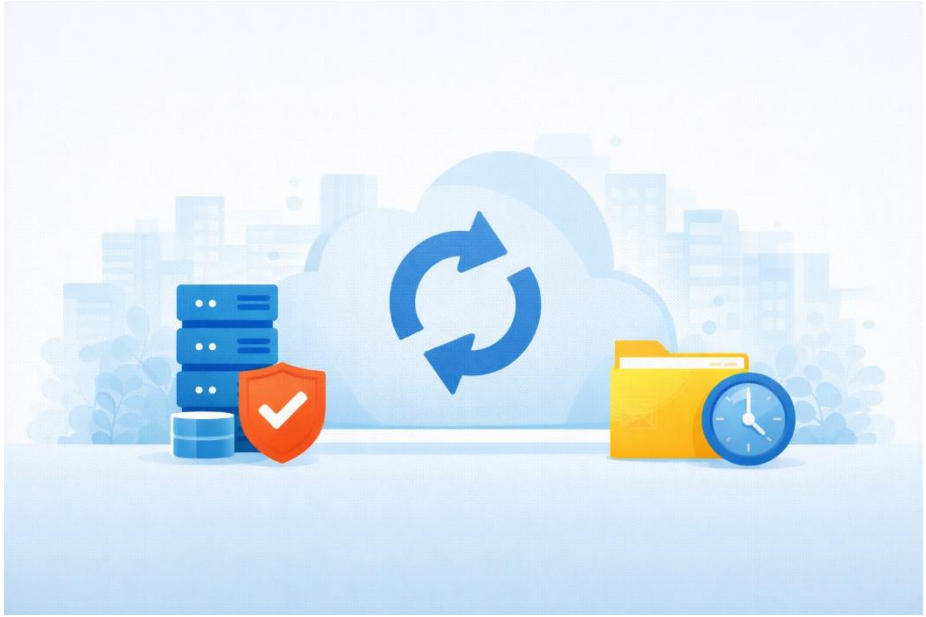
Scenārijs B: Uzlauzts e-pasts

Rīcība:

- Nekavējoties pārtraukt lietot kontu
- IT bloķē piekļuvi
- Pārbaudīt citus kontus
- Nomainīt paroles un ieslēgt MFA
- Ja nepieciešams, paziņot klientiem

Datu valsts inspekcija

Datu dublējumu plāns



Rokasgrāmatā nosaki:

- Kur glabājas dublējumi
- Cik bieži tie tiek veidoti
- Vai dublējumi ir pārbaudīti
- Kas atbild par atjaunošanu
- Vai ir ārējā (offline) rezerves kopija

Datu valsts inspekcija

Darbības pēc incidenta

- Pārliecināties par sistēmu normālu darbību
- Analizēt notikušo
- Izstrādāt mācības un uzlabojumus
- Apmācīt darbiniekus
- Veikt uzlabojumus rokasgrāmatā

Datu valsts inspekcija

Kam ziņot incidenta gadījumā

- **Datu valsts inspekcija** - ja incidenta rezultātā ir skarti Personas dati
- **CERT.LV** - kontakts kiberincidentu gadījumos
- **Valsts policija** - ja ir krāpšana vai finansiāli zaudējumi

Datu valsts inspekcija

Personas datu apstrādes aizsardzības pārkāpums

Kas ir Personas datu apstrādes aizsardzības pārkāpums?

- "Personas datu aizsardzības pārkāpums" ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem (Vispārīgā datu aizsardzības regula 4.pants 12.punkts).

Kad jāiesniedz Personas datu apstrādes aizsardzības pārkāpuma paziņojums?

- Personas datu aizsardzības pārkāpuma gadījumā datu pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā **72 stundu laikā** no brīža, kad pārkāpums tam kļuvis zināms iesniedz Personas datu apstrādes aizsardzības pārkāpuma paziņojumu.

Kad nav jāiesniedz Personas datu apstrādes aizsardzības pārkāpuma paziņojums?

- Datu pārzinis var neiesniegt Paziņojumu gadījumos, kad ir maz ticams, ka personas datu aizsardzības pārkāpums varētu radīt risku fizisku personu tiesībām un brīvībām.

Paziņojuma iesniegšana - https://pazinojums.dvi.gov.lv/

Datu valsts inspekcija

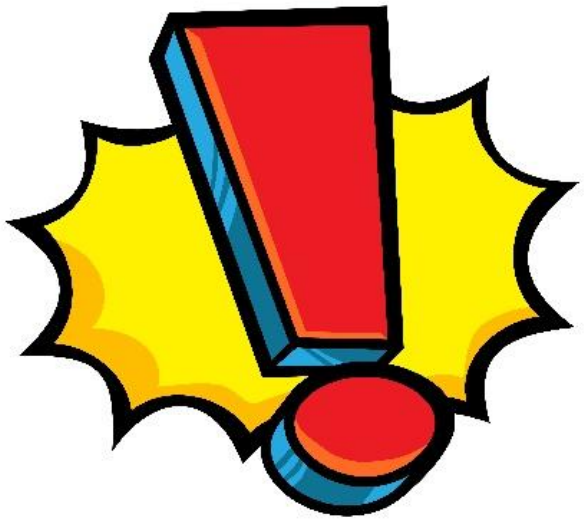
Biežākās kļūdas

- Ignorēt incidenta pazīmes
- Mēģināt pašiem “novērst” pirms ziņošanas
- Dzēst pierādījumus
- Restartēt ierīci nekavējoties
- Pāragra vai incidenta saturoša dublējuma atjaunošana no dublējuma kopijas

Datu valsts inspekcija

Galvenie pamatprincipi

- ✓ **Saglabāt mieru**
- ✓ **Informēt atbildīgos**
- ✓ **Neizslēgt, bet izolēt**
- ✓ **Dokumentēt visu**
- ✓ **Uzlabot rokasgrāmatu pēc katra incidenta**



Datu valsts inspekcija

Paldies par uzmanību!

Datu valsts inspekcija

Jānis – Janis.Kravcovs@dvi.gov.lv

pasts@dvi.gov.lv

www.dvi.gov.lv

Prezentācijā izmantoto attēlu avoti: Bing tiešsaistes krātuve, MI ģenerēti attēli.