Datu valsts inspekcija

Droša datu pārsūtīšana

Prevencijas nodaļas
Informācijas sistēmu drošības pārvaldnieks
Jānis Kravcovs

Datu valsts inspekcija

Failu pārsūtīšana un drošības izaicinājumi

- **Datu pārtveršana (Man-in-the-Middle)**
- **Nešifrētu datu pārsūtīšana**
- **Neautorizētas piekļuves iespēju (failu koplietošanas gadījumā)**
- **Zemais drošības līmenis publiskajos Wi-Fi tīklos**
- **Cilvēciskais faktors**

Datu valsts inspekcija

Pamatprincipi

Personas datu aizsardzības prasības attiecas arī uz failu pārsūtīšanas procesiem. Atbilstoši Datu Regulas prasībām, failu pārsūtīšanas procesam, kurā iesaistīti personas dati, ir jānotiek tādā veidā, kas nodrošina:

Datu konfidencialitāti – tikai pilnvarotām personām ir piekļuve datiem

Datu integritāti – dati netiek mainīti pārsūtīšanas laikā

Datu pieejamību – pilnvarotām personām ir iespēja piekļūt datiem, kad tas ir nepieciešams

Datu valsts inspekcija

Datu glabāšana mākoņpakalpojumā

Dati fiziski neatrodas konkrētā uzņēmuma telpās vai ierīcēs, kas var radīt paaugstinātus datu drošības riskus:

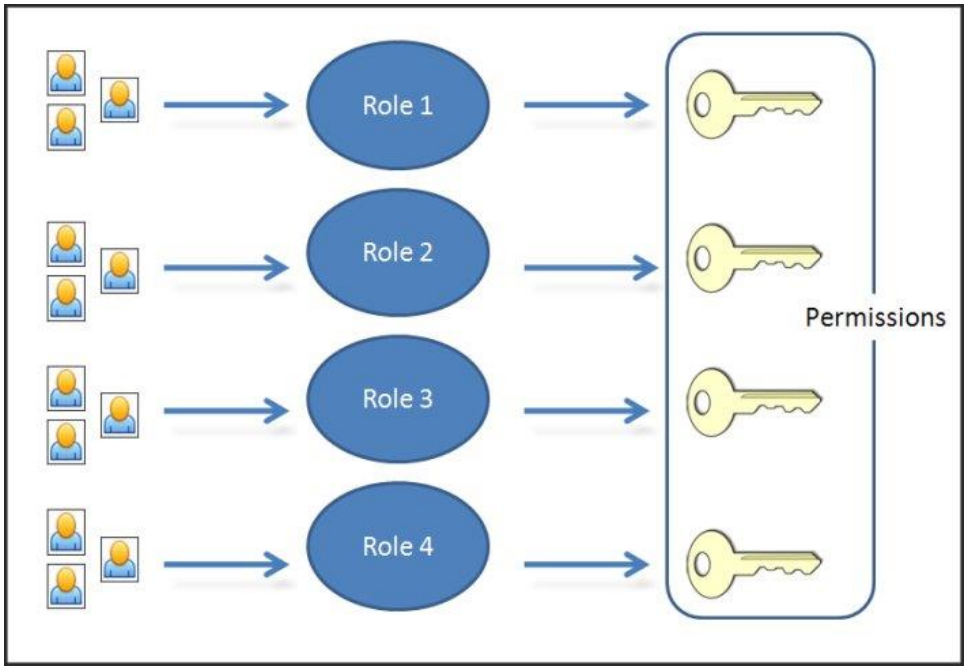
- Pārliecināties par reputāciju
- Datu apstrādes un aizsardzības riska līmenis ir atbilstošs Eiropas Savienības normatīvajam regulējumam
- Atbilstība sertifikācijai (ISO 27001)
- Pilna kontrole pār datiem un iespēja noteikt piekļuves tiesības
- Dati tiek glabāti Eiropas Savienībā
- Tehniskā atbalsta pieejamība
- Neatgriezeniska datu dzēšana, izbeidzot līgumattiecības

Datu valsts inspekcija

Piekļuves tiesību piešķiršana failu koplietošanas pakalpojumos

Katram, kas iesaistīts datu koplietošanā, jābūt piekļuves līmeņiem, kas ierobežo failu rediģēšanu vai koplietošanu, vai pat tā lejupielādi. Koplietojot failus var būt arī pielietota to papildus šifrēšana.

- Ievēro principu – minimālais piekļuves tiesību apjoms.

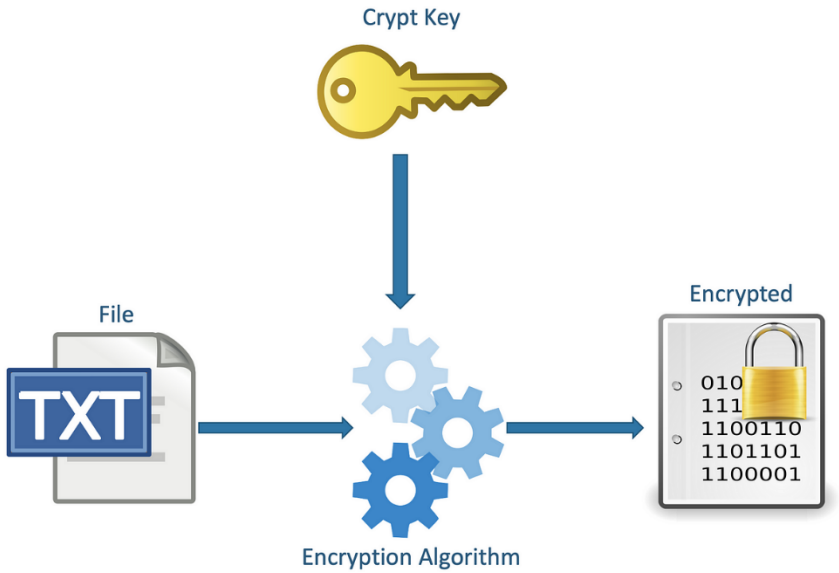


Datu valsts inspekcija

Droša datu pārsūtīšana

Augsti riski pastāv gadījumos, kad personas dati tiek pārsūtīti, piemēram, izmantojot elektronisko pastu:

- Izstrādāta droša informācijas pārsūtīšanas procedūra
- Pārsūtītie personas dati tiek šifrēti



Datu valsts inspekcija

E-pasta šifrēšana

E-pasta šifrēšana ir process, kurā e-pasta saturs tiek pārveidots dažādu simbolu un burtu virknējumā, kas nav lasāmi personām bez atbilstošas atslēgas vai piekļuves tiesībām. Pastāv divi galvenie šifrēšanas veidi:

- **Transporta līmeņa šifrēšana** (Transport Layer Security - TLS)

- **End-to-end šifrēšana** (E2EE) - **PGP** (Pretty Good Privacy) un **S/MIME** (Secure/Multipurpose Internet Mail Extensions

Datu valsts inspekcija

Office 365 un e-pasta šifrēšana

Bez iepriekš uzskaitītā, Office 365 nodrošina savu iebūvētu e-pasta šifrēšanas funkcionalitāti. Šo funkcionalitāti nodrošina *Microsoft Information Protection* risinājums

Office Message Encryption (OME) - risinājums, kas nodrošina elastīgu un lietotājam draudzīgu e-pasta šifrēšanu. Tas šifrē ziņojumus tā, lai saņēmēji varētu tiem piekļūt neatkarīgi no izmantotā e-pasta pakalpojuma (piemēram, Gmail.com, Inbox.lv, u.c.). Galvenās **OME** funkcijas ietver:

- **Integrācija ar Outlook**: Lietotāji var viegli pievienot šifrēšanas funkciju Outlook vidē, izvēloties opciju šifrēt ziņojumu vai izmantot sagatavotus drošības noteikumus, kas automātiski piemēro šifrēšanu.
- **Lietotāju autentifikācija**: Pirms šifrētā e-pasta satura piekļuves saņēmējiem ja viņš neietilpst organizācijas struktūrā, ir jāautentificējas, piemēram, izmantojot **vienreizēju kodu** vai **Microsoft kontu**. Tas nodrošina, ka informācija ir pieejama tikai pilnvarotiem saņēmējiem.
- **Nosacījumu politika un aizsardzības iestatījumi**: Office 365 organizācijas administrators var izveidot pielāgotus drošības noteikumus, un pamatojoties uz noteiktiem atslēgvārdiem vai klasifikācijas tagiem, automātiski piemēro šifrēšanu e-pastiem ar sensitīvu saturu, piemēram, finanšu vai veselības datiem.

Datu valsts inspekcija

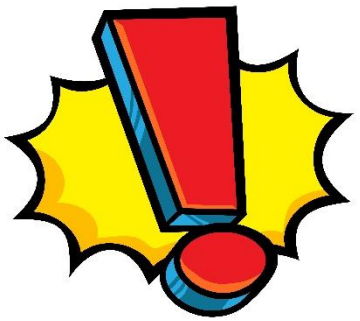
Der atcerēties!!!

Ja adresātam tiek sūtīts šifrēts e-pasts, tad papildus nosūtītajam šifrētam e-pastam ir nepieciešams nosūtīt nešifrētu e-pastu ar sekojošu informāciju:

- Izskaidrot, ka iepriekš tika nosūtīts šifrēts e-pasts (ja iepriekš nevienojāties).
- Soli pa solim izskaidrot, kā veikt e-pasta atšifrēšanu.

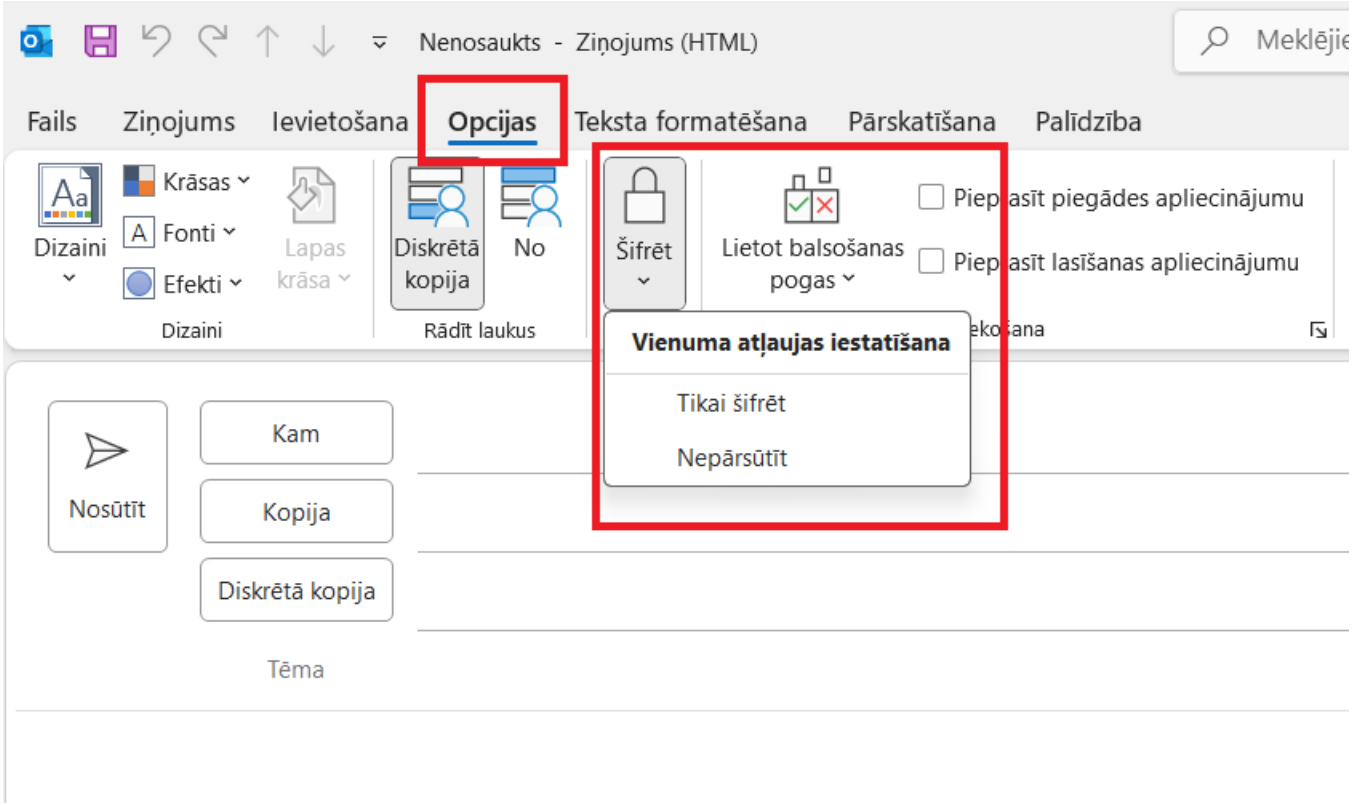
Ja adresātam tiek sūtīts e-pasts ar šifrētu pielikumu, tad papildus šajā e-pastā nepieciešams norādīt sekojošu informāciju:

- Par to, ka e-pasts satur šifrētu pielikumu.
- Ja iepriekš neesat vienojušies par atšifrēšanas paroli, tad būtu nepieciešam lietot tādu šifrēšanas kuru zina tikai saņēmējs.
- Vai arī atšifrēšanas paroli nosūtīt pa citu saziņas kanālu.



Datu valsts inspekcija

Kā sākt e-pasta šifrēšanu

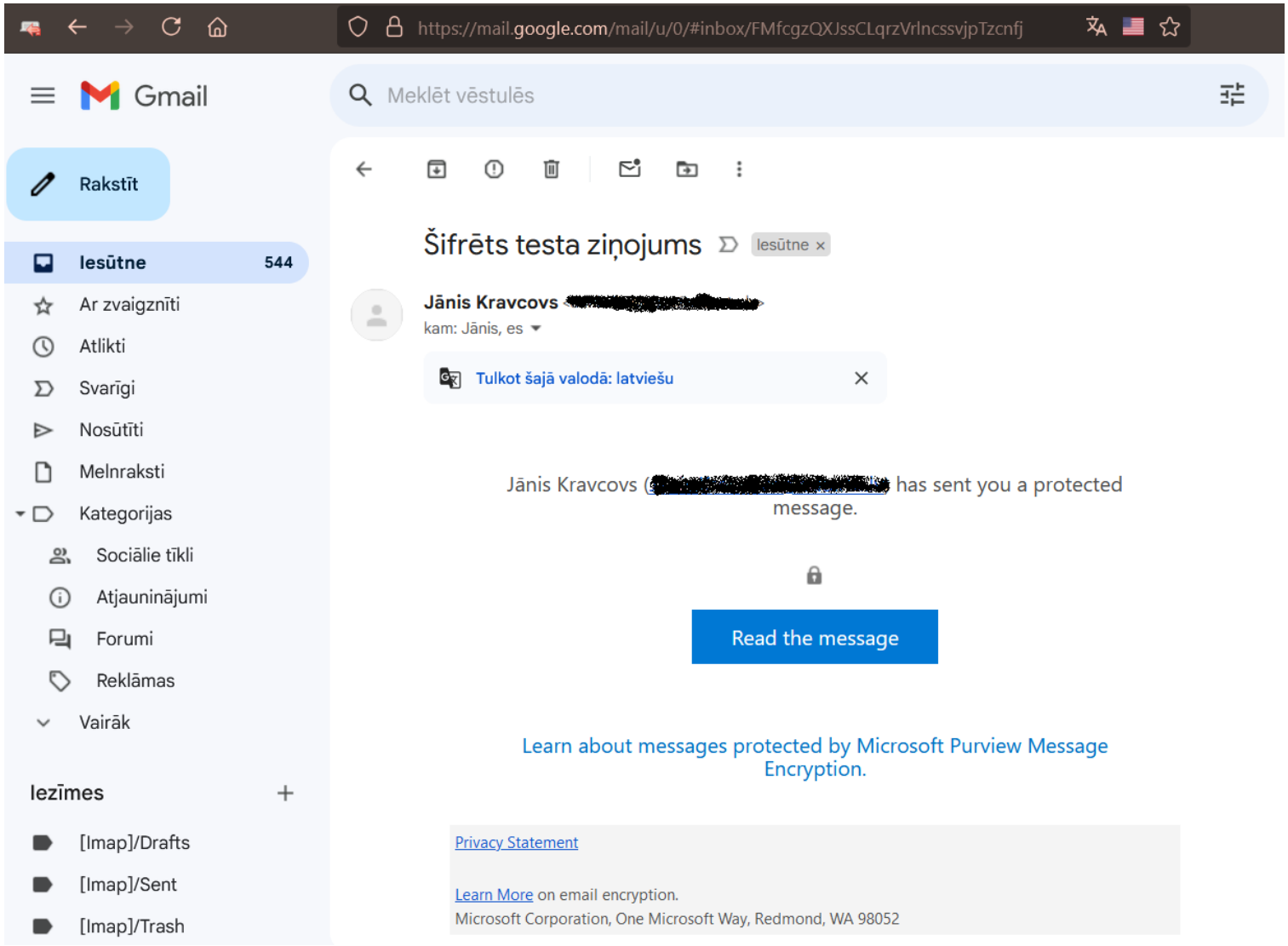


Tikai šifrēt (Encrypt Only) – Nošifrē dokumentu un tā pielikumus

Nepārsūtīt (Do Not Forward) – Nošifrē dokumentu un tā pielikumus, kā arī neļauj pārsūtīt un kopēt e-pasta saturu

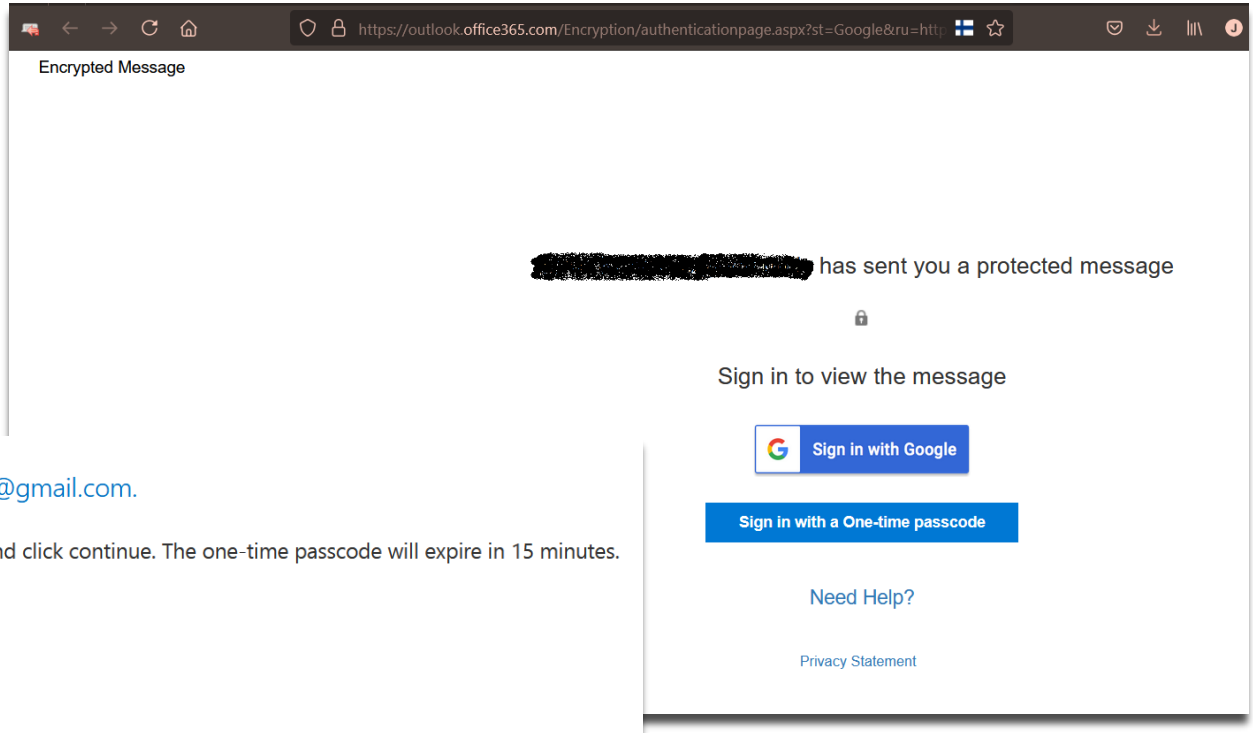
Datu valsts inspekcija

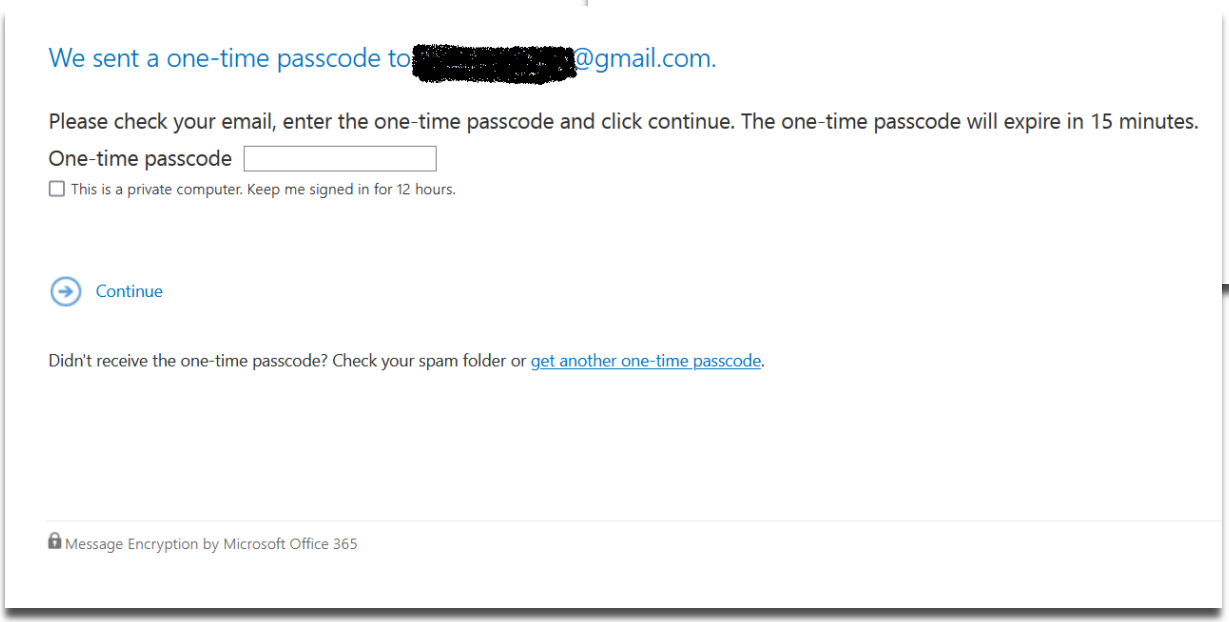
Ko redz saņēmējs ārpus organizācijas



Datu valsts inspekcija

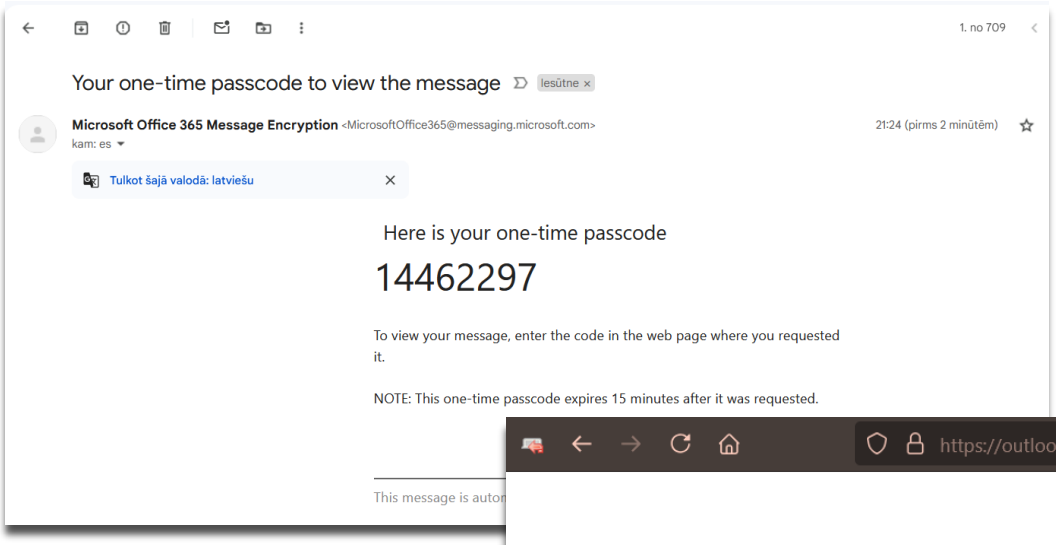
Ko redz saņēmējs ārpus organizācijas

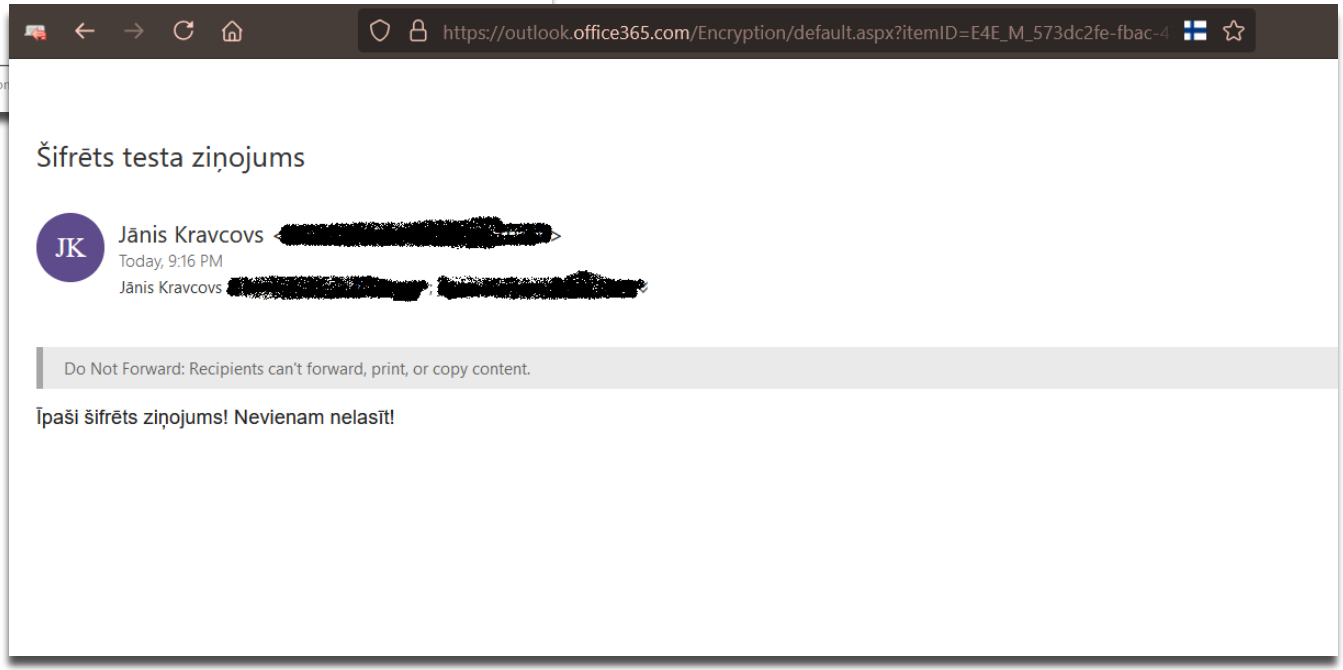




Datu valsts inspekcija

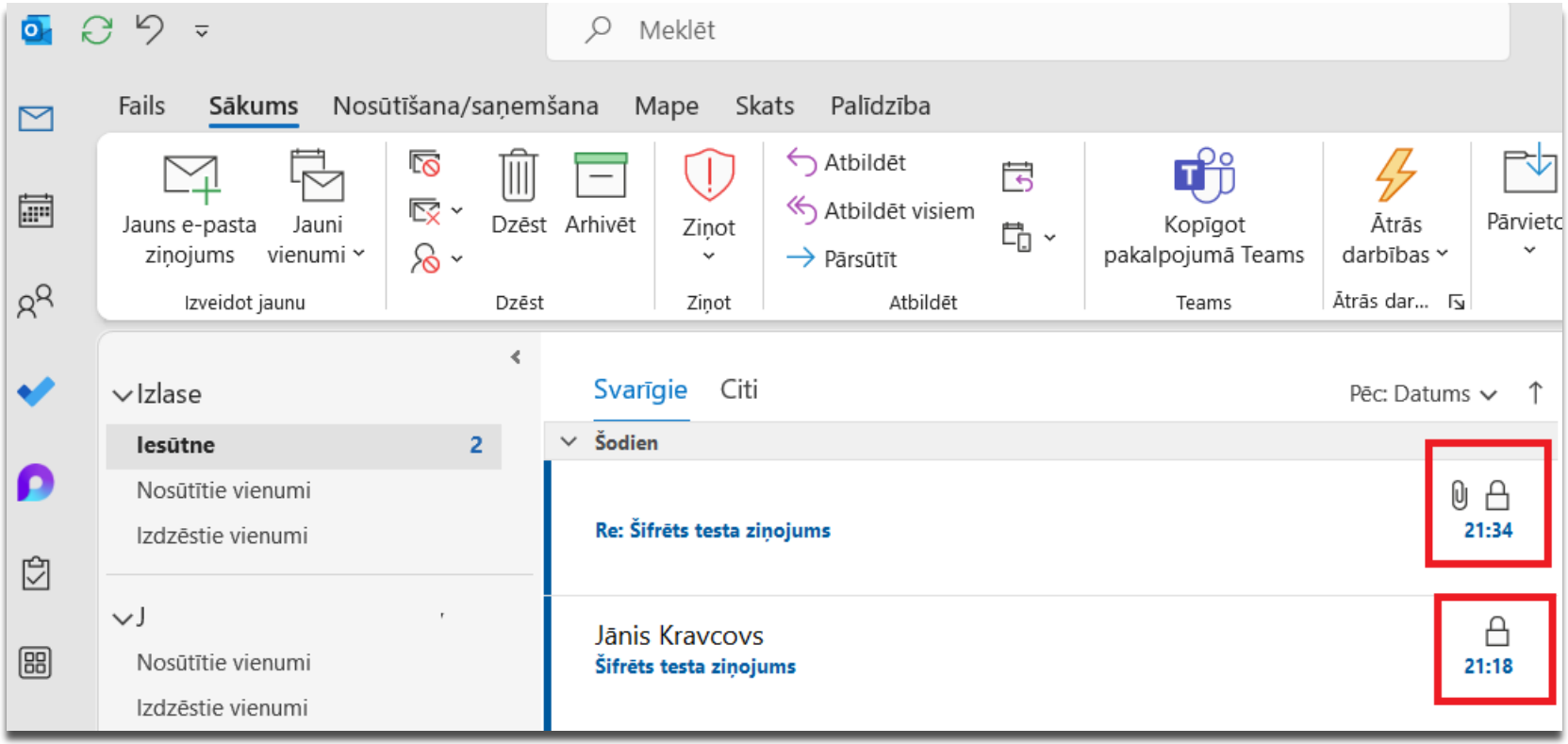
Ko redz saņēmējs ārpus organizācijas





Datu valsts inspekcija

Šifrēta e-pasta atzīme iekš Outlook



Turpinot iesāktā e-pasta saraksti, sūtot atbildes e-pastus (Reply), visi e-pasti, sarakstes ietvaros, tiek sūtīti izmantojot šifrēšanu.

Datu valsts inspekcija

Drošas pielikumu nosūtīšanas metodes

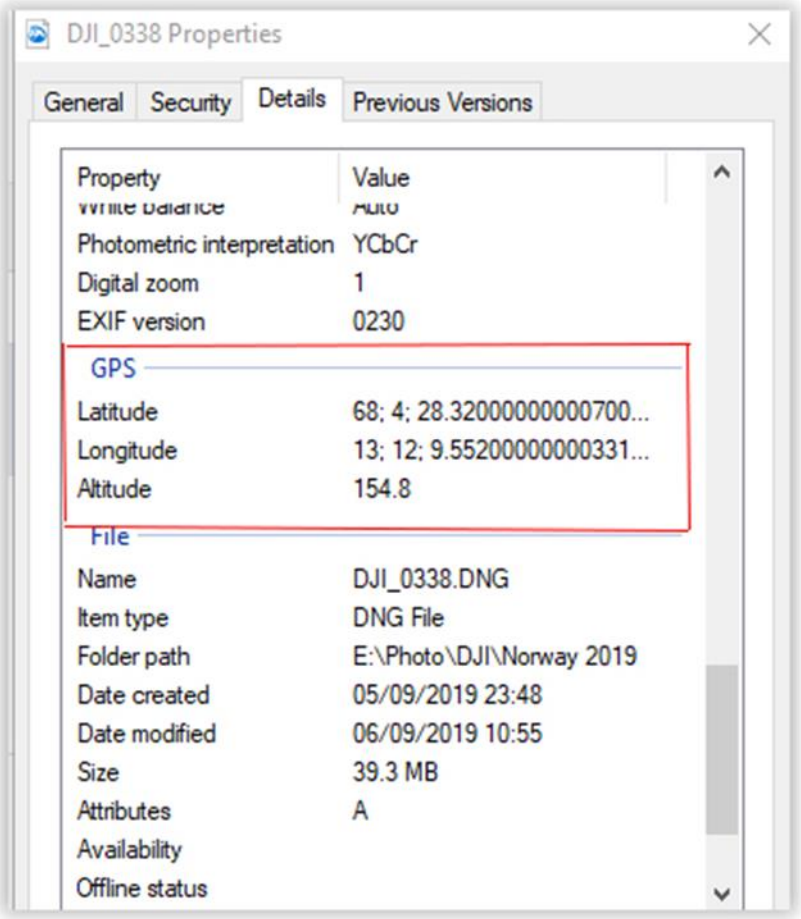
Papildus e-pasta šifrēšanai ir būtiski nodrošināt pielikumu drošību. Failu pielikumu aizsardzība ir īpaši svarīga, ja tie satur personu datus

- **Aizsargāti dokumenti:** Failos, kuros ietverts aizsargājams saturs, var aizsargāt ar paroli vai pielietot šifrēšanas rīkus kurus atbalsta dažādas arhivēšanas programmas, piemēram, 7-ZIP. Microsoft Word un Excel ir iespējams iestatīt dokumenta šifrēšanu un piekļuves paroli.
- **Failu pārbaude pirms koplietošanas:** Pirms pielikuma nosūtīšanas ieteicams pārbaudīt:
  - vai izvēlētais koplietojamais fails ir saņēmējam adresējams
  - vai fails nesatur konfidenciālu informāciju, kas nav nepieciešama sūtīšanas nolūkam. Piemēram, ir iespējams noņemt metadatus un citus ierakstus, kas varētu būt nevajadzīgi vai riskanti.

Datu valsts inspekcija

Metadati failos

- **Informācija ar GPS koordinātēm**
- **Ar kādu ierīci uzņemts foto**
- **Dokumenta autora vārds un uzvārds**
- **Dokumenta autora e-pasts**
- **Dokumenta autora telefona numurs**



Datu valsts inspekcija

Datu noplūdes riski valsts iestādēs

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

Datu subjekta anketas publiskošana tīmekļa vietnē

Iestādes darbinieks tukšas PDF formas vietā publiski izvietoja formu tīmekļa vietnē, kuru iepriekš bija aizpildījis datu subjekts. PDF forma saturēja identifikācijas datus, proti, kontaktinformāciju (e-pastu), adresi, personas kodu, datus par personu apliecinošu dokumentu, dzimšanas datus un informāciju par dzimumu.

Līdz pārkāpuma konstatēšanas brīdim, minētā PDF datne tika lejupielādēta 46 reizes.

Par minēto pārkāpumu tika informēts datu subjekts.

Datu valsts inspekcija

Datu subjekta anketas publiskošana tīmekļa vietnē

Iestādes veiktās darbības:

- **uzlaboti darba procesi, lai nepieļautu līdzīgu pārkāpumu izveidošanos nākotnē**
- **ieviests priekšskatījums ikvienai informācijas vienībai, kura paredzēta publiskošanai**
- **izstrādātas vadlīnijas darbiniekiem**

Datu valsts inspekcija

Komisijas locekļu pieteikuma anketas publiskošana tīmekļa vietnē

Noplūdusi komisijas locekļa pieteikuma anketa no informācijas sistēmas, jo darbinieka cilvēciskas kļūdas dēļ netika atzīmēta ierobežotas piekļuves informācijas atzīme noteiktajam pielikumam. Skartie dati: vārds, uzvārds, personas kods, izglītība, latviešu valodas prasme, dzīves vietas adrese, tālrunis, darba vieta.

Skarto datu subjektu skaits: **11**

Informāciju par datu noplūdi iestāde saņēma no skartiem datu subjektiem.

Datu valsts inspekcija

Komisijas locekļu pieteikuma anketas publiskošana tīmekļa vietnē

Iestādes veiktās darbības:

- **Nekavējoties tika veiktas nepieciešamās darbības, lai pārtrauktu skarto datu subjektu publiskošanu**
- **Pārrunas ar darbinieku par informācijas drošību**

Datu valsts inspekcija

E-pasts, kura pielikums saturēja datu subjekta datus tika nosūtīts citai personai

Darbinieks neuzmanības kļūdas rezultātā nosūtīja e-pastu ar pielikumu citam adresātam. Pielikumā bija administratīvais lēmums par administratīvā akta izdošanas termiņa pagarināšanu.

Skartie dati: vārds, uzvārds, personas kods, kontaktinformācija.

Skarto datu subjektu skaits: **1**

Faktu konstatēja darbinieks, kurš nosūtīja e-pastu.

Par minēto pārkāpumu tika informēts datu subjekts.

Datu valsts inspekcija

E-pasts, kura pielikums saturēja datu subjekta datus tika nosūtīts citai personai

Iestādes veiktās darbības:

- **Veicot iekšējo izmeklēšanu par notikušo un novērtējot iespējamību, ka cilvēkfaktors varētu atkārtoties, pārzinis ir pieņēmis lēmumu, ka darbiniekiem tiks organizētas ne tikai ikgadējās apmācības datu aizsardzībā, bet periodiski tiks organizētas apmācības īsākā un detalizētākā veidā tieši par datu aizsardzības pārkāpumiem, lai vērstu darbinieku uzmanību uz dažādām situācijām, kas ikdienā var notikt.**

Datu valsts inspekcija

Vienotās pieteikšanās modulis - autentifikācija

Vienotās pieteikšanās modulis (turpmāk - VPM) kļūdainas darbības rezultātā, gadījumos, kad lietotāji vienlaicīgi (milisekudes ietvaros) veicot vienlaicīgu autentifikāciju, VPM izsauktajam portālam atgrieza otra lietotāja autentifikācijas rekvizītus. Tādejādi 1.5 mēneša periodā 129 personas dažādos portālos autentificējās ar cita lietotāja rekvizītiem.

Tehnoloģiska kļūda, pieļauta izstrādes (programmēšanas) gaitā, kļūdas novēršanai tika piesaistīts Vienotās pieteikšanās moduļa uzturētājās

Skarto datu subjektu skaits: **129**

Datu valsts inspekcija

Vienotās pieteikšanās modulis - autentifikācija

Iestādes veiktās darbības:

- **Tika piesaistīts TVP moduļa uzturētās, lai nepieļautu šādas turamākās darbības**
- **Tika apzināts visas iestādes kuras TVP autentifikācijas modulī izmato citu Drošības talonā atribūtu, nekā to kurš minēts dokumentācijā**

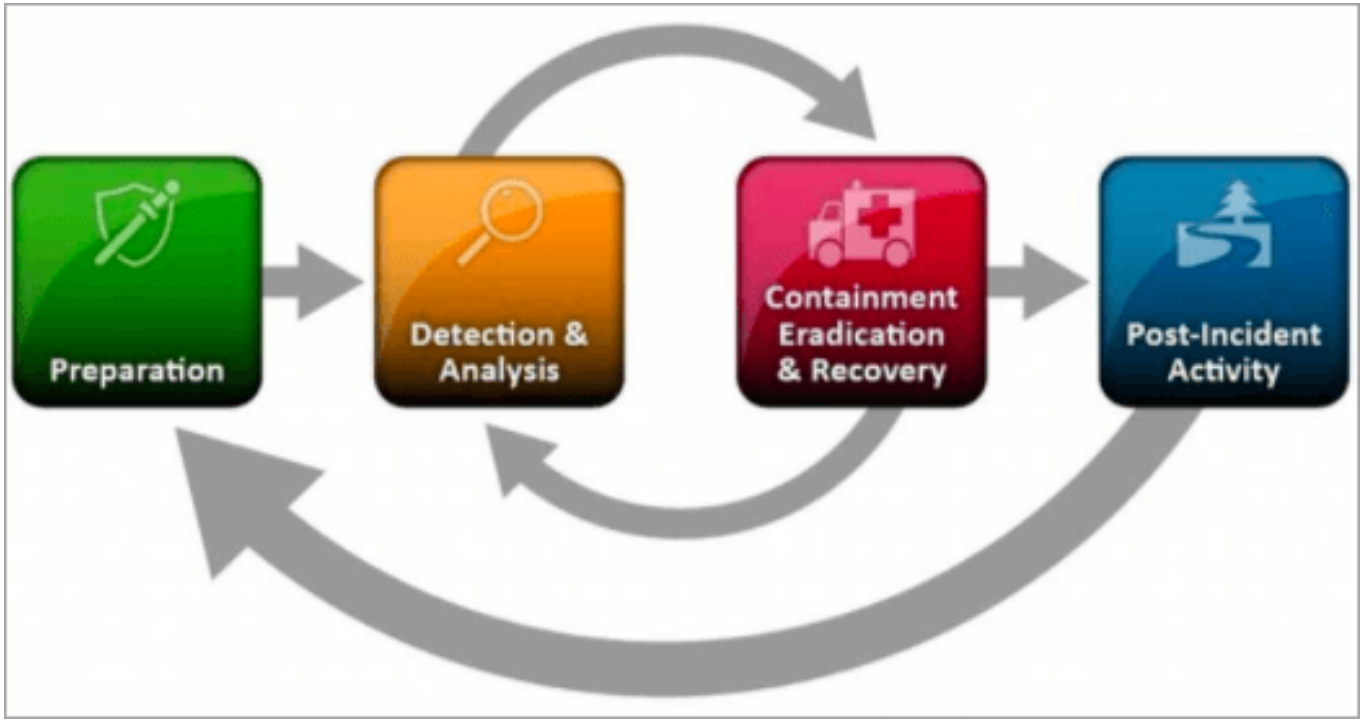
Datu valsts inspekcija

Incidentu pārvaldība un ātra reaģēšana uz drošības pārkāpumiem

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

Sagatavošanās fāze

- Rīku un resursu sagatavošana
- Komandas apmācība
- Komunikācijas un eskalācijas plāns

Datu valsts inspekcija

Incidenta noteikšana un analīze

- Nepārtraukta sistēmu uzraudzīšana
- Tehnoloģiju izmantošana
- Incidenta analīze

Datu valsts inspekcija

Ierobežošana, izskaušana un atgūšana

- Ierobežošanas darbības
- Ļaunatūras izskaušana
- Atjaunošana un pārbaude

Datu valsts inspekcija

Darbības pēc incidenta un mācības nākotnei

- Analīze un mācības
- Drošības uzlabojumi
- Atskaites un ziņošana
- Apmācības un simulācijas

Datu valsts inspekcija

Jautājumi?

Datu valsts inspekcija

Paldies par uzmanību!

Prezentācijā izmantoto attēlu avoti: Bing tiešsaistes krātuve, DVI attēlu arhīvs.