Cik kiberdrošas ir Latvijas pašvaldības? Pētījuma rezultāti.

Kaspars Iesalnieks

2019. gada 3. oktobris

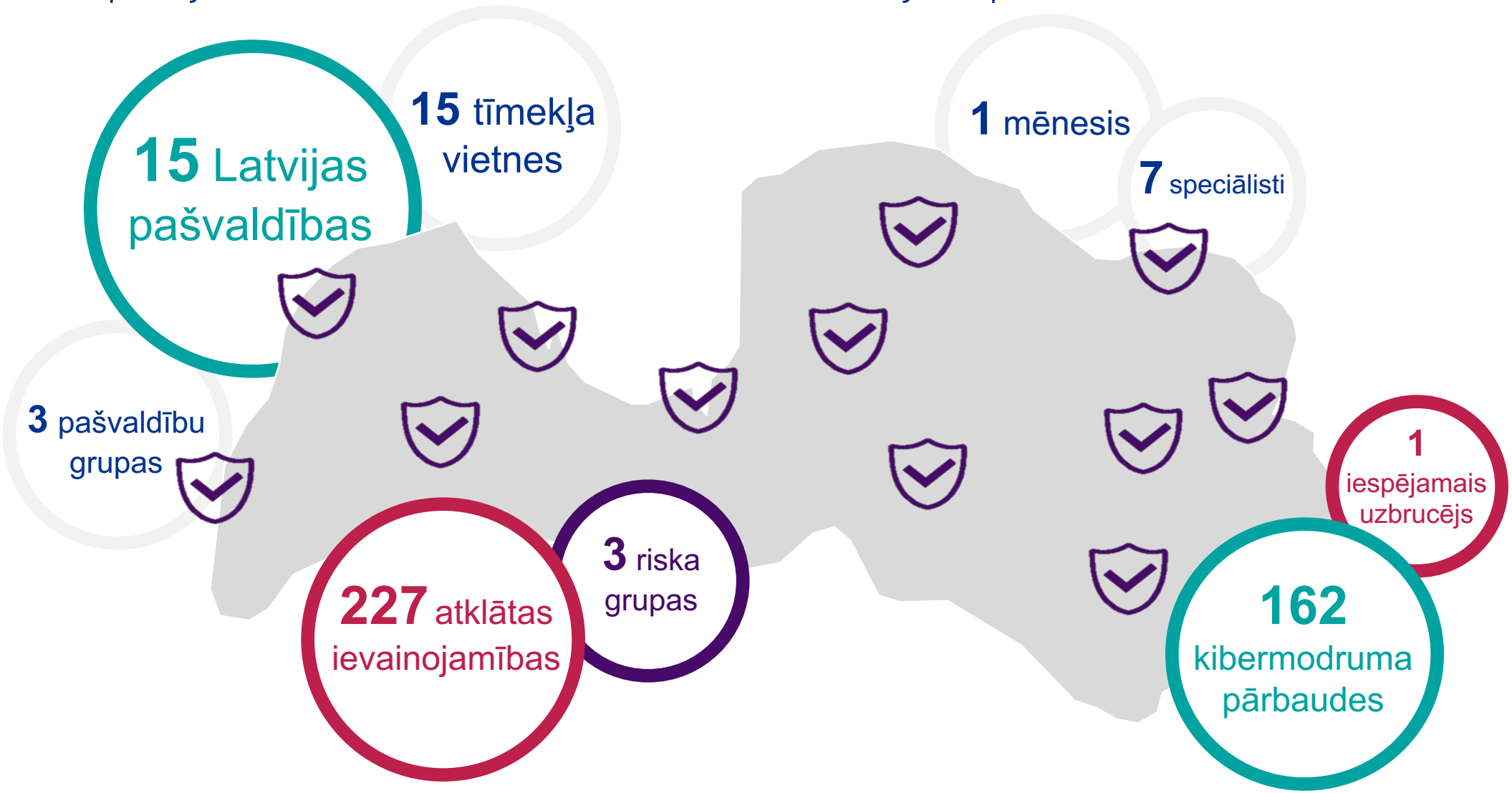
Iniciatīvas autors un izpildītājs:

Partneri:

LATVIJAS PAŠVALDĪBU SAVIENĪBA

Vides aizsardzības un reģionālās attīstības ministrija

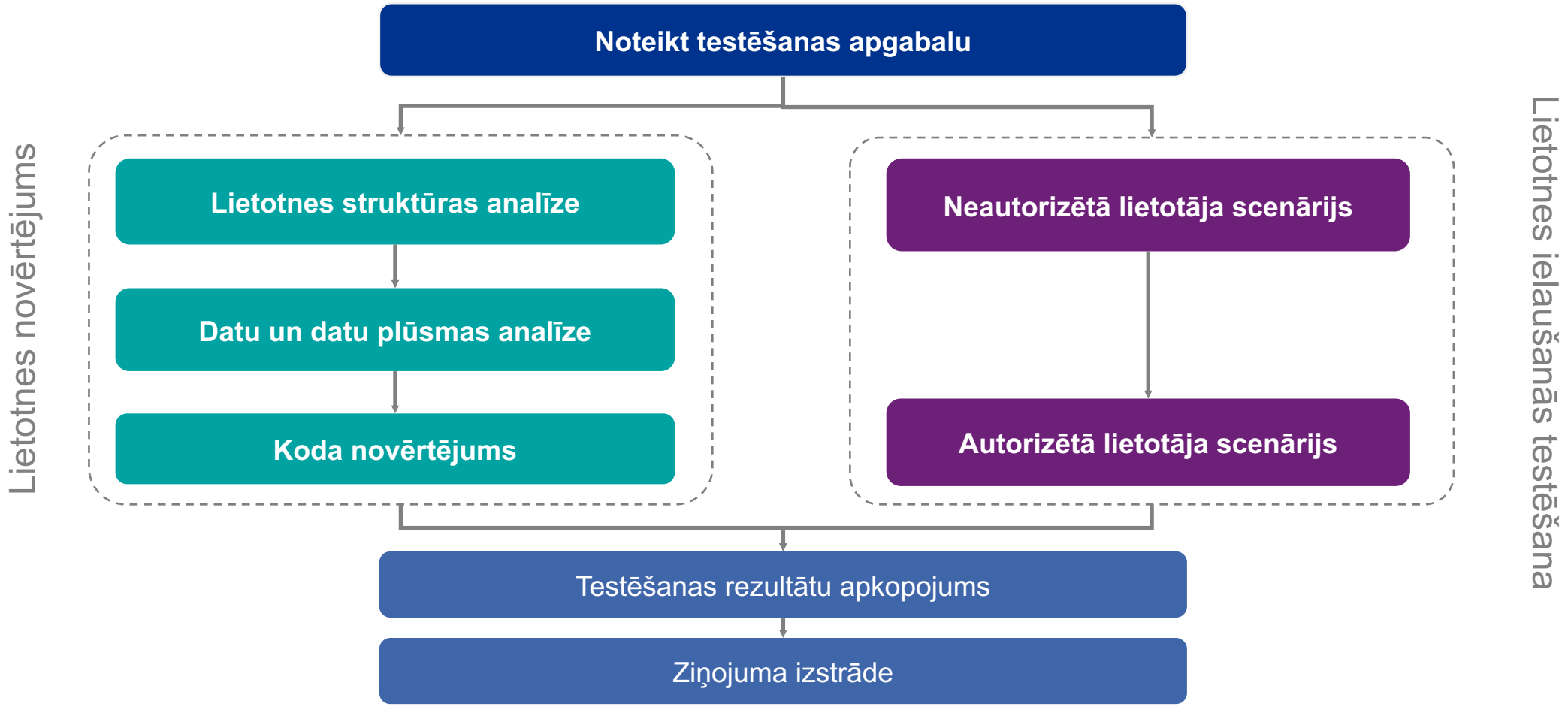
Par projektu: "Cik kiberdrošas ir Latvijas pašvaldības?"



KPMG

Mājaslapu kiberdrošības novērtējuma rezultāti

Pieeja mājaslapu novērtējumam balstoties uz OWASP rekomendācijām



Mājaslapu kiberdrošības novērtējumā izmantotie rīki

Pasīvā testēšana

Atvērtā pirmkoda informācijas vākšanas rīki:

dig, nslookup for DNS exploration

FOCA

whois

GHDB, tīmekļa meklēšanas servisi un arhīvi

Pasīvie tīkla analīzes rīki: tcpdump wireshark

Mājaslapu kiberdrošības novērtējumā izmantotie rīki

Pasīvā testēšana

Atvērtā pirmkoda informācijas vākšanas rīki:

dig, nslookup for DNS exploration FOCA

whois GHDB, tīmekļa meklēšanas servisi un arhīvi

Pasīvie tīkla analīzes rīki: tcpdump wireshark

Ievainojamību novērtēšana

Servisu skenēšanas rīki:

Nessus Metasploit Framework 3 Nexpose Netcat nikto

Fuzzers – jaunu ievainojamību atklāšanas rīki:

peach Taof Scapy

Mājaslapu kiberdrošības novērtējumā izmantotie rīki

Pasīvā testēšana

Atvērtā pirmkoda informācijas vākšanas rīki:

dig, nslookup for DNS exploration FOCA

whois GHDB, tīmekļa meklēšanas servisi un arhīvi

Pasīvie tīkla analīzes rīki: tcpdump wireshark

Ievainojamību novērtēšana

Servisu skenēšanas rīki:

Nessus Metasploit Framework 3 Nexpose Netcat nikto

Fuzzers – jaunu ievainojamību atklāšanas rīki:

peach Taof Scapy

Tīkla testēšana

Dažādi skripti dažādu tīklu testēšanai:

TCP servisiem NFS un SMB servisi

UDP servisiem Attālinātās piekļuves programmatūra

Tīkla kartēšana / pakešu vākšanas rīki:

Scapy Hping3 snoop, Esniff DSNIFF tcpdump, etherfind

Network Instruments' Observer NMAP ping, sping, probe

traceroute unicornsan

Mājaslapu kiberdrošības novērtējumā izmantotie rīki

Pasīvā testēšana

Atvērtā pirmkoda informācijas vākšanas rīki:

dig, nslookup for DNS exploration FOCA

whois GHDB, tīmekļa meklēšanas servisi un arhīvi

Pasīvie tīkla analīzes rīki: tcpdump wireshark

Ievainojamību novērtēšana

Servisu skenēšanas rīki:

Nessus Metasploit Framework 3 Nexpose Netcat nikto

Fuzzers – jaunu ievainojamību atklāšanas rīki:

peach Taof Scapy

Tīkla testēšana

Dažādi skripti dažādu tīklu testēšanai:

TCP servisiem NFS un SMB servisi

UDP servisiem Attālinātās piekļuves programmatūra

Tīkla kartēšana / pakešu vākšanas rīki:

Scapy Hping3 snoop, Esniff DSNIFF tcpdump, etherfind

Network Instruments' Observer NMAP ping, sping, probe

traceroute unicornsan

Scenāriju testēšana

Paroļu uzlaušana:

John the Ripper Cain and Abel rainbow tables, Ophcrack CeWL

Web: Accunetix Internet Explorer - ActiveX un Silverlight testēšanai

Burp Suite Pro Firefox ar drošības testēšanas paplašinājumiem

SSL: Nessus SSL plugins Ssldump SSLStrip, THCSSLCheck

Tīkla testēšanas rīki: Iodide DNS viltošanas rīki

Scapy Immunity CANVAS Metasploit Framework SYN plūdu rīki

Bailiwicked – DNS cache inficēšana TCP pakešu secības uzbrukumu rīki

IP viltošanas rīki Avota maršrutizēšana / datu plūsmas pāradresācija

227 IEVAINOJAMĪBAS

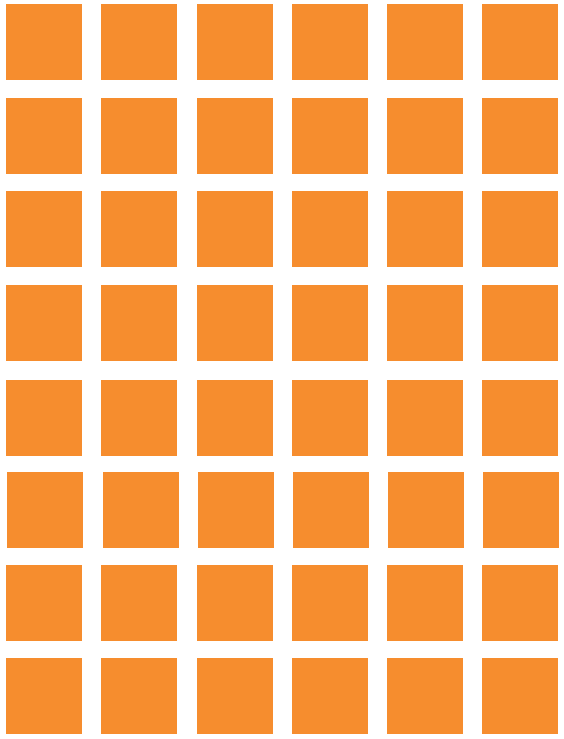
- Ievainojamības tika atklātas visās 15 pašvaldību mājas lapās
- Vairāku zema vai vidēja līmeņa ievainojamību vienlaicīga pastāvēšana var radīt jau nopietnāku vietnes drošības apdraudējumu.

Atklāto ievainojamību riska līmenis

6% augsts

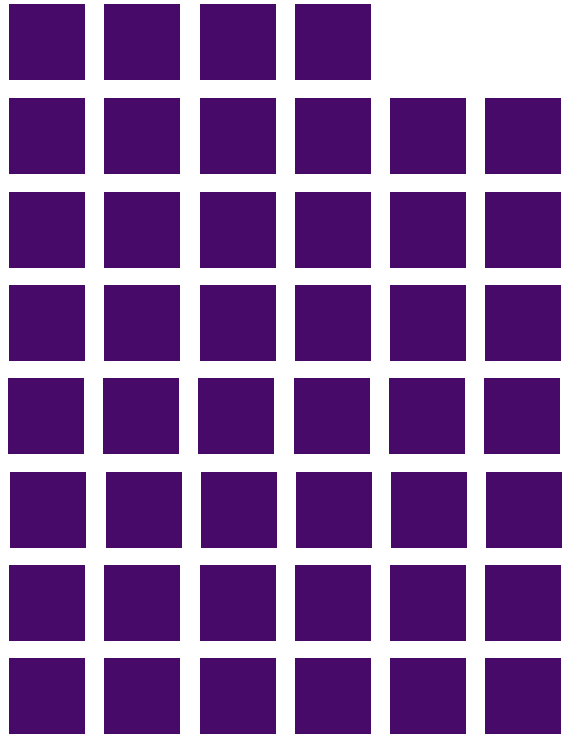
10 no 15 pašvaldībās

48% vidējs



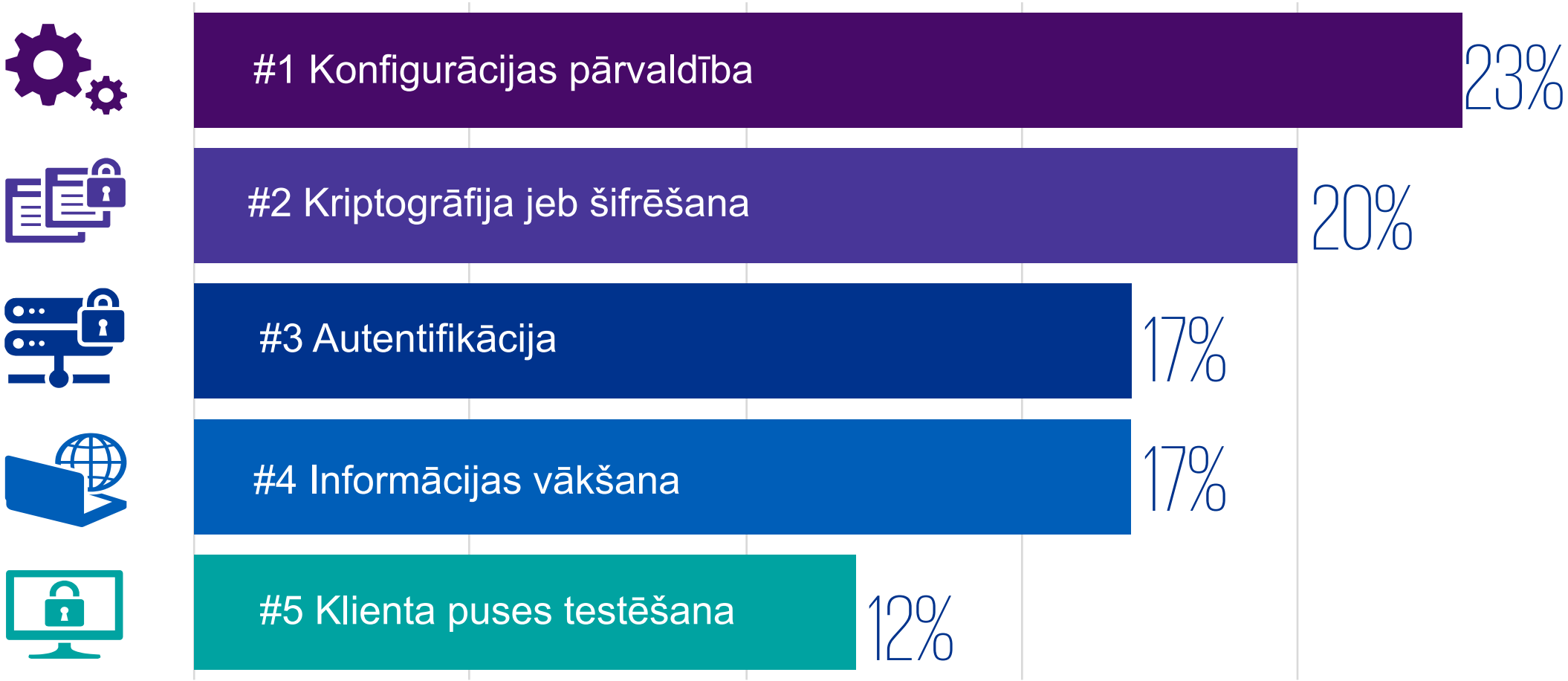
Visās pašvaldībās

46% zems



Visās pašvaldībās

Izplatītāko ievainojamību tops



KPMG

Piemērs #1

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Pastāv risks, ka sistēmai ir nevajadzīgi liela uzbrukuma virsma.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Pastāv risks, ka sistēmai ir nevajadzīgi liela uzbrukuma virsma.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Pastāv risks, ka Sistēmai ir nevajadzīgi liela uzbrukuma virsma.

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Pastāv risks, ka Sistēmai ir nevajadzīgi liela uzbrukuma virsma.

Izmantojot kļūdu kodu analīzi ir iespējams iegūt papildu informāciju par tīmekļa vietni.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Pastāv risks, ka Sistēmai ir nevajadzīgi liela uzbrukuma virsma.

Izmantojot kļūdu koda analīzi ir iespējams iegūt papildu informāciju par tīmekļa vietni.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Pastāv risks, ka uzbrucējs vai ļaunprātīgs lietotājs var noklausīties datu plūsmu.

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

KPMG

Piemērs #2

Atklāto problēmu riski

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Atklāto problēmu riski

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Direktoriju šķērsošanas / datņu iekļaušanas pārvaldības problēmas.

Atklāto problēmu riski

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Tīmekļu vietnē nav uzstādīts drošības risinājums.

Direktoriju šķērsošanas / datņu iekļaušanas pārvaldības problēmas.

Atklāto problēmu riski

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Tīmekļu vietnē nav uzstādīts drošības risinājums.

Direktoriju šķērsošanas / datņu iekļaušanas pārvaldības problēmas.

Atklāto problēmu riski

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Tīmekļu vietnē nav uzstādīts drošības risinājums.

Direktoriju šķērsošanas / datņu iekļaušanas pārvaldības problēmas.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Atklāto problēmu riski

Atklātā problēma ļauj uzbrucējiem izmantot tīkla resursus, lai veiktu trešo pušu resursu skenēšanu.

Pastāv risks, ka ārējais uzbrucējs var nesankcionēti piekļūt *admin* sadaļai.

Uzbrucējs var izveidot vietni, kuras iFrame tiek ievietots tīmekļa vietnē un pieprasījums var tikt nosūtīts leģitīmajam lietotājam.

Tīmekļu vietnē nav uzstādīts drošības risinājums.

Direktoriju šķērsošanas / datņu iekļaušanas pārvaldības problēmas.

Potenciālais uzbrucējs var pasīvi novērot tīkla aktivitāti un iegūt piekļuves datus tīmekļa vietnes satura *admin* sadaļai.

Atklāto problēmu riski

Secinājumi

1. Drošības līmenis nav atkarīgs no pašvaldības lieluma, finansējuma, darbinieku skaita

2. Neviena no testēto pašvaldību mājaslapām nav pietiekami kiberdroša

3. Vājākās mājas lapas varētu padarīt nepieejamas dažu minūšu laikā

Ieteikumi mājaslapu drošības uzlabošanai

TOP 5

- ☑ Izmantot datu pārraides šifrēšanas risinājumus
- ☑ Regulāri pārskatīt piekļuves pārvaldības kontroles
- ☑ Veikt IT infrastruktūras iestatījumu pārskatīšanu
- ☑ Izmantot rīkus netipisku darbību identificēšanai un pārvaldībai
- ☑ Veikt regulārus kiberdrošības novērtējumus

KPMG

Sociālās inženierijas simulācijas rezultāti

Kibermodrības novērtējuma norise

162 darbinieki
15 pašvaldībās

Darbinieku kontaktinformācija no pašvaldību mājaslapām

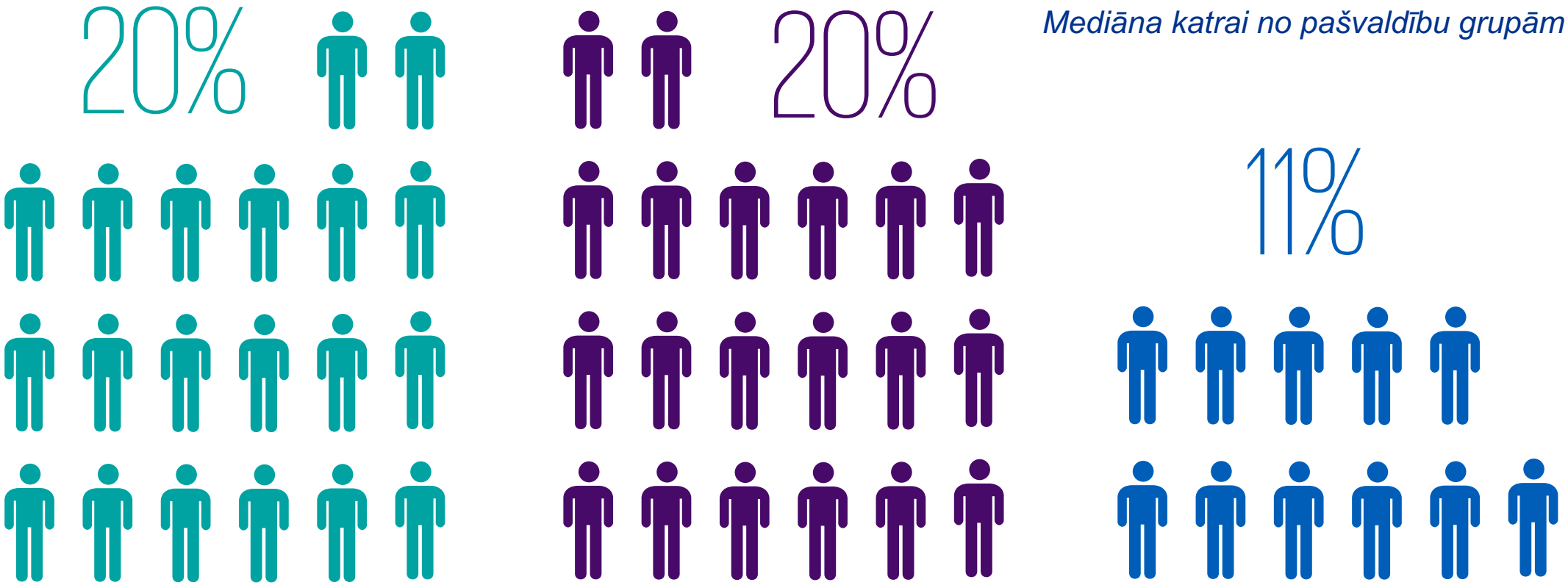
Aizdomīgas vēstules sūtījums pašvaldību darbiniekiem

Pikšķerēšanas uzbrukuma simulācija

“16% darbinieku nav pamanījuši kaitīgās vēstules pazīmes un var kļūt par uzbrucēja upuriem reāla uzbrukuma gadījumā.”

Cik procentu darbinieku ir atvēruši e-pastam pievienoto saiti?

Mediāna katrai no pašvaldību grupām



Mazās pašvaldības **Vidējās pašvaldības** **Lielās pašvaldības**

Apmācīts darbinieks - droša organizācija

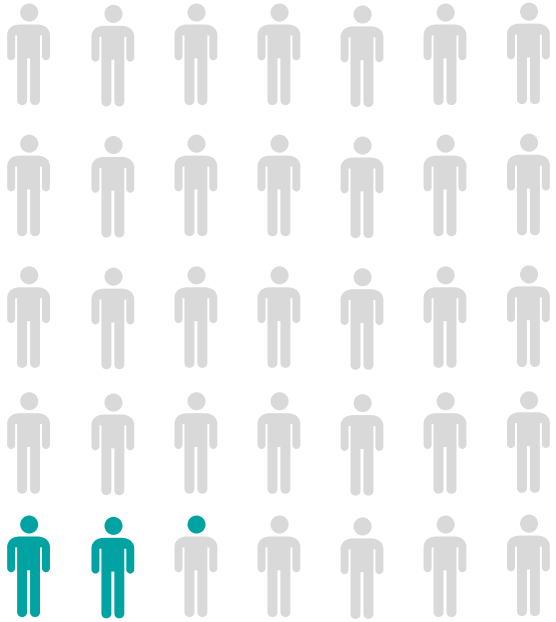
34,7%

Bez iepriekšējām apmācībām

14,5%

Pēc 90 dienām pēc veiktajām apmācībām

2,1%



Pēc 12 mēnešiem pēc regulāro apmācību veikšanas

KnowBe4 - 2019 Phishing By Industry Benchmarking Report

Statistika institūcijām ar 1 - 249 darbiniekiem, ASV

KPMG

Simulācijas norise

Nosūtītās vēstules piemērs

Jānis Bērziņš 2019. gada 21. marts 19:56

Ļ. cien. Vārds Uzvārds,

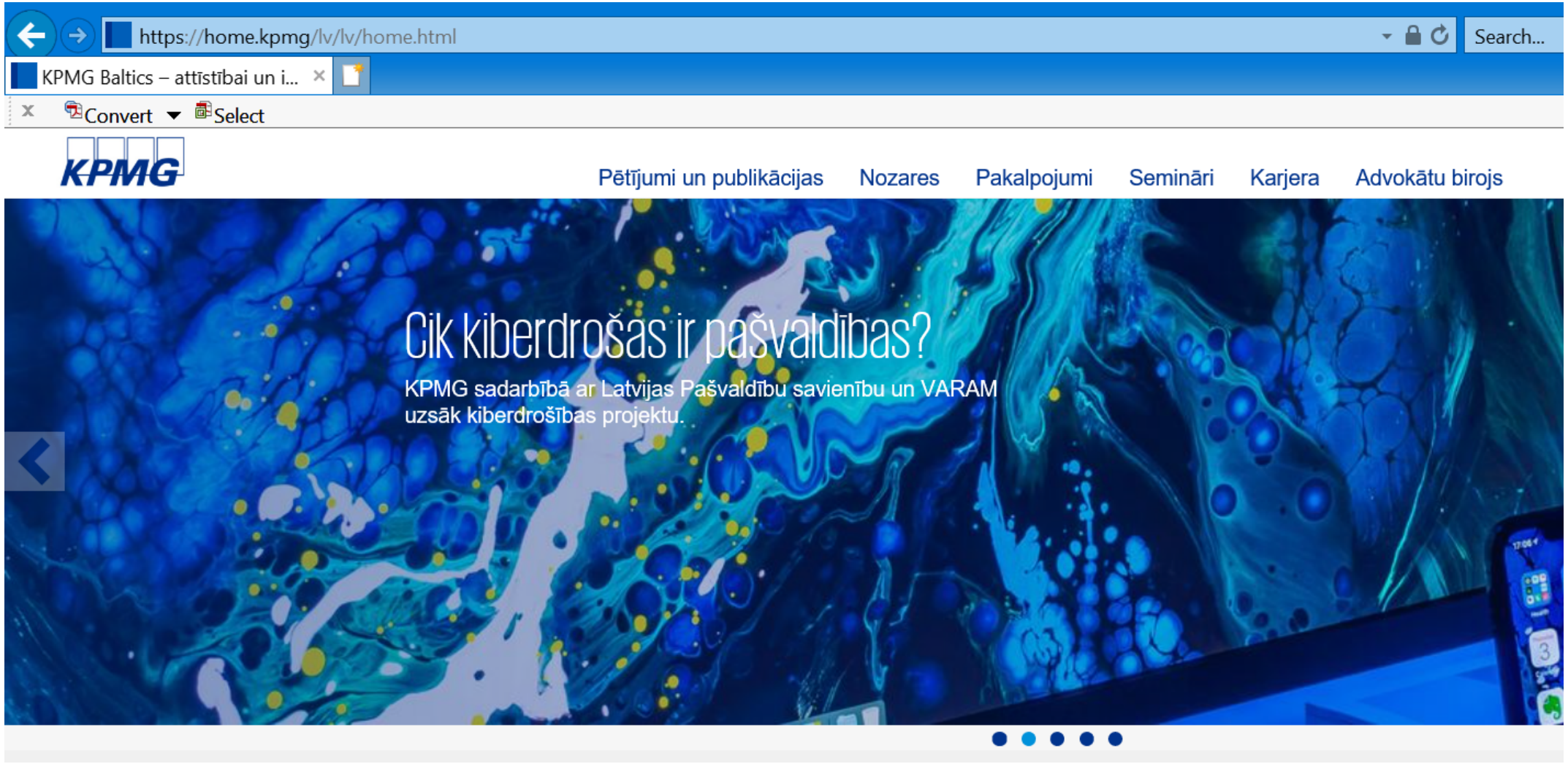
Sakarā ar izmaiņām pašvaldības darbinieku atalgojumā, zemāk atrodamajā saitē nosūtu atjaunoto algu sarakstu, kas stājas spēkā sākot ar 2019. gada 2. ceturksni.

Algu saraksts pieejams šeit

Ar cieņu,

Jānis Bērziņš,
Grāmatveža palīgs

Kur noveda pievienotā saite?



4% darbinieku

ir sākuši komunikāciju ar aizdomīgās vēstules sūtītāju

Secinājumi

1. Kibermodrības trūkumi tika konstatēti visu lielumu pašvaldībās

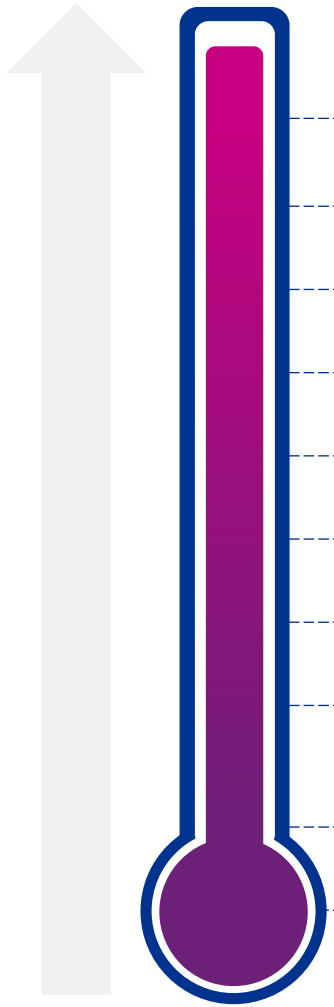
2. Pašvaldību darbiniekiem nav pietiekošu zināšanu kiberdrošības jomā

3. Gandrīz visām novērtētajām pašvaldībām nav automatizēto kontroļu mēstuļu identificēšanai

KPMG

Starptautiskā pieredze un tendences

OWASP kiberdrošības risku TOP 10



A1	Injection *(ļaunprātīga koda ievietošana)*
A2	Broken Authentication *(nepareiza autentifikācijas pārvaldība)*
A3	Sensitive Data Exposure *(nepareiza sensitīvo datu pārvaldība)*
A4	XML External Entities (XXE) *(XML injekcijas)*
A5	Broken Access Control *(nepareiza pieejas tiesību kontroļu pārvaldība)*
A6	Security Misconfiguration *(nedroša konfigurācija)*
A7	Cross-Site Scripting (XSS) *(atstarotā starpvietņu skriptēšana)*
A8	Insecure Deserialization *(nedroša deserializācija)*
A9	Using Components with Known Vulnerabilities *(izmanto komponentes ar zināmām ievainojamībām)*
A10	Insufficient Logging & Monitoring *(nepietiekams monitorings un notikumu pārvaldība)*

Pašvaldības kļūst par kāroto mērķi

Hackers Won't Let Up in Their Attack on U.S. Cities

Baltimore is still recovering month after more than one group breached its network

American towns under cyberattack from an NSA-built software

May 26, 2019 4:59 PM EDT

BBC Home News Sport Reel More

NEWS

Technology

Second US town pays up to ransomware hackers

26 June 2019

Town Avoids Paying Massive $5 Million Ransom In Cyberattack

September 6, 2019 · 5:29 PM ET

Kiberuzbrukumi Eiropā #2019

DELFI EN > Politics

How Lithuanian defense minister became a target: cyber and fake news attack was just the beginning (8)

Lietuva
Aprīlis 2019

Kiberuzbrukumi Eiropā #2019

Cyber Threats | Cyber Attack | TAGS | Cyber Attack | Elections | Finland

Finland election results service hit by Cyber Attack

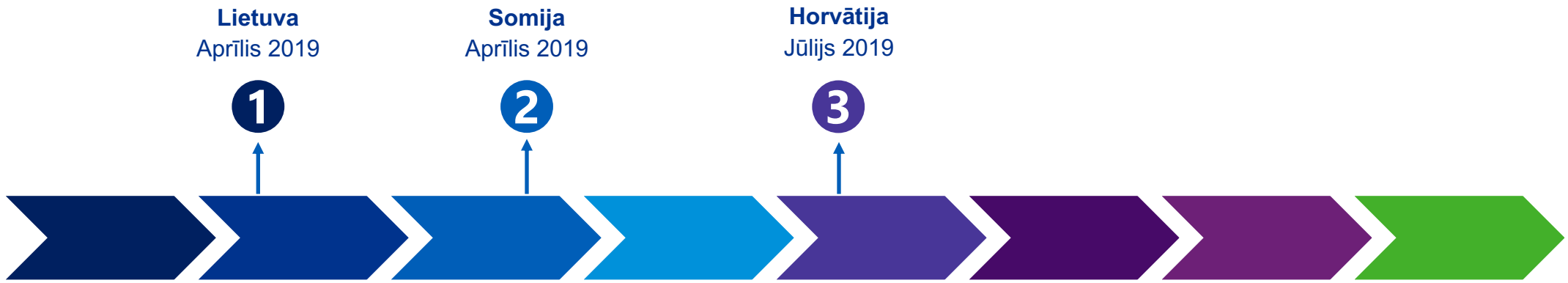
Lietuva
Aprīlis 2019

Somija
Aprīlis 2019

Kiberuzbrukumi Eiropā #2019

Croatia hit by waves of cyber attacks with a new malware: SilentTrigger

8 July 2019 Francesco Bussoletti Cyber, Defence and Security



Kiberuzbrukumi Eiropā #2019

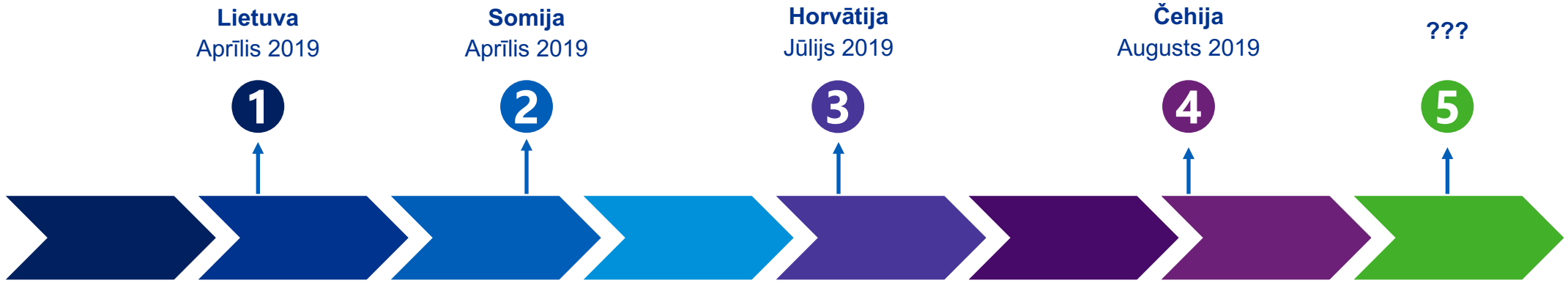
Czechs blame foreign state for Foreign Ministry cyberattack

August 13, 2019

Kiberuzbrukumi Eiropā #2019

Top draudi 2017	Nov.	Top draudi 2018	Nov.	Prognozētās izmaiņas
1. Ļaunprogrammatūra (malware)	→	1. Ļaunprogrammatūra (malware)	→	→
2. WEB uzbrukums	↑	2. WEB uzbrukums	↑	→
3. WEB aplikācijas uzbrukums	↑	3. WEB aplikācijas uzbrukums	→	→
4. Pikšķerēšanas uzbrukums	↑	4. Pikšķerēšanas uzbrukums	↑	→
5. Spams	↑	5. Pakalpojumatteices uzbrukums (DoS)	↑	↑

ENISA Threat Landscape Report 2018



Kiberdrošības tendences 2019

1. Pikšķerēšanas paņēmieni mainās, tomēr e-pastu pikšķērēšana joprojām paliek par vispopulārāko uzbrukumu veidu

2. Pieaug kiberuzbrukumu skaits, kas veikts mobilajām ierīcēm

3. Turpina pieaugt uzbrukumu skaits pašvaldībām un uzņēmumiem, izmantojot izspiedējvīrusu *(ransomware)*

4. Aizvien lielāks uzsvars tiek likts uz datu privātumu, suverenitāti un atbilstību starptautiskiem standartiem

5. Pieaug investīcijas kiberdrošības pārvaldības automatizācijā

Kiberdrošības tendences 2020

1. Institūcijas turpinās ar vien vairāk investēt kiberdrošībā

2. Pieaugs mākslīgā intelekta un mašīnmācīšanas risinājumu ietekme uz kiberdrošību

3. Kiberuzbrukumi pret komunālo pakalpojumu sniedzējiem un publisko infrastruktūru turpinās pieaugt

Pirmie soļi uz drošāku kibertelpu

Apmācīt

darbiniekus un

uzturēt kiberdrošas

IT saimniecības

Kaspars Iesalnieks

KPMG IT konsultāciju vadītājs