



Risinājumi IT infrastruktūras sagatavošanai un uzturēšanai atbilstoši GDPR prasībām

Sarmīte Mickeviča

Lattelecom Drošības risinājumu
pakalpojumu vadītāja



Cik uzņēmumi ir gatavi GDPR prasībām?



Cik aizsargāta ir biznesa kritiskā informācija?

80%

no ES uzņēmumiem ir
saskārušies ar vismaz
vienu IT drošības incidentu
pagājušā gadā

469

Dienas vidēji
nepieciešamas ES
uzņēmumam, lai atklātu
ielaušanos

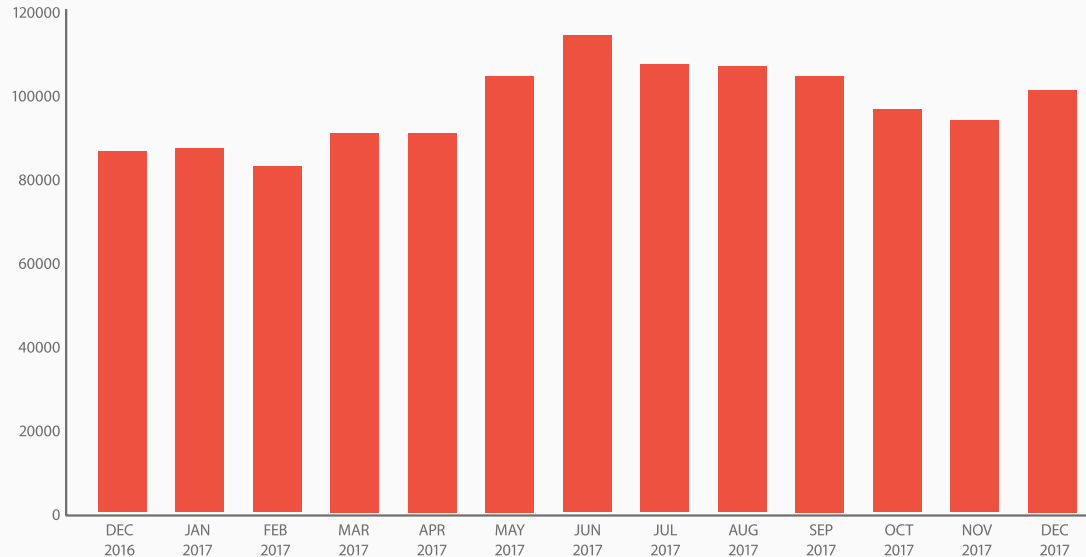
69%

no ES uzņēmumiem nav
izpratnes par to iespējamo
IT risku apjomu

60%

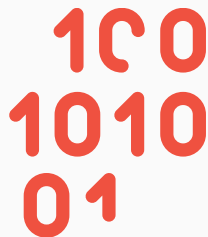
no ES uzņēmumiem nav
vērtējuši iespējamus
zaudējumus no IT drošības
incidentiem

Apdraudēto iekārtu skaits 2017.gadā Latvijā



Avots: CERT.LV darbības pārskats par 2017. gadu

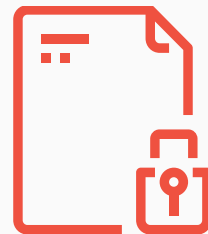
Datu apstrādes sistēmu integritāte, konfidencialitāte, pieejamība



Integritāte
Datu pārveidošana

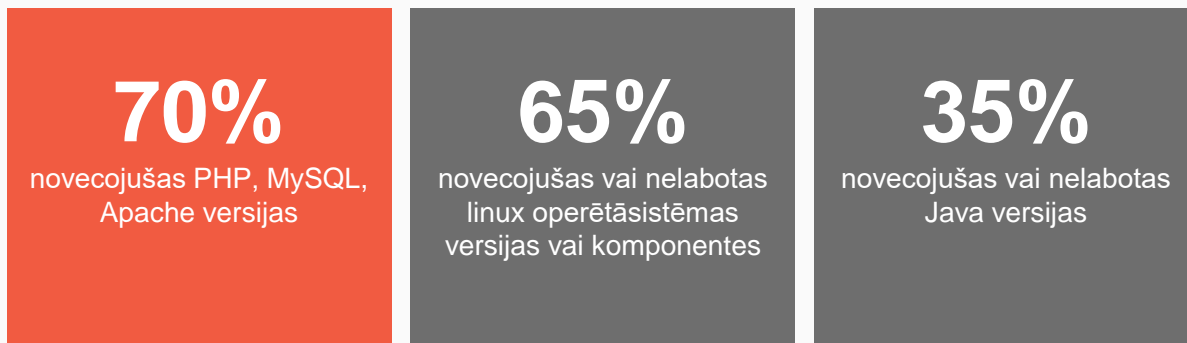


Konfidencialitāte
Personas datu pazaudēšana
nesankcionēta lietošana
izpaušana



Pieejamība

Drošības auditos atklātās ievainojamības



Drošības auditos atklātās ievainojamības



Kādas ievainojamības ir izmantotas kiberuzbrukumos?

Ievainojamība dod iespēju uzbrucējam apdraudēt personas datu integritāti, pieejamību vai konfidencialitāti.

Visbiežāk kiberuzbrukumos izmanto **zināmas ievainojamības**

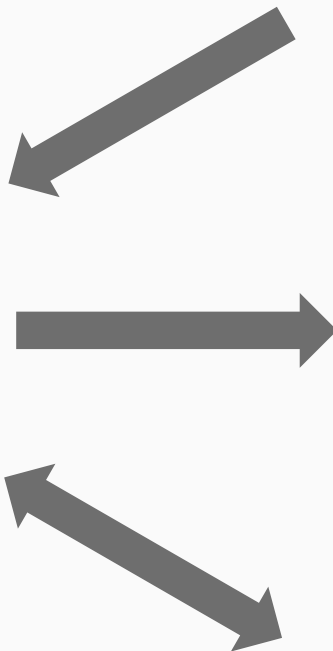
- Nedrošas paroles
- nedrošas konfigurācijas iekārtām, serveriem, u.c.
- «aizmirsti» jauninājumi – OS, aplikācijām, mikrokodam u.c.
- WannaCry, NotPetja izmantoja vienu un to pašu zināmo ievainojamību

Ievainojamību pārbažu pakalpojums

- Atklāj ievainojamības reāllaikā
- Pārbauda konfigurāciju atbilstību labākajai praksei
- Nodrošina ievainojamību pārbažu automatizāciju
- Darba uzdevumi sistēmu administratoriem

Ārējā tīkla pārbaude

Klienta
pašapkalpošanās
portāls:
[https://mssp.
lattelecom.lv:3780](https://mssp.lattelecom.lv:3780)



Klienta iekārtas ar
publisku IP adresi

Ievainojamību un
atbilstību pārskati
katrai IP adresei.

Globālā ievainojamību
datu bāze. Atjaunojas
ik pēc 6 stundām.

Ārējā tīkla pārbaude

Klienta pašapkalpošanās portāls:
<https://mssp.lattelecom.lv:3780>



Klienta iekārtas ar publisku IP adresi

Klienta iekārtas iekštīklā, iekšējās IP adreses

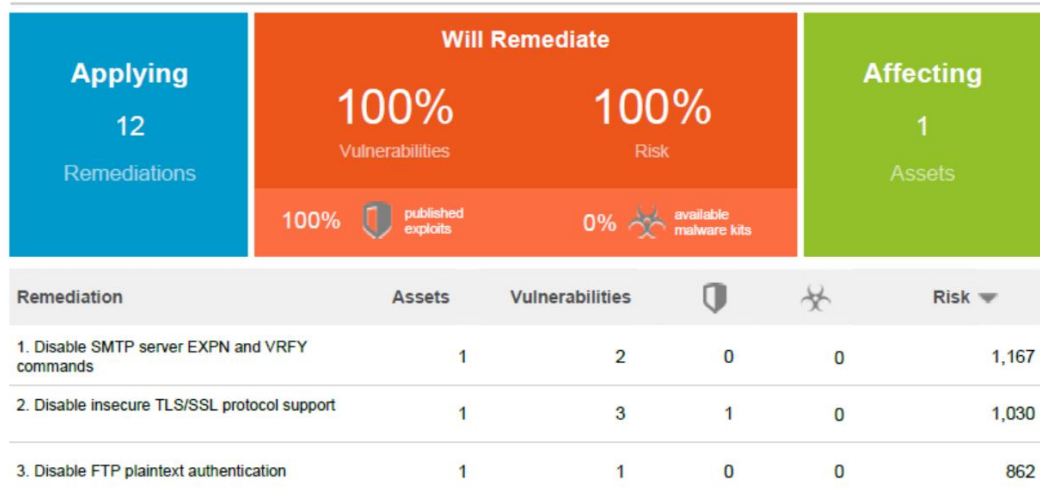
Ievainojamību un atbilstību pārskati katrai IP adresei.

Globālā ievainojamību datu bāze. Atjaunojas ik pēc 6 stundām.

Ievainojamību novēršanas pārskats

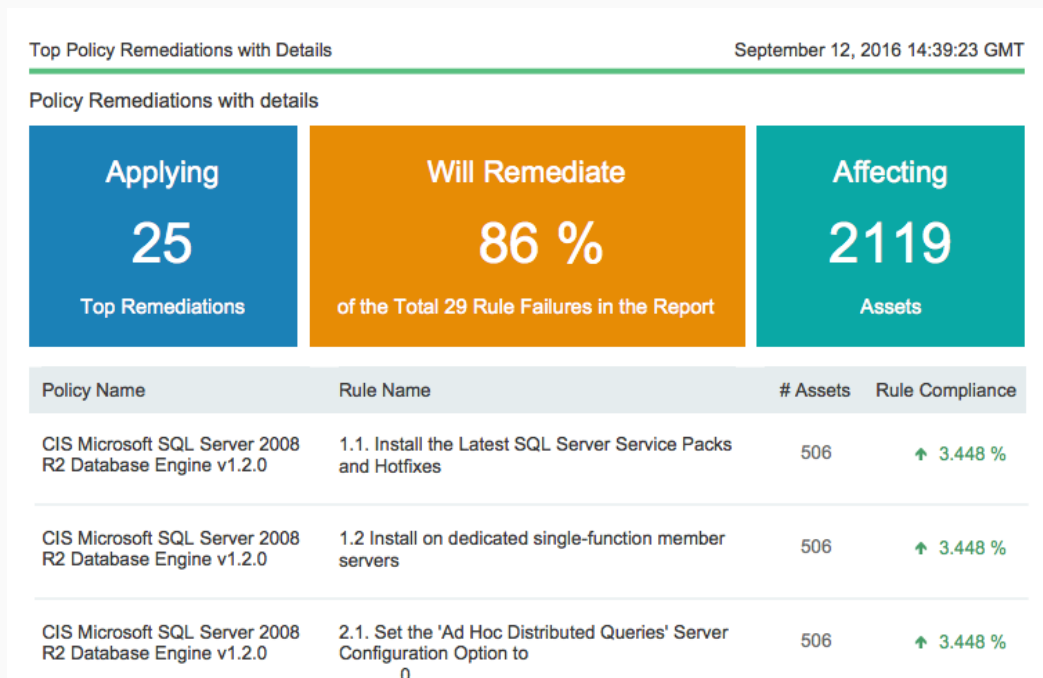
Top 25 Remediations by Risk

April 11, 2017 4:23:04 AM EDT



IT apdraudējumi tiek sakārtoti pēc to kritiskuma un tiek norādīti veidi kā šos apdraudējumus novērst.

Politiku neatbilstības novēršanas pārskats



Pieejamas vairāk kā 20 ievainojamību pārbaūžu atskaites - PCI iekšējā pārbaude, HIPAA atbilstība, Microsoft hotifix, Internet DMZ.

Web un mobilo aplikāciju drošības un personas datu apstrādes atbilstības pārbaudes pakalpojums

Personas datu apstrādes atbilstības
novērtējums web lapai un mobilajai aplikācijai

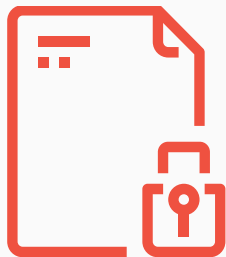
Flash/Flex, Silverlight

Web & Mobile, JSON, REST, AMF, SOAP, AJAX

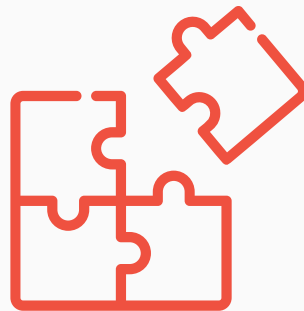
Javascript

Statiskās lapas

GDPR prasības drošības risku novēršanai



Datu anonimizācija un
šifrēšana



Iespēja laicīgi
atjaunot datus
pēc drošības incidenta



Datu apstrādes
līdzekļu drošība

Iekārtu drošības un pārvaldības pakalpojums

- **F-Secure Protection Service for Business**
- Labākā «0 – day» pretvīrusu aizsardzība, Deep Guard tehnoloģija
- Datoru, mobilo iekārtu un serveru aizsardzība
- Programmatūras jauninājumu monitorings un vadība



Datu centru pakalpojumi



GDPR datu pārkāpumu ziņošana



Datu noplūde
nesankcionēta lietošana



72h laikā no
incidenta norises



Ziņot atbildīgajām
institūcijām

Drošības incidentu un notikumu monitoringa sistēmas pakalpojums

- Auditācijas pierakstu savākšana
- Auditācijas pierakstu glabāšana pārskatāmā veidā
- Drošības incidentu kritēriju definēšana un klasificēšana
- Incidentu izskatīšana un ziņošana 24 * 7

Lattelecom drošības risinājumu attīstība



PCI DSS
Level 2
sertifikāts



IT sistēmu
drošības nepilnību
identificēšana

Web un mobilo
aplikāciju drošības
nepilnību pārbaudes



Kiberdrošības
draudu diagnostika
SaaS 24x7



Iekārtu drošības un
pārvaldības
pakalpojums

2013

2014

2015

2016

2017

2018

Pirmais TIER III
datu centrs
Ziemeļeiropā



DDoS uzbrukumu
aizsardzība



PCI DSS
Level 1
sertifikāts



Drošības incidentu
un notikumu
monitorings



Web un mobilo
aplikāciju personas
datu apstrādes
atbilstības
pārbaudes



Lattelecom IT drošības pakalpojumi

1. GDPR atbilstības juridiskais novērtējums

2. GDPR atbilstības tehniskais novērtējums (IT audits)

3. IT drošības pakalpojumi

4. Datu centru pakalpojumi

- Uzņēmuma ar datu apstrādi saistīto dokumentu novērtējums;
- Datu plūsmu identificēšana un to raksturojums;
- Datu apstrādes reģistrs;
- Incidentu atklāšanas un novēršanas kārtība;
- Līgumu un piekrišanas dokumentu izstrāde atbilstoši Regulas prasībām
- Uzņēmuma datu apstrādes sabiedrisko attiecību procesa nodrošināšanai novērtējums

Lattelecom IT drošības pakalpojumi

1. GDPR atbilstības juridiskais novērtējums

2. GDPR atbilstības tehniskais novērtējums (IT audits)

3. IT drošības pakalpojumi

4. Datu centru pakalpojumi

- Serveru (tehniskās) telpas atbilstības novērtējums;
- **IT infrastruktūras darbības un drošības novērtējums:**
 - Fizisko iekārtu darbības analīze;
 - Operētājsistēmu/Datu bāžu darbības un drošības analīze;
- **IS drošības politikas izstrāde:**
 - IS drošības un darbības politika
 - Informācijas resursu klasifikācija
 - Informācijas sistēmu risku analīze

Lattelecom IT drošības pakalpojumi

1. GDPR atbilstības juridiskais novērtējums

2. GDPR atbilstības tehniskais novērtējums (IT audits)

3. IT drošības pakalpojumi

4. Datu centru pakalpojumi

- IT sistēmu drošības nepilnību regulāra identificēšana
- WEB un mobilo aplikāciju drošības nepilnību pārbaudes
- Web un mobilo aplikāciju personas datu apstrādes atbilstības pārbaudes
- Iekārtu drošības un pārvaldības pakalpojums
- Drošības incidentu un notikumu monitorings

Lattelecom IT drošības pakalpojumi

1. GDPR atbilstības juridiskais novērtējums

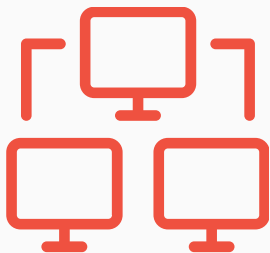
2. GDPR atbilstības tehniskais novērtējums (IT audits)

3. IT drošības pakalpojumi

4. Datu centru pakalpojumi

- **Fiziskā drošība** - IT&T infrastruktūras izvietošana Lattelecom DC
- **Apmācīts IT personāls** - iekārtu un sistēmu uzturēšana LTC
- **Droša pakalpojumu sniedzēja infrastruktūra** - regulāri testēta un uzraudzīta pret drošības riskiem

Ar ko sākt?



Pārzini tīklu un identificē
vājos punktus



Novērtē aplikāciju
ievainojamību



Monitorē lietotāju
uzvedību

Izveido incidentu
reaģēšanas programmu



Ietaupi laiku & resursus –
izvēlies ekspertu radītus
risinājumus



Paldies!

Sarmīte Mickeviča

Lattelecom Drošības risinājumu
pakalpojumu vadītāja

+371 29493944

lattelecom