Kiberdrošības situācija Latvijā

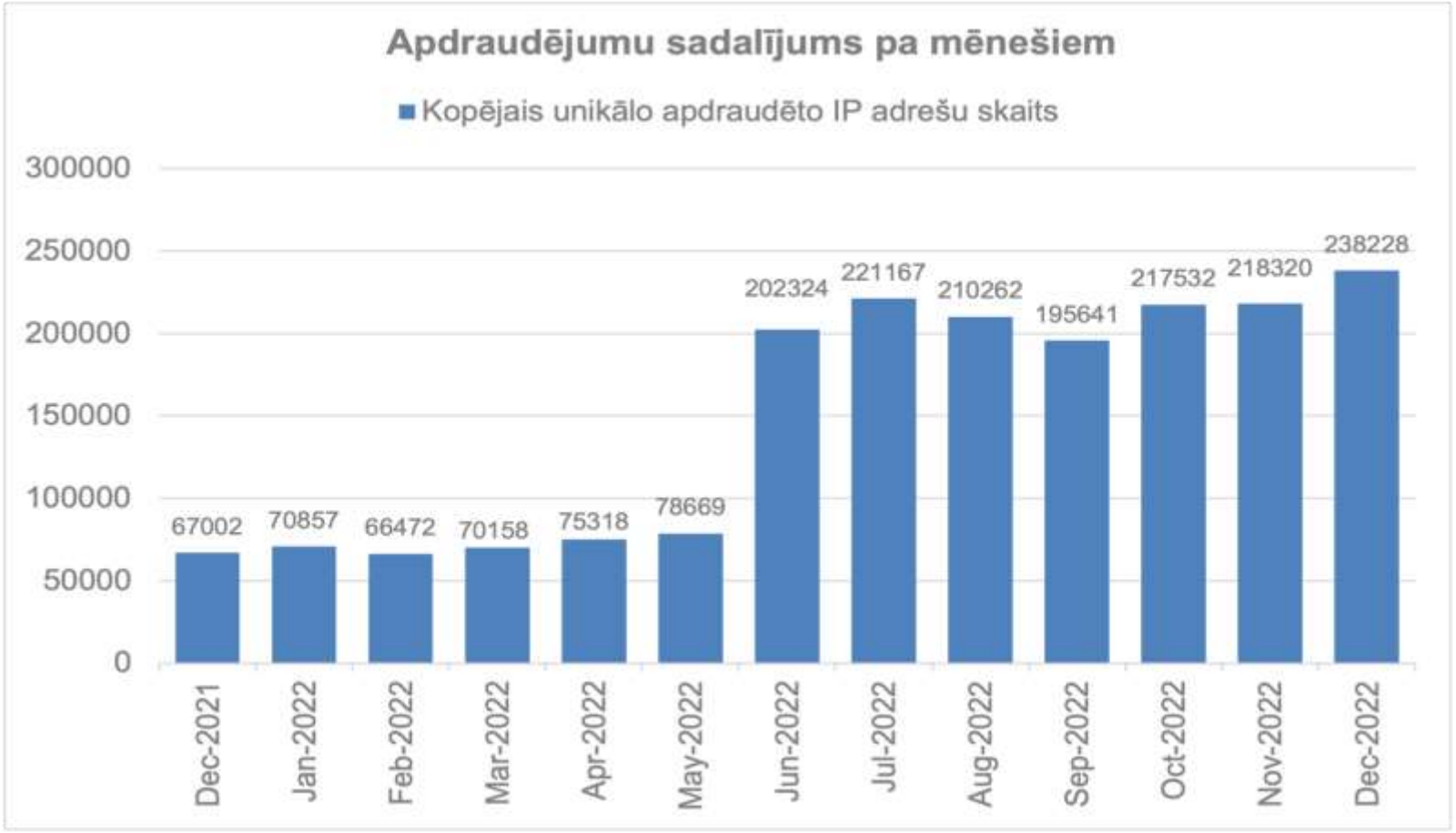
Latvijas Pašvaldību savienības sanāksme

20.04.2023. – Egils Stūrmanis, CERT.LV

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

2022.gads Latvijas kibertelpā

- Incidentu pieaugums – 40%
- Valsts sektoram uzbrukumu apjoms – x4
- Ievainojamību meklēšana – x7



Valsts soļi brieduma veicināšanā

- Pieņemta jaunā Kiberdrošības stratēģija (2023-2026)
- Kiberdrošības likums (ITDL vietā)
- Nacionālā Kiberdrošības centra veidošana
- MK442 pārstrāde
- Uzraudzības sistēmas izveide

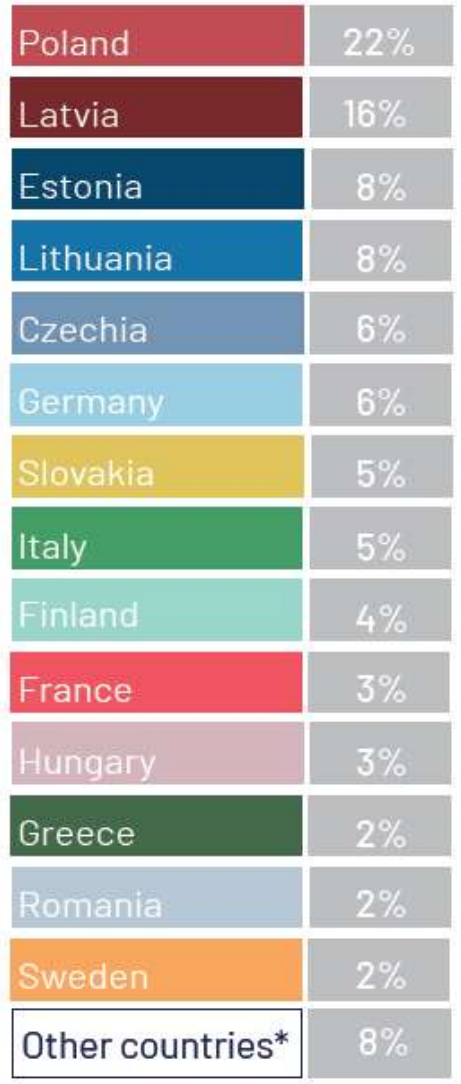
Kas Latvijai uzbrūk?

Krievija realizē plaša mēroga kiberoperācijas vismaz kopš 2007. gada (Agent-BTZ, Turla, …)

Latvijā kiberdrošības apdraudējuma līmenis noteikts kā augsts kopš 2022. gada janvāra.

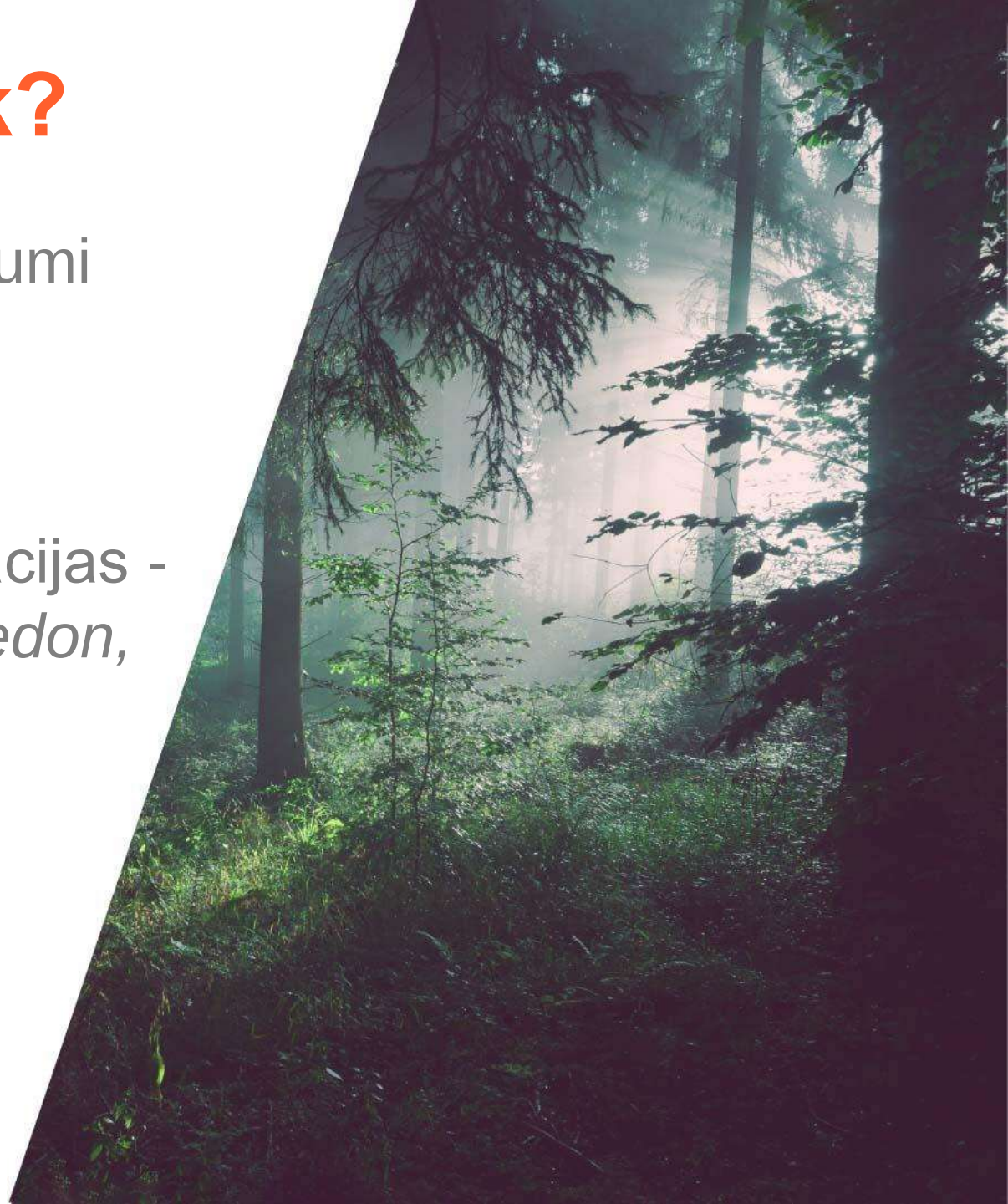
Kam visvairāk uzbrūk Eiropas savienībā?

CERT - EU apskats
«RUSSIA'S WAR ON UKRAINE:
ONE YEAR OF CYBER OPERATIONS»



Kā Latvijai uzbrūk?

- Piekļuves lieguma – *DDoS* uzbrukumi
- Citas haktīvistu aktivitātes
- RU dienestu atbalstītas kiberoperācijas - *Whispergate, Ghostwriter, Gamaredon, Turla...*



DDoS noturība

Esam cienījami pret stāvējuši apjomīgākajiem un ilgstošākajiem *DDoS* uzbrukumiem pateicoties

un daudziem citiem partneriem!

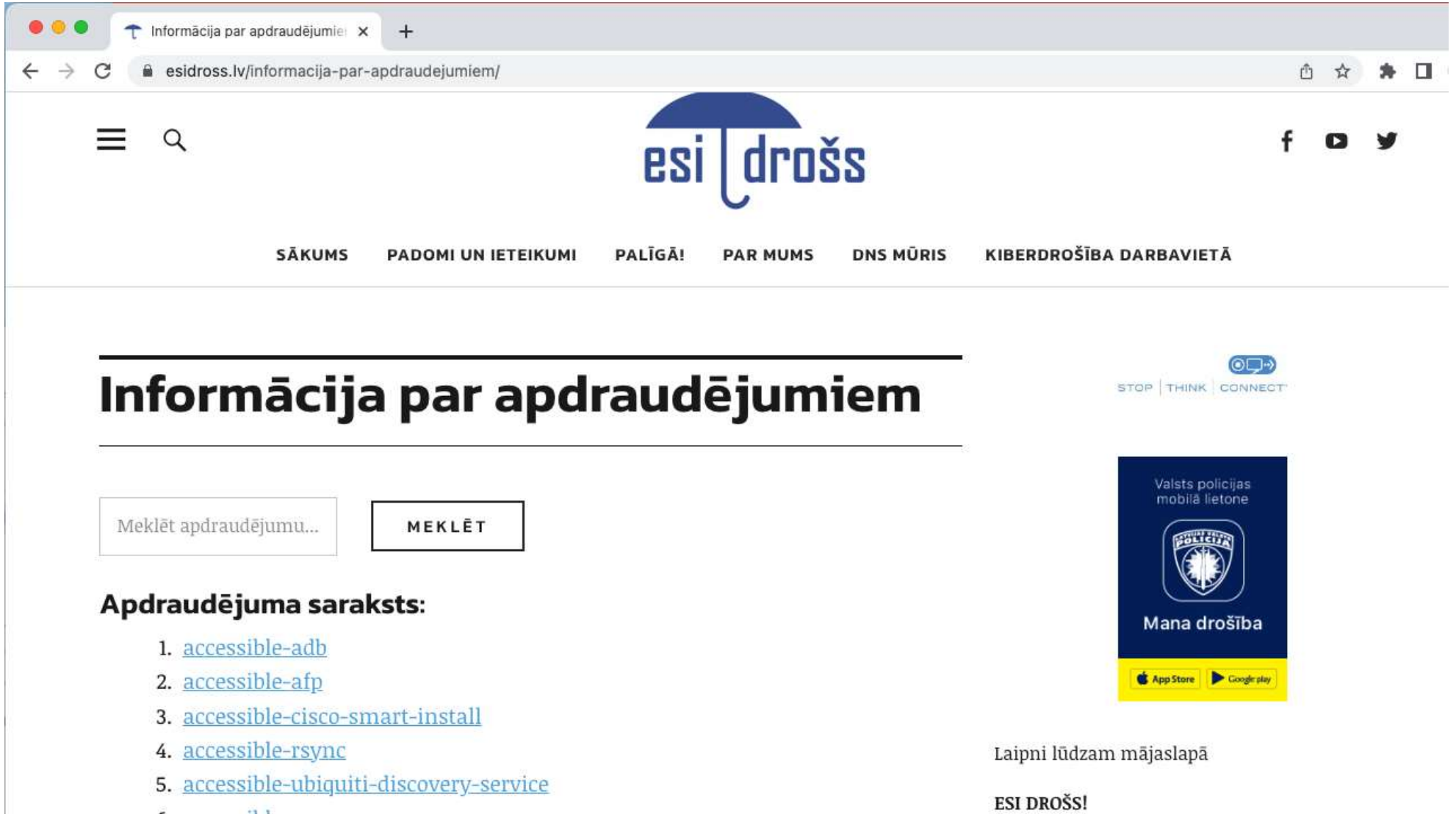
Proaktīvās apziņošanas platforma

Subject: Inficeto IP saraksts [cert@cert.lv] notikumu diapazons [1]
Date: Thu, 30 Mar 2023 09:12:02 +0300
From: cert@cert.lv
To: zina@cert.lv

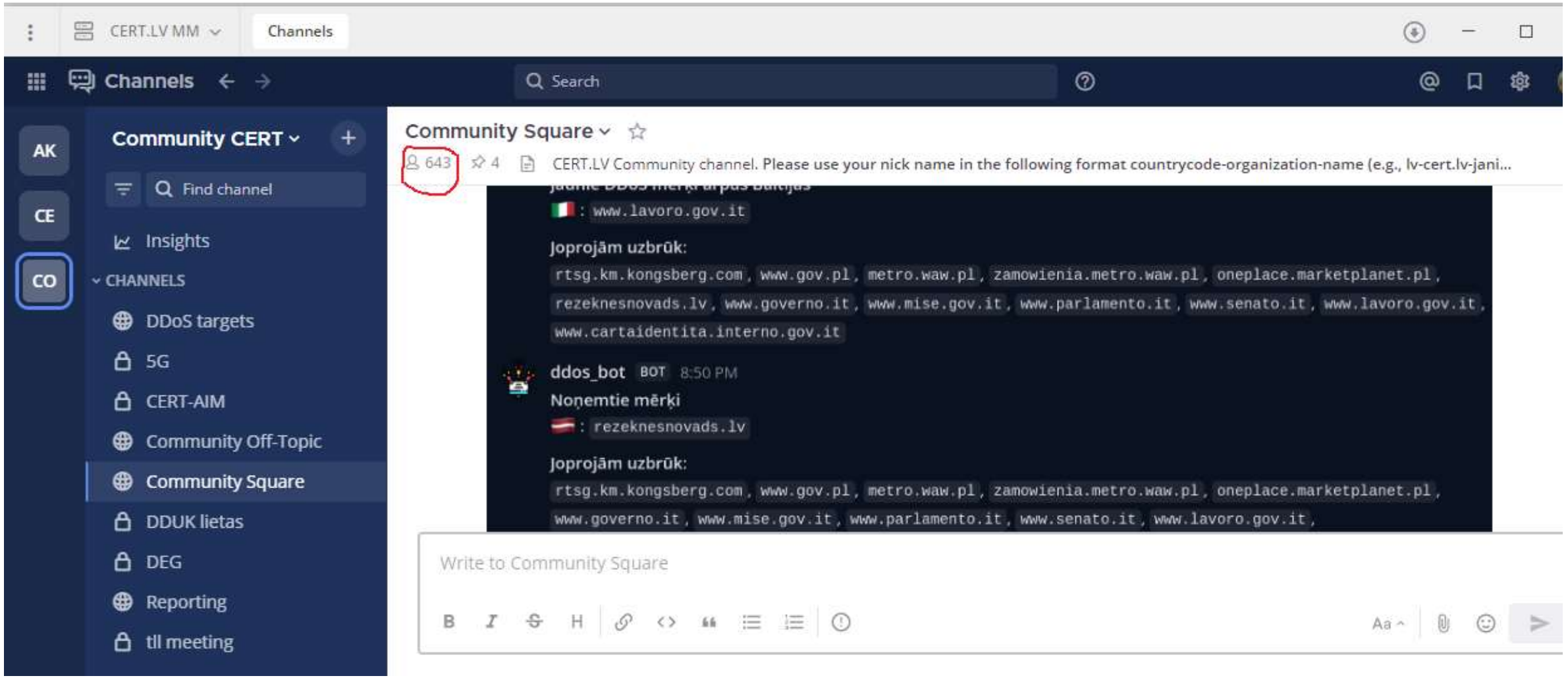
; CERT.LV ziņojums
; Copyright 2023 CERT.LV. Lauku apraksts:
;
; time - laiks UTC formātā
; ip - avota IP adrese
; asn - avota autonomā sistēma (ja pieejama)
; identifier – apdraudējuma identifikators
; type – apdraudējuma tips
; destination - mērķa IP adrese (ja pieejama)
; destination_port - mērķa ports (ja pieejams)
; destination_asn - mērķa autonomā sistēma (ja pieejama)
; url - saistītā tīmekļa vietne (ja pieejama)
; domain - saistītās tīmekļa vietnes domēna nosaukums (ja pieejams)
; priority - prioritāte (1-zema, 2-vidēja, 3-augsta, 4-ļoti augsta)
; hash - kontrolsumma (izmantojama papildus informācijas iegūšanai https://www.esidross.lv/cert-lv-bridinajums/?hash/<hash>)

time,ip,asn,identifier,type,destination,destination_port,destination_asn,url,domain,priority,hash
2023-03-28 04:52:04,91.240.x47.x8,29345,accessible-http:http,other,0.0.0.0,,,,,1,hash
2023-03-28 07:22:40,91.240.x47.x9,29345,accessible-http,other,0.0.0.0,,,,,1,hash
2023-03-28 07:22:40,91.240.x47.x9,29345,accessible-http:http,other,0.0.0.0,,,,,1,hash

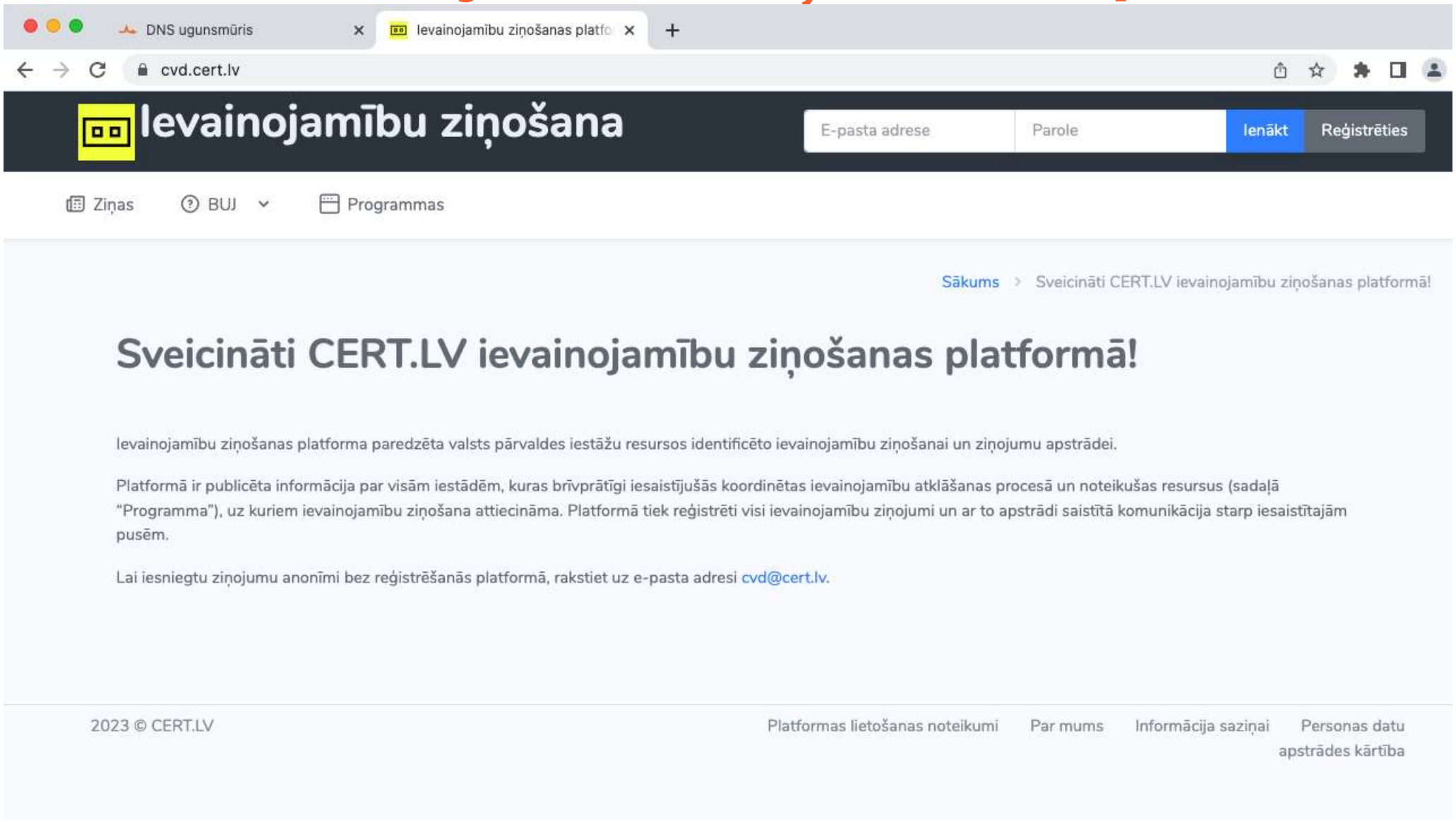
Esidross.lv tīmekļa vietne



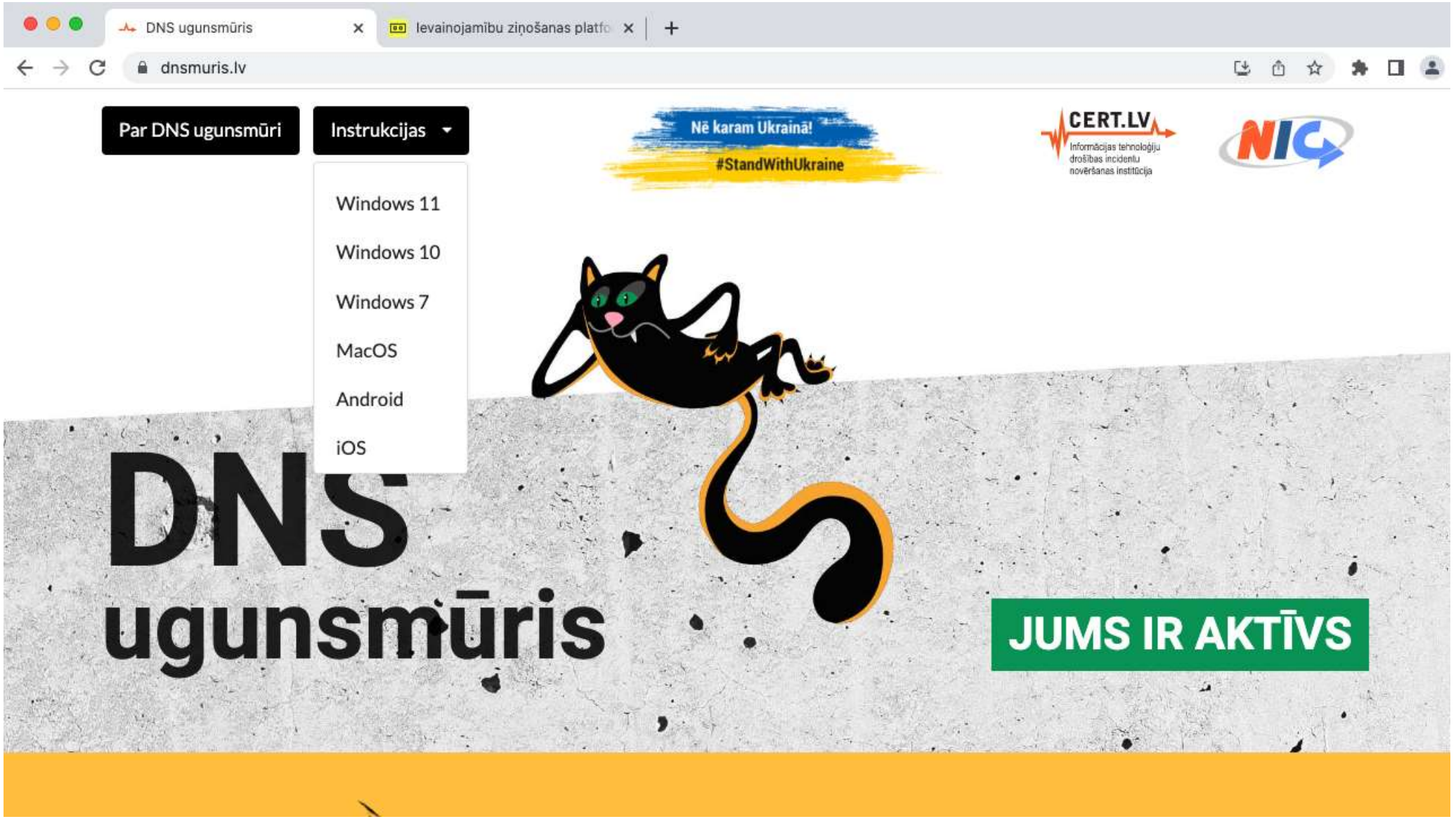
Kopienas saziņas platforma



CERT.LV Ievainojamību ziņošanas platforma



DNS mūris


DNS ugunsmūris
dnsmuris.lv
Par DNS ugunsmūri
Instrukcijas
Windows 11
Windows 10
Windows 7
MacOS
Android
iOS
Nē karam Ukrainā!
#StandWithUkraine
CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija
NIC
DNS
ugunsmūris
JUMS IR AKTĪVS

Briedums un kibernoturība

- Spējam ātri pielāgoties un mobilizēties
- Strādājam nelielās, taču efektīvās komandās
- Mēs pazīstam viens otru
- Mēs uzticamies un viens otram pierādām, ka varam uzticēties
- Mums ir Kiberaizsardzības vienība Zemessardzē

CERT.LV

Paldies!

https://www.cert.lv

certlv

certlv