



# Piekļuves lieguma uzbrukumi prezidentūras laikā

DIDZIS OZOLIŅŠ  
Datu pārraides daļas vadītājs  
VAS «LVRTC»

---



# Kas mēs esam

---





## Kas mēs patiešām esam

---

KRITISKĀ INFRASTRUKTŪRA

DATU PĀRRAIDE

DATU CENTRI



## LVRTC un piekļuves lieguma uzbrukumi

---



EU2015.LV

Latvijas prezidentūra  
Eiropas Savienības  
Padomē



## Uzbrukumu intensitāte

---

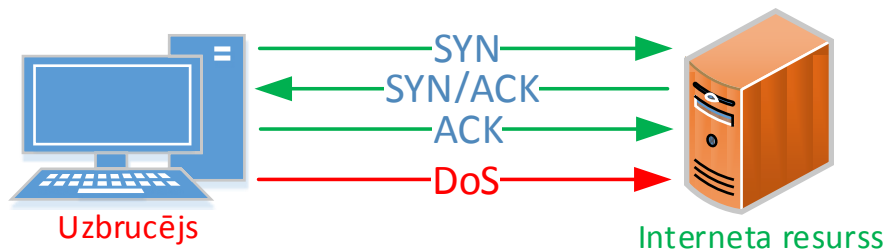
- Skaits;
- Jauda;
- Periodiskums.



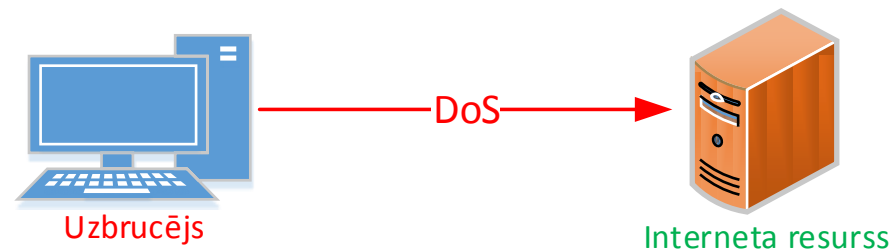
## Uzbrukumu veidi

---

### Sesijas bāzēts



### Bez sesijas



Maza joslas platuma uzbrukumi;  
Apjoma uzbrukumi.



## Uzbrukums #1

---

Parametrs	Vērtība
Vektors	UDP straumēšana
Apjoms	5Gbit/s, 400k pps
Ilgums	<1h
Tips	Apjoma, bez sesijas

KAS iesaistīts?

VAI uzbrukums?

KO darīt?

KĀ un KAS uzbrūk?

KO darīt?



## Uzbrukums #2

---

Parametrs	Vērtība
Vektors	TCP SYN straumēšana
Apjoms	60k pps
Ilgums	40 minūtes
Tips	Apjoma, bez sesijas

KAS iesaistīts?

VAI uzbrukums?

KO darīt?

KĀ un KAS uzbrūk?

KO darīt?

---





## Uzbrukums #3

---

Parametrs	Vērtība
Vektors	HTTPS straumēšana
Apjoms	norma*5
Ilgums	on/off 3 diennaktis
Tips	Apjoma, sesijas bāzēts

KAS iesaistīts?

VAI uzbrukums?

KO darīt?

KĀ un KAS uzbrūk?

KO darīt?

---



## Galvenie piekļuves lieguma uzbrukumu cēloņi

---

- Politiskās aktivitātes;
- Materiālā labuma gūšana;
- Citu uzbrukumu slēpšana;
- Prieka/ziņkāres pēc.



Latvijas prezidentūra  
Eiropas Savienības  
Padomē

EU2015.LV



## Kopsavilkums

---

- Uzbrukumi ir un par 99.(9)% būs arī pēc prezidentūras;
- Rūpīgi plānojot un pārskatot rīcībā esošos resursus, var sasniegt daudz. Piemēram:
  - Uzraudzības sistēma;
  - NetFlow, SIEM;
  - BGP (RTBH, FlowSpec, QPPB).
- Atceramies par drošību – veicot drošības uzlabojumus vienā virzienā, var tikt radīti papildus riski citā virzienā.



Paldies!

DIDZIS OZOLIŅŠ  
Datu pārraides daļas vadītājs  
didzis.ozolins@lvrtc.lv

---