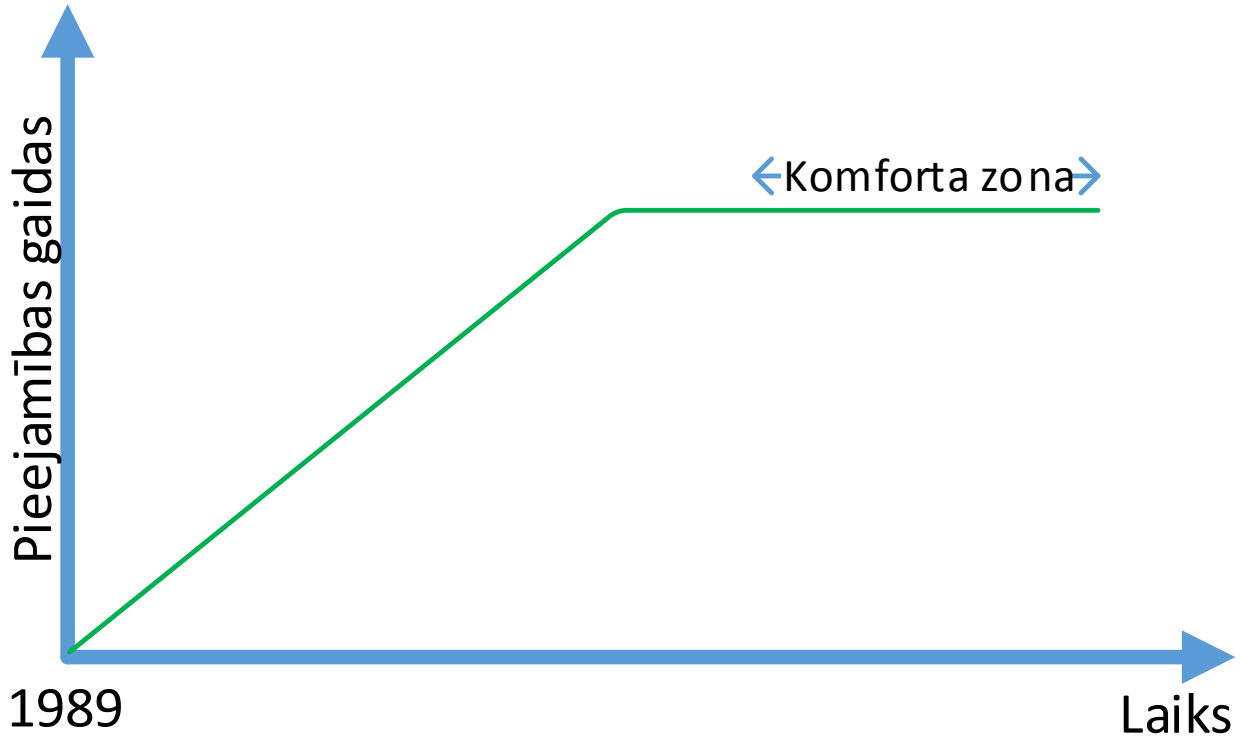
Piekļuves lieguma uzbrukumu veidi un iespējamā uzbrukumu seku mazināšana.

Didzis Ozoliņš

Datu pārraides daļas vadītājs

LATVIJAS VALSTS
RADIO UN TELEVĪZIJAS CENTRS

Komforta zona



- Mobilitāte;
- Neatkarība.

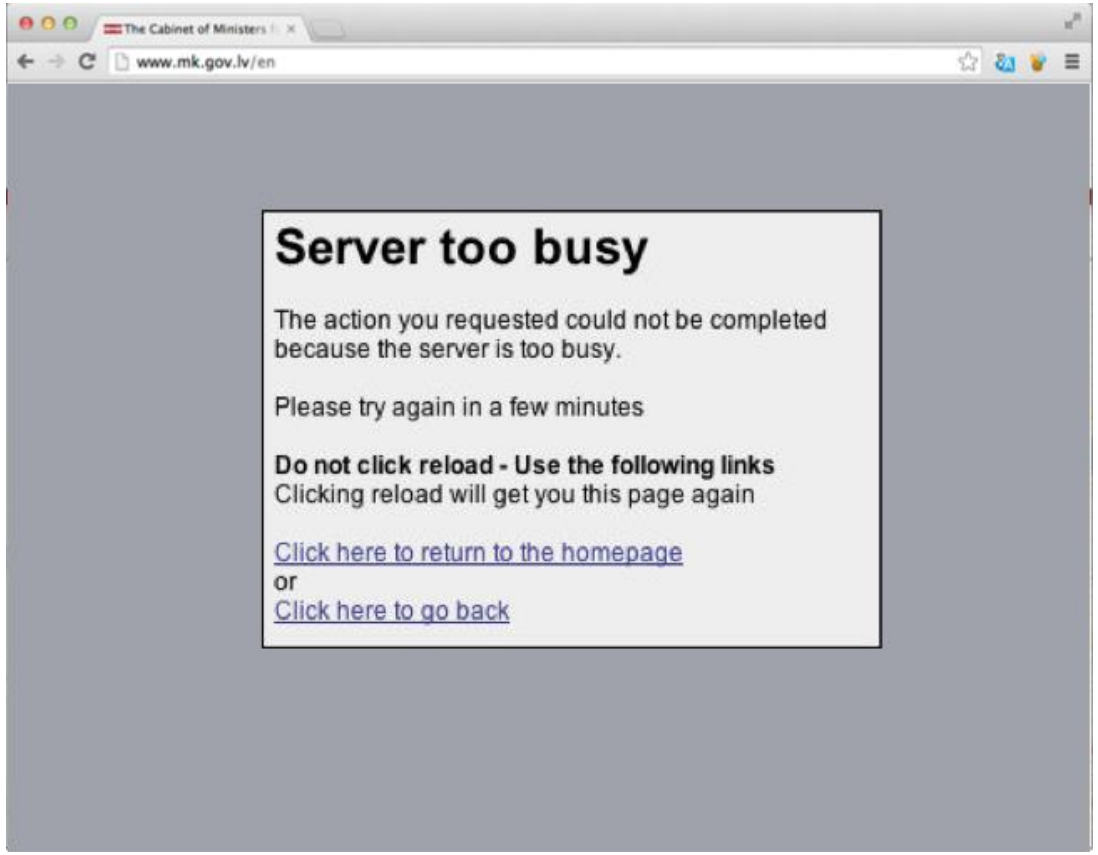
Interneta resursu pieejamība

Valsts pārvalde, tās klienti un partneri sagaida, ka valsts (un ne tikai) interneta resursu pieejamība būs 100%.

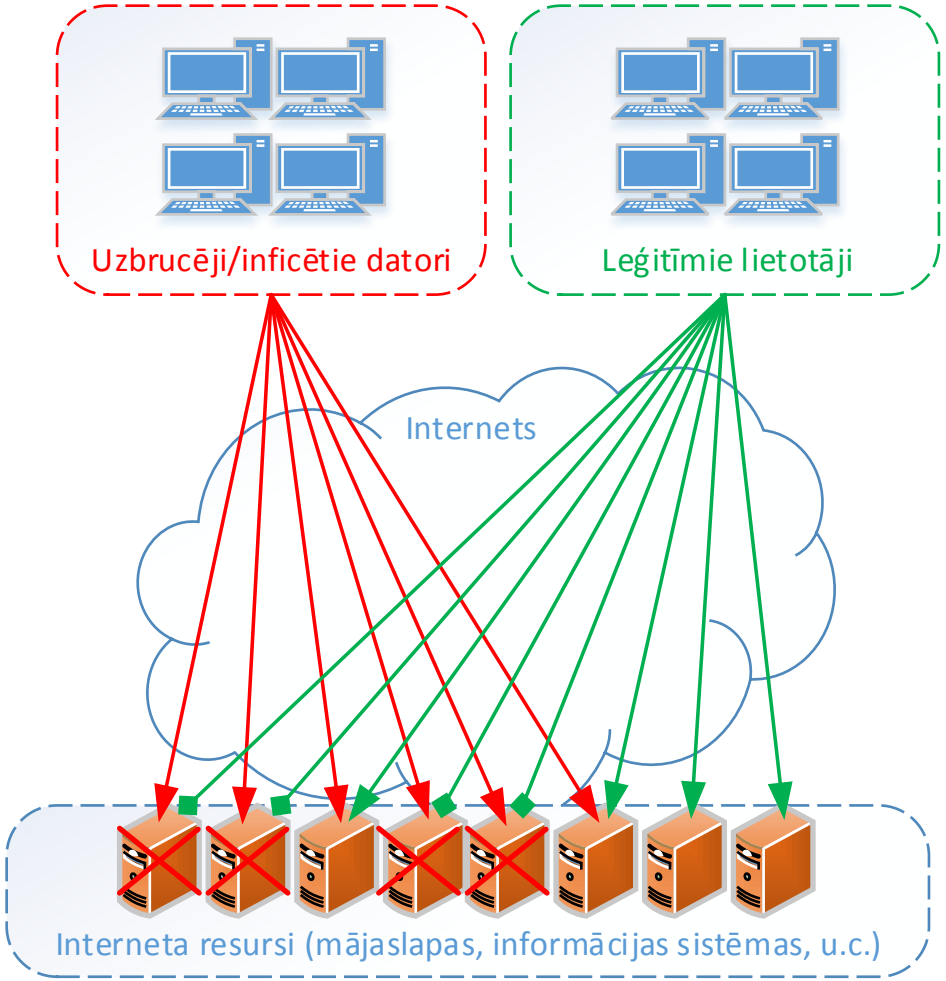
Pieejamība atkarīga no vairākiem faktoriem, kur viens no neparedzamākajiem un ietekmīgākajiem ir piekļuves lieguma jeb DoS uzbrukumi.

Kas ir DoS (Denial of Service) uzbrukums?

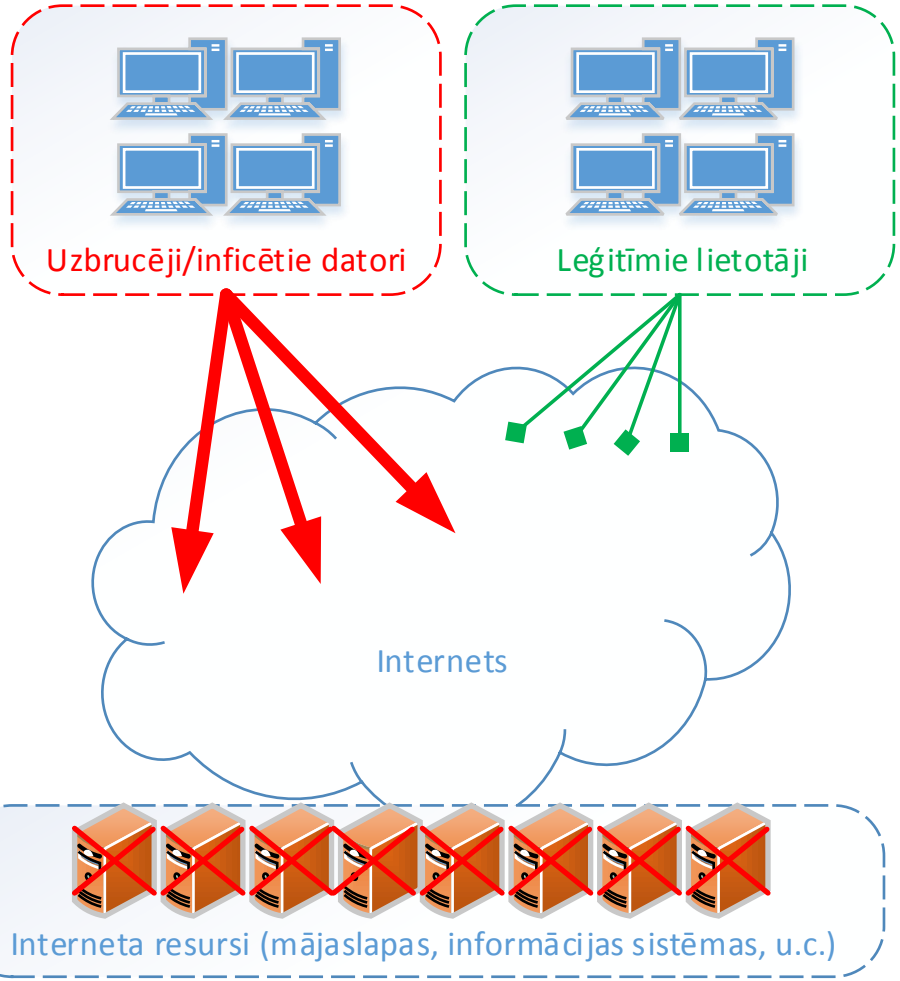
Mēģinājums padarīt konkrētu interneta resursu nepieejamu tā lietotājiem.



Uz konkrētu resursu vērsts



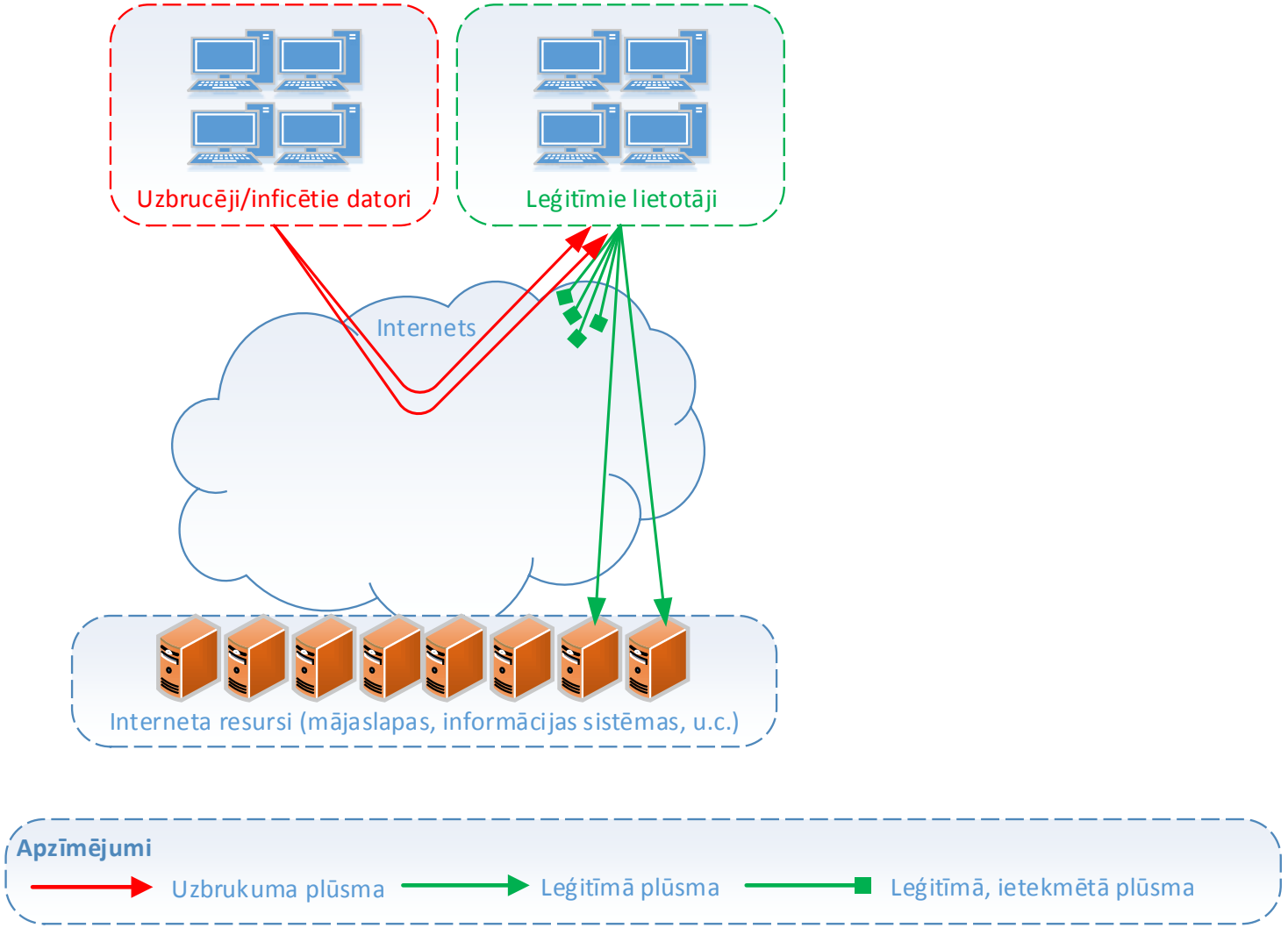
Uz pakalpojuma sniedzēju vērsts



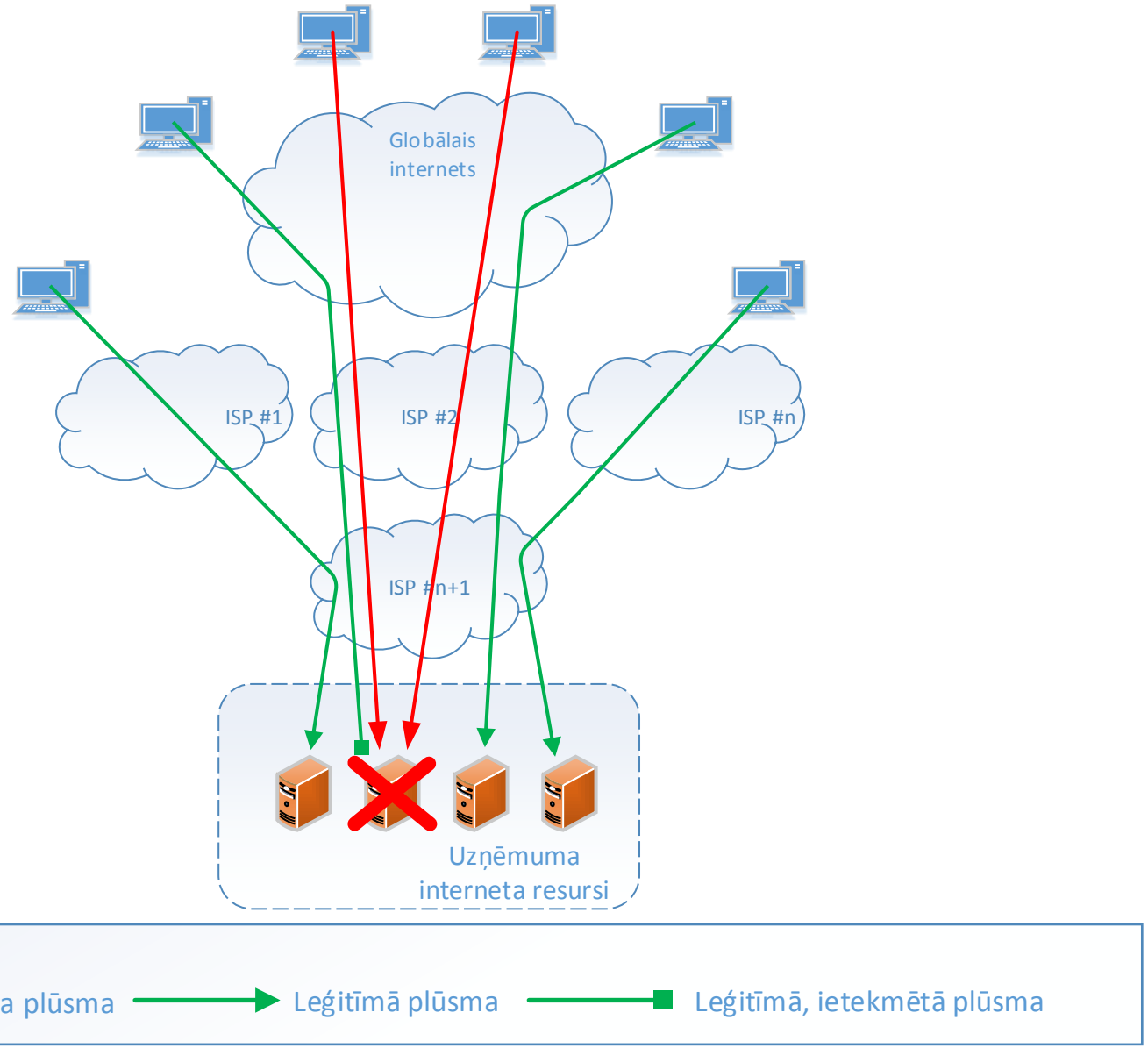
Apzīmējumi

Uzbrukuma plūsma — Leģitīmā plūsma — Leģitīmā, ietekmētā plūsma

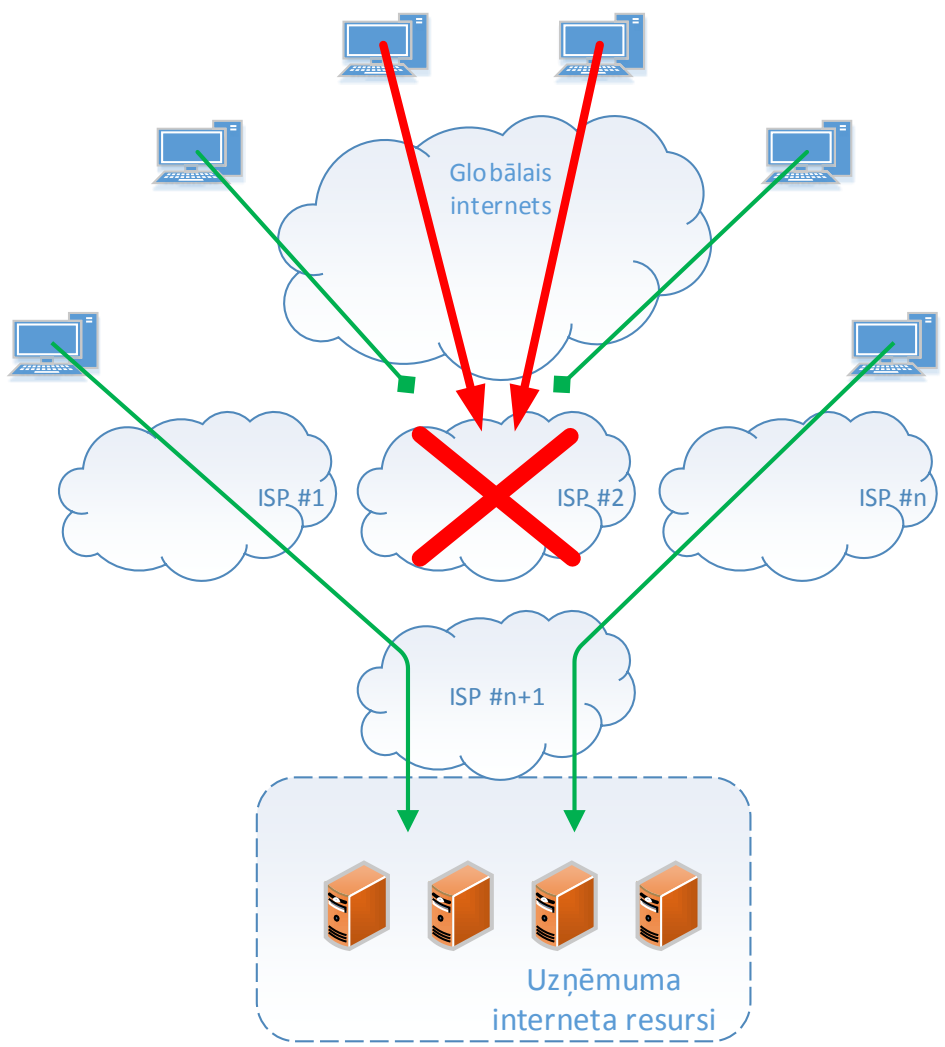
Uz resursu lietotājiem vērsts

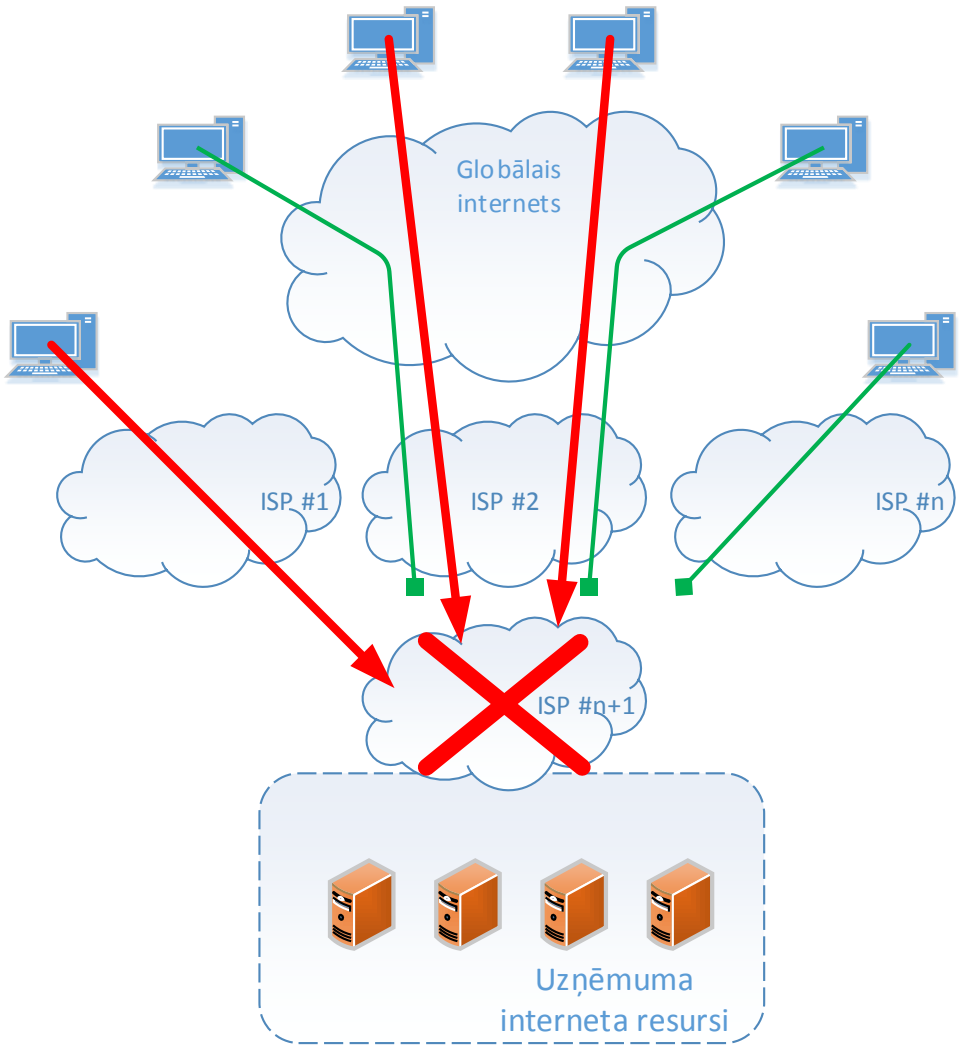


Maza joslas platuma uzbrukumi



Apjoma uzbrukumi

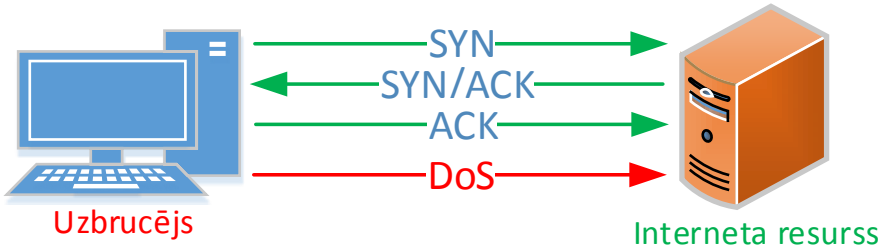


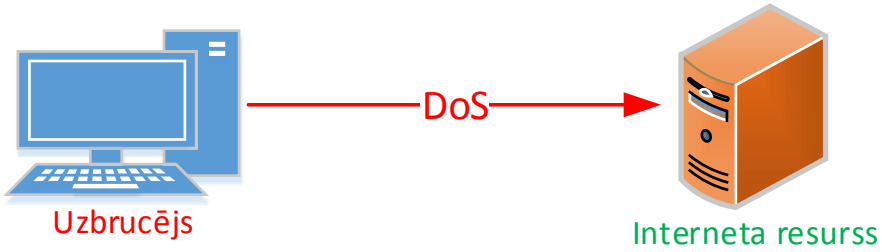


Apzīmējumi

Uzbrukuma plūsma — Leģitīmā plūsma — Leģitīmā, ietekmētā plūsma

Stateful vs stateless





Grūti noskaidrot patieso uzbrukuma avotu == Win/Win situācija uzbrucējam

Galvenie DoS uzbrukumu cēloņi

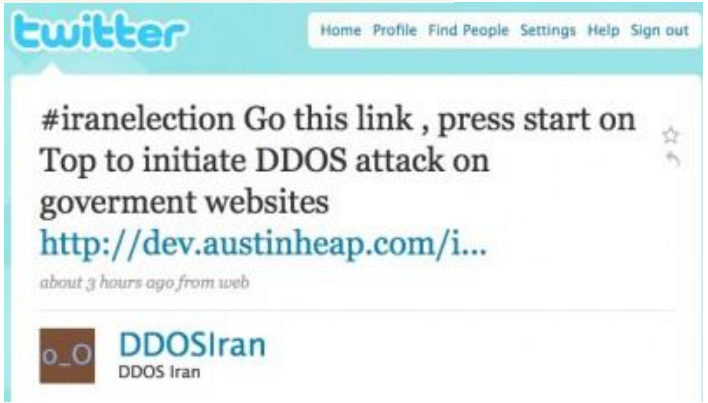
- Politiskās aktivitātes;
- Materiālā labuma gūšana;
- Citu uzbrukumu slēpšana;
- Prieka pēc.

Cik viegli ir veikt DoS uzbrukumu?

- Publiski un bez maksas pieejama programmatūra;
- «DoS kā serviss» pakalpojums;
- Ar vienu datorpeles «klikšķi».

Secinājums: Uzbrukumus jebkurā laikā var veikt jebkurš, kam ir piekļuve internetam.

Uzbrukumi var būt nedēļām ilgi.



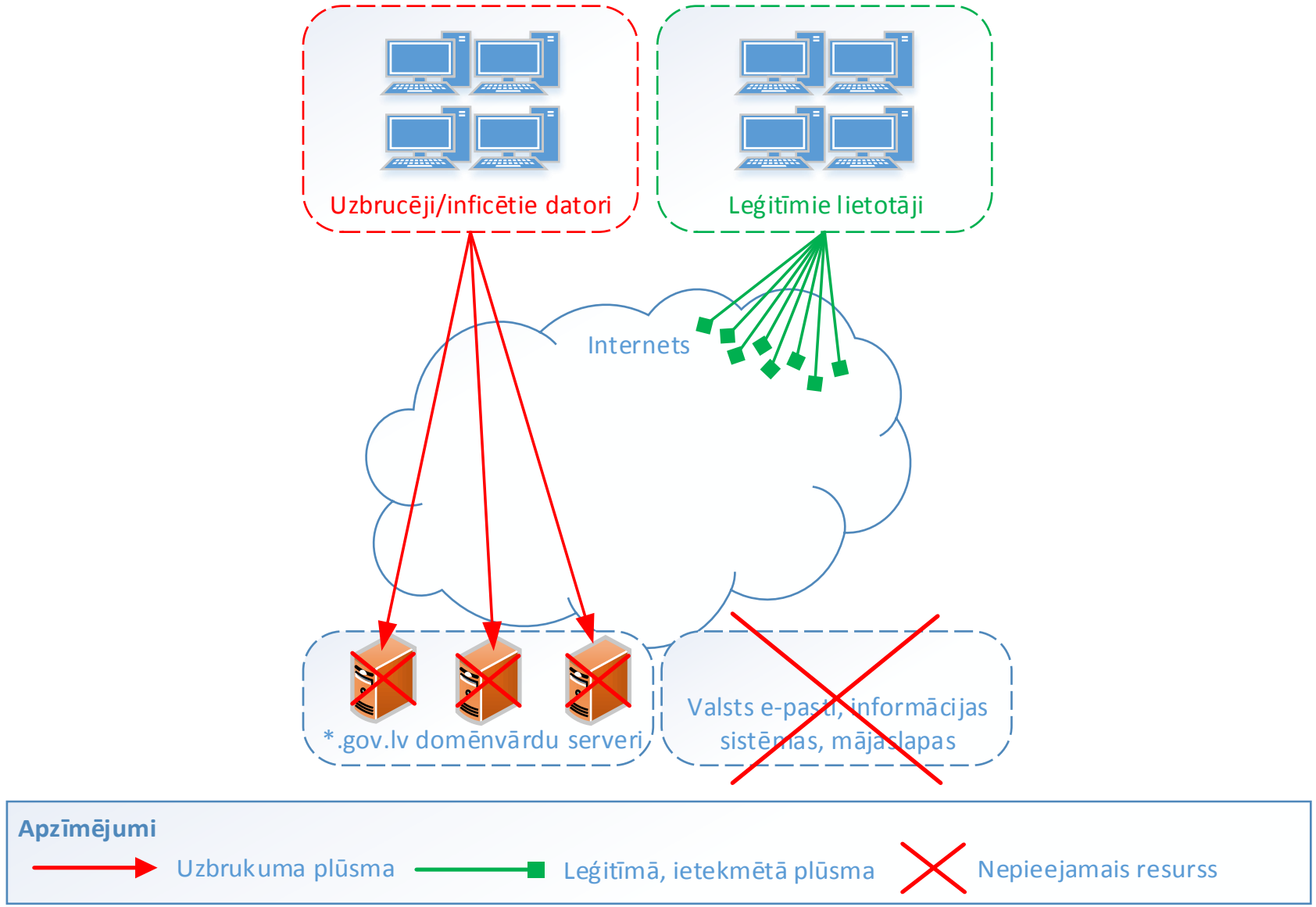
Uzbrukumu ietekme

Izvēloties pareizu uzbrukuma mērķi, ietekme var būt milzīga.

Mērķtiecīgi uzbrukumi tiek veikti brīžos, kad resursu nepieejamība atstāj vislielākās sekas gan finansiālā, gan reputācijas ziņā.

- Reputācija;
- Materiālie zaudējumi;
- Stress;
- Valsts funkcijas tiek apturētas.

Uzbrukums *.gov.lv domēnvārdu serveriem



Kaimiņvalstu pieredze

Ziņu dienesti, valsts pārvalde;

>100Gbit/s;

>50Mpps.

CyberBerkut

ICMP/UDP → SSL

Nopietnu uzbrukumu varbūtība

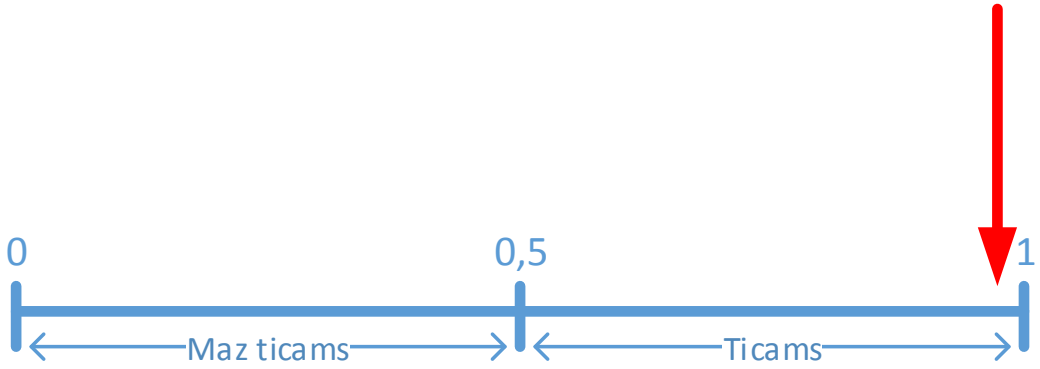
- Pieredze;

  +

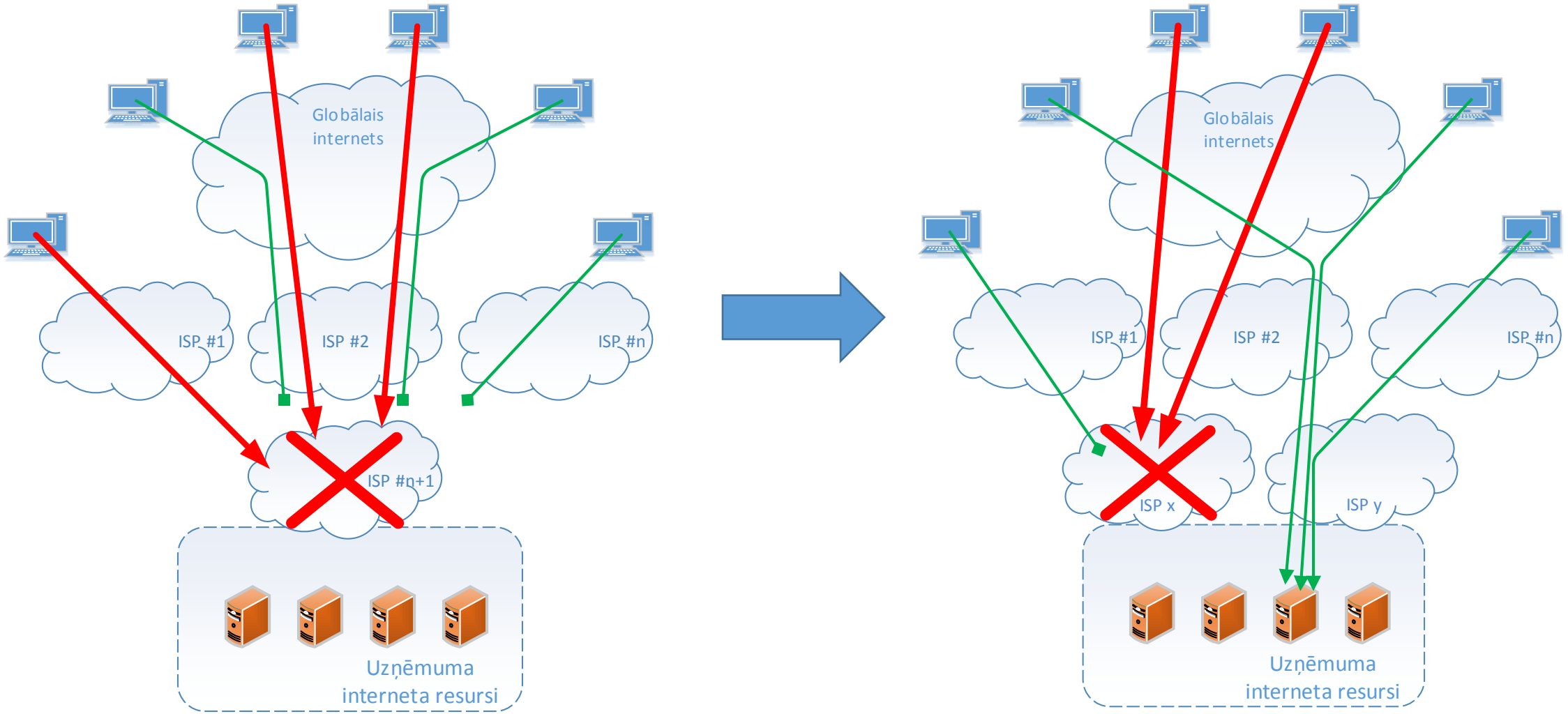
- Galveno uzbrukumu cēloņu analīze;

  +

- Uzbrukumam nepieciešamo rīku pieejamība.



Ietekmes mazināšana #1



Ietekmes mazināšana #2

- Procedūra kā rīkoties uzbrukuma gadījumā:
  - Novēršana;
  - Klientu informēšana.
- Infrastruktūras uzraudzība (SNMP, NetFlow, u.c.);
- Regulārs ārējā perimetra IT drošības audits;
- Programmatūra.

Secinājumi

- Balstoties uz kaimiņvalstu pieredzi, ES prezidentūras laikā (kā arī pēc tam) valsts kritiskie interneta resursi tiks pakļauti apjomīgiem uzbrukumiem;
- Ir preventīvo pasākumu kopa, ko veicot, uzbrukumu radītā ietekme uz kritiskajiem interneta resursiem tiks minimizēta;
- Preventīvos pasākumus jāsāk ieviest jau tagad, jo Latvijas prezidentūra ES sāksies 2015. gada 1. janvārī.

Paldies par uzmanību!