Aizsardzības ministrija

Aktualitātes Latvijas kibertelpā.

Edgars Kiukucāns
Kiberdrošības politikas departamenta direktors
Edgars.Kiukucans@mod.gov.lv

Aizsardzības ministrija

Situācija Latvijas kibertelpā

Situācija Latvijas kibertelpā ir stabila, bet ar augsta riska potenciālu plašākiem incidentiem

Uzsvars uz tehniski vienkāršiem uzbrukumiem (ar izņēmumiem). Turpinās DDoS un pikšķerēšanas uzbrukumi

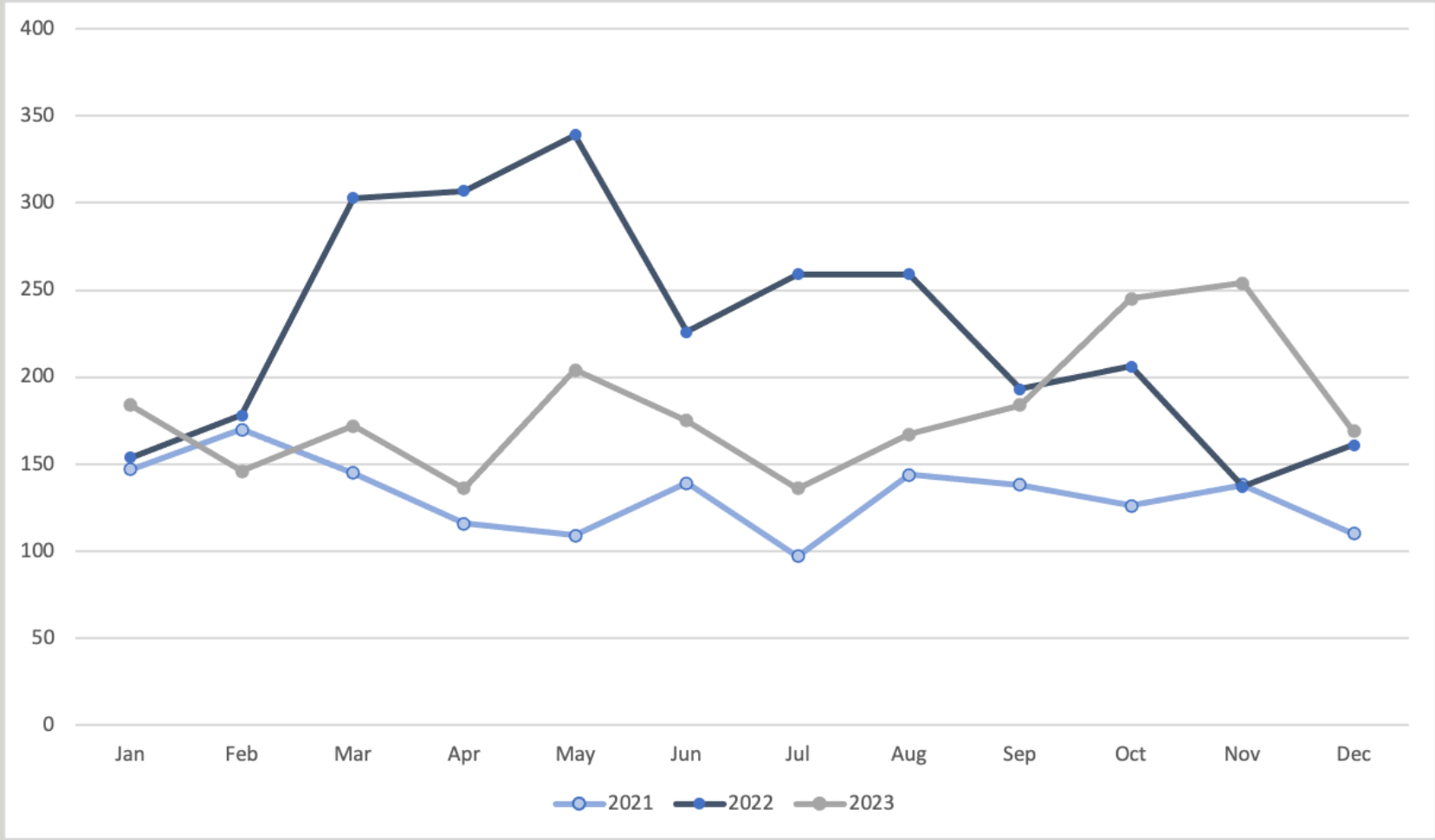
Vairums uzbrukumu nāk no aktieriem / grupējumiem saistītiem ar Krievijas Federāciju, aktivitātes neslēpjot

Pieaudzis dažādu krāpniecisko aktivitāšu skaits (Latvijas Pasta, Valsts policijas u.c. vārdā)

Uzbrukumi notiek viļņveidīgi, bieži saistīti ar politiskām vai sociālām aktivitātēm

Aizsardzības ministrija

Saņemto ziņojumu skaits par incidentiem 2021/2022/2023.g.



Aizsardzības ministrija

Kiberdrošības politika – pamatprincipi un atbildības

PAMATPRINCIPI

- **Visaptverošās valsts aizsardzības sistēmas elements**
- **Daļēji centralizēts modelis**, kas balstās uz savstarpēju sadarbību
- **Nacionālā IT drošības padome** – centrālais nacionāla līmeņa formāts informācijas apmaiņai un sadarbības veicināšanai

Aizsardzības ministrija

- Izstrādā nacionālo kiberdrošības stratēģiju, nozares politiku, normatīvos aktos un koordinē starptautisko sadarbību

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

- Sniedz atbalstu valsts institūcijām IT drošības jomā, un IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns
- Organizē informatīvus un izglītojošus pasākumus

MILCERT.LV

- Nodrošina AM un tās padotības iestāžu, tostarp NBS informācijas un komunikācijas tehnoloģiju uzraudzību

SATVERSMES AIZSARDZĪBAS BIROJS
EXPLORARE ET SERVARE
LATVIJAS REPUBLIKA

- Sadarbībā ar CERT.LV nodrošina kritiskās infrastruktūras aktuālo risku novērtēšanu un pārvaldīšanu

Aizsardzības ministrija

Kiberdrošības stratēģija 2023-2026

Galvenie darbības virzieni:

- Kiberdrošības pārvaldības pilnveidošana
- Kiberdrošības veicināšana un izturētspējas stiprināšana
- Sabiedrības izpratne, izglītība un pētniecība
- Starptautiskā sadarbība un tiesiskums kibertelpā
- Kibernoziedzības novēršana un apkarošana

Galvenie jaunie elementi:

- Jaunais pārvaldības modelis
- Publiskā-privātā sektora sadarbības uzlabošana
- Vienotas kiberhigiēnas vadlīnijas
- Kiberdrošības pratības veicināšana, izglītošanas veicināšana
- Plašāka kiberelementu izspēle teorētiskās un praktiskās mācībās

Aizsardzības ministrija

Aktivitātes kibernoturības veicināšanai

Centralizētie pakalpojumi

- DDoS
- DNS Ugunsmūris
- AB sensori
- Ielaušanās testi

Informatīvās aktivitātes

- Sektorālie semināri
- "Check-list"
- Regulāri brīdinājumi par ievainojamībām

Draudu medību operācijas




CVD

- CERT.LV koordinētais ievainojamību atklāšanas process (CVD platforma) jeb "baltie hakeri"

Aizsardzības ministrija

2024. gada prioritātes

Nacionālā kiberdrošības centra izveide (papildu personāls, struktūras izmaiņas, jaunas uzraudzības funkcijas)

NIS2 direktīvas pārņemšana (direktīva par pasākumiem nolūkā panākt vienādi augsta līmeņa kiberdrošību visā Savienībā)

Nacionālās kiberdrošības likums

MK noteikumi

Kiberkrīžu vadības plāns

Kiberdrošības stratēģijas 2023.-2026. gadam ieviešana

Aizsardzības ministrija

Nacionālais kiberdrošības centrs

Kiberdrošības politikas veidošana un uzraudzība

Valsts IKT minimālo drošības prasību ievērošanas uzraudzība

NIS2 direktīvas ieviešana un strukturēta prasību uzraudzība

CENTRS

Kiberdrošības incidentu risināšana

Drošības operāciju centri valsts koplietošanas datu centros

Eiropas Kiberdrošības kompetenču centra (ECCC) Latvijas NCC

Aizsardzības ministrija

NIS2 direktīva

Direktīvas mērķis

nodrošināt vienādi augstu kiberdrošības līmeni visā Eiropas Savienībā

Atbilstības un ziņošanas pienākumi

Saskaņota kiberrisku pārvaldība

Direktīvas subjektu uzraudzība

Aizsardzības ministrija

Paldies par uzmanību!