Kiberuzbrukums notiks! Kā rīkoties tā laikā

Artūrs Filatovs
Latvijas Valsts Radio un Televīzijas Centrs
Kiberdrošības Biznesa virziena Vadītājs

LVRTC

ŠODIEN PAR

Kiberdrošības situācija un ko sagaidīt 2023	**Kiberuzbrukums/ Kiberincidents/ kiberkrīze**	**Sagatavoties situācijai**
Kiberkrīzes novēršana	**Secinājumi, atskaites, uzlabojumu plānošana**	**Uzlabojumu ieviešana un validēšana**

KIBERDROŠĪBAS SITUĀCIJA ES

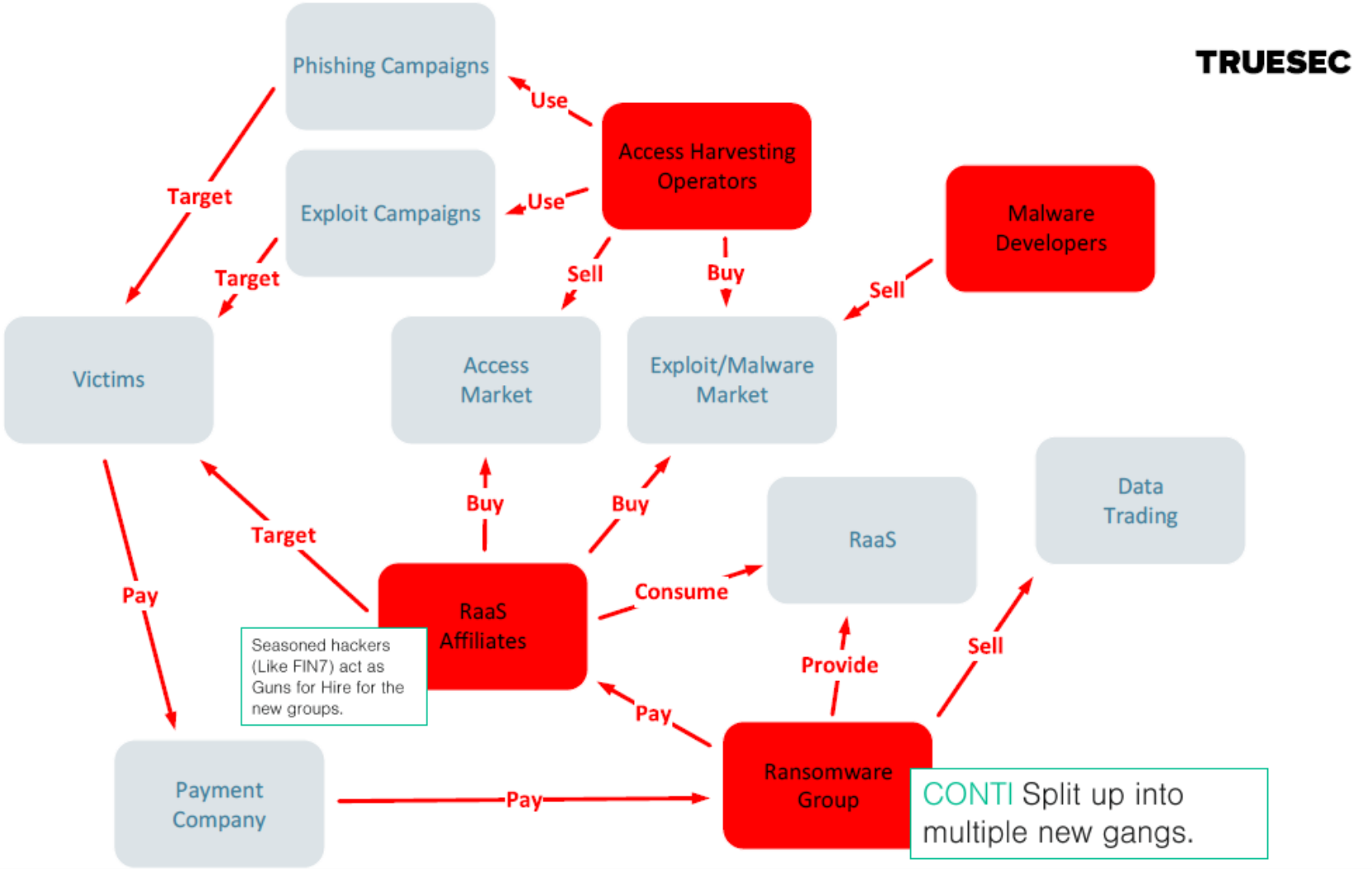
- 95,3% gadījumu nav zināms, kā kibernoziedzinieki ieguva sākotnējo piekļuvi mērķa organizācijai;
- Tiek lēsts, ka vairāk nekā 60% no skartajām organizācijām, iespējams, ir maksājušas izpirkuma maksu;
- Aptuveni 58,2% no visiem nozagtajiem datiem satur GDPR personas datus.

LVRTC

APDRAUDĒJUMUI 2022 UN IZAICINĀJUMI 2023

- **Ransomware –** ir un būs par vienu no top prioritātēm ar ko cīnīsies EU uzņēmumi.
- **0-day ievainojamības -** arvien ātrāk tās tiek izmantonas un arvien grūtāk mazināt incidenta riskus
- **Ģeopolitika -** joprojām spēcīgi ietekmēs IT operācijas un kiberdrošību reģionā
- **Desktruktīvi uzbrukumi**– Krievijas un Ukrainas situācija tikai vēl eskalēsies, EU atbalsts radīs jaunus kiberriskus no terorisma atbalstošam valstīm
- **Hacker-as-a-service** - biznesa modelis kļūst arvien populārāks, un tas aug kopš 2021. gada.
- **DDOS** - Ievērojams pieaugums DDOS uzbrukumu pieejamībai, un notiekošais karš ir galvenais šādu uzbrukumu iemesls.
- **Hacktivism22** - Jauns haktivisma22 vilnis ir novērots īpaši kopš Krievijas un Ukrainas krīzes sākuma

Hacker-as-a-service – kibernoziegums kā bizness



- No 1 EUR mēs tērējam kiberdrošībai, kibernoziedznieki saņem 8 EUR
- Kiberdrošības tirgus 2023 gadā tiek lēst +- 1,6 -2 Triljoni
- Ikgadējais kibernoziedzības tirgus pieaugums ir ~ 15%
- Līdz 2025. gadam kibernoziedzības tirgus pieaugs līdz 10,5 triljoniem USD

Kiberuzbrukums = Kiberincidents vai Kiberkrīze

- **Kiberincidents (negadījums)** –ir situācija, kas sākotnēji ir neliela un var izraisīt krīzi, kas var izraisīt zaudējumus vai darbības traucējumus. Kiberincidents neparalizē visu uzņēmumu kritisko sistēmu darbību, bet gan ir atiecināms uz konkrētu servisu vai IT sistēmu darbības traucējumu.

- **Kiberkrīze** - ir situācija, kas ir lielāka un nopietnāka salīdzinājumā ar kiberincidentu. Krīze var radīt lielāku nenoteiktību un traucēt kritiskās uzņēmumu sistēmas tā kad uzņēmuma darbība ir apdraudēta un pilnībā apturēta.

LVRTC

MĀJASDARBS PIRMS KIBERKRĪZES

IT drošības pārvaldība un noturība, IT perimetrs

Regulējumi, MK Noteikumi, standarti, likumi

Galveno Kiber apdraudējumu identificēšana

Plānu esamība un to validācija (CCP, IRP, DRP, CP)

Kiberkrīzes komandas izveide un apmācība

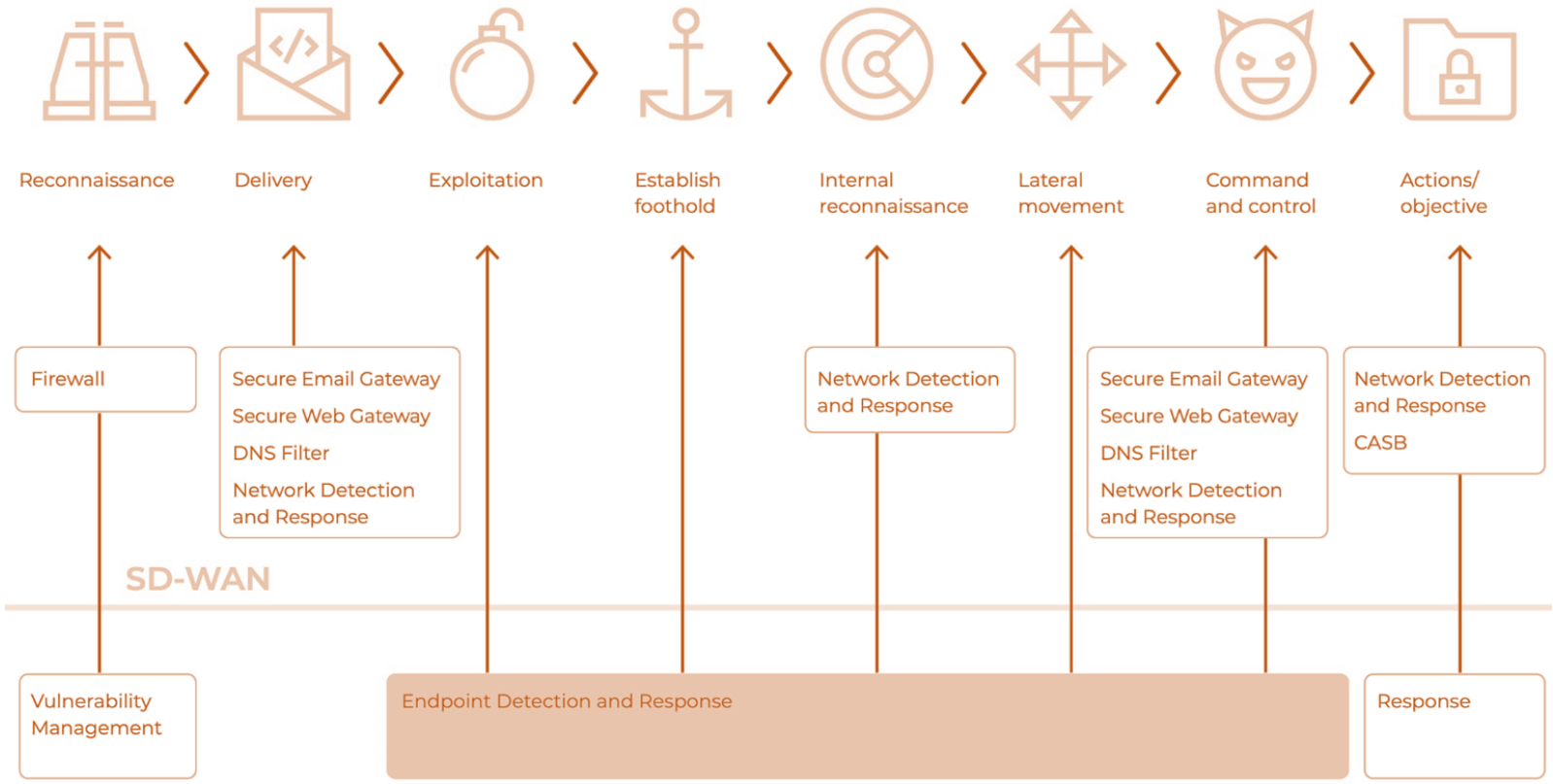
Darbinieku iesaiste, kiberhigēna, apmācības

IETEIKUMI KIBERKRĪZES PLĀNA IZVEIDEI

- Izveidojiet ārkārtas kiberdrošības incidentu reaģēšanas komandu
- Definējiet, ko kiberdrošības krīze nozīmē jūsu organizācijai
- Izveidojiet eskalācijas procesa blokshēmas krīzes situācijām
- Izveidojiet saziņas veidnes kiberdrošības krīzes situācijās
- Izveidojiet kiberkrīzes komandas diagrammu un uzskaitiet ārkārtas kontaktpersonas ātrai saziņai un sadarbībai


LVRTC
Ko darīt lai kiberincidents nepāraug kiberkrīzes situācijā?

UZBRUCĒJU SOĻI UN MŪSU AIZSARDZĪBAS IESPĒJAS



Cloud Security pakalpojums

DDOS Pakalpojums

XDR Pakalpojums

LVRTC

PIRMĀS MINŪTES KIBERUZBRUKUMA LAIKĀ

1. Darbiniekam, kurš pirmais saskaras ar apdraudējumu, ir jābrīdina IT personāls un vadība
2. IT personālam jāizolē IT sistēma no tīkla un jāuzsāk infekcijas dokumentēšana
3. Uzņēmumam jāpārbauda rezerves kopijas mākonī
4. IT komandai uz vietas jāsāk īstenot kiberdrošības protokoli (IRP,DRP u.c)
5. IT komandai jāpievērš darbinieku uzmanība un jāizglīto viņi par uzbrukumu vai infekciju
6. Izmantojiet drošības sistēmas, lai izsekotu iespējamos ļaunprātīgos rīkus (SOC, SIEM, XDR, Flow)
7. Pārliecināties ka visas darbības tika izpildītas un krīzes situācija novērsta

Kiberkrīze ir klāt

LVRTC

KIBERKRĪZES GRUPAS SASAUKŠANA

- Kiberkrīzes komandā (KK) jāiekļauj incidentu reaģēšanas vadītājs, kas var būt IT direktors un IT drošības pārzinis, vairāki kiberdrošības analītiķi un draudu pētnieki, tīkla speciālisti, ārējie kiberdrošības pakalpojumu sniedzēji.
- KK komanda koordinēs darbību ar dažādu uzņēmuma ieinteresēto pušu pārstāvjiem – Vadība/HR/PR/Riska novērtētāji/Juristi/
- Kiberdrošības speciālistu komanda izmeklēs kiberuzbrukumu, bet pārējie atbalstīs darbu un mazinās kaitējumu, ar ko uzņēmums saskarsies.
- Tiesībaizsardzības iestāžu un varasiestāžu informēšana

LVRTC

PADZIĻINĀTA KIBERINCIDENTA IZMEKLĒŠANA

Incidenta atklāšana

Drošības incidenta atklāšana var notikt dažādos veidos:

- Par pārkāpumu ziņo darbinieks/gala lietotājs/klients;
- Atklātas aizdomīgas darbības vai notikums;
- Kāda no drošības uzraudzības sistēmām atklāj drošības incidentu un paziņo par to;
- Drošības analītiķis atklāj aizdomīgas darbības vai incidentu.

Sākotnēja izmeklēšana

Sākotnēji zināmās informācijas ievākšana un apkopošana:

- Cēlonis;
- Tīkla informācija;
- Riska līmenis;
- Iesaistītie lietotāji;
- Noskaidrot, vai nepieciešama padziļināta izmeklēšana;
- Klienta informēšana par drošības incidentu.

Kategorizē-šana

Tiek noteikts:

- Konkrēts incidenta risks;
- Notikušā incidenta ietekme un sekas;
- Tehniskā resursa stāvoklis.

Izmeklēšana

Visas nepieciešamās informācijas ievākšana, apkopošana un padziļināta izpēta, lai noskaidrotu:

- Galveno incidenta iemeslu;
- Iespējamās darbības incidenta seku novēršanai;
- Preventīvās darbības.
- Ārējo kompetento iestāšu piesaiste

Risinājums

- Pielāgota un individuāla risinājuma sniegšana, kas piemērots konkrētajam incidentam;
- Sistēmu atjaunināšana
- DRP iedarbināšana
- Risinājuma soļu veikšanas ieviešana un uzraudzība.

Secinājumi

Līdz ar incidenta ietekmes vai seku novēršanu:

- Pilna atskaite par incidentu, ietekmi, riskiem u.c
- tiek apkopota visu veikto darbību informācija un iekļauta vienotā vai īpaši pielāgotā nodevumā;
- Uzlabojumu plāna izveide un finansiālie aprēķini

AKTĪVU NOROBEŽOŠANA UN KIBERDROŠĪBAS NODROŠINĀŠANA

- KK nekavējoties pārliecinās, ka kiberincidents ir kontrolēts un izolēts IT sistēmā. Ja nē, tad tiek izolēta tīkla daļa, uz kuru ir mērķēts kiberuzbrukums.
- KK ir jāpārliecinās, ka uzbrukuma vai ielaušanās pamatcēlonis vai cēloņi joprojām nav saglabājušies IT sistēmās/Tīklā
- Jāapskata visi uzņēmuma aktīvi un jāpārbauda, vai tiem nav nodarīti bojājumi.
- Kad tīkls ir drošībā, KK komanda nodrošina iespēju nekavējoties atjaunot uzņēmuma darbībai kritiski svarīgās IT sistēmas

DOKUMENTĒŠANA UN IZMEKLĒŠANA

- KK komanda vēlreiz pārbauda notikumus, lai noskaidrotu faktus.
- Pārbauda, kas notika uzbrukuma atklāšanas laikā un kā uzbrukums attīstījās vēlāk. Jānosaka uzbrukuma veids un tā galvenie cēloņi.
- Izmeklēšanā vienmēr jāievēro kiberdrošības plānā noteiktie soļi un ik uz soļa jāstrādā saskaņā ar uzņēmuma politikām un viss jādokumentē lai to vēlāk varētu iesniegt kompetentajām iestādēm (DVI, Cert.lv, VP, FKTK, VDD...)

ATBILSTĪBAS PRASĪBU IEVĒROŠANA UN KOMUNIKĀCIJA AR SABIEDRĪBU

- KK komandai kopā ar vadītājiem, PR dienesta un juridiskā dienesta (vai citiem atkarībā no situācijas) darbiniekiem pirms informācijas izpaušanas jārīko sanāksme, lai pārrunātu visus incidenta aspektus un pieeju sabiedrības informēšanai
- GDPR - 72h
- NIS2 – 24h

Paldies par uzmanību!