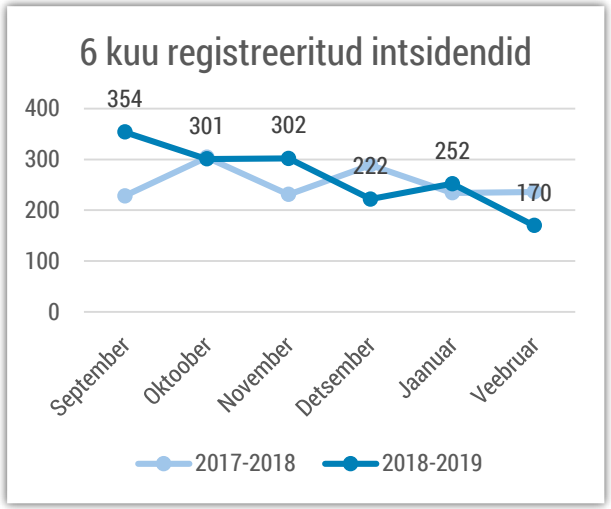
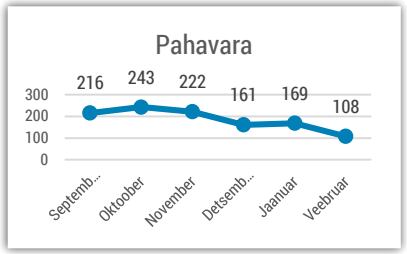
Olukord küberruumis – veebruar 2019

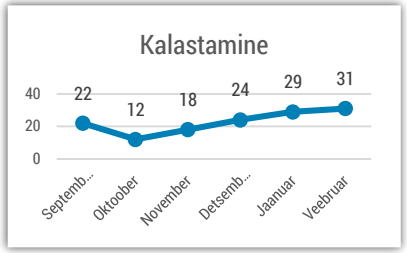
- Veebruaris registreerisime 170 intsidenti, mida oli vähem kui jaanuaris ning mullu samal ajal.
- Täheldasime suuremate mõjudeta pahavara Loki-Bot lainet ja pankadega seotud õngitsuskampaaniat.
- Riigikogu valimiste ajal pöörasime eraldi tähelepanu valimistehnoloogiate turvalisusele.
- Venemaa katsetab Runeti lahti ühendamist internetist.
- Ukraina valmistub võimalikuks välisriigi mõjutuskampaaniaks küberruumis.



Intsidendid, millel oli mõju infosüsteemide konfidentsiaalsusele, terviklikkusele või käideldavusele.



Hoolimata langustrendist on registreeritud intsidentidest jätkuvalt kõige suurem osa pahavaral. Kõige rohkem saame teateid botnet*-idega nakatunud arvutitest Eesti küberruumis.*



CERT-EE-le edastatud teated edukatest kalastamise (phishing) *intsidentidest on viimaste kuude jooksul tõusutrendis.*

Olukord Eesti küberruumis

Saime jätkuvalt teavitusi ettevõtetelt, kes langesid **meilikontode kaaperdamise järel finantspettuse ohvriks**. Tegemist on samasuguse pettusega, mida oleme kirjeldanud juba septembrikuust – ettevõttele allhanget pakkuva partneri meilikonto kompromiteeritakse. Kliendiga suhtlemine kaaperdatakseja palutakse seejärel tasuda arve uuele pangakontole. Meile teadaolevalt said Eesti ettevõtted veebruaris niimoodi vähemalt 16 000 eurot kahju.

Täheldasime veebruaris õngitsuskirjade lainet, mis püüdsid pankade Swedbank ja SEB sümboolikat kasutades **varastada inimeste internetipankade paroole ning meelitada autoriseerima Smart-ID'ga võltsi internetipanka sisenemist**.

Sügisel Eesti asutusi kimbutanud **kasutajaandmeid varastavat pahavara Loki-Bot märgati taas ringi liikumas**. Sedakorda saadeti pahavaraga nakatatud manusega e-kirju näiliselt Tartu ja Tallinna Ülikooli nimel. Teadaolevalt mõju ei olnud, kuid juhtum näitlikustab vajadust rakendada oma infosüsteemides turvastandardeid, mis oleks ära hoidnud pahavara laine.

Tuvastasime pahavaraga Magecart nakatunud väikseid Eesti veebipoode. **Pahavaraga on võimalik varastada ostu sooritada sooviva kliendi krediitkaardi andmeid**. Tõenäoliselt nakatati veebilehed pahavaraga kasutades ära aegunud tarkvara. Tegu ei ole esimese sellelaadse juhtumiga. Näiteks eelmisel aastal teavitas lennufirma British Airways, et nende kliendiandmed (sh krediitkaardiandmed) on häkkerite poolt varastatud.

Tegevused küberjulgeoleku parandamisel Eestis

Veebruarikuus pöörasime eraldi tähelepanu Riigikogu valimiste turvalisusele. Valimistel on väga palju erinevaid küberturvalisuse aspekte, millega alustasime tööga juba mullu sügisel. Näiteks pakkusime koostöös valimisteenistusega **kandidaatidele ja kampaaniameeskondadele küberhügieeni koolitusi**. Samuti andsime erakondadele võimaluse, et soovi korral võivad meie eksperdid anda **esialgse hinnangu nende meiliserverite ja kodulehekülgede turvapildile**. Pea kõik erakonnad seda võimalust ka kasutasid.

Valitsus eraldas valimiste infosüsteemide info- ja küberturvalisuse taseme tõstmiseks ligi **304 000 eurot**, millega saime **rohkem süsteeme testida, riigivõrgule teenustõkestusrünnete kaitsemeetmed osta ja pakkuda paremat teenindust e-hääletusel osalejatele**.

Üks meie ülesannetest valimiste ajal on majutada, hoida töös ja turvata e-hääletust. E-hääletuse toimumise ajal ühtegi olulise mõjuga intsidenti me ei näinud. Klienditugi aitas jooksvalt valijaid, kelle arvutites valijarakendus tõrkus kas viirusetõrje, aegunud tarkvara või teatud ID-kaartide ja operatsioonisüsteemide koosmõju tõttu.

Lisaks juba tavapäraselt 24/7 toimivale CERT-EE tööle ja e-valimiste intsidente jälgivale rakkerühmale **olime valimisperioodil kõrgendatud valmisolekus**, et Eestis olulise mõjuga küberintsidentide puhul informatsiooni jagamist korraldada. Valimisperioodil ei näinud me ühtegi sellist intsidenti Eesti küberruumis, mis oleks oluliselt mõjutanud valimiste läbiviimist.

Toimusid kahepoolsed läbirääkimised Saksamaa küberjulgeolekuametiga BSI, kus üheks oluliseks teemaks oli sakslaste infoturbe standard IT-Grundschutz, mis on Eestis andmekogusid kasutavatele riigi ja KOV asutustele kohustusliku standardi ISKE alus. Küberturvalisuse strateegia alusel oleme alustanud protsessi, et kirjutada Eesti turvastandard ümber nii, et seda oleks lihtsam ja praktilisem igapäevaselt kasutada. Kohtumiste tulemusel lepiti kokku, et **Eesti jätkab IT-Grundschutzi kasutamist ning uuendatud standard antakse meile kasutusse tasuta**.

RIA ning Politsei- ja Piirivalveameti eestvedamisel **valmis identiteedi- ja dokumendihalduse valge raamat**, mis kaardistab valdkonna hetkeolukorra ja toob välja ekspertide esmased vaated järgneva 10 aasta arengute kohta. Tegu on esimese selle valdkonna dokumendiga, mis kirjeldab identiteedihaldusega seotud osapoolte rolle, trende ning esialgset riski- ja arenguplaani. Raamat on aluseks riigi olulistele strateegiadokumentidele ja arengukavadele ning selle valmimisele on kaasa aidanud hulk riigiasutusi ja asjast huvitatud osapooli erasektorist.

Rahvusvaheline keskkond

Ukraina korraldab koos Euroopa Liiduga ühisõppuseid, mille käigus harjutatakse võitlust Venemaalt pärinevate küberohtudega. Stsenaariumite käigus harjutatakse võimalikke vastutegevusi vastavalt küberrünnetele, sh valimistesse sekkumisel. Ukrainas toimuvad presidendivalimised 31. märtsil. Venemaad on varasemalt süüdistatud teise riigi valimistesse sekkumises.

Venemaa plaanib märtsi õppuse käigus lühiajaliselt ühendada lahti oma interneti (RUNET) selleks, et hinnata taristu vastupidavust välise küberrünnaku korral. Sel ajal ei saa välismaalt ühendust Venemaal asuvate interneti teenustega ning vastupidi – Venemaalt on välised teenused kättesaamatud. Internetivõrgust välja ühendamine ei ole uudne nähtus. Näiteks suleti aastavahetusel Kongo Demokraatlikus Vabariigis internetiühendus rahutuste vältimiseks, kuna sotsiaalmeedias levisid väärad presidendi valimistulemused.

Ühendkuningriigi parlamendi komitee, mis uuris libauudiseid ja desinformatsiooni levikut sotsiaalmeedias, tegi ettepaneku **kohustada sotsiaalmeedia veebilehti järgima eetikakoodeksit**. Veebilehed peaksid olema kohustatud eemaldama oma keskkonnast kahjustavat sisu ning desinformatsiooni levitavaid allikaid. Raportis toodi eraldi välja Facebook, mida süüdistati teadlikult ning kavatsetult privaatsuse ja konkurentsi seaduse rikkumises.

Küberturbeettevõtted avalikustasid raporti, milles on omistanud Hiina häkkerirühmitusele APT10 ühe suurima Euroopa ettevõtetele pilveteenust pakkuva Norra firma Visma ründamise. Sissetung infosüsteemidesse suudeti piisavalt kiirelt tuvastada, nii et kahju piirdus ettevõtte-sisese andmevargusega. Ükski kliendisüsteem ei olnud intsidendist mõjutatud. USA valitsusasutused on hoiatanud pilveteenustele keskenduva häkkimislaine eest koodnimega Operatsioon Cloud Hopper juba alates 2017. aastast.

Poola kaitseminister tutvustas Cyber.mil.pl konverentsil plaani luua küberkaitseüksus, mis tegeleks küberjulgeoleku ohtudega. Üksus moodustatakse Poola Krüptoloogiakeskuse ja Sõjaväe Informatsioonitehnoloogia Inspektsiooni (*Military Inspectorate of Information Technology*) baasil.