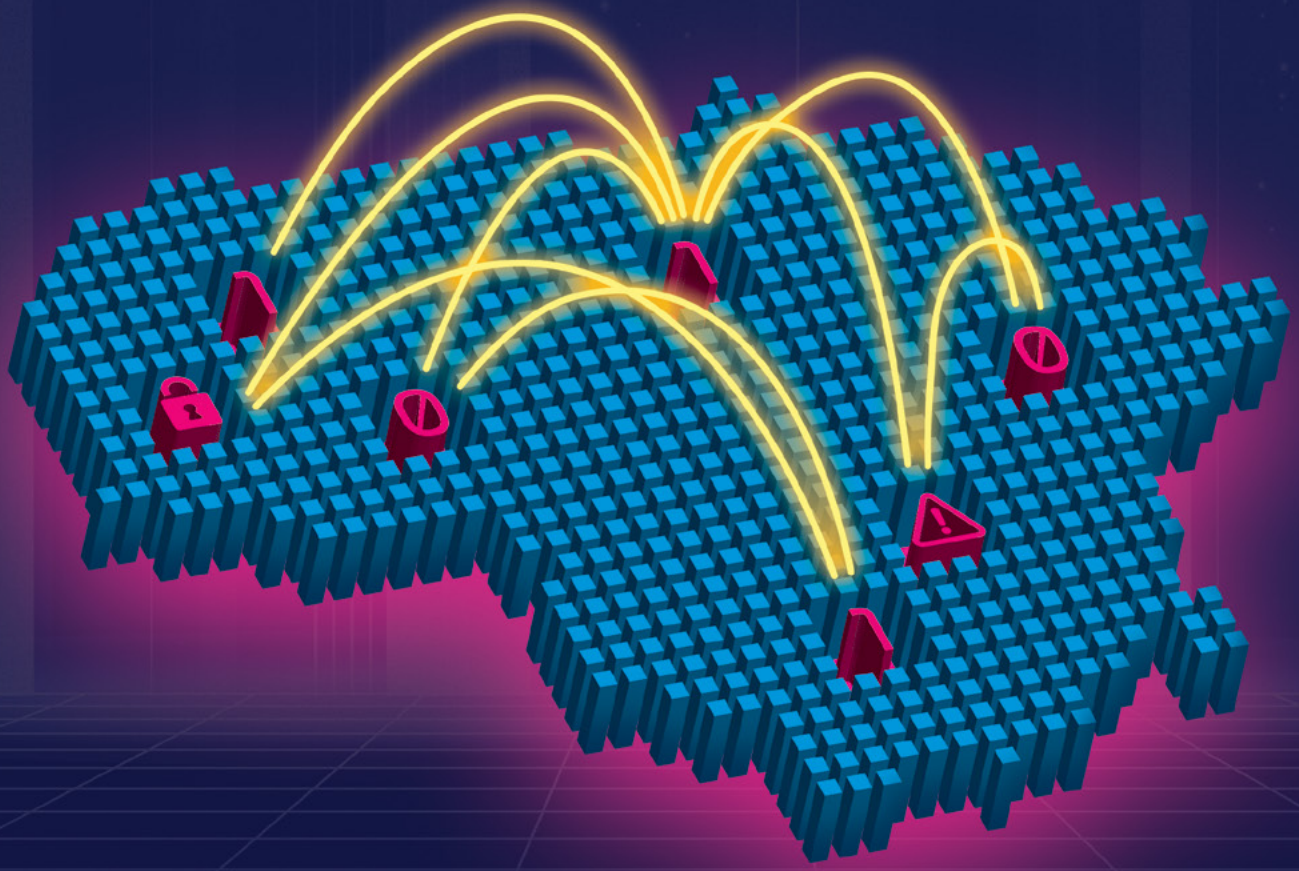
NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2020



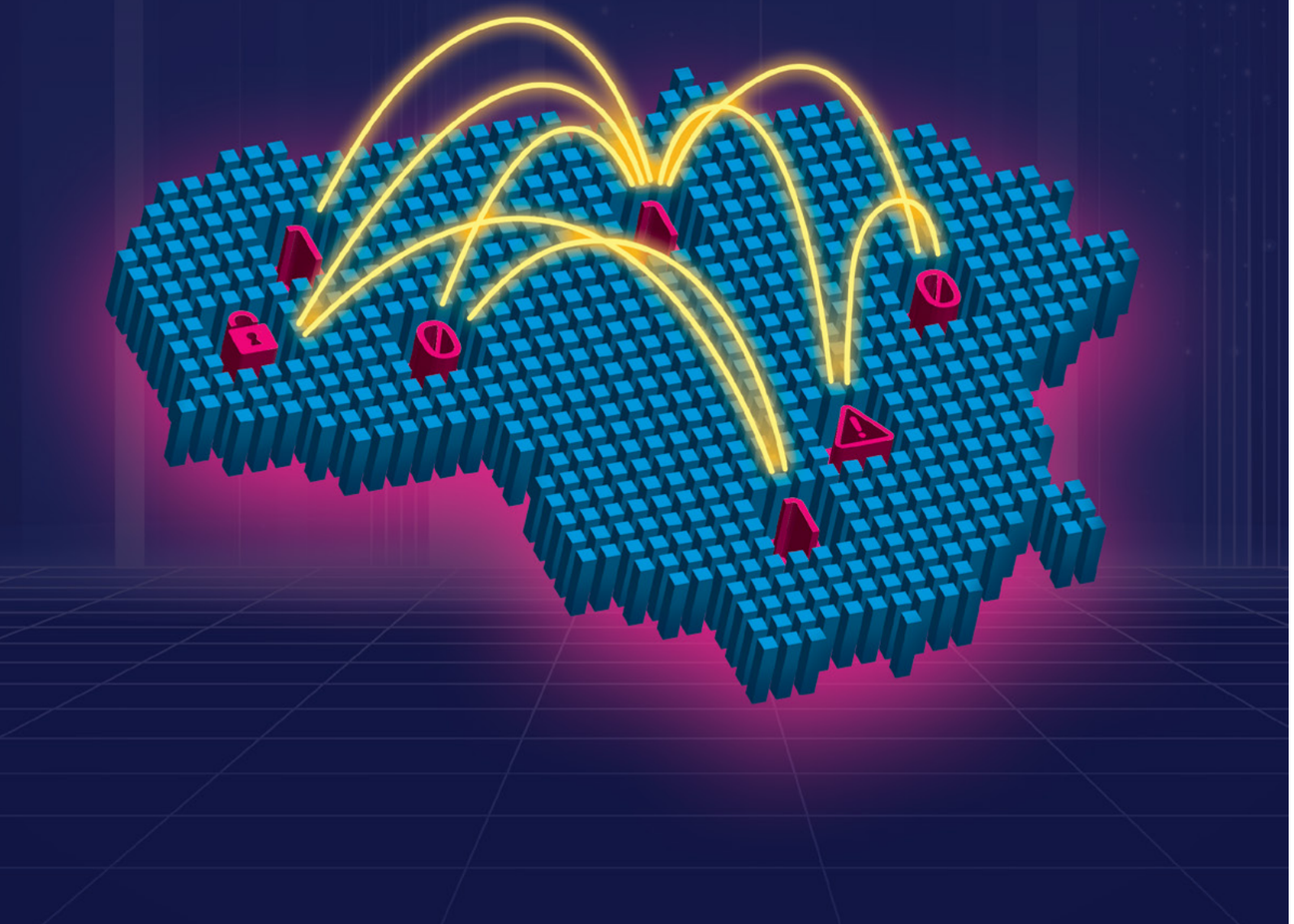
KRAŠTO APSAUGOS MINISTERIJA

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2020

KRAŠTO APSAUGOS MINISTERIJA

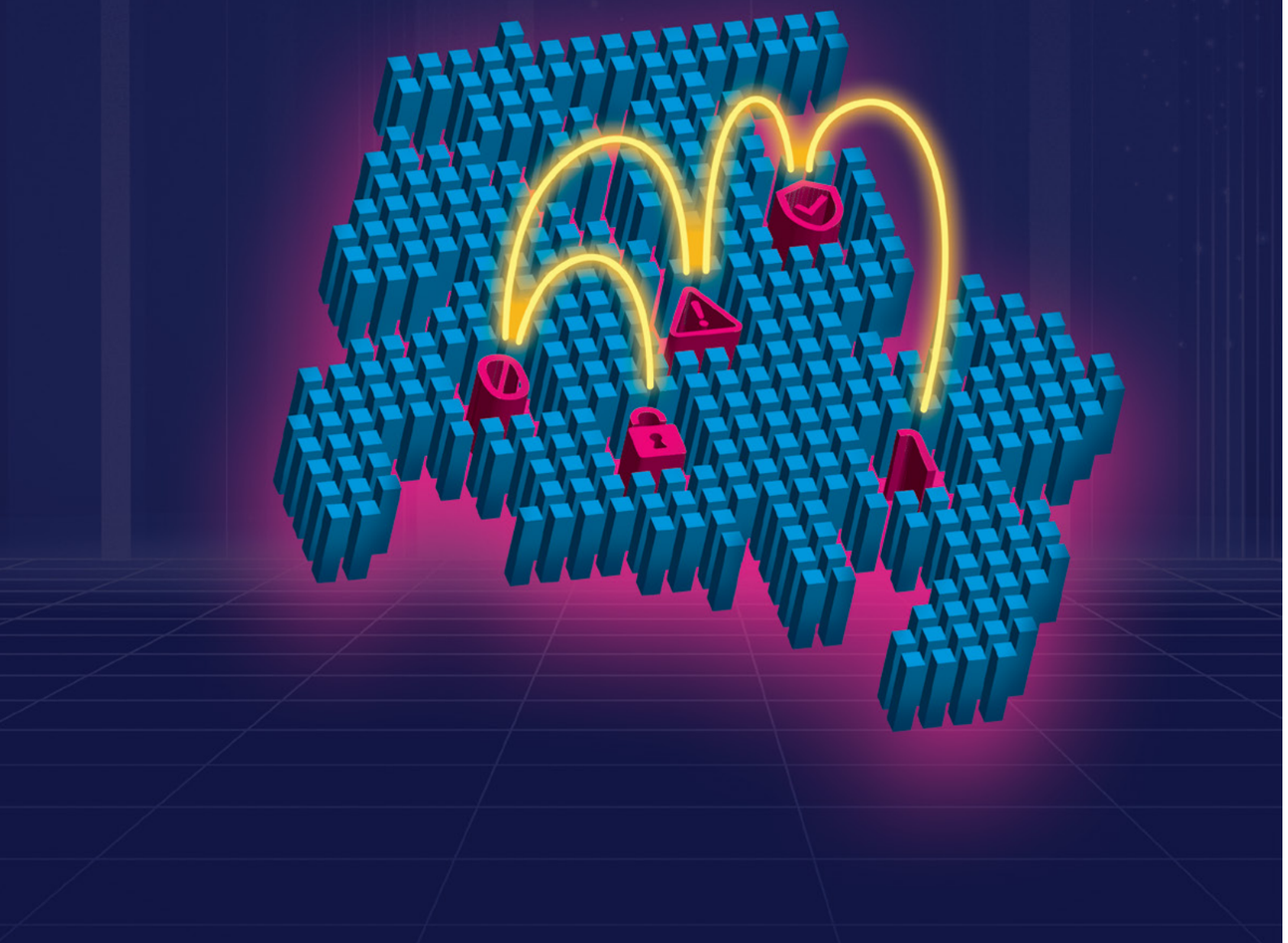
00



Turinys

Dominančią temą galite pasiekti paspaudę ant jos pavadinimo

01 Įžanga



Įžanga

Margiris Abukevičius
Krašto apsaugos viceministras

Nacionalinė kibernetinio saugumo būklės ataskaita teikiama jau penktus metus iš eilės. Joje pristatomi svarbiausi mūsų valstybės kibernetinio saugumo politikos formavimo ir įgyvendinimo rezultatai bei iššūkiai, su kuriais susiduriame.

Pirmą kartą kibernetinio saugumo būklė apžvelgiama plačiau, ne tik iš Krašto apsaugos ministerijos, kaip pagrindinės už kibernetinio saugumo politikos formavimą atsakingos institucijos, perspektyvos. Kitos valstybės institucijos ir įstaigos taip pat prisideda prie kibernetinio saugumo didinimo šalyje: Valstybinė duomenų apsaugos inspekcija – tirdama asmens duomenų saugumo pažeidimo atvejus, Lietuvos policija – vykdydama kibernetinių nusikaltimų prevenciją, užkardymą ir tyrimą, Ryšių reguliavimo tarnyba – siekdama švaresnės kibernetinės erdvės ir saugodama viešųjų elektroninių ryšių paslaugų vartotojų teisę į nepertraukiamą paslaugų teikimą, Lietuvos kariuomenės Strateginės komunikacijos departamentas – vykdydamas priešiškų informacinių operacijų aptikimą ir neutralizavimą.

Kibernetinių incidentų skaičius Lietuvoje, kaip ir visame pasaulyje, kasmet didėja. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos duomenimis, 2020 m. kibernetinių incidentų padaugėjo 25 proc., o su kenkimo programinės įrangos platinimu susijusių incidentų skaičius padidėjo net 49 proc. Tai neabejotinai nulėmė gyvenimo dėl COVID-19 pandemijos perkėlimas į virtualią erdvę bei kitos priežastys, tokios kaip sparčiai augantis prie interneto prijungtų įrenginių skaičius bei kibernetinio saugumo higienos trūkumas. Lietuvos visuomenė, kaip ir kitos pasaulio valstybės, 2020 m. susidūrė su kibernetiniais incidentais ir grėsmėmis. Tai per el. laiškus plintanti „Emotet“ kenkimo programinė įranga, išpirkos reikalavimai, kad nebūtų vykdomi paskirstyto atsisakymo aptarnauti kibernetiniai incidentai (angl. *Ransom Distributed Denial of Service* (RDDoS)), taip pat plintantys JAV kompanijos „SolarWinds“ programinės įrangos atnaujinimai su kenkimo kodu. 2020 m., kaip ir kasmet, daugėjo informacinių atakų skaičius. Nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui skaičius, nors ir nedaug, bet taip pat padidėjo, o elektroninis sukčiavimas buvo vienas dažniausių kibernetinių nusikaltimų. Lietuvos bankų asociacijos duomenimis, 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. Eur.

Vertindami praėjusius metus ir pirmus 2021 m. mėnesius, matome, jog pagrindiniai kibernetinio saugumo iššūkiai yra susiję su žinomų pažeidžiamumų išnaudojimu, paviršutiniškai ar nepakankamai tiksliai vertinamomis informacijos saugumo rizikomis, per lėtai gerėjančia interneto svetainių būkle, stringančiu kibernetinio saugumo reikalavimų įgyvendinimu, kibernetinio saugumo higienos trūkumu, nekritiškai vertinama informacija socialiniuose tinkluose. Kalbant apie kibernetinio saugumo higienos trūkumą, reikėtų pabrėžti, kad privataus sektoriaus atstovai, nepakankamai dėmesio skirdami savo organizacijų kibernetiniam saugumui, padidina kibernetinių incidentų riziką, o jau įvykusių kibernetinių incidentų padarinius gali patirti kiekvienas Lietuvos gyventojas.

Pandemijos išryškintoms kibernetinio saugumo rizikoms didėjant, ypač svarbu, kad kibernetinis saugumas išliktų valstybės politikos prioritetu. XVIII Vyriausybės programos nuostatų įgyvendinimo plane daug dėmesio skiriama šiai sričiai: efektyvesnės ir tarptautinius standartus atitinkančios kibernetinio saugumo reikalavimų sistemos sukūrimui ir griežtesnei reikalavimų laikymosi kontrolei, nepatikimų tiekėjų eliminavimui, kibernetinio saugumo atsparumo didinimui. Numatyti darbai kibernetinio saugumo srityje įpareigoja Krašto apsaugos ministeriją, bendradarbiaujant su kitais viešojo ir privataus sektorių atstovais, mokslo ir studijų institucijomis, siekti didesnio šalies kibernetinio atsparumo ir efektyvesnio kibernetinių incidentų užkardymo, nes kibernetinis saugumas yra visų atsakomybė.

Į turinį

02
Santrauka

01 Kibernetinio saugumo grėsmės, priešiškų valstybių interesai bei visuomenės atsparumo įtaka Lietuvos kibernetinio saugumo būklei

Kibernetinio saugumo rizikos Lietuvoje didėjo

Visą pasaulį apėmusi COVID-19 pandemija, informacinių ir ryšių technologijų (toliau – IRT) plėtra ir nuolat didėjantis prie interneto prijungtų išmaniųjų įrenginių skaičius lėmė, kad 2020 m. kibernetinio saugumo rizikos[01] Lietuvoje didėjo. Registruotų kibernetinių incidentų skaičius per metus išaugo 25 proc., nuo 3241 kibernetinių incidentų 2019 m. iki 4330 incidentų 2020 m.

Kibernetinių incidentų priežastimi dažniausiai tapdavo žinomų pažeidžiamumų išnaudojimas, interneto naudotojų kibernetinio saugumo higienos trūkumas ir socialinės inžinerijos metodais[02] paremti elektroniniai laiškai. 2020 m. Lietuvoje, kaip ir visame pasaulyje, buvo ypač suaktyvėjusi „Emotet" kenkimo programinės įrangos (toliau – PĮ) veikla. Naudotojams neapdairiai atidarius el. laiškuose esančius užkrėstus dokumentus arba paspaudus nuorodas į suklastotas interneto svetaines, buvo sudaromos sąlygos iš galinių įrenginių neteisėtai gauti informaciją ir (ar) toliau vykdyti kitus kibernetinius incidentus. Daugumos kibernetinių incidentų galima buvo išvengti, jei būtų laikomasi kibernetinio saugumo higienos[03] reikalavimų, pvz., laiku įdiegiami programinės įrangos atnaujinimai ar kritiškai vertinama el. laiškais gaunama informacija.

Prie kibernetinio saugumo rizikų didėjimo 2020 m. prisidėjo COVID-19 pandemijos suvaldymui nustatyti apribojimai, dėl kurių daugelio žmonių darbas, ugdymas ir laisvalaikis persikėlė į internetą, gyvus susitikimus pakeitė nuotoliniai, smarkiai išaugo įvairių informacinės visuomenės paslaugų poreikis ir tuo iš karto pasinaudojo piktavaliai. Palyginti su ankstesniais metais, Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) 2020 m. fiksavo 49 proc. daugiau kibernetinių incidentų, susijusių su kenkimo PĮ.

Daugiau dėmesio ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių kibernetiniam saugumui

Tinkamo ryšių ir informacinių sistemų (toliau – RIS) funkcionavimo užtikrinimas yra neatsiejama ypatingai svarbos informacinės infrastruktūros (toliau – YSII) valdytojų ir valstybės informacinių išteklių (toliau – VII) valdytojų ir (arba) tvarkytojų darbo dalis, todėl YSII ir VII kibernetinio atsparumo klausimai yra ypač aktualūs. Deja, ne visais atvejais šie klausimai yra pakankamai efektyviai sprendžiami, todėl kai kurie kibernetinio saugumo subjektai gali būti labiau paveikti kibernetinių incidentų.

2020 m. NKSC atliko 6 kibernetinio saugumo subjektų, valdančių VII ir YSII, RIS patikrinimus dėl atitikties kibernetinio saugumo reikalavimams[04] (toliau – reikalavimai). Rezultatai rodo, kad reikalavimų įgyvendinimo procesas yra vis dar lėtas. Tai lemia ne tik aplaidus VII valdytojų požiūris į reikalavimų įgyvendinimą, kompetentingų kibernetinio saugumo, informacinių technologijų specialistų ir (ar) reikalingos kompetencijos trūkumas, bet ir pačių informacinių sistemų bei registrų sudėtingumas, kurį, savo ruožtu, lemia nuolatinė IRT plėtra.

01
Kibernetinio saugumo rizika – kibernetinio incidento tikimybė ir poveikis.

02
Socialinė inžinerija – tai piktavalio ir potencialios jo aukos kontaktas, manipuliuojant pastarojo emocijomis, siekiant įgyti asmeninę informaciją, prieigą prie duomenų ar kito skaitmeninio turto.

03
Pavyzdžiui, pagrindiniai kibernetinio saugumo patarimai skirti smulkioms ir vidutinėms įmonėms, kuriais gali pasinaudoti ir kiti asmenys, besidomintys savo kibernetiniu saugumu, patraukliai ir suprantamai išdėstyti Krašto apsaugos ministerijos inicijuotame ir 2020 m. birželio mėn. išleistame leidinyje „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas". Leidinį galima rasti Krašto apsaugos ministerijos interneto svetainėje http://kam.lt/lt/naujienos_874/leidiniai/2020_m._isleisti_leidiniai.html

04
Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo".

Į turinį

Nesaugios interneto svetainės

Lietuvoje nuolat augant registruojamų .lt domenų skaičiui ir jam perkopus 200 tūkst. ribą, didėja ir su tuo susijusios kibernetinio saugumo rizikos. Dažniausios nesaugių svetainių priežastys yra prasta jų priežiūra, neatnaujinamos turinio valdymo sistemos (toliau – TVS), vieša prieiga prie svetainių TVS ir nesaugūs slaptažodžiai. Pasinaudodami tuo, piktavaliai į nesaugias svetaines gali ne tik įkelti įvairias melagienas ar tendencingai pateiktą turinį, bet ir jos lankytojus „užkrėsti" kenkimo PĮ, nukreipti juos į kitas suklastotas interneto svetaines ir (ar) pavogti svarbius duomenis. 2020 m. NKSC atliko 734 tūkst. interneto svetainių patikrinimų (interneto svetainės NKSC tikrinamos periodiškai, dažnai po keletą kartų) ir fiksavo 322 svetaines su kenkimo kodais.

NKSC taip pat vykdo periodinius viešojo sektoriaus interneto svetainių pažeidžiamumo patikrinimus ir apie apliktus pažeidžiamumus informuoja šių svetainių valdytojus. Palyginti su ankstesniais metais, viešojo sektoriaus interneto svetainių kibernetinio saugumo situacija šiek tiek pagerėjo, nuo 17 proc. iki 9 proc. sumažėjo svetainių, į kurias lengva įsilaužti, skaičius, tačiau 2020 m. saugios buvo tik buvo 56 proc. viešojo sektoriaus svetainės (2019 m. – 40 proc.). Nors svetainių saugumo problemų yra daug ir jas bandoma spręsti įvairiomis priemonėmis, situaciją sunkina interneto svetainių valdytojų pasyvumas ir nekompetencija, netinkamos sutartys su svetainių kūrėjais, taip pat dažnai neveiklumą yra bandoma pateisinti biudžeto trūkumu arba apeliuojama į ateityje suplanuotus naujų sistemų pirkimus.

Rinkimų į Lietuvos Respublikos Seimą metu didesnių kibernetinių incidentų išvengta

2020 m. įvykę rinkimai į Lietuvos Respublikos Seimą pareikalavo sutelktų NKSC ir Lietuvos Respublikos vyriausiosios rinkimų komisijos (toliau – VRK) pastangų užtikrinant rinkimų kibernetinį saugumą. Pasirengimo laikotarpiu papildomai buvo pasitelktos ir tarptautinės Kibernetinės greitojo reagavimo pajėgos (toliau – pajėgos) (angl. *Cyber Rapid Response Teams* (CRRT)). Specialistai atliko kibernetinio saugumo pažeidžiamumų vertinimą VRK informacinėje sistemoje ir prie rinkimų saugumo užtikrinimo prisidėjo savo ekspertinėmis įžvalgomis.

Pačių rinkimų metu nebuvo nustatyta bandymų neteisėtai prisijungti prie rinkimų informacinių sistemų, tačiau buvo fiksuota išorinė informacinės sistemos perimetro žvalgyba, bendromis NKSC ir VRK pastangomis blokuoti 386 IP adresai, siejami su galimai neteisėta veikla. Kitų incidentų išvengta, todėl galima teigti, kad 2020 m. rinkimai į Lietuvos Respublikos Seimą buvo saugūs.

Sutrikdytų paslaugų žala Lietuvos gyventojams

2020 m. informacinių technologijų saugumo ir kibernetiniai incidentai, sutrikdydami organizacijų ir valstybės institucijų ir įstaigų teikiamas paslaugas, padaro žalos ir gyventojams. Vienas tokių informacinių technologijų saugumo incidentų įvyko 2020 m. liepos mėn., kai po smarkios liūties vanduo pateko į VĮ Registrų centro patalpas ir dėl to buvo sutrikdytas daugiau kaip 20 valstybės registrų ir valstybės informacinių sistemų darbas. Laikinai nebuvo pasiekiami tokie pagrindiniai valstybės registrai kaip Lietuvos Respublikos gyventojų registras, Juridinių asmenų, Nekilnojamojo turto kadastras ir registras. Ilgiausiai užtruko atkurti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinę sistemą (toliau – e. sveikatos sistema). Šios sistemos atkūrimo laikas neatitiko jai numatyto maksimalaus priimtino paslaugos neveikimo laiko.

Lietuvos gyventojai galėjo patirti žalą ir 2020 m. gruodžio 29 d., kai, siekiant sustabdyti per el. laiškus plintančią „Emotet" kenkimo PĮ, buvo laikinai apribotas Nacionalinio visuomenės sveikatos centro (toliau – NVSC) elektroninio pašto veikimas ir dėl to sutrikdytas informacijos gavimo ir teikimo visuomenei procesas.

Dalis kibernetinių incidentų yra siejami su Rusija ir svarbiausiais įvykiais Lietuvoje

Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos ir Lietuvos Respublikos valstybės saugumo departamento teigimu[05], Rusijos žvalgybos tarnybų valdomos kibernetinės grupuotės 2020 m. Lietuvoje rengė kibernetines atakas prieš Lietuvos aukščiausias valdžios, užsienio politiką ir nacionalinį saugumą užtikrinančias institucijas, energetikos ir švietimo įstaigas. Rusijos žvalgybos tarnybų valdomos grupuotės taip pat išnaudojo Lietuvos informacinių technologijų paslaugų sektoriaus infrastruktūrą kibernetinėms atakoms prieš taikinius Vakarų valstybėse, pvz., dalis 2020 m. liepos mėn. paviešintų Rusijos žvalgybos tarnybų kibernetinio šnipinėjimo grupuotės APT29 atakų prieš vakciną nuo COVID-19 ligos kuriančias organizacijas Vakaruose buvo vykdomos pasinaudojant Lietuvos IT infrastruktūra.

Priešiškų valstybių žvalgybos ir jų remiami piktavaliai ar jų grupuotės veikia siekdami politinių, karinių, ekonominių ir (ar) ideologinių tikslų. Dalis 2020 m. Lietuvoje registruotų kibernetinių incidentų yra susiję su politiniais, geopolitiniais, strateginiais įvykiais Lietuvoje, regione ir visame pasaulyje, todėl daroma prielaida, kad priešiškos žvalgybos tarnybos siekia neteisėtais būdais gauti informacijos apie Lietuvos RIS pažeidžiamumus, įgyti asmeninio pobūdžio naudotojų informaciją (prisijungimų prie paskyrų duomenis) ir tai panaudoti kitiems kibernetiniams incidentams.

2020 m. pabaigoje, Vyriausybių pasikeitimo išvakarėse, buvo įvykdytas vienas didžiausių ir kompleksiškiausių Lietuvoje pastaraisiais metais kibernetinių-informacinių išpuolių. Pasinaudojant interneto svetainių puslapių TVS saugumo spraga, buvo neteisėtai prisijungta prie ne mažiau kaip 24 viešojo sektoriaus interneto svetainių ir jose publikuotos trys skirtingo turinio melagingos naujienos. Atlikus incidento tyrimą nustatyta, kad jam buvo pasirengta iš anksto, o pats incidentas vykdytas organizuotai.

Nesaugios įrangos ir technologijų naudojimas didina kibernetinio saugumo rizikas

Dalis kibernetinių incidentų yra siejami su nesaugios įrangos naudojimu, todėl 2020 m. NKSC atliko pramonėje ir buityje naudojamų IP kamerų ir bevielio tinklo maršrutizatorių tyrimus. Buvo nustatytos spragos, didinančios kibernetinių ar duomenų praradimo galimybes. Išvados plačiai pristatytos visuomenei.

Papildomas rizikas kelia ir nepatikimų IRT gamintojų, kontroliuojamų priešiškų valstybių, įrangos ir technologijų naudojimas YSII ir VII, įskaitant ir 5G ryšio infrastruktūrą. Tokios įrangos buvimas sudaro sąlygas vykdyti kibernetines operacijas – perimti informaciją, vykdyti ardomąją veiklą, sabotuoti infrastruktūros veiklą. Todėl nesaugios įrangos eliminavimas iš YSII ir VII yra vienas iš XVIII Vyriausybės kibernetinio saugumo prioritetų ir tam bus skiriama ypač daug dėmesio.

05 Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos ir Lietuvos Respublikos valstybės saugumo departamento ataskaita „Grėsmių nacionaliniam saugumui vertinimas 2021", http://kam.lt/download/70537/2021%20lt%20el_.pdf

Į turinį

RIS spragų[06] atskleidimo praktika yra vienas iš efektyvių būdų sustiprinti šalies kibernetinį saugumą

Vis daugiau ir plačiau kalbama apie RIS spragų atskleidimo praktikos taikymą ir jos naudą ne tik atskirų organizacijų, bet ir visos valstybės lygiu. Nedaug kibernetinio saugumo subjektų turi pasitvirtinę RIS spragų atskleidimo tvarką, todėl apie aptiktą spragą etiški kompiuterių įsilaužėliai gali pranešti viešai arba jos neatskleisti. Siekdama didesnės kibernetinio saugumo brandos, 2020 m. Krašto apsaugos ministerija inicijavo Kibernetinio saugumo įstatymo pakeitimus, kuriais siekiama įteisinti RIS spragų atskleidimo modelį Lietuvoje. NKSC, kaip ir kitos organizacijos, pvz. AB „Ignitis grupė“ ar Vilniaus miesto savivaldybė, RIS spragų atskleidimo tvarką savo iniciatyva taiko jau keletą metų ir yra gavę nemažai vertingų pranešimų, kurie leido užkirsti kelią galimiems kibernetinio saugumo incidentams.

Didžiausią grėsmę asmenų skaitmeniniam turtui kelia duomenis šifruojanti ir išpirkos reikalaujanti kenkimo PĮ (angl. *ransomware*), RIS veiklos, teikiamų paslaugų trikdymas (toliau – *DDoS*), duomenų vagystės (angl. *phishing*), sukčiavimas internete

2020 m. didžiausią nusikalstamų veikų kibernetinėje erdvėje dalį (virš 90 proc.), kaip ir 2019 m., sudarė elektroninis sukčiavimas, neteisėtas prisijungimas prie informacinės sistemos ir neteisėtas elektroninių duomenų perėmimas ir panaudojimas. Šie nusikaltimai įvykdyti dėl asmeninių motyvų. Lietuvos bankų asociacijos (toliau – LBA) duomenimis, 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. eur. Nors COVID-19 pandemija neturėjo didelės įtakos bendrai kriminogeninei situacijai, tačiau 2020 m. nusikaltėliai išnaudojo su pandemija susijusią situaciją nusikalstamiems kėslams: toliau tobulino ir pagal aplinkybes pritaikė savo veiklos metodus, nusikalstamoms veikoms vykdyti naudojo IRT. Nusikaltėliai, siekdami savo nusikalstamų tikslų, dažniausiai vykdė socialine inžinerija pagrįstas duomenų vagystes. Taip pat pažymėtina, kad vienas sparčiausiai plintančių sukčiavimo internete būdų – investicinis sukčiavimas, sukeliantis didžiulių nuostolių.

Asmens duomenų saugumo pažeidimai dažnai glaudžiai susiję su kibernetiniais incidentais ir nusikaltimais

Asmens duomenų saugumo pažeidimas[07] (toliau – ADSP) sudaro sąlygas piktavaliams perimti asmens duomenis, kurie gali būti panaudojami kibernetiniams incidentams ir nusikaltimams vykdyti.

2020 m. Lietuvoje reikšmingiausi pagal paveiktų asmenų skaičių ir poveikį ADSP buvo susiję su informacinės visuomenės paslaugų ir duomenų pasiekiamumo prieinamumo trikdžiais bei vientisumo pažeidimais (pvz., 2020 m. liepos mėn. įvykęs e. sveikatos sistemos sutrikimas) bei su atvejais, kai, taikant socialinės inžinerijos metodus ir nesant kibernetinio saugumo higienos, buvo užvaldomos naudotojų paskyros siekiant finansinės naudos (pvz., 2020 m. kovo mėn. UAB „Vinted“ el. prekybos platformoje buvo prisijungta prie naudotojų paskyrų be jų žinios), taip pat platinant kenkimo PĮ. Ir nors per 2020 m. Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) gautų pranešimų apie ASDP skaičius nelabai (3,5 proc.) padidėjo, galima daryti prielaidą, kad apie nemažą dalį ADSP VDAI vis dar nėra informuojama, nes gana dažnai ADSP būna susiję su įvykusiais kibernetiniais incidentais, kurių skaičius kasmet auga. 2020 m. Lietuvoje daugeliu atvejų buvo prarastas asmens duomenų konfidencialumas[08], todėl kibernetinio saugumo priemonių taikymas ir jų laikymasis asmens duomenų apsaugos srityje yra viena iš ADSP prevencijos sąlygų.

06
RIS spraga – ryšių ir informacinės sistemos trūkumas, dėl kurio gali įvykti kibernetinis incidentas.

07
Asmens duomenų saugumo pažeidimas – saugumo pažeidimas, dėl kurio netyčia arba neteisėtai sunaikinami, prarandami, pakeičiami, be leidimo atskleidžiami persiųsti, saugomi arba kitaip tvarkomi asmens duomenys arba prie jų be leidimo gaunama prieiga.

Lietuvos viešųjų elektroninių ryšių tinklai atlaikė dėl COVID-19 pandemijos išaugusį srautą, tačiau didėjo vaikų seksualinio išnaudojimo vaizdų kiekis internete ir konsultacijų, kaip saugiai naudotis socialiniais tinklais, poreikis

2020 m. pavasarį Lietuvoje dėl COVID-19 pandemijos paskelbus karantiną, gerokai išaugo naudojimasis elektroninių ryšių paslaugomis. Per metus Lietuvo Respublikos Ryšių reguliavimo tarnyba (toliau – RRT) iš viso gavo 10 pranešimų iš keturių viešųjų elektroninių ryšių tinklų teikėjų apie įvykusius viešųjų elektroninių ryšių tinklų vientisumo pažeidimus, tačiau jie didelės įtakos viešųjų elektroninių ryšių tinklų vientisumui neturėjo, o fiksuoti gedimai operatyviai pašalinti.

2020 m. 37 proc. padidėjo pranešimų, gautų RRT interneto karštąja linija. Per metus gauti 1373 pranešimai (2019 m. – 998 pranešimai). Tiek suaugusiems, tiek vaikams daugiau laiko praleidus internete, išaugo vaikų seksualinio išnaudojimo medžiagos apimtys kibernetinėje erdvėje. 2020 m. nustatyti 78 atvejai, kai Lietuvos tarnybinėse stotyse buvo aptikti vaikų seksualinio išnaudojimo vaizdai, ir šie atvejai buvo perduoti tirti Policijos departamentui (2019 m. tokių atvejų buvo 44). Šios tendencijos Lietuvoje sutampa su pasaulinėmis tendencijomis, nurodytomis tokių institucijų, kaip Interpolas, ataskaitose. RRT duomenimis, 2020 m. taip pat išaugo suteiktų konsultacijų, kaip sklandžiai naudotis internetu, skaičius. RRT, administruodama interneto svetainę **www.esaugumas.lt** ir konsultuodama besikreipiančius žmones, 2020 m. suteikė beveik 40 proc. daugiau konsultacijų interneto naudotojams nei 2019 m.

Su Lietuvos visuomenės gebėjimais atpažinti melagingas naujienas kartu tobulėja ir informaciniai incidentai

Informacinę aplinką stebintis ir analizuojantis Lietuvos kariuomenės Strateginės komunikacijos departamentas (toliau – LK SKD) 2020 m. fiksavo 18 proc. daugiau prieš Lietuvos nacionalinio saugumo ir gynybos interesus nukreiptos informacijos atvejų nei 2019 m. Iš viso per 2020 m. nustatyta 3412 tokios veiklos atvejų, šis skaičius, palyginti su 2018 m. ir 2019 m., tolygiai augo (atitinkamai 2456 ir 2890 atvejų).

LK SKD, analizuodamas Lietuvos informacinę aplinką, nustatė, jog nuo 2020 m. pradžios prieš Lietuvą, NATO ir atskiras NATO nares buvo įvykdyta 10 priešiškų informacinių operacijų, kurios išsiskyrė savo mastu ir pasirengimo lygiu, septynios iš jų buvo hibridinės atakos. 2020 m. didžiausios grėsmės Lietuvos informaciniam saugumui iš esmės liko tos pačios – Rusijos Federacija ir jos vyriausybės kontroliuojamos žiniasklaidos priemonės, kurių veikla daugiausia buvo nukreipta priešiškai ES ir NATO nuomonei formuoti. 2020 m. Lietuva sulaukė didesnio ir Baltarusijos žiniasklaidos neigiamo dėmesio dėl vykusių prezidento rinkimų Baltarusijoje.

08
Konfidencialumo pažeidimas – neleistinas arba netyčinis asmens duomenų atskleidimas arba prieigos prie asmens duomenų suteikimas.

Į turinį

03 Svarbiausi 2020 m. įvykiai kibernetinio saugumo srityje

01 SAUSIS

- Savo veiklą pradėjo krašto apsaugos sistemos saugumo operacijų centras (MilCERT)

02 VASARIS

- RRT Lietuvos elektroninės informacijos prieglobos paslaugų teikėjus pakvietė prisijungti prie Memorandumo dėl švarios interneto aplinkos kūrimo

03 KOVAS

- Patvirtintas Kibernetinio saugumo pajėgumo plėtros planas krašto apsaugos sistemoje
- „Vinted" el. prekybos platformoje įvyko asmens duomenų saugos pažeidimas – nukentėjo apie 19 320 asmenų
- Darbuotojams pradėjus dirbti iš namų, piktavaliai pradėjo aktyviau eksploatuoti darbuotojų nuotolinių prieigų pažeidžiamumus
- Parengtos Proceso veiksmų su virtualiosiomis valiutomis atlikimo metodinės rekomendacijos

04 BALANDIS

- Fiksuojamas išaugęs grasinimų sutrikdyti paslaugas skaičius, prašant išpirkos (angl. *Ransom Distributed Denial of Service* (RDDoS)). Papildomai vykdomos demonstracinės kibernetinės atakos
- Lietuvos policija fiksavo neteisėtos internetinės prekybos apsaugos priemonėmis, melagingų skelbimų dėl pigiau nei vidutinė rinkos kaina parduodamų apsaugos priemonių, klastotų šios kategorijos prekių elektroninės prekybos atvejų piką ir šalies mastu surengė operaciją pažeidimams išaiškinti

05 GEGUŽĖ

- NKSC atliko „Hikvision" ir „Dahua" gamintojų vaizdo stebėjimo kamerų kibernetinio saugumo analizę ir paskelbė rekomendacijas

06 BIRŽELIS

- Smulkioms ir vidutinėms įmonėms parengtas leidinys „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas"
- VDAI atnaujino asmens duomenų saugumo priemonių ir rizikos įvertinimo gaires
- Prasideda NKSC ir VRK paruošiamieji darbai, siekiant užtikrinti Seimo rinkimų kibernetinį saugumą

07 LIEPA

- Lietaus vandeniui užliejus VĮ Registrų centro serverinę, sutriko daugiau nei 20 registrų ir valstybės informacinių sistemų darbas
- Apskričių policijos komisariatuose priskirti ir apmokyti pareigūnai darbui su iš JAV gaunama informacija apie galimą vaikų išnaudojimą kibernetinėje erdvėje

08 RUGPJŪTIS

- KAM pradėjo vertinti YSII valdytojų sandorius dėl jų atitikimo nacionalinio saugumo interesams

09 RUGSĖJIS

- KAM parengė Kibernetinio saugumo įstatymo pakeitimus, siekdama įteisinti RIS spragų atskleidimo modelį / sudaryti sąlygas IRT produktų, procesų ir paslaugų sertifikavimui
- KAM pradėtas vykdyti projektas, skirtas kibernetinio saugumo inovacijų plėtrai skatinti
- Lietuvos policija dalyvavo sėkmingoje tarpregioninėje operacijoje, nukreiptoje prieš vaikų išnaudojimą kibernetinėje erdvėje
- Pasirašytas JAV ir Lietuvos susitarimo memorandumas 5G apsaugos klausimais

10 SPALIS

- Sudarytos sąlygos vykdyti Regioninio kibernetinio saugumo centro veiklas
- 5G paslaugų teikėjai įtraukti į nacionaliniam saugumui užtikrinti svarbių įmonių sąrašą
- Pradėjo veikti asmens duomenų tvarkymo sklaidai skirta programėlė „ADA gidas"
- FIksuojamas naujų reikalavimų sumokėti išpirką, grasinant RDDoS kibernetiniais incidentais, skaičiaus augimas. Toliau vykdomos demonstracinės kibernetinės atakos
- NKSC fiksavo „Emotet" kenkimo PĮ plitimo piką
- NKSC atliko mobiliosios programėlės „KoronaStopLT" kibernetinio saugumo vertinimą

11 LAPKRITIS

- AB „Telia Lietuva" įjungė bandomąjį 5G technologijos ryšį Vilniuje, Kaune ir Klaipėdoje
- NKSC kartu su Austrijos partneriais pradėjo vykdyti ES dvynių projektą, siekdami sustiprinti Sakartvelo kibernetinį saugumą
- NKSC atliko 9 rinkoje paplitusių telekonferencinių programinių sprendimų kibernetinio saugumo apžvalgą ir parengė rekomendacijas dėl saugesnio jų naudojimo
- Lietuvos policija ir bankai, reaguodami į galimus sukčiavimo atvejus, pradėjo bendradarbiauti ir parengė gyventojams atmintinę, kaip netapti sukčių auka

12 GRUODIS

- KAM parengė atnaujintą YSII sąrašą
- KAM parengė pasiūlymus dėl naujos kibernetinio saugumo reikalavimų sistemos projekto
- VDAI parengė gaires, skirtas asmenims, dalyvaujantiems informacinių sistemų, kuriose tvarkomi asmens duomenys, kūrimo procesuose
- Įvykdytas plataus masto kibernetinis-informacinis incidentas prieš Lietuvą
- Lietuvos policija ir vienas didžiausių interneto paslaugų teikėjų pasirašė bendradarbiavimo sutartį dėl saugesnės aplinkos internete kūrimo ir neteisėtos veikos užkardymo
- Pradėjo plisti JAV kompanijos „SolarWinds" PĮ atnaujinimai su kenkimo kodu

04

Kibernetinio saugumo aplinkos stiprinimas

01 Kibernetinio saugumo aplinkos stiprinimas

Kibernetinio saugumo srities procesams dažniausiai daro įtaką valstybės formuojama ir įgyvendinama politika bei plėtojamas tarptautinis bendradarbiavimas. Krašto apsaugos ministerija, būdama atsakinga už kibernetinio saugumo politikos formavimą ir organizuodama, koordinuodama bei kontroliuodama jos įgyvendinimą, toliau tęsė nuo 2018 m. pradėtus kibernetinio saugumo srities konsolidavimo darbus, kurių esminiai 2020 m. rezultatai pristatomi šioje dalyje.

XVIII Vyriausybės programos nuostatų įgyvendinimo plane numatyta nemažai priemonių, susijusių su kibernetinio saugumo stiprinimu valstybėje. Vienas iš krašto apsaugos ministro strateginių darbų – užtikrinti, kad kritinėje infrastruktūroje (įskaitant 5G) būtų naudojama tik patikimų gamintojų įranga

Krašto apsaugos ministerijos inicijuoti teisės aktai kibernetinio saugumo srityje

2020 m. kovo mėn. parengtas ir patvirtintas Kibernetinio saugumo pajėgumo plėtros planas, kuriuo remiantis bus stiprinami krašto apsaugos sistemos (toliau – KAS) institucijų, veikiančių kibernetinio saugumo srityje, ir kitų įstaigų kibernetinio saugumo pajėgumai.

2020 m. rugsėjo mėn. parengti Lietuvos Respublikos kibernetinio saugumo įstatymo ir Lietuvos Respublikos administracinių nusižengimų kodekso pakeitimo įstatymo projektai, numatantys Lietuvos rinkos subjektams galimybę IRT produktus, procesus ir paslaugas sertifikuoti pagal Europos kibernetinio saugumo sertifikavimo schemas[09] ir įteisinantys RIS spragų atskleidimo modelį[10].

Siekiant didinti penktosios kartos judriojo ryšio (5G) saugumą, 2020 m. birželio 30 d. Lietuvos Respublikos Seime priimtas Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymo pakeitimo ir papildymo įstatymas, kuriuo įmonės, teikiančios 5G ryšio paslaugas ar valdančios šioms paslaugoms teikti reikalingą infrastruktūrą, Krašto apsaugos ministerijos siūlymu nuo 2020 m. spalio mėn. įtrauktos į nacionaliniam saugumui užtikrinti svarbių įmonių sąrašą. Tokios 5G įmonės privalo įgyvendinti papildomas saugumo priemones (taip pat kibernetinio saugumo), o savo veiklą organizuoti ir vykdyti taip, kad nekiltų grėsmė nacionalinio saugumo interesams.

2020 m. gruodžio mėn. parengtas ir Lietuvos Respublikos Vyriausybei pateiktas Lietuvos Respublikos Vyriausybės nutarimo, kuriuo siūloma patvirtinti atnaujintą YSII ir jos valdytojų sąrašą, projektas. YSII ir jos valdytojų identifikavimas ir gynyba yra viena iš svarbiausių nacionalinio kibernetinio saugumo tikslų, nes YSII valdytojai užtikrina būtiniausių paslaugų teikimą gyventojams ir verslui.

Krašto apsaugos ministerija 2020 m. atliko Lietuvos teisės aktų, kuriuose nustatyti kibernetinio saugumo, elektroninės informacijos saugos reikalavimai, tarptautinių standartų, metodikų ir geriųjų

09 Šiais pakeitimais įgyvendinamas 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (Kibernetinio saugumo aktas).

10 Šis pakeitimas dera su 2020 m. gruodžio mėn. pabaigoje Europos Komisijos pateiktu pasiūlymu direktyvai dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti (toliau – TIS2 direktyva).

Į turinį

Lietuvos Respublikos Seimui 2021 m. pritarus Krašto apsaugos ministerijos siūlomam RIS spragų atskleidimo modeliui, atsiras teisinis aiškumas dėl asmenų, aptikusių RIS spragas, teisinės padėties, bus sudarytos sąlygos teisėtai pranešti apie spragas, koordinuoto proceso metu šias spragas pašalinti ir taip prisidėti prie geresnės kibernetinio saugumo situacijos Lietuvoje

praktikų analizę ir parengė pasiūlymus dėl naujos kibernetinio saugumo reikalavimų sistemos, kuria siekiama:

- suformuoti išsamų ir lankstų kibernetinio saugumo reikalavimų rinkinį, atsižvelgiant į tarptautinius standartus, metodikas ir gerąsias praktikas bei Lietuvos situaciją;
- paskatinti kibernetinio saugumo reikalavimų spartesnį ir kokybiškesnį įgyvendinimą;
- pasiūlyti tinkamas kibernetinio saugumo reikalavimų įgyvendinimo ir stebėsenos priemones.

2020 m. rugpjūčio 1 d. įsigaliojo Lietuvos Respublikos viešųjų pirkimų ir Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymų pakeitimai, susiję su YSII valdytojų sandorių vertinimu dėl jų atitikimo nacionalinio saugumo interesams. YSII valdytojai, pasirengdami pirkimui, privalo kreiptis į Krašto apsaugos ministeriją, kuri pradėjo atlikti vertinimus ir teikti motyvuotas rekomendacijas YSII valdytojams dėl sutarties vykdymo metu galinčių kilti technologinių rizikų, susijusių su YSII, ir reikalavimų, susijusių su nacionaliniu saugumu, nustatymo pirkimo dokumentuose tikslingumo.

Krašto apsaugos ministerijos vykdytos iniciatyvos kibernetinio saugumo stiprinimo ir tarptautinio bendradarbiavimo srityje

2020 m. sausio mėn. pradėjo veikti KAS saugumo operacijų centras (MilCERT). MilCERT užtikrina KAS informacinių sistemų kibernetinį saugumą. Planuojama, kad visu pajėgumu MilCERT dirbs po kelerių metų, kai bus parengta pakankamai personalo nenutrūkstamam KAS informacinių sistemų stebėjimui ir gynybai organizuoti.

2020 m. buvo tęsiamas Europos Sąjungos (toliau – ES) Nuolatinio struktūrizuoto bendradarbiavimo projektas „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ ir pasiektas pajėgų pradinis operacinis pajėgumas (angl. *Initial Operational Capability*). 2020 m. budinčių pajėgų rotacijai vadovavo Lietuva. Pajėgas sudarė kibernetinio saugumo specialistai iš Lietuvos, Lenkijos, Nyderlandų ir Rumunijos. Šios pajėgos 2020 m. nuotoliniu būdu dalyvavo dvejose kibernetinio saugumo pratybose. Pajėgų kibernetiniai gebėjimai ir veikimo procedūros 2020 m. buvo išbandytos pakviečiant pajėgas atlikti kibernetinio saugumo pažeidžiamumų vertinimą VRK informacinėje sistemoje.

2020 m. žengti dar keli žingsniai Kaune kuriant Regioninį kibernetinės gynybos centrą. Spalio mėn. NKSC pradėjo vykdyti centro funkcijas, o JAV patvirtino skirsiančios 10 mln. dolerių kibernetinio saugumo mokymų infrastruktūros sukūrimui Kaune. Centras turėtų tapti pagrindine Lietuvos ir JAV dvišalio bendradarbiavimo kibernetinėje srityje platforma, taip pat bus bendradarbiaujama su Sakartvelo bei Ukrainos kibernetinio saugumo specialistais. Svarbiausi centro uždaviniai – skatinti inovatyvių kibernetinio saugumo technologijų kūrimą, rengti kibernetinio saugumo specialistus ir tarpusavyje keistis informacija apie kibernetines grėsmes.

Krašto apsaugos ministerijos atstovai aktyviai prisidėjo prie 2020 m. rugsėjo mėn. Europos Komisijos (toliau – EK) ir ES Kibernetinio saugumo agentūros (ENISA) iniciatyva įsteigto Kibernetinių krizių bendradarbiavimo tinklo (angl. *Cyber Crisis Liaison Organisation Network* (CyCLONe)) kūrimo. Šis

tinklas padės efektyviau koordinuoti ES valstybių narių veiksmus ir priimti sprendimus ES mastu, įvykus kibernetinio saugumo incidentui.

2020 m. lapkričio mėn. pasirašytas ketinimų protokolas dėl projekto „Kibernetinio greitojo reagavimo įrankių rinkinio Europos gynybai - CYBER4DE“ (angl. *Cyber Rapid Response Toolbox for European Defence* - CYBER4DE“) vykdymo. Jame numatyti bendri reikalavimai kibernetinio greitojo reagavimo įrankių kūrimui ir suteikti įgaliojimai 5 Nuolatinio struktūrizuoto bendradarbiavimo projekto „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ šalims dalyvėms, atstovaujančioms konsorciumui, pateikti paraišką siekiant gauti finansinę paramą projektui „Kibernetinio greitojo reagavimo įrankių rinkinys Europos gynybai“.

Krašto apsaugos ministerijos veikla kibernetinio saugumo kultūros kėlimo srityje

Siekiant didinti viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo brandos lygį, 2020 m. birželio mėn. visuomenei pristatytas leidinys „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas“. Jame aptariama kibernetinio saugumo svarba ir pateikiama praktinių patarimų. Leidinys publikuojamas Krašto apsaugos ministerijos interneto svetainėje **http://kam.lt/lt/naujienos_874/leidiniai/2020_m._isleisti_leidiniai.html**

ES siekia sustiprinti savo pajėgumus apsaugoti Europą nuo kibernetinių grėsmių ir didinti ES kibernetinio saugumo pramonės konkurencingumą, todėl Europos Komisija 2018 m. inicijavo Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centro steigimą ir Nacionalinių koordinavimo centrų tinklo įkūrimą. VšĮ „Investuok Lietuvoje“ inicijuotos ir įgyvendinamos programos „Kurk Lietuvai“ dalyviai Krašto apsaugos ministerijoje 2020 m. rugsėjo mėn. pradėjo vykdyti projektą, kurio tikslas – išanalizuoti Lietuvos kibernetinio saugumo inovacijų ekosistemą ir pateikti pasiūlymus jos plėtrai ir potencialo panaudojimui. Šis projektas prisidės prie Europos Parlamento ir Tarybos reglamento, kuriuo įsteigiamas Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijų centras ir Nacionalinių koordinavimo centrų tinklas (2018/0328) (toliau – ECCC reglamentas), įgyvendinimo. Daugiau informacijos apie programos „Kurk Lietuvai“ dalyvių vykdytą projektą žr. interneto svetainėje **http://kurklt.lt/projektai/kibernetinio-saugumo-ekosistemos-pletra/**

Krašto apsaugos ministerija 2020 m. gegužės mėn. inicijavo reikminių tyrimų projektą „Kibernetinio saugumo kompetencijų modelio kūrimas“, kuris buvo atrinktas Lietuvos mokslų tarybos kaip tyrimas valstybei ypač aktualia mokslinių tyrimų ir eksperimentinės (socialinės, kultūrinės) plėtros programų tema. Numatoma, jog projekto rezultatai bus naudingi įgyvendinant Nacionalinės kibernetinio saugumo strategijos trečiojo tikslo „Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą“ antrąjį uždavinį „Ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją“, o parengto Nacionalinio kibernetinio saugumo kompetencijų žemėlapio išvados ir rekomendacijos bus vertingos nacionaliniu lygiu. Daugiau informacijos apie reikminių tyrimų projekto „Kibernetinio saugumo kompetencijų modelio kūrimas“ žr. interneto svetainėje **https://spektras.lmt.lt/anotacija.php?PW7yZqb2JRhX3IepLSnjSgu1AuqHlXMj0d74VL7Q7/E=**

2020 metų kovo 4 d. Zagrebe šešios Europos šalys – Lietuva, Estija, Kroatija, Lenkija, Nyderlandai, Rumunija – pasirašė bendradarbiavimo susitarimą (angl. MOU), kuris teisiškai įgalina Lietuvos vadovaujamo PESCO (angl. Permanent Structured Cooperation, PESCO) projekto metu įkurtas pajėgas veikti skirtingų šalių jurisdikcijose, apibrėžia jų veikimo būdus, teisinį statusą, funkcijas ir procedūras

Į turinį

Siūloma plėsti į TIS2 direktyvos apimtį įtrauktų sektorių skaičių prie jau esančių sektorių papildomai įtraukiant vandens nuotekų, viešojo administravimo, kosmoso, pašto ir kurjerių paslaugų, atliekų tvarkymo, cheminių medžiagų, maisto ir gamybos sektorius

ES teisėkūros iniciatyvos, siekiant sustiprinti Europos kibernetinės erdvės atsparumą ir paskatinti inovacijas

2020 m. gruodžio 16 d. Europos Komisija ir Europos išorės veiksmų tarnyba paskelbė bendrą komunikatą Europos Parlamentui ir Tarybai „Europos Sąjungos skaitmeninio dešimtmečio kibernetinio saugumo strategija“ (toliau – Strategija). Papildomai EK pateikė naują teisėkūros pasiūlymą, kaip efektyviau spręsti ypatingos svarbos subjektų ir tinklų kibernetinio atsparumo klausimus – TIS2 direktyvą.

Pagrindinės Strategijos rekomendacijos: visoje ES sukurti dirbtiniu intelektu (DI) grindžiamą saugumo operacijų centrų (SOC) tinklą, taip pat naują bendrą kibernetinio saugumo padalinį (angl. *Joint Cyber Unit* (JCU)). Siūloma tobulinti ES Kibernetinio saugumo diplomatijos priemonių rinkinį (angl. *EU Cyber diplomacy toolbox*), stiprinti bendradarbiavimą kibernetinės gynybos srityje, rengti ES išorės kibernetinių gebėjimų stiprinimo programą (*EU External Cyber Capacity Building Agenda*) ir įsteigti ES kibernetinės diplomatijos tinklą (*EU Cyber Diplomacy Network*), stiprinti ES institucijų apsaugą ir ES Reagavimo į kompiuterių incidentus tarnybos (CERT-EU) mandatą.

Daugiau informacijos apie Strategiją žr. interneto svetainėje **https://ec.europa.eu/digital-single-market/en/news/eus-cybersecurity-strategy-digital-decade**

TIS2 direktyva tikimasi išspręsti pastebėtus 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti ir jos netolygaus įgyvendinimo ES valstybėse narėse trūkumus bei atsižvelgti į besikeičiančią kibernetinio saugumo situaciją.

TIS2 direktyvos pasiūlymu siekiama:

- praplėsti direktyvos reguliavimo sritį, įtraukiant juridinius asmenis iš papildomų sektorių;
- pačiuose sektoriuose juridinius asmenis atrinkti pagal jų dydį (su tam tikromis išimtis);
- suvienodinti taikomus kibernetinio saugumo reikalavimus;
- aiškiau apibrėžti ir efektyvinti pranešimų apie kibernetinius incidentus procesą;
- suvienodinti nuostatas dėl kibernetinio saugumo reikalavimų stebėsenos;
- stiprinti valstybių narių bendradarbiavimą ir operatyvią pagalbą, įskaitant efektyvesnį krizių valdymo procesą.

Daugiau informacijos apie TIS2 direktyvą žr. interneto svetainėje **https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union**

2020 m. gruodžio 18 d. ES Tarybos COREPER I atstovai vienbalsiai pritarė pasiektam politiniam sutarimui su Europos Parlamentu dėl ECCC reglamento. Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijų centras (toliau – ECCC) kartu su nacionalinių

koordinavimo centrų tinklu turės tapti pagrindiniu ES instrumentu skatinant Europos kibernetinio saugumo inovacijas, mokslinius tyrimus, technologijas ir pramonę. ECCC veikla bus finansuojama iš 2021–2027 m. ES daugiametėje finansų programoje numatytų finansavimo priemonių „Europos Horizontas“ ir „Skaitmeninės Europos Programa“, kurių kibernetinio saugumo sričiai numatoma bendra lėšų suma turėtų siekti apie 4 mlrd. eurų. Planuojama, kad ECCC reglamentas galėtų būti patvirtintas ir įsigaliotų nuo 2021 m. II ketv.

2020 m. gruodžio 8 d. ES valstybių narių vyriausybių atstovų konferencijoje dviejų slapto balsavimo turų metu atrinkta ir patvirtinta ECCC vieta Bukarešte, Rumunijoje. Be Rumunijos, savo kandidatūras steigti ECCC buvo iškėlusios dar 6 ES valstybės narės – Belgija, Ispanija, Lenkija, Lietuva, Liuksemburgas ir Vokietija. Įsigaliojus ECCC reglamentui, kiekviena ES valstybė narė per 6 mėn. turės paskirti nacionalinius koordinavimo centrus, kad suinteresuotoms pusėms būtų sudarytos sąlygos bendradarbiauti, kurti ir vykdyti tyrimus ar bendrus projektus tiek nacionaliniu, tiek ES mastu.

Daugiau informacijos apie reglamentą žr. interneto svetainėje **https://ec.europa.eu/digital-single-market/en/proposal-european-cybersecurity-competence-network-and-centre**

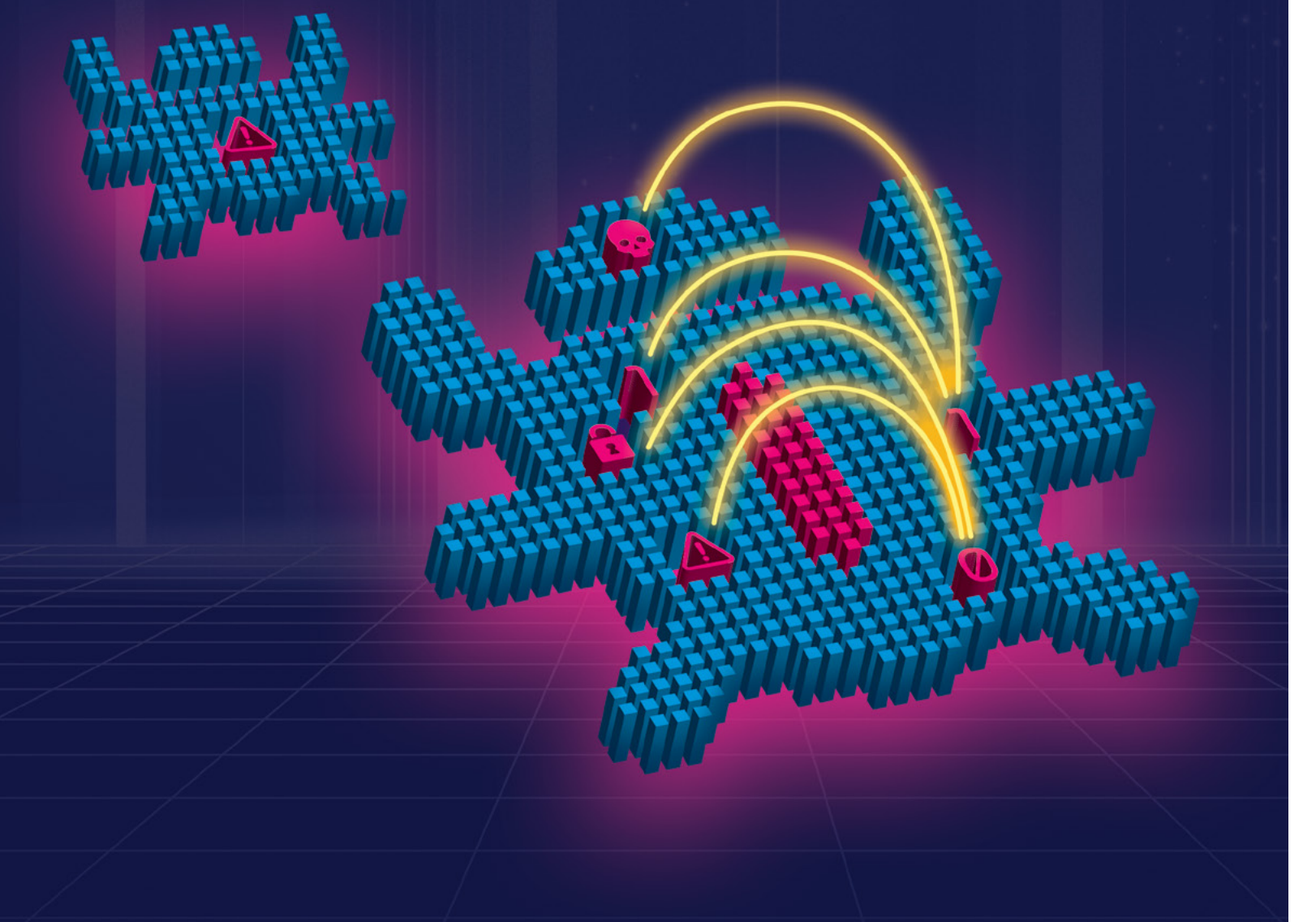
Krašto apsaugos ministerija siūlė Vilniuje įsteigti ECCC. Ir nors ES valstybių narių vyriausybių atstovai centro būstinės vieta atrinko Rumunijos pasiūlymą, Lietuva surinko 5 valstybių narių balsus, į priekį užleisdama tik Rumuniją su 6 balsais ir Belgiją su 8 balsais

Kaip ES užtikrina kibernetinį saugumą

< 01 pav. >

05

Įvykių, dariusių įtaką Lietuvos kibernetinio saugumo būklei, apžvalga



01 Kibernetinio saugumo užtikrinimo iššūkiai

NKSC svarbiausi pasiekimai

Suvaldyta **4330** kibernetinių incidentų Lietuvoje (iš jų **67** vidutinio poveikio ir **1** didelio poveikio kibernetinis incidentas)

Automatinėmis priemonėmis apdorota **306 tūkst.** kibernetinių įvykių, susijusių su Lietuvos IP adresais

Atlikti **6** Lietuvos kibernetinio saugumo subjektų patikrinimai

Įdiegtos **8** techninės kibernetinio saugumo priemonės (sensoriai) YSII, o bendras NKSC įdiegtų sensorių skaičius padidėjo iki **45**

46 proc. apklaustųjų mano, jog Lietuvos institucijos tinkamai užtikrina šalies kibernetinį saugumą[11]

Atlikti **8** tipų vaizdo stebėjimo IP kamerų technologiniai kibernetinio saugumo tyrimai ir **4** bevielio tinklo maršrutizatorių modelių gamyklinių nustatymų saugumo vertinimai. Išvados paviešintos Lietuvoje, taip pat sulaukė susidomėjimo / įvertinimo iš kitų ES šalių

600 naudotojų pasinaudojo nemokamu interneto svetainių saugumo pasitikrinimo įrankiu, kuris veikia pagal žinomų saugumo spragų Atviro žiniatinklio programų saugumo projekto (angl.. *Open Web Application Security Project* (OWASP))[12] metodiką

Organizuotos nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2020", kuriose dalyvavo **73** kibernetinio saugumo subjektai

Įvykdyta **30** kibernetinio saugumo pagrindų mokymų, publikuoti **94** pranešimai kibernetinio saugumo temomis socialiniuose tinkluose, NKSC interneto svetainėje paskelbta **10** informacinių kibernetinio saugumo biuletenių ir **18** naujienų

11 Krašto apsaugos ministerijos užsakymu 2020 m. gruodžio 15–30 d. atlikta 1008 respondentų apklausa. 12 https://owasp.org/

< 02 pav. >

Į turinį

dr. Rytis Rainys
NKSC direktorius

Vadovo žodis

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos kibernetinį saugumą vertina kaip taikomų organizacinių ir techninių priemonių visumą, kuria siekiama apsaugoti sistemas bei jose tvarkomą ir tinklais perduodamą informaciją nuo kibernetinėje erdvėje kylančių grėsmių. Dėl užsitęsusios COVID-19 pandemijos išaugo interneto naudojimo ir informacinės visuomenės paslaugų poreikis, o daugelis kasdienių veiklų, tokių kaip darbas ir ugdymas, organizuojami nuotoliniu būdu. Dėl šių priežasčių kibernetinis saugumas yra aktualus praktiškai visiems. Tai dar labiau sustiprina faktas, kad nusikaltėliai ir programišiai aktyviai pasinaudoja šia situacija vykdydami kibernetines atakas. 2020 m. kibernetinių incidentų Lietuvoje fiksuota ketvirtadaliu daugiau nei ankstesniais metais.

NKSC misija – būti kibernetinio saugumo kompetencijos centru, kad interneto naudotojai bendraudami, mokydamiesi ir dirbdami kibernetinėje erdvėje jaustųsi saugiai. NKSC pagal Kibernetinio saugumo įstatymą kartu su kitomis institucijomis įgyvendina kibernetinio saugumo politiką.

KĄ SAUGO?

- Lietuvos kibernetinę erdvę ir kibernetinio saugumo subjektus.

NUO KO SAUGO?

- Nuo kibernetinių incidentų ir jų neigiamo poveikio.

KAIP SAUGO?

- Organizuodamas kibernetinių incidentų valdymą bei atlikdamas jų analizę.
- Reaguodamas į kibernetinius incidentus KAS.
- Atlikdamas kibernetinio saugumo subjektų ir jų valdomų sistemų atitikties kibernetinio saugumo reikalavimams priežiūrą.
- Atlikdamas įslaptintos informacijos ir sistemų akreditaciją.
- Organizuodamas dalijimąsi informacija apie galimus ir įvykusius kibernetinius incidentus Kibernetinio saugumo informaciniame tinkle.
- Atlikdamas įrenginių ir programų kibernetinio saugumo tyrimus.
- Vykdydamas tarptautinio bendradarbiavimo veiklas.

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

www.nksc.lt cert@nksc.lt 1843

Kibernetinių incidentų statistika ir tendencijos

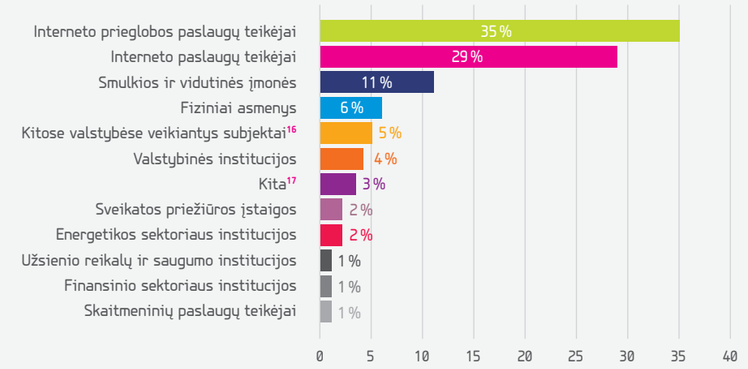
2020 m. šalyje registruota 4 330 kibernetinių incidentų, iš jų 4 262 nereikšmingo poveikio[13], o 67 – vidutinio poveikio[14] ir 1 – didelio poveikio[15]. Bendras kibernetinių incidentų skaičius 2020 m. buvo 1089, daugiau nei 2019 m., t. y. 25 proc. prieaugis. Skirstant kibernetinius incidentus pagal grupes, matyti, kad NKSC fiksavo incidentų augimą nepageidaujamų laiškų, klaidinančios informacijos platinimo, kenkimo PĮ, mėginimų įsilaužti, paslaugų trikdymo grupėse. Bendras kibernetinių incidentų skaičius išaugo 25 proc. (žr. **03 pav.**).

Nr.	Kibernetinio incidento grupės	Kibernetinių incidentų kiekis	Pokytis palyginti su 2019 m.
01	Nepageidaujamų laiškų, klaidinančios informacijos platinimas	739	+29 %
02	Kenkimo PĮ	1966	+49 %
03	Informacijos rinkimas (angl. *phishing*)	962	–14 %
04	Mėginimas įsilaužti	171	+73 %
05	Sėkmingas įsilaužimas	61	–13 %
06	Paslaugų trikdymas (angl. DDoS)	75	+67 %
07	Neteisėta veikla, sukčiavimas	85	–62 %
08	Kiti incidentai (individualūs, neatitinkantys nė vienos iš nurodytų grupių aprašymų)	271	–24 %
	Iš viso:	**4330**	**+25 %**

< **03 pav.** 2020 m. kibernetinių incidentų statistika >

Įvertinus kibernetinių incidentų pasiskirstymą pagal nukentėjusius subjektus, daugiausia incidentų nustatyta elektroninės informacijos prieglobos paslaugų teikėjų informaciniuose ištekliuose, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjų bei smulkių ir vidutinių įmonių ryšių ir informacinėse sistemose (žr. **04 pav.**). Pažymėtina, kad pagal Kibernetinio saugumo įstatyme pateiktą kibernetinio saugumo subjekto sąvokos apibrėžimą, fiziniai asmenys į šį apibrėžimą nepatenka, tačiau NKSC – visada (telefonu ar el. paštu) šiuos asmenis konsultuoja dėl kibernetinio saugumo užtikrinimo. Fiziniai asmenys dažniausiai kreipiasi dėl darbo stočių sutrikimų ar galimos nusikalstamos veikos jų atžvilgiu įvykdymo.

NKSC patvirtintų kibernetinių incidentų (4330) pasiskirstymas pagal subjektų veiklos sritis



< **04 pav.** >

13
Nustatytas kibernetinis incidentas ir jo poveikis atitinka bent vieną iš kriterijų: RIS trikdoma < 1 val.; paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 100, arba 5 proc.; paslauga teikiama, bet trikdoma; nuostoliai < 250 000 Eur.

14
Nustatytas kibernetinis incidentas ir jo poveikis atitinka du ir daugiau kriterijų: RIS trikdoma ≥ 1 val., bet < 2 val.; paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius < 1000, arba 25 proc.; paslauga trikdoma dalyje šalies teritorijos; pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas; nuostoliai ≥ 250 000, bet < 500 000 Eur.

15
Nustatytas kibernetinis incidentas ir jo poveikis atitinka du ir daugiau kriterijų: RIS trikdoma ≥ 2 val.; paveiktų paslaugos gavėjų ar kompiuterizuotų darbo vietų skaičius ≥ 1000, arba 25 proc.; paslauga trikdoma visos šalies teritorijos ir (ar) ≥ 1 ES šalyje; pažeistas informacijos ar RIS konfidencialumas ir (ar) vientisumas; nuostoliai ≥ 500 000 Eur.

16
„Kitose valstybėse veikiantys subjektai" – organizacijos, kurias paveikė kibernetiniai incidentai, susiję su Lietuvos RIS.

Į turinį

17

„Kita“ – viešojo saugumo ir teisinės tvarkos, kultūros, maisto produktų, transporto ir pašto, švietimo, aplinkos, finansinio, turizmo, geriamojo vandens paslaugas teikiantys subjektai.

18

https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Skirtingos kibernetinės atakos gali būti susijusios tarpusavyje ir vykdomos lygiagrečiai ar nuosekliai, pvz., kartais piktavaliai gali vykdyti „šoninio judėjimo“ (angl. *lateral movement*) kibernetines atakas, tokias kaip informacijos rinkimas, siekdami įvykdyti kitą kibernetinę ataką, kuri ir yra galutinis jų tikslas (žr. **05 pav.**). Didelę grėsmę kelia kibernetinės atakos, kurių metu pavyksta sėkmingai išnaudoti RIS pažeidžiamumus ir į RIS įdiegti kenkimo kodą.

Galima kibernetinio incidento vykdymo eiga[18]

01

Informacijos rinkimas

- socialiniuose tinkluose;
- įstaigos interneto svetainėje;
- internetu pasiekiamose organizacijos RIS sistemose.

02

Atakos būdo parinkimas

- pažeidžiamumo identifikavimas;
- tinkamiausios priemonės parinkimas ar sukūrimas pažeidžiamumui išnaudoti.

03

Pristatymas

- kenkimo kodas pristatomas el. paštu, USB laikmenoje, interneto svetainėje.

04

Pažeidžiamumo išnaudojimas

- bandoma atspėti slaptažodžius RIS sistemose;
- atsiunčiamas kenkimo kodas apeinant kibernetinio saugumo priemones.

05

Kenkimo kodo įdiegimas

- atsiunčiami papildomi kenkimo kodo failai;
- užtikrinamas automatinis kodo paleidimas.

06

Kontrolės perėmimas

- įgaunama nuotolinė prieiga prie užvaldytos RIS, kompiuterio ir kitų informacinių išteklių.

07

Tikslų įgyvendinimas

- daromas neigiamas poveikis, t. y. vykdomas informacijos surinkimas iš užvaldytos infrastruktūros arba vykdomos tolesnės atakos.

< 05 pav. >

NKSC rekomendacijos kibernetinių incidentų prevencijai

Rizika	Rekomendacija
Naudotojas paspaus nuorodą į interneto svetainę, užkrėstą kenkimo kodu	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar rodomas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
Naudotojas įves savo slaptažodį suklastotoje interneto svetainėje	Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. naudojamas TLS sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių žingsnių autentifikavimo įrankius (pvz., slaptažodis, mobilusis įrenginys, piršto antspaudas). Stengtis bankų, socialinių tinklų, el. pašto adresus suvesti naršyklėje patiems, išsisaugoti šių adresų nuorodas naršyklėje.
Naudotojas pats atskleis savo prisijungimo slaptažodžius piktavaliui	Naudoti mažiausiai dviejų žingsnių autentifikavimą (angl. *2-factor-authentification* (2FA)), saugoti savo prisijungimo slaptažodžius, jokiais būdais nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone. Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas). Prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pvz., pasitikslinti aplinkybes paskambinus telefonu.
Naudotojas įdiegs kenkimo PĮ	Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pvz., iš nelegalių PĮ platinimo šaltinių).
Naudotojas pasiduos piktavalio manipuliacijoms	Neatlikti skubotų veiksmų, nepasiduoti emocijoms, detaliai išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.
Pasinaudojęs pažeidžiamumu, piktavalis įdiegs kenkimo PĮ į RIS	Naudoti legalią OS ir PĮ, naudoti antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti naujai išleistus OS, PĮ atnaujinimus.
Naudotojas parsisiųs kenkimo PĮ iš interneto šaltinių	Nesisiųsti failų iš nepatikimų šaltinių, naršyklėje įdiegti įskiepius suklastotoms interneto svetainėms atpažinti, parsisiųstus įtartinus failus skenuoti antivirusine PĮ, tikrinti failus dėl jų grėsmių žinomuose šaltiniuose, pvz., http://www.virustotal.com.

Kenkimo PĮ iš užkrėstos atminties laikmenos bus paleista automatiškai	Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą, prieš atidarant laikmenoje esančius failus leisti antivirusinei PĮ nuskenuoti juos.
Kenkimo PĮ užšifruos kompiuteryje esančius duomenis	Periodiškai daryti atsargines duomenų kopijas, jas saugoti kitame įrenginyje, atskirai nuo tos vietos, kurioje jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pvz., išorinėje laikmenoje).
Kenkimo PĮ sukurs piktavaliui prieigą prie konfidencialios informacijos	Šifruoti konfidencialią informaciją, jeigu būtina, apsaugoti ją saugiu slaptažodžiu. Informacijai perduoti naudoti kriptografines priemones, pvz., elektroninių laiškų šifravimą.
Kompiuteris bus užkrėstas per RIS tinklą	Įstaigose naudoti tinklo segmentavimą, keletą filtravimo priemonių (pvz., tinklo ir darbo stoties ugniasienę), svarbias RIS atskirti fiziškai.

< 06 pav. >

2020 m. gerokai išaugo skaičius Lietuvos IP adresų, įtrauktų į RIS trikdymo atakas, taip pat IP adresų, užkrėstų kenkimo PĮ

Kibernetinių įvykių statistika ir tendencijos

NKSC, atsižvelgdamas į kibernetinių incidentų kriterijų sąrašą[19], taip pat į ES kibernetinio saugumo agentūros (ENISA) ir tinklų ir informacijos saugumo kompiuterinių incidentų tyrimo tarnybų (angl. *Computer Security Incident Response Team* (CSIRT)) suvienodintą kibernetinių incidentų klasifikavimą, analizavo kibernetinius įvykius[20], kurie paliekami apdoroti automatizuotoms priemonėms ir nėra priskirti kibernetiniams incidentams[21] (žr. **07 pav.**). 2020 m. Lietuvoje fiksuotas tik šiek tiek mažesnis kibernetinių įvykių skaičius nei 2019 m. (žr. **08 pav.**).

Kibernetinio incidento nustatymo procesas

< 07 pav. >

19
Sąrašas nustatytas Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

20
Automatinėmis priemonėmis ir programomis apdoroti procesai yra traktuojami kaip kibernetiniai įvykiai.

21
Pagal Kibernetinio saugumo įstatymą kibernetiniu incidentu laikomas įvykis ar veika, galintys sukelti ar sukeliantys neigiamą poveikį RIS ar perduodamai informacijai.

Remiantis kibernetinių įvykių statistika, galima teigti, kad gerokai išaugo skaičius Lietuvos IP adresų, įtrauktų į RIS trikdymo atakas, taip pat IP adresų, užkrėstų kenkimo PĮ.

Nr.	Kibernetinių įvykių tipai	Kiekis	Pokytis palyginti su 2019m.
01	RIS pažeidžiamumai	188 280	–6 %
02	Kenkimo PĮ	91 788	+34 %
03	Informacijos rinkimas	22 534	–40 %
04	Bandymai nesankcionuotai prisijungti	2 764	-7 %
05	RIS trikdymas (angl. DDoS)	1 087	+206 %
	Iš viso:	**306 453**	**-0.7 %**

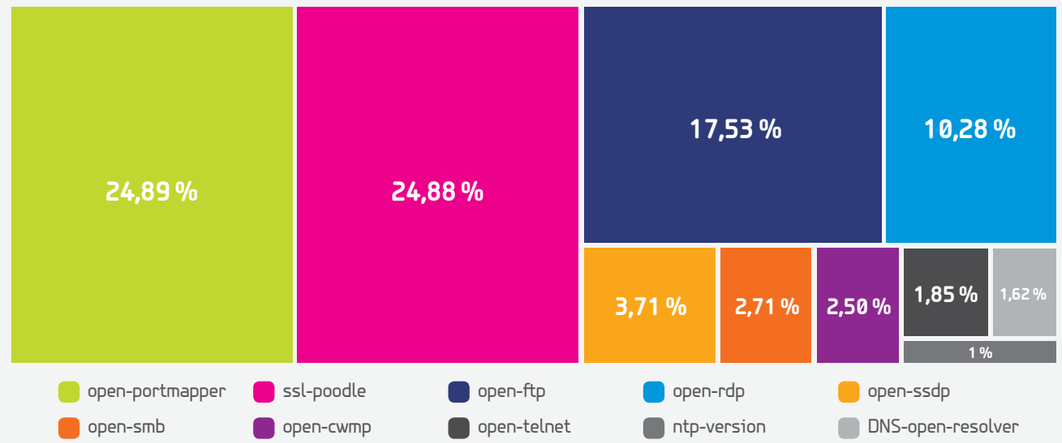
< 08 pav. > Kibernetiniai įvykiai, susiję su Lietuvos IP adresais

Kibernetinių incidentų priežastys dažniausiai buvo žinomų pažeidžiamumų išnaudojimas bei interneto naudotojų kibernetinio saugumo higienos trūkumas

Interneto tinkle veikiančių RIS, kompiuterių, IP įrenginių ir daiktų interneto prietaisų Lietuvoje yra daug. Šie įrenginiai gali turėti PĮ pažeidžiamumų, įranga gali būti laiku neatnaujinta ar padarytos konfigūracijos klaidos. Šios priežastys lemia, kad egzistuoja kibernetinio saugumo pažeidžiamumai, kuriais gali būti pasinaudota vykdant kibernetines atakas. Analizuojant automatinėmis priemonėmis nustatytus kibernetinio saugumo pažeidžiamumus, ryškėja tendencija, kad dažniausiai susiduriama su nesaugios ir nešifruotos nuotolinės prieigos atvejais arba nepakankamai saugių kriptografinių algoritmų naudojimu (žr. **09 pav.**). Dažniausiai prieš atviras ir neapsaugotas prieigas vykdomos slaptažodžių parinkimo atakos. Atspėjus nesudėtingą prisijungimo vardą ir slaptažodį, gaunama neteisėta prieiga prie informacinių išteklių. Įgavus prieigą prie šių išteklių galima juos užšifruoti, pavogti, vykdyti kitas kibernetines atakas[22].

22
https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Labiausiai paplitusių kibernetinio saugumo pažeidžiamumų tipų techniniai duomenys



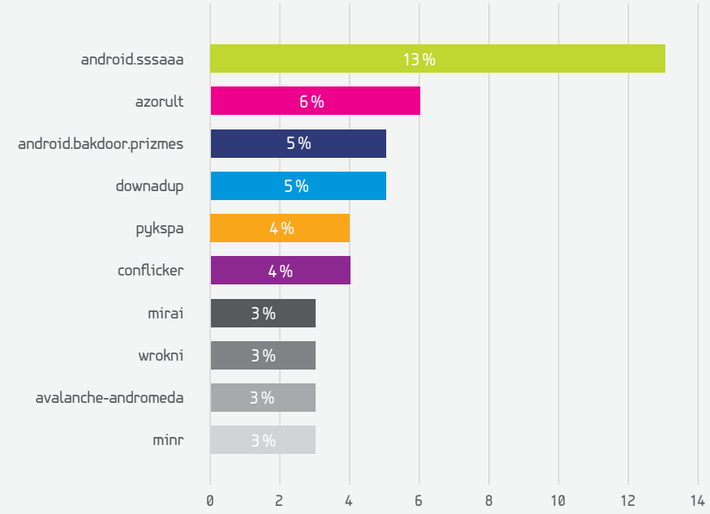
< 09 pav. >

Į turinį

Daugiausia kibernetinių incidentų 2020 m. patyrė elektroninės informacijos prieglobos paslaugų ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai bei smulkios ir vidutinės įmonės

NKSC turimomis automatinėmis priemonėmis Lietuvos IP rėžyje aptinkamos kenkimo PĮ kiekiai statistiškai išaugo 34 proc., palyginti su 2019 m. (žr. **10 pav.**). Šie atvejai detalizuoti pagal kenkimo PĮ tipus, tačiau išskirti būtų galima su „Android" operacinėmis sistemomis susijusią kenkimo PĮ[23].

NKSC priemonėmis aptiktų 91 788 kenkimo PĮ atvejų pasiskirstymas pagal tipus



< 10 pav. >

NKSC, atlikęs Lietuvoje paplitusių bei interneto tinklo paslaugų teikėjų naudojamų belaidžio tinklo prietaisų gamyklinių nustatymų saugumo vertinimą, nustatė, kad nesaugių prietaisų Lietuvoje yra nemažai. Išsiaiškinta, kad nesaugiausi yra maršrutizatorių Technicolor *TG389ac* ir *TG789vac v2* modeliai, *D-Link DIR-825/AC/G1* bei dauguma *TP-LINK* modelių. NKSC pažymi, kad dėl didelės apimties ne visi rinkoje esantys maršrutizatoriai buvo ištirti, o prekyboje gali būti ir daugiau modelių, turinčių panašų pažeidžiamumą.

2020 m. NKSC taip pat gavo nemažai pranešimų apie pažeidžiamumus įvairiose interneto svetainėse. Tai „SQL injection", „Cross-Site Scripting" ir kiti pažeidžiamumai, kurie atsiranda dėl pasenusių TVS ir jų komponentų, silpnų šifravimo algoritmų, neteisingos konfigūracijos. Naudotojų prisijungimo, asmens duomenys bei kiti jautrūs duomenys tampa vieši ir dėl žmogiškųjų klaidų, menkos programinio kodo kontrolės, netinkamo informacinių išteklių žurnalinių įrašų (angl. *event logging*) vedimo ar žurnalinių įrašų politikos nebuvimo.

2020 m. Lietuvoje buvo identifikuota ir keliasdešimt pažeidžiamų virtualiųjų privačių tinklų (toliau – VPN) (angl. *Virtual Private Networks* (VPNs)) įrenginių, o pasinaudojus žinoma saugumo spraga, aptikti ir šių įrenginių naudotojų prisijungimo duomenys. Tai itin jautrūs duomenys, suteikiantys piktavaliams galimybę patekti į vidinius organizacijų tinklus ir atlikti visą spektrą kenkimo veiksmų. Visi sistemų naudotojai (tiek verslo subjektai, tiek valstybinės įstaigos) buvo informuoti, o spragos operatyviai ištaisytos.

23 https://www.shadowserver.org/what-we-do/network-reporting/drone-botnet-drone-report/

NKSC rekomendacijos kibernetinių įvykių prevencijai:

- Rekomenduotina pramoninių valdymo sistemų saugumą užtikrinti šias sistemas izoliuojant atskiruose tinkluose, o jų išorinį pasiekiamumą apriboti ir kontroliuoti. Esant išorinio pasiekiamumo būtinybei, nuotolinę prieigą suteikti tik personalui iš konkrečių dedikuotų IP adresų (angl. *allowlist*), papildomai sustiprinant autentifikavimo priemones, pritaikant dviejų žingsnių autentifikavimą ar kitus mechanizmus.
- Maršrutizatorių savininkai raginami peržiūrėti savo prietaisų nustatymus. Jeigu belaidžio tinklo slaptažodį sudaro tik skaitmenys arba skaitmenys bei didžiosios raidės nuo A iki F, o slaptažodžio ilgis tėra 8–10 simbolių, tuomet būtina pasirūpinti savo prieigos saugumu, pakeičiant slaptažodį į patikimesnį. Saugų slaptažodį turėtų sudaryti bent 12–14 simbolių iš didžiųjų ir mažųjų raidžių, skaitmenų ir specialiųjų simbolių.
- Nuolat vykdyti elementarią kibernetinės saugos higieną – laiku atnaujinti PĮ, naudojant saugius slaptažodžius, tinkamai administruoti naudotojus ir jų teises, taikyti tinkamas žurnalinių įrašų bei duomenų kopijų politikas.

Lietuva 2020 m., kaip ir kitos pasaulio valstybės, susidūrė su kibernetiniais incidentais ir grėsmėmis, susijusiomis su „Trojan.Emotet", RDDoS, kenkimo kodo plitimu atnaujinant „SolarWinds" programinę įrangą

Incidentų analizė

„Emotet" kenkimo PĮ platinimo banga

Lietuvoje nuo 2020 m. spalio mėn. buvo fiksuojamas labai išaugęs „Emotet" kenkimo PĮ platinimo atvejų skaičius, tai sutapo su pasauline šios kenkimo įrangos platinimo tendencija[24]. El. laiškų adresatams atidarius užkrėstus priedus, į kompiuterį įdiegiama kenkimo PĮ ir paimama atitinkama informacija (pvz., iš el. laiškų) tolesniam kenkimo PĮ platinimui (žr. **11 pav.**).

Ši kenkimo PĮ platinama nuolatos[25], tačiau rudenį ir metų pabaigoje itin aktyviai . Pvz., 2020 m. gruodžio 29 d., imituojant Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos (toliau – NVSC) darbuotojos el. laiško adresą, buvo siunčiami laiškai apie neva prastai veikiančią mobiliąją programėlę „KoronaStopLT" su pridėtu galimai „užkrėstu" dokumentu. NKSC duomenimis, tokius netikrus NVSC laiškus gavo Lietuvos Respublikos Vyriausybės, įvairių ministerijų atstovai, taip pat asmenys, su kuriais NVSC specialistai bendravo vykdydami epidemiologinę diagnostiką.

„Emotet" kenkimo PĮ platinama per elektroninio pašto paskyras, jos veikimo būdai yra nuolatos keičiami, todėl NKSC rekomenduoja el. pašto sistemų valdytojams patikslinti el. pašto apsaugos taisykles, politiką ir filtrus (pvz., organizacijos tinklo perimetre sustabdant „archyvinių" ir „vykdomųjų" failų, dokumentų su „macros" komandomis siuntimą, o sustabdytus priedus papildomai patikrinti, pvz., interneto svetainėje **www.virustotal.com**).

NKSC, siekdamas užkardyti „Emotet" kenkimo PĮ platinimą, teikė rekomendacijas[26], kaip apsisaugoti nuo tokių kibernetinių incidentų, taip pat teikė paramą BĮ Kertiniam valstybės telekomunikacijų centrui (toliau – KVTC) nuo šios kenkimo PĮ plitimo saugant Saugiojo valstybinio duomenų perdavimo tinklo naudotojus. Savo ruožtu, Lietuvos Respublikos generalinės prokuratūros ir Lietuvos kriminalinės policijos biuro pareigūnai, bendradarbiaudami su Nyderlandų, Vokietijos, JAV, Jungtinės Karalystės, Prancūzijos, Kanados ir Ukrainos institucijomis, koordinuojant ES teisėsaugos agentūrai (toliau – Europolas) ir Europos teisminio bendradarbiavimo padaliniui (toliau – Eurojustas), tarptautinės operacijos metu uždarė daugiau kaip 700 „Emotet" kenkimo PĮ valdymo stočių (angl. *command and control*). Buvo suduotas stiprus smūgis šio tipo kenkimo PĮ platintojams pasauliniu mastu[27].

24 https://www.enisa.europa.eu/publications/malware

25 NKSC 2020 m. fiksavo 139 kibernetinius incidentus, susijusius su „Emotet" PĮ platinimu.

26 https://www.nksc.lt/naujienos/siunciant_dideli_kieki_virusu_uzkrestu_elektronini.html

27 https://policija.lrv.lt/lt/naujienos/tarptautines-operacijos-metu-uzkirstas-kelias-vienos-pavojingiausiu-kenkejisku-programu-emotet-plitimui-visame-pasaulyjeelektronini.html

Į turinį

„Emotet“ kenkimo PĮ veikimo algoritmas

01 Pristatymas

Atsiunčiamas el. laiškas su susirašinėjimo iškarpa su slaptažodžiu, suarchyvuotu priedu, dokumentu, vykdomuoju failu, nuoroda

Naudotojas atidaro užkrėstą priedą

Atsiunčiamas „Emotet“ kenkimo kodas

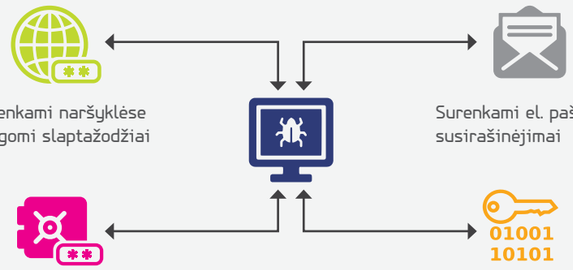
02 Užtikrinamas tęstinumas

„Emotet“ sukuria registro įrašą automatiniam paleidimui, įsiterpiama į veikiančius procesus

03 Siunčiamos instrukcijos

„Emotet“ siunčia informaciją į valdančią (C2) tarnybinę stotį apie naujai užkrėstą kompiuterį ir laukia tolesnių komandų

04 Vykdomos atakos



Surenkami naršyklėse saugomi slaptažodžiai

Surenkami el. pašto susirašinėjimai

Surenkami slaptažodžiai iš slaptažodžių saugojimo programų

Surenkami prisijungimų duomenys

< 11 pav. >

Kibernetinių incidentų, susijusių su kenkimo PĮ, skaičius, palyginti su praėjusiais metais, išaugo net 49 proc.

VRK ir NKSC bendradarbiavimas, užtikrinant rinkimų kibernetinį saugumą

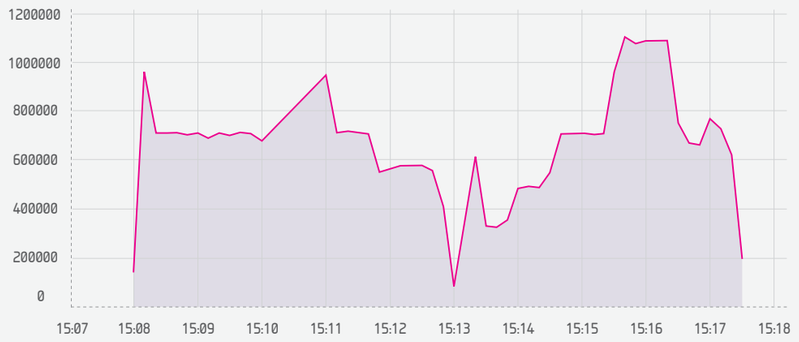
NKSC vertinimu, vienas iš svarbiausių kibernetinio saugumo požiūriu įvykių 2020 m. – pagalba VRK užtikrinant rinkimų į Lietuvos Respublikos Seimą kibernetinį saugumą. NKSC ir VRK bendradarbiavimo patirtis 2019 m. ir NKSC 2020 m. vasarą vykdytas VRK informacinės sistemos kibernetinio saugumo vertinimas sudarė sąlygas iš anksto identifikuoti galimus kibernetinių incidentų rizikos šaltinius.

Rinkimų metu NKSC vykdė VRK informacinės sistemos perimetro stebėjimą, o informacija apie įtartiną veiklą automatinėmis priemonėmis buvo perduodama VRK darbuotojams ir ji nedelsiant būdavo blokuojama. Bendromis NKSC ir VRK pastangomis blokuoti 386 IP adresai, siejami su galimai neteisėta veikla. Vis dėlto buvo fiksuojama kibernetinių incidentų rizika ir pagrindinė problema, su kuria buvo susidurta blokuojant įtartinus IP adresus, – nekontroliuojamos darbo stotys rinkimų apygardose. Rinkimų periodu NKSC taip pat fiksavo ir vertino kenkimo veiklos atvejus prieš VRK rinkimams skirtas sistemas, t. y. išorinę informacinės sistemos perimetro žvalgybą, bandymus atlikti neteisėtus prisijungimus grubios jėgos (angl. *Brute Force*) metodais[28], saugumo pažeidžiamumų paiešką. Taip pat buvo stebimas kenkimo veiklos suaktyvėjimas ir prieš kitas valstybės informacines

[28] Bandant atspėti slaptažodžius pagal simbolių sekas arba sudarytus galimų slaptažodžių rinkinius.

sistemas, kai buvo tikimasi, kad, nukrypus dėmesiui į rinkimus, bus nepastebėti kiti kibernetiniai incidentai ir (ar) įvykiai. Pvz., buvo fiksuojamas suaktyvėjęs BĮ Kertinio valstybės telekomunikacijų centro žvalgymas, blokuoti DDoS (žr. **12 pav.**).

Trumpalaikė DDoS ataka prieš Kertinį valstybės telekomunikacijų centrą 2020 m. spalio 23 d.



< 12 pav. >

Rinkimų periodu taip pat buvo stebimas 120 su rinkimais susijusių internetinių svetainių prieinamumas bei publikuojamo turinio vientisumas, tarp kurių buvo politinių partijų (16), žiniasklaidos (44) ir savivaldybių (60) svetainės. NKSC fiksavo šių interneto svetainių pasiekiamumo problemas – visos jos fiksuotos tik dėl techninių priežasčių, tad neigiamo poveikio rinkimų organizavimui šiuo pažiūriu taip pat nebuvo nustatyta. Todėl, NKSC vertinimu, 2020 m. vykę rinkimai į Lietuvos Respublikos Seimą kibernetinio saugumo požiūriu buvo saugūs.

NKSC su VII valdytojais ir (ar) tvarkytojais derindamas saugos dokumentus pastebi, kad šiam procesui įtakos turi ne tik aplaidus valdytojų požiūris į reikalavimų įgyvendinimą, kompetentingų kibernetinio saugumo, informacinių technologijų specialistų ir (ar) reikalingos kompetencijos trūkumas, bet ir pačių informacinių sistemų bei registrų sudėtingumas, kurį, savo ruožtu, lemia nuolatinė IRT plėtra

Sutrikusi e. sveikatos sistema – nepakankamai įvertintos gamtos stichijų keliamos rizikos[29]

2020 m. liepos mėn. dėl vandens patekimo į duomenų centro patalpas buvo sutrikdytas daugiau kaip 20 valstybės registrų ir valstybės informacinių sistemų darbas, tarp jų Lietuvos Respublikos gyventojų registro, Juridinių asmenų registro, Nekilnojamojo turto kadastro ir registro bei e. sveikatos sistema darbas. Pastarosios sistemos atkūrimo laikas neatitiko šiai sistemai numatyto maksimalaus priimtino paslaugos neveikimo laiko, todėl nukentėjo šios sistemos naudotojai. Ir nors NKSC susipažinus su VĮ Registrų centro atliktais rizikų vertinimais bei veiklos tęstinumo (angl. *business continuity*) valdymo planu, konstatuota, kad serverinės užliejimo rizika buvo numatyta, tačiau problemos laiku atstatant teikiamų paslaugų prieinamumą gali indikuoti, kad galimos panašaus pobūdžio problemos ir kitose valstybės institucijose, kai jose informacijos saugumo rizikos vertinamos paviršutiniškai ar nepakankamai tiksliai, o įvertintoms yra taikomos nepakankamos kibernetinio saugumo priemonės, kurios nesumažina rizikų iki priimtino lygio. Dėl šios priežasties gali išaugti kibernetinių incidentų tikimybė. Taip pat galima manyti, jog institucijų veiklos tęstinumo užtikrinimo galimybės yra ne visada pakankamos, įskaitant ir paslaugų atkūrimą įvykus nelaimei (angl. *disaster recovery*), institucijos savo veiklą ekstremalios situacijos metu valdo *ad hoc* būdais.

[29] Šis e. sveikatos sistemos sutrikimas taip pat aprašytas pagal VDAI kompetenciją, tiriant ADSP VĮ Registrų centre (žr. ataskaitos dalį „Asmens duomenų saugumo pažeidimų įtaka kibernetinio saugumo būklei“, 69 p.).

Į turinį

2020 m. gerokai išaugo skaičius Lietuvos IP adresų, įtrauktų į RIS trikdymo atakas, taip pat IP adresų, užkrėstų kenkimo programine įranga

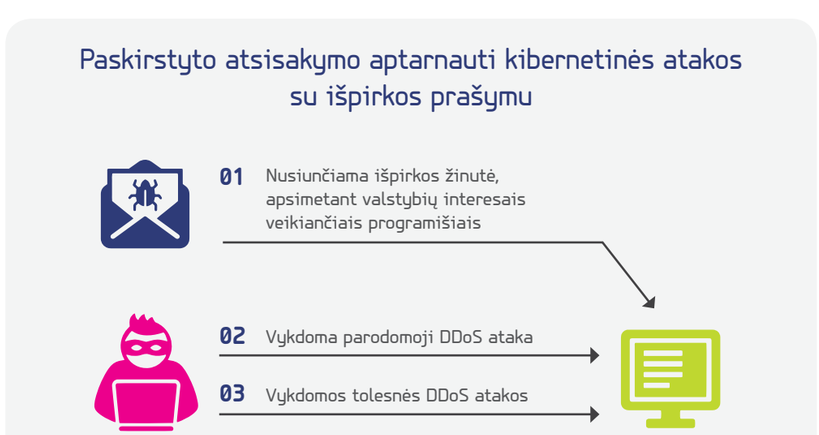
Grasinimai sutrikdyti paslaugas, prašant išpirkos (angl. *Ransom Distributed Denial of Service (RDDoS)*)

Kibernetiniai incidentai prieš Lietuvos kibernetinio saugumo subjektus, kai buvo grasinama kibernetiniais incidentais prašant išpirkos, buvo fiksuojami 2020 m. balandžio ir spalio mėnesiais. Visais atvejais buvo grasinama DDoS. Remiantis Lietuvoje fiksuojamais atvejais bei bendradarbiaujant su Europos tinklų ir informacijos saugumo kompiuterinių incidentų tyrimo tarnybomis, nustatyta, kad daugiausia buvo taikytasi į finansinio sektoriaus ir interneto paslaugų teikėjų DNS infrastruktūrą[30]. NKSC pabrėžia, kad kiekvienam subjektui informavusiam apie tokio pobūdžio grasinimus buvo suteiktos rekomendacijos.

Pagrindiniai tokių kibernetinių incidentų būdai (žr. **13 pav.**) ir požymiai:

1. gaunamas išpirkos reikalaujantis laiškas, neva nuo pasaulinio lygio grupuočių *Lazarus Group, Fancy Bear, Armada Collective* ir pan. Laiškai siunčiami iš @protonmail.com elektroninių paštų;
2. nusiuntus žinutę, atliekama bandomoji ataka. Kai kuriais atvejais taikomasi į vieną IP adresą, kitais – į keletą. Atakų trukmė ir dydis dažniausiai būna skirtingas;
3. atakų intensyvumas svyruoja apie 300 Gbit/s;
4. atakos vykdomos: „ARMS, DNS Flood, GRE Protocol Flood, SNMP Flood, SYN Flood ir WSDiscovery Flood“ metodais, taip pat „UDP, CLDAP, DNS, WS-Discovery, GRE, NTP, SNMP“ protokolais.

NKSC rekomenduoja stebėti informacinę infrastruktūrą dėl anomalijų ir nemokėti išpirkos, nes tai negarantuoja, kad Jūsų įmonė bus apsaugota.



< 13 pav. >

Lietuvos kibernetinės erdvės žvalgyba, išnaudojant žinomus pažeidžiamumus

Žvalgymo veiksmais siekiama surasti nesaugias nuotolines prieigas arba gerai žinomus pažeidžiamumus, leidžiančius nesudėtingais būdais vykdyti komandas nuotoliniu būdu. NKSC techninėmis kibernetinio saugumo priemonėmis (sensoriais) stebi YSII bei VII dėl galimų kibernetinių incidentų. Buvo nustatyta, kokių paslaugų dažniausiai yra ieškoma atliekant žvalgymąsi. Daugiausia vyksta

30 https://www.nksc.lt/naujienos/nksc_ispeja_apie_suaktyvejusias_paskirstyto_atsisa.html

23 „Telnet“ prievado skenavimų, nors praktikoje jis naudojamas vis rečiau, nes jį pakeitė 22 „SSH“ paslauga nuotoliniam prisijungimui. Skenavimų statistikos imtyje išsiskiria „Mikrotik“ prievadų žvalgymo skaičius, kuris, tikėtina, susijęs su plačiai nuskambėjusiu pažeidžiamumu[31], leidusiu nuotoliniu būdu išgauti prisijungimo prie įrenginio duomenis, įskaitant slaptažodžius. Dažniausiai Lietuvos kibernetinės erdvės žvalgyba buvo vykdoma iš Seišelių, Rusijos, JAV ir Kinijos valstybės (žr. **14 pav.**).

Nr.	Valstybė	Proc.
01	Seišeliai	22 %
02	Rusija	22 %
03	JAV	22 %
04	Kinija	12 %
05	Nyderlandai	10 %
06	Prancūzija	3 %
07	Bulgarija	3 %
08	Ispanija	2 %
09	Taivanas	2 %
10	Ukraina	2 %

< **14 pav.** Valstybės, iš kurių dažniausiai atliekami žvalgymosi veiksmai >

NKSC atkreipia dėmesį, kad ši informacija nebūtinai reprezentuoja tikrai tas valstybes, iš kurių buvo vykdoma Lietuvos kibernetinės erdvės žvalgyba, nes yra gana paprasta naudotis kitų valstybių paslaugomis, siekiant paslėpti tikruosius žvalgybą vykdančius veikėjus arba pradinį kibernetinio incidento šaltinį. Detalesnė populiariausių IP adresų informacija, iš kurių buvo vykdoma žvalgymosi veikla, yra susijusi su tokias paslaugas teikiančiomis interneto svetainėmis arba prieglobos paslaugas teikiančiais subjektais (žr. **15 pav.**).

Nr.	IP adresas	Sietinas domenas
01	80.82.64.73	http://scanner.openportstats.com
02	194.26.25.127	https://sshvps.net
03	80.82.77.234	http://scanner.openportstats.com
04	194.26.29.107	https://sshvps.net
05	5.188.206.34	https://pinspb.ru
06	141.98.11.12	https://serveroffer.lt
07	94.102.51.28	https://websec-test.com
08	45.143.220.169	http://zumy.eu
09	94.102.51.95	http://increditserve.net
10	185.176.27.42	https://ngs.ru

Žvalgymo veiksmais siekiama surasti nesaugias nuotolines prieigas arba gerai žinomus pažeidžiamumus, leidžiančius nesudėtingais būdais realizuoti valdymo komandas nuotoliniu būdu

<15 pav.

Populiariausi 10 IP adresų, iš kurių buvo vykdoma valstybės informacinių išteklių ir ypatingos svarbos informacinės infrastruktūros žvalgyba

31 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14847

Į turinį

Piktavaliai, siekdami gauti patikimesnių duomenų, atsižvelgia į saugumo specialistų dažnai naudojamą praktiką pakeisti žinomus prievadus į mažiau žinomus (pvz., MS-RDP prievadą iš 3389 į 3390) (angl. *security by obscurity*). Įvertinus žvalgymosi informaciją, matyti, kad piktavaliai nuolatos ieško paprasčiausio būdo išnaudoti pažeidžiamumus. Dėl šios priežasties ir toliau dažniausiai ieškoma prievadų, kurių pažeidžiamumus yra paprasta išnaudoti arba apie kurių išnaudojimą yra turima daugiausia informacijos (žr. **16 pav.**).

Nr.	Prievadas	Kiekis	Paslauga	Galimos kibernetinės atakos
01	23	31 %	Telnet	Nešifruota nuotolinė valdymo prieiga, prie kurios galima bandyti autentifikuotis arba įsiterpti į komunikacijas.
02	445	14 %	MS-DS	Microsoft „SMB" informacijos tarp įrenginių dalijimosi paslauga (išnaudojant spragą buvo vykdoma „WannaCry" ataka). Yra nustatyti pažeidžiamumai, kai nuotoliniu būdu be autentifikavimosi galima siųsti komandas į paslaugą.
03	1433	13 %	MS-SQL	Tinkamai neapsaugojus, nuotoliniu būdu galima siųsti komandas į paslaugas, kenkimo PĮ ar gauti duomenų bazėje esančius duomenis.
04	5060	8 %	SIP	Dažnai naudojamas IP telefonijoje. Pažeidus atsisakymo aptarnauti kibernetinėms atakoms (angl. *Distributed Denial of Service*).
05	80	7 %	HTTP	Vykdant autentifikaciją HTTP metodu, kuris yra nešifruotas, galima perimti komunikacijas ir prisijungimų duomenis.
06	8291	7 %	Mikrotik	Galimybė išnaudoti „WinboxExploit" pažeidžiamumą ir nuotoliniu būdu iš pažeidžiamų „Mikrotik" maršrutizatorių išgauti prisijungimų duomenis bei slaptažodžius.
07	22	6 %	SSH	SSH protokolas, pakeitęs „Telnet", laikomas saugesniu dėl aktyvuotos šifravimo funkcijos. Tačiau prieš atvirai prieinamą paslaugą galima vykdyti *brute-force* atakas.
08	7547	6 %	TR-069	Aplikacijos lygmens protokolas galinių įrenginių valdymui (pvz., gali būti taikomasi norint įrenginius įtraukti į užvaldytų įrenginių tinklą (angl. *botnet*)).
09	3389	5 %	MS-RDP	Nuotolinė „Microsoft Remote Desktop" prieiga, kuriai esant atvirai vykdomos slaptažodžių parinkimo atakos, o prisijungus šifruojami duomenys, prašoma išpirkos, vykdomos duomenų vagystės.
10	8080	3 %	HTTP	Vykdant autentifikavimą HTTP metodu, kuris yra nešifruotas, galima perimti komunikacijas ir prisijungimų duomenis.

< 16 pav. Statistiškai labiausiai žvalgomi prievadai >

NKSC rekomendacijos, kaip apsaugoti kompiuterį nuo įsilaužėlių

- Ugniasienėje apribokite nenaudojamus prievadus.
- Nesant galimybės apriboti prievadų, pakeiskite juos į rečiau naudojamus.
- Naudokite „reverse Proxy", kad nebūtų įmanoma iš išorės identifikuoti aktyvių paslaugų ir techninės ar PĮ.
- Prieigas prie paslaugų valdykite pagal leistinus IP adresus.
- Segmentuokite prieigą, jai naudokite kriptografines priemones (pvz., VPN) bei saugius sertifikatus.

NKSC interneto svetainių saugumo audito įrankiu galima nemokamai pasitikrinti, ar valdomoje interneto svetainėje nėra saugumo spragų. Šiuo saugumo įrankiu 2020 m. pasinaudojo per 600 svetainių valdytojų

Interneto svetainių saugumo problematika

Lietuvoje registruojamų .lt domenų skaičius nuolat didėja ir jau perkopė 200 tūkst. ribą. Didėjant interneto svetainių[32] skaičiui, didėja ir svetainių, turinčių įvairių pažeidžiamumų.

Nesaugių interneto svetainių priežastys dažniausiai yra:

- prasta jų priežiūra;
- neatnaujintos TVS[33] ir jų komponentai;
- vieša prieiga prie interneto svetainės TVS administravimo;
- nesaugi slaptažodžių naudojimo praktika.

Dėl to išaugo grėsmės lietuviško domeno interneto svetainių lankytojams bei jų įrenginiams būti išnaudotiems piktavalių. Dažniausiai nesaugiose interneto svetainėse yra įterpiamas kenkimo programinis kodas, kuris pagal savo specifiką atlieka žalingą veiklą, pvz., įtraukia įrenginius į „botnet" veiklą, nukreipia naudotojus į suklastotus interneto svetainių puslapius, kuriuose bandoma surinkti asmeninius arba kreditinių kortelių duomenis.

Siekdamas nustatyti pažeistas interneto svetaines, NKSC periodiškai automatinėmis priemonėmis vykdo visų Lietuvos interneto svetainių patikrą specialioje virtualioje aplinkoje – smėliadėžėje (angl. *sandbox*), kuri pagal specialių taisyklių rinkinį nustato interneto svetainės puslapio grėsmės lygį. Aptikęs galimai pažeistą interneto svetainę, NKSC tai vertina kaip kibernetinį incidentą ir toliau atlieka jo valdymą, bendrauja su interneto svetainės valdytoju ir kitomis priemonėmis siekia, jog kenkimo kodas interneto svetainėje būtų pašalintas. Periodiškai yra tikrinamos visos aktyvios .lt domeno svetainės, tokiu būdu 2020 m. buvo atlikta 734 tūkst. interneto svetainių patikrinimų (skenavimus kartojant maždaug kas 3 mėn.). NKSC, šiuo būdu vykdydamas Lietuvos interneto svetainių patikrą, registravo 322 interneto svetaines, kuriose nustatytas kenkimo kodas.

2020 m. atlikus interneto svetainių skenavimus, iš 187 431 aktyvių aukščiausiojo .lt domeno interneto svetainių su TVS identifikuota 70 821. Populiariausia atvirojo kodo TVS Lietuvoje, vertinant visą .lt domeno sritį, buvo *Wordpress* (26,17 proc.), *Joomla* (2,33 proc.) ir *Prestashop* (1,74 proc.). Vertinant viešojo sektoriaus TVS, daugiausia buvo *Wordpress* (30,72 proc.) ir *Joomla* (13,25 proc.),

32 Interneto svetainė – informacinių technologijų pagrindu veikianti informacinė sistema ar informacinės sistemos sudedamoji dalis (komponentė, posistemis), skirta informacijai skelbti ir įvairioms paslaugoms IRT priemonėmis teikti.

33 TVS – tai technologinis sprendimas, skirtas interneto svetainės turiniui kurti ir redaguoti. Dažniausiai ši sistema apima ir jos pačios komponentų, naudotojų bei jų teisių administravimą.

Į turinį

Daugiausia kibernetinių incidentų 2020 m. patyrė elektroninės informacijos prieglobos paslaugų ir viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjai bei smulkios ir vidutinės įmonės

tarp Lietuvos įmonių – *Kryptis* (6,93 proc.), *Fresh Media* (6,73 proc.), *Idamas* (3,31 proc.) bei užsienio atviro kodo *TVS CMS Made Simple* (5,62 proc.) (žr. **17 pav.**).

Nr.	TVS	Paplitimas Lietuvoje	Paplitimas viešajame sektoriuje
01	Wordpress	26,17 %	30,72 %
02	Joomla	2,33 %	13,25 %
03	Prestashop	1,74 %	<1 %
04	Opencart	1,33 %	<1 %
05	Wix	1,07 %	<1 %
06	Kryptis	<1 %	6,93 %
07	Fresh Media	<1 %	6,73 %
08	CMS Made SImple	<1 %	5,62 %
09	Idamas	<1 %	3,31 %
10	Drupal	<1 %	1,91 %
11	Kita	3,51 %	4,02 %
12	Nenustatyta[34]	62,21 %	27,21 %

< **17 pav.** Populiariausios identifikuotos TVS Lietuvoje >

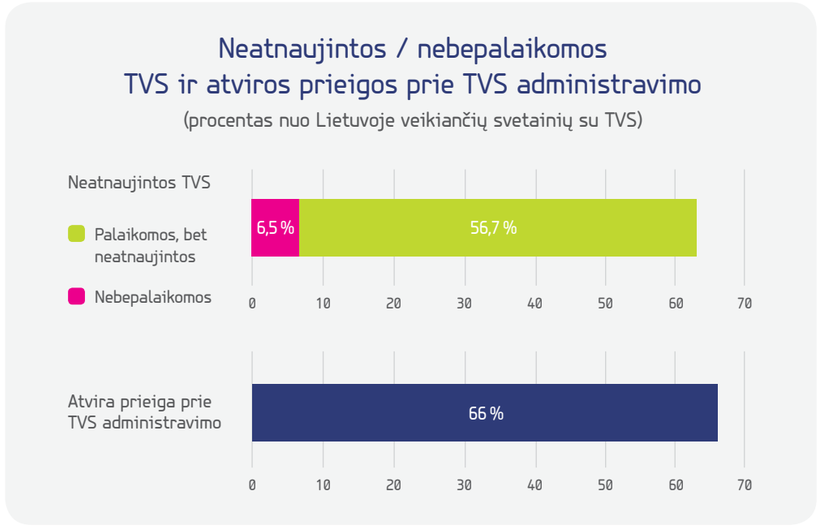
2020 m. atliktų skenavimų rezultatai (žr. 18 pav.):

Iš visų interneto svetainių su TVS **56 proc.** naudoja neatnaujintą TVS PĮ, kuri nėra saugi dėl paviešintų pažeidžiamumų. Tai sudaro **21 proc.** iš visų aktyvių .lt domeno interneto svetainių.

Deja, **6,5 proc.** naudojamų TVS yra gamintojo nebepalaikomos, todėl nelieka net teorinės galimybės pašalinti saugumo spragų.

Iš visų identifikuotų interneto svetainių su TVS **66 proc.** turėjo atvirą prieigą prie TVS administravimo (tai sudaro **25 proc.** visų aktyvių .lt svetainių), todėl piktavaliai gali bandyti į jas įsilaužti, automatinėmis priemonėmis generuodami prisijungimo vardus bei slaptažodžius.

34 Nenustatyta TVS – apima visas interneto svetaines, kuriose yra duomenų prieglobos tiekėjų ar vardų registracijos paslaugas teikiančių įmonių pirminiai (angl. *default*) interneto svetainių puslapiai, interneto svetaines, kurių domenai nukreipia į kitas svetaines, socialinių tinklų paskyros; taip pat svetainės, kurių TVS norima paslėpti arba neaptikta požymių, pagal kuriuos jas galima būtų identifikuoti.

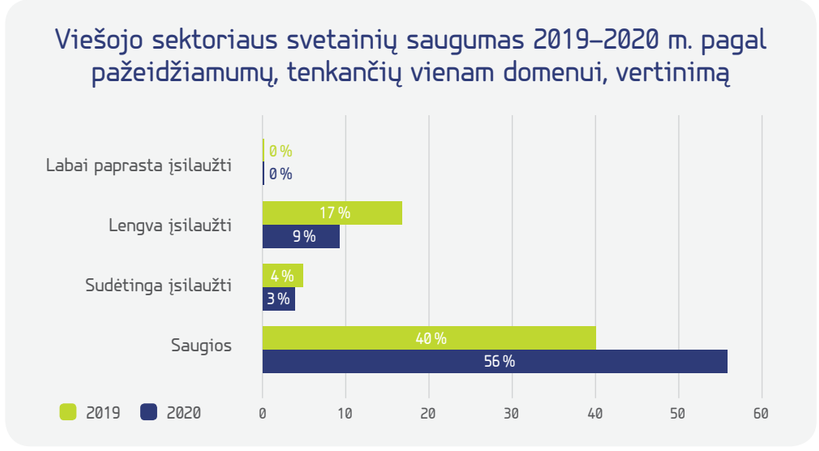


< 18 pav. >

Nors viešojo sektoriaus atstovų interneto svetainių, į kurias galima įsilaužti, skaičius sumažėjo, o saugių svetainių skaičius padidėjo, tačiau, NKSC vertinimu, svetainių kibernetinio saugumo situacija dar nėra gera

Piktavaliai išnaudoja šias spragas kenkimo veiklai atlikti, t. y. svetainės tampa kibernetinių atakų taikiniais. Dažniausiai svetainės atakuojamos automatizuotomis priemonėmis. Piktavalių sukurti užvaldytų kompiuterių tinklai skenuoja internetu pasiekiamas svetaines, ieško silpnų vietų – neatnaujintų pažeidžiamų TVS komponentų – ir per jas braunasi į vidų. Atradęs spragų, kenkimo kodas perima svetainės valdymą, įsiterpia į esamus svetainės failus, kuria naujus, naudoja įvairias jo aptikimą apsunkinančias priemones. Užkratas taip pat gali įdiegti „galines duris" (angl. *backdoor*), kurios naudojamos išlaikyti svetainės kontrolę, jeigu jos savininkui pavyktų pašalinti dalį pažeistų failų ar ištaisyti esamas spragas.

NKSC taip pat vykdo periodinius viešojo sektoriaus interneto svetainių pažeidžiamumo patikrinimus ir apie aptiktus kritinės[35] svarbos pažeidžiamumus informuoja šių svetainių valdytojus. Išanalizavus 2020 m. patikrinimų duomenis, matyti, kad viešojo sektoriaus interneto svetainių kibernetinio saugumo situacija šiek tiek pagerėjo, palyginti su ankstesniu laikotarpiu, tačiau ji dar nėra gera. Svetainių, į kurias galima įsilaužti, skaičius sumažėjo, o saugių[36] svetainių skaičius padidėjo (žr. **19 pav.**)



< 19 pav. >

35 Kritiniai pažeidžiamumai yra tie, kurių bendra vertinamų kriterijų vertė yra nuo 7,5 iki 10 balų pagal Bendrąją pažeidžiamumo vertinimo sistemą (angl. *Common Vulnerability Scoring System* (CVSS)).

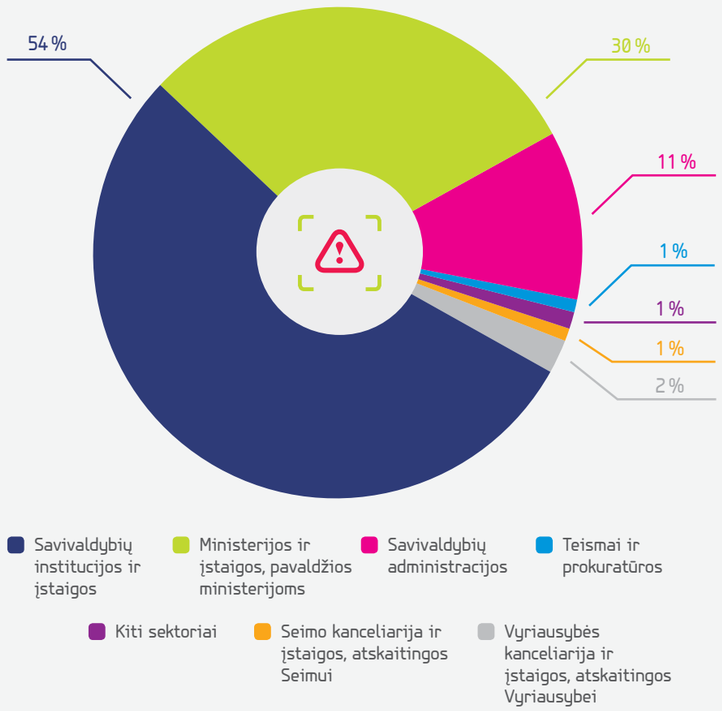
36 Saugiomis svetainėmis laikomos tos svetainės, kuriose pažeidžiamumų nenustatyta, ir tos, kuriose nustatyti pažeidžiamumai nesiekia 5 balų pagal Bendrąją pažeidžiamumo vertinimo sistemą.

Į turinį

Priešiškų valstybių žvalgybos ir jų remiami piktavaliai ar jų grupuotės šnipinėja siekdami politinių, karinių, ekonominių ir (ar) ideologinių tikslų. COVID-19 pandemija priešiškos žvalgybos tarnyboms sudarė daugiau galimybių veikti kibernetinėje erdvėje ir išnaudoti joje atsiradusius pažeidžiamumus, priversti konkrečius asmenis atidaryti užkrėstus elektroninių laiškų priedus ar kenkimo kodo užvaldytas nuorodas

Dažniausiai aptinkami pažeidžiamumai viešojo sektoriaus svetainėse susiję su neatnaujinta svetainės aptarnaujančių serverių PĮ. Kaip ir kitų pažeidžiamumų atveju, viešojo sektoriaus svetainių spragų ir su jomis susijusių incidentų buvo galima išvengti laikantis kibernetinės saugos higienos – laiku atnaujinant PĮ, naudojant saugius slaptažodžius, tinkamai administruojant vartotojus ir jų teises, taikant tinkamas žurnalinių įrašų bei duomenų kopijų politikas.

Bendras interneto svetainių pažeidžiamumas viešojo sektoriaus įstaigose



< 20 pav. >

Nacionalinių kibernetinio saugumo pratybų „Kibernetinis skydas 2020" metu kibernetinio saugumo subjektams buvo išryškinta svetainių saugumo problematika, analizuojamas konkretus nesaugios svetainės pavyzdys ir dėl to kylančios grėsmės. Kiekvienais metais pratybose pateikiamas užvaldytos svetainės scenarijus. Buvo nagrinėjamas incidentas, susijęs su piktavalio atspėtu svetainės prisijungimo slaptažodžiu ir prisijungimu prie interneto svetainės TVS administravimo. Dalyviai buvo kviečiami įvertinti, ar jų svetainės prieiga yra saugi, ar tinkamai valdomos paskyros, ar tinkama slaptažodžių politika ir pan.

Nors interneto svetainių saugumo problemų daug ir jas bandoma spręsti skirtingomis priemonėmis, situaciją apsunkina svetainių valdytojų pasyvumas ir reikiamos kompetencijos stoka. Kitos, iš dalies objektyvios, svetainių valdytojų neveikimo priežastys yra: interneto svetainių priežiūros paslaugų negavimas, netinkamos sutartys su svetainių kūrėjais, sudėtingi ir ilgai trunkantys viešieji pirkimai. Dažnai svetainių valdytojai teisinasi lėšų trūkumu arba apeliuoja į ateitį suplanuotais naujų interneto svetainių pirkimais.

Kadangi kibernetinė erdvė yra sparčiai besikeičianti ir nepastovi, nuolatos reikia tikrinti savo valdomas interneto svetaines dėl atsiradusių naujų pažeidžiamumų. Interneto svetainių valdytojai įvertinti savo svetainių puslapių pažeidžiamumą gali ir patys, pasinaudoję NKSC svetainių saugumo audito įrankiu[37]. Juo galima nemokamai pasitikrinti, ar turimoje svetainėje nėra saugumo spragų. Įrankis pateiks situacijos ataskaitą pagal Atviro žiniatinklio programų saugumo projekto metodiką ir nurodys, kokie pažeidžiamumai aptikti. Turėdami tokią informaciją, svetainių valdytojai galės ištaisyti rastus trūkumus ir pagerinti valdomų informacinių išteklių saugumo būklę. Šiuo saugumo įrankiu per 2020 m. pasinaudojo per 600 svetainių valdytojų.

NKSC rekomenduoja numatyti ir tinkamai suplanuoti lėšas, reikalingas interneto svetainių priežiūrai, tinkamai parengti interneto svetainių pirkimo dokumentus ir tolesnio jų aptarnavimo sutartis, į jas įtraukiant nuostatas dėl kibernetinio saugumo užtikrinimo.

Kitos išsamios NKSC rekomendacijos interneto svetainių pažeidžiamumų prevencijai pateikiamos interneto svetainėje
https://www.nksc.lt/rekomendacijos/interneto_svetainiu_apsauga.html

Incidentų analizė

Plataus masto kibernetinis-informacinis incidentas prieš Lietuvos Respubliką[38]

2020 m. gruodžio 9 d. pasinaudojus vieno iš Lietuvos interneto svetainių kūrėjo saugumo spraga slaptažodžių valdymo procesuose, buvo vykdomi neteisėti prisijungimai prie interneto svetainių, kuriose buvo skelbiama tikrovės neatitinkanti informacija. Neteisėti prisijungimai fiksuoti prie mažiausiai 24 viešojo sektoriaus svetainių, kurių didžioji dalis priklauso savivaldybių administracijoms. Prisijungę prie interneto svetainių, piktavaliai įkėlė tris skirtingas tikrovės neatitinkančios naujienas: „Lenkijos diplomatas sulaikytas įvažiuojant į Lietuvą", „Šiaulių oro uosto infrastruktūros modernizavimo yra FEIKAS", „Karo prievolės ir komplektavimo tarnybos regioniniai padaliniai patikslina karo prievolininkų šauktinių sąrašus". Tuo pačiu metu buvo platinami suklastoti el. laiškai imituojant Krašto apsaugos ministerijos, Užsienio reikalų ministerijos ir Šiaulių savivaldybės administracijos el. pašto adresus. Laiškuose buvo atkartojamas melagienų turinys ir pateikiamos nuorodos į pažeistas svetaines.

Įvertinus tyrimo metu surinktą medžiagą, nustatyta, kad šiam incidentui buvo pasirengta iš anksto, o pats incidentas vykdytas organizuotai ir planingai. Siekiant įvykdyti tokias hibridines atakas pasinaudojama žinomais pažeidžiamumais, naudojami socialinės inžinerijos metodai ir įgyti prisijungimų prie interneto svetainių ar kitų informacinių sistemų duomenys. Šiuo atveju buvo orientuojamasi į vieno konkretaus Lietuvos TVS gamintojo pažeidžiamumą, susijusį su autentifikavimosi mechanizmu ir slaptažodžių sudarymo algoritmu. Tokiu būdu buvo gauta galimybė prisijungti prie interneto svetainių ir platinti melagingą informaciją. Melagingoms žinutėms sustiprinti buvo platinamos suklastotos Lietuvos valstybės institucijų darbuotojų el. pašto žinutės - toks kibernetinio incidento *modus operandi* NKSC buvo fiksuotas ir anksčiau, tik šiuo atveju kibernetinis incidentas buvo vykdomas daug platesniu mastu. Tokie kibernetiniai incidentai rodo, jog interneto svetainių kūrėjai ir valdytojai neskiria pakankamo dėmesio gerosioms kibernetinio saugumo praktikoms, o NKSC specialistų rekomendacijos[39] taikomos nepakankamai.

NKSC bendravo su kiekviena šio kibernetinio incidento paveikta institucija, teikė nurodymus pažeidžiamumui užkardyti. Rekomendacijos taip pat tiesiogiai buvo pateiktos Lietuvos interneto svetainių kūrėjui, kurio kuriamoje TVS buvo surasta spraga.

37
Nemokama NKSC žiniatinklio taikomųjų programų programinio kodo žinomų spragų patikrinimo paslauga https://site-check.cert.lt

38
Šis incidentas taip pat aprašytas pagal Lietuvos policijos kompetenciją, dėl šio įvykio pradėjus ikiteisminį tyrimą (žr. ataskaitos dalį „Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis", 61 p.) ir pagal LK SKD kompetenciją, analizuojant informacinį incidentą (žr. ataskaitos dalį „Lietuvos nacionaliniams interesams priešiškos informacijos vertinimas", 75 p.).

39
https://www.nksc.lt/rekomendacijos/interneto_svetainiu_apsauga.html

Į turinį

NKSC atliekami kibernetinio saugumo subjektų patikrinimai rodo, kad subjektai deklaruoja geresnę kibernetinio saugumo būklę, negu yra iš tikrųjų

YSII valdytojų bei VII valdytojų ir (ar) tvarkytojų kibernetinio saugumo būklė

NKSC atlieka YSII valdytojų bei VII valdytojų ir (ar) tvarkytojų atitikties reikalavimams priežiūrą. Ši priežiūra 2020 m. buvo atliekama vykdant kibernetinio saugumo patikrinimus subjektų RIS.

2020 m. NKSC atliko 6 pasirinktų kibernetinio saugumo subjektų kibernetinio saugumo patikrinimus. Patikrinimai buvo vykdomi pagal klasikinę tokio pobūdžio auditų metodologiją – vertinant aprašytus procesus, techninėmis priemonėmis identifikuojant saugumo spragas, vykdant darbuotojų interviu, stebint kibernetinio saugumo valdymo procesus, radiniams priskiriant rizikų reikšmes, parengiant bei pristatant kibernetinio saugumo užtikrinimo rekomendacijas. Papildomai, atliekant patikrinimus buvo panaudoti aktyvaus įsibrovimo (angl. *penetration testing*) metodai bei remtasi gerosiomis praktikomis ir standartais, pvz., Atviro žiniatinklio programų saugumo projekto metodika.

Aktyvaus įsibrovimo metodais buvo tikrintas RIS atsparumas kibernetiniams incidentams. Nustatyta skirtingo lygio[40] pažeidžiamumų, leidžiančių piktavaliams įvykdyti kibernetinius incidentus. Dažniausiai šiuos pažeidžiamumus galima suskirstyti į penkias grupes, t. y. nesaugių kriptografinių priemonių naudojimas, nepatikimas prieigos prie paslaugų valdymas, nesaugus prisijungimo duomenų valdymas, nesaugios konfigūracijos, pasikartojantys neatnaujintos bei pažeidžiamos PĮ naudojimo atvejai (žr. **21 pav.**).

40
Pažeidžiamumai klasifikuojami pagal Bendrąją pažeidžiamumo vertinimo sistemą, https://nvd.nist.gov/vuln-metrics/cvss

NKSC patikrinimų metu nustatyti dažniausiai pasitaikantys didelės ir vidutinės reikšmės pažeidžiamumai bei prieš juos nukreiptų galimų kibernetinių incidentų pavyzdžiai

Nesaugių kriptografinių priemonių naudojimas

Nepatikimi šifravimo algoritmai, pasenę protokolai, nesaugus sertifikatų išdavimas bei išduotų valdymas ir pan.

Nepatikimos prieigos prie paslaugų

Atviri prievadai, neapribotas prisijungimas iš interneto prie naudotojų bei administratorių prisijungimų valdymo skydo, neribota galimybė jungtis prie paslaugų su neteisingais prisijungimų duomenimis.

Blogas slaptažodžių valdymas

Gamyklinių slaptažodžių naudojimas, bendros naudotojų paskyros, trumpi slaptažodžiai, naudojant vieną arba du faktorius, tų pačių slaptažodžių naudojimas.

Nesaugios konfigūracijos

Neaprašyti SPF, DNSSEC, DKIM, DMARC ir kiti įrašai, galimybė naršyti aplankuose, nevykdoma įvedamų duomenų validacija ir pan.

Neatnaujintos PĮ naudojimas

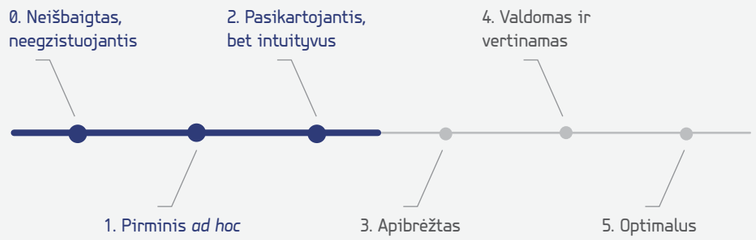
Neatnaujintos TVS, tarnybinių ir darbo stočių OS bei kita PĮ.

GALIMOS ATAKOS PRIEŠ PAŽEIDŽIAMUMUS

- Man-in-the-middle
- Distributed Denial of Service
- Social enigineering
- SQL injection
- Buffer overflow
- Clickjacking
- Rainbow tables
- Spoofing
- Cross-site scripting
- etc.

< 21 pav. >

Apibendrinus atliktų patikrinimų išvadas, galima teigti, kad dažniausiai kibernetinio saugumo subjektų kibernetinio saugumo būklė neatitinka deklaruojamos, t. y. kibernetinio saugumo subjektai dažniausiai savo RIS kibernetinį saugumą vertina geriau, negu yra iš tikrųjų. Pvz., organizacijų aprašyti kibernetinio saugumo procesai ne visada yra vykdomi, darbuotojams nėra priskiriamos konkrečios atsakomybės, egzistuoja RIS pažeidžiamumai. Pažymėtina, kad kibernetinio saugumo užtikrinimas organizacijose vis dar užtikrinamas neišbaigtais, pasikartojančiais ir intuityviais principais (žr. **22 pav.**) [41].



< 22 pav. >

Kibernetinio saugumo subjektai, įgyvendindami kibernetinio saugumo reikalavimus, dažnai susiduria su šiomis problemomis: įvairūs pažeidžiamumai įrenginiuose, įvykių bei naudotojų veiksmų nesaugojimas bei neefektyvios kibernetinių incidentų valdymo procedūros

Atliktų kibernetinio saugumo patikrinimų rezultatai parodė, kad kibernetinio saugumo subjektai nevienodai įgyvendina organizacinius reikalavimus. Ypač iškyla sunkumų įgyvendinant organizacinius reikalavimus, susijusius su pažeidžiamumų nustatymu, įvykių bei naudotojų veiksmų analize, kibernetinių incidentų valdymo organizavimu (žr. **23 pav.**). Dėl šios priežasties RIS tampa pažeidžiamos ir sudaromos sąlygos įvykti kibernetiniams incidentams panaudojant žinomus pažeidžiamumus (pvz., saugumo spragos dėl neatnaujintos PĮ, konfigūracijos klaidos, gamyklinių nustatymų naudojimas ir pan.). Nepakankamas šių reikalavimų įgyvendinimas apribroja kibernetinio saugumo subjektų galimybes laiku aptikti ir užkardyti kibernetinius incidentus.

Organizaciniai reikalavimai, su kurių įgyvendinimo sunkumais susiduriama, bei jų įgyvendinimo teigiamas efektas

Pažeidžiamumų nustatymo procesas

Laiku nustatomi ir užkardomi pažeidžiamumai

Pvz., uždaromi atviri prievadai, nešifruotos prieigos

Įvykių bei naudotojų veiksmų analizė

Aptinkamos anomalijos bei kibernetiniai incidentai

Pvz., aptinkamos kompromituotos naudotojų paskyros

Kibernetinių incidentų valdymo organizavimas

Nustatomos kibernetinių incidentų priežastys bei realus poveikis

Pvz., identifikuojama, jog naudojami nesaugūs slaptažodžiai

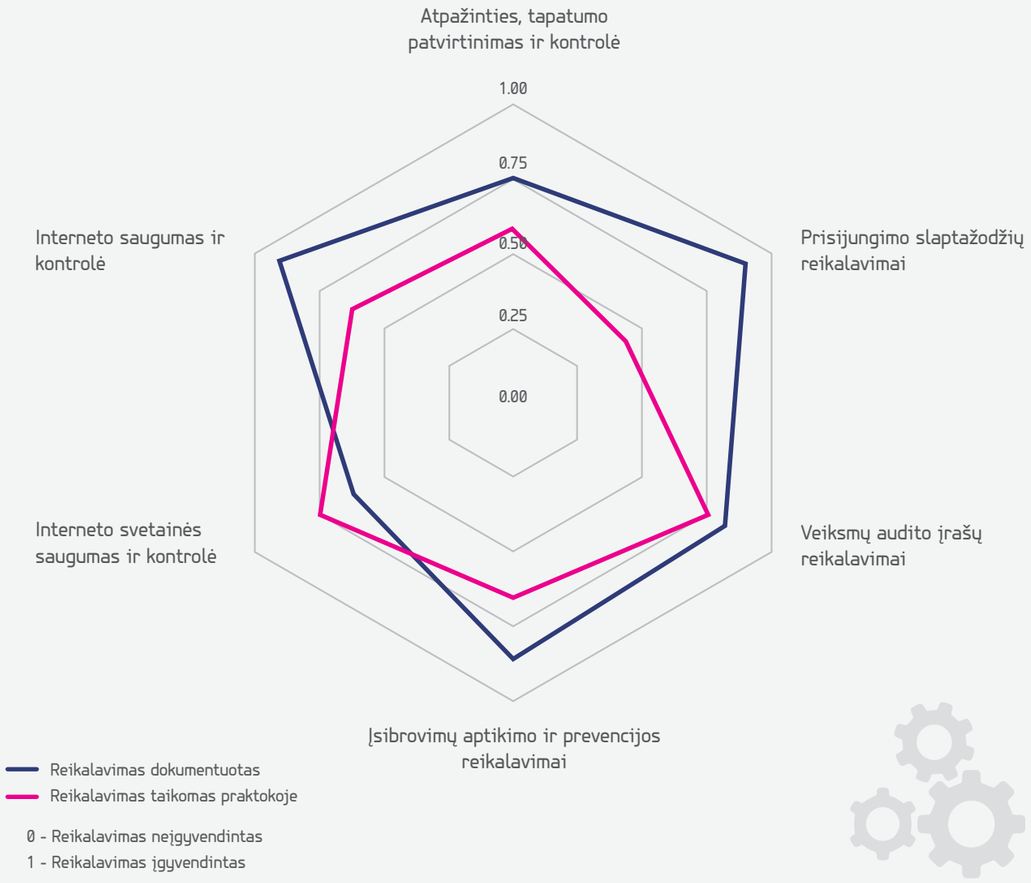
41
https://www.isaca.org/resources/news-and-trends/industry-news/2020/effective-capability-and-maturity-assessment-using-cobit-2019

< 23 pav. >

Į turinį

NKSC pažymi, kad kibernetinio saugumo subjektai taip pat tinkamai nesilaiko nustatytų techninių reikalavimų. Konkretūs techniniai kibernetinio saugumo reikalavimai dažnai įgyvendinami intuityviai, ne visa apimtimi ir ne visoms RIS (žr. **24 pav.**).

Apibendrintas tikrintų kibernetinio saugumo subjektų techninių reikalavimų įgyvendinimas



< 24 pav. >

Taip pat pažymėtina, kad, reikalavimams įsigaliojus nuo 2016 m., o NKSC nuo 2018 m. pradėjus derinti VII valdytojų parengtus saugos dokumentus, 2020 m. tik kiek daugiau nei pusė visų VII valdytojų (t. y. 165 iš 322) vadovaujasi su NKSC suderintais saugos dokumentais. Tokiam vangiam ir gana ilgam saugos dokumentų derinimo procesui įtakos turi ne tik aplaidus VII valdytojų požiūris į reikalavimų įgyvendinimą, kompetentingų kibernetinio saugumo, informacinių technologijų specialistų ir (ar) reikalingos kompetencijos trūkumas, bet ir pačių informacinių sistemų bei registrų sudėtingumas, kurį, savo ruožtu, lemia nuolatinė IRT plėtra.

RIS spragų atskleidimo praktika yra vienas iš efektyvių būdų sustiprinti šalies kibernetinį saugumą

Inicijuoti Kibernetinio saugumo įstatymo pakeitimai RIS spragų atskleidimo modeliui įteisinti

Etiškų kompiuterių įsilaužėlių veikla ieškant RIS spragų, informacinių sistemų valdytojų ir (ar) tvarkytojų informavimas apie atrastas kibernetinio saugumo problemas yra reikšmingas indėlis į šalies kibernetinį saugumą. Iki šiol Lietuvos Respublikos teisės aktuose nebuvo įteisintas RIS spragų atskleidimo modelis, o kibernetinio saugumo subjektai dažniausiai neturi pasitvirtinę RIS spragų atskleidimo tvarkos, todėl apie aptiktą RIS spragą etiški kompiuterių įsilaužėliai (arba „baltakepuriai“) gali pranešti viešai arba neatskleisti visai. Kai tokie kompiuterių įsilaužėliai, aptikę RIS spragą apie ją praneša viešai, informacinių sistemų valdytojai ir (ar) tvarkytojai netenka galimybės pašalinti spragos iš anksto, o piktavaliai gali šią spragą išnaudoti kibernetinėms atakoms atlikti. Tačiau jeigu informacija apie RIS spragą lieka neatskleista, tikėtina, kad ši spraga liks nepašalinta, o ją anksčiau ar vėliau vis tiek išnaudos piktavaliai. Tad abiem atvejais tikėtina, kad bus padaryta žala organizacijos reputacijai ir piktavaliams bus suteikta galimybė pasinaudoti šia spraga. Taip pat svarbu pažymėti, kad etiški kompiuterių įsilaužėliai, ieškodami RIS spragų, rizikuoja užsitraukti baudžiamąją atsakomybę pagal LR BK 196-198[2] str. Siekdamos aukštesnės kibernetinio saugumo brandos Lietuvoje ir atsižvelgdamos į minėtą problematiką, 2020 m. Krašto apsaugos ministerija kartu su NKSC inicijavo Kibernetinio saugumo įstatymo pakeitimus RIS spragų atskleidimo modeliui įteisinti. Šiais įstatymo pakeitimais siekiama apibrėžti RIS spragos sąvoką ir nustatyti sąlygas, kurių laikantis būtų galima teisėtai ieškoti šių spragų.

NKSC, kaip ir kitos organizacijos, pvz., AB „Ignitis grupė“ ar Vilniaus miesto savivaldybė, RIS spragų atskleidimo praktiką taiko savo iniciatyva jau keletą metų. NKSC savo interneto svetainėje publikavo specialią pranešimų formą[42], skirtą pranešti apie RIS spragas. Visi pranešimai registruojami, informacija įvertinama ir imamasi veiksmų apie RIS spragą informuoti organizaciją ar valstybės instituciją, pažymint, kad apie RIS spragą buvo pranešta vadovaujantis RIS spragų atskleidimo praktika.

Ryškėja tendencija, kad pilietiškų asmenų bei socialiai atsakingų organizacijų daugėja, tad ir informacija apie rastas RIS spragas ar jau pažeistas informacines sistemas NSKC pasiekia vis dažniau. 2020 m. NKSC gavo nemažai pranešimų apie RIS spragas įvairiose interneto svetainėse, o 2020 m. pabaigoje buvo gauta informacija apie spragas VPN įrenginiuose. Keletas atvejų registruota ir dėl viešai prieinamų pramoninių valdymo sistemų įrankių.

Incidentų analizė

RIS spragų atskleidimo tvarkos praktinis taikymas

UAB „Critical Security“ specialistai iš anksto pranešė NKSC apie vieno populiaraus maršrutizatoriaus modelio gamyklinio slaptažodžio pažeidžiamumą. NKSC išanalizavo pateiktą informaciją ir atliko kitų rinkoje naudojamų bevielio tinklo prietaisų gamyklinių nustatymų saugumo vertinimą. Tyrimo metu nustatyta, kad Lietuvoje interneto naudotojų plačiai naudojami tinklo maršrutizatoriai turi pažeidžiamumą, kuriuo pasinaudojus per gana trumpą laiką galima išgauti belaidžio (Wi-Fi) tinklo slaptažodį. Tai leistų įsilaužėliui naudotis naudotojo namų interneto prieiga, šnipinėti duomenų srautą, vykdyti kitas nusikalstamas veikas. Šis pavyzdys parodo, kaip viešojo ir privataus sektorių bendradarbiavimas gali vykti praktikoje. Disponuodamas pranešta informacija, NKSC turėjo laiko atlikti papildomus tyrimus ir informuoti paveiktus subjektus, kurie, savo ruožtu, ėmėsi veiksmų dar iki šios informacijos viešo atskleidimo. Belaidžių tinklų gamyklinių slaptažodžių problemos viešinimas turėtų paskatinti naudotojus labiau pasirūpinti savo saugumu.

42 https://www.nksc.lt/pranesti-spraga.html

2020 m. NKSC vykdė aktualius kibernetinio saugumo srities tyrimus, susijusius su pramonėje ir buityje naudojamų IP kamerų, mobiliųjų programėlių ir telekonferencinių programinių sprendimų saugumu

NKSC vykdyti aktualūs kibernetinio saugumo srities tyrimai

2020 m. NKSC vykdė aktualius kibernetinio saugumo srities tyrimus, susijusius su pramonėje ir buityje naudojamų IP kamerų, mobiliųjų programėlių ir telekonferencinių programinių sprendimų saugumu. Šiuos tyrimus inspiravo visuomenės ir politikos formuotojų nuogąstavimai dėl nepatikimų gamintojų įrangos kibernetinio saugumo problemų, nuotolinio darbo priemonių saugumo ir asmens duomenų praradimo pavojaus naudojant COVID-19 liga sergančiųjų kontrolei skirtą programėlę.

IP kamerų kibernetinio saugumo vertinimas

2020 m. NKSC atliko pramonėje ir buityje naudojamų kamerų tyrimus. Paaiškėjo, kad nors įrenginių funkcijos sudėtingėja, senos saugumo spragos netaisomos. Susirūpinimą kelia ir tai, kad naujuose įrenginiuose naujų spragų, palyginti su ankstesniais gaminiais, gerokai daugėja. Nauji gaminiai, taikomi buityje, naudoja debesų kompiuterijos paslaugas, kai ryšys tarp įrenginio ir naudotojo organizuojamas per trečiųjų šalių serverius, tai kelia[43] duomenų (kameromis atlikti vaizdo įrašai) praradimo grėsmę.

Aplinkos stebėjimo IP kamerų technologinio tyrimo ataskaita pateikta interneto svetainėje
https://www.nksc.lt/doc/biuleteniai/2020-05-27%20Hikvision%20ir%20Dahua%20kameru%20kibernetinio%20saugumo%20vertinimas.pdf

Namų vartojimo vaizdo stebėjimo kamerų kibernetinio saugumo vertinimo ataskaita pateikta interneto svetainėje
https://www.nksc.lt/doc/biuleteniai/2020_10_06_buitiniu-kameru-tyrimas_cen.pdf

Mobiliosios programėlės „KoronaStopLT“ kibernetinio saugumo vertinimas

2020 m. rudenį NKSC atliko Vokietijoje sukurtos ir Lietuvoje kosmetiškai modifikuotos mobiliosios programėlės, skirtos koronavirusinės infekcijos COVID-19 kontaktams sekti panaudojant skaitmeninę kontaktų sekimo technologiją, tyrimą. Siekdamas įsitikinti programėlės ir jos infrastruktūros saugumu, NVSC užsakė Lietuvoje parengtos programėlės „KoronaStopLT“ (toliau – programėlė), veikiančios „iOS“ ir „Android“ platformose, saugumo vertinimą. Tyrimo metu atlikta detali programėlės kodo „iOS“ ir „Android OS“ platformose ir serverio programinių sprendimų analizė, įvertintas skaitmeninės kontaktų sekimo technologijos saugumas, atlikti programėlės kuriamų duomenų srautų stebėjimai, belaidžio ryšio trakto matavimai. Tai leido nustatyti potencialius programėlės ir jos infrastruktūros kibernetinio saugumo neapibrėžtumus, pateikti produkto saugumą didinančias korekcines įžvalgas ir rekomendacijas tolesnei jo plėtrai.

Išsami tyrimo medžiaga pateikta interneto svetainėje
https://www.nksc.lt/doc/biuleteniai/2010-10-27%20KoronaStop-sutrumpinta-3psl.pdf

43
https://ipvm.com/reports/hikvision-lithuania-vuln

Telekonferencinių programinių sprendimų saugumo vertinimas

Verslui ir institucijoms pradėjus vykdyti dalį veiklos nuotoliniu būdu, gerokai išaugo nuotolinės komunikacijos poreikis, todėl NKSC aktyviai stebi ir vertina telekonferencijų platformų kibernetinio saugumo bei asmens duomenų privatumo aspektus.

NKSC 2020 m. atliko devynių rinkoje paplitusių telekonferencinių programinių sprendimų kibernetinio saugumo apžvalgą ir parengė rekomendacijas, kaip saugiau naudotis produktų funkcionalumu. Apžvalgoje nagrinėti devyni telekonferenciniai sprendimai: „Cisco WebEx Meetings“, „Google Meet“, „Microsoft Teams“, „BigBlueButton“, „Zoom“, „Jitsi Meet“, „Skype for Business“, „Slack“ ir „GoToMeeting“.

Detali telekonferencinių programinių sprendimų apžvalga, nurodant palaikomas kibernetinio saugumo funkcijas, pateikta interneto svetainėje
www.nksc.lt/doc/biuleteniai/telekonferenciju-platformu-apzvalga-202011.pdf

Į turinį

Feliksas Dobrovolskis
RRT direktorius

Vadovo žodis

Lietuvos ryšių sektorius – vienas dinamiškiausių mūsų šalies ūkio segmentų. Tai patvirtina tiek metai iš metų augančios šio sektoriaus pajamos, tiek tendencijos rinkose. Nuolat jas stebime, nes, kaip nacionalinis reguliuotojas, siekiame prisidėti prie palankios aplinkos naujovėms ryšių sektoriuje kūrimo, investicijų skatinimo, pažangių, prieinamų ir saugių paslaugų naudotojams užtikrinimo.

Pažangi ir atspari el. ryšių infrastruktūra – itin svarbi šiandienos valstybės atrama, ką puikiai parodė dėl pandemijos paskelbto karantino realijos. Verslui ir valdžios institucijoms, besimokantiems ir dirbantiesiems staiga pradėjus dirbti nuotoliniu būdu, Lietuvos e. ryšių tinklai patyrė beprecedentį išbandymą ir jį atlaikė. Praėjusių metų patirtys parodė, kad Lietuvoje e. ryšių tinklai gerai išplėtoti, o operatoriai deramai užtikrina jų vientisumą, tai, savo ruožtu, sudaro mums visiems galimybes veikti net ypatingomis sąlygomis.

Kitas svarbus aspektas, kurį stebėjome karantino mėnesiais, – pasauliniu mastu internete itin išaugusios draudžiamos informacijos, tokios, kaip vaikų seksualinio išnaudojimo vaizdai, apimtys. Kadangi didelė visuomenės dalis – tiek suaugusieji, tiek vaikai – skaitmeninėje erdvėje praleidžia daug laiko, susidaro ypač palankios sąlygos veikti piktavaliams. Tad sutelktos institucijų pastangos, užtikrinant švaresnę skaitmeninę erdvę, yra svarbios kaip niekada anksčiau.

RRT misija – užtikrinti veiksmingą konkurenciją, investicijas, inovacijas ir patrauklių paslaugų įvairovę elektroninių ryšių, pašto, geležinkelių transporto, patikimumo užtikrinimo paslaugų srityse, taip pat viešojo sektoriaus duomenų teikimo atlyginimų pagrįstumą. RRT, nors tiesiogiai ir neįgyvendina kibernetinio saugumo politikos, tačiau dalimi veiklų prisideda prie to, kad asmenys galėtų sklandžiai naudotis internetu.

KĄ SAUGO?

- Viešųjų elektroninių ryšių paslaugų naudotojų teisę į nepertraukiamą paslaugų teikimą.
- Nepilnamečių ir kitų asmenų teisę į švarią skaitmeninę erdvę.

NUO KO SAUGO?

- Nuo elektroninių ryšių tinklų vientisumo pažeidimų.
- Nuo draudžiamos skleisti ar neigiamą poveikį nepilnamečiams darančios informacijos internete.

KAIP SAUGO?

- Dalyvaudama kaip tarpininkė informacijos apie vientisumo pažeidimus, kurie turėjo didelės įtakos viešųjų ryšių tinklų veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, sklaidai ir užtikrindama, kad viešųjų ryšių tinklų teikėjai įgyvendintų tinkamas technines ir organizacines savo viešųjų ryšių tinklų vientisumo priemones.
- Vykdydama karštosios linijos „Švarus internetas“ veiklą ir kartu su partneriais imdamasi veiksmų, kad patyčios ir kita draudžiama skleisti informacija kuo greičiau būtų pašalinta, o neigiamą poveikį nepilnamečiams daranti informacija būtų atitinkamai pažymėta ir apribota.

RRT

www.rrt.lt / www.esaugumas.lt / www.švarusinternetas.lt rrt@rrt.lt +370 5 210 5633

02 Elektroninių ryšių tinklų vientisumo užtikrinimas ir draudžiamos viešai skleisti informacijos identifikavimas internete

Tiek elektroninių ryšių tinklų vientisumo užtikrinimas, tiek draudžiamos viešai skleisti informacijos identifikavimas internete yra svarbūs veiksniai, kurie siejasi su šalies kibernetinio saugumo aspektais

Šiuolaikinių valstybių gerovė yra glaudžiai susijusi su elektroninių ryšių tinklų egzistavimu, sklandžiu jų veikimu ir tinklais teikiamų paslaugų įvairove. Paskutiniais metais šis sektorius patyrė esminių permainų, susijusių su ryšių technologijų pokyčiais.

Viešųjų elektroninių ryšių paslaugos taip pat vaidina svarbų vaidmenį užtikrinant nacionalinį saugumą, reagavimą į ekstremalias situacijas ir šalies ekonominę plėtrą.

Viešųjų elektroninių ryšių paslaugų nepertraukiamas teikimas gali būti sutrikdytas ne tik dėl kibernetinio incidento, bet ir dėl kitų priežasčių, tokių kaip tinklo įrangos gedimai, elektros energijos tiekimo sutrikimai ir kt. Tokie viešojo ryšių tinklo ar jo dalies pažeidimai, nesusiję su įvykiais ar veika kibernetinėje erdvėje, tačiau sutrikdantys šiuo tinklu teikiamų viešųjų elektroninių ryšių paslaugų nepertraukiamą teikimą yra vadinami vientisumo pažeidimais[44]. Informacija apie tokius viešojo ryšių tinklo ar jo dalies pažeidimus, remiantis Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių, patvirtintų Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus įsakymu Nr. 1V-394 „Dėl Viešųjų ryšių tinklų vientisumo užtikrinimo taisyklių patvirtinimo“, nustatyta tvarka ir kriterijais, yra pateikiama Lietuvos Respublikos ryšių reguliavimo tarnybai (toliau – RRT).

Tiek vaikams, tiek suaugusiems vis daugiau veiklų vykdant kibernetinėje erdvėje, tampa ypač svarbu užtikrinti, kad internete nesklistų draudžiama informacija[45] ir kad būtų stabdomos skaitmeninės patyčios, o neigiamą poveikį nepilnamečiams daranti informacija būtų jiems nepasiekiama. RRT, vykdydama interneto karštosios linijos „Švarus internetas“ veiklą, pagal Lietuvos Respublikos švietimo įstatymo 23^2 straipsnyje aprašytas procedūras priima asmenų pranešimus apie internete rastą draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darančią informaciją bei kartu su partneriais imasi veiksmų, kad ši informacija būtų kuo greičiau pašalinta (jei ji yra draudžiama) arba būtų apribota prieiga prie jos (jei ji daro neigiamą įtaką nepilnamečiams).

Viešųjų ryšių tinklų vientisumo užtikrinimas Lietuvoje

Pagal Lietuvos Respublikos elektroninių ryšių įstatymo (toliau – ERĮ) 42^1 straipsnio 1 dalį, viešųjų ryšių tinklų teikėjai privalo įgyvendinti tinkamas technines ir organizacines priemones savo teikiamų viešųjų ryšių tinklų vientisumui užtikrinti, kad šiais tinklais būtų nepertraukiamai teikiamos viešosios elektroninių ryšių paslaugos. Be to, ERĮ 42^1 straipsnio 4 dalyje yra numatyta, kad įvykus vientisumo pažeidimui, kuris turėjo didelę įtaką viešojo ryšių tinklo veikimui arba viešųjų elektroninių ryšių paslaugų teikimui, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjas (toliau – teikėjas) privalo nedelsdamas apie šį vientisumo pažeidimą informuoti RRT.

2020 m. RRT gavo 10 pranešimų iš keturių teikėjų apie įvykusius viešųjų ryšių tinklų vientisumo pažeidimus. Du viešųjų ryšių tinklų teikėjai RRT pateikė 5 pranešimus apie jų mobiliojo ryšio tinkluose įvykusius pažeidimus, taip pat 5 pranešimai buvo gauti iš kitų dviejų viešųjų ryšių tinklų

44 Lietuvos Respublikos elektroninių ryšių įstatymo 3 straipsnio 71^1 d.

45 Draudžiama skleisti informacija – viešoji informacija, kuri pagal Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymą yra priskirtina draudžiamai skleisti informacijai, tai yra kuria iš vaikų ar kitų asmenų tyčiojamasi arba jie niekinami dėl tautybės, rasės, lyties, kilmės, neįgalumo, seksualinės orientacijos, socialinės padėties, kalbos, tikėjimo, įsitikinimų, pažiūrų ar kitais panašiais pagrindais arba kuri yra pornografinio turinio, skatina vaikų seksualinę prievartą, jų išnaudojimą, pateikia savitikslį smurtą ir (ar) yra kitais įstatymais draudžiama viešoji informacija (Švietimo įstatymo 23^2 straipsnio 2 dalies 1 p.).

Į turinį

teikėjų dėl vientisumo pažeidimų, įvykusių fiksuoto ryšio tinkluose. Pagrindinės viešųjų ryšių tinklų vientisumo pažeidimų priežastys ir palyginimas su ankstesniais metais pateikta lentelėje (žr. **25 pav.**):

	2018 m.		2019 m.		2020 m.	
Viešųjų ryšių tinklų vientisumo pažeidimų priežastys	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius	Pranešimų apie pažeidimus skaičius	Galutinių paslaugų gavėjų, kuriems turėjo įtakos vientisumo pažeidimai, skaičius
Elektros energijos tiekimo sutrikimai	2	151 200	4	50 676	1	1 000
Kabelio nutraukimas, remontas	3	5 195	2	62 270	1	16 419
Tarptinklinio ryšio paslaugų sutrikimai	2	53 000	–	–	–	–
Tinklo įrangos gedimai	2	220 558	8	105 045	8	1 000 000 <*
Iš viso:	9		14		10	

<25 pav.>

* Buvo pranešta apie keletą atvejų, kai judriojo ryšio tinkle paveiktų naudotojų buvo „visi“ arba „40 proc. naudotojų“, be to, ne visos paslaugos buvo nutrauktos, pvz., veikė 4G technologija teikiamos interneto prieigos paslaugos arba tik daliai naudotojų duomenų perdavimo paslaugos sutriko, todėl skaičius preliminarus.

Kaip matyti iš pateiktų duomenų, pandemijos metu itin išaugęs naudojimasis elektroninių ryšių paslaugomis labai nepadidino viešųjų ryšių tinklų vientisumo sutrikimų skaičiaus.

RRT, atsižvelgdama į nustatytą tarpinstitucinį reagavimo į svarbiausių infrastruktūrų sutrikimus modelį[46], apie tris didelio masto vientisumo pažeidimus, kuriuos sukėlė trumpalaikiai tinklo įrangos gedimai, pranešė Lietuvos Respublikos Vyriausybės kanceliarijai, Priešgaisrinės apsaugos ir gelbėjimo departamentui prie Vidaus reikalų ministerijos, Lietuvos Respublikos valstybės saugumo departamentui ir NKSC. Visi šie atvejai buvo fiksuoti pirmojo karantino pradžios metu (atitinkamai 2020 m. kovo 16 d. ir 2020 m. balandžio 25 d.)[47].

Apibendrinant 2020 m. viešųjų ryšių tinklų vientisumo situaciją pagal RRT teiktus pranešimus apie vientisumo pažeidimus, reguliariai teiktą RRT stebėsenos informaciją apie situaciją tinkluose ir įvertinus RRT specialistų nuolat atliekamus viešųjų elektroninių ryšių paslaugų spartos ir kokybės matavimus, matyti, kad Lietuvos viešųjų ryšių tinklų pajėgumai buvo ir yra pakankami (teikėjų buvo nuolat didinami, siekiant patenkinti augantį poreikį), o tinkluose nebuvo fiksuojama daugiau gedimų nei ankstesniais metais, o fiksuoti gedimai pašalinti operatyviai.

46
Keitimosi informacija apie ypatinguosius ir ekstremaliuosius įvykius su Lietuvos Respublikos Vyriausybės kanceliarija, Priešgaisrinės apsaugos ir gelbėjimo departamentu prie Vidaus reikalų ministerijos ir Lietuvos Respublikos Valstybės saugumo departamentu tvarkos aprašas, patvirtintas Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2018 m. gegužės 7 d. įsakymu Nr. 1V-442 „Dėl Keitimosi informacija apie ypatinguosius ir ekstremaliuosius įvykius su Lietuvos Respublikos Vyriausybės kanceliarija, Priešgaisrinės apsaugos ir gelbėjimo departamentu prie Vidaus reikalų ministerijos ir Lietuvos Respublikos Valstybės saugumo departamentu tvarkos aprašo patvirtinimo“.

Švaraus interneto kūrimas, vykdant interneto karštosios linijos „Švarus internetas“ veiklą ir konsultacijų interneto naudotojams teikimas

Lietuvos Respublikos švietimo įstatymo 23[2] straipsnyje reglamentuojama pranešimų apie patyčias ir kitos pagal Nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymą draudžiamos ar neigiamą poveikį nepilnamečiams darančios informacijos teikimo RRT tvarka, nustatyta RRT pareiga imtis veiksmų, kad draudžiama skleisti informacija būtų kuo greičiau pašalinta iš interneto, ir suteikta teisė duoti privalomus nurodymus elektroninės informacijos prieglobos ar viešųjų ryšių tinklų paslaugų teikėjams dėl draudžiamos skleisti informacijos pašalinimo arba prieigos prie jos panaikinimo, taip pat šių paslaugų teikėjų prievolė vykdyti privalomus RRT nurodymus.

RRT nuo 2007 m. yra įsteigusi ir administruoja interneto karštąją liniją „Švarus internetas“, kurios adresas yra **www.švarusinternetas.lt**. Šia karštąja linija visi interneto naudotojai gali pranešti apie rastą internete draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darantį turinį. Kiekvienas gautas pranešimas yra ištiriamas RRT ekspertų, laikantis nustatytų procedūrų, ir pasitvirtinus, jog atitinkamas turinys yra išties draudžiamas pagal Lietuvos teisės aktus ir saugomas Lietuvoje esančiose tarnybinėse stotyse, perduodamas tolesniam tyrimui Policijos departamentui prie Vidaus reikalų ministerijos bei kreipiamasi į informacijos prieglobos paslaugų teikėją, kad šis turinys būtų kuo greičiau pašalintas arba būtų nutraukta prieiga prie jo. Jei Lietuvoje draudžiamas turinys yra skelbiamas užsienio tarnybinėse stotyse ir tas turinys galimai yra draudžiamas ir pagal kitos šalies įstatymus, tada pranešimas persiunčiamas tolesniam tyrimui atitinkamos šalies interneto karštajai linijai, INHOPE narei. Tuo atveju, jei turinys nėra draudžiamas, bet galimai darantis neigiamą poveikį nepilnamečiams, pranešimas yra persiunčiamas Žurnalistų etikos inspektoriaus tarnybai.

RRT administruojama interneto karštoji linija jau nuo 2008 m. yra tarptautinės interneto karštųjų linijų asociacijos INHOPE, šiuo metu vienijančios 47 interneto karštąsias linijas iš 43 šalių, narė.

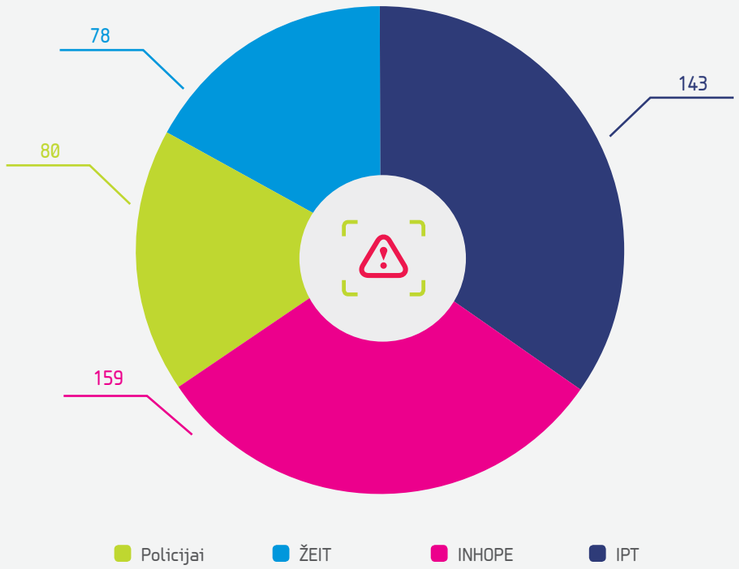
RRT interneto karštoji linija veikia kaip filtras, iš visų gautų pranešimų atrenka pagrįstus atvejus, dėl kurių RRT arba kitos kompetentingos institucijos, pvz. policija, galėtų imtis tolesnių veiksmų. RRT, kaip ir kitų INHOPE asociacijos vienijamų interneto karštųjų linijų, pagrindinis svarbiausias tikslas - kuo greičiau pašalinti draudžiamą skleisti turinį iš interneto. Per 2020 m. RRT interneto karštąja linija gavo 1373 pranešimus (2019 m. buvo gauti 998 pranešimai). RRT specialistai, vertinantys gautus pranešimus, nustatė, kad 460 atvejų (t. y. 33,5 proc. visų gautų pranešimų) nurodytas turinys buvo išties draudžiamas arba darantis neigiamą poveikį nepilnamečiams, todėl buvo galima imtis atitinkamų veiksmų (žr. **26 pav.**):

RRT duomenimis, 2020 m. Lietuvos viešųjų ryšių tinklų pajėgumai buvo pakankami, o pandemijos metu gerokai išaugęs naudojimasis elektroninių ryšių paslaugomis labai nepadidino viešųjų ryšių tinklų vientisumo sutrikimų skaičiaus

47
Nors sutrikimų trukmė neviršijo Ekstremaliųjų įvykių kriterijų sąrašo, patvirtinto Lietuvos Respublikos Vyriausybės 2006 m. kovo 9 d. nutarimu Nr. 241 „Dėl Ekstremaliųjų įvykių kriterijų sąrašo patvirtinimo“, 4.11-4.13 papunkčiuose nustatytų ekstremaliųjų įvykių trukmės, įvertinusi viešųjų elektroninių ryšių tinklų ir paslaugų svarbą, RRT priėmė sprendimą pranešti apie juos anksčiau minėtoms institucijoms.

2020 m., kai daug laiko tiek suaugusieji, tiek vaikai praleido namuose, išaugo vaikų seksualinio išnaudojimo medžiagos apimtys skaitmeninėje erdvėje

Veiksmai, atlikti su pranešimais



- 159 pranešimai (2019 m. – 262 pranešimai) apie vaikų seksualinio išnaudojimo vaizdus persiųsti kitų šalių karštosioms linijoms, tarptautinės interneto karštųjų linijų asociacijos INHOPE narėms.
- 143 pranešimai persiųsti įvairių šalių, taip pat ir Lietuvos, interneto paslaugų teikėjams, svetainių savininkams, socialinių tinklų valdytojams su NTD (angl. *Notice and Take Down*) žyma apie jų svetainėse ar tinkluose esantį neteisėtą interneto turinį, siekiant, kad jis būtų kuo skubiau pašalintas.
- 80 pranešimų persiųsti tolesniam tyrimui Policijos departamentui, nes įtariamas neteisėtas turinys, 78 atvejais tai buvo vaikų seksualinio išnaudojimo vaizdai, saugomi Lietuvos tarnybinėse stotyse (2019 m. Policijos departamentui buvo persiųsti 44 pranešimai).
- 78 pranešimai persiųsti tolesniam tyrimui Žurnalistų etikos inspektoriaus tarnybai, nes įtariama neigiamą poveikį nepilnamečiams daranti informacija.
- 133 pranešimai buvo apie patyčias ir smurtą kibernetinėje erdvėje, 53 atvejais informacija pasitvirtino ir buvo imtasi atitinkamų veiksmų, kad turinys būtų kuo skubiau pašalintas.

< 26 pav. >

Siekdama sukurti tokią elektroninės informacijos prieglobos paslaugų teikėjų ir RRT bendradarbiavimo aplinką, kurioje būtų sklandžiai vykdoma draudžiamos informacijos šalinimo ar galimybės ją pasiekti panaikinimo procedūra, 2020 m. vasario mėn. RRT paskelbė Memorandumą dėl švarios interneto aplinkos (**https://svarusinternetas.lt/memorandumas/10**), prie kurio pakvietė

prisijungti Lietuvos elektroninės informacijos prieglobos paslaugų teikėjus. Iki šios dienos prie Memorandumo jau yra prisijungę 10 paslaugų teikėjų, tuo patvirtinančių savo įsipareigojimą ir siekį prisidėti prie švaresnės ir saugesnės interneto aplinkos kūrimo.

RRT taip pat administruoja interneto svetainę **www.esaugumas.lt**, kurioje visiems interneto naudotojams teikia informaciją, kaip sklandžiai naudotis internetu: socialiniais tinklais, elektronine bankininkyste, elektronine prekyba ir t.t. RRT specialistai papildomai konsultuoja, padeda socialinių tinklų naudotojams dėl neteisėtai paskelbtos asmeninės ar žalingos informacijos pašalinimo, užgrobtų paskyrų susigrąžinimo, tinkamų saugumo ir privatumo parinkčių nustatymo socialiniuose tinkluose[48]. Ir nors gana dažnai socialinių tinklų naudotojai RRT specialistų teiraudavosi, kaip atgauti užblokuotas ar užgrobtas paskyras, atvejų, kad tai būtų susiję su panaudotais kibernetinių atakų įrankiais, nebuvo pastebėta. Karantino metu, kai internete gerokai daugiau laiko praleidžia tiek suaugusieji, tiek vaikai, tokių konsultacijų poreikis irgi išaugo (2019 m. suteiktos 429 konsultacijos, o 2020 m. - 600 konsultacijų, t.y. beveik 40 proc. daugiau).

RRT, administruodama interneto svetainę www.esaugumas.lt 2020 m. interneto naudotojams suteikė 40 proc. daugiau konsultacijų, kaip sklandžiai naudotis internetu

Rekomendacijos:

- Jei internete aptikote galimai draudžiamą skleisti arba neigiamą poveikį nepilnamečiams darantį turinį, būtinai praneškite karštąja linija **www.švarusinternetas.lt**, taip prisidėsite prie švaresnės skaitmeninės erdvės kūrimo tiek suaugusiems, tiek ir vaikams.
- Jeigu norite daugiau sužinoti, kaip saugiai ir atsakingai naudotis IRT technologijomis, apsilankykite svetainėje **www.esaugumas.lt**.

48 Pvz., socialinių tinklų naudotojams buvo aktualūs klausimai dėl jų „Facebook“ paskyrų privatumo ir saugumo nustatymų: kaip nustatyti, kas gali matyti įrašus jūsų laiko juostoje, kas gali jus rasti pagal jūsų nurodytą el. pašto adresą, kas gali skelbti įrašus jūsų laiko juostoje, kaip užblokuoti FB naudotoją, kaip pasirinkti 3-5 „Facebook“ draugus, kurie galėtų padėti susigrąžinti paskyrą, jei ji būtų užgrobta, kaip pasikeisti slaptažodį, kaip aktyvuoti dviejų žingsnių autentifikaciją, kaip įjungti pranešimus apie tai, kad kažkas be jūsų žinios bando prisijungti prie paskyros, kaip peržiūrėti prisijungimų prie paskyros istoriją ir pan.

Į turinį

Renatas Požėla
Policijos generalinis komisaras

Vadovo žodis

Lietuvos Respublikoje, kaip ir kitose ES šalyse vis didėjant elektroninių, arba nusikalstamų, veikų kibernetinėje erdvėje grėsmei, tokio pobūdžio nusikaltimai jau tapo vienu iš policijos veiklos prioritetų. Tokius nusikaltimus darantys asmenys ypač greitai prisitaiko prie besikeičiančių aplinkybių, naudojasi pokyčių neapibrėžtumu, siekdami nusikalstamų tikslų. Lietuvos policija nuolat stebi nusikalstamumo pokyčius kibernetinėje erdvėje, identifikuoja kriminogenines rizikas ir imasi veiksmų joms šalinti.

Reaguodama į kriminogeninę situaciją Lietuvoje ir pasaulyje, Lietuvos policija įgyvendina kibernetinių pajėgumų plėtrą, kuri pagrįsta keturiais ramsčiais:

01. nusikalstamų veikų kibernetinėje erdvėje žvalgybos informacijos gerinimas;
02. tarpinstitucinio bendradarbiavimo ir prevencijos stiprinimas;
03. centrinių ir regioninių policijos pajėgumų plėtojimas;
04. perspėjimų dėl grėsmių kibernetinėje erdvėje visuomenei teikimas.

Lietuvos policijos misija – efektyviai naudojant turimus išteklius ginti Lietuvos žmonių teises ir laisves, saugoti visuomenę ir valstybę, padėti žmogui, šeimai ir bendruomenei. Lietuvos policija pagal Kibernetinio saugumo įstatymą kartu su kitomis institucijomis įgyvendina kibernetinio saugumo politiką.

KĄ SAUGO?

- Lietuvos žmonių teises ir laisves, visuomenę ir valstybę.

NUO KO SAUGO?

- Nuo nusikalstamų veikų ir jų neigiamo poveikio.

KAIP SAUGO?

- Tirdama, atskleisdama ir užkardydama nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui.
- Apribodama viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikimą paslaugų gavėjui ir (arba) nurodydama taikyti priemones, kuriomis šalinamos nusikalstamų veikų kibernetinėje erdvėje priežastys, kai paslaugų gavėjas galimai dalyvauja ar jo naudojama RIS įranga galimai yra naudojama nusikalstamai veikai.
- Inicijuodama kibernetinių incidentų tyrimus ir teikdama nurodymus interneto naudotojams kartu su NKSC.
- Perspėdama visuomenę dėl grėsmių kibernetinėje erdvėje.

LIETUVOS POLICIJA

www.epolicija.lt info@policija.lt 112

03 Nusikalstamų veikų kibernetinėje erdvėje mastas ir poveikis

Nusikalstamos veikos kibernetinėje erdvėje pasaulio ekonomikai 2020 m. kainavo daugiau nei 1 trln. dolerių

Sparčiai modernėjančios IRT, negrynųjų pinigų operacijos, kriptovaliuta ne tik palengvina kasdieninį gyvenimą, bet ir sudaro sąlygas kibernetinėje erdvėje lengviau atlikti net iki šiol „tradiciniais“ laikomus nusikaltimus, tokius kaip sukčiavimas ar turto prievartavimas. Sudėtingėjantys socialinės inžinerijos metodai, vis didėjantys duomenų ir informacijos kiekiai informacinėse sistemose ir serveriuose, taip pat anoniminiame tinkle galimos įsigyti nusikalstamų veikų vykdymo paslaugos (angl. *Cybercrime-as-a-Service* (CaaS)) atveria galimybes nusikaltėliams nusikalstamas veikas vykdyti ne tik atsitiktinai, bet ir tikslingai siekiant pakenkti iš anksto pasirinktai aukai.

Vadovaujantis Lietuvos Respublikos baudžiamojo kodekso (toliau – LR BK) nuostatomis, nusikalstamos veikos elektroninėje erdvėje suprantamos plačiąja[49] ir siaurąja[50] prasmėmis. Šioje ataskaitoje daug dėmesio skiriama abiem nusikaltimų veikų modeliams ir pasirinkta vartoti sąvoka „nusikalstamos veikos kibernetinėje erdvėje“.

2020 m. atlikto McAfee ir Strateginių ir tarptautinių studijų centro (angl. *the Center for Strategic and International Studies* (CSIS)) tyrimo „Paslėpta nusikalstamų veikų kibernetinėje erdvėje kaina“ (angl. *The Hidden Costs of Cybercrime*)[51] duomenys parodė, kad nusikalstamos veikos kibernetinėje erdvėje pasaulio ekonomikai 2020 m. kainavo daugiau nei 1 trln. dol. (į bendrą sumą įtraukiant nuostolius ir kibernetiniam saugumui skiriamas pinigų sumas). Tyrėjai konstatavo, kad tai reikšmingas šuolis nuo 2018 m. vykdyto tyrimo metu nustatytos 600 mlrd. dolerių sumos. Toks spartus nuostolių augimas susijęs su keliomis priežastimis: pirma, dauguma šalių pradėjo rinkti ir gauti išsamesnę informaciją apie tokių nusikalstamų veikų sukeltus nuostolius; antra, nusikaltėliai ėmė taikyti daug efektyvesnes technikas tokių nusikalstamų veikų vykdymui ir, trečia, duomenis šifruojanti ir išpirkos reikalaujanti kenkimo PĮ bei duomenų vagystės yra populiariausi kibernetinių atakų vektoriai. Taigi, atsižvelgiant į nusikalstamų veikų kibernetinėje erdvėje žalos mastą ir spartų augimą, galima teigti, kad šios nusikalstamos veikos yra daug pelningesnis užsiėmimas nei pasaulinis narkotikų verslas. Nusikalstamų veikų kibernetinėje erdvėje vykdymo paslaugos juodojoje rinkoje tapo pelninga veikla ir įgavo pagreitį dėl sparčiai plėtojamų IRT ir jų galimybių išnaudojimo. Savo ruožtu, nusikalstamų veikų kibernetinėje erdvėje rinkos plėtra lemia ir mažėjančius kibernetinių incidentų kaštus. Pavyzdžiui, galima užsisakyti įvykdyti DDoS ir tam nereikia nei specifinių įgūdžių, nei daug pinigų.

Nusikalstamų veikų kibernetinėje erdvėje statistiniai duomenys ir tendencijos

Tradiciškai vis dar manoma, kad valstybių remiami piktavaliai yra daug pajėgesni įvykdyti sudėtingas kibernetines atakas, tačiau pastaruoju metu pasaulyje ryškėja tendencija, jog nusikaltėlių grupuotės taip pat turi pakankamai įgūdžių ir resursų kibernetiniams incidentams, tokiems kaip pažangios ir tęstinės nuolatinės grėsmės (angl. *advanced persistent threats* (APTs)), įvykdyti[52].

Lietuvoje veikiantys asmenys dažnu atveju taip pat veikia ne pavieniui, o gerai organizuotose grupėse, kurių identifikavimas, kaip ir tokio pobūdžio nusikalstamų veikų ištyrimas, yra sudėtingas ir komplikuotas tiek dėl nusikalstamai veikai panaudotų IRT gausos, tiek dėl teisinių sunkumų,

49
Nusikaltimai kibernetinėje erdvėje plačiąja prasme apibrėžiami kaip bet kokie nusikaltimai, kuriems įvykdyti vienaip ar kitaip buvo panaudotos IRT, o nusikaltimo faktui įrodyti turi būti taikomos specifinės nusikaltimų kibernetinėje erdvėje tyrimo priemonės.

50
Nusikaltimai kibernetinėje erdvėje siaurąja prasme – tai nusikaltimai, tiesiogiai darantys įtaką elektroninių duomenų ir informacinių sistemų saugumui, kitaip tariant, pati informacinė sistema yra nusikaltimo tikslas.

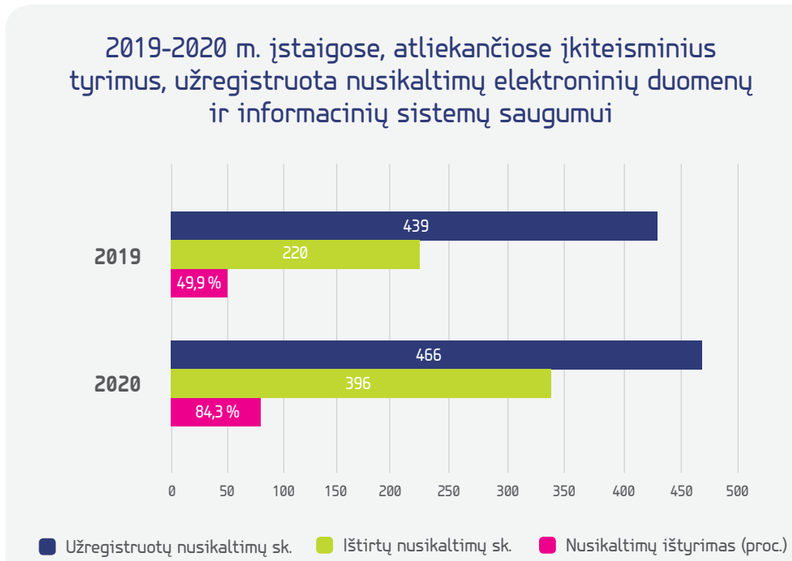
51
https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

52
Nai Fovino I., Barry G., Chaudron S., Coisel I., Dewar M., Junklewitz H., Kambourakis G., Kounelis I., Mortara B., Nordvik J.p., Sanchez I. (Eds.), Baldini G., Barrero J., Coisel I., Draper G., Duch-Brown N., Eulaerts O., Geneiatakis D., Joanny G., Kerckhof S., Lewis A., Martin T., Nativi S., Neisse R., Papameletiou D., Ramos J., Reina V., Ruzzante G., Sportiello L., Steri G., Tirendi S., Cybersecurity, our digital anchor, EUR 30276 EN, Publications Office of the European Union, Luxembourg, 2020, ISBN 978-92-76-19957-1, doi:10.2760/352218, JRC121051.

2020 m. šalyje buvo užregistruoti 466 nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui, tačiau jų ištyrimas, palyginti su 2019 m., padidėjo net trečdaliu

susijusių su tokių veikų padarymo vietos nustatymu ir su ikiteisminiam tyrimui svarbių duomenų (informacijos) gavimu iš trečiųjų šalių. Nuo šių nusikalstamų veikų nukenčia ne tik Lietuvos, bet ir užsienio fiziniai ir juridiniai asmenys.

Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos duomenimis, 2020 m. šalyje buvo užregistruoti 466 nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui (LR BK 196-198[2] str.)[53] (2019 m. - 439). Palyginti su 2019 m., šių nusikaltimų užregistruota 27 atvejais, arba 6,2 proc., daugiau. Bendroje nusikalstamumo struktūroje nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui 2020 m. sudarė 1 proc. 2020 m. šių nusikaltimų ištyrimas sudarė 84,3 proc. Palyginti su 2019 m., ištyrimas yra 34,4 proc. didesnis (žr. **27 pav.**).



< 27 pav. >

Detalesnė informacija apie kiekvieną iš LR BK 196–198[2] str. nusikaltimų elektroninių duomenų ir informacinių sistemų saugumui (žr. 28 pav.):

Pagal LR BK 196 str. „Neteisėtas poveikis elektroniniams duomenims“ 2020 m. buvo užregistruotas 31 nusikaltimas. (2019 m. - 13). 2020 m., palyginti su 2019 m., šių nusikaltimų užregistruota 18 atvejų, arba 138,5 proc., daugiau.

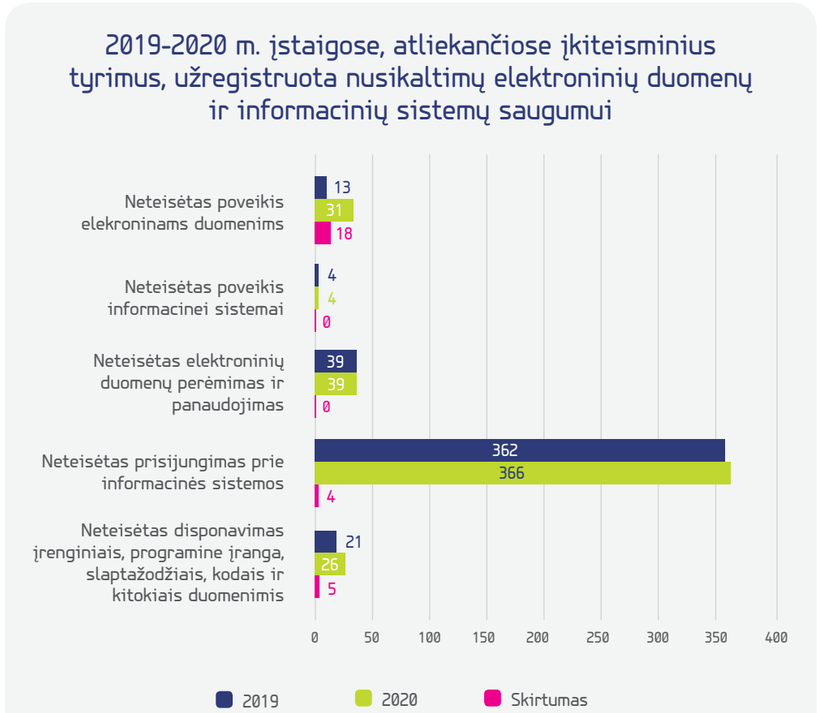
Pagal LR BK 197 str. „Neteisėtas poveikis informacinei sistemai“ 2020 m. užregistruoti 4 nusikaltimai. (2019 m. - 4).

Pagal LR BK 198 str. „Neteisėtas elektroninių duomenų perėmimas ir panaudojimas“ 2020 m. užregistruoti 39 nusikaltimai. (2019 m. - 39).

Pagal LR BK 198[1] str. „Neteisėtas prisijungimas prie informacinės sistemos“ 2020 m. užregistruoti 366 nusikaltimai. (2019 m. - 362). 2020 m., palyginti su 2019 m., šių nusikaltimų užregistruota 4 atvejais, arba 1,1 proc., daugiau.

53
https://www.ird.lt/lt/reports/view_item_datasource?id=8900&datasource=54945

Pagal LR BK 198[2] str. „Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis“ 2020 m. užregistruoti 26 nusikaltimai. (2019 m. - 21). 2020 m., palyginti su 2019 m., šių nusikaltimų užregistruota 5 atvejais, arba 23,8 proc., daugiau.



< 28 pav. >

Lietuvoje vyraujančios nusikalstamos veikos kibernetinėje erdvėje – elektroninis sukčiavimas, neteisėtas prisijungimas prie informacinės sistemos, neteisėtas elektroninių duomenų perėmimas ir panaudojimas

Kaip ir praėjusiais metais, 2020 m. didžiausią nusikalstamų veikų kibernetinėje erdvėje dalį (daugiau nei 90 proc.) Lietuvoje sudarė nusikalstamos veikos kibernetinėje erdvėje plačiąja prasme - tai elektroninis sukčiavimas, neteisėtas prisijungimas prie informacinės sistemos ir neteisėtas elektroninių duomenų perėmimas ir panaudojimas. Šie nusikaltimai įvykdyti dėl asmeninių motyvų.

2020 m. nusikalstamos veikos kibernetinėje erdvėje, susijusios su neteisėtu prisijungimu prie informacinės sistemos ar neteisėtu elektroninių duomenų perėmimu ir panaudojimu, įvykdytos dėl asmeninių motyvų. Jas didžiąja dalimi lėmė konfliktai artimoje aplinkoje (33 proc.), darbo kolektyvuose (22 proc.) ir bendramokslių nesutarimai (11 proc.). Dažniausiai neteisėtą poveikį patyrė socialinių tinklų (50 proc.), elektroninio pašto (30 proc.) paskyrų naudotojai. Šie nusikaltimai buvo įvykdyti naudojant svetimus informacinių sistemų naudotojų tapatybės patvirtinimo duomenis.

2020 m. analizuojant nusikalstamas veikas, suprantamas siauraja prasme, pastebėta, kad šie nusikaltimai buvo susiję su išpirkos reikalaujančios kenkimo PĮ panaudojimu ir neteisėtu prisijungimu prie informacinių sistemų siekiant sutrikdyti jų veiklą. Panaudojant išpirkos reikalaujančią kenkimo PĮ buvo atakuojami serveriai ar naudotojų kompiuteriai, socialinių tinklų paskyros ir interneto svetainės. Didžioji dalis kibernetinių incidentų įvykdyta taikant socialinės inžinerijos metodus, kita dalis buvo kibernetinio pobūdžio atakos. Naudojant išpirkos reikalaujančią kenkimo PĮ, grasinta paskelbti nukentėjusiojo duomenis arba visam laikui blokuoti prieigą prie jų, nebent bus sumokėta

Į turinį

Neskubėkite priimti sprendimų, susijusių su pinigais, ir tvirtinti elektroninių mokėjimų, ypač kai netikėtai kreipęsis asmuo žada įspūdingą investicijų grąžą arba atlygį už skubų pavedimą

išpirka, taip pat vykdyti DDoS. Pusė šių atvejų pasižymėjo išpirkos reikalavimu kripto valiuta, kiti – JAV doleriais ir eurais. Vienas iš dažniausių tokių kibernetinių incidentų vykdymo būdų – masiškai siunčiamos žinutės ar reklamos elektroniniu paštu (angl. *Spam*).

Daugeliu atvejų neteisėti prisijungimai prie informacinių sistemų siekiant sutrikdyti jų veiklą taip pat buvo nukreipti į serverius ar kompiuterius, socialinių tinklų ir informacinių sistemų naudotojus. Pusė šių atvejų buvo susiję su kenkimo PĮ panaudojimu, siekiant užšifruoti elektroninius duomenis arba užvaldyti svetimas socialines paskyras. Dažniausiai jauni asmenys, neteisėtai įgiję kito asmens elektroninės tapatybės duomenis, skleidė melagingas ir (ar) nepadoraus turinio žinutes.

Lietuvos kriminalinės policijos biuras pažymi, kad 91 proc. elektroninio sukčiavimo atvejų sudarė neteisėti lėšų įgijimai iš sąskaitų[54], 5 proc. – finansinio mokėjimo pervedimai į įtariamųjų sąskaitas[55].

Neteisėtam lėšų įgijimui iš sąskaitų dažniausiai buvo taikomi socialinės inžinerijos metodai (75 proc.)[56]. Taikant socialinės inžinerijos metodus, buvo naudojami tiek elektroninės bankininkystės informacinių sistemų naudotojų tapatybės duomenys, tiek techninė ar PĮ. Techninės ar PĮ panaudojimo atvejais (79 proc.) bandyta įgyti asmeninę, finansinę ar saugumo informaciją tekstinėmis žinutėmis (SMS)[57] su nuorodomis į suklastotas bankų interneto svetaines. Pagrindiniai atakų objektai buvo elektroninės bankininkystės informacinių sistemų naudotojų (tiek fizinių, tiek juridinių asmenų) paskyros.

Visais finansinio mokėjimo pervedimo į įtariamųjų sąskaitas atvejais buvo taikomi socialinės inžinerijos metodai ir rengiamos sukčiavimo, naudojant netikrą elektroninį paštą, atakos[58]. Joms parengti dažniausiai buvo naudojama nuotolinės prieigos kenkimo PĮ, skirta neteisėtai prieigoms prie informacinių sistemų (angl. *Remote access trojan* (RAT)) gauti. Pagrindiniai kibernetinių atakų objektai buvo juridinių asmenų elektroninio pašto paskyros.

Su užsienio valstybėmis[59] siejamos nusikalstamos veikos dažniausiai buvo daromos iš Rumunijos, Latvijos, JAV, Jungtinės Karalystės, Rusijos.

Išviliotų pinigų suma svyruoja nuo kelių dešimčių eurų iki kelių dešimčių tūkstančių eurų. 2020 m. didžiausia pagal pirminę informaciją dėl sukčiavimo patirta žala viršija 2 600 000 JAV dolerių (2 450 000 eurų).

Lietuvos policijos informaciją apie elektroninį sukčiavimą papildo ir LBA 2020 m. surinkti duomenys apie finansinį sukčiavimą ir jo padarytą žalą[60]. 2020 m. LBA ir jos nariai ne tik ėmėsi iniciatyvos kas ketvirtį fiksuoti incidentų kibernetinėje erdvėje skaičių ir daromą žalą, bet ir pradėjo bendradarbiauti su Lietuvos kriminalinės policijos biuru[61]. LBA duomenimis, 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. Eur. Daugiausia nuostolių padaryta perimant susirašinėjimą elektroniniu paštu ir įtraukiant žmones į investicinio sukčiavimo pinkles. Per praėjusius metus LBA nariai užfiksavo 1336 elektroninių sukčiavimo atvejus. Bendra tendencija – asmeniniu nusikaltėlių kontaktu su auka bei įtaiga paremtų incidentų dalis šiek tiek mažėja, o įmantresnių schemų, kurių taikinyje atsiduria ne vien asmenys, bet ir įmonės bei organizacijos, – daugėja. Daugiausia žalos 2020 m. Lietuvos gyventojai patyrė dėl vadinamojo investicinio sukčiavimo, kai nusikaltėliai manipuliacijomis priverčia neva investuoti į rizikingus instrumentus, o iš tiesų išvilioja pinigus. Šitaip netekta 1,7 mln. eurų. Tokie incidentai pernai, palyginti su kitais sukčių scenarijais, buvo ir gausiausi – užfiksuoti net 295 atvejai. „Investicijų brokeriai" dažnai skambina iš užsienietiškų numerių, naudoja populiarias pokalbių programėles, pvz., „Viber" ar „WhatsApp". Itin daug nuostolių ne tik gyventojams, bet ir įmonėms pridaro susirašinėjimo el. paštu perėmimas, klastojant sąskaitų faktūrų duomenis. Per visus praėjusius metus užfiksuotas 51 toks atvejis, padaryta žala siekė daugiau kaip 1 mln. eurų. Pranešta ir apie 9 atvejus, kai sukčiai, apsimetę įmonės vadovais, privertė darbuotojus atlikti pavedimus, šitaip netekta 138 tūkst. eurų.

54
Pavyzdžiui, telefoninio sukčiavimo būdu sužinomi naudotojų elektroninės bankininkystės ir prisijungimo prie sąskaitų duomenys, kuriais pasinaudodami sukčiautojai vėliau inicijuoja finansines operacijas, skirtas lėšoms iš nukentėjusiųjų sąskaitų į savo pervesti.

55
Kitaip tariant, buvo veikiama pagal vadinamąją „buhalterio apgavystės" schemą, pavyzdžiui, sukčiautojai perima komercinio sandorio šalių susirašinėjimą ir nurodo apmokėjimą už prekes ar paslaugas atlikti į pakeistą sąskaitą.

56
Kiti atvejai, kuriuos Lietuvos kriminalinės policijos biuras vertina ne kaip socialinės inžinerijos metodus, buvo „Smart-ID" programėlės aktyvavimas nuotoliniu būdu naudotojų įrenginiuose, kai buvo prašoma įvesti naudotojo duomenis ir (ar) patvirtinti inicijuotas finansines operacijas. Taip pat policijoje buvo registruojami nukentėjusiųjų pareiškimai, kad buvo nuskaitytos lėšos jų sąskaitose už prekes ar paslaugas, kurių nepirko. Šiais atvejais nukentėjusieji teigė, kad saugiai naudojosi e. bankininkyste, prisijungimo duomenų nebuvo perleidę ir pametę ir nebuvo susidūrę su sukčiautojų kėsinimusi išgauti duomenis. Dalis tokių atvejų rodo, kad egzistuoja prekyba vogtais informacinių sistemų naudotojų duomenimis.

57
Angl. „smishing" – apgaulinga tekstinių pranešimų siuntimo tvarka, tariamai gaunama iš patikimų kompanijų, siekiant paskatinti asmenis atskleisti asmeninę informaciją, pvz., slaptažodžius ar kreditinių kortelių numerius).

LBA duomenimis, suklastojus tekstines žinutes (SMS) (angl. *smishing*) arba el. laišką ir mėginant išgauti asmeninius prisijungimo duomenis išviliota 168 tūkst. eurų – per metus pranešta apie 143 tokius incidentus.

LBA duomenimis, 2020 m. elektroninių sukčių Lietuvoje gyventojams padaryta žala perkopė 4,5 mln. eurų

Lietuvos policijos prevencinė veikla

Lietuvos policija per pastaruosius 5 metus įgyvendino 1,5 tūkst. įvairių prevencinių priemonių. Šių priemonių taikymo mastas nuo 2015 m. išaugo 80 proc.

Prevencinės priemonės orientuotos į Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3) rengiamose Organizuoto nusikalstamumo internete grėsmių (angl. *Internet Organised Crime Threat Assessment* (IOCTA))[62] ir teritorinio bei nacionalinio sunkaus ir organizuoto nusikalstamumo grėsmių vertinimo ataskaitose nurodytas pagrindines nusikalstamų veikų kibernetinėje erdvėje grėsmes – elektroniniai sukčiavimai, nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui, vaikų išnaudojimas pornografijai.

Viena iš dažniausiai taikomų prevencinės veiklos priemonių – visuomenės švietimas. Patarimus, kaip apsisaugoti nuo sukčių galima rasti Lietuvos policijos interneto svetainėje **https://policija.lrv.lt/lt/policija-pataria**.

Taip pat Lietuvos kriminalinės policijos biuro interneto svetainėje **http://lkpb.policija.lrv.lt/lt/naujienos/patarimai-kaip-atpazinti-sukcius-ir-ka-daryti** kviečiame susipažinti su vykdoma sukčiavimų kibernetinėje erdvėje kampanija **#CyberScams**. Ji skirta supažindinti visuomenei su labiausiai paplitusiais sukčiavimo kibernetinėje erdvėje būdais ir išmokyti apsaugoti save ir savo turtą (pateikiama pavyzdžių, kai darbuotojas apgaulės būtu priverčiamas apmokėti netikrą sąskaitą faktūrą arba atlikti pavedimą, kai gaunamas apgaulingas el. laiškas iš banko, kai gaunamos apgaulingos trumposios SMS žinutės bandant išgauti asmeninę, finansinę ar saugos informaciją; taip pat pateikiama informacija, kaip atrodo netikros bankų interneto svetainės ir pan.).

58
Angl. „phishing" – apgaulinga elektroninio pašto siuntimo tvarka, tariamai gaunama iš patikimų kompanijų, siekiant paskatinti asmenis atskleisti asmeninę informaciją, pvz., naudotojų vardus, slaptažodžius ar kreditinių kortelių numerius).

59
Valstybės, kuriose buvo registruoti IP adresai, telekomunikacinio ryšio operatoriai, atidarytos bankų sąskaitos neteisėtoms lėšoms pervesti.

60
Atkreipiame dėmesį, kad LBA užfiksuotų elektroninių sukčiavimų atvejų ir policijos įstaigose pradėtų ikiteisminių tyrimų dėl sukčiavimo kibernetinėje erdvėje skaičius yra ne toks pats.

61
Bankui pastebėjus, kad klientas galimai atlieka pavedimus sukčiams, į perspėjimo mechanizmą yra įtraukiama ir policija. Šis specialus reagavimo į galimus sukčiavimo atvejus algoritmas garantuos operatyvų atsaką galimos finansinės aferos atveju ir padės apsaugoti žmones nuo apgavysčių.

62
Europolo Europos kovos su elektroniniu nusikalstamumu centro (EC3) kasmet leidžiamose organizuoto nusikalstamumo internete grėsmių vertinimo ataskaitose galima sužinoti apie dinamiškas ir besivystančias nusikaltimų kibernetinėje erdvėje tendencijas Europoje.

Į turinį

LBA duomenimis, romantinių sukčiavimų 2020 m. užfiksuota 82, padaryti nuostoliai siekia 451 tūkst. eurų

Lietuvos policijos patarimai

- Peržiūrėkite privatumo sąlygas ir nustatymus savo socialinių tinklų paskyrose; instaliuokite įrenginiuose antivirusinę programą; apsaugokite savo įrenginius slaptažodžiais ir biometriniais duomenimis.
- Nesiųskite avanso asmenims, kurių nepažįstate, pirkite tik iš patikimų interneto parduotuvių, atkreipkite dėmesį į pirkėjų įvertinimus.
- Niekada elektroniniu paštu, socialiniuose tinkluose, SMS žinutėmis ar skambučiais neatskleiskite savo asmeninės ar finansinės informacijos. Valstybinės institucijos, bankai, sveikatos priežiūros įstaigos niekada nesikreips su prašymu elektroniniu paštu ar telefonu atskleisti asmeninę informaciją (pvz., asmens kodą, kreditinės ar debetinės kortelės numerį, banko autentifikavimo kodą ir kt.).
- Kritiškai vertinkite elektroniniu formatu (elektroniniame pašte, socialiniuose tinkluose, SMS žinutėse) gaunamas nuorodas! Nesidalykite įtartinomis socialiniuose tinkluose platinamomis žinutėmis, o dar geriau – jų apskritai neplatinkite! Būtinai įvertinkite tokių gaunamų laiškų autentiškumą ir turinį, atkreipdami dėmesį į pateiktas nuorodas ir pridedamus priedus. Įsitikinti siunčiamos nuorodos autentiškumu galite užvedę pelytę ant adreso (nespaudžiant) – nuorodoje neturėtų atsirasti kitos interneto svetainės adresas.
- Jokiu būdu neatidarykite įtartinų laiškų, juose esančių nuorodų ar pridedamų failų! Gavę tokių laiškų, iškart juos ištrinkite. Jeigu paspaudėte ant įtartinos nuorodos, būtinai pasikeiskite elektroninio pašto slaptažodį!
- Prieš įvedant į tinklalapio formą prisijungimo duomenis svarbu atkreipti dėmesį, kad atidarytas tinklalapis yra apsaugotas SSL / TLS sertifikatu ir tinklalapio domenas atitinka tinklalapio dizainą (jeigu tai yra žinomas jums tinklalapis).

Incidentų analizė

Sudėtingas ir didelės apimties ikiteisminis tyrimas, turėjęs įtakos ne tik nacionalinei, bet ir tarptautinei nusikaltimų kibernetinėje erdvėje situacijai

Lietuvos kriminalinės policijos biuro ir Lietuvos Respublikos generalinės prokuratūros bendromis pastangomis buvo išaiškinta tarptautinė nusikalstama grupuotė ir jos nariai, kurių aukomis tapo ne mažiau kaip 84 fiziniai asmenys ir 21 juridinis asmuo. Neteisėtai užvaldžius nukentėjusių asmenų banko sąskaitas pasisavinta apie 250 000 eurų, tačiau pareigūnų, bankų ir finansinių paslaugų įmonių pastangomis dalį neteisėtų bankinių pavedimų pavyko sustabdyti ir nukentėjusiesiems grąžinta apie 150 000 eurų neteisėtai užvaldytų pajamų.

Šis ikiteisminis tyrimas buvo vykdomas 2019–2020 m. SEB ir „Swedbank“ bankų klientai kreipėsi į policiją, nes pradėjo gauti klaidinančius elektroninius pranešimus su melagingais siūlymais atnaujinti savo paskyras bei interneto nuorodomis, nukreipiančiomis į netikras minėtų bankų interneto svetaines. Nukentėjęs asmenys netikrose bankų interneto svetainėse, naudodamiesi programėle „Smart-ID“ ir suvedę prisijungimo kodus, perdavė organizuotos grupės nariams savo arba atstovaujamų juridinių asmenų elektroninės bankininkystės duomenis, kuriuos vėliau kaltininkai panaudojo neteisėtai prisijungdami prie nukentėjusių asmenų paskyrų tikrose SEB ir „Swedbank“ bankų interneto svetainėse. Nusikalstamu būdu užvaldyti pinigai buvo pervedami į Lietuvos, Lenkijos, Airijos, Anglijos, Liuksemburgo, Olandijos, Ispanijos, Maltos, Prancūzijos bankus ar įmones, teikiančias elektroninių pinigų paslaugas. Atlikus aktyvius ikiteisminio tyrimo veiksmus, pavyko išsiaiškinti, kad nusikaltimai buvo vykdomi Rumunijos Respublikos piliečių.

Tiriant šias nusikalstamas veikas nustatyta, kad identiški sukčiavimo atvejai plinta ir Estijoje, o juos vykdo ta pati nusikalstama organizuota grupuotė. Siekiant užkardyti daromus nusikaltimus ir sulaikyti įtariamuosius, Lietuvos Respublikos generalinės prokuratūros ir Lietuvos kriminalinės policijos biuro iniciatyva 2020 m. kovo mėn. Europos teisminio bendradarbiavimo padalinyje (Eurojustas) buvo sudaryta Lietuvos, Estijos ir Rumunijos jungtinė tyrimo grupė.

Glaudus tarpinstitucinis bendradarbiavimas leido efektyviai surinkti būtinus duomenis apie įtariamus Rumunijos piliečius. 2020 m. rugsėjo mėn. pabaigoje visi įtariamieji buvo sulaikyti Rumunijoje. Prie Rumunijos teisėsaugos institucijoms ruošiamo perduoti ikiteisminio tyrimo dėl keturių šalies piliečių baudžiamojo persekiojimo pridėti dar 48 Lietuvoje pradėti ikiteisminiai tyrimai, o nusikalstamas veikas padariusiems asmenims inkriminuojamos net 249 nusikalstamos veikos.

Policija gruodžio 9 d. pradėjo ikiteisminį tyrimą dėl neteisėto poveikio elektroniniams duomenims, neteisėto prisijungimo prie informacinės sistemos ir neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis

Policija, gavusi 2020 m. gruodžio 9 d. iš NKSC ataskaitą apie kibernetinį incidentą, galimai turintį nusikalstamos veikos požymių, pradėjo ikiteisminį tyrimą dėl neteisėto poveikio elektroniniams duomenims, neteisėto prisijungimo prie informacinės sistemos ir neteisėto disponavimo įrenginiais, programine įranga, slaptažodžiais, kodais ir kitokiais duomenimis. Nustatyta, kad šie neteisėti veiksmai buvo vykdomi 2020 m. gruodžio 9 d. 17.00–21.00 val., pasinaudojus vieno iš Lietuvos interneto svetainių kūrėjo saugumo spraga slaptažodžių valdymo procesuose.

Įvertinus tyrimo metu surinktą medžiagą, galima teigti, kad kibernetinė ataka buvo vykdoma tikslingai, jos įvykdymui buvo pasiruošta iš anksto.

Raimondas Andrijauskas
VDAI direktorius

Vadovo žodis

Valstybinė duomenų apsaugos inspekcija didžiuojasi Lietuvos politika kibernetinio saugumo srityje. Mes, asmens duomenų apsaugos priežiūros institucija, taip pat įgyvendiname kibernetinio saugumo politiką: tik pradėjus kurti Kibernetinio saugumo įstatymą, prisidėjome prie kibernetinio saugumo sistemos kūrimo Lietuvoje ir, dalyvaudami Kibernetinio saugumo tarybos veikloje, toliau prisidedame prie jos tobulinimo.

Valstybinės duomenų apsaugos inspekcijos veikla yra tiesiogiai susijusi su kibernetiniu saugumu. Vykdydami Bendrajame duomenų apsaugos reglamente ir Kibernetinio saugumo įstatyme nustatytas užduotis, bendradarbiaujame su Nacionaliniu kibernetinio saugumo centru. Tirdami kibernetinius incidentus, susijusius su asmens duomenų ir privatumo apsaugos pažeidimais, sutelkiame išteklius ir keičiamės informacija.

Siekiant užtikrinti skaitmeninės visuomenės gerovę, kibernetiniu saugumu turėtų būti rūpinamasi ne tik Lietuvoje, bet ir kitose šalyse. Europos Sąjungos asmens duomenų apsaugos priežiūros institucijas vienijanti Europos duomenų apsaugos valdyba, siekdama, kad būtų užkirstas kelias galimai žalai ir kad būtų kuo geriau apsaugoti asmenys ir jų duomenys, 2021-2023 m. strategijoje skatina asmens duomenų apsaugos priežiūros institucijų bendradarbiavimą su kitomis organizacijomis.

VDAI yra asmens duomenų apsaugos priežiūros institucija, kurios misija – ginti žmogaus teisę į asmens duomenų apsaugą. VDAI pagal Kibernetinio saugumo įstatymą kartu su kitomis institucijomis įgyvendina kibernetinio saugumo politiką.

KĄ SAUGO?

- Asmenų teisę į asmens duomenų apsaugą.

NUO KO SAUGO?

- Nuo asmens duomenų tvarkymo neužtikrinant teisės aktų reikalavimų arba neteisėto asmens duomenų tvarkymo ir nuo netyčinio duomenų praradimo, sunaikinimo ar sugadinimo.

KAIP SAUGO?

- Atlikdama organizacijų asmens duomenų tvarkymo ar duomenų saugumo patikrinimus.
- Nagrinėdama pranešimus, susijusius su asmens duomenų saugumo pažeidimais, ir atlikdama tyrimus.
- Teikdama organizacijoms išankstines konsultacijas, susijusias su naujų technologinių sprendimų vertinimu dėl organizacinių ir techninių priemonių tinkamumo ir duomenų tvarkymo saugumo.
- Atlikdama asmens duomenų tvarkymo auditus valstybės informacinėse sistemose.

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

vdai.lrv.lt | ada@ada.lt | +370 5 271 2804 | mobilioji programėlė „ADA gidas“

04 Asmens duomenų saugumo pažeidimų įtaka kibernetinio saugumo būklei

BDAR numatyta, kad pavojų atitinkančio lygio saugumo užtikrinimas – viena iš esminių asmens duomenų tvarkymo sąlygų

Su ADSP vis dažniau susiduria viešojo ir privataus sektorių atstovai, nes visuomenės ir valstybės gyvenimas tampa vis labiau priklausomas nuo elektroninių duomenų ir jų sąsajų, debesų kompiuterijos ir darbo jėgos mobilumo.

IRT, kurios tapo neatsiejama šiuolaikinio gyvenimo dalimi, pakeitė ir tradicinį visuomenės supratimą apie tai, kokios priemonės reikalingos norint pasitikėti valstybės ir savivaldybių institucijomis, įstaigomis ir socialine aplinka, kurioje gyvename. Spartėjant skaitmenizacijos procesams, didėja ir tvarkomų asmens duomenų kiekiai. Dauguma duomenų nėra struktūrizuoti ir valdyti prieigą prie jų bei juos apsaugoti tampa vis sudėtingiau.

Tokius duomenis ypač sudėtinga apsaugoti dėl:

- didelio jų kiekio ir nenuspėjamų tarpusavio sąsajų;
- nuolat tobulinamų socialinės inžinerijos metodų;
- vis išradingesnių asmens duomenų panaudojimo, siekiant gauti finansinės ir kitos naudos, būdų.

Siekiant stiprinti visuomenės pasitikėjimą informacinės visuomenės paslaugomis, elektronine komercija, daiktų internetu (angl. *internet of things*) ir skatinti naudotis išmaniaisiais prietaisais (pvz., išmanieji telefonai, laikrodžiai, automobiliai, šaldytuvai ir pan.), valstybės raginamos imtis priemonių kibernetinio ir asmens duomenų saugumo srityje.

Lietuvoje, kaip ir kitose ES šalyse, nuo 2018 m. asmens duomenų apsauga užtikrinama vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau - BDAR). BDAR numatyta, kad kibernetinio saugumo užtikrinimas yra esminė asmens duomenų tvarkymo sąlyga[63], nes praktika rodo, jog kibernetiniai incidentai, įvykstantys dėl netinkamų ar netinkamai taikomų techninių ar organizacinių priemonių, pažeidžia šimtų milijonų asmenų teises, daro didelę įtaką su tuo susijusių organizacijų reputacijai bei lemia finansinius nuostolius. Netinkamas asmens duomenų tvarkymas, asmens duomenų apsaugos principų ignoravimas sudaro sąlygas piktavaliams išnaudoti šias spragas finansinei naudai gauti, pvz., ADSP metu atsiradusios saugumo spragos - tinkama terpė piktavaliams perimti asmens duomenis ir juos panaudoti kibernetinėms atakoms ir nusikaltimams vykdyti. Taigi ne veltui pastaraisiais metais asmens duomenys įvardijami kaip XXI a. valiuta.

2020 m. Lietuvoje reikšmingiausi pagal paveiktų asmenų skaičių ir poveikį ADSP buvo susiję su informacinės visuomenės paslaugų ir duomenų pasiekiamumo prieinamumo trikdžiais bei vientisumo pažeidimais (pvz., 2020 m. liepos mėn. įvykęs VĮ Registrų centro valdomų IS ir registrų veiklos sutrikimas) ir su atvejais, kai taikant socialinės inžinerijos metodus ir pasinaudojant organizacijų lengvabūdišku požiūriu į bazinius kibernetinio saugumo principus buvo užvaldomos naudotojų paskyros siekiant finansinės naudos (pvz., 2020 m. kovą UAB „Vinted“ el. prekybos platformoje buvo prisijungta prie naudotojų paskyrų be jų žinios), taip pat su tolesniu kenkimo PĮ platinimu.

63 BDAR 5 str. 1 d. f p. numato, kad asmens duomenys turi būti „tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo (vientisumo ir konfidencialumo principas)“. Be to, BDAR 32 str. įpareigoja tiek duomenų valdytoją, tiek tvarkytoją įgyvendinti tinkamas technines ir organizacines priemones, kad būtų užtikrintas asmens duomenų saugumas, vadovaujantis rizika pagrįstu metodu.

Į turinį

Per 2020 m. VDAI gavo 181 pranešimą apie ADSP

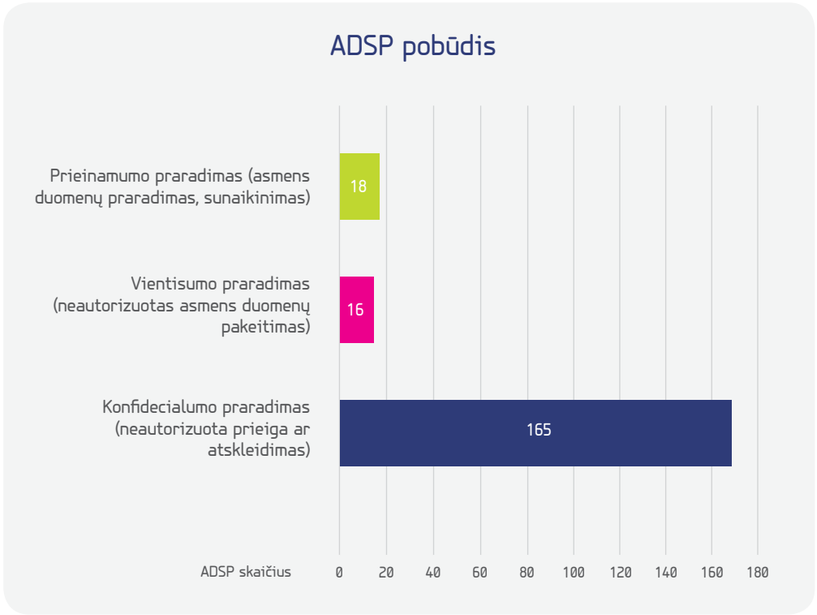
Asmens duomenų saugumo pažeidimai Lietuvoje

Per 2020 m. VDAI gavo 181 pranešimą apie ADSP. Palyginti su 2019 m., tokių pranešimų padaugėjo nežymiai (3,5 proc.).

Statistiškai tai gana nedidelė imtis, todėl neįmanoma daryti vienareikšmiškų išvadų ar matyti aiškių tendencijų. Beje, palyginti su kibernetinių incidentų skaičiumi Lietuvoje, tikėtina, kad apie nemažą dalį ADSP VDAI vis dar nėra informuojama, nes gana dažnai ADSP būna susiję su įvykusiais kibernetiniais incidentais. Pasitaiko, kad duomenų valdytojai, susidūrę su kibernetiniu incidentu, tiesiog nežino arba pamiršta, kad kiekvienu atveju reikėtų įvertinti, ar jis nėra susijęs su asmens duomenimis, ar neturi ADSP požymių.

Dažniausiai ADSP 2020 m., kaip ir 2019 m., vyko duomenų valdytojų ir (ar) tvarkytojų ir viešųjų el. ryšių tinklų bei viešųjų elektroninių ryšių paslaugų teikėjų interneto svetainėse ar informacinėse sistemose. VDAI negali patvirtinti, kad Lietuvoje, kaip ir kitose valstybėse, ryškėja tendencija, jog vis daugiau ADSP įvyksta naudojantis debesų kompiuterijos paslaugomis (dėl vis didėjančio duomenų kiekio „debesyse“), kita vertus, neatmestina tikimybė, kad apie tokius ADSP VDAI nėra informuojama, nes jų neaptinkama arba įvyksta tarptautinėse įmonėse, kurios pasirinkusios kitą pranešimo apie ADSP pateikimo jurisdikciją.

Pagal ADSP pobūdį (gali būti daugiau nei vienas požymis) Lietuvoje statistiškai neabejotinai vyrauja konfidencialumo pažeidimai – net 165 ADSP atvejais buvo prarastas asmens duomenų konfidencialumas. 18 ADSP atvejų buvo susiję su duomenų pasiekiamumo / prieinamumo pažeidimais, 16 ADSP atvejų buvo prarastas duomenų vientisumas (žr. **29 pav.**).

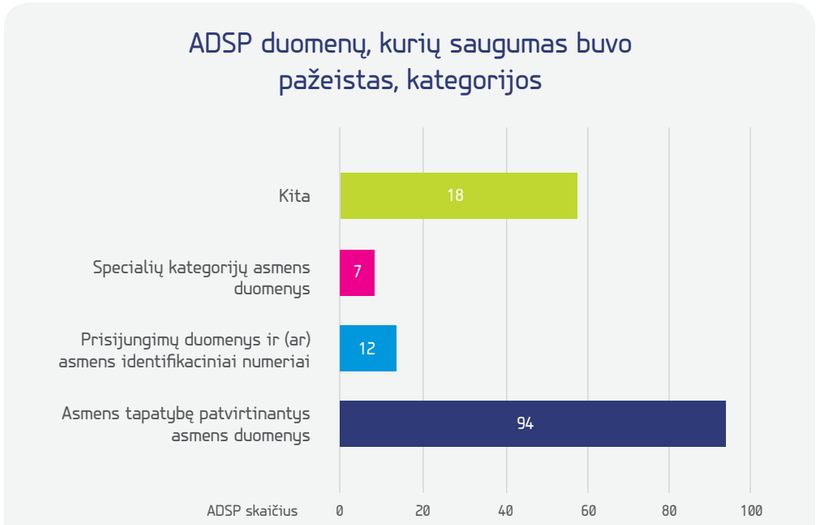


< 29 pav. >

Pagal sukeltus padarinius ir potencialią žalą asmenims keli prieinamumo pažeidimai 2020 m. buvo itin dideli, jų padarinius jautė didelė Lietuvos gyventojų dalis (pvz., 2020 m. liepos mėn. įvykęs VĮ Registrų centro valdomų IS ir registrų veiklos sutrikimas, „Smart-ID“ tapatybės patvirtinimo paslaugos sutrikimai).

Apžvelgiant asmens duomenų, kurių saugumas buvo pažeistas, kategorijas, vyrauja „Asmens tapatybę patvirtinantys asmens duomenys“[64] – iš viso nustatyti 94 tokie atvejai, „Prisijungimo duomenys ir (ar) asmens identifikaciniai numeriai“[65] – 12 atvejų. Šių kategorijų asmens duomenys dažniausiai buvo panaudojami neteisėtai prieigai prie informacinių sistemų, interneto svetainių ir tolesnei neteisėtai veiklai, pvz., kenkimo PĮ platinimui, sukčiavimui, susijusiam su el. prekyba ar pinigų pervedimu ir pan. „Specialių kategorijų asmens duomenys“[66] – 7 atvejai, 57 kartus pažeistų duomenų kategorija buvo nurodyta kaip „Kita“[67] (žr. **30 pav.**)

Dažniausia ADSP priežastis – žmogiškoji klaida



< 30 pav. >

Skirstant ADSP pagal duomenų valdytojų veiklos rūšis, dažniausiai apie ADSP pranešė organizacijos, kurių pagrindinė veikla susijusi su „Finansų ir kreditų veikla“ (37 pranešimas), „Valstybės ir savivaldybių institucijų veikla“ (27 pranešimai) ir „Teisėsauga ir teisėtvarka“ (16 pranešimų), „Sveikatos paslaugos“ (13 pranešimų), „Elektroninių ryšių ar tinklų teikimas“ (8 pranešimai) ir „Elektroninės parduotuvės“ (9 pranešimai) (žr. **31 pav.**).

64 Vardas, pavardė, amžius, gimimo data, lytis, el. paštas ir kt.

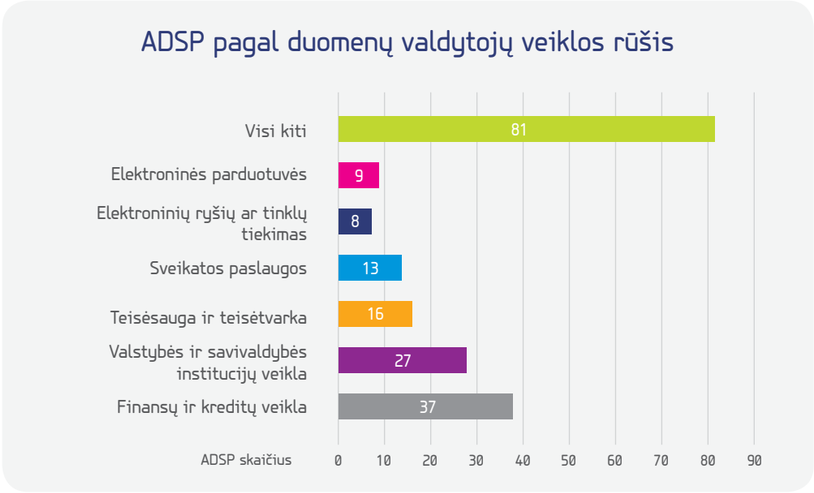
65 Asmens kodas, mokėtojo kodas, slaptažodžiai.

66 Duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys, duomenys apie lytinį gyvenimą ir lytinę orientaciją.

67 Tai reiškia, kad tais atvejais arba nukentėjo labiau specifiniai duomenys (pvz., finansiniai duomenys, kredito istorijų duomenys) arba tai buvo keleto asmens duomenų kategorijų derinys, kai nebuvo galima aiškiai išskirti vienos vyraujančios kategorijos.

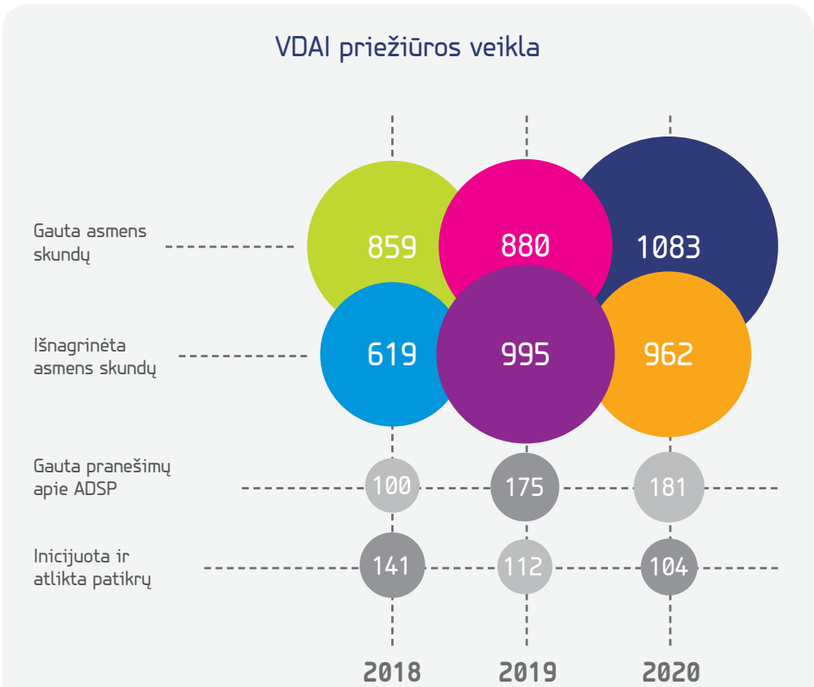
Į turinį

Finansų sektorius operatyviai praneša apie ADSP dėl gana griežtų sektorinių reikalavimų



< 31 pav. >

Šie duomenys, viena vertus, gali reikšti, kad ADSP daugiausia patiria finansų, valstybės institucijų, teisėsaugos sektoriai, tačiau tai gali lemti tokios aplinkybės, kaip griežtesni teisės aktų reikalavimai ir (ar) jų laikymasis, pavyzdžiui, finansų sektorius operatyviai praneša apie ADSP dėl gana griežtų sektorinių reikalavimų, kurių privalo laikytis, o valstybės ir savivaldybių ar teisėsaugos institucijos yra įpratusios griežčiau laikytis reglamentuotų reikalavimų.



< 32 pav. >

ADSP prevencija ir VDAI patarimai, kaip saugiai tvarkyti duomenis

Efektyviausia priemonė minimizuoti kibernetinių incidentų ir ADSP kiekį yra darbuotojų mokymai

Kibernetinio saugumo priemonių taikymas ir jų laikymasis asmens duomenų apsaugos srityje yra būtina sąlyga, kad visuomenė pasitikėtų valstybės ir savivaldybių institucijomis ir įstaigomis ir kitomis organizacijomis bei naudotųsi jų teikiamomis informacinės visuomenės paslaugomis. Todėl šiuolaikinėje skaitmeninėje visuomenėje nepaprastai svarbus tiek viešojo, tiek privataus sektoriaus atstovų tinkamas dėmesys kibernetiniam ir asmens duomenų saugumui organizaciniame ir įgyvendinimo lygmenyje bei pačios visuomenės kibernetinio saugumo sąmoningumo lygis.

BDAR reikalaujama, kad organizacijos įgyvendintų „tinkamas technines ir organizacines" asmens duomenų apsaugos priemones. Kokios priemonės yra tinkamos, priklauso nuo duomenų jautrumo ir rizikos laipsnio, jei asmens duomenys bus pažeisti. Iš esmės, kuo jautresni duomenys (pvz., žmogiškųjų išteklių įrašai, finansiniai duomenys, sveikatos įrašai), tuo griežtesnių priemonių reikia, kad jie būtų apsaugoti.

Siekdama padėti sumažinti riziką patirti ADSP, VDAI pateikia patarimų, kaip sustiprinti duomenų apsaugą.

Siūlomos įgyvendinti organizacinės priemonės:

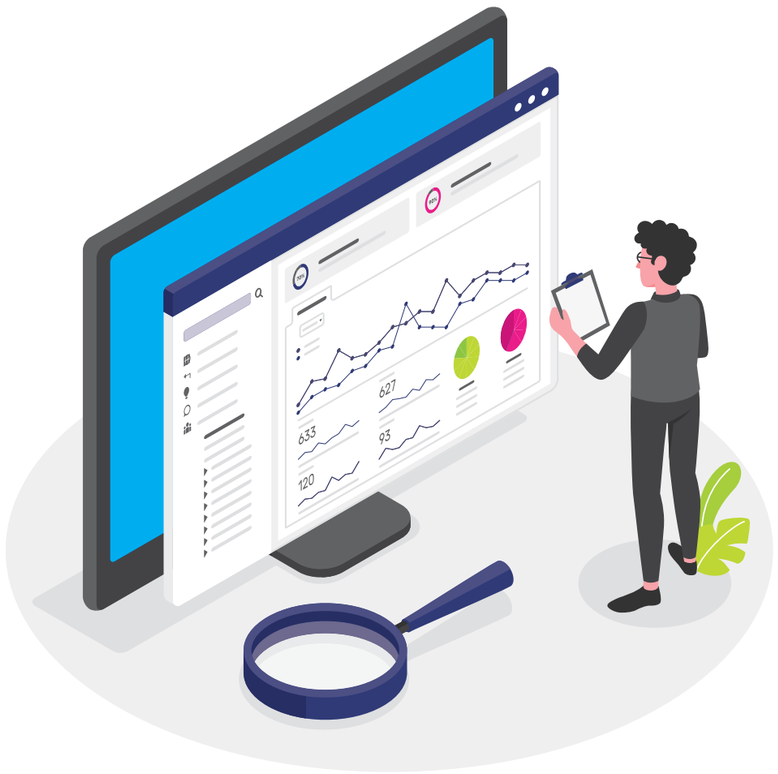
- Supraskite, kokius duomenis turite, ir juos klasifikuokite. Negali apsaugoti informacijos, jei nežinai, kur ji saugoma ar kaip naudojama, kur laikomos atsarginės kopijos ir t. t. Įsitikinkite, kad žinote, kokie duomenys jūsų organizacijoje yra kritiškai svarbūs ar jautrūs, juos būtina suklasifikuoti pagal svarbos ar kritiškumo lygį.
- Užtikrinkite fizinę dokumentų ir įrenginių su duomenimis saugą – laikykite asmens duomenis saugiai, kad niekas neturėtų prieigos be jūsų leidimo.
- Nuolat laikykitės „švaraus stalo" ir „švaraus spausdintuvo" taisyklių, jokie dokumentai su asmens duomenimis neturi likti be jūsų priežiūros.
- Būtinai nurodykite atgalinį adresą, kai siunčiate siuntas ar pašto vokus su dokumentais, kad per klaidą juos gavęs kitas asmuo galėtų grąžinti siuntą jos neatidaręs.
- Mokykite darbuotojus laikytis geriausios duomenų saugumo praktikos, paaiškinkite duomenų saugumo svarbą ir informuokite apie neskelbtinus duomenis organizacijoje. Patarkite, kaip išvengti klaidų, dėl kurių gali įvykti ADSP. Saugumas turėtų būti organizacijos kultūros dalis.

Siūlomos įgyvendinti techninės priemonės:

- Prieigai prie sistemų turi būti nustatyta aiški slaptažodžių politika. Ji gali prasidėti nuo draudimo saugoti slaptažodžius sistemose jų neužšifravus, įpareigojimo laikytis slaptažodžių simbolių kiekio, keitimo dažnumo ir kitų reikalavimų bei perspėjimo nenaudoti to paties slaptažodžio skirtingoms paslaugoms ar įrenginiams.
- Tokios grėsmės kaip išpirkos reikalaujanti programinė įranga ar informacijos užvaldymas yra labai žalingi ir ilgai trunkantys pažeidimai, jie paprastai sukelia laikiną ar nuolatinį duomenų ir paslaugų neprieinamumą. Patikimos rezervinės kopijos yra būtinos norint atstatyti duomenis įvykus incidentui, organizacijoje turi būti aiškiai nustatyta, kaip yra atliekamas rezervinis kopijavimas.

Į turinį

- Viena iš efektyviausių saugumo priemonių – nuolat atnaujinti sistemas, nes gamintojai išleidžia saugos pataisas ir patobulinimus, kai aptinkamos problemos. Turi būti užtikrinami atnaujinimai ne tik įrenginių operacinėms sistemoms, bet ir taikomosioms programoms ar programėlėms įrenginiuose. Tai turėtų būti paskutinės gamintojo pateikiamos versijos. Dažnai atnaujinamų sistemų naujinimas turėtų būti dokumentuotas ir atsekamas.
- Kartais, atliekant techninės priežiūros darbus, programinės įrangos testavimą ar suteikiant vienkartinę prieigą prie sistemos, pritaikomi tokie nustatymai, kurie gali kelti pavojų saugumui. Šie laikini saugumo pakeitimai ar prieigos leidimai dažnai būna neprižiūrimi ir galiausiai tampa nuolatiniai, todėl atsiradusi saugumo spraga lieka atvira. Pavyzdžiui, dažnai tai būna prieigos prie duomenų bazės ar nuotolinio serverio per internetą suteikimas nesilaikant įprasto ar rekomenduojamo saugumo lygio ir nuostatų.
- Pagrindinė priemonė informacijos konfidencialumui užtikrinti yra nustatyti privalomą šifravimą, bent jau nešiojamiems prietaisams, nes juos galima lengvai pamesti arba juos gali pavogti. Ši rekomendacija taikoma ne tik nešiojamiesiems kompiuteriams, bet ir telefonams, planšetiniams kompiuteriams, USB atmintinėms, išoriniams standiesiems diskams ir rezervinėms kopijoms, saugomoms kur nors kitur.



Incidentų analizė

Liūtis sutrikdė Registrų centro veiklą

2020 m. liepos mėn. plačiai nuskambėjo ADSP atvejis VĮ Registrų centre. Per įtrūkusias pastato konstrukcijas prasiskverbė vanduo ir užliejo žemesniame pastato aukšte įrengtą serverinę ir sukėlė ilgalaikį serverinėje esančios techninės įrangos veiklos sutrikdymą ir serveriuose esančių duomenų nepasiekiamumą bei grėsmę jų vientisumui.

VĮ Registrų centras, atstatydamas kitų registrų ir informacinių sistemų veiklą ir duomenis, išskyrus e. sveikatos sistemą, neviršijo teisės aktuose nustatyto leidžiamo neveikimo laiko. Tačiau atstatant e. sveikatos sistemos veiklą ir duomenis buvo susidurta su dideliais sunkumais ir techniniais nesklandumais, nes galimai Registrų centras nebuvo tinkamai pasirengęs užtikrinti registruose ir informacinėse sistemose saugomų duomenų svarbą ir kritiškumą atitinkantį asmens duomenų saugumo lygį. Turimos patalpos (serverinės) neatitiko duomenų centrams keliamų aukšto patikimumo bei apsaugos nuo fizinių grėsmių reikalavimų, todėl, neturint patikimų dubliavimo sistemų, nebuvo įmanoma užtikrinti tokio patikimumo lygio, kuris leistų nepertraukiamai veikti registrams ir informacinėms sistemoms ir užtikrintų atsparumą trikdžiams.

Didelio masto nutekintų duomenų panaudojimas el. prekybos platformoje

2020 m. kovo mėn. UAB „Vinted“ el. prekybos platformoje buvo prisijungta prie naudotojų paskyrų be jų žinios, pasinaudojus kitose (šiuo atveju nesusijusiose su „Vinted“) svetainėse nutekintais prisijungimo duomenimis. Dalis nutekintų prisijungimo duomenų buvo neunikalūs ir pakartotinai naudojami keliose svetainėse ar sistemose. Per šį incidentą nukentėjo apie 19 320 asmenų. „Vinted“ el. prekybos platformos naudotojų paskyrose esanti informacijos dalis buvo pakeista be jų žinios ir kilo grėsmė, kad mokėjimo kortelių duomenys bus panaudoti atlikti neautorizuotiems mokėjimams ar bus prarasti „Vinted“ platformos piniginėje esantys pinigai.

plk. Gintaras Koryzna
LK SKD direktorius

Vadovo žodis

Dėl globalizacijos ir informacinių technologijų evoliucijos daugelis pasaulio šalių, skirtingai žvelgiančių į demokratines vertybes, yra susijungusios į bendrą informacinę aplinką, kurioje keičiamasi informacija beveik be jokių apribojimų. Manipuliavimas suklastotomis ir provokuojančiomis naujienomis, skaitmeniniais programiniais produktais ir kibernetinių išpuolių vykdymas sukuria sąlygas daryti įtaką demokratinių valstybių natūraliai raidai. Robotai socialiniuose tinkluose ir komentaruose, samdomi nuomonės formuotojai kursto karą bei skatina tautinę, rasinę, religinę ir socialinių skirtumų nesantaiką.

Valstybės raidos tvarumas tiesiogiai susijęs su valstybės strateginiu, ekonominiu, energetiniu, aplinkos, kibernetiniu, socialiniu bei informaciniu saugumu ir jų užtikrinimas priklauso ir nuo sąmoningų piliečių – valstybės gynėjų. Siekiant apsaugoti ir ginti ne tik nacionalinę – NATO teritoriją, bet ir vakarų visuomenės informacinę aplinką yra įsteigtas Lietuvos kariuomenės Strateginės komunikacijos departamentas.

LK SKD yra KAS institucija, kuri, įgyvendindama strateginės komunikacijos uždavinius nacionaliniu bei tarptautiniu mastu, vykdo informacinės aplinkos vertinimą.

KĄ SAUGO?

- Nacionalinę-NATO informacinę aplinką.

NUO KO SAUGO?

- Nuo priešiškų organizacijų ir valstybių vykdomų informacinių operacijų[68].

KAIP SAUGO?

- Vertindamas informacinę aplinką (kartu su NKSC stebi ir analizuoja informacinius ir kibernetinius incidentus).
- Bendradarbiaudamas su valstybinėmis ir tarptautinėmis institucijomis, žiniasklaida bei nevyriausybinėmis organizacijomis, padeda užkardyti ir (ar) neutralizuoti informacines operacijas.
- Informuodamas visuomenę apie vykdomą manipuliaciją jos jausmais, įsitikinimais bei interesais siekiant ją klaidinti.
- Siekdamas prevenciškai ir (ar) efektyviai mažinti prieš Lietuvos nacionalinio saugumo ir gynybos interesus nukreiptos informacijos padarinius, skatina visuomenę kritiškai mąstyti.
- Remdamas visuomenės pilietiškumo ugdymą, koordinuodamas kariuomenės ir visuomenės bendradarbiavimą.

LIETUVOS KARIUOMENĖS
STRATEGINĖS KOMUNIKACIJOS
DEPARTAMENTAS

kariuomenė.lt info@mil.lt 8 618 26857

05 Prieš Lietuvos nacionalinio saugumo ir gynybos interesus nukreiptos informacijos vertinimas

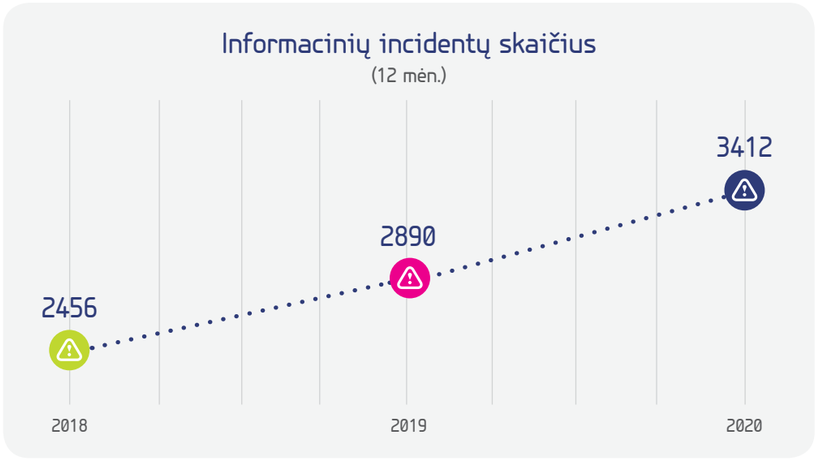
XXI amžius ir konfliktai – naujos karo erdvės. Viena iš jų – informacinė erdvė (Lietuvos karinė doktrina)

Tyčinis visuomenės klaidinimas ar bandymai dezinformacija arba melagingomis naujienomis (angl. *fake news*) paveikti tam tikrų visuomenės grupių nuostatas yra senas ir gerai žinomas būdas valstybių ir visuomenių vystymosi istorijose. Tačiau XXI a. dėl IRT priemonių įvairovės ir interneto sklaidos melagingos naujienos įgavo milžinišką pagreitį: manipuliavimas informacijos turiniu ir melagingų naujienų rengimas tampa gana paprastu procesu, o socialiniai tinklai dėl juose dažnai nekritiškai vertinamo turinio – efektyviu melagingų naujienų sklaidos šaltiniu.

Pažymėtina, kad kibernetiniai ir informaciniai incidentai ar kombinuotos (hibridinės) atakos[69] yra informacinių operacijų elementai. Tai yra gerai organizuota ir finansuota veikla, kurią gali vykdyti nusikaltėliai, piktavaliai, teroristai, taip pat autoritariniai režimai, siekdami ekonominių, ideologinių ir politinių tikslų. Informacinių operacijų metu gali būti ne tik suklaidinta visuomenė, bet ir sukelta įvairių sunkių padarinių – nuo ekonominių nuostolių, žmonių žūties iki demokratinių valstybių puoselėjamų vertybių (su)naikinimo per kišimąsi į rinkimus, keliant žmonių nepasitikėjimą valstybės santvarka ir valdžios priimamais sprendimais. Nors visuomenės sąmoningumas didėja ir gebėjimas atpažinti melagingas naujienas stiprėja, tačiau kartu tobulėja informacinėms operacijoms vykdyti pasirenkamos modernios IRT, naudojami įvairesni informacijos sklaidos kanalai ir būdai.

Prieš Lietuvos nacionalinius interesus vykdytos informacinės operacijos ir jų tendencijos

Vykdant 2020 m. informacinės aplinkos vertinimą nuo 2020 m. pradžios iki birželio 1 d. LK SKD stebėsena buvo orientuota į COVID-19 pandemijos įtaką informacinei aplinkai, o nuo 2020 m. birželio 1 d. iki metų pabaigos – į Lietuvai svarbias sritis[70]. Bendras Lietuvai priešiškos / nedraugiškos informacinės veiklos atvejų skaičius 2020 m. padidėjo 18 proc. ir tai sudarė 3412 atvejų. Šis atvejų skaičius, palyginti su 2018 ir 2019 m., tolygiai augo (atitinkamai 2456 ir 2890 atvejų).



< 33 pav. >

68 Informacinė operacija – suplanuoti ir koordinuoti veiksmai ir priemonės siekiant paveikti norimą auditoriją.

69 Hibridinė ataka – kibernetinis incidentas kartu su informaciniu incidentu. Informacinis incidentas – vienkartinis ne ES ir (ar) NATO valstybių narių ar jų subjektų informacinis veiksmas, kuriuo, tendencingai informuojant visuomenę, siekiama paveikti su Lietuvos Respublikos nacionalinio saugumo interesais susijusių sprendimų priėmimo procesą ir kuris tiesiogiai nėra susijęs su kitais tokiais veiksmais. (Lietuvos Respublikos Vyriausybės 2020 m. rugpjūčio 26 d. nutarimas Nr. 955 „Dėl Strateginės komunikacijos nacionalinio saugumo srityje koordinavimo tvarkos aprašo patvirtinimo“).

70 Gynyba, užsienio politika, ekonomika ir energetika, konstitucinių pagrindų apsauga, kultūra ir švietimas, socialinė apsauga.

Į turinį

2020 m. daugėjo priešiškų informacinių operacijų ir sudėtingėjo jų pobūdis, vyravo hibridinės operacijos

Vertinant Lietuvos informacinę erdvę, nuo 2020 m. pradžios prieš Lietuvą, NATO aljansą ir atskiras NATO nares buvo įvykdyta 10 (iš jų 7 hibridinės atakos) priešiškų informacinių operacijų. Šios informacinės operacijos buvo susijusios su trimis pagrindiniais įvykiais:

01. COVID-19 pandemijos situacija pasaulyje ir karantinu Lietuvoje;
02. Lietuvos ir Lenkijos tarptautiniais santykiais bei jungtine komunikacija dėl rinkimų Baltarusijoje;
03. Lietuvos Seimo porinkiminiu periodu, kai vyko valdžios perdavimo procesas.

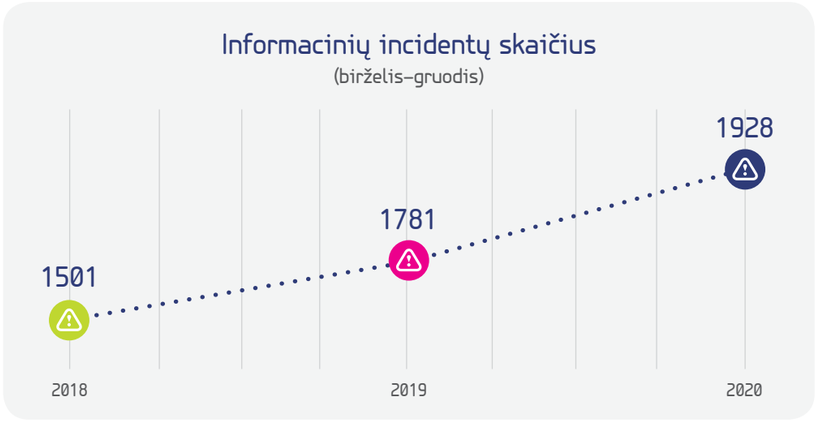
Priešiškų informacinių operacijų metu buvo ieškoma galimų technologinių ir procedūrinių pažeidžiamumų bei siekiama išsiaiškinti sprendimų priėmimo procesų struktūrą ir greitį. Vertinant priešiškų informacinių operacijų modelius su vykdytais 2018 ir 2019 m., galima daryti išvadą, kad 2020 m. vykdytos priešiškos informacinės operacijos išsiskyrė savo mastu bei pasirengimo (žinių apie nacionalinius ir tarptautinius procesus) lygiu.

2020 m. informaciniai incidentai prieš Lietuvą ir valstybės interesus dažniausiai buvo vykdomi per interneto svetaines bei socialinius tinklus. Tuo tarpu hibridinių atakų metu buvo įsilaužiama į Lietuvos regioninės žiniasklaidos interneto svetaines ir (ar) neteisėtai prisijungiama prie jų bei imituojami oficialių Lietuvos valstybės institucijų ir įstaigų elektroniniai laiškai, siekiant suklaidinti naudotoją ir (ar) elektroninio laiško gavėją.

Vertinant 2020 m. vykdytas informacines operacijas Lietuvoje, nustatytos šios informacinių incidentų ir hibridinių atakų tendencijos:

- priešiškų ir nacionalinių visuomenės informavimo kanalų sinergija;
- priešiškose visuomenės informavimo priemonėse (televizijos programose) buvo platinamos melagingos naujienos, klaidinanti informacija verčiama į lietuvių kalbą ir skelbiama socialiniuose tinkluose;
- įvykdžius kibernetinius incidentus buvo skelbiamos melagingos naujienos lietuviškuose interneto žiniasklaidos priemonių interneto svetainėse, vagiamos privačių asmenų, Lietuvos valstybės tarnautojų ir institucijų, žurnalistų, NATO generalinio sekretoriaus, sąjungininkų vyriausybių narių ar karinių pajėgų vadų tapatybės, jų vardu siunčiami sufalsifikuoti (angl. *spoofing*) elektroniniai laiškai ar pranešimai spaudai;
- incidentai buvo vykdomi siekiant Lietuvai negatyvaus efekto, juos siejant su strateginiais vidaus (pavyzdžiui, su LR Seimo porinkiminiu periodu, kai vyko valdžios pasikeitimo procesas) ir užsienio politikos įvykiais (pavyzdžiui, su Lietuvos ir Lenkijos jungtine iniciatyva dėl Baltarusijos nedemokratinių rinkimų);
- fiksuotas ir tikslingas neigiamos informacijos apie Lietuvos valstybę ir ES bei NATO partnerius amplifikavimas, galėjo būti naudojamasi parduodamomis interneto kompanijų reklamos paslaugomis, siekiant didinti peržiūrų „Youtube“ ir kituose socialiniuose tinkluose skaičius;
- buvo naudojamasi socialiniais tinklais, siekiant organizuoti nesankcionuotas protesto akcijas, kuriose žmonės buvo nuteikinėjami prieš skiepus nuo COVID-19 ligos, kurstomi nesilaikyti paskelbto karantino taisyklių ir nedėvėti kaukių ir kitų apsaugos priemonių.

Iš viso per 2020 m. III–IV ketvirčius buvo identifikuota 1928 Lietuvai priešiškos informacinės veiklos atvejų (arba vidutiniškai apie 321 per mėnesį) (žr. **34 pav.**).

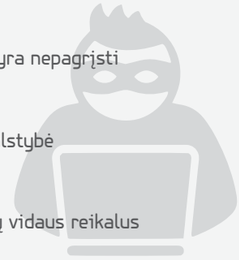


< 34 pav. >

Pasibaigus prezidento rinkimams Baltarusijoje, Lietuva sulaukė padidėjusio Baltarusijos žiniasklaidos neigiamo informacinio srauto

Vertinant 2018, 2019 ir 2020 m. duomenis, pastebėta, jog informaciniai incidentai daugiausia buvo nukreipti prieš gynybos, užsienio politikos, ekonomikos ir energetikos sektorius. 2020 m. II pusmetį įvykę informaciniai incidentai pagal strategiškai svarbius Lietuvai sektorius pasiskirsto taip: gynyba – 24,53 proc.; užsienio politika – 24,22 proc.; ekonomika ir energetika – 23,55 proc.; konstitucinių pagrindų apsauga – 12,81 proc.; kultūra ir švietimas – 11,67 proc.; socialinė apsauga – 3,22 proc. Konstitucinių pagrindų apsaugos bei kultūros ir švietimo sektoriams šių metų II pusmetį skirta kiek mažiau dėmesio, o socialinės apsaugos sektorius pabrėžtas mažiausiai (žr. **36 pav.**). Dažniausi naratyvai minėtuose sektoriuose yra šie:

NARATYVAS 01	NATO yra grėsmė Lietuvos nacionaliniam saugumui
NARATYVAS 02	NATO provokuoja Rusiją ir Baltarusiją
NARATYVAS 03	Lietuvos kariuomenė yra nepasirengusi apginti valstybės
NARATYVAS 04	Lietuvoje yra perrašomi ir klastojami istoriniai faktai
NARATYVAS 05	Lietuva yra socialiai ir ekonomiškai žlugusi valstybė
NARATYVAS 06	Lietuvos energetiniai tikslai yra nepagrįsti
NARATYVAS 07	Lietuva yra nedemokratinė valstybė
NARATYVAS 08	Lietuva kišasi į kitų valstybių vidaus reikalus

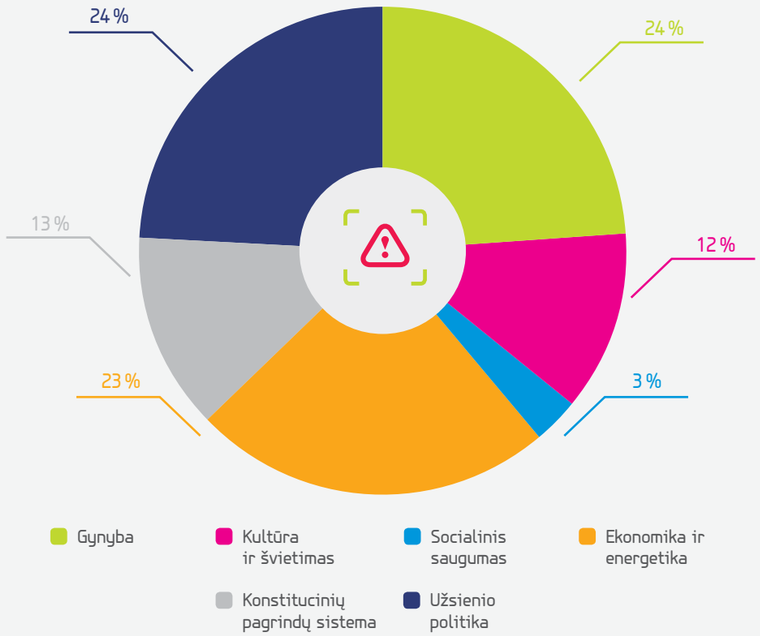


< 35 pav. >

Į turinį

2020 m. grėsmės Lietuvos informaciniam saugumui išliko tos pačios. Pagrindinis informacinių grėsmių šaltinis išliko Rusijos Federacija bei jos vyriausybės kontroliuojamos žiniasklaidos priemonės, kurių veikla buvo nukreipta Lietuvos, NATO ir ES valstybių visuomenių nuomonei formuoti

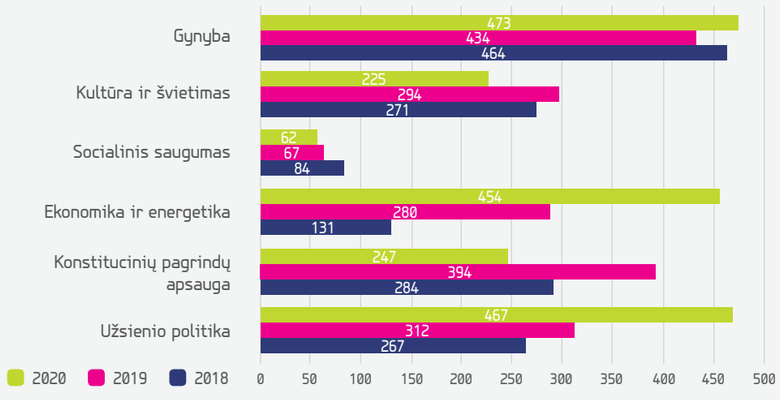
Informaciniai incidentai pagal sektorius
(birželis–gruodis)



< 36 pav. >

Atsižvelgiant į trejų paskutinių metų antrųjų pusmečių tendencijas, galima pastebėti, kad 2020 m. II pusmetį intensyviausi buvo liepos, rugsėjo, lapkričio ir gruodžio mėnesiai. Tai sutapo su reikšmingais užsienio politikos ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti formuodami neigiamą šalies įvaizdį Vakaruose ir skatindami Lietuvos visuomenės auditorijų tarpusavio susipriešinimą (žr. **37 pav.**).

Informacinių incidentų skaičius pagal sektorius
(birželis–gruodis)



< 37 pav. >

Incidentų analizė

Melagingos naujienos „Lenkijos diplomatas sulaikytas Lietuvos pasienyje“, „Lietuvos šaukiamojo amžiaus piliečiai turi prisistatyti į prievolės centrus“, „Šiaulių oro uosto infrastruktūros modernizavimo yra feikas“ paskelbtos kartu su kibernetiniais incidentais

Situacija

Lietuvos Respublikoje fiksuojamas augantis susirgimų koronavirusu (COVID-19) ir mirčių nuo šios ligos skaičius. Vyksta Lietuvos Respublikos Seimo porinkiminis valdžios perdavimo procesas. Vykdomos informacinės kampanijos (peticijos, informacijos sklaida socialiniuose tinkluose bei žiniasklaidoje) prieš Lietuvos kariuomenės karinį poligoną vakarų Lietuvoje bei atnaujintą Karo policijos įstatymą. Skleidžiamas melas apie Karo policijos panaudojimą priverstiniam skiepijimui.

Eiga

2020 m. gruodžio 9 d. buvo neteisėtai prisijungta prie Lietuvos Respublikos valstybės ir savivaldybių institucijų ir įstaigų interneto svetainių ir jose paskelbtos melagingos naujienos (angl. *defacement*). Vėliau, imituojant (angl. *spoofed*) Užsienių reikalų ministerijos, Šiaulių savivaldybės administracijos bei Krašto apsaugos ministerijos adresatus, buvo išsiųsti el. laiškai su melaginga informacija Lietuvos Respublikos valstybės institucijoms.

Kas atsitiko

Įvykio metu buvo vykdoma 3 krypčių komunikacija, skirta Lietuvos Respublikos šaukiamojo amžiaus piliečiams bei Lietuvos Respublikos valstybinių institucijų – KAM, URM, VRM, SM bei Lietuvos Respublikos rajonų savivaldybių personalui apgauti ir (pa)veikti. Kelių valandų skirtumu (18:17-20:29 val. 9 d.) apgaulės būdu išsiuntinėti laiškai institucijoms, jų turinys ir tikslinės auditorijos turi informacinės operacijos požymių. Informacinių operacijų metu siekta sukelti šauktinių amžiaus grupės visuomenės nepasitenkinimą, mažinti pasitikėjimą oficialiais informaciniais kanalais, sukelti sumaištį ir lėtinti sprendimų priėmimo procesą institucijose, trikdyti tarptautinius santykius. Vertinant bendrą situaciją, informacinės atakos pradžios laiką, atakuotų valstybinių institucijų tipą ir mastą, komunikacijos turinį bei galimustikslus, darytina prielaida, kad pagrindinis informacinių operacijų tikslas - (pa)veikti valdžios perdavimo-perėmimo procesą, taip pat Lenkijos ir Lietuvos tarptautinį bendradarbiavimą.

Interneto žiniasklaidos interneto svetainėse kauno.diena.lt, klaipeda.diena.lt, diena.lt, kaunas.kasvyksta.lt ir baltictimes.com paskelbta melaginga naujiena: „JAV karys susirgo korona virusu“

Situacija

Situacija. 2020 m. sausio mėn. pasaulyje sparčiai plinta COVID-19 liga, vis daugiau kalbama apie karantino būtinybę. Sausio 30 d. Pasaulio sveikatos organizacija paskelbia ekstremalią situaciją globaliu mastu. Lietuva rengiasi birželio 4 d. numatytoms tarptautinėms pratyboms „Defender Europe 20“. Lietuvoje vykdoma NATO eFP misija ir glaudžiai bendradarbiaujama su JAV. Lietuvos visuomenės nerimo lygis sparčiai auga dėl plintančio viruso[71].

Eiga

Sausio 28 d. interneto svetainėje, sukurtoje naudojant *Wordpress* TVS, anglų kalba pasirodė melaginga informacija, esą sausio 17 d. leitenantas Mo iš Lietuvoje dislokuoto JAV bataliono buvo pristatytas į Lietuvos ligoninę. Kaip teigiama, negalavimo priežastis – naujo tipo koronavirusas. Sausio 31 d. melaginga naujiena atsidūrė ir Lietuvos informacinėje erdvėje. Įvykdžius kibernetines atakas, buvo įsilaužta į interneto žiniasklaidos interneto svetaines kauno.diena.lt, klaipeda.diena.lt, diena.lt, kaunas.kasvyksta.lt ir baltictimes.com ir jose paskelbta melaginga naujiena lietuvių kalba. Šios naujienos tariamam autentiškumui sustiprinti buvo suklastotas JAV bataliono Lietuvoje vado Steveno Johnsono komentaras ir pasinaudota naujienų agentūros BNS vardu. Sausio 31 d. suklastojus Lietuvos kariuomenės atstovo elektroninio pašto adresą (angl. *spoofed*), keletai šalies institucijų buvo išsiųsta melegingų laiškų.

Kas atsitiko

Atlikus įvykio visą dekonstrukciją kartu su NKSC bei kitomis institucijomis paaiškėjo, kad agresorius, pasinaudodamas JAV karių buvimu Lietuvoje, pasauline pandemija ir Lietuvos žmonių aukštu nerimo lygiu, siekė diskredituoti Lietuvos strateginius partnerius platindamas melagingą informaciją (neva JAV kariai bus ažvežę virusą į Lietuvą) per interneto svetaines ir socialinius tinklus bei tuo pagrįsti savo ilgalaikį naratyvą, kad „NATO kelia grėsmę Lietuvos žmonėms“. Taip pat įsilaužtas į naujienų portalus ir juose paskelbdamas melagingą informaciją siekė sukelti visuomenės nepasitikėjimą registruotais žiniasklaidos kanalais. Trečia, ko siekė agresorius, tai daryti poveikį sprendimo priėmimo proceso trukmei ir tarpinstituciniam pasitikėjimui, nes kai institucijos sulaukė laiškų iš kitos oficialios institucijos su melagingu turiniu, atsirado dvigumo autentikavimo poreikis, tai iš esmės prailgino komunikacijos laiką. Apibendrinus visą informaciją, teigtina, kad agresorius informacinę operaciją vykdė trimis etapais arba visi etapai buvo vykdomi skirtingų organizacijų/veikėjų. Pirmas etapas – informacinės aplinkos supratimas, laiko, geografijos, strateginių įvykių bei žmogiškojo faktoriaus supratimas. Antras etapas – potencialių materialių bei nematerialių taikinų identifikavimas ir pasirengimas (melagingo turinio sukūrimas 3 kalbomis, laikino portalo ir paskyrų sukūrimas, registracija su laikinomis paskyromis į „opednews“ tipo žinių portalus bei pokalbių kambarius „chat rooms“, žinisklaidos portalų programinių pažeidžiamumų radimas arba pirkimas iš kibernetinių nusikaltėlių, elektroninių laiškų suklastojimas (angl. *spoofing*). Trečias etapas – aktyvavimas: interneto svetainės puslapio su melaginga informacija startavimas, prisijungimas su laikinomis paskyromis prie „opednews“ tipo portalų bei pokalbių kambarių ir melagingos informacijos paskelbimas kaskadiniu principu (šaltinio nuoroda į nuorodą), melagingos informacijos paskelbimas įsilaužtuose žinių portlauose bei suklastotų laiškų išsiuntimas respondentams (angl. *tracking pixel*).

71 https://trends.google.com/trends/explore?geo=LT&q=Karantinas,Koronavirusas,Virusas

LK SKD pagrindiniai patarimai, kaip geriau atpažinti informacinius incidentus ir (ar) klaidinančią informaciją

- Blogos ar geros informacijos nėra, yra tik vertinga arba nevertinga kiekvienu individualiu atveju.
- Naudojant informaciją, reikėtų vadovautis principu laikas – pinigai.
- Atsirinkti konkrečius informacijos šaltinius iš milijardų galimų, turinčius pridėtinę vertę ir teikiančius patikimą informaciją.
- Patikima informacija gali būti laikoma ta, už kurią laiduoja valstybė, verslo bei draudimo kompanijos.
- Pasirodžius neįprastai informacijai patikimuose kanaluose, galima įtarti, kad buvo įvykdyta hibridinė ataka ir neteisėtai paskelbta klaidinanti informacija, todėl rekomenduotina tuo pačiu metu naudoti bent du tris patikimus šaltinius.
- Įtarus, kad informacija yra galimai netiksli ar klaidinanti, rekomenduotina apie tai informuoti informacijos kanalo valdytoją.

Į turinį

06

COVID-19 pandemijos įtaka

01 Valstybės institucijų atsakas į COVID-19 pandemijos sukeltus iššūkius

2020-ieji neabejotinai įsirėš į atmintį: prasidėję neregėto masto pandemija baigėsi ne ką mažesne įtampa, nors pasaulis su viltimi sutiko žinią apie sukurtą vakciną nuo COVID-19 ligos. Koronaviruso pandemija dar kartą įrodė, kokia svarbi valstybės ir visuomenės gyvenime yra saugi ir funkcionuojanti RIS. IRT saugumas turėtų būti centrinė viso skaitmenizavimo proceso ašis, nes tai svarbu ne tik skaitmenizavimo procesui įsibėgėjus, bet ir pačioje pradžioje.

NKSC ir kitos valstybės institucijos ir įstaigos į šią krizę sureagavo gana greitai: parengė reikiamas rekomendacijas ir pritaikė atitinkamas technines priemones, kad gyventojai, verslas, valstybės institucijos ir įstaigos prisitaikytų prie naujos realybės.

NKSC prioritetas pandemijos metu – užtikrinti YSII ir VII kibernetinį saugumą ir atsparumą kibernetinėms grėsmėms

Kaip įsitikinome, COVID-19 liga turėjo milžiniškos įtakos organizacijų veiklos tęstinumui, nes reikėjo sparčiai pertvarkyti visus veiklos procesus ir tęsti veiklą naujomis, daugiausia paremtomis IRT naudojimu, aplinkybėmis. Todėl priklausomybė nuo IRT siaučiant pandemijai dar labiau padidėjo ir tai neišvengiamai sukėlė naujų iššūkių ir įtampos kibernetinio saugumo srityje. Nusikaltėliai, piktavaliai ir priešiškai nusiteikusios valstybės pandemijos sukelta įtampa pasinaudojo savo tikslais: iš asmenų viliojo pinigus, bandė išgauti komercines paslaptis, asmens duomenis, vykdė informacines atakas. Smulkios ir vidutinės įmonės, bandydamos kuo skubiau pertvarkyti savo veiklą ir išgyventi, ne taip skrupulingai laikėsi bazinių kibernetinio saugumo reikalavimų[72] (pvz., neužtikrino darbuotojų turimos informacijos ir ryšio apsaugos, naudojant VPN, nenaudojo kelių žingsnių autentifikavimo darbuotojams nuotoliniu būdu jungiantis prie savo paskyrų, darbuotojai dirbo su asmeniniais įrenginiais, kurie yra ne tokie saugūs kaip įmonės aplinkoje ir t. t.). Kadangi YSII ir VII valdytojai ir (ar) tvarkytojai dažnai tik formaliai įgyvendino reikalavimus[73], kibernetinio saugumo užtikrinimo problema karantino metu vis labiau ryškėjo.

Šią itemptą situaciją galima prilyginti krizei, tad atsakas į ją taip pat turėjo ir turi būti toks, kaip ir į bet kurią kitą krizę – turi būti priimti atitinkami sprendimai dėl kibernetinio saugumo rizikos (t. y. ją sumažinant, priimant, išvengiant ar perduodant), kad būtų užtikrinama viešojo ir privataus sektorių atstovų veikla trumpuoju, vidutiniu ir ilgiuoju laikotarpiais. Didesnė rizika (pvz., atidarant tinklo prieigas, įdiegiant nepakankamai patikrintas technologijas ir pan.) galėtų būti prisiimta tik pradiniame krizių atsiradimo laikotarpyje, vėliau reikėtų įsitikinti, ar prisiimta rizika išskirtinėmis aplinkybėmis vis dar atitinka organizacijoms priimtiną rizikos laipsnį. Taip pat ši pandemija parodė, kad ne tik kibernetinės grėsmės, bet ir krizės, iš pažiūros visai nesusijusios su kibernetiniais incidentais, tikimybė turi paskatinti organizacijas nuolat atnaujinti veiklos tęstinumo valdymo planus. Todėl NKSC rekomenduoja, kad organizacijos kibernetinio saugumo rizikas įtrauktų į visą savo veiklą apimantį rizikos vertinimą, vientisų veiklos tęstinumo ir krizių prevencijos planus.

2020 m. pavasarį (COVID-19 plitimo piko ir karantino metu) daug dėmesio buvo skiriama sveikatos priežiūros sektoriaus atstovų interneto svetainėms. Po atlikto interneto svetainių pažeidžiamumų patikrinimo sveikatos priežiūros įstaigoms buvo oficialiai pranešta apie rastus trūkumus ir paraginta susitvarkyti aptiktas spragas

72 Baziniai saugumo reikalavimai smulkioms ir vidutinėms įmonėms patraukliai ir aiškiai išdėstyti 2020 m. birželio mėn. išleistame leidinyje „Kibernetinis saugumas ir verslas. Ką turėtų žinoti kiekvienas įmonės vadovas“ (žr. 29 p.).

73 Žr. ataskaitos dalį „YSII valdytojų bei VII valdytojų ir (ar) tvarkytojų kibernetinio saugumo būklė“, 42 p.

Į turinį

NKSC 2020 m. stebėjo suaktyvėjusį COVID-19 ligos temos naudojimą įvairių klastočių kampanijose (suklastoti el. laiškai ir el. parduotuvės, reklamuojančios vakcinas, vaistus ar medicininę įrangą). Didelių kibernetinių incidentų, susijusių su koronaviruso infekcija, nenustatyta.

Vis dėlto šios ligos įtaką Lietuvos kibernetinio saugumo būklei rodo (žr. 38 pav.):

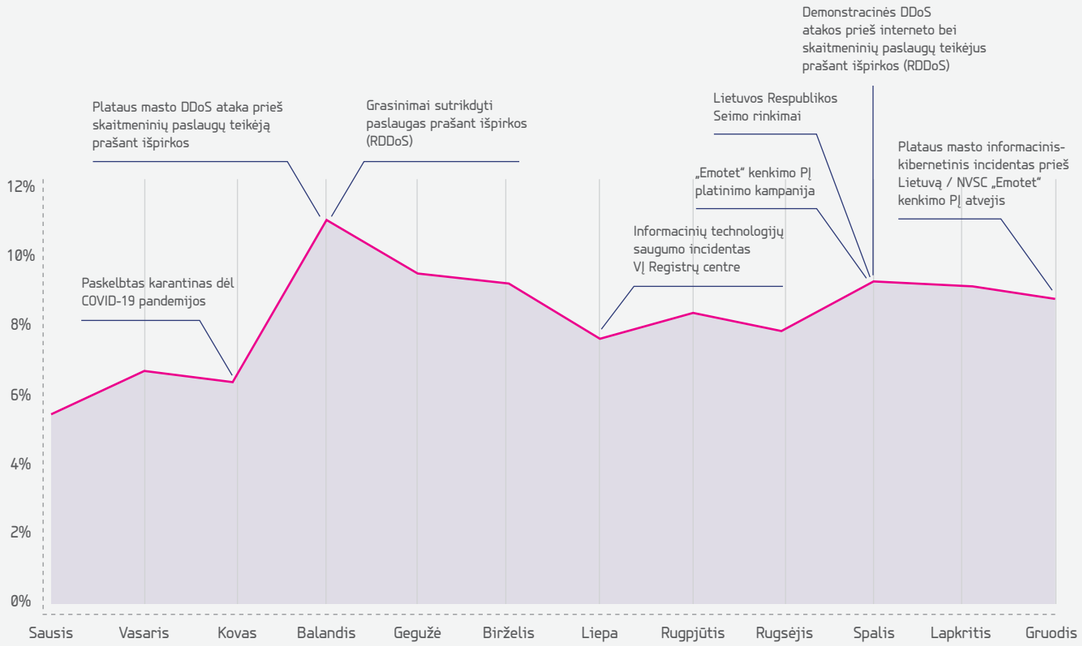
- padidėjęs incidentų, susijusių su „Emotet" kenkimo PĮ[74] bei kitų kenkimo PĮ plitimu per el. laiškus, skaičius, kai darbuotojai, dirbdami nuotoliniu būdu, dažniau bendravo el. laiškais[75];
- padidėjęs kibernetinių incidentų, susijusių su duomenis šifruojančios bei išpirkos reikalaujančios PĮ plitimu, skaičius, kai darbuotojai, dirbami nuotoliniu būdu, aktyviau naudojosi nuotolinio darbalaukio protokolo (angl. *remote desktop protocol* (RDP))[76] paslaugomis;
- išaugęs kibernetinių incidentų skaičius švietimo įstaigose, kai buvo trikdomos nuotolinės pamokos, pašaliniai asmenys transliavo nepageidaujamą turinį, buvo vykdomi DDoS kibernetiniai incidentai ir pan.;
- padidėjusi kibernetinio saugumo rizika, kai ne visi darbdaviai išdavė savo darbuotojams iš anksto sukonfigūruotas IRT priemones darbui nuotoliniu būdu.

74 Lietuvoje nuo spalio mėn. buvo nustatyta „Emotet" kenkimo PĮ platinimo banga, o metams baigiantis ši kenkimo programa paveikė informaciją apie COVID-19 ligos situaciją Lietuvoje visuomenę informuojantį NVSC.

75 Pavyzdžiui, 2020 m. gruodžio 29 d., imituojant NVSC darbuotojos el. pašto adresą, buvo siunčiami laiškai su pridėtu galimai užkrėstu dokumentu. Adresatams atidarius tokį laišką, virusas pateko į vidinį NVSC tinklą. Užkrėsti institucijos kompiuteriai, atsisiuntę papildomas bylas, pradėjo siųsti netikrus laiškus ar dalyvauti kitokio pobūdžio kenkimo veikloje.

76 Šis protokolas turi žinomų saugumo spragų, tad turėtų būti naudojamas su papildomomis saugumo priemonėmis (pvz., kelių žingsnių autentifikavimo priemonėmis), nes jį labiau ėmė išnaudoti piktavaliai, bandydami įsilaužti į organizacijų tinklus.

Kibernetinio saugumo grėsmės COVID-19 pandemijos metu



< 38 pav. >

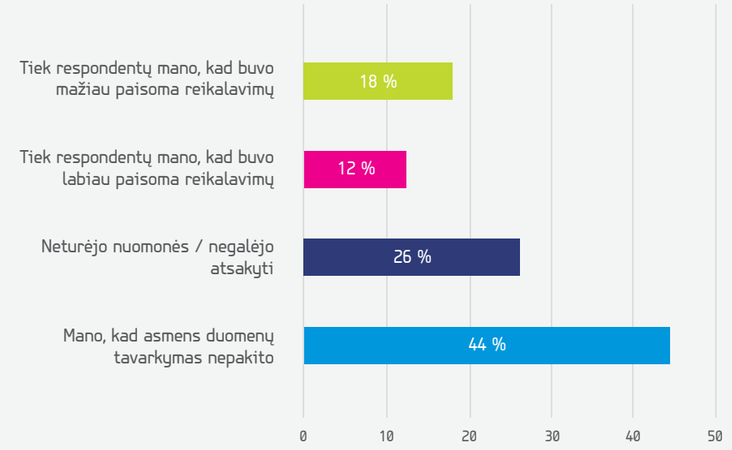
2020 m. kovo 16 d. Lietuvoje paskelbus karantiną ir daugeliui žmonių pradėjus dirbti nuotoliniu būdu, NKSC darbuotojams ir organizacijų IT personalui parengė ir savo interneto svetainėje publikavo rekomendaciją nuotolinio darbo tema – „Bazinės kibernetinio saugumo rekomendacijos nuotoliniam darbui". Vėliau reaguojant į situaciją buvo parengtos ir publikuotos kitos rekomendacijos: „Dėl komunikacijų platformos „Zoom" saugumo", „Slaptažodžių stiprumas, sudėtingumas ir sauga", „Tapatybės vagystės", „Telekonferencinių programinių sprendimų apžvalga ir rekomendacijos", „Kaip užtikrinti daiktų interneto įrenginių saugumą".

Svarbu pažymėti, kad „Zoom" platforma per 2020 m. ištaisė daugumą saugumo spragų. Taip pat NKSC specialistai nuolat viešojo ir privatus sektoriaus atstovams teikė patarimus, ką reikėtų daryti gavus įtartinų el. laiškų, žinučių ar sulaukus telefoninių skambučių.

Asmens duomenų saugumas COVID-19 pandemijos metu

2020 m. COVID-19 pandemija ir jos sukeltos visuomeninio gyvenimo permainos paskatino dar spartesnius skaitmenizacijos bei IRT įtraukimo ir panaudojimo daugelyje gyvenimo sričių procesus. VDAI stebėjo, kaip viešojo ir privataus sektorių atstovai taiko priemones, skirtas pandemijos padariniams Lietuvoje sušvelninti. 2020 m. buvo atliktas reprezentatyvus Lietuvos gyventojų nuomonės apklausos tyrimas. Daugelis respondentų į klausimą: „Kaip vertinate asmens duomenų tvarkymą COVID-19 pandemijos laikotarpiu?" atsakė nemanantys, kad koronaviruso infekcija turėjo įtakos asmens duomenų tvarkymui (žr. **39 pav.**):

Duomenų tvarkymas COVID-19 pandemijos laikotarpiu



< 39 pav. >

Kaip teigia VDAI, daugelis taikomų efektyvių priemonių, skirtų pandemijai suvaldyti, gali būti susijusios su skirtingų rūšių asmens duomenų tvarkymu bei poreikiu jais dalytis ne tik tarp sveikatos priežiūros įstaigų ir jų veiklą koordinuojančių institucijų, bet ir atitinkama apimtimi su visuomene. Visgi netgi tokiomis išskirtinėmis sąlygomis vertėtų nepamiršti, kad privaloma užtikrinti atitinkamo lygio duomenų subjektų asmens duomenų apsaugą, kad būtų užkirstas kelias galimam asmenų persekiojimui, šmeižimui ar net susidorojimui. VDAI pažymi, kad BDAR nedraudžia tvarkyti asmens duomenų siekiant

2020 m. pirmą kartą istorijoje žmogaus mirčiai galėjo įtakos turėti duomenis šifruojanti ir išpirkos reikalaujanti kenkimo PĮ, sutrikdžiusi vienos iš Vokietijos ligoninių RIS veiklą

Nauji tyrimai ir įvykiai rodo, kad ADSP poveikis pajuntamas ne tik iškart, kai pažeidimas aptinkamas, bet ir daug vėliau – finansinį tokio pažeidimo poveikį organizacijos gali pajusti praėjus ir daugiau nei 2 metams po pirminio incidento

Europos Sąjungos kibernetinio saugumo agentūros (ENISA) duomenimis, piktavaliai ir toliau rengs seksualinės prievartos (angl. sextortion) atakas prieš paauglius ir jaunuolius, o patyčių internete pandemijos metu ir net po jos tik daugės

suvaldyti pandemiją, tačiau kaip ir įprastomis sąlygomis turi būti užtikrintas jų tvarkymo tikslingumas ir teisėtumas. Taigi, siekiant užtikrinti teisėtą asmens duomenų tvarkymą, turėtų būti atsižvelgiama į atitinkamas aplinkybes ir visais atvejais reikėtų prisiminti, kad visos priemonės, kurių imamasi tokiu atveju, turi atitikti bendruosius teisės principus ir neturėtų būti negrįžtamos. Nepaprastoji padėtis yra ta teisinė sąlyga, kuri gali pateisinti žmogaus teisių ir laisvių apribojimus, tačiau tik tuomet, kai šie apribojimai yra proporcingi ir taikomi tik šios nepaprastosios padėties laikotarpiu.

VDAI karantino pradžioje nustatė atvejų, kai be pagrindo buvo renkami atvykstančiųjų į kurortinę savivaldybę duomenys ir skelbiami užsikrėtusiųjų maršrutai nepakankamai nuasmeninus informaciją, tai sukėlė visuomenės susirūpinimą asmens duomenų saugumu ir privatumu.

Europos duomenų apsaugos valdyba[77], vienijanti visų ES valstybių asmens duomenų apsaugos priežiūros institucijas, tarp kurių yra VDAI, prasidėjus COVID-19 pandemijai, sudarė priežiūros institucijų atstovų nuotolinę grupę asmens duomenų apsaugos klausimams identifikuoti ir apsispręsti dėl tolesnių veiksmų. Parengtos ir toliau rengiamos metodinės rekomendacijos tokiomis temomis, kaip įvairios kontaktų atsekimo mobiliosios programėlės, nuotolinis darbas, nuotolinis mokymasis, nuotolinės sveikatos priežiūros paslaugos, klientų registravimas ir kt.[78].

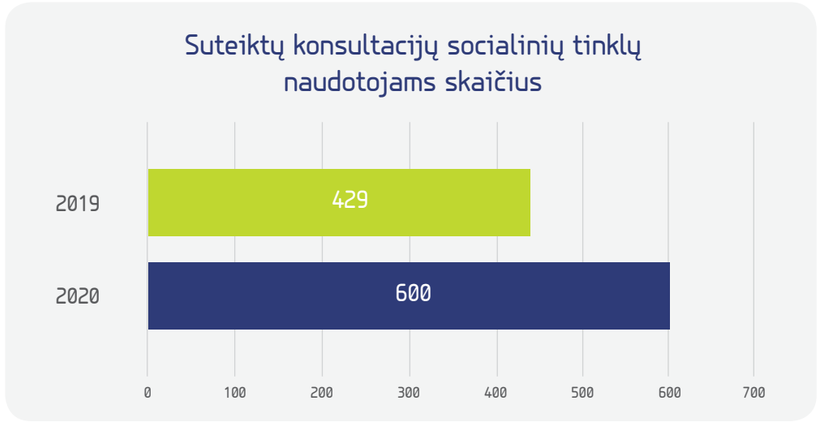
COVID-19 pandemijos įtaka viešųjų elektroninių ryšių tinklų vientisumui ir išaugęs konsultacijų interneto naudotojams poreikis

Viešųjų elektroninių ryšių paslaugos dėl koronaviruso infekcijos paskelbto karantino tapo ypač svarbios, nes verslas ir viešasis sektorius persiorientavo ir didžiąją dalį paslaugų pasiūlė teikti internetu, o žmonės pradėjo dirbti ir mokytis nuotoliniu būdu. Natūralu, kad tai gerokai padidino elektroninių ryšių srautus ir tapo nemenku išbandymu viešųjų ryšių tinklams. Pavasarį, pirmojo karantino Lietuvoje metu, RRT su viešųjų ryšių tinklų teikėjais susitarė ir dėl papildomo periodinio informacijos apie tinklų būklę teikimo tol, kol bus įsitikinta, kad viešųjų elektroninių ryšių tinklų būklė yra gera ir sutrikimų dėl pandemijos nefiksuojama. Tad, RRT vertinimu, 2020 m. Lietuvos viešųjų ryšių tinklų pajėgumai visus metus išliko pakankami (viešųjų ryšių tinklų teikėjų netgi buvo nuolat didinami, siekiant patenkinti augantį poreikį), viešųjų ryšių tinkluose nebuvo nustatyta daugiau gedimų atvejų nei ankstesniais metais, o įvykę gedimai pašalinti operatyviai.

Tuo pat metu RRT, administruodama interneto svetainę **www.esaugumas.lt**, suteikė beveik 40 proc. daugiau konsultacijų interneto naudotojams, kaip sklandžiai naudotis internetu. 2019 m. suteiktos 429, o 2020 m. – 600 konsultacijos (žr. **40 pav.**).

77
https://edpb.europa.eu/about-edpb/about-edpb_lt

78
https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_lt



< 40 pav. >

Europolas pažymi, kad pandemijos sukelta krizė parodė, kaip efektyviai nusikaltėliai geba prisitaikyti prie sudėtingos situacijos ir ją išnaudoti savo tikslams. Savo nusikalstamos veiklos metodus pritaikė taip, kad šie atitiktų pandemijos kontekstą, pasinaudojo situacijos neapibrėžtumu ir žmonių siekiu gauti patikimą informaciją

Pažymėtina, kad 2020 m., kai daug laiko tiek suaugusieji, tiek vaikai praleido namuose, išaugo vaikų seksualinio išnaudojimo medžiagos apimtys skaitmeninėje erdvėje. Šias pasaulines tendencijas, fiksuojamas tokių institucijų, kaip Interpolas, ataskaitose[79], patvirtina ir Lietuvos interneto karštosios linijos skaičiai: 2020 m. nustatyti 78 atvejai, kai Lietuvos tarnybinėse stotyse aptikta vaikų seksualinio išnaudojimo vaizdų. Šie atvejai buvo perduoti tirti Policijos departamentui (2019 m. nustatyti 44 tokie atvejai).

COVID-19 pandemijos įtaka Lietuvos kriminogeniniams procesams

2020 m. nusikaltėliai veikė gana aktyviai. Pandemijos metu jie sugebėjo pasinaudoti žmonių baimėmis ir abejonėmis. Išnaudodami esamą situaciją, kūrė ir taikė naujus metodus nusikalstamoms veikoms vykdyti. Netrukus po to, kai Lietuvoje, buvo paskelbtas karantinas, nusikaltėliai, apsimetę medikais, pareigūnais, NVSC ar kitų tarnybų pareigūnais, siūlė dezinfekuoti namus, apžiūrėti asmenis ar kambarius ir pan. Karantinui užsitęsus, gyventojams pradėtos siųsti suklastotos bankų SMS žinutės su užkrėstomis nuorodomis, kurias paspaudus nuo sąskaitos būdavo nuskaičiuojami pinigai, melagingais siūlymais buvo viliojama itin pelningai investuoti ar įsigyti „fantastiškų“ prekių. Ir tai tik keletas tokios nusikalstamos veikos pavyzdžių. Tačiau vis tik šis oportunistiškas nusikaltėlių elgesys pandemijos metu neatspindi visos kriminogeninės situacijos Lietuvoje 2020 m.

Lietuvos policija, rengdamasi galimoms situacijoms, susijusioms su pandemija, ir siekdama efektyviai planuoti veiklą[80] ir prioritetus, nuo 2020 m. kovo mėn. vertino besiklostančią situaciją ir analizavo šalyje vykstančius kriminogeninius procesus. Remiantis atlikta grėsmių analize, prognozuota, kad tiek artimiausiu metu, tiek ir ilgalaikėje perspektyvoje gali didėti sukčiavimo atvejų, nes atsiskaitymai, pirkimai ir kt. kelsis į kibernetinę erdvę, o sukčiai bandys tuo pasinaudoti. Tiek oficialiai, tiek neoficialiai platinama informacija apie grėsmes, rekomendacijas ir paslaugas dėl viruso ir karantino gali būti palanki sukčiavimo organizatoriams kurti naujas turto išviliojimo strategijas. Karantino laikotarpiu policija periodiškai platino informacinius pranešimus ir įspėjimus dėl galimų rizikų, teikė rekomendacijas, kaip apsisaugoti nuo nusikalstamų veikų poveikio.

Analizuojant ir vertinant turimus duomenis, 2020 m. nustatyti šie su COVID-19 pandemija tiesiogiai sietini sukčiavimo bei neteisėtos komercinės veiklos kibernetinėje erdvėje atvejai: neteisėta internetinė prekyba apsaugos priemonėmis, melagingi skelbimai dėl pigiau nei vidutinė rinkos

79
Pvz. Interpol, *COVID19 - Child Sexual Exploitation and Abuse threats and trends* https://www.interpol.int/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf

80
Pavyzdžiui, nuo balandžio mėn. policijoje pradėjo veikti reagavimo į C kategorijos pranešimų (tai pranešimai, kai nekyla grėsmė žmogaus sveikatai ar gyvybei) centras. Jame dirbantys pareigūnai rinko pirminę informaciją apie įvykį, teikė policijos įstaigų pajėgų valdymo padaliniams pasiūlymus dėl pajėgų siuntimo į įvykio vietą pagal gaunamus pranešimus, konsultavo ir teikė pagalbą gyventojams (pavyzdžiui, dėl dokumentų pateikimo būdo ir t. t.) nuotoliniu būdu. Į A ir B kategorijos pranešimus (tai pranešimai, kai yra ar gali kilti reali grėsmė žmogaus sveikatai ir gyvybei) policija ir toliau reagavo įprastu būdu.

Į turinį

2020 m. grėsmės Lietuvos informaciniam saugumui išliko tos pačios. Pagrindinis informacinių grėsmių šaltinis išliko Rusijos Federacija bei jos vyriausybės kontroliuojamos žiniasklaidos priemonės, kurių veikla buvo nukreipta Lietuvos, NATO ir ES valstybių visuomenių nuomonei formuoti

kaina parduodamų apsaugos priemonių, klastotų šios kategorijos prekių elektroninė prekyba. Tačiau šie kriminogeniniai reiškiniai buvo epizodiniai ir didelės įtakos nusikaltimų kibernetinėje erdvėje situacijai nepadarė.

Lietuvos policija buvo aktyvi ir vykdydama Kibernetinio saugumo įstatyme nustatytus įpareigojimus. 2020 m. sausio–lapkričio mėn., siekdama kibernetinėje erdvėje užkardyti galimus nusikaltimus, susijusius su 78 galinio tinklo įrenginiais, pateikė nurodymus taikyti priemones, kuriomis šalinamos nusikalstamų veikų kibernetinėje erdvėje priežastys. Dėl 33 atvejų pateiktas nurodymas apriboti viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų teikimą paslaugų gavėjui ir taikyti priemones, kuriomis šalinamos nusikalstamų veikų kibernetinėje erdvėje priežastys.

COVID-19 pandemijos įtaka informacinei aplinkai

Pandemijos sukelta krizė pasaulyje atvėrė naujas galimybes dezinformacijai arba melagingoms naujienoms sklisti. Jos pasižymėjo pražūtingais padariniais: per pirmus tris 2020 m. mėnesius mažiausiai 800 žmonių mirė, o 5 900 buvo paguldyti į ligoninę, kai išgėrė metanolio, patikėję internete paskleistomis melagingomis naujienomis, jog didelė alkoholio koncentracija gali juos apsaugoti ar net išgydyti nuo COVID-19 ligos. 2020 m. balandžio mėn. Didžiosios Britanijos telekomunikacijų prekybos asociacija „Mobile UK“ pranešė, kad buvo sudegintos 77 mobiliojo ryšio bazinės stotys, nes žmonės buvo įtikinti, jog COVID-19 liga paplito dėl šių stočių skleidžiamo 5G ryšio[81].

Situacija Lietuvos informacinėje aplinkoje taip pat buvo įtempta, nes agresoriai skleidė melagingus pranešimus COVID-19 ligos tema. Nuo 2020 m. vasario 1 d. iki birželio mėn. su Lietuva susijusioje informacinėje aplinkoje LK SKD nustatė[82] apie 1 484 informacinius incidentus, susijusius su informacija apie COVID-19 ligą. Palyginti su ankstesnių metų to paties laikotarpio duomenimis, pastebimas ryškus informacijos srauto pakilimas, kuris du tris kartus viršija įprastus informacijos srauto rodiklius. Pandemijos metu ypač „suklestėjo“ sąmokslo teorijų žanras. Nuo vasario 1 d. Lietuvos informacinėje erdvėje pastebėtas tiek trečiųjų šalių, tiek nevalstybinių veikėjų aktyvus įsitraukimas kuriant ir platinant klaidinančio pobūdžio apie COVID-19 ligą informaciją. Karantino metu buvo atremtos trys priešiškos su COVID-19 susijusios informacinės operacijos, nukreiptos prieš Lietuvos kariuomenę, JAV kariuomenę ir NATO. Per Rusijos Federacijos valdomas visuomenės informavimo priemones ir vakarų socialinius tinklus buvo siekiama diskredituoti Lietuvos vadovybės bei ES ir NATO organizacijų pastangas suvaldyti pandemijos padarinius. Daugeliu atvejų informacinės operacijos buvo nukreiptos prieš Lietuvos tautines bendrijas ir socialiai jautrias grupes. Agresoriai teigė, kad Lietuvos Respublikos Vyriausybė nebuvo tinkamai pasiruošusi kovoti su COVID-19 liga ir nesugeba priimti tinkamų sprendimų pandemijos padariniams suvaldyti, todėl kenčia nekalti žmonės. Buvo siekiama nuteikti piliečius prieš valstybės vadovybę skleidžiant nepagrįstą kritiką ir patyčias.

Apibendrinant galima teigti, kad LK SKD atliktos analizės rezultatai leidžia daryti prielaidą, jog Rusijos Federacija Lietuvoje ir pasauliniu mastu pasinaudojo COVID-19 pandemijos sukelta situacija, siekdama šių tikslų: suformuoti teigiamą savo įvaizdį (apginti savo įvaizdį), per Jungtines Tautas panaikinti jai taikomas ES sankcijas, atkurti savo įtaką Europos regione bei sumažinti pasitikėjimą NATO ir ES organizacijų efektyvumu.

81
https://www.businessinsider.com/77-phone-masts-fire-coronavirus-5g-conspiracy-theory-2020-5

82
LK SKD veikla dėl pandemijos metu vykusių pokyčių informacinėje ir fizinėje aplinkoje 2020 m. išskiriama į du pusmečius – I ir II. Sausio–gegužės mėn. buvo vykdoma priešiškos informacinės aplinkos stebėsena, orientuota į COVID-19 pandemijos situaciją, o nuo birželio 1 d. iki gruodžio 31 d. – pagal Lietuvai svarbias strategines sritis (gynybos, kultūros ir švietimo, socialinio saugumo, ekonomikos ir energetikos, konstitucinių pagrindų apsaugos bei užsienio politikos).

Valstybės institucijos ir įstaigos, įvertindamos pandemijos poveikį savo veiklos sričiai ir siekdamos padėti žmonėms, parengė ir paviešino įvairias rekomendacijas, gaires, patarimus, aktyviai diskutavo ir informavo visuomenę apie su pandemija susijusias rizikas visuomenės informavimo priemonėse ir nuotoliniuose renginiuose

Į turinį

NKSC ir kitų valstybės institucijų veiksmai, siekiant padėti žmonėms ir verslui pandemijos metu

Kovo 16 d.

NKSC parengė rekomendaciją „Bazinės kibernetinio saugumo rekomendacijos nuotoliniam darbui“ ir paskelbė ją savo interneto svetainėje

Kovo 23 d.

Lietuvos policija išplatino pirmuosius pranešimus visuomenei, kokiais būdais sukčiai ir vagys pradėjo išnaudoti susidariusią situaciją

Kovo 26 d.

RRT parengė infografiką su rekomendacijomis „Ryšių ištekliai naudokimės taupiai ir atsakingai“

Kovo 27 d.

RRT kartu su elektroninių ryšių paslaugų teikėjais parengė švietimo įstaigoms rekomendacijas ir patarimų infografiką, kaip sklandžiai organizuoti nuotolinio mokymosi procesą ir išvengti elektroninių ryšių tinklų nesklandumų

Kovo 31 d.

RRT operatoriams parengė rekomendacijas dėl elektroninių ryšių paslaugų nenutrūkstamo teikimo užtikrinimo karantino metu

Balandžio 02 d.

Keičiantis kriminogeninės situacijos struktūrai, Lietuvos policija išplatino visuomenei patarimus dėl nusikalstamos / kenkimo veikos kibernetinėje erdvėje

Balandžio 06 d.

VDAI parengė rekomendaciją „Trys žingsniai dėl nuotolinio mokymosi organizavimo“ ir paskelbė ją savo interneto svetainėje

Balandžio 07 d.

Policija pradėjo teikti konsultacijas ir pagalbą gyventojams nuotoliniu būdu

Balandžio 08 d.

RRT kartu su LR švietimo, mokslo ir sporto ministerija ir Nacionaline švietimo agentūra mokytojams parengė rekomendacijas dėl saugumo internete nuotolinių mokymų metu ir išplatinto švietimo įstaigoms

Balandžio 08 d.

RRT tėvams ir globėjams parengė rekomendacijas dėl vaikų saugumo internete ir paskelbė jas savo interneto svetainėje

Balandžio 09 d.

VDAI parengė rekomendaciją „Darbuotojų asmens duomenų tvarkymas, organizuojant darbą nuotoliniu būdu“ ir paskelbė ją savo interneto svetainėje

Balandžio 22 d.

NKSC parengė rekomendaciją „Dėl komunikacijų platformos „Zoom“ saugumo“ ir paskelbė ją savo interneto svetainėje

Gegužės 08 d.

Lietuvos policija „Youtube“ kanale suorganizavo informacinę konferenciją „Ar COVID-19 gali pakeisti įprastą policijos darbą?“

Gegužės 18 d.

VDAI parengė rekomendaciją „Rekomendacijos dėl asmens duomenų apsaugos aspektų, teikiant sveikatos priežiūros paslaugas nuotoliniu būdu“ ir paskelbė ją savo interneto svetainėje

Liepos 07 d.

NKSC parengė rekomendaciją „Slaptažodžių stiprumas, sudėtingumas ir sauga“ ir paskelbė ją savo interneto svetainėje

Liepos 31 d.

NKSC parengė rekomendaciją „Tapatybės vagystės“ ir paskelbė ją savo interneto svetainėje

Rugpjūčio 18 d.

Lietuvos policija parengė radijo stotims įrašus (komentarus) apie populiariausius sukčiavimo būdus elektroninėje erdvėje ir patarimus, kaip apsisaugoti

Rugsėjo 25 d.

Lietuvos policija informavo visuomenę apie plintančius fiktyvių brokerių siūlymus investuoti netikrose finansavimo platformose

Rugsėjo 25 d.

Lietuvos policija įspėjo apie policijos vardu siunčiamus el. laiškus su nuoroda į netikrą policijos interneto svetainę

Spalio 28 d.

NKSC parengė rekomendaciją „Kaip užtikrinti daiktų interneto įrenginių saugumą“ ir paskelbė ją savo interneto svetainėje

Lapkričio 09 d.

Lietuvos policija visuomenę įspėjo apie plintančias apgavystes telefonu – kai neva prisistatant banko tarnautoju bandoma išgauti elektroninės bankininkystės prisijungimo kodus

Lapkričio 11 d.

NKSC parengė rekomendaciją „Telekonferencinių programinių sprendimų apžvalga ir rekomendacijos“ ir paskelbė ją savo interneto svetainėje

Gruodžio 16 d.

Lietuvos policija dalijo gyventojams patarimus apie metų pabaigoje pagausėjusius sukčiavimo atvejus kibernetinėje erdvėje

2021

Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt
2021-04-07. Tiražas 400 egz. Užsakymas Nr. GL-136

Dizaineris Andrej Garbar
Kalbos redaktorė Inga Šorienė
Naudotos iliustracijos iš Freepik.com grafinio archyvo

Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius
Spausdino Lietuvos kariuomenės Karo kartografijos centras,
Muitinės g. 4, Domeikava, LT-54359 Kauno r.

Leidinio bibliografinė informacija pateikiama
Lietuvos nacionalinės Martyno Mažvydo bibliotekos
Nacionalinės bibliografijos duomenų banke (NBDB).

ISBN 978-609-412-214-9

9 786094 122132

NACIONALINĖ KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2020