„Co-funded by the Prevention of and Fight against Crime Programme
of the European Union“

Kibernetinius nusikaltimus tirs greičiau

Pripratome gyventi elektroninių įrenginių apsuptyje ir jie mums tapo tarsi „nematomais“. Bendraujame išmaniaisiais telefonais, naudotis kompiuteriais, planšetėmis, video kameromis ir fotoaparatais, išmaniaisiais televizoriais, vairuoti mums padeda navigacinės sistemos, namus saugo per atstumą valdomos apsaugos sistemos. Mokėjimus galime atlikti internetu arba iš mobiliojo telefono, o video žaidimus labiau įpratę žaisti įprastomis žaidimų konsolėmis.

Net jei visų šių įrenginių neturime patys, jais naudojamės netiesiogiai – visos komunalinių paslaugų sistemos valdomos elektroniniais įrenginiais, pvz., mokėjimo įstaigoje visos operacijos bus atliekamos per kompiuterinę bankinę sistemą, o diagnozę gydytojai nustatinės naudodami įvairius diagnostinius prietaisus, paciento būklė bus stebima į tinklą sujungtų kompiuterių.

Tačiau elektroniniais įrenginiais naudojamasi ir nusikaltimams vykdyti. Apvogti sąskaitą galima įlaužus praktiškai per bet kurį elektroninį prietaisą, nes dažnai pamirštama, kad visi šiuolaikiniai išmanieji prietaisai geba „bendrauti“ tarpusavyje ir veikia kaip atskiras kompiuteris.

Kaip pažymėta IOCTA ataskaitoje, Lietuva patenka tarp didžiausia duomenų praradimo rizika pasižyminčių ES šalių (Šaltinis: IOCTA ataskaita, Europol, 2015). Paprastai siekiama įvairiais būdais prieiti prie finansinių duomenų – nuo mokėjimo kortelių vagysčių, sukčiavimo internete, prisijungimo duomenų užgrobimo ir pan. 2014 m. buvo žinomi kaip duomenų vagysčių metai, nes tais metais ES buvo užvaldyta daugiau 40 milijonų vartotojų duomenų, o vien 2013 m. sukčiavimo, naudojant mokėjimo korteles, ir sukčiavimo internete mastai sudarė 1,44 milijardus eurų ir šie mastai auga maždaug 8 proc. kasmet (*Šaltinis: ten pat*).

Elektroniniais įrenginiais padarytų nusikaltimų, dar vadinamų kibernetiniais, kasmet skaičius sparčiai auga. Kibernetiniai nusikaltimai tampa vis agresyvesni, užslėpti, kai nuostoliai paaiškėja tik po kurio laiko. Keičiasi ir nusikaltėliai – dabar kibernetiniams nusikaltimams vykdyti užtenka turėti bendruosius IT įgūdžius.

Dar viena nauja tendencija: kibernetiniai ir „klasikiniai“ nusikaltimai susilieja, nes nusikaltimams planuoti ir organizuoti, pėdsakams paslėpti ir pan. naudojami elektroniniai įrenginiai, t.y. tie patys kasdienio naudojimo išmanieji įrenginiai, tokie kaip mobilieji telefonai, kompiuteriai, planšetės ar net žaidimų konsolės. Tuo tarpu nusikaltimui elektroninėje erdvėje nustatyti, įkalčiams surinkti ir nusikaltimams įrodyti teisme reikia specialių žinių ir gebėjimų.

Todėl ir Lietuvos teisėsauga turi prisitaikyti prie įvykusių technologinių ir socialinio gyvenimo pokyčių bei įgyti naujas kompetencijas kibernetiniams nusikaltimams tirti.

Be to, netgi fizinių nusikaltimų atvejais dažnai galima rasti mobilųjį telefoną, o sukčiavimas, klastojimas, kontrabandos organizavimas beveik neįsivaizduojami be kompiuterių ar interneto naudojimo.

Tiriant tiek fizinius, tiek kibernetinius nusikaltimus informacijos bus ieškoma ir elektroniniuose įrenginiuose, pvz., įtariamojo ar aukos mobiliajame telefone, kompiuteryje, spausdintuve, GPS navigatoriuje, automobilio elektroninėje valdymo sistemoje, bus tikrinamas susirašinėjimas elektroniniu paštu, internetiniai ar Skype pokalbiai, tikrinami atsisiųsti failai, Facebook paskyra, naršymo internete istorija, tikrinami debesų kompiuterijoje saugomi duomenys, pirkimai internetu, visi kontaktai, su kuriais buvo komunikuota per bet kurį elektroninį įrenginį. Jau yra kriminalistinių įrankių, leidžiančių atstatyti iš elektroninių įrenginių pašalintus duomenis.

Todėl atliekant kratą, nusikaltimo vietos apžiūrą ar ieškant tyrimui svarbios informacijos dažnai tenka surinkti visus elektroninius įrenginius, kuriuose galėtų būti tyrimui aktualios informacijos.

Atsiradus didelės talpos išorinės atminties laikmenoms vis dažniau informacija saugoma būtent jose, o ne tik standžiajame diske ar paties elektroninio įrenginio atmintyje. Tuo tarpu išorinės atminties laikmenos gali būti labai įvairių formų, jas lengva paslėpti kituose daiktuose. Išorinės laikmenos gali atrodyti ir taip:

Dar ne visi pareigūnai žino labiausiai paplitusias išorinių laikmenų formas, todėl dalis potencialių įkalčių, kuriuose yra skaitmeninė informacija, nėra surenkami, arba atvirkščiai, dažnai surenkama perteklinė technika, įrenginiai, kuriuos tenka suregistruoti, saugoti ir tirti, nors ne visuose bus reikalingos informacijos. Sudėtinga logistika, brangus sandėliavimas ir ištyrimas reikalauja papildomų išteklių – lėšų, patalpų, kompetentingų pareigūnų ir atitinkamos technikos. Visa tai apsunkina bendrą teisėsaugos institucijų darbą, o tyrimai trunka ilgai.

Arba susiduriama su kitu kraštutinumu, pvz., ne visada analizuojami įvykio vietos tinklai, jų prieigos bei juose aptinkama informacija, ne visuomet surenkama informacija iš periferinių įrenginių ar bendros infrastruktūros kompiuterizuotų sistemų, o įvykio vietoje dažniausiai nėra atliekami gyvos sistemos analizės veiksmai, dėl to prarandama dalis informacijos ir įkalčių.

Šioms problemoms spręsti Lietuvos teisėsaugai buvo parengta sertifikavimo programa „Elektroninių objektų surinkimas“. Ši programa yra skirta operatyvinių grupių pareigūnams, ikiteisminį tyrimą atliekantiems kriminalinės policijos pareigūnams, kriminalistinių tyrimų specialistams, dalyvaujantiems atliekant įvykių vietų tyrimus ir apžiūras, kurie savo veikloje dažnai susiduria su problemomis įvykio vietose surinkdami elektroninius objektus, apmokyti.

Pagal sertifikavimo programą „Elektroninių objektų surinkimas“ 2015 m. jau įvyko pilotiniai mokymai teisėsaugos pareigūnams – iš anksto paruoštoje klasėje buvo atliekama kratos simuliacija bei elektroninių objektų surinkimas (krata, fotografavimas, objektų surinkimas, protokolavimas, fotolentelės sudarymas ir pan.). Po praktinių mokymų buvo atliekama vykusios kratos simuliacijos apžvalga bei aptariamos probleminės situacijos, su kuriomis susidurta renkant elektroninius objektus.

„Tokių mokymų poreikis Lietuvoje yra didžiulis, nes augant nusikaltimų elektroninėje erdvėje skaičiui, tinkamai surinkti elektroninius objektus turi mokėti visi tyrėjai ar operatyviniai darbuotojai, vykstantys į įvykio vietas ar dalyvaujantys kituose procesiniuose veiksmuose, kurių metu gali būti paimami elektroniniai

objektai”, - pažymi Sergej Boldyrev, Vilniaus apskrities Vyriausiojo policijos komisariato ekspertas ir dėstytojas.

Surinkus elektroninius objektus toliau atliekama jų detali analizė, ieškant nusikalstamos veikos įrodymų ar susijusios informacijos. Paprastai didžiausias dėmesys skiriamas populiariausios Windows grupės operacinių sistemų (toliau – OS) analizei (Windows 7, XP, 8, 8.1, Vista), kurios KasperskyLab duomenimis 2014 m. sudarė 98,88 proc. visų naudotų operacinių sistemų.

Kaip atlikti tokią analizę Lietuvos teisėsaugos pareigūnai bus mokomi pagal kitą parengtą sertifikavimo programą „Windows artefaktai“ , kuri leis per ženkliai trumpesnį laikotarpį apmokyti ir parengti kvalifikuotus ekspertus ir specialistus, galinčius atlikti Windows OS artefaktų analizę. Gausios procesinių veiksmų iliustracijos padeda išmokti tinkamai atlikti Windows artefaktų analizę.

Abi sertifikavimo (mokymų) programos buvo parengtos panaudojant Ispanijos S21SEC, kibernetinio saugumo paslaugų teikimo ir technologijų vystymo srityje dirbančio instituto sertifikavimo programas „Elektroninių objektų surinkimas“ ir “Windows artefaktų analizė”, jas lokalizavus ir pritaikius Lietuvos teisėsaugos poreikiams bei Lietuvoje atliekamiems IT tyrimams. Programų parengimą ir pilotinių mokymų organizavimą finansavo Europos Komisija pagal įgyvendinamą Prevencijos ir kovos su nusikaltimais 2007-2013 m. programos (Prevention of and fight against crime 2007-2013, ISEC) finansuojamą projektą „Lietuvos kibernetinių nusikaltimų kompetencijų ir tyrimų centras“.

Parengtos programos leis Lietuvos teisėsaugai greičiau ištirti elektroniniais įrenginiais padarytus nusikaltimus, tačiau lengviau būtų laikytis paprastų kibernetinio saugumo patarimų.

10 kibernetinio saugumo patarimų:

1. Nesusigundykite pernelyg patraukliais pasiūlymais įsigyti prekes ar paslaugas – tai per daug gerai, kad būtų tiesa.
2. Saugokite savo debetines ir kreditines korteles taip, kaip saugotumėte grynus pinigus, nelaikykite kartu užrašytų PIN kodų ar slaptažodžių.
3. Visus elektroninius laiškus, kuriuose prašoma jūsų asmeninių duomenų, laikykite įtartinais.
4. Apsaugokite savo kompiuterius, planšetes ir išmaniuosius telefonus sudėtingais slaptažodžiais – geriau raidžių, skaičių ir simbolių deriniu, ir naudokite antivirusines ir prieš-šnipinėjimo programas.
5. Apsaugokite savo mobiliuosius prietaisus, kai naudojatės Wi-Fi viešosiose vietose – neapsaugoti asmeniniai ar kiti svarbūs duomenys gali būti atsisiųsti be jūsų žinios.
6. Pirkite internetu tik iš patikimų šaltinių ir naudokite interneto saugumo protokolą, vadinamą 3D Secure, kurio patikimumą garantuoja Visa/SecureCode/SafeKey. Apie jį teiraukitės savo banke ar mokėjimo kortelę išdavusioje institucijoje.
7. Reguliariai tikrinkite savo mokėjimo kortelių išklotines – tai leis greitai nustatyti neautorizuotus nuskaitymus.
8. Naršydami internete naudokite HTTPS ar SSL protokolus – tai galite nustatyti pagal simbolius, esančius naršyklės URL juostoje.
9. Būkite apdairūs ir niekada neatsakykite į elektroninius laiškus, kuriuose prašome pateikti jūsų asmeninius duomenis arba kuriuose pateikiami pasiūlymai neteisėtai užsidirbti „lengvų pinigų“.
10. Siųskitės failus ar programinę įrangą tik iš patikimų šaltinių.

Ir visuomet saugokite savo išmanųjį telefoną – šiuolaikinį „raktą“ ir „piniginę“ kartu.