

Šioje vietoje demonstracijos
metu rodomas VPK logotipas

KIBERNETINĖS ERDVĖS SAUGUMAS – DABARTIS IR ATEITIS

Vilniaus apskrities vyriausiojo policijos komisariato
viršininko pavaduotojas Antoni Mikulskis
2014 m. balandžio 30 d.



I. ELEKTRONINĖ ERDVĖ IR JOS PAVOJAI



INFORMACINIŲ TECHNOLOGIJŲ (IT) NAUDOJIMAS KASDIENIAME GYVENIME

- naršyti internete
 - keistis failais
 - naudotis elektroniniu paštu
 - bendrauti ir susirašinėti socialiniuose tinkluose
 - prisijungti prie banko sistemų
 - atlikti finansines operacijas ir kt.

Informacinių technologijų naudojimas kasdieniame gyvenime apdorojant didėjančius informacijos srautus vis labiau daro įtaką jo kokybei, todėl svarbu apsaugoti informaciją nuo sunaikinimo, sugadinimo ar kitokio pakeitimo.



TAMSIOJI IT PANAUDOJIMO PUSĖ

Kompiuteriai vis dažniau tampa ne tik teisėtos veiklos, bet ir nusikaltimų, vykdomų vien elektroninėje erdvėje, įrankiais :

- nelegali prekyba;
- neapykantos skatinimas ar kurstymas;
- šmeižtas;
- sukčiavimas internete;
- asmens duomenų vagystės ir su tuo susiję nusikaltimai;
- vaikų seksualinis išnaudojimas;
- įsilaužimai į sistemas;
- draudžiamo turinio platinimas;
- autorių teisių pažeidimai ir kt.

Kibernetinė erdvė naudojama ir kaip klasikinių nusikaltimų pagalbinė priemonė:

- informacijos apie žudymo įrankius paieškai;
- informacijos mainai tarp teroristinių grupuočių;
- nusikaltimų planavimui bei kt.



GRESMĖS ELEKTRONINĖJE ERDVĖJE

- Didelės apimties kibernetinės atakos prieš informacines sistemas.

- Užkrėstų ir valdomų kompiuterių tinklų (botnet) atakos.

Šios atakos vis labiau koordinuojamos, yra sisteminio pobūdžio, asmenis, rengiančius šias atakas, sieja pastovūs tarpusavio ryšiai bei pasiskirstymas vaidmenimis ar užduotimis. Šios atakos yra susijusios su organizuotu nusikalstamumu.

- Nusikalstamos veikos, padaromos panaudojant kompiuterio virusus, t. y. užkrečiant asmenų, įmonių ir organizacijų kompiuterius, kurie nepakankamai dėmesio skiria kompiuterinės informacijos saugai, naudoja nelegalią programinę įrangą, laiku neatnaujina turimos legalios programinės įrangos bei antivirusinės programinės įrangos ir ugniasienių.



KAS VYKSTA TOLIAU?

Užkrėtus kompiuterius kenkėjiška programine įranga, vėliau juos stengiamasi panaudoti:

- **finansinei naudai gauti** (pinigų vagystės iš internetinės bankininkystės sąskaitų, virtualių pinigų vagystės (Webmoney, Bitcoin), turto prievartavimas ir įvairūs sukčiavimai, nusikaltimo padarymas internete už pinigus kaip paslauga, informacijos vagystės ir prekyba ja, kt.);
- **komerciniam šnipinėjimui** (siekiant sužlugdyti konkurentus, rinkti juos kompromituojančią informaciją, pavogti intelektualinę nuosavybę, perimti apmokėjimus už prekes ir pan.);
- **politiniam šnipinėjimui** (siekiant perimti neviešo pobūdžio „jautrią“ informaciją, valstybės paslaptis, kompromituojančią informaciją, infiltruotis į kritines infrastruktūras ir kt.);
- **asmens duomenų vagystėms** (prisijungimo duomenų prie įvairių sistemų, bazių, socialinių tinklų išgavimui, kompromitavimui, neteisėtam naudojimuisi);
- **informaciniam karams ir kibernetinėms atakoms** (2007 m. atakos prieš Estiją, 2013 m. Šiaurės Korėjos atakos prieš pietų Korėjos IT infrastruktūrą, Ddos atakos ir neviešo pobūdžio pokalbių paviešinimas Lietuvoje).



BENDRAVIMAS SOCIALINIUOSE TINKLAPIUOSE. PAVOJAI

- Elektroninė erdvė naudojama bendrauti ir susirašinėti tarpusavyje, taip pat ir socialiniuose tinkluose. Tačiau neretas atvejis, kai šiuose tinkluose sutinkama neigiamo poveikio informacija.
- Didelė problema – netinkamas elgesys internete, tyčiniai veiksmai, kurie nukreipti pažeminti, įbauginti, kontroliuoti, manipuliuoti, įžeisti, melagingai diskredituoti asmenį. Tai veiksmai, kuriais siekiama kitaip pakenkti arba varžyti kitą asmenį ir interneto turinys, kuris yra žalingas piliečiams, įskaitant vaikus.
- Socialiniai tinklai taip pat yra priemonė, kurią nusikaltėliai naudoja seksualiai išnaudojamiems vaikams surasti, pokalbiams su vaikais „nevaikiškomis“ temomis, rinkti medžiagą, kuri vėliau panaudojama patyčioms ir įbauginimui, sudaryti sau galimybę kontroliuoti vaiką.



INTERNETINĖ PREKYBA

- Internete intensyviai vyksta prekyba ***padirbtais vaistais ir plataus vartojimo prekėmis***
- Daroma žala visuomenės sveikatai, klaidinami pacientai ir vartotojai.
- Vietiniu lygmeniu kovoti su šiomis grėsmėmis nebepakanka.
- Būtinai kovos su šiais reiškiniais veiksmų geresnis koordinavimas bei bendradarbiavimas tarptautiniu lygiu.



VAIKŲ SEKSUALINIS IŠNAUDOJIMAS INTERNETE

- Internetas – keitimosi vaikų seksualinio išnaudojimo failais priemonė;
- Internetas – priemonė, kurią nusikaltėliai naudoja seksualiai išnaudojamiems vaikams surasti;
- Internetas – nusikaltėlių paieškos ir įrodymų rinkimo priemonė;
- Informacijos gavimas iš užsienio šalių Interneto paslaugų tiekėjų.



INTERNETINĖS PAŽINTYS

Grėsmės susipažinti internete su linkusiais daryti nusikaltimus, neretai labai sunkius, asmenimis.

Pavyzdys> paminėtinas Smurtinių nusikaltimų tyrimo skyriuje atliktas ikiteisminis tyrimas, kuomet miško masyve, prie Nemenčinės plento, Vilniuje, buvo rastas mažametės lavonas su smurto žymėmis veide ir smaugimo žymėmis kakle.

Tyrimo metu nustatyta, jog mažametė su įtariamuoju susipažino internetiniame tinklapyje *Facebook*, po to bendravo internetinėje svetainėje *Skype* pagalba.



II. ELEKTRONINIŲ NUSIKALTIMŲ TYRIMAS



LIETUVOS RESPUBLIKOS BAUDŽIAMASIS KODEKSAS

Lietuvos Respublikos (toliau – LR) baudžiamajame kodekse (toliau – BK) išskirti šie nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui:

- neteisėtas poveikis elektroniniams duomenims (LR BK 196 straipsnis);
- neteisėtas poveikis informacinei sistemai (LR BK 197 straipsnis);
- neteisėtas elektroninių duomenų perėmimas ir panaudojimas (LR BK 198 straipsnis), neteisėtas prisijungimas prie informacinės sistemos (LR BK 198(1) straipsnis);
- neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis (LR BK 198(2) straipsnis).



Ne visos nusikalstamos veikos, kurios gali būti padarytos pasitelkiant informacines technologijas, yra nusikalstamos veikos, padarytos elektroninėje erdvėje.

Vieni iš dažniausiai pasitaikančių nusikaltimų naudojant informacines technologijas yra:

- ✓ šmeižiančio (LR BK 154 str. 2d.);
- ✓ įžeidžiančio (LR BK 155 str. 1d.) turinio komentary ar informacijos talpinimas;
- ✓ neapykantos skatinimas ar kurstymas diskriminuoti žmonių grupę ar jai priklausančią asmenį dėl lyties, seksualinės orientacijos, rasės, tautybės (LR BK 170 str.) paviešinant informaciją internete;
- ✓ vaiko išnaudojimas pornografijai (LR BK 162 str.);
- ✓ disponavimas pornografinio turinio dalykais (LR BK str. 309 straipsnis);
- ✓ sukčiavimai (LR BK 182 straipsnis);
- ✓ disponavimas elektronine mokėjimo priemone arba jos duomenimis (LR BK 214 straipsnis);
- ✓ neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas (LR BK 215 straipsnis);
- ✓ nusikaltimai intelektinei ir pramonei nuosavybei (XXIX skyrius), kiti nusikaltimai.

Labai didelis tokių nusikalstamų veikų latentiškumas.

- ✓ Fiziniai ir juridiniai asmenys, prieš kuriuos padarytos nusikalstamos veikos, dažnai nesikreipia į teisėsaugos institucijas dėl šių veikų, siekdami nesugadinti savo reputacijos, nenorėdami viešinti informacijos dėl spragų informacinėse sistemose bei informacinių sistemų apsaugos priemonėse.
- ✓ Kartais šie asmenys nežino, kad prieš juos padaryta ar daroma nusikalstama veika, arba to nesuvokia (pvz.: LR BK 198(1) straipsnis. Neteisėtas prisijungimas prie informacinės sistemos, LR BK 198(2) straipsnis. Neteisėtas disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis). Taip pat reikia atkreipti dėmesį, kad dažnai neteisėtingai kvalifikuojamos tokios nusikalstamos veikos ir tyrimai pradėti pagal LR BK 182 straipsnis (sukčiavimas), LR BK 215 str. (neteisėtas elektroninės mokėjimo priemonės ar jos duomenų panaudojimas).



ĮRODINĖJIMO PROBLEMATIKA

- ✓ Nusikalstamas veikas darantys asmenys išnaudoja technologinę pažangą savo kėslams.
- ✓ Kiekvieną kartą atliekant ikiteisminius tyrimus, susiduriama su naujais ir išradingesniais būdais nuslėpti nusikalstamas veikas, sunaikinti šių veikų pėdsakus, tyrimui reikšmingus daiktus, dokumentus ir įrodymus.
- ✓ Tiriant nusikaltimą, vis dažniau tenka aiškintis dėl kompiuterinėje erdvėje paliktų pėdsakų arba remtis vien tik jais. Tyrimų procesą galima apibrėžti kaip įkalčių identifikavimą, surinkimą, išsaugojimą, analizę bei analizės išvadų parengimą.

Procesą apsunkina:

- ✓ *Tarptautinis Interneto pobūdis* (problemos gaunant duomenis iš užsienio šalių Interneto paslaugų tiekėjų).
- ✓ *Galimybės likti anonimiškam.*
- ✓ *Įrodymų rinkimas ir fiksavimas* (pvz.: duomenys apie IP adresus pas Interneto paslaugų tiekėjus saugomi 6 mėn., greitai galima pašalinti įrodymus, reikšmingą informaciją).
- ✓ *Duomenų gavimą apsunkinančių veiksmų naudojimas* (BULLETPROOF HOSTING, sisteminių įrašų nebuvimas, netikrų tapatybės duomenų naudojimas).
- ✓ *Failų šifravimas.*
- ✓ *Slaptažodžių ir informacijos, susijusios su įtariamaisiais, paieška Internete.*
- ✓ *Aktyvus tarptautinis bendradarbiavimas.*
- ✓ *Failų šalinimas.*
- ✓ *Debesų kompiuterija.* Ji pastaruoju metu sparčiai tobulėja. Debesų kompiuterijoje visi vartotojo duomenys ir jam reikalingos programos yra kažkur kitur, šių paslaugų teikėjo kompiuteriuose, dažniausiai ne Lietuvos Respublikos teritorijoje. Paties vartotojo kompiuteris turi tik minimalų programinės įrangos kiekį – operacinę sistemą ir interneto naršyklę. Visi kiti ištekliai gaunami iš „debesies“ interneto linijomis. Tokiu atveju, jei nusikaltimui įvykdyti būtų panaudoti Debesų kompiuterijos resursai, nebūtų galimybės išimti kompiuterių tyrimui, kadangi vartotojo kompiuteris yra tik prieiga prie jo resursų, o Debesies paslaugų teikėjo skaičiavimo centre saugomi duomenys daugybės, tarpusavyje nesusijusių, vartotojų.



TYRIMŲ SPECIFIKA IR SUDĖTINGUMAS

- Dažnai pasitaiko, kad nusikalstama veika padaroma iš kitos valstybės (dažniausiai JAV, Airija, Didžioji Britanija ar Norvegija) teritorijoje esančio kompiuterio ir ten gyvenančio jo naudotojo.
- Nustačius šiuos duomenis, siunčiamas teisinės pagalbos prašymas kitai valstybei dėl duomenų pateikimo. Toks susirašinėjimas yra ilgas ir ne visada duodantis teigiamų rezultatų.
- Kai kuriose šalyse net ir nustačius IP adreso vartotoją, baudžiamasis persekiojimas tampa neįmanomas, nes toje šalyje pagal galiojančius įstatymus ši veika yra nebaudžiama ir duomenys apie IP naudotoją nepateikiami. Generalinės prokuratūros 2009-12-23 *Metodinės rekomendacijos Nr. 12.14-40 „Dėl nusikalstamų veikų, padarytų rasiniais, nacionalistiniais, ksenofobiniais, homofobiniais ar kitais diskriminacinio pobūdžio motyvais, ikiteisminio tyrimo organizavimo, vadovavimo jam ir atlikimo ypatumų“* numato, kad tokiais atvejais ikiteisminio tyrimo pareigūnas ar prokuroras turėtų teisės aktuose nustatyta tvarka raštu išreikalauti iš ikiteisminio tyrimo įstaigos ar prokuratūros (prokuroro) analogiškos nusikalstamos veikos ikiteisminio tyrimo atveju gautų dokumentų, kurie patvirtintų aukščiau paminėtas aplinkybes, kas supaprastintų ikiteisminio tyrimo atlikimą.
- Kitais atvejais šalys duomenų pateikti negali, nes praeina laikas, numatytas informacijai apie IP naudotoją saugoti. Būtina svarstyti apie galimybę tokius duomenis gauti be teisinės pagalbos prašymo siuntimo užsienio valstybėms., pvz. : pasinaudojant LR baudžiamojo proceso kodekso 155 str. numatyta galimybe gauti informaciją siunčiant prašymą tiesiogiai įmonei, administruojančiai atitinkamą IP adresą.
- Internetinėje erdvėje atsirado galimybė keisti IP adresą ir tokiais atvejais yra visiškai neįmanoma susekti šio IP adreso vartotojo.
- Ilgas paskirtų informacinių technologijų tyrimų atlikimo terminas – iki 2 metų.
- Ribotos techninės galimybės, nes kasdien atsiranda įvairios piratinės programos, kurių pagalba keičiami IP adresai, jie užkrečiami virusu.
- Specialistų trūkumas ir nepakankamas tyrėjų, atliekančių ikiteisminius tyrimus dėl elektroninėje erdvėje padarytų nusikaltimų, mokymų organizavimas (arba jų organizavimas užsienio kalba).
- Nepakankama prevencinė politika, pavyzdžiui neįprastai didelis informacijos srautas kompiuteryje gali byloti apie jo apkrovą ir leidžia daryti prielaidą, kad galbūt vykdomi neteisėti procesai, tačiau į tai laiku nekreipiamas tinkamas dėmesys ir nereaguojama.



IKITEISMINIŲ TYRIMŲ SĖKMĘ LEMIA

- Tinkamas pirminių neatidėliotinių tyrimo veiksmų parinkimas ir atlikimas bei šioje srityje turimi darbo įgūdžiai, glaudus bendradarbiavimas su specialistais, laiku ir operatyviai nustatytas IP.

Pavyzdys>internetiniame tinklalapyje www.delfi.lt. po straipsniu „Mano istorija: eitynės Vilniuje pasitiko vaivorykštėmis ir įžeidimu“, pasivadinęs slapyvardžiu „Surikas“ parašė komentarą, kuriuo viešai kurstė smurtauti, fiziškai susidoroti su žmonių grupe ar jai priklausančiu asmeniu dėl seksualinės orientacijos.

Buvo nustatyta, kad IP adresas priklausė didelei statybų bendrovei, kuri vienu išoriniu IP adresu yra registravusi virš 10 vidinių IP adresų; geranoriškas bendradarbiavimas su bendrovės atstovu, šiuo atveju Informacinių technologijų skyriaus vadovu – t. y. tinkamas pasirengimas jo apklausai ir kokybiškas jos atlikimas, kurios metu buvo nustatytos ikiteisminiam tyrimui labai svarbios aplinkybės ir tuoj pat po apklausos, pastarajam sutikus ir jam dalyvaujant, atliktas pagrindinis tyrimo veiksmas – 8 kompiuterių apžiūros, kurių vartotojai prisijungdavo prie internetinio tinklo vienu IP adresu. Šios apžiūros metu buvo nustatytas kompiuteris, iš kurio buvo parašytas minėtas komentaras, po to buvo nustatytas ir jį parašęs asmuo.



IKITEISMINIŲ TYRIMŲ SĖKMĘ LEMIA

Nusikaltimo padarymo mechanizmo nustatymas, tinkamai pasirinkta tyrimo kryptis.

Pavyzdys> sėkmingai Vilniaus aps. VPK NTV Nusikaltimų nuosavybei tyrimo skyriaus Operatyviniame poskyryje atliekamas ikiteisminis tyrimas dėl nusikalstamų veikų, numatytų LR BK 182 str. 2 d., 214 str. 1 d. ir 215 str. 1 d., įvykdymo.

- Atliekant ikiteisminį tyrimą, buvo nustatyta, kad Lietuvos Respublikoje veikia asmenys, kurie neteisėtai užvaldę elektroninių mokėjimo priemonių duomenis, įsigyja Danijos, Vokietijos ir kitų šalių interneto parduotuvėse vertingas elektronikos prekes interneto svetainėse įsidarbinusių kurjeriais asmenų vardu. Vėliau tie patys asmenys, organizuoja šių prekių gabenimą į Lietuvą, kur jos yra realizuojamos. Siuntiniai su prekėmis siunčiami asocialių asmenų arba asmenų, kurių tapatybę patvirtinantys dokumentai buvo prarasti, vardu.
- Tyrimo metu buvo nustatyta, kad nusikaltėliai naudojami duomenų bazė, kuri, reikalui esant, perkeliama iš vienos interneto svetainės į kitą. Duomenų bazę administruoja vienas asmuo, kuris suteikia prisijungimo vardus ir slaptažodžius kitiems nusikalstamos schemos dalyviams. Jie savo ruožtu skirstomi į 2 grupes: 1) „stuffers“ – asmenys, kurie yra atsakingi už vertingų prekių įgijimą interneto parduotuvėse panaudojant svetimų elektroninių mokėjimo priemonių duomenis ir 2) „buyers“ – asmenys, kurie yra atsakingi už prekių persiuntimą ir realizavimą.
- Tyrimo metu buvo nustatyta, kad Lietuvoje su minėta duomenų bazė dirbo mažiausiai 3 asmenys, kurie buvo atsakingi už atsiųstų prekių atsiėmimą ir realizavimą. Dviem iš jų šiuo metu pareikštas įtarimas dėl aukščiau minėtų nusikaltimų padarymo, dar vieno asmens duomenys šiuo metu nustatinėjami. Visi jie veikė vienoje organizuotoje grupėje. Šio ikiteisminio tyrimo metu buvo nustatyta ir kita šios nusikalstamos grupės nusikaltimų darymo kryptis, kai įvairių pasaulio šalių piliečiams per specialiai šiems nusikaltimams daryti sukurtus internetinius puslapius buvo siūloma pirkti lėktuvų skrydžių bilietus, tačiau pirkėjai jų negaudavo. Per „Western Union“ pinigų pervedimo sistemą šių sukčiavimų metu išvilioti pinigai buvo išgryninami Lietuvos bankomatuose.

Kitas pavyzdys> Vilniaus aps. VPK NTV Ekonominių nusikaltimų tyrimo skyriuje buvo atliktas ikiteisminis tyrimas dėl to, kad įtariamas asmuo, įgydamas kito asmens atidarytos sąskaitos internetinės bankininkystės vartotojo identifikavimo duomenis, t. y. elektroninės mokėjimo priemonės naudotojo tapatybės patvirtinimo priemonių duomenis (vartotojo ID, identifikavimo kodų kortelę ir slaptažodį), kompiuteriu pateikęs melagingus duomenis, užsiregistravo internetiniame tinklapyje www.smscredit.lt ir paėmė 950 Lt kreditą. Tokių epizodų byloje yra penki, t. y. byloje 5 nukentėjusieji. Nusikalstamos veikos padarymo schema ta pati, t. y. prisijungiama prie el. bankininkystės, sukūrus elektroninį puslapį, identišką AB „SEB“ banko el. bankininkystės puslapiui ir jį su virusu patalpinus į nukentėjusiųjų kompiuterius, paimamas greitis kreditas, o pinigai išgryninami. Nukentėjusysis galvodamas, kad naudojami tikro banko el. bankininkyste, įvesdavo visus savo el. bankininkystės kodus. Tačiau ikiteisminio tyrimo metu nei vienas iš nukentėjusiųjų neprisipažino, kad pats įvedė savo kodus, todėl nebuvo įrodyta, kad buvo sukurtas el. bankininkystės puslapio antrininkas.



TYRĖJŲ KOMPETENCIJOS KLAUSIMAS

- nagrinėjimų objektų specifikos suvokimas (pėdsakai skirtingose operacinėse sistemose, viešojoje erdvėje (pvz., socialiniuose tinkluose, komentaruose naujienų portaluose), tinklo įrenginiuose, mobiliuosiuose prietaisuose ir kt.) bei gebėjimas juos tinkamai nagrinėti;
- įstatymų, reglamentuojančių bendruosius nusikaltimų tyrimo procesus, greitai besikeičiančius bei kuriamus teisinius dokumentus elektroninei erdvei reglamentuoti, išmanymas;
- gebėjimas vertinti skirtingas rizikas (pvz., kas turės didesnės neigiamos įtakos kompanijai : teisėsaugos organų įtraukimas į tyrimą ir informacijos, kad organizacijos informacijos saugos sistema buvo pažeista, pavišimas ar tyrimo vykdymas savo jėgomis bei nuostolių kompensavimas).



TYRĖJŲ KOMPETENCIJA

Nusikaltimų elektroninėje erdvėje tyrimo įrankiai ir metodikos lėmė vis didėjančius reikalavimus besiformuojančiam profesionalių nusikaltimų elektroninėje erdvėje tyrėjų sluoksniui.

Tačiau ir nusikaltėliai tapo atsargesni, jiems tapo žinoma, jog jų veiksmai gali būti sekami, o palikti pėdsakai - panaudoti teisme.

Paskutinės tendencijos rodo, jog nusikaltėliai, anksčiau ignoravę šią grėsmę arba apie ją tiesiog nežinoję, imasi priemonių, siekdami apsunkinti nusikaltimų tyrėjų darbą: taiko duomenų šifravimo metodikas, naudoja automatizuotas įkalčių naikinimo priemones bei vengia tiesiogiai naudoti savo kompiuterius nusikaltimams vykdyti.

Todėl asmenims, tiriantiems šias nusikalstamas veikas, reikalingas nuolatinis žinių ir techninės bazės atnaujinimas.

Ypatingas dėmesys turi būti skiriamas:

- materialinės-techninės bazės sukūrimui;
- tinkamam ir racionaliam žmogiškųjų resursų panaudojimui;
- mokslo pasiekimų įdiegimui ir tyrėjų praktinių įgūdžių lavinimui.



DĖKOJU UŽ DĖMĖSĮ!