CYBERCRIME EXIT

OPAS KYBERRIKOSTEN SOVITTELUUN

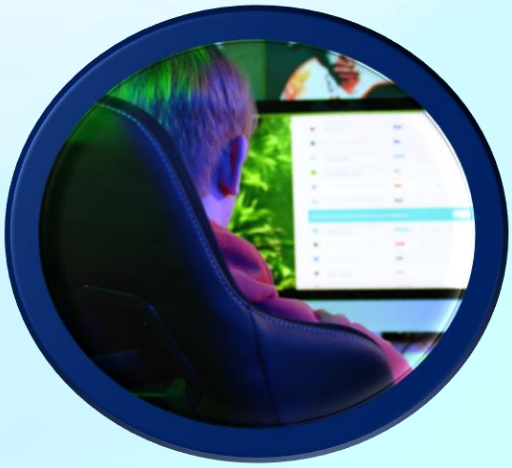
Euroopan unionin osarahoittama

2024

SISÄLLYS

1 KYBERRIKOKSET

Tämä opas käsittelee nuorten tekemiä kyberrikoksia sekä niiden sovittelua. Kyberrikokset ovat tietoverkkoja ja tietojärjestelmiä hyödyntäen tehtyjä sekä niihin kohdistuvia rikoksia.



Tutkimustiedon mukaan, nuorten kyberrikosten määrä on nousussa ja yhä nuoremmat voivat syyllistyä esimerkiksi tietomurtoon ajattelematta sen vakaviakin seurauksia. Rikoksentekovälineet kehittyvät ja ovat yhä useampien saatavilla, eikä rikosten tekeminen välttämättä vaadi merkittävää tietoteknistä osaamista. Tunnusomaista kyberrikoksille on, että ne toimivat usein valmistelevina tai liitännäisrikoksina erilaisille muille rikoksille.

1.1 MIKSI NUORET TEKEVÄT KYBERRIKOKSIA?

Kuten monessa muussa rikostyypissä, myös kyberrikosten taustalla vaikuttavat tekijän nuoren iän tuoma kokemattomuus, joka osaltaan vähentää ymmärrystä laillisten ja laittomien toimien välillä. Nuoret ovat taitavia tietoverkkojen käyttäjiä ja kiinnostus tekniikasta voi tempaista mukanaan. Teon taustalla voi vaikuttaa myös halu saada mainetta tekemällä jotain, mitä ei saisi. Uteliaisuus lisää riskiä kokeilla laittomia polkuja, sillä riski jäädä kiinni koetaan pieneksi.

Poliisi huomioi rikosten ennalta estämisen ja selvittämisen sekä syyteharkintaan saattamisen lisäksi rikosasioiden sovittelun mahdollisuuden. Sovittelun voi huomioida kaikissa rikosasioissa, eikä se ole tiettyjä poikkeuksia lukuun ottamatta rikoslaji- tai rikosnimikesidonnainen.

Haittaohjelma
Haittaohjelmalla aiheutetaan tarkoituksellisesti ei-toivottu tapahtuma tietojärjestelmään tai sen osaan. Voidaan pyrkiä esim. purkamaan suojauksia tai kalastella salasanoja. Tällaisia ovat mm. virukset, madot, troijalaiset tai näiden yhdistelmät.

Hakkeri
Henkilö, joka on taitava käyttämään tietotekniikkaa ja omaa luovaa ongelmanratkaisutaitoa tietoteknisissä haasteissa. Hakkeri voi käyttää taitojaan esim. internetin turvallisuuden lisäämiseen. Taitoja voi käyttää myös rikollisesti esim. tunkeutumalla suojattuun järjestelmään.

2 SOVITTELU

Rikosasioiden sovittelu on lailla säädetty, vapaaehtoisuuteen perustuva oikeusjärjestelmälle rinnakkainen tai sitä täydentävä menettelytapa. Suomessa sovittelu nojaa ihmis- ja perusoikeuksiin sekä restoratiivisen eli korjaavan oikeuden arvoihin ja periaatteisiin. Korjaavan oikeuden menettelyyn lukeutuvat kaikki luovat ongelmanratkaisumallit.

Rauhanomainen keskustelu rikosta koskettaneiden osapuolten sekä ulkopuolisen sovittelijan kesken.

Suuri merkitys etenkin nuorten rikosasioissa.

Sovittelun hyödyt:

- ✓ Turvallinen paikka, jossa on tilaa avoimelle vuoropuhelulle.
- ✓ Mahdollisuus kuulla myös toisen osapuolen kertomus asiasta.
- ✓ Mahdollisuus rikoksen tekijälle kohdata uhri ja kantaa vastuu teostaan.
- ✓ Seurausten konkretisoituminen.
- ✓ Pienentää pitkällä aikavälillä riskiä uusintarikollisuuteen tai rikollisiin tekoihin.

Soveltuu erityisesti tapauksiin, joissa

- ✓ Tekijä alle 18-vuotias.
- ✓ Ensikertaa tehdyt rikostapaukset.
- ✓ Esitutkinnan rajoittaminen on todennäköistä.

Hyödyt asianomistajalle:

- ✓ Vahvistaa oikeusturvaa.
- ✓ Opastusta ja ohjausta jatko- ja tukipalveluihin.
- ✓ Mahdollisuus saada hyvitys myös henkisellä tasolla.

Sovittelualoitteen voi tehdä:

- ✓ Poliisi
- ✓ Syyttäjä
- ✓ Viranomainen
- ✓ Lapsen tai nuoren huoltaja
- ✓ Muu laillinen edustaja
- ✓ Muu konfliktista tietävä henkilö esim. opettaja tai nuorisotyöntekijä.

Asianosaiset ovat omassa asiassaan parhaita asiantuntijoita. Heillä on ajantasaisin tieto ongelmasta sekä sen mahdollisesta ratkaisusta.

Sovittelun avainsanoja:

- ✓ Vapaaehtoisuus
- ✓ Osallisuus
- ✓ Luottamuksellisuus
- ✓ Puolueettomuus
- ✓ Turvallisuus
- ✓ Oikeudenmukaisuus

3 CASE ESIMERKKEJÄ

3.1 CASE 1

A huomasi, ettei pystynyt kirjautumaan sosiaalisen median tililleen. Kirjautumista ylläpitävistä lokeista selvisi, että tilille oli kirjauduttu monelta eri paikkakunnalta.

Tilin kaapannut B otti A:n yhteyttä ja uhkasi levittää tililtä löytämäänsä tietoa. Tämän lisäksi B poisti A:n tililtä tämän seuraajia ja käytti A:n tiliä vihapuheen välittämiseen.

B oli vaihtanut A:n sosiaalisen median tilille omat yhteystietonsa, joiden pohjalta B:n henkilöllisyys oli mahdollista selvittää. Kävi ilmi, että B ja A tunsivat toisensa. B uhkasi paljastaa tietoja A:n tililtä, mikäli tämä paljastaisi B:n henkilöllisyyden.

A:n vanhemmat ottivat yhteyttä kouluun, sillä asiasta oli koitunut A:lle paljon haittaa, kuten alakuloisuutta, uniongelmia ja vetäytymistä muista luokkalaisista. Tilin väärinkäytöstä oli aiheutunut A:lle myös mainehaittaa ja haasteita ystävyyssuhteisiin, jonka vuoksi A:n koulunkäynti kärsi.

Myöhemmin A näki sattumalta B:n Wilma-tunnukset ja kostoksi aiemmasta kirjautui B:n Wilmaan ja lähetteli tämän nimissä epäasiallisia viestejä koulun opettajille.

Asiaa selvitettiin koulun sekä A:n ja B:n huoltajien kesken. Koulussa käytyjen selvitysten lisäksi A:n huoltajat olivat yhteydessä sovittelutoimeen. Tietomurtojen lisäksi rikosnimikkeinä olivat identiteettivarkaus ja kunnianloukkaus.

Tietomurto (Rikoslaki, RL 37:8 §)
Oikeudeton tunkeutuminen toisen henkilön tai yrityksen tietoihin. Esimerkiksi käyttää toisen käyttäjätunnusta luvatta, tai muuten murtaa tietojärjestelmän turvajärjestelyn.

Identiteettivarkaus (RL 38:9a §)
Toisena henkilönä esiintyminen, joka aiheuttaa sille, jota tieto koskee taloudellista vahinkoa tai vähäistä suurempaa haittaa. Haitta voi olla esim. asian selvittämisestä ja oikaisemisesta johtuva suuri vaivannäkö. Teolla tarkoituksellisesti erehdytetään kolmatta tahoa.

Kunnianloukkaus (RL 23:9 §)
Esittää toisesta valheellisen tiedon tai vihjauksen tai muulla tavalla halventaa toista. Aiheuttaa toiselle kärsimystä ja vahinkoa. Esimerkiksi herjaaminen, solvaus, kaikenlainen haukkuminen.

4 CASE 2

Poliisi sai tiedon kouluun kohdistuneesta uhkauksesta, joka oli lähetetty koulun oppilaan Wilman kautta. Uhkauksen tehnyt oppilas X tavoitettiin kotoaan ja hän vannoi, ettei ollut tehnyt uhkausta.

Asiaa selvitettiin X:n vanhempien kanssa. Keskustelun lomassa hän muisti, että oli jutellut eräällä keskustelufoorumilla uuden tuttavuuden Y:n kanssa. Y oli lähettänyt keskustelun yhteydessä X:lle linkin, jota X oli klikannut. Y oli tätä kautta saanut haltuunsa X:n tietokoneen, jota hyödyntäen Y lähetti koulu-uhkauksen X:n nimissä.

Y oli alle 15-vuotias ja hän oli käyttänyt teossa harhautustarkoituksessa muuta kuin omaa IP-osoitettaan.

Perätön vaarailmoitus (RL 34:10 §)
Perättömän ilmoituksen tekeminen pommista, tulipalosta, merihädästä, suuronnettomuudesta tai muusta vastaavasta hädästä. Aiheuttaa pelastus- tai turvallisuustoimen tai pakokauhua.

5 CASE 3

Koulun työntekijä otti yhteyttä sovittelutoimeen ja kertoi, että hänen vähemmälle käytölle jäänyt sähköpostitilinsä oli kaapattu ja tililtä oli lähetetty uutiskirjeen muodossa koulun henkilökunnalle epäasiallisia viestejä. Osa viesteistä oli ohjautunut roskapostiin, mutta osa vastaanottajista oli saanut viestin suoraan saapuneiden kansioon.

Työntekijälle oli selvinnyt, että viestit oli lähetetty ilmaisen, julkisen huijaustyökalun kautta. Lokitiedoista selvisi, että tekijä oli ennen viestien lähettämistä testannut palvelua omaan sähköpostiosoitteeseensa. Tekijäksi oli selvinnyt koulun yläasteikäinen oppilas, joka tunnusti tekonsa ja oli siitä pahoillaan.

Tietomurrossa tulee olla kyse tahallisesta toiminnasta. Henkilön on tiedettävä, että hän tunkeutuu luvattomasti tietojärjestelmään tai sen erikseen suojattuun osaan.

Tietojärjestelmään tunkeutuminen tarkoittaa pääsyn hankkimista järjestelmässä käsiteltyihin, varastoituihin tai siirrettyihin tietoihin tai dataan. Tunkeutuminen tapahtuu käytännössä esimerkiksi tekijälle kuulumatonta käyttäjätunnusta käyttäen. Tunkeutuminen ei edellytä, että oikeudettomasti saatuja tietoja käytetään, luetaan tai selataan.

6 ESIMERKKI SOVITTELUSSA RATKAISTUSTA RIKOSASIASTA

6.1 MITÄ TAPAHTUI?

Kaveruksilla L ja M oli tapana vaihdella keskenään tietyn sosiaalisen median sovelluksen tilejään, ja yhteisellä päätöksellä luoda sisältöä toistensa tileille. L päätti luvatta kokeilla, pääsisikö M:n tilin tunnuksilla kirjautumaan myös muille M:n tileille. L onnistui kirjautumaan kahdelle muullekin M:n sosiaalisen median tilille ja levitti sieltä löytämäänsä arkaluontoista sisältöä eteenpäin. Tietojen leviämisestä aiheutui M:lle ongelmia ja jopa uhkauksia.

M kertoi asiasta huoltajalle, joka teki asiasta rikosilmoituksen poliisille tietomurrosta, identiteettivarkaudesta sekä yksityiselämää loukkaavan tiedon levittämisestä.

6.2 MITEN ASIA OHJAUTUI SOVITTELUUN?

Tutkinnassa tapauksen saanut poliisi huomasi pian, että sovittelu tukisi parhaiten preventiivistä vaikutusta, sillä sovittelussa tapaus käsiteltäisiin rikosprosessia laajemmin. Poliisi päätti toimia asiassa nopeasti, vielä kun tapahtumat olivat asianosaisilla tuoreesti mielessä ja ehdotti sovittelua.

L ja M huoltajineen olivat halukkaita sovittelemaan tapausta. M ei kuitenkaan olisi halunnut enää kohdata L:n kanssa kokemansa kiusaamisen ja uhkailun vuoksi. Sovittelun ohjaaja keskusteli nuorten ja heidän huoltajiensa kanssa sovittelun hyödyistä, ja kaikki osapuolet päättivät osallistua sovitteluun.

6.3 OIVALLUKSIA SOVITTELUSSA?

M kertoi tapaamisessa hänen tileiltään levinneiden tietojen olleen erittäin henkilökohtaisia. Arkaluontoisten tietojen leviämisestä oli aiheutunut hänelle ongelmia ja turvattomuuden tunnetta. M oli jopa rajoittanut liikkumistaan, koska ei kokenut oloaan turvalliseksi. M koki myös toimineensa itse väärin, koska L oli saanut hänen tunnuksensa ja salasanansa selville. M:a huoletti, että tietomurto tapahtuisi uudelleen vielä haitallisemmin seurauksin, ja hän oli alkanut epäillä omia taitojaan internetin käytössä sekä ihmistuntemustaan.

L ei ennen sovittelua ollut ymmärtänyt, miten syvästi hänen toimintansa oli vaikuttanut M:n turvallisuuden tunteeseen. L:n tulevaisuuden suunnitelmissa oli pyrkiä IT-alalle ja hän pohti voisiko merkintä tietomurrosta olla esteenä tulevaisuuden ammatille. L oivalsi sovittelutapaamisessa toimineensa väärin, mutta voivansa ottaa oppia tapahtuneesta. Hän oli kiinnostunut opiskelemaan tietoverkkoihin liittyviä asioita lisää ja otti vastaan neuvoja, miten voisi lähteä toteuttamaan tulevaisuuden suunnitelmiaan.

Yksityiselämää loukkaava tiedon levittäminen (RL 24:8 §)

Oikeudettomasti joukkotiedotusvälinettä käyttämällä tai muuten toimittaa lukuisten ihmisten saataville toisen yksityiselämästä tiedon, vihjauksen tai kuvan. Teko aiheuttaa vahinkoa ja kärsimystä loukatulle.

7 VAHINGONKORVAUS

Sovintoon pääseminen on joissain tilanteissa vahingonkorvausten näkökulmasta asianomistajan kannalta rikosprosessia parempi ratkaisu.

- ✓ Arvioidaan henkilövahinkoasiain neuvottelukunnan suositusten pohjalta.
- ✓ Korvaukset lisäävät ymmärrystä asianosaisten tilanteista.
- ✓ Voi olla esimerkiksi rahakorvaus tai työkorvaus.

Myös alle 15-vuotias on korvausvastuussa aiheuttamastaan vahingosta. Kyberrikoksesta aiheutunut vahinko voi olla mittavaa, ja osalle nuorista teoista seurannut vahingonkorvausvastuu ja vahingonkorvausten määrä voi tulla yllätyksenä.

7.1 CASE 5

P oli ladannut Internetistä sovelluksen, jota hyödyntämällä hänen onnistui päästä huoltajansa pankkitilille, jossa hän teki luvattomia ostoja. P päätti myös siirtää rahaa omalle tililleen.

Asian huomattuaan P:n huoltaja teki P:stä rikosilmoituksen. Pankki korvasi P:n huoltajan varat ja vaati P:ltä vahingonkorvausta yli 3 000 euroa laillisine viivästyskorkoineen. Pankki vaati P:tä myös korvaamaan pankille asian selvittämisestä aiheutuneet kustannukset, yhteensä 300 euroa.

Maksuvälinepetos (RL 37:8 §:n 3. kohta)

Hankkii itselleen tai toiselle oikeudetonta taloudellista hyötyä maksuvälineeseen liittyvää dataa syöttämällä, muuttamalla, tuhoamalla, vahingoittamalla, siirtämällä tai poistamalla taikka tietojärjestelmän toimintaan muuten puuttumalla saa aikaan rahan tai rahan arvon siirron lopputuloksen vääristymisen ja siten aiheuttaa toiselle vahinkoa.

7.2 CASE 6

Käräjäoikeus tuomitsi 15-vuotta täyttäneen V:n nuorena henkilönä tehdystä tietomurrosta ja luvattomasta käytöstä 15 päiväsakkoon. V oli lisäksi velvollinen korvaamaan asian selvittämisestä aiheutuneista kuluista ja ajanhukasta n. 400 euroa.

Luvaton käyttö (RL 28:7 §)

Luvattomasti käyttää toisen irtainta omaisuutta tai kiinteää konetta tai laitetta. Ei koske suojaamattoman langattoman tietoverkkoyhteyden kautta muodostetun internet-yhteyden käyttämistä.

8 HAUSKANPIDOSTA RIKOLLISELLE TIELLE LUISUMINEN

Tietojärjestelmän häirintä (RL 38:7a §)
Aiheuttaa toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla, taikka muulla niihin rinnastavalla tavalla estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä.

Käräjäoikeudessa tuomitut alle 18-vuotiaat vastaajat A ja B olivat tehneet hajautettuja palvelunestohyökkäyksiä lukuisiin eri tietojärjestelmiin. Verkkopalvelujen toiminnalle aiheutui verkkohyökkäysten takia vakavia häiriöitä tai ne olivat estyneet kokonaan. Hyökkäykset kohdistuivat mm. eri pankkien verkkopalveluihin. A oli lisäksi pyrkinyt kiristämään pankeilta rahaa bitcoin maksujen muodossa, jotta palvelunestöhyökkäykset loppuisivat. Käräjäoikeus määräsi vastaajien maksamaan palvelunestohyökkäyksistä aiheutuneista vahingoista yli 10 000 euron korvaukset.

Toinen vastaajista kertoi, että motiivina teoille oli mm. hauskanpito. Palvelunestohyökkäysten kokeilu oli hänen kohdallaan alkanut tietokonepeleissä huijaamisesta sekä pelimaailman häirinnästä. Myöhemmin toiminta luisui pelaajien ja järjestelmänvalvojien häirintään sekä koneiden hakkerointiin.

Palvelunestohyökkäys, eli ”dossaus” (DoS, Denial of Service)

”Dossaamisella” hyökkääjä lähettää rikoksen kohteeksi valikoituneeseen tietojärjestelmään luonteeltaan teknisesti haitallista tai volyymiltään liian suuren määrän tietoliikennettä, josta aiheutuu tietojärjestelmän häiriintyminen tai täydellinen lamaantuminen.

Palvelunestohyökkäys toteutetaan yleensä hajautettuna. (DDoS) Tällöin se toteutetaan useista eri lähteistä yhtä aikaa.

8.1 ASIANOMISTAJANA YRITYS

Asianomistajan ollessa yritys, nuoren voi olla vaikea suhtautua tekemäänsä rikokseen sen vakavuuden vaatimalla tavalla. Säännöt voidaan kokea epäreiluina ja heitä koskemattomina, sillä ajatellaan, että yritykseen kohdistuneella rikoksella ei ole varsinaista uhria eikä se näin ole vakava asia.

Sovittelutapaamisessa asianomistajaa edustaa jokin henkilö yrityksestä, jolloin myös yritys saa kasvot nuoren mielessä. Sovittelussa pääpaino ei ole rikoksesta epäillyn rankaiseminen, vaan virheistä oppii parhaiten vastuunkannon myötä.

9 APUKYSYMYKSIÄ

Sovittelussa on kyse asianosaisten keskinäisestä keskustelusta, jota neutraalit tapahtumien ulkopuoliset henkilöt ohjaavat. Turvallinen paikka sovittelutapaamisessa luo tilaisuuden avoimelle vuoropuhelulle, jolloin nuoret itse voivat miettiä ratkaisua tapahtuneelle, aikuisten opastuksella.

Nuoren kanssa keskustellaan lisäksi siitä, mitä tapahtumat tarkoittavat lainsäädännön ja rikosseuraamusten näkökulmasta sekä mitä teon myötä olisi voinut seurata. Ihminen on kokonaisuus, jolloin rikos vaikuttaa fyysisesti, psyykkisesti ja sosiaalisesti tämän elämään.

Kyberrikosten sovittelu tapahtuu samalla periaatteella kuin minkä tahansa muunkin rikoksen sovittelu. Ohessa on keskustelun tueksi apukysymyksiä, joita voi ottaa huomioon niin sovittelutapaamisessa kuin myös ankkuripuhutuksessa tai laillisuuskasvatuksessa.

- ✓ Onko sinulla kiinnostusta haavoittuvuuksien skannaamiseen tai niiden raportointiin?
- ✓ Millaisia vaikutuksia kyberrikoksilla on muihin?
- ✓ Mitkä asiat kybermaailmassa kiehtovat sinua?
- ✓ Mikä sinua kiinnostaa erityisesti tietojärjestelmissä?
- ✓ Mitä ajatuksia herää tietojärjestelmiin liittyvästä epäeettisestä toiminnasta?
- ✓ Mikä sinua erityisesti kiinnostaa tietotekniikassa?
- ✓ Mikä sinua kiinnostaa erityisesti tietokoneissa?
- ✓ Onko sinulla kiinnostusta osallistua hakkerointihaastekampanjoihin?

Haavoittuvuus
Alttius tietoturvaan kohdistuville uhkille, joka mahdollistaa vahingon toteutumisen ja jota voidaan käyttää vahingon aiheuttamisessa. Esim. palvelimet, joissa on helposti arvattavat salasanat tai ei lainkaan salasanoja.

10 LÄHTEET JA HYÖDYLLISTÄ LUKEMISTOA

Ankkuritoiminnan vaikuttavuus, Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 2022:40. https://julkaisut.valtioneuvosto.fi

Cybercrime Exit, Koulutusmateriaali, Keskusrikospoliisi, Kyberrikostorjuntakeskus. www.poliisi.fi/cybercrime-exit

Kyberturvallisuuden sanasto, Sanastokeskus TSK 2018 https://turvallisuuskomitea.fi

Käsikirja lasten ja nuorten sovitteluihin, Aseman lapset 2022 https://www.julkari.fi

Poliisihallituksen ohje rikoksen uhrin ohjaaminen ja rikosasioiden sovittelu (POL-2018-41886) https://thl.fi

Rakennamme sovintoa, Opas rikosten ja riitojen sovitteluun, THL 2013 https://www.julkari.fi

Yle, Kyberrikollinen paljastaa: Halusin kostaa kaiken kokemani vääryyden https://yle.fi

Yle, Teinipoika hankki pääsyn nopeampaan nettiin ja latasi pelejä – oikeus tuomitsi tietomurrosta https://yle.fi

Lainsäädäntö ja virallislähteet:

Laki rikosasioiden ja eräiden riita-asioiden sovittelusta (1015/2005)

Rikoslaki (39/1889, RL)

HE 329/2014 vp

HE 153/2006 vp

HE 94/1993 vp

LaVM 33/2014 vp – HE 329/2014 vp