Bug bounty -ohjelmat osana julkishallinnon tietoturvaa

Maaria Kuisma
Lapin yliopisto
Oikeustieteiden tiedekunta
Pro gradu -tutkielma
Oikeusinformatiikka
Kevät 2020

Lapin yliopisto, Oikeustieteiden tiedekunta

Työn nimi: Bug bounty -ohjelmat osana julkishallinnon tietoturvaa
Tekijä: Maaria Kuisma
Opetuskokonaisuus ja oppiaine: Oikeustiede, oikeusinformatiikka
Työn laji: Tutkielma X Lisensiaatintyö _
Sivumäärä: XIV+107
Vuosi: 2020

Tiivistelmä:
Tässä tutkimuksessa perehdytään bug bounty -ohjelmien käyttämiseen julkishallinnossa. Tutkimuksessa selvitetään, mitä bug bounty -ohjelmat ovat, miten ne toimivat ja mitä hyötyjä ja riskejä niiden käyttämiseen liittyy. Tämän ohella perehdytään tietoturvaan teoreettisesta näkökulmasta, sekä julkishallinnon ja tietoturvan väliseen yhteyteen. Lisäksi käydään läpi tieto- ja viestintärikoksia koskevaa lainsäädäntöä peilaten sitä ohjelmiin osallistumiseen ja ohjelmien järjestämiseen.

Tutkimuksen tarkoituksena on selvittää, millä perusteilla bug bounty -ohjelmien järjestäminen ja niihin osallistuminen kotimaisessa julkishallinnossa ovat Suomen lain mukaisia. Lisäksi tarkoituksena on vastata kysymykseen, kuka päättää ohjelman käynnistämisestä julkishallinnossa. Taustatavoitteena on myös tuoda bug bounty -ohjelmia tai julkishallinnon tietojärjestelmiin liittyviä tietoturvaliitännäisiä yksityiskohtia yleisesti ottaen tiettävämmäksi juridiikan kentällä.

Tutkimus edustaa oikeusinformatiikan tutkimusalaa. Oikeudenaloista tutkimus voidaan asemoida informaatio-oikeuden ja ICT-oikeuden rajapinnalle. Näitä kolmea yhdistää kiinnostus taloustieteellistä näkökulmaa kohtaan, mistä syystä tutkimuksessa on perehdytty ohjelmien järjestämiseen myös taloustieteen perspektiivistä. Tutkimuksen rikosoikeudellista osiota sen sijaan on lähestytty oikeusdogmatiikan näkökulmasta. Lähdemateriaali koostuu suurelta osin ICT-alan bug bounty -ohjelmia tai muuta tietoturvan testausta käsittelevistä artikkeleista, sillä aihetta on lähestytty juridiikan näkökulmasta vain vähäisesti myös kansainvälisellä tasolla. Erityisesti tutkimuksen rikosoikeudellisen analyysin kohdalla myös Verohallinnon Tulorekisteriä koskevan ohjelman sääntöjä on käytetty lähteenä, rikoslain kriminalisointeja näihin sääntöihin peilattaessa.

Kuten jo tutkimuksen otsikosta käy ilmi, bug bounty -ohjelmat voivat olla osa julkishallinnossa käytettävien tietojärjestelmien tietoturvaa – yksinään ne eivät riitä, vaan tietoturvan ylläpidossa ja testaamisessa on käytettävä myös muita menetelmiä. Tietojärjestelmän tuotantoympäristöön kohdistuvan bug bounty -ohjelman järjestäminen ja ohjelmaan osallistuminen on pääsääntöisesti voimassaolevan lainsäädännön mukaista toimintaa, tiettyjen rikosoikeudellisten kriminalisointien kohdalla ohjelmaan osallistuva henkilö saattaa kuitenkin syyllistyä rikokseen. Erityisesti on korostettava ohjelman sääntöjen merkitystä loukatun suostumuksen lähteenä: ohjelmien sääntöjen laatimisen kohdalla tulisi vastaisuudessa kiinnittää tarkemmin huomiota juridisiin yksityiskohtiin.

Avainsanat:
Bug bounty -ohjelma, haavoittuvuus, hakkeri, tietoturva, tietosuoja, joukkoistaminen

Sisällys

LÄHTEET

KIRJALLISUUS

Aarnio, Aulis: Tulkinnan taito. Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Alma Talent Oy. 2006.

Akerlof, George A.: The Market for ”Lemons”: Quality Uncertainty and the Market Mechanism. The Quarterly Journal of Economics, Vol. 84, No. 3. Elokuu 1970, s. 488–500.

Anderson, Ross: Security in Open versus Closed Systems – The Dance of Boltzmaan, Coase and Moore. (s. 1–15). Technical report, Cambridge University, England, 2002.

Andreasson, Ari & Koivisto, Juha: Tietoturvaa toteuttamassa. Tietosanoma Oy. Helsinki 2013.

Andreasson, Ari; Riikonen, Jaana & Ylipartanen, Arto: Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tietosanoma Oy. Helsinki 2019.

Algarni, Abdullah M. & Malaiya, Yashwank K.: Software Vulnerability Markets: Discoveries and Buyers. International Journal of Computer, Information Science and Engineering 8, no. 3. 2014, s. 71–81.

Alhazmi, O. H. & Malaiya, Y. K.: Modeling the Vulnerability Discovery Process. Proceedings of the 16th IEEE International Symposium on Software Reliability Engineering (ISSRE’05), 2005.

Brady, Robert M.; Anderson, Ross J. & Ball, Robin C.: Murphy’s law, the fitness of evolving species, and the limits of software reliability. Technical Report, No 471. University of Cambridge, Computer Laboratory. Syyskuu 1999.

Bacon, David F.; Chen, Yiling; Parkes, David C. & Rao, Malvika: A market-based approach to software evolution. Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications. Lokakuu 25–29, 2009, Orlando, Florida, USA, s. 973–980. New York: ACM Press.

Böhme, Rainer: A Comparison of Market Approaches to Software Vulnerability Disclosure. In: Proceedings of the 2006 international conference on Emerging Trends in Information and Communication Security (ETRICS’06). Springer-Verlag, Berlin, Heidelberg 2006, s. 298–311.

Cavusoglu, Hasan; Cavusoglu, Huseyin & Raghunathan, Srinivasan: Emerging Issues in Responsible Vulnerability Disclosure. Paper presented in the Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University. Kesäkuu 2005.

Doupé, Adam; Cova, Marco & Vigna, Giovanni: Why Johnny Can’t Pentest: An Analysis of Black-box Web Vulnerability Scanners. In: Proceedings of the 7th international

conference on Detection of intrusions and malware, and vulnerability assessment (DIMVA'10). Springer-Verlag, Berlin, Heidelberg. 2010, s. 111–131.

Edmundson, Anne; Holtkamp, Brian; Rivera, Emanuel; Finifter, Matthew, Mettler, Adrian & Wagner, David: An Empirical Study of the Effectiveness of Security Code Review. In: Proceedings of the 5th international conference on Engineering Secure Software and Systems (ESSoS'13). Springer-Verlag, Berlin, Heidelberg. 2013, s. 197–212.

Egelman, Serge; Herley, Cormac & van Oorschot, Paul C.: Markets for Zero-Day Exploits: Ethics and Implications. In: Proceedings of the 2013 New Security Paradigms Workshop (NSPW '13). Association for Computing Machinery, New York, NY, USA. 2013, s. 41–46.

Elazari Bar On, Amit: Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties. (Huhtikuu 12, 2018). An edited, final version of this paper in Rewired: Cybersecurity Governance, Ryan Ellis and Vivek Mohan eds. Wiley, 2019.

Finifter, Matthew; Akhawe, Devdatta & Wagner, David: An Empirical Study of Vulnerability Rewards Programs. In: Proceedings of the 22nd USENIX conference on Security (SEC'13). USENIX Association, USA, 273–288. 2013.

Frei, Stefan; Schatzmann, Dominik; Plattner, Bernhard & Trammell, Brian: Modelling the Security Ecosystem – The Dynamics of (In)Security. In: Economics of Information Security and Privacy. Springer, Boston, MA. 2010, s. 79–106.

Fryer, Huw & Simperl, Elena: Web Science Challenges in Researching Bug Bounties. In: Proceedings of the 2017 ACM on Web Science Conference (WebSci '17). Association for Computing Machinery, New York, NY, USA. 2017, s. 273–277.

Gillespie, Alisdair A.: Cybercrime. Key Issues and Debates. Routledge. London 2016.

Hakamies, Kaarlo: 24. RL 36: Petos ja muu epärehellisyys, päivitetty 1.11.2008. Teoksessa: Rikosoikeus, 2004. Tekijät: Lappi-Seppälä, Tapio; Hakamies, Kaarlo; Helenius, Dan; Koskinen, Pekka; Majanen, Martti; Melander, Sakari; Nuotio, Kimmo; Nuutila, Ari-Matti; Ojala, Timo & Rautio, Ilkka. Alma Talent Oy. Sähköinen painos, 2004. Vuodesta 2004 lähtien teos on ollut osa päivitettävää Alma Talent Fokus -palvelua.

Hallberg, Pekka: 1. Perusoikeusjärjestelmä. Teoksessa: Hallberg, Pekka; Karapuu, Heikki; Ojanen, Tuomas; Scheinin, Martin; Tuori, Kaarlo & Viljanen, Veli-Pekka: Perusoikeudet. Alma Talent Oy, Helsinki. 2005, sähköinen, päivittyvä teos.

Hata, Hideaki; Guo, Mingyu & Babar, M. Ali: Understanding the Heterogeneity of Contributors in Bug Bounty Programs. In: Proceedings of the 11th ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM '17). IEEE Press. 2017, s. 223–228.

Hemmo, Mika & Hoppu, Esko: Sopimusoikeus. Alma Talent Oy. 2006. Sähköinen painos, teosta päivitetään neljä kertaa vuodessa. Viimeisin päivitys 18.12.2019.

Himanen, Pekka: Hakkerietiikka ja informaatioajan henki. WSOY. Helsinki 2001.

Ingo, Henrik: Avoin Elämä. Näin toimii Open Source. Ei kustantajaa. Kirjan teksti (poislukien kannen kuva ja epilogi) on julkaisuhetkellä vapautettu yhteisomistukseen (Public Domain). Tekstiä voi vapaasti kopioida, julkaista ja muokata, kokonaan tai osittain. Kirja on luettavissa ja kopioitavissa internetissä: http://www.avoinelama.fi. 2005.

Jokela, Antti: Rikosprosessioikeus, 5., uudistettu painos. Alma Talent Oy, yhteistyössä Lakimiesliiton Kustannus. 2018.

Kilovaty, Ido: Freedom to Hack. Ohio State Law Journal. Vol. 80:3, 2019, s. 455–520.

Koulu, Riikka: Digitalisaatio ja algoritmit – oikeustiede hukassa? Lakimies 7–8/2018, s. 840–867.

Koskinen, Pekka: Rikosoikeuden yleiset opit ja rikosvastuun perusteet, päivitetty 1.11.2008. Teoksessa: Rikosoikeus, 2004. Tekijät: Lappi-Seppälä, Tapio; Hakamies, Kaarlo; Helenius, Dan; Koskinen, Pekka; Majanen, Martti; Melander, Sakari; Nuotio, Kimmo; Nuutila, Ari-Matti; Ojala, Timo & Rautio, Ilkka. Alma Talent Oy. Sähköinen painos, 2004. Vuodesta 2004 lähtien teos on ollut osa päivitettävää Alma Talent Fokus -palvelua.

Kuehn, Andreas: New Paradigms in Securing Software Vulnerabilities – An Institutional Analysis of Emerging Bug Bounty Programs and their Implications for Cybersecurity. 9th Annual GigaNet Symposium, Istanbul, Turkey. Syyskuu 2014.

Kulla, Heikki: Hallintomenettelyn perusteet. 10., uudistettu painos. Alma Talent Oy, yhteistyössä Lakimiesliiton Kustannus. 2018.

Laszka, Aron; Zhao, Mingyi & Grossklags, Jens: Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms. In: Askoxylakis et al. (Eds.): ESORICS 2016, Part II, LNCS 9879, s. 161–178, 2016. Springer International Publishing Switzerland 2016.

Lebraty, Jean-Fabrice & Lobre-Lebraty, Katia: Crowdsourcing: One Step Beyond. ISTE Ltd and John Wiley & Sons, Inc. London & Hoboken 2013.

Maillart, Thomas; Zhao, Mingyi; Grossklags; Jens & Chuang, John: Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond with Bug Bounty Programs. Journal of Cybersecurity 3, no. 2. 2017, s. 81–90.

Mäenpää, Olli: Yleinen hallinto-oikeus. 1. painos. Alma Talent Oy, yhteistyössä Lakimiesliiton Kustannus. 2017.

Määttä, Kalle: Oikeustaloustieteen aakkoset. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. Hakapaino Oy. Helsinki 1999.

Neuvonen, Riku: Viestintä- ja informaatio-oikeuden perusteet. 2. uudistettu painos. Kauppakamari. 2019.

Nevalainen, Sami: Kyberrikokset ja Suomen rikosoikeus. Defensor Legis N:o 2/2019, s. 131–148.

Nuutila, Ari-Matti & Ojala, Timo: Kuoleman- ja vammantuottamusrikokset, päivitetty 1.11.2008. Teoksessa: Rikosoikeus, 2004. Tekijät: Lappi-Seppälä, Tapio; Hakamies, Kaarlo; Helenius, Dan; Koskinen, Pekka; Majanen, Martti; Melander, Sakari; Nuotio, Kimmo; Nuutila, Ari-Matti; Ojala, Timo & Rautio, Ilkka. Alma Talent Oy. Sähköinen painos, 2004. Vuodesta 2004 lähtien teos on ollut osa päivitettävää Alma Talent Fokus -palvelua.

Ozment, Andy: Bug Auctions: Vulnerability Markets Reconsidered. Workshop on Economics and Information Security. Toukokuu 2004: Minneapolis, MN, USA.

Ozment, Andy: The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting. Version [914] to be presented at: The Workshop on Economics and Information Security. Kesäkuu 2005: Cambridge, MA, USA.

Ozment, Andy & Schechter, Stuart E.: Milk or Wine: Does Software Security Improve with Age? In USENIX Security Symposium, vol. 6. 2006.

Pöysti, Tuomas: Kohti digitaalisen ajan hallinto-oikeutta. Lakimies 7–8/2018, s. 868–903.

Rautio, Ilkka: 26. RL 38: Tieto- ja viestintärikokset, päivitetty 1.11.2008. Teoksessa: Rikosoikeus, 2004. Tekijät: Lappi-Seppälä, Tapio; Hakamies, Kaarlo; Helenius, Dan; Koskinen, Pekka; Majanen, Martti; Melander, Sakari; Nuotio, Kimmo; Nuutila, Ari-Matti; Ojala, Timo & Rautio, Ilkka: Rikosoikeus. Alma Talent Oy. Sähköinen painos, 2004. Vuodesta 2004 lähtien teos on ollut osa päivitettävää Alma Talent Fokus -palvelua.

Rescorla, Eric: Is finding security holes a good idea? In: Workshop on Economics and Information Security. Toukokuu 2004. Minneapolis, Minnesota.

Riekkinen, Juhana: Sähköiset todisteet rikosprosessissa. Tutkimus tietotekniikan ja verkkoyhteiskuntakehityksen vaikutuksista todisteiden elinkaareen. Alma Talent Oy. Helsinki 2019.

Ruohonen, Jukka, & Allodi, Luca: A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities. The 17th Annual Workshop on the Economics of Information Security (WEIS 2018). 2018.

Råman, Jari: Regulating Secure Software Development. Analysing the potential regulatory solutions for the lack of security in software. Acta Universitatis Lapponiensis 102. University of Lapland, Faculty of Law. University of Lapland Printing Centre. Rovaniemi 2006.

Saarenpää, Ahti: Oikeusinformatiikka. Teoksessa: Oikeus tänään. Osa I. Neljäs, uudistettu painos, 2016. Toim. Marja-Leena Niemi. Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 64. Rovaniemi 2016, s. 67–273.

Saarenpää, Ahti; Pöysti, Tuomas; Sarja, Mikko; Still, Viveca & Balboa-Alcoreza, Ruxandra: Tietoturvallisuus ja laki. Näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä. Tutkimusraportti. Valtiovarainministeriö, Hallinnon kehittämisosasto. Lapin yliopisto, Oikeusinformatiikan instituutti. Edita Oy. Helsinki 1997.

Tapani, Jussi; Tolvanen, Matti & Hyttinen, Tatu: Rikosoikeuden yleinen osa. Vastuuoppi. 3., uudistettu painos. Alma Talent Oy, yhteistyössä Lakimiesliiton Kustannus. 2019.

Telang, Rahul & Wattal, Sunil: Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical Investigation. Paper presented in the Fourth Workshop on the Economics of Information Security, Kennedy School of Government, Harvard University. Kesäkuu 2005.

Tuori, Kaarlo: Kriittinen oikeuspositivismi. Werner Söderström lakitieto. Helsinki 2000.

Van Goethem, Tom; Piessens, Frank; Wouter, Joosen & Nikiforakis, Nick: Clubbing Seals: Exploring the Ecosystem of Third-party Security Seals. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14). Association for Computing Machinery, New York, NY, USA. 2014, s. 918–929.

Viljanen, Pekka: 7.3 Vahingontekorikokset. Teoksessa: Frände, Dan; Matikkala, Jussi; Tapani, Jussi; Tolvanen, Matti; Viljanen, Pekka & Wahlberg, Markus: Keskeiset rikokset. Neljäs, uudistettu ja laajennettu laitos. Edita. 2018.

Viljanen, Veli-Pekka: 6. Yksityiselämän suoja (PL 10 §). Teoksessa: Hallberg, Pekka; Karapuu, Heikki; Ojanen, Tuomas; Scheinin, Martin; Tuori, Kaarlo & Viljanen, Veli-Pekka: Perusoikeudet. Alma Talent Oy, Helsinki. 2005, sähköinen, päivittyvä teos.

Voutilainen, Tomi: Hyvä sähköinen hallinto. 2. painos. Edita Publishing Oy. Helsinki 2007.

Voutilainen, Tomi: Oikeus tietoon. Informaatio-oikeuden perusteet. 2. uudistettu painos. Edita Publishing Oy. Helsinki 2019.

Zhao, Mingyi; Grossklags, Jens & Chen, Kai: An Exploratory Study of White Hat Behaviors in a Web Vulnerability Disclosure Program. In: Proceedings of the 2014 ACM Workshop on Security Information Workers (SIW '14). Association for Computing Machinery, New York, NY, USA. 2014, s. 51–58.

Zhao, Mingyi; Grossklags, Jens & Liu, Peng: An Empirical Study of Web Vulnerability Discovery Ecosystems. Teoksessa: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). ACM, New York, NY, USA. 2015, s. 1105–1117.

Zhao, Mingyi; Laszka, Aron; Maillart, Thomas & Grossklags, Jens: Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs. HCOMP Workshop on Mathematical Foundations of Human Computation. Marraskuu 2016.

VIRALLISLÄHTEET

AOA 4653/4/14, 31.12.2015. Yrittäjien rakentamisilmoitukset vain sähköisesti – AOA Sakslin: Verohallinto unohti asiakkaan oikeudet.

AOK D: 435/1/92, A: 13.4.1993. Verohallituksen tietoon saatettu käsitys voimassa olevan verotustietokannan mukaisen verolipun toimittamisesta verovelvollisille sekä verohallinnon aiheuttamien ohjelmointivirheiden korjaamisesta.

HE 94/1993 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 30/1998 vp. Hallituksen esitys Eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HE 153/2006 vp. Hallituksen esitys Eduskunnalle Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen hyväksymisestä, laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta sekä laeiksi rikoslain, pakkokeinolain 4 luvun, esitutkintalain 27 ja 28 §:n ja kansainvälisestä oikeusavusta rikosasioissa annetun lain 15 ja 23 §:n muuttamisesta.

HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 60/2018 vp. Hallituksen esitys eduskunnalle laeiksi digitaalisten palvelujen tarjoamisesta sekä sähköisestä asioinnista viranomaistoiminnassa annetun lain muuttamisesta.

HE 284/2018 vp. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi.

HaVM 13/2018 vp. Hallintovaliokunnan mietintö koskien hallituksen esitystä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (9/2018 vp).

VAHTI 2/2010: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.

Valtiovarainministeriön julkaisu 28/2016: Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi. OECD:n suositus ja liiteasiakirja.

Verohallinnon syventävä vero-ohje: Palkka ja työkorvaus verotuksessa. Diaarinumero: VH/3003/00.01.00/2018. Antopäivä 4.1.2019, voimassa 4.1.2019 alkaen.

OIKEUSKÄYTÄNTÖ

KKO 1989:42.

KKO 2003:36.

EIT 17.7.2008, 20511/03, I. vastaan Suomi.

INTERNET-LÄHTEET

Aitonurmi, Joonas: Bug Bounty kutsuu hakkerit mukaan tietoturvajahtiin. Suomidigi, Blogit, Digitalisaation suunnannäyttäjät. 2018. Osoitteessa: https://suomidigi.fi/bug-bounty-kutsuu-hakkerit-mukaan-tietoturvajahtiin/ (Käyty 28.9.2019.)

Bergstöm, Samuli: Verohallinnon BugBounty kampanja. 31.5.2018. Osoitteessa: https://valtioneuvosto.fi/documents/10623/9718807/Verohallinnon_Bug-Bounty_20180831.pdf/86f9498d-5bcb-47c8-a3fd-e4f3901acc91/Verohallinnon_Bug-Bounty_20180831.pdf.pdf (Käyty 28.9.2019.)

Euroopan komissio, uutinen 5.4.2019: EU-FOSSA Bug Bounties in Full Force. Osoitteessa: https://ec.europa.eu/info/news/eu-fossa-bug-bounties-full-force-2019-apr-05_en (Käyty 19.12.2019.)

Facebookin bug bounty -ohjelman säännöt, päivitetty 15.10.2019. Osoitteessa: https://www.facebook.com/whitehat (Käyty 19.12.2019.)

Google application security – Google Security Reward Programs. Osoitteessa: https://www.google.com/about/appsecurity/programs-home/ (Käyty 19.12.2019.)

Hackrfi Oy:n Internet-sivut: etusivu. Osoitteessa: https://www.hackr.fi/ (Käyty 28.9.2019.)

Hackrfi Oy:n Internet-sivut: Kutsuohjelma – Väestörekisterikeskus – Suomi.fi Bug Bounty. Osoitteessa: https://www.hackr.fi/ohjelmat/suomifi.html (Käyty 19.12.2019.)

Hackrfi Oy:n Internet-sivut: Tulorekisteri bug bounty. Osoitteessa: https://www.hackr.fi/ohjelmat/tulorekisteri.html (Käyty 20.12.2019.)

Hackrfi Oy:n Internet-sivut: Väestörekisterikeskuksen suomi.fi-palvelua koskevan bug bounty -ohjelman säännöt. Osoitteessa: https://www.hackr.fi/ohjelmat/suomifi-saannot-v20.pdf (Käyty 20.12.2019.)

Herrasmieshakkerit-podcast, 0x03, julkaistu 5.12.2019. Osoitteessa: https://www.f-secure.com/fi/business/our-approach/herrasmieshakkerit (Käyty 2.1.2020.)

Kauppalehti / Tivi: Verohallinto kutsuu hakkerit apuun: ensimmäinen bug bounty -ohjelma valtionhallinnossa. 2.10.2017. Osoitteessa: https://www.tivi.fi/uutiset/verohallinto-kutsuu-hakkerit-apuun-ensimmainen-bug-bounty-ohjelma-valtionhallinnossa/a22339c8-0145-33d1-92c9-a0d967ed9ca7 (Käyty 28.9.2019.)

Kyberturvallisuuskeskuksen Internet-sivut: CERT. Osoitteessa: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/cert (Käyty 10.4.2020.)

Latvanen, Kari – Tivi: Kannattaako kybervalvonta ulkoistaa? Soc-palvelu maksaa yli 10 000 euroa kuukaudessa. Julkaistu 24.10.2019. Osoitteessa: https://www.tivi.fi/uutiset/kannattaako-kybervalvonta-ulkoistaa-soc-palvelu-maksaa-yli-10-000-euroa-kuukaudessa/f6df42a0-00aa-4558-af34-d558761821ff (Käyty 12.5.2020.)

LähiTapiolan Bug Bounty -hakkeriohjelma maailman kärkeen - samassa sarjassa Googlen ja Applen kanssa. Uutinen, 17.8.2017. Osoitteessa: https://www.lahitapiola.fi/tietoa-lahitapiolasta/uutishuone/uutiset-ja-tiedotteet/uutiset/uutinen/1310391443539 (Käyty 6.4.2019.)

LähiTapiolan bug bounty -ohjelma HackerOne.com-palvelussa. Osoitteessa: https://hackerone.com/localtapiola (Käyty 19.12.2019.)

Meyer, Bernard: We found 6 critical PayPal vulnerabilities – and PayPal punished us for it. Blogikirjoitus, 17.2.2020. Osoitteessa: https://cybernews.com/security/we-found-6-critical-paypal-vulnerabilities-and-paypal-punished-us/ (Käyty 9.3.2020.)

Niemi, Petri – Yle: Kunnilla heikkoja salasanoja ja huteria palomuureja- Lahti maksoi kyberhyökkäyksen torjunnasta liki miljoonan ja jakaa nyt oppeja muillekin. Julkaistu 27.12.2019. Osoitteessa: https://yle.fi/uutiset/3-11121273 (Käyty 31.12.2019.)

Opetus ja kulttuuriministeriö, uutinen 10.9.2018: Hakkerit parantamaan kansallisen MPASSid-tunnistuspalvelun tietoturvaa. Osoitteessa: https://minedu.fi/artikkeli/-/asset_publisher/hakkerit-parantamaan-kansallisen-mpassid-tunnistuspalvelun-tietoturvaa (Käyty 19.2.2019.)

Peiponen, Pasi – Yle: Katso paljastava piilokameravideo – Ylen toimittaja testasi tärkeiden yritysten ja laitosten tilaturvallisuutta: Lähes kaikilla puutteita kulunvalvonnassa. Julkaistu 25.7.2018. Osoitteessa: https://yle.fi/uutiset/3-10320853 (Käyty 3.5.2020.)

Petäinen, Minna – Taloustaito: Hakkerit testaavat verottajan Omavero-palvelun tietoturvaa. Julkaistu 2.10.2017. Osoitteessa: https://www.taloustaito.fi/Vero/hakkerit-testaavat-verottajan-omavero-palvelun-tietoturvaa/ (Käyty 28.9.2019.)

Reda, Julia: In January, the EU starts running Bug Bounties on Free and Open Source Software. Julkaistu 27.12.2018, päivitetty 16.1.2019. Osoitteessa: https://juliareda.eu/2018/12/eu-fossa-bug-bounties/ (Käyty 17.2.2019.)

Sanastokeskus TSK, Tietotekniikan termitalkoot, bug bounty. Päivitetty 26.8.2018. Osoitteessa: http://www.tsk.fi/tsk/termitalkoot/fi/node/266 (Käyty 4.10.2019.)

Sanastokeskus TSK, Tietotekniikan termitalkoot, nollapäivähaavoittuvuus. Päivitetty 26.8.2018. http://www.tsk.fi/tsk/termitalkoot/fi/node/266 (Käyty 1.3.2020.)

Sanastokeskus TSK, Tietotekniikan termitalkoot, tietoturva. Päivitetty 6.7.2015. Osoitteessa: http://www.tsk.fi/tsk/termitalkoot/fi/node/266 (Käyty 26.10.2019.)

Senaattori Mark. R. Warnerin lehdistötiedote 3.11.2019: Bipartisan Legislation to Improve Cybersecurity of Internet-of-Things Devices Introduced in Senate & House. Osoitteessa: https://www.warner.senate.gov/public/index.cfm/2019/3/bipartisan-legislation-to-improve-cybersecurity-of-internet-of-things-devices-introduced-in-senate-house (Käyty 9.3.2020.)

Shirey, R.: Internet Security Glossary. Internet Engineering Task Force (IETF), Request for Comment (RFC). Version 2, RFC 4949, August 2007. Osoitteessa: https://www.rfc-editor.org/info/rfc4949 (Käyty 29.9.2019.)

Swinhoe, Dan – CSO-online: What is the cost of a data breach? Julkaistu 29.8.2019. Osoitteessa: https://www.csoonline.com/article/3434601/what-is-the-cost-of-a-data-breach.html (Käyty 7.5.2020.)

Traficom – Liikenne- ja Viestintävirasto, Kyberturvallisuuskeskus, Tietoturva Nyt!, uutinen: Bug Bounty -ohjelmien avulla tietoturvaongelmat voi kääntää PR-voitoksi. Julkaistu 20.8.2019. Osoitteessa: https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/bug-bounty-ohjelmien-avulla-tietoturvaongelmat-voi-kaantaa-pr-voitoiksi (Käyty 28.9.2019.)

Traficom – Liikenne- ja Viestintävirasto, Kyberturvallisuuskeskus, Tietoturvamerkki.fi -sivuston etusivu. Osoitteessa: https://tietoturvamerkki.fi/ (Käyty 2.1.2020.)

Ulkoministeriö, tiedote 29.11.2019: Ulkoministeriö käynnistää palkkionmetsästysohjelman verkkopalvelujen haavoittuvuuksien etsimiseksi. Osoitteessa: https://valtioneuvosto.fi/artikkeli/-/asset_publisher/ulkoministerio-kaynnistaa-palkkionmetsastysohjelman-verkkopalvelujen-haavoittuvuuksien-etsimiseksi (Käyty 19.12.2019.)

The United States Digital Service: Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon. Osoitteessa: https://www.usds.gov/report-to-congress/2016/hack-the-pentagon/ (Käyty 19.12.2019.)

Verohallinto, uutinen: Bug bounty palkittiin vuoden kybertekona. Julkaistu 23.11.2017. Osoitteessa: https://www.vero.fi/tietoa-verohallinnosta/uutishuone/uutiset/uutiset/2017/bug-bounty-palkittiin-vuoden-kybertekona/ (Käyty 28.9.2019.)

Verohallinto, uutinen 14.11.2019: Verohallinto ja Väestörekisterikeskus kannustavat suomalaisia: Tehdään kansallinen ekoteko ja luovutaan paperipostista. Osoitteessa: https://www.vero.fi/tietoa-verohallinnosta/uutishuone/uutiset/uutiset/2019/verohallinto-ja-v%C3%A4est%C3%B6rekisterikeskus-kannustavat-suomalaisia-tehd%C3%A4%C3%A4n-kansallinen-ekoteko-ja-luovutaan-paperipostista/ (Käyty 19.12.2019.)

Verohallinto, Tulorekisteri, lehdistötiedote: Hakkerit kutsutaan testaamaan Tulorekisterin tietoturvaa. Julkaistu 28.10.2019. Osoitteessa: https://www.vero.fi/tulorekisteri/tietoa-meist%C3%A4/yhteystiedot/medialle/lehdistotiedotteet2/hakkerit-kutsutaan-testaamaan-tulorekisterin-tietoturvaa/ (Käyty 14.12.2019.)

Verohallinnon tiedote 2.10.2017: Verohallinto hyödyntää hakkereita OmaVero-verkkopalvelun tietoturvan testauksessa. Osoitteessa: https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/uutiset/uutiset/2017/verohallinto-hy%C3%B6dynt%C3%A4%C3%A4-hakkereita-omavero-verkkopalvelun-tietoturvan-testauksessa/ (Käyty 12.2.2019.)

VRK – Kokemuksia Bug Bounty -ohjelmasta. VAHTI Kesä-seminaari 31.8.2018. Osoitteessa: https://vm.fi/documents/10623/9718807/VRK_Bug+Bounty_VAHTI_3108_2018.pdf/d25be8ff-e807-4400-a635-4b8135b82cfc/VRK_Bug+Bounty_VAHTI_3108_2018.pdf.pdf (Käyty 26.1.2019.)

MUUT LÄHTEET

Jarnola, Miika: Bug Bountyn hyödyt tietoturvatestauksessa: tapaustutkimus - Lähitapiola. Pro gradu -tutkielma, Jyväskylän yliopisto. 2018.

Korhonen, Rauno: Tietoturvallisuus 2015. Hallinto-oikeuden ja oikeusinformatiikan pooli ONPOOL5, luentokalvot. 25.3.2015.

Korhonen, Suvi: Isku ihmisen haavoittuvuuksiin. Tivi, lokakuu 2019, s. 18–23.

Kyberturvallisuuden sanasto 2018. TSK 52. Sanastokeskus TSK ry, Huoltovarmuuskeskus. Helsinki 2018.

Lehtonen, Asko: Tietotekniikkaoikeus. Informaatio- ja tietotekniikkaoikeus, luentokalvot kl. 2015.

Määttä, Kalle: Oikeustaloustiede-opintojakson (12.–14.2.2019) luentokalvot, Lapin yliopisto.

Sähköpostikeskustelu 3.10.2019, Hanna Leskelä – Kielitoimiston neuvonta, Kotimaisten kielten keskus.

Sähköpostikeskustelut 2019–2020, Juho Vuorio – Verohallinnon Turvallisuus- ja riskienhallintayksikkö.

Verohallinnon 28.10.2019 alkaen käynnissä olevan Tulorekisteri-tietokantaa koskevan bug bounty -ohjelman säännöt.

LYHENTEET

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incidence Response Team
DDOS	distributed denial of service, hajautettu palvelunestohyökkäys
DOS	denial of service, palvelunestohyökkäys
DVV	Digi- ja väestötietovirasto
EIT	Euroopan ihmisoikeustuomioistuin
ENISA	Euroopan unionin kyberturvallisuusvirasto
HE	hallituksen esitys
HL	hallintolaki
L	laki
NDA	non-disclosure agreement, salassapitosopimus
OECD	Organisation for Economic Co-operation and Development, Taloudellisen yhteistyön ja kehityksen järjestö
PL	perustuslaki
RL	rikoslaki
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä
VDP	Vulnerability Disclosure Program, haavoittuvuuksien julkaisuohjelma
vp	valtiopäivät
VRK	Väestörekisterikeskus
VRP	Vulnerability Rewards Program, haavoittuvuuspalkkio-ohjelma
XSS	cross-site scripting

KUVAT

1 Johdanto

1.1 Tutkimuksen aihe ja lähtökohdat

Bug bountylla tarkoitetaan haavoittuvuuden tai ohjelmavirheen löytämisestä ja raportoimisesta tarjottavaa palkkiota.[1] Bug bounty -ohjelma sen sijaan on organisoitu projekti, jonka puitteissa yksityishenkilöt saavat, ilman pelkoa rikosoikeudellisista seuraamuksista, yrittää etsiä ohjelman kohteesta erityisesti tietoturvaan vaikuttavia haavoittuvuuksia tai ohjelmavirheitä. Bug bounty -ohjelmat ovat viime vuosina muotoutuneet pieneksi ilmiöksi myös kotimaisen tietoturvatestaamisen kentällä – kansainvälinen läpimurto on sen sijaan saavutettu jo joitain vuosia ennen Suomea. Ohjelmien hyödyt on niitä toteuttavissa organisaatioissa tunnistettu siinä määrin, että ensimmäiset kokeilut eivät ole jääneet viimeisiksi: esimerkiksi Verohallinnossa ollaan tällä hetkellä (keväällä 2020) toteuttamassa sekä Tulorekisteriin että OmaVero-palveluun kohdistuvia bug bounty -ohjelmia[2]. Verohallinnon ensimmäinen, vuosina 2017–2018 toteutettu ohjelma oli myös rajattu koskemaan OmaVero-palvelua. Muista kotimaisista julkishallinnon toimijoista käynnissä olevia bug bounty -ohjelmia on ollut Väestörekisterikeskuksella[3] ja ulkoministeriöllä[4]. Myös opetus- ja kulttuuriministeriössä on aiemmin ollut käynnissä bug bounty -ohjelma[5].

Yksityisellä sektorilla bug bounty -ohjelmia on käytetty jonkin verran enemmän kuin julkisella. Kansainvälisinä esimerkkeinä voidaan mainita Facebook[6] ja Google[7], kotimaisena esimerkkinä voidaan mainita aiheen tiimoilta useasti tietotekniikan alan julkaisuissa esiintynyt LähiTapiola[8]. Bug bounty -ohjelmia on kuitenkin käytetty julkisella sektorilla sellaisissakin organisaatioissa kuin Yhdysvaltain puolustusministeriössä[9], eli hyvinkin

[1] Sanastokeskus TSK, Tietotekniikan termitalkoot, *bug bounty*, lisätty 26.8.2018.
[2] Ks. Verohallinto, Tulorekisteri, lehdistötiedote: Hakkerit kutsutaan testaamaan Tulorekisterin tietoturvaa.
[3] Hackr.fi-sivusto: Kutsuohjelma – Väestörekisterikeskus – Suomi.fi Bug Bounty. Nyttemmin kyseessä on organisaatiomuutoksen johdosta Digi- ja väestötietoviraston bug bounty -ohjelma.
[4] Ulkoministeriö, tiedote 29.11.2019: Ulkoministeriö käynnistää palkkionmetsästysohjelman verkkopalvelujen haavoittuvuuksien etsimiseksi.
[5] Opetus- ja kulttuuriministeriö, uutinen: Hakkerit parantamaan kansallisen MPASSid-tunnistuspalvelun tietoturvaa.
[6] Facebookin bug bounty ohjelman säännöt, päivitetty 15.10.2019.
[7] Google application security – Google Security Reward Programs.
[8] LähiTapiolan bug bounty -ohjelma HackerOne.com-palvelussa.
[9] The United States Digital Service: Identifying Security Vulnerabilities in Department of Defense Websites – Hack the Pentagon.

korkean profiilin kohteissa, joiden tietoturvan ja ylipäätään organisaation kiinnostuksen tietoturvaa kohtaan voi olettaa olevan erittäin korkealla tasolla. Tammikuussa 2019 käynnistyi 14 Euroopan komission rahoittamaa bug bounty -ohjelmaa[10]. Ohjelmia ei siis maailmalla julkishallinnossakaan ole nähty uhkana, vaan mahdollisuutena.

Tämän tutkimuksen tavoitteena on antaa tietoa erityisesti kotimaisen julkishallinnon toimijoille siitä, mikä on bug bounty -ohjelma ja voisiko tällaista ohjelmaa soveltaa kyseisen organisaation toimintaan. Tutkimuksen tavoitteena on lisäksi selvittää, millaisia asioita bug bounty -ohjelman suunnittelussa ja toteuttamisessa tulee ottaa huomioon parhaan ja mahdollisimman tuloksellisen lopputuloksen saavuttamiseksi. Tarkoituksena on, että tutkimustuloksia voidaan vastaisuudessa hyödyntää julkishallinnon bug bounty -ohjelmia toteutettaessa.

Tutkimus kuuluu oikeusinformatiikan alaan. Eräiden tahojen mukaan oikeusinformatiikka ei ole oma oikeudenalansa, vaan oikeuden yleistiede tai tutkimuksellinen näkemys, jonka puitteissa pyritään tarkastelemaan oikeudellisia ilmiöitä erityisesti teknologiaväritteisesti[11]. Tämän näkemyksen mukaan oikeusinformatiikka voidaan nähdä eräänlaisena metaoikeudenalana, joka luo tiedonhallinnallisia metodeja ja toimintamalleja muiden oikeudenalojen tutkimusten käyttöön[12]. Toisten tahojen näkökulmasta oikeusinformatiikka taas voidaan laskea omaksi oikeudenalakseen[13], jonka suurin suosio tosin on 1990-luvun jälkeen hiipunut[14]. Tyypillistä oikeusinformatiikan tutkimukselle on ilmiöiden kuvailu, josta nostetaan esille oikeudellista funktiota. Tästä syystä oikeusinformatiikan tutkimus ei ole säännöskeskeistä, vaan siinä tutkitaan tietoteknologian hyödyntämistä oikeudellisissa toiminnoissa tai oikeudellisen tiedon hallintaa.[15]

[10] Reda, 27.12.2018; Euroopan komissio, uutinen 5.4.2019: EU-FOSSA Bug Bounties in Full Force. Suurin osa näistä ohjelmista on keväällä 2020 tauolla tai päättynyt.
[11] Voutilainen 2019, s. 53–54. Saarenpää on esittänyt oikeusinformatiikasta seuraavanlaisen määritelmän: ”Oikeusinformatiikka on vakiintunut, kansainvälinen oikeustieteellinen tutkimus- ja opetusala. Sen puitteissa tutkitaan ja opetetaan oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiä suhteita yleisesti eri muodoissaan samoin kuin niiden yhteydessä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä.” Välittömästi tämän jälkeen Saarenpää kategorisoi oikeusinformatiikan oikeudenalaksi. Saarenpää 2016, s. 67.
[12] Neuvonen 2019, s. 17.
[13] Koulu 2018, s. 848.
[14] Koulu 2018, s. 849.
[15] Voutilainen 2019, s. 53–54.

Oikeudenalajaottelultaan tutkimus kuuluu informaatio-oikeuden ja tietoteknologiaoikeuden (ICT-oikeus)[16] rajapintaan[17], mutta tutkimuksessa tuodaan esiin myös julkisoikeudellisia, erityisesti valtiosääntö- ja hallinto-oikeudellisia näkökulmia, sillä tutkimuksen tarkastelukohteena ovat julkisoikeudelliset toimijat. Informaatio-oikeus myös perinteisesti kiinnittyy julkisoikeuteen[18]. Näiden ohella tutkimuksella on myös rikosoikeudellinen ulottuvuus, sillä tutkimuksessa käsitellään rikoslaissa sanktioituja tieto- ja viestintärikoksia suhteessa bug bounty -ohjelman toteuttamiseen.

Informaatio-oikeuden keskiössä ovat tieto ja informaatio sekä niiden käsittely.[19] Toisaalta informaatio-oikeus käsittelee viranomaisjulkisuuteen ja rekistereihin sekä muuhun informaationhallintaan liittyviä kysymyksiä[20]. Oikeudenalana informaatio-oikeus ilmentyy usean eri oikeudenalan kysymyksissä, kuten juurikin edellä mainittujen valtiosääntöoikeuden, hallinto-oikeuden, rikosoikeuden ja henkilöoikeuden kohdalla.[21]

Tietotekniikkaoikeutta sen sijaan voidaan Lehtosen[22] näkemyksen mukaisesti pitää oikeusinformatiikan osana, jonka puitteissa tutkitaan tietotekniikan ja sen tuotteiden ja palveluiden kehittämiseen, käyttöönottoon ja käyttämiseen liittyviä oikeudellisia sääntely- ja tulkintaongelmia. Tietotekniikkaoikeuden sijaan käytetään nykyään myös laveampaa, ICT-oikeus -termiä, jolloin tarkastelussa ovat myös viestinnän ja eri viestintäverkkojen tuottamat oikeudelliset kysymykset.

Bug bounty -ohjelmien tarkoituksena on parantaa kohdejärjestelmän tietoturvaa. Tietoturvan ylläpitäminen taas on osa rikollisuuden ennaltaehkäisyä. Niinpä bug bounty -ohjelmatkin ovat keino ehkäistä rikollisuutta.

---

[16] Mainitut termit ovat Voutilaisen (2019) käyttämiä. Tietoteknologiaoikeuden tai ICT-oikeuden lähikäsitteisiin kuuluvat nähdäkseni myös termit IT-oikeus ja internetoikeus, jotka Neuvosen mukaan lähestyvät viestintäoikeuden alaa: ks. Neuvonen 2019, s. 17. Jo pelkästään terminologian moninaisuus kertoo, että oikeudenalajaottelu ei ole tältä osin tarkkarajaista ja täsmentynyttä. Onkin helppo yhtyä Neuvosen (2019, s. 17) näkemykseen nimikkeisiin liittyvän keskustelun irrelevanttiudesta.
[17] Saarenpää pitää informaatio-oikeutta ja tietotekniikkaoikeutta oikeusinformatiikan erityiseen osaan kuuluvina tutkimus- ja opetusaloina. Saarenpää 2016, s. 131.
[18] Voutilainen 2019, s. 55–56.
[19] Voutilainen 2019, s. 15.
[20] Neuvonen 2019, s. 16.
[21] Voutilainen 2019, s. 25.
[22] Lehtonen 2015, s. 1–2.

Tietoturva laajassa merkityksessä ei tietenkään rajoitu vain teknologiaan, vaan tietoturvaa on myös moni asia, joihin ei välttämättä liity teknologiaa laisinkaan, kuten kulunvalvonta, tilojen lukitus ja asiakirjojen turvallinen hävittäminen[23]. Tässä tutkimuksessa keskitytään kuitenkin vain tietoturvan digitaalisessa muodossa olevaan informaation käsittelyyn, jolloin voidaan käyttää myös käsitettä kyberturvallisuus[24].

Tutkimuksen taustatarkoituksena on tuoda oikeustiedettä ja tietoturvaa lähemmäs toisiaan – erityisesti tarkoituksena on tehdä tietoturvaa tiettäväksi oikeustieteen parissa[25]. Kaikilla elämän osa-alueilla, myös julkishallinnossa, on käytössä yhä enenevissä määrin sähköisiä palveluja. Julkishallinnon toimintoja digitalisoidaan jatkuvasti ja samalla pyritään siihen, että palveluita käytettäisiin ensisijaisesti sähköisesti[26], vaikkei yksityishenkilöitä voidakaan tällä hetkellä käyttäjinä velvoittaa siihen[27]. Sähköisten palveluiden käyttämistä on kuitenkin pyritty ensisijaistamaan lainsäädännössä[28] ja käynnissä on useampia hankkeita julkishallinnon toimintojen digitalisoimiseksi[29].

Mitä enemmän ja useampia palveluita digitalisoidaan, sitä enemmän näiden palveluiden teknologisiin ratkaisuihin liittyy tietoturvariskejä. Riskien minimoimiseksi tarvitaan uudenlaisia ratkaisuja, kuten tietoturvatestauksen joukkoistamista bug bounty -ohjelmien avulla. Uudenlaiset testausmenetelmät ja niiden hyödyntäminen taas vaativat tutkimusta, myös juridiset näkökulmat huomioon ottaen – tämä tutkimus vastaa juuri tähän tarpeeseen.

---

[23] Sanastokeskus TSK, Tietotekniikan termitalkoot, *tietoturva,* lisätty 6.7.2015. Sanastokeskus TSK:n Tietotekniikan termitalkoot -projektissa on laadittu suosituksia suomenkielisistä tietotekniikan termeistä.
[24] Kyberturvallisuuden sanasto 2018, termi 28: *kyber-*.
[25] Tietoturvaa ja sen tiettäväksi tekemistä oikeustieteen parissa voidaan perustella esimerkiksi seuraavasti: Tutkimusprosessin aikana olin tekemisissä useiden eri juristien kanssa, aina opiskelijoista asiantuntijoiden kautta professoreihin, jotka ovat profiloituneet useille eri juridiikan aloille. Opintojensa loppuvaiheessa olevalta henkilöltä on usein tapana kysyä, mistä aiheesta gradu on tekeillä. Jo hyvissä ajoin ennen gradun valmistumista olin lakannut laskemasta, kuinka monelle henkilölle olin kertonut gradun käsittelevän bug bounty -ohjelmia, ja tämän jälkeen välittömästi saanut selittää parilla virkkeellä, mitä tarkoittaa bug bounty.
[26] Ks. esim. Verohallinto, uutinen 14.11.2019: Verohallinto ja Väestörekisterikeskus kannustavat suomalaisia: Tehdään kansallinen ekoteko ja luovutaan paperipostista.
[27] Myös oikeushenkilöiden kohdalla on esteitä sähköisen asioinnin velvoittamisen suhteen. AOA 4653/4/14, 31.12.2015, joka koskee Verohallinnon käytäntöjä ja (pien)yritystoimintaa. Ks. myös HE 60/2018 vp, s. 66–67.
[28] Ks. esim. L tulotietojärjestelmästä (53/2018) 11.1 §.
[29] Ks. esim. valtiovarainministeriön Valtionavustustoiminnan kehittämis- ja digitalisointihanke VM212:00/2018, asettamispäivä 8.3.2019; työ- ja elinkeinoministeriön säädösvalmisteluhanke koskien yrityspalvelujen asiakastietojärjestelmästä annetun lain ja taloudelliseen toimintaan myönnettävän tuen yleisistä edellytyksistä annetun lain muuttamista. TEM094:00/2018, asettamispäivä 17.12.2018.

Tutkimus on toteutettu yhteistyössä Verohallinnon Turvallisuus- ja riskienhallintayksikön kanssa. Tutkimuksen aiheeseen eli bug bounty -ohjelmiin on päädytty kirjoittajan ja Turvallisuus- ja riskienhallintayksikön yhteisen mielenkiinnonkohteen takia. Verohallinto on ystävällisesti luovuttanut materiaalia tutkimusta varten, kuvannut organisaation toimintatapoja ja bug bounty -ohjelman järjestämistä sekä kommentoinut tutkimuksen tekstiä sen eri vaiheissa.

Tietoturvallisuus koskee yhtä lailla sekä julkista että yksityistä sektoria, jolloin sen tarkastelussa ei voida keskittyä puhtaasti vain toiseen näkökulmaan.[30] Sama ajatus on hyvin havaittavissa myös tässä tutkimuksessa, sillä vaikka tarkastelussa pyritäänkin julkishallinnon näkökulmaan, rakentuu tutkimusaihe myös pitkälti alustayritysten (englanniksi esim. *vulnerability coordination platform*) sekä yksittäisten hakkerien (yksityinen sektori) toiminnan tarkasteluun.

1.2 Tutkimusasetelma ja työn rakenne

Bug bounty -ohjelmien ideana on, että yksityishenkilö saa ilman pelkoa rikosoikeudellisista seuraamuksista yrittää murtautua tiettyyn tietojärjestelmään tai sen osaan, ja mikäli henkilö onnistuu tehtävässä ja raportoi siitä asianmukaisesti, saa hän siitä palkkion. Tietomurto ja sen yritys on kuitenkin määritelty rangaistaviksi teoiksi rikoslain (RL, 39/1889) 38:8:ssä (muutossäädös 368/2015). Bug bounty -ohjelmia on kuitenkin jo toteutettu myös kotimaisella kentällä. Tutkimuksen aiheeseen perehtyessäni en kuitenkaan ole löytänyt julkaistuna sellaista juridista pohdintaa, jonka perusteella ohjelman toteuttamista voitaisiin pitää juridisesti oikeutettuna. Tässä tutkimuksessa pyritäänkin selvittämään, onko bug bounty -ohjelman toteuttaminen Suomen lain mukaista vai ei, ja millä perusteilla. Tutkimuksellisena näkökulmana on keskitytty julkishallintoon, erityisesti Verohallinnon lähtökohdista. Alatutkimuskysymyksenä on sen määrittäminen, mikä taho on julkishallinnollisessa organisaatiossa oikea antamaan luvan ohjelman käynnistämiseen.

Tietoturvaa tarkastellaan tässä tutkimuksessa myös perusoikeuksien näkökulmasta. Tietoturvalla turvataan muun muassa yksityishenkilöiden henkilötietoja, jolloin tietoturvalla

[30] Saarenpää et al 1997, s. LXIX.

turvataan tietosuojaa. Tietosuoja taas linkittyy yksityisyyden suojaan, joka on perustuslain (PL, 731/1999) turvaama perusoikeus (PL 10 §).

Tietoturvallisuuden ohjaukseen liittyy oikeudellisen perspektiivin ohella erottamattomasti sekä tekninen näkökulma että taloudellisen riskienhallinnan ja optimoinnin ulottuvuus.[31] Tutkimuksessa ei myöskään keskitytä puhtaan juridisiin kysymyksiin, vaan bug bounty -ohjelmia tarkastellaan myös oikeustaloustieteellisestä näkökulmasta. Oikeustaloustieteellisellä tarkastelulla pyritään tukemaan tutkimuksen sitä tarkoitusta, jonka myötä halutaan lisätä tietoisuutta tämän testausmuodon olemassaolosta ja sen käyttöpotentiaalista julkishallinnossa. Oikeustaloustieteellinen tarkastelu keskittyy kustannustehokkuuden näkökulmaan. Tutkimuksessa ei kuitenkaan pyritä löytämään julkishallinnon perspektiivistä kaikkein kustannustehokkainta mallia järjestää bug bounty -ohjelma, vaan ohjelman kustannustehokkuutta verrataan aiempaan tutkimukseen nojautuen suhteessa muihin tietoturvatestaamisen muotoihin sekä testaamatta jättämiseen.

Vaikka tutkimuksessa pääsääntöisesti tarkastellaan ohjelmia niiden julkishallinnollisen järjestäjän näkökulmasta, tuodaan tutkimuksessa esiin myös ohjelmaan osallistuvan hakkerin näkökulmaa: tämä tarkastelu linkittyy erityisesti edellä mainittuun kustannustehokkuusaspektiin. Esiin nostetaan hakkerin näkökulmasta ohjelmaan osallistumiseen liittyviä riskejä sekä motivaatiotekijöitä, jotka selittävät osaltaan sitä, miksi bug bounty -ohjelmat ylipäätään mahdollistuvat yhteiskunnallisina konstruktioina; bug bounty -ohjelma ei menesty, mikäli yksikään hakkeri ei osallistu siihen.

Informaatiota voidaan käsitellä sekä manuaalisesti että automaattisesti, joihin molempiin tietoturva liittyy oleellisesti. Tutkimuksessa tietoturvaa käsitellään kuitenkin vain elektronisen toimintaympäristön ja tietotekniikan käytön perspektiivistä. Tästä syystä tutkielman voi sanoa kuuluvan kyberturvallisuuden tutkimusalaan.

Tutkimuksen ensimmäisessä luvussa selostetaan tutkimuksen taustaa ja lähtökohtia. Lisäksi ensimmäisessä luvussa perustellaan tutkimuksessa käytettyjä terminologisia valintoja. Tutkimuksen toisessa luvussa perehdytään yleisellä tasolla siihen, mikä on bug bounty -ohjelma ja mitä tavoitteita ohjelmien järjestämisellä on. Kolmannessa luvussa

[31] Saarenpää et al. 1997, s. 11.

esitellään aiheeseen liittyviä taloustieteen teorioita ja perehdytään taloustieteen, ohjelmien ja juridiikan väliseen liittymäpintaan. Neljännessä luvussa lähestytään tietoturvan ja juridiikan välistä suhdetta muun muassa perusoikeuksien kautta ja avataan tietoturvan teoreettista puolta. Luvussa viisi käsitellään rikoslain tieto- ja viestintärikoksiin liittyviä sanktiointeja ja peilataan niitä bug bounty -ohjelman toteuttamiseen ja ohjelmaan osallistumiseen. Luvussa kuusi keskitytään tutkimuksen varsinaisiin tutkimuskysymyksiin ja pohditaan bug bounty -ohjelmia ja niiden toteuttamista juridisesta perspektiivistä. Seitsemännessä luvussa esitetään tutkimuksen johtopäätökset ja hahmotellaan mahdollisia jatkotutkimusaiheita.

1.3 Metodologiset lähtökohdat

Vaikka tutkielma edustaakin oikeusinformatiikkaa, käytetään tutkimusmetodina myös oikeusdogmatiikkaa. Oikeusdogmatiikan – lainopin – kannanotot koskevat oikeusjärjestykseen kuuluvan normin sisältöä[32]. Oikeusdogmatiikka keskittyy voimassaolevaan oikeuteen, normien eli pitämisen – *sollenin* – maailmaan. Voimassaolevalla oikeudella tarkoitetaan lainsäädännön lisäksi lainvalmisteluaineistoja sekä erityisesti ylimpien tuomioistuinten ratkaisuja.[33] Voimassaolevan oikeuden tarkastelu perustuu oikeuslähdeopille, jonka myötä erilaisille oikeuslähteille annetaan tulkinnassa erilainen painoarvo sen mukaan, millaisessa prosessissa syntyneestä oikeuslähteestä on kyse. Oikeuslähteet jaotellaan vahvasti velvoittaviin (kuten lainsäädäntö), heikosti velvoittaviin sekä sallittuihin lähteisiin – oikeusdogmatiikan pääasiallinen menetelmä on näiden tekstien tulkinta[34]. Erityisesti sallittujen oikeuslähteiden sisältö määräytyy tapauskohtaisesti, sillä kiellettyinä oikeuslähteinä voidaan pitää ainoastaan lain ja hyvän tavan vastaisia sekä avoimen puoluepoliittisia argumentteja.[35]

Oikeusdogmaattisen tutkimuksen tavoitteena on tuottaa systematisoivaa analyysiä siitä, kuinka voimassaolevaa lainsäädäntöä tulisi tulkita. Oikeusdogmatiikan systematisoivaa puolta voidaan nimittää teoreettiseksi ja tulkitsevaa puolta käytännölliseksi lainopiksi,

[32] Aarnio 2006, s. 236.
[33] Hirvonen 2011, s. 21–24.
[34] Hirvonen 2011, s. 36.
[35] Aarnio 2006, s. 292–293.

mutta näitä ei kuitenkaan voida täysin erottaa toisistaan. Näiden ohella lainoppi keskittyy myös oikeusperiaatteiden tulkintaan ja punnintaan, sekä yhteensovittamiseen, mikä edellyttää oikeusnormien tulkintaa.[36]

Hienosyisemmin oikeusdogmatiikkaa tarkasteltaessa tämän tutkimuksen oikeusdogmaattinen lähestyminen painottuu legalistiseen lähestymistapaan, jossa lain sanamuodot ja lainsäätäjän tarkoitus näyttelevät pääroolia. Legalismiin kuuluu, että oikeuslähteiden tulkinta ei ole joustavaa, ja käsitteillä on suuri merkitys tulkinnan kannalta.[37] Oikeusdogmatiikan menetelmät soveltuvat tämän tutkimuksen tarkoituksiin, sillä tavoitteena on oikeuslähteitä tekstianalyyttisesti tutkimalla tuottaa voimassaolevan oikeuden mukainen tulkinta bug bounty -ohjelmien sallittavuudesta sekä niiden käynnistämiseen päätösvaltaisesta tahosta.

Oikeustaloustiede on niin kutsuttu oikeuden monitiede, joka tutkii oikeuden sisällön vaikutusta talouden toimintaan sekä oikeusnormien taloudellista tehokkuutta. Oikeustaloustieteessä apuna käytetään taloustieteen menetelmiä.[38] Tämän tutkimuksen kannalta taloustieteen menetelmät rajoittuvat taloustieteen eräisiin teorioihin.

Tutkimuksessa tarkastellaan, miten bug bounty -ohjelmat käyttäytyvät oikeudellisena ilmiönä markkinoilla – tietoturvan ja sen testaamisen kenttä tulee siis ymmärtää markkinana. Markkinoilla käyttäytyminen on sidoksissa myös bug bounty -ohjelman toteuttamisen muotoon, jonka juridinen oikeutus on eräs tutkielman tarkastelukohde. Bug bounty -ohjelman tarkastelu oikeustaloustieteellisestä perspektiivistä liittyy myös siihen, miksi ohjelmat ylipäätään toimivat oikeudellisena ilmiönä: oikeustaloustieteellisten näkökulmien avulla voidaan selittää hakkerien halukkuutta osallistua ohjelmiin.

Taloustieteellisestä näkökulmasta tutkimus edustaa mikrotaloustiedettä, jossa tarkastellaan talousyksiköiden käyttäytymistä markkinoilla[39]. Tutkimuksessa tarkastellaan bug bounty -ohjelman tilaajan, alustayrityksen sekä hakkerin käyttäytymistä.

[36] Ks. esim. Aarnio 2006, s. 238.
[37] Aarnio 2006, s. 238.
[38] Hirvonen 2011, s. 29, 54.
[39] Määttä 1999, s. 17.

Tutkimus on siis metodiltaan oikeusdogmatiikkaa ja oikeustaloustiedettä yhdistelevä. Monimetodinen lähestymistapa on oikeusinformatiikan tutkimukselle ominaista[40]. Tutkimuskysymykset – bug bounty -ohjelman toteuttamisen juridisten lähtökohtien kuvaaminen ja sen toteuttamiseen luvan antavan pätevän tahon paikallistaminen – ovat vahvasti oikeusdogmatiikan avulla selvitettäviä. Tutkimuksen pääasiallinen tarkoitus – bug bounty -ohjelmien esitteleminen julkishallintoon soveltumisen näkökulmasta – sen sijaan edellyttää laaja-alaisempaa tarkastelua, kuten hakkereiden motivaatiotekijöihin ja ohjelmien markkinamalliin perehtymistä. Kaiken kaikkiaan bug bounty -ohjelmat perustuvat tilaajan, alustayrityksen ja hakkerien väliselle luottamukselle, jolloin tilaajan on syytä ymmärtää myös, millaisista lähtökohdista hakkerit toimivat.

Digitalisaatioon liittyvät kysymykset edellyttävät tieteidenvälistä tarkastelua, mikä voi haastaa oikeustieteen tutkimusperinteitä.[41] Tutkimuksen lähdemateriaalina on käytetty paljon tietotekniikan alan kirjallisuutta, mikä on ominaista oikeusinformatiikalle. Oikeusinformatiikka ylipäätään painottaa tieteidenvälisyyttä ja on lähestymistavaltaan erilainen kuin perinteinen oikeusdogmatiikka. Tästä syystä tutkimuksen pääpaino ei ole oikeusdogmaattisessa tarkastelussa.

1.4 Aiempi tutkimus

Bug bounty -ohjelmiin, haavoittuvuuksien etsimiseen ja tämän etsimisen joukkoistamiseen liittyen on tehty paljon tutkimusta. Tutkimus on pääosin englanninkielistä, kuten tietotekniikan alalla yleensä. Tämän tutkimuksen teon yhteydessä olen lukenut noin 30 artikkelia, jotka käsittelevät jollain tavalla ohjelmistoihin liittyvien haavoittuvuuksien paikallistamista ja löydettyjen haavoittuvuuksien yksityiskohtien julkaisemista, ohjelmien markkinamallia, erilaisiin ohjelmiin liittyvää taloudellista hyötysuhdetta sekä vuorovaikutusta haavoittuvuuden löytäjän ja haavoittuvuuden sisältäneen ohjelmiston edustajien välillä. Artikkelimassasta on havaittavissa alalla tapahtunut kehitys viimeisen 20 vuoden aikana: sen sijaan että pohdittaisiin, kannattaako haavoittuvuuksien etsimiseen kannustaa vai ei, on alettu keskittyä siihen, miten haavoittuvuuksien etsimistä voitaisiin

[40] Ks. esim. Saarenpää 2016, s. 98.
[41] Koulu 2018, s. 842.

optimoida mahdollisimman tehokkaaksi. Tutkimus on pääosin empiiristä: haastattelututkimusta on edelleen kuitenkin vähäisesti, ja hakkereihinkin kohdistuva tutkimus perustuu pääasiassa kerättyyn numeeriseen dataan. Näille tutkimuksille ominaista on matemaattisten mallien luominen kuvaamaan toimijoita ja heidän välistänsä vuorovaikutusta.

Yhtenä harvana aihetta juridisesta näkökulmasta lähestyvänä artikkelina voidaan pitää Elazari Bar Onin artikkelia vuodelta 2018[42], jossa hän on tarkastellut ohjelmien sääntöjä ja kannustanut selkeämpään ja laajempaan turvasatamien (*safe harbor*) käyttöön ohjelmien yhteydessä. Sääntöihin ja turvasatamiin panostamalla voidaan Elazarin mukaan välttää hyvällä asialla oleviin hakkereihin kohdistuvat oikeussyytteet ja kasvattaa luottamusta ohjelmien tilaajien ja hakkeriyhteisön välillä.

Kotimaista tutkimusta bug bounty -ohjelmista on tehty hyvin rajallisesti. Toisaalta, tietotekniikan alalla ei havaintojeni mukaan ole merkityksellistä tehdä samanlaista jakoa kotimaisen ja kansainvälisen tutkimuksen välillä kuin oikeustieteessä. Oikeudellisesta näkökulmasta tutkimuksen aihe on Suomessa ennalta tutkimaton. Kotimaisesta juridisesta kirjallisuudesta on kuitenkin paikallistettavissa joitain kyberrikollisuuteen liittyviä lähteitä, joista oleellisimpana voidaan tämän tutkimuksen kannalta pitää Nevalaisen artikkelia kyberrikoksista Suomen rikosoikeudessa.[43] Nevalainen on artikkelissaan luonut yleiskuvaa kyberrikoksista sekä sivunnut kyberrikollisuuden ominaispiirteitä.

Kotimaiselta juridisen kirjallisuuden kentältä olen lähestynyt aihetta erityisesti tietoturvaan ja tietosuojaan liittyvän kirjallisuuden kautta. Vaikka Saarenpään et al. kirjoittaman teoksen julkaisusta (1997) onkin jo vierähtänyt yli kaksi vuosikymmentä, pitää teoksen väite tietoturvallisuutta koskevan oikeustieteellisen perustutkimuksen vähäisestä määrästä edelleen paikkansa. Mainitun teoksen tarkoituksena onkin ollut oikeudellisen ymmärryksen lisääminen tietoturvallisuuden luonteesta ja sijoittautumisesta oikeudelliseen systematiikkaan sekä tietoturvallisuuden yleisten oppien kehittäminen lainvalmistelun ja sääntelytarpeiden tunnistamisen laajuudessa.[44]

[42] Elazari Bar On 2018.
[43] Nevalainen 2019.
[44] Ks. Saarenpää et al. 1997, s. XI, 3.

Råmanin väitöskirja (Regulating Secure Software Development, 2006) on yksi harvoista teoksista, jotka yhdistävät juridiikkaa ja ohjelmistokehitystä. Kirjan aiheena on ohjelmistokehityksen turvallisuuden sääntely ja se, voisiko sääntelyn avulla parantaa ohjelmistojen turvallisuutta. Tutkimuksen näkökulmana ovat vahvasti kaupalliset ohjelmistot, joille vapailta markkinoilta löytyy kilpailijoita, joten tässä suhteessa tutkimuksen aihe poikkeaa omasta tutkimuksestani suuresti. Råman on käsitellyt väitöskirjassaan ainakin ohjelmistokehityksen kustannustehokkuutta erityisesti ohjelmistojen turvallisuuden näkökulmasta, ohjelmistojen laatua, sekä löydettyjen haavoittuvuuksien raportointia ohjelmistokehittäjille.[45]

Voutilaisen tuore teos (Oikeus tietoon. Informaatio-oikeuden perusteet) vuodelta 2019 käsittelee tietosuoja-asetusta ja vuodenvaihteessa 2020 voimaan astunutta tiedonhallintalakia kattavasti.[46] Teoksessa on myös esitelty laaja-alaisesti informaatio-oikeutta oikeudenalana. Mainittua teosta, joka ei ole niinkään tutkimus vaan oppikirja, on käytetty lähteenä erityisesti tietosuojan ja julkishallinnossa toteutettavan tiedonhallinnan osalta, kuten myös informaatio-oikeutta oikeudenalana kuvailtaessa.

1.5 Terminologiset valinnat

Tietoturva-alalla käytetään usein eri termejä kuvaamaan samoja asioita – terminologiset valinnat saattavat vaihdella hyvinkin käyttäjä- tai kirjoittajakohtaisesti, myös alan ammattilaisten kesken.[47] Bug bounty -ohjelmalle ei ole virallista suomenkielistä vastinetta, mikä on johtanut aiheesta suomen kielellä kirjoitettaessa moninaisiin eri kirjoitusasuihin ja termivalintoihin. Tutkimuksen teon yhteydessä on törmätty ohjelmasta kirjoitettaessa muun muassa seuraaviin ratkaisuihin[48]:

[45] Råman 2006.
[46] Voutilainen 2019.
[47] Råman 2006, s. 6.
[48] Verohallinto, uutinen 23.11.2017; Traficom, uutinen 20.8.2019; Kauppalehti/Tivi 2.10.2017; Petäinen – Taloustaito 2.10.2017; Aitonurmi – Suomidigi 2018; Korhonen – Tivi, lokakuu 2019; Bergström 31.5.2018; Jarnola 2018; Hackr.fi, etusivu; Ulkoministeriö, tiedote 29.11.2019.

Bug Bounty -kampanja	Bug Bounty
BugBounty -kampanja	BugBounty
Bug Bounty -palvelu	Bug bounty
Bug Bounty -ohjelma	bug bounty
Bug bounty -ohjelma	
bug bounty -ohjelma	bugipalkkio-ohjelma
bug bounty -toiminta	bugien metsästysohjelma
bug bounty -alusta	haavoittuvuuspalkkio-ohjelma
bug bounty -pilottihanke	haavoittuvuuspalkinto-ohjelma
bug bounty -projekti	palkkionmetsästysohjelma

Yleisen kielenkäytön ja keskinäisen ymmärryksen kannalta olisi suotavaa, että samasta asiasta käytettäisiin vain yhtä tai mahdollisimman vähälukuista joukkoa eri termejä ja että näiden termien kirjoitusasu olisi vakioitu. Sanastokeskus TSK:n Tietotekniikan termitalkoot -projektin yhteydessä englanninkieliselle termille *bug bounty* on annettu suomenkielisiksi vastineiksi *virheenlöytöpalkkio*, *haavoittuvuuspalkkio* tai *bugipalkkio*.[49]

Tietotekniikan termitalkoot -projektin ehdottamista suomenkielisistä termeistä *virheenlöytöpalkkio* ei vaikuta vakiintuneen kotimaiseen kielenkäyttöön. *Bugipalkkio-ohjelma* sen sijaan olisi terminä melko ymmärrettävä, sillä ohjelmistovirhettä tai haavoittuvuutta tarkoittava sana *bugi* on vakiintunut arkiseen kielenkäyttöön. Bugipalkkio-ohjelma olisi terminä myös helppo yhdistää englanninkieliseen termiin. Vaikka bugipalkkio-ohjelma esiintyykin joissain lähteissä, ei se silti ole toistaiseksi saavuttanut yhtä suurta suosiota kuin englanninkielisen termin käyttäminen. Näiden kahden termin ohella yhtenä mahdollisena käännöksenä bug bounty -ohjelmalle voisi olla *ohjelmavirheen löytöpalkkio*[50], joka kuitenkin on melko pitkä, eikä ole kielenkäytössä vakiintunut.[51]

Tässä tutkimuksessa pyritään käyttämään johdonmukaisesti seuraavia termejä kuvaamaan käsiteltävänä olevaa asiaa: *bug bounty*, kun viitataan joko rahana tai tuotteena maksettavaan palkkioon, johon saaja on oikeutettu joko bug bounty -ohjelmassa tai sen ulkopuolella havaitsemansa ja raportoimansa haavoittuvuuden johdosta, ja *bug bounty -oh-*

[49] Sanastokeskus TSK, Tietotekniikan termitalkoot, *bug bounty*, lisätty 26.8.2018.
[50] Ehkäpä vielä täsmällisempi termi olisi *ohjelmistovirheen* löytöpalkkio. Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[51] Sähköpostikeskustelu 3.10.2019, Hanna Leskelä, Kielitoimiston neuvonta, Kotimaisten kielten keskus.

jelma, kun viitataan ohjelmaan (ja sen toteuttamiseen ja ylläpitämiseen), jonka tarkoituksena on saada yksityishenkilöt yrittämään tunkeutumista tiettyyn tietojärjestelmään tai sen osaan, erikseen määriteltyjen sääntöjen puitteissa. Lisäksi käytetään termejä *haavoittuvuuspalkkio* ja *haavoittuvuuspalkkio-ohjelma*, kun on erityinen tarve käyttää suomenkielistä termiä bug bountyn ja bug bounty -ohjelman sijasta. Tutkimuksessa käytettyihin termivalintoihin on vaikuttanut se, että Verohallinnossa ilmiön kuvaamiseen käytetään mainittuja termejä.

Termivalintoja voidaan perustella myös siten, että englannin kielestä peräisin oleva termi *bug bounty* sekä sen johdannainen *bug bounty -ohjelma* ovat vakiintuneet tietoturva-alalla käyttöön myös suomenkielisessä arkisessa kontekstissa. Valitut kirjoitusasut ovat suomen kieliopin mukaisia[52]. Englanninkielisessä kielenkäytössä bug bounty on myös arkinen, yleisesti käytössä oleva termi, jota virallisempana terminä voidaan pitää *vulnerability rewards program* -termiä. Mainittu *vulnerability rewards program* taas vastaa suomen kielen tutkimuksen aiheena olevaa toimintaa koskevaa virallisempaa ilmaisua *haavoittuvuuspalkkio-ohjelma*.

Suomenkielisissä lähteissä on esiintynyt myös termi *haavoittuvuuspalkinto-ohjelma*. Termi ei kuitenkaan ole siinä mielessä sopiva, että englanninkielinen termi *bounty* on vakiintunut vastaamaan suomenkielistä sanaa *palkkio*, eikä *palkinto*.[53] Tästä syystä tutkimuksessa käytetään toisinaan suomenkielisenä vaihtoehtona termiä haavoittuvuuspalkkio-ohjelma.

Koska bug bounty -ohjelmat ovat alkaneet yleistyä Suomessa ja niitä on jo useampaan otteeseen käytetty kotimaisen julkishallinnon parissa, olisi suotavaa, että toimintaa kutsuttaisiin johdonmukaisesti tietyllä termillä ja että myös termin kirjoitusasu olisi johdonmukainen. Tässä tutkimuksessa käytettäväksi valitut termit on perusteltu, kuten myös niiden kirjoitusasut, mutta jatkokeskustelussa ja ilmiöön viitatessa voidaan yhtä hyvin käyttää myös muita termejä. Erityisesti Sanastokeskuksen Tietotekniikan termitalkoot -projektissa käsitellyt ja suositellut termit kannattaa huomioida käytettäviä termejä valitessa.

[52] Sähköpostikeskustelu 3.10.2019, Hanna Leskelä, Kielitoimiston neuvonta, Kotimaisten kielten keskus.
[53] Sähköpostikeskustelu 3.10.2019, Hanna Leskelä, Kielitoimiston neuvonta, Kotimaisten kielten keskus.

Tutkimuskirjallisuudessa esiintyy useita erilaisia vaihtoehtoja, kun kuvataan yksityishenkilöitä, jotka osallistuvat bug bounty -ohjelmaan, kuten testaaja, tietoturva-asiantuntija, tietoturvatutkija, ja niin edelleen. Tutkimuksessa käytetään säännönmukaisesti termiä *hakkeri* kuvaamaan näitä bug bounty -ohjelmaan osallistuvia yksityishenkilöitä. Termivalinnalla on haluttu tuoda selvästi esille, että puhutaan ohjelmaan osallistuvista henkilöistä, eikä esimerkiksi ohjelman tilaamassa organisaatiossa työskentelevistä henkilöistä. Hakkeri-sanaa käytetään kuvaamaan niin kutsuttuja ”valkohattuja”, eli hyvällä asialla olevia henkilöitä. Jos tekstissä tarkoitetaan niin kutsuttuja. ”black hat” -toimijoita (*malicious hackers* tai *attackers*), puhutaan vihamielisistä hakkereista. Valinnan taustalla on se, että tutkimuksessa on haluttu normalisoida sanan hakkeri käyttöä ja haluttu esimerkiksi erottaa tämä termistä krakkeri[54]. Myös kyberturvallisuuden sanaston mukaan hakkeri-sanalla voidaan tarkoittaa luvalliseen toimintaan osallistuvaa henkilöä.[55] Kuten edellä bug bounty -ohjelma -termiä käsiteltäessä, myös hakkeri-termin kohdalla on nähtävissä, että tieteenalan terminologia on moninaista ja täsmentymätöntä.[56]

[54] Krakkerilla tarkoitetaan henkilöä, joka yrittää tunkeutua tietojärjestelmään luvattomasti. Shirey, R.: RFC 4949.

[55] Kyberturvallisuuden sanasto 2018, termi 41: *hakkeri*. Saman termin kohdalla on huomautuksissa todettu *vihamielisellä hakkerilla* tarkoitettavan henkilöä, joka toimii esimerkiksi luvattomasti.

[56] Esimerkiksi Nevalainen 2019, s. 131 määrittelee hakkeroinnin oikeudenvastaiseksi toiminnaksi. Nevalainen kuitenkin tunnistaa myös tämän tutkimuksen yhteydessä käytetyn valintaperusteen (s. 136, alaviite 28). Terminologiaa on esitellyt myös mm. Gillespie 2016, s. 43–45. Kansallisessa lainvalmisteluaineistossa on viitteitä siitä, että hakkeroinnilla tai hakkerilla tarkoitettaisiin nimenomaisesti oikeudenvastaista toimintaa tai toimijaa (ks. HE 94/1993 vp, s. 140).

2 Bug bounty -ohjelmat pähkinänkuoressa

Tässä luvussa esitellään bug bounty -ohjelman toteuttamista. Bug bounty -ohjelman voi järjestää usealla eri tavalla[57], joista tässä keskitytään pääpiirteittäin vain yhteen malliin. Tämän jälkeen tarkastellaan ohjelmaan liittyvien eri toimijoiden hyötyjä ja riskejä ohjelman suhteen. Viimeisessä alaluvussa esitellään joitakin tutkimuskirjallisuudesta poimittuja kannanottoja, joiden pohjalta bug bounty -ohjelmia voitaisiin parantaa entisestään.

2.1 Bug bounty -ohjelman rakenne

Kuten jo edellä todettua, annetun määritelmän mukaan *bug bountylla* tarkoitetaan haavoittuvuuden tai ohjelmavirheen löytämisestä ja raportoimisesta tarjottavaa palkkiota.[58] Kaikki bugit eivät ole haavoittuvuuksia, vaan ne voivat olla myös muunlaisia virheitä ohjelman koodissa. Tässä mielessä ”bug bounty program” on englanninkielisenäkin terminä hieman puutteellinen kuvaamaan haavoittuvuuspalkkio-ohjelmia, koska yleisesti ottaen ohjelmat keskittyvät tietoturvaliitännäisten haavoittuvuuksien paikallistamiseen, eivätkä kaikkien ohjelmiston käyttöön vaikuttavien virheiden etsimiseen. Usein ohjelman säännöissä on rajattu tällaiset muut kuin tietoturvaan vaikuttavat bugit ohjelman ulkopuolelle.

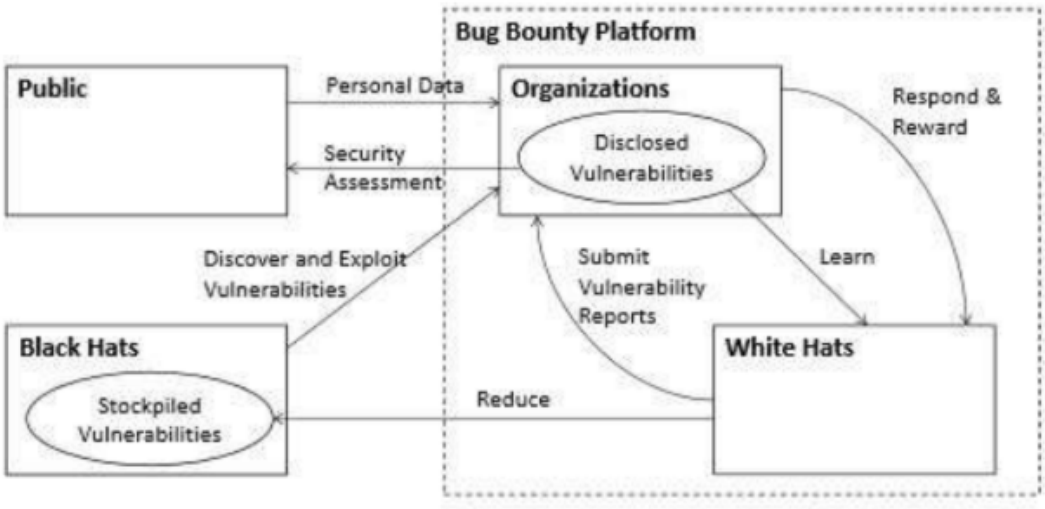
Haavoittuvuuspalkkio-ohjelmista puhuttaessa tulee myös tehdä ero haavoittuvuuspalkkio-ohjelmien ja haavoittuvuuksien julkistamisohjelmien (VDP, *Vulnerability Disclosure Program*) välille. VDP:ssä tarkoitus on, että hakkerit etsivät haavoittuvuuksia ja raportoivat ne julkisille alustoille, kuten postituslistoille. VDP:n erottaa haavoittuvuuspalkkio-ohjelmasta (VRP, *Vulnerability Rewards Program*) se, että haavoittuvuuspalkkio-ohjelmassa keskeistä on löydetystä haavoittuvuudesta maksettu palkkio: bug bounty -ohjelmat ovat siis VRP-ohjelmia. VDP:ssä tärkeimpänä hakkeria motivoivana tekijänä on tiedon jakaminen, yhteisöllinen oppiminen sekä maineen kerryttäminen. Toinen ero ohjelmien välillä on, että haavoittuvuuspalkkio-ohjelmissa haavoittuvuuksien yksityiskohtia ei

[57] Erilaisia malleja on esitelty mm. Ruohosen & Allodin artikkelissa, 2018.
[58] Sanastokeskus TSK, Tietotekniikan termitalkoot, *bug bounty*, lisätty 26.8.2018.

usein julkaista. Haavoittuvuuspalkkio-ohjelma voi olla suoraan ohjelmistoyrityksen itsensä järjestämä, tai vaihtoehtoisesti ohjelmistoyritys voi ostaa palvelun alustayritykseltä, joka toteuttaa haavoittuvuuspalkkio-ohjelmaan liittyvät käytännön toimenpiteet.[59]

Bug bounty -ohjelmat ovat eräänlaista tietoturvan testaamisen joukkoistamista[60]. Yritykset ja muut toimijat tuottavat palveluita, jotka ovat yhteydessä Internetiin. Näissä palveluissa voidaan, kuten Verohallinnon tapauksessa, säilyttää ja käsitellä henkilötietoja tai muita ei-julkiseksi tarkoitettuja tietoja, jolloin palveluiden tulee olla esimerkiksi voimassaolevan tietosuojalainsäädännön mukaisia. Tietosuojaa turvataan tietoturvalla: tietoturvaan liittyvät ratkaisut pyrkivät siihen, että tietoja pääsee katselemaan tai käsittelemään vain sellainen henkilö tai taho, jolla siihen on oikeus.

Seuraavassa Zhaon et al. laatimassa kuvassa[61] on esitetty bug bounty -ohjelman toimintamalli, jossa ohjelman toteuttamisessa on mukana erillinen alustayritys (*platform*). Verohallinnossa käytössä olleet bug bounty -ohjelmat ovat toimineet jotakuinkin kuvassa esitetyn kaltaisella mallilla.



Kuva 1: Haavoittuvuuksien paikallistamisen ekosysteemin rakenne Zhaon et al. (2015, s. 1107) mukaan.

[59] Ks. esim. Zhao et al. 2014.
[60] Ks. esim. Elazari Bar On 2018.
[61] Zhao et al. 2015, s. 1107.

Ennen ohjelman aloittamista ohjelmalle määritellään rajat (*scope*), kuten millaisia haavoittuvuuksia koskevia raportteja otetaan vastaan, osallistumiseen liittyvät kriteerit kuten osallistujan ikä, muut ehdot esimerkiksi raportointiin liittyen, sekä kuvataan raporttien tarkastusprosessi. Ohjelman rajauksena voi olla jokin yksittäinen ohjelmistotuote, ohjelmistotuotteiden joukko, palveluinfrastruktuuri tai koko organisaatio.[62]

Kuvan 1 mallin mukaisesti tilaaja (*organization*) ostaa alustayritykseltä (*platform*) palvelun, jonka mukaisesti alustayritys tuottaa tilaajalle bug bounty -ohjelman. Ohjelmalle laaditaan säännöt ja rajat (*scope*) jonka sisällä yksityishenkilöinä toimivat hakkerit (*white hats*) saavat murtautua tai yrittää murtautua ohjelman kohteena oleviin järjestelmiin. Mikäli hakkerit havaitsevat bugeja, raportoivat he näistä alustayritykselle. Alustayritys tarkastaa hakkerien raportit, ja mikäli raportti osoittautuu paikkansapitäväksi, maksaa alustayritys kunkin haavoittuvuuden ensiksi raportoineelle hakkerille palkkion, jonka suuruus riippuu haavoittuvuuden laadusta, yleensä vakavuusasteesta. Ohjelmien tavoitteena on muun muassa vähentää vihamielisten, oikeudetta järjestelmään tunkeutuvien hakkereiden (*black hats*) toimintamahdollisuuksia ja houkutuksia[63] tukkimalla järjestelmien haavoittuvaisuuksia hyväntahtoisten hakkerien avustuksella.

Se, millainen hakkeri voi osallistua kuhunkin bug bounty -ohjelmaan, riippuu ohjelman säännöistä: osa ohjelmista toimii kutsuperiaatteella, osa taas on avoimia kaikille halukkaille. Esimerkiksi Verohallinnon OmaVero-järjestelmää koskevaan ensimmäiseen bug bounty -ohjelmaan saivat osallistua kaikki halukkaat, mutta osallistujalla tuli olla tunnukset, jolla palveluun pystyi kirjautumaan. Lisäksi ohjelmaan tuli rekisteröityä alustayrityksen kautta – rekisteröitymisen vaatimus on yleinen käytäntö, joskin poikkeuksiakin on olemassa[64]. Verohallinnon Tulorekisteriä koskeva bug bounty -ohjelma sen sijaan on eräänlainen versio kutsuohjelmasta.

Alustayrityksen roolin voi myös pilkkoa useampaan osaan: alustan, jolle esimerkiksi haavoittuvuusraportit palautetaan, voi hankkia yhdeltä taholta, ja varsinaisen raporttien läpikäymisen ja palkkioiden maksamisen toiselta taholta. Tilaajaorganisaation resursseista

[62] Kuehn 2014.
[63] Ks. esim. Elazari Bar On 2018.
[64] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.

riippuen tilaaja voi myös itse huolehtia raporttien tarkistamisesta, viestinnästä ja palkkioiden maksamisesta.[65] Mikäli tilaajalla on tarpeeksi resursseja käytettävissään, voi se luonnollisesti vastata itse ohjelmasta kokonaisuudessaan.

Bug bounty -ohjelmien välillä löytyy eroavaisuuksia myös sen suhteen, millaisia tietoja testattavasta kohteesta osallistuvilla hakkereilla on käytettävissään. Esimerkiksi Verohallinnon bug bounty -ohjelmat ovat olleet mallia *black box*, eli osallistujat eivät näe ohjelman kohteena olevan tietojärjestelmän lähdekoodia. On olemassa myös sellaisia ohjelmia, joissa lähdekoodi on osallistujien saatavilla. Hakkereilla on tietyt strategiat, joiden mukaan he etsivät haavoittuvuuksia. Yksi strategia on etsiä tietyntyyppisiä haavoittuvuuksia tietyn ajanjakson aikana, koska jokainen haavoittuvuustyyppi edellyttää omanlaisia taitoja haavoittuvuuksien löytämiseksi. Toinen mahdollinen strategia on käydä perinpohjaisesti läpi tietty verkkosivu tietyn ajanjakson aikana, sillä sivuston arkkitehtuuriin ja koodiin perehtyminen edistää haavoittuvuuksien löytämistä.[66]

Kun palvelun kysyntä lisääntyy, lisääntyy myös sen tarjonta. Bug bounty -ohjelmien kysyntää alkaa vähitellen olla Suomessakin – yksityisellä sektorilla erityisesti LähiTapiola on kunnostautunut aktiivisena bug bounty -ohjelmien tai sen kaltaisten ohjelmien tilaajana[67]. Julkisella sektorilla bug bounty -ohjelmia on toteutettu ainakin Verohallinnossa[68], Väestörekisterikeskuksessa ja sen jatkona Digi- ja väestötietovirastossa[69] sekä opetus- ja kulttuuriministeriössä[70]. Kansainvälisiä suuria toimijoita, bug bounty -ohjelmien alustoja, ovat esimerkiksi HackerOne, Bugcrowd ja Intigriti.

Bug bounty -ohjelmiin osallistuvat hakkerit eivät lähtökohtaisesti ole työ- tai toimeksiantosuhteessa ohjelman tilanneen organisaation tai alustayrityksen kanssa.[71] Hakkerit ovat yksityishenkilöitä ja osallistuvat kuhunkin bug bounty -ohjelmaan puhtaasta vapaasta tahdosta, ilman ulkoisia velvoitteita osallistua siihen.

---

[65] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[66] Haavoittuvuuksien etsimisen strategioista tarkemmin ks. Zhao et al. 2014.
[67] LähiTapiola, uutinen 17.8.2017.
[68] Verohallinnon tiedote, 2.10.2017.
[69] Väestörekisterikeskus – Kokemuksia Bug Bounty -ohjelmasta, 31.8.2018.
[70] Opetus- ja kulttuuriministeriö, uutinen 10.9.2018.
[71] Tämä on usein kielletty säännöissä, kuten myös ohjelman kohteen kehittämiseen tai testaamiseen osallistuminen. Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.

Bug bounty -ohjelmia ei nähdäkseni voi varsinaisesti pitää kilpailuina, mutta niissä on yllättävän paljon kilpailullisia piirteitä: ohjelmassa maksetaan palkkio taitavalle henkilölle (hakkeri), joka nopeimmin vastaa tehtävänantoon (löytää bugin). Toisaalta edes kilpailun järjestäjä (tilaaja ja alustayritys) ei tiedä, onko kilpailussa ylipäätään mahdollista saada palkkiota. Alustayritys on yritys, jonka ensisijaisena tavoitteena on vähintäänkin kotimaisessa osakeyhtiömuodossa toimiessaan tehdä omistajilleen voittoa (osakeyhtiölaki 624/2006, 1:5). Yritys toimii liiketaloudellisin perustein ja sen liiketoiminta muodostuu ”kilpailujen” eli bug bounty -ohjelmien järjestämisestä. Yritys ei kuitenkaan ole vastuussa siitä, että ”kilpailusta” voisi voittaa yhtään mitään. Koska tietojärjestelmät ovat ihmisten tekemiä, ja ihmiset tekevät virheitä, on kuitenkin todennäköistä, että järjestelmistä löytyy virheitä – siis haavoittuvuuksia. On siis todennäköistä, että bug bounty -ohjelmien kohteena olevista järjestelmistä löytyy haavoittuvuuksia, vaikka niitä ei ennalta kyetäkään määrittelemään. Lisäksi tietoturva ei ole stabiilia, vaan turvallisuuden taso muuttuu ajassa. Tämä tarkoittaa sitä, että vaikkei tunnettua tai ennalta tuntematonta haavoittuvuutta löytynytkään jostain teknisestä ratkaisusta vuosi sitten, voi siitä tänään sellainen löytyä. Tietoturvaa tulisikin ajatella prosessina, ei projektina[72]. Koska haavoittuvuuksien löytyminen on todennäköistä – vaikka todennäköisyyden astetta onkin vaikea määrittää – on bug bounty -ohjelmaan osallistumisesta silti yleisesti ottaen jaossa palkkioita osaavimmille ja nopeimmille hakkereille. Mikään taho ei kuitenkaan edelleenkään ole vastuussa siitä, että ”kilpailusta” voisi voittaa yhtikäs mitään.

2.2 Ohjelman hyötyjä ja riskejä eri toimijoiden näkökulmasta

Seuraavassa tarkastellaan ohjelmaan liittyvien eri toimijoiden – erityisesti ohjelman tilaajan, alustayrityksen ja hakkerin – näkökulmasta bug bounty -ohjelman järjestämisen ja siihen osallistuvien hyötyjä, kuten myös ohjelmaan liittyviä riskejä. Kuten seuraavista alaluvuista voidaan havaita, ohjelmien hyötyjä ja riskejä on tutkimuskirjallisuudessa tarkasteltu lähinnä ohjelman tilaajan tai ohjelman kohteen näkökulmasta.

[72] Ks. esim. Andreasson & Koivisto 2013, s. 241.

2.2.1 Tilaaja

Tilaaja, kuten Verohallinto, maksaa alustayritykselle palvelun järjestämisestä, mikäli ei se tuota bug bounty -ohjelmaa itsenäisesti. Tilaajan yhtenä tärkeimpänä tavoitteena on parantaa ohjelman kohteen tietoturvaa. Tietoturvan tason parantumista voidaan pitää ohjelman käytöstä koituvana suorana hyötynä. Hyötyjen todellisuutta voidaan kutenkin myös kritisoida: Mikäli haavoittuvuusraporttien määrä jää alhaiseksi, tilaaja saa potentiaalisen varmistuksen järjestelmiensä tietoturvan senhetkisestä korkeasta tasosta. Syynä raporttien vähyyteen voi kuitenkin olla liian pienet palkkiot, liian kapea rajaus ohjelmalle, korkea aloituskynnys osallistua ohjelmaan, ja niin edelleen. Jos taas relevantteja raportteja saadaan runsaasti, tilaaja voi paikata ohjelman kohteessa olevat haavoittuvuudet ja kohteen tietoturvan taso paranee. Bug bounty -ohjelmissa testauksen kattavuus jää kuitenkin usein epäselväksi, ja esimerkiksi aktiivisten hakkereiden määrällä on suuri vaikutus siihen, kuinka paljon haavoittuvuuksia löydetään[73].

Ohjelmasta riippuen haavoittuvuuspalkkio-ohjelmien on eräissä tutkimuksissa todettu olevan 2–100 kertaa kustannustehokkaampia tapoja toteuttaa tietoturvan testaamista verrattuna asiantuntijan palkkaamiseen.[74] Vaikka haavoittuvuuspalkkio-ohjelmat voivat olla kustannustehokas tapa paikallistaa haavoittuvaisuuksia järjestelmistä,[75] testauksen epäselvästä kattavuuden asteesta johtuen suosituksena on usein, että bug bounty -ohjelma ei olisi ensimmäinen keino järjestelmän tietoturvan testaamiseksi, vaan pikemminkin täydentävä testausmuoto.[76]

Bug bounty -ohjelman käyttämisellä on etunsa suhteessa siihen, että ohjelmaa ei olisi ja hakkeri olisi löytänyt haavoittuvuuden. Tuolloin hakkeri saattaisi vain julkistaa haavoittuvuuden (*full disclosure*) jollakin asialle omistautuneella julkaisualustalla, kuten keskustelupalstalla.[77] Riippuen raportin laajuudesta ja yksityiskohdista, julkistaminen voi vaarantaa hakkeroidun organisaation immateriaalioikeuksia tai paljastaa liikesalaisuuksia, mistä julkistuksen tehnyttä hakkeria voidaan yrittää saada oikeudelliseen vastuuseen. On

[73] Zhao et al. 2014.
[74] Finifter et al. 2013, s. 286.
[75] Finifter et al. 2013, s. 280.
[76] Mm. sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[77] Bug bounty -ohjelma ei toki estä hakkeria julkistamasta haavoittuvuuden yksityiskohtaisiakin tietoja, mutta mikäli tämä on ohjelman säännöissä kielletty, on kyseessä silloin sääntörikkomus.

siis sekä hakkerin että organisaation näkökulmasta kannattavaa ylläpitää bug bounty -ohjelmaa, jolloin organisaation on mahdollista kontrolloida sitä, millaisia yksityiskohtia löydetyistä haavoittuvuuksista julkaistaan, vai julkaistaanko mitään.[78]

Bug bounty -ohjelman käyttäminen nähdään myös usein PR-hyötynä, sillä ohjelman käynnistämisellä voidaan viestiä kuluttajille tai järjestelmän käyttäjille siitä, että tilaaja on kiinnostunut ohjelman kohteen tietoturvasta. Mainehyöty saattaa kuitenkin kääntyä myös riskiksi: mikäli ohjelman kohteesta löytyy paljon haavoittuvuuksia, viestii se, että ohjelman kohteen tietoturvan taso ei alun perin ole ollut kovin korkealla. Tämä taas voi johtaa maineen kärsimiseen. Maineriskit voivat aktualisoitua niin julkishallinnossa kuin yksityisellä sektorilla.

Turvallisuuden merkityksen ymmärryksen kasvaessa kasvaa myös turvallisuuteen panostamisen arvostaminen. Kun ohjelmistossa on vähän haavoittuvuuksia, ja ne vähätkin löydetyt korjataan nopeasti, voidaan tätä käyttää markkinoinnissa organisaation eduksi kasvattamalla organisaation hyvää mainetta turvallisten ohjelmistojen käyttäjänä tai tuottajana.[79] Bug bounty -ohjelmilla voidaan viestittää ohjelmistoa harkitseville käyttäjille, että ohjelmiston turvallisuuteen on panostettu ja että se on laadukas.[80] Erityisesti tällä on merkitystä yritysten kohdalla, mutta hyötyjä voidaan nähdä myös julkishallinnollisen organisaation kohdalla, jolla ei lakisääteisestä monopolistaan johtuen ole kilpailijoita: julkishallinnon organisaatioilla on edelleen lakiin perustuva velvollisuus huolehtia tietoturvan riittävästä tasosta sekä tietosuojasta.

Bug bounty -ohjelman tilaajan maineella, toisin sanoen ohjelman maineella, on myös vaikutusta siihen, kuinka hyvin ohjelma onnistuu, eli kuinka paljon haavoittuvuusraportteja palautetaan. Mitä enemmän haavoittuvuuksia raportoidaan, sitä enemmän on myös havaittu löydettyjä haavoittuvuuksia.[81] Voidaankin siis pitää ohjelman onnistumisen kannalta tärkeänä, että tilaaja ja alustayritys toimivat luotettavasti ja vakuuttavasti, sillä se lisää osallistumisintoa ja sen myötä parantaa osallistumisen kattavuutta.

[78] Ks. esim. Råman 2006, s. 88. Tässä tutkimuksessa ei käsitellä tämän tarkemmin tietoturvaan tai ohjelmistonkehitykseen liittyviä immateriaalioikeuksia tai liikesalaisuuksia sääntelevää lainsäädäntöä.
[79] Ks. Råman 2006, s. 236–237.
[80] Egelman et al. 2013; ks. myös Laszka et al. 2016, s. 161.
[81] Maillart et al. 2017.

Kuten tässä tutkimuksessa myöhemmin tarkemmin käydään läpi, haavoittuvuuksien etsimistä ja jakamista voidaan kuvata markkinamallin avulla. Kun organisaatiot osallistuvat bug bounty -ohjelmien myötä haavoittuvuusmarkkinoille itse, ei markkinoiden sääntely jää yksin haavoittuvuuksia raportoivan tahon, hakkereiden, valtaan.[82] Näillä jo olemassa olevilla haavoittuvuusmarkkinoilla hakkerit toimivat omista lähtökohdistaan ja motiiveistaan, kuten kasvattaakseen mainettaan.[83] Osallistumalla markkinoille organisaatiot saavat tuotua esiin myös omia motiivejaan. Markkinoilla mukana oleminen auttaa ymmärtämään markkinoita, jolloin niiden toimintaa voidaan myös mallintaa ja ennakoida[84], eli turvallisuustoimenpiteitä on mahdollista kehittää entistäkin tehokkaammiksi.

Eräät organisaatiot ovat kritisoineet sitä, että hakkerit ottavat ennalta arvaamattomasti yhteyttä ilmoittaakseen haavoittuvuuden ja toteavat julkaisevansa sen, mikäli asialle ei tehdä mitään. Näiden organisaatioiden puolelta tällaiseen toimintaan on suhtauduttu jopa kiristyksenä.[85] Kun organisaatiolla on käynnissä bug bounty -ohjelma, hakkereille annetaan selvät säännöt ja ohjeet siitä, miten organisaatiota tulee lähestyä, jotta väärinkäsityksiltä ja epätoivotuilta yhteydenotoilta vältyttäisiin.

Kaikki hakkerit eivät kuitenkaan ole hyväntahtoisia hakkereita. Siksi bug bounty -ohjelmiin kuuluvana riskinä on, että joukossa on myös vihamielisiä hakkereita, joilla on osallistuessaan ohjelmaan niin oikeudellisessa kuin hakkerietiikan mielessä kyseenalaisia motiiveja. Ainakaan toistaiseksi tätä riskiä ei ole bug bounty -ohjelmia toteuttavissa tai tilaavissa organisaatioissa pidetty niin suurena, että se peittäisi bug bounty -ohjelmista saavutettavat hyödyt[86]. Tätä riskiä myös taklataan käytännössä järjestämällä kutsuohjelmia, joihin kutsuttavat osallistujat ovat tunnettuja henkilöitä[87]. Ohjelmien yleisenä hyötynä voidaan nähdä myös, että hakkereiden raportoimat haavoittuvuudet kaventavat vihamielisten hakkereiden mahdollisuuksia löytää ja käyttää hyväkseen ohjelmistoissa olevia haavoittuvuuksia.[88]

---

[82] Ks. Råman 2006, s. 232–233.
[83] Egelman et al, 2013; Råman 2006, s. 238, 244.
[84] Egelman et al. 2013.
[85] Råman 2006, s. 238, 244.
[86] Organisaatioissa, joissa bug bounty -ohjelmia sen sijaan ei ole otettu käyttöön, saatetaan olla päädytty toisenlaisiin johtopäätöksiin.
[87] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[88] Kilovaty 2019, s. 504–505. Kilovaty tosin yhdistää tämän ajatuksen lainsäädännön avulla aikaan saataviin muutoksiin, kun itse koen, että markkinat kykenevät sääntelemään itse itseään, eikä lainsäätäjän oh-

Bug bounty -ohjelmien yhtenä selvimpänä hyötynä on se, että tavallista useampi henkilö antaa aikansa ja työpanoksensa haavoittuvuuksien etsimiselle. Laaja ja heterogeeninen joukko hakkereita tutkii ohjelmistoja – näin laajan joukon palkkaaminen työntekijänä tutkimaan ohjelmistoa tulisi todennäköisesti erittäin kalliiksi. [89]

On perusteltua väittää, että merkittävästi suurempi määrä testaajia löytää enemmän haavoittuvuuksia kuin pieni määrä testaajia, vaikka jälkimmäisillä olisikin enemmän aikaa ja lähdekoodi käytettävissään.[90] Samalla haavoittuvuuksien löytymisen kannalta on tehokkaampaa, että kaikki testaajat testaavat yhtäaikaisesti ohjelman kaikkia ominaisuuksia kuin että tehtäväalueet olisi jaettu.[91]

Hyväntahtoisten hakkerien toiminnalla on suuri merkitys kyberturvallisuudelle sekä VDP:ille että haavoittuvuuspalkkio-ohjelmille. Yksi syy tälle on se, että osa hyväntahtoisista hakkereista on kyberturvallisuuden asiantuntijoita. Mahdollistamalla hyväntahtoisten hakkerien osallistumisen haavoittuvuuksien etsintään saadaan käyttöön laajempi osaamispohja ja uudenlaisia näkökulmia verrattuna yritysten sisäisiin turvallisuusasiantuntijoihin. Mitä enemmän ohjelmissa on osallistujia, sitä laajemmalta osaamiskentältä osallistujia on, mikä taas johtaa siihen, että haavoittuvuuksia löydetään enemmän.[92]

Ohjelmistojen testausta voidaan mitata ja näistä mittauksista voidaan antaa tuloksia ohjelmiston turvallisuudesta. Useissa lähteissä on kuitenkin todettu, että tulokset eivät kerro ohjelmiston hyvyydestä tai turvallisuudesta kovinkaan paljon: ne kertovat vain testissä suoriutumisesta. Kun testattu ja turvalliseksi todettu ohjelmisto annetaan rajatun ryhmän ulkopuolelle testattavaksi, löytyy siitä usein lisää merkittäviä haavoittuvuuksia. Toisin sanoen: mitä enemmän testaajia, sitä useampia haavoittuvuuksia löydetään.[93]

---

jaukselle ole tästä syystä tarvetta. Sinänsä Kilovatyn havainto siitä (s. 508), ettei haavoittuvuuksien julkistamiselle ole yhtä yhtenäistä menettelyä eikä auktoriteettiasemassa oleville säännöille olisi tarvetta, on oikea. Aiheeseen liittyvien moninaisuuksien vuoksi en kuitenkaan koe, että lainsäädäntö olisi paras mahdollinen auktoriteetti.

[89] Laszka et al. 2016, s. 161.

[90] Ks. esim. Anderson 2002, jossa kirjoittaja on käyttänyt kuvauksessaan lukumäärinä ”muutamaa tusinaa” ja ”kymmeniä tuhansia”.

[91] Ks. Brady et al. 1999.

[92] Zhao et al. 2014.

[93] Ks. Brady et al. 1999.

Toistaiseksi ei ole olemassa systemaattista algoritmista lähestymistapaa, jolla haavoittuvuuksista päästäisiin eroon samalla nopeudella kuin uusia ohjelmistoja luodaan. Haavoittuvuuksien paikallistamiseen laaditut ohjelmistot eivät kykene löytämään ja tunnistamaan kaikkia mahdollisia haavoittuvuuksia. Ihmisaivot ovat siis yhä yksi tehokkaimmista keinoista tutkia uusia ongelmia.[94]

Suurella osallistujamäärällä on kuitenkin myös kääntöpuolensa. Jos bug bounty -ohjelmasta tulee erittäin suosittu, muodostuvat ohjelman pyörittämisen kustannukset – esimerkiksi raporttien tarkastamisesta johtuvat kustannukset – suuriksi. Resurssien kohdentaminen ei siis ole yksinkertaista. Pohdittavaksi nousee myös kysymys siitä, onko ohjelman toteuttaminen ylipäätään taloudellisesti kannattavaa.[95]

Eräänä bug bounty -ohjelmien riskinä voidaan pitää niiden puitteissa palautettuja heikkolaatuisia, irrelevantteja tai jopa virheellisiä haavoittuvuusraportteja, sekä sellaisia raportteja, joissa raportoitu haavoittuvuus ei ole kuulunut bug bounty -ohjelman rajauksen piiriin. Osa näistä epätoivotuista raporteista on selitettävissä automaattiskannereiden käytöllä, osa esimerkiksi heikolla ohjelman sääntöihin perehtymisellä. Käytännössä ei-toivottujen raporttien määrä on merkittävä.[96] Heikkolaatuiset raportit syövät ohjelman kustannustehokkuutta.

Ohjelman järjestämisen haasteisiin kuuluu myös sopivan palkkiotason löytäminen. Toisaalta erityisesti kriittisiä ympäristöjä – kuten rahoitusta, terveydenhuoltoa ja julkista hallintoa – koskien on kyseenalaista, voiko palkkio koskaan olla niin korkea, että jokin taho ei olisi halukas maksamaan laittomilla markkinoilla laillisia markkinoita korkeampaa hintaa löydetystä haavoittuvuudesta. Vaikka laillisilla markkinoilla onkin hakkerin näkökulmasta riskittömämpää toimia kuin laittomilla markkinoilla, minkä takia palkkion ei tarvitse olla suuruudeltaan samaa luokkaa kuin laittomilla markkinoilla, on organisaatioilla silti oltava varaa maksaa palkkio, mikä voi ylittää monen organisaation maksukyvyn.[97] Jos palkkiot mitoitetaan liian suuriksi, erityisesti pitkäkestoisissa ohjelmissa palkkioiden maksaminen voi vähentää haavoittuvuuksien ehkäisemiseen käytettäviä resursseja.[98]

[94] Maillart et al. 2017; ks. Doupé et al. 2010.
[95] Fryer & Simperl 2017.
[96] Laszka et al. 2016, s. 162.
[97] Böhme 2006.
[98] Egelman et al. 2013.

Vaikka palkkion maksaminen yleisesti ottaen kannustaa hakkeria työskentelemään paremmin, ei raha kuitenkaan motivoi kaikkia testaajia. Rahan ohella hakkeria voivat motivoida esimerkiksi eettiset seikat.[99]

Kuten jo edellä on esitetty, bug bounty -ohjelmia kohtaan voidaan esittää myös vasta-argumentteja. Kriittisimpien näkökulmien mukaan toiminta on epäilyttävää ja moraalisesti arveluttavaa. Ohjelmat mahdollistavat sen, että niihin osallistuu myös vihamielisiä hakkereita, ja edelleen kyberrikollisen piirit voivat risteytyä järjestäytyneen rikollisuuden ja terrorismin kanssa, eikä niitä tule rahoittaa. Haavoittuvuuksista maksamisen on spekuloitu myös kannustavan haavoittuvuuksien piilottamisen järjestelmiin myöhempää löytämistä varten.[100]

Yleisen tietoturvakehityksen näkökulmasta kriittisenä tekijänä voidaan nähdä myös ohjelmistokehittäjien hitaus tai passiivisuus. Jos ohjelmistokehittäjä ostaa haavoittuvuuden, se voi vaatia salassapitosopimusta kaupan ehtona, mikä voi johtaa siihen, että haavoittuvuus korjataan paljon hitaammin verrattuna tilanteeseen, jossa haavoittuvuus olisi vain julkaistu. On myös esitetty, että bug bounty -ohjelmat eivät ole kustannustehokkain tapa allokoida resursseja. Kustannustehokkaampaa olisi esimerkiksi käyttää palkkioita kannustamaan ohjelmistonkehittäjiä tekemään vähemmän virheitä.[101]

2.2.2 Alustayritys

Bug bounty -ohjelmassa toimivan alustayrityksen tärkeimpänä hyötynä ohjelmaan osallistumisesta on raha: ohjelmaan osallistuminen mahdollistaa yrityksen olemassaolon. Sen sijaan alustayrityksen liiketoiminnalliset riskit ovat liiketoiminnan pyöriessä melko vähäiset. Alustayritykseen kohdistuvat riskit painottuvat sellaisiin yksityiskohtiin, joihin se kykenee itse pääasiassa vaikuttamaan. Tällaisia ovat esimerkiksi se, että ohjelman järjestelyt on hoidettu huonosti: hakkereiden raportteihin ja viesteihin ei vastata tarpeeksi nopeasti, tai että alustayritys ei maksakaan palkkioita ohjelmassa sovitulla tavalla. Näistä seikoista aiheutuu maineriski, mikä voi vaikuttaa seuraavien toimeksiantojen saamiseen.

[99] Egelman et al. 2013.
[100] Egelman et al. 2013.
[101] Egelman et al. 2013.

Mikäli alustapalveluihin liittyvät tehtävät on jaettu kahtia, kuten siten, että yksi yritys vastaa varsinaisen alustan tarjoamisesta ja toinen yritys muusta ohjelman pyörittämisestä, voidaan riskejä pitää molempien osalta edelleen melko vähäisinä ja sellaisina, että niihin voidaan hyvin pitkälti vaikuttaa omalla toiminnalla. Alustayrityksen kannalta ohjelman kiistattomana hyötynä on siis oman liiketoiminnan mahdollistuminen.

Vaikka bug bounty -ohjelmiin liittyvässä yritystoiminnassa toteutetaan hakkerietiikkaa ja open source -maailmasta tuttua vapaan käytön ja jakamisen periaatetta, on prosessissa toimija, jonka liiketaloudellinen malli perustuu sille, että muiden henkilöiden hyväntahtoisuus ja innokkuus ensinnäkin mahdollistavat tämän toimijan olemassaolon ja toisekseen voiton tekemisen. Kuitenkin jo ennen bug bounty -ohjelmien yleistymistäkin on ollut useita yrityksiä, jotka ovat, enemmän tai vähemmän onnistuneesti, yhdistäneet liiketoimintaansa open source -ajattelua[102].

2.2.3 Hakkeri

Bug bounty -ohjelman toimijana hakkerit voidaan jakaa kahteen kategoriaan: niihin, jotka raportoivat haavoittuvuuden ja saavat siitä palkkion, ja toisaalta niihin, jotka eivät saa antamastaan panoksesta palkkiota, joko siitä syystä, etteivät he paikallista haavoittuvuuksia, tai siitä syystä, että joku toinen on raportoinut heidän löytämänsä haavoittuvuuden jo aiemmin. Hakkerien osalta ohjelmiin osallistumisen hyödyt ja riskit ovat siis huomattavasti moninaisempia kuin esimerkiksi alustayrityksen kohdalla.

Yhdistävänä hyötynä kaikkien hakkerien osalta voidaan nähdä mahdollisuus yrittää murtautua järjestelmään joutumatta siitä rikosoikeudelliseen vastuuseen. Ilman bug bounty -ohjelman olemassaoloa murtautumisen yrittäminen olisi rangaistava teko. Lisäksi, mikäli se alustayrityksen toimintamalliin kuuluu, haavoittuvuuksia paikallistavilla hakkereilla on mahdollisuus saada mainetta ja kunniaa yrityksen julkisena esittämässä suoritustaulukossa (esim. *leaderboard*).

[102] Tapauskertomuksia open source -maailman yrityksistä ja niiden liiketoimintamalleista on eritelty esim. teoksessa Ingo 2005, s. 61–147.

Hakkereita motivoivia tekijöitä ovat tunnustus ja kiitos löydetystä haavoittuvuudesta, taloudellinen korvaus, ja toisaalta myös löytöjen tuoma kuuluisuus ja oman maineen kasvattaminen, joka voi poikia uusia mahdollisuuksia taloudelliseen hyötymiseen,[103] esimerkiksi työllistymällä tietoturva-alan yrityksiin. Näiden ohella motivaationa haavoittuvuuksien etsimiselle on esimerkiksi tiedonjakaminen ja yhteisöllinen oppiminen[104]. Tämän lisäksi motivaatiotekijöiksi, joiden vuoksi hakkerit puuhastelevat laitteiden ja ohjelmistojen parissa, voidaan lukea ajanviete ja yleinen kiinnostus, oppimisen ilo, itsensä haastaminen tai aito halu parantaa tutkimansa kohteen ja samalla koko Internetin tietoturvaa[105].

Luonnollisesti myös hakkereiden näkökulmasta ohjelmista voidaan paikallistaa riskejä. Bug bounty -ohjelmat voidaan nähdä tapana ulkoistaa testaaminen halvalla[106]. Karrikoidun inhorealistisesti esitettynä bug bounty -ohjelmat perustuvat oman alansa asiantuntijoiden ja jopa huippuasiantuntijoiden puhtaasti provisiopalkatuille, sopimuksettomille ”työsuhteille”, jossa edes ”työtehtävän” positiivinen täyttäminen[107] eli järjestelmässä olevan haavoittuvuuden paikallistaminen ja siitä raportoiminen ei takaa palkkion maksua. Bug bounty -ohjelmien käyttämisestä ja niiden perusrakenteesta voidaan siis edellä kuvatulla tavalla paikallistaa työoikeudellisia ongelmia.

Vaikka hakkeri olisikin vain iloinen ja tyytyväinen siihen, että hän ylipäätään saa yrittää murtautua järjestelmään ja toteuttaa kykyjään, on kuitenkin olemassa riski siitä, että hakkerin hyvää tarkoittava osallistuminen bug bounty -ohjelmaan onkin jollakin tavalla rikosoikeudellisesti rangaistava teko, jolloin hakkerille jää rahapalkintojen sijaan – ilman asianmukaisesti laadittua turvasatamaa – käteen rikosoikeudellinen tuomio ja vahingonkorvausvaatimuksia. Tästä syystä asianmukaisesti laadittu niin kutsuttu turvasatama (*safe harbor*) on tärkeä osa ohjelmien sääntöjä ja politiikkaa. Eräs ohjelmiin erityisesti aiem-

[103] Algarni & Malaiya 2014; Zhao et al. 2015.
[104] Zhao et al. 2015.
[105] Kilovaty 2019, s. 480–481. Ks. myös Himanen 2001 ja Ingo 2005.
[106] Egelman et al. 2013.
[107] Käytettyä terminologiaa selventää vastakkainen ajatus: Työtehtävän negatiivinen täyttäminen voisi tarkoittaa sitä, että hakkeri ei tietomurtoa yrittäessään paikallista yhtäkään haavoittuvuutta, mikä mahdollisesti tarkoittaa, että järjestelmän tietoturvan laatimisessa on onnistuttu. Jotta tällaiseen tulokseen voidaan tulla, tarkoittaa se kuitenkin, että tähän ”ei bugeja” -havaintoon hakkerin tulee käyttää todennäköisesti runsaasti työaikaa, eikä tuloksena ole mitään, mistä olisi edes mahdollista saada palkkio. Työtehtävä on tästä huolimatta täytetty onnistuneesti.

min liittynyt ongelma on, että osallistuakseen ohjelmaan hakkeri saattaa joutua hyväksymään ohjelman kohteena olevan järjestelmän käyttöehdot, joiden mukaan oikeudeton tunkeutuminen järjestelmään tai sen yrittäminen voi rikkoa näitä käyttöehtoja[108].

Haavoittuvuuksien raportointihalukkuutta on voinut vähentää varsinkin aiemmin se, että raportoijat ovat pelänneet oikeustoimia esimerkiksi U.S. Digital Millennium Copyright Act -säädöksen, EU:n tekijänoikeusdirektiivin tai jonkin vastaavan kansallisen säädöksen vuoksi. Erityisesti silloin, jos säännökset on kirjoitettu epäselvästi tai ovat avoimia tulkinnalle, ovat tietoturva-asiantuntijat varovaisia haavoittuvuuksien raportoinnin suhteen, sillä oikeuskeinoja on käytetty tällaisissa tilanteissa raportoijia vastaan.[109]

Sekä USA:ssa että Euroopassa on viety eteenpäin kyberturvallisuuteen liittyvää lainsäädäntöä, ja lainsäädäntöä edelleen kehittämällä voitaisiin mahdollisesti huomioida hakkerien oikeusturva tällaisissa ongelmallisissa tilanteissa[110]. Voidaan kuitenkin argumentoida, että ainakin bug bounty -ohjelmiin liittyvän turvasatamaongelman suhteen tehokkaampi toimintamalli olisi kehittää pikemminkin ohjelmien säännöt tai politiikat sekä sopimukset sellaisiksi, että hakkerit eivät bug bounty -ohjelmaan osallistuessaan syyllistyisi rangaistaviin tekoihin tai sopimusrikkomuksiin[111]. Markkinavoimat voisivat olla itsenäisesti halukkaita tekemään nämä muutokset, ilman juridista ohjausta[112]. Ollaankin siis oikeustaloustieteelliseltä kannalta sääntelyongelmien ytimessä: millaisia ohjauskeinoja tulisi käyttää, jotta sääntelytaakka ja hallinnollinen taakka muodostuisivat mahdollisimman kevyiksi, mutta tosielämän ongelmilta, väärinkäytöksiltä ja markkinoiden vääristymiseltä vältyttäisiin? Kyse on pohjimmiltaan kustannustehokkuudesta ja tasapainoilusta hallinnollisen, taloudellisen ja informaatio-ohjauksen sekä erilaisten itsesääntelykeinojen välillä[113].

Hakkerin roolin suhteen bug bounty -ohjelmia ei voi tarkastella puhtaasti yrittäjät–kuluttajat-vastakkainasettelun näkökulmasta. Alustayritys voidaan paikallistaa yritys–kuluttaja-dikotomian yritykseksi, ostajayritys voidaan paikallistaa dikotomian kuluttajaksi,

[108] Elazari Bar On, 2018.
[109] Råman 2006, s. 259.
[110] Elazari Bar On 2018.
[111] Elazari Bar On 2018.
[112] Elazari Bar On 2018.
[113] Määttä, luentokalvot 12.–14.2.2019.

mutta hakkerin rooli näiden kahden toimijan välissä jää kaksitahoiseksi: Yhtäältä hakkerin rooli lähentelee yrittäjää, sillä hakkerien yhtenä tavoitteena kuitenkin on saada rahallinen korvaus ajankäytöstään. Toisaalta hakkerit voidaan nähdä dikotomian viitekehyksessä myös kuluttajina, joille tarjotaan ohjelmissa mahdollisuus tehdä jotakin, mikä muutoin ei olisi sallittua. Tästä syystä hakkerien roolia voi olla haastavaa kuvata taloustieteen yleisten paradigmojen mukaisesti.

Osa hakkereiden motivaatiotekijöihin keskittyneestä tutkimuksesta on tullut siihen tulokseen, että mitä korkeampi palkkio, sen suuremmat todennäköisyydet koko ohjelmalla onnistua. Toisaalta on myös tutkimusta, jonka mukaan haavoittuvuusraportteja palautetaan myös sellaisiin kohteisiin, jossa ei makseta palkkiota laisinkaan. Yleisesti ottaen voidaan kuitenkin todeta, että mitä suuremmat palkkiot tilaaja lupaa, sitä suuremmalla todennäköisyydellä tilaajan tarpeet tulevat täytetyksi ja tilaaja saa kilpailuedun suhteessa muihin bug bounty -ohjelmiin.[114] Ohjelmissa maksettavilla palkkioilla on siis suuri merkitys, ja palkkiot ilmentävät ajattelunmuutosta: vaativien haavoittuvuuksien etsimistä ei pidetä enää mukavana ajanvietteenä, jota hakkerit toteuttavat hedonistisista tai altruistisista syistä. Päinvastoin: myös Suomessa on henkilöitä, jotka elättävät itsensä bug bounty -ohjelmiin osallistumalla[115]. Tämä vahvistaa käsitystä rahallisten palkkioiden olennaisuudesta.[116]

2.2.4 Muut toimijat

Edellä tarkemmin eriteltyjen toimijoiden lisäksi bug bounty -ohjelmiin voidaan liittää muitakin toimijoita. Yksi toimija ovat alihankkijat, jotka ovat laatineet ohjelman kohteena olevan ohjelmiston tai osan siitä. Erityisesti julkishallinnossa tilanne on usein se, että tietojärjestelmät on hankittu yksityiseltä sektorilta. Myös näiden järjestelmien kehitys ja ylläpito on usein ulkoistettu. Tietojärjestelmän toimittajalla voi lisäksi olla useita alihankkijoita, jotka kukin vastaavat omasta osastaan tietojärjestelmän kehityksessä ja ylläpidossa. Nämä toimittajat ja alihankkijat eivät suoraan liity bug bounty -ohjelmiin, mutta

[114] Fryer & Simperl 2017.
[115] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[116] Ks. Maillart et al. 2017.

ohjelmien puitteissa paikallistetut haavoittuvuudet päätyvät mitä todennäköisimmin toimittajien ja alihankkijoiden paikattaviksi.

Kun on kyse julkishallinnossa toteutettavasta bug bounty -ohjelmasta, on otettava huomioon, että ohjelman rahoitus on mitä todennäköisimmin peräisin verovaroista. Tässä suhteessa ohjelman toimijana voidaan pitää veronmaksajia, myös niitä yksilöitä, jotka eivät osallistu tietojärjestelmän käyttämiseen. Siinä missä tietojärjestelmien tietoturvaa ylläpidetään ja parannetaan verovaroin, myös mahdollisiin tietoturvaloukkauksiin reagoidaan verovaroin. On kuitenkin hyvin todennäköistä, että ennaltaehkäisevä turvallisuuteen panostaminen tulee huomattavasti halvemmaksi, kuin tietomurron kohteeksi joutuneiden järjestelmien uudelleen käyttöön saaminen. Veronmaksajien näkökulmasta riskinä on se, että mikäli ohjelmaa ei toteuteta asiantuntevasti, saattavat palvelut väliaikaisesti heikentyä esimerkiksi palvelun suuren kuormituksen tai korjaustöiden vuoksi, ja toisaalta se, että ohjelman järjestämisen kustannushyödyt jäävät vähäisiksi.

Tietojärjestelmällä on myös käyttäjiä, niin tilaajaorganisaatiossa kuin asiakkaana. Veronmaksajien kannalta tarkastellut hyödyt ja riskit vaikuttavat myös järjestelmän käyttäjiin ja asiakkaisiin, jopa suoremmin kuin veronmaksajiin yleisellä tasolla.

Bug bounty -ohjelman ulkoisvaikutuksena voidaan pitää myös sitä, että haavoittuvuuksia paikallistamalla ja paikkaamalla koko Internetin turvallisuus lisääntyy. Tämän ohella bug bounty -ohjelmat voivat kannustaa uusia henkilöitä tietoturvallisuusalalle[117]. Ohjelmilla voi siis olla positiivisia vaikutuksia yksityishenkilöiden elämänkulkuun ja myös turvallisuusalan tulevaisuudennäkymiin yleensä. Bug bounty -ohjelmat voivat osin myös vastata pillinpuhaltajien (nk. *whistleblowers*) tarpeeseen,[118] joskin bug bounty -ohjelmien tilaajat ovat usein todennäköisesti itsekin kiinnostuneita puuttumaan turvallisuusliitännäisiin epäkohtiin.

Vielä yhtenä ohjelmaan liittyvänä toimijana voidaan pitää CERT-toimijoita. CERT-toimijoiden tehtävänä on esimerkiksi selvittää verkkopalveluihin ja viestintäpalveluihin kohdistuvia tietoturvaloukkauksia ja niiden uhkia, kerätä tietoa tällaisista tapahtumista sekä tiedottaa yleisesti tietoturva-asioista. CERT-toiminnan tavoitteena on lisäksi yleisten

[117] Egelman et al. 2013.
[118] Pilliinpuhaltajista tarkemmin ks. esim. Neuvonen 2019, s. 255–258.

viestintäverkkojen ja viestintäpalveluiden turvallisen ja häiriöttömän toiminnan varmistaminen ja yhteiskunnan elintärkeiden toimintojen turvaaminen.[119]

Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskus on Suomessa kansallinen CERT-toimija. Kyberturvallisuuskeskuksen tehtäviin kuuluu muun muassa tukea, ohjata ja valvoa tietoturvallisuutta ja yksityisyyden suojan toteutumista sähköisessä viestinnässä, ylläpitää kansallisen kyberturvallisuuden tilannekuvaa, edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta sekä tukea toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin. (L Liikenne- ja viestintävirastosta 935/2018, 3.1 §.)

Osa hakkereista saattaa myös bug bounty -ohjelmien puitteissa tehdä ilmoituksen löytämästään haavoittuvuudesta Kyberturvallisuuskeskukselle.[120] Julkishallinnollisten toimijoiden ottaessa yhä enenevissä määrin käyttöön bug bounty -ohjelmia tulisi pohtia myös sitä, tulisiko CERT-toimijoiden tai vastaavien toimijoiden osallistua bug bounty -ekosysteemeihin – siis olla isompana vaikuttajana ja esimerkiksi toimia alustayrityksen tavoin.[121]

2.3 Tutkimuskirjallisuudessa esiin nousseita kehittämisnäkökulmia

Tutkimuskirjallisuudessa on annettu paljon tilaa sille, miten bug bounty -ohjelmista voitaisiin tehdä entistä tehokkaampia ja kuinka niiden toimintaa voitaisiin optimoida entisestään. Tässä alaluvussa nostan esiin joitakin huomioita.

Vaikka bug bounty -ohjelmat ovat yleistyneet vasta 2010-luvulla, on esimerkiksi Råman väitöskirjassaan (2006) jo hahmotellut eräänlaista bug bounty -ohjelman mallia. Råmanin mukaan haavoittuvuuden raportoinnissa kannattaa olla mahdollisimman yksityiskohtainen, ja toisaalta raportointi voisi Råmanin mukaan tapahtua jonkinlaisen koordinaattorin

[119] Kyberturvallisuuskeskuksen Internet-sivut, CERT, 10.4.2020. Tarkempaa informaatiota Kyberturvallisuuskeskuksesta ja sen tehtävistä CERT-toimijana löytyy mainittujen Internet-sivujen RFC 2350 -osiosta.
[120] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[121] Ks. Ruohonen & Allodi 2018.

kautta, eikä suoraan ohjelmistonkehittäjälle.[122] Råman myös esittää, että tällaisen haavoittuvuuksien välittäjän mukana olo prosessissa edistää haavoittuvuusraporttien uskottavuutta ohjelmistokehittäjien silmissä, ja toisaalta välittäjien avulla tieto haavoittuvuudesta saattaa levitä laajemmalle. Näillä välittäjillä Råman kuitenkin viittaa CERT- tai CSIRT-organisaatioihin[123], kun taas bug bounty -ohjelmien kannalta alustayritysten yksi tehtävä on verifioida lähetettyjä raportteja, eli lisätä aiheellisten raporttien uskottavuutta ohjelman tilaajan näkökulmasta.

Zhao et al. ehdottavat tutkimuksessaan, että haavoittuvuuspalkkio-ohjelmien järjestäjien ei tulisi keskittyä ainoastaan ahkerimpiin osallistujiin, vaan kannattavaa olisi yrittää houkutella osallistujiksi mahdollisimman paljon eri henkilöitä. Osallistujien suurempi joukko todennäköisesti tarkoittaa erilaisten löydettyjen haavoittuvuuksien laajempaa kirjoa ja ylipäätään enemmän löydettyjä haavoittuvuuksia. Suurempaan etsijöiden houkutteluun panostaminen voi kuitenkin tarkoittaa sitä, että tarpeen olisi luoda uusia palkitsemisen keinoja ja ohjelmien uudenlaista organisointia, sillä osallistujajoukon kasvattaminen todennäköisesti kasvattaa myös päällekkäisten tai saman sisältöisten raporttien määrää. Osallistujien motivaatioon saattaa alentavasti myös vaikuttaa se, että vain ensimmäinen haavoittuvuuden löytäjä huomioidaan.[124]

Toisaalta Zhao et al. ovat tulleet siihen tulokseen, että tehtävissä, jotka edellyttävät asiantuntemusta ja sisältävät kilpailullisen piirteen bug bounty -ohjelmien tapaan, mahdollisimman suuri osallistujajoukko ei tuota aina parasta mahdollista lopputulosta. Sen sijaan bug bounty -ohjelmissa tulisi pyrkiä kontrolloimaan osallistujien välistä kilpailua ja monimuotoistamaan osallistujien osaamisalaa.[125] Samantyylisiä tuloksia ovat esittäneet myös Edmundson et al., joiden tutkimuksen tuloksena ei voitu määrittää mittaria, jolla voitaisiin ennustaa yksittäisen testaajan pätevyyttä tilanteessa, jossa tämän taidoista ja osaamisesta ei ole aikaisempaa kokemusta. Siksi tässä tutkimuksessa todetaankin, että paras tapa arvioida testaajan osaamista ja tehokkuutta on tarkastella näiden aikaisempia suorituksia.[126]

[122] Råman 2006, 249.
[123] Råman 2006, s. 253.
[124] Zhao et al. 2014; Zhao et al. 2015.
[125] Zhao et al. 2016.
[126] Edmundson et al, 2013.

Yhtenä mahdollisuutena haavoittuvuuksien entistä tehokkaammaksi löytämiseksi Zhao et al. näkee, että jo löydetyistä haavoittuvuuksista julkaistaisiin enemmän teknisiä yksityiskohtia. Tällä tavalla hakkerit voisivat oppia toistensa löydöistä.[127] Ajatus voi toimia VDP:iden kohdalla, mutta bug bounty -ohjelmien kohdalla herää erinäisiä kriittisiä näkökulmia: yhtenä suurena, jos ei suurimpana, motivaatiotekijänä bug bounty -ohjelmiin osallistumiselle on haavoittuvuuksista maksettavat (rahalliset) palkkiot. Kuinka valmiita hakkerit ovat jakamaan omaa osaamistaan, kun sen jakaminen johtaisi siihen, että oma osaaminen ja asiantuntijuus eivät olisikaan enää niin harvinaista erityisosaamista? Tämä tietenkin johtaisi myös siihen, että asiantuntevan hakkerin mahdollisuudet löytää haavoittuvuuksia ensimmäisenä pienentyisivät, sillä entistä suurempi joukko hakkereita olisi nyt osaavampaa. Bug bounty -ohjelmien yksi piirre on myös, että teknisiä haavoittuvuustietoja ei julkaista siitä syystä, että palvelun ostaja ei halua julkaista liikaa tietoja ohjelmistojensa tietoturvan tasosta. Tämän vuoksi ostaja on halukas maksamaan löytäjälle, ja palkkion maksun ehtona usein on, että haavoittuvuuden löytäjällä ei ole oikeutta julkaista tietoja haavoittuvuudesta.

Ruohosen & Allodin mukaan pelillistäminen (*gamification*) voisi motivoida hakkereita osallistumaan ohjelmiin entisestään. Pelillistämiseen kuuluu esimerkiksi suoritustaulukoiden jatkuva päivittyminen ja erilaiset merkit tai mitalit kaikista tuotteliaimmille raportoijille.[128]

Yhtenä ohjelmiin liittyvänä ongelmana on todettu, että hakkerit eivät pysy kovin montaa vuotta bug bounty -ohjelmien parissa: suurin osa ohjelmien löydöksistä tehdään ensimmäisen kolmen harrastuneisuusvuoden aikana. Algarni & Malaiya esittävät hypoteesin, että syynä olisi maineen kerääntyminen kahden-kolmen vuoden aikana siten, että hakkeri voi siirtyä yrityksen palkkalistoille tai sopimuskumppaniksi, jolloin tulotaso ei heittele löydettyjen haavoittuvuuksien mukaan, vaan on tasaisempi – jotkut saattavat myös perustaa oman yrityksen. Näitä havaintoja tukee myös tarkastelluille hakkereille esitetyt kysymykset.[129]

[127] Zhao et al. 2014.
[128] Ruohonen & Allodi 2018.
[129] Algarni & Malaiya 2014.

Kuten edellä on todettu, ohjelmien puitteissa palautetaan erittäin paljon puutteellisia tai irrelevantteja raportteja. Yksi pääsyy kelvottomien haavoittuvuusraporttien tuottamiselle liittyy siihen, että hakkereilla ja organisaatoilla on erilaiset kannustimet ohjelmaan osallistumiseen: hakkerit ovat kiinnostuneita hyväksyttävien raporttien määrien kasvattamisesta, kun taas organisaatiot ovat kiinnostuneita myös kelvottomien raporttien määrän vähentämisestä. Laszka et al. ehdottavat, että epäsuhtaan voitaisiin puuttua esimerkiksi alentamalla hieman hyväksyttävistä raporteista maksettavaa palkkiota ja samanaikaisesti maksamalla ylimääräisen palkkion perustuen raportin tarkkuuteen.[130] Ohjelmissa toimivien alustayritysten liiketoimintamalliin usein myös liittyy tavoite raporttien parantamisesta[131]. Tämä voi lisätä organisaatioiden kiinnostusta ostaa palveluita alustayritykseltä.

Maillart et al. esittävät, että uusien haavoittuvuuksien löytämisen todennäköisyys pienenee nopeasti, ja tätä pienenemistä on vaikea kompensoida riittävällä palkkioiden kasvattamisella. Tämän lisäksi ohjelman tilaajalla on tavoitteena saada mahdollisimman suuri ja monipuolinen joukko etsimään haavoittuvuuksia, mikä taas lisää kilpailua osallistuvien hakkereiden välillä. Lopputuloksena Maillart et al. toteavat, että hakkereilla on paljon kannustimia vaihtaa vastajulkaistuihin ohjelmiin, joiden kohteissa on vielä paljon helposti paikallistettavia haavoittuvuuksia.[132]

Zhao et al. ehdottavat tutkimuksessaan, että haavoittuvuuksiin liittyvässä tutkimuksessa ei tulisi keskittyä pelkästään haavoittuvuuksien teknisiin yksityiskohtiin ja haavoittuvuuksien paikallistamiseen tähtääviin työkaluihin, vaan tutkimuspainoarvoa tulisi antaa myös sille, miten hakkerit tekevät löydöksensä. Haavoittuvuuksien löytyminen on kuitenkin hyvin vahvasti sidoksissa haavoittuvuuksia etsivien henkilöiden tietotaitoon ja kokemukseen.[133] Tutkimuksen fokusta pitäisi tällä perusteella siis ehkäpä siirtää jonkin verran ihmistieteiden puolelle, esimerkiksi hakkereiden toimintamallien tai oppimisstrategioiden suuntaan. Ongelmana kuitenkin on, että hakkerin kerryttämään tietotaitoon liittyvässä tutkimuksessa hakkerin erikoistaidot tai osaaminen saattaisivat tulla tietoon yleisemminkin, jolloin hakkeri menettäisi kilpailuvalttinsa suhteessa muihin tahoihin.

[130] Laszka et al. 2016, s. 172.
[131] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[132] Maillart et al. 2017.
[133] Zhao et al. 2014.

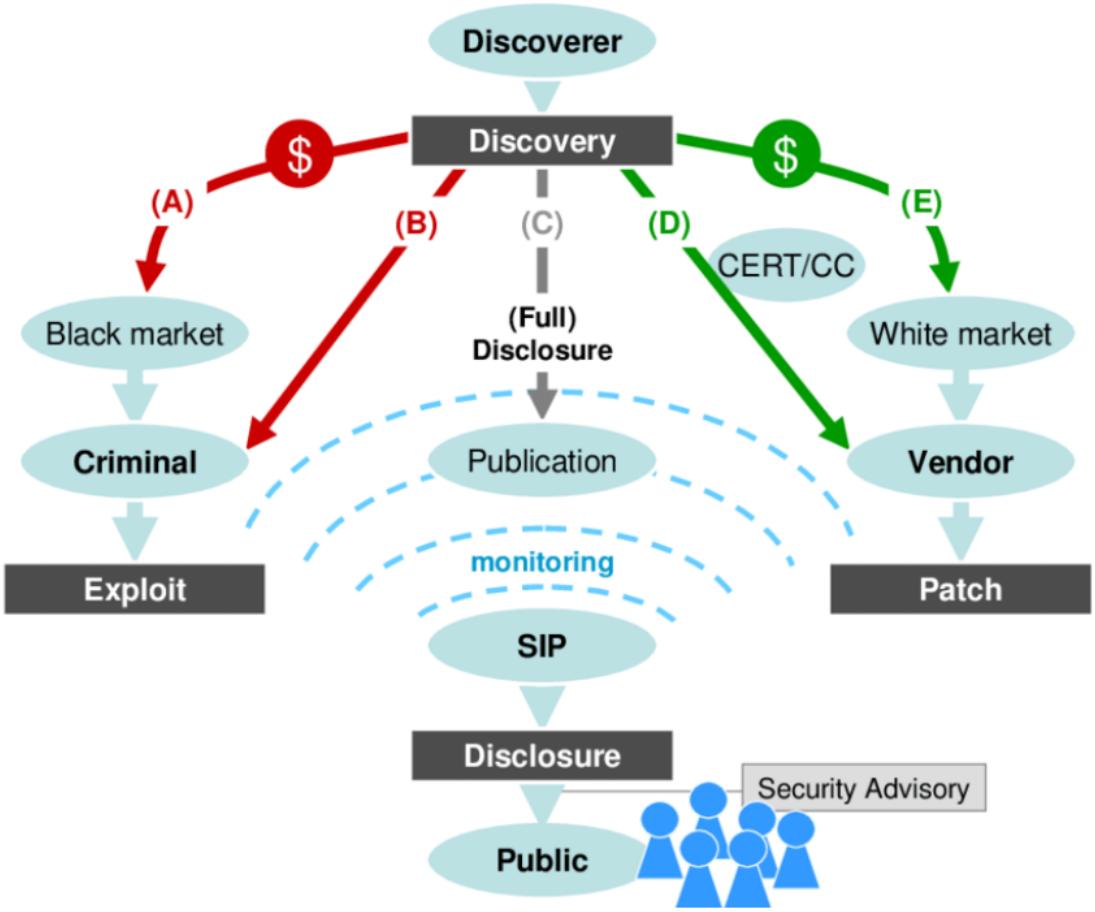
3 Taloustieteellinen perspektiivi ohjelmiin

Tässä luvussa perehdytään haavoittuvuusmarkkinoiden markkinamalliin Frein et al. (kuva 2) mallin kautta. Malli kuvastaa erilaisia mahdollisia polkuja haavoittuvuuden julkiseksi tulemiselle ja rahalliselle hyötymiselle. Lisäksi luvussa selitetään tietoturvan testaamisen joukkoistaminen teoreettisesta näkökulmasta, sekä pohditaan tietoturvan testaamista sääntelyteoreettiselta kannalta. Edelleen luvussa syvennytään tietoturvan testaamiseen kustannustehokkuuden perspektiivistä ja kuvataan tietoturvan sitruunaongelma. Lopuksi esitellään bug bounty -ohjelmille vaihtoehtoisia tai sitä täydentäviä tietoturvan testaamisen muotoja.

3.1 Haavoittuvuusmarkkinoiden markkinamalli

Markkinoita voidaan niiden laillisuuden asteen mukaan jaotella monella tavalla, kuten Algarnin & Malaiyan mukaan säännellyiksi markkinoiksi (*regulated market*), online-foorumeiksi, harmaiksi markkinoiksi (*gray market*) ja mustaksi pörssiksi (*black market*).[134] Frei et al. ovat artikkelissaan laatineet oman mallinnuksensa (kuva 2) haavoittuvuusmarkkinoista. Mallinnuksessa markkinoiden eri mahdollisia toimintamuotoja kuvataan viitenä eri polkuna, joilla kullakin on erilaisia ominaisuuksia ja vaikutuksia. Polkujen D ja E tilannetta voidaan kuvata puhtaiksi tai laillisiksi markkinoiksi – polku E saattaisi edustaa myös Algarnin & Malaiyan säänneltyjä markkinoita. Polkujen A ja B tilannetta sen sijaan voidaan kutsua pimeiksi markkinoiksi, laittomiksi markkinoiksi tai mustaksi pörssiksi. Näiden välissä polkua C sen sijaan voidaan pitää ilmentymänä harmaista markkinoista. Harmaat markkinat edustavat esimerkiksi tilannetta, jossa ei voida moraaliselta kannalta täysin määrittää sitä, onko haavoittuvuus paikallistettu lain mukaisesti tai käytetäänkö paikallistettua haavoittuvuutta kestävällä tavalla. Toisaalta polkuun C liittyy joissain määrin sattumanvaraisuutta sen suhteen, tullaanko haavoittuvuutta käyttämään hyväksi, joten senkin puolesta polkua C voidaan pitää ilmentymänä harmaista markkinoista.

[134] Algarni & Malaiya 2014.



Kuva 2 Turvallisuusekosysteemin pääasialliset prosessit ja suhde haavoittuvuuden elinkaaren tapahtumiin. Frei et al. 2010.

Kuvassa esitetty polku A kuvaa tilannetta, jossa hakkeri (kuviossa *discoverer*) paikallistaa haavoittuvuuden ja myy sen pimeillä markkinoilla (*black market*) rikolliselle (*criminal*), joka käyttää haavoittuvuutta hyväkseen (*exploit*). Polku B sen sijaan kuvaa tilannetta, jossa hakkeri käyttää itse hyväkseen löytämäänsä haavoittuvuutta, jolloin hakkeri myös syyllistyy rikokseen. Polut A ja B ovat tietojärjestelmän omistajan näkökulmasta epätoivottuja skenaarioita, sillä ne johtavat haavoittuvuuden hyväksikäyttöön ja tietojärjestelmän omistajan mahdolliseen taloudelliseen tai muuhun haittaan.

Polku C kuvaa tilannetta, jossa hakkeri julkaisee joko kokonaan (*full disclosure*) tai osittain (*disclosure*) löytämänsä haavoittuvuuden. Julkaisun jälkeen haavoittuvuuteen voi ensiksi päästä käsiksi joko hyväntahtoisia hakkereita tai vihamielisiä hakkereita, kuin myös tietojärjestelmän omistaja tai ohjelmiston kehittäjä. Koska haavoittuvuuden korjaaminen

ei tapahdu yleensä hetkessä, on todennäköistä, että haavoittuvuutta ehditään käyttää hyväksi ennen sitä[135]. Tästä syystä myöskään polku C ei ole tietojärjestelmän omistajan tai ohjelmistonkehittäjän kannalta optimaalinen tapahtumankulku.

Polkuun C liittyvällä SIP-toimijalla (*Security Information Provider*) kuvataan joko yksityistä tai julkista toimijaa, jonka tehtävänä on kerätä ja julkaista turvallisuusliitännäistä informaatiota ja jolla on tärkeä rooli turvallisuusekosysteemissä. Kuvassa SIP:n roolia tiedonkerääjänä on kuvattu kaarevilla katkoviivoilla. SIP:n palveluiden avulla yleisöllä (*public*) on pääsy tarkistettuun, ajantasaiseen ja ymmärrettävään tietoturvaa koskevaan informaatioon. SIP:n olemassaololla on merkitystä koko turvallisuusekosysteemin toimintaan ja sitä voidaan verrata avoimessa yhteiskunnassa toimivaan vapaaseen lehdistöön.[136] Tämä yksityinen tai julkinen SIP-toimija voi olla myös CERT-toimija.

Polku D kuvaa tilannetta, jossa hakkeri paikallistaa haavoittuvuuden ja ilmoittaa siitä suoraan ohjelmistonkehittäjälle (*vendor*) tai CERT-toimijalle, joka ilmoittaa haavoittuvuuden kehittäjälle. Tässä skenaariossa ei, kuten myöskään B ja C skenaarioissa, liiku rahaa. Polku E:n kohdalla sen sijaan hakkeri voi odottaa saavansa korvauksen laillisille markkinoille (*white market*) tuottamastaan haavoittuvuusraportista. Markkinoilta raportti siirtyy edelleen kehittäjälle, joka laatii tarvittavat korjaukset (*patch*).

Jos tietojärjestelmän omistaja tai ohjelmistokehittäjä haluaa välttää vaihtoehdot A–C, ja toivoo, että tietojärjestelmässä olevat haavoittuvuudet ilmenisivät polkujen D ja E kuvaamalla tavalla, tulee sen myös panostaa näihin polkuihin: markkinat eivät toimi itsestään.[137]

Taloudellista hyötymistä voi esitetyn mallin mukaan tapahtua poluilla A ja E. Taloudellisen hyötymisen kannalta polku A on vihamielisen hakkerin näkökulmasta haastava. Vaikka hakkeri löytäisikin ostajan löytämälleen haavoittuvuudelle, voi olla vaikea määrittää haavoittuvuuden arvoa, ja toisaalta haavoittuvuuden vaikutuksia voi olla vaikea osoittaa potentiaaliselle ostajalle. Bug bounty -ohjelmissa haavoittuvuuden arvo määri-

[135] Frei et al. 2010.
[136] Frei et al. 2010.
[137] Frei et al. 2010.

tellään etukäteen: hakkerit tietävät, millaisista haavoittuvuuksista maksetaan ja alustayritykset varmistavat maksujen toteutumisen.[138] Hakkerin näkökulmasta on siis varmempaa toimia polun E mukaisesti. Se, että prosessissa on mukana alustayritys, lisää entisestään ohjelman luotettavuutta hakkerin näkökulmasta. Tilaaja tai ohjelmistonkehittäjä ei voi vain ottaa raportteja vastaan ja jättää maksamatta relevantista raportista väittämällä sitä duplikaatiksi. Lisäksi alustayritys voi objektiivisesti arvioida löydetyn haavoittuvuuden vakavuusasteen, johon palkkion maksaminen pääasiassa perustuu.[139]

Aiemmin hakkerit määrittivät, milloin löydetty haavoittuvuus julkaistaan ja missä kanavassa. Bug bounty -ohjelmien yleistymisen jälkeen markkinoilla on tapahtunut valtasuhteiden muutos: päätöksen haavoittuvuuden julkaisusta tekee ohjelmistokehittäjä tai tietojärjestelmän omistaja.

Haavoittuvuusmarkkinoiden täytyy olla tarpeeksi kehittyneet, jotta ne olisivat toimivat.[140] Ohjelmistonkehittäjät ovat kehittäneet erilaisia prosesseja haavoittuvuuksien raportointiin. Ainakin 2000-luvun alussa ohjelmistonkehittäjien motiivina tälle vaikuttaa olleen toive, että raportointipolitiikat olisivat selkeitä ja kustannustehokkaasti hallittavissa, jotta prosessit olisivat ennustettavampia ja helpommin kontrolloitavia. Ohjelmistokehittäjien taka-ajatuksena raportointipolitiikkojen kehittämiselle ei siis tuolloin ole ollut parempi turvallisuuden taso koko yhteiskunnan näkökulmasta, vaan pikemminkin sidosryhmien intressien täyttäminen ja julkisuuskuvan säilyttäminen.[141]

Nyttemmin haavoittuvuuksien julkaisemiseen on muodostunut strukturoituja menetelmiä, kuten bug bounty -ohjelmia, joissa korostetaan raportoijan ja ohjelmistokehittäjän yhteistyötä turvallisuusliitännäisten haavoittuvuuksien suhteen. Raportoijan ja ohjelmistokehittäjän lisäksi prosessissa saattaa olla mukana koordinaattori[142]. Strukturoitujen menetelmien muodostumisesta huolimatta vielä 2000-luvulla ohjelmistokehittäjien välinpitämättömyys haavoittuvuusraportteja kohtaan oli yleistä.[143]

---

[138] Fryer & Simperl 2017. Fryer & Simperl käyttävät alustayrityksen kohdalla termiä *trusted third party* (TTP).
[139] Ks. esim. Ozment 2004. Ozment käyttää tässä yhteydessä alustayrityksen sijaan termiä *trusted third party* (TTP).
[140] Ks. esim. Ozment & Schechter 2006; Ozment 2004.
[141] Råman 2006, s. 255.
[142] Koordinaattoreilla tarkoitetaan useimmiten CERT-tahoja. Koordinaattorin roolista tarkemmin, ks. esim. Cavusoglu et al. 2005.
[143] Råman 2006, s. 258–259.

Raha motivoi niin yrityksiä kuin yksityishenkilöitä osallistumaan haavoittuvuuksiin liittyvään tietojen vaihtoon. Jos toimivia laillisia markkinoita ei ole, yksittäiset hakkerit toimivat sekä altruistisista syistä että saadakseen mainetta – ja mahdollisesti myös saadakseen rahallisen korvauksen laittomilta markkinoilta. Lailliset markkinat asettavat rahallisen kompensaation tärkeimmäksi motivoivaksi tekijäksi haavoittuvuuksien etsimiselle, ja saattavat palkkiotason avulla vaikuttaa siihen, että hakkeri ei myisikään haavoittuvuuksia laittomilla markkinoilla. Ohjelmistokehittäjien näkökulmasta motivoiva tekijä turvallisuuteen panostamiseen on sen sijaan tyytyväisten asiakkaiden luottamus, jonka rahallinen arvo voidaan mitata vain pitkällä aikavälillä. Toimivat ja lailliset markkinat lisäävät yrityksen lyhyen tähtäimen hyötyjä ja antavat etua kilpailijoihin nähden. Toimivien markkinoiden ylläpitäminen ja niillä toimiminen vaatii kuitenkin kustannuksia, mikä kasvattaa yrityksen intressiä pitää huolta tietoturvasta.[144]

Bug bounty -ohjelmat eivät ole ainoa malli markkinoille, jota tutkimuskirjallisuudessa on esitetty, vaan haavoittuvuuksien raportointia varten on luotu useampia erilaisia markkinoihin perustuvia mekanismeja, joiden tarkoituksena on kannustaa yksityishenkilöitä raportoimaan havaitsemistaan haavoittuvuuksista.[145] Ehdotuksia markkinamalliksi löytyy esimerkiksi eräänlaisten huutokauppamallien puolesta.[146] Haavoittuvuusmarkkinoita voidaan hallita myös Baconin et al. kuvaaman mallin (*vulnerability markets*) avulla. Tämän mallin mukaan haavoittuvuuden hinta on suhteessa sen löytymiseen kuluneeseen aikaan – palkkio kasvaa sitä suuremmaksi, mitä kauemmin haavoittuvuuden löytyminen kestää. Kun haavoittuvuus on paikallistettu, raportoitu ja verifioitu, putoaa palkkio aloitustasolle tai nollaantuu. Mikäli kukaan ei raportoi haavoittuvuuksia eikä näin ollen lunasta palkkiota, voidaan ohjelmistoa pitää turvallisena. Esitettyä mallia voidaan kuvata myös tietynlaisena huutokauppamallina.[147]

Markkinoihin perustuvien mallien haittoina, sivuvaikutuksina tai epäkohtina voidaan pitää esimerkiksi sitä, että raportoidun haavoittuvuuden korjaaminen saa aikaan uusia haavoittuvuuksia. Toisaalta voi käydä myös niin, että haavoittuvuuden korjaamisoperaatio ei

[144] Böhme 2006.
[145] Bacon et al. 2009.
[146] Ks. esim. Ozment & Schechter 2006; Ozment 2004.
[147] Bacon et al. 2009.

olekaan korjannut haavoittuvuutta kokonaisuudessaan ja kyseenalaiseksi jää, onko jäljelle jääneestä haavoittuvuudesta laadittu uusi raportti samalla uusi haavoittuvuus. Yhden haavoittuvuuden korjaaminen saattaa myös samalla korjata useita muita haavoittuvuuksia, joista on myös voitu jo raportoida palkkion toivossa.[148]

3.2 Tietoturvatestaamisen joukkoistaminen

Bug bounty -ohjelmissa on kyse eräästä joukkoistamisen muodosta. Joukkoistaminen (*crowdsourcing*) taas on yksi ulkoistamisen muoto – joukkoistaminen on toimintaa, jossa organisaation tietty tehtävä ulkoistetaan joukolle.[149] Joukko koostuu luonnollisista, anonyymeistä henkilöistä ja yhtenä joukon ominaisuutena on erilaisten tulkintojen laaja kirjo.[150] Arvo, jonka tietyn tehtävän joukkoistaminen tuottaa organisaatiolle, piilee nimenomaisesti joukon jäsenten moninaisuudessa ja itsenäisessä, riippumattomassa toiminnassa.[151]

Bug bounty -ohjelmien kontekstissa joukkoistaminen voidaan määritellä toiminnaksi, jossa tietyllä joukolla (hakkerit) on selkeä tavoite (paikallistaa haavoittuvuudet), ja jossa voidaan määritellä hyöty niin joukon jäsenen kuin (selkeästi määritellyn) tilaajan näkökulmasta. Suurimpaan osaan joukkoistamisprojekteista verrattuna bug bounty -ohjelmien konsepti on poikkeava. Bug bounty -ohjelmissa hyväksytään kaikki validit yksittäiset raportit, eikä konsensusta vaadita, mikä erottaa bug bounty -ohjelmat esimerkiksi sellaisista joukkoistamisprojekteista, joissa pyritään tunnistamaan tiettyjä kohteita valokuvista.[152]

Bug bounty -ohjelmat, jotka toimivat kutsuperiaatteella, ilmentävät joukkoistamisen sitä muotoa, jossa joukon jäseniin on tutustuttu etukäteen ja heistä on poimittu potentiaalisimmat henkilöt, tavoitteena edelleen kasvattaa joukkoistamisen tehokkuutta. Mikäli joukolle tehdään tällaista karsintaa, voidaan kuitenkin argumentoida sen puolesta, että tällöin joukko tuottaa organisaatiolle vähemmän arvoa: joukon moninaisuus pienenee. Kyseessä

[148] Bacon et al. 2009.
[149] Lebraty & Lobre-Lebraty 2013, s. 15, 44.
[150] Lebraty & Lobre-Lebraty 2013, s. 20, 48.
[151] Lebraty & Lobre-Lebraty 2013, s. 23.
[152] Fryer & Simperl 2017.

on eräänlainen joukkoistamisen paradoksi. Joukon toimintaa voidaan kuitenkin organisaation toimesta parantaa takaamalla jäsenten riippumattomuus sekä pyrkimällä ennustamaan tai määrittämään joukon yleistä käyttäytymistä, jotta sille voitaisiin antaa virikkeitä.[153]

Tutkimuskirjallisuudessa on erilaisia näkökulmia ja suhtautumisia siihen, että yksityishenkilöt etsivät ohjelmistoista haavoittuvuuksia ja julkaisevat tietoja niistä.[154] Viimeisimmissä tutkimuksissa on kuitenkin käännytty sille kannalle, että joukkoistaminen järjestelmissä olevien haavoittuvuuksien paikallistamiseksi on kannattavaa.

Joukkoistaminen on prosessi, johon kuuluu kilpailullisia elementtejä maksujen, palkintojen tai muunlaisten palkkioiden muodossa työn toteuttamiseksi tai informaation tuottamiseksi. Usein joukkoistamisen kohteena olevasta suuremmasta kokonaisuudesta muodostetaan pienempiä palasia.[155] Tässäkin mielessä bug bounty -ohjelmat poikkeavat perinteisimmistä joukkoistamisen muodoista, sillä ohjelmassa yhden hakkerin toimintakenttänä on koko ohjelma, eikä vain osaa siitä.

Myös tietoturvan testaaminen loppukäyttäjillä on eräänlaista joukkoistamista, mutta ainoana tietoturvatestauksen menetelmänä se on kyseenalainen[156]. Bug bounty -ohjelmat ovat eräänlainen jalostettu versio loppukäyttäjillä testaamisesta: kritisoidussa tapauksessa loppukäyttäjille ei korvata heidän näkemäänsä aikaa ja vaivaa välttämättä mitenkään, loppukäyttäjät eivät aina ole yhtä vihkiytyneitä tietoturvan testaamiseen kuin bug bounty -ohjelmiin osallistuvat hakkerit ja – toisin kuin kritisoidun loppukäyttäjillä testaamisen kohdalla – bug bounty -ohjelman järjestäminen on ainakin jossain määrin koordinoitua toimintaa. Bug bounty -ohjelmat myös harvoin ovat ainoa tietoturvatestaamisen muoto, jota ohjelmistonkehityksessä käytetään.

[153] Lebraty & Lobre-Lebraty 2013, s. 23.
[154] Ks. esim. Ozment 2005 ja Rescorla 2004.
[155] Bacon et al. 2009.
[156] Råman 2006, s. 89.

3.3 Sääntelyteoreettinen näkökulma

Haavoittuvuusmarkkinat ovat ajan myötä kehittyneet itseään säänteleviksi. Ennen tätä kehitystä pääasiallisena toimintamuotona oli, että hakkerin paikallistaessa haavoittuvuuden tämä julkaisi sen Internetin keskustelupalstoilla (ns. *full disclosure*), erityisesti silloin, kun ohjelmistoyritys ei reagoinut hakkerin yhteydenottoihin halutulla tavalla. On ymmärrettävää, että ohjelmistoyritykset eivät arvostaneet tai arvosta tätä toimintamenettelyä, mikä onkin johtanut toisinaan oikeudellisiin vaatimuksiin hakkereita kohtaan.

Tietoturva alkoi kuitenkin saada entistä enemmän huomiota erilaisten hyökkäysten lisääntyessä 2000-luvulla, mikä on vaikuttanut ohjelmistoyritysten asiakkaiden asiakastyytyväisyyteen niin tietosuojan kuin palveluiden toimintavarmuuden kannalta. Ohjelmistoyritysten oli siis ryhdyttävä panostamaan tietoturvaan. Vielä 2000-luvun alkuvuosina turvallisuusliitännäisiä haavoittuvuuksia on usein piiloteltu negatiivisen julkisuuden pelossa tai siitä syystä, että haavoittuvuuden aiheuttamaa riskiä ei ole ymmärretty[157]. Vähitellen ohjelmistokehitysyritysten mentaliteetti ”ei kerrota” alkoi muuttua muotoon ”kerrotaan avoimesti”[158], ja ohjelmistoyrityksissä havahduttiin huomamaamaan, että jo jonkin aikaa vapaaehtoiset henkilöt ovat ilmoittaneet niille paikallistamistaan haavoittuvuuksista – miksi näitä vapaaehtoisten ilmoituksia ei siis hyödynnettäisi. Yritykset myös havahtuivat siihen, että ne voivat kannustaa hakkereita etsimään palveluistaan haavoittuvuuksia, jolloin hakkerin houkutus ansaita osaamisellaan rahaa myymällä haavoittuvuus pimeillä markkinoilla pienenisi.

Ajan mittaan markkinat ovat kehittyneet entisestään ja alkaneet vahvemmin säännellä itse itseään: esimerkiksi bug bounty -ohjelmissa ohjelman säännöt ovat nykyään vakiomuotoinen osa ohjelmia, samoin kuin sääntöjen yksityiskohtana esimerkiksi turvasatamat[159]. Haavoittuvuuksien raportoinnista on muodostunut ICT-alan itsesääntelymekanismi, jossa eri toimijoilla on yleisiä ohjelinjoja sekä heidän kanssaan toimimiseen, että heille itselleen.[160] Bug bounty -ohjelman säännöt ovat yksi esimerkki alan itsesääntelystä.

---

[157] Råman 2006, s. 123.
[158] Esimerkiksi kansainvälisesti toimiva kuljetus- ja logistiikkayhtiö Maersk on kertonut julkisuudessa avoimesti siihen kohdistuneesta NotPetya -hyökkäyksestä vuonna 2017.
[159] Turvasatamien merkityksestä bug bounty -ohjelmille ks. esim. Elazari Bar On 2018; Kilovaty 2019, s. 487.
[160] Råman 2006, s. 229.

Tähän asti haavoittuvuusmarkkinoiden itsesääntely on siis toiminut, ja siihen yleisellä tasolla luotetaan kaikkien osapuolten toimesta, eikä kansallisvaltioilla ole ollut kovin suuria pyrkimyksiä luoda sääntelyä joukkoistetun tietoturvantestauksen ympärille. Ainakaan Suomessa ei ole havaittavissa tällaisia lainsäädäntöhankkeita[161]. EU-tasolla uusinta lainsäädäntökehitystä edustaa vuonna 2019 voimaan astunut niin kutsuttu kyberturvallisuusasetus, joka tosin keskittyy ENISAn tehtävien määrittelyyn ja eurooppalaisen kyberturvallisuuden sertifiointikehykseen[162].

Juridisella sääntelyllä ei voida saada aikaan optimaalisia markkinoita haavoittuvuuksien paikallistamiselle: sen sijaan taloudelliset vetovoimat tulevat sääntelemään markkinoita.[163] Ohjelmistojen haavoittuvuusasteeseen kyetään puuttumaan paremmin itsesääntelevien markkinamekanismien avulla kuin keskitetysti toteutetulla sääntelyllä.[164]

Markkinoiden sääntelyn toteuttaminen itsesääntelynä – tässä tapauksessa luomalla bug bounty -ohjelmia ja määrittämällä niille politiikkoja, käytäntöjä ja sääntöjä – edellyttää, että näitä itse asetettuja sääntöjä ja kriteereitä myös noudatetaan kaikkien osapuolten taholta: hakkereiden, alustayritysten ja ohjelmistokehittäjien. Jos alustayritys ei toimi itse asettamiensa kriteerien mukaisesti, rapauttaa se hakkerien raportointihalukkuutta, ja riskinä on esimerkiksi hakkerien siirtyminen myymään löydettyjä haavoittuvuuksia laittomille markkinoille.[165] Esimerkkinä erilaisista alalle muodostuneista käytännöistä voidaan mainita alustayritysten pyrkimykset heikkolaatuisten raporttien määrän vähentämiseksi, joita on sisällytetty myös ohjelmien sääntöihin.[166]

Itsesääntelyynkin liittyy problematiikkaa. Sääntelyn, myös itsesääntelyn, tulee olla mittasuhteiltaan sopusoinnussa, sillä liian tiukat säännöt voivat vähentää myös toivotunlaisten raporttien määrää.[167] Käytännöt ja säännöt eivät myöskään ole samanlaisia jokaisen

[161] Sen sijaan USA:ssa on ollut pyrkimyksiä kyberturvallisuusliitännäiseen sääntelyyn, ks. esim. senaattori Mark R. Warnerin lehdistötiedote 11.3.2019.
[162] Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus).
[163] Algarni & Malaiya 2014.
[164] Bacon et al. 2009.
[165] Ks. esim. Meyerin kokemukset PayPalin HackerOne-alustalla toteutetusta boug bounty -ohjelmasta. Meyer 17.2.2020.
[166] Laszka et al. 2016, s. 162–163.
[167] Laszka et al. 2016, s. 162–163.

alustayrityksen tai bug bounty -ohjelman toteuttajan kohdalla, vaan niissä esiintyy variaatiota, mikä voi entisestään aiheuttaa epäselvyyttä hakkerien joukossa.

Toinen esimerkki itsesääntelystä on hakkereiden ja ohjelmistokehittäjien välille syntynyt menettely, jossa bug bounty -ohjelman tai VDP:n ulkopuolella haavoittuvuuden ohjelmistokehittäjälle raportoinut hakkeri antaa kehittäjälle riittävän paljon aikaa, esimerkiksi 30–45 päivää, reagoida ja korjata haavoittuvuus, ennen kuin julkaisee haavoittuvuuden. Tällaista menettelyä voidaan pitää eettisesti hyväksyttävänä menettelynä.[168] Mitä yksityiskohtaisemmin haavoittuvuusraportti on laadittu, sitä suopeammin ja vakavammin ohjelmistonkehittäjä siihen todennäköisesti suhtautuu.[169]

3.4 Kustannustehokkuus ja tietoturvan sitruunaongelma

Kustannustehokkuudella juridiikan kontekstissa tarkoitetaan sitä, että yhteiskuntapoliittiset tavoitteet saavutetaan mahdollisimman matalilla kustannuksilla.[170] Tietoturvaa voidaan pitää yhtenä tällaisena yhteiskuntapoliittisena tavoitteena. Julkishallinnollisen toimijan tulee pyrkiä taloudelliseen tehokkuuteen[171]. Tämä ilmenee hallintolain (HL, 434/2003) 7 §:ään paikallistettavasta hallinnon palveluperiaatteesta, johon oleellisena osana kuuluu myös viranomaisen toiminnan tuloksellisuus.[172] Palveluperiaate ilmentää hyvän hallinnon periaatteita. Tuloksellisuuteen yhdistyy samalla myös asianmukaisuus, joka tietystä näkökulmasta katsottuna voi toteutua vain tuloksellisen toiminnan tukemana.[173] Nykyistä hallintolakia valmisteltaessa tehokuudella ei olekaan tarkoitettu pelkästään taloudellista tehokkuutta, vaan myös yksityisen ja julkisen vallan välistä kätevää, virheetöntä ja joustavaa asiakassuhdetta.[174]

[168] Ks. Råman 2006, s. 245.
[169] Råman 2006, s. 249.
[170] Määttä, luentokalvot 12.–14.2.2019.
[171] Kulla 2018, s. 8.
[172] Mäenpää 2017, s. 172.
[173] Ks. myös Kulla 2018, s. 74.
[174] Kulla 2018, s. 71–72.

Tuloksellisuutta voidaan jaotella edelleen toiminnan tuottavuuteen, taloudellisuuteen ja vaikuttavuuteen, joista tuottavuus tähtää mahdollisimman suureen tuotokseen ja taloudellisuus siihen, että toiminta toteutetaan mahdollisimman pienin kustannuksin.[175] Viranomaistoiminnan tulee siis olla taloudellisesti tehokasta jo hallinnon palveluperiaatteen mukaisesti. Täten onkin perusteltua, että viranomaistoiminnassa huomioidaan palveluiden tuottamisen ja lakisääteisten tehtävien toteuttamisen kustannustehokkuus ja myös etsitään aktiivisesti uusia, kustannustehokkaampia vaihtoehtoja toiminnan toteuttamiseen.

Myös julkishallinnossa toimintaa on pyritty tehostamaan palveluita ulkoistamalla. ICT-palveluiden ulkoistamisen tavoitteena on yleensä parantaa toiminnan tehokkuutta, laatua ja joustavuutta. Näiden ohella tavoitteena on myös palvelujen kokonaiskustannusten alentaminen. Toisaalta ulkoistamisessa voi olla kyse siitä, että organisaatiossa ei ole tarpeeksi asiantuntemusta tietyn asiakokonaisuuden hallintaan.[176] Kun ICT-palveluita ulkoistetaan, niitä hankittaessa organisaatioiden tulee kiinnittää huomiota niin tietoturvallisuuteen, varautumiseen, palvelun laatuun kuin kustannustehokkuuteenkin.[177]

Haavoittuvuuksien etsimisen arvo on yksinkertainen: haavoittuvuuksien löytymisen kannalta on parempi, että ”hyvät tyypit” löytävät ne ja ne korjataan, kuin että ”pahat tyypit” löytävät ne ja niitä käytetään hyväksi.[178] Kustannustehokkuuden näkökulmasta bug bounty -ohjelmissa on pohjimmiltaan kyse mahdollisimman optimaalisen menettelyn valitsemisesta tietoturvan testaukselle. Lyhyesti ilmaistuna ohjelman toteuttamiseen kuluu vähemmän taloudellisia resursseja kuin jos testaus järjestettäisiin sisäisenä testauksena. Lisäksi testaajajoukko on monipuolisempi kuin mitä sisäisellä testaamisella saataisiin, joten löydetyt haavoittuvuudetkin ovat todennäköisesti moninaisempia.

Tietoturvauhat ovat niin yleisiä, että uusia merkittäviä haavoittuvuuksia paljastuu miltei joka kuukausi. Haavoittuvuuksien paljastumisella on myös taloudelliset seurauksensa, eivätkä taloudelliset menetykset ole pelkästään suoria, kuten järjestelmien uudelleenasennuksesta koituvat kulut, vaan niitä ilmenee myös epäsuorasti. Tällainen on esimerkiksi verkkopalveluiden luottamuksen vähenemisestä johtuvat vaihtoehtoiskustannukset, ku-

[175] Kulla 2018, s. 127.
[176] Andreasson & Koivisto 2013, s. 77.
[177] Andreasson & Koivisto 2013, s. 78.
[178] Rescorla 2004. Lihavoinnit poistettu tässä.

ten mainehaitat, jotka syntyvät uutisoidusta haavoittuvuudesta ja saattavat aiheuttaa verkkopalveluiden käytön vähentymistä.[179]. Sekä suorat että epäsuorat kustannukset koskevat niin yksityistä sektoria kuin julkishallintoakin, vaikka niillä onkin hieman erilaisia vaikutuksia.

Yksityisellä sektorilla haavoittuvuuden julkiseksi tulemisesta on haittaa myös yrityksen markkina-arvolle[180] – vaikka julkisella sektorilla ei voidakaan määrittää organisaation markkina-arvoa, ovat mainehaitat ja niiden seuraukset silti mahdollisia, ellei todennäköisiä. Yksityisellä puolella esimerkiksi verkkokaupoissa kuluttajat voivat siirtyä uutisoitujen tietoturvaongelmien vuoksi kilpailijan verkkokaupan asiakkaiksi. Julkisella sektorilla asiakas voi alkaa vältellä sähköisten palveluiden käyttöä ja pitäytyä paperisissa lomakkeissa, tai esimerkiksi asioida viranomaisessa paikan päällä sen sijaan, että asioisi sähköisesti tai ylipäätään lukisi tarvitsemansa tiedon viranomaisen nettisivuilta.[181] Julkishallinnossa korkean tietoturvan ja siitä viestimisen välttämisen vaihtoehtoiskustannuksena on siis muiden kuin sähköisten palveluiden kustannusten kasvaminen. Koska sähköisten palveluiden käyttäminen olisi taloudellisesti kannattavampaa kuin paperisten tai fyysisten asiakaspalveluiden tuottaminen, toiminnan kustannustehokkuus kärsii huonon tietoturvan tilanteessa. Mainehaittojen torjumisella on siis oma vaikutuksensa kustannustehokkuudelle ja järjestelmän tietoturvan korkea taso ja myös tästä korkeasta tietoturvan tasosta, luotettavuudesta, viestiminen ovat osa kustannustehokkuutta.

Tietoturvaa voidaan lähestyä taloustieteen perspektiivistä myös sitruunaongelman kautta. Sitruunaongelma on taloustieteen teoria, joka kuvaa ostajan ja myyjän välistä tiedollista epäsymmetriaa.[182] Tietoturvallisuus ei ole näkyvää tai muilla tavoin havaittavaa, ja sitä on myös haastava mitata[183], joten sitä on pidettävä luottamushyödykkeenä[184]. Luottamus-

[179] Van Goethem et al. 2014.
[180] Tietoturvahaavoittuvuuksien julkaisun vaikutuksista ohjelmistokehittäjien markkina-arvoon on kirjoittanut esimerkiksi Telang & Wattal 2005, jotka vertaavat tutkimustuloksiaan artikkelissaan myös muuhun aihepiiriä käsittelevään tutkimukseen, ks. erit. taulukko 5, s. 10. Telangin & Wattalin tutkimuksen mukaan haavoittuvuuden julkiseksi tuleminen alentaa merkittävästi ohjelmistokehittäjän markkina-arvoa, joskaan ei välttämättä kovin pitkäkestoisesti (s. 9).
[181] Ks. myös Voutilainen 2007, s. 109.
[182] Ks. Akerlof 1970.
[183] Esim. Ozment 2004.
[184] Jaottelusta luottamushyödykkeisiin, kokemushyödykkeisiin ja etsintähyödykkeisiin ks. esim. Määtän luentokalvot 2019, Lapin yliopisto.

hyödykkeellä tarkoitetaan hyödykettä, johon tutustuminen tai muihin tuotteisiin vertaaminen ei auta sen päättelyssä, onko tuote laadukas: on vain luotettava siihen, että se toimii[185]. Koska ostaja – tai palvelun käyttäjä – ei voi erottaa, mikä ohjelmisto on turvallinen ja mikä ei, kaikkien ohjelmistojen hinta putoaa epäturvallisten ohjelmistojen tasolle. Tästä syystä kehittäjillä ei ole suurta intressiä panostaa tietoturvallisuuteen.[186] Markkinahyödykkeiden epätäydellinen informaatio johtaa lopulta siihen, että markkinoilla on vain huonolaatuisia hyödykkeitä, tai ei hyödykkeitä ollenkaan[187]. Epävarmuuteen voidaan kuitenkin pureutua takuun, brändin tai lisensoinnin avulla[188]. Tietyn ohjelmiston tietoturvan laatua voidaan yrittää viestiä näiden kaikkien avulla, mutta nämäkään eivät takaa sitä, että ohjelmistossa ei olisi haavoittuvuuksia. Tietoturvakentällä ei kuitenkaan nykyään pelkästään luoteta, vaan tietoturvaa myös seurataan. Seurantakaan ei anna täyttä varmuutta tietoturvan tasosta, mutta se parantaa tilannekuvaa.[189]

Sitruunaongelman lisäksi tietoturvaan soveltuu taloustieteellisistä teorioista myös yhteismaan ongelma. Kun samassa verkossa toimivista tietokoneista yhden kohdalla lipsutaan tietoturvasta, kasvaa koko verkon riski joutua hyökkäyksen kohteeksi. Sen sijaan, jos yhden tietokoneen kohdalla erityisesti panostetaan tietoturvaan, pienentää se koko verkon riskiä joutua hyökkäyksen kohteeksi. Yksilöt ovat taipuvaisia vapaamatkustajuuteen ja odottamaan, että joku muu huolehtisi tietoturvasta heidän puolestaan.[190]

Sitruunaongelman mukaan ohjelmistokehittäjät eivät panosta tietoturvaan ja yhteismaan ongelman mukaan tietoturvaan panostaminen ei kiinnosta myöskään kuluttajia. Tätä umpikujaa voidaan nimittää markkinahäiriöksi. Markkinahäiriöihin voidaan puuttua sääntelyllä, mitä tosin ei pidetä kovin tehokkaana. Toinen tapa puuttua markkinahäiriöön on sellaisten uusien markkinamekanismien luominen, jotka antavat palautetta ja vähentävät ongelmia jo niiden lähteillä. Tällä tavalla voidaan oikeuttaa haavoittuvuusmarkkinat teoreettisella tasolla.[191] Bug bounty -ohjelmia voidaan käyttää vastaamaan tietoturvan sit-

[185] Ks. esim. Råman 2006, s. 126.
[186] Böhme 2006.
[187] Akerlof 1970.
[188] Akerlof 1970, s. 499–500.
[189] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[190] Böhme 2006.
[191] Böhme 2006.

ruunaongelmaan: kuten jo edellä todettua, ohjelmaa käyttämällä voidaan signaloida kuluttajille tai asiakkaille, että tietojärjestelmän turvallisuuteen panostetaan. Ohjelman kohteen luotettavuus paranee myös siitä syytä, että siinä on ohjelman päättymisen jälkeen potentiaalisesti vähemmän haavoittuvuuksia kuin ennen ohjelmaa.

Kustannustehokkuutta on tutkimuskentällä ylipäätään analysoitu pääsääntöisesti vain tilaajan tai ohjelmistoyrityksen näkökulmasta. Kustannustehokkuutta voidaan kuitenkin lähestyä myös alustayrityksen tai hakkerin perspektiivistä. Koska tämä tutkimus keskittyy julkishallinnon näkökulmaan, todettakoon vain mainintana, että hakkerin kustannustehokkuusajatteluun vaikuttaa esimerkiksi Pietarin paradoksi. Tämän paradoksin mukaan hakkerin saattaa olla kannattavampaa vaihtaa aina uusimpaan bug bounty -ohjelmaan, sillä uusimmassa ohjelmassa on todennäköisesti jäljellä eniten löytämättömiä haavoittuvuuksia.[192] Myös muihin kuin ohjelman tilaajiin keskittyvä talous- ja käyttäytymistieteellisten teorioiden tarkastelu onkin siis oleellisessa osassa kustannustehokkuuden parantamista tilaajien kohdalla.

3.5 Muita tietoturvan testaamisen ja valvonnan muotoja

Bug bounty -ohjelmat eivät ole ainoa tapa, jolla tietoturvaa voidaan testata, ylläpitää tai jolla tietoturvan tasosta voidaan viestiä. Ylipäätään tietoturvan perustukset laaditaan jo järjestelmän arkkitehtuuria suunniteltaessa. Tässä alaluvussa esitellään lyhyesti esimerkkejä muista tietoturvan testaamisen ja valvonnan muodoista.

Sisäinen testaus tarkoittaa ohjelmistoyrityksen sisällä tapahtuvaa testausta ja koodin läpikäymistä. Ohjelmistokehittäjät pyrkivät vähentämään ohjelmistoissa olevien haavoittuvuuksien määrää esimerkiksi testaamalla ja auditoimalla ohjelmistoja. Näillä keinoilla ei kuitenkaan voida eliminoida kaikkia haavoittuvuuksia esimerkiksi siitä syystä, että taloudelliset rajat tulevat vastaan tai että ohjelmistot ovat teknisesti kompleksisia.[193]

Koodikatselmointi tarkoittaa sitä, että ohjelmistoyrityksen ulkopuoliselta taholta ostetaan palvelu, jossa tahon edustajat käyvät läpi ohjelmiston koodia. Penetraatiotestauksessa

[192] Maillart et al. 2017. Pietarin paradoksista tarkemmin ks. esim. Maillart et al. 2017.
[193] Zhao et al. 2014.

taas tavoitteena on hyökätä järjestelmään. Testauspalvelu tilataan pääsääntöisesti ulkopuoliselta taholta. Penetraatiotestaus ei välttämättä rajoitu vain tietojärjestelmien tietoturvallisuuteen, vaan myös fyysisen toimintaympäristön tietoturvallisuuteen. Testauksen aikana voidaan esimerkiksi lähettää kalasteluviestejä työntekijöille, tiputella muistitikkuja strategisiin paikkoihin tai esiintyä huoltoyhtiön edustajana pyrkien kävelemään sisään tiloihin, joihin kulku on rajoitettu[194].

Yksityisten tietoturvayritysten myöntämät tietoturvasertifikaatit ovat sovelluksissa tai Internet-sivuilla näkyvissä olevia kuvia, jotka implikoivat sitä, että kuvan haltija täyttää sertifikaatin antajan asettamat tietoturvakriteerit. Kun ympäristössä vallitsee epävarmuus, yritykset voivat yrittää erottautua kilpailijoista infrastruktuuriensa turvallisuuden parantamisen lisäksi siten, että ne pyrkivät myös vakuuttamaan palveluiden käyttäjät palveluiden turvallisuudesta. Tietoturvasertifikaatti osoittaa, että verkkosivusto on turvallisuusyrityksen tutkima, eikä sivustolla ole havaittu ongelmia, kuten haavoittuvuuksia tai haittaohjelmia.[195]

Yksityisten tietoturvayritysten turvallisuussertifikaatteja ei kuitenkaan eräiden tutkimusten mukaan voida pitää kovin luotettavina osoituksina siitä, että sivusto olisi turvallinen.[196] Sertifikaatti, joka maksaa sadoista euroista tuhansiin euroihin vuodessa[197], ei siis ole välttämättä kovin kustannustehokas tapa parantaa sivuston tai ohjelmiston turvallisuutta. Sertifikaateilla voidaan kuitenkin pyrkiä osoittamaan kuluttajille, että sivuston haltija tai ohjelmiston kehittäjä on kiinnostunut tietoturvasta. Sama viestinnällinen aspekti voidaan löytää myös julkisista bug bounty -ohjelmista. Sen sijaan ISO-sertifikaatteja tai sellaisia sertifikaatteja, joissa esimerkiksi ENISA on ollut mukana määrittelyprosessissa, voidaan pitää luotettavampana osoituksena tuotteen laadusta ja sen tietoturvan tasosta[198].

Kansallinen tietoturvamerkki taas eroaa joissain määrin turvallisuussertifikaatista. Kansallinen tietoturvamerkki on Liikenne- ja viestintävirasto Traficomin myöntämä ja kertoo siitä, että merkillä varustettu tuote tai palvelu on suunniteltu turvalliseksi. Merkki on

[194] Ks. esim. Peiponen – Yle 25.7.2018.
[195] Van Goethem et al. 2014.
[196] Van Goethem et al. 2014.
[197] Van Goethem et al. 2014.
[198] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.

suunniteltu erityisesti IoT-laitteita varten, ja se myönnetään vain laitteille, jotka täyttävät Traficomin asettamat tietoturvavaatimukset.[199] Tätäkin merkkiä voidaan kritisoida esimerkiksi siitä, että parhaimmillaankin merkki on katsaus tiettyyn ajanhetkeen. Lomake, johon merkki perustuu, kysyy hyvin perustason asioita, ja lisäksi on olemassa tarkastus, josta ei ollut saatavilla lisätietoja. Toki on parempi, että tuotteella on merkki kuin että sitä ei ole, mutta merkki ei ole turvallisuuden tae. Minimissään merkin hyöty on siinä, että kun tuotteessa on merkki, niin kuluttaja havaitsee, että laite on kiinni Internetissä.[200]

Tietoturvavalvomo (*Security operation center*, SOC) on organisaatioon perustettu toiminto, jonka tehtävänä on seurata ajantasaista tietoturvaan liittyvää tilannetta, kuten esimerkiksi organisaation järjestelmistä tulevia tietoturva-aiheisia ilmoituksia. Tietoturvavalvomon tehtävänä on havaita, analysoida ja vastata tietoturvaloukkauksiin.[201]

[199] Traficom – Tietoturvamerkki.fi -sivuston etusivu.
[200] Ks. myös Herrasmieshakkerit-podcast, jakso 0x03, julkaistu 5.12.2019.
[201] Ks. esim. Latvanen – Tivi, 24.10.2019.

4 Tietoturva ja oikeus

Tässä luvussa lähestytään tietoturvaa teoreettisesta ja juridisesta näkökulmasta. Erityisesti ensimmäinen alaluku keskittyy tietoturvan teoriapuolen avaamiseen. Toisessa alaluvussa perehdytään siihen, millä tavalla tietoturva linkittyy oikeustieteen teoreettiselle tasolle. Kolmannessa alaluvussa syvennytään sääntelyperustaan, jonka myötä viranomaisella on velvollisuus kehittää ja ylläpitää tietoturvaa, ja neljännessä alaluvussa avataan sitä, miten tietoturvaan panostamalla voidaan edistää kyberrikollisuuden torjuntaa.

4.1 Tietoturvan teoreettista taustaa

Kyberturvallisuuden sanaston mukaan tietoturvalla tai tietoturvallisuudella tarkoitetaan järjestelyjä, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus.[202] Kumoutuneessa valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) määriteltiin tietoturvallisuus asetuksen 3.1 §:n 2 kohdassa. Tietoturvallisuudella tarkoitettiin tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä. Kumoutuneen asetuksen sisällöllisesti osin korvanneessa tiedonhallintalaissa (L julkisen hallinnon tiedonhallinnasta, TihL, 906/2019) ei määritellä tietoturvaa. Sen sijaan mainitussa laissa tietoturvallisuustoimenpiteellä tarkoitetaan 2.1 §:n 8 kohdan mukaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Juridiset määritelmät eivät siis ole täysin yhteneväiset, mutta melko lähellä toisiaan. Tietoturva on säädöstasolla määritelty ainakin laissa sähköisen viestinnän palveluista (917/2014), jonka mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (3.1 §:n 28 k).

Yleisessä kielenkäytössä tietoturva ja tietoturvallisuus tarkoittavat käsitteellisesti ja sisällöllisesti samaa asiaa, mutta niiden määrittelyssä voidaan kuitenkin nähdä joitain eroja.

[202] Kyberturvallisuuden sanasto 2018, termi 10: tietoturva; tietoturvallisuus.

Erottelun mukaan tietoturva käsittää hallinnolliset ja tekniset toimet tietojen suojaamiseksi, kun taas tietoturvallisuus tarkoittaa tavoitetilaa, johon pyritään toteuttamalla edellä mainittuja toimia.[203] Turvallisuus taas voidaan määritellä olotilaksi, jossa mahdollisuus uhkan toteutumiselle on pienimmillään, tosin reaalimaailmassa absoluuttisen turvallisuuden tason saavuttaminen on lähes mahdotonta.[204] Tässä tutkimuksessa tietoturvaa ja tietoturvallisuutta käytetään synonyymeinä toisilleen.

Tietojärjestelmällä sen sijaan yleensä tarkoitetaan tietyssä organisaatiossa käytettävää tietojenkäsittely- ja siirtolaitteiden muodostamaa verkostoa. Tietojärjestelmät voidaan myös ymmärtää toiminnallisina kokonaisuuksina niiden tuottamien palvelujen perusteella, jolloin ratkaisevaa ei välttämättä ole tekninen kokonaisuus.[205] Tiedonhallintalaissa tietojärjestelmä määritellään tietojenkäsittelylaitteista, ohjelmistoista ja muusta tietojenkäsittelystä koostuvaksi kokonaisjärjestelyksi (2.1 §:n 3 k).

Kuten lainsäädännön määritelmätkin antavat ymmärtää, oikeudellisessa mielessä tietoturvallisuus koostuu informaation, tietojenkäsittelyn ja tietoliikenteen luottamuksellisuutta, eheyttä, aitoutta ja käytettävyyttä sekä näiden ylläpitoa ja suojaamista sääntelevistä normeista. Oikeudellisena käsitteenä tietoturvallisuutta voidaan kuvata myös oikeudellisesti järjestetyksi strategiseksi riskienhallintatoiminnoksi.[206]

Sekä yksityisen sektorin että julkishallinnon keskeisten toimintojen tehokas ja häiriötön ylläpito ja kehittäminen edellyttävät tietojenkäsittelyn ja tietoliikenteen tietoturvallisuudesta varmistumista – tällä tarkoitetaan tietojärjestelmien luottamuksen, eheyden ja käytettävyyden (tai saatavuuden) turvaamista.[207] Englanniksi sama asia ilmaistaan käyttämällä akronyymiä CIA (*confidentiality, integrity, availability*). Luottamuksellisuuden, eheyden ja käytettävyyden tai saatavuuden muodostamaa kokonaisuutta voidaan kutsua myös tietojenkäsittelyrauha-nimiseksi oikeushyväksi[208].

Lyhyesti ilmaistuna tiedon luottamuksellisuudella tarkoitetaan sitä, että tieto on saatavilla vain niille henkilöille, joilla on oikeus saada se. Eheydellä tarkoitetaan tiedon muodon

[203] Voutilainen 2007, s. 112.
[204] Saarenpää et al. 1997, s. 21.
[205] HE 94/1993 vp, s. 155.
[206] Korhonen 25.3.2015, s. 40–41.
[207] Saarenpää et al. 1997, s. V.
[208] Ks. HE 94/1993 vp, s. 155; ks. myös Nevalainen 2019, s. 136.

säilyttämistä tahattomalta tai lainvastaiselta muuttamiselta. Tiedon käytettävyyttä ja saatavuutta taas voidaan pitää lähes synonyymisinä tiedon ominaisuuksina, joihin kuuluu esimerkiksi se, että tieto on saatavilla silloin, kun sille on tarvetta. Tiedon käytettävyys sisältää myös sen, että tieto on siihen oikeutettujen tahojen saatavilla.[209] Luottamuksellisuus, eheys ja käytettävyys tiivistävät tietoturvan perimmäisen tarkoituksen. Tietoturvallisuudella suojataan organisaatioiden omaan toimintaan, yhteiskunnan toimintaan ja kansalaisiin liittyviä tietoja: oikeat ja luotettavat tiedot ovat keskeinen osa niin julkishallinnon kuin yksityisen sektorin päätöksentekoa ja toimintavarmuutta[210].

Tietoturvaa voidaan jaotella eri tavoin, ja turvallisuus ylipäätään voidaan jakaa kahteen osa-alueeseen: tilaan, jossa uhkaavista asioista huolimatta turvallisuutta haittaavia tekijöitä ei esiinny, sekä turvallisuustoimiin jotka on suunniteltu tuon tilan saavuttamiseksi. Absoluuttinen turvallisuus on kuitenkin molempien osa-alueiden kohdalla utopiaa: kaikkia uhkia ei voida ennakoida ja turvallisuustoimenpiteiden pettäminen on aina mahdollista.[211]

Tietoturvan jaottelusta esimerkkinä Andreasson & Koivisto jakavat tietoturvan kahdeksaan eri osa-alueeseen, joita ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus.[212] Edellisen jaottelun lisäksi tietoturva voidaan jakaa tekniseen ja hallinnolliseen tietoturvaan. Vaikka yksittäinen henkilö on harvoin sekä teknisen että hallinnollisen tietoturvan asiantuntija, on erityisesti tietosuojan kannalta oleellista, että esimerkiksi organisaatiossa toimivalla tietosuojavastaavalla on perustiedot näistä molemmista osa-alueista.[213]

Tietoturvassa on kyse rahasta ja vallasta; siitä, kuka saa lukea, kirjoittaa tai suorittaa minkäkin ohjelman.[214] Tietoturvallisuus tulee organisoida, ja sitä tulee toteuttaa siten, että se tukee parhaalla mahdollisella tavalla organisaation perustehtävää ja strategian mukaisten

[209] Ks. esim. Voutilainen 2007, s. 113.
[210] Andreasson & Koivisto 2013, s. 32.
[211] Esim. Råman 2006, s. 19.
[212] Andreasson & Koivisto 2013, s. 52.
[213] Andreasson et al. 2019, s. 133.
[214] Anderson 2002.

tavoitteiden saavuttamista. Tietoturvallisuus on osa lain toteuttamista ja hyvää hallintotapaa, ja toisaalta tietoturvallisuuden toteuttamisen tulee olla myös kustannustehokasta.[215]

Tietoturva ja sen taso tietyssä ohjelmistossa ei ole stabiilia, vaan muuttuu ajassa. Tämän vuoksi ohjelmisto tai verkkopalvelu, jota pidettiin turvallisena pari vuotta sitten, ei välttämättä nauti samanlaista statusta enää tänä päivänä.[216] Oikeastaan tietoturvan tasoa ei tarvitse verrata edes siihen, millainen tietoturvan taso oli vuosia takaperin, vaan sitä voidaan verrata edelliseen päivään tai jopa edelliseen tuntiin: uusien haavoittuvuuksien paljastumiseen ja korjaamiseen on varauduttava jatkuvasti[217]. Äkilliset muutokset johtuvat nollapäivähaavoittuvuuksien (*zero day vulnerability*) löytymisestä.

Nollapäivähaavoittuvuus on tietoturva-aukko, jonka olemassaolosta ohjelman kehittäjät eivät ole tietoisia ennen kuin haavoittuvuus on tullut julkiseksi. Termi viittaa siihen, että ohjelman kehittäjillä on nolla päivää aikaa haavoittuvuuden poistamiseen siitä hetkestä, kun haavoittuvuus julkaistaan.[218]. Nollapäivähaavoittuvuuksia voidaan paikallistaa siten, että järjestelmään tai verkkosivulle kohdistuu hyökkäys, jossa haavoittuvuutta käytetään hyväksi. Toivottavampaa kuitenkin olisi, että haavoittuvuus paikallistettaisiin ennen, kun vihamielinen taho käyttää sitä hyväkseen. Ohjelmistossa oleva, vakavakin haavoittuvuus voi olla piilevänä vuosikausia, ennen kuin se havaitaan syystä tai toisesta[219].

Turvallisuusliitännäinen haavoittuvuus mahdollistaa oikeudettoman käytön, tietojen tuhoamisen, muuttamisen tai varastamisen tietojärjestelmästä[220] – siis sellaiset asiat, joita tietoturvan luottamuksellisuudella, eheydellä ja käytettävyydellä suojellaan. Haavoittuvuudet eivät aiheuta haittaa pelkästään organisaatioille, vaan tietoturvaloukkauksen seurauksena myös luonnolliselle henkilölle voi aiheutua fyysistä, aineellista, aineetonta, taloudellista tai sosiaalista vahinkoa[221],

[215] Andreasson & Koivisto 2013, s. 32.
[216] Ks. esim. Råman 2006, s. 71, alaviite 155.
[217] Alhazmi & Malaiya 2005.
[218] Sanastokeskus TSK, Tietotekniikan termitalkoot, *nollapäivähaavoittuvuus*, lisätty 26.8.2018.
[219] Ozment & Schechter 2006. Ozmentin &Schechterin OpenBSD-käyttöjärjestelmään ja sen eri versioihin keskittyneen tutkimuksen mukaan käyttöjärjestelmän julkaistuissa versiossa jo alun perin olleen haavoittuvuuden eliniän mediaani on vähintään 2,6 vuotta.
[220] Ks. esim. Kuehn 2014.
[221] Andreasson et al. 2019, s. 171.

Suurimmassa osassa tietojärjestelmiä on jonkinlaisia haavoittuvuuksia, mutta se ei tarkoita, että näitä järjestelmiä ei voisi käyttää. Kaikki haavoittuvuudet eivät johda hyökkäykseen, eivätkä kaikki hyökkäykset menesty.[222] Haavoittuvuuksien paikallistaminen on kuitenkin tärkeää sen vuoksi, että paikallistamalla ja paikkaamalla haavoittuvuudet ennen kuin niitä ehditään käyttää vääriin tarkoituksiin turvataan tietojärjestelmän toiminnan jatkuvuutta ja estetään luvaton tunkeutuminen järjestelmään. Haavoittumattomuutta voidaan edistää muun muassa varajärjestelmin, varmuuskopioinnilla sekä järjestelmään sisään syötettävän informaation validoinnilla. Lisäksi tietojärjestelmään tunkeutumista estävät toimet, kuten palomuurit ja salauksen käyttö tukevat järjestelmän turvallisuutta.[223] Vaikka tietty yksittäinen haavoittuvuus ei vaikuttaisi vakavalta, haavoittuvuuksien kokonaisvaikutus voi useampia tällaisia haavoittuvuuksia ketjuttamalla ja yhdessä käyttämällä kasvaa huomattavan merkittäväksi – haavoittuvuuksien ketjuttamista myös usein käytetään hyökkäyksissä[224]. Tästä syystä myös harmittomilta vaikuttavat haavoittuvuudet on syytä paikallistaa ja korjata.

Haavoittuvuus on tietoturvan ja tietojärjestelmän laadun yhdistävä tekijä. Ohjelmiston huono laatu ei kuitenkaan aina tarkoita sitä, ettei ohjelmisto olisi turvallinen. Toisaalta turvallisuuteen vaikuttavat heikkoudet eivät aina ilmene ongelmina ohjelmiston käytettävyydessä, mikä tekee turvallisuuteen liittyvien haavoittuvuuksien havaitsemisesta haastavaa.[225]

Tietojärjestelmiä testataan haavoittuvuuksien paikallistamiseksi. Tietoturvan testaus on kuitenkin vain yksi osa tietoturvaa: tietoturvan rakentaminen alkaa jo tietojärjestelmää suunniteltaessa, eli turvallisuuden peruspilarit valetaan tietojärjestelmän arkkitehtuurissa ratkaisuissa. Arkkitehtuurin ja testaamisen ohella tietoturvaan vaikuttaa myös järjestelmien käyttäjien toiminta, joka muodostaakin usein suurimman riskin tietoturvalle.

Tietoturvallisen järjestelmän kehittäminen edellyttää sekä aikaa että rahaa järjestelmän kehittämisvaiheessa. Koska tietoturva ei useinkaan ole kuluttajille näkyvä ominaisuus eikä siitä ole välittömiä hyötyjä, vaan sen hyödyt ilmenevät vasta pitkän ajan kuluessa,

[222] Råman 2006, s. 21.
[223] Ks. Saarenpää et al. 1997, s. 76–77.
[224] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[225] Råman 2006, s. 21 ja alaviite 45.

syntyy erityisesti kaupallisessa ohjelmistokehityksessä kiusaus nipistää tietoturvaan tarvittavista resursseista.[226] Lisäksi liian tiukaksi määritellyt tietoturvakriteerit voivat johtaa tietoturvariskeihin, mikäli käyttäjät pyrkivät kiertämään tietoturvatoimenpiteitä, joiden he kokevat hankaloittavan järjestelmän käyttöä. Tietoturvan oikean tason eli tarpeellisten tietoturvatoimenpiteiden määrittäminen voi tästäkin syystä olla hankalaa.[227]

Tietoturvan ja sen suojaamisen tarpeen arviointia voidaan määrittää uhkien kautta. Uhka voidaan määritellä sen mahdollisuutena, että informaatioon tai informaatiojärjestelmään kohdistuva vahinko tai häiriö syntyy. Toisaalta uhalla voidaan tarkoittaa myös tällaisen potentiaalisen häiriön tai vahingon kuvausta.[228] Tietoturvallisuuden keskeinen funktio on hallita uhkia ja niiden aiheuttamaa epävarmuutta[229]. Riski sen sijaan voidaan määritellä epävarmuuden vaikutukseksi tavoitteisiin, jossa vaikutus tarkoittaa poikkeamaa odotetusta. Sanalla riski on usein negatiivinen konnotaatio, vaikka riski voi olla myös myönteinen ja saada aikaan mahdollisuuksia.[230]

Tietoturvallisuus on alituista tietoturvariskien ja tietoturvatoimenpiteistä aiheutuvien kustannusten optimointia, mikä edellyttää lähtökohtaisesti uhkien ja riskien taloudellista arvottamista.[231] Tietoturvallisuustoimien kustannusten taloudellinen optimointi ei kuitenkaan liity pelkästään uhkien ja riskien arvottamiseen: suojattavan informaation taloudellinen vaihdanta-arvo ja tuottoarvo vaihtelevat laajalla skaalalla. Tilanteissa, joissa tiedolla on korkea absoluuttinen arvo erityisesti perusoikeuksien takia, on tietoa suojattava siitäkin huolimatta, että suojaamisen kustannukset nousisivat korkeiksi.[232] Tietoturvallisuuden ideaalisena päämääränä onkin informaation ja sen käsittelyn tietoturvallisuusominaisuuksien optimaalinen suojaaminen ja turvaaminen.[233]

Juridiikan kannalta tietoturvan tärkeys ei rajoitu itse tietoturvaan, vaan tietoturvan tärkeys yhdistyy hyvin kiinteästi tietosuojaan. Tietoturvalla ymmärretään ensisijaisesti tiedon eheyden eli integriteetin säilyttämistä ja teknisin keinoin tapahtuvaa suojelua. Tietosuo-

[226] Råman 2006, s. 80.
[227] Andreaason & Koivisto 2013, s. 46–47.
[228] Saarenpää et al. 1997, s. XXXV.
[229] Saarenpää et al. 1997, s. LXX.
[230] Kyberturvallisuuden sanasto 2018, termi 1: riski.
[231] Saarenpää et al. 1997, s. XXXV.
[232] Saarenpää et al. 1997, s. 49–50.
[233] Saarenpää et al. 1997, s. 54, kursiivi poistettu tässä.

jalla taas tarkoitetaan perinteisesti yksityisyyttä loukkaavan tiedon oikeudettoman saannin estämistä. Tietoturvan ja tietosuojan välillä ei ole selkeää rajaa, vaan ne kietoutuvat toisiinsa. Tietosuojaan kiinteästi kuuluvaan yksityisyyden käsitteeseen kuuluu toisaalta oikeus määrätä itseään koskevan tiedon käytöstä, mikä liittyy irrottamattomasti myös tiedon eheyteen. Toisaalta tiedon eheyden suojaaminen edellyttää tietojen saannin rajoituksia eli jonkinasteista salaisuussuojaa, eli tietojärjestelmiin tai tietoon pääsyä on kontrolloitava ja rajoitettava.[234] Henkilötietojen suoja jäisi kovin puutteelliseksi, mikäli ei olisi olemassa tietoturvaa ja tietoturvallisuustoimenpiteitä. Tietoturva voidaankin nähdä yhtenä tietosuojan osa-alueena, joka mahdollistaa tietosuojan toteutumisen.

Tietosuoja keskittyy luonnollisten henkilöiden henkilötietojen suojaamiseen. Henkilötiedolla tarkoitetaan yleisen tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja, kuten esimerkiksi nimeä, sijaintitietoja tai henkilölle tunnusomaista taloudellista tekijää. Olennaista on se, että tämän tiedon avulla tietyn henkilön voi tunnistaa[235]. Henkilötietojen käsittelyllä tarkoitetaan tietosuoja-asetuksen 4 artiklan 2 kohdan mukaisesti toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti.

Henkilötietojen asianmukaisesta käsittelystä on vastuussa rekisterinpitäjä. Rekisterinpitäjä on joko luonnollinen tai oikeushenkilö, jolla on mahdollisuus määritellä käsiteltävät henkilötiedot ja niiden käsittelytapa.[236] Henkilötietojen tietoturvaloukkauksesta on kyse silloin, kun tietojen salassapito, saatavuus tai eheys vaarantuvat, eli kun henkilötietoja esimerkiksi tuhoutuu, häviää tai muuttuu oikeudettomasti, niitä luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle, tietosuojavaltuutetulle, ilman aiheetonta viivytystä, viimeistään 72 tunnin kuluttua loukkauksen havaitsemisesta.[237]

Tietoturvaloukkauksista voidaan tehdä ilmoitus Kyberturvallisuuskeskukselle, ja jos on aihetta epäillä rikosta, voidaan myös tehdä rikosilmoitus poliisille. Koska henkilötietojen tietoturvaloukkaus rajoittuu vain henkilötietoja koskeviin loukkauksiin, on tietomurron

[234] HE 94/1993 vp, s. 132.
[235] Ks. esim. Neuvonen 2019, s. 233.
[236] Neuvonen 2019, s. 234.
[237] Andreasson et al. 2019, s. 172. Ks. myös yleisen tietosuoja-asetuksen 33 artikla.

kohteena olevan järjestelmän sisällöllä merkitystä, kun arvioidaan, onko organisaatiolla ilmoitusvelvollisuutta yleisen tietosuoja-asetuksen perusteella.[238]

Lopuksi lienee vielä hyvä nostaa esiin, että tietoturvalla ei turvata ainoastaan tietosuojaa tai salassapitoa, vaan sillä on liittymänsä myös esimerkiksi tekijänoikeuksien turvaamiseen.[239] Tietoturvalla on siis moninaisia yhteyksiä useille elämän eri osa-alueille. Tietoturva, tietosuoja, salassapitokysymykset sekä tietoliikenteen toiminnan ja luotettavuuden turvaaminen ovat kaikki toisiinsa kietoutuneita kysymyksiä[240].

4.2 Tietoturva perusoikeutena ja oikeusperiaatteena

Tietoturvan sääntelyn perusta on kansainvälisissä ihmisoikeussopimuksissa ja perusoikeuksissa. Kansallisessa lainsäädännössä tietoturvasta säädetään useissa laeissa ja asetuksissa, useamman eri hallinnonalan toimintaa säädellen. Tietoturvallisuuden oikeuslähdeperustaa voidaan paikallistaa myös korkeimman oikeuden ratkaisukäytäntöön, hallinnon virallislähteisiin ja eri alojen itsesääntelyyn.[241] Myös esimerkiksi OECD:llä on pitkät perinteet tietoturvasuositusten saralla, ja näitä suosituksia on omaksuttu myös kansalliseen lainsäädäntöön[242].

Tietoturvallisuuden oikeusperiaate- ja perusoikeustasoinen tarkastelu voidaan aloittaa perustuslain tarkastelulla. Perustuslain 2.3 §:n mukaan julkisen vallan käyttö perustuu lakiin ja kaikessa julkisen vallan käytössä on tarkoin noudatettava lakia. Tietoturvallisuus sisältyy oikeudellisena ulottuvuutena tai oletuksena useisiin perusoikeuksiin[243], esimerkiksi oikeuteen henkilökohtaiseen vapauteen, yksityiselämän ja henkilötietojen suojaan, viestinnän vapauteen, viranomaisen asiakirjajulkisuuteen, omaisuudensuojaan sekä hyvän hallinnon takeisiin.[244] Ilmeisimmät liittymäpinnat tietoturvalla lienee kuitenkin yksityi-

[238] Andreasson et al. 2019, s. 171.
[239] Saarenpää et al. 1997, s. 65.
[240] HE 94/1993 vp, s. 133.
[241] Korhonen 25.3.2015, s. 56.
[242] Ks. esim. valtiovarainministeriön julkaisu 28/2016, joka on sisällöltään OECD:n tuorein, vuoden 2015 suositus Digitaaliseen turvallisuuteen kohdistuvien riskien hallinta taloudellisen ja yhteiskunnallisen hyvinvoinnin edistämiseksi liitteineen, käännettynä suomeksi.
[243] Saarenpää et al. 1997, s. 421.
[244] Saarenpää et al. 1997, s. LXII.

syyden suojaan. Yksityiselämän suojasta säädetään perustuslain 10 §:ssä. Pykälän 1 momentin jälkimmäisestä virkkeestä ilmenevän sääntelyvarauksen mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Henkilötietojen suoja kuuluu lähtökohtaisesti yksityiselämän suojan piiriin[245]. Tietoturvan ohella myös tietosuojalla on kiinteä liittymä perus- ja ihmisoikeuksiin sekä näiden taustalla vaikuttaviin kansainvälisiin lähteisiin.[246] Sääntelytausta määrittää kansallista sääntelyämme ja sitä, millaiseksi oikeusperiaatteet ja oikeuskulttuurimme ajan myötä muodostuvat[247].

Yksityisyyden suoja on yksi informaatio-oikeuden kannalta keskeisiä ihmis- ja perusoikeuksia. Ihmisoikeudella tarkoitetaan oikeutta, joka kuuluu peruuttamattomasti ja luovuttamattomasti kaikille ihmisille kaikkialla ja joka vahvistetaan kansainvälisissä sopimuksissa. Perusoikeudella taas tarkoitetaan kansallisessa lainsäädännössä säädettyä, kaikille kyseisen valtion lainkäyttöpiirissä oleville kuuluvaa oikeutta.[248] Yksityisyyden, yksityiselämän ja henkilötietojen suojan ohella verkkoyhteiskunnassa erityisen merkityksellisinä perus- ja ihmisoikeuksina voidaan pitää ainakin seuraavia, toisiinsa kiinteästi liittyviä oikeuksia: kotirauhaa, viestinnän luottamuksellisuutta sekä sanan- ja ilmaisunvapautta. Nämä perus- ja ihmisoikeudet kietoutuvat sekä toisiinsa,[249] tietosuojaan että tietoturvaan.

Tietosuojan, jota turvataan tietoturvalla, voidaan katsoa koostuvan vaatimuksista, joilla turvataan yksilön perusoikeuksien toteutuminen henkilötietojen käsittelyssä, toisaalta sillä tarkoitetaan myös julkisten ja salassapidettävien henkilötietojen käsittelyn laissa säädettyjä toiminnallisia edellytyksiä ja mahdollisuuksia. Tietosuojan ytimessä on henkilötietojen käsittely, johon liittyy kiinteästi luottamuksellisuus, oikeusturva ja hyvä hallinto,

---

[245] Viljanen 2005, III Yksittäiset perusoikeudet – 6. Yksityiselämän suoja (PL 10 §) – Henkilötietojen suoja. Kirjailija päivittänyt tekstin 9.2.2011.
[246] Andreasson et al. 2019, s. 28. Tarkemmin lueteltuna henkilötietojen suojan kansainvälisoikeudellista sääntelytaustaa ovat Euroopan ihmisoikeussopimus (SopS 85-86/1998), Yhdistyneiden Kansakuntien KP-sopimus, (kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus, 8/1976), Euroopan neuvoston yleissopimus yksilöiden suojelusta automaattisessa tietojenkäsittelyssä (SopS 35–36/1992), Euroopan neuvoston yleissopimus viranomaisen asiakirjojen julkisuudesta (16/2015), Århusin sopimus (tiedonsaantia, yleisön osallistumisoikeutta sekä muutoksenhaku- ja vireillepano-oikeutta ympäristöasioissa koskeva yleissopimus, SopS 121/2004 ja SopS 122/2004) sekä Euroopan unionin perusoikeuskirja (2000/C 364/01). Näiden ohella yhtenä keskeisimpänä sääntelyinstrumenttina voidaan pitää EU:n tietosuoja-asetusta (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)).
[247] Oikeuden monitasomallista ks. Tuori 2000.
[248] Neuvonen 2019, s. 55–56; Hallberg 2005, I Johdanto – 1. Perusoikeusjärjestelmä – Perusoikeuksien suhde ihmisoikeuksiin. Kirjailija päivittänyt tekstin 6.4.2010.
[249] Riekkinen 2019, s. 49.

lainmukaisuus, läpinäkyvyys, saatavuus ja käyttökelpoisuus sekä ajantasaisuus.[250] Yhtenä osana tietosuojaa tietoturva on myös sinällään perusoikeus: tietosuojaa ei ole, jos ei ole tietoturvaa.

Oikeus tietoturvallisuuteen voidaankin määritellä keskeiseksi informaatioyhteiskunnan kansalaisille kuuluvaksi oikeudeksi ja sekä tietoturvan suojaaminen että turvaaminen kuuluvat lainsäätäjän ja julkisen vallan perusvelvoitteisiin.[251] Vaikka tietoturva ei sinällään puhtaasti esiinnykään perustuslain perusoikeuksien joukossa, sisältyy vaatimus tietoturvasta useampiin perusoikeuksiin, jolloin myös tietoturvaa voidaan pitää perusoikeutena. Sen lisäksi, että tietoturvaa voidaan tarkastella yksilöllisenä oikeutena, voidaan tietoturvaa pitää myös kollektiivisena hyvänä, takeena verkkoyhteiskunnan toiminnasta[252].

Tietoturva ei ole kuitenkaan pelkästään perusoikeus: oikeus tietoturvaan on myös informaatio-oikeudellinen periaate, joka sisältää vaatimuksen hyvästä tiedonhallintatavasta niin viranomaisten kuin muiden rekisterinpitäjien osalta.[253] Informaatio-oikeuden periaatteisiin voidaan tietoturvallisuuden ja tietosuojan ohella lukea vähintään tiedollinen itsemääräämisoikeus, julkisuusperiaate, kerättävän tiedon tarkkarajaisuus, sananvapaus, oikeus viestintään ja luottamuksellisen viestinnän suoja[254].

Tietoturvaperiaatteen alaan kuuluu, että rekisteröity voi luottaa tietojaan käsiteltävän siten, että tiedot eivät päädy vieraille tahoille.[255] Informaatio-oikeudellisena oikeusperiaatteena tietoturvallisuus yhdistää tietoturvaa sääntelevää normikokonaisuutta ja näiden normien soveltamista. Oikeusperiaatteena tietoturvallisuus on informaatioyhteiskunnan keskeisimpiä oikeusperiaatteita,[256] ja se vaikuttaa niin julkisoikeuden kuin yksityisoikeuden alalla[257]. Tietoturvallisuutta onkin kuvattu systeemiperiaatteena – systeemiperiaatteet toimivat monimutkaisen oikeusjärjestyksen koherenssin perustana[258].

[250] Voutilainen 2019, s. 68–69.
[251] Saarenpää et al. 1997, s. VI.
[252] Råman 2006, s. 4, alaviite 9.
[253] Neuvonen 2019, s. 47.
[254] Voutilainen 2019, s. 48–53.
[255] Neuvonen 2019, s. 47.
[256] Korhonen 25.3.2015, s. 49.
[257] Saarenpää et al. 1997, s. 426, 522.
[258] Saarenpää et al. 1997, s. LXXI–LXXII.

Tietosuojalainsäädäntö muodostaa tietoturvallisuusoikeuden keskeisen normilähteen, ja tietoturvallisuuden periaatteita sovelletaankin nimenomaan tietosuojalainsäädännön alalla.[259] Tietosuoja ja tietoturvallisuus on kuitenkin erotettava toisistaan: Tietosuoja muodostuu normeista, jotka koskevat yksityisyyden suojaa henkilötietojen käsittelyssä. Tietoturvallisuus sen sijaan on aineellisiin oikeuksiin nähden välineellinen asia.[260]

Oikeusperiaatteina tietosuojaa ja tietoturvaa voidaan myös konkretisoida käytännön tasolle. Näiden ensisijaisena päämääränä on turvata organisaatioiden vastuulla olevien palvelujen jatkuvuus, eli mahdollistaa organisaation palveluihin liittyvien ICT-ratkaisujen käytettävyys sekä prosesseissa, rekistereissä ja palveluissa käytettävien tietojen eheys ja luottamuksellisuus – kaikissa olosuhteissa.[261]

4.3 Viranomaisen velvollisuus tietoturvan kehittämiseen

Julkisen hallinnon käyttämien tietojärjestelmien ja informaation tietoturvallisuudesta huolehtimisen vaatimus voidaan johtaa perustuslain 2.3 §:n hallinnon lainalaisuusperiaatteeseen.[262] Perustuslain 22 §:n mukaan julkisen vallan tulee turvata perusoikeuksien ja ihmisoikeuksien toteutuminen, kuten esimerkiksi perustuslain 10 §:ssä säädetty yksityiselämän suoja. Perusoikeuksien kannalta julkisella vallalla on positiivinen toimintavelvoite, eli julkisen vallan tulee aktiivisella toiminnalla edistää perusoikeuksien toteutumista. Valtiovallan positiivista toimintavelvoitetta on kuvattu EIT:n ratkaisussa I. vastaan Suomi[263]. EIT katsoi, että Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohta edellyttää käytännöllisiä ja tehokkaita takeita, joilla voidaan sulkea pois luvattoman pääsyn mahdollisuudet tietojärjestelmään.[264] Valtion positiivisena velvollisuutena on siis huolehtia tietojärjestelmässä olevien tietojen suojaamisesta.[265]

Hallinto on myös vastuussa tietojärjestelmien asianmukaisesta toimivuudesta sekä tietojenkäsittelyn ja tietojärjestelmien riskien asianmukaisesta hallinnasta.[266] Viranomaisen

[259] Korhonen 25.3.2015, s. 53.
[260] Korhonen 25.3.2015, s. 54.
[261] Andreasson et al. 2019, s. 77.
[262] Korhonen 25.3.2015, s. 58.
[263] EIT 17.7.2008, 20511/03, I. vastaan Suomi.
[264] Ks. myös Voutilainen 2019, s. 36–37.
[265] Voutilainen 2019, s. 37.
[266] Saarenpää et al. 1997, s. 424–425.

tehtäviin kuuluu myös varmistaa, että tietoturvallisuuden asettamat vaatimukset toteutuvat ja että tietoturvallisuuden toteuttamiseen on riittävät resurssit niin talouden, toiminnallisuuden kuin henkilöstön näkökulmasta.[267] Tietoturvatoimenpiteillä edistetään myös yhteiskunnan palvelujen toimintavarmuutta.[268]

Kansallisessa lainsäädännössä on lukuisia normeja, jotka omalta osaltaan tukevat tietoturvallisuuden tavoitteiden eli luottamuksen, eheyden ja saatavuuden suojaamista vahingoilta ja vahingoittamiselta[269]. Tällaisia normeja ovat säädöstasolla esimerkiksi tiedonhallintalaki (906/2019), tiedonhallintalakia täydentävä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), tietosuojalaki (1050/2018), digipalvelulaki (L digitaalisten palveluiden tarjoamisesta 306/2019), laki sähköisestä asioinnista viranomaistoiminnassa (13/2003), laki sähköisen viestinnän palveluista (917/2014), julkisuuslaki (621/1999), hallintolaki (434/2003), rikoslaki (39/1889) sekä laki verotustietojen julkisuudesta (1346/1999). Kaiken kaikkiaan kansallisessa lainsäädännössä tietoturvasta ja tietosuojasta voidaan katsoa edes joissain määrin säädettävän sadoissa eri säädöksissä. Säädöstasoa alemmista normeista sen sijaan voidaan korostaa Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeiden merkitystä. VAHTI-ohjeista oleellisin on vuoden 2020 alussa kumoutunutta tietoturva-asetusta (valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010) täydentänyt Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010)[270]. Mainitusta ohjeesta ei toistaiseksi ole olemassa päivitettyä versiota.

Kansainvälisestä sääntelystä yksi viime vuosina laajasti esillä ollut, tieturvastakin säännöksiä omaava säädös on EU:n yleinen tietosuoja-asetus. Tietoturvan sääntelyyn liittyy kansainvälisellä tasolla myös standardointia. ISO 27001-standardin mukaan organisaatioiden tulee määritellä tietoturvallisuuden hallintapolitiikka ottaen huomioon muun muassa liiketoiminnan ominaispiirteet, suojattavat kohteet ja teknologia. Tietoturvallisuuden hallintapolitiikan tulee myös muun muassa ottaa huomioon lakisääteiset ja hallinnolliset vaatimukset ja sopimuksiin liittyvät tietoturvavelvoitteet sekä olla johdon hyväksymä.[271] ISO 27001 on niin sanottu vaatimusstandardi, jota vasten organisaatio voi sertifioida

[267] Voutilainen 2019, s. 53.
[268] Voutilainen 2019, s. 37.
[269] Saarenpää et al. 1997, s. 418.
[270] VAHTI 2/2020.
[271] Andreasson & Koivisto 2013, s. 36.

oman toimintansa. ISO 27002 sen sijaan on niin sanottu soveltamisstandardi, joka kuvaa, miten vaatimusstandardin vaatimukset voidaan saavuttaa.[272]

Myös ylimpien lainvalvojien ratkaisukäytännön mukaan viranomaisten tulee lainalaisuusperiaatteen mukaisesti oma-aloitteisesti ja aktiivisesti pyrkiä selvittämään ja korjaamaan hallinnon tietojärjestelmien aiheuttamia virheitä sekä estämään tällaisten virheiden syntyminen.[273]

Tietoturvallisuuden merkitys osana hyvää hallintoa on nähty jo viime vuosituhannen puolella, hallitusmuodon aikana (HM 16.2 §), jolloin myös ajatus julkisen vallan positiivisesta toimintavelvoitteesta turvata perus- ja ihmisoikeuksia on jo ollut olemassa (HM 16 a §).[274] Myös hallintolakia koskevassa hallituksen esityksessä 30/1998 vp todetaan asiakirjahallintoon liittyen, että viranomaisen tulee ylläpitämiensä tietojärjestelmien osalta huolehtia riittävistä tietoturvatoimenpiteistä.[275]

Tietoturvallisuuden kiinteä yhteys hyvään sähköiseen hallintoon voidaan kytkeä myös perustuslain oikeusturvaa koskevan 21 §:n tarkasteluun: jokaisella on oikeus saada asiansa käsitellyksi ilman aiheetonta viivytystä toimivaltaisessa viranomaisessa.[276] Hyvän hallinnon ohella tietoturvallisuus on myös osa hyvää tiedonhallintatapaa,[277] josta säädettiin vielä vuodenvaihteeseen 2020 asti julkisuuslain 18 §:ssä. Tiedonhallintalaki, joka astui voimaan 1.1.2020, on korvannut mainitut hyvää tiedonhallintatapaa koskevat säännökset[278].

Uuden tiedonhallintalain myötä tietoturvaa koskevaa sääntelyä nostettiin lain tasolle, aiemman asetustasoisen sääntelyn sijaan.[279] Tietoturvallisuutta koskeva sääntely löytyy tiedonhallintalain 4 luvusta. Lain 12 §:ssä säädetään henkilöstöturvallisuuteen liittyvistä tietoturvallisuustoimenpiteistä. Tiedonhallintayksikön on tunnistettava tehtävät, jotka edellyttävät erityistä luotettavuutta. Tämä suunnittelu- ja arviointivelvollisuus edellyttää

[272] Andreasson & Koivisto 2013, s. 37.
[273] AOK D: 435/1/92, A: 13.4.1993. Samansuuntaisesti myös EOA D:73/4/96, A: 22.4.1996.
[274] Saarenpää et al. 1997, s. 423–424.
[275] HE 30/1998 vp, s. 78–79.
[276] Voutilainen 2007, s. 115. Voutilainen yhdistää mainitun säännöksen hyvän hallinnon perusoikeudelliseen sääntelyyn.
[277] Saarenpää et al. 1997, s. 465.
[278] HE 284/2018 vp, s. 1.
[279] HE 284/2018 vp, s. 8.

tehtäväkohtaista arvioita kustakin tehtävästä ja siitä, millaisia tietoja henkilöstö pääsee kunkin tehtävän puitteissa käsittelemään. Tiedonhallintalaissa ei kuitenkaan säädetä siitä, mitä tällaisen suunnittelun ja arvioinnin jälkeen tiedonhallintayksikön tulisi tehdä tietoturvallisuustoimenpiteinä, mutta samassa yhteydessä on viitattu henkilöturvallisuusselvityksen laatimista sääntelevään turvallisuusselvityslakiin (726/2014) ja yksityisyyden suojasta työelämässä annettuun lakiin (759/2004).[280]

Tiedonhallintalain 13 §:n mukaan tiedonhallintayksikön velvollisuutena on aktiivisesti seurata toimintaympäristön tietoturvallisuuden tilaa, varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuus niiden koko elinkaaren ajan, arvioida riskejä ja tunnistaa olennaiset riskit, jotka voivat vaikuttaa tietoaineistojen luottamuksellisuuteen, eheyteen, saatavuuteen taikka tietojärjestelmän käyttöön ja vikasietoisuuteen, ja lisäksi velvollisuutena on mitoittaa tietoturvallisuustoimenpiteet riskienhallinnan prosessin mukaisesti.[281] Tähän liittyy oleellisena osana myös käyttäjäkeskeisen suunnittelun ja ohjelmiston käytettävyyden huomiointi.[282]

Lain 14 §:ssä säädetään tietoaineistojen siirtämisestä tietoverkossa. Säännöksen mukaan viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on pykälän mukaan järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Tiedonhallintalain 15 § koskee tietoaineistojen turvallisuuden varmistamisesta. Pykälän mukaan viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen tietoaineistojen muuttumattomuus on riittävästi varmistettu. Tietoaineistot tulee suojata teknisiltä ja fyysisiltä vahingoilta, ja tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys tulee varmistaa. Tämän lisäksi tulee varmistaa tietoaineistojen saatavuus ja käyttökelpoisuus. Tietoaineistojen saatavuutta saa rajoittaa ainoastaan silloin, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu. Pykälän 1 momentin viimeisen kohdan mukaan tietoaineistot voidaan tarvittavilta osin arkistoida. Edelleen pykälän 2

[280] Voutilainen 2019, s. 330–331.
[281] Voutilainen 2019, s. 331–332.
[282] Voutilainen 2019, s. 333.

momentin mukaan tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.

Tiedonhallintalain 16 §:ssä säädetään käyttöoikeuksien hallinnasta. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina.[283] Voutilaisen analyysin mukaan vaikuttaa siltä, että käyttöoikeuksien sääntely koskisi vain tietojärjestelmää työkseen käyttäviä henkilöitä, eikä asiakasta[284]. Esimerkiksi bug bounty -ohjelmassa on kuitenkin nimenomaan tarkoituksena, että osallistuja rinnastuu käyttöoikeuksien puolesta järjestelmää käyttävään asiakkaaseen, eikä osallistujille anneta työntekijöihin rinnastettavia käyttöoikeuksia.

Lain 17 §:ssä säädetään lokitietojen keräämisestä. Pykälän mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Tietojärjestelmissä olevien tietojen käytön ja luovutuksen seurannan ohella lokitietojen keräämisen tarkoituksena on tietojärjestelmän teknisten virheiden selvittäminen. Viimeisessä lain tietoturvallisuutta koskevassa pykälässä säädetään turvallisuusluokiteltavista asiakirjoista valtionhallinnossa (18 §).

Myös yleisen tietosuoja-asetuksen myötä on toteutettava käytäntöä, jossa ei riitä, että rekisterinpitäjä noudattaa lakeja, vaan tämän täytyy oma-aloitteisesti ja aktiivisesti osoittaa, että tietosuojavaatimukset on otettu mukaan organisaation henkilötietojen käsittelyprosesseihin ja -käytäntöihin.[285] Tietosuoja-asetuksen 24 artiklan 1 kohdan mukaisesti on rekisterinpitäjän vastuulla toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta. Artiklan sääntelyn mukaisesti on erityisesti huomioitava käsittelyn luonteeseen, laajuuteen, asiayhteyteen, tarkoitukseen sekä henkilön oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit, joihin kuuluu muun muassa tietojenkäsittelyyn liittyvä riski siitä, kun käsitellään suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää[286]. Rekisterinpitäjän vastuulle

[283] Voutilainen 2019, s. 334.
[284] Voutilainen 2019, s. 334.
[285] Andreasson et al. 2019, s. 25.
[286] Tietosuoja-asetuksen johdanto-osan 75 kohta. Ks. myös Voutilainen 2019, s. 122–123.

kuuluu tietosuojaperiaatteiden toimeenpanoa varten muun muassa omavalvonnan kautta tehtävä käytönvalvonta, tietojärjestelmien tietoturva, tietojen salaus, auditoinnit, tarkastus- ja valvontajärjestelmät, käytännesäännöt ja sertifikaattien käyttöönotto.[287]

Tietosuoja-asetuksen 5 (1) f alakohdassa säädetään henkilötietojen käsittelyn periaatteisiin kuuluvaksi eheys ja luottamuksellisuus. Tämä tarkoittaa, että henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, ja erityisesti on huomioitava suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta ja vahingoittumiselta. Mainittujen seikkojen estämiseksi on toteutettava tarvittavat tekniset ja organisatoriset toimet, joista säädetään tarkemmin tietosuoja-asetuksen 32 artiklassa ja kansallisessa lainsäädännössä.[288]

Tietosuoja-asetuksen 32 artiklan 1 kohta sisältää esimerkinomaisen luettelon teknisistä ja organisatorisista toimenpiteistä henkilötietojen suojaamiseksi. Yhtenä luettelon osana on maininta menettelystä, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.

Tietosuoja-asetuksen 4 artiklan 12 kohdan mukaan henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Tämä tarkoittaa sitä, että tietoihin pääsy ilman perusteita, joko vahingossa tai laittomasti, on tietosuoja-asetuksen mukainen tietoturvaloukkaus.[289]

Rekisterinpitäjällä on myös velvollisuus ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle (33 artikla) ja henkilötietojen käsittelijällä on velvollisuus ilmoittaa tietoturvaloukkauksista rekisterinpitäjälle (33 artikla 2 k). Kansallisena valvontaviranomaisena Suomessa toimii tietosuojalain 8 §:n mukaisesti tietosuojavaltuutettu.

[287] Andreasson et al. 2019, s. 30.
[288] Ks. myös Voutilainen 2019, s. 135.
[289] Ks. myös Voutilainen 2019, s. 203.

Tietosuoja-asetuksessa ei ole säädetty siitä, millä tavoin rekisterinpitäjä voi osoittaa noudattaneensa tietosuojaa koskevia vaatimuksia. Käytännössä rekisterinpitäjälle on muodostuttava evidenssi siitä, että se on toiminut tietosuojaa koskevien säännösten mukaisesti.[290] Osoitusvelvollisuutta voidaan toteuttaa myös esimerkiksi siten, että organisaatio on sitoutunut noudattamaan alalla hyväksyttyjä sertifiointimekanismeja[291].

Vaikka tietoturvallisuus onkin erittäin merkittävä osa viranomaistoimintaa, on sitä toteutettaessa noudatettava suhteellisuusperiaatetta. Tarpeettoman raskaat tietoturvajärjestelyt voivat kääntyä itseään vastaan – vaikeakäyttöiset palvelut saavat niin käyttäjät kuin asiakkaat siirtymään toisaalle,[292] mikä voi kääntyä hallinnon toiminnan tehokkuuden periaatetta vastaan[293]. Tietoturvallisuuden suhteellisuusperiaatteeseen kuuluu, että tietoturvallisuustoimenpiteiden tarpeellisuutta arvioitaessa otetaan huomioon informaation ja tietojenkäsittelyn laatu, informaation määrä ja ikä sekä tietoturvallisuustoimenpiteistä johtuvat kustannukset suhteessa tekniseen kehitykseen, käsittelyn riskeihin ja suojattavan informaation luonteeseen.[294]

Viranomaisella on myös velvollisuus tiedottaa toiminnastaan. Tiedottamisvelvollisuus perustuu julkisuuslain 19 §:ään, jossa säädetään viranomaisen velvollisuudesta tiedottaa keskeneräisissä asioissa, ja 20 §:ään, jossa säädetään viranomaisen velvollisuudesta tuottaa ja jakaa tietoa. Nykyaikaiseen viranomaistoimintaan kuuluu aktiivinen toiminta, jolla tarkoitetaan ohjeistamista ja tiedottamista viranomaistoiminnasta ja viranomaisen hallussa olevista tiedoista.[295] Julkisuuslain 20 §:n mukaisesti viranomaisen on edistettävä avoimuutta, julkaistava tietoa toiminnastaan ja huolehdittava toimintaansa koskevien tietojen saatavuudesta. Tiedottamisvelvollisuus liittyy myös löydettyihin haavoittuvuuksiin: ohjelmistonkehittäjän tulee informoida asiakkaitaan tuotteesta löydetyistä haavoittuvuuksista.[296]

[290] Voutilainen 2019, s. 126.
[291] Voutilainen 2019, s. 127.
[292] Voutilainen 2007, s. 117–118.
[293] Voutilainen 2019, s. 202.
[294] Korhonen 25.3.2015, s. 51.
[295] Neuvonen 2019, s. 227.
[296] Råman 2006, s. 316–318, 448.

4.4 Tietoturva ja kyberrikollisuuden torjunta

Teknologinen kehitys on luonut rikollisuudelle uusia ilmenemismuotoja. Viime vuosikymmenten rikollisuuden kehityslinjat voidaan jaotella tietoverkkosidonnaiseen tietoverkkorikollisuuden syntymiseen ja perinteisen rikollisuuden linkittymiseen kaikkialle ulottuviin tietoverkkoihin koko yhteiskunnan verkottumisen seurauksena.[297] Erityisesti kaksi viimeistä kulunutta vuosikymmentä ovat mahdollistaneet ja edistäneet uusia, aiemmasta rikollisuudesta poikkeavia muotoja.[298]

Termeinä kyberrikollisuutta, tietoverkkorikollisuutta ja verkkorikollisuutta voidaan pitää jotakuinkin toistensa synonyymeinä.[299] Termi *cybercrime* ja sen vastineet korostavat rikollisuusilmiön kytkeytymistä toisiinsa verkottuneisiin päätelaitteisiin ja niiden muodostamaan kyberavaruuteen yksittäisten, erillisten tietokoneiden sijaan.[300] *Cybercrime*-termin ohella englanninkielisessä kirjallisuudessa käytetään myös ainakin termejä *e-crime*, *computer crime*, *hi-tech crime* ja *digital crime*, jotka enemmän tai vähemmän tarkoittavat samaa asiaa kuin *cybercrime*.[301]

Kyberrikollisuus on samanlaista rikollisuutta kuin kybermaailman ulkopuolellakin toimiva rikollisuus – motiivit rikoksentekemiselle ovat pääpiirteittäin samoja, usein motiivina on raha[302]. Monet tietoturvallisuutta koskevat uhat eivät ole uusia, vaan uusi toimintaympäristö vain painottaa uudella tavalla joitakin uhkatyypin erityispiirteitä.[303] Tietotekniikkarikoksen olennaisena piirteenä voidaan pitää sitä, että tietotekniikkaan kuuluva hyödyke muodostaa joko rikoksen modernin tekovälineen tai rikoksen kohteen.[304] Tietojärjestelmässä itsessään voi olla joko sinällään jotain arvokasta, tai järjestämää voidaan käyttää välineenä johonkin muuhun.

Tietoverkot muodostavat rikollisuudelle kuitenkin uudenlaisen toimintaympäristön ja infrastruktuurin. Rikollisuus saa sellaisia uusia muotoja, jotka eivät olisi mahdollisia fyysi-

[297] Riekkinen 2019, s. 3. Kursiivi poistettu.
[298] Riekkinen 2019, s. 159.
[299] Riekkinen 2019, s. 161.
[300] Riekkinen 2019, s. 161.
[301] Gillespie 2016, s. 1.
[302] Niemi – Yle, 27.12.2019.
[303] Saarenpää et al. 1997, s. XXXIV.
[304] Lehtonen 2015, s. 72.

sessä maailmassa. Tietoverkkoympäristössä niin uhrien kuin rikoskumppaneiden tavoittaminen on helpompaa, ja tietoverkot mahdollistavat eri identiteettien käyttämisen, mikä vaikeuttaa kiinnijäämistä.[305] Oleellisia piirteitä ovat myös vapaus maantieteellisistä rajoitteista ja rikollisten vaikeampi edesvastuuseen saattaminen, erilaiset tekovälineet perinteiseen rikollisuuteen verrattuna sekä etäisyys uhrista – uhria ei välttämättä tarvitse kohdata laisinkaan, tai rikollisella ei välttämättä ole edes tiedossaan uhrien henkilöllisyyttä tai lukumäärää.

Oman haasteensa rikosoikeudelliselle tarkastelulle asettaa rikoslain alueellinen ulottuvuus. Olisi täysin mahdollista, että myös julkishallinnossa toteutettaviin bug bounty -ohjelmiin osallistuisi ulkomailla asuvia henkilöitä[306]. Suomen lainkäytön piiri ei ulotu kuin eräissä tapauksissa valtion rajojen ulkopuolelle – kyberympäristöä valtiolliset rajat eivät sen sijaan juurikaan kiinnosta. Mahdollisissa kansainvälisliitännäisissä ongelmatapauksissa tulisi ensin valita oikeudenkäynnin forum. Internetin tapauksessa noudatetaan yleisesti ottaen kansallisia lakeja. Internet kuitenkin koostuu toisiinsa yhteydessä olevista palvelimista, ja nämä palvelimet ovat fyysisiä laitteita, jotka sijaitsevat jossakin valtiossa. Entisestään vaikeusastetta lisäävät pilvipalvelut, joissa data on voitu jakaa useille eri palvelimille, jotka sijaitsevat eri valtioissa.[307]

Jos teon seurauksena voidaan katsoa tapahtuneen rikoksia useammassa valtiossa, on todennäköistä, että oikeusprosessi tapahtuisi siinä valtiossa, jossa syytettykin sijaitsee, sillä huomioon tulee ottaa myös tuomion täytäntöönpanoon liittyvät seikat.[308] Tämän tutkimuksen puitteissa ei kuitenkaan ole mahdollista perehtyä syvällisemmin lain- tai foruminvalintakysymyksiin kansainvälisoikeudellisesta näkökulmasta.[309]

Rajankäynti sen välillä, milloin rikollisuus voidaan luokitella kyberrikollisuudeksi ja milloin perinteiseksi rikollisuudeksi, ei ole aina helppoa. Onko rikollisuus kyberrikollisuutta aina, kun rikoksen tekemiseen liittyy jokin tietotekninen laite tai väline? Onko pankki-

[305] Riekkinen 2019, s. 43; ks. myös Gillespie 2016, s. VII.
[306] Tällä hetkellä useampaan kansallisen julkishallinnon tietojärjestelmään kohdistuvaan bug bounty -ohjelmaan kuitenkin kuuluu joko säännöissä oleva este tai sellainen käytännön vaatimus, kuten verokortti tai suomalainen pankkitili, jotka rajoittavat palkkion maksua ja täten myös ohjelmaan osallistumista. Ks. Hackrfi Oy:n nettisivut.
[307] Gillespie 2016, s. 24–27.
[308] Gillespie 2016, s. 29–29.
[309] Aiheesta lisää, ks. esim. Gillespie 2016, s. 28 ss.

kortin varastaminen ja sillä automaatista rahan nostaminen kyberrikollisuutta? Kun yrityksen kirjanpito on sähköisessä muodossa, onko kirjanpitorikoksen tekeminen kyberrikollisuutta? Siitä voidaan olla yksimielisiä, että kun sähköpostiviesteillä kalastellaan salasanoja, kyseessä on kyberrikollisuus, mutta onko sosiaalisessa mediassa kunnianloukkaukseen syyllistyminen kyberrikollisuutta? Kun entistä useampi yhteiskunnan palvelu on sähköisessä muodossa, onko mielekästä ylipäätään erottaa perinteinen rikollisuus ja kyberrikollisuus toisistaan?

Tietoverkkorikokset jaetaan tietoverkkoympäristöön kohdistuviin rikoksiin (esim. *computer-focused*) sekä tietoverkkoja hyödyntäen tehtyihin rikoksiin (esim. *computer-related*), jotka voivat olla mitä tahansa rikollisuutta, jossa käytetään tietoverkkoja hyväksi – esimerkiksi nettipetokset.[310] Toisenlaisen jaottelun mukaan tietoturvallisuusrikokset voidaan rikostyyppeinä jakaa kolmeen kategoriaan: tietoturvallisuusvelvoitteiden laiminlyönteihin, tieto- ja viestintäjärjestelmiin tai itse tietoon kohdistuviin rikoksiin, sekä rikoksiin, joiden tunnusmerkistöön kuuluu informaation oikeudeton julkistaminen tai levittäminen.[311]

Kolmannen jaottelun mukaan tietoverkkorikokset voidaan jakaa tietokoneavusteisiin tai tietokoneisiin liittyviin rikoksiin, tietokoneilla ja tietoverkossa käsiteltävään sisältöön liittyviin rikoksiin sekä teknisiin laitteisiin, tietojärjestelmiin, tietoverkkoihin ja erityisesti niiden luottamukseen, käytettävyyteen ja eheyteen liittyviin rikoksiin.[312] Tämän jaottelun kolmas kategoria kuuluu tietoverkkorikosten ydinalueeseen. Näiden rikosten rangaistavuus perustuu yleensä nimenomaisiin tietoverkkosidonnaisiin kriminalisointeihin, joiden suojelukohteena ovat tietojärjestelmien luottamuksellisuus, eheys ja käytettävyys.[313]

Rikostyyppeihin jaottelua voidaan tehdä myös muunlaisesta näkökulmasta. Rikosoikeudellisesta näkökulmasta kyberrikokset voidaan jakaa kahteen kategoriaan: kyberriippuvaisiin rikoksiin (*cyber-dependent crime*), joita ei voi tehdä ilman kyberympäristöä, ja rikoksiin, joiden tekemiseen hyödynnetään kyberympäristöä (*cyber-enabled crime*).[314] Bug bounty -ohjelmien tarkastelun voidaan katsoa kuuluvan kyberriippuvaisiin rikoksiin,

[310] Englanninkieliset termit Gillespie 2016, s. 4.
[311] Saarenpää et al. 1997, s. LIX.
[312] Riekkinen 2019, s. 162–164.
[313] Riekkinen 2019, s. 162–164.
[314] Nevalainen 2019, s. 131, 133. Nevalaisen mukaan terminologia tai luokittelu ei ole vakiintunutta, vaan pikemminkin käyttäjäriippuvaista.

sillä kyberympäristö on se paikka, jossa nämä ohjelmat toteutuvat. Rikokset, joissa hyödynnetään kyberympäristöä, sen sijaan ovat mahdollisia seurauksia siitä, mitä oikeudettomalla tietojärjestelmään tunkeutumisella voidaan saada aikaan, eivätkä täten liity yhtä kiinteästi bug bounty -ohjelmien toteuttamiseen.

Kyberrikollisuuden torjunnan kustannustehokkuuden näkökulmasta ennakollinen tietoturvaan panostaminen on erityisen hyödyllistä. Esimerkiksi kunnalliseen sektoriin kohdistui vuonna 2019 useita tietomurtoja ja haittaohjelmaiskuja – pelkästään Lahden kaupunkiin kohdistunut haittaohjelmahyökkäys aiheutti lähes miljoonan euron kulut, vaikka hyökkäykseen kyettiinkin reagoimaan nopeasti.[315]

[315] Ks. esim. Niemi – Yle, 27.12.2019.

5 Bug bounty -ohjelmat rikoslain näkökulmasta

Tässä luvussa käsitellään bug bounty -ohjelmissa tapahtuvaa toimintaa rikoslain näkökulmasta. Luvussa selvitetään, voiko jokin rikoslain kriminalisointi täyttyä ohjelman järjestämisen tai siihen osallistumisen yhteydessä. Tätä ennen perehdytään rikosoikeuden yleisiin oppeihin tahallisuuteen, syyteoikeuteen ja loukatun suostumukseen liittyen.

Rikoslaissa (39/1889) tieto- ja viestintärikoksista säädetään lain 38 luvussa. Luvun kriminalisoinneilla suojellaan tietoturvallisuutta oikeushyvänä[316]. Luvun säännöksiä tieto- ja viestintärikoksista on uudistettu kattavasti rikoslain kokonaisuudistuksen yhteydessä vuonna 1995 (muutossäädös 578/1995), ja lukuun on tämänkin jälkeen tehty useita muutoksia. Rikoslain nykyinen tieto- ja viestintärikoksia koskeva sääntely pohjautuu uusimmilta osiltaan pitkälti Euroopan neuvoston tietoverkkorikollisuutta koskevaan yleissopimukseen (SopS 59–60/2007) ja sen lisäpöytäkirjaan (189, SopS 83–84/2011), sekä Euroopan unionin tietojärjestelmiin kohdistuvista hyökkäyksistä annettuun puitepäätökseen (2005/222/YOS, EUVL L 69/67, 16.3.2005) ja Euroopan parlamentin ja neuvoston direktiiviin tietojärjestelmiin kohdistuvista hyökkäyksistä (2013/40/EU).[317]

Rikoslain luku 38 ei ole kuitenkaan ainoa paikka, jossa säädetään tieto- ja viestintärikosliitännäisistä rikoksista ja niiden sanktioinnista, vaan esimerkiksi myös yleisvaarallisia rikoksia koskevassa rikoslain 34 luvun 9 a §:ssä säädetään vaaran aiheuttamisesta tietojenkäsittelylle (muutossäädös 368/2015) ja 9 b §:ssä tietoverkkorikosvälineen hallussapidosta (muutossäädös 540/2007). Samoin viranomaisen toiminnan julkisuudesta annetun lain (621/1999) 35 §:ssä säädetään samaan kategoriaan kuuluvista asioista.[318] Lisäksi esimerkiksi tilanteessa, jossa saatetaan toisen henkilön omistama tietokone louhimaan virtuaalivaluuttaa, on kyse luvattomasta käytöstä (RL 28:7). Tämän ohella voitaisiin tulkita, että esimerkiksi Verohallinnon valtakunnalliset tietojärjestelmät olisivat RL 34 luvun 1 pykälän 2 momentin mukaisia tietojärjestelmiä, joihin voisi kohdistua teko, joka tuomittaisiin tuhotyönä[319].

[316] Korhonen 25.3.2015, s. 56 ja 87.
[317] Ks. esim. Rautio 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 26. RL 38: Tieto- ja viestintärikokset, Yleistä, Rangaistavuuden laajeneminen; Nevalainen 2019, s. 137.
[318] Ks. myös HE 94/1993 vp, s. 134 ss.
[319] Lehtonen 2015, s. 124–125. Samaan kategoriaan Lehtonen arvioi kuuluvan myös Kelan, ulosoton, poliisin ja pankkitoiminnan tietojärjestelmät.

Tietojärjestelmien turvallisuuden kannalta on tärkeää, että jo järjestelmään tunkeutuminen on rangaistavaa riippumatta siitä, voidaanko näyttää toteen vaikkapa luvattoman käytön, viestintäsalaisuuden loukkauksen tai yritysvakoilun yritystä. Sellainenkin hakkeri, joka ei käytä järjestelmää, voi järjestelmään päästessään aiheuttaa sille vahinkoja. Tästä syystä hakkerointia itsessään on pidetty vaarallisena toimintana.[320] Lainvalmisteluaineistossa hakkerointi on määritelty toiminnaksi, jossa tietojärjestelmää suojaavia tietoja kuten käyttäjätunnuksia selvitetään luvattomasti tai järjestelmään murtaudutaan näitä luvattomia tietoja hyväksi käyttäen[321]. Hakkerointi määritellään tässä tutkimuksessa kuitenkin siten kuin tietoturvayhteisö sen määrittelee, ei samalla tavalla kuin mainitussa hallituksen esityksessä.

Rikoslain luvussa 38 käytetyt tietojärjestelmän ja datan käsitteet on määritelty luvun 13 §:ssä (368/2015). Pykälän 1 momentissa viitataan tietojärjestelmän osalta tietoverkkorikosdirektiivin[322] 2 artiklan a kohtaan. Tietojärjestelmällä tarkoitetaan lainkohdan mukaan myös laitetta tai toisiinsa kytkettyjä tai liitettyjä laitteita, joista yksi tai useampi on ohjelmoitu automaattista tietojenkäsittelyä varten, sekä dataa, jota kyseisessä laitteessa tai toisiinsa kytketyissä tai liitetyissä laitteissa varastoidaan, käsitellään, haetaan tai välitetään sen tai niiden toimintaa, käyttöä, suojausta tai huoltoa varten.

Datan osalta pykälän 2 momentissa viitataan tietoverkkorikosdirektiivin 2 artiklan b kohtaan. Datalla tarkoitetaan lainkohdan mukaan myös sellaisessa muodossa olevien tosiseikkojen, tietojen tai käsitteiden esitystä, että se soveltuu käsiteltäväksi tietojärjestelmässä, sekä ohjelmaa, jonka avulla tietojärjestelmä pystyy suorittamaan jonkin toiminnon.

Rikoslain tieto- ja viestintärikoksia sekä muita tietoturvallisuuteen liittyviä rikoksia koskevan sääntelyn voidaan katsoa olevan tarpeettoman hienojakoista, mikä liittyy yleisemminkin kansainvälisiin sopimuksiin tai muihin kansainvälisiin velvoitteisiin perustuviin kriminalisointeihin. Sääntely sisältää esimerkiksi toissijaisuuslausekkeita,[323] ja toisaalta rikoslain säännökset kyberrikoksiin liittyen ovat tunnusmerkistöiltään osin päällekkäisiä,

[320] HE 94/1993 vp, s. 140.
[321] HE 94/1993 vp, s. 140.
[322] Tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta annettu Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU.
[323] Viljanen 2018, s. 559.

mikä voi johtaa tulkinnanvaraisuuteen ja sen myötä vaarantaa oikeusvarmuutta. Näiden eri ajankohtina ja eri tilanteita varten laadittujen säännösten tulkintaa ei voida korjata pelkästään lainopin tai oikeuskäytännön keinoin.[324]

> Tieto- ja viestintärikoksiin liittyvän sääntelyn erityispiirteenä voidaan nostaa vielä esiin seuraava havainto: Rikoslain muutossäädöksen 368/2015 hallituksen esityksessä on käytetty tietomurtoa koskevan pykälän yksityiskohtaisissa perusteluissa eräitä tietoteknisiä termejä – kuten SQL-injektio ja XSS (*cross-site scripting*) – antamaan esimerkkejä siitä, millainen toiminta saattaa täyttää tietomurron tai vaikkapa datavahingonteon tai petoksen tunnusmerkistön.[325] Tietotekniikan alan erikoissanaston käyttö vie lukijan alueelle, jossa tavallinen toimisto-ohjelmien käyttäjä ei enää täysin ymmärrä tekstin sisältöä. Termien käyttäminen on konkreettinen esimerkki siitä, että tieto- ja viestintärikosten kohdalla tarvitaan erityistä asiantuntijuutta jo pelkästään ymmärtämään, millaiset teot voivat olla rikoksia ja millaiset eivät[326]. Tämä asettaa vaatimuksia sekä esitutkintaviranomaisten, syyttäjien, asianajajien, oikeudenkäyntiavustajien että tuomarien osaamiselle, puhumattakaan lainsäätäjistä.

5.1 Tahallisuus

Rikosvastuun edellytyksenä on, että rikos on tehty tahallisesti. Rikoksesta voidaan rangaista tuottamuksellisena vain, mikäli siitä on erikseen säädetty. Rikoslain kontekstissa tuottamuksella tarkoitetaan laiminlyöntiä, huolimattomuutta, piittaamattomuutta säännöksistä tai muuta kuin tarkoituksellista rikollista toimintaa. Tahallisuus on määritelty rikoslain yleisessä osassa RL 3:6:ssä, ja tahallisuuden tulee kattaa kaikki rikoksen ainesosat, jotka sisältyvät rikostunnusmerkistöön. Tahallisuudessa tekijän on tullut tarkoittaa tietyn seurauksen toteutumista tai tietää tietyn seurauksen olevan todennäköinen tulos toiminnastaan, tai vaihtoehtoisesti tietää tietyistä olosuhteista, että teko on rikos. Todennäköisyyden aste on noin viisikymmentä, eli seurauksen on pitänyt todennäköisemmin tapahtua kuin olla tapahtumatta.[327]

---

[324] Nevalainen 2019, s. 148.
[325] HE 232/2014 vp, s. 35.
[326] Ks. myös Riekkinen 2019, s. 190 ja Lehtonen 2015, s. 6.
[327] Neuvonen 2019, s. 265–266.

Legaliteettiperiaatteen mukaisesti rangaistavaa on vain se, mitä on rangaistavaksi säädetty.[328] Rikoslain tulkinnassa on erityisesti kiellettyä analogioiden tekeminen. Jotta rikoksesta voitaisiin tuomita, tulee sekä tarkoitustunnusmerkkien että tekotapatunnusmerkkien täyttyä, samoin kuin syy-yhteyden (seuraustunnusmerkit). Tarkoitustunnusmerkeillä tarkoitetaan sitä, että tekijän tarkoituksena on saada aikaan tunnusmerkistökuvauksessa mainittu seuraus: tekijä toimii toisin sanoen tietyssä tarkoituksessa tavoitellen tiettyä päämäärää.[329] Tekotapatunnusmerkillä tarkoitetaan pykälässä kuvattua tekoa. Syy-yhteyden arviointi liittyy nimenomaisesti sellaisiin rikoksiin, joissa tunnusmerkistön täyttyminen edellyttää seurauksen aiheuttamista[330].

5.2 Asianomistajarikos ja syyteoikeus

Rikokset ovat virallisen syytteen alaisia, jollei toisin ole säädetty. Rikoksen asianomistajalla on kuitenkin virallisen syytteen alaisissa rikoksissakin toissijainen oikeus nostaa syyte itse, jos virallinen syyttäjä on päättänyt jättää syytteen nostamatta. Asianomistajarikoksiksi kutsutaan rikosta, josta virallinen syyttäjä ei saa nostaa syytettä, ellei asianomistaja ole esittänyt syyttämispyyntöä. Asianomistajarikokset ovat usein vähäisiä rikoksia, joiden syytteeseenpanoon ei ole katsottu olevan yleistä intressiä, ellei asianomistaja itse ole aloitteellinen asiassa. Tällaisia rikoksia ovat esimerkiksi kunnianloukkausrikokset.[331] Virallisen syytteen alaisista rikoksista syyttäjän on syytekynnyksen ylittyessä nostettava syyte, vaikka asianomistaja ei olisikaan ilmoittanut rikosta syytteeseen pantavaksi. Asianomistajarikoksista syyttäjä saa nostaa syytteen ainoastaan, jos asianomistaja on ilmoittanut rikoksen syytteeseen pantavaksi. Asianomistajarikoksessa asianomistajan ilmoitus on muodollinen edellytys (prosessinedellytys) syytteen tutkimiselle tuomioistuimessa.[332]

Vaikka rikos olisikin asianomistajarikos, voi syyttäjä tietyissä tapauksissa nostaa syytteen ilman asianomistajan myötävaikutusta. Esimerkiksi rikoslain tieto- ja viestintärikoksia

[328] Korhonen 25.3.2015, s. 93.
[329] Tapani et al. 2019, s. 265–266.
[330] Tapani et al. 2019, s. 231.
[331] Koskinen 2004, päivitetty 1.11.2008, ei sivunumerointia. I Yleisiä kysymyksiä, 7. Rikosoikeuden yleiset opit ja rikosvastuun perusteet, Syytevallan järjestely ja asianomistajan asema, Syytevallan järjestely.
[332] Jokela 2018, s.263.

koskevan 38 luvun kohdalla tällaisia syitä ovat, että rikoksentekijä rikoksen tehdessään on ollut yleistä posti- tai teletoimintaa harjoittavan laitoksen palveluksessa tai että erittäin tärkeä yleinen etu vaatii syytteen nostamista (RL 38:10.1–2). Erittäin tärkeän yleisen edun on katsottu vaativan syytteen nostamista esimerkiksi viestintäsalaisuuden loukkauksesta tai tietomurrosta silloin, kun on kysymys yleistä järjestystä tai tietoliikenteen toimivuutta yleisesti vaarantavasta menettelystä[333].

Rikoslain 38 luvun kriminalisoinneista valtaosa on asianomistajarikoksia[334]. Esimerkiksi viestintäsalaisuuden loukkaus, törkeä viestintäsalaisuuden loukkaus, tietojärjestelmän häirintä[335] ja tietomurto (RL 38:3, 38:4, 38.7 a sekä 38:8) ovat määrätyissä tapauksissa asianomistajarikoksia. Törkeä tietojärjestelmän häirintä ja törkeä tietomurto (RL 38:7 b ja 38.8 a) ovat kuitenkin virallisen syyteen alaisia. Tietoliikenteen häirintä (RL 38:5–7) on tässä suhteessa asetettu eri asemaan, sillä se on aina virallisen syytteen alainen[336].

Kuten törkeä vahingonteko, törkeä datavahingontekokin on aina virallisen syytteen alainen. Datavahingonteko ja lievä datavahingonteko ovat sitä vastoin asianomistajarikoksia, mutta eivät aina. Lievä datavahingontekokin on virallisen syytteen alainen, jos teon kohteena on muu kuin yksityinen omaisuus, kuten valtion, kunnan tai muun julkisyhteisön omaisuus[337].[338]

[333] HE 94/1993 vp, s. 158.
[334] HE 94/1993 vp, s. 146.
[335] Tietojärjestelmän häirintä on lisätty tähän joukkoon muutossäädöksellä 540/2007. Ks. myös HE 153/2006 vp, s. 67.
[336] HE 93/1993 vp, s. 158. Tietoliikenteen häirintä koskee ensisijaisesti julkista etua, mistä syystä sitä on ehdotettu virallisen syytteen alaiseksi.
[337] HE 66/1988 vp, s. 127.
[338] Aiemman lain aikana annettu prejudikaatti KKO 1989:42 vastaa myös nykyisen lain kantaa. Mainitussa tapauksessa A oli rikkonut evankelis-luterilaisen kirkon seurakuntien omistaman huoltorakennuksen ikkunan mennäkseen rakennukseen nukkumaan. KKO totesi, että koska seurakunnat ovat julkisyhteisöjä, niiden omaisuuteen kohdistuneella vahingonteolla ei ollut loukattu ainoastaan silloisessa RL 35:4:ssä tarkoitettua yksityisen oikeutta, joten virallinen syyttäjä sai nostaa silloisessa RL 35:3.1:ssa tarkoitetusta vahingonteosta syytteen, vaikka asianomistaja ei ollut ilmoittanut sitä syytteeseen pantavaksi. Täten myös julkisyhteisöön kohdistuneesta datavahingonteosta voidaan nostaa syyte, vaikka asianomistaja ei olisi aktiivinen. Ks. myös Viljanen 2018, s. 561.

5.3 Oikeudenvastaisuus ja loukatun suostumus

Teko on oikeudenvastainen kun se täyttää jonkun rikoksen tunnusmerkistön. Lisäksi tekijän tulee menetellä teon suhteen tahallisesti tai tuottamuksellisesti.[339] Oikeudenvastaisuus ei sovellu menettelyyn, jolle on riittävän selkeä lakiin perustuva oikeus[340]. Loukatun suostumus on oikeuttamiskeino, joka poistaa teon oikeudenvastaisuuden. Jotta loukatun suostumusta voitaisiin pitää teon oikeudenvastaisuuden poistavana tekijänä, tulee suostumuksen olla vapaaehtoisesti etukäteen annettu. Teon täytyy myös olennaisissa kohdin vastata sitä, mihin kohde on käsittänyt antavansa suostumuksensa. Kaikkiin rikoksiin ei voi pätevästi antaa suostumustaan – tällaisia ovat esimerkiksi törkeimmät pahoinpitelyt.[341] Tätä voidaan perustella sillä, että katumusriski on liian suuri ja teon seuraus liian lopullinen[342]. Myöskään esimerkiksi kiskonnan kohdalla loukatun suostumuksella ei ole merkitystä[343].

Loukatun suostumuksen ohella oikeudenvastaisuuden voi poistaa myös jokin rikoslain 4 luvun vastuuvapausperusteista (kuten hätävarjelu RL 4:4, pakkotila RL 4:5 tai teoriassa jopa kieltoerehdys RL 4:2), joskin näitä lainkohtia voitaneen soveltaa sangen harvoin tietotekniikkaan liittyvissä yhteyksissä.[344]

Loukatun suostumus tulee arvioitavaksi, jos jollekulle aiheutetaan vahinkoseuraus suostumukseen perustuen.[345] Suostumuksen voi antaa se, johon teko kohdistuu. Perusoikeuksien suojaan liittyvissä tapauksissa tulee loukatun suostumuksen arvioinnissa olla kuitenkin pidättyväinen[346]. Rikoslain 38 luvussa määritellyistä tieto- ja viestintärikoksista teon

---

[339] Tapani et al. 2019, s. 393.
[340] Rautio 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 26. RL 38: Tieto- ja viestintärikokset, Konkurrenssi.
[341] Koskinen 2004, päivitetty 1.11.2008, ei sivunumerointia. I Yleisiä kysymyksiä, 7. Rikosoikeuden yleiset opit ja rikosvastuun perusteet, Rikoksen rakenne (yleinen tunnusmerkistö), Oikeudenvastaisuus, Oikeuttamisperusteet, Muita oikeuttamisperusteita, Suostumus.
[342] Nuutila & Ojala 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 10. RL 21: Henkeen ja terveyteen kohdistuvat rikokset, Kuoleman- ja vammantuottamusrikokset, Kuolemantuottamus (RL 21:8), Teon huolimattomuus, Yhteinen riskinotto.
[343] Hakamies 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 24. RL 36: Petos ja muu epärehellisyys, Kiskontarikokset, Kiskonta (RL36:6), Sääntelyn taustaa.
[344] Hätävarjelusta, pakkotilasta ja kieltoerehdyksestä tarkemmin ks. esim. Tapani et al. 2019, s. 389–448.
[345] Nuutila & Ojala 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 10. RL 21: Henkeen ja terveyteen kohdistuvat rikokset, Kuoleman- ja vammantuottamusrikokset, Kuolemantuottamus (RL 21:8), Teon huolimattomuus, Yhteinen riskinotto.
[346] Rautio 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 26. RL 38: Tieto- ja viestintärikokset, Konkurrenssi.

oikeudenvastaisuus voidaan poistaa loukatun suostumuksella esimerkiksi viestintäsalaisuuden loukkauksen ja tietojärjestelmän häirinnän kohdalla.[347]

5.4 Tietoturvaan liittyvien rikosten tunnusmerkistöt

Seuraavassa käsitellään rikoslain tunnusmerkistöjä, jotka ovat oleellisia bug bounty -ohjelman kannalta. Tarkastelu toteutetaan pääasiassa suhteessa Verohallinnon Tulorekisteriä koskevaan bug bounty -ohjelmaan, ja tarkastelussa on otettu huomioon myös tämän ohjelman säännöt[348]. Tarkoituksena on selvittää, voiko ohjelmaan osallistuva henkilö syyllistyä johonkin rikokseen. Vastaus löytyy tarkastelemalla kutakin tunnusmerkistöä ja peilaamalla sitä ohjelman sääntöjen ohella tahallisuuteen, syyteoikeuteen ja loukatun suostumukseen.

5.4.1 Vaaran aiheuttaminen tietojenkäsittelylle

Vaaran aiheuttamisesta tietojenkäsittelylle säädetään rikoslain 34 luvun 9 a pykälässä seuraavasti:

> Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle
>
> 1) tuo maahan, hankkii käyttöön, valmistaa, myy tai muuten levittää taikka asettaa saataville
>
> a) sellaisen laitteen tai tietokoneohjelman taikka ohjelmakäskyjen sarjan, joka on suunniteltu tai muunnettu vaarantamaan tai vahingoittamaan tietojenkäsittelyä tai tieto- tai viestintäjärjestelmän toimintaa taikka murtamaan tai purkamaan sähköisen viestinnän teknisen suojauksen tai tietojärjestelmän suojauksen, taikka
>
> b) tietojärjestelmän toiselle kuuluvan salasanan, pääsykoodin tai muun vastaavan tiedon taikka
>
> 2) levittää tai asettaa saataville ohjeen 1 kohdassa tarkoitetun tietokoneohjelman tai ohjelmakäskyjen sarjan valmistamiseksi,

[347] Ks. Rautio 2004, päivitetty 1.11.2008, ei sivunumerointia. II Rikoslajit, 26. RL 38: Tieto- ja viestintärikokset, Viestintärikokset.
[348] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

> on tuomittava, jollei teosta muualla laissa säädetä ankarampaa tai yhtä ankaraa rangaistusta, vaaran aiheuttamisesta tietojenkäsittelylle sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Tunnusmerkistön täyttymisen edellytyksenä on tekijän aikomus aiheuttaa haittaa tai vahinkoa tietojenkäsittelylle, tieto- tai viestintäjärjestelmän toiminnalle tai näiden turvallisuudelle. Bug bounty -ohjelmien perimmäisenä tarkoituksena on parantaa tietoturvaa, ja Tulorekisteriä koskevan ohjelman säännöissä on myös kielletty verotuksen toimintaa haittaavat tai suurella todennäköisyydellä haittaavat toimet. On siis lähtökohtaisesti oletettava, että sääntöjen puitteissa bug bounty -ohjelmaan osallistuvalla henkilöllä ei ole aikeenaan haitata tai vahingoittaa tietojenkäsittelyä, ja mikäli näin tapahtuisi, tulisi kyseeseen ohjelman sääntörikkomus. Näin ollen bug bounty -ohjelmaan ohjelman sääntöjen puitteissa osallistuva henkilö ei voi syyllistyä RL 34:9 a:n mukaiseen vaaran aiheuttamiseen tietojenkäsittelylle.

5.4.2 Tietoverkkorikosvälineen hallussapito

Tietoverkkorikosvälineen hallussapito on kriminalisoitu RL 34:9 b:ssä, jossa kriminalisointi koskee RL 34:9 a:n 1 momentin 1 kohdan a ja b alakohdissa tarkoitettuja tilanteita.

Tietoverkkorikosvälineen hallussapidosta säädetään rikoslain 34:9 b:ssä seuraavasti:

> Joka aiheuttaakseen haittaa tai vahinkoa tietojenkäsittelylle taikka tieto- tai viestintäjärjestelmän toiminnalle tai turvallisuudelle pitää hallussaan 9 a §:n 1 kohdan a alakohdassa tarkoitettua laitetta, tietokoneohjelmaa tai ohjelmakäskyjen sarjaa taikka b alakohdassa tarkoitettua salasanaa, pääsykoodia tai muuta vastaavaa tietoa, on tuomittava tietoverkkorikosvälineen hallussapidosta sakkoon tai vankeuteen enintään kuudeksi kuukaudeksi.

Tunnusmerkistön täyttymisen edellytyksenä on jälleen tekijän aikomus aiheuttaa haittaa tai vahinkoa tietojenkäsittelylle, tieto- tai viestintäjärjestelmän toiminnalle tai näiden turvallisuudelle. Piittaamatta siitä, mitä laitteita ja välineitä RL 38 luvun 9 a pykälässä on lueteltu, ja vaikka näitä välineitä usein käytetäänkin bug bounty -ohjemaan osallistuessa, rikollista sellaisen välineen käyttämisestä tulee vasta siinä vaiheessa, kun kriteeri haitan tai vahingon aiheuttamisen tarkoituksesta täyttyy. Niin kauan, kun bug bounty -ohjelmaan osallistuvan henkilön tarkoituksena on toteuttaa ohjelman sääntöjä ja pyrkiä parantamaan

ohjelman kohteen tietoturvaa haavoittuvuuksia paikallistamalla, ei tämä voi syyllistyä RL 34:9 b:n mukaiseen tietoverkkorikosvälineen hallussapitoon.

5.4.3 Datavahingonteko

Datavahingonteon perusmuotoisesta kvalifioinnista säädetään RL 35:3 a:ssä, törkeästä 35:3 b:ssä ja lievästä 35:3 c:ssä. Datavahingon perusmuotoisen kvalifioinnin tunnusmerkistö kuuluu seuraavasti:

> Joka toista vahingoittaakseen oikeudettomasti hävittää, turmelee, kätkee, vahingoittaa, muuttaa, saattaa käyttökelvottomaksi tai salaa tietovälineelle tallennetun tiedon tai muun tallennuksen taikka tietojärjestelmässä olevan datan, on tuomittava datavahingonteosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Tunnusmerkistön täyttymisen edellytyksenä on tekijän vahingoittamistarkoitus, ja tämän ohella teko on tehtävä oikeudettomasti. Tulorekisteriä koskevan ohjelman säännöissä on erikseen kielletty esimerkiksi koodi-injektiot taustajärjestelmiin siten, että järjestelmässä tai taustajärjestelmässä olevia tietoja muutetaan tai poistetaan, joten oikeutusta datavahingontekoon ei ole annettu. Sen sijaan bug bounty -ohjelmaan osallistuvalla henkilöllä ei lähtökohtaisesti ole vahingoittamistarkoitusta. Näin ollen sääntöjen puitteissa ohjelmaan osallistuva henkilö ei voi syyllistyä datavahingontekoon.

On toki mahdollista, että ohjelmaan osallistuva henkilö ilman vahingoittamistarkoitusta tulee esimerkiksi hävittäneeksi tai muuttaneeksi tietojärjestelmässä olevaa dataa. Tuolloin tilaaja voi käyttää oikeussuojakeinoja tekijää kohtaan ja teon vahingoittamistarkoituksen ja tahallisuuden arviointi jää esitutkintaviranomaisten, syyttäjän ja tuomioistuimen harkittavaksi.

5.4.4 Viestintäsalaisuuden loukkaus

Viestintäsalaisuuden loukkauksen perusmuotoisesta kvalifioinnista säädetään RL 38:3:ssä ja törkeästä 38:4:ssä. Viestintäsalaisuuden loukkauksen perusmuotoisen kvalifioinnin tunnusmerkistö kuuluu seuraavasti:

> Joka oikeudettomasti
>
> 1) avaa toiselle osoitetun kirjeen tai muun suljetun viestin taikka suojauksen murtaen hankkii tiedon sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä taikka
>
> 2) hankkii tiedon televerkossa tai tietojärjestelmässä välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä taikka tällaisen viestin lähettämisestä tai vastaanottamisesta,
>
> on tuomittava viestintäsalaisuuden loukkauksesta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Kriminalisoinnin käsitteessä kirje kattaa minkä tahansa suljetun viestin, aina mainoskirjeestä yksityiskirjeisiin, sekä postipaketteihin, jotka sisältävät jonkinlaisen viestin. Kirjeen tulee olla suunnattu jollekulle henkilölle, eli niin sanottu osoitteellinen viesti – kriminalisointi ei kata osoitteettomia viestejä. Sähköposti, puhelu ja muu televerkossa lähetetty viesti saavat laajan tulkinnan. Niihin liittyy myös havainto siitä, että ei pelkästään viestin sisältö, vaan myös sen metatietojen selvittäminen oikeudettomasti täyttää rikoksen tunnusmerkistön.[349]

Bug bounty -ohjelman puitteissa voi aktualisoitua tilanne, jossa ohjelmaan osallistuva hakkeri päätyy näkemään muun suljetun viestin, tai todentaakseen ja raportoidakseen paikallistamansa haavoittuvuuden murtaa suojauksen pykälän 1 momentin 1 kohdan mukaisesti. Ohjelmien säännöissä ei kuitenkaan lähtökohtaisesti anneta lupaa – oikeutusta – tällaisten viestien lukemiseen. Tulorekisteriä koskevan ohjelman sääntöjen mukaan, mikäli hakkeri löytää sellaisen haavoittuvuuden, jonka vuoksi saadaan näkyville sellaista tietoa, joka ei olisi ilman haavoittuvuutta mahdollista, on raportoijan pidettävä tällä tavoin saamansa tiedot salassa välittämättä tai ilmaisematta niitä kolmansille osapuolille[350].

Viranomaisen tietojärjestelmässä olevat, ulkopuoliselta suojatut viestit voivat joko olla viranomaisen asiakirjoja (esimerkiksi hallinnon asiakkaan viestit viranomaiselle tätä kos-

[349] Neuvonen 2019, s. 240.
[350] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

kevassa asiassa, JulkL 5.2 §), tai sitten eivät (esimerkiksi viranomaisen henkilöstön virkistystoimintaan liittyvä viestinvaihto)[351]. Viestintäsalaisuuden loukkauksen kriminalisoinnin perusteet ovat perustuslain 10.2 §:n sääntelyssä: kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Perustuslaissa turvattu viestinnän suoja suojaa sekä viestin lähettäjää että viestin vastaanottajaa.[352] Tällöin esimerkiksi hallinnon asiakasta, joka on viestinyt tietojärjestelmässä viranomaisen kanssa, voidaan pitää asianomistajana teossa, joka loukkaa hallinnon asiakkaan viestintäsalaisuutta. Jotta teko olisi oikeutettu, hallinnon asiakkaalta tulee siis edellyttää loukatun suostumusta, joka tulee antaa etukäteen. En ole kuitenkaan havainnut, että julkishallinnon bug bounty -ohjelmien yhteydessä tällaista loukatun suostumusta hallinnon asiakkaalta olisi kysytty. Mikäli bug bounty -ohjelman puitteissa täyttyisi viestintäsalaisuuden loukkaamiseen vaadittava teko, hallinnon asiakas ei myöskään mahdollisesti koskaan saisi tietää, että hänen oikeuttaan luottamukselliseen viestintään on loukattu. Sekä viestintäsalaisuuden loukkaus että törkeä viestintäsalaisuuden loukkaus ovat asianomistajarikoksia, joista syyttäjä voi nostaa syytteen vain, jos erittäin tärkeä yleinen etu sitä vaatii (RL 38:10.2).

Mikäli tietojärjestelmään murtautumisen seurauksena saadaan hankittua tieto jonkin ulkopuoliselta suojatun viestin sisällöstä, tulee sovellettavaksi viestintäsalaisuuden loukkaus, vaikka teko sinänsä täyttäisikin tietomurron tunnusmerkistön. Tietomurtoa pidetään tuolloin valmisteluluontoisena tekona, lisäksi tietomurtoa koskevat säännökset sisältävät toissijaisuuslausekkeen.[353] Tilanne kuitenkin eroaa tietomurrosta vasta siinä vaiheessa, kun järjestelmään tunkeutunut hakkeri näkee järjestelmässä olevaa viestinvaihtoa tai viestinvaihtoon liittyviä metatietoja.

Viestintäsalaisuuden loukkaukseen syyllistyminen edellyttää teolta tahallisuutta. Bug bounty -ohjelmissa on nimenomaisesti tarkoituksena murtautua järjestelmään, joten tästä näkökulmasta tahallisuus täyttyy. Ohjelman tarkoituksena ei kuitenkaan ole, että haavoittuvuuden paikallistamisen yhteydessä hakkeri tarkastelisi järjestelmässä olevia tietoja tai viestintää. Tahallisuutta tulee siis arvioida tapauskohtaisesti. Esitutkintaviranomaisten,

[351] HE 30/1998 vp, s. 57–58.
[352] HE 309/1993 vp, s. 53–54.
[353] HE 232/2014 vp, s. 11–12.

syyttäjän ja tuomioistuimen tehtävänä on arvioida tarkemmin tekijän tarkoitusperiä ja suhteuttaa se teon tahallisuuteen.

Kuitenkin henkilö, joka paikallistaa viestintää tai sen metatietoja paljastavan haavoittuvuuden bug bounty -ohjelmassa, saattaa syyllistyä viestintäsalaisuuden loukkaukseen siitäkin huolimatta, että noudattaa ohjelman sääntöjä.

Viestintäsalaisuuden loukkauksen törkeä tekomuoto täyttyy muun muassa silloin, jos yksityiselämälle aiheutuu merkittävää haittaa. Näin voi tapahtua, jos viestinnän kohteena ovat terveystiedot, merkittävä haitta maineelle tai ihmissuhteiden tuhoutuminen. Toisaalta, tekijän täytyy olla tietoinen siitä, että viesti saattaa sisältää yksityiselämän kannalta arkaluontoisia tietoja, ja rikoksen on oltava kokonaisuutena arvostellen törkeä. Satunnainen päähänpisto, joka sattumalta kattaa törkeän tekomuodon vaikutukset, ei tee teosta törkeää.[354] Näillä perustein bug bounty -ohjelmaan osallistuessa olisi huomattavan epätodennäköistä syyllistyä viestintäsalaisuuden loukkauksen törkeään tekomuotoon, mikäli ohjelman sääntöjä noudatetaan.

> Jos bug bounty -ohjelman kohteena olisi muu kuin julkishallinnon tietojärjestelmä, voisi järjestelmän käyttöehdoissa tai sopimusehdoissa olla erillisenä mainintana, että käyttäjä antaisi luvan viestintäsalaisuuden loukkaamiseen järjestelmään kohdistettavien turvallisuustoimenpiteiden yhteydessä. Tuolloin bug bounty -ohjelmassa toimiva hakkeri, joka päätyisi näkemään käyttäjän viestintää tai sen metatietoja, ei syyllistyisi viestintäsalaisuuden loukkaamiseen.

5.4.5 Tietoliikenteen häirintä

Tietoliikenteen häirinnästä säädetään RL 38:5:ssä, teon törkeästä kvalifioinnista säädetään 38:6:ssä ja lievästä 38:7:ssä. Tietoliikenteen häirinnän perusmuotoisen kvalifioinnin tunnusmerkistö kuuluu seuraavasti:

> Joka puuttumalla postiliikenteessä taikka tele- tai radioviestinnässä käytettävän laitteen toimintaan, lähettämällä ilkivaltaisessa tarkoituksessa radiolaitteella tai televerkossa häiritseviä viestejä tai muulla vastaavalla tavalla oikeudettomasti estää

[354] Neuvonen 2019, s. 240.

> tai häiritsee postiliikennettä taikka tele- tai radioviestintää, on tuomittava tietoliikenteen häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Pykälässä mainitaan televiestintä ja televerkko, joilla tarkoitetaan tietoliikenneverkkoa. Internet on pykälässä tarkoitettu tietoliikenneverkko. Tietoliikenteen häirinnän tunnusmerkistöön kuuluu, että häirintä on toteutettu oikeudettomasti ja että tekijällä on ilkivaltainen tai häiritsevä tarkoitus – siis että toiminta on tahallista.

Bug bounty -ohjelmien säännöissä suljetaan usein palvelunestohyökkäykset (DOS, *denial of service*) ja hajautetut palvelunestohyökkäykset (DDOS *distributed denial of service*) sallittujen toimien ulkopuolelle. Tulorekisteriä koskevan bug bounty -ohjelman sääntöjen periaatteellisiin rajauksiin kuuluu kuitenkin, että testauksessa ei saa käyttää haitallista tai häiriötä aiheuttavaa kuormaa tai syötettä *sen enempää kuin mitä teknisen tietoturvahaavoittuvuuden olemassaolon todentaminen edellyttää*, tai että tietoturvatestaamisen suorittaminen ei saa *merkittävällä tavalla* vaikuttaa ohjelman kohteena olevan palvelun saatavuuteen[355]. Säännöissä siis sallitaan pienimuotoinen tietoliikenteen häirintä. Tämä on myös perusteltua, sillä järjestelmän kuormitusasteella voi olla vaikutusta järjestelmän toimintaan ja turvallisuusliitännäisiin yksityiskohtiin. Tahallisuuden vaatimus siis täyttyy jo osana normaalia testaustoimintaa.

Ohjelman kohdejärjestelmän kapasiteetti tuskin on ohjelmaan osallistuvan hakkerin tiedossa. Tästä syystä hakkeri ei voi ennalta tietää, millaiset toimenpiteet vaikuttavat merkittävästi ohjelman kohteena olevan palvelun saatavuuteen, tai milloin kuormaa on enemmän kuin mitä haavoittuvuuden olemassaolon todentaminen edellyttää. On siis täysin ohjelman tilaajan määriteltävissä, milloin nämä kriteerit ovat ylittyneet. Tuolloin tilaaja voi käyttää oikeussuojakeinoja tekijää kohtaan ja teon häirintätarkoituksen ja tahallisuuden arviointi jää esitutkintaviranomaisten, syyttäjän ja tuomioistuimen harkittavaksi.

Tulorekisteriä koskevan ohjelman sääntöjen mukaan Verohallinto myöntää ohjelmaan osallistuville tietoturvatestaajille oikeuden toteuttaa järjestelmään haavoittuvuustestaustoimia ja -toimenpiteitä, jotka voitaisiin tulkita tietoliikenteen häiritsemisen yritykseksi. Sääntöjen tässä osassa ei siis anneta oikeutusta muuhun kuin tietoliikenteen häirinnän

[355] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

yritykseen, joka ilman tällaista loukatun suostumusta olisi rangaistava teko. Kuitenkin, kuten edellä todettua, säännöistä voidaan tulkita, että myös pienimuotoinen tietoliikenteen häirintä olisi sallittua.

Edelleen ohjelman sääntöjen mukaan Verohallinto sitoutuu olemaan tekemättä ohjelman sääntöjen mukaisesti tehdyistä tietoturvatestaajien haavoittuvuustestaustoimista ja -toimenpiteistä tutkintapyyntöjä rikoslain 38 luvun 5 §, 6 § tai 7 §:n tarkoittamissa tapauksissa ja olemaan vaatimatta niistä rikosoikeudellisia seuraamuksia. Mainitut pykälät koskevat tietoliikenteen häirinnän kaikkia kvalifiointeja. En tulkitsisi sääntöjen kohdan antavan oikeutusta tietoliikenteen häirintään, vaan pelkästään siinä todettavan, että Verohallinto sitoutuu olemaan tekemättä tutkintapyyntöjä. Tietoliikenteen vähäistä suuremman tai merkittävän häirinnän katsoisin olevan sääntöjen vastaista toimintaa, johon ohjelman tilaaja suhtautuisi sääntörikkomuksena.

Tietoliikenteen häirintä on myös aina virallisen syytteen alainen rikos[356], jolloin tekoon syyllistynyttä henkilöä voidaan syyttää tietoliikenteen häirinnästä, liittyi asiaan asianomistajan myötävaikutusta tai ei. Koska ohjelman säännöissä oikeutus tietoliikenteen häirintään on nimenomaisesti annettu vain yritykseen, ja muista sääntöjen kirjauksista voitaisiin päätellä, että lievä tietoliikenteen häirintä olisi myös sallittua, ei perusmuotoiseen tai törkeään tietoliikenteen häirintään ole säännöissä annettu oikeutusta, joten kyseessä olisi kiistatta oikeudenvastainen teko.

5.4.6 Tietojärjestelmän häirintä

Kun tarkastellaan rikoslain tunnusmerkistöjä jonkin tietyn tietojärjestelmän näkökulmasta, voi järjestelmään kohdistua sekä tietoliikenteen että tietojärjestelmän häirintää. Tietoliikenteen häirinnässä teon kohteena on viestintä, kuten tietojärjestelmien välityksellä tapahtuva sähköinen viestintä. Tietojärjestelmän häirinnässä teon kohteena taas on tietojärjestelmä, mukaan lukien sähköisiä viestejä välittävät tietojärjestelmät. Jos tietojärjestelmän häirintää koskevassa pykälässä tarkoitettu teko kohdistuu sähköiseen viestin-

[356] HE 94/1993 vp, s. 158.

tään, tietoliikenteen häirintää koskevat säännökset syrjäyttävät tietojärjestelmän häirinnän. Tietojärjestelmän häirintää koskevat säännökset ovat kuitenkin tarpeellisia, sillä ne kattavat myös sellaisen toiminnan, joka kohdistuu yksittäiseen tietokoneeseen tai joka ei edes välillisesti liity viestien siirtoon.[357]

Tietojärjestelmän häirinnän perusmuotoisesta kvalifioinnista säädetään RL 38:7 a:ssä ja törkeästä 38:7 b:ssä. Perusmuotoisen kvalifioinnin tunnusmerkistö kuuluu seuraavasti:

> Joka aiheuttaakseen toiselle haittaa tai taloudellista vahinkoa dataa syöttämällä, siirtämällä, vahingoittamalla, muuttamalla tai poistamalla taikka muulla niihin rinnastettavalla tavalla oikeudettomasti estää tietojärjestelmän toiminnan tai aiheuttaa sille vakavaa häiriötä, on tuomittava tietojärjestelmän häirinnästä sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Yritys on rangaistava.

Esimerkiksi tunnusmerkistön datan syöttämisellä tarkoitetaan pykälässä sellaista hyökkäystä, joka aiheuttaa kohteessa toimintahäiriön kuitenkin siten, että tietojärjestelmässä olevaa dataa ei millään tavalla vahingoiteta. Toimintahäiriö voi olla seurauksena tarkoituksellisesta ylikuormituksesta tai esimerkiksi syötettävän datan häiriöitä aiheuttavista ominaisuuksista. Hyökkäys ei siten kohdistu järjestelmässä olevaan dataan, vaan järjestelmän toimintaan.[358]

Tietojärjestelmän häirinnän tunnusmerkistöön kuuluu, että teko on tahallinen ja että tekijällä on vahingoittamis- tai haittaamistarkoitus. Lisäksi teon seurauksena tietojärjestelmän toiminta joko estyy kokonaan tai häiriintyy vakavasti. Tämän ohella teko on oltava tehty oikeudetta.[359] Haittaamistarkoitus ja tarkoitus aiheuttaa taloudellista vahinkoa eivät kuitenkaan tue bug bounty -ohjelmien yleistä tarkoitusta tietojärjestelmän turvallisuuden parantamisesta, eivätkä ne ole myöskään ohjelman puitteissa sallittuja tekoja.

Tulorekisteriä koskevan bug bounty -ohjelman säännöissä ei ole erikseen annettu oikeutusta RL 38:7 a:n tai 38:7 b:n mukaisiin toimiin. Ohjelman säännöissä on kuitenkin todettu vahingon rajoittamiseen liittyen, että testauksessa ei saa käyttää haitallista tai häi-

[357] HE 153/2006 vp, s. 65.
[358] HE 153/2006 vp, s. 65.
[359] HE 153/20016 vp, s. 65–66.

riötä aiheuttavaa kuormaa tai syötettä *sen enempää kuin mitä teknisen tietoturvahaavoittuvuuden olemassaolon todentaminen edellyttää*, tai että tietoturvatestaamisen suorittaminen ei saa *merkittävällä tavalla* vaikuttaa ohjelman kohteena olevan palvelun saatavuuteen [360]. Tällä perusteella voitaisiin katsoa, että ohjelman puitteissa on annettu oikeutus pienimuotoiseen tietojärjestelmän häirintään.

Oikeutus on tarpeen, sillä tavanomaisiin testausmetodeihin ja -toimenpiteisiin voi kuulua sellaisia tekoja, jotka estävät järjestelmän toimintaa jollakin tavalla. Sääntöjen kohta on kuitenkin siinä mielessä tulkinnanvarainen, että avoimeksi jätetään, mitä tarkoittaa haitallisen tai häiriötä aiheuttavan kuorman tai syötteen käyttäminen *sen enempää kuin mitä teknisen tietoturvahaavoittuvuuden olemassaolon todentaminen edellyttää*.

Ohjelman sääntöjen mukaan sääntöjen vastainen toiminta voi johtaa rikosoikeudellisiin seuraamuksiin[361]. On siis täysin tilaajan yksipuolisesta tulkinnasta riippuvaista, milloin tämä kokee, että tietojärjestelmälle on aiheutettu häiriötä enemmän kuin olisi ollut tarpeen ja että oikeustoimenpiteisiin on ryhdyttävä. Teon haitan tai vahingoittamistarkoituksen arviointi jää esitutkintaviranomaisten, syyttäjän ja tuomioistuimen harkittavaksi.

Edellä esitetyn ohella on vielä huomioitava rikoslain syyteoikeutta koskeva sääntely. Syyteoikeutta koskevassa RL 38:10:ssä ei ole rajoitettu syyttäjän oikeutta nostaa syytettä törkeän tietojärjestelmän häirinnän (RL 38:7 b) kohdalla. Tämä tarkoittaa sitä, että syyttäjän on nostettava syyte, mikäli sen tietoon tulee, että henkilön epäillään syyllistyneen törkeään tietojärjestelmän häirintään. Ohjelman tilaaja voi toki ilmoittaa, ettei sillä ole vaatimuksia asian suhteen, mutta tilaajan ilmoitus tai sitoutuminen olemaan vaatimatta rangaistusta tai vahingonkorvausta ei poista hakkerin rikosoikeudellista vastuuta.

5.4.7 Tietomurto

Tietomurron perusmuotoisesta kvalifioinnista säädetään RL 38:8:ssä ja törkeästä tekomuodosta 38:8 a:ssä Tietomurron perusmuotoisen kvalifioinnin tunnusmerkistö kuuluu seuraavasti:

[360] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[361] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen enintään kahdeksi vuodeksi.
>
> Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta
>
> 1) teknisen erikoislaitteen avulla tai
>
> 2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin
>
> oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta.
>
> Yritys on rangaistava.
>
> Tätä pykälää sovelletaan ainoastaan tekoon, josta ei ole muualla laissa säädetty ankarampaa tai yhtä ankaraa rangaistusta.

Sekä pykälän 1 että 2 momentissa kuvattu tekotapa edellyttävät teon oikeudettomuutta. Sen sijaan tietomurtoon syyllistyminen ei pykälän 1 momentin kohdalla edellytä vahingonteko- tai tiedonhankkimistarkoitusta.[362] Toisaalta, pykälän 2 momenttiin liittyy oleellisesti selon ottaminen 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta tai datasta[363]. Tekijän tahallisuutta kuitenkin edellytetään,[364] mutta bug bounty -ohjelmissa tahallisuus, pyrkimys päästä murtautumaan kohdetietojärjestelmään, täyttyy jo ohjelmien perimmäisen tarkoituksen vuoksi. Selon ottaminen, johon pykälän 2 momentissa viitataan, ei taas enää kuulu bug bounty -ohjelmien tarkoitukseen kuin korkeintaan haavoittuvuuden todentamisen yhteydessä.

Tietojärjestelmään tunkeutumisella tarkoitetaan pykälässä pääsyn hankkimista järjestelmässä käsiteltyihin, varastoituihin tai siirrettyihin tietoihin. Lisäksi teon rangaistavuuden edellytyksenä on, että tunkeutuminen tapahtuu järjestelmän turvajärjestelyn murtamalla. Turvajärjestelyn läpäisemistapaa kuvataan säännöksessä sanalla *murtaa*, jota on käytetty kielikuvamerkityksessä korostamaan juuri sitä, että turvajärjestelyn läpäisyn on oltava

[362] Ks. myös HE 94/1993 vp, s. 155–156.
[363] HE 232/2014 vp, s. 35.
[364] Ks. myös HE 94/1993 vp, s. 155–156.

luvatonta.[365] Tietomurron teko täyttyy – eikä jää yritysasteelle – siinä vaiheessa, kun tietojärjestelmän tunnistuskontrolli on onnistuttu läpäisemään.[366]

Tulorekisteriä koskevan bug bounty -ohjelman säännöissä on erikseen todettu, että tilaaja myöntää ohjelmaan osallistuville tietoturvatestaajille oikeuden toteuttaa tilaajan järjestelmään haavoittuvuustestaustoimia ja -toimenpiteitä, jotka voitaisiin tulkita tietomurron yritykseksi.[367] Säännöissä siis nimenomaisesti annetaan oikeutus *tietomurron yritykseen*. Sen sijaan oikeutusta tietomurtoon ei ole annettu.

Mikäli bug bounty -ohjelmassa toimiva henkilö onnistuu paikallistamaan haavoittuvuuden, jonka avulla tietojärjestelmään pääsee tunkeutumaan, niin tietojärjestelmään sisälle meneminen esimerkiksi tämän haavoittuvuuden raportoimiseksi ei ole ohjelman sääntöjen mukaan ollut ohjelman tilaajan oikeuttama teko, eikä tilaaja ole säännöissä edes sitoutunut olemaan tekemättä tutkintapyyntöjä RL 38:8:n tarkoittamissa tilanteissa tai olemaan vaatimatta näistä rikosoikeudellisia seuraamuksia[368]. Tästä syystä haavoittuvuuden paikallistamisessa onnistunut hakkeri saattaa syyllistyä tietomurtoon.

Tietomurtoa koskevaa 38 luvun 8 §:ää on muutettu pykälää koskevalla viimeisimmällä lakimuutoksella (368/2015) sellaiseksi, että se ei kata pelkästään murtautumista salauksen murtamalla, vaan murtamisella on ymmärrettävä myös esimerkiksi tietojärjestelmässä olevan haavoittuvuuden hyväksikäyttö[369].

> Pykälän 2 momenttia koskevan hallituksen esityksen mukaan esimerkiksi *cross-site scripting* -haavoittuvuuden (XSS) hyödyntäminen, joka saattaa olla bug bounty -ohjelmassa palkkioon oikeuttava haavoittuvuus, käyttäminen hyökkäyksessä ei yleensä merkitse selon ottamista tietojärjestelmässä olevasta tiedosta tai datasta, joten se arvioidaan tietomurron sijaan tapauskohtaisesti esimerkiksi vaaran aiheuttamisena tietojenkäsittelylle, luvattomana käyttönä, datavahingontekona, petoksena tai maksuvälinepetoksena.[370]

[365] HE 94/1993 vp, s. 155.
[366] HE 94/1993 vp, s. 156.
[367] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[368] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[369] Ks. HE 232/2014 vp, s. 35.
[370] HE 232/2014 vp, s. 35.

5.4.8 Tietosuojarikos

Tietosuojarikos poikkeaa edellä käsiteltyjen rikosten tarkastelusta siinä mielessä, että näkökulmana on se, voiko bug bounty -ohjelman järjestäjä syyllistyä tähän rikokseen. Tietosuojarikoksesta säädetään RL 38 luvun 9 pykälässä seuraavasti:

> Joka muutoin kuin luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annetussa Euroopan parlamentin ja neuvoston asetuksessa (EU) 2016/679 (yleinen tietosuoja-asetus), jäljempänä yleinen tietosuoja-asetus, tarkoitettuna rekisterinpitäjänä tai henkilötietojen käsittelijänä tahallaan tai törkeästä huolimattomuudesta hankkii henkilötietoja niiden käyttötarkoituksen kanssa yhteensopimattomalla tavalla, luovuttaa henkilötietoja tai siirtää henkilötietoja vastoin
>
> 1) yleisen tietosuoja-asetuksen,
>
> 2) tietosuojalain (1050/2018),
>
> 3) henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018) tai
>
> 4) henkilötietojen käsittelyä koskevan muun lain
>
> henkilötietojen käyttötarkoitussidonnaisuutta, luovuttamista tai siirtämistä koskevaa säännöstä ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava tietosuojarikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.
>
> Tietosuojarikoksesta tuomitaan myös se, joka tahallaan tai törkeästä huolimattomuudesta toimii vastoin sitä, mitä 1 momentin 1–4 kohdassa tarkoitetussa säädöksessä säädetään henkilötietojen käsittelyn turvallisuudesta.

Pykälän 1 momentin sääntelyä sovelletaan ainoastaan tilanteessa, jossa henkilön ei voida katsoa toimineen rekisterinpitäjänä tai henkilötietojen käsittelijänä. Esimerkkinä tilanteesta, jossa joku saattaisi syyllistyä 1 momentin nojalla tietosuojarikokseen, on lainvalmisteluaineistossa annettu niin sanottu urkintatapaus, jossa henkilö, jolla on esimerkiksi työtehtäviensä puitteissa oikeus käsitellä henkilötietoja, käsittelee niitä tavalla, joka ei liity työtehtävien suorittamiseen.[371] Pykälän 1 momentti koskee lähinnä rekisterinpitäjän

[371] HE 9/2018 vp, s. 124.

ja henkilötietojen käsittelijän alaisuudessa toimivia henkilöitä – rekisterinpitäjän ja henkilötietojen käsittelijän rikkomukset on jo sanktioitu hallinnollisina seuraamusmaksuina tietosuoja-asetuksen ja kansallisen tietosuojalain nojalla.[372]

Oleellista onkin tarkastella pykälän 2 momenttia, jonka mukaan minkä tahansa henkilötietojen käsittelyä koskevan lain henkilötietojen käsittelyn turvallisuutta koskevien säännösten rikkomisesta tuomitaan tietosuojarikoksesta. Momentin mukaan tietosuojarikokseen syyllistyminen edellyttää tahallisuutta tai törkeää huolimattomuutta. Pykälän 2 momentti koskee myös rekisterinpitäjinä ja henkilötietojen käsittelijöinä toimivia luonnollisia henkilöitä[373].

Voutilaisen esittämän tulkinnan mukaan pykälän 2 momentti on rangaistavuuden ennakoitavuuden näkökulmasta ongelmallinen: Henkilötietojen turvallisuutta koskevat säännökset tietoturvallisuustoimenpiteistä tietosuojalain 6.2 §:ssä ovat suosituksia, eli niiden noudattamatta jättäminen ei ole rangaistavaa. Yleisessä tietosuoja-asetuksessa sen sijaan säädetään tietoturvallisuustoimenpiteistä vain esimerkinomaisesti, joten noudattamatta jättäminen ei ole rangaistavaa. Rikosasioiden tietosuojalaissa pääosa turvallisuutta koskevista säännöksistä on tarkoitusperusteisia, ja varsinaiset toimet jäävät rekisterinpitäjän harkintaan. Rekisterinpitäjän laatimat käsittelyohjeet eivät taas ole suoraan säädöksiin sidottuja, joten niiden noudattamatta jättäminen ei voi olla rangaistavaa. Pykälän 2 momentin rangaistussääntö on siis varsin tulkinnanvarainen ja soveltamiskelvoton. Henkilötietojen käsittelyä koskevien säännösten rikkomista on oikeuskäytännössä kuitenkin arvioitu esimerkiksi virkavelvollisuuden rikkomisena tai tuottamuksellisena virkavelvollisuuden rikkomisena.[374]

[372] Ks. myös Voutilainen 2019, s. 213–214.
[373] HaVM 13/2018 vp, s. 46, ks. myös Voutilainen 2019, s. 215.
[374] Voutilainen 2019, s. 215–216.

6 Bug bounty -ohjelman käyttäminen julkishallinnossa

6.1 Ohjelman käytön juridinen oikeutus

Viranomaisella on velvollisuus huolehtia tietojärjestelmiensä tietoturvasta. Tämä velvollisuus voidaan johtaa muun muassa kansainvälisistä ihmis- ja perusoikeuksista, perustuslaista, tiedonhallintalaista, tietosuojaa koskevasta sääntelystä, hallinto-oikeuden yleisistä periaatteista, Euroopan ihmisoikeustuomioistuimen ratkaisukäytännöstä sekä ylimpien laillisuusvalvojien ratkaisukäytännöstä[375]. Missään oikeuslähteessä ei kuitenkaan yksityiskohtaisesti määritellä, millaisia toimenpiteitä viranomaisen tulee toteuttaa täyttääkseen positiivisen toimintavelvoitteensa tietoturvasta huolehtimisen kohdalla. Tiedonhallintalain 13.1 §:n mukaisesti tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan, ja tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti[376]. Edelleen tiedonhallintalain 13.2 §:n mukaan viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti. Olennaisilla tietojärjestelmillä tarkoitetaan pykälässä sellaisia tietojärjestelmiä, jotka ovat kriittisiä viranomaisen lakisääteisten tehtäviä toteuttamisen kannalta erityisesti hallinnon asiakkaille palveluja tuotettaessa[377]. Koska bug bounty -ohjelmia voidaan pitää kustannustehokkaina menetelminä tietoturvaliitännäisten haavoittuvuuksien paikallistamiseksi, voidaan niiden käyttöä julkishallinnossa tältä osin pitää perusteltuna.

Bug bounty -ohjelmiin liittyy kuitenkin teoreettinen mahdollisuus siitä, että ohjelmaan osallistuva yksityishenkilö päätyy näkemään jotakin tietojärjestelmässä olevaa tietoa, jonka näkemiseen tällä ei ole oikeutta. Tämä mahdollisuus edellyttää ensinnäkin sitä, että tietojärjestelmässä on olemassa haavoittuvuus, joka tällaisen tarkastelun mahdollistaa, ja toisekseen sitä, että hakkeri onnistuu paikallistamaan tämän haavoittuvuuden. Vaikka ohjelman säännöissä olisikin erikseen huomioitu tällaisen tilanteen mahdollisuus sitouttamalla hakkeri olemaan paljastamatta kolmansille osapuolille tietojärjestelmässä olevia

[375] Viranomaisen velvollisuutta tietojärjestelmien tietoturvasta huolehtimiseen on käsitelty yksityiskohtaisemmin luvussa 4.3.
[376] Riskiarvioinnin tulee olla jatkuvaa toimintaa, ks. HE 284/2018 vp, s. 92.
[377] HE 284/2018 vp, s. 92.

tietoja, ei hakkerilla kuitenkaan lainsäädännön näkökulmasta ole välttämättä ollut näiden tietojen näkemiseen oikeutta. Ongelma konkretisoituu erityisesti yksityishenkilöiden viestinnän kohdalla.

Yleisen tietosuoja-asetuksen mukaan organisaatioiden on huolehdittava tarpeellisista turvallisuustoimenpiteistä henkilötietojen suojaamiseksi. Kuten muissakaan oikeuslähteissä, yleisessä tietosuoja-asetuksessakaan ei määritellä, millaisia yksittäisiä toimia tietosuojan ja tietoturvan turvaamiseksi tulee toteuttaa, jolloin on organisaation tietoturvasta vastaavan tahon päätösvallassa määritellä se, millaiset tietoturvallisuustoimet kulloinkin ovat oikeasuhtaisia ja tarkoituksenmukaisia henkilötietojen suojaamiseksi.

Yleisen tietosuoja-asetuksen 32 artiklan 1 kohdan mukaan rekisterinpitäjän velvollisuuksiin kuuluu teknisten ja organisatoristen toimenpiteiden toteuttaminen riskiä vastaavan turvallisuustason varmistamiseksi. Riskin arvioinnissa on huomioitava uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat eri asteiset riskit. Esimerkiksi artiklan 1 (b) kohdan mukaan teknisenä ja organisatorisena toimenpiteenä pidetään kykyä taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus. Bug bounty -ohjelmia voidaan pitää tällaisena toimenpiteenä.

Rekisterinpitäjän tulee ilmoittaa henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle yleisen tietosuoja-asetuksen 33 artiklan mukaisesti. Vaikka organisaatiossa olisi käynnissä bug bounty -ohjelma, ei se poista sitä seikkaa, että henkilötietojen tietoturvaloukkauksen tapahtuessa tulee toimia yleisen tietosuoja-asetuksen säännösten mukaisesti. Yleisen tietosuoja-asetuksen 33 artiklan 1 kohdan mukaan henkilötietojen tietoturvaloukkauksen tapahtuessa rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä 55 artiklan mukaisesti toimivaltaiselle valvontaviranomaiselle. Samassa kohdassa kuitenkin jatketaan, että ilmoitusta ei tarvitse tehdä, jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Mikäli bug bounty -ohjelman puitteissa hakkeri pääsee löytämänsä haavoittuvuuden johdosta katsomaan tietojärjestelmässä olevia henkilötietoja, tapahtuu henkilötietojen tieto-

turvaloukkaus. Koska bug bounty -ohjelmaan osallistuvan hakkerin pääasiallisena tarkoituksena on kuitenkin parantaa kohdejärjestelmän tietoturvaa eikä suinkaan käyttää järjestelmässä olevia tietoja hyväkseen, ei voida katsoa, että henkilötietojen tietoturvaloukkauksesta todennäköisesti aiheutuisi luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski. Näin ollen bug bounty -ohjelman puitteissa tapahtuvasta henkilötietojen tietoturvaloukkauksesta ei tarvitsisi ilmoittaa yleisen tietosuoja-asetuksen 55 artiklan mukaiselle toimivaltaiselle valvontaviranomaiselle, jona Suomessa toimii tietosuojalain 8 §:n mukaisesti tietosuojavaltuutettu.

Yleisen tietosuoja-asetuksen 34 artiklan mukaan henkilötietojen tietoturvaloukkauksesta tulee ilmoittaa rekisteröidylle ilman aiheetonta viivytystä, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Edelleen artiklan 3 kohdan mukaan ilmoitusta rekisteröidylle ei vaadita, mikäli rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, tai mikäli rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski ei enää todennäköisesti toteudu.

Bug bounty -ohjelman perimmäinen tarkoitus on pyrkiä murtautumaan tietojärjestelmään, mikä voi johtaa henkilötietojen katseluun. Kuten edellä todettua, ei kuitenkaan voida katsoa, että hakkerin mahdollinen onnistuminen haavoittuvuuden paikallistamisessa ja tietojärjestelmään tunkeutumisessa muodostaisi korkean riskin henkilöiden oikeuksille ja vapauksille. Koska tietoturvaloukkaus myös liittyy rekisterinpitäjän teknisten suojatoimenpiteiden toteuttamiseen kyseisissä henkilötiedoissa, ei yleisen tietosuoja-asetuksen 34 artiklan 3 kohdankaan mukaan rekisteröidylle tarvitse ilmoittaa henkilötietojen tietoturvaloukkauksesta. Edelleen, bug bounty -ohjelmissa rekisterinpitäjän lähtökohtaisena tarkoituksena on toteuttaa jatkotoimenpiteitä, toisin sanoen korjata haavoittuvuus, joilla varmistetaan, ettei artiklan 1 kohdassa tarkoitettu rekisteröidyn oikeuksiin ja vapauksiin kohdistuva riski, mikäli se voitaisiin arvioida korkeaksi, enää todennäköisesti toteudu.

Bug bounty -ohjelmien julkishallinnossa käyttämisen juridista oikeutusta voidaan lähestyä myös yleisen tietosuoja-asetuksen 6 artiklan henkilötietojen käsittelyn lainmukaisuutta koskevan sääntelyn kautta. Henkilötietojen käsittely on artiklan mukaan lain mukaista, mikäli yksikin artiklan 1 kohdan alakohdista täyttyy. Artiklan 1 (c) kohdan mukaan henkilötietojen käsittely on sallittua, mikäli käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Koska rekisterinpitäjällä on lakisääteinen velvollisuus pitää huolta käsittelyjärjestelmien ja palveluiden jatkuvasta luottamuksellisuudesta, eheydestä, käytettävyydestä ja vikasietoisuudesta (32 artikla 1 (b) kohta), voidaan tulkita, että henkilötietojen käsittely on sallittua sellaisten toimenpiteiden yhteydessä, jotka tähtäävät käsittelyjärjestelmän turvallisuuden ylläpitoon ja parantamiseen, kuten bug bounty -ohjelmissa.

Voidaan siis todeta, että sekä yleisesti tietoturvaa koskeva sääntely että myös henkilötietojen suojaan keskittyvä yleinen tietosuoja-asetus mahdollistavat bug bounty -ohjelmien tai sen tyyppisten testaustoimenpiteiden käyttämisen tietyin edellytyksin. Testaustoimenpiteiden yhteydessä paikallistetuista haavoittuvuuksista, jotka johtavat rekisteröityjen henkilötietojen paljastumiseen, ei edes tarvitse informoida tietosuojavaltuutettua tai rekisteröityjä, mikäli ohjelmassa toimitaan ohjelman sääntöjen mukaisesti, eikä haavoittuvuuden paikallistamisen yhteydessä paljastettuja henkilötietoja välitetä tai ilmaista kolmansille osapuolille[378].

Edellä tutkimuksen luvussa 5 on käsitelty sitä, voiko hakkeri syyllistyä johonkin rikokseen bug bounty -ohjelmaan osallistuessaan. Syyllistymistä on tarkasteltu muun muassa suhteessa loukatun suostumukseen, joka annetaan ohjelman säännöissä. Ohjelman säännöillä ja niiden yksityiskohdilla on siis suuri merkitys sen suhteen, voiko hakkeri syyllistyä ohjelmaan osallistuessaan rikokseen. Verohallinnon Tulorekisteri-ohjelman sääntöihin lainsäädäntöä peilattaessa voidaan todeta, että tietyissä tilanteissa rikokseen syyllistyminen on mahdollista, esimerkiksi tietoliikenteen häirinnän tai viestintäsalaisuuden loukkauksen suhteen, vaikka hakkeri olisikin toteuttanut testaustoimenpiteitä hyvissä aikeissa. Viestintäsalaisuuden loukkauksen kohdalla hyvätkään ohjelman säännöt eivät poista teon oikeudenvastaisuutta tietyissä tilanteissa. Viime kädessä rikokseen syyllistymiseen liittyvä harkinta tapahtuu tuomioistuimessa.

[378] Ks. Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

Bug bounty -ohjelmassa toteutettavat testaustoimenpiteet teoreettisella tasolla vaarantavat luonnollisten henkilöiden perusoikeuksia, kuten oikeutta yksityisyyteen ja oikeutta henkilötietojen suojaan. Kun bug bounty -ohjelma kohdistuu julkishallinnon tietojärjestelmään, jonka olemassaolo perustuu lakiin, ei silloin kuitenkaan ole merkitystä sillä, antaako rekisteröity suostumuksensa henkilötietojensa käsittelylle, mitä esimerkiksi henkilötietojen katseleminen on: viranomaisen lakiin perustuva velvollisuus tietojärjestelmän tai rekisterin tietoturvan turvaamiseksi on määrittävä tekijä. Samoin rikosoikeudellisesta näkökulmasta loukatun suostumuksen antamisen suhteen oleellista on nimenomaisesti tietojärjestelmän omistajan tai rekisterinpitäjän suostumus sille, että tietojärjestelmään kohdistetaan testaustoimenpiteitä.

6.2 Ohjelman käynnistämisestä päättäminen

Tiedonhallintalain 2.1 § 2 kohdassa määritellään tiedonhallintayksikkö viranomaiseksi, jonka tehtävänä on järjestää tiedonhallinta tämän tiedonhallintalain vaatimusten mukaisesti. Julkishallinnossa viranomaisen tietojärjestelmien tietoturvallisuustoimenpiteistä, jollaisena bug bounty -ohjelmia voidaan pitää, vastaa siis yleisellä tasolla tiedonhallintayksikkö. Täsmällisemmin, tietoturvallisuustoimenpiteiden toteuttamisen järjestämisvastuussa on tiedonhallintayksikön johto. Johdon on huolehdittava, että tietoturvallisuustoimenpiteet on suunniteltu ja niiden toteuttaminen on resursoitu riittävästi,[379] eli johdolla on myös aktiivinen toimintavelvoite tietoturvallisuustoimenpiteiden tekemiseen.

Vastuuta tietoturvallisuudesta ja tietoturvallisuustoimenpiteiden tekemisestä voidaan määrittää edelleen tarkemmin. Tietoturvatyöhön tulee nimetä vastuuhenkilö, esimerkiksi tietoturvapäällikkö, jolle tulee osoittaa myös riittävät resurssit hoitaa ja toteuttaa organisaation tietoturvavelvoitteita. Tämä vastuuhenkilö raportoi johdolle. Johdon ja esimiesten tehtävänä on varmistaa, että tietoturva toteutuu organisaation kaikilla tasoilla.[380]

Yleisen tietosuoja-asetuksen 5 artiklan 1 (f) kohdan mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien

[379] Voutilainen 2019, s. 329.
[380] Andreasson & Koivisto 2013, s. 33.

suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”). Saman artiklan 2 kohdan mukaan rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että 1 kohtaa on noudatettu (”osoitusvelvollisuus”). Edelleen tietosuoja-asetuksen 32 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Yleisen tietosuoja-asetuksen mukaan rekisterin turvallisuus on siis rekisterinpitäjän vastuulla: rekisteritoimintojen lainmukaisuudesta ja henkilötietojen käsittelyn oikeellisuudesta vastaa juridinen rekisterinpitäjä[381].

Tiedonhallintalakia sovelletaan lain 3.1 §:n mukaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun viranomaiset käsittelevät tietoaineistoja. Yleistä tietosuoja-asetusta sen sijaan sovelletaan asetuksen 2 artiklan 1 kohdan mukaan henkilötietojen osittaiseen tai kokonaan automaattiseen käsittelyyn, sekä muussa kuin automaattisessa muodossa sellaisten henkilötietojen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Kun bug bounty -ohjelma kohdistuu viranomaisen tietojärjestelmään, jota pidetään myös yleisen tietosuoja-asetuksen tarkoittamana henkilörekisterinä, on kyseessä tilanne, jossa tiedonhallintayksikkö ja rekisterinpitäjä ovat tosiasiassa sama taho.

Tietosuoja-asetuksen mukainen rekisterinpitäjä taas ei välttämättä julkishallinnossa ole viranomainen yleisellä tasolla, vaan esimerkiksi viranomaisen tietty yksikkö tai osasto. Esimerkiksi Tulorekisterin kohdalla rekisterinpitäjänä ei toimi Verohallinto, vaan Verohallinnon Tulorekisteriyksikkö (L tulotietojärjestelmästä 53/2018, 4.1 §).

Edellä luvussa 5 käsiteltyjen rikoslain tieto- ja viestintärikoksiin liittyvissä tunnusmerkistöissä lähes jokaisen tunnusmerkistön kohdalla on kysymys siitä, onko teolle ollut oikeutus vai ei. Ohjelman käynnistämisestä päättäminen sisältää ajatuksen siitä, että ohjelman kohteen omistaja antaa oikeutuksen ohjelman kohteeseen kohdistuviin testaustoimenpiteisiin. Ohjelman käynnistämisestä päättämisestä vastuussa oleva taho on vastuussa myös

[381] Andreasson & Koivisto 2013, s. 108.

ohjelman sääntöjen hyväksymisestä. On siis tämän saman tahon vastuulla, että ohjelman säännöt ovat täsmälliset, eivätkä aiheuta vahinkoa organisaatiota kohtaan.

6.3 Ohjelman sääntöjen merkitys

Jokaisella ohjelmalla on omat sääntönsä. Ohjelman sääntöjen sisällöt eivät vaihtele pelkästään eri tilaajien tai alustayritysten välillä, vaan poikkeavuuksia sääntöjen sisällöissä saattaa löytyä esimerkiksi saman tilaajan eri tietojärjestelmiin toteutettavien bug bounty -ohjelmien välillä. Säännöistä on kuitenkin paikallistettavissa sellaisia yleisiä piirteitä tai periaatteita, jotka suurimmassa osassa ohjelmia ovat yhteneväisiä. Tällainen on esimerkiksi se, että ohjelmaan osallistuva henkilö ei saa vahingoittaa tietojärjestelmiä tai tarpeettomasti haitata niiden toimintaa. Sääntöjen tarkastelu on tässä tutkielmassa tehty suhteessa Verohallinnon Tulorekisteriä koskevan bug bounty -ohjelman sääntöihin[382].

Ohjelman säännöt ovat se instrumentti, jolla annetaan ohjelmaan osallistuvalle hakkerille loukatun suostumus toimintaan, joka ilman tätä suostumusta katsottaisiin lain vastaiseksi teoksi. Tästä syystä säännöillä on suuri merkitys ohjelmien puitteissa toteutettavan toiminnan lainmukaisuuden arvioinnille. Sääntöjä voidaan myös verrata vakiosopimukseen, joka ohjelmaan osallistuvan hakkerin tulee hyväksyä ja jonka yksityiskohtien mukaisesti hakkerin tulee toimia.

Verohallinnon Tulorekisteriä koskevan ohjelman sääntöjen mukaan tarkoituksena on, että ohjelmaan osallistuminen ja siihen liittyvän tietoturvatutkimuksen suorittaminen ei aiheuta ennalta arvaamattomia tietoturvariskejä Verohallinnon asiakkaille, asiakastiedoille tai verotuksen toiminnalle. Edelleen ohjelman periaatteellisiin rajauksiin kuuluu esimerkiksi, että testauksessa ei saa käyttää haitallista tai häiriötä aiheuttavaa kuormaa tai syötettä sen enempää kuin mitä teknisen tietoturvahaavoittuvuuden olemassaolon todentaminen edellyttää, tai että tietoturvatestaamisen suorittaminen ei saa merkittävällä tavalla vaikuttaa ohjelman kohteena olevan palvelun saatavuuteen.[383] Ohjelman säännöistä voidaan

[382] Ohjelma on alkanut Hackrfi-palvelussa 28.10.2019 ja on voimassa toistaiseksi. Ohjelman säännöt eivät ole saatavilla Hackrfi Oy:n nettisivuilla.
[383] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.

paikallistaa yksityiskohta, jonka mukaan tilaaja sitoutuu olemaan tekemättä rikosilmoituksia RL 38:5, 6 ja 7:n nojalla. Sääntöjen mukaan tilaaja ei kuitenkaan ole sitoutunut olemaan tekemättä rikosilmoituksia esimerkiksi tietomurtoa koskevan RL 38:8:n nojalla, vaikka säännöissä tilaaja myöntääkin ohjelmaan osallistuville tietoturvatestaajille oikeuden toteuttaa haavoittuvuustestaustoimia ja -toimenpiteitä, jotka voitaisiin tulkita tietomurron yritykseksi.[384]

Sopimusoikeuden tulkintaperiaatteisiin kuuluvan epäselvyyssäännön mukaan epäselvyyksiä tulkitaan sen osapuolen vahingoksi, joka on laatinut sopimuksen. Periaate perustuu siihen, että sopimuksen laatineella taholla on yleensä paremmat mahdollisuudet vaikuttaa sopimustekstin sisältöön ja ehtoihin. Epäselvyyssäännöllä on korostettu merkitys vakiosopimusten tulkinnassa.[385] Tässä tapauksessa vahvempana osapuolena voidaan pitää vakiosopimuksen laatijaa, eli joko alustayritystä tai tilaajaa. Ohjelmaan osallistuvan hakkerin siis tuskin tarvitsisi, omasta mielestään sääntöjen mukaisesti toimiessaan, pelätä seuraamuksia RL 38:8:n nojalla. Tältäkin ongelmalta voitaisiin kuitenkin välttyä, mikäli säännöissä olisi kiinnitetty enemmän huomiota juridisiin yksityiskohtiin.

Ohjelman sääntöjen vastainen toiminta voi ohjelman sääntöjen mukaan johtaa rikosoikeudellisiin seuraamuksiin.[386] Tämä on loogista, sillä tilaaja on antanut oikeutuksen tietoturvatoimenpiteisen toteuttamiseen vain ohjelman sääntöjen puitteissa – sääntöjen vastaisesti toimiessa oikeutusta toimenpiteisiin ei ole. Ohjelman tilaajalla ei nähdäkseni ole säännöissä erikseen tarpeen pidättää oikeutta tehdä sääntöjen vastaisesta toiminnasta tutkintapyyntöjä poliisille tai vaatia asiassa rangaistusta ja vahingonkorvausta[387].

Sen lisäksi, että ohjelmaan osallistuvan hakkerin tulee hyväksyä ohjelman säännöt, täytyy tämän myös, ainakin Tulorekisteriä koskevan ohjelman kohdalla, allekirjoittaa salassapitosopimus[388]. Allekirjoittamiseen käytetään Visma Sign -palvelua[389]. Allekirjoittamisen jälkeen alustayritys antaa hakkerille luvan osallistua Tulorekisteriä koskevaan bug

[384] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[385] Hemmo & Hoppu 2006, 7. Sopimuksen keskeinen sisältö – Sopimuksen tulkinta – Sopimusten tulkintaperiaatteista – Epäselvyyssääntö.
[386] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[387] Vrt. Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[388] Tietoturva-alalla, kuten tässäkin tapauksessa, vaikuttaa yleensä olevan käytössä vain salassapitosopimuksen englanninkielinen lyhenne NDA (*non-disclosure agreement*).
[389] Palvelun avulla toteutetaan sähköinen tunnistautuminen, jolloin hakkerin henkilöllisyys tulee selville, joskin vain alustayritykselle.

bounty -ohjelmaan: ohjelman tilaaja luottaa alustayrityksen arvioon siitä, kannattaako tietyn henkilön antaa osallistua, eikä tämä menettelytapa ole aivan poikkeuksellinen.[390] Valitettavasti tutkimuksen teon yhteydessä ei ole ollut käytettävissä ohjelmaan osallistumiseen liittyvää salassapitosopimusta tämän salassapitosopimuksen yksityiskohtien analysoimiseksi.

Voidaan kuitenkin pohtia, onko kahdelle erilliselle sopimusinstrumentille, ohjelman säännöille ja salassapitosopimukselle, tosiasiassa tarvetta – sähköisen tunnistautumisen ohella, mitä sellaista salassapitosopimus tuo lisää, mitä säännöissä ei olisi jo määritelty osallistumisen ehdoksi? Tulorekisteriä koskevan ohjelman säännöissä nimittäin on salassapitoon viittaava kohta, jonka mukaan raportoijan on pidettävä salassa sellaiset tiedot, jotka löydetyn haavoittuvuuden vuoksi saadaan näkyville, välittämättä tai ilmaisematta niitä kolmansille osapuolille. Edelleen säännöissä on määritelty myös, että lähettäessään raportin raportoija sitoutuu raportin sisältämän haavoittuvuuden julkaisukieltoon: haavoittuvuudesta ei saa antaa tietoa kolmansille osapuolille[391]. Mikäli salassapitosopimuksen ja ohjelman sääntöjen sisältö voidaan tulkita toisistaan poikkeavalla tavalla, voi se aiheuttaa epäselviä tilanteita sopimusten noudattamisen suhteen.

Bug bounty -ohjelmien säännöistä voidaan vielä yleisesti ottaen todeta, että ohjelman säännöissä tai muutoin ohjelman yhteydessä julkaistu tieto siitä, että ohjelman sääntöjen mukaisesti toimivaan hakkeriin ei tulla kohdistamaan oikeudellisia vaatimuksia, vähentää epävarmuutta ja luo luottamuksellista ilmapiiriä.[392] Tällä tavalla voidaan kannustaa hakkereita osallistumaan testaustoimintaan.

6.4 Bug bounty -ohjelman järjestäminen julkishallinnossa

Kun julkishallinnollisessa organisaatiossa pohditaan bug bounty -ohjelman käyttöönottoa, olisi hyvä täsmentää eräitä seikkoja ohjelman malliin liittyen hyvissä ajoin. Jo ohjelman käyttöä harkittaessa on tehtävä päätös siitä, toteutetaanko ohjelma sisäisenä työnä

[390] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.
[391] Tulorekisteriä koskevan bug bounty -ohjelman säännöt.
[392] Kuehn 2014.

vai hankintana. Sisäisenä työnä toteuttaminen edellyttää muun muassa monialaista tietoturvatestaamisen osaamista ja henkilöstöresursseja haavoittuvuusraporttien läpikäyntiin. On todennäköistä, että suurimmalla osalla julkishallinnon organisaatioista ei ole tarvittavia resursseja ohjelman täysin itsenäiselle järjestämiselle. Bug bounty -ohjelman tai muun vastaavan haavoittuvuuksien julkistamisohjelman toteuttamisrakenne tulee täsmentää aikaisessa vaiheessa, tosin malli määräytyy osin jo senkin mukaan, millaisia palveluntarjoajia on olemassa. Edellä tässä tutkimuksessa, luvussa 2.1 kuvattu rakenne on melko tavallinen. Täsmennystä tähän rakenteeseen voi tehdä esimerkiksi päättämällä, onko kyseessä kaikille halukkaille avoin ohjelma vaiko jonkin asteinen kutsuohjelma.

Viimeistään ohjelman käynnistämisen yhteydessä on hyvä päättää, onko kyseessä jatkuvaksi aiottu ohjelma, vai asetetaanko ohjelmalle päättymispäivä. Esimerkiksi Verohallinnon Tulorekisteriä koskevan bug bounty -ohjelman päättymispäivää ei ole määritelty ennalta, vaan kyseisen ohjelman päättymisajankohta määrittyy sen mukaan, havaitaanko siitä olevan hyötyä[393]. Koska bug bounty -ohjelma on siis julkisella sektorilla lähestulkoon aina hankinta, sovelletaan siihen hankintalainsäädäntöä, esimerkiksi hankintalain (L julkisista hankinnoista ja käyttöoikeussopimuksista, 1397/2016) 25–26 §:n sääntelyä kansallisista ja EU-kynnysarvoista. Tämä tulee huomioida myös ohjelman kestoa määritettäessä.

Alustayrityksellä tai muulla ohjelman toteuttajalla on myös joissain määrin vaikutusta siihen, millainen henkilö voi osallistua ohjelmaan. Esimerkiksi Verohallinnon Tulorekisteriä koskevaan ohjelmaan osallistuminen on mahdollista laajallekin joukolle, mutta palkkio voidaan alustayrityksen ilmoituksen mukaan maksaa vain henkilöille, joilla on suomalainen verokortti ja pankkitili. Myös kieli rajaa osallistujia. Esimerkiksi Hackrfi Oy:n nettisivuista on olemassa sekä suomenkielinen että englanninkielinen versio. Englanninkielisillä sivuilla ei kuitenkaan markkinoida Verohallinnon Tulorekisteriä koskevaa bug bounty -ohjelmaa eikä esimerkiksi DVV:n suomi.fi-sivustoa koskevaa ohjelmaa (entinen VRK:n ohjelma). Käytännössä näihin ohjelmiin osallistuminen on siis rajattu vain suo-

[393] Sähköpostikeskustelut 2019–2020, Juho Vuorio, Verohallinnon Turvallisuus- ja riskienhallintayksikkö.

men kieltä ymmärtäville henkilöille. Ohjelmaan osallistuakseen hakkerin on myös ymmärrettävä ohjelman säännöt, sillä sääntöjen noudattaminen on pakollista ohjelmaan osallistuessa.

Ohjelmien palkkioiden maksaminen aiheuttaa myös tietynlaisia rajauksia osallistujajoukkoon: Verohallinnon Tulorekisteri-ohjelman tapauksessa palkkiot maksetaan työkorvauksena, mikä edellyttää myös verokortin ja tilinumeron toimittamista alustayrityksenä toimivalle Hackrfi Oy:lle. Palkkion maksaa Hackrfi Oy.[394] Palkkion määrittäminen työkorvaukseksi ottaa kantaa palkkion verotukselliseen kohteluun. Ennakkoperintälain (1118/1996) 25 §:ssä säädetään ennakkoperintärekisteristä. Pykälän 1 momentin 1 kohdan mukaan suorituksen maksajan on toimitettava ennakonpidätys työstä, tehtävästä tai palveluksesta muuna kuin palkkana maksettavasta korvauksesta, jos saajaa ei ole merkitty ennakkoperintärekisteriin.

Työkorvaus on pääsääntöisesti saajansa elinkeinotoiminnan tuloa. Mikäli saajan ansiotoiminta on kuitenkin pienimuotoista, katsotaan työkorvaus henkilökohtaiseksi ansiotuloksi. Näin on esimerkiksi silloin, kun kyse on yksittäisistä ja satunnaisista työsuorituksista, joiden tekijä ei harjoita yritystoimintaa, mutta ei ole myöskään työsuhteessa työn teettäjään.[395] Bug bounty -ohjelman kohdalla ei voida kuitenkaan tietää, harjoittaako osallistuva hakkeri elinkeinotoimintaa, eli ei tiedetä, tulisiko palkkio laskea osaksi tämän elinkeinotoiminnan tuloja vai ansiotuloja. Työkorvaukset eli haavoittuvuuksien raportoinnista maksettavat palkkiot ovat mitä todennäköisimmin yksittäisiä ja satunnaisia, mikä sinänsä puoltaisi palkkioiden ansiotuloiksi lukemista, mutta eivät välttämättä vähäisiä eli pienimuotoista. Sekä Hackrfi Oy:n alustalla pyörivissä Tulorekisteriä että suomi.fi-palvelua koskevissa ohjelmissa palkkiohaitarin on ilmoitettu olevan 100–30 000 euroa – haitarin yläpäästä maksettavia palkkioita ei voitane pitää enää millään mittapuulla vähäisinä, sillä maksimipalkkio ylittää monen palkansaajan vuositulojen määrän. Tässä yhteydessä lyhyesti voidaan todeta, että palkkion maksu on juridisesti muunlainen kuin itsestään selvä kysymys.

[394] VRK:n suomi.fi-palvelua koskevan bug bounty -ohjelman säännöt, s. 5. Sääntöjen kirjoitusmuoto jättää epäselväksi sen, tuleeko palkkioon oikeutetun henkilön toimittaa suomalaisen verokortin lisäksi suomalainen tilinumero, vai voidaanko palkkio maksaa myös ulkomaiselle tilille.
[395] Verohallinnon syventävä vero-ohje: Palkka ja työkorvaus verotuksessa.

Julkishallinnossa ei myöskään voida maksaa palkkiota haavoittuvuuden paikallistamisesta ilman käynnissä olevaa ohjelmaa. Lainvalmisteluaineistossa on suhtauduttu kielteisesti siihen, että tietojärjestelmiin voisi yrittää murtautua tai murtautua omaksi huvikseen. Perusteluna on käytetty esimerkiksi sitä, että pahaa tarkoittamattomasta testaustoiminnasta ei voida erottaa niitä tahoja, jotka pyrkivät järjestelmään sitä väärinkäyttääkseen tai vahingoittaakseen.[396] Oikeuskäytännössä on todettu jo pelkän porttiskannerin käyttämisen täyttävän tietomurron yrityksen[397]. Tästä syystä tulisi suhtautua kielteisesti myös siihen, että tietojärjestelmiin kohdistuvaa, hyväntahtoistakaan haavoittuvuuksien etsintää toteutettaisiin ilman käynnissä olevaa bug bounty -ohjelmaa tai muuta menetelmää, jossa tietojärjestelmän omistaja erikseen on oikeuttanut järjestelmään kohdistuvat testaustoimenpiteet. Tällä perusteella voidaan myös todeta, että ilman käynnissä olevaa bug bounty -ohjelmaa haavoittuvuuden paikallistaneelle hakkerille ei tulisi maksaa palkkiota tämän paikallistamasta ja raportoimastaan haavoittuvuudesta. Vaikka teko sinänsä olisikin oikeustajun mukainen, ei loukatun, eli tietojärjestelmän omistajan, suostumusta voi antaa jälkikäteen[398]. Toisaalta on havaittava, että rikokseen syyllistyminen edellyttää pääsääntöisesti tahallisuutta.

Rekisteröidyn tiedollisen itsemääräämisoikeuden kannalta on keskeistä, että rekisteröity saa tiedon henkilötietojen käsittelystä sekä oikeuksistaan tässä käsittelyssä. Henkilötietojen suojaan kuuluukin siis rekisterinpitäjän velvollisuus huolehtia henkilötietojen käsittelyn läpinäkyvyydestä rekisteröidylle muun muassa informointivelvollisuutena.[399] Sääntelyä voidaan tulkita niin, että bug bounty -ohjelmista tulisi tiedottaa rekisteröidyn informointivelvollisuuden täyttämisen näkökulmasta. Bug bounty -ohjelmassa rekisteröidyn tietoja ei varsinaisesti ole tarkoitus käsitellä, mutta aitona riskinä on, että henkilö, jolla ei ole normaalitilanteessa oikeuta tarkastella rekisteröidyn tietoja, onnistuu näitä tietoja kuitenkin tarkastelemaan.

[396] HE 94/1993 vp, s. 140.
[397] Ks. KKO 2003:36.
[398] Koskinen 2004, päivitetty 1.11.2008, ei sivunumerointia. I Yleisiä kysymyksiä, 7. Rikosoikeuden yleiset opit ja rikosvastuun perusteet, Rikoksen rakenne (yleinen tunnusmerkistö), Oikeudenvastaisuus, Oikeuttamisperusteet, Muita oikeuttamisperusteita, Suostumus.
[399] Voutilainen 2019, s. 84–85.

7 Johtopäätökset

Bug bounty -ohjelmat voivat olla osa tietoturvan testaamista julkishallinnossa, mutta eivät ainoa ratkaisu. Edelleen on käytettävä muitakin tietoturvan testaamisen muotoja, kuten ohjelmistojen kehittämisvaiheessa tapahtuvaa testausta ja penetraatiotestausta. Usein bug bounty -ohjelmia järjestettäessä kannattaakin käyttää ensin suppeampaa asiantuntijajoukkoa, ja käyttää ohjelman mukanaan tuomaa laajempaa hakkerien kirjoa vasta sen jälkeen. Ohjelman käynnistämisestä voidaan katsoa päättävän ja sääntöjen sisällöstä vastaavan ohjelman tilaajan tietoturvasta vastaava taho yhdessä organisaation johdon kanssa.

Erityisesti rikoslain 38:3:n mukaisen viestintäsalaisuuden loukkauksen kohdalla bug bounty -ohjelman juridista oikeutusta voidaan kuitenkin kyseenalaistaa julkishallinnossa toteutettavan ohjelman yhteydessä. Ohjelman tilaaja ei voi ennalta antaa suostumusta ohjelman puitteissa mahdollisesti tapahtuvaan tekoon, jonka asianomistaja se ei ole. Tässä suhteessa myöskään ohjelmien puitteissa tapahtuva itsesääntely ei julkishallinnon näkökulmasta ole riittävää, vaan ongelmaan tulisi puuttua lainsäädännön tasolla.

Bug bounty -ohjelmien käyttämistä julkishallinnon tietoturvan turvaajana voidaan kuvata perusoikeuksien kollisiona tai jopa perusoikeusparadoksina: Yhtäältä henkilöllä, jonka tietoja järjestelmässä käsitellään, on oikeus siihen, että tietojärjestelmän turvallisuustoimenpiteistä huolehditaan asianmukaisesti ja että niitä pyritään kehittämään proaktiivisesti. Toisaalta bug bounty -ohjelman käyttäminen aiheuttaa henkilötietojen suojan vaarantumisen ja yksityisyyden suoja tai luottamuksellinen viesti saattavat tulla loukatuksi. Paradoksin bug bounty -ohjelman käyttämisestä tekee se, että yksityisyyttä, henkilötietojen suojaa tai viestinnän luottamuksellisuutta potentiaalisesti loukkaamalla voidaan parantaa tätä yksityisyyden suojaa. Niin kauan kuin loukkaaminen tai sen mahdollisuus on vähäistä ja loukkaamisen seurauksena tapahtuva turvallisuuden tason parantaminen voidaan katsoa suuren mittakaavan eduksi, on bug bounty -ohjelmien käyttäminen julkishallinnossa nähdäkseni oikeutettua.

Ohjelmien käyttäminen julkishallinnossa ei ohjelman juridisen oikeutuksen näkökulmasta eroa merkittäviltä osin siitä, että organisaatio palkkaisi jonkin tietoturvayrityksen tekemään penetraatiotestausta samaan tietojärjestelmään, johon bug bounty -ohjelma

kohdistuu. Oikeudellisesta näkökulmasta erona on lähinnä se, että yritykseen työsuhteessa olevat henkilöt on mahdollisesti helpompi tavoittaa rikosoikeudellisia seuraamuksia varten, ja näihin työntekijöihin kohdistuisi todennäköisesti korkeampi maineriski, mikäli he syyllistyvät rikoksiin testaustoimenpiteitä tehdessään. Penetraatiotestausta joltakin yritykseltä hankittaessa yrityksen työntekijät voivat esimerkiksi päätyä katselemaan tietojärjestelmässä olevia henkilötietoja yhtä lailla kuin bug bounty -ohjelmaan osallistuvat henkilöt.

Bug bounty -ohjelman käyttäminen on joka tapauksessa eettisesti ja juridisesti kestävämpää, ja mitä suurimmissa määrin todennäköisesti kustannustehokkaampaa kuin se, että jokin merkittävä nollapäivähaavoittuvuus tulisi esiin sen jälkeen, kun vihamielinen hakkeri olisi sitä käyttänyt hyväkseen. Bug bounty -ohjelman toteuttamiseen, haavoittuvuuksien korjaamiseen ja palkkioiden maksamiseen käytettävät varat ovat todennäköisesti hyvin pieni summa verrattuna siihen, mitä haavoittuvuuden hyväksikäytön johdosta voi tapahtua. Kustannukset nousevat äkkiä miljooniin euroihin[400].

Tutkimuksen johtopäätöksenä voidaan myös esittää, että bug bounty -ohjelman organisoinnissa olisi hyödyllistä olla mukana juridista osaamista. Ohjelmien järjestämiseen liittyy oikeudellista rajapintaa lukuisilta osin – tunnistaa voidaan ainakin hankintaoikeudelliset, vero-oikeudelliset, työoikeudelliset, rikosoikeudelliset, sopimusoikeudelliset sekä tietosuojaan ja tietoturvaan liittyvät näkökulmat, joista erityisesti kaksi viimeistä linkittyvät edelleen perusoikeuksiin sekä yleishallinto-oikeuteen. Ohjelman järjestäminen vaatii lisäksi ainakin projektiosaamista ja teknologista osaamista.

Nykyinen Verohallinnossa käytössä oleva bug bounty -ohjelman järjestämismalli vaikuttaa melko byrokraattiselta. Karsiiko byrokraattisuus potentiaalisia osallistujia? Ohjelman järjestämisestä aiheutuu järjestäjälle suoraan sekä taloudellisia kustannuksia (hankinnat) että välillisesti taloudellisia kustannuksia (mm. virkamiesten työaika). Voidaankin siis kysyä: Onko ohjelman järjestäminen todellakin sen arvoista? Ylletäänkö kustannustehokkuudessa tarpeeksi korkealle tasolle? Hallinnon ja hallinto-oikeuden digitalisaation

[400] Ks. esim. Swinhoe – CSOonline.com, 29.8.2019. Kyberrikollisuuden kustannuksista ks. myös esim. Gillespie 2016, s. 13.

myötä ilmenevä muutos ja muutostarpeet, jotka esiintyvät tällä hetkellä erityisesti kysymyksissä päätöksenteon automatisoimisesta[401], saavat ilmenemismuotonsa myös tietoturvan testauksessa. Byrokratian keventämiselle ja hallinnon uudelleen ajattelulle on painetta, jotta testauksesta voitaisiin tehdä ketterämpää ja vaikuttavampaa.

Byrokratiaan liittyy olennaisesti se, että korkean elintason maassa asuvan hakkerin palkkion lunastamiseen käytetty aika ja vaiva kasvavat suuremmaksi kuin palkkion suuruus. Niin kauan, kun ohjelmaan osallistuminen on käytännössä rajattu henkilöihin, joilla on mahdollisuus toimittaa palkkion maksua varten suomalainen verokortti, tulee osallistujamäärä pysymään suhteellisen rajattuna – ei pelkästään kieli- ja verokortin toimittamisen mahdollisuuden näkökulmista, vaan myös siksi, että hakkerille kohdistuva hallinnollinen taakka kasvaa suuremmaksi kuin mikä on osallistumisen potentiaalinen taloudellinen tuotto. Se, että ohjelmista kyettäisiin tosiasiassa laatimaan sellaisia, että hallinnollinen taakka minimoituisi tai että osallistuminen olisi mahdollista myös muualta kuin korkean elintason valtioista, saattaisi lisätä kiinnostusta ohjelmia kohtaan ja parantaa ohjelmien kustannustehokkuutta relevanttien raporttien muodossa. Ohjelman tilaavan tai toteuttavan organisaation riskinä erityisesti Suomen ulkopuolelta osallistuvien hakkereiden kohdalla on mahdolliseen rikosoikeudelliseen vastuuseen saattaminen, mikäli hakkerin osallistuminen ei tapahdu ohjelman sääntöjen puitteissa. Tämä asettaa kysymykseksi myös sen, voidaanko julkishallinnossa järjestää sellaista bug bounty -ohjelmaa, jossa osallistujan rikosoikeudelliseen vastuuseen saattaminen olisi lähes mahdotonta.

Ohjelman tilaaja voi kuitenkin kannustaa hakkereita ohjelmaan osallistumiseen tukemalla myös muita kuin taloudellisia motiiveja. Näitä ovat hakkerin nimen tai nimimerkin esiin tuominen, joka tosin toimii vain niiden henkilöiden kohdalla, jotka motivoituvat julkisuudesta ja tunnustuksesta. Toinen motivaatiotekijä saattaa olla ohjelman kohde ja sen rajaus: kuinka mielenkiintoinen ohjelman kohde on hakkerin näkökulmasta. Tähän ohjelman tilaaja ei voi välttämättä vaikuttaa. Sitä, mikä tekee ohjelmasta mielenkiintoisen, tulisi kysyä hakkereilta, jotta ohjelman tilaajalla olisi edes teoriassa mahdollisuus vaikuttaa ohjelman kiinnostavuuteen. Tekeekö osallistumisesta mielenkiintoista esimerkiksi ohjelman kohteen linkittyminen kriittiseen infrastruktuuriin tai julkishallinnon ydintoimintoihin? Tätä olisi hyvä selvittää jatkotutkimuksessa.

[401] Ks. Pöysti 2018, s. 871–872.

Lopuksi voidaan todeta, että juridiikassa tulisi kiinnittää enemmän huomiota tietoturvaan. Oikeustieteen kentällä tulisi vähintäänkin ymmärtää tietoturvan merkitys ja tärkeys osana tietojärjestelmien hankintaa, kehitystä ja ylläpitoa, mutta toisaalta osana kaikkea julkista toimintaa. Julkinen hallinto jo nykyisellään, ja tulevaisuudessa yhä entistä enemmän, on sähköistä hallintoa. Yhtä lailla tärkeää olisi tutkia juridisesta näkökulmasta muitakin tietoturvaan ja sen testaamiseen liittyviä ilmiöitä kuin bug bounty -ohjelmia.