LähiTapiolan Bug Bounty –ohjelma

Mitkä ovat riskit, toimintamallit ja hyödyt haavoittuvuusohjelman käynnistämisestä skeä mitkä ovat vaikutukset yrityskulttuuriin tietoturvallisuuden näkökulmasta

15.Turvallisuusjohdon koulutusohjelma

Kehitysprojekti

Leo Niemelä

LähiTapiola

13.4.2018

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Sovellusten ja palvelujen julkaiseminen avoimeen internettiin on aina riskialtista. Kun web-sivu tai sovellus julkaistaan internettiin, altistuu organisaatio tietoturvahyökkäykselle tahtoi yritys sitä tai ei. Tässä tutkielmassa tutkitaan voivatko yritykset kehittää digitaalista turvallisuutta käynnistämällä haavoittuvuusohjelman sekä mitkä niiden vaikutukset ovat sovelluskehitystiimeihin ja yrityksen tietoturvakulttuuriin. Valkohattuisten hakkereiden avulla on mahdollisuus suojatua hyvinkin vakavia haavoittuvuuksia vastaan. Tutkielmassa käsitellään läheisesti LähiTapiola –ryhmän Bug Bounty –ohjelman tuloksia syyskuusta 2015 aina maaliskuuhun 2018.

Tämä tutkielma väittää miten organisaatiot voivat löytää haavoittuvuuksia verkkopalveluista hyödyntämällä valkohattuisia hakkereita sekä ohjeistaa yrityksiä miten hallitulla prosessilla voidaan Bug Bounty –ohjelma käynnistää.

Sisältö

LähiTapiolan Bug Bounty –ohjelma 1
1 Yleistä Bug Bounty -ohjelmista 1
1.1 Mikä on Bug Bounty -ohjelma 1
1.2 Minkälaisia haavoittuvuusohjelmia yritykset voivat käynnistää 1
1.2.1 Vulnerability Disclosure Policy (VDP) 1
1.2.2 Bug Bounty Program 1
1.2.3 Private Bug Bounty Program 1
1.2.4 Time-bound Bug Bounty 1
1.3 Haavoittuvuusohjelmien politiikka 1
1.4 Mikä on hakkereiden motiivi ja keitä he ovat? 1
2 LähiTapiolan Bug Bounty –ohjelman käynnistys ja taustatekijät 1
2.1 Riskiarviointi ja johdon hyväksyntä 1
2.1.1 Hyödyt 1
2.1.2 Uhkat 1
2.2 Haavoittuvuusohjelman ohjausryhmä (Bug Bounty Management Team) 1
2.3 Haavoittuvuusohjelman politiikka ja palkkiomallit 1
2.4 Miten rakennettaan luottamus hakkereiden keskuudessa 1
3 Avaimet menestyksekkään Bug Bounty –ohjelman käynnistämiseen 1
3.1 Bug Bounty –ohjelman prosessi 1
3.2 Haavoittuvuuksien korjaaminen ja palkkioiden maksu 1
3.3 Tilastoja LähiTapiolan haavoittuvuusohjelmasta 1
3.4 Avoimuus avainelementtinä 1
4 Haavoittuvuusohjelman hyödyt LähiTapiolalle 1
4.1 Vaikutukset tietoturvakulttuuriin 1
4.2 Yrityskuvaan liittyvät muutokset 1
4.3 Muutokset tietoturvatestauksen prosesseihin 1
4.4 Haavoittuvuuksien löydökset ja liitokset sovelluskehitykseen 1
4.5 Muutokset liiketoiminnan tietoturvaprosesseihin 1
5 Johtopäätökset 1

1 Yleistä Bug Bounty -ohjelmista

1.1 Mikä on Bug Bounty -ohjelma

Bug Bounty –ohjelma on eri komponenteista koostuva prosessi, jossa vapaaehtoiset tietoturvatutkijat testaavat verkkopalveluiden turvallisuutta ja raportoivat tietoturvahaavoittuvuuksista formaalisti kohdeyritykselle. Ohjelmissa yritykset maksavat rahallisia palkkioita tietoturvatutkijoille, jotka löytävät yrityksen järjestelmistä haavoittuvuuksia. Ensimmäisen ohjelman käynnisti Netscape vuonna 1995 ja tämän jälkeen useat isot toimijat kuten Google, Microsoft, Facebook ovat käynnistäneet omat haavoittuvuusohjelmansa. Suomessa julkinen Bug Bounty –ohjelma on käynnissä seuraavissa yrityksissä: F-Secure Oyj, Vero, Visma Software, LähiTapiola sekä Bonus Way sekä Väestö-rekisterikeskus (tilanne 12.4.2018).

1.2 Minkälaisia haavoittuvuusohjelmia yritykset voivat käynnistää

Erilaisia haavoittuvuusohjelmia ja niiden toteutustapoja on useita. Alla on lueteltu tyypillisimmät haavoittuvuusohjelmat.

1.2.1 Vulnerability Disclosure Policy (VDP)

Organisaatioilla on formaalinen tapa vastaanottaa haavoittuvuustietoja, joita voi lähettää kuka tahansa. Usein tämä tapahtuu lomakkeella tai haavoittuvuustiedot pyydetään lähettämään vapaamuotoisesti esim. security@yritys.fi –osoitteeseen. Toimintatapa on ohjeistettu ISO standardissa 29147.

1.2.2 Bug Bounty Program

Avoin ohjelma, johon voi osallistua kuka tahansa valkohattuinen hakkeri ja mahdollisuus saada vastineeksi rahapalkkioita.

1.2.3 Private Bug Bounty Program

Rajoitettu pääsy organisaation Bug Bounty –ohjelmaan. Tyypillisesti ohjelman omistama taho valitsee ne hakkerit ketkä voivat osallistua haavoittuvuuksien etsintään ja saada vastineeksi rahapalkkioita.

1.2.4 Time-bound Bug Bounty

Ohjelma joka on rajattu aikajaksolle. Tyypillisesti hakkerit kutsutaan mukaan tällaiseen ohjelmaan.

1.3 Haavoittuvuusohjelmien politiikka

Tärkeimpänä haavoittuvuus- ohjelman komponenttina on yrityksen laatima ns. Vulnerability Disclosure Policy. Tässä politiikassa tulee yrityksen määrittää kriittisimmät haavoittuvuus - ohjelman komponentit joita ovat:

- **Lupaus** – Yrityksen johdon lupaus asiakkaille ja kumppaneille asianmukaisen tietoturvallisuuden järjestämiseksi hyödyntämällä Bug Bounty -ohjelmaa
- **Kohteen kuvaus** – mitkä yrityksen järjestelmät, domainit tai web-sivustot ovat kohteena
- **Turvasatama** – hakkereille luvataan, ettei heitä syytetä hakkeroinista mikäli toimivat yrityksen laatiman ohjeistuksen mukaisesti
- **Prosessi** – kuvaus siitä kuinka yritys käsittelee tietoturvatutkijoiden haavoittuvuudet

1.4 Mikä on hakkereiden motiivi ja keitä he ovat?

Raha ei ole valkohattuisten hakkereiden ainoa motiivi, mutta kuitenkin tärkein. Hakkerit haluavat haastaa itsensä ja tekemällä hakkeroinnilla hyvää. Kuulumalla hakkeriyhteisöön, kuten HackerOne, aloittelevat tietoturvatutkijat saavat myös tukea ja opastusta yhteisön jäseniltä.

Yhä useammin nuoret ja taitavat valkohattuiset hakkerit saavat töitä tietoturvayrityksistä ja jatkavat myös bugien metsästystä vapaa-ajallansa.

2 LähiTapiolan Bug Bounty –ohjelman käynnistys ja taustatekijät

Tietojen luottamuksellinen käsittely kuuluu LähiTapiolan ydintehtäviin. Vakuutus- ja rahoituslainsäädäntö sekä henkilötietolaki asettavat henkilötietojen käsittelylle selkeät rajat ja määräävät tietojen salassapidosta. Tämän vuoksi kaikki ICT-järjestelmät testataan tarkasti ennen niiden käyttöönottoa.

LähiTapiola-ryhmään kuuluvissa yhtiöissä käsitellään paljon asiakkaiden tärkeitä henkilötietoja, joten kiinnitämme tietosuojaan erityistä huomiota ja yrityksen olemassaolo perustuu asiakkaiden luottamukseen.

Tavoitteena on, että kuulemme kaikista mahdollisista tietoturvahaavoittuvuuksista palveluissamme. Rahapalkkiota tarjotaan sellaisten tietoturvahaavoittuvuuksien löytämisestä, jotka raportoidaan koordinoidulla ja palkintoohjelman ehtojen mukaisesti.

2.1 Riskiarviointi ja johdon hyväksyntä

Haavoittuvuusohjelman käynnistämisen suunnittelussa on huomiota kiinnitettävä erityisesti riskiarviointiin sekä ylimmän johdon sitouttamiseen. Riskiarvioinnissa on kiinnitettävä huomiota mitkä ovat ohjelmasta saadut hyödyt/vahvuudet sekä mitkä ovat heikkoudet/uhat. LähiTapiola tuotti Bug Bounty –ohjelman riskiarvinnoinnin toukokuussa 2015. Ohjelmasta saatavat hyödyt ja uhkat katsoimme silloin olevan:

2.1.1 Hyödyt

- LähiTapiola edelläkävijä (positiivinen julkisuus/viesti ja erottautuminen muista alan toimijoista)
- Ilmoitusten palkintomalli maltillinen ja vain oikeista/todennetuista havainnoista palkitaan
- Maksamme tuloksista, emme tietoturvatestaamiseen käytetystä ajasta
- Onnistuessaan ja tavoittaessaan riittävän massan, perinteisen yhden testaajan sijasta asiakkaiden järjestelmiä testaa moninkertainen määrä
- Ohjelman kautta LähiTapiola viestittää myös asiakkailleen, että LähiTapiola ottaa tietoturvahaasteet vakavasti ja haluaa tarjota mahdollisimman tietoturvallisesti toteutettuja ja testattuja verkkopalveluita asiakkailleen

2.1.2 Uhkat

- Liian tehokas testaus (käyttäjät tekevät liian tehokasta testausta)
- Järjestelmien kaatuminen/kaataminen
- Internetiin avoimia järjestelmiä vastaan hyökätään joka tapauksessa
- Ilmoitusten määrän massiivinen kasvu, erityisesti kansainvälistyminen
- Ohjelma tuottaa odottamattoman suuren määrän ilmoituksia, aikaa/resursseja tarvitaan ilmoitusten läpikäyntiin, asiakkaan puolella lisää lähinnä tehtävien päätöksien määrää
- Kansainvälisille Bug Bounty –listoille päätyminen – testausvoluumi kasvaa merkittävästi
- Ensivaiheessa ohjelma vain suomenkielellä ja palkitsemismalli maltillinen, osallistujat voidaan rajata (palkitseminen vain todennetuille ja suomenkieliselle lähettäjälle)
- Ohjelma ei tavoita kriittistä massaa, epäkiinnostavuus, pienet palkkiot

2.2 Haavoittuvuusohjelman ohjausryhmä (Bug Bounty Management Team)

Asiakkaille tarjottavien verkkopalveluiden kompleksisuuden vuoksi sekä monitoimittajaympäristön haasteen näkökulmasta perustimme ohjelmaa varten Bug Bounty management team –ryhmän. Ryhmä kokoontuu säännöllisesti ja osallistujia on kaikista tärkeimmistä IT-kumppaneista, jotka kehittävät ja/tai ylläpitävät LähiTapiolan verkkopalveluita. Ryhmä kokoontuu vähintään kerran kuukaudessa ja kokouksissa läpikäydään kaikki uudet sekä avoimet haavoittuvuudet, niiden korjauksen status sekä tehdään tarvittavat työtilaukset nojautuen olemassa oleviin tilausprosesseihin. Ryhmän tehtävänä on myös päättää valkohattuisille hakkereille annettavista palkkioista ja niiden määristä.

2.3 Haavoittuvuusohjelman politiikka ja palkkiomallit

LähiTapiolan Bug Bounty –ohjelman politiikka on julkinen. Politiikka sijaitsee web-osoitteessa: https://hackerone.com/localtapiola

Politiikkamme tarkoituksena on kertoa eettisille hakkereille meidän tapamme toimia bounty markkinoilla. Kerromme avoimesti, miten käsittelemme haavoittuvuudet, milloin maksamme palkkiot ja miten käsittelemme ns. duplikaatit jotka joku on jo aikaisemmin löytänyt. Myös selkeys siitä mitkä eivät ole kohteena tai minkälaisista havainnoista emme maksa palkkioita ovat erittäin tärkeitä tietoja hakkereille.

Ylläpidämme haavoittuvuuspolitiikkaa jatkuvasti ja muutoksia olemme tehneet vuodesta 2015 useita. Vuonna 2016 mm. lisäsimme kolmannen osapuolen komponentteihin (ohjelmakirjastoihin) liittyvien palkkiointien politiikkaa, jossa maksamme tällaista havainnoista 100USD palkkion riippumatta siitä mikä on haavoittuvuuden vakavuus. Tämä siksi, että kolmansien osapuolten ohjelmakirjastoista löytyy haavoittuvuuksia jatkuvasti ja me emme voi vaikuttaa niiden syntymiseen.

Politiikka-sivustolla ylläpidämme tarkkaa tietoa siitä mitkä ovat hakkeroinnin kohteena ja mikä on kohteiden liiketoiminta-arvo LähiTapiolalle. Tämä määrittely tulee siitä kuinka kriittistä informaatiota palvelu sisältää. Sivustolta valkohattuiset hakkerit löytävät aina täsmällisen tiedon, mikäli lisäämme tai poistamme ohjelmamme hakkeroinnin kohteita.

2.4 Miten rakennettaan luottamus hakkereiden keskuudessa

Laadimme vuonna 2016 sisäisen Bug Bounty IR-prosessi- sekä viestintäohjeen. Ohjeistuksessa kuvataan, miten kommunikoimme hakkereiden kanssa, mitä heille voi sanoa ja mitä ei tule sanoa. Alla on otteita viestintäohjeestamme:

- Speak like an engineer would speak to another engineer, i.e., dispense with corporate-speak and cybercyberbulls*it.
- Always be courteous but keep your commentary short.
- Do not use adjectives to describe vulnerabilities (e.g., "bad", "critical", "low" risk). Describe only the technical facts. Instead of "low" risk, talk about risk being accepted

Luottamuksen rakentamisen peruspilareita ovat:

- Maksetaan oikeantasoiset palkkiot haavoittuvuuksista ja perusteluiden on oltava selkeät
- Kommunikointi on oltava nopeaa, selkeää ja suoraviivaista
- Haavoittuvuustietoa ja eri tekniikoita jaetaan hakkereille avoimesti, jotta he voivat kehittyä tietoturvatutkijoina

3 Avaimet menestyksekkään Bug Bounty –ohjelman käynnistämiseen

3.1 Bug Bounty –ohjelman prosessi

Jokaisella yrityksellä on omanlaisensa sovelluskehitysympäristönsä sekä liiketoimintamallinsa. Bug Bounty soveltuu parhaiten yrityksille, joilla on jotain suojattavaa, käsittelevät tai prosessoivat asiakkaiden tietoja julkisissa verkkopalveluissa.

Primäärinä avaimena pidetään yrityksen johdon sitoutumista uudenlaiseen toimintatapaan sekä juristien ymmärrys haavoittuvuusohjelman tarkoitusperästä. Käynnistämällä ohjelman ns. private mallilla yritys voi hallitusti käynnistää haavoittuvuusohjelman ja toimintatapa sisältää vähän riskejä.

Hakkereille maksettavat palkkiot on oltava kiinnostavalla tasolla. Mikäli pääpalkinto sijoittuu 5000-10000EUR välille yritys saa tällöin parhaimpia ja taitavimpia valkohattuisia hakkereita kiinnostumaan ohjelmasta. Vuosibudjetointi kannattaa suhteuttaa niin että se on 2-3 kertaa pääpalkinnon verran.

Ohjelman laadukas pyörittäminen vaatii aina sisäistä organisoitumista. Palveluvaste hakkereille on oltava kohtuullisella tasolla ja palkkioiden maksu löytäjille kannattaa tehdä jo aikaisessa vaiheessa silloin kun bugi on vahvistettu paikkansapitäväksi.

3.2 Haavoittuvuuksien korjaaminen ja palkkioiden maksu

Organisaation avatessa bug bounty –ohjelman haavoittuvuuksia on varauduttava ottamaan vastaan välittömästi käynnistyksen alkuvaiheessa. LähiTapiolan käynnistäessä rajoitetun Private -ohjelman ensimmäisen bugin löytymiseen meni aikaa 1h 7min. Kun siirryimme avoimeen Bug Bounty –ohjelmaan ensimmäiseen raporttiin meni aikaa 46 minuuttia. Avoimessa ohjelmassa ensimmäisen viikon aikana saimme 38 raporttia.

Riippuen palvelun kohteesta voi haavoittuvuuksien korjaus olla nopea prosessi tai korjaamiseen voi mennä huomattavasti aikaakin. Hakkereiden kiinnostavuus ohjelmaa kohtaan pysyy hyvällä tasolla, mikäli korjaukset tehdään nopeasti sekä palkkiot maksetaan samaan aikaan kuin korjaus viedään tuotantoon. Tilanteessa jossa haavoittuvuuden korjaaminen on haasteellinen ja se vie aikaa suositellaan hakkerin palkitseminen tekemään silloin kun haavoittuvuus validoidaan olevan paikkansapitävä.

Vuonna 2015-2016 perustimme isoimpien palkkioiden maksun alla olevan taulukon mukaisesti. Näinä vuosina suurin mahdollinen palkkio oli USD20.000.

Vulnerability	Reward	Comments and Restrictions
• Remote execution of arbitrary code on a server or VM	USD 20.000	Code is running outside a sandbox, but does not need to be root. Basically, an attacker-provided code running on VM as a normal user would suffice.
• Server side database injection or data extraction	USD 10.000	If the database in question is a cache (e.g., key/value cache) that does not hold any personal data or user content, the payment could be reduced. However, database injection already shows a fairly severe bypass of input validation and output encoding, and as such, should be treated as a significant finding (more so as many database query languages are Turing complete).
• Bypassing an authentication or authorisation mechanism (server-side)	USD 10.000	Endpoint device forensics that bypass platform-provided security mechanisms, or methods that rely on an attacker having root or administrator access, do not count.
• A leak of users' personal content without having to interact with victim • Unauthorised altering of another user's content, without having to interact with victim	USD 10.000	For example, stored archival copies of agreements, or email / customer service messages etc. available from the service
• Remote (arbitrary) Code Execution on clients, with SYSTEM / Kernel / root privileges	USD 6.000	A "client" would be a non-browser based client application, e.g., a mobile application. On a client, "remote" means that the vulnerability can be exploited by an

Muutimme vuoden 2017 alussa haavoittuvuuksien arvioinnin ns. ”business impact” analyysiin. Tässä arvioinnissa emme keskity niinkään haavoittuvuuden tekniseen pisteytykseen esim. CVV pisteytykseen (Common Vulnerability Scoring System) vaan haavoittuvuutta arvioidaan niiden riskien mukaan jota haavoittuvuus voi aiheuttaa LähiTapiolan liiketoiminnalle. Tämä valinta on osoittautunut hyväksi ja toimivaksi malliksi.

LähiTapiolan Bug Bounty palkkioiden laskentamalli perustuu yhdeksään (9) eri pääkohtaan jotka ovat:

1. Mikä on haavoittuvuuden ns. impact LähiTapiolan palveluille (Consequence)
2. Koskeeko haavoittuvuus asiakkaitamme ja jos niin kuinka suurta osaa heistä (Customer Scope)
3. Koskeeko haavoittuvuus toimihenkilöitämme ja jos niin kuinka suurta osaa heistä (Branch User Scope)
4. Kuinka montaa järjestelmää haavoittuvuus koskee (System Extent)
5. Vaatiiko haavoittuvuuden hyödyntäminen tunnistautumista palveluumme (Authentication Requirement)
6. Onko haavoittuvuuden hyödyntäminen helppoa vai vaikeaa. Tässä arvioidaan mm. sitä vaatiiko hyödyntäminen minkälaista interaktiota käyttäjän kanssa. (Exploitability)
7. Mikä on hyödyntämisen aikaikkuna. Lasketaanko hyödyntäminen minuuteissa vai rajattomassa aikaikkunassa. (Exploitability Time Frame)
8. Mikä on haavoittuvuudessa hyödynnettävien tietojen arvo LähiTapiolalle. (Data Classification)
9. Onko haavoittuvuus löydetty sellaisesta palvelusta, joka on määritelty Bug Bounty –ohjelmaamme mukaan. (Scope)

Näistä tiedoista muodostetaan arvio palkkiosta hakkerille, joka on tällä hetkellä välillä USD50 – USD50.000.

3.3 Tilastoja LähiTapiolan haavoittuvuusohjelmasta

Bug Bounty –ohjelman olemassaolon aikana olemme maksaneet palkkiota valkohattuisille hakkereille yhteensä $110,861 dollaria (12.4.2018 mennessä). Olemme kiittäneet 162 hakkeria ja maksaneet palkkioita perustuen 225 raporttiin.

Yhteensä 172 korjausta olemme tehneet tietojärjestelmiimme ja keskimääräinen palkkio on ollut $493 dollaria. Vastaamme hakkereille keskimäärin 10 tunnin sisällä yhteydenotosta ja keskimääräinen ratkaisuaika on kaksi kuukautta.

3.4 Avoimuus avainelementtinä

LähiTapiola on linjannut Bug Bounty –ohjelman mahdollisimman avoimeksi. Yhteistyössä hakkereiden kanssa, molempien osapuolten hyväksynnällä, julkaisemme haavoittuvuusraportteja HackerOne –portaalissa. Avoimuus hakkeriyhteistössä ja haavoittuuvuusraporttien julkaiseminen on yksi elementti myös valkohattuisen hakkerin osaamisen kehittämisessä. Raporteissa näkyy yksityiskohtaisesti miten haavoittuvuus on todennettu ja millä tavoin.

HackerOne –portaalin LähiTapiolan profiilisivustolla näkyvät myös palkkioiden maksuun liittyvää statistiikkaa; paljonko olemme maksaneet valkohattuisille hakkereille sekä mikä on palvelumme vasteaika.

4 Haavoittuvuusohjelman hyödyt LähiTapiolalle

4.1 Vaikutukset tietoturvakulttuuriin

Käynnistimme suomalaisvetoisen hakkeriohjelman vuonna syksyllä 2015 ja saimme paljon positiivista mediahuomioita. Siirsimme ohjelmamme kansainväliseksi keväällä 2016. Pitkäjänteinen työ palkittiin loppuvuonna 2017 kun LähiTapiola palkittiin yhdessä Veron sekä Visman kanssa vuoden 2017 kyberpalkinnolla.

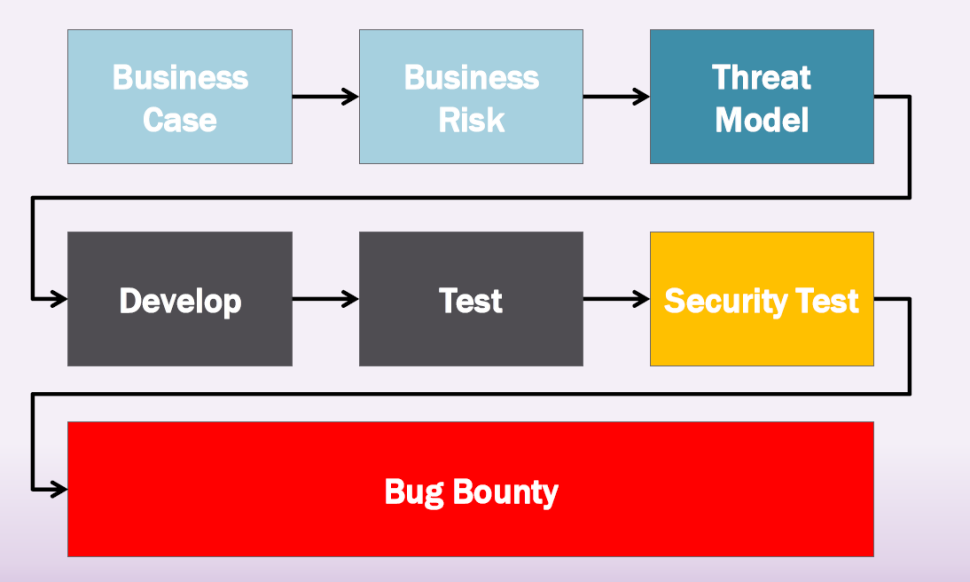
Usein tietoturvallisuus koetaan yrityksessä negatiiviseksi asiaksi ja joskus jopa liiketoiminnan kehityksen hidasteeksi. Bug Bounty –ohjelman kautta tietoturvallisuus on saatu jalkautumaan liiketoiminnan keskuuteen positiivisessa valossa.

4.2 Yrityskuvaan liittyvät muutokset

LähiTapiola investoi huomattavasti palvelujen digitalisointiin ja verkkopalveluiden turvallisuus on oltava erinomaisella tasolla. Haavoittuvuusohjelman alkuvaiheessa havaitsimme kuinka bug bounty –ohjelman kautta saimme positiivista näkyvyyttä suomalaisessa mediassa. Tietoturvallisuuden osalta LähiTapiola on yhä avoimempi ja tällaista toiminta tapaa tukee myös tuleva uusi EU –tietosuoja-asetus. Yritysten on mm. ilmoitettava asiakkaisiin kohdistuneet tietoturvapoikkeamat mahdollisimman pian havainnon jälkeen.

4.3 Muutokset tietoturvatestauksen prosesseihin

Liittoutuminen valkohattuisten hakkereiden kanssa muuttaa erityisesti sovelluskehityksen tietoturvatarkastukseen (pentestaus) liittyviä prosesseja nopeuttaen tietoturvatestauksien läpivientiä huomattavassa määrin. Perinteisessä teknisessä tietoturvatestauksessa testataan palvelun turvallisuus hyvinkin laajamittaisesti ja kestoltaan tämä voi olla useita päiviä. Tietyissä tapauksissa tietoturvatestaus voi estää muun testaamisen ts. palvelu jäädytetään teknisen tietoturvatestauksen ajaksi. Hyödyntämällä valkohattuisia hakkereita voidaan tietoturvatestauksessa tarkistaa vain kriittisimmät palvelun komponentit. Tuotantoon siirron jälkeen (mikäli verkkopalvelu julkaistaan internettiin) valkohattuiset hakkerit jatkavat palvelun turvallisuuden tarkistamista. Tällainen toimintatapa mahdollistaa tietoturvatestauksen rakentamisen mahdollisimman läpinäkyväksi liiketoiminnalle. Valkohattuisille hakkereille maksetaan tuloksista ei käytetystä ajasta



Kuva 1Bug Bounty sovelluskehitysprosessissa (Copyright MintSecurity)

4.4 Haavoittuvuuksien löydökset ja liitokset sovelluskehitykseen

Jatkuva haavoittuvuusohjelman prosessi, missä valkohattuiset hakkerit löytävät bugeja, johtaa jatkuvaan sovelluskehityksen parantumiseen. Mikäli ohjelmistokehittäjät, yhteistyökumppanit sekä palveluiden vastuuhenkilöt liitetään tiiviisti osaksi bug bounty –ohjelmaa sovelluskehityksen laatu tulee parantumaan. Ohjelma on hyvin käytäntöön sijoittuva prosessi ilman standardeja tai tietoturvan prosessimalleja.

LähiTapiola käy säännöllisesti lävitse yhteistyökumppaneiden kanssa palveluista löydetyt haavoittuvuudet, niiden syntymekanismit ohjelmistokehittämisessä sekä miten niitä voidaan jatkossa estää. Tällä jatkuvalla mallilla sovelluskehitys on yhä turvallisempaa muuttuvassa digitaalisessa maailmassa.

LähiTapiolan palveluista löydetyt haavoittuvuudet eivät poikkea globaaleista tilastoista. LähiTapiolan palveluiden TOP löydökset ovat:

- Cross-site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Erilaiset injektiot
- Tietojen vuotamiseen liittyvät haavoittuvuudet
- Istuntojen hallintaan liittyvät haavoittuvuudet
- Konfiguraatiovirheet

4.5 Muutokset liiketoiminnan tietoturvaprosesseihin

Bug Bounty –ohjelma on luonut uuden tavan liiketoiminnan digitaalisten palveluiden turvallisuuden varmistamiseen. Muutos on siirtynyt ehkä hieman kankeasta ja korostuneesta testauksesta joustavaan ja enemmän läpinäkyvään toimintamalliin.

Tietoturvallisuus otetaan huomioon jo alkuvaiheessa, kun liiketoiminta on käynnistämässä uuden palvelumallin tai tuotteen suunnittelua. Olemme luonnollinen osa palvelun elinkaarta aina sen suunnittelusta toteutukseen saakka.

Uhkamallinnus

Kaikki käynnistyvät projektit ja palvelumallit käyvät lävitse uhkamallinnuksen. Hyvin alkuvaiheessa toteutettavassa turvallisuuteen fokusoituvassa uhkamallinuksen työpajassa on osallistujia projektijohdosta, liiketoiminnan sekä ICT projektipäälliköitä, tietoturva-asiantuntijoita sekä digitaalisen palvelun tuottavan yrityksen edustajia. Uhkamallinnuspajassa mallinnetaan ne tärkeimmät riskit, jotka kohdistuvat palveluun. Työpajat ovat kestoltaan 2-3 tuntia ja tärkeimpiä kysymyksiä ovat:

- Käsitelläänkö uudessa palvelussa henkilötietoja?
- Rakennetaanko palvelumalliin maksuväyliä tai suoritetaanko palvelussa rahallisia transaktioita
- Integroidaanko palvelu osaksi LähiTapiolan muita ICT –ratkaisuja vai onko palvelu erillään

Uhkamallinnuksessa keskitytään hyvin tarkasti siihen mitä sisäinen tietoturvatestaus tulee pitämään sisällään. Työpajan lopputuotoksena palvelun tuleva tietoturvatestaaja saa selkeät uhkiin perustuvat askelmerkit lopullisen palvelun testaamiseen.

Tietoturvatestaus

Varsinainen tietoturvatestaus tehdään ulkopuolisen tietoturva-asiantuntijan toimesta. Testauksessa keskitytään työpajassa nousseisiin uhkiin jotka liittyvät henkilötietojen turvaamiseen, turvallisten maksuratkaisujen toteuttamiseen sekä palvelun turvallisesta integroimisesta olemassa oleviin ympäristöihin. Tämän ns. sisäisen tietoturvatestauksen käytettyä aikaa olemme saaneet radikaalisesti vähennettyä, koska testaus kohdistuu primääreihin uhkiin joita palvelussa mahdollisesti voi olla.

Siirto Bug Bounty -ohjelmaan

Mikäli palvelu julkaistaan julkiseen internettiin, käyttöönoton yhteydessä sovitaan palvelun siirrosta LähiTapiolan Bug Bounty –ohjelmaan. Tyypillisesti uusi domain lisätään LähiTapiolan haavoittuvuusohjelmaan noin 14 päivän jälkeen tuotantoon siirrosta. Tieto julkaistaan hakkereille HackerOne –portaalissa.

5 Johtopäätökset

Niiden kokemuksien perusteella mitä LähiTapiolalla on Bug Bounty –ohjelmista voidaan ohjelman käynnistymistä suositella, mikäli tietyt ehdot toteutuvat. Nämä ovat kuvattuna kappaleessa 3.1.

Erityistä huomiota tulee kiinnittää yrityksen johdon ottamisesta suunnitteluun mukaan hyvinkin alkuvaiheessa. Tarkka argumentointi, riskianalyysi sekä hyödyt (yrityskuva, kustannustehokkuus euroina tms.) on tuotava selkeästi esille. Tällä hetkellä Suomesta saa hyvin apua ja osaamista haavoittuvuusohjelman suunnitteluun, käynnistämiseen ja ylläpitämiseen.

Parhaimmillaan Bug Bounty –ohjelman pyörittäminen antaa kaikille osapuolille uskomattomia tarinoita ja hienoja kokemuksia.

”Happy hacking and hack for good!”