Riku Ylönen

Pelikonsoleiden verkkopalveluiden tietoturvauhat

Tietotekniikan kandidaatintutkielma

3. tammikuuta 2020

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Riku Ylönen

Yhteystiedot: riku.j.ylonen@studentjyu.fi

Ohjaaja: Tytti Saksa

Työn nimi: Pelikonsoleiden verkkopalveluiden tietoturvauhat

Title in English: Security threats to game consoles web services

Työ: Kandidaatintutkielma

Sivumäärä: 18+0

Tiivistelmä: Tutkielman tavoitteena on eritellä pelikonsoleiden verkkopalvelujen tietoturvauhkia ja hyökkäyksiä. Pelikonsoleiden käytön yleistymisen myötä myös hyökkäyksistä niitä kohtaan on tullut kiinnostavampia ja tuottoisampia. Tutkielmassa käsitellään tietoturvauhkatyyppejä sekä 2011 ja 2014 tapahtuneita hyökkäyksiä PlayStation Networkiin ja Xbox Liveen. Hyökkäykset olivat toteutettu käyttäen hajautettua palvelunestohyökkäystä (DDoS) ja SQL-injektiota. Verkkopalveluissa esiintyy useita haavoittuvuuksia eikä kaikkia hyökkäyksiä pystytä estämään. Verkkopalveluiden tietoturvallisuutta on mahdollista kuitenkin kehittää ja vaikka kaikkia hyökkäyksiä ei voida täysin estää, niiden vaikutusta voidaan lieventää.

Avainsanat: PSN, Xbox Live, DDoS-hyökkäys, SQL-injektio, verkkopalvelu

Abstract: The objective of this thesis is to study between security threats and attacks on game console web services. With the increasing use of game consoles, attacks on them have also become more interesting and lucrative. The paper deals with the types of security threats as well as the 2011 and 2014 attacks on PlayStation Network and Xbox Live. The attacks were implemented using distributed denial of service attack (DDoS) and SQL injection. There are many vulnerabilities in web services and not all attacks can be prevented. However, the security of web services can be improved and although not all attacks can be completely prevented, their impact can be mitigated.

Keywords: PSN, Xbox Live, DDoS attack, SQL injection, web service

Sisältö

1 Johdanto

Konsolipelaaminen on yleistynyt viime vuosina. Nykyään konsolipelaaminen ei ole enää pelkästään yksinpelaamista, vaan siitä on tullut myös sosiaalinen tapahtuma. PlayStation -pelaajat voivat pelata joko toisiaan vastaan tai yhdessä muita vastaan, sekä pelaajat voivat kommunikoida keskenään esimerkiksi puhumalla mikrofonien välityksellä. Jotta konsolipelejä pystyisi pelaamaan kavereiden kanssa paikasta riippumatta, pitää muutaman edellytyksen toteutua. Itsestään selvien edellytysten, kuten internetin omistuksen lisäksi pelaajien pitää kuulua kyseisen konsolin verkkopalveluun, jotta verkkopelaaminen olisi mahdollista. Sonyn verkkopalvelun aktiivisten käyttäjien määrä on noussut 10 miljoonan vuositahtia muutaman vuoden ajan (Statista 2019b). Suuri käyttäjämäärä houkuttelee myös väärinkäyttäjiä ja rikollisia. PlayStation Networkiin ja Xbox:n Xbox Live-verkkopalveluun onkin kohdistunut useita hyökkäyksiä.

Tässä tutkielmassa luku 2 käsittelee pelikonsoleiden verkkopalveluita ja tarkemmin käsitellään PlayStation Network ja Xbox Live-verkkopalvelua. Luvussa 3 kerrotaan verkkopalveluihin kohdistuvista turvallisuusuhista, kuten palvelunestohyökkäyksestä ja SQL-injektiosta. Luvussa 4 tarkastellaan jo aiemmin sattuneita hyökkäyksiä verkkopalveluita kohtaan. Lopuksi luvussa 5 tehdään yhteenveto tutkielman pääkohdista.

2 Pelikonsoleiden verkkopalvelut

Verkkopalvelu on yksinkertaisen määritelmän mukaan sovellus, jonka avulla voidaan käyttää muita sovelluksia verkossa. Karkeasti määriteltynä lähes kaikki asiat, joilla on URL-osoite ovat verkkopalveluita (Alonso ym. 2004). Perusedellytys verkkopalveluille on, että tiettyjä protokollia käyttäen voidaan verkon välityksellä tarjota pala koodia etäkoneiden saataville. Verkkopalveluiden sana verkko, viittaa keinoihin, joilla päästään käsiksi toiminnallisuuksiin. Sana palvelu viittaa siihen, että toimintoihin päästään niin, ettei tarvitse ladata tai asentaa koodia. Verkkopalveluita voidaan kuvata palveluntarjoajan ja kuluttajan välisenä suhteena (Apshankar ym. 2002).

2.1 PlayStation Network (PSN)

Vuonna 2006 julkaistu Sony PlayStation Network (PSN) on pelikonsoli PlayStationin verkkopalvelu, joka yhdistää miljoonia konsolipelaajia ympäri maailman (Milburn 2018). PSN:ssä oli maaliskuussa 2019 noin 94 miljoonaa kuukausittaista aktiivista käyttäjää (Statista 2019b). PSN antaa mahdollisuuden käyttäjälle jakaa pelissä pelaamalla saatuja saavutuksiaan ja ennätyspisteitä muille käyttäjille sekä jakaa pelivideoita muiden käyttäjien saataville. Pelaamisen seurantaa varten pelikonsolin täytyy olla kytkettynä internetiin sekä pelaajalla täytyy olla Sonyn pilvipalveluiden käyttöoikeus (Davies ym. 2015).

Maksullinen PS Plus-jäsenyys mahdollistaa verkkomoninpelin (Milburn 2018). PS Plus sisältöön kuuluvat lisäksi esimerkiksi käyttäjäprofiilit ja ryhmäviestit (Davies ym. 2015). PS Plus -tilauspalvelulla oli 2018 vuoden lopussa hieman yli 38 miljoonaa käyttäjää (Statista 2019b). PlayStation Store on online-kauppa ja sieltä on mahdollista ostaa muun muassa pelejä. PS Storessa on myös laaja valikoima Sonyn ja yhteistyökumppaneiden tarjoamia viihdepalveluja (Milburn 2018). PSN-tilillä pitää olla henkilötiedot sekä maksutiedot, jolloin verkkoselaimella katsottuna PSN-tili paljastaa käyttäjän oikean nimen, osoitteen, luotto- tai maksukorttitiedot, tapahtumahistorian sekä linkitetyt laitteet.

2.2 Xbox Live

Microsoftin Xbox Live -verkkopalvelu on julkaistu vuonna 2002. Verkkopalvelussa oli vuoden 2019 alussa 64 miljoonaa kuukausittaista aktiivista käyttäjää (Statista 2019a). Xbox Live käyttäjätili on sama kuin Microsoftin käyttäjätili, joten käyttäjä tarvitsee vain yhdet kirjautumistunnukset. Jokaisella pelaajalla on oma pelaajaprofiili, johon kuuluu nimimerkki (gamertag), joka luodaan, kun kirjaudutaan ensimmäisen kerran Xbox-konsolilta Xbox Live-palveluun. Gamertag on enintään 15 merkkiä pitkä ja se on yksilöllinen. Xbox Live-jäsenyys on ilmainen ja siihen kuuluu useita ominaisuuksia (Qualls 2019). Xbox Live Marketplace-kauppa on suositusjärjestelmä, jonka avulla käyttäjä voi tutkia sisältöä, joka on tehty suositusalgoritmin mukaan. Suositusjärjestelmä suosittelee käyttäjille pelejä ja elokuvia (Koenigstein ym. 2012).

Gamertagin avulla eri pelaajia voi etsiä Xbox Live-verkkopalvelusta, sekä lisätä muita käyttäjiä ystäväluetteloon. Pelissä saavutettuja saavutuksia on mahdollista vertailla gamertagien kesken, mutta käyttäjät pystyvät myös itse rajaamaan, ketkä pystyvät näkemään käyttäjän oman pelihistorian. (Jakobsson 2011). Xbox Live on ilmainen palvelu, mutta käyttäjän on mahdollista ostaa Xbox Live Gold-taso. Xbox Live Gold-tason merkittävimmät erot ilmaiseen Xbox Live-tasoon ovat, että Gold-tason pelaajat pystyvä pelaamaan verkkopelejä muiden käyttäjien kanssa. Gold-taso tarjoaa pelaajille lisäksi jäsenetuja sekä kuukausittain vaihtuvia ilmaisia pelejä (Qualls 2019). Xbox Live Gold-palvelu tarjoaa hyvän tavan pelata kavereiden kanssa. Palvelu on suosittu tapa pitää yllä online-ystävyyksiä sekä solmia uusia ystävyyssuhteita (Ledbetter 2012).

3 Verkkopalveluiden tietoturvauhkatyyppejä

Verkkopalveluista on tullut suosittuja, koska ne ovat helppokäyttöisiä ja verkkopalveluiden alustat ovat riippumattomia. Toisaalta nämä ominaisuudet altistavat verkkopalvelut useille eri tietoturvauhkille, koska silloin myös merkityksellinen data on kaikkien saatavilla (Vorobiev ja Han 2006). Verkkopalveluilla on paljon käyttäjiä, joten se tekee verkkosivustoista ja niiden käyttäjistä houkuttelevia kohteita hyökkäyksille. Yksi kriittisimmistä turvallisuusuhkista verkkosivustoille ovat dynaamiset ja vuorovaikutteiset hyökkäykset, kuten injektiohin perustuvat hyökkäykset (Huang ym. 2017). Myös The Open Web Application Security Project (OWASP) julkaiseman tietoturvauhkalistauksen mukaan vakavimpina uhkina ovat injektiohyökkäykset. Muita verkkopalveluiden turvallisuusuhkia ovat OWASP listauksen mukaan väärät määritykset turvallisuudelle, käyttäjille asetetut liian löysät rajoitukset sekä autentikointiin liittyvät toteutusvirheet (OWASP 2017).

3.1 Hajautettu palvelunestohyökkäys

Palvelunestohyökkäyksen (Denial of service, DoS) tarkoituksena on se, että hyökkääjä kohdistaa hyökkäyksen palvelimen resursseihin, jolloin resurssit eivät ole käyttäjien saatavilla. Palvelunestohyökkäyksessä hyökkääjä lähettää useita pyyntöjä uhreille eli kohdepalvelimille, tarkoituksenaan se, ettei palvelin pysty palvelemaan oikeita käyttäjiä. Palvelunestohyökkäys voidaan suorittaa mm. kaatamalla palvelin, kaatamalla reititin, tai ylikuormittamalla verkkoa suurella liikenteellä (Karre 2013).

Hajautetussa palvelunestohyökkäyksessä (Distributed denial of service, DDoS) hyökkääjä hyökkää koordinoidusti yhtä aikaa käyttäen DoS-hyökkäystä. DDoS hyökkäyksessä on yksi todellinen hyökkääjä eli isäntä, sekä jokin määrä hyökkääviä agentteja, zombeja. Isäntä on vastuussa zombien hallinnasta ja antaa zombeille komentoja, joita zombit tottelevat. Zombit luovat todellisen hyökkäyksen ja ovat vastuussa liikenteestä. Mitä useampi hyökkääjä, sitä vaikeampaa uhrin on havaita hyökkäys (Karre 2013).

DDoS-hyökkäysten tunnistamiseksi havaitsemisjärjestelmän pitäisi pystyä erottamaan hyökkäysliikenne normaalista verkkoliikenteestä (Karre 2013). Palvelunestohyökkäysten torju-

miseen sekä tunnistamiseen voidaan käyttää koneoppimista ja tilastollisia menetelmiä. On useita tilastollisia DDoS-hyökkäysten havaitsemismekanismeja, mutta useilla havaitsemismekanismeilla on kaksi suurta puutetta. Tilastollisten havaitsemismekanismien puutteet liittyvät korrelaation mittaamiseen. Korrelaation mittaaminen aiheuttaa suuren laskennallisen ajan DDoS-hyökkäyksen tunnistamiseen, joten se ei pysty tunnistamaan hyökkäystä reaaliaikaisesti. Toinen ongelma liittyy korrelaation mittausmenetelmiin, sekä korrelaatiokertoimen tarkkuuteen. Reaaliaikainen DDoS-hyökkäyksen havaitseminen vaatii minimimäärän toimintoja käytettäväksi, kun analysoidaan verkkoliikennettä. Korrelaatioon perustuva hyökkäyksen havaitseminen vaatii saataville enemmän toimintoja kuin mitä reaaliaikainen torjunta mahdollistaa. Koska toimintoja ei ole tarpeeksi käytettävissä, hyökkäyksen havaitsemistodennäköisyys ei ole korkea (Hoque, Kashyap ja Bhattacharyya 2017).

Korrelaatio on tilastollinen menetelmä, joka mittaa kahden tai useammin asian välistä lineaarista yhteyttä. Korrelaatio voi vaihdella -1 ja 1 välillä. Korrelaatio -1 tarkoittaa täydellistä negatiivista riippuvuutta, korrelaatio 0 tarkoittaa, ettei asioiden välillä esiinny riippuvuutta ja 1 tarkoittaa täydellistä positiivista riippuvuutta. Korrelaatiokertoimia on kahta päätyyppiä, Spearmanin järjestyskorrelaatiokerroin ja Pearsonin tulomomenttikorrelaatiokerroin. Pearsonin korrelaatiokerroin soveltuu parhaiten normaalijakautuneille muuttujille. Spearmanin korrelaatiokerroin soveltuu muuttujille, jotka poikkeavat normaalijakaumasta. Korrelaatiokerrointyypin valinta riippuu mitattavien muuttujien tyypeistä (Mukaka 2012). Pearsonin korrelaatiokerroin voidaan laskea seuraavasti:

$$\rho_{X,Y} = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_x \sigma_y}$$

jossa X ja Y ovat satunnaismuuttujia ja tulokseksi saadaan $\rho_{X,Y}$, joka ilmaisee X ja Y välistä korrelaatiota. μ_X ja μ_Y ovat odotusarvoja sekä σ_X ja σ_Y ilmaisevat X:n ja Y:n keskihajonnat (Thapngam ym. 2011).

NaHiD-metodi mittaa korrelaation lähes samanlailla kuin Pearsonin korrelaatiokerroin, mutta toisin kuin Pearsonin korrelaatiokerroin, NaHiD-metodi laskee objektien absoluuttisen etäisyyden toisistaan. NaHiD-metodi on tehokkaampi kuin Pearsonin ja Spearmanin mittausmenetelmät, kun mitataan kahdesta satunnaista otoksesta, joissa parametrit vaihtelevat

vähän.

$$NaHiD(_{X,Y}) = 1 - \frac{1}{n}\sum_{i=1}^{n} \frac{|\, x(i) - y(i) \,|}{||\, meanX - \sigma_X \,| - X(i) \,| + ||\, meanY - \sigma_Y \,| - Y(i) \,|}$$

jossa $NaHiD(_{X,Y})$ on muuttujien X ja Y välinen korrelaatio. X ja Y ovat muuttujia ja meanX on muuttujan X keskiarvo sekä meanY on muuttujan Y keskiarvo. σ_X on muutujan X keskihajonta ja σ_Y on muuttujan Y keskihajonta (Hoque, Kashyap ja Bhattacharyya 2017).

3.2 SQL-injektio

SQL eli Structured Query Language on tekstikieli, jota käytetään vuorovaikutuksessa relaatiotietokantojen kanssa (Anley 2002). SQL-injektio on haavoittuvuus, jolle altistutaan, kun annetaan hyökkääjälle mahdollisuus vaikuttaa SQL-kyselyyn. Huonosti rakennettuun tietokantakyselyyn lisätään haitallisia osia, jotka suoritetaan normaalin kyselyn yhteydessä. SQL-injektion toteuttamiseen vaaditaan, että sovellus ei tarkasta tai puhdista käyttäjän syötteitä (Clarke 2012). SQL-injektiotyyppejä ovat muun muassa loogisesti virheelliset kyselyt, tautologiaan perustuvat kyselyt sekä UNION-hyökkäys (Kanchana ja Sarala 2012). UNION-operaattoria käyttämällä hyökkääjän on mahdollista saada kaikki haluamansa tieto tietokannasta. Virheellisiin kyselyihin pohjautuva SQL-injektio perustuu virheviesteihin, joita tietokantapalvelin lähettää. Tietokantapalvelimen lähettämät virheviestit sisältävät tietoja tietokannan rakenteesta. (Voitovych ja Yuvkovetskyi 2016) Tautologiaan perustuvassa SQL-injektiossa tavoite on injektoida koodi yhteen tai useampaan ehdolliseen lauseeseen, jotta lauseen paluuarvo on lopulta aina tosi. Yleisin tavoite tautologiaan perustuvassa SQL-injektiossa on autentikointisivujen ohittaminen (Halfond, Viegas ja Orso 2006).

Kirjautuessaan palveluun käyttäjä yleensä kirjoittaa web-palvelun tekstikenttään käyttäjänimen ja salasanan. Jos syötetyt arvot löytyvät tietokannasta, niin käyttäjä pääsee kirjautuneena palveluun. Jos syötettyjä arvoja ei löydy tietokannasta, niin pääsy evätään. Hyökkääjällä on myös mahdollista syöttää tietoja erityisillä symboleilla, jotka voivat vahingoittaa tietokannan logiikkaa tai rakennetta. Jos hyökkääjä pystyy suorittamaan mielivaltaisia kyselyitä, on hyökkääjällä mahdollisuus poistaa, lisätä ja muokata tietokannan tietoja. SQL-injektio on mahdollista, koska SQL-kyselyiden syötteitä ei tarkasteta tai ne jätetään suodattamatta (Voitovych ja Yuvkovetskyi 2016).

(McClure, Scambray ja Kurtz 2012) esittävät kirjassaan esimerkkejä syötteistä, joiden avulla SQL-injektio on mahdollista toteuttaa, jos sovellus on haavoittuvainen:

1. Kirjautuminen ilman tunnuksia
    - Käyttäjänimi: *’ OR ''=’*
    - Salasana: *’ OR ’''=’*
2. Kirjautuminen käyttäen vain käyttäjänimeä
    - Käyttäjänimi: admin’--
3. Kirjautuminen fiktiivisenä käyttäjänä
    - Käyttäjänimi: ’ union select 1, ’user’,
    - ’passwd’ 1-

4 Verkkopalveluihin kohdistuneet hyökkäykset

Verkkopalveluihin kohdistuvat hyökkäykset voivat kohdistua asiakkaan tietoihin tai verkkopalvelun saatavuuteen. Tietomurto tapahtuu, kun ulkopuoliset pääsevät verkkopalvelussa olevan asiakkaan henkilökohtaisiin tietoihin käsiksi. Palvelussa olevat häiriöt ilmenevät, kun verkkopalvelun asiakkaat joutuvat odottamaan pitkään sivujen latautumista tai palvelu on kaatunut (Goode ym. 2017). Hyökkäyksiä tapahtuu jatkuvasti, sillä on vaikeaa, ellei mahdotonta kirjoittaa haavoittumatonta koodia (Huang ym. 2017). Huang ym. (2017) mukaan Symantecin viimeisin Internet Security Threat raportti esittää, että päivittäin tapahtuu yli 229 000 verkkosivustoihin kohdistuvaa hyökkäystä ja yli 76 prosentilla verkkosivustoista on havaitsemattomia haavoittuvuuksia.

4.1 Vuoden 2011 hyökkäys

Vuonna 2011 PSN:stä tuli taistelukenttä yritysten IP-käytäntöjen ja hakkereiden välillä, mikä johti lopulta suureen hyökkäykseen Sonyn tietokantoihin (Milburn 2018). Huhtikuussa 2011 tapahtui hyökkäys Sonyn PSN:iin (Cachin ja Schunter 2011). Sony ei aluksi ollut tietoinen hyökkääjien murtautumisesta tietokantoihin, joten hyökkääjät ehtivät kerätä rekisteröityjen käyttäjien henkilökohtaisia tietoja (Milburn 2018). Hyökkääjät pääsivät käsiksi käyttäjien oikeisiin nimiin, salasanoihin, kotiosoitteisiin, ostohistoriaan sekä luottokorttinumeroihin. Pahin peliyhteisöä koskenut tapahtuma johti 77 miljoonan ihmisen tietojen ja näistä 12 miljoonan ihmisen luottokorttitietojen paljastumiseen (Armerding 2017). Välittömät kustannukset Sonylle olivat arvion mukaan noin 171 miljoonaa yhdysvaltain dollaria ja analyytikoiden mukaan epäsuorat kustannukset olivat yli miljardi dollaria (Goode ym. 2017).

Ennen varsinaista tietomurtoa hyökkääjät olivat useita kertoja kohdistaneet DDoS-hyökkäyksen Sonyn palvelimiin ja saaneet Sonyn palvelimet kaadettua. Sonyn tietokantoihin päästiin lopulta käsiksi SQL-injektiolla. Hyökkääjät ilmoittivat päässeensä yhdellä injektiolla käsiksi aivan kaikkiin tietoihin (Martin 2011). Vuoden 2011 hyökkäys herätti keskustelua Sonyn palomuurien teknisistä ominaisuuksista, palvelinarkkitehtuurista ja salausstandardeista (Milburn 2018). Vuoden 2011 hyökkäyksen raportit kertovat, että hyökkääjät olivat antaneet

etukäteisvaroituksen järjestelmän haavoittuvuudesta. Raportit siitä, että hyökkääjät pystyvät helposti saamaan arkaluontoista tietoa, vahvistaa väitettä, että Sony olisi voinut suojautua paremmin ja varautua ennalta hyökkäyksiin (Sullivan 2016).

4.2 Vuoden 2014 hyökkäys

Vuoden 2014 lopulla Sony koki erilaisia häiriöitä ja lopulta siihen kohdistui verkkohyökkäys 24. päivä marraskuuta 2014. Hyökkäyksessä Sony Pictures Entertainment:n (SPE) tietokoneiden näytölle ilmestyi neonvärinen luuranko ja useita yrityksen kiintolevyjä tyhjennettiin (Haggard ja Lindsay 2015). Myös Xbox Live joutui hyökkäyksen kohteeksi. Hakkeriryhmä nimeltä Lizard Squad käytti DDoS-hyökkäystä PSN ja Xbox Live-palveluita vastaan. Hyökkäys tukki verkon niin, että oikeat käyttäjät eivät päässet käyttämään verkkopalveluita (Thurrott 2014). Vuoden 2014 hyökkäys oli ainutlaatuinen toteutukseltaan ja vaikutuksiltaan (Sullivan 2016). Useita päiviä myöhemmin hyökkääjät alkoivat jakaa tiedostoina internetissä Sonyn elokuvia sekä yksityisiä tietoja, kuten yhtiön sisäisiä sähköpostiviestejä, elokuvasopimuksia ja työntekijöiden terveystietoja. Hyökkääjät jakoivat tiedostoja pienissä erissä viikkojen ajan (Haggard ja Lindsay 2015). Sonyn työntekijöiden luottokortti- ja pankkitiedot tulivat julkisiksi ja niitä käytettiin vilpillisesti. Vuoden 2014 hyökkäys Sonya vastaan oli kuitenkin enemmän kuin rikollinen teko tai murto yksityisyyttä vastaan. Hyökkäys oli isku koko Yhdysvaltojen valtiota vastaan. Muutamat asiantuntijat uskovat, että vuoden 2014 hyökkäykseltä Sony ei olisi voinut suojautua mitenkään (Sullivan 2016).

4.3 Tietoturvauhkatyyppien ilmeneminen hyökkäyksissä

Tässä alaluvussa käsittelen PlayStationin ja Xboxin verkkopalveluihin kohdistuneita hyökkäyksiä sekä miten luvussa 3 esitetyt tietorurvauhat ilmenevät hyökkäyksissä. Käsittelemäni hyökkäykset toteutuivat vuosina 2011 ja 2014. Tietoturvauhkatyypeistä esiintyi useimmin hajautettu palvelunestohyökkäys eli DDoS. Verkkopalveluihin kohdistui myös injektiohyökkäyksiä kuten SQL-injektio.

Vuosien 2011 ja 2014 hyökkäyksistä tai niiden teknisestä toteutuksesta ei ole yksityiskohtaista tietoa, koska Sony ei kerro niistä paljoa vedoten turvallisuussyihin. Hyökkäysten to-

teutuksista voidaan tehdä vain edistyneitä arvauksia (Anthony 2011). Hakkeriryhmä LulzSec ilmoitti hyökänneensä SonyPictures.com sivustoon eli Sonyn tytäryhtiöön SQL-injektiolla. LulzSec ilmoitti saaneensa pääsyn yhtiön kaikkiin tiedostoihin (Martin 2011). On mahdollista, että PSN kohtaan käytettiin täysin samantyyppistä hyökkäystä kuin SonyPicturesiin. Vuonna 2011 Sony kohtasi useampia hyökkäyksiä, jotka kohdistuivat PSN:iin. On kuitenkin vaikea todistaa, että PSN kohtasi SQL-injektio hyökkäyksen, vaikka se näyttää hyvin todennäköiseltä (Horner ja Hyslip 2017).

Hakkeriryhmä Lizard Squad väitti olevansa vastuussa vuoden 2014 hyökkäyksestä ja käyttäneensä DDoS-hyökkäystä kaataen Xbox Liven ja PSN:in. Hyökkäys ylikuormitti palvelun, jolloin käyttäjät eivät päässeet käyttämään palvelua (Martin 2011). Sony ei itse suoraan maininnut DDoS-hyökkäystä, mutta mainitsi epäsuorasti hyökkäyksestä vuoden 2014 blogitekstissään. Blogissa kerrottiin, että PSN on yritetty kaataa vaikuttamalla siihen keinotekoisella hyvin suurella verkkoliikenteellä (PlayStation.Blog 2014).

5 Yhteenveto

Sonyn verkkopalvelun PSN:n tietoturvallisuus ei ole ollut sillä tasolla, mitä niin suuren yrityksen tietoturvallisuudelta voitaisiin odottaa. Tästä kertovat 2011 ja 2014 toteutetut hyökkäykset. Xbox Live -verkkopalvelun tietoturva on todennäköisesti ollut paremmalla tasolla, kun hyökkäysten vaikutukset eivät ole olleet läheskään yhtä suuret kuin PSN:llä. Hyökkäykset aiheuttivat suuret taloudelliset ja imagolliset tappiot Sonylle ja sitä kautta vaikuttivat käyttäjien luottamukseen. Hyökkäykset heikentävät herkästi pelaajien luottamusta verkkopalveluun ja osa saattaa lopettaa verkkopalvelun käyttämisen ja siirtyä käyttämään muiden yritysten verkkopalveluja. Lisäksi hyökkäysten salailu ja heikko tiedottaminen hyökkäysten etenemisestä on omiaan heikentämään luottamusta yritykseen. Kiinnostava kysymys on se, kuinka Sony on reagoinut hyökkäyksiin ja kuinka se on yrittänyt parantaa haavoittuvuuksia. Epäilemättä Sony on ottanut opikseen hyökkäyksistä, mutta minkälaisia parannuksia Sony on tehnyt verkkopalveluunsa, siitä ei ole saatavilla julkista tietoa.

Verkkopalvelujen tietoturvallisuuteen liittyy paljon tunnistamattomia sekä tunnettuja uhkia. Tunnetut uhat voivat muuttaa muotoaan tai kehittyä, joten puolustautuminen uhkia vastaan edellyttää jatkuvaa kehitystyötä. Uhkiin varautumiseen kuuluu uhkien priorisointi. Uhkiin pitäisi varautua niin, että todennäköisyyksiltään ja vaikutuksiltaan suuret uhkat olisivat priorisoitu korkealle, esimerkiksi varautuminen SQL-injektiohyökkäyksiin tulisi priorisoida korkealle. Priorisointi voi johtaa siihen, että vaikutuksiltaan vähäisimmät hyökkäykset voivat todennäköisesti onnistua.

Reaaliaikainen hajautetun palvelunestohyökkäyksen havaitseminen on osoittautunut ongelmalliseksi. Luvussa 3.1 esitetty NaHiD-havaitsemismetodi on tarkempi kuin Pearsonin korrelaatiokertoimeen perustuva metodi, mutta sekään ei vielä ole tarpeeksi tehokas. Tulevaisuudessa olisi hyvä kehittää havaitsemismetodeja tarkemmiksi.

Kaikkia hyökkäyksiä ei voida estää, mutta tulevaisuuden haasteita on pyrkiä minimoimaan vaikutuksia sekä pystyä reagoimaan nopeasti erilaisiin hyökkäyksiin, joita ei välttämättä edes vielä tunneta. Uhkiin varautuminen on jatkuvaa työtä.

Lähteet

Alonso, Gustavo, Fabio Casati, Harumi Kuno ja Vijay Machiraju. 2004. *Web Services: Concepts, Architectures and Applications.* Springer.

Anley, Chris. 2002. *Advanced SQL Injection In SQL Server Applications.* Saatavilla WWW-muodossa, `https://crypto.stanford.edu/cs155old/cs155-spring06/sql_injection.pdf`, viitattu 28.12.2019.

Anthony, Sebastian. 2011. *How the PlayStation Network was Hacked.* Saatavilla WWW-muodossa, `https://www.extremetech.com/gaming/84218-how-the-playstation-network-was-hacked` viitattu 29.12.2019.

Apshankar, Kapil, Henry Chang, Mike Clark, Eduardo B. Fernandez, Peter Fletcher, Whitney Hankison ja et al. 2002. *Web Services Business Strategies and Architectures.* Springer.

Armerding, Taylor. 2017. "The 16 biggest data breaches of the 21st century". *Computerworld Hong Kong; Newton.*

Cachin, Christian, ja Matthias Schunter. 2011. "A cloud you can trust". *IEEE Spectrum* 48:28–51.

Clarke, Justin. 2012. *SQL injection attacks and defense.* Elsevier.

Davies, Matthew, Huw Read, Konstantinos Xynos ja Iain Sutherland. 2015. "Forensic analysis of a Sony PlayStation 4: A first look". Teoksessa *Digital Investigation vol. 12, Supplement 1,* 81–89. Elsevier. doi:`10.1016/j.diin.2015.01.013`.

Goode, Sigi, Hartmut Hoehle, Viswanath Venkatesh ja Susan Brown. 2017. "User Compensation as a Data Breach Recovery Action: An Investigation of the Sony PlayStation Network Breach". *MIS Quarterly* 41:703–727.

Haggard, Stephan, ja Jon Lindsay. 2015. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace". *AsiaPacific Issues* 117:1–8.

Halfond, William, Jeremy Viegas ja Alessandro Orso. 2006. “A Classification of SQL Injection Attacks and Countermeasures”. *College of Computing Georgia, Institute of Technology:* 1–11.

Hoque, N, H Kashyap ja D.K Bhattacharyya. 2017. “Real-time DDoS attack detection using FPGA”. Teoksessa *Computer Communications vol. 110,* 48–58. Elsevier. doi:10.1016/j.comcom.2017.05.015.

Horner, Matthew, ja Thomas Hyslip. 2017. “SQL INJECTION: THE LONGEST RUNNING SEQUEL IN PROGRAMMING HISTORY”. *The Journal of Digital Forensics, Security and Law : JDFSL* 12:97–107.

Huang, Hsiu-Chuan, Zhi-Kai Zhang, Hao-Wen Cheng ja Shiuhpyng Winston Shieh. 2017. “Web Application Security: Threats, Countermeasures, and Pitfalls”. *Computer* 50:81–85.

Jakobsson, Mikael. 2011. “The Achievement Machine:: Understanding Xbox 360 Achievements in Gaming Practices”. *Game Studies. The international journal of computer game research* 11.

Kanchana, Natarajan, ja Subramani Sarala. 2012. “Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks”. Teoksessa *Computer Communications vol. 110,* 790–796. Elsevier. doi:10.1016/j.protcy.2012.05.129.

Karre, Santhosh Kumar. 2013. “Distributed Detection of DDoS Attack”. Teoksessa *International Journal of Future Computer and Communication vol. 2, no. 6,* 628–632. IJFCC. doi:10.1109/WIFS.2016.7823917.

Koenigstein, Noam, Nir Nice, Ulrich Paquet ja Nir Schleyen. 2012. “The Xbox recommender system”. *RecSys ’12: Sixth ACM Conference on Recommender Systems* 1:281–284.

Ledbetter, Jeffrey, Andrew Kuznekoff. 2012. “More Than a Game: Friendship Relational Maintenance and Attitudes Toward Xbox LIVE Communication”. Teoksessa *Communication Research vol. 39, issue 2,* 269–290. Sage. doi:10.1177/0093650210397042.

Martin, Adam. 2011. “LulzSec’s Sony Hack Really Was as Simple as It Claimed”. *The Atlantic* September 22, 2011.

McClure, Stuart, Joel Scambray ja George Kurtz. 2012. *Hacking exposed 7 : network security secrets solutions.* McGraw-Hill cop. 2012.

Milburn, Colin. 2018. *Respawn: Gamers, Hackers, and Technogenic Life.* Durham: Duke University Press.

Mukaka, MM. 2012. "A guide to appropriate use of Correlation coefficient in medical research". *Malawi Medical Journal* 24(3):69–71.

OWASP. 2017. *OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks.* Saatavilla WWW-muodossa, `https://www.owasp.org/images/7/72/OWASP_Top_10-2017_(en).pdf.pdf` viitattu 28.12.2019.

PlayStation.Blog. 2014. *Update: PlayStation Network is Back Online.* Saatavilla WWW-muodossa, `https://blog.us.playstation.com/2014/08/24/playstation-network-update-2/` viitattu 29.12.2019.

Qualls, Eric. 2019. *What Is Xbox Live (Previously Xbox Silver)?* Saatavilla WWW-muodossa, `https://www.lifewire.com/what-is-xbox-live-silver-3563184`, viitattu 28.12.2019.

Statista. 2019a. *Number of monthly active users (MAU) of Microsoft Xbox Live from fiscal 1st quarter 2016 to 2nd quarter 2019.* Saatavilla WWW-muodossa, `https://https://www.statista.com/statistics/531063/xbox-live-mau-number/`, viitattu 27.11.2019.

———. 2019b. *Number of PlayStation Network users 2014-2019.* Saatavilla WWW-muodossa, `https://www.statista.com/statistics/272639/number-of-registered-accounts-of-playstation-network/`, viitattu 27.11.2019.

Sullivan, Clare. 2016. "The 2014 Sony hack and the role of international law". *Journal of National Security Law Policy* 8:1–27.

Thapngam, Theerasak, Shui Yu, Wanlei Zhou ja Gleb Beliakov. 2011. "Discriminating DDoS attack traffic from flash crowd through packet arrival patterns". *The First International Workshop on Security in Computers, Networking and Communications:* 952–957.

Thurrott, Paul. 2014. “Hacker Group Takes Down Xbox Live, PSN”. *Windows IT Pro (Online)* Dec 8, 2014.

Voitovych, O.P., ja O.S. Yuvkovetskyi. 2016. “SQL Injection Prevention System”. *2016 International Conference "Radio Electronics InfoCommunications"(UkrMiC):* 1–4.

Vorobiev, Artem, ja Jun Han. 2006. “Security Attack Ontology for Web Services”. Teoksessa *2006 Semantics, Knowledge and Grid, Second International Conference.* IEEE. doi:10.1109/SKG.2006.85.