Matias Ruonala, Miro Hintikka, Ville Schulz, Joel Simola

Tietoturva web-sovelluksissa

Metropolia Ammattikorkeakoulu

Alaantutustumistehtävä

Raportti

21.9.2023

Sisällys

Sisällysluettelo

1 Johdanto 3

2 Web sovellus ympäristönä 3

2.1 Mikä on web-sovellus? 3
2.2 Web-sovelluksen hyödyt ja haitat 4

3 Yleisimmät web-sovellusten tietoturvauhat 4

3.1 Kolme suurinta web-sovelluksen haavoittuvuutta 5
3.1.1 Viallinen valtuuksien tarkistus (Broken Access control) 5
3.1.2 Epäonnistuneet salausmenetelmät (Cryptographic failures) 5
3.1.3 Injektio (Injection) 6
3.2 Tietoturvan huomiointi sovelluskehityksessä 7

4 Toimenpiteet tietomurron tapahtuessa 7

4.1 Etukäteen suoritettavia toimenpiteitä 7
4.2 Tietomurron havaitseminen 8
4.3 Tietomurron jälkeisiä toimenpiteitä 8

5 Käyttäjän vastuu tietoturvasta 9

5.1 Tietoturvan ylläpito 10
5.2 Minkä takia tietoturvasta huolehtiminen on tärkeää? 10
5.3 Arkielämän esimerkki huonosta tietoturvasta 11

6 Yhteenveto 11

Lähteet 13

1 Johdanto

Tämä raportti on kirjoitettu osana viestinnän kurssin alaantutustumistehtävää. Olemme tutustuneet web-sovellusten toimintaan tietoturvan näkökulmasta ja tässä dokumentissa kerromme, mitä olemme aiheesta oppineet.

Toinen luku esittelee mikä web-sovellus on, miten se on pääpiirteissään rakennettu, ja mitä hyötyjä ja haittoja web-sovelluksella on natiiviin mobiilisovellukseen verrattuna.

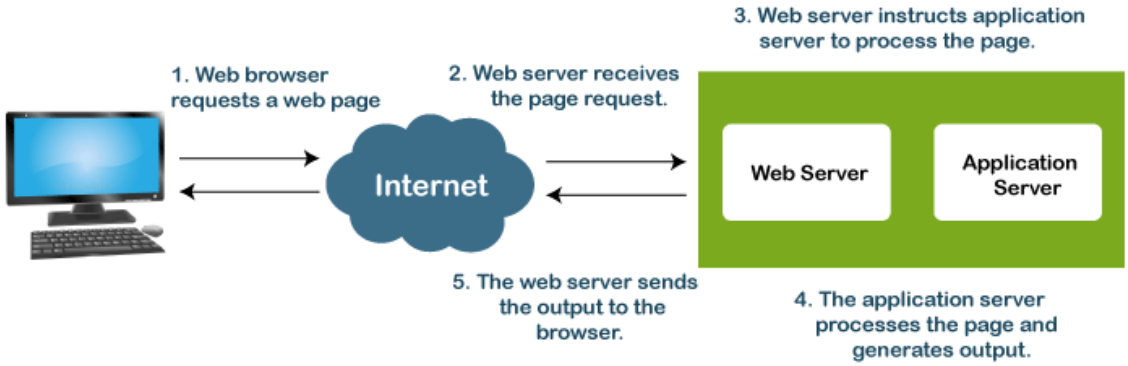
Kolmas luku kuvailee yleisimpiä web-sovelluksiin kohdistuvia tietoturvauhkia ja miten niitä tulee huomioida sovellusta kehittäessä. Neljännessä luvussa kerrotaan, miten tietomurron aiheuttamat haittavaikutukset voidaan pitää mahdollisimman pieninä.

Viides ja viimeinen luku esittelee, miten käyttäjä voi omilla toimillaan vaikuttaa tietoturvan tasoon. Viimeisenä kerromme lyhyesti Psykoterapiakeskus Vastaamon tietomurrosta esimerkkinä siitä, miten minkään järjestelmän tai sovelluksen ei tulisi tietoturvaansa toteuttaa.

2 Web sovellus ympäristönä

2.1 Mikä on web-sovellus?

Web-sovellus on verkkopalvelimella suoritettava ohjelmisto, jota käyttäjä ohjaa verkkoselaimellaan (1). Sovelluksen käyttäjää lähellä oleva osa, niin sanottu frontend, on verkkosivu. Frontend vastaanottaa käyttäjän syötteen ja näyttää käyttäjälle halutun sisällön. Palvelinpuoli eli backend koostuu verkkopalvelinosasta sekä sovelluspalvelinosasta. Backend huolehtii asiakaspyyntöjen käsittelystä, laskennasta sekä tiedonhallinnasta ja tallentamisesta. Kuva 1 esittelee tyypillisen web-sovelluksen rakenteen ja toiminnallisen järjestyksen karkeasti. (2)



Kuva 1: Web-sovelluksen rakenne ja sovelluskulku (3)

2.2 Web-sovelluksen hyödyt ja haitat

Koska web-sovellusta voi käyttää internet-selaimella, se ei ole laitteistoriippuvainen. Toisin sanoen riittää, että ohjelmistokehittäjä suunnittelee yhden ohjelmiston ja käyttöliittymän, mitä voi käyttää millä tahansa laitteella ja käyttöjärjestelmällä, jossa on asennettuna moderni verkkoselain (1). Web-sovelluksen tuotantokustannukset ovat matalammat, kuin esimerkiksi natiivisovellusten, jotka räätälöidään joka alustalle erikseen (4).

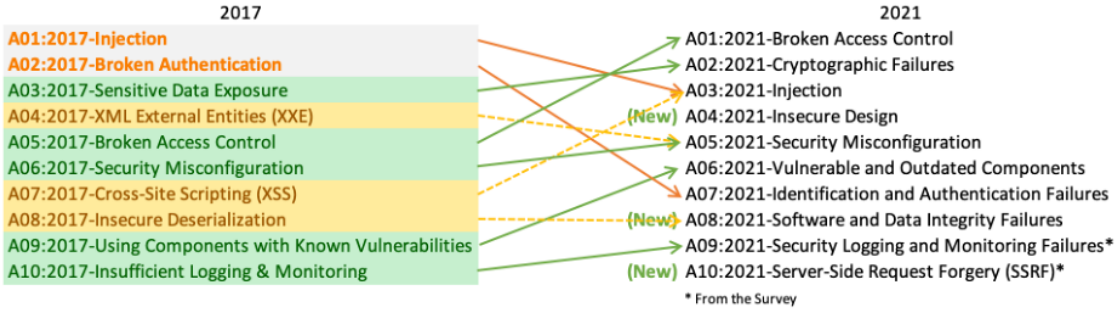
Web-sovelluksen käytettävyys internetin yli on myös yksi sen suurista heikkouksista. Ne ovat alttiita monenlaisille verkkohyökkäyksille, mistä kerromme seuraavassa luvussa enemmän.

3 Yleisimmät web-sovellusten tietoturvauhat

Web-sovelluksiin kohdistuu nykypäivänä monia erilaisia uhkia, joita vastaan yritykset joutuvat taistelemaan päivittäin. Tätä voisi ajatella eräänlaisena kissa ja hiiri -leikkinä. Kun uusi haavoittuvuus löydetään, pitää se paikata mahdollisimman nopeasti ilman, että siitä aiheutuu suurta vahinkoa yritykselle tai yrityksen asiakkaille. (5)

3.1 Kolme suurinta web-sovelluksen haavoittuvuutta

The Open Worldwide Application Security Project, eli OWASP, on voittoa tavoittelematon yhdistys, joka työskentelee parantaakseen sovelluksien tietoturvaa. Yhdistys on koonnut vuoden 2021 yleisimpiä haavoittuvuuksia listaksi, joka näkyy alla. (6; Kuva 2)



Kuva 2: OWASP top-10 tietoturvahaavoittuvuudet 2017 ja 2021 (6)

3.1.1 Viallinen valtuuksien tarkistus (Broken Access control)

Valtuuksien tarkistus valvoo, ettei web-sovelluksen käyttäjä pysty ylittämään hänelle myönnettyjä oikeuksiaan. Viallinen valtuuksien tarkistus voi antaa käyttäjälle luku- tai muokkausoikeuden luvattomiin tietoihin. Tältä voi välttyä oikeanlaisella suunnittelulla ohjelman kehityksen alkuvaiheessa. Käyttäjälle kannattaa myöntää vain ne oikeudet, jotka ovat sovelluksen toiminnan kannalta välttämättömiä.

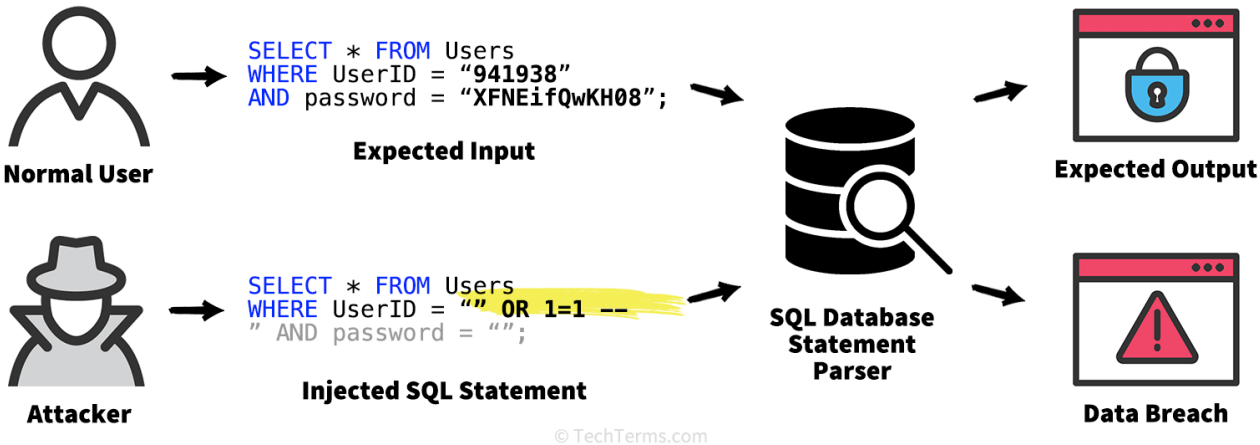
3.1.2 Epäonnistuneet salausmenetelmät (Cryptographic failures)

Tiedon salaamista salakirjoitusmenetelmin on käytetty jo muinaisen Egyptin ja Rooman ajoista asti, mutta tietokoneiden aikana salakirjoitusjärjestelmät ja niiden tutkimus on edistynyt huomattavasti. Salakirjoitusmenetelmää käytetään useissa sovelluksissa, esimerkkinä mainittakoon pankkisovellukset ja pikaviestimet. (7)

Epäonnistuneilla salausmenetelmillä tarkoitetaan tiedon huonoa salausta esimerkiksi vanhentuneella salausalgoritmilla tai salauksen puuttumista kokonaan. Tähän kehittäjä voi vaikuttaa muistamalla salata arkaluontoisen tiedon säilyttäessään sekä siirtäessään sitä. Sovelluskehittäjän tulee myös käyttää ajantasaista tiedonsiirtoteknologiaa ja huolehtia, etteivät evästeet tallenna arkaluontoista tietoa. (8)

3.1.3 Injektio (Injection)

Injektiohyökkäyksistä yleisimmät ovat SQL-injektio, NoSQL-injektio ja object-relational mapping, lyhyemmin ORM (9). Structured query language, eli SQL, on kyselykieli, jota käytetään ohjelmoinnissa tietokantoihin tallennettun tiedon hakemiseen. SQL-injektio kuuluu yhteen vanhimmista verkkosovellushaavoittuvuuksista. Se on hyökkäys, jossa virheellisellä käyttäjäsyötteellä hyökkääjä voi ujuttaa SQL-kyselyjä verkkosovellukseen, ja saa siten pääsyn tietokannan tietoihin. Mitä keskitetympää tieto on, sitä pahempaa jälkeä injektiohyökkäykset saavat aikaan. Näitä hyökkäyksiä vastaan voidaan suojautua esimerkiksi käsittelemällä käyttäjän syötettä ennen kuin sillä haetaan tietoja verkkosivuston käyttämästä tietokannasta. (10; Kuva 3)



Kuva 3: SQL-injektio havainnollistettuna (11)

3.2 Tietoturvan huomiointi sovelluskehityksessä

Web-sovelluksissa käytettävät teknologiat kehittyvät koko ajan. Uusia ominaisuuksia lisätään vanhoihin web-sovelluksiin yritysten vaatiessa niiltä jatkuvasti enemmän. Kehittäjät ovat vielä toistaiseksi ihmisiä ja biologinen evoluutio ei ole mitenkään pysynyt teknologisen kehityksen vauhdissa. On täysin tavallista, että uuden projektin lähdekoodiin jäisi virheitä, jotka saattavat vaarantaa sovelluksen tietoturvan. Yleensä ohjelmistokehittäjän työ ei ole täysin uuden sovelluksen luomista, vaan jonkun aikaisemman kehittäjän kirjoittaman sovelluksen ylläpitoa. Alkuperäinen sovellus on saatettu kirjoittaa huomioimatta sen tulevaa päivitettävyyttä tai aikana, jolloin tietoturvakysymyksiä ei osattu ottaa kunnolla huomioon. Tämän takia tietoturvallista sovellusta voi olla vaikea toteuttaa ilman, että muutokset rikkovat olemassa olevia toimintoja tai yritykselle kriittisiä laitteita. (12)

Vaikka sovelluksen kehittäjä huomioisi kaikki web-sovellusten tunnetut haavoittuvuudet, se ei aina riitä suojautumaan tietomurroilta. Luvussa neljä käsittelemmekin toimenpiteitä, miten tietomurron vaikutuksia voidaan minimoida.

4 Toimenpiteet tietomurron tapahtuessa

Tietomurto on luvaton tunkeutuminen tietojärjestelmään, palveluun, laitteeseen tai sovelluksen luvatonta käyttöä kaapattujen tunnuksien avulla (13, s. 2). Web-sovellus voi joutua tietomurron uhriksi kaikista tietoturvan toimenpiteistä huolimatta, joten web-sovelluksen kehittäjän on syytä osata oikeat toimenpiteet tietomurron vahinkojen rajoittamiseksi.

4.1 Etukäteen suoritettavia toimenpiteitä

Osa toimenpiteistä täytyy tehdä jo ennen mahdollista tietomurtoa, jotta niistä olisi hyötyä tietomurron aiheuttamien vahinkojen korjaamisessa (13, s. 3).

Varmuuskopio on kopio web-sovelluksen tärkeimmistä tiedoista ja järjestelmistä. Varmuuskopio voidaan tehdä esimerkiksi web-sovellukselle kriittisestä

SQL-tietokannasta. Tietomurrossa murtautuja saattaa varastaa, tuhota tai muuten tärvellä web-sovelluksen tietoja tai järjestelmiä. Varmuuskopion avulla varastetut, tuhotut tai tärvellyt tiedot ja järjestelmät voidaan palauttaa nopeasti ja tehokkaasti tietomurron jälkeen. Ainakin osa varmuuskopioista on syytä pitää irti verkosta, jolloin ne eivät ole uhattuna tietomurron tapahtuessa. Lisäksi varmuuskopioiden palauttamista kannattaa kokeilla säännöllisesti, jotta toimenpide onnistuu, kun sille on todellinen tarve. (15, s.11; 5 s. 2)

Loki on aikajärjestyksessä kirjattu tallenne tapahtumista. Yleisiä lokeja ovat esimerkiksi tapahtumalokit ja muutoslokit. Lokien avulla pystytään seuraamaan web-sovelluksen toimintaa normaalitilanteessa ja tietomurron sattuessa lokeja voidaan käyttää murron selvittämiseen. Lokeja käyttämällä voidaan esimerkiksi havaita tietomurto, selvittää tietomurron ajankohta ja mihin murtautuja pääsi käsiksi. Koska lokitiedot ovat tärkeitä tietomurtojen selvittämisessä, on pidettävä huolta siitä, että mahdollinen murtautuja ei kykene muokkaamaan niitä. (5, s. 3, 16)

4.2 Tietomurron havaitseminen

Tietomurto täytyy ensin havaita ennen kuin sille voidaan tehdä mitään. Tietomurto voidaan havaita monilla eri tavoilla. Tapoja ovat esimerkiksi epäkohdat web-sovelluksen toiminnassa, lokeista havaitaan epäilyttävää toimintaa, jokin kolmas osapuoli kertoo murrosta tai murtautuja ottaa itse yhteyttä kiristämistarkoituksessa, mistä kerromme esimerkin raportin lopussa kappaleessa 5.3. (5, s. 5, 13).

4.3 Tietomurron jälkeisiä toimenpiteitä

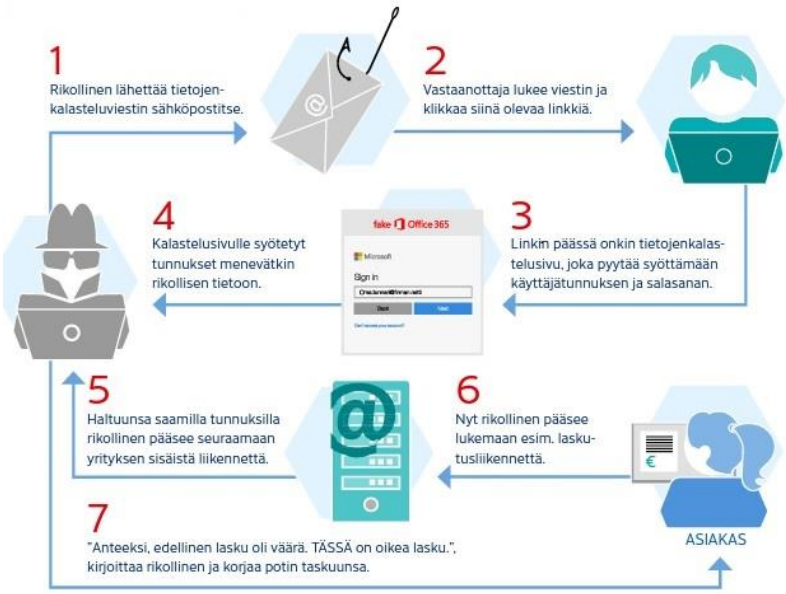
Tietomurron jälkeen on tärkeää ryhtyä toimenpiteisiin, jotta murron vaikutukset voidaan rajoittaa ja vahingot minimoida. Ensin täytyy eristää tietomurron saastuttama järjestelmä, jotta murtautuja ei pysty käyttämään sitä hyökkäyksen edistämiseen. Murtautuja ei pysty hallitsemaan järjestelmää tai varastamaan sieltä tietoja, jos järjestelmän internet-yhteys on katkaistu. Eristetystä järjestelmästä

aloitetaan tietomurron laajuuden selvittäminen käyttämällä kerättyjä lokitietoja. Tietomurrosta on syytä tehdä ilmoitus ryhmille, joita tietomurto koskettaa. Jos tietomurrossa on murtautujan käsiin päätyneitä henkilötietoja, on tietomurrosta ilmoitettava välittömästi tietosuojavaltuutetulle. (5, s. 6–9)

Saastuneesta järjestelmästä kerätään tunnistetiedot, joiden avulla järjestelmän saastuneet osat voidaan tunnistaa. Tunnistetietoja ovat esimerkiksi lokeista saatavat tapahtuma-ajat ja saastuneen järjestelmän verkkoliikenne. Mahdolliset vääriin käsiin päätyneet tunnukset ja salasanat pitää estää tai muuttaa, jotta murtautuja ei voi käyttää niitä tulevaisuudessa. Kun kaikki saastuneet osat ovat tunnistettu, järjestelmä siivotaan haittaohjelmista ja murtautujan jättämistä takaovista. Siivouksen jälkeen aloitetaan järjestelmän palauttaminen normaaliin toimintaan käyttämällä varmuuskopioita. (5, s. 10–13)

5 Käyttäjän vastuu tietoturvasta

Suurimman tietoturvauhan muodostaa käyttäjä itse. Käyttäjä voi omilla teoillaan vaikuttaa käytöstä aiheutuviin riskeihin. (17) Tämän takia yrityksiä suositellaan järjestämään tietoturvakoulutuksia, joissa opastetaan käyttäjät toimimaan oikein. Traficom on luonut tätä varten yritysten johdolle oman oppaan tietotuvallisuudesta. (18) Alla olevassa kuvassa esimerkki siitä kuinka esimerkiksi websovelluksen käyttäjä voi huolimattomuudellaan aiheuttaa isoakin vahinkoa.



Kuva 4: Esimerkki käyttäjän aiheuttamasta tietoturvariskistä. (18)

5.1 Tietoturvan ylläpito

Yksi tärkeimmistä suojautumiskeinoista on riittävän monimutkainen salasana, joka yhdistelee kirjaimia, numeroita ja erikoismerkkejä (19). Sovellusten viimeisimpien päivityksien lataaminen on suositeltavaa, sillä niillä pyritään paikkaamaan ohjelmistosta löytyviä tietoturva-aukkoja. Monivaiheinen tunnistautuminen yhdistettynä edellä mainittuun on yksi tehokkaimmista suojauskeinoista, mitä käytetään esimerkiksi pankkisovelluksissa ja muissa henkilökohtaisissa palveluissa. Oman sähköpostiosoitteen ja muiden henkilökohtaisten tietojen luovuttamisesta kannattaa olla tarkkana, sillä niiden joutuminen vääriin käsiin voi aiheuttaa tietoturvariskin. (20)

5.2 Minkä takia tietoturvasta huolehtiminen on tärkeää?

Monelle saattaa tulla yllätyksenä, kuinka paljon heillä on menetettävää, kun tulee kysymykseen henkilökohtainen tietoturva ja sen murtuminen. Murtautuja voi käyttää henkilökohtaisia laitteita sekä käyttäjän omaa internet-yhteyttä muihin vahingollisiin tekoihin. Pahimmassa tapauksessa uhri menettää omaisuutensa, identiteettinsä tai muutoin arkaluontoisia tietoja voi päätyä vääriin käsiin. Myös maine saattaa olla uhattuna, jolloin vahinkojen korjaaminen voi osoittautua erittäin hankalaksi ja niillä voi olla pitkäkantoiset jälkiseuraukset. (21) Alla oleva kuva selventää mitä kaikkea tulisi ottaa huomioon, kun halutaan parantaa yksilön tietoturvaa.

Kuva 5: 13 vinkkiä parempaan tietoturvaan (21)

5.3 Arkielämän esimerkki huonosta tietoturvasta

Vuosina 2018–2019 tapahtunut Psykoterapiakeskus Vastaamon tietovuoto on hyvä esimerkki erittäin huonosti toteutetusta tietoturvasta. Siinä ulkopuolinen pääsi käsiksi asiakkaiden huonosti suojattuihin henkilökohtaisiin tietoihin, joita hän koitti myöhemmin käyttää kiristyksen välineenä. Kiristäjä vaati 200–500 euroa uhreilta, jotta hän ei julkaisisi tietoja julkisesti. (22) Potilastiedot kuitenkin julkaistiin osittain internetin pimeillä markkinoilla eli Tor-verkossa, mahdollisesti vahingossa (23). Varastettujen tietojen määräksi vahvistettiin elokuussa 2023 yhteensä 33086 kpl (24). Kiristäjä väitti kirjautuneensa tietokantaan oletuskäyttäjätunnuksella ja -salasanalla. Lisäksi Vastaamon ”Potilasrekisteri”-niminen alasivu on ollut löydettävissä Google-haulla ja potilasrekisteriin liittyvä tietokantaportti oli auki avoimesta verkosta tuleville yhteyksille. (25) Tapaukselta olisi voinut mahdollisesti välttyä, jos Vastaamon järjestelmän olisi ohjelmoinut ammattilainen eikä yrityksen toimitusjohtaja, joka on itseoppinut ohjelmoija. Potilastiedot olisi pitänyt tallentaa pseudonymisoituna niin, että tietokannassa olevien henkilötietojen avulla ei voisi päätellä asiakkaan oikeaa henkilöllisyyttä. (22)

6 Yhteenveto

Web-sovellukset ovat erittäin haavoittuvia ulkoisille verkkohyökkäyksille juuri etäkäyttöominaisuuksiensa takia. Muun muassa alustariippumattomuuden sekä matalien tuotantokustannusten takia web-sovellukset ovat kuitenkin suosittuja.

Web-sovellusta kehittäessä täytyy huolehtia riittävästä tietosuojasta ja sovelluksen tietoturvaominaisuudet on pidettävä ajan tasalla. Uusia haavoittuvuuksia kuitenkin löydetään ja mikään järjestelmä ei ole täysin vedenpitävä. Siksi tietomurtoihin pitää varautua ja tietomurron laajuus sekä sen aiheuttamat seuraukset on pidettävä mahdollisimman vähäisinä esimerkiksi aktiivisen tietoliikenneseurannan sekä nopean reagoinnin avulla.

Vaikka sovelluksen kehittäjä tai palveluntarjoaja ei juuri kykene vaikuttamaan käyttäjästä aiheutuviin tietoturvariskeihin, ei niiden merkitystä tule väheksyä. Jokaisen henkilön vastuulla on huolehtia omasta tietoturvastaan, ja organisaatioiden intresseissä on kouluttaa työntekijöistään vastuullisia verkonkäyttäjiä. Käyttäjän huolimattomuus voi johtaa suuriinkin tietovuotoihin.

Toimiva tietoturva on näkymätöntä, mutta kuten Vastaamon tapauksesta opimme, sen murtuminen koskettaa meitä kaikkia.

Matias Ruonala kirjoitti johdannon, yhteenvedon ja esittelyn web-sovelluksista (luku 2). Miro Hintikka kirjoitti web-sovellusten haavoittuvuuksista (luku 3). Joel Simola kirjoitti tietomurtoihin varautumisesta sekä toimista, mihin ryhtyä tietomurron tapahtuessa (luku 4). Ville Schulz esitteli Vastaamon surullisenkuuluisan tietomurron sekä käsitteli käyttäjän vastuuta tietoturvassa (luku 5).

Lähteet

1 https://www.britannica.com/topic/Web-application 22.9.2023

2 https://www.techtarget.com/searchsoftwarequality/definition/Web-application-Web-app 22.9.2023

3 https://www.javatpoint.com/web-application 30.9.2023

4 https://www.geeksforgeeks.org/advantages-and-disadvantages-of-web-app-development/ 22.9.2023

5 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/TietomurtoToimintaohje.pdf 1.10.2023

6 OWASP https://owasp.org/www-project-top-ten 21.03.2023

7 Veikko Siivola Salakirjoituksen historia https://www.cs.helsinki.fi/u/kerola/tkhist/k2000/alustukset/salakirjoitus/crypto.html 24.09.2023

8 OWASP https://owasp.org/Top10/A02_2021-Cryptographic_Failures/ 1.10.2023

9 OWASP https://owasp.org/Top10/A03_2021-Injection/#description 21.09.2023

10 NordVPN https://nordvpn.com/fi/blog/sql-injektio/ 21.09.2023

11 https://techterms.com/definition/sql_injection 24.09.2023

12 Secarma blogi kirjoitus https://secarma.com/software-security-a-developers-point-of-view-part-one/ 22.09.2023

13 https://www.comptia.org/blog/log-data-key-to-identifying-cybersecurity-threats 28.9.2023

14 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf 26.9.2023

15 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-keraat-ja-kaytat-lokitietoja 26.9.2023

16 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-suojaudut-tietomurroilta 25.9.2023

17 https://www.sttinfo.fi/tiedote/69882446/vaitos-562020-ihminen-on-tietoturvan-heikoin-lenkki-vestman?publisherId=69817172 22.9.2023

18 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf 25.9.2023

19 https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-2-suojautuminen-uhkatekijoilta/salasanojen-turvallinen-kaytto/ 23.9.2023

20 https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla 24.9.2023

21 https://materiaalit.triuvare.fi/artikkelit/mita-jokaisen-toimitusjohtajan-tulee-tietaa-tietoturvasta 25.9.2023

22 https://yle.fi/a/3-11613667 29.9.2023

23 https://yle.fi/a/3-11616210 29.9.2023

24 https://www.aamulehti.fi/rikos/art-2000009757940.html selattu 30.9.2023

25 https://www.hs.fi/kotimaa/art-2000006702821.html 30.9.2023