TIETOTURVAUHAT JA NIIDEN MERKITYS YRITYKSELLE

Johanna Hakonen

Sisällysluettelo

1 Johdanto

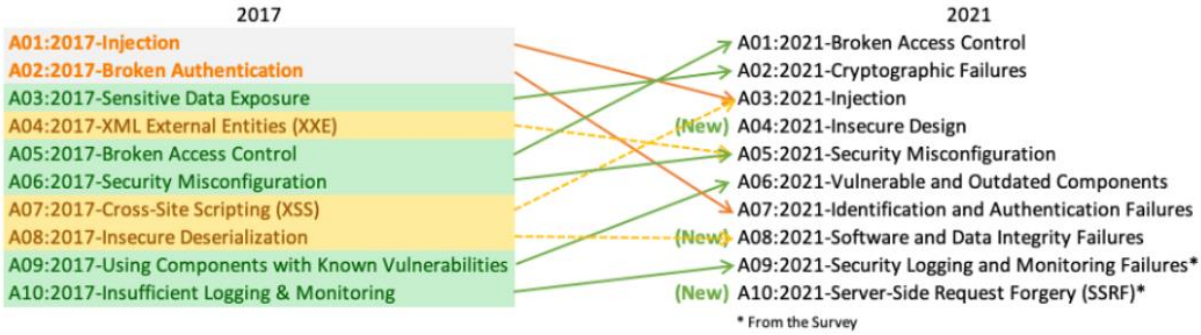
Asiakasyritys on fiktiivinen fysioterapiakeskus Physio, jonka hoitohenkilökunnan määrä on viisi ja tietohallinnosta vastaa yksi henkilö. IT-ympäristö sisältää Windows-palvelimen ja -työasemia ja Active Directoryn. Yrityksellä on Physio-verkkosivut ajanvarausta varten ja Kanta-palveluun liitetty potilastietojärjestelmä. Yrityksessä käsitellään terveydenhuollon asiakas- ja potilastietoja. Tässä pohditaan tämän hetken yleisimpiä ja kriittisimpiä tietoturvauhkia ja niiden aiheuttamia riskejä Physiolle.

2 Yleisimmät ja kriittisimmät tietoturvauhat

Kyberturvallisuuskeskuksen Pienyritysten kyberturvallisuusoppaan (Kyberturvallisuuskeskus, 2025) mukaan yleisimmät kyberuhat ovat tietojenkalastelu, haittaohjelmat ja kiristyshaittaohjelmat. ChatGPT (OpenAI, 2025) listaa myös haittaohjelmat (esim. kiristyshaittaohjelmat), tietojenkalastelu, käyttäjätunnusten ja salasanojen murrot, sisäpiiriuhat (huolimattomuus tai tietoinen vahingonteko), päivitysten ja haavoittuvuuksien hallinnan laiminlyönti sekä IoT-laitteiden tietoturvariskit.

OWASP Foundationilta (The Open Worldwide Application Security Project) on tulossa tämän vuoden 2025 Top 10 -lista web-sovellusten tietoturvariskeistä, edelliset ovat vuosilta 2017 ja 2021 (Kuva 1) (OWASP, 2025). Vuonna 2021 yleisimpiä olivat rikkinäinen käyttöoikeuksien valvonta, kryptografiset

viat, injektiot, ei-turvallinen suunnittelu ja virheelliset tietoturva-asetukset. Physio-web-sovelluksen haavoittuvuudet voivat johtaa asiakastietojen varastamiseen ja tuhoamiseen tietokannasta.



Kuva 1. 10 Suurinta web-sovellusten tietoturvariskiä.

2.1 Tietojenkalastelu

Tietojenkalastelussa työntekijä saa viestin, joka näyttää tulevan tutulta henkilöltä tai organisaatiolta (Kyberturvallisuuskeskus, 2025). Rikollinen on voinut myös murtaa jonkin toisen käyttäjän tilin ja viesti voi tulla oikeasti tutusta paikasta. Haitallisia linkkejä on myös sosiaalisessa mediassa tai internetsivustoilla. Työntekijältä yritetään saada luottamuksellista tietoa, kuten tunnuksia tai luottokortin numeroa. Physiossa tunnuksia voidaan käyttää asiakas- ja potilastietojen varastamiseen, josta seuraa GDPR-sanktioita, toimintahäiriöitä ja mainehaittaa.

2.2 Haittaohjelmat

Haittaohjelmilla aiheutetaan harmia, kuten varastetaan ja salataan tärkeää tietoa, kuten pankkitunnuksia tai salasanoja, louhitaan luvatta virtuaalivaluuttaa tai seurataan tietokoneen käyttäjän toimintaa (Kyberturvallisuuskeskus, 2025). Myös näin voi Physion asiakas- ja potilastietoja päätyä vääriin käsiin.

2.3 Kiristyshaittaohjelmat

Kiristyshaittaohjelma pääsee tietokoneelle usein aidolta näyttävän sähköpostiviestin mukana, jossa on linkki tai liitetiedosto (Kyberturvallisuuskeskus, 2025). Ohjelma salaa ja varastaa tiedostot ja rikollinen lupaa poistaa salauksen maksua vastaan. Physiolla tämäkin merkitsisi asiakas- ja potilastietojen menetystä.

Lähdeluettelo

Kyberturvallisuuskeskus. (23. Maaliskuu 2025). *Pienyritysten kyberturvallisuusopas*. Noudettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

OpenAI. (17. Maaliskuu 2025). *ChatGPT*. Noudettu osoitteesta chatgpt.com

OWASP. (23. Maaliskuu 2025). *OWASP Top Ten*. Noudettu osoitteesta https://owasp.org/www-project-top-ten/