SALAUSMENETELMÄT

Johanna Hakonen

Sisällysluettelo

1 Johdanto

Vertailtiin eri salausmenetelmiä ja valittiin fysioterapiakeskus Physioon tarkoituksenmukaiset salausmenetelmät ChatGPT:n avulla (OpenAI, 2025). Yritys käsittelee henkilö- ja terveystietoja, joten niiden suojaaminen on tärkeää.

Varaussivusto on vasta kehitysvaiheessa, sivuja testataan Render-palvelussa (https://physio.onrender.com), johon on yhdistetty Githubista physio-web-pages-tietovarasto (https://github.com/hannahakonen/physio-web-pages) ja asiakastietokanta on MongoDB Atlas -palvelussa.

2 Salausmenetelmät

2.1 Tallennettavan datan salaus

Asiakastietojen salaukseen sopisi BitLocker, joka on Windowsin salausohjelma, jolla voidaan suojata työasemien ja palvelimen koko levy. Avain varmuuskopioidaan Active Directory Domain Services (ADDS) -hakemistopalveluun (Microsoft, BitLocker, 2025). Bitlocker käyttää oletuksena XTS-AES 128-bittistä salausmenetelmää.

Lisäksi Windowsin tiedostojen salausjärjestelmällä (Encrypting File System, EFS) voi salata yksittäisiä tiedostoja ja kansioita. Siinä käytetään asymmetristä salausta (Microsoft, File Encryption, 2025).

MongoDB Atlas -tietokantapalvelu käyttää AES-256-salausta datan turvaamiseen (MongoDB, 2025).

2.2 Tiedonsiirron salaus

Verkkoliikenne tulee suojata TLS-salausprotokollalla (Transport Layer Security), joka on käytössä jo ajanvaraussivujen kehitysvaiheessa Githubissa sekä Render- ja MongoDB Atlas-palveluissa, jotka toimivat HTTPS-protokollalla.

VPN-yhteyttä (Virtual Private Network) tulisi käyttää jatkossa, jos työntekijät käsittelevät asiakastietoja etänä.

2.3 Sähköpostin ja viestinnän salaus

Jos terveysasioita käsitellään sähköpostitse, tulisi viestit salata ja varmentaa tietoturvaprotokollilla kuten S/MIME:llä (Secure/Multipurpose Internet Mail Extension) ja PGP:llä (Pretty Good Privacy). PGP on avoimen lähdekoodin ohjelmistopaketti, joka pohjautuu luottamusverkkoon (web of trust) ja avainten vaihtoon (GeeksforGeeks, 2025). Sitä käytetään VPN:ssä ja tekstiviesteissä. S/MIME käyttää julkisen avaimen salausta eli epäsymmetristä salausta digitaalisiin allekirjoituksiin, sähköpostien salaukseen ja purkamiseen.

2.4 Tunnistautumisen ja salasanojen suojaaminen

Microsoft ei tue monivaiheista tunnistautumista (multifactor authentication, MFA) toimialueympäristössä eikä suosittele 3. osapuolen ratkaisuja vaan tulisi käyttää Windows Helloa tai PIN-koodia. Microsoftin MFA:ta voidaan käyttää ottamalla käyttöön M365.

Salasanoja voidaan suojata salasanaholveilla kuten Bitwarden, 1Password ja KeePass. Ne auttavat pitämään kirjautumistiedot turvassa ja vähentävät heikkojen salasanojen käyttöä. FIDO2/U2F-tunnistautumisessa käytetään fyysistä turva-avainta.

Varaussivustossa käytettävässä Node.js-ajoympäristössä on bcrypt-kirjasto (NPM, 2025), jolla salasanat hajautetaan ennen tietokantaan tallennusta ja salasanan tarkistamista.

3 Valitut salausmenetelmät

Physiossa otetaan käyttöön asiakastietojen salaukseen BitLocker, kirjautumiseen Windows Hello ja salasanojen suojaukseen Bitwarden.

Työntekijöiden salasanat tallennetaan MongoDB-tietokantaan hajautettuna bcrypt-algoritmilla. Ajanvaraussivustoon liittyvät verkkopalvelut käyttävät HTTPS-protokollaa eli TLS-salausprotokolla on käytössä.

Viestit salataan S/MIME:llä-protokollalla, jos lähetetään asiakastietoja. Lisäksi VPN-yhteys otetaan käyttöön, jos asiakastietoja käytetään etänä.

4 Tapausesimerkit

4.1 Physio case-esimerkki: työasemien suojaus Bitlockerilla (kesken)

Käynnistettiin palvelin ja päivitettiin VMware Tools ja suoritettiin Windows Updaten ehdottama päivitys Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.421.1944.0), Windows Malicious Software Removal Tool x64 - v5.132 (KB890830) ja 2025-02 Cumulative Update for Microsoft server operating system version 21H2 for x64-based Systems (KB5051979). Otettiin snapshot sammutettuna 20250217.

Käynnistettiin työasema ja päivitettiin VMware Tools ja suoritettiin ehdotetut päivitykset: Suojaustietojen päivitys tuotteelle Microsoft Defender Antivirus – KB2267602 (versio 1.421.1944.0), Windowsin haittaohjelmien poistotyökalu (x64), v5.132 (KB890830) ja 2025-02 Kumulatiivinen päivitys Windows 10 Version 22H2 x64 -pohjaisille järjestelmille (KB5051974). Otettiin snapshot sammutettuna 20250217.

Bitlocker vaatii suojatun käynnistyksen tilan (Secure Boot) mutta se ei ollut päällä työasemassa (Microsoft, BitLocker, 2025). Se tarkistettiin Järjestelmätiedot-ohjelmasta (msinfo32.exe): Suojatun käynnistyksen tila: Ei käytössä ja Laitesalauksen tuki-kohdassa ilmoitetaan, että ”Automaattisen laitesalauksen epäonnistumisen syyt: ”TPM-turvapiiri ei ole käytettävissä, PCR7-sidontaa ei tueta, Laitteiston suojaustestin käyttöliittymä epäonnistui, ja laite ei ole modernin valmiustilan laite, Havaittiin kielletty DMA-yhteensopiva väylä tai kiellettyjä DMA-yhteensopivia laitteita, TPM-turvapiiri ei ole käytettävissä”. Ei voida laittaa suojattua käynnistyksen tilaa päälle (Edit virtual machine settings > Options-välilehti > Access Control), koska salausta ei voida lisätä snapshottien vuoksi.

Jätetään siis työasemien suojaus Bitlockerilla pois tästä projektista ajanpuutteen vuoksi. Jos sitä jatkossa halutaan kokeilla, luodaan uusi virtuaalinen työasema, josta ei oteta snapshotteja ja laitetaan suojattu käynnistyksen tila heti alussa päälle (Pureinfotech, 2025). AD:ssa luodaan sille oma ryhmänsä/OU:nsa (Bitlocker-työasemat) ja kohdistetaan luotava Bitlocker-GPO vain siihen.

4.2 Case-esimerkki: Testout Security Pro OpenStego-salaus

Tehtiin laboratoriotyö 3.1.11 Hide Files with OpenStego eli käytettiin steganografiaa Ja salattiin tekstitiedosto liittämällä se kuvatiedostoon. Lisäksi testattiin purkua.

5 Jatkoehdotukset

Ottamalla Microsoft 365 käyttöön voidaan käyttää myös Microsoftin MFA:ta.

Maksupalveluihin liittyvät salausmenetelmät tulisi selvittää vielä.

Lähdeluettelo

GeeksforGeeks. (2025, Helmikuu 14). *Difference between PGP and S/MIME*. Retrieved from https://www.geeksforgeeks.org/difference-between-pgp-and-s-mime/

Microsoft. (2025, Helmikuu 17). *BitLocker*. Retrieved from https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/

Microsoft. (2025, Helmikuu 18). *File Encryption*. Retrieved from https://learn.microsoft.com/en-us/windows/win32/fileio/file-encryption

MongoDB. (2025, Helmikuu 17). *MongoDB Data Encryption*. Retrieved from https://www.mongodb.com/products/capabilities/security/encryption

NPM. (2025, Helmikuu 17). *bcryptjs*. Retrieved from https://www.npmjs.com/package/bcryptjs

OpenAI. (2025, Helmikuu 8). *ChatGPT*. Retrieved from https://chatgpt.com/

Pureinfotech. (2025, Helmikuu 17). *How to enable TPM and Secure Boot on VMware to install Windows 11*. Retrieved from https://pureinfotech.com/enable-tpm-secure-boot-vmware-install-windows-11/