HP WOLF SECURITY

HP Engage

Päätelaitteiden tietoturva terveydenhuollossa

Yleiskatsaus

Terveydenhuollon tiedot ovat olleet jo pitkään kyberrikollisten tähtäimessä. Tietomurrosta aiheutuu paljon kustannuksia, ja se on rikollisille tuottoisaa. Näin ollen ei ole yllättävää, että terveydenhuollon toimijat ovat saaneet entistä enemmän lunnasvaatimuksia hyökkäyksistä.[1]

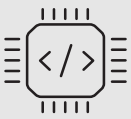
Miten näin käy?

- Sähköposteilla kommunikoidaan laajasti terveydenhuollon organisaatioiden välillä, ja lisääntyneet etäterveyspalvelut ovat lisänneet mahdollisia kyberrikollisten tekemiä tietojen sieppauksia. Tosiasiassa sähköposti onkin yleisin (94 %) kyberrikollisten ensihyökkäyskohde organisaatioon.[2]
- Hoitoalan ammattilaiset tarvitsevat usein pääsyn tietoihin etänä, joten heistä tulee kalasteluhyökkäysten pääkohteita. Tietomurto saattaa tapahtua, kun työntekijä (hoitojärjestelmän sähköpostitilillä) vastaa kalasteluyritykseen syöttämällä kirjautumistietonsa, mikä mahdollistaa kyberrikollisille pääsyn verkkoon.
- Kalasteluhyökkäyksiä voi tapahtua myös verkkoselailuympäristössä, yhteistyösovelluksissa tai sähköisten asiakirjojen kautta. Näitä uhkia on jatkuvasti osaltaan siksi, että perinteinen virustorjunta ja seurantapohjaiset tietoturvan työkalut eivät ole olleet riittävän vahvoja. Terveydenhuollon laitokset joutuvat yhä uudelleen uhreiksi ja siksi tarvitsevatkin ratkaisuja, joilla tällaiset hyökkäykset saadaan pysäytettyä heti.

TÄRKEIMMÄT ASIAT

- Terveydenhuollon IT-toimintojen tiimit tarvitsevat suunnitelman laitteiden vikasietoisuudelle ja palautumiselle.
- Pitkän elinkaaren HP Engage -järjestelmät on suunniteltu, laitteistotasolta alkaen, olemaan tietoturvallisia ja vikasietoisia ei vain nykyisten hyökkäysten suhteen, vaan myös jatkuvasti kehittyvien tulevien hyökkäysten suhteen.
- Terveydenhuollon organisaatiot, jotka käyttävät HP Wolf Securityn[3] kattavaa monikerroksista tietoturvaa, voivat alentaa IT-kustannuksiaan vähemmillä tukipuheluilla ja korjaustoimilla haittaohjelmahyökkäysten sattuessa.

HP:n KATTAVA MONIKERROKSINEN TIETOTURVA



BIOS

Käyttö-
järjestelmä

Sovellukset

Fyysinen
tietoturva

Ollakseen täysin suojattuina hyökkäyksiä vastaan järjestelmä- ja päätelaitetasolla, terveydenhuollon organisaatioiden täytyy ottaa huomioon eri kerrosten riskit ja lähestyä asiaa kokonaisvaltaisesti turvatakseen ympäristönsä. Jokainen kerros muodostaa mahdollisen riskialueen, ja ne täytyykin suojata sellaisilla tietoturvatyökaluilla, jotka:

- havaitsevat uhat
- pysäyttävät ja poistavat ne
- palauttavat nopeasti järjestelmän joka tasolla

HP:n kattava monikerroksinen lähestymistapa päätelaitteiden tietoturvaan alkaa jo käyttöjärjestelmän alapuolella perustavanlaatuisella suojauksella BIOS-tasolla, jatkuu sitten käyttöjärjestelmään ja sen ulkopuolella oleviin tekijöihin, ja ulottuu aina fyysiselle tasolle sisäänrakennetuilla tietoturvaominaisuuksilla.

PC-alustan suojaus

HP Sure Start[4]

Järjestelmän laiteohjelmisto-ongelmien korjaaminen on kallista, monimutkaista ja se voi aiheuttaa merkittäviä käyttökatkoja terveydenhuollon toimintaan. Pitkän elinkaaren HP Engage -järjestelmät HP Sure Start -ratkaisulla valvovat jatkuvasti järjestelmän BIOSia/laiteohjelmistoa ja itsekorjautuvat, jos hyökkäykset, piilohallintaohjelmat tai muun tyyppiset korruptoitumiset vaurioittavat BIOSia. Jos BIOSin/laiteohjelmiston peukalointia havaitaan, HP Sure Start yhdessä HP Endpoint Security Controllerin kanssa vaihtaa kohteeksi joutuneen BIOSin/laiteohjelmiston uuteen puhtaaseen versioon ja käynnistää järjestelmän täysin toimivalla BIOSilla/laiteohjelmistolla. HP:n perustavanlaatuisen suojauksen ansiosta terveydenhuollon työntekijät pysyvät tuottavina ilman keskeytyksiä.

HP Sure Admin[5]

Käyttämällä heikkoja salasanoja tai samaa moniin järjestelmiin voi avata väyliä hyökkäyksille. Terveydenhuollon IT-hallinnoijat eivät tarvitse enää salasanoja käyttämällä HP Sure Admin -ratkaisua. Tässä modernissa BIOS-hallintatyökalussa käytetään digitaalisia varmenteita ja vahvaa julkisen avaimen salausjärjestelmää. Näin IT-hallinnoijat voivat hallita tietoturvallisesti ja etänä järjestelmän BIOS-asetuksia verkon kautta ilman salasanoja.

HP Sure Run[6]

Terveydenhuollon IT-ympäristöt pitävät yllä monia prosesseja, jotka ovat kriittisiä potilaiden hyvinvoinnille. Haittaohjelmahyökkäykset, jotka uhkaavat näitä jatkuvia toimintoja, täytyy pysäyttää heti. HP Sure Run valvoo avainprosesseja, lähettää tietoturvailmoituksia käyttäjille ja IT-hallinnoijille kaikista tietoturva-asetusten muutoksista ja käynnistää avainprosessit automaattisesti uudelleen, jos edistynyt haittaohjelma yrittää sammuttaa ne.

HP Sure Recover[7]

Kun järjestelmän käyttäjään osuu tuhoisa hyökkäys, terveydenhuollon IT-hallinnointi tarvitsee palautusjärjestelmän estääkseen käyttökatkot ja tuottavuuden menetyksen. HP Sure Recover hyödyntää HP Endpoint Security Controllerin kykyä palauttaa käyttöjärjestelmä, jos kovalevy on vaarantunut tai korruptoitunut. Käyttäjille voidaan antaa tukea etänä ja näköistiedosto saadaan palautettua, vaikka heidän ensisijainen levynsä olisi pyyhkiytynyt täysin.

Sovellustason tietoturva

Vaikka alusta olisikin tietoturvallinen, sen ulkopuoliset sovellukset voivat silti olla haavoittuvaisia. HP Wolf Security -tietoturva[3] sisältää myös laitteistotason eristysteknologian, tunnusten suojauksen kalasteluyrityksiltä sekä uuden sukupolven virustorjunnan, jotka antavat vertaansa vailla olevan suojauksen sovellusten tasolla.

HP Sure Sense
Uuden sukupolven virustorjuntaohjelma[8]

Perinteinen virustorjuntasuojaus ei aina tunnista uusia hyökkäyksiä. HP Sure Sense käyttää syväoppivaa tekoälyä tunnistamaan ja eristämään ennennäkemättömät hyökkäykset, joten se ennaltaehkäisee virustartuntoja ennen kuin ne tapahtuvat. Kyseessä on kevyt ohjelmistoagentti, joka ei vaadi jatkuvia päivityksiä suojatakseen järjestelmääsi reaaliaikaisesti. HP Sure Sense suojaa päätelaitteita vuorokauden ympäri toimimalla käyttöjärjestelmässä yhdessä HP Sure Runin kanssa, olipa päätelaite yhteydessä verkkoon tai ei.

HP Sure Click Enterprise käyttää päätelaitteiden eristysteknologiaa[8]

Kattava suojaus selainpohjaisia, sähköposti- tai sosiaalisen median hyökkäyksiä vastaan ei ole koskaan ollut näin elintärkeää. HP Sure Click on laitteistotason tietoturvallisen verkkoselauksen ratkaisu käyttöjärjestelmässä. Se eristää verkkosisällön keskusyksikköeristettyyn virtuaalikoneeseen, jossa haittaohjelmat eivät voi vaikuttaa muihin sovelluksiin, asiakirjoihin, intranetiin tai käyttöjärjestelmään. Haittaohjelma poistetaan automaattisesti, kun verkon välilehti suljetaan. Näin vältytään kalliilta palautustoimilta ja käyttökatkoilta. HP Sure Click eristää myös uhat PDF-, Microsoft Word-, ja Microsoft Excel- tiedostoissa vain luku -muotoon.

Fyysinen tietoturva

Fyysisiä laitehyökkäyksiä on vaikea havaita ja korjata. Pitkän elinkaaren HP Engage -järjestelmät sisältävät laitteen fyysiseen suojaukseen integroituja suojausominaisuuksia väärinkäyttäjiä vastaan, kuten biometrinen todennus, kannen lukitus ja liitäntöjen poistaminen käytöstä. Fyysiset laitteiden varkaudet tai kadottamiset, etenkin mobiiliympäristössä, voivat aiheuttaa terveydenhuollon organisaatioille tarpeettoman riskin. HP Engage Go 10 -tabletin voi turvallisesti lukita muunneltavaan HP Engage Go 10 -telakkaan[9] tai HP Engage Go 10 -monilaturiin[9]. Jos tabletti on käyttövalmiina telakassa, se voidaan avata mekaanisesti. Tämän mahdollistaa HP Smart Dock -sovellus, jonka avulla käyttäjät voivat avata tablettinsa automaattisesti HP Engage Go 10 Convertible Dock -telakasta syöttämällä salasanan tai PIN-koodin, käyttämällä Windows Hello- tai kasvojen tunnistusta tai sormenjälkilukijaa monivaiheista todennusta varten.[10]

Fyysinen tietoturva

	LOPPUTULOS	KUVAUS	TOIMINNOT
Häiriö- ja hätäpalautus	Häiriö- ja hätäpalautus	Palauttaa työntekijöiden tuottavuuden, jos päätelaite korruptoituu	Palauttaa puhtaan käyttöjärjestelmän kaikissa pitkän elinkaaren HP Engage -järjestelmissä käyttökatkojen välttämiseksi ja toimintojen jatkumiseksi; tietoturvallinen asiakkaan Windows-käyttöjärjestelmän palautus etänä käyttämällä HP Sure Recoveria
Toimintojen jatkuminen	Toimintojen jatkuminen	Vähentää käyttökatkoja, häiriöitä ja IT-tukea vaativia pyyntöjä toiminnan tehokkuuden edistämiseksi	Nopea käyttöjärjestelmän palautus, itsekorjautuva BIOS ja saumattomat laiteohjelmistopäivitykset
PC-alustan eheys	PC-alustan eheys	HP:n eristysteknologia ja karanteenisäiliö tietoturvauhkia varten	Käyttämällä laitetason suojausta, joka pohjautuu Zero Trust -periaatteisiin, haittaohjelmaa estetään saastuttamasta tietokonetta
Vahinkojen ennaltaehkäisy	Vahinkojen ennaltaehkäisy	Arkaluontoisten tietojen ja/tai laitteiden menetys valvomattomien PC-järjestelmien kautta	USB-valvonta, tietoturvallinen BIOS, HP Smart Dock
IT-kustannusten säästöt	IT-kustannusten säästöt	Alhaisemmat omistuksen kokonaiskustannukset vähempien tukipyyntöjen ja haittaohjelmahyökkäysten ratkaisutoimenpiteiden kautta	
Vaatimustenmukaisuus	Auttaa noudattamaan HIPAA- ja GDR-säännösvaatimuksia	Tietojen suojaus auttaa osaltaan onnistuneessa vaatimustenmukaisuuden noudattamisessa sääntelyvaatimusten osalta	

Yhteenveto

Vakaa ja jatkuva toiminta on kriittistä terveydenhuollon organisaatioille. Prosessien ylläpito on ratkaisevaa potilaan hoidon kannalta. Monet nykypäivän virustorjuntaratkaisut eivät ole riittäviä suojaamaan kriittisiä tietoja jatkuvilta kyberhyökkäysuhilta. Terveydenhuollon organisaatiot tarvitsevat uuden ja kattavan lähestymistavan, joka tarjoaa suojauksen joka tasolla, alkaen vahvasta perustasta. HP:n kattava monikerroksinen tietoturva alkaa juuritason luotettavuudesta, HP Endpoint Security Controllerista. Se tarjoaa laitteistotason suojauksen ja on avaintekijä HP Sure Start-, Sure Run-, ja Sure Recover -ratkaisujen vikasietoisuuden taustalla. Tämä monen kerroksen tietoturvakokonaisuus säilyttää alustan eheyden ja vähentää radikaalisti keskeytyksiä ja mahdollisia katastrofaalisia tietomurtoja ja -menetyksiä.

Lähteet:

1 Tietomurtojen kustannusten raportti Cost of a Data Breach Report 2021, IBM Security, heinäkuu 2021. Kyberhyökkäykset terveydenhuollon alalla ovat jatkaneet kasvuaan jo vuosia. Keskimääräisissä tietomurtokustannuksissa on ollut kasvua 29 % vuonna 2021. Miksi? Koska terveydenhuollon data tarjoaa kyberrikollisille suurimmat tuotot, se nostaa terveydenhuollon laitokset heidän uhriensa kärkeen. Esimerkki artikkeleissa: San Diego Health Faces Class Action Lawsuits Over Phishing Attack – CalHIPAA ja UC San Diego Health announces data breach - The San Diego Union-Tribune (sandiegouniontribune.com)

2 https://www.teiss.co.uk/r3/cth_schedule/94-of-cyber-at-tacks-start-with-an-email-how-resilient-is-your-endpoint-protection-solution/

Vastuuvapauslausekkeet:

3 HP Wolf Security for Business edellyttää Windows 10 -käyttöjärjestelmää tai uudempaa, sisältää monenlaisia HP:n tietoturvaominaisuuksia ja sen saa HP Engage -tuotteisiin. Tuotteen tietoturvaominaisuudet näkee tuotetiedoista.

4 HP Sure Start -ohjelmiston (6. sukupolvi) saa tiettyihin HP-järjestelmiin ja se edellyttää Windows 10 -käyttöjärjestelmää.

5 HP Sure Adminin edellytykset: Windows 10 tai uudempi, HP BIOS, HP Manageability Integration Kit osoitteesta http://www.hp.com/go/clientmanagement sekä HP Sure Admin Local Access Authenticator -älypuhelinsovellus Android- tai Apple-kaupasta.

6 HP Sure Start -ohjelmiston (4. sukupolvi) saa tiettyihin HP-järjestelmiin ja se edellyttää Windows 10 -käyttöjärjestelmää.

7 HP Sure Recoverin (4. sukupolvi) saa tiettyihin HP-järjestelmiin, ja se edellyttää Windows 10- tai uudempaa käyttöjärjestelmää ja avointa verkkoyhteyttä. Tärkeät tiedostot, tiedot, valokuvat, videot ja vastaavat on varmuuskopioitava ennen HP Sure Recover -ratkaisun käyttöä tietojen menettämisen välttämiseksi. Verkkopalautusta Wi-Fi-yhteyden kautta voi käyttää vain järjestelmissä, joissa on Intel Wi-Fi -moduuli.

8 HP Wolf Pro Security: HP Wolf Pro Security -suojauksen saa esiladattuna tiettyihin HP-laitteisiin ja sen saa tilauksella ja käyttölisensseillä. Saat lisätietoja HP:n myyntiedustajalta.

9 Lisävarusteet myydään erikseen.

10 Konfiguroi HP Smart Dock luodaksesi hyväksyttyjen käyttäjien luettelon.

4AA8-2479ENW, tammikuu 2023

HP WOLF SECURITY