Terveys- ja hyvinvointialojen opintokokonaisuus

Kyberturvallisuuskoulutuksen ja siihen liittyvän yhteistyön kehittäminen korkeakouluissa

OPETUS- JA KULTTUURIMINISTERIÖ
UNDERVISNINGS- OCH KULTURMINISTERIET

jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

03A - Haittaohjelmat

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Haittaohjelmat

Kuvaus

- Haittaohjelmilla viitataan erilaisiin verkkorikollisten käyttämiin ja levittämiin ohjelmiin, kuten viruksiin ja vakoiluohjelmiin.
  - Tarkoituksena voi olla päästä käsiksi arkaluonteisiin tietoihin, rahapalveluihin (esim. nettipankki) ja aiheuttaa vahinkoa uhriensa laitteille.
- Tyypillistä haittaohjelmille on myös, että laite kaapataan kokonaan tai että monelle laitteelle tunkeudutaan samanaikaisesti.
- Haittaohjelmat kategorisoidaan leviämisen, toiminnan ja haittatyypin perusteella. Haittaohjelmat eivät leviä pelkästään tietokoneilla, vaan myös mobiililaitteet ja tabletit ovat houkuttelevia kohteita.

Lähde: https://www.f-secure.com/fi/articles/what-is-malware, viitattu 20.9.2024

jamk

Haittaohjelmat

Uhka esimerkkejä

- Henkilökohtaisten tietojen varastaminen kiristämistä tai identiteettivarkautta varten.
- Salasanojen ja kirjautumistietojen varastaminen käyttäjätilin kaappausta varten.
- Laitteesi ja tiedostojesi lukitseminen sekä lunnaiden vaatiminen.
- Arkaluontoisen materiaalin varastaminen.
- Tiedon kerääminen työpaikastasi ja sen järjestelmistä.
- Tietokoneen käyttösi vakoilu tai näppäimistösi painallusten tallentaminen.

Lähde: https://www.f-secure.com/fi/articles/what-is-malware, viitattu 20.9.2024

jamk

Haittaohjelmat

Haittaohjelmatyyppejä

- **Virus**: Haittaohjelma, joka käyttää hyväkseen aukkoja ohjelmien tietoturvassa ja ujuttaa uutta koodia ohjelmaan.
- **Troijalainen (Trojan)**: Näyttää tavalliselta ohjelmistolta tai tiedostolta, mutta todellisuudessa se on naamioitu virus, joka varastaa luottamuksellisia tietoja, kaappaa laitteen tai vakoilee sen toimintaa.
- **Tietokonemato (Worm)**: Tietokonemato kopioi itsensä helposti laitteelta toiselle ja leviää siksi nopeasti.
- **Kiristyshaittaohjelma (Ransomware)**: Salaa tai lukitsee tiedostoja, käyttäjätilejä ja laitteita. Verkkorikolliset vaativat uhreiltaan lunnaita lukituksen purkamiseksi.
- **Vakoiluohjelma (Spyware / Info Stealer)**: Seuraa ja kaappaa laitteesi viestintää, selaustietoja ja muuta tietoliikennettä. Voi sisältää myös ominaisuuden näppäinpainallusten kaappaamiseen.

Lähde: https://www.f-secure.com/fi/articles/what-is-malware, viitattu 20.9.2024

jamk

Haittaohjelmat

Makro haittaohjelmat

- Piiloutuvat MS Office –tiedostoihin ja toimitetaan usein sähköpostien liitteinä tai ZIP-tiedostojen sisällä
  - Esimerkkejä MS Office makrotetuista tiedostoista: .xls**m**, .doc**m** (vertaa .xlsx, .docx)
  - Tiedostot usein käytetään nimiä, joiden tarkoitus on houkutella tai pelotella käyttäjiä avaamaan ne. Useimmiten näyttävät esim. laskuilta, kuiteilta, oikeudellisilta asiakirjoilta.
- Yleisyys on vähentynyt merkittävästi, sillä oletuksena nykyään MS Office ei suorita makroja. Makrot ovat kuitenkin asetettavissa käyttöön käyttäjän toimesta.
  - Usein haittakoodin tekijät yrittävät saada käyttäjän aktivoimaan makrot erilaisten valevirheiden ja muiden houkutteluiden ja pelottelun keinoin.

Lähde: https://learn.microsoft.com/en-us/defender-endpoint/malware/macro-malware, viitattu 13.2.2025

jamk

Haittaohjelmat

Leviäminen

- Tyypillisimmät haittaohjelmien leviämistavat ovat:
  - Sähköpostien liitteiden tai linkkien kautta.
  - Haitallisten verkkosivujen kautta (esim. ilmainen versio maksullisesta ohjelmasta, lataa tästä).
  - Sosiaalisen median ja pikaviestintäpalveluiden kautta.
  - USB-muistitikut ja muut ulkoiset tallennusvälineet (esim. houkuttelevasti ”unohdettu” muistitikku tai DVD-levy pöydällä).
- Haittaohjelmat saattavat levitä käyttäjän tietämättä. Esimerkkinä, kaapattu sosiaalisen median tili, joka saattaa lähettää tutuilleen linkkejä ”avaa tämä, en ole nähnyt mitään vastaavaa” tai kaapattu sähköpostitili voi lähettää kaikille kontakteilleen sähköpostin.

jamk

Haittaohjelmat

Kuviteltu sairaala esimerkki “MedMal”

- Kuvitellaan, että sairaalan tietojärjestelmään on päässyt haittaohjelma nimeltä “MedMal”. Tämä haittaohjelma toimii monella tavalla:
  1. **Tietojen varastaminen**: MedMal kerää potilaiden henkilökohtaisia ja terveystietoja ja lähettää ne hyökkääjälle. Tämä johtaa potilaiden yksityisyyden loukkaamiseen ja mahdollisesti identiteettivarkauksiin.
  2. **Järjestelmän häirintä**: MedMal estää pääsyn kriittisiin järjestelmiin, kuten potilastietokantoihin ja lääkintälaitteisiin. Tämä voi viivästyttää hoitoa ja vaarantaa potilaiden turvallisuuden.
  3. **Kiristyshaittaohjelma**: MedMal lukitsee sairaalan tietojärjestelmät ja vaatii lunnaita niiden avaamiseksi. Tämä voi aiheuttaa merkittäviä taloudellisia menetyksiä ja häiritä sairaalan toimintaa.
  4. **Leviäminen verkkolaitteiden välillä**: MedMal leviää sairaalan verkossa olevien laitteiden välillä, kuten tietokoneiden, lääkintälaitteiden ja palvelimien kautta. Tämä nopeuttaa haittaohjelman leviämistä.
- **Yhteenveto**: MedMal-haittaohjelma vaarantaa potilaiden tiedot, hidastaa hoitoa ja voi aiheuttaa taloudellisia menetyksiä. On tärkeää, että sairaalan henkilökunta on tietoinen tällaisista uhista ja noudattaa tietoturvakäytäntöjä niiden ehkäisemiseksi.

Esimerkki tuotettu generatiivista tekoälyä hyödyntäen

jamk

Haittaohjelmat

Loppukäyttäjän puolustuskeinot

- IT voi tehdä paljon estoja, mutta kaikkea ei pystytä estämään tai pakottamaan järjestelmistä. Tämän vuoksi on hyvä huomioida seuraavat seikat loppukäyttäjän asemassa:
  - Älä avaa epäilyttäviä sähköposteja tai eteenkään epäilyttäviä liitetiedostoja.
    - Raportoi ja poista epäilyttävät sähköpostit.
    - Selvitä mihin ja miten työpaikallasi raportoidaan epäilyt. Nämä vaihtelevat työpaikkakohtaisesti.
  - Älä liitä koneeseen tuntematonta USB-tikkua tai muuta ”kannettavaa” tallennusmediaa.
    - Pahat tekijät saattavat jättää haitallisia tikkuja houkutteleville paikoille, kuten julkisten tilojen pöydille, siinä toivossa, että joku yhdistää tikun työkoneeseen.
  - Älä käytä muita kuin yrityksen tarjoamia laitteita ottaaksesi yhteyttä tai kirjautuaksesi yrityksen palveluihin, verkkoihin tai sähköpostiin. Muiden laitteiden ylläpitoa ei pystytä valvomaan keskitetysti.

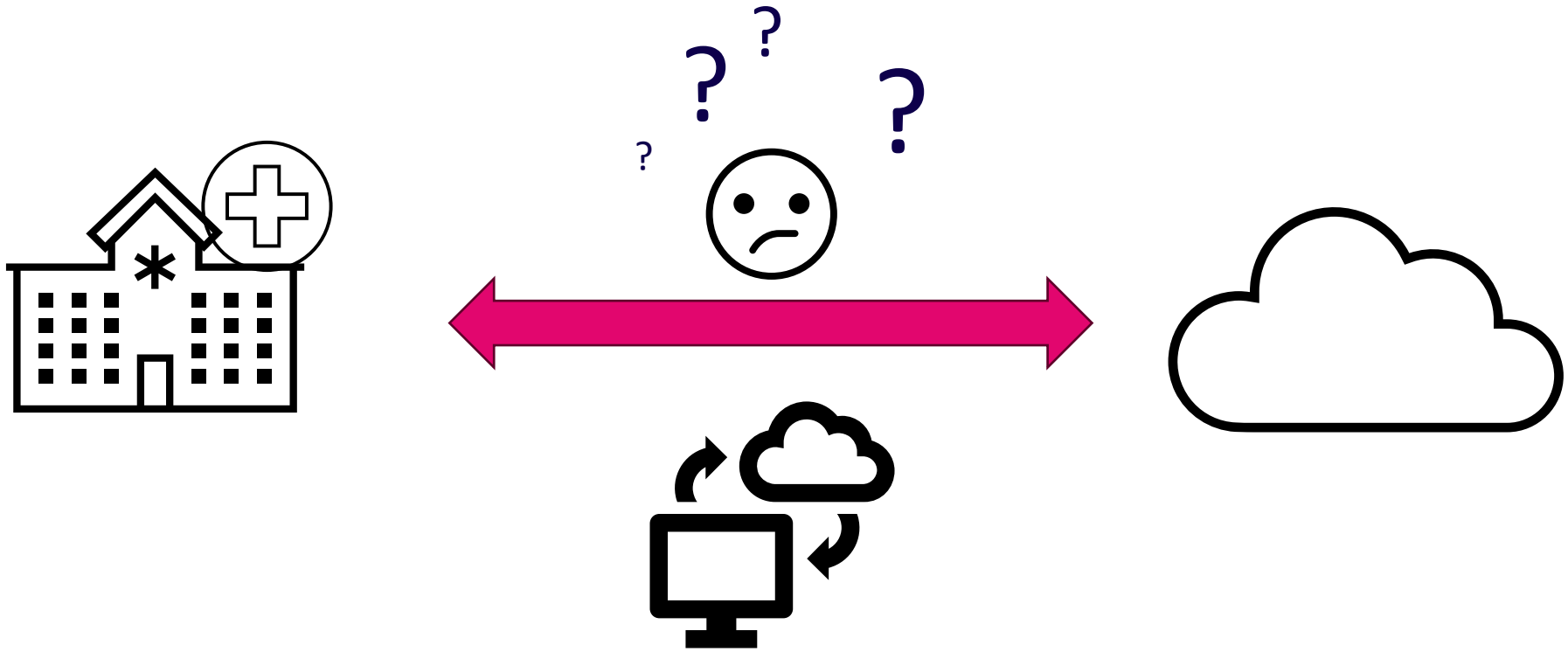
jamk

Terveys- ja hyvinvointialojen opintokokonaisuus

03B – Tietojärjestelmät, älylaitteet ja pilvipalvelut

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Tietojärjestelmät ja pilvitallennus



jamk

Tietojärjestelmät ja pilvitallennus

Asiakastiedot ja potilastiedot

- Asiakastiedot ja potilastiedot ovat arkaluontoista tietoa. Kyseisiä tietoja saa tallentaa vain työnantajan määräämiin järjestelmiin, näitä ovat esimerkiksi erilaiset elektroniset potilastietojärjestelmät ja asiakastietojärjestelmät.
- Mihin näitä tietoja ei sovi tallentaa:
  - Käyttäjien omille tileille, esim.: onedrive.
  - USB-tikuille.
  - Paikalliselle kiintolevylle.
  - Pikaviestintäpalvelut, kuten: whatsapp.

jamk

Tietojärjestelmät ja pilvitallennus

Miksi tietoja ei sovi tallentaa muualle?

- **Tietoturva:** Erityisesti suunnitellut järjestelmät on rakennettu suojaamaan arkaluonteisia tietoja. Ne sisältävät monimutkaisia turvatoimia, kuten salauksen ja pääsynhallinnan, jotka estävät luvattoman pääsyn tietoihin.
  - Paikalliset kiintolevyt ja USB-tikut eivät yleensä tarjoa samaa suojan tasoa ja ovat alttiita fyysisille uhille (esim. varkaus ja vahingoittuminen).
- **Tietosuoja:** Lainsäädäntö, kuten GDPR vaatii, että henkilötiedot käsitellään ja säilytetään turvallisesti. Erityiset järjestelmät on suunniteltu täyttämään nämä vaatimukset, kun taas muut tallennusvälineet voivat altistaa yrityksen tietosuojarikkomuksille ja sakoille.
- **Varmuuskopiointi ja palautus:** Erityiset järjestelmät sisältävät usein automaattiset varmuuskopiointitoiminnot, jotka varmistavat, että **tiedot voidaan palauttaa nopeasti ja helposti hätätilanteessa**.
- **Käytettävyys ja saavutettavuus:** Erityiset järjestelmät on suunniteltu siten, että ne ovat helposti käytettävissä ja saavutettavissa valtuutetuille käyttäjille, mutta samalla ne **estävät luvattoman pääsyn**.

jamk

Tietojärjestelmät ja pilvitallennus

Esimerkki skenaario

- Kuvitellaan tilanne, jossa kunta ostaa ostopalveluna fysioterapeuttipalvelun, jossa fysioterapeutti tekee inhimillisen virheen ja tallentaa arkaluonteisen asiakastiedon väärään paikkaan omalle USB-tikulleen sen sijaan, että käyttäisi erityisesti tätä varten tarkoitettua järjestelmää.
    1. **Virheellinen tallennus**: Fysioterapeutti tallentaa vahingossa asiakkaan henkilökohtaiset tiedot, kuten osoitteen, terveystiedot ja sosiaaliturvatunnuksen USB-tikulle, koska työskentelee työpuhelimestansa jaetun wifi-yhteyden päässä ja kännykästä loppuu akku kesken työskentelyn.
    2. **Tietojen katoaminen tai varastaminen**: USB-tikku unohtuu julkiselle paikalle ja joutuu vääriin käsiin. Koska nämä tallennusvälineet eivät ole suojattuja, kuka tahansa voi päästä käsiksi tietoihin.
    3. **Tietojen väärinkäyttö**: Henkilö, joka löytää tai varastaa tallennusvälineen, on suuressa velkavankeudessa ja käyttää tietoja väärin. Tämä voi johtaa identiteettivarkauteen, jossa asiakkaan henkilötietoja käytetään esimerkiksi luottojen ottamiseen tai muiden rikosten tekemiseen.
    4. **Luottamuksen menetys**: Asiakas saa tietää tietovuodosta ja menettää luottamuksensa fysioterapeuttiin ja koko organisaatioon. Tämä voi johtaa jopa irtisanomisiin tai oikeusmenettelyihin.
    5. **Oikeudelliset seuraukset**: Organisaatio voi joutua oikeudellisiin ongelmiin tietosuojalainsäädännön rikkomisesta. Tämä voi johtaa suuriin sakkoihin ja maineen menetykseen.

jamk

Älylaitteet

Yleisesti

- Älylaitteilla (smart devices) tarkoitetaan laitteita, jotka ovat yhteydessä internetiin, useimmiten ne määritellään verkkoon liitetyiksi laitteiksi, jotka yhdistävät fyysisen ja virtuaalisen maailman.
- Sosiaali- ja terveydenhuolto alalla käytetään paljon älylaitteita ja etäteknologiaa, ne tarjoavat monia etuja sekä potilaille että hoitohenkilökunnalle.

jamk

Älylaitteet

Sairaalassa käytettäviä älylaitteita - esimerkkejä

- Älykkäät lääkinnälliset laitteet: Älykkäät insuliinipumput, verenpainemittarit ja glukoosimittarit.
- Puettavat laitteet: Älykellot, aktiivisuusrannekkeet ja EKG-rekisteröintilaitteet.
- Etäseurantajärjestelmät: Telemetrialaitteet (esim. tahdistin) ja etämonitorointijärjestelmät.
- Älykkäät lääkkeiden annostelulaitteet: Älykkäät infuusiopumput ja lääkkeiden annostelulaitteet.
- Virtuaaliset avustajat ja chatbotit: Terveysneuvontaa tarjoavat chatbotit ja virtuaaliset avustajat.
- Älykkäät kodin terveyslaitteet: Älykkäät vaa'at, verenpainemittarit ja happisaturaatiomittarit.

- Näiden laitteiden kyberturvallisuus on kriittistä potilasturvallisuuden ja tietosuojan kannalta.
  - Varmista, ettei näitä laitteita yhdistetä suojaamattomiin verkkoihin, kuten julkisiin wifi-yhteyksiin.

jamk

Älylaitteet

Skenaario esimerkki

- Hyökkäyksiä älylaitteisiin on tavattu maailmalla, vaikka useimmin kohteet ovatkin tietojärjestelmiä itsessään.
- Tunnetaan myös hyökkäyksiä, joissa kohteena on ollut esimerkiksi insuliinipumput. Lyhyt artikkeli (melko teknisellä kielellä) lääkintälaitteisiin löytyy tästä:
  - https://www.zdnet.com/article/more-than-half-of-medical-devices-have-critical-vulnerabilities/
- Kaikkeen näistä ei ole tyypillisesti osana hoitohenkilökunta, mutta tietoisuus näistä on jo yksi tapa ehkäistä potentiaalisia ongelmia.

jamk

Älylaitteet

Toinen esimerkki tammikuulta 2025

- Turvallisuusongelmat Contec CMS8000 ja Epsimed MN-120 potilasmonitoreissa voivat vaarantaa potilaat, kun laitteet yhdistetään internetiin. Kolme haavoittuvuutta on tunnistettu:
  1. Potilasmonitoria voi ohjata luvaton käyttäjä.
  2. Laitteiden ohjelmistossa on takaovi, joka voi vaarantaa laitteen tai siihen liitetyn verkon.
  3. Kun potilasmonitorit yhdistetään internetiin, ne kykenevät keräämään ja siirtämään potilastietoja, mukaan lukien henkilötietoja ja suojattuja terveystietoja, terveydenhuollon ympäristön ulkopuolelle.

Lähde: https://medtechintelligence.com/news_article/fda-safety-communication-cybersecurity-vulnerabilities-with-certain-patient-monitors-from-contec-and-epsimed/, viitattu 12.02.2025

jamk

Asetus lääkinnällisistä älylaitteista

Euroopan parlamentin ja neuvoston asetus (EU) 2017/745

- Asetus pyrkii varmistamaan lääkinnällisten laitteiden turvallisuuden ja suorituskyvyn EU:n markkinoilla, mukaan lukien kyberturvallisuusnäkökohdat.
- Keskeiset Kohdat:
  - **Tietoturvavaatimukset**: Laitteiden on oltava suojattuja kyberuhkia vastaan.
  - **Riskienhallinta**: Kattava riskienhallinta koko laitteen elinkaaren ajan.
  - **Kliiniset tutkimukset**: Tietoturvatoimenpiteet kliinisten tutkimusten aikana.
  - **Ilmoitetut laitokset**: Tarkastavat kyberturvallisuusvaatimusten täyttymisen.

Lähde: https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32017R0745, viitattu 16.1.2025

jamk

Älylaitteet

Kiinteistöautomaatio

- Kiinteistöissä löytyy myös muita verkottuneita laitteita, jotka kaikki ovat tyypillisesti liitettynä tietoverkkoihin. Tyypillisesti nämä rajataan loogisesti ulos samoista verkkoalueista, joissa työntekijöiden verkko toimii, mutta fyysisesti toimivat samoissa tiloissa.

jamk

Älylaitteet

Kiinteistöautomaatio - esimerkkejä

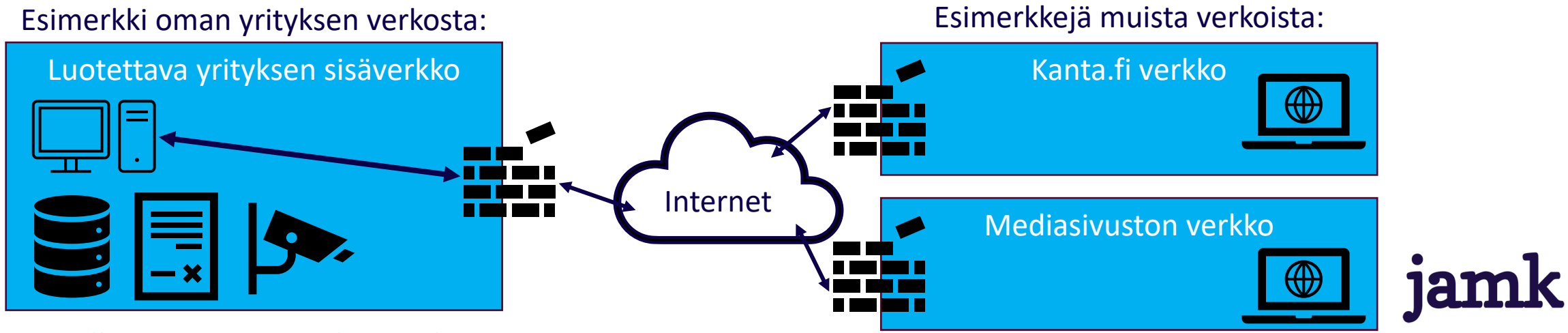
- Rakennusautomaatio tai taloautomaatiojärjestelmät ja yksittäiset ilmanvaihtokoneet ja lämmönjakolaitteet vievät tietoja paikalliseen valvomoon tai etävalvomoon.
- Älykäs valaistus (neuvotteluhuoneiden tai auditorion valaistukset, liiketunniste valot, hätävalaistus).
- Turvallisuusvalvonta (kamerat, erilaiset älykkäät anturit, paloturvallisuus, murtohälytys yms.).
- **Kulunvalvonta** (etäohjatut ovijärjestelmät, portit, yms.) Huom! Käyttötarkoituksesta riippuen osa näistä voi olla verkotettu samoihin verkkoihin, vaikkapa kulkukortti oikeuksien varmistamiseksi, voi olla jopa integroituna työajanseurantaan tms.
- Kolmannen osapuolten laitteet (kolikkoautomaatit, raha-automaatit, yms.)

jamk

Palomuuri ja luotetut verkot

Palomuuraus ja luotetut verkot

- **Palomuuri** valvoo ja hallitsee sisään- ja uloskäyvää verkkoliikennettä ennalta määriteltyjen tietoturvasääntöjen perusteella toimien esteenä luotetun (sisä-) ja epäluotetun (ulko-) verkon välillä.
  - **Palomuurin tehtävä** on suodattaa liikennettä estääkseen luvattoman pääsyn ja sallien samalla lailliset yhteydet.



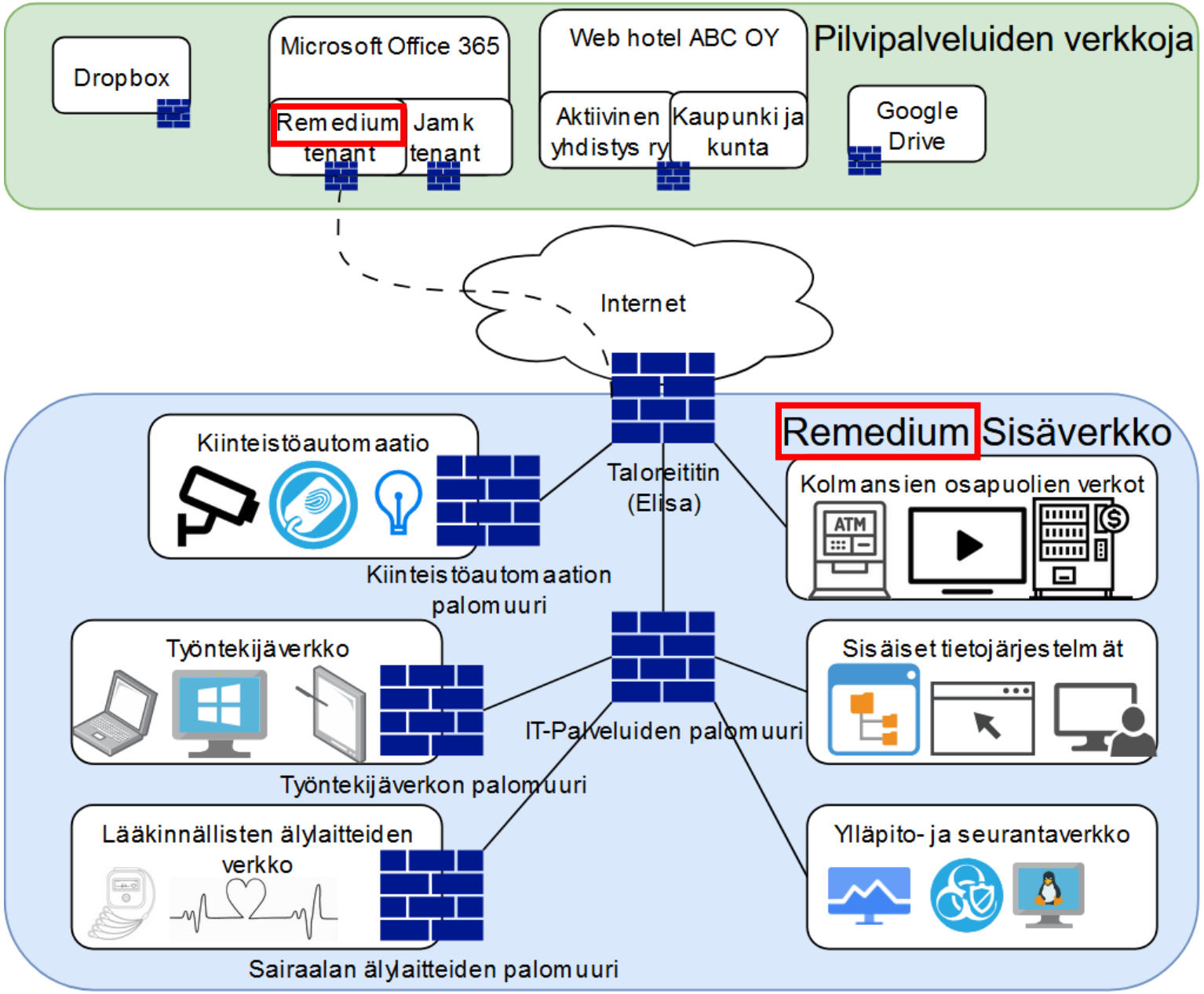
Lähde: https://www.paloaltonetworks.com/cyberpedia/what-is-a-network-firewall, viitattu 19.12.2024

Älylaitteet

Verkkokuva esimerkki (1/6)

- Tässä yksinkertaistettu esimerkki, kuinka laitteet ja verkot saattavat olla liitetty toisiinsa.

  Remedium on tässä esimerkissä kuvitteellinen sairaala, jonka sisäverkossa toimii myös kiinteistöautomaatiota ja kolmansien osapuolien laitteita, kuten mini kioskeja

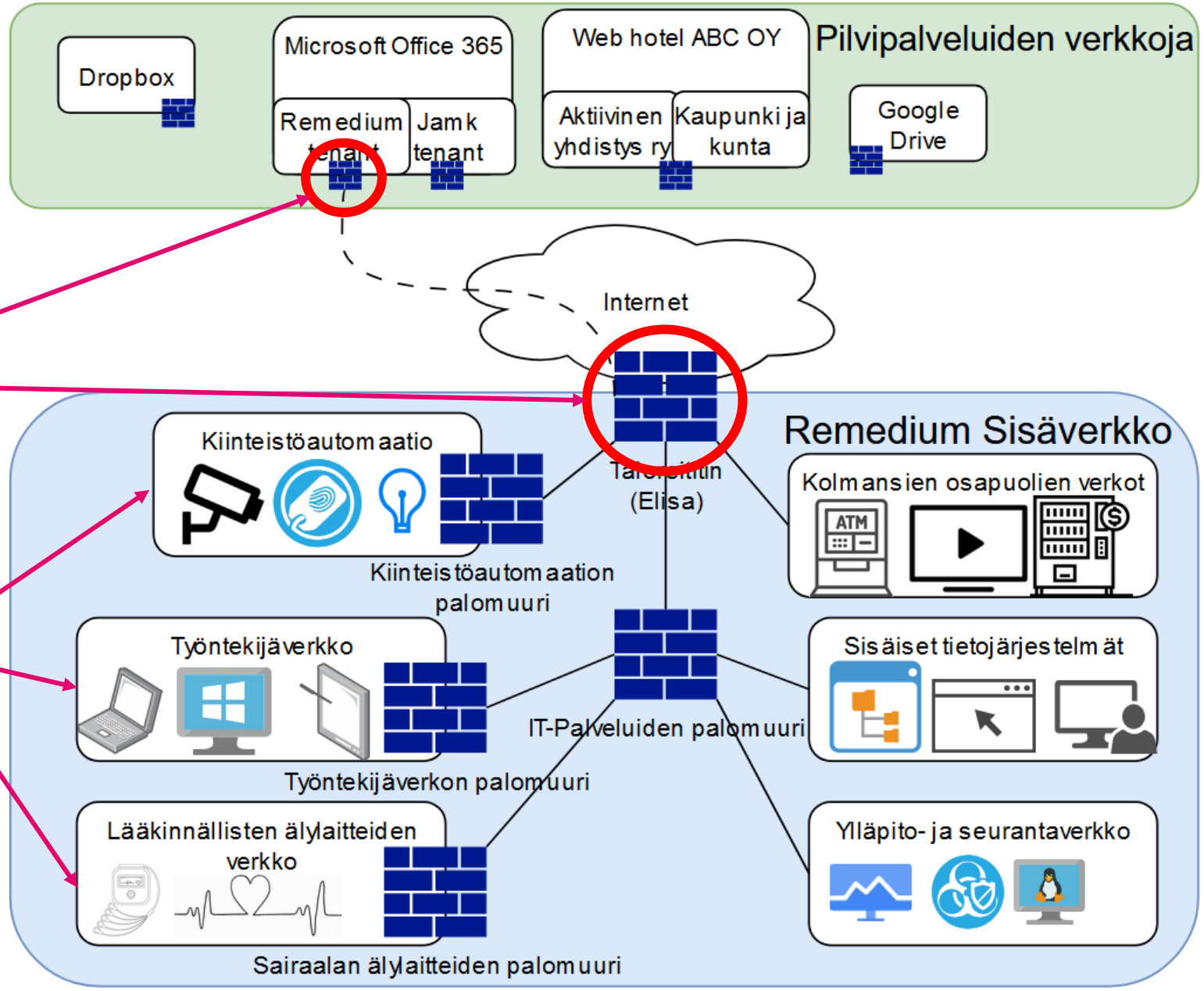


Älylaitteet

Verkkokuva esimerkki (2/6)

Siniset tiilimuurit esittävät eri verkko-osioiden välisiä palomuureja (tai reitittimiä)

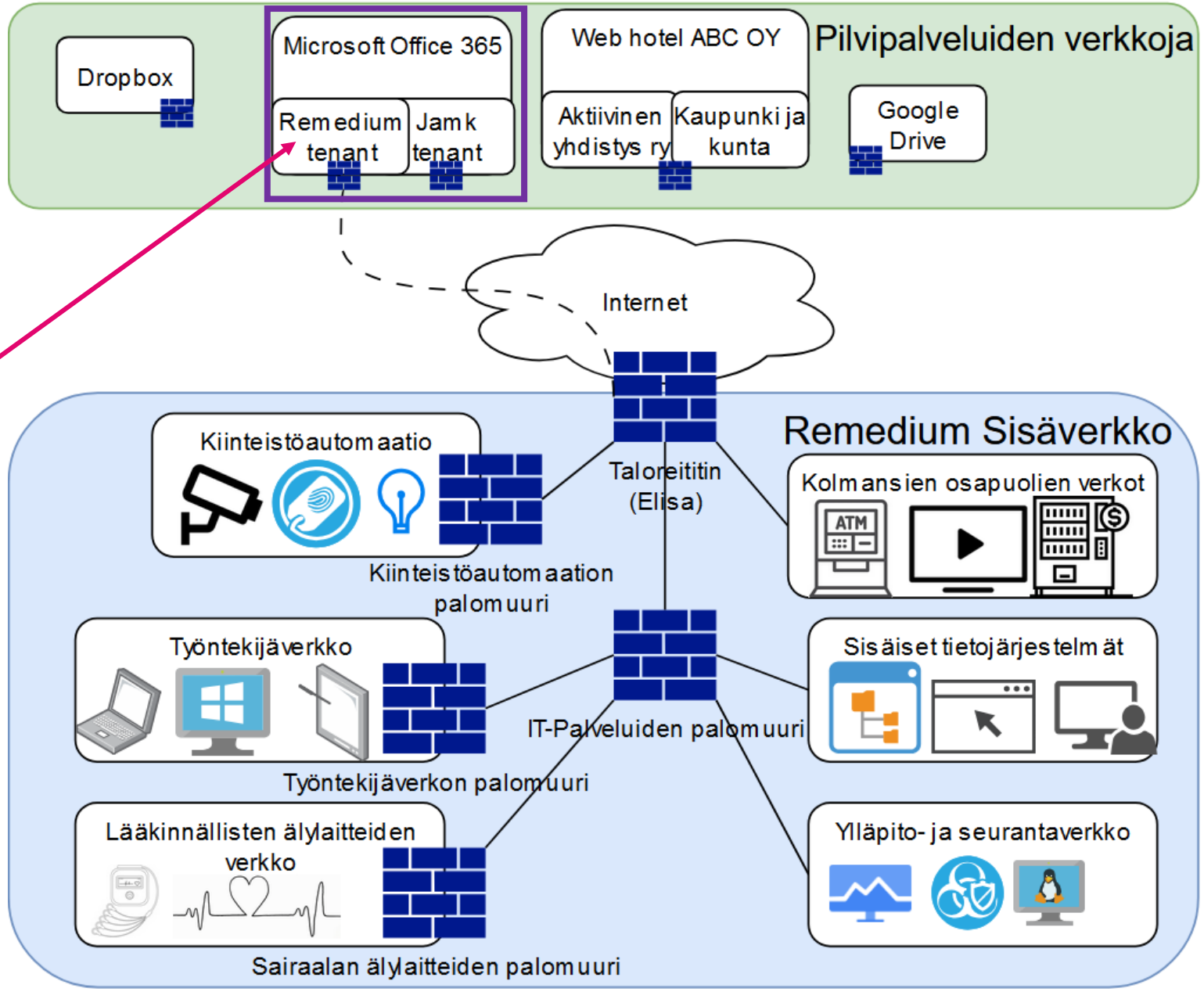
- Kuvan valkoiset laatikot ovat omia loogisia kokonaisuuksia



Älylaitteet

Verkkokuva esimerkki (3/6)

- Joillakin pilvipalveluilla kuten Microsoft Office 365 palvelulla on omat eristetyt osiot eri yrityksille tai yrityskokonaisuuksille, tämä ei kuitenkaan päde kaikkiin pilvipalveluihin, älä pidä tätä oletusarvona.

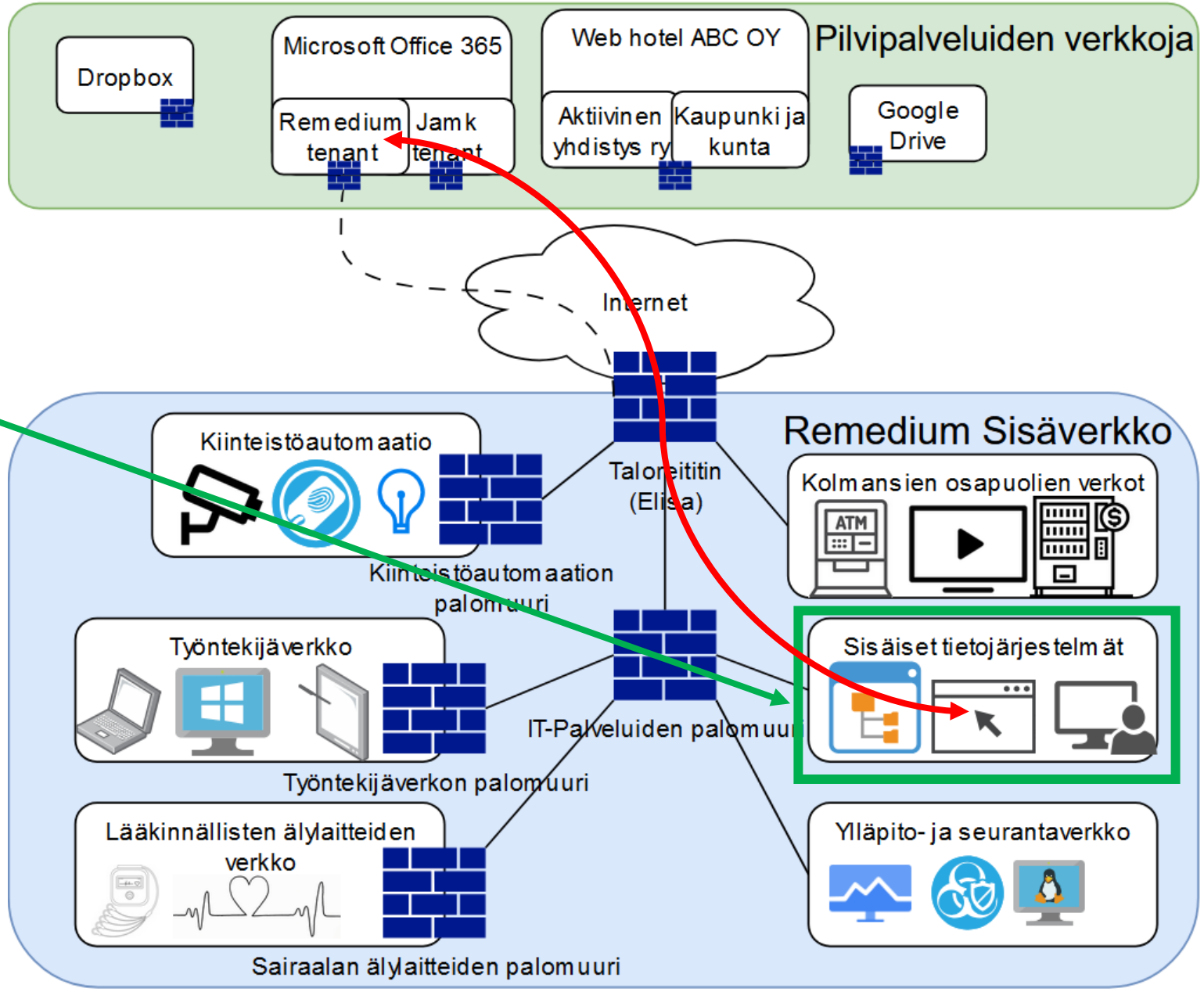


Älylaitteet

Verkkokuva esimerkki (4/6)

Sisäiset tietojärjestelmät ovat useimmiten omassa eristetyssä ympäristössänsä tietoliikenteen näkökulmasta.

- Osa niistä saattaa kommunikoida ulkomaailmaan
- Osa pitää tietonsa vain yrityksen sisässä
- Usein näille osille on omat eristetyt verkkonsa

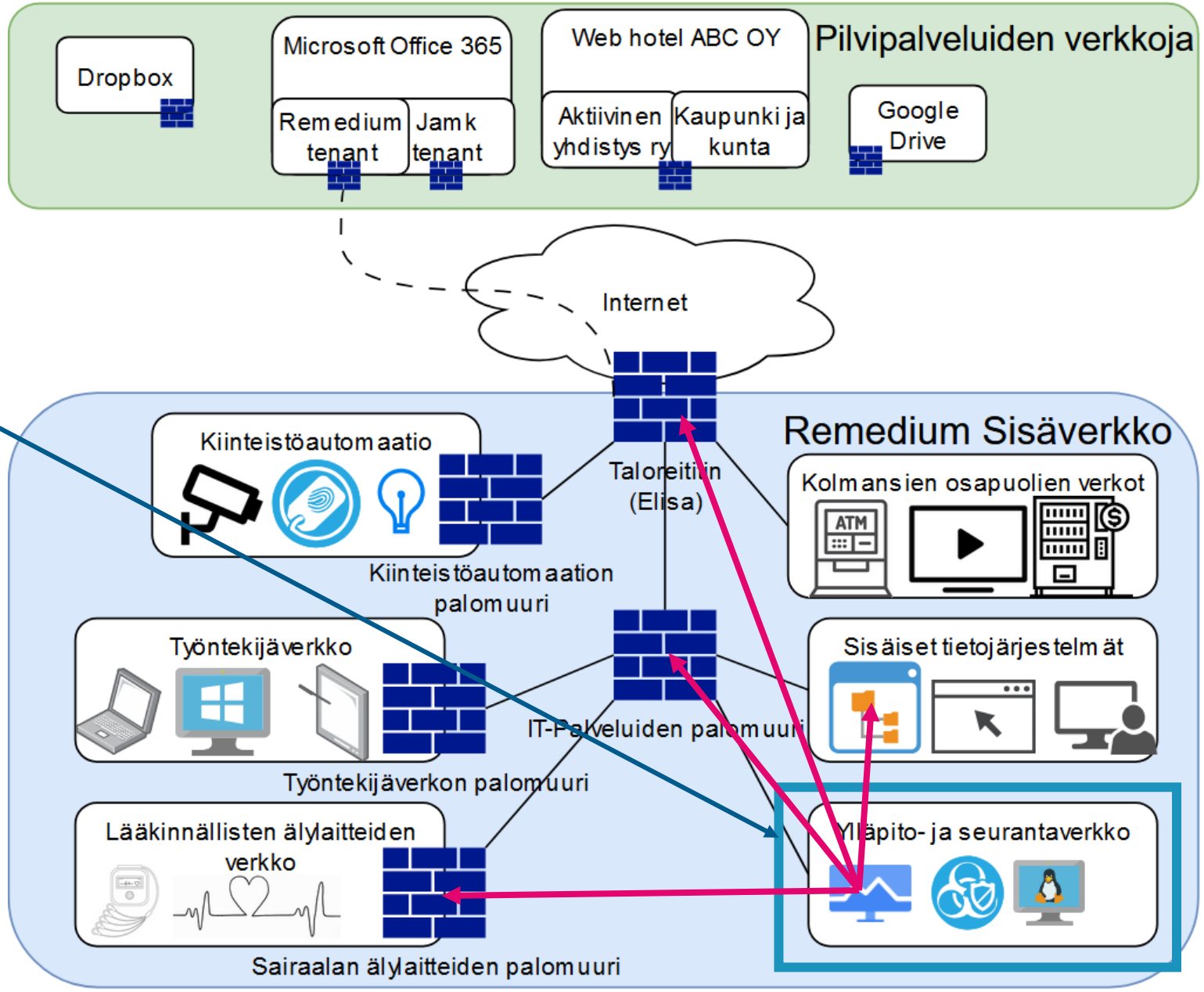


Älylaitteet

Verkkokuva esimerkki (5/6)

Ylläpito- ja seurantaverkko on tyypillisesti asetettu seuraamaan poikkeuksellista liikennettä yrityksen omista laitteista, mukaan lukien käyttäjien omat työkoneet.

- Seurantaverkko ei pysty seuraamaan pilvipalveluiden verkkoja tai työntekijän henkilökohtaisia tilejä esim. google tili

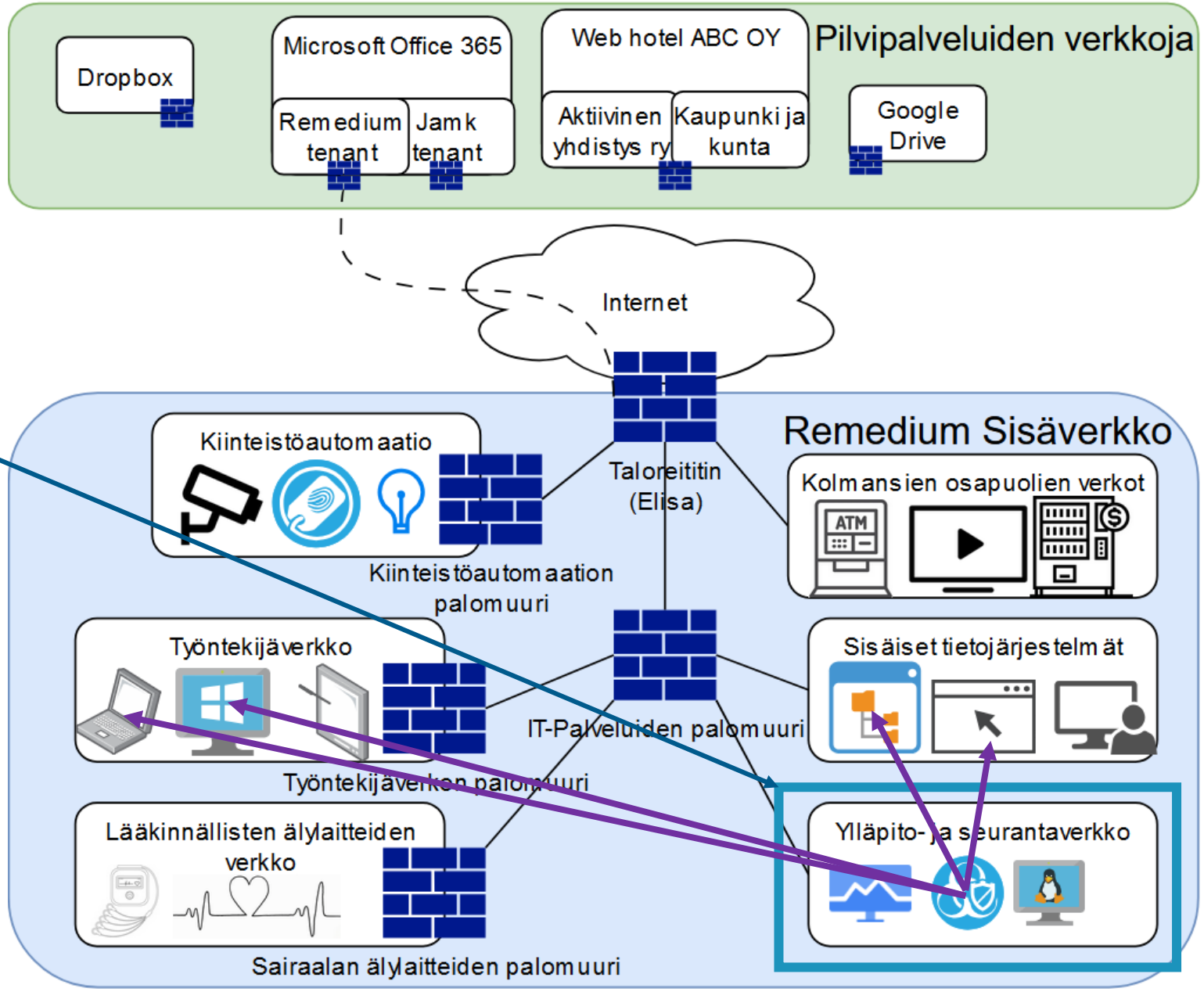


Älylaitteet

Verkkokuva esimerkki (6/6)

Seurantaverkossa on usein keskitetty tietoturvaohjelmisto (EDR), jonka pystyy asentamaan tyypillisesti vain yhteensopiviin työkoneisiin

- Näitä ei tyypillisesti pysty ottamaan käyttöön älylaitteissa (esim. EKG-laitteet)



Konesalit

Konesali/Datakeskus/Palvelinkeskus

- Huone tai rakennus, jossa on useita tietokoneita ja niiden oheisjärjestelmiä, jotka tallentavat ja käsittelevät suuria määriä dataa.
- Konesalit voivat olla paikallisia tai ne voivat sijaita muualla
- Tai joissakin ratkaisuissa sekä että, tällöin osa palveluista on paikallisia ja osa pilvessä tai toisessa konesalissa

Lähde: https://en.wikipedia.org/wiki/Data_center, viitattu 19.12.2024

Kuva: Microsoft powerpoint stock images

jamk

Älylaitteet ja pilvipalvelut

Esimerkki

- 🩺 **Esimerkki: Pilvipalvelun oletukset – "Laura ja Office 365"**
- **Tilanne:**
  Laura käyttää sairaalan tarjoamaa Office 365 -tiliä. Hän olettaa, että kaikki tiedostot ovat automaattisesti suojattuja, ja tallentaa potilastiedoston OneDriveen ilman lisäasetuksia.
- **Mitä tapahtuu:**
  - Vaikka Office 365 on sairaalan tarjoama, tiedoston jakamisasetukset voivat olla liian avoimet.
  - Laura ei huomaa, että tiedosto on jaettu "kaikille organisaatiossa".
  - Kollegat, joilla ei ole hoitosuhdetta potilaaseen, voivat nähdä tiedot.
- **Opetus:**
  Vaikka pilvipalvelu olisi virallinen, tiedostojen jakamisasetukset pitää tarkistaa. Käytä vain potilastietojärjestelmiä arkaluontoisten tietojen käsittelyyn.

Esimerkki tuotettu generatiivisen tekoälyn avulla

jamk

Älylaitteet ja pilvipalvelut

Esimerkki

- 🩺 **Esimerkki: Älylaitteen haavoittuvuus – "Mira ja potilasmonitori"**
- **Tilanne:**
  Mira käyttää potilasmonitoria, joka näyttää potilaan elintoimintoja. Monitori on yhdistetty suoraan internetiin, jotta lääkäri voi tarkastella tietoja etänä.
- **Mitä tapahtuu:**
  - Monitorissa on ohjelmistovirhe, joka mahdollistaa ulkopuolisen ohjauksen.
  - Potilastiedot voivat vuotaa ulos sairaalan verkosta.
  - Laitteen toimintaan voidaan vaikuttaa, mikä voi vaarantaa potilaan hoidon.
- **Opetus:**
  Lääkinnälliset laitteet tulee yhdistää vain suojattuihin verkkoihin. Internet-yhteys voi altistaa laitteen haavoittuvuuksille, ellei sitä ole suunniteltu turvalliseen etäkäyttöön.

Esimerkki tuotettu generatiivisen tekoälyn avulla

jamk

Tietojärjestelmät

Yleisiä tietojärjestelmiä potilaiden ja asiakkaiden hallinnointiin

- **Kanta-palvelut**: Kansallinen terveysarkisto, joka sisältää potilastiedon arkiston, sähköisen reseptin ja Omakanta-palvelun. Kanta-palvelut mahdollistavat potilastietojen turvallisen jakamisen eri toimijoiden välillä.
- **Effica**: Laajasti käytetty potilastietojärjestelmä. Tukee terveydenhuollon ammattilaisten työtä tarjoamalla kattavat työkalut potilastietojen hallintaan ja hoitoprosessien seurantaan.
- **Pegasos**: Potilastietojärjestelmä, joka on suunniteltu erityisesti perusterveydenhuollon ja erikoissairaanhoidon tarpeisiin. Tarjoaa monipuoliset työkalut potilastietojen hallintaan ja hoidon suunnitteluun.
- **Pro Consona**: Asiakastietojärjestelmä, joka on suunniteltu erityisesti sosiaalihuollon tarpeisiin.
- **Apotti**: Integroitu sosiaali- ja terveydenhuollon tietojärjestelmä, joka yhdistää potilas- ja asiakastiedot yhteen järjestelmään. Tukee palveluprosesseja ja mahdollistaa tiedon sujuvan kulun eri toimijoiden välillä.

jamk

Tietojärjestelmät

Esimerkkejä potilastietojärjestelmistä

- **Sairaala**
  - Apotti
  - ESKO
  - Lifecare
  - Mediatri
  - Pegasos
  - Radiologien PACS/RIS
  - Uranus
- **Terveyskeskus**
  - Apotti
  - GFS (Graafinen Finstar)
  - Lifecare
  - Mediatri
  - Pegasos
- **Yksityinen/muu**
  - Acute
  - DynamicHealth
  - Softmedic

Lähde: https://www.laakariliitto.fi/site/assets/files/5229/tiedotemateriaalit_polte_2021_final.pdf, viitattu 2.11.2024

jamk

Tietojärjestelmät

Yleiset Ohjelmistot - Työarkeen

- **Microsoft 365 ohjelmistot**: Teams, Word, Excel, Outlook, Onedrive
- **Muut tyypilliset ohjelmistot**: Zoom, Adobe Acrobat Reader, Trello, Dropbox, Miro
- **Paikalliset tietoturvaohjelmistot (Anti-virus)**: F-Secure, McAfee, Norton, Kaspersky
- **Keskitetyt tietoturvaohjelmistot (EDR)**: CrowdStrike, Sophos, FireEye, SentinelOne
- **Muita käytettäviä työkaluja ja virtualisoidut palvelut**:
  Etätyöpöytäsovellus (RDP), VPN, VMRC, TeamViewer, AnyDesk, Chrome Remote Desktop

jamk

Tietojärjestelmät

Yleiset Ohjelmistot - Tiedonjakoon

- **Näihin palveluihin ei sovi laittaa arkaluontoista tietoa, kuten potilas- tai asiakastietoja:**
    - **Pikaviestintä ohjelmat**: Whatsapp, Signal, Telegram, Facebook messenger
    - **Tiimiviestintään ohjelmistoja**: Slack, Microsoft Teams, Google Chat, Discord, Mattermost
    - **Pilvipalvelut tiedostojen jakoon**: Google Drive, Dropbox, Microsoft OneDrive, iCloud Drive

jamk

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences