IT-KUNTOKARTOITUS

Laaja kartoitus

Yhteistyökumppani:	Esimerkkitili Oy (kuvitteellinen)
Toimiala:	Tilitoimisto, Kuopio
Henkilöstö:	25 henkilöä
Kartoittaja:	Kalle Huttunen, KMH IT
Päivämäärä:	Maaliskuu 2026
Taso:	Laaja (2 500 € + alv)

Tämä on anonyymisoitu malliraportti. Esimerkkitili Oy on kuvitteellinen yritys. Raportin tarkoitus on näyttää konkreettisesti, mitä IT-kuntokartoituksen Laaja-tasolla saa. Todellisissa raporteissa löydökset, suositukset ja kustannusarviot perustuvat asiakkaan ympäristöön.

KMH IT · Suoraa puhetta, oikeita tuloksia

kmhit.fi · kalle.huttunen@kmhit.fi · 045 331 2224

Sisällys

1. Yhteenveto johdolle
2. Tilannekuva
3. Löydökset
4. Toimenpidesuunnitelma
5. Kustannusarvio

1. Yhteenveto johdolle

Esimerkkitili Oy:n IT-ympäristö pitää perusasiat pystyssä, mutta pinnan alla on vakavia riskejä. Tietoturvan perusta — käyttäjätunnusten hallinta, päätelaitteiden suojaus ja pääsynhallinta — on puutteellinen. Jos joku haluaisi päästä käsiksi asiakkaiden taloushallintodataan, kynnys olisi tällä hetkellä matalalla.

Kriittisimmät havainnot

- **Ylläpitotunnuksilla ei ole monivaiheista tunnistautumista (MFA).**
  Yksi kaapattu salasana riittää koko ympäristön hallintaan.
- **Jaettuja tunnuksia käytetään päivittäin.**
  Kukaan ei tiedä kuka teki mitä. Jäljitettävyys on nolla.
- **Työkalupalvelimelle pääsee pelkällä IP-osoitteella ja jaetulla salasanalla.**
  Palvelin on avoin kenelle tahansa joka tietää osoitteen.
- **Kriittisiä tietoturvapäivityksiä puuttuu osasta laitteita.**
  Tunnetut haavoittuvuudet ovat hyökkääjien ensimmäinen kohde.
- **Roskapostisuodatus puuttuu kokonaan.**
  Tietojenkalastelu on tilitoimistojen yleisin hyökkäysvektori.

Suositus

Kriittiset korjaukset (MFA, jaetut tunnukset, palvelimen pääsynhallinta) pitää tehdä heti. Nämä eivät vaadi suuria investointeja — kyse on konfiguraatiosta ja toimintatapojen muutoksesta. Arvioitu työmäärä kriittisiin korjauksiin: 2–3 päivää. Tämän jälkeen ympäristö on merkittävästi turvallisempi kuin tänään.

2. Tilannekuva

Kartoituksessa käytiin läpi Esimerkkitili Oy:n IT-ympäristö kokonaisuutena: laitteet, ohjelmistot, lisenssit, käyttäjähallinta, tietoturva ja toimintamallit. Alla ympäristön perustiedot.

Ympäristön perustiedot

Osa-alue	Tilanne
Henkilöstö	25 henkilöä, ei omaa IT-vastaavaa
Pilviympäristö	Business Basic -lisenssit (25 kpl). Ei Intunea, ei edistynyttä tietoturvaa.
Sähköposti	Exchange Online. Jakelulistoja käytössä, jaetut postilaatikot tuntemattomia käyttäjille.
Laitteet	~30 kannettavaa/pöytäkonetta. Ei keskitettyä hallintaa. Ikähajonta 1–6 vuotta.
Palvelimet	1 Windows-työkalupalvelin (toimialaohjelmisto). Ei uudelleenkäynnistetty 2 kk.
IT-toimittaja	Ulkoinen toimittaja, reagoi vain tiketteihin. Ei proaktiivista seurantaa.
Tietoturva	MFA puuttuu admin-tunnuksilta. Ei ehdollista pääsynhallintaa. Ei roskapostisuodatusta.
Käyttäjähallinta	Jaetut tunnukset käytössä. Ei JML-prosessia (tulo/muutos/lähtö).
Dokumentaatio	Ei IT-dokumentaatiota. Salasanat Excel-tiedostossa jaetulla levyllä.
Vastuut	Prosesseilla ja ohjelmistoilla ei nimettyjä vastuukäyttäjiä.

Lisenssitilanne

Lisenssi	Määrä	Käytössä	Huomio
Business Basic	25	22	3 käyttämätöntä lisenssiä (entiset työntekijät)
Toimialaohjelmisto	25	25	Palvelinversio, ylläpitosopimus voimassa
Virus/palomuuri	—	—	Vain Windowsin oma Defender, ei keskitettyä hallintaa

3. Löydökset

Alla kaikki kartoituksessa havaitut löydökset priorisoituna. Jokaisesta kerrotaan mitä havaittiin, miksi se on riski ja mitä suosittelen tehtäväksi.

KRIITTINEN | KORKEA | KESKITASO | MATALA

KRIITTINEN

K1 MFA puuttuu ylläpitotunnuksilta

Havainto: Global Admin -tunnuksilla ei ole monivaiheista tunnistautumista. Kirjautuminen onnistuu pelkällä salasanalla mistä tahansa.

Riski: Yksi vuotanut tai arvattu salasana antaa hyökkääjälle täydet oikeudet koko pilviympäristöön: sähköpostit, tiedostot, käyttäjätunnukset. Tilitoimistossa tämä tarkoittaa pääsyä satojen asiakkaiden taloustietoihin.

Suositus: Ota MFA käyttöön kaikilla admin-tunnuksilla välittömästi. Tämän jälkeen ota käyttöön kaikilla käyttäjillä. Business Basic sisältää MFA:n — lisäkustannus 0 €.

K2 Jaetut tunnukset päivittäisessä käytössä

Havainto: Useampi työntekijä kirjautuu samoilla tunnuksilla toimialaohjelmistoon ja jaettuihin kansioihin. Salasana on "yleisessä tiedossa".

Riski: Jäljitettävyys on nolla. Jos joku tekee virheen tai tahallisen muutoksen asiakkaan kirjanpitoon, on mahdotonta selvittää kuka. GDPR edellyttää henkilökohtaista tunnistautumista.

Suositus: Lopeta jaettujen tunnusten käyttö. Luo jokaiselle henkilökohtainen tunnus. Toimialaohjelmiston lisenssimalli on tarkistettava — usein henkilökohtaiset tunnukset eivät vaadi lisälisenssejä.

K3 Työkalupalvelin avoin verkosta

Havainto: Palvelimelle pääsee kirjautumaan kun tietää IP-osoitteen ja jaetun tunnuksen. Ei VPN:ää, ei IP-rajausta, ei monivaiheista tunnistautumista. Palvelinta ei ole käynnistetty uudelleen kahteen kuukauteen.

Riski: Palvelin on käytännössä avoin internetiin. Brute force -hyökkäykset RDP-porttiin ovat arkipäivää — tämä on yksi yleisimmistä kiristysohjelmien tartuntareiteistä.

Suositus: Sulje suora RDP-pääsy internetistä välittömästi. Ota käyttöön VPN tai vaihtoehtoinen etäyhteys. Käynnistä palvelin uudelleen ja asenna kaikki odottavat päivitykset.

K4 Kriittiset tietoturvapäivitykset asentamatta

Havainto: Osasta laitteita puuttuu useita viikkoja vanhoja tietoturvapäivityksiä. Päivitysten asennusta ei seurata keskitetysti.

Riski: Tunnetut haavoittuvuudet ovat hyökkääjien ensimmäinen kohde. Patch-viiveellä hyökkääjä pääsee sisään tunnetulla menetelmällä.

Suositus: Asenna puuttuvat päivitykset kaikille laitteille. Ota käyttöön keskitetty päivitysten hallinta (Intune tai vastaava).

KORKEA

H1 Roskapostisuodatus puuttuu

Havainto: Sähköpostiympäristöön ei ole konfiguroitu roskapostisuodatusta, SPF/DKIM/DMARC-asetuksia ei ole tarkistettu, eikä phishing-suojausta ole käytössä.

Riski: Tilitoimistot ovat tietojenkalastelun ykköskohteita. Ilman suodatusta huijausviestit päätyvät suoraan käyttäjien postilaatikkoon.

Suositus: Konfiguroi SPF, DKIM ja DMARC. Ota käyttöön roskapostisuodatus. Business Basic sisältää Exchange Online Protection — lisäkustannus 0 €.

H2 Ei JML-prosessia (tulo/muutos/lähtö)

Havainto: Kun työntekijä aloittaa, vaihtaa roolia tai lähtee, ei ole määriteltyä prosessia tunnusten luomiseen, muuttamiseen tai poistamiseen. Kolme käyttämätöntä lisenssiä kuuluu entisille työntekijöille joiden tunnukset ovat edelleen aktiivisia.

Riski: Entisten työntekijöiden aktiiviset tunnukset ovat vakava tietoturvariski. He pääsevät edelleen käsiksi asiakastietoihin.

Suositus: Poista entisten työntekijöiden tunnukset välittömästi. Luo yksinkertainen JML-prosessi: kuka tekee, mitä tekee, milloin tekee.

H3 Salasanat Excel-tiedostossa jaetulla levyllä

Havainto: IT-ympäristön salasanat (admin-tunnukset, palvelimet, palvelut) ovat Excel-tiedostossa johon kaikilla on lukuoikeus.

Riski: Kuka tahansa työntekijä — tai ulkopuolinen joka pääsee verkkoon — näkee kaikkien järjestelmien salasanat.

Suositus: Ota käyttöön salasananhallintaohjelma (esim. Bitwarden, avoimen lähdekoodin, ilmainen tiimeille). Poista Excel-tiedosto.

KESKITASO

M1 Ei keskitettyä laitteiden hallintaa

Havainto: Kannettavia ja pöytäkoneita ei hallita keskitetysti. Asetukset, päivitykset ja ohjelmistoasennukset tehdään laitteella käsin.

Riski: Laitteen kadotessa tai rikkoutuessa ei voida tyhjentää etänä. Uuden laitteen käyttöönotto kestää tunteja.

Suositus: Harkitse Intunea tai vastaavaa MDM-ratkaisua. Vaatii lisenssipäivityksen (Business Basic → Business Premium tai vastaava).

M2 Jaetut postilaatikot tuntemattomia

Havainto: Käyttäjät eivät tiedä jaettujen postilaatikoiden olemassaolosta. Jakelulistoja käytetään kaikkeen — myös tilanteisiin joihin jaettu postilaatikko sopisi paremmin.

Riski: Asiakasviestintää katoaa, kun sähköpostit menevät yhden ihmisen henkilökohtaiseen laatikkoon. Loma-aikana kukaan ei seuraa.

Suositus: Selvitä tarpeet ja perusta jaetut postilaatikot (esim. info@, kirjanpito@, palkanlaskenta@). Kouluta käyttäjät.

M3 Ohjelmistoilla ja prosesseilla ei nimettyjä vastuukäyttäjiä

Havainto: Kukaan ei ole nimetty vastuuhenkilöksi yhdellekään ohjelmistolle tai prosessille. Ongelmat ratkaistaan "kuka ehtii" -periaatteella.

Riski: Kun vastuuta ei ole, kukaan ei seuraa muutoksia, päivityksiä tai häiriöitä. IT-toimittajan laskutusta ei osaa kukaan arvioida.

Suositus: Nimeä jokaiselle ohjelmistolle ja prosessille vastuuhenkilö. Ei vaadi teknistä osaamista — kyse on siitä kuka pitää silmällä.

MATALA

L1 IT-dokumentaatio puuttuu kokonaan

Havainto: Ympäristöstä ei ole kirjallista dokumentaatiota: verkkorakenne, palvelimet, lisenssit, sopimukset, yhteyshenkilöt. Kaikki tieto on IT-toimittajan päässä.

Riski: Jos toimittajasuhde päättyy, tieto lähtee heidän mukanaan. Uuden toimittajan aloitus kestää viikkoja.

Suositus: Luo perusdokumentaatio: verkkokaavio, laiteluettelo, lisenssiluettelo, sopimukset, yhteyshenkilöt. Tämä voidaan tehdä kartoituksen jatkona.

L2 Vanhentuvia laitteita (1–2 vuoden sisällä)

Havainto: Neljä kannettavaa on 5+ vuotta vanhoja. Ne toimivat, mutta suorituskyky heikkenee ja takuut ovat umpeutuneet.

Riski: Laitteen hajoaminen aiheuttaa odottamattoman kustannuksen ja tuottavuuskatkon. Vanhat laitteet eivät saa enää ajuripäivityksiä.

Suositus: Suunnittele laitteiden uusinta 6–12 kk aikajänteellä. Budjetoi 4 laitetta.

4. Toimenpidesuunnitelma

Priorisoitu aikajana. Tärkeimmät ensin — kriittiset korjaukset eivät vaadi suuria investointeja.

HETI	Löydös	Toimenpide	Työmäärä
	K1	MFA käyttöön admin-tunnuksille	2h
	K3	Sulje palvelimen suora RDP-pääsy, ota VPN/vaihtoehto käyttöön	4–8h
	K2	Lopeta jaetut tunnukset, luo henkilökohtaiset	4–8h
	K4	Asenna puuttuvat tietoturvapäivitykset	2–4h
	H2	Poista entisten työntekijöiden tunnukset	1h

1 KUUKAUDEN SISÄLLÄ	Löydös	Toimenpide	Työmäärä
	K1	MFA käyttöön kaikille käyttäjille + koulutus	4h
	H1	SPF/DKIM/DMARC + roskapostisuodatus	3–4h
	H3	Salasananhallintaohjelma käyttöön	3–4h
	H2	JML-prosessin luominen	4h

3 KUUKAUDEN SISÄLLÄ	Löydös	Toimenpide	Työmäärä
	M1	Laitteiden hallinnan arviointi (Intune tms.)	Arviointi 4h
	M2	Jaetut postilaatikot + koulutus	4–6h
	M3	Vastuuhenkilöiden nimeäminen	2h (palaveri)

6 KUUKAUDEN SISÄLLÄ	Löydös	Toimenpide	Työmäärä
	L1	IT-dokumentaation luominen	8–12h
	L2	Laitteiden uusintasuunnitelma + budjetointi	2h
	M1	Keskitetyn laitehallinnan käyttöönotto (jos päätetty)	8–16h

5. Kustannusarvio

Arvio korjausten kustannuksista. Hinnat ovat suuntaa-antavia ja perustuvat kokemukseeni vastaavista ympäristöistä. Lopulliset kustannukset riippuvat toteutustavasta ja toimittajasta.

Työkustannukset (konsultointi/toteutus)

Vaihe	Toimenpiteet	Arvio
Heti	MFA, RDP-sulku, jaetut tunnukset, päivitykset, vanhat tunnukset	**1 500–2 500 €**
1 kk	MFA kaikille + koulutus, sähköpostisuojaus, salasanahallinta, JML	**1 500–2 000 €**
3 kk	Laitehallinnan arviointi, jaetut postilaatikot, vastuutus	**1 000–1 500 €**
6 kk	Dokumentaatio, laiteuusinta-suunnitelma, laitehallinnan käyttöönotto	**2 000–3 500 €**
Yhteensä (arvio)		**6 000-9 500 € + alv**

Mahdolliset lisäkustannukset

Asia	Kustannus	Huomio
Lisenssipäivitys (Business Premium)	~5 €/käyttäjä/kk	Tarvitaan Intuneen. +1 500 €/v koko organisaatiolle.
Salasananhallinta (Bitwarden)	0 € (Teams-tili)	Avoimen lähdekoodin, ilmainen tiimeille.
VPN-ratkaisu	0–50 €/kk	WireGuard (avoin lähdekoodi) tai kaupallinen.
Laitteiden uusinta (4 kpl)	3 000–5 000 €	Kannettavat, 6 kk aikajänteellä.

Mitä seuraavaksi?

Tämä raportti on teidän. Teette sillä mitä haluatte — ei jatkovelvoitteita, ei sidonnaisuuksia. Voitte toteuttaa korjaukset itse, nykyisen IT-toimittajanne kanssa tai pyytää minua auttamaan.

Jos haluatte keskustella löydöksistä tai suunnitella toteutusta, otan mielelläni puhelun tai tapaamisen. Ensimmäiset kriittiset korjaukset ovat muutaman päivän työ — ja niiden jälkeen olette merkittävästi turvallisemmassa asemassa kuin tänään.

Kalle Huttunen
KMH IT
kalle.huttunen@kmhit.fi
045 331 2224
kmhit.fi

Suoraa puhetta, oikeita tuloksia.