IT-palvelut (Bittitiimi)

Simo Horsmanheimo	Tietohallintopäällikkö
Ville Kotilainen	IT-suunnittelija, tiimiohjaaja
Mikko Nippula	IT-suunnittelija
Jyri Väistö	IT-suunnittelija
Tarja Tielinen	IT-asiantuntija
Ari Vasara	IT-asiantuntija
Joona Mustonen	IT-tukihenkilö

SAMPO
Saimaan ammattiopisto

IT-palvelut (Bittitiimi)

IT-palvelu on yksi tärkeimmistä palveluista, jota organisaatio tarvitsee. Monissa asioissa käännytään IT-palveluiden puoleen, oli sitten kysymyksessä mm. ruokapalvelut, kiinteistöpalvelut tai opintopalvelut jne.

IT-palvelujen rooli on vastata laitteiden, järjestelmien ja tietoliikenteen häiriöttömästä toiminnasta yhdessä muiden toimijoiden kanssa. Antaa opastusta ja käytöntukea niiden käyttämisestä niin lähi- kuin etätuen kautta.

Toteuttaa mm. tarpeiden mukaisia palveluja, oppimisympäristöjä, tiimi- ja neuvottelutiloja yhdessä asiakkaiden ja sidosryhmien kanssa.
Osallistuu kaikkiin hankintoihin, jossa tietoturvaan liittyvät asiat on otettava huomioon ja vastaa sovittujen tuotteiden hankinnasta. On myös mukana hakkeissa ja projekteissa.

IT-palvelut (Bittitiimi)

IT-palvelu löytyy Imatran ja Lappeenrannan toimipisteistä.

Olemme tavoitettavissa arkisin klo 7:30-15 aikana. Muina aikoina sovittava erikseen.

Otamme vastaan tukipyyntöjä:

Helpdesk	helpdesk.edusampo.fi
Asiakaspalvelunumero	040 570 5715
Sähköposti	it-palvelut@edusampo.fi

Myös sähköpostit, puhelinsoitot, käytävä- tai kahvipöytäkeskustelut IT-palveluiden henkilöiden suuntaan.

IT-palvelut (Bittitiimi)

Tukiasemia	100
Valvontakameroita	121
Dokumenttikameroita	137
Kytkimet	189
Tukiasemat (Wifi)	160
Maksupäätteet, kassat	24
Kopiokoneita	29
Kannettavat	1542
Työasemat	1191

Tulostimet	167
Puhelimet	406
Dataprojektorit	162
Dokumenttikamerat	137
Tietojärjestelmiä	133
Virtuaalipalvelimia	115
Fyysisiä palvelimia	13
Käyttäjätunnuksia	4100

IT-palvelut (Bittitiimi)

Budjettia:

Henkilöstökulut	n. 400 000 €
Palveluiden ostot	n. 160 000 €

- ICT-palvelut
- tietoliikennepalvelu

Aineet, tarvikkeet ja tavarat	n. 20 000 €
Muut toimintakulut	n. 10 000 €

- Vuokrat
- Koneiden ja laitteiden vuokrat

IT-palvelut (Bittitiimi)

Hankinnat:

Hankinnat tehdään yhdessä asiakkaiden kanssa yhdessä, kuten hankintaohjeessamme on ohjeistettu.

Puitetoimittajat:

- Kannettavat, työasemat, näytöt jne.
- Kopiokoneet
- AV-laitteet
- Microsoft-lisenssit
- Puhelimet

Kilpailutuksen tai hintatiedustelun kautta muut.

IT-palvelut (Bittitiimi)

Yhteistyö, verkostoituminen

- Toimittajien kanssa, Telia, Meita, Microsoft jne.
- Muiden oppilaitoksien kanssa
  - Kotka, Kouvola, Savonlinna yhteistyö aloitettu
- Projektien kautta
- Kaikkien kanssa (opiskelijoiden, henkilökunnan, sidosryhmien)

Kouluttautuminen:

- Henkilöstökoulutuksiin osallistumalla
- Ammattitaitoa ylläpidetään oma-aloitteisesti
  - Webinaarit
- Yhteiset koulutukset (M365, Tietokeskus 3 krt/vuosi)
- IT-palveluiden sisäinen koulutus, suunnittelijat

IT-palvelut (Bittitiimi)

Tietoturvasta yleistä:

- Käytettävä vahvoja salasanoja
- Käyttöjärjestelmät ajan tasalla -> päivitykset
- Ohjelmistot ajan tasalla -> päivitykset
- Monivaiheinen tunnistautuminen
- Varmuuskopiointi
- Käyttöoikeudet
- Käyttäjätunnukset
  - Roolit ja tehtävät
- Säilytysajat
- Lokit
- Riskienhallinta jne.

IT-palvelut (Bittitiimi)

SOC-tiimi

Tiimijäsenet: Simo Horsmanheimo, Mikko Nippula ja Jyri Väistö

Yleisesti Security Operations Center (SOC): Tämä on tietoturvavalvomo, jossa asiantuntijat valvovat yrityksen tietoturvavalmiuksia. SOC havaitsee, analysoi ja reagoi tietoturvaloukkauksiin ympäri vuorokauden.

SOC-tiimi valvoo, ehkäisee, havaitsee ja reagoi kaikkiin kyberuhkiin ja -välikohtauksiin. Toimimme toimistotyöajan puitteissa ja arkisin.

Tiimi osallistuu Taisto-harjoitukseen yhdessä muiden sovittujen henkilöiden kanssa.

Hyödynnämme Ohjeita ja oppaita tietoturvasta | Kyberturvallisuuskeskus ja seuraamme Ajankohtaista | Kyberturvallisuuskeskus sivustoa.

Kaikille palvelimien/järjestelmien ylläpitäjille tulee joka päiväiset ilmoitukset sähköpostiin haavoittuvuuksista.

IT-palvelut (Bittitiimi)

Microsoft 365 (M365) tarjoaa laajan valikoiman tietoturvatyökaluja, jotka auttavat suojaamaan organisaatioita erilaisilta kyberuhilta. Tässä muutamia keskeisiä työkaluja ja ominaisuuksia:

- Microsoft Defender for Office 365: Suojaa sähköpostia ja yhteistyötyökaluja kehittyneiltä uhkilta, kuten tietojenkalastelulta ja haittaohjelmilta.
- Azure Active Directory (Azure AD): Tarjoaa identiteetin ja pääsynhallinnan, mukaan lukien monivaiheisen tunnistautumisen (MFA) ja ehdollisen pääsyn.
- Microsoft Cloud App Security: Pilvisovellusten suojausratkaisu, joka auttaa tunnistamaan ja torjumaan pilvipalveluihin kohdistuvia uhkia.
- Microsoft Information Protection: Suojaa arkaluontoisia tietoja ja auttaa varmistamaan tietojen vaatimustenmukaisuuden.
- Advanced Threat Analytics (ATA): Tunnistaa ja tutkii kehittyneitä uhkia, vaarantuneita identiteettejä ja haitallista käyttäytymistä.
- Exchange Online Protection (EOP): Suojaa sähköpostijärjestelmiä roskapostilta ja haittaohjelmilta

IT-palvelut (Bittitiimi)

Käytämme erilaisia käytäntöjä, joita ovat esimerkiksi seuraavat:

Exchange Online Protection -käytännöt

AntiPhishPolicy on käytäntö, joka auttaa suojaamaan Microsoft 365 -palveluja **tietojenkalasteluhyökkäyksiltä**. Tämä käytäntö sisältää erilaisia suojausasetuksia, kuten monivaiheisen tunnistautumisen käyttöönoton, valvontalokit ja hälytykset, jotka auttavat havaitsemaan ja estämään tietomurtoja.

HostedContentFilterPolicy on käytäntö, joka auttaa suojaamaan Microsoft 365 -palveluja r**oskapostilta**. Tämä käytäntö sisältää erilaisia suojausasetuksia, kuten roskapostin tunnistamisen ja estämisen.

MalwareFilterPolicy on käytäntö, joka auttaa suojaamaan Microsoft 365 -palveluja **haittaohjelmilta**. Tämä käytäntö sisältää erilaisia suojausasetuksia, kuten haittaohjelmien tunnistamisen ja estämisen.

IT-palvelut (Bittitiimi)

Defender for Office 365 -käytännöt:

SafeAttachmentPolicy on käytäntö, joka auttaa suojaamaan Microsoft 365 -palveluja **haitallisilta liitteiltä**. Tämä käytäntö sisältää erilaisia suojausasetuksia, kuten liitteiden tarkistamisen virtuaalisessa ympäristössä ennen niiden toimittamista vastaanottajille.

SafeLinksPolicy on käytäntö, joka auttaa suojaamaan Microsoft 365 -palveluja **haitallisilta linkeiltä**. Tämä käytäntö sisältää erilaisia suojausasetuksia, kuten linkkien tarkistamisen ja uudelleenohjauksen turvallisille sivuille.

Microsoft Sentinel on pilvipohjainen SIEM (Security Information and Event Management) -ratkaisu, joka **tarjoaa kattavan näkymän** organisaation tietoturvaan. Se hyödyntää tekoälyä ja automaatiota tietoturvauhkien havaitsemiseen, analysointiin ja torjuntaan.

IT-palvelut (Bittitiimi)

Haasteet / parannettavaa:

- Ennakointi, havainnointi, seuranta, resurssit
- Rikolliset ovat aina edellä
  - Tekoälyä hyödynnetään rikolliseen käyttöön
- Käyttäjien osaamisen ylläpitäminen
- Riskienhallinta
- Laitekannan uusinta / rahoitus
- Windows11 käyttöönotto

Kiitos !