Kansikuva: Julia Kivelä
Pieni kannen kuva: Tero Takatalo-Eskola

10 KOHTAA KYBER-TURVALLISUUDEN PARANTAMISEKSI MATKAILUALALLA

TEM: Matkailuelinkeinon elpymistä edistävät kehityshankkeet 2020-2021.
Matkailun vastuullisuus näkyväksi Keski-Suomessa

VISIT Jyväskylä REGION

jamk

10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla

01 Tunnista ja listaa yrityksen toiminnan kannalta kriittinen tieto

Yrityksen toiminnan ja sen jatkuvuuden kannalta kaikki tieto ei ole yhtä kriittistä.

Kriittisen tiedon tunnistaa siitä, että yrityksen toiminta vaarantuu vakavasti, mikäli tieto ei ole käytettävissä, sen sisältö vääristyy tai tulee julkiseksi. Myös liiketoimintasuunnitelmat, tilaisuuksien valmisteluun liittyvät suunnitelmat ja tarjoukset sekä kiinteistöautomatiikan tai laitehuoltorekisterien sisältämät tiedot voivat olla yritykselle kriittistä tietoa.

Matkailualan erityispiirteenä on, että alalla käsitellään ja yhdistellään runsaasti henkilö- ja maksukortteihin liittyviä tietoja. Näiden tietojen käsittelyyn tulee kiinnittää erityistä huomioita.

02 Kartoita yrityksen digitaalinen toimintaympäristö ja listaa siihen kuuluvat järjestelmät

Yrityksen digitaalinen toimintaympäristö muodostuu niistä laitteista, joissa yrityksen tietoja käsitellään, siirretään tai tallennetaan. Tällaisia ovat esimerkiksi tietokoneet, verkkolaitteet, tulostimet, matkapuhelimet, kassa-, myynti-, varaus- ja sähköpostijärjestelmät. Myös video-, kulun- ja kiinteistövalvonta- sekä lukitusjärjestelmät on hyvä huomioida.

Digitaalinen toimintaympäristö eli käytettävät laitteet, sovellukset ja järjestelmät muuttuvat nopeatempoisella matkailualalla jatkuvasti. Uusia laitteita voi tulla mukaan myös kesken toimintakauden, jonka vuoksi säännöllinen listauksen päivitys on suositeltavaa.

03 Varmista, että tietojen varmuuskopiointi on hoidettu tarkoituksen-mukaisesti

Huolehdi, että toiminnan kannalta kriittiset ja tärkeät tiedot varmuuskopioidaan ja kopioita säilytetään turvallisessa paikassa. Ota huomioon kaikki laitteet, joilla tietoa käsitellään, esimerkiksi: tietokoneet, tablettitietokoneet ja matkapuhelimet. Varmuuskopiot on suojattava kiristyshaittaohjelmien varalta ja luvattomalta käytöltä. Varmuuskopioiden palauttamistakin on silloin tällöin hyvä harjoitella.

Varmuuskopioinnin ottamisen 'rytmitys' kannattaa määrittää sen mukaan, miten pitkältä ajalta tiedon katoaminen vaikuttaa liiketoimintaan ja huomioida oman matkailutoiminnan sesongit.

04 Asenna käytössä oleviin laitteisiin haittaohjelmien torjuntasovellus ja viimeisimmät ohjelmistopäivitykset

Ohjelmistojen ja haittaohjelmien torjuntasovellusten pitäminen ajan tasalla on helpoin tekninen tapa tiedon suojaamiseen. Kaikkiin laitteisiin, joista on pääsy yrityksen tietojärjestelmiin, tulisi asentaa haittaohjelmien torjuntasovellus. Laitteiden, myös verkkolaitteiden, käyttöjärjestelmät ja ohjelmistot on tärkeää päivittää säännöllisesti.

Ohjelmistojen asennukset ja niiden päivitykset kannattaa tehdä vain luotetuista lähteistä saaduilla ohjelmilla.

05 Selvitä yrityksen käyttämien ulkoisten palveluiden tieto-suojaan ja kyber-turvallisuuteen liittyvät vastuut ja velvollisuudet

Palveluntoimittajan vastuut ja velvollisuudet esimerkiksi tietojen suojaamiseen, tallentamiseen tai pokkeamista ilmoittamiseen liittyen on hyvä selvittää. Huomioitavia asioita ovat myös tietojen saatavuus tai mahdollinen siirto seuraavalle palveluntuottajalle sopimuksen päätyttyä. Nämä asiat ovat usein helpointa selvittää jo hankintavaiheessa. Kriittisten tietojen tai järjetelmien, kuten internetliittymien, osalta palvelusopimukseen kannattaa määrittää konkreettisia vaatimuksia niiden käytettävyydelle. Kannattaa myös selvittää, mitä velvoitteita sopimukset mahdollisesti asettavat tilaajalle.

Matkailutoimialalle on tyypillistä, että yhteistyötä tehdään erilaisten myynti- ja markkinointialustatoimittajien kanssa. Yhteistyö on kannatettavaa ja lisää usein merkittävästi myynnin volyymiä. Yhteistyön aloituksen yhteydessä on kuitenkin vastuullista tarkistaa tieto- ja kyberturvallisuuteen liittyvät vastuut ja velvollisuudet.

06 Laadi toimintaohjeet tietomurtojen tai tietosuoja-loukkausten varalle

Tietomurtoon tai kyberpoikkeamaan varautuminen nopeuttaa palautumista normaalitilanteeseen. Suunniteltavia asioita ovat esimerkiksi seuraavat: keneltä pyydetään apua tilanteen selvittämiseen sekä miten ja mitä tapahtuneesta tiedotetaan henkilökunnalle, asiakkaille ja mahdollisesti yhteistyökumppaneille. Tarvittavia toimenpiteitä voivat lisäksi olla myös viranomaisilmoitukset poliisille, kyberturvallisuuskeskukselle ja mahdollisesti tietosuojavaltuutetulle. Kriisiviestintäsuunnitelma, joka sisältää valmiin tiedotepohjan, on hyvä laatia ennakkoon.

Matkailualalla vastuullinen toiminta, asiakkaiden yksityisyys ja turvallisuus ovat erityisen merkityksellisiä – myös mainehaittojen torjumiseksi. Ennakkoon varautuminen minimoi mahdollisten häiriötilanteiden haitat.

07 Ota käyttöön vahvat salasanat ja poista oletussalasanat käytöstä

Heikot salasanat ja oletussalasanat ovat todellinen kyberturvallisuusriski. Oletussalasanat on vaihdettava laitteiden käyttöönottojen yhteydessä esimerkiksi helposti muistettaviksi lauseiksi. Käyttäjätunnusten on oltava henkilökohtaisia, ja tarpeettomat tunnukset on poistettava käytöstä. Salasanat on talletettava turvallisesti, mutta kuitenkin siten, että ne ovat aina ennalta sovittujen henkilöiden saatavilla. Mikäli salasanoja on paljon, salasanojen hallintasovellusten käyttäminen lisää turvallisuutta ja säästää aikaa.

Sesonkitoiminta ja sen mukanaan tuomat kausityöntekijät ovat matkailutoimialalle erittäin tyypillisiä, ja siksi salasanakäytäntöön kannattaa kiinnittää erityistä huomiota. Käyttöoikeudet kannattaa lähtökohtaisesti rajata minimiin erityisesti kausihenkilöstön ja harjoittelijoiden osalta ja muilta osin noudattaa yllä mainittua yleisohjetta.

08 Varaudu mobiililaitteiden anastamiseen tai häviämiseen

Kadonneen laitteen kautta saattaa saada pääsyn yrityksen luottamuksellisiin tietoihin tai niiden avulla voidaan tehdä haitallisia toimenpiteitä joko tarkoituksellisesti tai vahingossa. Laitteiden käyttöliittymä kannattaa lukita silloin, kun työpisteellä ei ole henkilökuntaa. Anastukselle alttiiden mobiililaitteiden paikannus, lukitus, tileiltä uloskirjaaminen tai tyhjennys kannattaa ohjeistaa ja harjoitella ennakkoon.

Usein menetetty tieto on arvokkaampi kuin itse fyysinen laite.

09 Vastuuta yrityksestä yksi henkilö huolehtimaan yrityksen tieto- ja kyberturvallisuudesta

Vastuuhenkilön tehtävinä ovat mm. henkilökunnan perehdytys ja opastus sekä sen varmistaminen, että yrityksen riskikartoituksessa ja palvelusopimuksissa on tieto- ja kyberturvallisuus huomioitu. Tehtävässä voi tarvittaessa tukeutua ulkopuoliseen palveluntarjoajaan.

Matkailuyrityksessä tehtävä on hyvä antaa kausityöntekijän sijaan mieluummin vakituisen henkilökunnan tehtäväksi tai luoda pidempiaikainen ostopalvelukumppanuus. On hyvä kuitenkin huomioida, että yritys ei voi ulkoistaa itse vastuuta ja että jokaisen työntekijän, myös kausiapulaisten, on osaltaan huolehdittava tieto- ja kyberturvallisuudesta.

10 Laadi yrityksen riskikartoitus ja kirjallinen riskienhallinta-suunnitelma.

Riskikartoituksen, jossa myös kyberturvallisuus on huomioitu, keskiöön kannattaa nostaa yrityksen kriittinen tieto ja toiminnot sekä tarkastella niitä uhkaavien tapahtumien todennäköisyyttä ja vaikuttavuutta.

Kartoituksen perusteella toimenpiteet voi kohdentaa tärkeimpien kohteiden kuntoon laittamiseen.

Kybersuojaustoimenpiteiden vuosikellon laatiminen

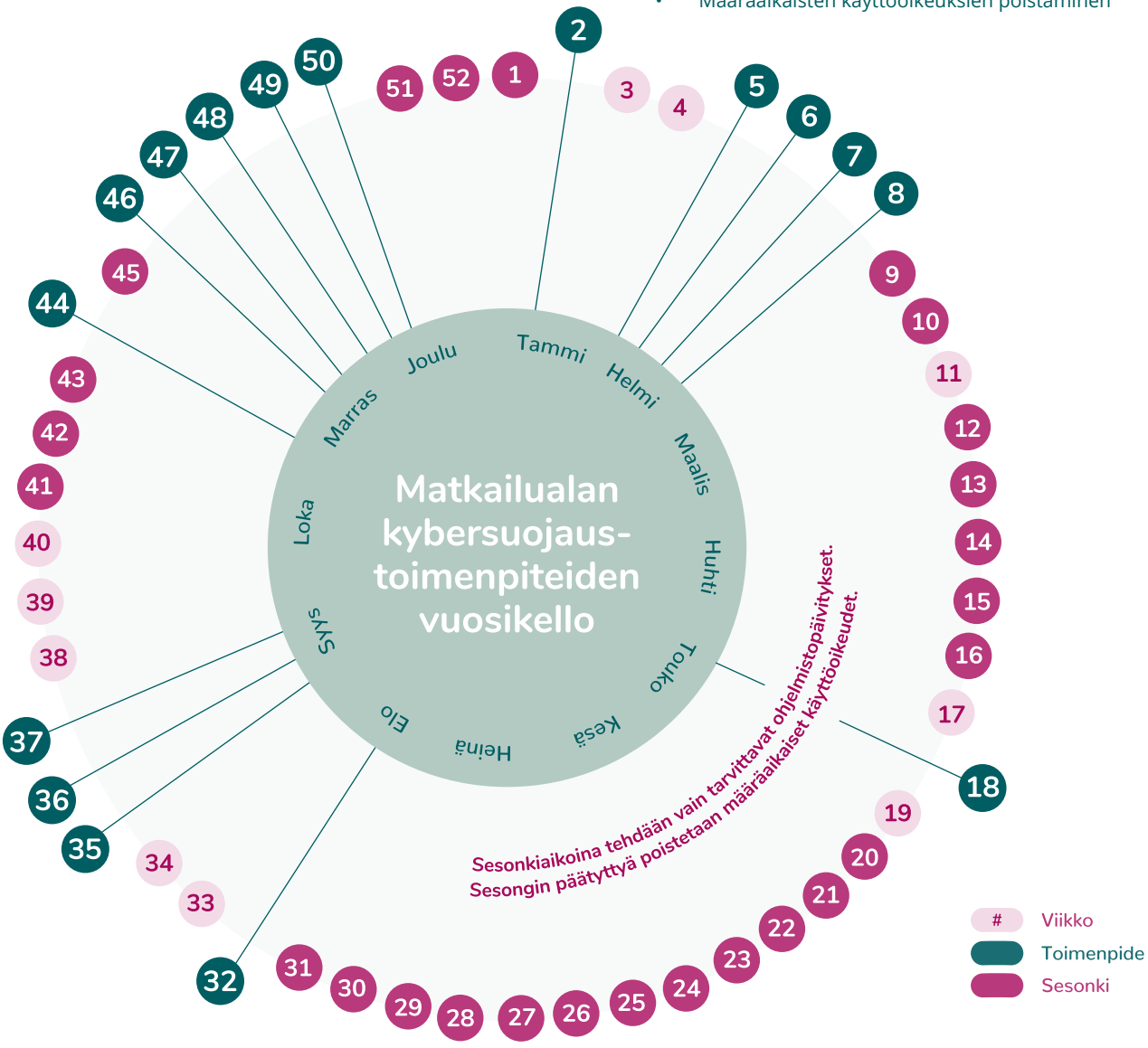
Jokaisella yrityksellä on sille ominainen vuosirytminsä, jota tahdittavat matkailun sesonkikaudet. Merkittävän osan kybersuojaustoimenpiteistä voi ja kannattaakin tehdä matkailusesonkien ulkopuolella. Vuosikellon laatimiseksi ensin kannattaa laatia toimenpidelista, joka on pyritty järjestämään loogiseen ja kronologiseen järjestykseen.

Kun lista on laadittu, toimenpiteet voidaan jakaa kalenterivuodelle pääsääntöisesti sesonkien ulkopuolelle. Kannattaa kuitenkin huomioida, että osa toimenpiteistä saattaa olla jatkuvia, myös sesonkikaudella. Osa tehtävistä voi olla vuoden mittaan useaan kertaan toistuvia, esimerkiksi sesongin jälkeen kiireapulaisten käyttöoikeuksien poisto tai salasanojen vaihtaminen.

Oheisessa esimerkissä on kolme sesonkikautta kuvattuna punaisella värillä. Vihreällä värillä on kuvattu suojaus- ja varautumistoimenpiteet aikataulutettuna sesonkien ulkopuolelle.

Esimerkki toimenpidelistasta:

- Kriittisen tiedon määrittely
- Digitaalisen toimintaympäristön kartoitus
- Käyttöoikeuksien tarkastus
- Riskikartoituksen tekeminen
- Riskien hallintasuunnitelmien laadinta
- Voimassa olevien palvelusopimuksien ajantasaisuuden tarkastaminen
- Ohjelmistopäivitysten tekeminen
- Salasanojen vaihto
- Tietosuoja- ja kyberpoikkeamien toiminta- ja tiedotussuunnitelmien laatiminen/päivitys
- Riskien hallintasuunnitelman toimeenpano
- Varmuuskopioinnin onnistumisen varmentamien
- Virustorjunnan kattavuuden tarkastaminen
- Tietosuojaan ja kyberturvaan liittyvän perehdytysmateriaalin päivitys
- Määräaikaisten käyttöoikeuksien poistaminen



Viikko Toimenpide

2 Salasanojen vaihto
5 Varmuuskopioinnin onnistumisen varmentamien
6 Virustorjunnan kattavuuden tarkastaminen
7 Tietosuojaan ja kyberturvaan liittyvän perehdytysmateriaalin päivitys
8 Riskien hallintasuunnitelman toimeenpano
18 Salasanojen vaihto
32 Salasanojen vaihto
35 Digitaalisen toimintaympäristön kartoitus
36 Käyttöoikeuksien tarkastus
37 Kriittisen tiedon määrittely
44 Salasanojen vaihto
46 Riskikartoituksen tekeminen
47 Riskien hallintasuunnitelmien laadinta
48 Voimassa olevien palvelusopimusten ajantasaisuuden tarkastaminen
49 Ohjelmistopäivitysten tekeminen
50 Tietosuoja- ja kyberpoikkeamien toiminta- ja tiedotussuunnitelmien laatiminen/päivitys