Kyberturvalliset
ekosystеemit Päijät-Häme

Pienyrityksen tietoturvaopas

Euroopan unionin
osarahoittama

Päijät-Hämeen liitto

LAB University of
Applied Sciences

SISÄLLYSLUETTELO

Euroopan unionin osarahoittama

Päijät-Hämeen liitto

LAB University of Applied Sciences

JOHDANTO

Tietoturvaa tulisi ajatella, käsitellä ja kehittää kokonaisuutena. Yrityksen on hyvä laatia yhteiset tietoturvakäytännöt, -suunnitelma ja -ohjeet, joita työntekijät voivat tukeutua. Tietoturva on sekä hallinnollista, että teknistä. Sen osa-alueet ovat luottamuksellisuus, eheys ja käytettävyys.

Luottamuksellisuus (confidentiality)

- Tiedon ominaisuus, joka ilmentää sitä, että tieto on vain sen käyttöön oikeutettujen käytettävissä eikä se paljastu muille

Eheys (integrity)

- Tiedon ominaisuus, joka ilmentää sitä, että tietoa ei ole muutettu luvatta tai että se ei ole muuttunut vahingossa ja että mahdolliset muutokset voidaan todentaa

Käytettävyys (saatavuus/availability)

- Ominaisuus, joka ilmentää sitä, että tieto, tietojärjestelmä tai palvelu on niihin oikeutettujen hyödynnettävissä haluttuna aikana ja vaaditulla tavalla

Tietoturvaopas auttaa yrityksen toimintaa keräämällä yleisimmät tietoturvallisuuteen liittyvät asiat yhden dokumentin taakse. Yritys pystyy oppaan avulla perehdyttämään uudet työntekijät nopeammin, ohjaamaan nykyisiä työntekijöitä tutustumaan siihen, sekä nopeuttamaan ongelmien ratkomista.

Tietoturvaopas sisältää yrityksen toiminnan kannalta välttämättömien laitteiden, ohjelmien ja tiedostojen käsittelyyn liittyviä toimintatapoja. Seuraavissa osioissa käydään läpi yleisimpiä tietoturvallisuuteen liittyviä ongelmakohtia, mitä haittaa niistä voi yritykselle syntyä, sekä miten niitä pystytään torjumaan.

KÄSITELISTA

Bottiverkko (Robot network)
Bottiverkko tarkoittaa suurta määrää saastuneita päätelaitteita, joita hallinnoi hakkeri. Bottiverkon laitteita käytetään usein rikolliseen toimintaan.

DNS -suodatus (Domain Name System)
DNS tulee sanoista Domain Name System, se on järjestelmä, joka kääntää nettiosoitteet IP-muotoon. Esimerkiksi yle.fi palauttaa IP-osoitteeksi 108.156.22.60. Suodattamalla DNS -osoitteita, palautetaan käyttäjälle vain turvalliset osoitteet, eli estetään käyttäjää päätymästä haitalliselle sivustolle.

Haittaohjelma (Malware)
Haittaohjelma on yleisnimitys ohjelmalle, jonka tarkoitus on aiheuttaa päätelaitteen käyttäjän kannalta ei-toivottuja tapahtumia.

IP -osoite (Internet Protocol Address)
IP-osoite on yksilöitävä osoite, jonka perusteella päätelaite tunnistetaan lähi- ja ulkoverkossa. Se on neljän numeron joukko, jotka on eroteltu pisteillä. Päätelaitteella on oma IP-osoite lähi- sekä ulkoverkossa. Esimerkiksi päätelaitteen lähiverkon osoite voi olla 192.168.80.105 ja ulkoverkon 82.225.104.44.

Kiristysohjelma (Ransomware)
Kiristysohjelman tarkoitus on salata tai lukita päätelaite tai osa sen tiedostoista sekä vaatia lukituksen purkamisesta lunnaita.

Konfigurointi (Configuration)
Konfiguraatiolla tarkoitetaan päätelaitteen, ohjelman, ohjelmiston, sovelluksen tai vastaavan asetusten säätämistä.

Kyberturva (Cyber security)
Kyberturva on osa tietoturvaa. Se keskittyy tiedon, tietojärjestelmien ja laitteiden turvallisuuden takaamiseen verkkoympäristössä.

KÄSITELISTA

Käyttöjärjestelmä (Operating system)
Käyttöjärjestelmä on ohjelmistokokonaisuus, joka huolehtii käyttämäsi päätelaitteen ja siihen asennettujen ohjelmien yhteistoiminnasta.

Käyttöoikeus (Access right)
Yrityksen hallinnoima oikeus käyttää yrityksen päätelaitteita, sovelluksia tai tiedostoja.

Lokitieto (Log data)
Tietojärjestelmän muistiin automaattisesti kirjautuva tapahtumatieto. Voi sisältää erilaisia tunnistautumistietoja.

Modeemi (Modem)
Modeemi on laite, joka yhdistää päätelaitteen verkkoon.

Monivaiheinen tunnistaminen (Multifactor Authentication, MFA)
Tavanomaisen tunnistautumisen (esimerkiksi käyttäjätunnus + salasana) lisäksi suoritettava ylimääräinen tunnistautuminen toisen menetelmän kautta (esimerkiksi sähköpostitse lähetettävä kertakäyttöinen koodi)

Palomuuri (Firewall)
Palomuuri on fyysinen laite tai ohjelma, jonka tarkoitus on estää luvaton tai asiaton pääsy verkosta tai verkon osasta toiseen.

Palvelin (Server)
Palvelin on tietokone, ohjelmisto tai näiden yhdistelmä, joka hoitaa tiettyjä tehtäviä muiden samaan verkkoon kytkettyjen tietokoneiden pyyntöjän ohjaamana tai niiden puolesta.

KÄSITELISTA

Pilvipalvelu (Cloud service)
Pilvipalvelulla tarkoitetaan hajautettua verkkopalvelua, jossa tietokoneita, ohjelmia, tallennustilaa tai muita tietoteknisiä palveluita käytetään verkon kautta.

Public Key Infrastucture (PKI)
PKI on sähköpostiviestinnän salausmenetelmä, jossa viestin lähettäjä käyttää julkista avainta ja viestinvastaanottaja yksityistä avainta.

Päätelaite (Data terminal equipment)
Päätelaite on mikä tahansa verkkoliikenteeseen yhdistettävä laite.

Reititin (Router)
Reititin on laite, joka vastaanottaa digitaalisen signaalin (esimerkiksi modeemilta) ja jakaa sen useammalle päätelaitteelle.

Sovellus, applikaatio (Program, application)
Sovellus tai applikaatio on käyttäjän käytettäväksi tarkoitettu ohjelma tai ohjelmakokonaisuus, joka toteuttaa tietyn tehtävän tai tiettyjä tehtäviä.

Tietokonemato (Worm)
Tietokonemato on haittaohjelma, joka leviää kopioimalla itseään päätelaitteella.

Tietoliikenneverkko (Telecommunications network)
Tietoliikenneverkko on laitteista ja niiden välisistä viestiyhteyksistä koostuva verkko, jota käytetään tiedon välittämiseen.

KÄSITELISTA

Tietoturva (Information security)
Tietoturva on yrityksen toiminnan kannalta välttämättömien laitteiden, ohjelmien ja tiedostojen käsittelyyn liittyviä turvallisia toimintatapoja.

Tietoturva-aukko (Vulnerability)
Tietoturva-aukko, eli haavoittuvuus, on ongelma tai virhe sovelluksessa, joka mahdollistaa sen väärinkäytön tai hyväksikäytön. Ne voivat pahimmillaan antaa ulkopuoliselle vapaan pääsyn päätelaitteeseen, häiritä laitteen toimintaa tai aiheuttaa muuta harmia.

Troijalainen (Trojan horse)
Troijalainen on haittaohjelma, joka on naamioitu näyttämään toiselta sovellukselta tai ohjelmalta.

Vakoiluohjelma (Spyware)
Vakoiluohjelman tarkoitus on vakoilla päätelaitetta, sen käyttöä ja lähettää keräämänsä tiedot ohjelmassa määritettyyn osoitteeseen.

Varmuuskopio (Back up)
Varmuuskopioinnilla tarkoitetaan tiedon kopiointia alkuperäisen tallennuspaikan lisäksi yhteen tai useampaan paikkaan.

Virustorjunta (Virus protection)
Virustorjunnalla tarkoitetaan haittaohjelmien estämistä päätelaitteelle. Sen tarkoitus on tunnistaa saastuneet tiedostot ja joko puhdistaa, poistaa tai eristää ne.

PÄÄTELAITTEIDEN SUOJAUS

MITÄ PÄÄTELAITTEET OVAT?

Yrityksillä on käytössään monia erilaisia päätelaitteita, joita henkilökunta käyttää työskentelyyn. Päätelaitteita ovat kaikki tietoliikenneverkkoon kytkettävät laitteet, kuten puhelimet, tabletit ja tietokoneet.

MITEN PÄÄTELAITTEITA SUOJATAAN?

Tietokoneet ja mobiililaitteet tulee suojata ulkopuolisilta käyttäjiltä. Henkilökunnalla tulee olla henkilökohtaiset käyttäjätunnukset, joita vaaditaan laitteiden käyttöön. Laitteet tulee myös lukita aina kun niitä ei käytetä aktiivisesti.

Laitteiden sisältämä tieto tulee salata. Mikäli laite päätyy vääriin käsiin, voi käyttäjä päästä laitteen kovalevyn sisältämiin tietoihin käsiksi, vaikka ei pystyisikään koneeseen kirjautumaan. Tästä syystä laitteen massamuistin sisällön salaus on tärkeä osa tietojen suojausta.

Etenkin yrityksen ulkopuolella, kuten julkisissa tiloissa mukana olevat laitteet tulisi suojata useammalla toisiaan täydentävällä suojauskeinolla. Näitä keinoja ovat muun muassa laitteen salaus, vahva tunnistautuminen, automaattinen lukitus, VPN ja ajantasainen haittaohjelmasuojaus. Näitä suojauskeinoja käyttämällä muodostetaan riittävä suojaus liikkuvaan työhön.

MITÄ TAPAHTUU JOS SUOJAUS PETTÄÄ?

Mikäli päätelaitteita ei suojata, voi niihin päästä ulkopuolinen käsiksi ja arkaluontoiset dokumentit sekä salassa pidettävät asiakirjat voivat joutua vääriin käsiin. Jos laite jätetään lukitsematta sen ääreltä poistuessa, voi kuka tahansa päästä käsiksi laitteen tietoihin ja tuhota niitä. Myös vakoilu- ja haittaohjelmia pystytään asentamaan laitteelle.

MITEN TOIMIA, JOS SUOJAUS PETTÄÄ?

Jos ulkopuolinen henkilö on päässyt kirjautumaan päätelaitteelle, tulee selvittää, mitä tietoa hän on saanut haltuunsa ja onko tiedostoja kopioitu. On myös syytä selvittää, miten ulkopuolinen on päässyt laitteelle.
Ulkopuolinen tunkeutuja on voinut saada laitteelta käsiinsä eri verkkopalveluiden tunnuksia ja salasanoja. Verkkopalveluiden ja laitteen salasanat tulee vaihtaa välittömästi.

PÄIVITYKSET

PÄIVITYKSET

Henkilökunnan ja yrityksen käytössä olevat käyttöjärjestelmät, sovellukset, applikaatiot ja ohjelmat on suositeltava päivittää aina uusimpaan ohjelmaversioon. Uusimmassa versiossa on yleisesti otettu huomioon mahdolliset turvallisuusriskit ja korjattu suurimmat viat. Päivitykset kannatta automatisoida, jotta ne ladataan ja asennetaan automaattisesti.

Etenkin käyttöjärjestelmä (Windows, MacOS ja Linux) tulisi päivittää aina uusimpaan versioon. Myös laitteet tulisi päivittää viimeistään silloin, kun niihin ei ole enää saatavilla tietoturvapäivityksiä.

PÄIVITYSTEN AUTOMATISOINTI

Päivitykset voidaan automatisoida tapahtumaan päivittäin tai viikoittain. Automatisointi tapahtuu esimerkiksi käyttöjärjestelmän kohdalla navigoimalla päivityksen asetuksiin (update setttings) ja valitsemalla "Päivitä automaattisesti" (Update automatically).

PÄIVITTÄMÄTTÖMÄTTÖMÄT LAITTEET JA JÄRJESTELMÄT OVAT HAAVOITTUVAISIA

Jos käyttöjärjestelmiä, sovelluksia, applikaatioita tai ohjelmia ei ole päivitetty uusimpaan versioon, pystyvät ulkopuoliset toimijat hyväksikäyttämään niiden haavoittuvuuksia. Haavoittuvuudet voivat pahimmillaan sallia pääsyn yrityksen verkkoon tai mahdollistaa haittaohjelmien asentamisen.

Mikäli päivityksiä ei asenneta automaattisesti tai päivittäminen epäonnistuu, tulisi ohjelmat päivittää manuaalisesti. Päivittämätön laite tulisi tarkistaa mahdollisten haavoittuvuuksien varalta. Mikäli päätelaitteelle ei enää ole saatavilla tietoturvapäivityksiä, tulisi se päivittää uudempaan laitteeseen.

PALOMUURIT JA VIRUSTORJUNTA

PALOMUURIT JA VIRUSTURVA YRITYKSEN LAITTEISSA

Yrityksen käytössä olevissa laitteissa tulee olla toimiva palomuuri ja ajantasainen virustorjunta. Virustorjunnan olisi hyvä suorittaa automaattisesti päivittäinen nopea skannaus sekä viikoittainen täysi skannaus.

MITÄ SUOJATAAN?

Suojaa käytössä olevat laitteet luotettavalla palomuurilla ja virustorjunnalla. Muun muassa F-Secure tarjoaa asiakkailleen kokonaisvaltaisen paketin, johon sisältyy Windows:in palomuurin kanssa yhteensopiva virustorjunta. Tämän lisäksi on suositeltavaa suojata yrityksen nettiyhteydet joko suoraan reitittimen omalla palomuurilla tai erillisellä palomuurilla.

MITÄ TAPAHTUU, JOS PALOMUURIA TAI VIRUSTORJUNTAA EI KÄYTETÄ?

Ilman toimivaa palomuuria, ulkopuoliset toimijat pystyvät pääsemään käsiksi yrityksen laitteisiin, dokumentteihin ja sähköpostiin. Virustorjunta puolestaan estää haittaohjelmien pääsyn koneelle.

MITÄ TEHDÄ, JOS ULKOPUOLINEN LÄPÄISEE PALOMUURIN TAI VIRUSTORJUNTA PETTÄÄ?

Jos palomuurin lävitse pääsee ulkopuolinen laite tai käyttäjä, tulee palomuurin toiminta selvittää ja poistaa haavoittuvuudet.

Vaikka virustorjunta olisi ajan tasalla ja päivitetty, voi viruksia silti päätyä laitteille. Mikäli näin tapahtuu, tulee saastuneet tiedostot poistaa heti ja selvittää mitä virus on ehtinyt tehnyt laitteella.

SALASANAKÄYTÄNNÖT

YLEISET SALASANAKÄYTÄNNÖT

Henkilökunta tiedostaa salasanakäytännöt ja tunnistaa vahvan salasanan. Salasanat tulee vaihtaa säännöllisesti ja uuden salasanan tulee olla eri kuin vanhan.

Yrityksen tulee ohjeistaa henkilökuntaa salasanojen luomisessa ja niiden turvallisesta käytöstä. Henkilökunnalla tulisi olla omat henkilökohtaiset salasanat, jotka ovat vähintään 12 merkkiä pitkiä, sisältävät sekä pieniä että isoja kirjaimia, numeroita ja erikoismerkkejä. Salasanojen ei tulisi olla sanoja tai lauseita, vaan niiden olisi hyvä olla sekoitus kirjaimia, numeroita ja merkkejä, joita ei pysty arvaamaan.

SALASANOJEN TURVAAMINEN

Salasanat pitäisi vaihtaa säännöllisesti eikä niitä ei tule tallentaa laitteille tekstimuodossa tai kirjoittaa ylös paperille. Samaa salasanaa ei myöskään tulisi käyttää eri palveluissa, sillä mikäli yhden palvelun tiedot vuotavat, voivat ulkopuoliset henkilöt päästä käsiksi myös toiseen palveluun. Samoja salasanoja ei tule myöskään käyttää henkilökohtaisissa palveluissa, kuten henkilökohtaisessa sähköpostissa.

TURVALLISEN SALASANAN LUOMINEN

Älä käytä salasanoja, jotka on helppo arvata. Helposti arvattava salasana on esim. qwerty, joka on jono merkkejä suoraan näppäimistöstä. Älä myöskään käytä etunimi+sukunimi yhdistelmää tai lyhyttä numerosarjaa, joka on syntymäaikasi. Ne on helppo arvata, mikäli kirjautujalla on nämä perustiedot sinusta tiedossa. Ne ovat myös asioita, jotka on helppo saada selville. Ulkopuolinen henkilö voi helposti murtaa helpon salasanan ja päästä käsiksi yrityksen infrastruktuuriin ja sen kautta laitteisiin sekä tiedostoihin.

Pidä huoli, että salasana pysyy turvassa eikä sitä ole helppo murtaa.

MITÄ TEHDÄ, JOS SALASANNAT VUOTAVAT?

Mikäli salasanakäytäntöä ei noudateta tai salasanavuotoja tapahtuu, pitää henkilökuntaa ohjeistaa uudestaan salasanakäytännöstä. Mikäli yrityksen tietoja on vuotanut, tulee heti selvittää mitä tietoja vuoti, mistä ja minne ne vuotivat.

MONIVAIHEINEN TUNNISTAUTUMINEN

Multifactor authentication, MFA

MIKÄ ON MONIVAIHEINEN TUNNISTAUTUMINEN?

Monivaiheisella tunnistautumisella tarkoitetaan esimerkiksi käyttäjätunnuksen ja salasanan lisäksi sovelluksella tai sähköpostiin lähetetyllä koodin avulla tunnistautumista. Kirjautumista ei pysty suorittamaan loppuun, ilman kirjautumisalustan ulkoista tunnistautumista.

Mahdollisuuksien mukaan, on suositeltavaa käyttää palveluihin kirjautumiseen monivaiheista tunnistautumista. Palveluiden käyttäminen vaatii monivaiheista tunnistautumista käyttäjiltään joko jokaisella kirjautumiskerralla tai tietyllä aikavälillä, kuten kerran viikossa.

Monivaiheinen tunnistautuminen ehkäisee tietovuotoja ja parantaa yrityksen tietoturvallisuutta vaikeuttamalla ei-toivottujen tahojen pääsyä palveluihin tai järjestelmiin.

MITEN MONIVAIHEINEN TUNNISTAUTUMINEN TOIMII?

Kirjautuessaan käyttäjää pyydetään hyväksymään kirjautuminen tai syöttämään näytöllä näkyvä koodi erilliseen tunnistautumissovellukseen eli Authenticatoriin. Vaihtoehtoisesti kirjautuminen voidaan pyytää vahvistamaan tekstiviestillä tai sähköpostiin tulleen kertakäyttöisen koodin avulla.

MIKSI MONIVAIHEINEN TUNNISTAUTUMINEN TULISI OTTAA KÄYTTÖÖN, MIKÄLI SE EI VIELÄ OLE?

Ilman monivaiheista tunnistautumista ulkopuoliset henkilöt pystyvät käyttämään hyväkseen vuotaneita salasanoja ja joissakin tapauksissa salasanan palauttamiseen tarkoitettuja työkaluja, kuten "Unohtuiko salasana?" tai "Unohtuiko käyttäjätunnus?". Pahimmassa tapauksessa käyttäjätili voidaan kaapata tätä haavoittuvuutta hyödyntäen.

Mikäli monivaiheista tunnistaminen ei ole käytössä ja yrityksen henkilökunnan tunnukset päätyvät ulkopuolisen käsiin, tulisi tunnukset deaktivoida mahdollisimman pian. Parhaiten suojaat yrityksen tietoja, kun otat käyttöön monivaiheisen tunnistautumisen kaikkiin palveluihin.

TIETOTURVAN VASTUUHENKILÖ

KUKA ON YRITYKSEN TIETOTURVAN VASTUUHENKILÖ?

Tietoturvan vastuuhenkilö on yrityksen määrittävä henkilö, joka vastaa tietoturvallisuuteen liittyvistä asioista. Käytännössä toimitusjohtaja kantaa loppu viimein vastuun tietoturvan toteutumisesta, mutta hän voi delegoida tehtäviä muulle henkilökunnalle.

TIETOTURVAN VASTUUHENKILÖN VASTUUT

Yritys on nimennyt henkilön, joka vastaa tietoturvasta. Vastuuhenkilö tarkistaa säännöllisesti tietoturvallisuuden riittävyyden ja uusimmat ohjeistukset ja on muodollisesti vastuussa tietoturvallisuuteen liittyvistä toimista.

Nimetty vastuuhenkilö auttaa pitämään tietoturvaan liittyvät asiat hallinnassa ja toimii yhteyshenkilönä, kun kysymyksiä tai ongelmatilanteita esiintyy.

KÄYTTÖOIKEUDET JA LOKITIEDOT

KÄYTTÖOIKEUKSIEN MERKITYS

Yritys huolehtii käyttöoikeuksista varmistamalla vain niihin oikeutettujen henkilöiden pääsyn tiettyihin ohjelmiin, palveluihin, kansioihin, tiedostoihin tai muuhun infrastruktuuriin.

HENKILÖKOHTAISET TUNNUKSET JA LOKITIETOJEN SEURANTA

Henkilökunnalla on omat henkilökohtaiset tunnukset, joilla he voivat kirjautua yrityksen laitteille, järjestelmiin sekä käyttää ohjelmia. Yritys hallitsee, päivittää ja seuraa käyttöoikeuksien ajantasaisuutta ja niiden käyttöä. Käyttäjien tiedot ja toiminnot tallentuvat palvelimelle, josta syntyy lokitietoja, joita yritys pystyy seuraamaan.

YHTEISKÄYTTÖISTEN TUNNUSTEN HAAVOITTUVUUS JA RISKIT

Mikäli yritys ei ole luonut henkilökohtaisia käyttöoikeuksia tai niitä ei hyödynnetä yrityksen toiminnassa, pystyvät ulkopuolisilla toimijoilla mahdollisuus päästä käsiksi laitteisiin, ohjelmiin, sähköpostiin. Pahimmissa tapauksessa yrityksen tietoja voidaan kopioida, levittää eteenpäin tai poistamaan. Yhteiskäyttöisten tunnusten seuranta on myös haastavaa. Niitä käyttämällä on hankala tunnistaa, kuka on kirjautunut laitteille tai järjestelmiin. Jos tietoja kopioidaan tai hävitetään, on tekijää vaikea tunnistaa.

TOIMENPITEET HAAVOITTUVUUDEN TOTEAMISEN JÄLKEEN

Jos yrityksen laitteisiin, ohjelmiin ja palveluihin pääsee ulkopuolinen käsiksi, tulisi yrityksen selvittää miksi tämä tapahtui. Ovatko henkilökunnan käyttäjätunnukset vuotaneet tai onko käyttöoikeuksissa ja niiden seurannassa puutteita.

HAITTAOHJELMAT

MIKÄ ON HAITTAOHJELMA?

Haittaohjelma (Malware) on yleinen käsite ohjelmalle, jonka tarkoitus on aiheuttaa vahinkoa tai kalastella tietoja. Haittaohjelmia ovat muun muassa mainosohjelmat, tietokonemadot, vakoilu- ja kiristysohjelmat sekä troijalaiset.

MAINOSOHJELMA

Mainosohjelmat (Adware) ovat haittaohjelmia, jotka yleensä asentuvat laitteelle toisen sovelluksen yhteydessä. Esimerkiksi asentaessaan laitteelle ilmaisversiota ohjelmasta, saattaa käyttäjä huomaamattaan samalla asentaa myös vakoiluohjelman.

TIETOKONEMATO

Tietokonemadot pyrkivät tunkeutumaan päätelaitteille tietoturva-aukkojen kautta ja leviämään saastuneen päätelaitteen avulla muihin päätelaitteisiin. Yleisin leviäminen tapahtuu sähköpostiviestin liitteen kautta. Kun käyttäjä avaa saastuneen liitteen, asentuu päätelaitteelle tietokonemato. Saastutettuaan päätelaitteen, voi mato alkaa lähettämään sähköpostiviestejä, kopioimaan ja/tai tuhoamaan tiedostoja tai vakoilemaan päätelaitetta.

VAKOILUOHJELMA

Vakoiluohjelmat päätyvät laitteille yleensä haitallisen linkin, esimerkiksi huijausviestin tai sähköpostiviestin kautta. Vakoiluohjelman avulla ulkopuolinen henkilö pystyy seuraamaan laitteen viestintää sekä pääsemään käsiksi selaustietoihin. Jotkin vakoiluohjelmat myös mahdollistavat laitteiden etäkäytön tai ylimääräisten ohjelmien asentamisen.

KIRISTYSOHJELMA

Kiristysohjelma salaa tai lukitsee päätelaitteen, jonka jälkeen se vaatii käyttäjää maksamaan salauksen tai lukituksen purkamisesta. Kiristysohjelmat tarttuvat yleisimmin haitallisen sivuston tai sähköpostiliitteen kautta.

TROIJALAINEN

Troijalainen naamioi itsensä tavalliseksi ohjelmaksi tai tiedostoksi, mutta on oikeasti virus, jolla pyritään varstamaan luottamuksellista tietoa, kaappaamaan laite tai vakoilemaan laitteen toimintaa. Troijalaisia esiintyy niin sähköpostiviesteissä liitteinä, huijausviesteissä sekä huijaussivustoilla.

HAITTAOHJELMAT

HAITTAOHJELMIEN AIHEUTTAMAT ONGELMAT

Haittaohjelmat varastavat tietoa, levittävät sitä eteenpäin, vakoilevat päätelaitteita sekä voivat lukita käyttäjät ulos niistä. Pahimmillaan päätelaitteet joudutaan uudelleenasentamaan. Mikäli haittaohjelmat pääsevät leviämään myös muihin yrityksen päätelaitteisiin, voidaan nekin joutua uudelleenasentamaan, jotta haittaohjelmat voidaan torjua ja estää.

Haittaohjelman saastuttama päätelaite saattaa yhdistää päätelaitteen bottiverkkoon, jolloin tietoja vuotaa ulkopuolelle.

MITEN TOIMIA, KUN HAITTAOHJELMA HAVAITAAN?

Suojauksen pettäessä, toimintatapa valitaan haittaohjelman mukaan.

Yleensä mainosohjelmien osalta sovelluksen poistaminen riittää. On silti hyvä tarkastaa, että mainosohjelma oli vain mainoksia varten, eikä sen yhteydessä päätelaitteelle asentunut mitään muuta.

Tietokonemadon kohdalla toimintatapa vaihtelee riippuen siitä, mikä mato saastutti päätelaitteen. Yleensä madon saastuttama laite joudutaan uudelleenasentamaan varmistuakseen, ettei mato pääse leviämään uudestaan. Pahimmassa tapauksessa myös muut saastuneen laitteen kanssa samassa lähiverkossa olevat laitteet joudutaan uudelleenasentamaan.

Vakoiluohjelman kohdalla ohjelma tulee poistaa välittömästi. Lisäksi tulee selvittää, mitä tietoja se on kerännyt tai lähettänyt eteenpäin. Poiston yhteydessä täytyy myös tarkastaa, onko sen kautta laitteelle asennettu jotain muuta.

Kiristysohjelman lunnaita ei tule koskaan maksaa eikä sen antamiin yhteystietoihin, puhelinnumeroon tai sähköpostiin tule ottaa yhteyttä. Kiristysohjelman saastuttama kone joudutaan yleensä uudelleenasentamaan.

Troijalaisen saastuttama päätelaite tulee skannata, troijalainen tuhota sekä selvittää, mitä troijalainen on päätelaitteella tehnyt.

Kaikissa tapauksissa tulee selvittää, miten haittaohjelma on päätelaitteelle päätynyt ja mahdollisuuksien mukaan estää kyseisen haittaohjelman päätyminen muille päätelaitteille.

VARMUUSKOPIOINTI JA PALAUTTAMINEN

VARMUUSKOPIOINTI

Paikalliset sekä pilvipohjaiset tallennusasemat kannattaa varmuuskopioida. Varmuuskopioinnilla tarkoitetaan tietojen ja tiedostojen tallentamista eri kohteisiin. Varmuuskopiointia on esimerkiksi tiedoston tallentaminen paikalliselle kiintolevylle sekä pilvipalveluun tai jo valmiin tiedoston kopiointi pilvipalveluun. Tällä tavalla yritys pystyy estämään tietojen ja tiedostojen katoamista, mikäli paikallinen kiintolevy hajoaa tai pilvipalveluun ei saada yhteyttä.

VARMUUSKOPIOINNIN AUTOMATISOIMINEN

Varmuuskopiointi kannattaa automatisoida. Kun tiedostoa muokataan tai tallennetaan paikalliselle kiintolevylle, siirtyy siitä automaattisesti samalla kopio myös pilvipalveluun.

Varmuuskopioinnin toiminta olisi hyvä tarkastaa aika-ajoin, esimerkiksi kerran kuukaudessa lataamalla tiedosto pilvipalvelusta paikalliselle kiintolevylle ja testaamalla tiedoston toiminta.

VARMUUSKOPIOINNIN TARJOAMA SUOJA JA PALAUTTAMINEN

Ilman varmuuskopiointia, voi yrityksen tiedostot tuhoutua kokonaan esimerkiksi laiterikon yhteydessä. Varmuuskopiointi suojaa myös tietokoneen yllättävän sammumisen aiheuttamat tiedostovirheet, sillä tiedoston edellisen varmuuskopioidun version pystyy palauttamaan.

VARMUUSKOPIOINNIN EPÄONNISTUMINEN

Mikäli varmuuskopiointi epäonnistuu, tulee sen syy selvittää. Syy voi johtua esimerkiksi tallennuskohteen kapasiteetin täyttymisestä tai kopiointivirheestä.

SÄHKÖPOSTIN SUOJAUS

SÄHKÖPOSTIN SUOJAAMINEN

Henkilökunnan ja yrityksen käyttämä sähköposti tulee olla suojattuna siten, ettei ulkopuoliset pääse siihen käsiksi. Tämä onnistuu esimerkiksi luomalla jokaiselle käyttäjälle oma sähköpostiosoite, käyttäjätunnus ja henkilökohtainen salasana.

SÄHKÖPOSTIN SALAUS

Sähköpostiliikenne on hyvä salata siten, että vain viestille määritetyt vastaanottajat pystyvät lukemaan sen. Salaustapoja on monia, kuten turvasähköpostipalvelu, Public Key Infrastructurea (PKI) tai yksityinen avaimen luominen, jolloin salatun viestin pääsevät lukemaan vain henkilöt, joilla avain on hallussa.

Yksi helppo tapa suojata lähetettävät tiedot, on lähettää salassa pidettävät tiedot salasanalla suojattuna liitetiedostona. Salasana on tällöin lähetettävä vastaanottajalle eri tavalla, kuten tekstiviestillä.

SUOJAAMATTOMAN SÄHKÖPOSTIN KAAPPAAMINEN

Suojaamaton sähköposti ja sähköpostiviesti voi olla mahdollista kaapata esimerkiksi haittaohjelman avulla. Tietomurron jälkeen ulkopuoliset toimijat pystyvät näkemään sähköpostit, kopioimaan niiden sisällön ja liitteet sekä pahimmillaan sulkemaan sähköposteja.

TOIMINTA SUOJAUKSEN PETTÄESSÄ

Jos sähköpostiliikenteen salaus pettää ja ulkopuolinen pääsee tarkastelemaan tai kaappaamaan sähköposteja, tulee yrityksen selvittää, mistä vuoto johtuu.

KULUNVALVONTA

KULUNVALVONNAN TARKOITUS

Yritys valvoo tai seuraa ketä yrityksen tiloissa liikkuu.

MITEN KULUNVALVONTA TOTEUTETAAN?

Yrityksellä on käytössään kulkulätkät tai avaimet, joiden avulla tiloissa kulkevat henkilöt voidaan tunnistaa. Tiloissa liikkumista seurataan tai valvotaan joko kameroilla tai sähköisesti.

MITÄ VOI TAPAHTUA, JOS KULUNVALVONTAA EI OLE?

Ulkopuoliset voivat päästä yrityksen tiloihin ja sitä kautta järjestelmiin. Dokumentteja, muistitikkuja tai päätelaitteita voidaan varastaa. Ulkopuoliset henkilöt voivat myös nähdä yrityksen toiminnalle arkaluontoisia asioita, kuten tärkeitä dokumentteja.

MITEN TOIMIA, JOS KULUNVALVONTA PETTÄÄ?

Jos yrityksen tiloihin pääsee kulunvalvonnasta huolimatta ulkopuolisia henkilöitä, tulee yrityksen selvittää, mistä tämä johtuu ja parantaa suojausta.

TIETOJENKALASTELU

MITÄ ON TIETOJENKALASTELU ELI PHISHING?

Tietojenkalastelulla, eli phishingillä, tarkoitetaan haitallisen linkin tai sähköpostiliitteen naamioimista joksikin muuksi. Käyttäjä houkutellaan avaamaan linkki, joka ohjaa haitalliselle sivulle, jolla varastetaan käyttäjän tiedot.

PHISHING SIVUSTOT

Phishing sivustot pyrkivät matkimaan aitoja sivustoja olemalla hyvin samankaltaisia sekä sisällöltään, ulkonäöltään kuin osoitteeltaan. Usein ne kuitenkin erottaa tarkastelemalla linkin tarkkaa osoitetta. Osoite ei ole täsmälleen sama kuin oikealla palvelulla, vaan palvelimen nimi on eri. Verkkosivuille pitää mennä aina suoraan tallennetusta ja varmistetusta kirjanmerkistä tai kirjoittamalla osoite itse. Ei klikkaamalla viestissä olevaa linkkiä.

RIKOLLISEN MOTIIVIT TIETOJENKALASTELUSSA

Usein phishing sivustot pyytävät käyttäjää kirjoittamaan sähköpostiosoitteen tai käyttäjätunnuksen, sekä salasanan. Tällöin tiedot tallentuvat sivuston tietoihin ja kulkevat tätä kautta sivuston ylläpitäjälle.

Tietojenkalastelulla pyritään saamaan haltuun käyttäjätunnuksia ja salasanoja, joiden avulla voidaan kaapata käyttäjätilit ja kirjaudutaan käyttäjätunnuksilla eri palveluihin.

MITEN TOIMIA, JOS YRITYS JOUTUU TIETOJENKALASTELUN KOHTEEKSI?

Jos yritys joutuu tietojenkalastelun kohteeksi, pitää siitä välittömästi ilmoittaa eteenpäin ja selvittää, mitä tietoja yrityksestä on saatu selville.

TEKSTIVIESTIHUIJAUKSET

MITÄ OVAT TEKSTIVIESTIHUIJAUKSET?

Tekstiviestihuijaukset ovat tekstiviestejä, joiden lähettäjätieto on yleensä väärennetty esimerkiksi samaksi kuin Posti, S-Pankki tai Gigantti, ja jotka sisältävät haitallisen linkin.

TEKSTIVIESTIHUIJAUSTEN SISÄLTÖ YLEISESTI

Viesteissä voidaan väittää jonkin paketin hävinneen, tilauksessa olevan toimitusvaikeuksia, maksun epäonnistuneen tai tullimaksun jääneen maksamatta. Viestin linkki johtaa huijaussivustolle, joka pyrkii varastamaan käyttäjätietoja.

MITEN TIETOJENKALASTELU VOI ONNISTUA TEKSTIVIESTIHUIJAUKSESSA?

Käyttäjä erehtyy klikkaamaan huijauslinkkiä ja antaa tietonsa sivustolle, jolloin ne päätyvät ulkopuoliselle taholle. Näiden tietojen avulla pystytään kirjautumaan käyttäjän tileille ja kaapata ne.

MITEN TOIMIA, JOS JOUTUU TEKSTIVIESTIHUIJAUKSEN UHRIKSI?

Jos yrityksen henkilökunta on joutunut tekstiviestihuijauksen uhriksi, tulee yrityksen selvittää, mitä tietoja yrityksestä tai sen henkilökunnasta on tätä kautta levinnyt. Mikäli tekstiviestihuijaus on edeltänyt linkin avaamista, täytyy myös selvittää, onko päätelaitteelle asentunut haittaohjelmia.

TULOSTIMIEN, KAMEROIDEN JA SENSOREIDEN SUOJAUS

MITEN LAITTEET SUOJATAAN?

Verkkotulostimet suojataan ulkopuoliselta liikenteeltä. Niitä pystyy käyttämään vain yrityksen sisäverkossa tai yrityksen ylläpitämillä tunnuksilla.

Valvontakamerat ja sensorit ovat vain yrityksen omassa lähiverkossa, eivätkä lähetä tietoa eteenpäin.

LAITTEIDEN SUOJATTU KÄYTTÄMINEN

Tulostamiseen tarvitaan käyttäjätunnus, salasana tai tulostajan yhdistäminen tulostimeen lähiverkosta.

Valvontakameroiden ja sensorien tarkasteluun tarvitaan käyttäjätunnus ja salasana.

MITÄ TAPAHTUU, JOS SUOJAUSTA EI OLE?

Ilman tulostimien suojaamista, voivat ulkopuoliset käyttäjät päästä näkemään tulostettavia dokumentteja tai ohjaamaan tulosteita muihin kohteisiin.

Suojaamattomiin valvontakameroihin ja sensoreihin on mahdollista päästä käsiksi ulkopuolelta ja sitä kautta saada haltuun yrityksestä tietoa.

MITEN TOIMIA, JOS SUOJAUSTA EI OLE OLLUT TAI SUOJAUS PETTÄÄ?

Jos yrityksen tulostimia ei ole suojattu, tulee yrityksen selvittää, onko joku ulkopuolinen päässyt tarkastelemaan tulosteita tai mahdollisesti kopioimaan niitä.

Mikäli yritys huomaa ulkopuolisen henkilön päässeen käsiksi valvontakameroihin tai sensoreihin, tulee ne sulkea välittömästi. Sulkemisen jälkeen on selvitettävä, mitä tietoja on saatu käsiksi ja suojata laitteet uudestaan.

VERKON LÄPINÄKYVYYS JA LAITESKANNERI

VERKON LÄPINÄKYVYYS JA VALVONTA

Verkon läpinäkyvyydellä tarkoitetaan verkkoliikenteen tarkastelua käyttäjän ja internetin välissä. Yritys pystyy halutessaan seuraamaan tätä liikennettä sekä havaitsemaan epäilyttävää toimintaa, mikä nopeuttaa vianselvitystä. Läpinäkyvyys myös nopeuttaa verkkoon kuulumattomien laitteiden tunnistamista ja verkon tilan valvomista. Verkkoliikenteen valvontaa toteutettaessa on tärkeää huomioida, ettei yksityisyyden suojaa loukata. Verkkoliikenteen sisältöä ei voi tästä syystä valvoa, mutta valvonnalla voidaan seurata, mitä laitteita verkossa on ja mihin ne ovat yhteydessä.

Yrityksellä on tiedossa, mitä laitteita sen lähiverkossa on ja niistä on olemassa laiterekisteri.

VERKKOLIIKENTEEN SEURANTA JA LAITEREKISTERI

Yritys pystyy halutessaan seuraamaan verkkoliikennettä esimerkiksi pääreitittimen kautta.

Yritys listaa lähiverkossaan olevat laitteet, pitää niistä yllä laiterekisteriä ja estää siihen kuulumattomien laitteiden pääsyn lähiverkkoon. Laiterekisteristä voidaan havaita, mikäli laitteita häviää listalta. Tällöin laite ei ole fyysisesti paikalla yrityksen tiloissa.

SEURAAMATTOMUUS JA LAITEREKISTERIN PUUTE

Mikäli yritys ei seuraa verkkoliikennettä tai verkon liikenne ei ole läpinäkyvää, voivat vieraat laitteet tai sovellukset päästä verkkoon sisälle ja sitä kautta käsiksi yrityksen tietoihin.

Jos laiterekisteriä ei ole tai sitä ei seurata, voi yrityksen laitteisiin kuulumaton laite pystyä yhdistämään suojaamattomaan lähiverkkoon ja pääsemään sitä kautta käsiksi yrityksen laitteisiin.

TOIMINTA HAAVOITTUVUUDEN HAVAITSEMISEN JÄLKEEN

Mikäli yrityksen verkkoliikenteeseen päätyy tuntemattomia laitteita tai sovelluksia, tulee niiden pääsy estää välittömästi. Lisäksi on selvitettävä, mitä tietoja ne ovat mahdollisesti yrityksestä saaneet selville tai mitä ne ovat verkossa tehneet.

Mikäli huomataan ei-laiterekisteriin kuulumattomia laitteita lähiverkossa, tulisi niiden pääsy estää heti ja selvittää kuuluvatko ne yrityksen laitteistoon vai ei.

VERKKOSIVUJEN SUODATUS

VERKKOSIVUJEN SUODATUS ELI DNS-SUODATUS

Yksi tapa tehdä työskentelystä turvallisempaa on hallita sitä, mille verkkosivuille tai mihin osoitteisiin yrityksen sisäverkossa olevista koneista voidaan ottaa yhteyttä. DNS -suodatuksen avulla yritys pystyy suodattamaan tunnettuja haitallisia nettisivuja. Tällä tavoin etenkin yleiset phishing sivut, jotka imitoivat aitoja sivuja, voidaan suodattaa pois. Tästä esimerkkinä monet https://sites.google.com/view/ joiden päätteet sisältävät office, facebook, access, post, bank ja niin edelleen näyttäen nopealla vilkaisulla aidolta sivulta, mutta vievät käyttäjän phishing sivustolle.

DNS-SUODATUKSEN ASENNUS

DNS-suodatuksen pystyy asettamaan reitittimen kautta. Suodatetut sivustot voidaan määritellä manuaalisesti. On mahdollista käyttää myös valmiita blokkilistoja (blocklist) joihin on määritelty yleisimmät haittasivustot.

DNS-SUODATUKSEN PUUTE

Jos DNS -suodatusta ei ole käytössä, on käyttäjillä mahdollisuus harhautua huijaussivustolle. Kirjautuminen sivustolle mahdollistaa ulkopuolisen pääsyn käsiksi kirjautujan käyttäjätunnuksiin.

DNS-SUOJAUKSEN VAHVISTAMINEN MANUAALISESTI

Mikäli DNS -suodatus ei toimi ja yrityksen henkilökunta päätyy huijaussivustolle, tulisi sivusto lisätä DNS -suodatukseen manuaalisesti, jotta sama ei toistuisi.

TIETOTURVAKOULUTUS

TIETOTURVAKOULUTUKSEN MERKITYS JA TARPEELLISUUS

Tietoturvakoulutuksia tulisi järjestää henkilökunnalle aina tarpeen mukaan. Tietoturvakoulutuksessa asiantuntija opastaa henkilökuntaa tietoturvaan liittyvissä asioissa, vastaa kysymyksiin ja tarvittaessa näyttää konkreettisesti tietoturvakäytäntöjä.

Tietoturvakoulutuksen tarve on hyvä kartoittaa aina muutaman vuoden välein. Koulutuksen tarvetta tulee pohtia uudestaan aina, kun laissa tulee isoja muutoksia tai tietoturva muuttuu kokonaisuutena; tulee uusia lakeja, uhkia tai muutoksia.

Tietoturvakoulutusten lisäksi kirjallinen, aina helposti saatavilla oleva tietoturvaohjeistus on tärkeä pitää ajan tasalla.

MITÄ TEHDÄ, JOS JOUTUU TIETOMURRON KOHTEEKSI?

MITEN TOIMIA, JOS JOUTUU TIETOMURRON KOHTEEKSI?

Yrityksen tulisi aina ilmoittaa tietomurroista Kyberturvallisuuskeskukseen joko heidän lomakkeellaan tai sähköpostitse cert@traficom.fi. Tarpeen vaatiessa on tehtävä myös rikosilmoitus.

Jos tietomurron seurauksena on saatu haltuun suojattavia tai salassa pidettäviä tietoja, on kyseessä tietovuoto. Mikäli rikollisen haltuun saamat tiedot sisältävät henkilötietoja, on kyseessä tietosuojarikkomus, josta täytyy tehdä ilmoitus tietosuojavaltuutetulle.

Näiden toimenpiteiden jälkeen murretut kohteet tulee eristää muusta ympäristöstä lisähaittojen torjumiseksi. Päätelaitteella käytössä olleiden käyttäjätilien salasanat tulee vaihtaa ja tunnukset lukita viipymättä. Mikäli yritys on pitänyt yllä lokitietoja, tulisi tietomurron aikaiset lokitiedot eristää, jotta niitä ei pääse muokkaamaan. Kun päätelaite on eristetty, salasanat vaihdettu ja käyttäjätunnukset lukittu, voi yritys palauttaa murretun järjestelmän varmuuskopion.

LÄHTEET

AO Kaspersky Lab. 2023. IP-osoite. https://www.kaspersky.fi/resource-center/definitions/what-is-an-ip-address

AO Kaspersky Lab. 2023. Kiristysohjelman määritelmä, esto ja poisto. https://www.kaspersky.fi/resource-center/threats/ransomware

AO Kaspersky Lab. 2023. Kuinka sähköposti salataan käyttäessä Outlook-, Gmail-, iOS- ja Yahoo-sovelluksia. https://www.kaspersky.fi/resource-center/preemptive-safety/how-to-encrypt-email

Ekonoja, A., Lahtonen, T. & Mäntylä, J. 2003. Matovirukset. Jyväskylän yliopiston IT-tiedekunta ja avoin yliopisto. https://appro.mit.jyu.fi/doc/tyovaline/virus/index3.html

Frendy. 2023. DNS-suodatus on käyttäjän ja verkon korvaamaton turva. https://frendy.fi/blogi/dns-suodatus-on-kayttajan-ja-verkon-korvaamaton-turva/

F-Secure. 2022. Mikä on palomuuri? https://www.f-secure.com/fi/articles/firewall

F-Secure. 2022. Mikä on haittaohjelma? Näin pysyt turvassa vaarallisilta ohjelmilta. https://www.f-secure.com/fi/articles/what-is-malware

F-Secure. 2022. Mitä on tietojenkalastelu eli phishing? Näin verkkourkinta toimii. https://www.f-secure.com/fi/articles/what-is-phishing

Helsingin yliopisto. Opiskelijan digitaidot. https://blogs.helsinki.fi/opiskelijan-digitaidot/

Kyberturvallisuuskeskus. 2019. Tekstiviestihuijauksia liikkeellä runsaasti – lue tarkasti, mihin olet sitoutumassa. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/tekstiviestihuijauksia-liikkeella-runsaasti-lue-tarkasti-mihin-olet-sitoutumassa

Kyberturvallisuuskeskus. 2020. Muista laitteiden, ohjelmistojen ja sovellusten päivittäminen! Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/muista-laitteiden-ohjelmistojen-ja-sovellusten-paivittaminen

LÄHTEET

Kyberturvallisuuskeskus. 2024. Monivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/monivaiheinen-tunnistautuminen-suojaa-kayttajatilejasi

Kyberturvallisuuskeskus. 2024. Pidempi parempi – Näin teet hyvän salasanan. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/pidempi-parempi-nain-teet-hyvan-salasanan

Kyberturvallisuuskeskus. 2025. Näin suojaudut tietomurroilta. Traficom. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/ohjeet-ja-oppaat-organisaatioille-ja-yrityksille/nain-suojaudut

Microsoft. S/MIME- tai Microsoft Purview -salattujen sähköpostiviestien lähettäminen Outlookissa. https://support.microsoft.com/fi-fi/office/s-mime-tai-microsoft-purview-salattujen-s%C3%A4hk%C3%B6postiviestien-l%C3%A4hett%C3%A4minen-outlookissa-373339cb-bf1a-4509-b296-802a39d801dc

Mills, M. 2020. ITIGIC. How to Protect the Printer at Home and Avoid Attacks. https://itigic.com/how-to-protect-printer-at-home-and-avoid-attacks/

Netvisor. 2026. Käyttäjät ja käyttöoikeudet – käyttöoikeuksien lisäys ja hallinta. https://support.netvisor.fi/fi/support/solutions/articles/77000470057-k%C3%A4ytt%C3%A4j%C3%A4t-k%C3%A4ytt%C3%B6oikeuksien-lis%C3%A4ys-ja-hallinta

NordVPN. 2021. Mikä on botnet eli bottiverkko? https://nordvpn.com/fi/blog/bottiverkko/

NortonLifeLock Inc, Kuinka virustorjunta toimii? https://fi.norton.com/antivirus

TEPA termipankki. Sanastokeskus Ry. https://termipankki.fi/tepa/fi/

Verohallinto. 2026. Tietoa huijauksista. https://www.vero.fi/tietoa-verohallinnosta/yhteystiedot-ja-asiointi/asioi-verkossa/tietoa-s%C3%A4hk%C3%B6isest%C3%A4-asioinnista/tietoa-huijauksista/