Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- Mitä varmistaa ja milloin
- Miten varmistaa
- Palauttaminen
- Tärkeimmät asiat

Varmuuskopiointi ja palautus

Yleiskatsaus

Ennemmin tai myöhemmin jotain tulee todennäköisesti menemään pieleen ja kadotat henkilökohtaisia tiedostoja, asiakirjoja tai valokuvia. Voit poistaa niitä vahingossa, laitteisiin voi tulla vikaa, tietokoneesi voi hävitä tai jokin haittaohjelma voi saastuttaa laitteesi. Tällaisissa tapauksissa varmuuskopiointi on ainoa tapa palauttaa tietosi. Tässä uutiskirjeessä kerromme mitä varmuuskopiointi on, miten varmistat tietosi ja kehität juuri sinulle sopivan varmistusstrategian.

Vierastoimittaja

Heather Mahalik on alan tunnetuimpia forensiikan asiantuntijoita, joka keskittyy älypuhelinten forensiikkaan. Hän on ollut kirjoittamassa ”Practical Mobile Forensics” -kirjaa, toiminut teknisenä toimittajana ”Learning Android Forensics”-kirjassa, ja osallistunut ”FOR585 Advanced Smartphone Forensics” ja ”FOR518 Macintosh Forensics” SANS-kurssien materiaalien kirjoittamiseen. Voit seurata häntä Twitterissä **@heathermahalik** ja osoitteessa: **www. smarterforesnics.com**.

Mitä varmistaa ja milloin

Varmuuskopiointi tarkoittaa kopioita tiedoistasi, jotka ovat tallennettuna jonnekin muualle kuin alkuperäiset tiedostot. Kun kadotat tärkeitä tietoja, voit käyttää varmistuksia tietojen palauttamiseen. Suurin haaste on yleensä siinä, että ihmiset eivät ota varmuuskopioita tiedoistaan, vaikka varmistus on yleensä kohtalaisen helppoa ja suhteellisen halpaa. Varmistettavien kohteiden valintaan on kaksi lähestymistapaa. Voit joko varmistaa tietyt tiedostot, jotka ovat sinulle erityisen tärkeitä, tai varmistaa kaikki tiedostot, mukaan lukien koko käyttöjärjestelmän. Ensimmäisessä lähestymistavassa varmistaminen on selkeämpää ja säästää kovalevytilaa, mutta toinen tapa on yksinkertaisempi toteuttaa ja kattavampi. Jos et ole varma siitä mitä tietoja haluat varmistaa, suosittelemme jälkimmäistä tapaa.

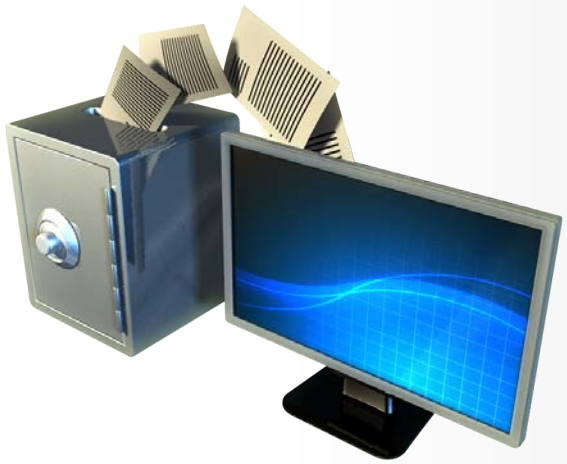
Seuraavaksi sinun tulee päättää kuinka usein haluat varmistaa tietosi. Yleisimmät vaihtoehdot ovat tunnin välein, päivittäin tai viikoittain. Kotikäyttöön tarkoitetut varmistussovellukset, kuten Applen ”Time Capsule” tai Microsoftin ”Windows Backup and Restore” mahdollistavat täysin automaattisen varmuuskopioinnin, johon ei käytännössä vaadita käyttäjältä mitään toimia. Näillä ratkaisuilla kaikki tietosi varmistuvat automaattisesti päivän mittaan samalla kun työskentelet koneellasi. Lisäksi jotkut palvelut tarjoavat niin sanottua ”jatkuvaa suojaa”, jossa uudet tai muutetut tiedostot varmistetaan välittömästi tiedostojen sulkemisen jälkeen. Suosittelemme vähintään päivittäistä varmistamista, mutta tärkeintä on kysyä itseltään kuinka paljon tietoja on varaa menettää, jos joudut palauttamaan tiedot viimeisimmästä varmistuksesta.

Miten varmistaa

Käytännössä voit varmistaa tietosi joko fyysiselle tai pilvipohjaiselle alustalle. Fyysinen alusta voi olla mikä tahansa fyysinen laite, kuten DVD, USB-muistitikku tai ulkoinen kovalevy. Minkä tahansa laitteen valitset, älä koskaan varmuuskopioi

Varmuuskopiointi ja palautus

samalle laitteelle missä alkuperäiset tiedostot sijaitsevat. Fyysisten laitteiden suurin haaste on laitteen tuhoutuminen tai häviäminen (esim. tulipalon tai varkauden kohdatessa). Näissä tapauksissa saatat menettää alkuperäisten tietojen lisäksi myös varmistukset. Tämän vuoksi varmistuslaitteet kannattaa säilyttää turvallisesti ja eri paikassa kuin varsinaiset laitteet. Varmistuslaitteisiin kannattaa merkitä mitä niihin on kopioitu ja milloin. Turvallisuuden lisäämiseksi voit myös salata (kryptata) varmuuskopiot.



Automaattiset, luotettavat varmistukset ovat usein viimeinen puolustuslinjasi tietojasi suojattaessa.

Pilvipohjaiset palvelut toimivat eri tavalla kuin fyysiset, näissä palveluissa tietosi ovat varmistettu johonkin internetissä sijaitsevaan palveluun. Riippuen siitä kuinka paljon tietoa haluat varmistaa, palvelu saattaa olla maksullinen. Palvelut toimivat yleensä niin, että käyttäjä asentaa laitteeseensa sovelluksen, joka automaattisesti varmistaa vaaditut tiedot. Etuna tässä lähestymistavassa on varmistusten sijaitseminen eri paikassa kuin alkuperäiset tiedot, jolloin laitteiden tuhoutuminen ei yleensä estä varmuuskopiosta palauttamista. Lisäksi pääset varmistettuihin tietoihin usein käsiksi käytännössä mistä vain, esimerkiksi matkustaessa. Haittapuolena pilvipohjaisessa varmistamisessa on nopeus, jolla tiedot varmistuvat, erityisesti jos varmistettavaa on paljon. Jos et ole varma kumpi lähestymistapa on sinulle sopivampi, voit käyttää fyysistä ja pilvipohjaista varmistamista rinnakkain, jolloin saat molempien parhaat puolet.

Varmistaessa ei kannata unohtaa mobiililaitteita. Näiden laitteiden etuna on usein se, että ne käyttävät jo alun perin erinäisiä pilvipalveluita, jolloin sähköpostit, kalenteritiedot ja kontaktit varmistuvat automaattisesti johonkin muualle. Laitteissa on kuitenkin todennäköisesti tiedostoja, jotka eivät varmistu itsestään, kuten laitteen konfiguraatiotietoja, valokuvia tai asetuksia. Varmistamalla mobiililaitteesi varmistat näiden tietojen säilymisen ja lisäksi helpotat laitteen käyttöönottoa esim. uutta laitetta asentaessa. Esimerkiksi Applen laitteet osaavat varmistaa automaattisesti iCloudiin, Android-laitteiden ja muiden mobiilialustojen kohdalla varmennustapa riippuu valmistajasta. Joissakin tapauksissa saatat joutua ostamaan erillisen varmistussovelluksen.

Palauttaminen

Tietojen varmuuskopiointi on vasta puolet taistelusta, lisäksi sinun pitää varmistua, että saat tiedot tarvittaessa palautettua. Voit varmistaa kuukausittain varmuuskopioiden toimivuuden palauttamalla muutamia tiedostoja ja tarkistamalla niiden sisällön. Muista myös tehdä kattavat varmistukset ennen jokaista isoa käyttöjärjestelmäpäivitystä, laitteen vaihtoa tai laitteen huoltoa ja varmista, että nämä toimivat kuten suunniteltu.

Varmuuskopiointi ja palautus

Tärkeimmät asiat

- Automatisoi varmistukset mahdollisimman pitkälle ja tarkista varmistusten toimivuus säännöllisesti.
- Palauttaessa kokonaista järjestelmää varmistuksesta, varmista että tietoturvapäivitykset ovat ajan tasalla ennen laitteen käyttöä.
- Vanhentuneet tai tarpeettomat varmuuskopiot saattavat olla haitaksi ja ne kannattaa tuhota, jotta asiattomat eivät pääse niihin käsiksi.
- Jos käytät pilvipohjaista varmistamista, tutki tarkkaan palveluntarjoajan taustat ja käyttöpolitiikka varmistaaksesi, että tarjoaja täyttää vaatimuksesi. Esimerkiksi, salaako palveluntarjoaja tietosi kun ne ovat tallennettu palveluun? Kuka pääsee käsiksi tietoihisi? Tarjoaako palvelu vahvan, esim. kaksivaiheisen tunnistautumisen.

LUE LISÄÄ

Liity kuukausittaisen OUCH! tietoturvatietoisuus-uutiskirjeen postituslistalle, lue OUCH! arkistoja ja tutustu SANS-järjestön muihin tietoturvatietoisuuteen liittyviin ratkaisuihin osoitteessa http://www.securingthehuman.org.

Elisa Appelsiini on korkean osaamisen IT-palvelutalo. Noin 400 IT-alan ammattilaisen voimin tuotamme monipuolisia ja tietoturvallisia tietotekniikkaan liittyviä pilvi-, työn tuottavuus-, konsultointi- ja ulkoistuspalveluja. Kehitämme myös asiakkaidemme liiketoimintaa tukevia sovelluksia ja tuotteita. Toimintamme perustuu syvään teknologiaosaamiseen ja aidosti asiakaslähtöiseen toimintaan.

Elisa Appelsiini is a comprehensive IT service provider owned by the leading provider of communications services in Finland, Elisa. Elisa Appelsiini helps its customers to enhance their business and increase competitiveness by offering high-end IT services in consulting, cloud, integration, software development and outsourcing.

Lähteet

Salasanalausekkeet:	http://www.securingthehuman.org/ouch/2015#april2015
Kaksivaiheinen tunnistautuminen:	http://www.securingthehuman.org/ouch/2013#august2013
Pilvipalveluiden turvallisuus:	http://www.securingthehuman.org/ouch/2014#september2014
Kryptaus:	http://www.securingthehuman.org/ouch/2014#august2014
Päivän vinkki:	http://www.sans.org/tip_of_the_day.php

Lisenssi

 Toimitus: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Käännös suomeksi: Kirill Filatov, CISO, Elisa Appelsiini Oy