Kuukausittainen uutiskirje tietoturvatietoisuuteen liittyvistä aiheista

OUCH!

Tässä numerossa…

- Mitä varmistaa ja milloin
- Palauttaminen
- Tärkeimmät asiat

Varmuuskopiointi ja palautus

Yleiskatsaus

Kun käytät tietokonetta tai mobiililaitetta tarpeeksi kauan, jossakin vaiheessa joku menee todennäköisesti vikaan ja henkilökohtaiset tiedostosi, valokuvasi tai muut tietosi häviävät. Saatat vahingossa poistaa väärät tiedostot, kärsiä laiterikosta, hukata laitteesi tai saada haittaohjelmatartunnan, pahimmassa tapauksessa salakirjoittavan haittaohjelman. Kun pahin tapahtuu, varmistukset ovat usein ainoa keino palauttaa digitaalinen omaisuutesi. Tässä uutiskirjeessä kerromme mitä varmuuskopiointi on, miten varmistat tietosi ja kehität juuri sinulle sopivan varmistusstrategian.

Vierastoimittaja

Keith Palmgren on 30 vuoden kokemuksen omaava kyberturva-ammattilainen. Hän toimii SANS-ohjaajana ja on kirjoittanut materiaalit SANS SEC301; “Introduction to Information Security.”-kurssille. Keith omistaa menestyvän tietoturvakonsultointiyrityksen ja toimii aktiivisesti Twitterissä: **@kpalmgren**

Mitä varmistaa ja milloin

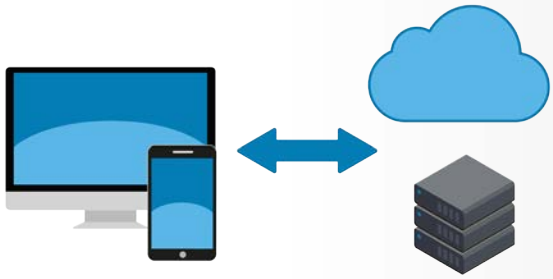
Varmuuskopiointi tarkoittaa kopioita tiedoistasi, jotka ovat tallennettuna jonnekin muualle kuin alkuperäiset tiedostot. Kun kadotat tärkeitä tietoja, voit käyttää varmistuksia tietojen palauttamiseen. Suurin haaste on yleensä siinä, että ihmiset eivät ota varmuuskopioita tiedoistaan, vaikka varmistus 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. Viimeisimpänä sinun on päätettävä kuinka varmistat, vaihtoehtoina on varmistaa joko fyysiselle tai pilvipohjaiselle alustalle ja kummassakin on omat hyvät ja huonot puolensa. Jos et ole varma kumpi lähestymistapa on sinulle sopivampi, voit käyttää fyysistä

Varmuuskopiointi ja palautus

ja pilvipohjaista varmistamista rinnakkain, jolloin saat molempien parhaat puolet.

Fyysinen alusta voi olla mikä tahansa omistamasi fyysinen laite, kuten USB-muistitikku ulkoinen kovalevy, vai verkkolevy. Fyysisille laitteille kopiointi mahdollistaa nopeat ja suuret varmistus- ja palautusmäärät. Ongelmana saattaa olla koneen haittaohjelmatartunnan leviäminen varmistuslaitteille. 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. 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. Kuten muissa pilvipalveluissa, tietoturva ja tietosuoja on suuressa roolissa, tarjoaako varmistuspalvelu vahvoja tietoturvakontrolleja, kuten datan salausta ja vahvaa autentikointia?

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

Varmuuskopiointi ja palautus

sisällön. Muista myös tehdä kattavat varmistukset ennen jokaista isoa käyttöjärjestelmäpäivitystä, laitteen vaihtoa tai laitteen huoltoa ja varmista, että nämä toimivat kuten suunniteltu.

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 securingthehuman.sans.org/ouch/archives.

Uutiskirjeen kääntäjä Kirill Filatov (KTM) on GIAC-sertifioitu tietoturvaa rakastava, kokenut IT-ammattilainen. Kirill turvaa tällä hetkellä Nebula Oy:n asiakkaiden liiketoimintaa konsultoimalla ja kehittämällä asiakkaiden tietoturvaviitekehyksiä ja toimintamalleja.

Lähteet

Salasanalausekkeet:	https://securingthehuman.sans.org/ouch/2017#april2017
Kaksivaiheinen tunnistautuminen:	https://securingthehuman.sans.org/ouch/2015#september2015
Pilvipalveluiden turvallisuus:	https://securingthehuman.sans.org/ouch/2016#november2016
Kryptaus:	https://securingthehuman.sans.org/ouch/2016#june2016
Kryptaavat haittaohjelmat:	https://securingthehuman.sans.org/ouch/2016#august2016

Lisenssi