ELINVOIMAA JA HYVINVOINTIA POHJOISEEN oamk.fi

ePOOKI

OULUN AMMATTIKORKEAKOULUN TUTKIMUS- JA KEHITYSTYÖN JULKAISUT ISSN 1798-2022

ePooki 57 / 2019

Internetin pilvipalveluiden tietoturvasta ja tietosuojasta

Korpela Teemu
23.9.2019 : :

Artikkelissa kuvataan internetin pilvipalveluiden käyttöön liittyviä tyypillisiä riskejä. Erilaisia tietoteknisiä toimintoja ja -palveluita on ollut mahdollista ulkoistaa internetiin jo pitkään ja epäonnistuneista hankinnoista ja tietoturva- ja tietosuojapoikkeamista löytyy myös runsaasti varoittavia esimerkkejä ja uutisointia.

Tietoteknisestä riskienhallinnasta ja tietoturvauhista

EU:n tietoturvallisuusvirasto ENISA laatii vuosittain listauksen yleisimmistä tietoturvauhista ja -trendeistä [1]. Listaa tarkastelemalla voi arvioida, millaisia uhkia organisaatio todennäköisesti kohtaa, voiko palvelua ulkoistaa tai tulisiko jonkin IT-palvelun tietoturvaa parantaa lisäpalveluilla. Toinen tällainen yksityiskohtaisempi tilasto on ladattavissa monikansalliselta tietoliikenneyhtiö Verizonilta, joka koostaa vuosittaisen raportin [2] yhteistyökumppanien ilmoittamista tietoturvapoikkeamista. Tällaiset tilastot auttavat hahmottamaan niitä todennäköisiä tietoturvapoikkeamia ja -riskejä, joita useimmat tietoverkkopalveluita tarjoavat ja hyödyntävät organisaatiot kohtaavat.

Myös Traficomin kyberturvallisuuskeskus laatii vuosittaisen katsauksen [3] kotimaisista tietoturvapoikkeamista ja sitä voi käyttää tietoteknisen riskiarvioinnin tukena. Kuviossa 1 on viestintäviraston (nykyisin Traficom) kyberturvallisuuskeskuksen laatima Top-5-listaus yleisimmistä tietoturvauhista ja varautumisesta vuonna 2017.

KUVIO 1. Organisaatioiden viisi yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017 [1]

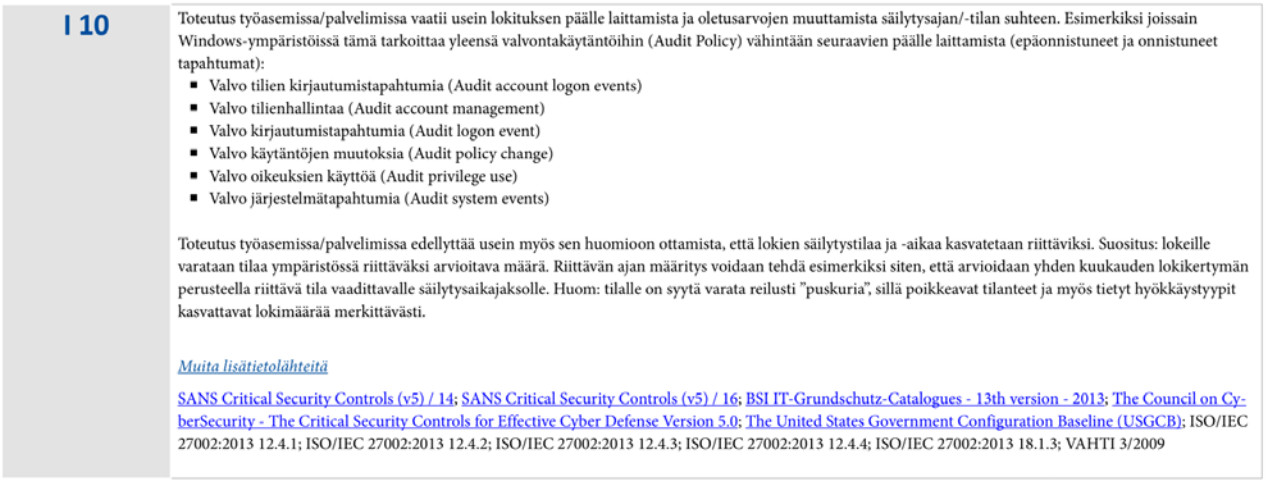
Pilvipalveluiden riskeistä ja vastuista

Kun tietoverkkopalvelua ollaan hankkimassa tai ulkoistamassa, tulee tietoturva ja tietosuoja ottaa huomioon jo varhaisessa vaiheessa. Internetin pilvipalveluita kuvaava fraasi: *"pilvipalvelu on vain jonkun toisen tahon omistama ja ylläpitämä tietokone ja -järjestelmä"* pitää erittäin hyvin paikkansa. Pilvipalvelun käyttö ei automaattisesti tarkoita tietoturvallisempaa kuin itse tuotettu ja ylläpidetty tietotekninen palvelu. Lisäksi pilvipalvelun ostajaorganisaatiolla säilyy ulkoistamisesta huolimatta ainakin osittainen vastuu siitä, että käyttäjien tiedot ovat turvassa, tiedot ja palvelut ovat tarvittaessa saatavilla ja tietoja käsitellään asianmukaisesti. Pilvipalveluiden käytöstä seuraa myös uusia tietoturvallisuushaasteita, joita ei ole täytynyt huomioida samanlaista palvelua itse tuottaessa ja ylläpitäessä.

Pilvipalveluiden ja yhteistyökumppanien tietoturva-auditoinnit

Pilvipalveluiden luonteeseen kuuluu, että ne sijaitsevat yleensä kokonaan organisaation oman IT-hallinnan ulkopuolella. Silloin järjestelmien toiminnan pintaa syvemmälle menevä tarkastelu ja auditointi on hyvin harvoin mahdollista palvelun asiakkaalle. Asiakasorganisaatio joutuu luottamaan sokeasti siihen, että palvelun tarjoaja ylläpitää hyviä käytänteitä tietoturvallisuuden ja tietosuojan toteuttamiseksi. Joskus pilvipalvelun ylläpitäjä on tehnyt sisäisiä ja ehkä myös ulkoistettuja tietoturva-auditointeja. Näiden auditointien tarkemmat tulokset eivät ole kuitenkaan yleensä palvelun asiakkaiden saatavilla.

Ideaalitilanteessa asiakas voi halutessaan suorittaa yhteistyökumppanille tai palvelulle jonkin auditointiviitekehyksen mukaisen tarkastuksen. Tällainen tarkastus voi olla esimerkiksi haastatteluna tehty täysi tai osittainen Katakri-auditointi [4]. Kuviossa 2 on näyte kansallisen tietoturva-auditointikiteeristön (Katakri) tekninen tietoturvallisuus -osuuden tarkastuslistasta. Katakri pitää sisällään kymmeniä vastaavia tietoturvateknisiä kysymyksiä ja -listoja, joita läpikäymällä voi arvioida miten organisaatiossa on huolehdittu erilaisista tietoturva- ja tietosuojahaasteista. Kuvion 2 listaamat valvontakäytännöt ovat sovellettavissa myös pilvipalvelun tapahtumien näkyvyyden parantamiseksi ja arvioimiseksi.



I 10

Toteutus työasemissa/palvelimissa vaatii usein lokituksen päälle laittamista ja oletusarvojen muuttamista säilytysajan/-tilan suhteen. Esimerkiksi joissain Windows-ympäristöissä tämä tarkoittaa yleensä valvontakäytäntöihin (Audit Policy) vähintään seuraavien päälle laittamista (epäonnistuneet ja onnistuneet tapahtumat):

- Valvo tilien kirjautumistapahtumia (Audit account logon events)
- Valvo tilienhallintaa (Audit account management)
- Valvo kirjautumistapahtumia (Audit logon event)
- Valvo käytäntöjen muutoksia (Audit policy change)
- Valvo oikeuksien käyttöä (Audit privilege use)
- Valvo järjestelmätapahtumia (Audit system events)

Toteutus työasemissa/palvelimissa edellyttää usein myös sen huomioon ottamista, että lokien säilytystilaa ja -aikaa kasvatetaan riittäviksi. Suositus: lokeille varataan tilaa ympäristössä riittäväksi arvioitava määrä. Riittävän ajan määritys voidaan tehdä esimerkiksi siten, että arvioidaan yhden kuukauden lokikertymän perusteella riittävä tila vaadittavalle säilytysaikajaksolle. Huom: tilalle on syytä varata reilusti "puskuria", sillä poikkeavat tilanteet ja myös tietyt hyökkäystyypit kasvattavat lokimäärää merkittävästi.

Muita lisätietolähteitä

SANS Critical Security Controls (v5) / 14; SANS Critical Security Controls (v5) / 16; BSI IT-Grundschutz-Catalogues - 13th version - 2013; The Council on CyberSecurity - The Critical Security Controls for Effective Cyber Defense Version 5.0; The United States Government Configuration Baseline (USGCB); ISO/IEC 27002:2013 12.4.1; ISO/IEC 27002:2013 12.4.2; ISO/IEC 27002:2013 12.4.3; ISO/IEC 27002:2013 12.4.4; ISO/IEC 27002:2013 18.1.3; VAHTI 3/2009

KUVIO 2. Katakri osa-alue I: Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys [2]

Joskus pilvipalveluita halutaan käyttää siten, että fyysisesti laitteet sijaitsevat edelleen asiakasorganisaation omissa tiloissa, mutta toimintoja ja ylläpitoa voidaan silti tehdä ja tuottaa myös palvelutoimittajan toimesta. Ei voidakaan siis yksiselitteisesti sanoa pilvipalvelun sijaitsevan aina jossain muualla. Koko käsite lähestyykin usein täyttä tai osittaista IT-palvelun ulkoistamista, eikä niinkään sitä, missä pilvipalvelu sijaitsee fyysisesti tai mistä käsin sitä ylläpidetään tai kehitetään.

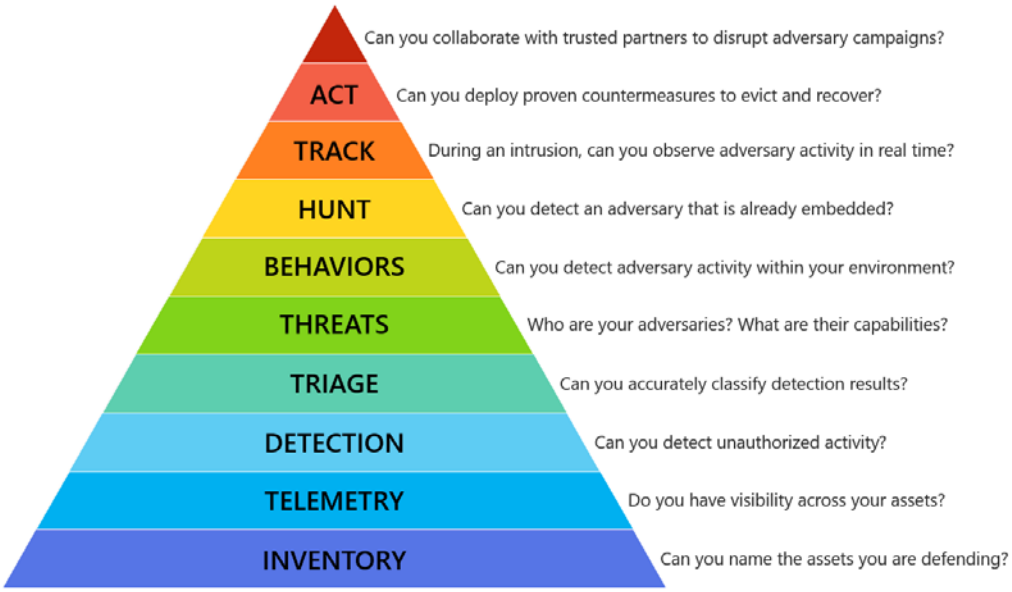
Pilvipalveluiden tapahtumien näkyvyyshaaste

Internetissä sijaitsevia pilvipalveluita käytettäessä ja ylläpidettäessä erilaisten käyttäjä- ja tietoverkkotapahtumien lokitietojen tallennus ja seuranta ovat olennaisen tärkeä osa tietoturvaa. On hyvin tavallista, että internetistä hankittu palvelu ei tarjoa kovin yksityiskohtaisia lokimerkintöjä. Tällöin mahdollisten väärinkäytösten havaitseminen saattaa kestää hyvinkin kauan. Tietoturvapoikkeamatilanteessa tapahtumien selvittäminen jälkikäteen saattaa olla haastavaa tai mahdotonta, jos käytettävissä olevat lokimerkinnät ovat vajavaiset tai puuttuvat kokonaan.

Erittäin tyypillinen ulkoistusesimerkki on sähköposti- ja kalenteripalvelut. Jos sähköpostitilin käyttäjän tunnus joutuu väärin käsiin ja käytössä ei ole monivaiheista tunnistautumista, miten käyttäjä tai IT-tuki voi havaita tämän? Tarjoaako sähköpostipalvelun toimittaja riittävät tapahtumalokit ja hälytykset tällaisten poikkeamien havaitsemiseen tai estämiseen?

Suomessa Kyberturvallisuuskeskus on varoittanut säännöllisesti Microsoftin 365 -palvelun käyttäjiin kohdistuvista tunnuskalasteluhyökkäyksistä ja on myös laatinut lyhyen oppaan [5] suojautumiseen. Joskus pilvipalvelussa täytyy maksaa lisähintaa paremmasta tapahtumanäkyvyydestä ja tietoturvallisuuteen liittyvien tapahtumalokien automatisoidusta analysoinnista. On myös melko tavallista, että asiakkaan täytyy itse osata kytkeä erilaisia tapahtumalokitustoimintoja käyttöön.

Kun pilvipalvelua hankkii, voisi miettiä miten nämä Maslowin tarvehierarkiaan (kuvio 3) mukautetut asiat toteutuvat pilvipalvelussa, jos tapahtuukin jokin yllättävä tietoturvapoikkeama.



KUVIO 3. The Incident Response Hierarchy of Needs [3]

Palveluita hankkivien organisaatioiden onkin syytä pohtia ja huomioida ensin tietoturvan ja tietosuojan perusasiat pilvipalveluissa, eikä keskittyä liikaa epätodennäköisiin tai vähemmän kriittisiin tietoturvahaasteisiin. Kuviosta 3 käy ilmi ne perusasiat, joita IT-forensiikka pyrkii hyödyntämään tietoturvapoikkeamien tutkinnassa. Samaa logiikkaa voidaan soveltaa myös tietojärjestelmien ja pilvipalveluiden ennalta tehtävään suojaamiseen. Tiedetäänkö organisaatiossa kaikki käytössä olevat pilvipalvelut? Jos ei edes tiedetä, missä ja mitä pilvipalveluita käytetään, ei verkkopalveluiden tapahtumia voi silloin myöskään seurata. Samaan tapaan täytyy myös selvittää, millaiset tapahtumatiedot palveluista on saatavilla? Voidaanko tapahtumatiedoista havaita poikkeamia ja väärinkäytöksiä? Jos tällaiset perusasiat eivät toimi, on organisaation turha toivoa esimerkiksi IT-järjestelmän väärinkäyttäjän seuraamista reaaliajassa. Tietomurron reaaliaikainen seuranta onkin tässä tarvehierarkiassa hyvin korkealla, eikä se välttämättä ole aina kovin olennaista. Tiukemman ja kattavan tietoturvan edellytys onkin huolehtia ensin perusasiat kuntoon. Ei myöskään riitä, että asiat on huolehdittu kuntoon vain kerran, vaan rahaa ja resursseja pitää uhrata myös jo tavoitetun tapahtumanäkyvyyden, seurannan ja tietoturvatason ylläpitämiseksi.

Yllättäviä kuluja väärinkäytöksistä ja erityistapahtumista

Internetistä hankitun pilvipalvelun tekninen toiminta ja kulurakenne on hyvä ymmärtää. Esimerkiksi palvelimia vuokraavan pilvipalvelun väärin käsiin joutuneella tunnuksella tai ylläpitorajapinnan tunnistautumisavaimella voidaan luoda vuokrapalvelimia ja laskea niillä esimerkiksi virtuaalivaluuttoja. Tässä esimerkissä [6] ohjelmistokehittäjä menetti Amazonin pilvipalvelun tunnistautumisavaimen ja sitä väärinkäytettiin välittömästi Litecoin-virtuaalivaluutan laskentaan. Tällaiset tunnusmenetysvahingot ja -väärinkäytökset ovat hyvin yleisiä. Tutkimusyhtiö Gartner onkin ennustanut, että tunnistautumis- ja ohjelmistorajapintoihin kohdistuvat hyökkäykset ovat yleisin tapa murtautua verkkopalveluun vuonna 2023. [7] [8]

Tiettyyn pilvipalveluun sitoutuminen saattaa aiheuttaa niin suuren järjestelmäriippuvuuden, että palvelun vaihtaminen tai rakentaminen toiseen pilvipalveluun saattaa olla ylivoimaisen kallista tai teknisesti haastavaa. Toisaalta ulkopuolelta hankittujen palveluiden keskittäminen yhdelle toimittajalle saattaa tuoda säästöjä, yhdenmukaistaa ja helpottaa järjestelmien käyttöä. Tässä ajatuksia herättävässä artikkelissa [9] esitellään liiallisesta hajauttamisesta ja sitoutumiskammosta johtuvia pulmia.

Ulkoistetun verkkopalvelun yllättävä suosio, palvelunestohyökkäys tai muu erityistapahtuma saattaa nostaa pilvipalvelun kuluja yllättäen. Monet verkkopalvelut voidaan määritellä joustaviksi, jossa palvelu voi tarvittaessa skaalautua suuriinkin käyttäjä- ja liikennemääriin. Tämä on hyvä pitää mielessä palvelua suunnitellessa ja monissa palveluissa voikin asettaa ylärajoja laskutukselle tai skaalautumiselle. Esimerkiksi yrityksen verkkomainosbudjetti saattaa huveta bottien, kilpailijan, nettitrollien, aktivistien ynnä muiden aiheuttamiin klikkauksiin ja latauksiin. Onkin arvioitu, että vain neljäsosa digitaalisten mainosten klikkaajista on oikeita ihmisiä [10].

Edistyneemmät tietoturvallisuutta parantavat ominaisuudet tulevat usein jälkikäteen pilvipalveluihin

On tavallista, että pilvipalveluun lisätään kovalla kiireellä erilaisia uusia toimintoja ja palveluita. Tietoturvaa parantavat ominaisuudet tulevat usein jälkijunassa. Lisäksi palvelua käyttävät tietojärjestelmien ylläpitäjät eivät välttämättä ehdi tutustumaan uusiin toimintoihin ja ominaisuuksiin.

Myös pilvipalveluita tuottavat yritykset kamppailevat samojen teknistä velkaa kerryttävien haasteiden kanssa kuin asiakasorganisaatiot. Jos tietoturvaa ja tietosuojaa ei ole huomioitu palvelussa jo varhaisessa vaiheessa, voi näiden toteuttaminen jälkikäteen olla haastavaa tai mahdotonta. Oheisessa Cyberark-yrityksen artikkelissa [11] esitellään, miten Amazon-yhtiön AWS-pilvipalvelussa voi piileskellä ja jatkaa väärinkäyttöä, jos järjestelmäylläpitäjän käyttäjätunnus on joutunut edes hetkeksi vääriin käsiin. Tällaisten tietomurtojen ja väärinkäytöksien havaitseminen voi olla erittäin haastavaa, jos pilvipalvelun toimittaja ei laadi hyviä ohjeita, työkaluja ja varoituksia järjestelmien käyttäjille. Lisäksi käyttäjiltä saatetaan vaatia edelleen monenlaisia tietoteknisiä taitoja, vaikka palvelu onkin hankittu muualta.

Pilvipalveluiden yhteiskäyttö

Verkkopalvelun rakentaminen webhotelliin on yksi tyypillisimmistä pilvipalveluesimerkeistä. Jos yksi yhteiskäytössä oleva palvelu tai palvelin murretaan, on joskus mahdollista, että murto laajenee myös muiden saman palvelimen sivustoihin tai tapahtuu tietovuotoja. Viiden suositun webhotellipalvelun tietoturvaa käsittelevässä raportissa [12] listataan tietoturvatutkijan löytämiä eriasteisia tietoturvapuutteita. Raportista käy hyvin ilmi, että vaikka palvelu olisi maineikas, suuri ja suosittu, ei se välttämättä tarkoita sitä, että palvelu olisi erityisen tietoturvallinen.

Yhteiskäytössä oleva palvelu (tai konesali) saattaa joutua palvelunestohyökkäyksien kohteeksi. Tällöin palvelunestohyökkäys saattaa vaikuttaa kaikkiin palvelun käyttäjiin. Suomi.fi-tunnistuspalvelu joutui elokuussa 2018 massiivisen palvelunestohyökkäyksen kohteeksi [13]. Tämän seurauksena valtion tieto- ja viestintätekniikkakeskuksen (Valtori) ja palveluntoimittajan monet muutkin verkkopalvelut lakkasivat toimimasta, vaikka ensisijaisena kohteena olikin vain Suomi.fi-palvelu.

Joskus pilvipalvelulla voi olla erittäin huono internet-maine. Tämä aiheutuu tyypillisesti siitä, että palvelua väärinkäytetään usein ja pilvipalvelun ylläpitäjät eivät rajoita tai estä väärinkäytöksiä riittävän nopeasti tai hyvin. Muualla internetissä liikennettä välittävät ja analysoivat palomuurit ja reitittimet eivät välttämättä luota huonomaineisiin IP-osoitteisiin tai -verkkoihin. Esimerkkejä tällaisista maine- ja suodatuslistoista löytyy muun muassa Firehol-palomuuriohjelmiston dokumentaatiosta [14].

Joskus pienimuotoinenkin yhteiskäyttö saattaa johtaa vaikeuksiin. Esimerkikki: oma web-sivusto hakee JavaScript-koodia internetissä olevilta palvelimilta. Mitä tapahtuu, jos tällainen muualla sijaitseva palvelin alkaa tarjoamaan haitallista ohjelmakoodia siellä tapahtuneen tietomurron tai väärinkäytön seurauksena? Sama riski tosin koskee myös koko ohjelmistotuotantoa, kun valmista ohjelmakoodia haetaan muualta [15].

Pilvipalvelun tarjoajasta ja toiminnasta tiedetään usein kovin vähän

Ulkoa hankitun palvelun toiminta saattaa jatkua pitkäänkin moitteetta ilman mitään ongelmia. Sitten palvelu häviää tai jotain muuta erityistä tapahtuu. Tässä on kaksi esimerkkiä: Kotimainen Foilchat-pikaviestintäpalvelu katosi yllättäen toukokuussa 2019 ja jätti asiakkaat ihmettelemään [16]. Toisessa esimerkissä konkurssin tehnyt tietotekniikkayritys NCIX myi käytetyt palvelimet asiakastietoineen eteenpäin [17].

Tietoturvapoikkeamat ja -murrot eivät tule aina ilmi. Vaikka pilvipalvelua tuottava yritys havaitseekin tietomurron, asiakkaita ei välttämättä aina informoida. Voi olla vaikea arvioida riskejä, jos jonkin palvelun käytöstä ei löydy tietoturvaa sivuavia esimerkkejä, tietoturvaan liittyvää uutisointia tai kommentteja. Tietoturvahaavoittuvuuksien ja -poikkeamien puuttuminen ei tarkoitakaan sitä, että palvelu olisi automaattisesti turvallinen tai että väärinkäytöksiä ja tietoturvapoikkeamia ei voisi tapahtua.

Vajavaiset tiedot pilvipalvelun toimittajasta aiheuttavat myös tietosuojahaasteita. Pilvipalvelua käyttäessä voi olla vaikeaa tai mahdotonta selvittää, että missä tietoa lopulta säilytetään tai kuinka sitä käsitellään. Palvelun toimittaja saattaa luvata yhtä, mutta toimia toisin. Joskus vaikuttaakin siltä, että palveluntoimittajat eivät ole itsekään aina ihan varmoja, että mihin tietoa siirtyy ja miten sitä käytetään. Eurooppalainen GDPR-tietosuojadirektiivi aiheuttaa tietosuojapaineita EU-alueella toimiville organisaatioille ja yrityksille. Tietosuojavaltuutetun toimisto on laatinut EU:n tietosuoja-asetusta käsittelevän verkkosivuston usein kysytyille kysymyksille [18].

Varjo-IT

Jos organisaatio ei kykene tuottamaan riittäviä IT-palveluita omille käyttäjille, saattaa käyttäjäkunta ryhtyä ulkoistamaan ja hankkimaan IT-organisaation ohi erilaisia ulkopuolella sijaitsevia palveluita. Erityisesti tiedon luottamuksellisuus saattaa vaarantua, jos tietoa varastoidaan tai siirretään luvatta ulkopuolisiin palveluihin. Varjo-IT onkin yhä suurempi haaste monille organisaatioille, koska erilaiset pilvipalvelut ovat yhä helpommin saatavilla myös peruskäyttäjille ja nämä palvelut ovat usein myös ainakin näennäisesti ilmaisia tai hyvin halpoja. Esimerkiksi monet ilmaiset VPN-ohjelmat ja -palvelut Android-puhelimille ovat haitallisia [19]. Tällaisen mahdollisesti haitallisen VPN-ohjelman asentava peruskäyttäjä ei välttämättä tiedosta riskiä.

Organisaatiot suhtautuvat usein vakavasti luvattomien IT-laitteiden ja -järjestelmien käyttöön. Tietojärjestelmien käyttäjille ei ole kuitenkaan aina täysin selvää, millaisten IT-järjestelmien käyttö on sallittua. Kuinka moni työntekijä on esimerkiksi lukenut ja tutustunut organisaation tietoturva- ja tietosuojapolitiikkaan ja ymmärtänyt mitä siellä sanotaan? Esimerkiksi Kanta-Hämeen sairaanhoitopiiri irtisanoi työntekijän, kun sairaalan tietoverkossa havaittiin työntekijän itsensä asentama ulkoinen tallennusmedia [20]. Tällaiset tiukat käyttösäännöt koskevat tyypillisesti myös pilvipalveluiden luvatonta käyttöä. Luvattoman käytön havaitseminen voi olla kuitenkin hyvin haastavaa, koska pilvipalvelut sijaitsevat miltei poikkeuksetta organisaation oman IT-hallinnan ulkopuolella ja tietoliikenneyhteydet ovat tyypillisesti salattuja. Lisäksi kiellettyjä pilvipalveluita käytetään työasioiden hoitamiseen usein myös kotoa käsin ja omilla henkilökohtaisilla IT-laitteilla.

Pilvipalvelut ovat uusista ja erilaisista riskeistä huolimatta erinomainen IT-järjestelmämuutos

Internetiin ulkoistettavia verkkopalveluita on ollut tarjolla jo kauan ja ne ovat tulleet jäädäkseen. Useimpien organisaatioiden on järkevää ulkoistaa ainakin sellaiset IT-palvelut, joiden tuottaminen ei kuulu organisaation ydintehtäviin ja -osaamiseen. Kaikista riskeistä huolimatta on todennäköisempää, että pilvipalvelun tuottaja ylläpitää ja kehittää palvelua tietoturvallisemmin kuin toimintojaan ulkoistava organisaatio kykenisi tekemään itse. Lisäksi palveluiden keskittäminen ja ulkoistaminen palveluun erikoistuneelle yritykselle on usein myös hyvin kustannustehokasta ja tuo myös parempia työkaluja IT-järjestelmien kokonaishallintaan. Tyypillisesti vikasietoisuus myös paranee, kun IT-palvelu tarjotaankin pilvipalveluna.

Pilvipalvelut eivät ole vain loppukäyttäjien selainpohjaisia palveluita, vaan organisaation kannattaa hyödyntää pilvipalveluita myös IT-järjestelmien ylläpitoon. Esimerkiksi vielä muutamia vuosia sitten oli hyvin tavallista ylläpitää tietoverkoissa olevia lähiverkkokytkimiä, reitittimiä, palomuureja ynnä muita verkon aktiivilaitteita irtonaisina ja itsenäisinä IT-laitteina. Tällainen ylläpitotapa on hyvin raskasta, kallista ja myös tietoturvatonta. Inhimillisten erehdysten määrät ja ylläpitokulut kasvavat, kun ylläpitotapahtumia ja laitteita on paljon ja toiminta ei ole keskitettyä. Moderni ylläpitotapa onkin keskittää tietoverkon aktiivilaitteiden hallinta pilvipalveluun, mikä tarjoaa hyvät työkalut ja näkyvyyden kaikkien laitteiden toimintaan ja seurantaan yhdestä paikasta. Esimerkki tällaisesta keskitetystä pilvipalvelusta on Cisco Systemsin Meraki-palvelu ja -laitteet [21].

Pilvipalvelut tuleekin nähdä mahdollisuutena kehittää ja uudistaa IT-järjestelmiä ja -käyttöä. Pilvipalveluiden käyttö tuo uusia ja erilaisia tietoturvahaasteita organisaatiolle ja kun nämä haasteet tiedostetaan hyvissä ajoin, on pilvipalveluiden käyttö turvallista ja tehokasta.

Lähteet

1. ^ENISA. ENISA Threat Landscape. Hakupäivä 26.8.2019. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends...

2. ^Verizon. 2019. Data Breach Investigations Report. Hakupäivä 26.8.2019. https://enterprise.verizon.com/resources/reports/dbir/
3. ^Viestintävirasto. 2019. Tietoturvan vuosi 2018 -katsaus kerää kyberturvallisuuden havainnot opeiksi ja luo katseen tulevaan. Hakupäivä 26.8.2019. https://www.traficom.fi/fi/ajankohtaista...
4. ^Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki. Hakupäivä 26.8.2019. https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta...
5. ^Traficom. 2019. Organisaatio! Torju Office 365 -tunnusten kalastelu oppaamme avulla. Hakupäiv 26.8.2019. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista...
6. ^Chadwick, L. 2013. My run in with Unauthorised Litecoin mining on AWS. Hakupäivä 26.8.2019. http://vertis.io/2013/12/16/unauthorised-litecoin-mining.html
7. ^Zumerle, D., D'Hoinne, M. & O'Neill, M. 2017. How to build an Effective API Security Strategy. Gartner Research. Hakupäivä 19.9.2019. https://www.gartner.com/doc/3834704/build-effective-api-security-strategy
8. ^Eliyahu, R. 2019. 5 Things You Need to Know About API Protection. SC Magazine 16.4. Hakupäivä 19.9.2019. https://www.scmagazine.com/home/opinion...
9. ^Tyler Treat: Multi-Cloud Is a Trap. Hakupäivä 26.8.2019. https://bravenewgeek.com/multi-cloud-is-a-trap/
10. ^Kabadaian, H. 2019. How Bots Steal Your Online Advertising Budget. Entrepreneur Europe 13.7.2018. Hakupäivä 26.8.2019. https://www.entrepreneur.com/article/313943
11. ^Hecht, A. 2018. The Cloud Shadow Admin Threat: 10 Permissions to Protect. Hakupäivä 26.8.2019. https://www.cyberark.com/threat-research-blog... https://github.com/cyberark/SkyArk
12. ^Yibelo, P. 2019. Report: We Tested 5 Popular Web Hosting Companies & All Were Easily Hacked. Hakupäivä 26.8.2019. https://www.websiteplanet.com/blog/report-popular-hosting-hacked/
13. ^Valtori. 2018. Sunnuntain 12.8. palvelunestohyökkäyksen yksityiskohtia selvitetään. Hakupäivä 26.8.2019. https://valtori.fi/artikkeli/-/asset_publisher...
14. ^All Cybercrime IP Feeds by FireHOL. Hakupäivä 26.8.2019. http://iplists.firehol.org/
15. ^Gilbertson, D. 2018. I'm harvesting credit card numbers and passwords from your site. Here's how. Hakupäivä 26.8.2019. https://medium.com/hackernoon...
16. ^Tivi: Suomalainen miljoona-startup katosi - yrityksen pikaviestiohjelma FoilChat lakkasi toimimasta. Hakupäivä 26.8.2019. https://www.talouselama.fi/uutiset...
17. ^Canadian retailer's servers storing 15 years of user data sold on Craigslist. Hakupäivä 26.8.2019. https://www.zdnet.com/article...
18. ^Tietosuojavaltuutetun toimisto. 2019. Usein kysyttyä. EU:n tietosuoja-asetus. Hakupäivä 19.9.2019. https://tietosuoja.fi/gdpr
19. ^Free VPN Risk Index: Android Apps. Hakupäivä 26.8.2019. https://www.top10vpn.com/free-vpn-android-app-risk-index/
20. ^Leinonen, L. 2016. Vakava sairaalan tietoturvapoikkeama johti työntekijän potkuihin – Potilastietojen ei uskota vaarantuneen. Yle Uutiset 19.12. Hakupäivä 19.9.2019. https://yle.fi/uutiset/3-9361946
21. ^Cisco Meraki. 2019. Hakupäivä 19.9.2019. https://meraki.cisco.com/

Kuvalähteet

1. ^KUVIO 1. Organisaatioiden viisi yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. Teoksessa Viestintävirasto. 2018. Tietoturva nyt! Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. Hakupäivä 26.8.2019. https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn2018011 61310.html
2. ^KUVIO 2. Katakri osa-alue I: Monitasoinen suojaaminen - Turvallisuuteen liittyvien tapahtumien jäljitettävyys. Teoksessa Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki. Hakupäivä

26.8.2019. https://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

3. ^KUVIO 3. The Incident Response Hierarchy of Needs. Teoksessa Swann, M. 2019. The Incident Response Hierarchy of Needs. Hakupäivä 26.8.2019. https://twitter.com/MSwannMSFT https://github.com/swannman/ircapabilities

Metatiedot

Nimeke: Internetin pilvipalveluiden tietoturvasta ja tietosuojasta

Tekijä: Korpela Teemu

Aihe, asiasanat: internet, pilvipalvelut, riskienhallinta, tietoturva, tietosuoja

Tiivistelmä: Internetin pilvipalvelut poikkeavat merkittävästi perinteisistä IT-kokonaisarkkitehtuureista, joissa järjestelmien ja palveluiden ylläpito ja kehittäminen on ollut tyypillisesti organisaation tai läheisen kumppanin vastuulla ja hallinnassa. Pilvipalveluita käyttäessä ja hankkiessa ei aina muisteta huomioida perinteisistä tietoturva- ja tietosuojahaasteista poikkeavia uusia riskejä ja haasteita. Tässä artikkelissa käsitellään muutamia yleisiä ongelmakohtia lyhyin esimerkein ja uutisviittauksin.

Julkaisija: Oulun ammattikorkeakoulu, Oamk

Aikamääre: Julkaistu 2019-09-23

Pysyvä osoite: http://urn.fi/urn:nbn:fi-fe2019091928918

Kieli: suomi

Suhde: http://urn.fi/URN:ISSN:1798-2022, ePooki - Oulun ammattikorkeakoulun tutkimus- ja kehitystyön julkaisut

Näin viittaat tähän julkaisuun

Korpela, T. 2019. Internetin pilvipalveluiden tietoturvasta ja tietosuojasta. ePooki. Oulun ammattikorkeakoulun tutkimus- ja kehitystyön julkaisut 57. Hakupäivä xx.xx.xxxx. http://urn.fi/urn:nbn:fi-fe2019091928918.