Kasutad Office 365-te? Ole nüüd hea ja tee seda turvaliselt!

Pilve kasutamine organisatsioonide poolt on praegu popim kui kunagi varem ja reeglina eeldatakse, et turvalisuse eest on pilves juba hoolitsetud. Tundub väga tore, aga miks on siis nii, et küberkurjategijad saavad jätkuvalt oma eelistatud ründevektoreid- näiteks e-posti - mugavalt edasi kasutada?

Trend Micro on võtnud teema ette ja on selgeks saanud, et kõik, kellel on plaan hakata kasutama pilvepõhiseid ärirakendusi, peaksid olema turvalisuse osas eriti valvsad ja Office 365 pole siinkohal mingi erand!

Office 365 sisseehitatud turvaelementidest üksi EI PIISA. Enne kindlate meetmete tarvidusele võtmist jääb turvaline pilvekeskkond ainult ettekujutuse viljaks, teatud täiendustega võid saada Office 365-st aga keskkonna, mis on isegi parem kui tootja turundus - ja müügimaterjalides kokku lubatud.

Mis need Office 365 turvaprobleemid siis täpsemalt on?
Hiljutine uuring tõi välja, et kõikidest 2014 a. suunatud rünnetest 60 % kasutas pahavara peitmiseks ikka endiselt kõige enam levinud dokumentide failiformaatide (Word, PowerPoint, Excel) turvaauke ja enam kui 90 % kõikidest rünnetest algas emailist, tavaliselt *spear-phishing* kirjadest. Kui Sinu asutus kasutab e-kirjadeks Office 365-te ja Sa loodad selle kaasasolevatele turvalisuse võimalustele, siis kobad paraku pimeduses.

Office 365 sisseehitatud turvalisuse võimalused ei avasta kahjuks peidetud ja suunatud ründeid. E-kiri on rünnete levinuim meetod, aga pahavara levitamiseks kasutatakse ka OneDrive-i ja SharePoint-i. Verizoni 2015 aasta andmelekete uuring tõi välja, et 75% rünnetest levis nakatunud patsiendist teise ohvrini 24 tunni jooksul.

Kaugtöö ja failide jagamine erinevate seadmete ja keskkondade vahel (mis pole üldse või pole veel turvapoliitikaga kooskõlas) tekitab mitmeid riske. Veel enam, ohtude avastamiseks kasutusel olevad võrgulekete tuvastussüsteemid ei näe kaugjuurdepääsu kasutajate ja Office 365 vahelist liiklust.

Trend Micro poolt avastatakse iga tund 12 500 uut unikaalset ohuallikat (mida levitatakse enamasti e-kirjade kaudu ja kasutajate kaitsmine nende ohtude eest nõuab dünaamilist kaitset reaalajas.

Mida paljud Office 365 kasutajad ei tea, on see, et Exchange Online'i turvalahendus kontrollib uusi pahavara definitsioone ainult ühe korra tunni jooksul, mis tähendab, et see pole võimeline avastama ja/või blokeerima ühtegi nullpäeva pahavara.

Nullpäeva pahavara kohta ütleb Microsoft ise: "Varasemast tundmatu pahavara variant, mida pole kunagi püütud ega analüüsitud, seega pole meie pahavaratõrje mootoritel selle avastamiseks ühtki olemasolevat definitsiooni."

Pilvelahenduste kasutamisel ja juurutamisel on turvalisus võtmeküsimuseks. Trend Micro Cloud App Security täiustab oluliselt Office 365 turvalisust erinevate ohtude takistamise ja pahavaratõrje funktsioonidega võimaldades pilvelahendusi kasutada suurema kindlustundega. Trend Micro Cloud App Security laiendab märkimisväärselt Office 365 sisseehitatud turvafunktsioone lisades teiste võimaluste hulgas ka liivakasti (sandbox) analüüsi funtsionaalsuse tuvastamaks 0-päeva pahavara PDF ja Office'i failides. Lisaks parandab Trend Micro Cloud App Security nähtavust kasutades andmelekete ennetamise võimalusi.

Cloud App Security integreeritakse otse Office 365-ga. Pole vaja suunata e-posti liiklust ümber ja lisaks laieneb kaitse ka e-kirjadest kaugemale pakkudes turvalisust ka SharePoint ja OneDrive pilvelahendustele.

Põhilised Trend Micro Cloud App Security eelised on:

- Vähendab *spear-phishing* e-kirjade riski ja failide kaitse tagatakse Exchange Online, SharePoint Online ja OneDrive for Business pilvelahendustele sealhulgas igas tunnis avastatud 12500 uute unikaalsete ohtude vastu.

- Kasutab liivakastipõhist (sandbox) analüüsi (mitte ainult staatilisi pahavara vastaseid mustrifaile), et uurida kahtlaste failide käitumist ja saadab kahtlased failid ning e-kirjad karantiini. Kasutab Deep Discovery liivakastitehnoloogiat, mis on hinnatud #1 NSS Labs poolt (2014 NSS Labs Breach Detection Systems raport).

- Jälgib kahtlaste failide reaalset käitumist liivakasti keskkonnas kasutades mitmeid erinevaid operatsioonisüsteemi ja rakenduste versioone.

- Säilitab täielikult Office 365 kasutajate ja administraatorite funktsionaalsuse. Otsene integreeritus Trend Micro ja Microsofti pilveteenuste vahel Microsoft API kaudu võimaldab suurt jõudlust ja skaleeritavust.

Kimmo Vesajoki ja Emilia Laitineni artiklist tõlkinud Stallion

https://www.linkedin.com/pulse/moving-office-365-do-securely-kimmo-vesajoki