Turvaline e-posti server aitab vältida suurt rahalist kahju

3. Aprill 2019

Eesti ettevõtted kannatavad vähekaitstud meiliserverite ja –süsteemide tõttu igakuiselt tuhandeid eurosid kahju. AKI ja RIA tuletavad ettevõtetele meelde, et nende kasutatavad meiliserverid oleksid häälestatud tagama e-kirjade usaldusväärsust ning kasutaksid vaid krüpteeritud andmeedastust ja sisse logimist.

Asutused nii avalikus kui erasektoris vahetavad omavahel iga päev e-kirjadega erineva konfidentsiaalsusega teavet. Sageli sisaldab teave inimeste eraelulisi tundlikke isikuandmeid. Olgu selleks e-poe tellimused, arved, teenuste tarbimisinfo, ametiasutuse tagasiside pöördumistele või perearsti suhtlus patsiendiga.

„Kõik need kirjad sisaldavad vähemal või suuremal määral inimeste eraelulist teavet. Kui see info jõuab valedesse kätesse, siis see annab aimu, milliseid teenuseid ja mis mahus inimene kasutab ning seda saab ära kasutada raha välja petmiseks," lausus RIA intsidentide lahendamise osakonna (CERT-EE) juht Tõnu Tammer.

"Kui e-posti aadress on lihtsalt võltsitav või kui internetis liikuv info satub krüpteerimata e-posti võrguliiklust pealt kuulates pahalaste kasutusse, võib inimene või ettevõtte sattuda erinevate küberkuritegude ja kelmuste ohvriks," kõneles Andmekaitse Inspektsiooni tehnoloogiadirektor Urmo Parm.

„Saame igapäevaselt teateid juhtumitest, kus inimese on sattunud pettuse või kelmuse ohvriks ning väga paljudel juhtudel on see võimalik just kehvasti kaitstud e-posti süsteemi tõttu. Ainuüksi märtsi teises pooles said paar ettevõtet enam kui 80 000 eurot kahju," ütles Tammer. Ta lisas, et ettevõtted peaksid kindlasti oma serverid või teenused üle kontrollima, et oleks tagatud turvaline e-kirjavahetus ja vajadusel tegema muudatused.

Tihti antakse CERT-EE-le teada väljapressimistest. „Inimeselt nõutakse raha, et kirja saatja ei avaldaks tema privaatseid andmeid. Inimesele luuakse pettekujutelm, et pahalasel on tema kohta delikaatset infot. Reaalsuses segatakse aga kokku tõene info, näiteks varasemalt lekkinud parool, ja valeinfo. Nii jääbki inimesele mulje, et tema kohta on päriselt sensitiivset infot, kuigi see pea kunagi nii ei ole," rääkis Tammer.

Veelgi tõsisem privaatsusriive kaasneb aga siis, kui e-posti teenusesse sisse logimisel võimaldatakse kasutajatunnuste ja paroolide krüpteerimata edastamist. Näiteks halvasti seadistatud wifi võrgus saab pahalane lihtsate vahenditega teada sama võrku kasutavate inimeste kasutajanimed ja salasõnad, kui e-teenuse pakkuja ei kasuta krüpteerimist. Nii võib ründaja oma kontrolli alla saada inimese kogu e-postkasti või mõne muu suhtluse või sotsiaalmeediakonto ja tõsiselt halvata inimese igapäevaelu. Tammeri sõnul saavad nõrgalt kaitstud meiliserveritest ja –süsteemidest alguse ka petuskeemid, kus ettevõtted saavad libaarveid. „Näiteks saab ettevõtte raamatupidaja arve või maksepalve justkui õigetelt lepingupartneritelt, kuid reaalsus mängib partnerit e-kirjadele silma peal hoidnud kurikael," märkis ta.

Krüpteerimine on üks esmaseid vaikimisi andmekaitse põhimõtteid, millega organisatsioonid saavad tagada isikuandmete infotehnilise turvalisuse. Sageli ei too krüpteerimine lisakulutusi, piisab, kui pädev IT-spetsialist vaatab üle olemasolev tehnoloogia turvasätted. Niisamuti on tehniliste vahenditega lihtsasti võimalik vältida sinu enda või sinu ettevõtte aadressilt tulevate võltsitud e-kirjade kohale jõudmist.

Mida teha turvalisuse tõstmiseks?

E-posti serverite vahelise andmevahetuse paremaks kaitsmiseks tuleb sisse lülitada STARTTLS tugi ning kindlasti eelistada krüpteeritud andmevahetust: seda nii e-kirjade saatmisel kui ka vastuvõtmisel. Samuti tuleks e-postiserveritel sisse lülitada SPF ja DMARC kontrollid ning samamoodi seadistada ka oma internetiaadress ehk domeen. Selle abil on võimalik vältida näiliselt iseenda või

ettevõtte aadressilt tulevate võltsitud e-kirjade kohale jõudmist sulle või sinu äripartneritele.

Oma kodulehe ja e-posti serveri seadistuste turvalisuse kontrollimiseks on olemas mitmed internetipõhised lahendused. Nende lühitutvustuse leiab RIA blogist (https://blog.ria.ee/oma-kodulehe-voi-e-posti-turvalisust-saab-testida-ig... [1]).

Allikas URL:
https://www.aki.ee/et/uudised/uudiste-arhiiv/turvaline-e-posti-server-aitab-valtida-suurt-rahalist-kahju

Lingid:
[1] https://blog.ria.ee/oma-kodulehe-voi-e-posti-turvalisust-saab-testida-igauks/