Linas Pečiūra: oleks naiivne eeldada, et oleme küberrünnakute haripunkti jõudnud

5 aastat tagasi - 15.04.2021 Autor: Linas Pečiūra

Käesolev aasta on küberrünnakute osas alanud väga ebameeldivalt. Juhtumeid on tuvastatud üle maailma, millest mõned polnud suunatud isegi organisatsioonidele, vaid ühiskonnale üldiselt. Näiteks Floridas tungisid häkkerid linna veepuhastusjaamadesse ja üritasid leelise kogust eluohtlikule tasemele tõsta. Need ei ole üksikud juhtumid – FBI uuringu kohaselt on küberrünnakute arv alates COVID-19 pandeemia algusest kasvanud koguni 300 protsenti.

Seega seisavad täna ettevõtted ja isegi tavalised tarbijad mitmete küsimuste ees: mida keelata, mida lubada ja kuidas kaitsta end andmete kadumise või häkkimise eest? Eriti olukorras, kus ettevõtted peavad oma töötajate andmeid kaitsma ja kindlaks tegema, et kurjategijad ei saa neid ära kasutada.

Juhtumid ei ole lihtsasti tuvastatavad

Tuleb alustada sellest, et kübervarguse juhtumid ei ole alati lihtsasti tuvastatavad. See kajastub ka uuringutes: ettevõtetel läheb tihti üle 200 päeva alates häkkimisest juhtumi tuvastamiseni. Seda enamasti seetõttu, et suur hulk häkkeritest kasutavad valeidentiteeti ja esitlevad ennast ettevõtte töötajana. See tähendab, et häkkimise ajal kasutakse varastatud kasutajanimesid ja paroole. Kõige levinum viis paroolide kättesaamiseks on andmepüük (phishing), kus kasutajat eksitatakse ning ta annab kelmidele ise teavet, mida saab ettevõtte vastu kasutada. Õnneks tänapäeval on olemas meetodeid selliste häkkerite peatamiseks: tööriistad, mis jälgivad pidevalt kõrvalekaldeid tavapärastest töömudelitest ning lubavad potentsiaalseid häkkereid tuvastada.

Oleme palju näinud, et mitmed organisatsioonid ei võta ka kõige lihtsamaid ekspertide soovitusi kuulda. Näiteks tuleks oma e-post seadistada sellisena, et kurjategijad ei saaks ettevõtte turvalisuse nõrkusi ära kasutada ja teeseldes end selle organisatsiooni kasutajana, saata teistele ettevõtte töötajatele e-kirju, mis julgustavad pahatahtlikule lingile peale vajutama või sensitiivset teavet avaldama. Häkkerid saavad ettevõtteid kahjustada väga lihtsal viisil, kasutades ära turvariskid kehvasti turvatud meiliserveris.

Pilve kolimine toob kaasa turvariske

Turvameetmete puhul ei ole ühte kindlat õiget suunda või retsepti igaühele. Siiski leidub kõikidel ühiseid väljakutseid. Näiteks olid paljud ettevõtted sunnitud pandeemia ajal suunduma digitaalsesse keskkonda ja varustama oma töötajaid vahenditega, mis lubavad kaugtööd teha. Tänapäeval piirdub kaugtöö sageli videokoosolekutega ja ei muutu küberruumis reaalseks koostöövormiks. Vähemalt hakatakse pidevalt rohkem uurma, kuidas saaks ettevõtetes tootlikkust tõsta ja IT-osakondades halduskulusid optimeerida. Selle tulemusena on ilmnemas veel kaks suundumust: organisatsioonid hindavad aktiivselt pilveserverite rakendamise võimalusi ja valmistuvad tulevasteks tehisintellekti projektideks.

Mis otsast tuleks alustada, kui andmeid turvaliselt digitaliseerida või pilve ümber kolida? Tavaliselt seavad ettevõtted oma tegevuse ja tootlikkuse optimiseerimise esikohale ja turvaküsimused kerkivad alles siis, kui nad otsustavad pilve liikuda või probleemid on tekkinud. Väga tihti on näha, et ettevõtted usaldavad pilve täielikult ning unustavad, et andmekaitse on organisatsiooni enda vastutus. Muidugi on ka ettevõtteid, kes ei usalda pilve üldse ja ülehindavad oma andmebaasi turvalisust. Õige vastus peitub mõlema lahenduse keskel – sa pead pilve ümber kolima, aga samal ajal pead hoolitsema oma IT-ressursside turvalisuse, jõudluse ja ülalpidamise eest. Tüüpilised vead on seotud elementaarse turvalisusega. Näiteks serverite värskendamist ja hooldamist unustatakse teha, töötajatele antakse ebavajalikke privileege ja kaheastmelist autentimiskaitset ei kasutata. Aga kõige suurem risk võib olla sisemiste protsesside ja protseduuride puudus, eriti reaalse turvaohu puhul.

Kuni küberrünnakud tasuvad end ära, on neid veelgi

Eriti riskantne on mõelda, et küberrünnakud on jõudnud haripunkti ja kahanevad tulevikus. Naiivne on eeldada, et uute tehnoloogiatega ei kaasne uued riskid. Näiteks nii-nimetatud deepfake tehnoloogia, mis omastab inimese visuaalset identiteeti, on muutumas üha populaarsemaks. Juba nähakse ette väga ohtlikke juhtumeid, kus tehisintellekti poolt kontrollitud robot osaleb ettevõtte kaugkoosolekul. Analüütikud juba lisavad selle oma aruannetesse ja võimalike ohtude nimekirja. Eksperdid näevad suuri ohte asjade internetis, mida jätkuvalt ülemäära hästi kaitsta ei osata. Seetõttu näeme juhtumeid, kus ühe või teise omavalitsuse elutähtsate infrastruktuuride võrkudesse (veevarustus, varajase hoiatamise süsteemid) on sisse tungitud. On tulnud ette olukordi, kus autode turvakaameraid on häkitud. Eelpool mainitud Florida veepuhastusjaama rünnak on vaid üks näide sellest.

Häkkerite rünnakute arv suureneb tulevikus. Rünnakute majanduslik aspekt määrab kõik: kas aja- ja hinna kulu on väärt selliste rünnakute läbiviimist, või on vahelejäämise risk liiga suur ja kuritegu mitte väärt? Nagu igas teises valdkonnas, hindavad kurjategijad esiteks sellega kaasnevaid riske ja kasu. Seega kuritegude avastamine, nende avalikustamine ja piisav õiguslik reageerimine, koostöös parima võimaliku andmete ja serverite kaitsega võib aidata seda olukorda tulevikus leevendada. Ettevõtted peaksid ise lisaks oma IT-ressursside kaitsmisele töötajaid välja koolitama, treenima ja nõustama. Kõige olulisem on see, et töötajad saaksid ise ohu ära tuvastada ja teaksid, kuidas sellises olukorras käituda.

LINAS PEČIŪRA
Tarkvaraettevõtte Crayon pilvelahenduste ja -teenuste juht Baltimaades

- Lahendused
- Turvalisus

Pilt