DIGITAALSE TURVALISUSE PÕHIMÕTTED: KUIDAS END KRIISIOLUKORRAS KAITSTA JA MIDA TEHA?

Tänapäeva digikeskkonnas peegeldab meie veebipõhine tegevus reaalseid protsesse. Nii nagu füüsilises maailmas, ei ole ka digiplatvormidel keegi pettuste, varguste, pettuse ja muude ohtude eest täielikult kaitstud. Digitehnoloogiate ja -teenuste areng on sillutanud teed paljudele leidlikele viisidele, kuidas ebaausad inimesed või organisatsioonid saavad juurdepääsu andmetele ja neid enda huvides ära kasutavad. Siiski on füüsilise maailma turvameetmetel, nagu uste lukustamine ja valve alla panemine, vasteid ka digimaailmas, nii et me saame riskid ära tunda ja end küberrünnakute eest kaitsta.

Mis on küberrünnak?

Küberrünnak tähendab küberkurjategijate, häkkerite või muude pahasoovijate tahtlikku katset tungida arvutisse, telefoni või süsteemi. Küberrünnaku esmane eesmärk on tavaliselt teabe muutmine, varastamine või hävitamine. Sellise tegevuse ajendiks võivad olla rahalised, poliitilised või ka konkurentsist tulenevad ärilised motiivid.

Kõige populaarsemad küberrünnaku liigid on järgmised.

- ***Pahavara.*** Mis tahes programm või kood, mille eesmärk on tahtlikult kahjustada arvutit, võrku või serverit. See on kõige levinum küberrünnaku liik.

- ***Teenust tõkestav rünnak (Denial of Service, DoS).*** Sihilik rünnak, mis ujutab võrgu üle valepäringutega, eesmärgiga häirida äritegevust. DoS-rünnaku ajal ei saa kasutajad teha tavapäraseid toiminguid, nagu pääseda juurde e-postile, veebisaitidele või muudele veebiressurssidele.

- ***Andmepüük.*** Küberrünnak, mille puhul kasutatakse eri kanaleid, nagu e-post, SMS-id, telefonikõned, sotsiaalmeedia ja sotsiaalse manipulatsiooni taktika, et meelitada ohvreid jagama tundlikku teavet, näiteks salasõnu või kontonumbreid. Andmepüüki kasutatakse tavaliselt pahavara levitamise vahendina.

Baltic Centre for Media Excellence
Google

VASTUPIDAVAD BALTIMAAD

- ***Imitatsioonrünnak.*** See tähendab, et ohvrite petmiseks jäljendavad ründajad usaldusväärseid allikaid, näiteks võltsivad e-posti aadresse või veebisaidi domeene. Nende rünnakute eesmärk on tavaliselt teabe varastamine, raha väljapressimine või pahavara või muu kurivara paigaldamine seadmetesse.

Kuidas end kaitsta?

Organisatsiooni digitaalne turvalisus põhineb suuresti töötajate teadlikkusel erinevatest riskidest ja organisatsiooni ressurssidest ning üldisel valmisoleku tasemel, sealhulgas küberhügieenil – igapäevaharjumustel, mis vähendavad küberrünnaku ohtu. Küberturvalisus sõltub sellest, kas organisatsioonil on olemas info- ja kommunikatsioonitehnoloogia süsteem ja kas see on kasutajatele tuttav. Pidage meeles: kriisi ajal on saadaval ainult need seadmed ja protokollid, mis on ette valmistatud enne kriisi puhkemist. Siin on 9 küsimust, mis aitavad teil küberturvalisuse kriisiks valmistuda ja valmis olla.

1. Kas riskianalüüs on tehtud?

Iga organisatsioon seisab silmitsi teatavate digitaalsete turvariskidega, mis sõltuvad tema tegevusalast, eesmärkidest, äripartneritest ning kasutatavatest IT-toodetest ja -teenustest. Organisatsioonile on väga oluline hinnata oma tööprotsessides kasutatavaid seadmeid ja tarkvara, selgitada välja, kellel on neile juurdepääs, teha kindlaks e-posti majutusteenuse osutaja ning kontrollida, kuidas töötajad oma e-posti kasutavad. Lisaks peaks organisatsioon tuvastama IT-toodete ja -teenuste potentsiaalsete ohtudega seotud tegevusvaldkonnad, näiteks veebisaidi serverite haldamine ja hooldus – olenemata sellest, kas seda tehakse allhankena või asutusesiseselt. Rünnaku tõenäosuse ja võimalike raskete tagajärgede vähendamiseks tuleb iga IT-toote, -teenuse ja nendega seotud tegevuste kohta teha eraldi riskihindamine. Tuleks teha korrapäraseid kontrolle, mis hõlmavad korduvaid riskianalüüse ning olemasolevate turvameetmete ja -protokollide läbivaatamist.

2. Kas te säilitate andmeid ja kas need on varundatud?

VASTUPIDAVAD BALTIMAAD

Üks olulisemaid ohte digitaalsele turvalisusele on organisatsiooni andmete võimalik kaotus, rikkumine või ajutine juurdepääsematus. Selle riski vähendamiseks on oluline luua arusaadav ja usaldusväärne andmete säilitamise ja varundamise süsteem. Organisatsioon peaks määrama, milliseid andmeid säilitatakse, kus need asuvad ja millistel töötajatel on neile juurdepääs. Tasub märkida, et küberründajad võtavad sageli sihikule ettevõtte võrgu varukoopiaid, mis rõhutab, kui oluline on varukoopiate säilitamine eraldi keskkonnas, põhivõrgust eraldatuna. Lisaks sellele on kriisi ajal tegevuse säilitamiseks hädavajalik võimaldada kõigile töötajatele kaugjuurdepääs vajalikele andmetele, võimaluse korral pilvetehnoloogiate abil.

3. Milline on töötajate arusaam küberhügieenist?

Olenemata infotehnoloogiatoodetesse ja -teenustesse tehtud investeeringutest sõltub organisatsiooni andmete, süsteemide ja seadmete turvalisus sellest, kas töötajad mõistavad küberhügieeni tähtsust. Töötajad, kes suudavad ohud kasutaja tasandil ära tunda, aitavad organisatsiooni üldisele turvataseme parandamisele märkimisväärselt kaasa. Oluline on korraldada töötajatele korrapäraseid koolitusi, et suurendada teadlikkust küberhügieenist. Kui organisatsioonil puuduvad ressursid sellise koolituse korraldamiseks, siis on erinevaid asutusi, mis toetavad avaliku sektori organisatsioone IT-turbe alase hariduse andmisel.

Kuidas järgida küberhügieeni nõudeid

- ***Uuendage tarkvara.*** Hoidke tarkvara ajakohasena oma arvutite ja telefonide tarkvarauuenduste abil vastavalt tootja soovitustele. Laadige uuendusi alla ainult kontrollitud allikatest, näiteks usaldusväärsetest tarkvarapoodidest, nagu App Store või Google Play.

- ***Kustutage kasutamata rakendusi korrapäraselt.*** Võimalike turvariskide vähendamiseks kustutage nutiseadmetest ja arvutitest rakendused ja programmid, mida enam ei kasutata.

- ***Isikupärastage rakenduse load.*** Kui installite telefoni uue rakenduse, vaadake üle, millistele andmetele see juurdepääsu taotleb, ja kaaluge, kas see on vajalik. Näiteks küsige endalt, miks vajab Instagrami rakendus juurdepääsu teie kontaktiloendile või mikrofonifunktsioonile, kui te neid funktsioone ei kasuta.

- ***Olge tundmatute e-kirjadega ettevaatlik.*** Kontrollige tundmatute saatjate e-kirjade õigsust. Kui e-kirjas tundub olevat midagi kahtlast, olge ettevaatlik.

- Olge ettevaatlik ka kahtlaste manuste ja linkide suhtes. Vältige tundmatute või kahtlaste e-kirjade linkide klõpsamist või manuste avamist, kuna need võivad sisaldada andmepüügi rünnakuid. Kui saate sellise e-kirja, lülituge e-kirjade vaatamise seadetes HTML-ist tavatekstile, et kuvada linkide tegelik allikas ja et vältida kolmanda poole skriptide automaatset käivitamist.

- Muutke oma salasõnu. Uuendage korrapäraselt oma salasõnu ja ärge kasutage mitmel platvormil sama salasõna. Kasutage oma salasõnade turvaliseks korraldamiseks tasuta saadaolevat salasõnahaldurit, nagu Bitwarden või Keepass. Salasõna loomisel tagage, et see koosneks tähtede, numbrite ja sümbolite kombinatsioonist. Lisaturvalisuse tagamiseks mõelge välja midagi ebatavalist ja võimatult raskesti äraarvatavat (nt MysteriousRaccoon21!).

- Võimaluse korral kasutage kaksikautentimist. Kasutage selliseid rakendusi nagu Google Authenticator, mis pakuvad täiendavat turvakihti ja mis nõuavad profiili sisselogimisel lisaks salasõnale ka ainulaadset numbrikombinatsiooni.

4. Kellel on eri süsteemide ja seadmete administraatoriõigused?

Organisatsiooni ostetud seadmed, sealhulgas arvutid, mobiiltelefonid, kaamerad ja tarkvara, on organisatsiooni omand. Seetõttu tuleb neid süsteeme hallata tsentraalselt ja kasutada ainult tööga seotud ülesannete täitmiseks. Selle võimaldamiseks peaks olema määratud üks töötaja, kes vastutab organisatsiooni infotehnoloogiataristu haldamise ja järelevalve eest. See inimene peaks tagama IT-vahendite korrapärase hoolduse ja uuendamise. Lisaks vastutab ta selle eest, et töötajad mõistaksid küberturvalisust ja järgiksid kehtestatud digitaalse ohutuse toiminguid. See hõlmab salasõnade keerukusnõuete täitmist, salasõnade korduskasutamise takistamist, võimaluse korral kaksikautentimise kasutamise edendamist ja muid asjakohaseid turbetavasid.

5. Kuidas logivad töötajad sisse sotsiaalmeedia platvormidele ja e-posti kontole?

Meediavaldkonnas on erinevate veebipõhiste suhtlus- ja sotsiaalmeediaplatvormide kasutamine väga oluline. Nendele platvormidele sisenetakse mitte ainult tööarvutitest, vaid ka isiklikest seadmetest,

näiteks telefonidest. On oluline, et iga töötaja looks oma kontodele kordumatud kasutajanimed ja salasõnad, ning võimaldada tuleb kaksikautentimist, et tagada sisselogimisel täiendav turvalisus. Kaksikautentimise võimalusi pakuvad mitmed rakendused ja teenused, näiteks Google Authenticator või Microsoft Authenticator. Oluline on valida kõige sobivam vahend või teenusepakkuja, mis vastab teie organisatsiooni vajadustele ja võimalustele.

6. Kuidas andmeid jagatakse ja vahetatakse?

Organisatsioonidele korraldatakse küberrünnakuid sageli pahatahtlike e-kirjade kaudu, mille eesmärk on pääseda juurde organisatsiooni andmetele ja teabele. Turvalisuse suurendamiseks on soovitatav kasutada krüptitud andmevahetust, eelkõige e-kirjade puhul. Krüptimine muudab e-kirja sisu tavatekstist krüptitud tekstiks, mis on juurdepääsetav ainult ettenähtud adressaadile. See funktsioon, mida pakuvad sellised teenused nagu Microsoft 365 tellimused, aitab kaitsta tundlikku teavet. Näiteks on Ameerika küberturvalisuse kaitse agentuur koostanud suunised e-posti turvalisuse suurendamiseks.

7. Milliseid sidekanaleid igaks otstarbeks kasutatakse?

Organisatsioonid ja nende töötajad kasutavad iga päev erinevaid suhtluskanaleid, nagu e-post, vestlusrakendused jne. Erinevate kriiside lahendamise plaanide koostamisel on väga oluline määrata eelnevalt kindlaks ja leppida kokku, milliseid sidekanaleid kriisiolukorras kasutatakse. Tuleks kehtestada selged suunised kanali administraatoriõiguste määramiseks, eelistatavalt vähemalt kahele usaldusväärsele inimesele. Kriisi ajal on soovitatav säilitada töötajate juurdepääs kahele suhtluskanalile: üks põhikanal, mida tavaliselt kasutatakse igapäevaseks suhtluseks, ja teine varukanal teises vestlusrakenduses. Sellega tagatakse teabevahetuse järjepidevus isegi siis, kui põhikanalil tekivad tehnilised probleemid. Kriisimeetmete protokollis tuleks kirjeldada, millal ja kuidas tuleks iga sidekanalit kasutada, et tagada teabe kiire ja tõhus levitamine.

8. Mida peaksid töötajad küberrünnaku korral tegema?

Küberrünnakud avalduvad eri vormides, kusjuures inimesed sageli ei tea, et nende arvuti, e-post või mobiiltelefon on ohustatud. Töötajate teadlikkuse ja reageerimisvõime suurendamiseks peaksid organisatsioonid looma keskkonna, kus julgustatakse teatama kahtlastest e-kirjadest, ebatavalistest sõnumitest suhtlusrakendustes või seadme kummalisest käitumisest. Oluline on, et töötajad tunneksid end kahtlustest teatades turvaliselt, kartmata hukkamõistu või naeruvääristamist, isegi kui mure osutub põhjendamatuks. Selle protsessi süstematiseerimiseks ja korraldamiseks tuleb

koostada aruandeprotokoll, milles täpsustatakse, kuidas ja kellele kahtlustest teatada. Mida vabamalt saavad töötajad oma muresid väljendada, seda paremini on vastutaval isikul võimalik tuvastada riske ja tagada organisatsiooni küberturvalisus.

VASTUPIDAVAD BALTIMAAD

9. **Kas olete valmis reageerima?**

Koostage tegevusprotokollid ja kirjeldage nendes meetmeid, mida töötajad peaksid võtma, kui organisatsiooni IT-tooted ja -teenused satuvad küberrünnaku või muude kriiside (nt üleujutuste või tulekahjude) tõttu ohtu. Uuendage seda teavet korrapäraselt ja tagage, et kõik töötajad on kriisimenetlusest hästi informeeritud.

Digitaalne turvalisus kriisiolukorras

Kui kriis tuleneb organisatsiooni infotehnoloogiliste toodete ja teenuste ohustamisest, näiteks küberrünnakust või andmelekkest:

1. Tunnistage kriisiolukorra ulatust. Hinnake kiiresti kriisi ulatust ning isoleerige ohustatud infotehnoloogiatooted ja -teenused, et vältida rünnaku levikut.
2. Informeerige töötajaid. Teavitage töötajaid kriisiolukorrast ja andke selged juhised selle lahendamiseks vajalike sammude kohta.
3. Eraldage ohustatud seadmed. Eemaldage ohustatud seadmed ettevõtte võrgust, et piirata rünnaku mõju.
4. Analüüsige ja töötage välja taastamiskava. Uurige rünnakut või andmete lekkimist, et teha kindlaks selle põhjus ja töötada välja terviklik taastamiskava. Aktiveerige kriisiaegne tegevuskava ja kohandage seda vastavalt konkreetsele olukorrale.

Kui kriis ei ole seotud organisatsiooni infotehnoloogiliste toodete ja teenuste ohustamisega:

1. Aktiveerige heakskiidetud sisesuhtluskanalid. Kasutage ainult kriisiaegses tegevuskavas määratletud sisesuhtluskanaleid.
2. Järgige suuniseid. Tagage, et järgitakse soovitustes 2, 3, 5 ja 6 esitatud juhiseid.
3. Kontrollige andmete turvalisust. Kinnitage vajalike andmete kättesaadavus pilveplatvormidel ja veenduge, et varukoopiad on juurdepääsetavad.
4. Kaitske kriitilisi ressursse: võtke meetmeid, et kaitsta kriisi ajal organisatsiooni kriitilisi ressursse.

Autor: Zane Štāla
Toimetaja: Krista Priedīte

Baltic Centre for Media Excellence
Google