SKAITMENINĖS SAUGOS PRINCIPAI: KAIP APSISAUGOTI IR KĄ DARYTI KRIZĖS ATVEJU?

Šiandienė skaitmeninė aplinka tokia, kad mūsų veikla internete atspindi realaus gyvenimo procesus. Kaip fiziniame pasaulyje, taip ir elektroninėje erdvėje niekas nėra visiškai apsaugotas nuo sukčiavimo, vagysčių, apgaulių ir kitų grėsmių. Skaitmeninių technologijų ir paslaugų atsiradimas sudarė sąlygas nesąžiningiems asmenims arba organizacijoms įvairiais išradingais būdais įgyti prieigą prie duomenų ir jais pasinaudoti. Tačiau kaip tikrajame pasaulyje yra saugos priemonės, pvz., durų užrakinimas ir signalizacija, taip yra ir panašios priemonės elektroninėje erdvėje, suteikiančios galimybę nustatyti grėsmes ir apsisaugoti nuo kibernetinių išpuolių.

Kas yra kibernetinis išpuolis?

Kibernetinis išpuolis – tai tyčinis kibernetinių nusikaltėlių, įsilaužėlių arba kitų piktavalių mėginimas prisijungti prie kompiuterio, telefono arba sistemos. Pagrindiniai kibernetinių išpuolių tikslai paprastai būna pakeisti, pavogti arba sunaikinti informaciją. Išpuolių veiksmus gali lemti finansiniai, politiniai ar net verslo konkurencijos motyvai.

Populiariausi kibernetinių išpuolių tipai:

- ***Kenkėjiška programinė įranga.*** Bet kokia programa arba kodas, tyčia sukurtas, kad būtų pakenkta kompiuteriui, tinklui arba serveriui. Tai labiausiai paplitęs kibernetinių išpuolių tipas.

- ***Atsisakymo teikti paslaugas (DoS) išpuolis.*** Tikslingas išpuolis, kai tinklas užtvindomas siunčiamų suklastotų užklausų, siekiant sutrikdyti verslo operacijas. DoS išpuolio metu naudotojai negali atlikti įprastų užduočių, pvz., prisijungti prie el. pašto, svetainių ir kitų interneto išteklių.

- ***Duomenų vagystė.*** Kibernetinis išpuolis, kurį vykdant naudojamasi įvairiais kanalais, pvz., el. paštu, SMS žinutėmis, telefono skambučiais, socialine žiniasklaida ir socialinės inžinerijos taktikomis, kad apgaulės būdu būtų išgauta slapta informacija – slaptažodžiai arba sąskaitų numeriai. Duomenų vagystė paprastai reikalinga, kad būtų įdiegtos kenkėjiškos programos.

Baltic Centre for Media Excellence
Google

TVIRTOS BALTIJOS ŠALYS

- ***Apsimetimo kuo nors išpuolis.*** Išpuolio vykdytojai kuo nors apsimeta, naudodamiesi pasitikėjimą keliančiais ištekliais, pvz., el. paštu ar svetainėmis, kad apgautų auką. Šių išpuolių tikslas paprastai yra pavogti informaciją, išvilioti pinigus arba įdiegti kenkėjišką programą bei kitokią kenkėjišką įrangą.

Kaip apsisaugoti?

Organizacijos elektroninės erdvės saugumas labai priklauso nuo jos darbuotojų informuotumo apie įvairias rizikas, taip pat organizacijos išteklių ir bendrojo pasiruošimo lygio, įskaitant „kibernetinę higieną“, t. y. kasdienius įpročius, kurie mažina kibernetinių išpuolių riziką. Kibernetinė sauga priklauso nuo to, ar yra įdiegta organizacijos informacinių ir ryšių technologijų sistema, ar ji gerai žinoma jos naudotojams. Atminkite, kad krizės metu bus įmanoma naudotis tik ta įranga ir protokolais, kurie buvo sukurti prieš krizę. Pateikiame 9 klausimus, kurie padės jums pasiruošti ir būti pasiruošusiems kibernetinės saugos krizei.

1. Ar atliktas rizikos vertinimas?

Kiekviena organizacija susiduria su tam tikra skaitmeninės saugos rizika, kuri priklauso nuo jos veiklos srities, tikslų, verslo partnerių ir naudojamų IT produktų bei paslaugų. Labai svarbu, kad organizacija įvertintų darbui naudojamus įrenginius ir programinę įrangą, nustatytų, kas turi prieigą prie jų, identifikuotų el. pašto prieglobos paslaugų teikėją ir išsiaiškintų, kaip darbuotojai naudojasi savo el. paštu. Be to, organizacija turi nustatyti veiklos sritis, susijusias su galimomis grėsmėmis IT produktais ir paslaugoms, pvz., interneto svetainių serverių administravimui ir priežiūrai, nesvarbu, ar ji teikiama išorės paslaugų teikėjų, ar įmonės viduje. Siekiant sumažinti išpuolio tikimybę ir galimų padarinių poveikį, turi būti atliktas atskiras kiekvieno IT produkto, paslaugos ir susijusios veiklos rizikos vertinimas. Turi būti atliekami nuolatiniai patikrinimai, apimantys neišnykstančios grėsmės analizę ir esamų saugos priemonių bei protokolų peržiūrą.

2. Ar saugote duomenis ir ar darote jų atsargines kopijas?

TVIRTOS BALTIJOS ŠALYS

Viena iš didžiausių grėsmių skaitmeninei saugai – galimas organizacijos duomenų praradimas, sugadinimas arba laikinas neprieinamumas. Norint sumažinti šią riziką, būtina įdiegti suprantamą ir patikimą duomenų saugojimo ir atsarginių kopijų darymo sistemą. Organizacija turi nurodyti, kurie duomenys privalo būti saugomi, kur jie yra ir kurie darbuotojai gali turėti prieigą prie jų. Pažymėtina, kad kibernetiniai įsilaužėliai dažnai kėsinasi į įmonių tinklo atsargines kopijas, todėl svarbu šias atsargines kopijas saugoti atskiroje aplinkoje, nesusietoje su pagrindiniu tinklu. Be to, norint tęsti veiklą krizės metu, labai svarbu visiems darbuotojams suteikti nuotolinę prieigą prie reikalingų duomenų, galbūt naudojant debesijos technologijas.

3. Kaip darbuotojai supranta kibernetinę higieną?

Nesvarbu, kiek būtų investuojama į informacinių technologijų produktus ir paslaugas, organizacijos duomenų, sistemų ir įrangos sauga priklauso nuo darbuotojų kibernetinės higienos įsisąmoninimo. Darbuotojai, gebantys atpažinti grėsmes naudotojo lygmeniu, labai prisideda prie bendrojo organizacijos saugumo. Svarbu reguliariai organizuoti darbuotojų mokymus, kad pagerėtų jų supratimas apie kibernetinę higieną. Jeigu organizacijai trūksta išteklių tokiems mokymams surengti, yra įvairių įstaigų, kurios padeda viešojo sektoriaus organizacijoms vykdyti mokymus IT saugumo klausimais.

Kaip laikytis kibernetinės higienos reikalavimų:

- ***Atnaujinkite programinę įrangą.*** Nuolat atnaujinkite kompiuterių ir telefonų programinę įrangą pagal gamintojo rekomendacijas. Atnaujinimus atsisiųskite tik iš patikrintų šaltinių, pavyzdžiui, patikimų programinės įrangos parduotuvių, tokių kaip „App Store“ arba „Google Play“.

- ***Reguliariai ištrinkite nenaudojamas programėles.*** Ištrinkite nebenaudojamas programėles ir programas iš išmaniųjų įrenginių ir kompiuterių, kad sumažintumėte riziką.

- ***Prisitaikykite leidimus, suteikiamus programėlei.*** Įdiegdami naują programėlę telefone peržiūrėkite, prie kurių duomenų ji prašo prieigos, ir apsvarstykite, ar būtina suteikti. Pavyzdžiui, pasvarstykite, kam „Instagram“ programėlei reikalinga prieiga prie jūsų kontaktų sąrašo arba mikrofono funkcijos, jeigu tuo nesinaudojate.

- ***Būkite atsargūs, gavę nežinomų siuntėjų el.*** laiškus. Tikrinkite nežinomų siuntėjų el. laiškų teisėtumą. Jeigu kas nors el. laiške atrodo įtartina, būkite atsargūs.

- ***Atsargiai, jeigu gavote įtartinų priedų ir nuorodų.*** Nespauskite nuorodų ir neatidarinėkite iš nepažįstamų asmenų gautų arba įtartinų el. laiškų priedų – gal mėginama gauti duomenis. Jei susiduriate su tokiais el. laiškais, jų peržiūros nustatymuose perjunkite HTML į paprastą tekstą, kad atskleistumėte tikrąjį nuorodų šaltinį ir išvengtumėte automatinio trečiųjų šalių scenarijų vykdymo.

- ***Pakeiskite slaptažodžius.*** Reguliariai atnaujinkite slaptažodžius ir nenaudokite to paties slaptažodžio keliose sistemose. Slaptažodžiams saugiai tvarkyti naudokite laisvai prieinamą slaptažodžių tvarkyklę, pvz., „Bitwarden“ arba „Keepass“. Kurdami slaptažodį, pasistenkite, kad jį sudarytų raidžių, skaičių ir ženklų derinys. Dėl didesnio saugumo sugalvokite ką nors, kas yra neįprasta ir sunkiai atspėjama (pvz., MysteriousRaccoon21!)

- ***Kai įmanoma, įgalinkite dviejų veiksnių autentifikavimą.*** Naudokite tokias programėles kaip „Google Authenticator“, kurios suteikia papildomą saugumo lygį, nes prisijungiant prie profilio kartu su slaptažodžiu reikalaujama unikalaus skaičių derinio.

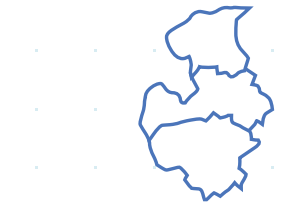
4. Kas turi įvairių sistemų ir įrenginių administratoriaus teises?

Organizacijos įsigyta įranga, įskaitant kompiuterius, mobiliuosius telefonus, kameras ir programinę įrangą, yra organizacijos nuosavybė. Todėl šios sistemos turi būti valdomos centralizuotai ir naudojamos tik su darbu susijusioms užduotims atlikti. Kad būtų paprasčiau, turi būti vienas asmuo, atsakingas už organizacijos informacinių technologijų infrastruktūros valdymą ir priežiūrą. Šis asmuo turi nuolat užtikrinti IT įrangos priežiūrą ir atnaujinimą. Be to, jis būtų atsakingas už tai, kad darbuotojai suprastų kibernetinės saugos svarbą ir laikytųsi nustatytų skaitmeninės saugos procedūrų. Tai apima slaptažodžių sudėtingumo reikalavimo, pakartotinio slaptažodžių naudojimo draudimo laikymąsi, skatinimą, kai įmanoma, naudoti dviejų veiksnių autentifikavimą ir taikyti kitą saugos praktiką.

5. Kaip darbuotojai prisijungia prie socialinės žiniasklaidos svetainių ir el. pašto?

Žiniasklaidai labai svarbios įvairios internetinės ryšių priemonės ir socialinės žiniasklaidos svetainės. Prie šių svetainių prisijungiama net tik naudojant darbo kompiuterius, bet ir asmeninius įrenginius,

pvz., telefonus. Labai svarbu, kad kiekvienas darbuotojas susikurtų unikalius savo paskyrų naudotojo vardus ir slaptažodžius, ir įjungtų dviejų veiksnių autentifikavimą, jog prisijungimas būtų saugesnis. Tam tikros programėlės ir paslaugos, pvz., „Google Authenticator“ arba „Microsoft Authenticator“, suteikia dviejų veiksnių autentifikavimo galimybę. Svarbu pasirinkti tinkamiausią įrankį arba paslaugų teikėją, atitinkantį jūsų organizacijos poreikius ir galimybes.



6. Kaip dalijamasi duomenimis ir jais keičiamasi?

Organizacijos dažnai susiduria su kibernetiniais išpuoliais, siunčiant kenkėjiškus el. laiškus, kuriais siekiama gauti prieigą prie organizacijos duomenų ir informacijos. Saugumui padidinti patartina įdiegti duomenų, kuriais keičiamasi, šifravimą, ypač el. laiškų atveju. Šifruojant el. laiško turinys iš paprasto teksto paverčiamas užšifruotu tekstu, kuriuo galės naudotis tik numatytas gavėjas. Ši funkcija, kuri prieinama naudojantis tokia paslauga kaip „Microsoft 365“ prenumerata, padeda apsaugoti konfidencialią informaciją. Pavyzdžiui, Amerikos kibernetinio saugumo agentūra yra pateikusi el. pašto saugumo didinimo gaires.

7. Kokie ryšių kanalai naudojami kiekvienu tikslu?

Organizacijos ir jų darbuotojai kasdien naudojasi įvairiais ryšių kanalais, pvz., el. paštu, pokalbių programėlėmis ir kt. Sudarant planus įvairių krizių atvejams, labai svarbu iš anksto nustatyti ir susitarti, kuriais ryšių kanalais bus naudojamasi krizės situacijoje. Turi būti aiškios gairės dėl kanalo administratoriaus teisių priskyrimo, pageidautina, kad šios teisės būtų suteiktos bent dviem patikimiems asmenims. Krizės atveju darbuotojams patartina turėti prieigą prie dviejų ryšių kanalų: vieno pagrindinio kanalo, kuris paprastai naudojamas kasdieniam bendravimui, ir kito atsarginio kanalo – kitoje pokalbių programėlėje. Taip užtikrinamas komunikacijos tęstinumas, net jei naudojantis pagrindiniu kanalu susiduriama su techninėmis problemomis. Krizės veiksmų protokole turi būti nurodyta, kada ir kaip reikėtų naudotis kiekvienu ryšių kanalu, kad būtų užtikrintas greitas ir veiksmingas informacijos skleidimas.

8. Ką darbuotojai turi daryti kibernetinės atakos atveju?

Kibernetinės atakos pasireiškia įvairiomis formomis, todėl žmonės dažnai nežino, kad buvo pažeistas jų kompiuteris, el. paštas arba mobilusis telefonas. Kad padidintų darbuotojų sąmoningumą ir atsakingumą, organizacijos turi kurti aplinką, kurioje būtų skatinama pranešti apie įtartinus el. laiškus, neįprastus pranešimus bendravimo programėlėse arba neįprastą įrenginio veikimą. Labai svarbu, kad darbuotojai jaustųsi saugūs pranešdami apie tai, kas įtartina, nesibaimintų dėl pasmerkimo ar išjuokimo, net jei paaiškėtų, kad įtarimai nepagrįsti. Pranešimo protokolo, kuriame būtų konkrečiai nurodyta, kaip

ir kam pranešti apie įtarimus, paruošimas sistemintų ir organizuotų šį procesą. Kuo laisviau darbuotojai gali išreikšti savo nuogąstavimus, tuo geriau atsakingas asmuo galės nustatyti riziką ir užtikrinti organizacijos kibernetinį saugumą.

TVIRTOS BALTIJOS ŠALYS

9. **Ar esate pasiruošę reaguoti?**

Sukurkite veiksmų protokolus, kuriuose būtų nurodyti veiksmai, kurių darbuotojai turi imtis, jeigu organizacija susidurtų su grėsme jos IT produktams ir paslaugoms dėl kibernetinio išpuolio arba kitų krizių (pvz., potvynių ar gaisrų). Reguliariai atnaujinkite šią informaciją ir užtikrinkite, kad visi darbuotojai būtų gerai informuoti apie krizių valdymo procedūras.

Skaitmeninis saugumas krizės metu

Jeigu krizė kyla dėl pavojaus, sukeliamo organizacijos informacinių technologijų produktams ir paslaugoms, pvz., kibernetinio išpuolio ar duomenų nutekėjimo:

1. Nustatykite pavojaus mastą. Greitai nustatykite krizės mastą ir izoliuokite pažeistus informacinių technologijų produktus ir paslaugas, kad būtų užkirstas kelias tolesniam išpuolio plitimui.
2. Informuokite darbuotojus. Praneškite darbuotojams apie krizės situaciją ir pateikite aiškius nurodymus, kokie veiksmai būtini, kad viską būtų galima išspręsti.
3. Izoliuokite pažeistą įrangą. Atjunkite pažeistą įrangą nuo įmonės tinklo, kad sumažintumėte išpuolio poveikį.
4. Analizuokite situaciją ir paruoškite atkūrimo planą. Ištirkite išpuolį arba duomenų nutekėjimą, kad nustatytumėte to priežastį ir paruoštumėte visapusišką atkūrimo planą. Suaktyvinkite krizių protokolą ir pritaikykite jį konkrečiai situacijai.

Jeigu krizė nesusijusi su organizacijos informacinių technologijų produktams ir paslaugoms kilusiu pavojumi:

1. Suaktyvinkite patvirtintus vidaus ryšių kanalus. Naudokite tik krizės protokole nurodytus vidaus ryšių kanalus.
2. Laikykitės gairių. Užtikrinkite, kad būtų laikomasi 2, 3, 5 ir 6 punktuose pateiktų rekomendacijų.
3. Tikrinkite duomenų saugumą. Patikrinkite, ar debesijos platformose yra būtini duomenys, ir užtikrinkite, kad būtų prieinamos atsarginės kopijos.
4. Apsaugokite svarbiausius išteklius: Imkitės priemonių, kad ištikus krizei apsaugotumėte svarbiausius organizacijos išteklius.

Autorė: Zanė Štala
Redaktorė: Krista Priedytė

Baltic Centre for Media Excellence
Google