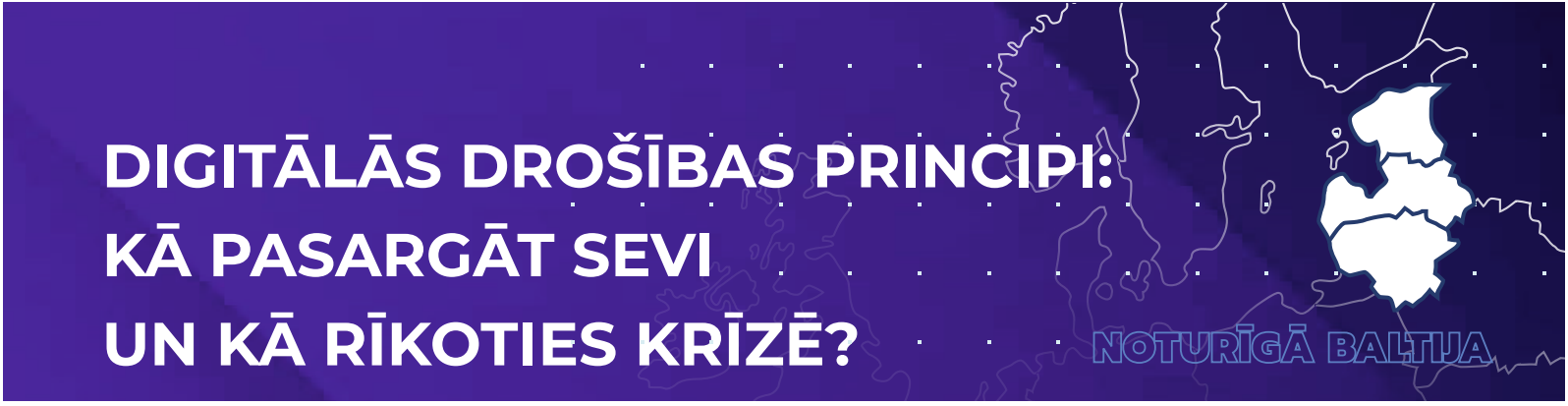
DIGITĀLĀS DROŠĪBAS PRINCIPI: KĀ PASARGĀT SEVI UN KĀ RĪKOTIES KRĪZĒ?



Digitālā vide ir kļuvusi par reālajai dzīvei līdzvērtīgu procesu krustpunktu. Tāpat kā realitātē, arī digitālajā pasaulē neviens nav simtprocentīgi pasargāts no krāpšanas, zādzībām, maldināšanas un citiem uzbrukumiem. Digitālās vides iespēju un pakalpojumu attīstība ir pavērusi ceļu daudzveidīgiem un nereti – arī visnotaļ radošiem – veidiem, kā negodprātīgiem indivīdiem vai organizācijām piekļūt datiem un tos izmantot savā labā. Taču, tieši tāpat kā reālajā dzīvē mēs sekojam līdzi savai drošībai, slēdzam māju durvis, ierīkojam signalizāciju un citādi cenšamies sevi pasargāt no ļaundariem, arī digitālajā vidē mēs varam atpazīt riskus un pasargāt sevi no kiberuzbrukumiem.

Kas ir kiberuzbrukums?

Kiberuzbrukums ir kibernoziedzinieku, hakeru vai kāda cita ļaundara mēģinājums piekļūt datoram, telefonam vai sistēmai. Biežākie kibernoziegumu mērķi ir izmainīt, nozagt vai iznīcināt informāciju. Šie noziegumi var būt finansiāli vai politiski motivēti, vai pat veikti konkurentu biznesa interesēs.

Populārākie kiberuzbrukumu veidi:

- *Ļaunprogrammatūra jeb ļaunprātīga programmatūra* – jebkura programma vai kods, kas Izveidots ar nolūku kaitēt datoram, tīklam vai serverim. Tas ir izplatītākais kiberuzbrukuma veids;

- *pakalpojumatteices uzbrukums (plašāk zināms kā DoS uzbrukums)* – ļaunprātīgs, mērķtiecīgs uzbrukums, kas pārpludina tīklu ar viltus pieprasījumiem, lai izjauktu biznesa operācijas. DoS uzbrukuma gadījumā lietotāji nespēj veikt ikdienas uzdevumus, piemēram, piekļūt e-pastam, tīmekļa vietnēm, tiešsaistes kontiem vai citiem resursiem, ko darbina kompromitēts dators vai tīkls;

- *pikšķerēšana* – kiberuzbrukuma veids, kas izmanto e-pastu, SMS, tālruni, sociālos medijus un sociālās inženierijas metodes, lai ieinteresētu upuri dalīties ar sensitīvu informāciju, piemēram, parolēm vai kontu numuriem, lejupielādēt failu, kas datorā vai tālrunī instalēs vīrusus u.c. Pikšķerēšana ir galvenā ļaunprogrammatūras izplatīšanas metode;

Baltijas Mediju izcilības centrs
Google

- ***izlikšanās*** ir paņēmiens, caur kuru kibernoziedznieks maskējas kā zināms vai uzticams avots, piemēram, viltojot e-pasta adreses domēnu, mājas lapas domēnu u.c. Šo uzbrukumu mērķi vibiežāk ir – nozagt informāciju, izspiest naudu vai ierīcei instalēt ļaunprogrammatūru vai citu kaitīgu programmatūru.

Kā sevi pasargāt?

Organizācijas digitālā drošība ir cieši saistīta ar darbinieku izpratni par dažādajiem riskiem, ar organizācijas resursiem un vispārējo sagatavotības līmeni, tostarp darbinieku "kiberhigiēnu" jeb prasmi ikdienā pieturēties pie tādiem ieradumiem, kas mazina kibernoziegumu iespējamību. Kiberdrošības pamatā ir katras organizācijas informācijas un komunikācijas tehnoloģiju sistēmas sakārtotība un pārzināšana, jo krīzes situācijā ir pieejams tikai tas aprīkojums, kas ieviests līdz krīzei, un arī darbinieki varēs darboties tikai saskaņā ar tiem darbības protokoliem, kas izstrādāti, ieviesti un praktizēti līdz krīzes situācijai. Tas vai nu atvieglos, vai apgrūtinās organizācijas darbu krīzes situācijā. Tālāk apkopoti 9 jautājumi, kas palīdzēs veikt sagatavošanās procesu un būt gataviem kiberdrošības krīzes situācijām.

1. Vai ir veikts risku izvērtējums?

Jebkura organizācija ir pakļauta zināmiem digitālās drošības riskiem. Tie atkarīgi no organizācijas darbības jomas un mērķiem, sadarbības partneriem, kā arī informācijas tehnoloģiju produktiem un pakalpojumiem, ko organizācija un tās darbinieki izmanto. Organizācijai ir jāizvērtē, kādas iekārtas un programmatūra tiek lietota darba procesā, kas tām var piekļūt, kas ir e-pasta servisa uzturētājs, kā notiek darbinieku autorizēšanās e-pastā. Tāpat jāidentificē tās darbības jomas, kas saistītas ar informācijas tehnoloģiju produktu un pakalpojumu potenciālo apdraudējumu, piemēram, kas administrē un uztur mājas lapas serveri – vai tas ir ārpakalpojums, vai to veic organizācija pati ar saviem iekšējiem resursiem. Par katru informācijas tehnoloģiju produktu un pakalpojumu, kā arī ar to saistīto darbības jomu ir nepieciešams veikt atsevišķu risku izvērtējumu, identificējot, cik tie ir iespējami un cik smagas var būt sekas. Tāpat jāievieš regulāras pārbaudes, atkārtojot risku analīzi un pārskatot ieviestos drošības pasākumus un protokolus.

2. Vai un kā notiek datu uzglabāšana un rezerves kopiju veidošana?

Viens no būtiskākajiem digitālās drošības apdraudējumiem ir organizācijas datu zaudēšana, sabojāšana vai īslaicīga nepieejamība. Tāpēc nepieciešams ievest datu uzglabāšanas un rezerves kopiju veidošanas sistēmu, kas definē, kādi dati tiek uzglabāti, kur tie tiek saglabāti un kuriem darbiniekiem ir iespēja tiem piekļūt. Statistika rāda, ka, kiberuzbrucējiem iekļūstot korporatīvā tīklā, tie gandrīz vienmēr cenšas nozagt tur esošās rezerves kopijas, tāpēc ir būtiski rezerves kopijas turēt citā – ar pamattīklu nesaistītā – vidē. Drošai darba veikšanai krīzes situācijā visiem darbiniekiem ir jābūt iespējai lietot darbam nepieciešamos datus arī attālināti, piemēram, izmantojot mākoņu tehnoloģijas.

3. Kāda ir darbinieku izpratne par kiberhigiēnu?

Neskatoties uz to, cik daudz laika un resursu organizācija būs ieguldījusi informācijas tehnoloģiju produktos un pakalpojumos, tās datu, sistēmu un iekārtu drošība ir cieši saistīta ar darbinieku izpratni par kiberhigiēnu. Jo labāk darbinieki spēj identificēt zema riska apdraudējumus ikdienas lietotāja līmeni, jo lielāka iespējamība, ka tiks pamanīts arī organizācijas apdraudējums. Tādēļ ir svarīgi organizēt regulāras darbinieku apmācības, lai veicinātu izpratni par kiberhigiēnu. Ja šādas apmācības nav iespējams nodrošināt ar organizācijai pieejamajiem resursiem, publiskā sektora organizācijām to var palīdzēt nodrošināt Informācijas tehnoloģiju drošības incidentu novēršanas institūcija CERT.LV.

Kā ievērot kiberhigiēnu?

- Sekot līdzi un saskaņā ar ražotāja rekomendācijām regulāri veikt datoru un telefonu programmatūru atjauninājumus, kā arī, atjauninot lietotņu versijas, izmantot tikai pārbaudītus avotus (ražotāju programmatūras veikalus – App Store, Google Play u.c.).

- Regulāri attīrīt viedierīces un datorus no lietotnēm un programmām, kas vairs netiek lietotas.

- Instalējot telefonā kādu lietotni, pārbaudīt, kādiem datiem šī lietotne pieprasa piekļuvi, kā arī izvērtēt, vai tiešām tas ir nepieciešams (piemēram, vai tiešām Instagram lietotnei jāpiekļūst kontaktu sarakstam vai mikrofona funkcijai pat tad, ja jūs nemaz neveicat video ierakstu ar skaņu vai nezvaniet caur Instagram).

- Saņemot e-pastu no nezināma sūtītāja, pārliecināties, vai sūtītājs ir reāla persona un vai e-pasta tekstā nekas nešķiet aizdomīgs.

- Saņemot savādus e-pastus, kas satur pielikumus vai saites, neklikšķināt uz šīm saitēm un neatvērt pielikumus. Tie var saturēt pikšķerēšanas uzbrukums. Saņemot šādu vēstuli, e-pasta skatījumu iestatījumos pārslēdziet no HTML uz plain text. Tā varēsiet redzēt saišu patiesos avotus un liegsiet jebkādu automātisku trešo pušu skriptu izpildi.

- Regulāri atjaunot savas paroles un neizmantot vienu un to pašu paroli vairākās vietās (paroļu sistematizēšanai var izmantot kādu no brīvpieejamajiem paroļu menedžeriem, piemēram, Bitwarden, vai Keepass). Izvēloties paroli, pieturēties pie principa, ka tā ne tikai satur burtus, ciparus, simbolus, bet arī saturiski apzīmē kaut ko neloģisku un grūti uzminamu (piemēram: SniegaGalva21!);

-Visur, kur iespējams, izmantot divu faktoru autentifikācijas iespēju. Šim nolūkam var izmantot, piemēram, Google Authenticator – autorizējoties savā profilā, papildus parolei tiks pieprasīta arī unikāla ciparu kombinācija, ko iespējams iegūt šajā lietotnē.

4. Kam ir piešķirtas administratora tiesības dažādās ierīcēs?

Organizācijas iegādātais aprīkojums (datori, mobilie telefoni, kameras u.c.) un to programmatūras ir organizācijas īpašums, tādēļ sistēmu pārvaldībai jānotiek centralizēti un tās jālieto tikai darba uzdevumu veikšanai. Lai to paveiktu, jābūt kādam atbildīgajam, kurš pārvalda un uzrauga organizācijai piederošo informācijas tehnoloģiju stāvokli, nodrošinot regulāru apkopi un atjauninājumu veikšanu. Tāpat šīs personas uzdevums ir arī sekot līdzi personāla izpratnei par kiberdrošību un darba procedūrām (piemēram, nodrošinot, ka nav iespējams izveidot pārāk vienkāršu e-pasta paroli vai lietot paroles atkārtoti, rūpējoties par to, ka visur, kur iespējams, darbinieki izmanto divu faktoru autentifikāciju u.c.).

5. Kā notiek pierakstīšanās tiešsaistes saziņas un sociālo mediju platformās un e-pastā?

Darbs medijos ir cieši saistīts ar dažādām tiešsaistes saziņas un sociālo mediju platformām. Tās tiek izmantotas ne tikai no darba datora, bet arī telefona un privātajām ierīcēm. Ir būtiski, lai katram

darbiniekam būtu unikāls lietotājvārds un parole, kā arī, autorizējoties būtu iespēja pielietot divu faktoru autentifikāciju. Ir izstrādātas dažādas lietotnes un pakalpojumi, kas nodrošina divu faktoru autentifikācijas principu, piemēram, *Google Authenticator vai Microsoft Authenticator.* Svarīgi izvēlēties organizācijas vajadzībām un iespējām atbilstošāko rīku vai pakalpojumu sniedzēju. Divu faktoru autentifikācijas principa izmantošana ļauj paroles pieprasītājam pārliecināties, ka tās ievadītājs ir patiesais paroles turētājs.

6. Kā notiek datu apmaiņa?

Bieži vien organizācijas kiberuzbrukumus piedzīvo, darbiniekiem saņemot e-pasta vēstuli. Šādi kiberuzbrukumi parasti nav saistīti ar mērķi kompromitēt konkrētās organizācijas digitālo infrastruktūru, biežāk ļaundari tā cenšas iegūt organizācijai piederošus datus un informāciju. Tāpēc ieteicams ieviest šifrētu datu apmaiņu, īpaši e-pastiem, kas nozīmē to, ka e-pasta saturs no vienkārši lasāma teksta tiek pārvērsts šifrētā tekstā, ko var izlasīt tikai tā adresāts. Šādu funkcionalitāti piedāvā, piemēram, Microsoft 365 abonements). To, kā pilnveidot e-pasta drošību, aprakstījusi Amerikas kiberdrošības aizsardzības aģentūra, bet jautājumu gadījumā var vērsties arī pie Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV speciālistiem.

7. Kādi komunikācijas kanāli kādam mērķim tiek izmantoti?

Organizācijas un to darbinieki ikdienā izmanto dažādus saziņas kanālus – e-pastu, tērzēšanas lietotnes u.c. Izstrādājot plānus dažādu krīžu pārvarēšanai, ir svarīgi tajos iekļaut un iepriekš vienoties par to, kurš komunikācijas kanāls tiktu izmantots saziņai krīzes situācijā. Ir jābūt pilnīgai skaidrībai par to, kuriem darbiniekiem ir piešķirtas kanāla administratora tiesības (ieteicams administratora tiesības piešķirt vismaz 2 personām). Krīzes situācijā vēlams darboties tā, lai darbiniekiem būtu pieejami divi komunikācijas kanāli. Viens, kas atzīts par pamata saziņas kanālu ikdienā izmantotajā lietotnē, kā arī otrs saziņas kanāls citā tērzēšanas lietotnē, ko iespējams izmantot, ja tehnisku iemeslu dēļ primārais saziņas kanāls nav pieejams. Krīzes darbības protokolā jābūt skaidri definētam tam, kad un kā lietot katru saziņas kanālu, lai informācija ātri un efektīvi sasniegtu adresātus.

8. Kā kiberuzbrukuma gadījumā rīkojas indivīds?

Kiberuzbrukumu veidi ir dažādi, tādēļ iespēja, ka persona, kuras dators, e-pasts vai mobilais telefons ir kompromitēts, nespēs identificēt, ka ir noticis kiberuzbrukums, ir liela. Lai veicinātu darbinieku izpratni un atsaucību, organizācijā jārada atvērta vide ziņošanai par aizdomīgiem e-pastiem, savādām ziņām saziņas lietotnēs, vai neparastu iekārtu uzvedību. Ir svarīgi, lai gadījumā, ja darbinieks ir ziņojis par kaut ko, kas radījis aizdomas, bet tas tomēr izrādās kļūdains ziņojums, darbinieks nesaņemtu nosodījumu vai izsmieklu. Lai sistematizētu un sakārtotu šo procesu,

organizācijai jāizstrādā ziņošanas protokols: kā un kam ziņot, ja kaut kas šķiet aizdomīgs. Jo brīvāk darbinieki varēs ziņot un izteikt savas aizdomas, jo veiksmīgāk atbildīgā persona varēs apzināt situāciju un riskus, turpinot rūpēties par organizācijas kiberdrošību.

NOTURĪGĀ BALTIJA

9. **Izstrādājiet rīcības protokolus!**

Izstrādājiet rīcības protokolus tam, kā organizācijas darbiniekiem būtu jārīkojas, ja organizācija piedzīvo informācijas tehnoloģiju produktu un pakalpojumu apdraudējumu. Neaizmirstiet arī par krīzes darbības protokoliem gadījumos, ja organizācijas darbība ir apdraudēta citu iemeslu dēļ (plūdi, ugunsgrēks u.c.). Regulāri atjauniniet informāciju un pārliecinieties, ka darbinieki zina, kā rīkoties krīzes situācijā.

Digitālā drošība krīzes situācijā

Ja krīze radusies organizācijas informācijas tehnoloģiju produktu un pakalpojumu apdraudējuma rezultātā (piemēram, kiberuzbrukums, datu noplūde u.c.):

1. Pēc iespējas ātrāk apziniet situācijas mērogu un izolējiet apdraudētos informācijas tehnoloģiju produktus un pakalpojumus, lai novērstu uzbrukuma seku izplatību.
2. Informējiet darbiniekus par krīzes situāciju, kā arī soļiem tās novēršanai.
3. Izolējiet apdraudēto iekārtu no korporatīvā tīkla.
4. Veiciet uzbrukuma analīzi vai nosakiet datu noplūdes iemeslu un izstrādājiet seku novēršanas plānu. Varat izmantot jau izstrādātas risku mazināšanas stratēģijas, tās pielāgojot konkrētajai situācijai.

Ja krīzes situācija iestājusies nesaistīti ar organizācijas informācijas tehnoloģiju produktu un pakalpojumu apdraudējumu:

1. Aktivizējiet un lietojiet tikai krīzes protokolā apstiprinātos iekšējās komunikācijas kanālus.
2. Pārliecinieties, ka ir ievērotas norādes, kas ietvertas 2., 3., 5. un 6. rekomendāciju punktā.
3. Pārbaudiet organizācijas datu drošību! Ja nepieciešams evakuēties no biroja, pārbaudiet, ka visi darbiniekiem nepieciešamie dati pieejami mākoņu platformās un tiem ir kopijas.
4. Pārliecinieties, ka organizācijas kritiskie resursi ir pasargāti.

Autore: Zane Štāla
Redaktore: Krista Priedīte

Baltijas Mediju izcilības centrs
Google