Co-funded by the
Erasmus+ Programme
of the European Union

Kiberdrošība

Satura rādītājs

Latvian School of Public Administration

Ievads

Mūsdienās ar tehnoloģiju uzlabojumiem un katru dienu izveidotām jaunām lietotnēm un rīkiem mums jāapzinās ne tikai tehnoloģiju pozitīvais pienesums, bet arī jāpievērš uzmanība draudiem, ko tehnoloģiskā attīstība rada. Mēs arvien vairāk sākam izmantot tehnoloģiju darbam un personīgām vajadzībām un koplietojam datus ar kolēģiem, ģimeni un draugiem, mums ir jāpārliecinās, ka mūsu dati ir aizsargāti, un mēs zinām, ar ko kopīgojam piekļuvi savai personiskajai informācijai.

Ikdienā mēs nodrošinām aizsardzību pret noziedzīgām darbībām ieviešot mājas drošības sistēmas, nedodam kredītkartes informāciju svešiniekiem uz ielas vai nedalāmies ar personisko informāciju ar cilvēkiem, kurus mēs nepazīstam. Tieši tāpat mums jārīkojas strādājot tiešsaistē, iepērkoties tiešsaistē vai daloties ar personisko informāciju dažādās sociālo mediju platformās. Kad izmantojam dažādas informācijas un komunikācijas tehnoloģijas, mums jāpievērš uzmanība kiberdrošībai, kas palīdz aizsargāt dažādus digitālos komponentus, datus un datorsistēmas no neatļautas piekļuves.

Kiberdrošību (sauktu arī par informācijas tehnoloģiju drošību) var raksturot kā kolektīvās metodes, tehnoloģijas un procesus, kas palīdz aizsargāt datorsistēmu, tīklu un datu konfidencialitāti, integritāti un pieejamību pret kiberuzbrukumiem vai neatļautu

piekļuvi, kuru mērķis ir izmantot jūsu datus. Kiberdrošības galvenais mērķis ir aizsargāt visas organizatoriskās vai personiskās vērtības gan no ārējiem, gan no iekšējiem draudiem.

Kiberdrošības risks ir ievainojamības vai zaudējumu varbūtība, kas rodas kiberuzbrukuma vai datu pārkāpuma dēļ jūsu organizācijas vai personas datiem. Tā kā arvien vairāk paļaujamies uz datoriem, tīkliem, programmām un sociālajiem medijiem, organizācijas un privātpersonas kļūst aizvien neaizsargātākas pret kiberdraudiem. Globālā savienojamība un pieaugošā mākoņpakalpojumu izmantošana ar sliktiem drošības uzstādījumiem nozīmē, ka palielinās kiberuzbrukumu risks.

Lai samazinātu kiberuzbrukumu risku, pastāv procesi un darbības, kas paredzētas, lai palīdzētu jums izvairīties no kiberuzbrukumiem un aizsargātu savus datus un citu sensitīvu informāciju no kibernoziedznieku neatļautas piekļuves. Procesus un darbības, kas paredzētas, lai izvairītos no kiberuzbrukumiem, sauc par kiberdrošības riska pārvaldību.

Kiberdrošības riska pārvaldība balstās uz kiberdrošības aizsardzības pasākumu īstenošanu un prioritāšu noteikšanu, pamatojoties uz iespējamiem draudiem. Kiberdrošības risku pārvaldība parasti ir atkarīga no riska analīzes, kas aprēķina kiberdrošības riskus. Citiem vārdiem sakot, pirms sākat lietot datoru vai jaunu sistēmu, rīku vai pirms aizdomīga e-pasta atvēršanas, jums ir jāanalizē riski, ko var izraisīt darbība. Ja jūs veicat pareizos piesardzības pasākumus, varat ievērojami samazināt kiberuzbrukumu risku.

Labākais veids, kā pārliecināties par jūsu datu drošību, ir iepazīties ar informāciju par dažādiem draudiem un kiberuzbrukumiem. Tāpēc šajā materiālā mēs jūs iepazīstināsim ar galvenajiem draudiem, kas var rasties, lietojot informācijas un komunikācijas tehnoloģijas, lai jūs varētu būt informēti un pamanīt aizdomīgas darbības tiešsaistē un pasargāt sevi.

Kiberdrošības nozīme un problēmas

Ņemot vērā strauji mainīgās tehnoloģijas un to, ka programmatūru ieviešana arvien pieaug dažādās nozarēs, tostarp finanšu, pārvaldības, militārajā, mazumtirdzniecības, veselības aprūpes, izglītības, enerģētikas un citās, arvien vairāk informācijas kļūst digitāla un

pieejama bezvadu un vadu ciparu sakaru tīklos un visuresošajā internetā. Visa šī slepenā informācija ir ļoti vērtīga noziedzniekiem un ļaundariem, tāpēc ir svarīgi to aizsargāt, izmantojot spēcīgus kiberdrošības pasākumus un procesus.

Laba kiberdrošības stratēģiju nozīme ir acīmredzama, jo bieži varam lasīt ziņās par dažādiem kiberuzbrukumiem un dzirdam no mūsu draugiem un kolēģiem, ka viņu dati tikuši uzlauzti. Bet, ja esat piesardzīgs un droši aizsargājat savus datus, jums nevajadzētu baidīties no dažāda veida tehnoloģiju izmantošanas. Ja esat iepazinies ar kiberdraudiem un zināt, kā no tiem izvairīties, varat droši un pārliecinoši izmantot informācijas un komunikācijas tehnoloģijas. Lai to izdarītu, mēs sniegsim jums visizplatītāko kiberuzbrukumu piemērus, lai jūs tos varētu atpazīt un atbilstoši rīkoties, lai nākotnē novērstu iespējamos kiberuzbrukumus.

Kas ir kiberuzbrukums?

Kiberuzbrukums ir ārēju vai iekšēju draudu vai uzbrucēju apzināts mēģinājums izmantot un apdraudēt organizācijas vai personas(-u) informācijas sistēmu konfidencialitāti, integritāti un pieejamību. Kiberuzbrucēji izmanto nelegālas metodes, rīkus un pieejas, lai radītu zaudējumus un traucējumus vai iegūtu neatļautu piekļuvi datoriem, ierīcēm, tīkliem, lietojumprogrammām un datu bāzēm.

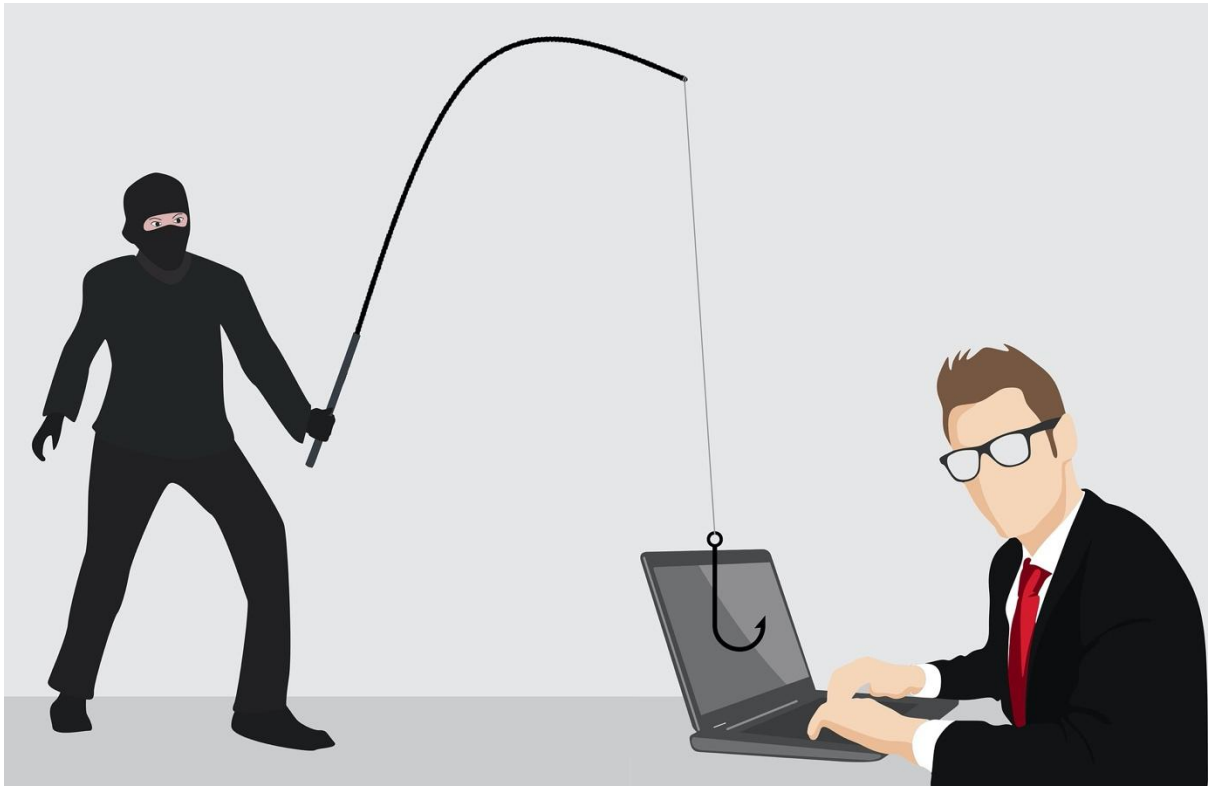
Kiberuzbrukumi ir ļoti dažādi, un šajā sarakstā ir uzsvērti daži svarīgākie uzbrukumi, kurus noziedznieki un uzbrucēji izmanto programmatūras izmantošanai. Apskatīsim dažādus kiberuzbrukumus, ar kuriem jūs varat saskarties.

Pikšķerēšana

Pikšķerēšana ir metode iegūt personisko informāciju, izmantojot maldinošus e-pastus un vietnes. Šī kiberuzbrukuma mērķis ir apmānīt e-pasta saņēmēju domāt, ka saņemtais ziņojums ir kaut kas viņiem vēlams vai vajadzīgs, piemēram, jūs varat saņemt e-

pastu no savas bankas vai apdrošināšanas kompānijas vai veikt pirkumu šķietami parastā tiešsaistes veikalā.

Šo metodi labi raksturo tās nosaukums pikšķerēšana, kas nāk no vārda "makšķerēšana". Hakeri izsūta viltus e-pastus, tāpat kā zvejnieki izmet ēsmu ar āķi, un cer, ka jūs uzķersieties. Bet tā vietā, lai izmantotu ēsmu, kā to darītu zvejnieki, kiberuzbrucēji maskējas kā uzticama persona, kas jums ir pazīstama (piemēram, jūsu banka vai kolēģis). Šo cilvēku vai firmu vārdā hakeri nosūtīs jums e-pastu ar vēlmi iegūt jūsu personas datus.



Šajos e-pasta ziņojumos parasti tiek prasīts noklikšķināt uz saites vai lejupielādēt pielikumu, taču, tāpat kā mēs arvien vairāk apzināmies pikšķerēšanas uzbrukumus, hakeri nāk klajā ar jaunām pikšķerēšanas shēmām. Visizplatītākie pikšķerēšanas uzbrukumi ir šādi:

- e-pasts par to, ka jūsu konts ir uzlauzts.

Kiberuzbrucēji jums var nosūtīt e-pastu uzticamas personas vārdā, kurā teikts, ka jūsu konts ir uzlauzts un viņi ir apkopojuši visus jūsu datus un personisko informāciju. Viņi var prasīt naudu, lai jūsu dati tiktu atgriezti.

- Paroles atiestatīšanas e-pasts

Jums atsūtīs e-pastu ar paziņojumu, ka jums ir jāmaina parole. Jums tiks lūgts sekot saitei, kur varat mainīt paroli, taču šīs shēmas mērķis ir savākt jūsu pieteikšanās ID, lai nozagtu datus.

- Maksājuma pieprasījums

Kiberuzbrucēji mēģinās maldināt jūs sniegt viņiem savu bankas vai kredītkartes informāciju, izliekoties, ka esat sūtījis e-pastu no savas bankas, sakot, ka jums ir jāveic vai jāapstiprina maksājums. Labākais veids, kā neiekrist šajā trikā, ir zināt savas bankas komunikācijas politiku vai sazināties ar banku ikreiz, kad saņemat dīvainas e-pasta vēstules.

- Ziedojums labdarībai

Šajā gadījumā kiberuzbrucēji jums nosūtīs e-pastu ar paziņojumu, ka esat laimējis loterijā, kāds tāls radinieks, par kuru pirmo reizi dzirdat, nesen miris un atstājis jums visu savu naudu, vai labdarības organizācija izvēlējusies ziedot jums naudu. Lai saņemtu naudu, jums tiks lūgts sekot saitei vai veikt nelielu maksājumu. Lai neuzķertos uz šo shēmu, galvenais ir atcerēties: ja tas izklausās pārāk labi, lai būtu patiesība, tā, visticamāk, nav patiesība.

Sociālā inženierija

Tradicionāli kiberuzbrucēji mēģina apdraudēt IT sistēmu un lietojumprogrammu drošību, mērķis ir izmantot cilvēkus, kuri izmanto tehnoloģijas, lai pārliecinātu lietotāju atklāt tādus noslēpumus kā paroles, karšu numurus utt. Vai piešķirt fizisku piekļuvi savam uzņēmumam, piemēram, uzdodoties par darbiniekiem, pārdevējiem vai atbalsta personālu. Šādi tiek izmantota cilvēku uzticību, mudinot atklāt informāciju, kas apdraud datu drošību.

Sociālā inženierija ir bīstama, jo tradicionālā aizsardzība pret vīrusiem vai ļaunprātīgu programmatūru jums nepalīdzēs no sociālās inženierijas uzbrukuma. Kad kiberuzbrucēji apkopos informāciju no jūsu organizācijas, viņi varēs ļaunprātīgi izmantot biznesu.

Visizplatītākā sociālās inženierijas tehnika ir pikšķerēšanas e-pasta ziņojumi, kurus apskatījām jau iepriekšējā nodaļā. Šajā gadījumā kiberuzbrucēji nosūtīs jums e-pastu, lūdzot noklikšķināt uz saites. Noklikšķinot uz saites, jūs ļausiet hakeriem piekļūt savai sistēmai.

Vēl viena tehnika ir fiziski pārkāpumi. Šajā scenārijā kiberuzbrucējs uzdodas par citu personu, lai no iekšienes iegūtu datus. Vēl viena metode ir zvanīšana - kiberuzbrucēji izveido scenāriju, lai iegūtu nepieciešamo informāciju.

Neļaujieties šiem kiberuzbrucēju uzbrukumiem un uzbrukuma gadījumā vienmēr ievērojiet drošības pasākumus. Nekad neatveriet aizdomīgas saites un neuzticieties cilvēkiem, kuri lūdz personisku informāciju. Ja neesat pārliecināts, vai šis cilvēks tiešām ir atbalsta servisa darbinieks, vienmēr sazinieties ar savu vadītāju, lai noskaidrotu, vai vadība ir

lietas kursā par notiekošo. Jebkurš IT sistēmas darbs vienmēr tiks plānots, un par to tiks informēti jūsu vadītāji.

Ļaunprātīga programmatūra

Ļaunprātīga programmatūra ir jebkura programmatūra, kas speciāli izveidota, lai radītu kaitējumu datoram, serverim, klientam vai datortīklam (turpretī programmatūru, kas dažu trūkumu dēļ nodara netīšu kaitējumu, parasti raksturo kā programmatūras kļūdu). Ļaunprātīga programmatūra ir datora kods, kas paredzēts, lai traucētu, atspējotu vai pārņemtu kontroli pār jūsu datorsistēmu.

Ļaunprātīga programmatūra parasti ir visdažādākajās formās un tiek paslēpta citā failā vai lietotnē. Kad ļaunprātīgā programmatūra atrodas jūsu datorā, tā darbojas, izmantojot datora tehniskos trūkumus vai ievainojamību.

Ir daudz ļaunprātīgu programmatūras veidu, ieskaitot datorvīrusus, tārpus, Trojas zirgus, izspiedējvīrusus, spiegprogrammatūru, reklāmprogrammatūru, negodīgu programmatūru, tīrītāju un baidatūru. Izspiedējvīruss bloķē inficētās sistēmas, līdz upuris samaksā izpirkuma maksu, lai to atbloķētu. Identifikācijas datu zagļi tiek izmantoti, lai iegūtu lietotājvārdus un paroles e-pastiem un citiem kontiem. Banku identifikācijas ļaunprātīgā programmatūra ir precīzāka un vērsta uz jūsu bankas datiem. Lai nozagtu jūsu datus, kiberuzbrucēji izmanto tastatūras, lai iegūtu paroles, kontu numurus un sensitīvāku informāciju.

Gandrīz visi vīrusi ir pievienoti neizpildāmam failam, kas nozīmē, ka vīruss var pastāvēt sistēmā, bet tas neizplatīsies, kamēr lietotājs neatver inficēto programmu. Vīrusi parasti tiek iegūti, pārlūkojot internetu, un tie izplatās, lejupielādējot failu, kas inficēts ar šo vīrusu.

Trojas zirgs ir kaitīga programmatūra, kas izskatās likumīga; parasti lietotāji tiek maldināti, vadot un izpildot to savās sistēmās. Trojas zirgi var ne tikai apstrādāt jūsu

sensitīvos datus, bet arī hakeriem nodrošināt piekļuvi jūsu sistēmai. Trojas zirgi tiek izmantoti, lai piekļūtu jūsu datoru finanšu un personiskajai informācijai.

Spiegprogrammatūra slepeni apkopo informāciju par lietotāja darbībām, piemēram, interneta lietošanu, un reģistrē taustiņsitienus reģistrēšanās procesa laikā, lai iegūtu paroles un citu sensitīvu informāciju.

Visas šīs ļaunprātīgās programmas vieno cilvēks. Hakeri var piekļūt jūsu datorsistēmai tikai tad, ja atverat inficētu failu, palaižat ļaunprātīgu failu vai noklikšķināt uz nedrošas tīmekļa saites. Tas ir, katram datora lietotājam vienmēr jāpatur prātā šie iespējamie piedāvājumi un divreiz jāpārdomā, pirms atverat nedrošus dokumentus vai saites, īpaši, ja tie nāk no nezināma sūtītāja.

Labākais veids, kā pasargāt sevi no ļaunprātīgas programmatūras, ir antivīrusa izmantošana, kas tiek regulāri atjaunināta. Tiek izmantoti dažādi pretvīrusu programmatūras, ugunsmūri un citas stratēģijas, kas palīdz aizsargāties pret ļaunprātīgas programmatūras ieviešanu, atklāt to, ja tā jau ir, un atgūties no ļaunprātīgas programmatūras saistītas ļaunprātīgas darbības un uzbrukumiem.

Paraugprakse kiberdrošības draudu novēršanai

Lai novērstu kiberuzbrukumus, jābūt diviem atbildības līmeņiem. Pirmais līmenis ir organizācijas līmenis. Kā aprakstīts iepriekš šajā materiālā, organizācijām būtu jāīsteno kiberdrošības risku pārvaldība un jāanalizē iespējamie draudi. Veicot šos preventīvos pasākumus, jūsu organizācija var būt labāk sagatavota kiberuzbrukumiem un zina, kā rīkoties, ja šāds uzbrukums notiek.

Spēcīga kiberdrošības stratēģija nebūtu veiksmīga, ja darbinieki netiktu izglītoti par kiberdrošību, uzņēmuma politiku un ziņošanu par incidentiem. Pat vislabākā tehniskā aizsardzība neko nedos, ja darbinieki veic neapzinātas vai tīšas ļaunprātīgas darbības, kuru rezultātā tiek izdarīti dārgi drošības pārkāpumi. Darbinieku izglītošana un izpratnes veicināšana par uzņēmuma politiku un drošības paraugpraksi, izmantojot seminārus,

nodarbības un tiešsaistes kursus, ir labākais veids, kā mazināt drošības pārkāpumu iespējamību.

Ieviesiet drošu paroļu glabāšanu. Organizācijām būtu jāliek saviem darbiniekiem izmantot drošas paroles, kas atbilst visiem nozares standartiem. Tās arī jāliek periodiski mainīt, lai palīdzētu aizsargāties no uzlaušanas.

Otrais pienākumu līmenis ir personīgais līmenis. Katrs cilvēks ir atbildīgs par savu rīcību tiešsaistē, un viņam vajadzētu padomāt, vai viņa rīcība var radīt potenciālu apdraudējumu datoram un datiem. Ar datoru vienmēr jāstrādā tikai tad, ja zināt, ka tajā ir aktīva pretvīrusu sistēma, kas nesen ir atjaunināta. Izmantojot antivīrusu sistēmu, jūs varat ievērojami samazināt ļaunprātīgas programmatūras risku.

Lai izvairītos no sociālās inženierijas un pikšķerēšanas uzbrukumiem, jums vienmēr jābūt ļoti uzmanīgam un jāpievērš uzmanība tam, kādus e-pastus atverat, kādām saitēm sekojat un kādus pielikumus lejupielādējat. Nekad neatveriet aizdomīgas saites un neuzticieties cilvēkiem, kuri lūdz personisku informāciju. Ja nejūtaties drošs par personu, kura jums zvana un apgalvo, ka ir bankas darbinieks vai atbalsta darbinieks jūsu organizācijā, vienmēr sazinieties ar savu banku vai vadītāju. Tas pats attiecas uz aizdomīgām e-pasta

vēstulēm. Ja nejūtaties pārliecināts par saturu un sūtītāju, neatveriet e-pastu un nesekojiet saitei.