vied pircējs

CEĻVEDIS UZŅĒMĒJDARBĪBAI TIEŠSAISTĒ

FINANŠU NOZARES ASOCIĀCIJA

mastercard

IEVADS

Pircēji Latvijā arvien vairāk iepērkas internetā. Reaģējot uz pircēju paradumu maiņu, uzņēmēji aizvien biežāk sākuši piedāvāt preces un pakalpojumus tiešsaistē — tas sniedz ērtību, drošību un biznesa kontroli. Būtiski, ka arī uzņēmēji rūpējas par digitālo drošību, tādējādi pasargājot savus klientus un biznesu.

Kiberdrošība tiešsaistē ietver tehnoloģijas, procesus vai darbības, kas izstrādātas, lai aizsargātu tīklus, iekārtas, programmas un datus no uzbrukumiem, bojājumiem vai nesankcionētas piekļuves.

Katru gadu visā pasaulē palielinās veikto kiberuzbrukumu skaits, kvalitāte un apjoms. Dati rāda, ka neatkarīgi no uzņēmuma lieluma tas var tikt pakļauts kiberuzbrukumu riskam. Tomēr tieši mazie un vidējie uzņēmumi ir mazāk gatavi šos uzbrukumus novērst. Lielākā daļa, proti, 60 % no kiberuzbrukumiem, ir vērsti tieši pret maziem vai vidējiem uzņēmumiem. Vienlaikus patērētāji gaida, ka vietnē saglabātā informācija būs drošībā. Ja šī uzticība tiek pievilta — 31 % respondentu norāda, ka nekad vairs neizmantos uzņēmuma pakalpojumus, ja no tā ir noplūdusi informācija vai tas ir ticis uzlauzts, liecina Cyber Readiness Institute apkopotie dati.

Šī e-grāmata vienkopus sniedz informāciju un praktiskus padomus, kas būtu jāzina katram uzņēmējam, kurš plāno vai kam jau ir tiešsaistes veikals, kā arī tiem, kas vēlas uzzināt vairāk par digitālo drošību. Tostarp informāciju par uzbrukumu veidiem, maksājumu metodēm, risinājumiem, kas palīdzētu mūsdienu uzņēmumam aizsargāties un atpazīt riskus, kā arī apkopoti noderīgi rīki un saites. Šis ir īstais brīdis iepazīties ar šī ceļveža saturu!

SATURA RĀDĪTĀJS

KĀDI IR UZBRUKUMU VEIDI TIEŠSAISTĒ?

Ļaunprogrammatūra jeb ļaunatūra

- Dažādu veidu kaitnieciskas programmas, kas tiek instalētas ierīcēs bez lietotāja ziņas.
- Šāda veida uzbrukums iespējo neatļautu darbību uzsākšanu datorā vai viedtālrunī, lai iegūtu vērtīgu informāciju, liegtu pieeju glabātajiem datiem vai apturētu ierīces darbību pavisam.
- Visbiežāk ļaunatūra tiek izplatīta e-pasta pielikumos, caur nelegālām vai inficētām tīmekļvietnēm, kā arī izmantojot reklāmas vai saites.

Paroļu uzlaušana vai piemeklēšana no uzlauztām datubāzēm

- Viens no vienkāršākajiem veidiem ir paroļu uzlaušana vai arī piemeklēšana no jau noplūdušām paroļu datubāzēm. Pierādīts, ka 6 simbolu paroles atmināšanai, kas sastāv tikai no cipariem, jaudīgam datoram nepieciešams vien pāris sekunžu.
- Cits uzbrukuma veids, kā piekļūt parolēm un tās izmantot, — no tīmekļvietnes datubāzes iegūt informāciju par lietotājiem, kas ietver arī paroles, ar šiem pašiem datiem piekļūt lietotāju kontiem citās vietnēs, jo nereti lietotājs izmanto vienu paroli vairākos portālos. Tāpēc īpaši svarīgi rūpēties par datu drošību, kurus uzticējis klients.
- Mūsdienās tikai parole nav uzskatāma par drošu autentifikācijas veidu. Lielākai drošībai nepieciešama vairākfaktoru autentifikācija. Mazāk sensitīvas informācijas aizsardzībai būtu vērts apsvērt iespēju autentificēties ar sociālo tīklu profilu.

Pikšķerēšana

- Veids, kā ļaundari cenšas iegūt no interneta lietotāja personīgu, slepenu informāciju, tostarp karšu vai internetbankas datus, piekļuves lietotājvārdus un paroles u. c. Ļaundaris var uzdoties arī par bankas, Valsts ieņēmumu dienesta vai policijas darbinieku. Atceries, ka banka nekad neprasīs sūtīt tavus identifikācijas datus pa e-pastu, ar īsziņu vai ar tālruņa starpniecību. Šādi dati nevienam nav jāizpauž.
- Šāds uzbrukums var tikt īstenots ar telefona zvana, īsziņas, e-pasta, dažādu tērzētavu starpniecību, aicinot atvērt saiti uz tīmekļvietni vai failu pielikumā, kas uzdodas par pazīstamu vietni un izskatās pēc tās, un aicina tajā ievadīt, piemēram, uzņēmuma bankas datus.

Nulles dienas uzbrukums

- Visas sistēmas ir pakļautas uzbrukumiem, par nulles dienas uzbrukumu sauc uzbrukumu, piemēram, mājaslapai, kad tas noticis pirmo reizi. Šādu uzbrukumu nav iespējams paredzēt, jo, attīstoties sistēmām, attīstās arī ļaundaru tehnikas.
- Ļaundari atrod ievainojamību sistēmā vai programmā, par kuru tās izstrādātājs iepriekš nav zinājis vai nav paspējis novērst, un piekļūst informācijai ierīcēs.
- Parasti iespējas veikt šāda veida uzbrukums tiek pietaupītas īpašiem mērķiem, kur iespējamais guvums ir sevišķi vērtīgs.
- E-komercijas vietnes parasti cieš no uzbrukumiem, izmantojot ievainojamības, kurām labojumi pieejami jau mēnešiem vai pat gadiem, un no tiem varētu izvairīties.

DDoS uzbrukums

- Saukts arī par Distributed Denial of Service jeb izplatīta pakalpojuma atteikums uzbrukumu pārslodzes dēļ.
- Šāda uzbrukuma gadījumā tiek izmantoti vairāki datori, lai pārslogotu tīmekļvietni, vienlaicīgi sūtot lielu daudzumu pieprasījumu. Tādējādi tiek pārslogotas sistēmas vai iekārtas, traucējot to darbību.

- Iespējams realizēt vienkāršākus DoS, jeb pakalpojumu atteices uzbrukumus, kas tiek mērķēti uz specifiskām datorsistēmas vietām, kas ir sevišķi jutīgas un to pārslodze izraisa kopēju sistēmas darbības traucējumu.

Sociālā inženierija

- Informācija par indivīdu un uzņēmumu bieži plaši pieejama internetā, tāpēc ļaundaris var mēģināt izlikties par to, kas viņš patiesībā nav.
- Dažāda veida uzbrukumi, kas īstenoti ar cilvēku savstarpējās komunikācijas palīdzību, psiholoģiski apmānot līdzcilvēku, lai tas izpaustu sensitīvu informāciju vai veiktu kādu darbību. Piemēram, uzdodoties par citu cilvēku vai izmantojot kopīgos kontaktus, lai iegūtu uzticību.

Atceries!

40 % no tiem, kuri ir saskārušies ar krāpšanu, nav spējuši to atpazīt un iekrituši, liecina aptaujas dati. Tava un kolēģu izpratne, zināšanas par riskiem ir būtiska jūsu uzņēmuma kiberdrošības nodrošināšanai.

KĀ AIZSARGĀT SAVU INTERNETA VEIKALU?

Izvēlies jau gatavus un drošus risinājumus internetveikala uzturēšanai un izveidei

- Tādējādi būs iespējams izvairīties no vietnes nepilnībām un būt pārliecinātam, ka tiek veiktas nepieciešamās izmaiņas, kas atbilst drošības standartiem.
- Šāda risinājuma izvēle aizņems mazāk laika tā ieviešanai. Ir vairākas vietnes, kas nodrošina šādus pakalpojumus, tostarp, piemēram, Mozello, Shopify, Wix un citas.

Lieto drošas un unikālas paroles un divu faktoru autentifikāciju

- Tas palīdzēs izvairīties no nepiederošu personu piekļūšanas uzņēmuma sistēmām. Statistika rāda, ka līdz pat 63 % no visiem kiberuzbrukumiem ir notikuši vāju vai nozagtu paroļu dēļ.
- Droša parole ir gara — vismaz 14–16 simbolu, kas ietver burtus, ciparus, citas zīmes. Lai būtu vieglāk atcerēties, var izmantot tā sauktās paroļu frāzes, kas ietver, piemēram, tev zināmas dziesmas vai dzejoļa vārdus, ciparus un simbolus.
- Alternatīva ir lietot paroļu pārvaldniekus, kas automātiski ģenerē paroles un glabā šifrētā veidā.
- Papildu drošībai ieteicams izmantot arī divu faktoru jeb stingro autentifikāciju, kas pieprasa apstiprināt pieeju vēl kādā veidā, piemēram, nosūtot SMS ar unikālu pieslēgšanās kodu vai papildu autorizācijas iespēja lietotnē.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS.

Regulāri atjaunini programmatūru

Lielākā daļa šo atjauninājumu tiek izstrādāti ar mērķi novērst ievainojamības sistēmā un uzlabot tās drošību.

Sadarbojies ar profesionāliem pakalpojumu sniedzējiem, kuri gatavi uzņemties atbildību par savu darbu

- Informācijas uzglabāšana profesionāļu uzturētos **virtuālos serveros** (mākonī) ir viens no veidiem, kā pasargāt informāciju no nelabvēļiem.
- Ieteicams, ka dati tiek uzglabāti kriptēti, kas nozīmē, ka algoritms tos pārvērš formātā, kas lietotājam bez pieejas atslēgas nav saprotams. Jāatceras, ka pieejas atslēgas jāglabā droši. Ja kāds tai piekļūst, tas var novest pie piekļuves datiem, savukārt, ja tā tiek pazaudēta, visi dati ir neatgriezeniski zuduši.
- Serveriem būtu atrodas attāli — apsargātās telpās, kur tiem nevar piekļūt nepiederošas personas. Tāpat ir ieteicams veidot datu rezerves kopijas, kas uzbrukuma gadījumā, kad piekļuve informācijai tiek liegta, var novērst to, ka vērtīga informācija tiek pazaudēta. Vienlaikus ir jāatceras un jāseko līdzi Payment Card Industry (PCI) standartiem, kas nosaka, kā informācija ir jāaizsargā tirgotājiem, kas pieņem karšu maksājumus.
- Payment Card Industry Security Standards Council piedāvā arī pašvērtējuma anketu, kas palīdzēs saprast esošo situāciju un veikt atbilstošus uzlabojumus, ja tādi nepieciešami. Vairāk informācijas var meklēt sadaļā Papildu resursi.

Veido rezerves datu kopijas

Uzbrukuma gadījumā, kad piekļuve informācijai tiek liegta, kopija var novērst to, ka vērtīga informācija tiek zaudēta. Tādējādi var tikt nodrošināta uzņēmuma nepārtraukta darbība.

Seko līdzi vietnes aizsardzībai

Lai pārliecinātos, ka vietne un uzņēmums ir pasargāts no uzbrukuma riskiem, ir pieejami dažādi **drošības testi un automātiski skeneri**, kas pārbauda sistēmu un ziņo par iespējamām nepilnībām. Šīs e-grāmatas beigās ir pieejams saraksts ar resursiem, kur iekļauti arī piemēri drošības testiem un citi risinājumi drošības uzturēšanai.

Atceries!

Ir svarīgi rūpēties par digitālo drošību ik dienu — regulāri mainīt paroles, veikt programmatūras atjauninājumus un saglabāt datu rezerves kopijas. Pārliecinies, ka uzņēmumā par to ir informēti visi!

DROŠAS MAKSĀJUMU METODES INTERNETĀ

2020. gada maija aptauja par Latvijas iedzīvotāju iepirkšanās paradumiem liecina — ja, iegādājoties preces vai pakalpojumus internetā, tiek dota iespēja izvēlēties, priekšroka būs maksājumiem ar maksājumu karti un pieslēgumu internetbankai. Turklāt teju 70 % Latvijas iedzīvotāju ir svarīgi, ka uzņēmumu preces un pakalpojumus var iegādāties tiešsaistē.

Atceries!

Droša maksājumu metode palīdzēs optimizēt pirkuma laiku un sniegs garantiju par pirkuma apmaksu.

Karšu maksājumi

- Karšu maksājumi ir viena no klientu iecienītām maksājumu metodēm internetā, kas ir drošs un pārbaudīts maksājumu veids. Mastercard ir populārākās maksājumu kartes Latvijā. Vairāk nekā 80 % no visām izsniegtajām kartēm ir tieši Mastercard.
- Karšu maksājumu pieņemšana tiešsaistes veikalā palielina kopējo uzticību vietnei, jo kartes lietotājs saņem papildu aizsardzību, atbalstot drošu jeb divu faktoru autentifikāciju, piemēram, nosūtot īsziņu ar unikālu pieslēgšanās kodu vai izmantojot internetbankas autentifikāciju.

- E-komercijā maksājumiem divu faktoru autentifikācija, piemēram, parole un E-Mobile vai SmartID, ir garantijas zīme, ka veikals ir drošs.
- Tirgotājs, pievienojoties divu faktoru autentifikācijas sistēmai maksājumiem, drīkst savā e-veikalā izvietot programmas logotipu, apliecinot, ka e-komercijas platforma ir pārbaudīta un gatava drošiem maksājumiem. Piemēram, šāda garantijas zīme ir Mastercard Identity Check logotips.

Savienojums ar internetbanku (BankLink)

- Drošs savienojums ar internetbanku ir viena no klientu visiecienītākajām maksājumu metodēm internetā, liecina Latvijas iedzīvotāju aptauja. Klients pēc preces vai pakalpojuma izvēlēšanās tiek novirzīts uz jau aizpildītu maksājuma uzdevumu savā internetbankā vai mobilajā lietotnē.
- BankLink nodrošina, ka tirgotājs var sagatavot maksājumu uzdevumu tieši pircēja internetbankā un klients var nekavējoties to apstiprināt, neveicot liekas papildu darbības.
- Viens no tirgotāja galvenajiem ieguvumiem, ka nauda kontā nonāk uzreiz.

Konsultācijas ar banku

Lai noskaidrotu, vai uzņēmuma izvēlētā maksājumu sistēma jau atbilst pieņemtajiem standartiem, ieteicams sazināties ar banku pārstāvjiem. Banka sniegs konsultācijas par attiecīgi labāko veidu, kā pasargāt sevi un savus klientus, iesakot drošas un pārbaudītas maksājumu metodes.

Atceries!

E-komercijā **divu faktoru autentifikācija maksājumiem**, piemēram, parole un E-Mobile vai SmartID, ir garantijas zīme, ka veikals ir drošs.

KĀ RĪKOTIES, JA NOTICIS KIBERUZBRUKUMS?

Ja uzņēmumā ir konstatēts uzbrukums digitālajā vidē, vispirms ir **jāslēdz tīmekļvietne**, lai nepieļautu tālāku datu noplūšanu un lietotāju inficēšanu. Vienlaikus nepieciešams nekavējoties **informēt lietotājus** par notikušo, lai tiem būtu iespēja sevi pasargāt turpmāk.

Kad tīmekļvietne ir slēgta un lietotāji informēti, **jāpiesaista drošības speciālists**, kas palīdzēs veikt situācijas analīzi, identificēs uzbrukuma apmēru un sniegs ieteikumus, kā izvairīties no uzbrukumiem nākotnē.

Atjaunot tīmekļa vietnes darbību drīkst tikai pēc tam, kad situācijas apstākļi ir noskaidroti un veikti nepieciešamie drošības pasākumi.

Četri soļi, ja noticis uzbrukums

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS.

KO SVARĪGI ATCERĒTIES?

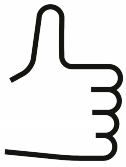
Internetveikals atrodas tā mērķim paredzētā platformā vai to ir veidojis profesionālis.

Tiek izmantotas unikālas, vismaz 14–16 simbolu garas un tikai lietotājam zināmas pieejas paroles.

Programmatūra tiek regulāri atjaunināta, vismaz reizi 3 mēnešos.

Visiem datiem ir pieejamas rezerves kopijas, kas tiek glabātas atsevišķi.

Internetveikalam ir pieslēgta droša maksājumu metode.



Nav novērotas aizdomīgas darbības vai biežas sūdzības no klientiem.

Ir veikti drošības testi.

LŪDZU, ŅEM VĒRĀ, KA ŠĪS IR INFORMATĪVAS VADLĪNIJAS, NEVIS PROFESIONĀLAS REKOMENDĀCIJAS.

PAPILDU RESURSI

DAŽĀDI

Jautājumi un atbildes par interneta maksājumu drošības prasību ieviešanu

- https://www.fktk.lv/mediju-telpa/nozares-temati/stingra-autentifikacija-maksajumiem-interneta/jautajumi-un-atbildes-par-jauno-interneta-maksajumu-drosibas-prasibu-ieviesanu/

Noteikts papildu periods, kas paredzēts stingrās autentifikācijas ieviešanai maksājumu karšu darījumiem e-komercijā

- https://www.fktk.lv/jaunumi/pazinojumi-medijiem/noteikts-papildu-periods-kas-paredzets-stingras-autentifikacijas-ieviesanai-maksajumu-karsu-darijumiem-e-komercija/

Request for input on the preparedness to meet the requirements on strong customer authentication (informācija angļu valodā)

- https://www.financelatvia.eu/wp-content/uploads/2020/01/EBA_Questionnaire_PSPs_acquiring.pdf
- https://www.financelatvia.eu/wp-content/uploads/2020/01/EBA_Questionnaire_PSPs_acquiring.pdf

Payment Card Industry pašvērtējuma anketa (informācija angļu valodā)

- https://www.pcisecuritystandards.org/pci_security/completing_self_assessment

Kā samazināt kiberriskus? (informācija angļu valodā)

- https://gcatoolkit.org/smallbusiness/

BANKU RESURSI

Citadeles bankas vebinārs "Kā nodibināt e-Uzņēmumu: no A līdz Z

- https://www.facebook.com/watch/?v=2615556711998222

Luminor: No biznesa uz e-biznesu!

- https://www.luminor.lv/lv/e-komercijas-atbalsts

SEB bankas E-akadēmija

- https://eakademija.seb.lv/#985

Uzzini, kā ērti atvērt interneta veikalu

- https://www.swedbank.lv/business/campaign/ecommerce?language=LAT&WT.mc_id=202006_ EcommerceCombiningForces_GDN_search_lv_lat