MĒNEŠA ZIŅU IZLAIDUMS NR. 08/2018

WWW.CERT.LV

AUGUSTĀ AKTUĀLI:

- Noderīgi padomi vecākiem
- Parakstīts jauns sadarbības memorands
- Kiberlaikapstākļi
- Kiberstāsti
- Apkrāpts divreiz
- Statistika – rīcība, atrodot nezināmu zibatmiņu
- Par „Yandex.Taxi" lietotnes drošību

Attēli: Pixabay.com

NODERĪGI PADOMI VECĀKIEM PAR BĒRNU DROŠĪBU INTERNETĀ

Sākoties jaunajam mācību gadam, **CERT.LV ir apkopojis noderīgus interneta resursus vecākiem par bērnu drošību internetā**. Bērni, lietojot internetu, ir pakļauti citādākiem riskiem. To nosaka viņu dabiskā ziņkāre, nevainīgums, tieksme pēc neatkarības un bailes no soda. Bērni var pieļaut kļūdas, piemēram, dokumenta vietā nejauši izdzēšot kādu programmu vai apmeklējot ļaundabīgu vietni un inficējot datoru ar vīrusu. Taču viņi to var neapzināties, vai var nepateikt, kas noticis, baidoties no soda.

Cits nopietnais drauds ir ļaunprātīgi lietotāji, kas cenšas manipulēt un apmānīt internetā citus, izmantojot viņu neuzmanību vai nezināšanu**. Bērni ir "viegls mērķis",** jo ir daudz atvērtāki un vairāk uzticas. Pat pieaugušie mēdz "uzķerties" uz krāpniecības mēģinājumiem.

Tāpat **par nopietnu problēmu ir uzskatāma aizskaroša, draudīga izturēšanās pret bērnu interneta vidē**. Apdraudējums palielinās, ja bērnam ir piekļuve e-pastam, tērzētavām (chat rooms) un/ vai sociālajiem tīkliem.

Ja esat saskārušies ar naidīgu vai neatbilstošu saturu, aicinām sazināties ar Drošāka interneta centru elektroniski vai zvanot **uz uzticības tālruni 116111.** Ja esat saskārušies ar krāpniecību internetā, ziņojiet CERT.LV uz e-pastu: cert@cert.lv vai zvanot uz tālruni +371 67085888.

NODERĪGI RESURSI:

Padomi drošākam internetam: https://cert.lv/lv/2018/02/padomi-drosakam-internetam

Sociālo tīklu drošības ceļvedis: https://drossinternets.lv/lv/materials/download/13

Mūsdienu tiešsaistes bērnu drošība: https://www.esidross.lv/2017/05/22/musdienu-tiessaistes-bernu-drosiba/

KIBERLAIKAPSTĀKĻI

				
PAKALPOJUMA PIEEJAMĪBA	**LIETU INTERNETS**	**DATU NOPLŪDE**	**ĻAUNATŪRA UN IEVAINOJAMĪBAS**	**KRĀPŠANA**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	„Yandex.Taxi" aicina neizmantot Lietuvā	Būtiski incidenti netika reģistrēti	Apkrāpt divreiz; krāpniecība Google un DHL vārdā

SEPTEMBRA OUCH!

IKMĒNEŠA INFORMĀCIJAS DROŠĪBAS BIĻETENS IKVIENAM

Biļetena tēma: CEO krāpšana jeb biznesa e-pastu kompromitēšana

Kibernoziedznieki turpina pilnveidot e-pastu krāpniecību, ko sauc arī par CEO krāpšanu vai biznesa e-pastu kompromitēšanu (CEO Fraud / BEC). Tas ir mērķtiecīgi organizēts uzbrukums, izmantojot e-pastu, lai apmānītu upuri, liekot tam veikt darbības, kuru rezultātā upuris labprātīgi šķiras no naudas vai informācijas. Vairumā gadījumu tiek mēģināts izkrāpt naudu. Šos uzbrukumus īpaši bīstamus padara tas, ka ļaundari pirms uzbrukuma veic potenciālā upura padziļinātu izpēti. Arī drošības risinājumi bieži vien ir bezspēcīgi šādu uzbrukumu priekšā, jo nav inficētu e-pastu pielikumu vai ļaundabīgu saišu, ko tehnoloģijas varētu atpazīt un nobloķēt.

Pilna raksta versija pieejama: https://cert.lv/uploads/ieteikumi/201809-OUCH-September-Latvian.pdf

PARAKSTĪTS SADARBĪBAS MEMORANDS AR UZBEKISTĀNAS IPSC

Vasarā CERT.LV veiksmīgu pārrunu rezultātā **noslēdza sadarbības memorandu ar Uzbekistānas Informācijas un sabiedrības drošības centru** (*Information and Public Security Center, IPSC*), kas pakļauts Uzbekistānas Republikas Informācijas tehnoloģiju un komunikāciju attīstības ministrijai**, par sadarbību kiberdrošības jautājumos un savstarpējo atbalstu nopietnu kiberdrošības incidentu gadījumā**. Memorands noslēgts uz 5 gadiem ar iespēju to pagarināt.

Uzbekistānas delegācija vasaras sākumā viesojās Latvijā, un vizītes ietvaros apmeklēja „Security Identification" konferenci Rīgā, kuras laikā tikās ar potenciālajiem sadarbības partneriem no Latvijas. CERT.LV arī saņēmusi uzaicinājumu no IPSC doties pieredzes apmaiņas vizītē uz Uzbekistānu.

APKRĀPT DIVREIZ – ĻAUNS JOKS VAI SKARBĀ REALITĀTE

Šodien radošums un izdoma ir viens no faktoriem, ko darba devēji meklē savos padotajos un jaunajos darbiniekos. CERT.LV pieredze rāda, ka kiberdrošība ir tā nozare, kur radošu un ar spilgtu fantāziju apveltītu prātu netrūkst – par nožēlu arī krāpnieku pusē. **Augustā CERT.LV rīcībā nonāca informācija par krāpšanas shēmu, kuras mērķis ir izvilināt naudu no jau vienreiz apkrāptiem upuriem.** Sākotnēji varētu šķist, ka tas ir kāds ļauns joks, bet realitāte ir skarba, un upuriem smiekli nenāk.

Jau **maija ziņās rakstījām par „zvanu troļļiem",** kas krievu valodā aicina Latvijas iedzīvotājus ieguldīt kriptovalūtā, solot pasakainu peļņu. CERT.LV rīcībā diemžēl ir nepilnīga informācija par patieso cietušo skaitu Latvijā, jo ne visi cietušie vēlas atzīt, ka krituši par upuri šķietami acīmredzamai krāpniecības shēmai. Taču cietušie ir, un, iespējams, ne tikai Latvijā.

Tomēr kā jau minējām, ļaundaru fantāzijai nav robežu un tapis plāns, kā „apstrādāt" jau esošos upurus. Pēc kāda nenoteikta laika ļaundari **atkārtoti no sveša numura zvana upurim, stādoties priekšā kā apdrošināšanas kompānija vai banka.** Mērķis ir iestāstīt un pārliecināt upuri, ka viņa sākotnēji **neveiksmīgie ieguldījumi ir bijuši apdrošināti**, un viņam pienākas kompensācija. Kompensācija vairākas reizes pārsniedz sākotnējo ieguldījumu – kas iedziļinoties šķiet pavisam neloģiski. Nauda bankā esot pieejama, viss kas no upura ir nepieciešams – e-pasts un rekvizīti uz kuriem summu pārskaitīt. E-pastā pēc īsa brīža tiek atsūtīts izraksts no kādas bankas Austrālijā, kurā redzama pieejamā summa, kā arī nodokļi un bankas izdevumi, kas pirms tam jāsedz, protams, upurim, lai varētu saņemt apdrošinājuma summu. **CERT.LV aicina visus, kas neveiksmīgi ieguldījuši naudu minētajā krāpnieku kriptovalūtu shēmā par to ziņot gan Valsts policijai, gan CERT.LV.** Kā arī būt uzmanīgiem un neuzķerties uz solījumiem par apdrošināšanas kompensāciju.

Par „Yandex.Taxi" lietotnes drošību

Sekojot līdzi Lietuvas Nacionālā kiberdrošības centra veiktajai izpētei, CERT.LV Latvijas Republikas Aizsardzības ministrijas uzdevumā augustā **veica neatkarīgu Krievijas kapitāla kompānijas "Yandex. Taxi" lietotnes ekspertīzi.**

Izpētes rezultātā gan CERT.LV, gan Lietuvas Nacionālā kiberdrošības centra speciālisti guva apstiprinājumu tam, ka „Yandex.Taxi" **lietotne veic saziņu ar tīkliem Krievijas Federācijā** un apmainās ar iegūtajiem datiem.

Kopumā vērtējot „Yandex.Taxi" lietotni, netika konstatēta funkcionalitāte, kas klaji un rupji pārkāptu ierastās normas. Kaut arī tiek apkopota pietiekami sensitīva informācija, piemēram, pilns uzstādīto lietotņu saraksts, lietotāja telefona numurs, Wi-Fi tīklu piekļuves punkti, informācija par apkārtnē esošiem mobilo sakaru torņiem, SMS, u.c.,- līdzīga funkcionalitāte ir simtiem citu plaši izmantotu lietotņu.

Lai arī „Yandex.Taxi" gadījums nav viennozīmīgi vērtējams kā ļaunprātīgs no tehniskā viedokļa, **jebkuru ar Krieviju saistītu programmatūru un pakalpojumu izmantošana atvieglo Krievijas Federācijas izlūkdienestiem iegūt sensitīvu informāciju.**

CERT.LV veiktās analīzes rezultātus apkopojusi Latvijas Republikas Aizsardzības ministrija un nosūtījusi tālāk izvērtēšanai Datu valsts inspekcijai un Latvijas Republikas Tieslietu ministrijai, lai noskaidrotu, vai „Yandex.Taxi" lietotnes apkopotie dati ir samērīgi un atbilstoši GDPR (Vispārīgā datu aizsardzības regula).

Kiberstāsti

• • •

Augustā CERT.LV saņēma ziņojumu no kāda interneta lietotāja, kas vēlējās pārbaudīt vai e-pasts par laimestu 950 000 GBP vērtībā no Google nav krāpniecība. Lietotājs esot arī nosūtījis atbildes e-pastā par sevi prasītos datus – adresi, tālruni, valstspiederību, vārdu un uzvārdu, un amatu. E-pastā, kas šķietami nāk no Google administrācijas, tiek apgalvots, ka lietotāja, kā uzticīga Google pakalpojuma izmantotāja, e-pasta adrese esot piedalījusies loterijā un laimējusi 950 000 GBP. CERT.LV apstiprināja, ka minētais e-pasts ir krāpnieciska rakstura un ieteica lietotājam pārtraukt jebkādu komunikāciju ar e-pasta sūtītāju. Kā arī norādīja, ka vēlāk visticamāk varētu tiktu atsūtīta vēstule ar lūgumu samaksāt nodokli, pārskaitījuma izdevumus, loterijas vai valsts nodokli, lai varētu saņemt laimestu. Rezultātā tiktu izkrāptas lielas naudas summas un, protams, nekāds laimests tā arī netiktu saņemts.

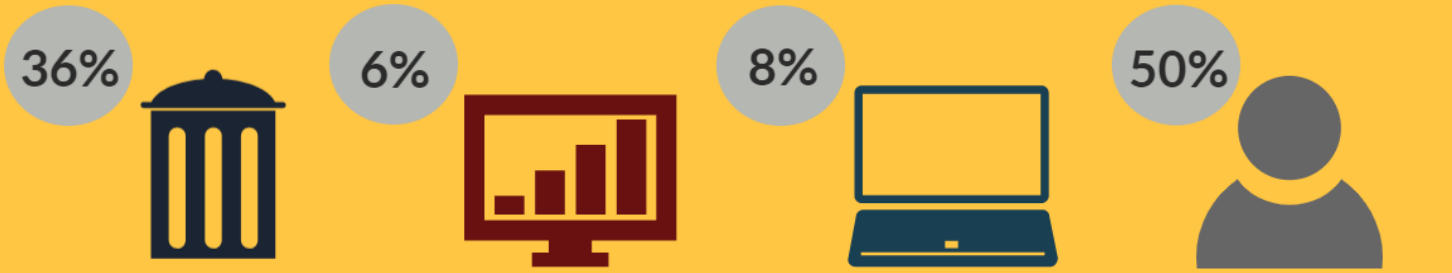
• • •

Mēneša beigās CERT.LV saņēma ziņojuma no kāda interneta lietotāja, kurš, apmeklējot ārzemju pieaugušo vietnes, nejauši uzdūries reklāmām, kas ved uz ārvalstu lapām ar bērnu pornogrāfiju. Lietotājs nepalika vienaldzīgs un saites uz nelegālajām lapām nodeva CERT.LV rīcībā. Saņemtā informācija tālāk nodota tiesībsargājošajām institūcijām. CERT.LV aicina ikvienu, kurš saskāries ar līdzīgiem materiāliem vai vietnēm, nestāvēt malā, bet ziņot Valsts policijai vai Drošāka interneta centram.

• • •

Vasaras noslēgumā kāds ziņotājs informēja CERT.LV par aizdomīgu e-pastu uzņēmuma DHL vārdā. E-pasts tika saņemts angļu valodā un vizuālais noformējums t.sk. valodas stils un paraksts tiešām atgādināja oriģinālo DHL tēlu. E-pastā, saistībā ar pēdējā laika pārpratumiem paku piegādē, lūgts vēlreiz apstiprināt sūtījuma gala adresi. Pretējā gadījumā tiek brīdināts, ka sūtījums var kavēties vai arī netikt piegādāts. E-pastā norādīta saite, kurā jāveic gala adreses atkārtota verifikācija. CERT.LV informēja lietotāju, ka tas ir krāpniecisks e-pasts, kur dotā saite ved uz DHL vizuāli līdzīgu vietni, lai izkrāptu lietotāja paroles un citus datus. Tāpat CERT.LV sazinājās ar lapas uzturētāju un panāca krāpnieciskās vietnes slēgšanu.

STATISTIKA: CILVĒKU RĪCĪBA, ATRODOT NEZINĀMU ZIBATMIŅU*



*CERT.LV rīkotās aptaujas rezultāti valsts un pašvaldības iestādēs (2017). Aptaujā piedalījās 664 respondenti.

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

2018.gada 9.oktobrī CERT.LV un ISACA Latvijas nodaļa sadarbībā ar LMT un dots. rīko starptautisku kiberdrošības jautājumiem veltītu konferenci "Kiberšahs 2018". Konference tiek daļēji finansēta no CEF projekta "Improving Cyber Security Capacities in Latvia" (INEA/CEF/ICT/A2017/1528784).

INFORMĀCIJA PAR „KIBERŠAHS 2018" PROGRAMMU, RUNĀTĀJIEM UN REĢISTRĒŠANOS PIEEJAMA ŠEIT:
https://cert.lv/lv/2018/09/kiberdrosibas-konference-kibersahs-2018

ADRESE: RAIŅA BULVĀRIS 29, RĪGA, LV-1459, LATVIJA;
TELEFONS: +371 67085888;
E-PASTS: ZIŅOT PAR INCIDENTU: CERT@CERT.LV / SABIEDRISKĀS ATTIECĪBAS: PRESE@CERT.LV
VIETNE: WWW.CERT.LV