Mēneša ziņu izlaidums Nr. 07/2018

WWW.CERT.LV

Jūlijā aktuāli:

- LinkedIn datu noplūde par sevi atgādina
- Dārgās ārzemju sarunas
- Kiberlaikapstākļi
- Kiberstāsti
- Statistika – piekļuve interneta resursiem
- Pētījums – atbildīga ievainojamību atklāšana
- Google Chrome turpmāk brīdinās par nedrošām vietnēm

Attēli: Pixabay.com

LinkedIn datu noplūde (2016) par sevi atgādina

Jūlijā aktīvi izplatījās e-pasti, kuros **krāpnieki apgalvoja, ka ir uzlauzuši un inficējuši upura iekārtu**, ierakstījuši pornogrāfiska rakstura video un **to izsūtīs visiem upura kontaktiem**, ja netiks samaksāta izpirkuma maksa. Draudu patiesumu krāpnieki cenšas pierādīt, **e-pastā upurim norādot arī viņa paroli.**

Vienīgais patiesais šajā sarakstē ir parole. To uzbrucēji ieguvuši kādā no publiski pieejamajām datu noplūdēm, piemēram, 2016. gadā tika nopludināti 164 miljonu LinkedIn lietotāju dati. Nekāda vīrusa un video nav.

Ko darīt, ja saņem šādu e-pastu? Neko. Krāpniekiem **nevajag maksāt, un nevajag mēģināt** ar viņiem komunicēt. Vienīgais, ko vajag darīt - ja joprojām lietojat e-pastā norādīto paroli, to steidzami nomainīt, un nodrošināt, lai katrā tīmekļa vietnē, kas jums ir svarīga, tiktu izmantota unikāla un droša parole un, ja iespējams, noteikti izmantojiet arī divu faktoru autentifikāciju!

Sīkāka informācija par krāpšanu pieejama šeit: https://cert.lv/lv/2018/07/krapnieki-kas-apgalvo-ka-zina-tavu-paroli

Kiberlaikapstākļi

				
Pakalpojuma pieejamība	**Lietu internets**	**Datu noplūde**	**Ļaunatūra un ievainojamības**	**Krāpšana**
Būtiski incidenti netika reģistrēti	Būtiski incidenti netika reģistrēti	LinkedIn datu noplūde (2016) par sevi atgādina	Būtiski incidenti netika reģistrēti	Ārzemju telefona zvani, Facebook - „man izlādējās telefons", „Es zinu tavu paroli"

Augusta OUCH!

Ikmēneša informācijas drošības biļetens ikvienam

Biļetena tēma: "Viedās mājas ierīces"

Vēsturiski internetam jūsu mājā varēja pieslēgties tikai dažas ierīces – portatīvais dators, tālrunis, spēļu konsole. Taču šodien internetam var pieslēgties daudz un dažādas ierīces, sākot no spuldzītēm, TV skaļruņiem, durvju atslēgām līdz pat automašīnai. Drīzumā tīklam varēs pieslēgties vairums ierīču. Šādas internetam pieslēgtas ierīces bieži dēvē arī par Lietu internetu (Internet of Things (IoT)) vai viedajām mājas ierīcēm. Kaut arī šādas ierīces, protams, piedāvā virkni ērtību, tomēr tās slēpj sevī arī unikālus apdraudējumus.

Pilna raksta versija pieejama: https://cert.lv/uploads/ieteikumi/201808-OUCH-Augusts.pdf

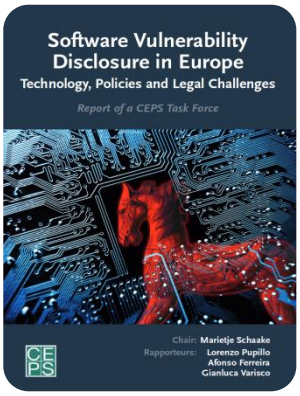
DĀRGĀS ĀRZEMJU SARUNAS

Daudzi Latvijas iedzīvotāji saņēma ārzemju zvanus no **nepazīstamiem numuriem no Baltkrievijas, Samoa un citām valstīm**. Zvani bija īsi, lai panāktu atzvanīšanu. Atzvanot lietotājs tiktu savienots ar paaugstinātas maksas numuru, un zvana apmaksa tiktu pieskaitīta lietotāja telefona rēķinam.

Lai arī mobilo sakaru operatori regulāri bloķē telefona numurus, no kuriem tiek veikti krāpnieciski zvani, arī **pašiem lietotājiem jābūt modriem** - sveši numuri, īpaši ārvalstu, jāignorē un jāinformē savs operators.

PĒTĪJUMS - ATBILDĪGA IEVAINOJAMĪBU ATKLĀŠANA EIROPĀ

Centre for European Policy Studies (CEPS) ir viena no vadošajām domnīcām Eiropas Savienībā - ar plašu sadarbības partneru tīklu visā pasaulē un attīstītu pētniecības funkciju. 2017. gada septembrī **CEPS pakļautībā tika izveidota īpaša darba grupa**, kurā piedalījās gan nozares eksperti, gan pārstāvji no ES un citām starptautiskām un sabiedriskām institūcijām. To vidū bija aicināts arī CERT.LV pārstāvis. Darba grupas kopīgo pārrunu un diskusiju rezultātā **tapa ziņojums, kurā apkopoti vērtīgi ieteikumi un secinājumi, kas domāti nākotnē virzītas vienojošas Eiropas politikas izstrādei** par atbildīgu ievainojamību atklāšanu.



Ziņojumā sniegts pārskats arī par labajiem prakses piemēriem atsevišķās Eiropas valstīs, ASV un Japānā. To vidū apskatīta situācija arī Latvijā.

VAIRĀK INFORMĀCIJAS:
Pētījuma digitālā versija pieejama šeit: https://www.ceps.eu/system/files/CEPS%20TFRonSVD%20with%20cover_0.pdf

Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges:
https://www.ceps.eu/publications/software-vulnerability-disclosure-europe-technology-policies-and-legal-challenges

GOOGLE CHROME TURPMĀK BRĪDINĀS PAR NEDROŠĀM VIETNĒM

Šā gada 24. jūlijā tika izlaista **interneta pārlūka *Chrome* jaunākā versija 68**, un līdz ar tās iznākšanu **Google Chrome turpmāk kā nedrošas skaidri izcels tās vietnes, kuras neizmanto HTTPS protokolu**.

Tas nozīmē, ka interneta lietotāji, nokļūstot mājaslapā, kur joprojām tiek izmantots nedrošais HTTP protokols, **par to tiks brīdināti no Google Chrome puses ar paziņojumu „Not Secure" jeb „Nav droši".** Šis brīdinājums nozīmē, ka vietnei nav SSL sertifikāta, lai varētu šifrēt datu plūsmu starp lietotāja datoru un mājaslapas serveri. **Īpaši jāpievērš uzmanība tām vietnēm, kurās nepieciešams ievadīt sensitīvus datus, piemēram, lietotājvārdu, paroli, kredītkartes informāciju utt.**

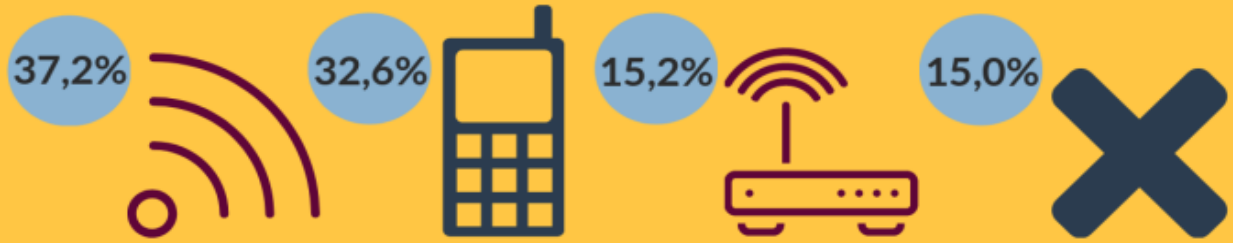
Tādēļ tiem interneta lietotājiem, kuri ikdienā izmanto Chrome pārlūku, būtu ieteicams pāriet uz jauno Chrome 68 versiju, kā arī pievērst uzmanību uznirstošajiem brīdinājumiem.

VAIRĀK INFORMĀCIJAS:
A secure web is here to stay: https://security.googleblog.com/2018/02/a-secure-web-is-here-to-stay.html

TUVĀKO PLĀNOTO PASĀKUMU KALENDĀRS

09. **OKTOBRIS** - Kiberdrošības konference "Kiberšahs 2018"

Statistika: piekļuve interneta resursiem no viedierīcēm*



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

Kiberstāsti

• • •

Iepriekšējās Jūnija aktualitāšu ziņās CERT.LV prognozēja, ka drīzumā arī Latviju varētu sasniegt *Office 365* e-pastu pikšķerēšanas kampaņa. Ilgi nebija jāgaida, jo jau jūlijā tika saņemts pirmais ziņojums par krāpnieku aktivitātēm arī Latvijā. Par krāpniecību ziņoja kāds Latvijas uzņēmums, kura darbinieki saņēmuši aizdomīgus e-pastus it kā no *Office 365* komandas. E-pastā (angļu valodā) tiek brīdināts, ka, ja netiks apstiprināta lietotāja identitāte, e-pasta darbība tiks apturēta. Lietotāja identitātes apstiprināšanai saņēmējam norādīta saite, kur tālāk tiek lūgts ievadīt e-pasta lietotāja datus. Daži no uzņēmuma darbiniekiem datus norādīja, taču uzņēmums laikus attapās, un visiem iesaistītajiem tika operatīvi nomainītas paroles. Uzņēmums zaudējumus necieta. Tā kā uzņēmuma pārstāvis bija iepazinies ar brīdinājumu un kampaņas aprakstu CERT.LV mājaslapā, tad par notikušo ziņoja arī CERT.LV, kur saņēma papildu ieteikumus pārbaudīt, vai nav novērojamas konfigurācijas izmaiņas e-pasta pāradresācijā un filtros, kā arī ieteikumu uzlabot e-pastu SPAM filtru.

• • •

Jūlija vidū tika saņemti vairāki ziņojumi no privātpersonām par uzlauztiem *Facebook* lietotāju kontiem un krāpniecisku ziņu izsūtīšanu lietotāju kontaktu lokam. Krāpnieku mērķis ir panākt, ka upuris jeb uzlauztā profila draugs / paziņa no sava privātā telefona uz maksas numuru nosūta kodu. Ļaundaris izliekas par uzlauztā profila īpašnieku, un sociālajā tīklā iesaistās sarunās ar īpašnieka draugiem / paziņām (iespējams tikai ar tiem, kam profilā norādīts tālruņa numurs). Cik zināms, tad visas sarunas sākas ar lūgumu izpalīdzēt, jo telefonam esot nosēdusies baterija, bet steidzami nepieciešams saņemt SMS. Sarakste šķiet īsta, jo ļaundari, piemēram, upuri uzrunā, izmantojot iesauku vai krievu valodā – vārda īso formu. Sarunā figurē tādi tel. nr. kā 1819 vai 1896. Upurim nodarītā skāde ir 50 līdz 80 EUR klāt mobilo pakalpojumu rēķinam. CERT.LV šādos gadījumos iesaka noteikti sazināties ar savu telekomunikācijas operatoru, kā arī ziņot par krāpšanas gadījumu Ekonomisko noziegumu apkarošanas pārvaldei (tel. 67208663). Tāpat *Facebook* profila īpašniekiem būtu ieteicams ieviesiet divu faktoru autentifikāciju.

• • •

Mēneša noslēgumā CERT.LV saņēma lūgumu pēc palīdzības, saistībā ar kādas lietotājas viltus profilu Facebook. Lietotāja nejauši konstatējusi, ka kāds viņas vārdā un viņai nezināmu iemeslu dēļ ir izveidojis viņas viltus profilu. CERT.LV šādi ziņojumi periodiski ir saņemti arī iepriekš, kaut arī neietilpst CERT.LV jurisdikcijā, jo saistīti ar saturu. CERT.LV kā vienu no iedarbīgākajām metodēm šādos gadījumos iesaka ziņošanu pašam Facebook. Vislabāk, ja par notikušo ziņo īstā profila īpašnieks, taču gadījumos, ja cilvēks Facebook nemaz nelieto, ziņot var arī kāds upura draugs, kas izmanto šo sociālo tīklu. Ziņot iespējams, atverot viltus profilu un labajā augšējā stūrī izvēloties daudzpunktes ikonu. Pēc tam jāizvēlas „Give feedback or report this profile" un tad attiecīgi nākamais solis ir izvēlēties opciju „Pretending to Be Someone".

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