Interneta lietotājiem bez maksas pieejama lietotne kiberkrāpnieku atvairīšanai

Rūpējoties par Latvijas kibertelpas drošību, kiberincidentu novēršanas institūcija CERT.LV piedāvā plašu ar kiberdrošību saistītu pakalpojumu klāstu, tostarp DNS ugunsmūri – aktīvās aizsardzības bezmaksas rīku individuālu lietotāju un organizāciju pasargāšanai no aktuālajiem kiberapdraudējumiem Latvijas kibertelpā, piemēram, viltus banku lapas, krāpnieciskas tirdzniecības platformas, vīrusus izplatošas vietnes u. c. Lai mudinātu sabiedrību vairāk rūpēties par savu digitālo drošību pirmssvētku iepirkšanās laikā, CERT.LV aicina ikvienu interneta lietotāju sākt lietot DNS ugunsmūri.

Kā norāda CERT.LV, lai gan kopējā situācija ir stabila, tomēr, ņemot vērā pašreizējo ģeopolitisko situāciju, apdraudējuma līmenis Latvijas kibertelpā joprojām vērtējams kā augsts. Visbiežāk kiberuzbrukumi tiek veikti ar mērķi iegūt lietotāju piekļuves datus sistēmām, platformām un iekārtām, lai tālāk iegūtu kontroli pār lietotāja kontiem un nozagtu finanšu līdzekļus. Latvijā regulāri notiek kampaņveidīgas krāpnieciskās aktivitātes – tiek izplatītas gan viltus vietnes, kas imitē banku un piegāžu uzņēmumu mājaslapas, gan sociālo mediju un e-pasta platformas, lai tālāk izkrāptu lietotāju piekļuves datus.

Aktīvās aizsardzības pakalpojums DNS ugunsmūris, kuru izveidoja un uztur CERT.LV sadarbībā ar augstākā līmeņa domēna .lv reģistra uzturētāju (NIC), ik dienu jau piecus gadus efektīvi un bez maksas pasargā ikvienu interneta lietotāju Latvijā no tieši Latvijā aktuālajām krāpnieciskās kampaņās izmantotām ļaundabīgām saitēm, vietnēm un kaitīga satura.

Lai veicinātu pakalpojuma lietošanu un padarītu to iedzīvotājiem viegli un ērti izmantojamu, CERT.LV šoruden pirmo reizi piedāvā DNS ugunsmūra lietotni, kas ērti lejuplādējama un aktivizējama mobilajās iekārtās Android un iOS lietotājiem. DNS ugunsmūra lietotne ne tikai pasargās no nevēlamu saišu apmeklēšanas, bet arī neļaus saņemt telefonzvanus, kurus CERT.LV būs identificējusi kā krāpnieciskus.

“Lai gan lielai daļai iedzīvotāju kiberaizsardzību vispirms nodrošina izvēlētais interneta pakalpojuma sniedzējs, kā papildu aizsardzību ar plašāku funkcionalitāti mēs rekomendējam iedzīvotājiem savās mobilajās iekārtās uzstādīt arī DNS ugunsmūra lietotni. Biežākie apdraudējumi, no kā lietotājus pasargā DNS ugunsmūris, ir pikšķerēšanas uzbrukumi ar mērķi izvilināt piekļuves datus darba e-pastam vai citiem resursiem, lai tālāk varētu organizēt jau daudz personalizētākus un sarežģītākus uzbrukumus. Vienas krāpniecības kampaņas ietvaros var būt izveidoti pat vairāki desmiti saišu ar līdzīgu vizuālo noformējumu un saturu, tāpēc ir svarīgi laikus šīs saites identificēt un ievietot DNS ugunsmūrī,” skaidro CERT.LV vadītāja Baiba Kaškina.

Pērn pētījumu centra SKDS veiktā iedzīvotāju aptauja rāda, ka 23% no 1005 respondentiem vismaz reizi dzīvē ir cietuši kiberincidentā. 18% gadījumu tas noticis mājās, bet 11% – darbavietā. No vismaz vienā kiberincidentā cietušajiem 68% cieta zaudējumus, no kuriem 25% bija finansiāla rakstura, 20% zaudēja piekļuvi savam e-pastam vai sociālo tīklu kontiem, bet 23% piedzīvoja emocionāla rakstura zaudējumus – stresu, bailes, apkaunojumu.

Kā skaidro CERT.LV, kiberkrāpnieki īpaši aktīvi kļūst tieši pirmssvētku periodā, kad iedzīvotāju modrības līmenis krītas un internetā tiek masveidā iegādātas svētku dāvanas un aktīvi izmantoti piegāžu uzņēmumu pakalpojumi. Noteiktos periodos katru gadu pastiprināta krāpnieku uzmanība tiek

pievērsta arī uzņēmumu un organizāciju grāmatvežiem, nosūtot viltus paziņojumus par it kā laikus neapmaksātu rēķinu vai nodokļa parādiem. Tāpat pieaudzis arī tādu uzbrukumu skaits, kur tiek izmantoti mākslīgā intelekta risinājumi ticamākai ziņojumu sagatavošanai un nosūtīšanai, kā arī tiek aktīvi īstenotas krāpniecības ar viltotiem zvanītāju identifikatoriem. Diemžēl arī Latvijā šādi gadījumi nav retums.

Par DNS ugunsmūri

CERT.LV ik dienu novēro dažādas krāpnieciskās kampaņas un operatīvi ievieto šo kampaņu indikatorus ugunsmūrī, lai tā lietotājus pasargātu no identificētajiem apdraudējumiem, piemēram, viltus banku vietnēm. DNS ugunsmūrī katru dienu tiek operatīvi ievietotas arī iedzīvotāju ziņotās un pamanītās krāpnieciskās saites.

DNS ugunsmūri var izmantot ikviens Latvijas iedzīvotājs, tostarp Latvijas iestādes un uzņēmumi. Pakalpojuma uzstādīšanai ir izveidotas soli pa solim pamācības populārākajām operētājsistēmām, kā arī mobilajiem telefoniem ir izveidota lietotne. DNS ugunsmūri var uzstādīt gan mobilajos telefonos un datoros, gan maršrutētājos.

DNS ugunsmūra pakalpojumam ir izveidota sava atsevišķa tīmekļvietne, kur publicēts pakalpojuma apraksts un instrukcijas, kā arī lapā var pārliecināties, vai jūsu uzstādītais DNS ugusnmūris jūsu iekārtā strādā un ir aktīvs.

DNS ugunsmūris tīmekļa vietne: https://dnsmuris.lv

Pēdējo divu gadu laikā pakalpojuma lietošana pieaugusi 5 reizes. Ik mēnesi DNS ugunsmūris apstrādā vidēji 1 milj. pieprasījumu, dienā bloķējot 8000 mēģinājumu atvērt krāpnieciskas saites. Pēdējo 2 nedēļu laikā no populārās WhatsApp krāpšanas lietotāji pasargāti 8236 reizes, nogādājot tos drošā piezemēšanās vietnē.

Par CERT.LV CERT.LV ir kiberincidentu novēršanas institūcija Latvijā, kas dibināta 2006. gadā. Tā ir „Latvijas Universitātes Matemātikas un informātikas institūta" (LU MII) struktūrvienība, kas darbojas Latvijas Republikas Aizsardzības ministrijas pakļautībā Nacionālās kiberdrošības likuma ietvaros. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā.

DNS ugunsmūra pakalpojumu nodrošina un uztur CERT.LV sadarbībā ar NIC, LU MII un Nacionālo kiberdrošības centru. Informatīvi DNS ugunsmūra kampaņu un ideju atbalsta Valsts policija, Patērētāju tiesību aizsardzības centrs, Finanšu nozares asociācija un Latvijas Pasts.