Šī lapa izdrukāta no DELFI portāla
Adrese: http://tehnika.delfi.lv/archive/print.php?id=38425767

CERT.lv darbības pirmajos divos mēnešos izmeklējis 1500 hakeru uzbrukumus

Foto: stock.xchng

LETA
10. maijs 2011 08:33

Savas darbības pirmajos divos mēnešos, februārī un martā, jaunā Informācijas tehnoloģiju drošības incidentu novēršanas institūcija jeb CERT.lv kopumā izmeklējusi 1500 hakeru uzbrukumus un citus incidentus, kas apdraud informācijas sistēmu drošību, intervijā biznesa portālam "Nozare.lv" teica CERT.lv vadītāja Baiba Kaškina.

"Februārī kopā esam apstrādājuši aptuveni 350 incidentus, martā - 1150. Atšķirība ir tik liela tāpēc, ka ņemam klāt uzraudzībā jaunus tīklus un paplašinām sadarbību ar interneta pakalpojumu sniedzējiem," teica Kaškina. Viņa paskaidroja, ka par daļu incidentu organizācija uzzina no avotiem, kas automātiski ziņo par starpgadījumiem, bet ir arī informācija no iestādēm un privātpersonām.

CERT.lv reakcija uz saņemtajām ziņām ir bijusi dažāda, jo ne visi starpgadījumi ir tādi, kas nekavējoties apdraud sistēmas un tajās glabātos datus.

"Ko esam darījuši? To, ko nu kurš incidenta veids pieprasa - vai nu tikai nodot tālāk informāciju, vai nu pieprasīt pārtraukt incidentu un sekot līdzi, ka tas ir izdarīts, vai palīdzēt meklēt vainīgos, sadarbojoties ar CERT-tipa komandām citās valstīs, vai palīdzēt atjaunot datus," stāstīja Kaškina.

Kaškina norādīja, ka CERT.lv ir ierobežoti naudas un cilvēku resursi: finansējums šī gada 11 mēnešiem ir 88 000 latu.

"Komandā ir desmit cilvēku, bet uz pilnu slodzi strādā četri vai pieci darbinieki. Ir iespēja piesaistīt gan operētājsistēmas "Linux" speciālistus, gan ("Microsoft") "Windows", gan tīklu speciālistus un juristus. Ir visas kompetences, bet pilnā mērā no esošā budžeta šiem cilvēkiem nevaram samaksāt. Tas ir labs kompromiss," Kaškina sacīja.

Kā izriet no internetā pieejamas informācijas par informācijas tehnoloģiju (IT) apdraudējumu veidiem, tie iedalāmi dažādās bīstamības pakāpēs. Var būt publiskota informācija, ka kāda sistēma ir teorētiski "uzlaužama" (tā sauktais "exploit" apraksts). Ir mānīšanas un krāpšanas centieni, uz kuriem upuris var "iekrist" vai arī tos ignorēt. Beidzot ir aktīvi hakeru pasākumi, ar tehniskiem līdzekļiem cenšoties pārvarēt kādas IT sistēmas aizsardzību.

Kaškina stāstīja, ka CERT.lv prioritāte ir mazināt tā saukto robottīklu izplatību, īpaši, ja Latvijas IT sistēmās ieperinās šo tīklu "komandieri". Tie ir serveri, kas uztur programmatūru, ar kuru var saskaņot un iedarbināt tūkstošiem "zombētu" datoru, kas veic kaitīgu darbību. "Robottīkli" (arī "botneti") apzīmē datoru kopas, kur katrs atsevišķais dators ar īpašu, slepeni ieperinātu programmatūru tiek vadīts no ārpuses un nav vairs sava saimnieka vai sistēmadministratora pilnīgā kontrolē. Šādus datorus apzīmē par "zombētiem" vai "zombijiem".

""Botneti" (robottīkli) ir liela problēma, ar kuru ir jācīnās. Viņi ir visur, privātpersonu datoros, uzņēmumos, arī valsts iestādēs. Neviens sektors nav pasargāts. Tiklīdz nav atjaunota vīrusu aizsardzība, ir izredzes nonākt vienā vai pat vairākos "zombiju" tīklos. Nav teikts, ka tie katru dienu darbojas. "Saimniekam" pietiek zināt, ka viņam ir 5000

datoru. To pakalpojumus viņš var pārdot, tos var izmantot surogātpasta sūtīšanai, kas nekaitē zombēšanas upurim, bet noslogo sakaru kanālus," Kaškina teica.

CERT.lv vadītāja teica, ka iestāde neraugās tikai uz vienu lielāko iespējamo apdraudējumu, kā zinātniskās fantastikas filmās, kur hakeri sagrauj ūdens piegādi, telekomunikācijas vai gaisa satiksmes vadību.

"Murgu scenārijus var izdomāt daudz un dažādus. Lielais vairums incidentu ir piederība robottīkliem, dažādu vīrusu sūtīšana. Bet par to neviens naktīs murgus neredz, tā ir ikdiena. Tad ir tādas lietas, kas ir nepatīkamas un no kurām ātri jātiek vaļā, un tās ir "phishing" jeb pikšķerēšanas lapas. Tie ir pikšķerēšanas mēģinājumi pret Latvijas organizācijām. Ja tādas lietas notiek, tad mēs nakts vidū ceļamies, lai tās novērstu," Kaškina stāstīja.

Pikšķerēšana ir interneta lietotāju mānīšana ar viltus e-pastiem un mājaslapām it kā no ticamiem avotiem. Pikšķerēšanā bieži izmanto kādas bankas vai iestādes mājaslapas vai e-pasta "vēstuļpapīra" dublikātu. Tajās prasa upurim ievadīt savas bankas konta vai kredītkartes paroles, prezentējot maldinošu stāstu par klientu saraksta vai datubāzes atjaunošanu vai arī it kā veicot aptauju.

CERT.lv sācis darboties šī gada 1.februārī, apvienojot Latvijas Universitātes Matemātikas un informātikas institūta datu drošības incidentu reaģēšanas grupu CERT.NIC.lv (visu šādu grupu starptautiskais nosaukums ņemts no "Computer Emergency Reaction Team") un Datoru drošības incidentu reaģēšanas vienību (DDIRV), kas darbojās pērn ar Latvijas Valsts radio un televīzijas centru (LVRTC) apvienotās un likvidētās Valsts informācijas tīklu aģentūras (VITA) paspārnē.

Ieteikt 0 Recommend