Iknedēļas ziņas
Sagatavotas 26.11.2015.
Numurs 2015/16

Kontakti: prese@cert.lv
Tālrunis: 67085888

Bīstams sertifikāts Dell datoros kompromitē šifrētus HTTPS savienojumus

Nedēļas sākumā parādījās ziņa, ka kompānijas Dell portatīvie datori nāk ar iepriekš uzinstalētu "root" sertifikātu un attiecīgu privāto atslēgu, kas apdraud šifrēto savienojumu drošību. Šis apdraudējums attiecas uz Dell lietotājiem, kas izmanto Windows operētājsistēmu un Internet Explorer, Edge vai Chrome pārlūkprogrammas.

Sīkāk par apdraudēju un kā to novērst: https://blog.hboeck.de/archives/876-Superfish-2.0-Dangerous-Certificate-on-Dell-Laptops-breaks-encrypted-HTTPS-Connections.html

CERT.LV pārstāvji piedalās NATO "Cyber Coalition 2015" treniņmācībās

No 16.-20. novembrim norisinājās ikgadējās NATO "Cyber Coalition 2015" treniņmācības, kurās piedalījās ap 600 kiberdrošības ekspertu no NATO un tās partneru dalībvalstīm, tai skaitā arī Latvijas pārstāvji no CERT.LV, LR Zemessardzes kiberaizsardzības vienības un nacionālajiem bruņotajiem spēkiem. Mācību mērķis bija pārbaudīt alianses un partneru spēju pārvarēt virkni sarežģītu drošības izaicinājumu. Izmantojot kontrolētu virtuālo vidi, visiem dalībniekiem tika sniegta informācija ar sižetiem, kas ietvēra tādus draudus kā, piemēram, mobilo ļaunatūru un spiegprogrammatūru vai konkrētu tīklu uzlaušanu.

Pateicoties veiksmīgai sadarbībai starp valstīm, dotie uzdevumi tika veiksmīgi atrisināti.

Vīrusu izplatība e-pasta pielikumos turpinās

Šoreiz inficētais e-pasta pielikums izsūtīts kurjerservisa DHL vārdā. Pielikumā esošais izpildāmais .exe fails saturēja datorvīrusu, kas veido savienojumus ar serveriem. Pēc izpildīšanas tas nodrošina savu turpmāko palaišanu, pievienojot reģistros attiecīgu RUN atslēgu.
Fails satur arī Remote Desktop savienojumam raksturīgas pazīmes un, iespējams, var tikt izmantots attālinātai piekļuvei pie inficētā datora.