OUCH! I 2020.gada aprīlis

OUCH!

SANS SECURITY AWARENESS

Ikmēneša informācijas drošības izdevums

Kāpēc ir svarīgi veikt atjauninājumus?

Ieskatam

Par spīti šodienas aktuālajiem notikumiem pasaulē, kiberuzbrucēji nesnauž, tie nepārtraukti meklē un atrod jaunas ievainojamības un nepilnības programmatūrās, kuras sabiedrība lieto katru dienu. Tā var būt programmatūra, ko izmantojam savos klēpjdatoros, aplikācijas viedtālruņos, vai pat programmatūra tādās iekārtās kā zīdaiņa pieskatīšanas monitors, kā arī jebkurās citās viedierīcēs jūsu mājā. Ļaundari visā pasaulē mēģina atrast un izmantot šo programmatūru vājās vietas, lai attālināti piekļūtu ierīcēm un tajās esošai informācijai. Turpretī programmatūru ražotāji un ierīču izplatītāji nepārtraukti strādā pie šo nepilnību labojumiem jeb izstrādā tā sauktos ielāpus, kurus iekārtās varam uzstādīt, veicot programmatūras atjauninājumus. Tāpēc viens no labākajiem veidiem, kā jūs varat sevi pasargāt, ir nodrošināt, lai visām jūsu izmantotajām iekārtām tiktu veikti jaunākie atjauninājumi, tā labāk pasargājot savas iekārtas un apgrūtinot kiberuzbrucēju ielaušanos.

Kā strādā atjauninājumi?

Der atcerēties, ka neviena aplikācija vai programmatūra nav ideāla – tām visām pastāv ievainojamību risks. Taču tiklīdz tiek atklāta programmatūras ievainojamība, ikviens ražotājs izstrādā programmatūras atjauninājumu (ko dēvē arī par ielāpu). Mūsdienās lielākajai daļai programmatūru un iekārtu ir jau rūpnieciski iestrādāts mehānisms, kurš, izmantojot interneta savienojumu, ļauj iekārtai vai programmatūrai automātiski savienoties ar ražotāja serveri un iegūt jaunākos atjauninājumus. Šis atjauninājums, kas būtībā nav nekas vairāk kā neliela programma, parasti veic pati instalēšanās darbus un novērš ievainojamību. Biežāk sastopamie programmatūru atjaunināšanas piemēri ir iekārtu operētājsistēmas, kā piemēram, Microsoft Windows vai OSX klēpjdatoros vai Android vai iOS viedtālruņos. Taču tas nav viss. Diemžēl bieži tiek piemirsts, ka ir jāatjaunina arī pašas programmas, kas darbojas jūsu ierīcēs, kā piemēram, klēpjdatora tīmekļa pārlūkprogramma, teksta apstrādes programma, ziņojumapmaiņas programmatūra vai tālruņa mobilās lietotnes (īpaši sociālo mediju lietotnes).

Tāpēc ikreiz, kad iegādājaties jaunu datorprogrammu vai jaunu mobilo lietotni, vispirms pārbaudiet, vai programmatūras piegādātājs aktīvi atjaunina šo programmu vai ierīci. Jo ilgāk tiek lietotas datorprogrammatūras bez atjauninājumiem, jo lielākas ir to vājās vietas, kuras kibernoziedznieki var izmantot. Tāpēc daudzi piegādātāji, kā piemēram, Microsoft, automātiski publicē jaunatklātos ielāpus vismaz reizi mēnesī.

Visbeidzot, ja vairs neizmantojat noteiktu datorprogrammu, programmatūru vai mobilo lietotni, noņemiet to no sistēmas. Jo mazāk programmatūru ir jāatjaunina, jo pasargātāki esat.

Atjaunināšana

Pastāv divi sistēmas atjaunināšanas veidi:

Automātiski — ja ierīce, operētājsistēma, programma vai mobilā lietotne konstatē, ka tiklīdz piegādātājs ir publicējis atjauninājumu, tā automātiski lejupielādē un instalē to. Automātisko atjauninājumu priekšrocība ir tā, ka jums nekas nav jādara. Programmatūra nodrošina, ka izmantotās tehnoloģijas ir aktuālas. Taču automātiskajai atjaunināšanai var būt arī trūkumi – atjaunināta programma var izraisīt problēmu, kuras rezultātā var tikt izmainīta kāda funkcionalitāte vai zaudēti dati. Tas reti atgadās ar personiskajām ierīcēm, biežāk var gadīties komplicētākām darba vidēm, kā, piemēram, lielām korporācijām – tieši tāpēc šāda izmēra organizācijas parasti izvēlas manuālu atjaunināšanu, lai varētu pārliecināties par atjauninājumu ietekmi uz sistēmām testa vidē pirms to uzstādīšanas.

Manuāli — ja ir pieejams ierīces, operētājsistēmas, programmas vai mobilās lietotnes atjauninājums, parasti jums par to paziņo, bet jums pašam tas ir jālejupielādē un jāinstalē manuāli. Šādi jūs varat labāk kontrolēt, kādi atjauninājumi un kad ir instalēti. Manuālo atjauninājumu trūkums ir tas, ka sistēmas atjaunināšana var aizņemt daudz ilgāku laiku vai jūs varat gluži vienkārši aizmirst instalēt tos.

Noslēgumā

Fiziskām personām, ģimenēm un maziem uzņēmumiem ir ļoti ieteicams iespējot un izmantot automātisko atjaunināšanu visās ierīcēs, kuras izmantojat. Tas nodrošinās, ka visām jūsu izmantotajām tehnoloģijām, sākot ar viedtālruni un klēpjdatoru un beidzot ar zīdaiņa pieskatīšanas monitoru, apkures sistēmu un durvju slēdzenēm, ir jaunākā programmatūra. Atjauninātas ierīces un programmatūras padara ļaundaru dzīvi grūtāku, uzbrukt jūsu iekārtām nav tik vienkārši. Automātiskās atjaunināšanas aktivizēšana ir viens no vienkāršākajiem un efektīvākajiem veidiem, kā sevi pasargāt un droši izmantot mūsdienu tehnoloģijas.

Viesredaktors

Don C.Weber ir informācijas tehnoloģiju drošības eksperts ar plašu pieredzi kopš 2002. gada DFIR, ielaušanās testu veikšanā, pētniecībā un vadībā. Dons ir piedalījies SANS Advisory Board, Ethics Committee, Gold Program un pašlaik ir ICS410 pasniedzējs. Ar Donu var sazināties @cutaway un https://www.cutawaysecurity.com.

Resursi:

Kā iegūt rezerves kopijas: https://www.sans.org/security-awareness-training/resources/got-backups
Četri vienkārši padomi, kā sevi pasargāt:
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Redakcija: Walter Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley | Tulkojums: CERT.LV