OUCH!
Ikmēneša informācijas drošības izdevums tev

Kāpēc ir svarīgi veikt atjauninājumus?

Pārskats

Kiberuzbrucēji nepārtraukti meklē un atrod jaunas ievainojamības jūsu ikdienā izmantotajā programmatūrā. Ievainojamība ir kļūda vai nepilnība programmatūras izstrādes procesā. 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. Kiberuzbrucēji izmanto un ekspluatē šīs programmatūras ievainojamības, lai attālināti ielauztos sistēmās, tostarp jūsu izmantotajās sistēmās. Turpretī programmatūru ražotāji un ierīču izplatītāji nepārtraukti strādā pie šo nepilnību labojumiem jeb izstrādā tā sauktos ielāpus, kurus iekārtās varam uzstādīt, veicot programmatūras atjauninājumus. Viens no labākajiem veidiem, kā sevi aizsargāt, ir nodrošināt, lai jūsu izmantotajās tehnoloģijās vienmēr būtu pieejami jaunākie atjauninājumi. Šie atjauninājumi ne tikai novērš zināmās ievainojamības, bet bieži vien arī pievieno jaunas drošības funkcijas, tādējādi kiberuzbrucējiem ir daudz grūtāk uzlauzt jūsu ierīces.

Kā strādā atjauninājumi?

Ja ir zināma programmatūras ievainojamība, izstrādātājs vai pārdevējs izveido programmatūras tehnisko defektu novēršanas programmu ievainojamībai (sauktu par ielāpu) un publisko atjauninājumu. Pēc tam sistēma lejupielādē un instalē šo atjauninājumu, novēršot ievainojamību. Piemēram, ir jāatjaunina šāda programmatūra:

- Operētājsistēmas, kas darbojas jūsu klēpjdatorā (piemēram, Microsoft Windows vai Apple OSX) vai viedtālrunī (piemēram, Android vai iOS).
- Mājas tīkla iekārtas, piemēram, interneta maršrutētājs vai Wi-Fi piekļuves punkti, vai mājas viedierīces, piemēram, termostati, durvju zvani, sadzīves ierīces vai drošības kameras.
- Programmas, kas darbojas jūsu ierīcēs, piemēram, klēpjdatora tīmekļa pārlūkprogramma vai tālruņa mobilās 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 kiberuzbrucēji var izmantot. Tāpēc daudzi piegādātāji, 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.

SANS SECURITY AWARENESS
© SANS Institute 2023

Visbeidzot, ja kāda no jūsu ierīcēm vai lietojumprogrammām ir veca un vairs netiek atbalstīta no ražotāja puses, iesakām tās aizstāt ar jaunākām versijām, kas tiek aktīvi atjauninātas un atbalstītas.

Kā atjaunināt

Sistēmas var atjaunināt divējādi.

1. **Manuāli (grūtais ceļš)**: Kad atjauninājums ir pieejams, atjauninājumu lejuplādējiet un instalējiet manuāli. Šādi jūs varat labāk kontrolēt, kādi atjauninājumi un kad ir instalēti. Manuālo atjauninājumu trūkums ir tas, ka ar tiem ir daudz vairāk darba, jo ne tikai jāseko līdzi, kad katra ierīce vai programma ir jāatjaunina, bet arī tās ir jāatjaunina manuāli, tāpēc to var viegli aizmirst izdarīt.

2. **Automātiski (vieglais ceļš)**: Jūs visās ierīcēs iespējojat automātisko atjaunināšanu, kas nozīmē, ka, tiklīdz tiek izdots jauns ielāps, ierīce to automātiski lejupielādē un instalē. Automātisko atjauninājumu priekšrocība ir tā, ka lielākā daļa darba tiek paveikta jūsu vietā. Taču automātiskajai atjaunināšanai var būt arī trūkumi – atjauninātā 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. Kad iespējojat automātiskos atjauninājumus, regulāri pārliecinieties, ka jūsu sistēma tiešām tiek atjaunināta.

No abām iespējām ir ļoti ieteicams iespējot un izmantot automātisko atjaunināšanu visās personiskajās ierīcēs. 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 nebūs tik vienkārši.

Viesredaktors

Dr. Džanela Strača (Janell Straach) ir pasniedzēja Raisa Universitātē (Rice University), kur viņa māca kiberdrošību un mākslīgo intelektu. Džanela ir organizācijas Women In CyberSecurity (WiCyS) valdes priekšsēdētāja. Ar Dr. Straču var sazināties pa e-pastu janell@wicys.org.

Resursi

Digitālā pavasara tīrīšana: https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Vai man nepieciešama drošības programmatūra?: https://www.sans.org/newsletters/ouch/security-software/
Emocionālie ierosinātāji – kā kiberuzbrucēji piemāna cilvēkus: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Tulkojums: CERT.LV

OUCH! To publicējis "SANS Security Awareness", un tas tiek izplatīts saskaņā ar "Creative Commons BY-NC-ND" 4.0 licenci. Jūs varat brīvi koplietot vai izplatīt šo rakstu, kamēr vien jūs to nepārdodat un nepārveidojat. Redakcijas kolēģija: Valters Skrivenss (Walter Scrivens), Fils Hofmans (Phil Hoffman), Alans Vagoners (Alan Waggoner), Leslija Ridauta (Leslie Ridout), Princesa Janga (Princess Young).