Ikmēneša informācijas drošības biļetens ikvienam

OUCH!

ŠAJĀ NUMMURĀ …

Ko var mācīties no WannaCry

Pārskats

Pēdējā laikā jūs droši vien esat redzējuši ļoti daudz ziņas par jaunu kiberuzbrukumu - “WannaCry”. Tas ir inficējis viakāk kā 200 000 datoru, liedzot daudzām organizācijām, tajā skaitā Lielbritānijas slimncām, piekļuvi datiem. Ir vairāki iemesli, kādēļ tieši šis uzbrukums piesaistīja tik lielu uzmanību. Pirmkārt, tas strauji izplatījās no datora uz datoru, izmantojot zināmu Windows programmatūras ievainojamību. Otrkārt, šis uzbrukums ietilpst tā saucamo izspiedējvīrusu kategorijā, tas nozīmē, ka tas nošifrē jūsu failus, liedzot pieeju datiem. Vienīgias veids, kā atgūt savus datus, ir atjaunot tos no rezerves kopijām vai samaksāt uzbrucējam apmēram 300 EUR izpirkuma maksu, lai atšifrētu datus. Treškārt, šādam uzbrukumam nevajadzēja būt iespējamam. Ievainojamība, ko “WannaCry” izmantoja, bija labi zināma Microsoft, kas bija izlaidis labojumu vairākus mēnešus iepriekš. Taču daudzas organizācijas šo labojumu neuzlika, vai vēl joprojām izmantoja tādas operētājsistēmas, piemēram, Windows XP, kas ir tik vecas, ka tām vairs neizstrādā atjauninājumus. Šajā izdevumā aprakstīsim trīs vienkāršus soļus, ko jūs varat izmantot, lai aizsargātos no līdzīgiem uzbrukumiem.

Viesredaktors

Dr. Johannes Ullrich ir SANS Tehnoloģiju institūta pētniecības dekāns un DShield.org dibinātājs. Viņš ir atbildīgs par **SANS Internet Storm Center**, kas monitorē aktuālos kiberdrošības draudus. Viņš māca „Tīkla aplikāciju drošības” (**DEV522**), „Ielaušanās atklāšanas” (**SEC503**) un „IPv6” (**SEC546**) kursus.

Atjauninājumi

Pirmkārt un galvenokārt, vienmēr atjauniniet savus datorus, mobilās iekārtas, aplikācijas un jebko, kas pieslēgts internetam. Kibernoziedznieki vienmēr meklē jaunas programmatūras ievainojamības. Kad tie atrod ievainojamību, tie izmanto īpašas programmas, lai ielauztos ierīcēs, ko jūs lietojat. Tajā pašā laikā uzņēmumi, kas izstrādā programmatūru, cenšas novērst ievainojamības izlaižot atjauninājumus. Ja jūsu iekārtās tiek uzstādīti atjauninājumi, tās uzlauzt ir daudz grūtāk. Tādēļ “WannaCry” izplatība ir tik muļķīga. Atjauninājumus, kas nepieciešami, lai to nepieļautu, Microsoft bija izlaidis gandrīz divus mēnešus iepriekš. Ja organizācijas būtu parūpējušās par savu datoru atjaunināšanu, uzbrukums nebūtu izdevies. Lai atjauninātu ierīces, kad vein iespējams, uzstādiet automātisko atjauninājumu uzlikšanu. Šis likums

Ko var mācīties no WannaCry

attiecas gandrīz uz visām iekārtām, kas pieslēgtas tīklam, ne tikai datoriem un mobilajām ierīcēm, bet arī televizoriem, kas pieslēgti internetam, mājas maršrutētājiem, spēļu konsolēm, ar laiku iespējams pat jūsu automašīnai. Ja operētārsistēmas ir tik vecas ,ka tām vairs nenodrošina atjauninājumus, piemēram, Windows XP, aizstājiet tās ar jaunākām, kuras tiek atbalstītas.

Lai aizsargātu sevi no WannaCry līdzīgiem uzbrukumiem, veiciet trīs vienkāršas darbības: atjauniniet datorus, aizsargājieties pret pikšķerēšanu un veidojiet rezerves kopijas jūsu sistēmām.

Rezerves kopijas

Dažos gadījumos kiberuzbrukumi var ietekmēt arī sistēmas, kas ir atjauninātas. Nākamais solis aizsardzībai ir rezerves kopiju veidošana. Rezerves kopijas ir tāda jūsu informācijas kopija, kas tiek glabāta kaut kur citur, nevis jūsu datorā vai mobilajā ierīcē. Un, kad dati tiek pazaudēti, tos var atjaunot no rezerves kopijām. Diemžēl cilveki bieži nespēj nodrošināt regulāras rezerves kopijas, lai arī tās ir vienkārši un lēti izveidot. Ir divu veidu rezerves kopijas – fiziskais datu nesējs vai glabāšana “mākonī”. Katrai pieejai ir savas priekšrocības un trūkumi. Jūs varat izmantot abus veidus vienlaicīgi, ja nevarat izvēlēties vienu no tām.

Fiziskie datu nesēji ir iekārtas, ko jūs kontrolējat, piemēram, ārējie USB diski vai tīkla ierīces, kas pieejamas jūsu mājās vai birojā. Jūsu pašu fiziskais datu nesējs ļauj jums kopēt un atjaunot lielus datu apjomus salīdzīnoši ātri. Šādas metodes trūkums ir, ja jūsu datorā ir ļaunatūra, piemēram, izspiedējvīrusi, iespējams, ka tā izplatīsies arī uz rezerves kopijām. Ja jūs izmantojat ārējas iekārtas rezerves kopijām, jums jāplāno glabāt rezerves kopijas citā drošā vietā. Atcerieties arī atbilstoši marķēt rezerves kopiju datu nesējus. “Mākoņu” glabātuves risinājumi ir tiešsaistes pakalpojumi, kas saglabā jūsu failus internetā. Parasti jūs instalējat aplikāciju datorā, kas parūpējas par rezerves kopijām. Priekšrocības ir vienkāršība, turklāt gadījumā, ja izspiedējvīruss inficē jūsu mājas datoru, tas parasti nespēj piekļūt rezerves kopijām “mākonī”. Trūkums ir tas, ka kopiju veidošana un arī atgūšana var prasīt ilgāku laiku, īpaši ja datu apjoms ir liels. Svarīgi arī ir privātuma un drošības apsvērumi. Vai rezerves kopiju pakalpojuma sniedzējs nodrošina drošības kontroles, piemēram, datu šifrēšanu un drošu autentifikāciju?

Ko var mācīties no WannaCry

Pikšķerēšana

Visbeidzot, ļaundari vienmēr maina un attīsta uzbrukuma metodes. Kibernoziedznieki bieži izmanto uzbrukuma veidu, ko sauc par pikšķerēšanu, lai uzbruktu un inficētu upurus. Pikšķerēšana nozīmē, ka noziedznieki nosūta jums e-pastu, ar ko cenšas jūs piespiest atvērt inficētu pielikumu vai apmeklēt ļaundabīgu interneta vietni. Abos gadījumos jūsu dators var tikt inficēts. "WannaCry" izmantoja savādāku uzbrukuma metodi, tomēr pikšķerēšana bieži tiek lietota dažāda cita veida uzbrukumos, arī vairumā izspiedējvīrusu. Turklāt tie, kas attīstīja "WannaCry", neapšaubāmi pilnveidos uzbrukuma metodes nākotnē un izmantos jaunus veidus, piemēram, pikšķerēšanu, lai inficētu vēl vairāk datoru. Aizsardzība pret šādiem e-pasta uzbrukumiem ir veselais saprāts. Ja e-pasts vai ziņojums šķiet dīvains, aizdomīgs vai pārāk labs, lai būtu patiesība, tas visdrīzāk ir uzbrukums.

UZZINIET VAIRĀK

Parakstieties uz OUCH! - ikmēneša biļetenu par informācijas tehnoloģiju drošību datoru lietotājiem, apmeklējiet OUCH! arhīvu, uzziniet vairāk par SANS informācijas tehnoloģiju drošības risinājumiem, apmeklējot tīmekļa vietni securingthehuman.sans.org/ouch/archives.

CERT.LV ir Latvijas Republikas Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. CERT.LV misija ir veicināt informācijas tehnoloģiju drošību Latvijā. Uzziniet vairāk https://www.cert.lv vai sekojiet mums Twiterī @certlv.

Resursi

Kas ir ļaunatūra:	https://securingthehuman.sans.org/ouch/2016#march2016
Izspiedējvīrusi:	https://securingthehuman.sans.org/ouch/2016#august2016
Rezerves kopijas:	https://securingthehuman.sans.org/ouch/2015#august2015
Pikšķerēšana:	https://securingthehuman.sans.org/ouch/2015#december2015
Droša "mākoņa" izmantošana:	https://securingthehuman.sans.org/ouch/2016#november2016

License

Redakcija: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Tulkojums: Edgars Tauriņš