Mėnesinis informacinio saugumo naujienlaiškis Tau

Ar į mano kompiuterį buvo įsilaužta?

Apžvalga

Nesvarbu, kokie saugūs besijaustumėte, naudojant kompiuterį, kaip ir vairuojant automobilį, anksčiau ar vėliau gali nutikti kas nors nenumatyto. Žemiau rasite užuominas, padėsiančias išsiaiškinti, ar į jūsų kompiuterį buvo įsilaužta ir patarsiančias ką daryti, jei taip nutiko. Kuo greičiau nustatysite, kad kažkas negero įvyko, tuo labiau tikėtina, jog šią problemą galėsite išspręsti.

Užuominos, kad buvo įsilaužta į jūsų kompiuterį

- **Jūsų antivirusinė programa rodo pranešimą, kad jūsų kompiuterio sistema yra užkrėsta virusu. Įsitikinkite, jog tokį pranešimą rodo būtent jūsų antivirusinė programa, o ne iš interneto svetainės iškylantis langas, kuriuo bandoma jus įtikinti paskambinti kokiu nors telefono numeriu arba įdiegti kokią programą. Nesate tikri, kas tai? Tuomet atidarykite savo antivirusinės programos langą.**
- **Ekrane iškyla langas, kuriame rašoma, kad jūsų kompiuteris buvo užšifruotas, todėl norėdami atgauti savo failus, turite sumokėti išpirką.**
- **Interneto naršyklė jus nukreipia į įvairias svetaines, kuriose neketinote lankytis.**
- **Jūsų kompiuterio sistema arba programos pastoviai išsijunginėja, darbalaukyje yra atsiradę nežinomų programų piktogramų arba ekrane iškilinėja keisti langai.**
- **Jūsų slaptažodis daugiau nebeveikia, nors žinote, kad jį įvedėte teisingai.**
- **Draugai jūsų klausia, kodėl jiems el. paštu siunčiate brukalus, kurių iš tiesų niekada nesiuntėte.**
- **Banko ataskaitoje matote, kad nuo jūsų kredito kortelės arba banko sąskaitos buvo nuskaityti pinigai už tai, ko nepirkote ir neužsisakinėjote.**

Kaip išspręsti šias problemas?

Jei įtariate, kad į jūsų kompiuterį buvo įsilaužta, tuomet kuo greičiau imsitės veiksmų, tuo bus geriau. Jei buvo įsilaužta į darbo kompiuterį, nebandykite šios problemos spręsti savarankiškai. Nedelsdami apie tai praneškite. Jei buvo įsilaužta į jūsų asmeninį kompiuterį arba paskyrą, tuomet galite imtis toliau aprašytų veiksmų:

Pakeiskite savo slaptažodžius. Tai reiškia, kad slaptažodžiai turi būti pakeisti ne tik jūsų kompiuteriuose ir mobiliuose įrenginiuose, bet ir jūsų turimose internetinėse paskyrose. Nekeiskite slaptažodžių, naudodamiesi kompiuteriu, į kurį buvo įsilaužta. Naudokitės kita sistema, kurios saugumu esate užtikrinti. Jei turite daugybę paskyrų, pradėkite nuo pačių svarbiausių. Jei negalite prisiminti visų savo slaptažodžių, naudokite slaptažodžių tvarkytuvę.

Finansiniai sprendimai. Dėl problemų, susijusių su jūsų kredito kortele arba bet kokiomis finansinėmis paskyromis, nedelsdami susisiekite su savo banko arba kredito kortelės įmonės atstovais. Skambinkite oficialiais jų telefono numeriais, kuriuos galite rasti savo banko kortelės galinėje pusėje, finansinių ataskaitų rekvizitų skiltyje arba oficialioje svetainėje, kurioje lankytumėtės iš patikimo kompiuterio. Taip pat apsvarstykite galimybę uždrausti prieigą prie jūsų kredito informacijos.

Antivirusinė programa. Jei apie užkrėstą failą praneša antivirusinė programa, atlikite jos rekomenduojamus veiksmus. Dauguma antivirusinių programų jums pateiks nuorodas, kurias paspaudę galėsite gauti daugiau informacijos apie konkretaus užkrato tipą.

Operacinės sistemos įdiegimas iš naujo. Jei virusais užkrėsto kompiuterio sutvarkyti nepavyko arba norite būti visiškai užtikrinti, kad jūsų kompiuterio sistema yra saugi, įdiekite kompiuterio operacinę sistemą iš naujo. Nediekite operacinės sistemos iš jos atsarginių kopijų, nes šios kopijos turėtų būti naudojamos tik jūsų asmeninių failų atkūrimui. Jei nesate tikri, kaip atkurti sistemą, apsvarstykite galimybę pasinaudoti profesionalų paslaugomis, kurie jums šioje srityje padėtų. Arba, jei jūsų kompiuteris ar kitas įrenginys yra pasenęs, paprasčiau gali būti tiesiog įsigyti naują. Galiausiai, atkūrę kompiuterio sistemą arba įsigiję naują įrenginį, įsitikinkite, kad jo sistema yra atnaujinta ir, jei tik įmanoma, įjunkite automatinį jos atnaujinimą.

Atsarginės kopijos. Svarbiausias veiksmas, kurio galite imtis, siekdami iš anksto apsisaugoti, yra reguliariai daryti atsargines kopijas. Dauguma sistemų kasdien ar net kas valandą automatiškai kurs jūsų failų atsargines kopijas. Nepriklausomai nuo to, kokį sprendimą pasirinksite naudoti, periodiškai patikrinkite, ar galite tuos failus atkurti. Gana dažnai vienintelis būdas viską atkurti po įsilaužimo yra atkurti duomenis iš atsarginių kopijų.

Teisėsauga. Jei jums kas nors kokiu nors būdu grasina, praneškite apie tai vietos teisėsaugai. Įvykus kibernetiniam incidentui, apie jį pranešti galite Nacionaliniam kibernetinio saugumo centrui https://www.nksc.lt/pranesti.html.

Kviestinis redaktorius

Dr. Johannes Ullrich *(@johullrich) yra SANS technologijų instituto mokslinių tyrimų fakulteto dekanas, „SANS Internet Storm“ centro direktorius ir SANS instituto mokslinės draugijos narys. Jis sukūrė „DShield“ bendradarbiavimo jutiklių tinklą ir yra „Internet Storm“ centro kasdieninės tinklalaidės apie tinklo saugos naujienas vedėjas.*

Šaltiniai

Atsarginės kopijos:	https://www.sans.org/u/JGP
Slaptafrazės:	https://www.sans.org/u/JGU
Slaptažodžių tvarkytuvės:	https://www.sans.org/u/JGZ
Kas yra kenkimo programa?:	https://www.sans.org/u/JH4
Prieigos prie kredito ataskaitos uždraudimas:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/