Publicația dumneavoastra lunară de sensibilizare asupra securității informatice

Sunt oare victima unui atac cibernetic?

Prezentare generală

Indiferent cât de precauți sunteți online, la fel precum condusul unei mașini, mai devreme sau mai târziu puteți fi victima unui accident. Mai jos aveți câteva indicii pentru a vă ajuta să aflați dacă ați fost victima unui atac cibernetic și ce să faceți in acest caz. Cu cât identificați atacul mai repede, cu atât este mai probabil să remediați problema.

Indicii ca ați fost victima unui atac cibernetic

Programul anti-virus generează o alertă despre o infecție a sistemului. Asigurați-vă că programul anti-virus este cel care generează alerta și nu o fereastră pop-up de pe un site care încearcă să vă convingă sa apelați un număr de telefon sau sa instalați altceva. Nu sunteți sigur? Deschideți programul anti-virus.

Aveți o fereastră pop-up care spune că v-a criptat computerul și trebuie să plătiți o răscumpărare pentru a vă putea accesa fișierele

Motorul dvs. de căutare (browser-ul) afișează pagini pe care nu ați cerut sa le vizitați

Computerul sau aplicațiile se blochează constant, aveți pictograme pentru aplicații necunoscute sau va apar ferestre pop-up ciudate.

Parola nu vă mai funcționează, deși știți că este corectă.

Prietenii vă întreabă de ce le trimiteți mesaje spam despre care știți că nu le-ați trimis.

Observați tranzacții pe cardul de credit sau retrageri din contul bancar pe care știți ca nu le-ați efectuat.

Cum să răspundeți

Dacă bănuiți că ați fost victima unui atac cibernetic, cu cât acționați mai repede, cu atât mai bine. În cazul în care atacul este legat de muncă, nu încercați să remediați dvs. problema ci raportați-o imediat departamentului IT. Dacă atacul a avut loc asupra unui sistem sau cont personal, găsiți mai jos câțiva pași pe care îi puteți urma:

Schimbați-vă parolele: Aceasta înseamnă nu numai schimbarea parolelor de la calculator și dispozitivele mobile, ci și parolele conturilor dvs. online. Asigurați-vă că nu folosiți calculatorul compromis pentru a schimba parolele, ci utilizați un alt calculator sau dispozitiv care știți că este securizat. Dacă aveți mai multe conturi, începeți cu cele mai importante. Daca nu puteți retine toate parolele atunci utilizați un program de gestiune a parolelor.

Financiar: Pentru problemele legate de cardul dvs. de credit sau de conturile financiare, sunați-va imediat banca sau compania de credit. Apelați-le la un număr de telefon oficial, cum ar fi cel de pe spatele cardului bancar, cel din extrasele de cont sau accesați-le site-ul de pe un calculator de încredere.

Anti-virus. Dacă programul anti-virus vă semnalează prezența unui fișier infectat, puteți urma pașii recomandați de acesta. Cele mai multe programe anti-virus conțin referințe online pe care le puteți accesa pentru a afla mai multe despre infecția respectivă.

Reinstalarea. Dacă nu reușiți să remediați computerul infectat sau doriți să vă asigurați că sistemul de operare este curat, o variantă mai sigură este reinstalarea acestuia. Nu îl reinstalați însă din copiile de siguranță (backup). Acestea (backup-urile) ar trebui să fie utilizate numai pentru recuperarea fișierelor personale. Dacă nu vă simțiți confortabil făcând singuri reinstalarea, apelați la un service profesionist pentru a vă ajuta. De asemenea, dacă calculatorul este vechi, s-ar putea să fie mai simplu și mai ieftin să cumpărați unul nou. Odată ce ați reinstalat sistemul sau ați achiziționat unul nou, asigurați-vă că este actualizat și că ați activat funcția de actualizare automată, ori de câte ori este posibil.

Copiile de siguranță (backup-uri). Cel mai important pas pe care-l puteți face pentru a vă proteja este să vă pregătiți din timp făcând copii de siguranță periodic. Exista multe soluții care salvează automat orice fișier nou sau recent modificat la intervale de o zi sau chiar o oră. Indiferent de soluția pe care o utilizați, verificați periodic că vă puteți restaura fișierele. In general, recuperarea datelor din copii de siguranță este singura cale prin care vă puteți restaura sistemul după un atac cibernetic reușit.

Acțiune legală: Dacă vă simțiți amenințați in vreun fel, semnalați incidentul autorităților competente.

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Aflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

Dr. Johannes Ullrich *(@johullrich) este Decanul Departamentului de Cercetare din cadrul Institutului Tehnologic SANS, directorul Centrului SANS Internet Storm și membru al SANS. A creat rețeaua de senzori de colaborare DShield și găzduiește podcastul zilnic al Internet Storm Center despre securitatea rețelelor.*

Resurse

Copiile de siguranță:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201708_ro.pdf
Propoziții - parolă:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201704_ro.pdf
Programele de gestiune a parolelor:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201709_ro.pdf
Ce sunt programele malware:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201603_ro.pdf