SANS SECURITY AWARENESS

De maandelijkse Security Awareness nieuwsbrief voor jou!

Ben ik gehackt?

Overzicht

Hoe zorgvuldig je ook bent, net als bij het besturen van een auto kan er vroeg of laat een ongeluk gebeuren. Hieronder vind je aanwijzingen om uit te vinden of je gehackt bent en zo ja, wat je moet doen. Hoe eerder je ontdekt dat er iets is gebeurd, hoe groter de kans dat je het probleem kunt oplossen.

Aanwijzingen dat je gehackt bent

Jouw antivirusprogramma genereert een waarschuwing dat je systeem geïnfecteerd is. Controleer of het je antivirussoftware is die de waarschuwing genereert, en niet een pop-upvenster van een website die je voor de gek probeert te houden door een nummer te bellen of iets anders te installeren. Niet zeker? Open dan je anti-virus programma.

Je krijgt een pop-up venster dat zegt dat je computer gecodeerd is en je moet losgeld betalen om je bestanden terug te krijgen.

Jouw browser brengt je naar allerlei websites waar je niet naartoe wilt.

Je computer of applicaties crashen voortdurend, er zijn pictogrammen voor onbekende apps of vreemde vensters die opduiken.

Je wachtwoord werkt niet meer, ook al weet je dat je wachtwoord juist is.

Vrienden vragen je waarom je ze spamt met e-mails waarvan je weet dat je ze nooit verstuurd hebt.

Er zijn kosten gemaakt met je creditcard of opnames van je bankrekening die je nooit hebt verricht.

Wat te doen

Als je vermoedt dat je gehackt bent; hoe eerder je handelt, hoe beter. Als de hack gerelateerd is aan het werk, probeer het probleem dan niet zelf op te lossen, maar meld het onmiddellijk. Als het een persoonlijk systeem of account is dat is gehackt, zijn hier enkele stappen die je kunt nemen

Wijzig je wachtwoorden: Dit omvat niet alleen het wijzigen van de wachtwoorden op je computers en mobiele apparaten, maar ook voor je online accounts. Gebruik de gehackte computer niet om je wachtwoorden te wijzigen, maar gebruik een ander systeem waarvan je weet dat het veilig is. Als je veel accounts hebt, begin dan eerst met de belangrijkste. Niet alle wachtwoorden kunnen gemakkelijk worden bijgehouden, gebruik een wachtwoordmanager.

Financieel: Voor problemen met je creditcard of eender welke financiële rekening, bel je meteen je bank of creditcardmaatschappij. Gebruik een vertrouwd telefoonnummer om hen te bellen, zoals vanaf de achterkant van de bankpas, je financiële overzichten of bezoek hun website vanaf een vertrouwde computer. Daarnaast kun je overwegen om je kredietbestanden te bevriezen.

Anti-virus. Als je door middel van jouw antivirussoftware op de hoogte wordt gebracht van een geïnfecteerd bestand, volg dan de aanbevolen acties. De meeste antivirussoftware hebben links die je kunt volgen om meer te weten te komen over de specifieke infectie.

Opnieuw installeren. Als je niet in staat bent om een geïnfecteerde computer te repareren of als je meer zekerheid wilt hebben over de veiligheid van je systeem, installeer je het besturingssysteem opnieuw. Herinstalleer niet opnieuw vanaf back-ups, in plaats daarvan moeten back-ups alleen worden gebruikt voor het herstellen van persoonlijke bestanden. Als je je ongemakkelijk voelt bij het herstellen, overweeg dan om een professionele service te gebruiken om je te helpen. Of, als jouw computer of apparaat oud is, kan het makkelijker zijn om een nieuwe aan te schaffen. Tot slot, zodra je je systeem opnieuw hebt geïnstalleerd of een nieuw systeem hebt aangeschaft, zorg ervoor dat het wordt bijgewerkt en schakel het automatisch bijwerken in wanneer mogelijk.

Back-ups. Een belangrijke stap om jezelf te beschermen is om je van tevoren voor te bereiden met regelmatige back-ups. Veel oplossingen maken dagelijks of zelfs elk uur automatisch een back-up van gegevens. Welke oplossing je ook gebruikt, controleer regelmatig of je in staat bent om deze bestanden te herstellen. Vaak is het herstellen van je gegevensback-ups de enige manier waarop je kunt herstellen van een hack.

Rechtshandhaving: Als je je op de een of andere manier bedreigd voelt, meld het incident dan aan de lokale politie. Als je het slachtoffer bent van Identity Theft en gevestigd bent in de Verenigde Staten, bezoek dan https://www.identitytheft.gov.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Dr. Johannes Ullrich *(@johullrich) is de decaan van de onderzoeksafdeling van het SANS Technology Institute, de directeur van het SANS Internet Storm Center en een SANS Fellow. Hij creëerde het DShield-samenwerkingsnetwerk en host de dagelijkse nieuwspodcast voor netwerkbeveiliging van het Internet Storm Center.*

Bronnen

Backups: https://www.sans.org/u/JGP
Passphrases: https://www.sans.org/u/JGU
Password Managers: https://www.sans.org/u/JGZ
What Is Malware: https://www.sans.org/u/JH4
Credit Freeze: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/