SANS SECURITY AWARENESS

Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Är jag hackad?

Inledning

Oavsett hur säker du är, precis som med bilkörning, kan du för eller senare råka ut för en olycka. Nedan finns ledtrådar som hjälper dig räkna ut om du har blivit hackad och om så är fallet, vad man ska göra. Att tidigt upptäcka om du blivit hackad ökar sannolikheten att du kan åtgärda problemet.

Ledtrådar att du har blivit hackad

Antivirusprogrammet varnar att ditt system är infekterat. Säkerställ att det är ditt antivirusprogram som genererar varningen, och inte ett popup-fönster från en webbplats som försöker lura dig att ringa ett nummer eller installera något. Vet du inte? Öppna ditt antivirusprogram.

Ett popup-fönster som meddelar att din dator har krypterats och du måste betala en lösensumma för att få tillbaka dina filer.

Din webbläsare tar dig till olika webbsidor som du inte tänkt besöka.

Din dator eller program kraschar ofta, det finns ikoner för okända program eller konstiga fönster som öppnas.

Ditt lösenord slutar att fungera även fast du vet att ditt lösenord är korrekt.

Vänner frågar dig varför du spammar dem med e-post som du vet att du aldrig har skickat.

Det finns köp genomförda med ditt kreditkort eller överföringar från ditt bankkonto som du inte har gjort.

Hur ska man agera

Om du misstänker att du har blivit hackad är ett skyndsamt agerande avgörande. Om intrånget är arbetsrelaterad, ska du inte försök att lösa problemet själv utan rapportera problemet omedelbart till din arbetsgivare. Om det är ett personligt system eller konto som hackats, kan du vidta någon av följande åtgärder.

Ändra dina Lösenord: Det omfattar att byta lösenord på dina datorer och mobila enheter, men också på dina online-konton. Använd inte den hackade datorn när du byter dina lösenord, använd ett annat system som du vet är säkert. Om du har många konton börjar du med de viktigaste först. Kan du inte hålla reda på alla dina lösenord, använd en lösenordshanterare.

Finansiell: Vid problem med ditt kreditkort eller bankkonton, ring omedelbart din bank eller kreditkortsföretag. Använd alltid ett betrott telefonnummer när du ringer till dem. Det finns till exempel på baksidan av ditt bankkort, på dina bankdokument eller besök deras hemsida från en säker dator. Dessutom, överväg att aktivera en bedrägerispärr, samt tillämpa uttagsgräns och landsbegränsningar på dina konton.

Antivirus: Om ditt antivirusprogram varnar för en infekterad fil, följer du de åtgärder som programmet rekommenderar. De flesta antivirusprogram har länkar till mer information om det specifika viruset.

Ominstallation: Om du inte kan fixa en infekterad dator och du vill vara trygg med att ditt system är säkert, ska du installera om operativsystemet. Gör inte en ominstallation med hjälp av säkerhetskopior, använd endast säkerhetskopior till att återställa dina personliga filer. Om du inte har kunskap att göra en ominstallation, bör du överväga att använda en professionell aktör. Om datorn eller enheten är gammal kan det vara enklare att köpa en ny. Slutligen, när du har installerat om ditt system eller köpt ett nytt ska du säkerställa att den är uppdaterad och aktivera automatiska uppdateringar när det är möjligt.

Säkerhetskopiering: För att skydda information till framtiden är regelbunden säkerhetskopiering viktig. Många system kan automatiskt säkerhetskopiera filer dagligen eller till och med varje timme. Oavsett system behöver återläsningstester genomföras regelbundet för att säkerställa att säkerhetskopiorna kan användas vid behov. Säkerhetskopiorna är ofta den enda möjligheten att återställas information om du har blivit hackad.

Brottsbekämpning: Om du känner dig hotat på något sätt ska du rapportera detta till din lokala polismyndighet. Om du är utsatt för identitetsstöld och vistas i Sverige kan du besöka https://polisen.se/utsatt-for-brott/olika-typer-av-brott/bedrageri/identitetsintrang/.

Gästskribent

Dr. Johannes Ullrich *(@johullrich) är Dekanus för forskning vid SANS Technology Institute, Direktör för SANS Internet Storm Center samt en hängiven SANS-anhängare. Han skapade sensornätverket DShield och är värd för Internet Storm Center´s dagliga podcast med nyheter inom nätverkssäkerhet.*

Källor

Backup: 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

OUCH! Publiceras av SANS Security Awareness och distribueras under Creative Commons BY-NC-ND 4.0-licens. Du kan fritt distribuera nyhetsbrevet eller använda det i ditt medvetenhetsprogram så länge du inte ändrar innehållet i nyhetsbrevet. För översättning eller mer information, vänligen kontakta www.sans.org/security-awareness/ouch-newsletter. Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Översatt av: Erik Täfvander & Johan Ahlberg