OUCH! | April 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Jeg har blitt hacket, hva nå?

Oversikt

Vi vet at du bryr deg om å beskytte datamaskinen din og dine mobile enheter, og at du tar grep for å sikre dem. Imidlertid er det slik at uansett hvor trygg du er i bruken av teknologi, kan du før eller siden komme til å bli hacket eller "kompromittert". I dette nyhetsbrevet vil du lære hvordan du kan finne ut om datamaskinen eller mobilen din er blitt hacket, og i så fall, hva du skal gjøre med saken. Og jo raskere du kan oppdage at noe er galt, desto fortere kan du handle, og da har du større mulighet til å begrense skaden som cyber-angriperen kan forårsake.

Gjesteredaktør

Samantha Davison (**@sam_e_davison**) er leder for sikkerhetsbevissthet og opplæringsprogrammer ved Uber, og gir opplæring til deres ansatte over hele verden, i mer enn 350 byer.

Tegn på at du har blitt hacket

Det kan være vanskelig å slå fast om du har blitt hacket, siden det sjelden finnes noen enkel måte å finne det ut på. Istedenfor kan du se etter spor etterlatt av hackere, ofte kalt indikatorer. Jo flere av disse du finner på ditt system, jo større er sjansen for at du har blitt hacket.

- Antivirus-programmet ditt gir deg en advarsel om at systemet er infisert, spesielt hvis det sier at det ikke klarte å fjerne en påvirket fil, eller ikke klarte å putte den i karantene.
- Startsiden i nettleseren din har blitt endret uten at du forventet det, eller nettleseren tar deg til nettsider du ikke ønsker å besøke.
- Det har kommet nye brukerkontoer på datamaskinen eller enheten din som ikke er opprettet av deg, eller det blir kjørt nye programmer som du ikke har installert.
- Datamaskinen/enheten eller applikasjonene på den krasjer i ett sett, det dukker opp ikoner for ukjente apper, og merkelige vinduer åpner og lukker seg.
- Et program ber om godkjenning til å gjøre endringer på systemet, men du driver ikke for øyeblikket med noen form for installasjon eller oppdatering.
- Passordet ditt fungerer ikke lenger når du forsøker å logge inn på systemet ditt, eller en brukerkonto på nettet, selv om du vet at det er det riktige passordet.
- Venner spør deg hvorfor du spammer dem med e-post som du vet du aldri har sendt.
- Mobilen din sender SMS-er til betalingsnumre uten din godkjenning.

Jeg har blitt hacket, hva nå?

- Mobilen din har plutselig uforklarlig høyt dataforbruk eller batteriforbruk.

Hva må du gjøre?

Hvis du tror datamaskinen din eller en av dine mobile enheter har blitt hacket, bør du respondere så snart som mulig. Hvis enheten eller maskinen ble gitt til deg av arbeidsgiver, eller brukt i jobbsammenheng, bør du ikke prøve å løse problemet selv. Ikke bare kan du komme til å gjøre mer skade, du kan også komme til å ødelegge verdifullt bevis som kunne ha blitt brukt i en etterforskning. Istedenfor burde du melde fra til din arbeidsgiver med en gang, som vanlig ved å kontakte brukerstøtte, sikkerhetsteamet, eller en leder. Hvis du av en eller annen grunn ikke får kontakt med arbeidsplassen, eller du er bekymret for forsinkelser, kan du koble maskinen eller enheten fra internett, og sette den i hvilemodus, dvalemodus, eller flymodus. Selv om du ikke er sikker på om du er hacket eller ikke, er det uansett bedre å melde fra nå for sikkerhets skyld. Hvis maskinen eller enheten er din egen personlige, kan du ta følgende grep for å løse saken på egenhånd:

Før eller siden kan datamaskiner eller mobile enheter bli kompromittert, jo fortere du oppdager en hendelse og handler deretter, jo bedre.

- **Endre passordene dine**: Ikke bare på datamaskinen din og alle mobile enheter, men også på alle brukerkontoer på nettet. Sørg for at du ikke bruker enheten som har blitt hacket for å endre passordene, gjør det istedenfor fra en enhet du vet er sikker.
- **Antivirus**: Hvis antivirus-programvaren din advarer deg om en infisert fil, kan du gjøre det den anbefaler. Som vanlig innebærer dette å sette filen i karantene, rense filen, eller slette filen. De fleste antivirus-programmer har linker du kan følge for å lære mer om den enkelte handlingen. Om du er i tvil kan du sette filen i karantene. Om det ikke er mulig, slett den.
- **Gjenoppbygning**: Hvis du ikke klarer å fjerne infeksjonen eller du bare vil være absolutt sikker på at systemet er helt rent, kan det være at den beste løsningen er å gjenoppbygge det fra grunnen av. For en datamaskin bør du følge instruksjonene gitt for dette av operativsystemets leverandør. I de fleste tilfeller vil det innebære å bruke innebygde verktøy for å reinstallere operativsystemet. Hvis disse verktøyene mangler, eller er korrumperte eller infiserte, bør du kontakte leverandøren for hjelp. Ikke reinstaller systemet fra gamle sikkerhetskopier, det kan være de har de samme sårbarhetene som gjorde det mulig for hackeren å få tilgang til systemet ditt i utgangspunktet. Sikkerhetskopier burde kun brukes for å få tilbake tapt data. For mobile enheter kan du følge instruksjoner gitt av mobilleverandøren eller teleoperatøren din, som oftest finner du dette på nettsidene deres. I mange tilfeller

Jeg har blitt hacket, hva nå?

er dette så enkelt som å tilbakestille enheten til fabrikkinnstillingene. Hvis du ikke er komfortabel med å gjøre gjenoppbyggingen selv, bør du vurdere å benytte deg av en profesjonell tjeneste for hjelp. Hvis datamaskinen eller enheten er veldig gammel, kan det være at det er billigst og enklest å kjøpe ny. Til slutt, etter at du er ferdig med gjenoppbygningen eller har kjøpt ny enhet, bør du sørge for at systemet er fullstendig oppdatert, og at automatiske oppdateringer er skrudd på.

- **Sikkerhetskopier**: Det viktigste du kan gjøre for å holde deg trygg, er å forberede deg med jevnlige sikkerhetskopier. Jo oftere du tar sikkerhetskopier, jo bedre. Noen løsninger for å gjøre dette vil automatisk sikkerhetskopiere enhver ny eller endret fil hver time. Og uansett hva slags løsning du tar i bruk for sikkerhetskopiering, bør du jevnlig kontrollere at du er i stand til å gjenopprette de sikkerhetskopierte filene. Gjenoppretting av data fra sikkerhetskopier er ofte den eneste måten å komme seg etter å ha blitt hacket.
- **Politi og myndigheter**: Meld fra om hendelsen til lokalt politi hvis du føler deg truet på noen måte.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på http://www.securingthehuman.org.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

Sikkerhetskopiering & gjenoppretning:	https://securingthehuman.sans.org/ouch/2015#august2015
Passordsetninger:	https://securingthehuman.sans.org/ouch/2015#april2015
Hva er skadevare:	https://securingthehuman.sans.org/ouch/2016#march2016
Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Oversatt av: NorSIS