SANS SECURITY AWARENESS
NorSIS Norsk senter for informasjonssikring
OUCH! | Januar 2018
Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Ditt trådløse nettverk
- Dine enheter
- Passord
- Sikkerhetskopiering

Få et sikkert cyberhjem

Oversikt

For en del år siden var det lett å sørge for god cybersikkerhet i hjemmet; de fleste hjem besto ikke av andre digitale enheter enn et trådløst nettverk og noen datamaskiner. I dag har imidlertid teknologien blitt langt mer kompleks, og er integrert i alle aspekter av livene våre, fra mobile enheter og spillkonsoller til termostaten og kanskje til og med kjøleskapet. Her har du fire enkle grep for å gjøre cyberhjemmet ditt sikrere.

Gjesteredaktør

Matt Bromiley jobber med incident response til daglig, da hjelper han klienter av alle sorter med å håndtere brudd i datasikkerheten. Han er også en SANS instruktør, han lærer bort FOR508: Kursene Advanced Digital Forensics og Incident Response. Du kan følge Matt på Twitter som **@mbromileyDFIR**.

Ditt trådløse nettverk

Nesten alle hjemmenettverk begynner med et trådløst Wi-Fi nettverk. Det er dette som lar alle enhetene dine koble seg til internett. De fleste trådløse hjemmenettverk kontrolleres av ruteren din, eller av et separat trådløst tilgangspunkt. Begge disse fungerer på samme måte ved å sende ut trådløse signaler, enhetene i huset kan så koble seg til nettverket via disse signalene. Dette betyr at det å sikre det trådløse nettverket ditt er en viktig del av det å beskytte hjemmet ditt. Vi anbefaler følgende grep:

- Endre standard administratorpassord på ruteren eller det trådløse tilgangspunktet, ut ifra hvilket som brukes for å kontrollere det trådløse nettverket. Administrator-tilgang brukes for å konfigurere innstillingene for det trådløse nettverket.
- Sørg for at kun folk du stoler på kan koble seg til det trådløse nettverket. For å gjøre det, må du sørge for god sikkerhet i tilkoblingsmetoden til nettverket. For øyeblikket er det beste alternativet å bruke sikkerhetsmekanismen kjent som WPA2. Ved å benytte denne kreves det et passord for at folk skal få koblet til nettverket, og etter at de er tilkoblet, vil de trådløse signalene deres være krypterte.
- Sørg for at passordet som brukes for å koble til nettverket er sterkt, og at det ikke er det samme som du bruker som administratorpassord til ruteren eller tilgangspunktet. Husk at du kun trenger å taste inn dette passordet én gang per enhet.
- Mange trådløse nettverk har støtte for det som kalles et gjestenettverk. Dette lar gjester koble seg til internett, men

Få et sikkert cyberhjem

det beskytter hjemmenettverket ditt ved å hindre at de kan koble seg til andre enheter på nettverket. Om du tar i bruk gjestenettverk, husk å aktiver WPA2, samt et unikt passord.

Er du usikker på hvordan du skal gjøre alt dette? Spør bredbåndsleverandøren din eller sjekk nettsiden deres, sjekk instruksjonene som fulgte med ruteren eller tilgangspunktet, eller sjekk produsentenes nettsider.

Følg disse fire enkle stegene for å sikre cyberhjemmet ditt; sikre ditt Wi-Fi-nettverk, aktivere automatiske oppdateringer, bruke unike passordsetninger, og aktivere sikkerhetskopiering.

Dine enheter

Det neste steget er å vite hvilke enheter som er koblet til ditt trådløse nettverk, og sørge for at alle disse enhetene er sikret. Dette pleide å være enklere når man kanskje bare hadde én eller to datamaskiner. I dagens samfunn kan imidlertid veldig mange ting kobles til nettet, inkludert mobiler, TV-er, spillkonsoller, babymonitorer, høyttalere, og til og med biler. Når du har identifisert alle enhetene, må du sørge for at de er sikret. Den beste måten å gjøre det på er å sørge for at du har automatisk oppdatering på der det er mulig. Cyberkriminelle finner konstant nye svakheter de kan utnytte på forskjellige enheter og operativsystemer. Ved å aktivere automatisk oppdatering vil datamaskiner og enheter alltid kjøre den mest oppdaterte programvaren, da blir det mye vanskeligere å hacke.

Passord

Det neste steget er å bruke et sterkt, unikt passord for alle dine enheter og brukerkontoer på nett. Nøkkelordene her er sterkt og unikt. Er du lei av komplekse passord som er vanskelige å huske og skrive? Vi også. Bruk passordsetninger istedenfor. Dette er en form for passord som består av en serie med ord som er lett å huske, som «Hvor er kaffen min?» eller «solskinn-smultringer-glad-fortapt». Jo lenger passordsetningen er, jo sterkere er den. At passordene er unike vil si at hver enhet og brukerkonto har forskjellige passord. På denne måten vil alle de andre brukerkontoene og enhetene fortsatt være trygge om et passord skulle lekke ut. Klarer du ikke huske alle disse sterke, unike passordene? Slapp av, det klarer ikke vi heller. Derfor anbefaler vi at du bruker et passordhvelv, et spesielt sikkerhetsprogram som lagrer alle passordene dine trygt i en kryptert, virtuell safe.

Til sist, aktiver totrinns bekreftelse overalt hvor det er mulig, spesielt på brukerkontoer på nett. Totrinns bekreftelse er langt sikrere enn andre alternativer. Denne løsningen bruker passord, men også et steg nummer to, som en engangskode sendt

Få et sikkert cyberhjem

til mobilen din på SMS eller generert av en app. Totrinns bekreftelse er sannsynligvis det aller viktigste tiltaket du kan gjøre for å sikre deg selv på nett, og det er mye enklere enn du tror.

Sikkerhetskopiering

Noen ganger kan du bli hacket, uansett hvor forsiktig du er. Om det skulle skje, er det ofte slik at du er nødt til å gjenopprette fra en sikkerhetskopi for å få tilbake viktige filer og data. Sørg for at du jevnlig sikkerhetskopierer viktig informasjon, og forsikre deg om at du kan gjenopprette fra dem. De fleste mobile enheter har støtte for automatisk sikkerhetskopiering til nettskyen. For mange datamaskiner kan du imidlertid være nødt til å kjøpe en form for programvare eller tjeneste for sikkerhetskopiering, som er relativt billig og enkelt å bruke.

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 securingthehuman.sans.org/ouch/archives.

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

Passordsetninger:	https://securingthehuman.sans.org/ouch/2017#april2017
Passordhvelv:	https://securingthehuman.sans.org/ouch/2017#september2017
Totrinns innlogging:	https://securingthehuman.sans.org/ouch/2017#december2017
Sikkerhetskopiering:	https://securingthehuman.sans.org/ouch/2017#august2017

Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS