SANS SECURITY AWARENESS
WelcomeSecurity Enabling value through it security
OUCH! | Januar 2018
Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

Lav et cyber sikkert hjem

Oversigt

For flere år siden var det simpelt at oprette et IT-sikkert hjem. De fleste hjem bestod blot af et trådløst netværk og flere computere. I dag er teknologien blevet langt mere kompleks og er integreret i alle dele af vores liv, fra mobile enheder og spilkonsoller til din termostat og endda måske dit køleskab. Her er fire enkle trin til at lave et IT-sikkert hjem.

Gæsteredaktør

Matt Bromiley er en "incident responder" om dagen, hvor han hjælper kunder der har haft brud på IT-sikkerheden. Han er også en SANS instruktør og underviser FOR508 "Advanced Digital Forensics and Incident Response" kurset. Følg Matt **@mbromileyDFIR**.

Dit trådløse netværk

Næsten alle hjemmenetværk starter med et trådløst netværk (eller Wi-Fi). Dette gør det muligt for alle dine enheder at oprette forbindelse til internettet. De fleste trådløse hjemmenetværk styres af din internetrouter eller et separat, dedikeret trådløst adgangspunkt. De arbejder begge på samme måde ved at sende trådløse signaler, som enhederne i dit hus bruger til at koble sig til internettet. Det betyder at sikring af dit trådløse netværk er en vigtig del af beskyttelsen af dit hjem. Vi anbefaler følgende trin for at sikre det.

- Skift administratorens adgangskode til din internetrouter eller trådløst adgangspunkt, alt efter hvad der styrer dit trådløse netværk. Administratorkontoen er det, der giver dig mulighed for at konfigurere indstillingerne for dit trådløse netværk.
- Sørg for, at kun personer, du har tillid til, kan oprette forbindelse til dit trådløse netværk. Gør dette ved at have høj sikkerhed. I øjeblikket er den bedste mulighed at bruge sikkerhedsmekanismen kaldet WPA2. Ved at aktivere denne kræves der en adgangskode for at oprette forbindelse til dit hjemmenetværk, desuden bliver al onlineaktivitet krypteret.
- Sørg for, at adgangskoden, der bruges til at oprette forbindelse til dit trådløse netværk, er et stærkt kodeord, og at det er anderledes end administratorkodeord. Husk, at du kun skal indtaste adgangskoden én gang for hver af dine enheder, da de gemmer og husker kodeord.
- Mange trådløse netværk understøtter det, der kaldes et gæstenetværk. Dette gør det muligt for besøgende at oprette

Lav et cyber sikkert hjem

forbindelse til internettet, men samtidig beskytte dit hjemmenetværk. Enheder på gæstenetværket kan ikke oprette forbindelse til enhederne på dit hjemmenetværk. Hvis du tilføjer et gæstenetværk, skal du sørge for at aktivere WPA2 samt lav et unikt kodeord til dette netværk.

Er du ikke sikker på, hvordan man gør dette? Spørg din internetudbyder eller tjek deres hjemmeside, læs vejledningen, der fulgte med din internetrouter eller trådløst adgangspunkt, eller søg oplysningerne på deres hjemmeside.

Følg disse fire enkle trin for at oprette et cyber sikkert hjem; sikre dit Wi-Fi-netværk, aktiver automatisk opdatering; brug unikke "passphrases" og foretag backup.

Dine enheder

Det næste skridt er at vide, hvilke enheder der er forbundet til dit trådløse hjemmenetværk, og at sørge for, at alle disse enheder er sikre. Dette plejede at være simpelt, da du kun havde en computer eller to. Men i dag kan næsten alting forbindes til dit hjemmenetværk, herunder dine smart-telefon, tv'er, spillekonsoller, babymonitorer, højttalere eller måske endda din bil. Når du har identificeret alle enheder på dit hjemmenetværk, skal du sikre dig, at de alle er sikre. Den bedste måde at gøre dette på er at sikre, at du har automatisk opdatering aktiveret på de enheder, hvor det er muligt. IT-kriminelle finder konstant nye svagheder i forskellige enheder og operativsystemer. Ved at sikre automatiske opdateringer, kører din computer og enheder altid den nyeste software, hvilket gør dem meget sværere at hacke.

Kodeord

Det næste trin er at bruge et stærkt, unikt kodeord til hver af dine enheder og online-konti. Det vigtige her er, at kodeorderne er stærke og unikke. Hvis du er træt af komplekse kodeord, der er svært at huske og vanskelige at skrive kan du vælge at bruge en "passphrase" i stedet. Dette er en type kodeord, der bruger en række ord, der er let at huske, f.eks. "Hvor er min kaffe?" Eller "Solskin-donuts-glad-tabt". Jo længere dit "passphrase" er, desto stærkere. Et unikt kodeord betyder at bruge forskellige kodeord til hver enhed og online-konto. På denne måde er alle dine andre konti og enheder stadig sikre, hvis et kodeord er kompromitteret. Kan du ikke huske alle de stærke, unikke kodeord? Bare rolig, vi kan heller ikke. Derfor anbefaler vi, at du bruger en "password-manager", som er et særligt sikkerhedsprogram, som sikkert gemmer alle dine kodeord i et krypteret, virtuelt sikkert pengeskab.

Lav et cyber sikkert hjem

Endelig bør du aktivere to-trins bekræftelse, når det er tilgængeligt, især for dine online-konti. To-trins bekræftelse er meget stærkere. Det bruger dit kodeord, men tilføjer også et andet trin, som f.eks. en kode sendt til din smart-telefon eller en app på din smart-telefon, der genererer koden for dig. To-trins bekræftelse er nok det vigtigste for at beskytte dig selv online, og det er meget lettere end du tror.

Backup

Uanset hvor forsigtig du er, kan du risikere at blive hacket. Hvis det er tilfældet, er gendannelse fra backup ofte den eneste måde, du kan gendanne dine personlige oplysninger på. Sørg for regelmæssigt at lave sikkerhedskopier af vigtige oplysninger, og kontroller, at du kan gendanne dem. De fleste mobile enheder understøtter automatisk sikkerhedskopiering til Skyen. For de fleste computere skal du muligvis købe en slags sikkerhedskopieringssoftware eller -service, som er relativt billigt og nem at bruge.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Tidligere udgivelser

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Password Manager:	https://securingthehuman.sans.org/ouch/2017#september2017
Two-factor-godkendelse:	https://securingthehuman.sans.org/ouch/2017#december2017
Backups:	https://securingthehuman.sans.org/ouch/2017#august2017

Licensinformation

Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity