OUCH! | Januar 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Ditt trådløse nettverk**
- **OpenDNS**
- **Enheter koblet til nettverket**

Sikre ditt hjemmenettverk

Oversikt

For noen år siden så var nettverk ganske enkle, kanskje ikke noe mer enn et trådløst aksesspunkt og en datamaskin eller to som surfer nettet. Siden den tid har hjemmenettverk blitt mer og mer komplekse. Ikke bare kobler vi til flere enheter, men vi gjør også mer med de enhetene vi har. I denne utgaven vil vi gå gjennom noen enkle steg for å lage et sikrere hjemmenettverk.

Gjesteredaktør

Kevin Johnson er CEO hos Secure Ideas, styrer **MySecurityScanner.com** og er senior instruktør på SANS instituttet. Du kan finne mer informasjon på **www.secureideas.com**.

Ditt trådløse nettverk

Nesten alle hjemmenettverk starter med et trådløst nettverk (noen ganger kalt et Wi-Fi nettverk). Dette er det som lar deg surfe nettet uten kabler med alle dine enheter, fra bærbare PC-er og nettbrett til spillkonsoller og TV-er. For at dette skal være mulig, trenger nettverket noe som kalles et trådløst aksesspunkt. Dette er en fysisk enhet som er koblet til ruteren (eller kanskje det er bygd inn i ruteren) og sender ut et trådløst signal som enhetene dine kan koble til. Når enhetene kobler til aksesspunktet, kan de koble seg til Internettet og andre enheter på nettverket. Som et resultat er det trådløse aksesspunktet et nøkkelpunkt i hjemmenettverket, vi anbefaler følgende steg for å sikre det.

- For de fleste trådløse aksesspunkt settes det opp et standard brukernavn og passord, disse er godt kjent og ofte lagt ut på Internett. Derfor er det viktig at du bytter standard administratorpassord til noe bare du vet. Sørg for at dette er et unikt passord som ikke brukes på noen andre kontoer.
- En annen innstilling du burde sette er navnet på det trådløse nettverket (noen ganger kalt SSID). Dette er navnet du vil se når du søker etter trådløse nettverk nær deg. Gi nettverket et unikt navn så du kan enkelt gjenkjenne det, men sørg for at det ikke inneholder noe personlig informasjon. Det er liten verdi i å konfigurere nettverket som skjult (eller non-broadcast). De fleste trådløse skannere eller en dyktig angriper kan enkelt finne nettverket selv om det er skjult.

Sikre ditt hjemmenettverk

- Det neste steget er å sørge for at bare personer du kjenner og kan stole på kan koble seg til det trådløse nettverket. Vi vil være sikker på at naboer eller fremmede ikke kan koble seg til eller overvåke nettverket. Du kan enkelt redusere denne risikoen ved å aktivere sterkere sikkerhet på aksesspunktet. Den beste muligheten i dag er å bruke WPA2. Bare ved å aktivere dette, så krever du at de som kobler seg til må bruke et passord, i tillegg er dataene som sendes over det trådløse nettverket kryptert. Unngå bruk av gammel sikkerhetsteknologi som WEP, eller ikke noe sikkerhet i det hele tatt som kalles et åpent nettverk. Et åpent nettverk tillater alle å koble seg til uten autentisering.
- Sørg for at passordet du bruker for å koble deg til det trådløse nettverket er et sterkt passord som er vanskelig å gjette og annerledes enn administratorpassordet. Husk at du trenger sannsynligvis bare å taste inn passordet én gang for hver av enhetene, så vil enheten huske passordet.
- Mange trådløse aksesspunkt støtter det som kalles et gjestenettverk. Et gjestenettverk lar besøkende koble til ditt trådløse aksesspunkt og surfe Internettet, men de kan ikke koble til noen av enhetene du har på nettverket. Hvis du legger til et gjestenettverk, sørg for at du aktiverer WPA2 og bruker et annet passord.
- Hvis du ikke greier å huske de forskjellige passordene kan du bruke en passordhåndterer for å lagre de sikkert.

For å beskytte hjemmenettverket ditt må du sørge for at du har et sikkert trådløst nettverk, du bruker OpenDNS eller lignende tjenester og du oppdaterer alle enhetene dine.

OpenDNS

Etter at du har et trådløst nettverk konfigurert så anbefaler vi at du konfigurerer hjemmenettverket til å bruke OpenDNS som din DNS server (eller lignende tjenester som Norton ConnectSafe for Home). Når du taster et navn inn i nettleseren bruker nettleseren DNS for å finne ut hvilken server den skal koble seg til. Tjenester som OpenDNS identifiserer kjente infiserte nettsider og stopper enheter fra å koble til disse nettstedene ved et uhell. Ofte gir disse tjenestene deg også muligheten til å blokke støtende eller upassende sider. Det som gjør denne metoden så effektiv er at du ikke trenger å installere noe på enheten, du trenger bare å forandre det trådløse aksesspunktet.

Sikre ditt hjemmenettverk

Enheter koblet til nettverket

Det neste steget er å vite hvilke enheter er koblet til nettverket og sørge for at disse er sikret. Dette var enklere før, når det bare var et par enheter koblet til nettverket. Nå kan nesten hva som helst kobles til nettverket, inkluder TV-er, spillkonsoller, babymonitorer, høyttalere, termometer, eller til og med bilen din. Etter at du har identifisert alle enheten på ditt hjemmenettverk, så blir du kanskje overrasket over hvor mange det er. Den beste måten å sikre alle disse enhetene på er ved å sørge for at de alltid kjører nyeste versjon av operativsystemet. Bruk automatisk oppdatering der det er tilgjengelig. Hvis dette ikke er en mulighet, sjekk etter oppdateringer månedlig og installer hvis nødvendig. Besøk også nettverksleverandørens nettsider, de tilbyr kanskje gratis verktøy og tjenester for å holde hjemmenettverket ditt sikret.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
Sikkerhetsskanner for nettverket:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
Passordhåndterere:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis