OUCH! | Februar 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Trådløst nettverk**
- **Dine enheter**

Slik sikrer du hjemmenettverket ditt

Oversikt

Hjemmenettverk var ganske enkle for flere år siden, de inkluderte ofte ikke mer enn et trådløst aksesspunkt og en datamaskin eller to brukt til surfing, netthandel, og spill. I dag er hjemmenettverk imidlertid langt mer komplekse. Vi kobler langt flere enheter til disse nettverkene, og bruker dem til mer enn bare nettsurfing og media. I dette nyhetsbrevet forklarer vi hvordan du kan sette opp et sikkert nettverk hjemme for deg og familien din.

Gjesteredaktør

Cheryl Conley leder teamet for sikkerhetsutdannelse og bevissthet hos Lockheed Martin, og bruker «The I Campaign™» for å nå over 100 000 ansatte. I tillegg til et globalt phishingprogram, inkluderer dette også fokusgrupper for både samarbeidspartnere og talsmenn. Følg Cheryl på Twitter: **@conleychera**.

Trådløst nettverk

Nesten alle hjemmenettverk starter med et trådløst nettverk (ofte kalt et WiFi-nettverk). Det er dette som gjør det mulig for deg å koble alle enhetene dine til internett, fra laptoper og nettbrett til spillkonsoller og TV-er. De fleste trådløse hjemmenett blir kontrollert av en router, som er enheten internettleverandøren din installerte i huset ditt for å koble deg på internett. I noen tilfeller blir imidlertid det trådløse nettverket kontrollert av et såkalt trådløst aksesspunkt, som igjen er koblet til routeren. Uansett hvilke av disse løsning nettverket ditt bruker, fungerer de på samme måte, ved å kringkaste trådløse signaler. Forskjellige enheter i huset ditt bruker dette signalet for å koble seg til det trådløse nettverket. Derfra kan enhetene dine koble seg til internett, og til andre enheter koblet til hjemmenettverket ditt. På grunn av dette er det å sikre det trådløse nettverket ditt en viktig del av å sikre hjemmet ditt. Vi anbefaler at du tar følgende grep:

- Endre standardpassordet til administrasjonssystemet til routeren eller det trådløse aksesspunktet, alt ettersom hvilke av dem som styrer det trådløse nettverket ditt. Administrasjonssystemet er det som lar deg konfigurere innstillingene for det trådløse nettverket ditt. Problemet er at mange routere og trådløse aksesspunkter ofte leveres med standardbrukernavn og standardpassord som er godt kjent, og ofte også tilgjengelig på nettet. Derfor burde du endre administrasjonspassordet til et sterkt unikt passord som bare du kjenner.
- Endre standardnavnet til det trådløse nettverket (også kjent som SSID). Det er dette navnet enhetene dine vil se når de søker etter trådløse nettverk. Gjør nettverksnavnet ditt unikt, så du kan identifisere det, men pass på at

Slik sikrer du hjemmenettverket ditt

det ikke inneholder personlig informasjon. Det er ikke noe poeng i å konfigurere nettverket ditt som skjult, siden de fleste trådløse scanning-verktøy eller enhver angriper med litt kunnskaper enkelt kan avsløre skjulte trådløse nettverk.

- Vær sikker på at kun folk du stoler på kan koble seg til ditt trådløse nettverk, og at tilkoblingen er kryptert. Dette gjør du ved å aktivere sterk sikkerhet. Det beste alternativet for øyeblikket, er sikkerhetsmekanismen kjent som WPA2. Når dette er aktivert, kreves det passord for å koblet til hjemmenettverket ditt, og når tilkoblet blir nettverkstrafikken kryptert. Ikke bruk gamle, utdaterte sikkerhetsmekanismer som WEP, og ikke la nettverket være åpent og usikret. Åpne nettverk lar hvem som helst få koble til det trådløse nettet ditt uten noen form for autentisering.

Beskytt hjemmenettverket ditt ved å sikre det trådløse nettverket, og oppdater og passordbeskytt alle enheter på nettverket ditt.

- Sørg for at passordet brukt til å koble til det trådløse nettverket er sterkt, og at det ikke er det samme som administrasjonspassordet. Husk at du sannsynligvis bare trenger å skrive inn passordet én gang for hver enhet.
- Mange trådløse nettverk støtter noe kjent som et gjestenettverk. Dette gjør det mulig for besøkende å koble til internett, men beskytter hjemmenettet ditt ved å ikke la dem koble seg til noen av enhetene på nettet ditt. Hvis du setter opp et gjestenettverk, sørg for at du aktiverer WPA2 med et sterkt passord for dette nettverket også.
- Skru av tjenester som lar enheter koble til nettverket uten å kjenne passordet eller konfigurasjonsinnstillingene, slik som «WiFi Protect Setup».
- Hvis du synes det er vanskelig å huske alle disse forskjellige passordene, anbefaler vi at du tar i bruk et digitalt passordhvelv for å lagre dem sikkert.

Hvis du ikke er sikker på hvordan du gjør alt dette, kan du forhøre deg med din internettleverandør, sjekke manualen som kom med routeren eller det trådløse aksesspunktet, eller sjekke nettsiden til leverandøren.

Dine enheter

Det neste steget vil være å finne ut av hva som er koblet til hjemmenettverket ditt, og sørge for at alle disse enhetene er sikre. Dette pleide å være enklere før, når det bare var noen få enheter tilkoblet. I dagens verden derimot, hvor alt alltid

Slik sikrer du hjemmenettverket ditt

skal være på nettet, kan hva som helst kobles til hjemmenettverket ditt, inkludert TV-er, spillkonsoller, babymonitorer, høyttalere, termostaten din og kanskje til og med bilen din. En enkel metode for å finne ut hva som er koblet til nettverket ditt, er å bruke en nettverksskanner som Fing. Slike apper kan installeres på PC-en din eller mobilen din, skanner det trådløse nettverket ditt og rapporterer alle enheter som er koblet til det. Når du har identifisert alle enhetene på nettverket ditt, må du forsikre deg om at alle er sikre. Den beste måten å gjøre dette på, er å forsikre deg om at de alltid kjører siste versjon av operativsystemet/fastvaren. Sørg alltid for at automatisk oppdatering er aktivert når det er mulig. Sørg for at du bruker et unikt, sterkt passord på alle enheter som krever passord. Til slutt bør du besøke nettsiden til internettleverandøren din, siden det kan være mulig at de tilbyr gratis verktøy til hjelp med å sikre hjemmenettverket ditt.

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

Passordsetninger:	https://securingthehuman.sans.org/ouch/2015#april2015
Passordhåndterere:	https://securingthehuman.sans.org/ouch/2015#october2015
Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016
Kartlegg hjemmenettverket ditt:	http://l.rud.is/home-network-mapping

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