OUCH! | May 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Tingenes internett (IoT)
- Problemer med IoT
- Hvordan beskytte dine IoT-enheter?

Tingenes internett

Hva er tingenes internett (IoT)

Før var teknologi ganske enkelt, du koblet datamaskinen til internett, og utførte dine daglige gjøremål. Så utviklet teknologien seg, og mobile enheter, som smarttelefoner og nettbrett, ble en del av livene våre. Med slike enheter har du så å si egenskapene til en stasjonær datamaskin i lommen. De er langt mer mobile, og samtidig brakte de med seg sine egne, unike sikkerhetsutfordringer. Det neste store tekniske fremskrittet er tingenes internet. Tingenes internett, som på engelsk kalles Internet of Things og ofte forkortes IoT, vil si at hverdagslige gjenstander som for eksempel ringeklokker, lyspærer, barneleker og termostater kobles til internett. Dette kan gjøre livene våre mye enklere – for eksempel ved å få lysene til å slå seg på automatisk når mobilen din merker at du nærmer deg hjemmet. IoT-markedet beveger seg fremover med stormskritt, nye produkter dukker opp hver uke. Men akkurat som mobile enheter, kommer IoT-enheter med sine egne unike sikkerhetsproblemer. I dette nyhetsbrevet skal vi hjelpe deg med å forstå hva disse risikoene er, og hva du kan gjøre for å sikre dine IoT-enheter, hjemmet ditt, og dermed også familien din.

Gjesteredaktør

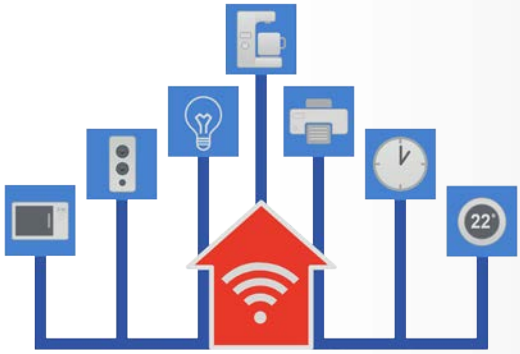
James Lyne (@jameslyne) er global leder for sikkerhetsforskning i sikkerhetsfirmaet Sophos. Han er en selverklært "massiv nerd", og de tekniske ferdighetene hans dekker mange områder innen sikkerhet. Han er en sertifisert instruktør ved SANS-instituttet, og holder ofte presentasjoner på industri-konferanser.

Problemer med IoT

Styrken til IoT er at de fleste av disse enhetene er enkle. For eksempel kan du bare plugge inn kaffemaskinen din, så vil den be om å få koble til det trådløse nettverket ditt. Men, all denne enkelheten har sin pris. Det største problemet med IoT-enheter er at mange av selskapene som lager dem ikke har noen erfaring med sikkerhet, kun med produksjon av husholdningsgjenstander. Eller så er de kanskje et oppstartfirma som prøver å utvikle produkter så effektivt og raskt som mulig. Slike organisasjoner har fokuset sitt på profitt, ikke cybersikkerhet. Som et resultat av dette har mange IoT-enheter i dag lite eller ingen innebygd sikkerhet. For eksempel har noen av dem velkjente standardpassord, som kanskje til og med finnes lagt ut på internett, og som ikke kan endres. I tillegg er det mange av disse enhetene som ikke kan konfigureres, slik at man blir nødt til å bruke dem med fabrikkinnstillingene. Og hva verre er: Mange av disse enhetene er vanskelige

Tingenes internett

og oppdatere, kanskje det ikke engang er mulig. Som et resultat kan mange av IoT-enhetene du bruker raskt bli utdaterte, med kjente sårbarheter som ikke lar seg fikse, slik at du havner i en permanent sårbar tilstand.



Vit hvilke IoT-enheter som er tilkoblet ditt nettverk. Isoler dem om mulig, hold dem oppdatert, og beskytt dem med sterke passordsetninger.

Hvordan beskytte dine IoT-enheter?

Så hva kan du gjøre? Vi ønsker selvfølgelig at du skal kunne utnytte fordelene med IoT-enheter både sikkert og effektivt. Disse dingsene tilbyr fantastiske muligheter som kan gjøre livet ditt enklere, spare deg for utgifter, og muligens forbedre den fysiske sikkerheten i hjemmet ditt. I tillegg er det mulig at du blir nødt til å ta i bruk teknologien før eller siden. Her er noen enkle grep du kan ta for å beskytte IoT-enhetene dine og deg selv:

- **Koble til kun det du trenger**: Den enkleste måten å sikre en IoT-enhet på er å ikke koble den til internett. Derfor er det lurt å ikke koble enheten til nettverket med mindre du har behov for at den skal være online.
- **Separert Wi-Fi nettverk**: Hvis du har behov for at IoT-enhetene dine skal være på nett, bør du vurdere å opprette et eget separat Wi-Fi nettverk kun for dem. På mange Wi-Fi aksesspunkter har man mulighet til å opprette ekstra nettverk, som et gjestenettverk. En annen løsning er å kjøpe et nytt aksesspunkt til bruk kun for IoT-enhetene. Dette vil holde IoT-enhetene isolert på et eget nettverk, og da kan de ikke brukes til å skade eller angripe datamaskiner eller mobiler som er tilkoblet det primære hjemmenettverket ditt (hvilket fremdeles er hovedinteressen til cyberkriminelle).
- **Oppdater hvis mulig**: Å holde IoT-enhetene sine oppdatert er like viktig som med PC-er og mobile enheter. Skru på automatisk oppdatering hvis det er en mulighet på IoT-enheten.
- **Sterke passord**: Endre passordet på IoT-enheten til et unikt, sterkt passord som bare du kjenner til. Klarer du ikke å huske alle passordene dine? Slapp av, det klarer ikke vi heller. Derfor bør du vurdere å ta i bruk en passordhåndterer for å lagre dem alle på en sikker måte.
- **Personvern**: Om det er mulig å konfigurere personverninnstillinger på IoT-enheten, burde du benytte det av det til å begrense hvor mye informasjon den deler. En mulighet er å slå helt av enhver mulighet til å dele, slik at den ikke deler noe.

Tingenes internett

- **Bytte ut enheten**: Etter hvert kan det være at IoT-enheten din har for mange kjente sårbarheter som ikke kan fikses, eller det kan være det er kommet ut nye enheter som har mye mer sikkerhet innebygd. Da bør du vurdere å bytte ut den gamle enheten din.

Hvilke enheter som passer til hvem er forskjellig, så vurder å sette deg inn i hva som er best praksis og se etter publikasjoner om sikring av enhetene du har. Dessverre blir de færreste IoT-enheter utviklet med sikkerhet i tankene, så mange produsenter har derfor lite sikkerhetsinformasjon og tilby. Men etter hvert som bevissthet rundt cybersikkerhet vokser, håper vi å se at flere og flere produsenter bygger sikkerhet inn i enhetene og gir god informasjon om hvordan man beskytter dem og holder dem oppdatert.

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
Slik sikrer du hjemmenettverket ditt:	https://securingthehuman.sans.org/ouch/2016#february2016

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