OUCH! | August 2018

OUCH!

SANS SECURITY AWARENESS

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

Smarthus-enheter

Hva er smarthus?

Før var det kun et fåtall av de digitale enhetene hjemme som kunne koble seg på nett, f.eks. laptop, smarttelefon, eller spillkonsoll. Nå om dagen er det imidlertid fler og fler ting som kan koble seg på nett, alt fra lyspærer og høyttalere til TV-er, dørlåser, og til og med bilen din. Snart vil nesten alle tingene i huset kunne ha internettilgang. Slike gjenstander med internettilgang går ofte under navnet tingenes internett (forkortes IoT pga. Internet of Things på engelsk), eller smarthus-enheter. Disse tingene er ofte svært praktiske og forenklende, men de bringer også med seg unike farer.

Hva er problemet?

Jo flere enheter som er tilkoblet hjemmenettverket ditt, jo mer kan gå galt. Hackere kan programmere enhetene dine til å angripe andre, produsenter kan samle inn store mengder informasjon om dine aktiviteter, og enheten kan bli infisert og låse deg ute. Mange av selskapene som lager slike gjenstander har ingen erfaring med cybersikkerhet og ser kun på sikkerhet som en kostnad. Som et resultat av det, har mange av internett-tingene som er til salgs lite eller ingen innebygd sikkerhet. For eksempel har mange enheter kjente standardpassord, eller det kan være umulig å oppdatere eller konfigurere dem.

Hvordan beskytter jeg meg selv?

Så hva kan du gjøre? Vi vil definitivt at du skal dra nytte av internett-ting, på en trygg og sikker måte. Disse tingene kan ha stor nytteverdi og gjøre livet ditt mye enklere. Og etter hvert som teknologien utvikler seg kan det være at du ikke har noe annet valg enn å ta i bruk smarthus-enheter og tingenes internett. Her er nøkkelgrepene du kan ta for å beskytte deg:

Koble kun til det du trenger: Det enkleste tiltaket for å sikre en smarthus-enhet er å ikke koble den til nettet. Om du ikke trenger at den er på nett, ikke koble den til det trådløse nettverket ditt. Har du virkelig behov for at en brødrister skal sende meldinger til mobilen din?

Vit hva du har tilkoblet: Hvilke gjenstander i hjemmet ditt er koblet på nett? Er du usikker, eller husker du ikke? Skru av det trådløse nettet og se hva som slutter å virke. Det avslører kanskje ikke alt, men du blir nok overasket over hvor mange ting du glemte.

Oppdater: Akkurat som med datamaskinen og mobilen er det kritisk at du holder alle enheter, også smarthus-enheter, oppdatert. Aktiver automatiske oppdateringer dersom det er mulig.

Passord: Endre passordene på smarthus-enhetene og internett-tingene til en unik, sterk passordsetning som kun du vet. Sannsynligvis må du kun skrive dem inn én gang for hver enhet. Sliter du med å huske alle passordene? Det gjør vi også. Vurder derfor å bruke et passordhvelv - et program som lagrer alle passordene på en trygg og sikker måte.

Personverninnstillinger: Dersom enheten gjør det mulig for deg å justere personverninnstillingene, burde du begrense mengden informasjon den samler inn og sender videre. En mulighet kan ganske enkelt være å slå av all innsamling.

Produsenten: Kjøp gjenstandene fra en produsent du kjenner til og stoler på. Se etter produkter med innebygd sikkerhet, slik som automatiske oppdateringer, mulighet til å endre standardpassord, og konfigurering av innstillinger.

Lytter alltid: Dersom en enhet tar imot stemmekommandoer lytter den alltid. For eksempel kan Alexa- og Google Home-enheter ta opp sensitive samtaler. Ta det med i betraktningen når du velger hvor i hjemmet du plasserer en slik enhet, og se gjennom personverninnstillingene.

Gjestenettverk: Vurder å koble smarthus-enheter og internett-ting til et separat trådløst nett for gjester, heller enn å koble dem til det primære trådløsnettet som du bruker med datamaskiner og mobiler. På denne måten er enhetene på hovednettverket ditt mye tryggere dersom en av de smarte gjenstandene skulle bli infisert.

Det er ingen grunn til å være redd for nye teknologier, men vær klar over mulige risikoer. Ved å ta disse få enkle grepene kan du få et langt sikrere smarthus.

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.

Gjesteredaktør

Robert M. Lee *(@RobertMLee) er sertifisert SANS-instruktør og forfatter av kurset FOR578 – Cyber Threat Intelligence og ICS515 – ICS Active Defence and Incident Response. Robert er også direktør og grunnlegger for cybersikkerhetsfirmaet Dragos.*

Ressurser

Passordsetninger:	https://www.sans.org/u/GEB
Passordhvelv:	https://www.sans.org/u/GEG
Slik sikrer du hjemmenettverket ditt:	https://www.sans.org/u/GEL