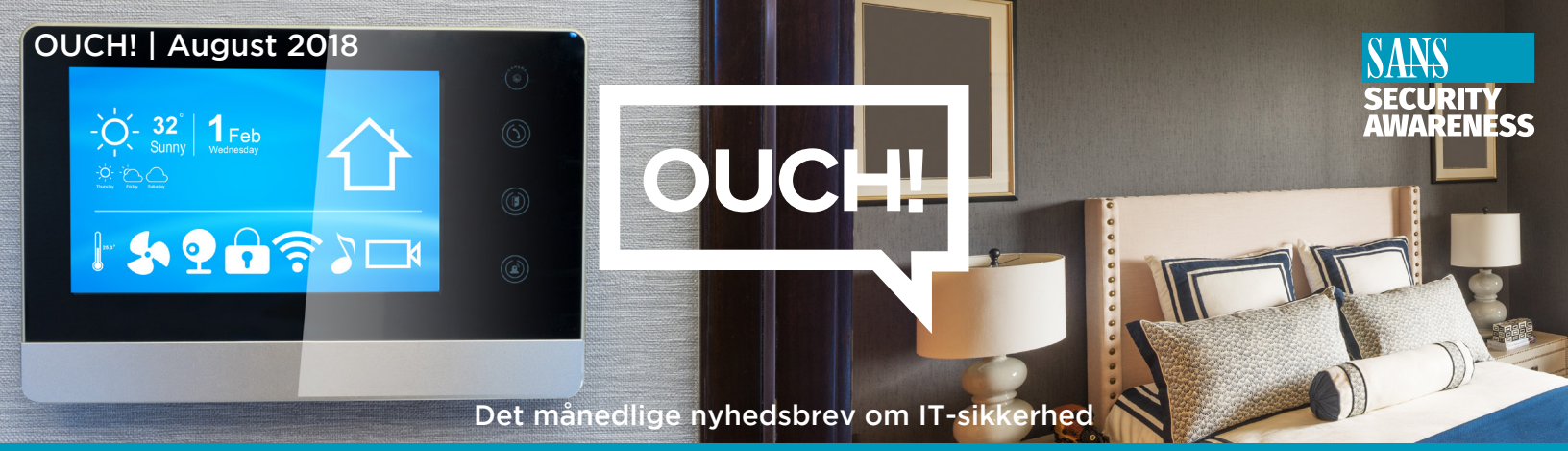
OUCH! | August 2018



OUCH!

SANS SECURITY AWARENESS

Det månedlige nyhedsbrev om IT-sikkerhed

Smart Home-enheder

Hvad er Smart Home-enheder?

Traditionelt kan kun få af dine enheder derhjemme forbindes til internettet, f.eks. din bærbare computer, smartphone eller spillekonsol. Men i dag forbindes flere og flere enheder til internettet, fra din lyspærer og højttalere til dit tv, dørlås eller endda din bil. Snart vil næsten alle enheder i dit hus være forbundet med internettet. Disse tilsluttede enheder går ofte under navnet "Internet of Things" (IoT) eller Smart Home-enheder. Mens det giver mange fordele og muligheder at tilslutte disse enheder til internettet udgør de også en IT-sikkerhedsrisiko.

Hvad er problemet?

Jo flere enheder der er forbundet til dit netværk, jo flere steder kan det gå galt. Hackere kan programmere dine enheder til at angribe andre, leverandører kan indsamle omfattende information om dine aktiviteter, eller dine enheder kan blive inficeret og låse dig ud. Mange af de virksomheder, der fremstiller enhederne, har ingen erfaring med IT-sikkerhed og ser kun sikkerhed som en udgift. Som følge heraf har mange af de enheder, du køber, lidt eller ingen sikkerhed indbygget i dem. For eksempel har nogle enheder standard adgangskoder, der er velkendte, eller måske kan du ikke opdatere eller konfigurere dem.

Hvordan kan jeg beskytte mig selv?

Så hvad kan du gøre? Vi vil anbefale dig at udnytte de mange muligheder, men du skal gøre det uden at gå på kompromis med IT-sikkerheden. Disse enheder kan gøre dit liv enklere og desuden, som teknologien udvikler sig, har du måske ikke andet valg end at bruge smarte enheder. Her er ting du kan gøre, for at beskytte dig selv.

Tilslut kun det, du har brug for: Det sikreste er ikke at forbinde enhederne til internettet. Hvis du ikke behøver at have din enhed til at være online, skal du ikke oprette forbindelse til dit Wi-Fi-netværk. Har du virkelig brug for at din brødrister, der sender dig beskeder til din telefon?

Hold styr på, hvad du har tilsluttet: Hvilke enheder har du tilsluttet dit hjemmenetværk? Er du ikke sikker eller kan du ikke huske det? Sluk dit trådløse netværk og se, hvad der ikke længere fungerer. Det kan ikke fange alt, men du vil blive overrasket over, hvor mange enheder du har glemt.

Opdateringer: Ligesom du husker at opdatere din computer og mobilenheder er det vigtigt at holde alle dine andre enheder opdaterede. Hvis din enhed har mulighed for automatisk at opdatere, skal du aktivere det.

Adgangskoder: Skift adgangskoderne på dine enheder til en unik, stærk adgangskode, som kun du kender. Du skal højst sandsynligt kun indtaste dem en gang. Kan du ikke huske alle dine adgangskoder? Bare rolig, det kan vi heller ikke. Overvej at bruge en "password manager" til sikkert at gemme dem alle sammen.

Beskyttelse af privatliv: Hvis din enhed giver dig mulighed for at konfigurere privatlivets indstillinger, kan du begrænse mængden af oplysninger, som den indsamler eller deler. En mulighed er at deaktivere enhver form for informationsdeling.

Leverandør: Køb dine enheder fra firmaer, som du kender og stoler på. Kig efter produkter, der understøtter IT-sikkerhed principper, som f.eks. automatisk opdatering, muligheden for at skifte adgangskoder og konfiguration af privatlivets indstillinger.

Lytter den med?: Hvis en enhed kan tage imod dine talekommandoer, lytter den konstant. For eksempel kan dine Alexa og Google Home-enheder optage følsomme samtaler. Overvej det, når du bestemmer, hvor du skal placere enhederne i dit hjem og gennemgå privatlivets indstillingerne.

Gæstenetværk: Overvej at sætte dine enheder på et separat "Gæste" WiFi-netværk i stedet for det primære WiFi-netværk, du bruger til dine computere og mobile enheder. På denne måde forbliver dine computere eller mobile enheder på dit primære netværk sikre, hvis en smart enhed bliver inficeret.

Der er ingen grund til at være bange for de nye teknologier, men du skal forstå hvilke risici de udgør. Ved at gøre disse få ting kan du hjælpe med at skabe et langt mere sikkert Smart Home.

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.

Gæsteredaktør

Robert M. Lee *(@RobertMLee) er certificeret SANS-instruktør og forfatter af FOR578 "Cyber Threat Intelligence" og ICS515 "ICS Active Defense and Incident Response". Robert er også direktør og grundlægger af det industrielle IT-sikkerhedsfirma Dragos.*

Hvis du vil vide mere

Passphrases:	https://www.sans.org/u/GEB
Password Managers:	https://www.sans.org/u/GEG
Securing Your Home Network:	https://www.sans.org/u/GEL