OUCH! | Maj 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Hvad er "Internet of Things (IoT)"?
- Problemer med IoT
- Sådan beskytter du dine IoT enheder

Internet of Things (IoT)

Hvad er "Internet of Things (IoT)"?

Før i tiden var teknologien simpel, man koblede sin computer på internettet og brugte det til sine daglige aktiviteter. Teknologien udviklede sig, og der kom flere mobile enheder ind i vores dagligdag. Med smartphones og tablets kan man have computerkraft svarende til en bærbar computer i lommen. Disse enheder er lette at tage med på farten og har dermed deres helt egne sikkerhedsproblemer.

Gæsteredaktør

James Lyne (**@jameslyne**) er "global head of security research" ved sikkerhedsfirmaet Sophos. Han er selvudnævnt "stor nørd" på mange forskellige områder, og hans tekniske viden om sikkerhed er meget bred. Han er certificeret instruktør ved SANS Institute, og er ofte hovedtaler ved sikkerhedskonferencer.

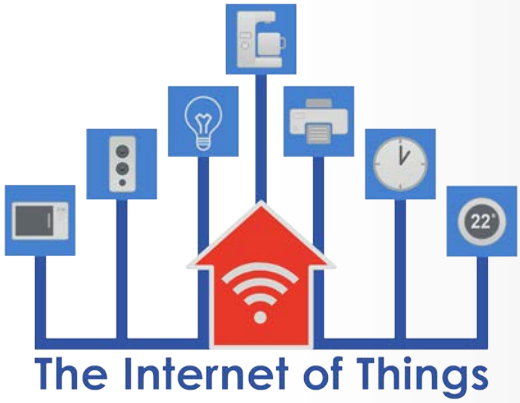
Det nyeste teknologiske fremskridt er "Internet of Things", som ofte forkortes IoT. IoT handler om at få de ting, man bruger i hverdagen, koblet til internettet. IoT enheder dækker over alt fra ringeklokker og pærer til dukker og termostater. At koble disse ting på nettet kan gøre vores hverdag meget lettere. Man kan eksempelvis få tændt lys i hjemmet, når man kommer hjem, blot fordi telefonen registrerer, at man er hjemme. IoT markedet udvikler sig med forbløffende hastighed, og der dukker nye apparater op hver uge. Men, ligesom de mobile enheder, har IoT enheder deres egne udfordringer til IT-sikkerhed. Dette nyhedsbrev vil hjælpe dig til at forstå disse risici, og hvad du kan gøre for at sikre dine IoT enheder, dit hjem og i sidste ende din familie.

Problemer med IoT

Styrken ved IoT er, at de fleste apparater er lette at sætte op. Eksempelvis skal du blot sætte din kaffemaskine i stikkontakten, og den beder om at få adgang til dit trådløse netværk. Men man betaler en pris for den simple opsætning. De fleste virksomheder, der fremstiller IoT enheder, har ekspertise i fremstilling af apparater til husholdningen. Til gengæld har disse virksomheder ofte ingen erfaring med IT sikkerhed. Det kan også være en opstartsvirksomhed, der prøver at udvikle et produkt hurtigt og billigt - eksempelvis gennem Kickstarter. Disse virksomheder har fokus på profit ikke på IT-sikkerhed. Dette resulterer i, at mange af de IoT enheder man køber i dag har lidt, eller slet ingen, IT-sikkerhed. Mange af enhederne har standard adgangskoder som er kendte, eller som man kan finde på internettet - og som ikke kan ændres. Oveni dette har man ved mange af disse enheder ingen mulighed for at konfigurere dem.

Internet of Things (IoT)

Det betyder at man hænger på de indstillinger, de kom med. For at gøre sagen værre er det svært at opdatere enhederne, hvis det overhovedet er muligt. Uden mulighed for opdateringer vil din IoT enhed hurtigt bliver forældet og kommer til at have kendte sikkerhedshuller som ikke kan rettes. Hvis først et sikkerhedshul er udnyttet af IT-kriminelle, forbliver du permanent sårbar.



Hold øje med hvilke IoT enheder du har på dit netværk, opret et separate netværk til dem hvis det er muligt, hold dem opdaterede og beskyt dem med sikre kodeord.

Sådan beskytter du dine IoT enheder

Hvad kan man så gøre? Vi vil opfordre dig til at udnytte mulighederne i IoT enheder på en sikker og effektiv måde. Disse produkter har fantastiske muligheder, der kan gøre dit liv lettere, spare penge og muligvis øge den fysiske sikkerhed i dit hjem. Som teknologien udvikles, er det desuden muligt, at du ikke kan vælge mellem at købe et produkt der er en del af IoT eller ej. Her er nogle forholdsregler du kan tage for at beskytte dine IoT enheder og dig selv:

- **Opkoble kun enheden på Internettet, hvis der er nødvendigt**: Den letteste måde at sikre dine IoT enheder på, er at undlade at koble det på Internettet.
- **Flere separate trådløse netværk**: Hvis du gerne vil have dine IoT enheder på nettet, bør du overveje at bruge et separate trådløst netværk til dem. På de fleste trådløse netværk har man mulighed for at lave flere separate netværk såsom et gæstenetværk. En anden mulighed er at købe et ekstra trådløst netværk, som du kun bruger til IoT enheder. Dette holder dine IoT enheder på et isoleret netværk, og disse enheder kan ikke blive brugt til at angribe din computer eller mobile enheder på dit primære netværk. Det er stadig adgangen til din computer eller mobile enheder, der har den største interesse hos IT-kriminelle.
- **Opdater**: Ligesom man skal holde sin PC og mobile enheder opdaterede skal man huske at opdatere sine IoT enheder. Hvis din IoT enhed har muligheden for automatisk opdatering anbefales det, at du slår denne funktion til.
- **Sikre adgangskoder**: Når du får din IoT enhed, skal du ændre adgangskoden til et sikkert kodeord, som kun du kender. Kan du ikke huske alle disse koder? Overvej at bruge en ”password manager” til sikkert at opbevare dem alle.

Internet of Things (IoT)

- **Privatindstillinger**: Hvis du har mulighed for at konfigurere dine privatindstillinger på dine IoT enheder så sørg for at dele så lidt information som muligt. En mulighed er at slå delingen af informationer fra.
- **Udskift**: På et tidspunkt vil din IoT enhed have for mange usikkerheder, der ikke kan rettes. Når dette sker bør du overveje at udskifte enheden. De nyere udgaver af enhederne har som regel et højere sikkerhedsniveau.

Der findes desværre ikke en standardløsningen, der passer til alle IoT enheder. Hvis man vil vi sikre sine enheder, kan det godt betale sig at finde ud af hvad god skik på området er og læse sikkerhedsvejledningerne der følger med enheden. Uheldigvis er det de færreste IoT enheder, der er udviklet med øje for IT-sikkerhed, så der er ikke mange producenter der har information om enhedernes IT-sikkerhed. Men bevidstheden om IT-sikkerhed vokser og vi håber på, at flere IoT-sælgere indlejrer IT-sikkerhed i deres produkter og giver mere information om, hvordan man skal beskytte og opdatere dem.

Hvis du vil vide mere

På http://www.securingthehuman.org kan du tilmelde dig det månedlige nyhedsbrev om IT-sikkerhed fra OUCH! Her kan du ligeledes få adgang til ældre udgaver af OUCH! og læse mere om SANS IT-sikkerhedsløsninger

WelcomeSecurity samarbejder med netop din virksomhed og med 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 http://www.welcomesecurity.net.

Tidligere udgivelser (ikke oversat til dansk)

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Securing Your Home Network:	https://securingthehuman.sans.org/ouch/2016#february2016

Licensinformation

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity