OUCH! | Oktober 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Dig selv
- Passphrase og to-trins-bekræftelse
- Opdateringer
- Backup

Fire gode råd om sikker brug af computere

Overblik

Efterhånden som teknologien spiller en større og større rolle i vores liv, vokser kompleksiteten. Teknologien ændrer sig så hurtigt, at det kan være svært at være opdateret på alle sikkerhedsanbefalingerne. Det virker som om, der hele tiden er nye retningslinjer for, hvad man bør og ikke bør gøre. Selvom detaljerne i IT-sikkerhed ændres med tiden, er der nogle grundlæggende forholdsregler, du altid kan tage for at beskytte dig selv. Uanset hvilken teknologi du bruger, og uanset hvilken sammenhæng du bruger teknologien i, vil vi anbefale, at du følger disse fire råd. Referencer til yderligere information om disse råd, findes nederst i dette nyhedsbrev.

Gæsteredaktør

Ryan Johnson fokuserer på at sikre, at organisationer er klar til at reagere på det uundgåelige sikkerhedsbrud. Han underviser i Advanced Network Forensics på SANS Institute. Du kan følge Ryan på Twitter som **@ForensicRJ**.

1. **Dig selv**: Vigtigst af alt, er at huske, at teknologi ikke kan stå alene når det kommer til at beskytte dig. IT-kriminelle har fundet ud, af at den letteste måde at bryde den mest komplicerede IT-sikkerhed er gennem dig. Den nemmeste måde at få fat i dit password, bankinformationer eller personlige oplysninger er ved at snyde dig til at give dem informationerne. De kan for eksempel ringe til dig og udgive sig for at være teknisk support fra Microsoft, og forsøge at bilde dig ind, at din computer er angrebet. I virkeligheden er det IT-kriminelle, der vil have adgang til din computer. En anden måde er at sende dig en e-mail og forklare, at en pakke ikke kan leveres og bede dig klikke på et link, for at bekræfte din adresse. I virkeligheden leder de dig videre til en ondsindet hjemmeside, der hacker din computer. Det er på denne måde ransomware og CEO svindel starter. I sidste ende er du det bedste forsvar mod IT-kriminelle. Vær opmærksom. Ved at bruge din sunde fornuft kan du genkende og stoppe de fleste angreb.

2. **Passphrases og to-trins-bekræftelse**: Det næste gode råd til at beskytte dig selv er at bruge et stærkt

© SANS Institute 2016

Fire gode råd om sikker brug af computere

og unikt password til hver af dine enheder og online konti. Et stærkt password er et, der ikke er let at gætte for hackere eller deres programmer. Hvis du er træt af komplekse passwords, der er svære at huske eller skrive, kan du overveje at bruge hele sætninger, eksempelvis ”Hvor er min kaffe?”. Dette kaldes en passphrase. Jo længere sætning du bruger, des stærkere er din passphrase. Et unikt password betyder, at du bruger forskellige passwords til forskellige enheder og online konti. Hvis et af dine passwords bliver gættet, vil alle de andre enheder og konti stadig være sikre. Hvis du er bange for, at du ikke kan huske alle disse passwords, kan du bruge en password manager. En password manager er en applikation til din smartphone eller computer, som gemmer alle dine passwords beskyttet.

Ved at følge disse fire råd er du godt beskyttet mens du udnytter de nyeste teknologier.

Et andet vigtigt råd til at beskytte din konto er to-trins-bekræftelse. Passwords er ikke længere nok til at beskytte dine konti, der er brug for noget stærkere og to-trins-bekræftelse er meget stærkere. Du skal stadig bruge dit password, men du skal også bruge noget mere, enten noget biometrisk (eksempelvis fingeraftryk) eller noget som kun du har (eksempelvis en kode der sendes til din smartphone). Brug denne mulighed på alle konti, også din password manager. To-trins-bekræftelse er måske det vigtigste råd i forhold til at beskytte dig selv, og det er lettere end du tror.

3. **Opdatering**: Sørg for at dine computere, mobile enheder, apps og alt andet der er koblet til internettet bruger den nyeste version af softwaren. IT-kriminelle leder hele tiden efter sårbarheder i det software, dine enheder bruger. Når de finder sårbarheder, bruger de specielle programmer til at udnytte og hacke sig ind på de enheder, du bruger. Det er et kapløb med de firmaer, der har udviklet softwaren og som kæmper for at lukke sårbarhederne ved at udgive opdateringer. Ved at installere disse opdateringer på din computer og dine mobile enheder gør du det meget sværere at hacke dig. Dette gælder også for TV, babyalarmer, trådløse routere, spilkonsoller og alt andet, der er forbundet til internettet. De fleste enheder giver mulighed for at opdatere automatisk, hvis du

© SANS Institute 2016

Fire gode råd om sikker brug af computere

slår denne mulighed til, kan du gøre det hele meget lettere for dig selv. Hvis der ikke længere ydes support med sikkerhedsopdateringer på dine enheder, er anbefalingen at du udskifter dem.

4. **Backup**: Ligegyldig hvor forsigtig du er, er der altid en risiko for at du bliver hacket. Hvis det sker, er den eneste mulighed ofte at installere alt forfra på din computer eller mobile enhed. Hvis du er rigtig uheldig, har den IT-kriminelle spærret din adgang til dine personlige filer, billeder og andet. Ofte er den eneste mulighed at gendanne det hele fra backup. Vær sikker på at du jævnligt tager backup af vigtige ting og sikrer at du kan genskabe dem. De flest operativsystemer og mobile enheder giver mulighed for automatisk backup. Vi anbefaler desuden at du gemmer din backup ude i skyen eller offline for at beskytte dem mod IT-kriminelle.

Hvis du vil vide mere

På securingthehuman.sans.org/ouch/archives 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 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.

Tidligere udgivelser (ikke oversat til dansk)

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
Two-Step Verification (oversat til dansk):	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015

Licensinformation

OUCH! er udgivet af SANS Securing The Human og distribueres under Creative Commons BY-NC-ND 3.0 licensen. Du er velkommen til at videregive dette nyhedsbrev eller bruge det i dit eget arbejde med IT-sikkerhed så længe du ikke ændrer i nyhedsbrevet. Hvis du har spørgsmål til oversættelsen eller andet er du velkommen til at kontakte ouch@securingthehuman.org.

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

© SANS Institute 2016