OUCH! | Juni 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Hvad er kryptering?**
- **Hvad kan du kryptere?**
- **Hvordan gør du det rigtigt?**

Kryptering

Hvad er kryptering?

Du har måske hørt folk tale om kryptering, og hvordan du bør bruge det til at beskytte dig selv og dine informationer. Men at kryptere kan være forvirrende, og du skal forstå begrænsningerne ved kryptering. I dette nyhedsbrev vil vi forklare, hvad kryptering er, hvordan det kan beskytte dig, og hvordan du implementerer det korrekt.

Gæsteredaktør

Francesca Bosco (**@francibosco**) er forsker og administrerer projekter indenfor IT-kriminalitet, IT-sikkerhed og misbrug af teknologi. Hun arbejder ved FNs "Interregional Crime and Justice Research Institute" og er medstifter af "Tech and Law Center".

Du har enormt meget følsomt data på dine enheder, det drejer sig bland andet om personlige dokumenter, billeder og e-mails. Hvis du mister en af dine enheder eller får den stjålet, vil den, der har din enhed, have adgang til alle disse personfølsomme informationer. Oveni dette udveksler du følsomme oplysninger, når du benytter dig af netbank og online handel. Hvis der er nogen, der overvåger disse aktiviteter, kan de stjæle dine informationer. Det kunne være dit kontonummer eller dit kreditkortnummer. Kryptering vil beskytte dig i disse situationer ved at sikre, at uautoriserede personer ikke kan få adgang til at læse eller ændre dine informationer.

Kryptering har eksisteret i flere tusinde år. I dag er kryptering meget sofistikeret, men det tjener det samme formål – at få en hemmelig besked sikkert fra et sted til et andet. Kryptering sikrer, at det kun er den rette modtager, der kan læse beskeden. Når information ikke er krypteret, kaldes det klartekst. Når information sendes som klartekst, kan alle let kan få adgang til informationen. Kryptering konverterer informationen til et ikke-læseligt format, som man kalder cipher-tekst. Moderne kryptering bruger komplekse matematiske operationer og en unik nøgle til at konvertere din klartekst til cipher-tekst. Nøglen er det, der låser dine informationer og låser dem op. I de fleste tilfælde er din nøgle et password

Hvad kan du kryptere?

Der er helt generelt to typer data man kan kryptere, data i hvile (for eksempel, data der er gemt på din mobile enhed) og data i bevægelse (Eksempelvis, din e-mail mens den bevæger sig igennem Internettet).

Kryptering

Kryptering af data i hvile er vigtigt i forhold til at beskytte dine informationer i tilfælde af, at du mister din mobile enhed, eller hvis den bliver stjålet. Moderne enheder indeholder enormt meget information, men er også meget lette at miste. Desuden er der andre typer mobile enheder, eksempelvis et USB-stik eller en ekstern harddisk, der kan indeholde følsom information. ”Full Disk Kryptering” (FDE) er en velbenyttet metode til at kryptere hele disken. Dette betyder, at alt på din maskine automatisk bliver krypteret, og du behøver ikke tage stilling til, hvad der skal krypteres, og hvad der ikke skal. I dag kommer de fleste computere med FDE, men du skal selv slå det til. På Mac computere hedder det FileVault, mens du på Windows computere kan bruge Bitlocker eller Device Encryption. De fleste mobile enheder understøtter også FDE. iOS på iPhones og iPads slår automatisk FDE til, når først en adgangskode er blevet sat. Fra Android 6.0, Marshmallow, sætter Google FDE som standard, hvis maskine opfylder visse minimums krav.

Kryptering er en god måde at sikre dine informationer, men din kryptering er aldrig stærkere end din nøgle.

Informationen er også sårbar, når den bliver overført fra en enhed til en anden. Hvis data ikke er krypteret, kan de blive overvåget, ændret og opfanget online. Det er derfor vigtigt, at du sikrer alle følsomme transaktioner, der foregår online. En normal måde at gøre dette på er HTTPS. Hvis en hjemmeside bruger HTTPS betyder det, at al trafik mellem din browser og hjemmesiden er krypteret. Du kan genkende en hjemmeside der bruger HTTPS kryptering på, at der er et ikon af en lås i din browser, eller ved at URL’en bliver grøn. E-mails er et andet eksempel på informationer det er muligt at kryptere. De fleste mail klienter indeholder muligheden for at kryptere dine beskeder, du skal blot slå det til. Et tredje og sidste eksempet er kryptering af chat-beskeder. Apps som iMessage, Wickr, Signal, WatsAppe og Telegram bruger en form for kryptering, som forhindrer en tredjepart i at få adgang til data, mens de bliver overført fra en enhed til en anden. Det betyder, at det kun er den person du kommunikerer med, der kan se, hvad du har sendt

Hvordan gør du det rigtigt?

Hvis du vil være sikker på, at du er beskyttet når du bruger kryptering, er det altafgørende, at du gør det korrekt

- Din kryptering er ikke stærkere end din krypteringsnøgle. Hvis nogen gætter dit password eller får adgang til din nøgle, vil de have adgang til den data, du forsøger at beskytte. Beskyt din nøgle. Hvis du bruger et

Kryptering

password, skal du være sikker på, at det er et stærkt og unikt password. Jo længere dit password er, des sværere er det for en hacker at gætte det eller knække det. Du må endelig ikke glemme dit password, uden din nøgle kan du heller ikke selv få adgang til dine informationer. Hvis du ikke kan huske alle dine passwords, anbefaler vi, at du bruger en password manager

- Din kryptering er ikke stærkere end sikkerheden på dine enheder. Hvis din enhed er blevet kompromitteret, eller er blevet inficeret med malware kan IT-kriminelle omgå din kryptering. Derfor er det vigtig, at du sørger for at beskytte dine enheder ved bl.a. at bruge anti-virusprogrammer, stærke passwords og holde enhederne opdaterede.
- Mange apps til mobiltelefoner og applikationer til computer tilbyder en stærk kryptering til at beskytte dine data og din kommunikation. Hvis den app eller den applikation du overvejer at benytte dig af ikke tilbyder kryptering, bør du overveje et alternativ.

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 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)

Forklaring af hvad kryptering er:	http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What Is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016

Licensinformation

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

