OUCH! | December 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Dine informationer**
- **Sådan sletter du sikkert informationerne fra dine enheder**
- **SIM- og hukommelseskort**

Sikker bortskaffelse af mobile enheder

Overblik

Mobile enheder, eksempelvis smartphone, smart watches og tablets, udvikles og nytænkes i en rasende fart, derfor er der personer, der udskifter disse enheder hvert år. Uheldigvis er der ikke mange, der tænker over hvor mange personlige oplysninger, der er på dem. I dette nyhedsbrev vil vi forklare hvilke oplysninger, der er på de mobile enheder, og hvordan man sikkert kan fjerne oplysningerne, før man smider dem væk eller returnerer dem. Hvis du har fået din telefon af din arbejdsgiver, eller hvis der er arbejdsrelaterede oplysninger på den, skal du kontakte deres IT afdeling og få styr på procedurer for backup og bortskaffelse, før du følger nedenstående råd.

Gæsteredaktør

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) er "Principal Forensic Scientist" leder af forensics ved ManTech CARD. Hun er leder og medforfatter til SANS Institute kurset "Advanced Smartphone Forensics (FOR585)" og underviser på "Windows Forensic Analysis (FOR408)". Hendes blog findes på **smarterforensics.com**.

Dine oplysninger

Mobile enheder indeholder ofte flere følsomme informationer, end du er klar over - der er ofte flere informationer på din telefon end på din computer. Den type information kan blandt andet være:

- Hvor du bor, arbejder og hvilke steder du ofte besøger.
- Kontakt informationer på alle i din adressebog.
- Hvilke telefonopkald du har foretaget, hvem der har ringet til dig og hvilke telefonopkald, du er gået glip af.
- Dine beskeder (SMS, voice og MMS).
- Dine chat i forskellige apps, spil og sociale medier.
- Hvor du har været baseret på informationer fra GPS eller sendemaster.
- Hvilke hjemmesider du har besøgt, din søgehistorik, cookies og cachede sider.
- Billeder, video, lydfiler og e-mails.
- Gemte kodeord og adgang til dine personlige konti eksempelvis din mobilbank eller e-mail
- Adgang til billeder, filer og informationer gemt i "Skyen".
- Informationer om dit helbred eksempelvis din alder, puls, blodtryk og diæt

Sikker bortskaffelse af mobile enheder

Sådan sletter du sikkert informationerne fra dine enheder

Som du kan se, er der mange følsomme informationer på dine mobile enheder. Uanset hvordan du vælger at skaffe dig af med dine enheder, om du bytter den for en ny, donerer den til velgørenhed, giver den til et familiemedlem eller smider den ud, er det vigtigt, at du først sletter alt følsom information. Du ved det måske ikke, men at slette data er ikke så let. Hvis du bare sletter det, er det let at genskabe det med programmer, man kan finde på internettet. Hvis du skal lave en sikker sletning af dine data, skal du overskrive dine data, så de ikke kan genskabes. Dette kaldes ”wiping”. Før du sletter dine data, er det en god ide at lave en backup, så du lettere kan få din nye enhed til at fungere.

Når du vil bortskaffe din mobile enhed skal du fabriksnulstille den og fjerne SIM-kort og SD-kort.

Den letteste metode til sikkert at slette informationer fra dine enheder er, at benytte sig af muligheden for at fabriksnulstille. Hvis man gør det, vil enheden have de samme informationer, som da den blev købt. Vi har fundet ud af, at denne metode er den sikreste og letteste metode til at fjerne data fra dine mobile enheder. Hvordan man gør, er forskelligt for de forskellige enheder. Herunder er nævnt hvordan man gør for to populære enheder.

- Apple iOS Enheder: Indstillinger | Generel | Nulstil | Slet alt indhold og indstillinger
- Android Enheder: Indstillinger |Personlige |Sikkerhedskopiering og nulstilling |Gendannelse af fabriksdata | Nulstil

Desværre er det ikke lige så let at fjerne personlige informationer fra en Windows telefon. Vi er ved at lave yderligere undersøgelser for at finde metoder der fjerner al information fra enheden. Hvis du stadig har spørgsmål om, hvordan du fabriksnulstiller din telefon skal du læse manualen til enheden eller lede på producentens hjemmeside. Husk på, at det ikke er nok bare at slette dine personlige informationer, de er lette at genskabe.

SIM-kort og eksterne kort

Udover den information der er på din enhed, skal du også overveje hvad du vil gøre ved dit SIM-kort (Subscriber Identity Module). SIM-kortet er det, den mobile enhed bruger til at lave et opkald eller oprette en dataforbindelse. Når du fabriksnulstiller din enhed indeholder SIM-kortet stadig informationer om dig og er knyttet til dig som bruger. Hvis du skifter til en anden enhed men beholder dit telefonnummer, skal du kontakte din udbyder og få overført dit SIM-kort. Hvis

Sikker bortskaffelse af mobile enheder

dette ikke er muligt, eksempelvis fordi din nye telefon bruger en andet størrelse SIM-kort, skal du beholde dit gamle SIM-kort og fysisk ødelægge det, for at forhindre nogen fra at genbruge det.

Der er desuden nogle mobile enheder, der bruger separate SD-kort (Secure Digital) til ekstra lagerplads. Disse SD-kort indeholder ofte billeder, applikationer og andet følsomt data. Husk at fjerne alle SD-kort fra din enhed, før du smider den ud (i nogle enheder er SD-kortet gemt sammen med batteriet). Disse kort kan ofte genbruges i en nyere enhed eller bruges som ekstra hukommelse på din computer, hvis du køber en USB-adapter. Hvis det ikke er muligt at genbruge dit SD-kort anbefaler vi, at du fysisk ødelægger det.

Hvis du er i tvivl om nogle af de ting, der er gennemgået i dette nyhedsbrev, skal du henvende dig i den butik, hvor du købte din enhed og få hjælp fra en tekniker. Hvis du vil smide din mobile enhed ud bør du i stedet overveje at donere den til en velgørende organisation.

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)

Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
Backup and Recovery:	https://securingthehuman.sans.org/ouch/2015#august2015
Advanced Smartphone Forensics Course:	https://sans.org/for585
OUCH Newsletter Archives:	https://securingthehuman.sans.org/ouch/archives

Licensinformation

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

