OUCH! | December 2016

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Sikker avhending av mobile enheter

Oversikt

Mobile enheter som smarttelefoner, smartklokker, og nettbrett fortsetter å utvikle seg og innovere med en forbløffende fart. Det resulterer i at enkelte bytter mobile enheter så ofte som hvert år. Dessverre kvitter altfor mange seg med enhetene sine uten å tenke over hvor mye personlig data det faktisk finnes på dem. I dette nyhetsbrevet går vi over hva slags personlig informasjon som finnes på den mobile enheten din, og hvordan du fjerner det fullstendig før du leverer den inn. Dersom du har din mobile enhet i forbindelse med jobben, eller hvis den har arbeidsrelatert innhold på seg, bør du forhøre deg med lederen din angående riktige prosesser for sikkerhetskopiering og avhending før du følger stegene beskrevet under.

Gjesteredaktør

Heather Mahalik (**@HeatherMahalik**; **+HMahalik**) er Principal Forensic Scientist, og leder etterforskningsinnsatsen ved ManTech CARD. Hun er kursleder og medforfatter av SANS instituttets kurs Advanced Smartphone Forensics (FOR585) og instruktør for Windows Forensics Analysis (FOR408). Hun blogger på **smarterforensics.com**.

Din informasjon

Mobile enheter lagrer langt mer sensitiv informasjon enn du er klar over, ofte mer enn datamaskinen din gjør. Typiske eksempler er

- Hvor du bor, hvor du jobber, og steder du ofte besøker
- Kontaktinformasjonen for alle i adresseboken din og alle knyttet til dine applikasjoner, blant annet familie, venner og kolleger
- Anropshistorikk som blant annet innkommende, utgående og tapte anrop
- SMS (tekstmeldinger), stemme- og multimediemeldinger
- Chatteøkter fra applikasjoner som sikker chat, spill og sosiale medier
- Posisjonshistorikk basert på GPS-koordinater eller mobilmast-historikk
- Surfehistorikk for nettbruk, søkelogg, informasjonskapsler (cookies), og mellomlagrede sider
- Personlige bilder, videoer, lydopptak og e-poster
- Lagrede passord og tilgang til personlige brukerkontoer, som nettbanken din eller e-postkontoen din
- Tilgang til bilder, filer eller annen informasjon lagret i Skyen
- Helserelatert informasjon, som alder, puls, blodtrykk eller diett

Sikker avhending av mobile enheter

Renske enheten

Som du kan se er det sannsynligvis en enorm mengde sensitiv informasjon på din mobile enhet. Uavhengig av hvordan du kvitter deg med den, uansett om du donerer den, bytter den med en ny, gir den bort til et familiemedlem, selger den eller bare kaster den, må du være sikker på at du først har rensket den for sensitiv informasjon. Du er kanskje ikke klar over det, men det å slette data er ikke nok. Det kan bli gjenopprettet med enkelthet kun ved bruk av gratis verktøy tilgjengelig fra internett. Istedenfor må du fjerne all informasjonen på enheten på en sikker måte. Dette gjøres ved å overskrive filene før sletting, og dermed gjøre dem umulig å gjenopprette. Husk å ta sikkerhetskopi før slettingen, på denne måten kan du gjenoppbygge enheten med enkelhet.

Gjør en fabrikk-tilbakestilling og fjern eventuelle SIM- og SD-kort om du skal kvitte deg med din mobile enhet.

Den enkleste måten å gjennomføre en sikker sletting av informasjonen på enheten din, er å bruke innstillingen for "tilbakestilling til fabrikkstandard". Dette vil tilbakestille enheten til den tilstanden den var i når du kjøpte den. Vi har funnet ut at fabrikk-tilbakestilling er den sikreste og enkleste metoden for å fjerne data fra din mobile enhet. Denne funksjonen varierer fra enhet til enhet, under finner du stegene for de to vanligste enhetstypene.

- Apple iOS-enheter: Settings | General | Reset | Erase All Content and Settings
- Android-enheter: Settings | Privacy | Factory Data Reset

Dessverre kan ikke personlig informasjon fjernes fra Windows Phone såpass enkelt, grundigere undersøkelser blir for tiden gjort for å finne metoder som sikrer fullstendig og endelig sletting av personlig informasjon fra enheten. Dersom du fortsatt lurer på hvordan tilbestilling til fabrikkstandard gjennomføres, kan du sjekke bruksanvisningen eller produsentens nettside. Husk at å bare slette data ikke er nok, da det enkelt kan gjenopprettes.

SIM & lagringskort

I tillegg til dataene lagret på enheten, må du også vurdere hva du skal gjøre med SIM-kortet ditt. Et SIM-kort er det en mobil enhet bruker for å koble til mobil-nettverket for å ringe og bruke mobildata. Når du gjennomfører en tilbakestilling til fabrikkstandard, vil informasjon om brukerkontoen knyttet til deg som bruker forbli på SIM-kortet. Dersom du beholder samme mobilnummer når du bytter enhet, kan du forhøre deg om muligheten til å ganske enkelt fortsette å bruke det samme SIM-kortet. Om dette ikke er mulig, f.eks. dersom den nye mobilen bruker en annen type SIM-kort, bør du beholde det gamle SIM-kortet og fysisk makulere eller ødelegge det, for å hindre at noen andre kan gjenbruke det.

Sikker avhending av mobile enheter

Noen mobile enheter bruker også et uttakbart SD-kort for ekstra lagringsplass. Disse lagringskortene inneholder ofte bilder, mobilapplikasjoner, og annet sensitivt innhold. Husk å fjerne eventuelle eksterne lagringskort fra den mobile enheten før du kvitter deg med den (på noen enheter er SD-kortet skjult i batterikammeret, f.eks. under batteriet). Disse kortene kan ofte bli gjenbrukt i nye mobile enheter, eller kan brukes som generiske lagringsenheter på datamaskinen din ved hjelp av en USB-adapter. Dersom gjenbruk av SD-kortet ikke er mulig, så anbefaler vi at du fysisk ødelegger det, akkurat som med SIM-kort som ikke kan gjenbrukes.

Dersom du er usikker på noen av disse stegene kan du ta med den mobile enheten din til butikken du kjøpte den i, og få hjelp av en opplært teknikker. Til slutt, dersom du planlegger å kaste den mobile enheten din, ber vi deg om å vurdere å donere den istedenfor. Det finnes mange flotte veldedige organisasjoner som tar imot brukte mobile enheter.

Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Ressurser

Slik sikrer du ditt nye nettbrett:	https://securingthehuman.sans.org/ouch/2016#january2016
Sikkerhetskopiering & gjenoppretning:	https://securingthehuman.sans.org/ouch/2015#august2015
Kurset Advanced Smartphone Forensics:	https://sans.org/for585
OUCH-nyhetsbrevets arkiv:	https://securingthehuman.sans.org/ouch/archives

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS

