Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Din personlige informasjon
- Sikker sletting av informasjon
- SIM- og SD-kort

Avhende mobile enheter

Oversikt

Mobile enheter, som smarttelefoner og nettbrett, utvikler og innoverer seg i usedvanlig høy fart. Dette betyr at mange av oss bytter telefon, så ofte som hver 18. måned. Dessverre så er det mange som kvitter seg med telefonen uten å tenke over hvor mye personlig informasjon de har lagret på enheten. I dette nyhetsbrevet vil vi gå gjennom hva slags personlig informasjon kan være lagret på enheten og hvordan du kan sikkert slette denne dataen før du avhender eller leverer den inn. Hvis den mobile enheten ble gitt ut av arbeidsgiver eller inneholder intern virksomhetsinformasjon, må du sørge for at du sjekker med overordnet angående sikkerhetskopi og avhendingsprosedyrer før du følger stegene under.

Gjesteredaktør

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) er en konsulent som holder til i Washington, DC. Han er hovedforfatter av SANS-kurset Mobile Device Security and Ethical Hacking (SEC575) og forfatter av SANS-kurset Incident Response Team Management (MGT535).

Din personlige informasjon

Mobile enheter har mye mer sensitiv informasjon enn du kanskje tror, sannsynligvis mer enn datamaskinen. Typisk informasjon, som du kan finne på mobile enheter er:

- Hvor du bor, jobber og steder du ofte besøker.
- Kontaktdetaljer for alle i adresseboka, inkludert familie, venner og kollegaer.
- Anropslogg, inkludert innkommende, utgående og tapte anrop.
- Tekst- og talemeldinger.
- Chat-meldinger i applikasjoner, som spill og sosiale medier.
- Lokasjonshistorikk basert på GPS koordinater eller mobilmaster.
- Nettleserhistorikk, informasjonskapsler (cookies) og bufrede nettsider.
- Personlige bilder, videoer, lydopptak og epost.
- Lagrede passord og tilgang til personlige kontoer som mobilbank eller epost.
- Tilgang til bilder, filer eller annen informasjon lagret i skyen.
- Helserelatert informasjon, som puls, blodtrykk eller diett.

© The SANS Institute 2014

Avhende mobile enheter

Sikker sletting av informasjon

Som du ser, så finnes det ufattelig mye sensitiv informasjon på mobile enheter. Uansett hvordan du avhender enheten, enten du donere den bort, gir den til et familiemedlem, selger den igjen eller kaster den bort; du må først sørge for at du sletter all sensitiv informasjon. Du trenger også å slette informasjonen hvis du returnerer telefonen eller bytter den ut med en annen telefon. Hvis du ikke gjør det, kan den som ender opp med telefonen lett få tilgang til all denne informasjonen. Før du begynner å slette må du sannsynligvis ta en sikkerhetskopi av all informasjonen, dette inkluderer bilder, videoer etc. Etter at du har slettet informasjonen, så vil det ikke være mulig å hente ut noen av dataene igjen.

Når du avhender mobile enheter, sørg for at du gjenoppretter til fabrikkinnstillinger og fjerner SIM- og SD-kort hvis det er aktuelt.

Etter at du har tatt sikkerhetskopi av dataene må du slette de på en sikker måte. Trykke "slett" inne i de aktuelle programmene er ikke godt nok. Data slettet på denne måten kan enkelt hentes ut med gratis verktøy. Du må i stedet bruke en metode som overskriver dataene, ikke bare frigjør plass, på engelsk kalles dette ofte "wiping". Den letteste måten å gjøre dette på er ved å bruke enhetens funksjon for "factory reset", eller "gjenopprett fabrikkinnstillinger". Dette vil returnere telefonen til samme stand som når den var først kjøpt. Vi har funnet ut at "gjenopprett fabrikkinnstillinger" er den enkleste og sikreste metoden for å slette data fra mobile enheter. Hvordan man bruker denne funksjonen, varierer fra enhet til enhet, under er beskrivelser for de tre mest populære enhetene:

- Apple iOS enheter: Innstillinger | Generelt | Nullstill | Slett alt innhold og alle innstillinger
- Android enheter: Innstillinger | Privat | Tilbakestilling | Fabrikkinnstillinger
- Windows Phone enheter: Innstillinger | Om | Tilbakestill mobilen

Hvis du fortsatt har spørsmål om hvordan du kan gå tilbake til fabrikkinnstillinger, sjekk eiermanualen eller leverandørens hjemmesider. Husk at sletting av dataene ikke er nok, de kan lett gjenopprettes.

SIM- og SD-kort

I tillegg til dataene lagret på enheten, må du også vurdere hva du skal gjøre med SIM-kort (Subscriber Identity Module). SIM-kort er det mobilen bruker for å opprette en telefonsamtale eller datatilkobling. Når du gjenoppretter til fabrikkinnstillinger, vil SIM-kortet beholde informasjon om din konto. Hvis du beholder telefonnummeret og bytter til

© The SANS Institute 2014

Avhende mobile enheter

en ny enhet, kan du snakke med selger angående overføring av SIM-kortet. Hvis dette ikke er mulig, for eksempel hvis den nye telefonen bruker et annerledes SIM-kort, burde du beholde det gamle kortet og fysisk ødelegge det. Da forhindrer du at andre kan bruke det.

Til slutt, noen mobile enheter bruker et separat SD-kort (Secure Digital) for ekstra lagringsplass. Disse kortene inneholder ofte bilder, applikasjoner og annen sensitiv data. Husk å fjerne disse kortene fra enheten før du avhender enheten (for noen enheter kan dette kortet være gjemt, muligens under batteriet). Disse kortene kan ofte gjenbrukes i den nye mobile enheten, eller så kan det bli brukt som et generelt lagringsmedium til datamaskinen. Hvis gjenbruk ikke er aktuelt, så er det best å fysisk ødelegge det.

Hvis du er usikker på noen av stegene i dette nyhetsbrevet, ta med enheten til butikken du kjøpte den for å få hjelp fra en opplært tekniker. Til slutt, hvis du planlegger å kaste vekk mobilen uansett, så spør vi om at du donerer den i stedet. Det er mange veldedige organisasjoner som tar imot mobile enheter.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

NIST SP800-88 Rev. 1:	http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
OUCH! Sikkerhetskopi:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#september2013
NorSIS om sikker sletting:	https://norsis.no/2013/12/sikker-sletting/

OUCH! utgis av SANS Securing The Human og er distribuert under Creative Commons BY-NC-ND 3.0 lisens.
Du kan fritt distribuere dette nyhetsbrevet eller bruke det i dine bevissthetsprogrammer, så lenge du ikke endrer nyhetsbrevet.
For å oversette eller mer informasjon, vennligst kontakt ouch@securingthehuman.org.

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis