OUCH! | August 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva skal man sikkerhetskopiere og når
- Hvordan ta sikkerhetskopiering
- Gjenoppretning
- Viktige punkter

Sikkerhetskopiering & gjenoppretning

Bakgrunn

Før eller senere vil det mest sannsynlig gå noe galt og du vil miste dine personlige filer, dokumenter eller bilder. Eksempler på dette er sletting av feil filer ved et uhell, maskinvarefeil, tap av bærbar PC eller infisering av datamaskinen. I situasjoner som dette er sikkerhetskopiering ofte den eneste måten du kan gjenoppbygge ditt digitale liv. I dette nyhetsbrevet forklarer vi hva sikkerhetskopiering er, hvordan du kan ta sikkerhetskopiering av dataen din og utvikle en strategi som passer for deg.

Gjesteredaktør

Heather Mahalik er en anerkjent digital etterforskningsekspert i bransjen, som fokuserer på smarttelefon etterforskning. Hun er medforfatter i boken «Practical Mobile Forensics», teknisk redaktør i «Learning Android Forensics» og medforfatter på «FOR585 Advanced Smartphone Forensics» og «FOR518 Macintosh Forensics» for SANS Instituttet. Følg Heather på **Smarterforesnics.com** og på Twitter: **@heathermahalik**.

Hva skal man sikkerhetskopiere og når

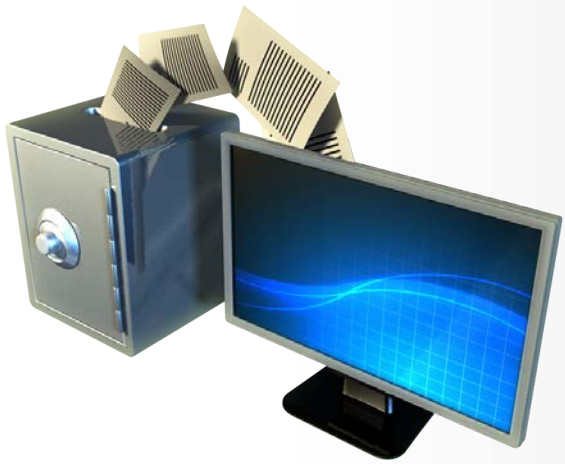
Sikkerhetskopier er kopier av din informasjon som blir lagret et annet sted. Når du mister viktig data, kan du gjenopprette denne dataen fra sikkerhetskopien. Problemet er at de fleste personer gjennomfører ikke sikkerhetskopieringer, noe som er veldig synd fordi det kan både være enkelt og billig. Det finnes to fremgangsmåter for å bestemme hva du skal ta sikkerhetskopi av: (1) spesifikke data som er viktigst for deg; eller (2) alt, inklusivt hele operativsystemet ditt. Den første fremgangsmåten effektiviserer sikkerhetskopiene dine og sparer harddiskplass, men den andre fremgangsmåten er enklere og mer fullstendig. Hvis du er usikker på hva du skal ta sikkerhetskopi av, så anbefaler vi å ta kopi av alt.

Det neste valget du må ta er hvor ofte det skal skje en sikkerhetskopi av dataen din. Vanlige alternativer inkluderer hver time, daglig, ukentlig, osv. For hjemmebruk gjør personlige sikkerhetskopieringsprogrammer som Apples Time Machine eller Microsofts Sikkerhetskopiering og gjenoppretting det mulig for deg å lage en automatisk «sett det på og glem det»-sikkerhetskopieringstidsplan. Disse løsningene tar stille sikkerhetskopi av dataene din gjennom hele dagen mens du jobber på eller vekk fra datamaskinen din. Andre løsninger tilbyr «kontinuerlig beskyttelse» der nye eller endrede filer blir umiddelbart kopiert så fort de blir lukket. Som et minimum anbefaler vi at du tar daglige sikkerhetskopieringer. Til syvende og sist, spørsmålet du bør stille deg er: «Hvor mye informasjon har jeg råd til å miste hvis jeg måtte gjenopprette fra sikkerhetskopien?»

Sikkerhetskopiering & gjenoppretning

Hvordan ta sikkerhetskopi

Det er to måter å ta sikkerhetskopi av dataene dine på: fysiske medier eller sky-basert lagring. Fysiske medier er hvilket som helst type maskinvare, for eksempel DVD-er, USB-disker eller eksterne harddisker. Uavhengig av hvilket media du skulle velge, ta aldri sikkerhetskopi av filene dine på samme enhet hvor originalene blir lagret. Problemet med fysiske medier er at hvis det skjer en hendelse på lokasjonen din (som brann eller tyveri) så kan du ikke bare miste datamaskinen men sikkerhetskopiene også. Derfor burde du ha en plan for lagring av sikkerhetskopiene utenfor området på en sikker lokasjon. Hvis du lagrer dem på et annet sted, sørg for å merke dem med hva som var sikkerhetskopiert og når. For ekstra sikkerhet, krypter sikkerhetskopiene dine.



Automatiserte, pålitelige sikkerhetskopier er ofte den siste sikkerhetsbarriere i beskyttelsen av din data.

Sky-baserte løsninger er annerledes, dette er en tjeneste hvor dine filer blir lagret et annet sted på Internettet. Avhengig av hvor mye data du ønsker å sikkerhetskopiere kan dette være en betalingsløsning. Dette fungerer ved å installere et program på din datamaskin som automatisk kopierer filene dine for deg. Fordelen med denne løsningen er at siden sikkerhetskopiene er i skyen og det skjer en hendelse i hjemmet ditt, så er sikkerhetskopiene fortsatt trygge. I tillegg så kan du få tilgang til sikkerhetskopiene, eller ofte kun enkeltfiler, fra nesten hvor som helst, selv når du reiser. Ulempen med skybaserte sikkerhetskopier (og gjenoppretning) er at de kan være tregere, særlig hvis du har store mengder data. Hvis du er usikker på hvilken sikkerhetskopiløsning som er den beste for deg (fysisk eller sky-basert) husk at du kan alltids benytte begge løsninger.

Og til slutt, ikke glem dine mobilenheter. Fordelen med mobilenheter er at mesteparten av dataene din blir allerede lagret i skyen, som for eksempel eposten din, kalenderhendelser eller kontakter. Men du kan ha informasjon som ikke er lagret i skyen, som konfigurasjonene til dine mobilapp-er, nylige bilder og systeminnstillinger. Ved å kopiere dine mobilenheter, så bevarer du ikke bare denne informasjonen men det er også lettere å gjenbygge en enhet, som for eksempel når du oppgraderer til en ny mobil. En iPhone/iPad kan sikkerhetskopiere automatisk til Apples iCloud. Android eller andre mobilenheter er avhengige av produsenten eller tjenesteleverandøren. I noen tilfeller må du kjøpe mobilapp-er som er utviklet spesifikt for sikkerhetskopiering.

Gjenoppretning

Kopiering av dataene din er bare halve kampen; du må være sikker på at du kan gjenopprette det. Sjekk hver måned at dine sikkerhetskopier fungerer ved å gjenopprette en fil og sjekke innholdet. I tillegg, sørg for å ta en fullstendig

Sikkerhetskopiering & gjenoppretning

sikkerhetskopi av systemet før en større oppgradering (som flytting til en ny datamaskin eller mobilenhet) eller en større reparasjon (som erstatning av harddisk) og sjekk at det er mulig å gjenopprette kopien.

Viktige punkter

- Automatiser sikkerhetskopieringen så langt det er mulig og sjekk dem jevnlig.
- Ved gjenbygging av hele systemer fra sikkerhetskopien, sørg for at du reinstallerer de siste sikkerhetsoppdateringer før du bruker det igjen.
- Utdaterte eller foreldede sikkerhetskopier kan bli en belastning, og bør ødelegges for å hindre at uautoriserte brukere får tilgang.
- Hvis du bruker en sky-basert løsning, undersøk prosedyrene og omdømmet til leverandører og sørg for at de oppfyller dine krav. For eksempel, krypterer de dataene dine når den blir lagret? Hvem har tilgang til dine sikkerhetskopier? Støtter de robust autentisering som to-stegs verifisering?

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

Passordsetninger:	http://www.securingthehuman.org/ouch/2015#april2015
To-steg verifisering:	http://www.securingthehuman.org/ouch/2013#august2013
Bruke nettskyen sikkert:	http://www.securingthehuman.org/ouch/2014#september2014
Kryptering:	http://www.securingthehuman.org/ouch/2014#august2014
Dagens tips:	http://www.sans.org/tip_of_the_day.php

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