OUCH! | August 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Sikkerhetskopiering: Hva, når og hvordan**
- **Gjenoppretting**
- **Nøkkelpoenger**

Sikkerhetskopiering og gjenoppretting

Oversikt

Om du bruker datamaskinen eller en mobil enhet lenge nok, vil noe før eller siden gå galt, og forårsake tap av personlige filer, dokumenter, eller bilder. Du kan for eksempel komme til skade for å slette feil fil, harddisken kan krasje, enheten kan bli borte, eller den kan bli infisert med skadevare som løsepengevirus. I slike tider er sikkerhetskopi ofte den eneste måten man kan gjenoppbygge sitt digitale liv. I dette nyhetsbrevet forklarer vi hva sikkerhetskopier er, hvordan man sikkerhetskopierer data, og hvordan du kan utvikle en enkel strategi for det som passer for deg.

Gjesteredaktør

Keith Palmgren er en cybersikkerhetsprofesjonell med over 30 års erfaring i IT-sikkerhetsfeltet. Han er seniorinstruktør hos SANS, og forfatter for kurset SANS SEC301; "Introduksjon til informasjonssikkerhet." Keith driver en suksessfull virksomhet som sikkerhetskonsulent, og er å finne på Twitter: **@kpalmgren**

Sikkerhetskopiering: Hva når og hvordan

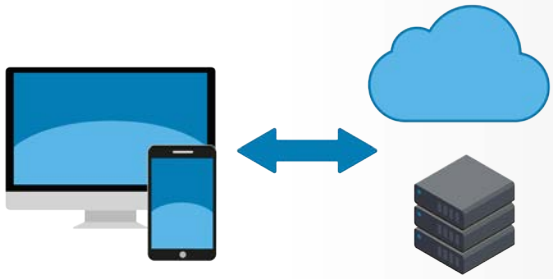
Sikkerhetskopier er kopier av informasjonen din som er lagret separat fra datamaskinen din, eller den mobile enheten. Når du mister verdifull data, kan du gjenopprette den fra sikkerhetskopien. Dessverre er det altfor mange som ikke tar jevnlige sikkerhetskopier, selv om det er veldig enkelt og koster lite eller ingenting. Det første steget er å bestemme seg for hva du skal sikkerhetskopiere. Det finnes to måter å tilnærme det seg på: (1) sikkerhetskopier kun spesifikk data som er viktig for deg; eller (2) alt, inkludert hele operativsystemet. Mange sikkerhetskopieringsløsninger er som standard satt opp til å bruke den første muligheten, de sikkerhetskopierer bare de mest brukte mappene. I mange tilfeller vil det være alt du trenger. Men dersom du ikke er sikker på hva du vil sikkerhetskopiere, eller vil være ekstra forsiktig, sikkerhetskopier alt.

For det andre må du bestemme deg for hvor ofte du vil sikkerhetskopiere. Innebygde sikkerhetskopieringsløsninger som Apples Time Machine eller Microsoft Windows Backup and Restore lar deg sette en automatisk tidsplan for sikkerhetskopiering. Vanlige innstillinger her inkluderer en gang i timen, daglig, ukentlig, osv. Andre løsninger tilbyr "kontinuerlig beskyttelse", hvor nye og endrede filer blir sikkerhetskopiert øyeblikkelig etter at du lagrer dokumentet. Som et minimum anbefaler vi automatisk daglig sikkerhetskopiering.

Til sist må du bestemme deg for hvordan du skal sikkerhetskopiere. Det er to måter å gjøre det på: Fysiske lagringsmedier, eller skylagring. Hver av dem har fordeler og ulemper. Om du er usikker, kan du godt bruke begge. Fysiske lagringsmedier er enheter du selv kontrollerer, som eksterne USB-disker eller nettverksdisker tilgjengelig på det trådløse nettet. Fordelen med å bruke dine egne fysiske lagringsenheter, er at det lar deg kopiere og gjenopprette store mengder data relativt

Sikkerhetskopiering og gjenoppretting

raskt. Ulempen er at dersom du blir infisert med skadevare som løsepengevirus, er det mulig at infeksjonen kan spre seg til sikkerhetskopien din. Også om du blir rammet av en katastrofe som brann eller tyveri, kan det resultere i at både datamaskinen og sikkerhetskopien går tapt. Om du bruker en fysisk lagringsenhet til sikkerhetskopiering, burde du derfor lagre en kopi av denne på et helt annet, sikkert sted. Sørg for at sikkerhetskopier du lagrer på et annet sted er tilstrekkelig merket.



Automatiserte, pålitelige sikkerhetskopier er ofte din siste skanse i forsvaret av dine data.

Skylagring er internettbaserte tjenester som lagrer filene dine på nettet. Som vanlig installerer du en applikasjon på datamaskinen din. Applikasjonen din sikkerhetskopierer automatisk filene dine enten etter et tidsskjema, eller ettersom du endrer dem. Fordelen med skylagring er at det er så enkelt, sikkerhetskopieringen er som oftest automatisk, og du kan som regel få tilgang til filene fra hvor som helst. I tillegg, siden dataene er lagret i skyen, vil de ikke bli påvirket av for eksempel brann eller tyveri som rammer hjemmet. Sist men ikke minst kan skylagret sikkerhetskopi være til hjelp med å gjenopprette data etter et løsepengevirusangrep, ettersom mange skyløsninger lar deg gjenopprette filer fra tidligere tidspunkter. Ulempen er at det kan ta lang tid å sikkerhetskopiere eller gjenopprette store mengder data. I tillegg er personvern og sikkerhet viktig. Tilbyr leverandøren sterk sikkerhet som kryptering av dataene dine, og to-trinns bekreftelse ved innlogging?

Og ikke glem de mobile enhetene dine. Med mobile enheter er mye data som for eksempel e-post, kalenderoppføringer, og kontakter, allerede lagret i nettskyen. App-konfigurasjonene, nylige bilder, og systempreferanser er imidlertid sjelden lagret i skyen. Ved å sikkerhetskopiere din mobile enhet vil du ikke bare sikre denne informasjonen, men det vil være lettere å overføre den når du får en ny enhet. En iPhone/iPad kan sikkerhetskopiere automatisk til Apples iCloud. Med Android og andre typer enheter avhenger det av produsenten. I enkelte tilfeller kan det være nødvendig å kjøpe en mobilapp laget spesielt for å sikkerhetskopiere.

Gjenoppretting

Å ta sikkerhetskopi er bare halve poenget, du må også forsikre deg om at du kan gjenopprette. Sjekk jevnlig at sikkerhetskopieringen fungerer ved å gjenopprette en fil, og kontroller at det er den samme som originalen. Sørg også får å ta en fullstendig sikkerhetskopi av hele systemet før en større oppgradering (som for eksempel å bytte til en ny datamaskin eller mobil enhet), eller en større reparasjon (som å bytte harddisk), og sørg for at du kan gjenopprette fra den.

Sikkerhetskopiering og gjenoppretting

Nøkkelpoenger

- Uansett hva slags løsning du benytter for å sikkerhetskopiere, bør du sørge for at det skjer automatisk, og sjekk også sikkerhetskopiene jevnlig.
- Når du gjenoppretter et system fra en sikkerhetskopi må du huske å installere alle de nyeste sikkerhetsoppdateringene som kom ut i mellomtiden før du tar i bruk systemet igjen.
- Utdaterte sikkerhetskopier som det ikke lenger er behov for er bare til bry, destruer dem for å forhindre at uvedkomne får tilgang til dem.
- Om du bruker en skyløsning, bør du undersøke policyene og ryktet til leverandøren for å forsikre deg om at de møter dine standarder. For eksempel, krypterer de dataene dine? Støtter de sterke innloggingssystemer som to-trinns bekreftelse?

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

Passordsetninger:	https://securingthehuman.sans.org/ouch/2017#april2017
Totrinns pålogging:	https://securingthehuman.sans.org/ouch/2015#september2015
Sikker bruk av nettskyen:	https://securingthehuman.sans.org/ouch/2016#november2016
Kryptering:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS