OUCH! | August 2017

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- **Backup: Hvad, hvornår og hvordan**
- **Gendannelse**
- **Centrale punkter**

# Backup og gendannelse

## Oversigt

Hvis du bruger en computer eller en mobilenhed tilstrækkeligt lang tid, vil noget før eller siden gå galt, hvilket kan resultere i tab af dine personlige filer, dokumenter eller fotos. Du kan for eksempel ved et uheld slette de forkerte filer, have en hardwarefejl, tabe en enhed eller blive smittet med skadelig software som ransomware. I disse tilfælde er backups ofte den eneste måde, du kan genopbygge dit digitale liv. I dette nyhedsbrev forklarer vi, hvad sikkerhedskopier er, hvordan du sikkerhedskopierer dine data og hvordan du udvikler en simpel strategi, der passer til dig.

### Gæsteredaktør

Keith Palmgren har over 30 års erfaring inden for IT Security. Han er "SANS Senior Instructor" og forfatteren af SANS SEC301; "Introduction to Information Security". Keith driver en vellykket virksomhed indenfor sikkerhedsrådgivning og er på Twitter: **@kpalmgren**

## Backup: Hvad, hvornår og hvordan

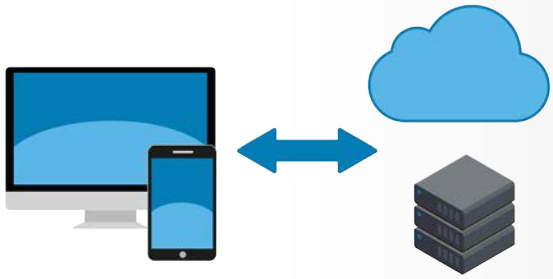
Sikkerhedskopier er kopier af dine oplysninger der er gemt et andet sted end på din computer eller mobilenhed. Når du mister værdifulde data, kan du gendanne data fra dine sikkerhedskopier. Desværre undlader for mange mennesker at lave sikkerhedskopier regelmæssigt, selvom de er enkle og billige. Det første skridt er at bestemme, hvad du vil sikkerhedskopiere. Der er to metoder: (1) specifikke data, der er vigtige for dig; Eller (2) alt, inklusive hele dit operativsystem. De fleste backup-løsninger er som standard konfigureret til at bruge den første tilgang, de sikkerhedskopierer data fra de mest brugte mapper. I mange tilfælde er det alt, hvad du behøver. Men hvis du ikke er sikker på, hvad du skal sikkerhedskopiere eller vil være ekstra forsigtig, skal du vælge at sikkerhedskopiere alt.

For det andet skal du beslutte, hvor ofte du vil sikkerhedskopiere dine data. Til personlige computere kan indbyggede sikkerhedskopieringsprogrammer som "Apples Time Machine" eller "Microsoft Window Backup and Restore" gøre det muligt at oprette en automatisk tidsplan for sikkerhedskopiering. Når man så har sat det til, behøver man ikke bekymre sig mere om det. Valgmulighederne omfatter hver time, dagligt, ugentligt osv. Andre løsninger tilbyder "kontinuerlig beskyttelse", hvor nye eller ændrede filer sikkerhedskopieres straks hver gang du gemmer et dokument. Vi anbefaler som minimum at du laver daglige sikkerhedskopier.

Endelig skal du beslutte, hvordan du vil sikkerhedskopiere. Der er to måder at sikkerhedskopiere dine data på: fysiske medier eller lagring i skyen. Hver tilgang har fordele og ulemper. Hvis du ikke er sikker på, hvilken tilgang du skal bruge, kan du bruge begge på samme tid. Fysiske medier er enheder, du styrer, såsom eksterne USB-drev eller Wi-

## Backup og gendannelse

Fi tilgængelige netværksenheder. Fordelen ved at bruge dine egne fysiske medier er, at de giver dig mulighed for at sikkerhedskopiere og gendanne store mængder data meget hurtigt. Ulempen ved en sådan tilgang er, hvis du bliver inficeret med malware, som ransomware, er det muligt for infektionen at sprede sig til dine sikkerhedskopier. Hvis du har en katastrofe, som f.eks. brand eller tyveri, kan det medføre, at du ikke kun taber din computer, men også sikkerhedskopierne. Som sådan, hvis du bruger eksterne enheder til sikkerhedskopiering, skal du have en plan om at gemme kopier af din backup på et sikkert sted som er ikke samme adresse som de enheder du har taget backup af. Sørg for, at eventuelle sikkerhedskopier, du gemmer, er korrekt mærket.



*Automatisk og pålidelig sikkerhedskopier er ofte dit sidste forsvar når du vil beskytte dine data.*

Sky-baserede løsninger er online-tjenester, der gemmer dine filer på internettet. Normalt installerer du et program på din computer. Programmet sikkerhedskopierer derefter automatisk filerne på din computer enten efter en tidsplan eller som du ændrer dem. Fordele ved løsninger i skyen er deres enkelhed, backup er næsten altid automatisk, og du kan normalt få adgang til dine filer alle steder. Da dine data befinder sig i skyen, vil katastrofer hjemme som f.eks. brand eller tyveri ikke påvirke din sikkerhedskopier. Ulempen er, at det kan tage lang tid at sikkerhedskopiere eller gendanne meget store mængder data. Privatlivet og sikkerheden er også vigtigt. Giver backup-tjenesten stærke sikkerhedskontroller, såsom kryptering af dine data og stærk validering af bruger?

Glem endelig ikke dine mobile enheder. På mobilenheder gemmes de fleste af dine data som e-mail, kalenderbegivenheder og kontakter allerede i skyen. Dine mobilappkonfigurationer, nyere fotos og systemindstillinger gemmes dog ikke altid i skyen. Ved at sikkerhedskopiere din mobilenhed bevarer du ikke kun disse oplysninger, men det er også lettere at overføre dine data, når du opgraderer til en ny enhed. En iPhone / iPad kan automatisk sikkerhedskopiere til Apples iCloud. Android eller andre mobile enheder afhænger af producenten eller serviceleverandøren. I nogle tilfælde må du muligvis købe en mobilapp, der er lavet specielt til at sikkerhedskopiere.

## Gendannelse

Sikkerhedskopiering af dine data er kun halvdelen af kampen; Du skal være sikker på, at du kan gendanne dem. Kontroller jævnligt, at dine sikkerhedskopier fungerer ved at hente en fil og validere oplysningerne. Sørg også for at lave en fuld sikkerhedskopiering af systemet før en større opgradering (som f.eks. at skifte til en ny computer eller mobilenhed) eller en større reparation (som at udskifte en harddisk) og kontrollere, at den kan genoprettes.

# Backup og gendannelse

## Centrale punkter

- Uanset hvilken løsning du bruger til at sikkerhedskopiere dine data, skal du sørge for at automatisere din sikkerhedskopiring og kontrollere den regelmæssigt.
- Når du genopbygger et system fra backup, skal du sørge for at opdatere med de nyeste sikkerhedsrettelser, inden du bruger systemet igen.
- Forældede sikkerhedskopier, der ikke længere er nødvendige udgør en risiko, og bør ødelægges for at forhindre adgang fra andre..
- Hvis du bruger en løsning i skyen, skal du undersøge leverandørens politikker og omdømme og sørge for, at de opfylder dine krav. Krypterer de dine data? Hvem har adgang til dine sikkerhedskopier? Understøtter de stærk godkendelse som totrinsbekræftelse?

## 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

Passphrases (ovesat til dansk ”Passphrases”): https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification (ovesat til dansk ”Totrinsbekræftelse”):
https://securingthehuman.sans.org/ouch/2015#september2015
Cloud Security (oversat til dansk “Hvordan burger man Skyen sikkert”):
https://securingthehuman.sans.org/ouch/2016#november2016
Encryption (oversat til dansk “Kryptering”): https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware (oversat til dansk “Ransomeware”): https://securingthehuman.sans.org/ouch/2016#august2016

## Licensinformation



Redaktion: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity

