

OUCH!

I DENNE UTGAVEN...

- Oversikt
- Valg av skyleverandør
- Sikring av data

Sikker bruk av nettskyen

Oversikt

Ordet “nettsky” kan ha forskjellige betydninger avhengig av hvem du spør, men som oftest betyr det at du bruker en tjenesteleverandør på nettet for å drifte datasystemene og dataene dine. En fordel med skyen er at du enkelt kan få tilgang til, og synkronisere data fra flere enheter overalt i verden, og du kan også enkelt dele informasjon med hvem du måtte ønske. Vi kaller slike løsninger for “nettskyen”

fordi man som oftest ikke vet nøyaktig hvor dataene er fysisk lagret. Eksempler på bruk av skytjenester er f.eks. å lage dokumenter i Google Docs, dele filer via Dropbox, sette opp en server i Amazon Cloud, lagre kundedetaljer i Salesforce, eller arkivere musikk og bilder med Apples iCloud. Disse skytjenestene kan gjøre deg mye mer produktiv, men de fører også med seg en unik risiko. I dette nyhetsbrevet skal vi gå gjennom hvordan du kan få det meste ut av nettskyen på en sikker måte.

Gjesteredaktør

Dave Shackelford ([@daveshackelford](https://twitter.com/daveshackelford)) er profesjonell konsulent og eier av Voodoo Security, og er forfatter av utallige SANS-treningskurs, inkludert SANS Security 579: Virtualisering og sikkerhet i privat sky, og Security 524: Grunnleggende skysikkerhet.

Valg av skyleverandør

Nettskyen er hverken god eller ond, den er et verktøy for å få ting gjort, både på jobb og hjemme. Men når du bruker disse tjenestene, gir du dine private data over i andres hender, og du forventer at de blir tatt hånd om slik at det er både sikkert, og tilgjengelig for deg. Derfor er det viktig at du gjør et klokt valg av skyleverandør. På jobben kan hør med din nærmeste leder og finn ut om virksomheten tillater at du bruker skytjenester. Om de gjør det, få bekreftet hvilke skytjenester du kan bruke, og hvilke policyer som gjelder for bruk av dem. Om du vurderer skytjenester til personlig bruk, ta dette til betraktning:

1. **Support:** Hvor enkelt er det å få hjelp eller svar på et spørsmål? Er det en e-postadresse man kan sende til, et offentlig forum man kan legge ut spørsmål på, eller en spørsmål & svar-side på nettsiden deres?
2. **Enkelhet:** Hvor enkelt er det å bruke tjenesten? Jo mer komplekst noe er, jo større er sannsynligheten for at du kan gjøre feil og ved et uhell lekke eller miste informasjonen din. Velg en skyleverandør du synes er enkel å forstå, konfigurere, og bruke.

Sikker bruk av nettskyen

3. **Sikkerhet:** Hva samles inn av informasjon om deg? Hvordan kommer dataene fra din maskin til skyen, og hvordan lagres de i skyen? Er de kryptert? I så fall, hvem vil kunne dekryptere dataene dine?
4. **Bruksvilkår:** Ta deg tid til å gå gjennom bruksvilkårene (ofte er de overaskende lettleste). Finn ut hvem som vil ha tilgang på dine data, og hva dine juridiske rettigheter er, samt eventuelle sikkerhetsansvarsområder leverandøren påtar seg, eller som kreves av deg.

Sikring av data

Når du har valgt en skyleverandør, bør du finne ut hvordan du skal gjøre skikkelig bruk av skytjenestene. Hvordan du aksesserer og deler dine egne data har ofte mye mer å si for sikkerheten til filene enn noe annet. Noen nøkkelgrep du kan ta inkluderer:

1. **Autentisering:** Bruk en sterk, unik passordsetning for å autentisere deg med sky-kontoen din. Om skyleverandøren din tilbyr 2-trinns bekreftelse anbefaler vi på det sterkeste at du tar i bruk det. Dette er en av de viktigste grepene du kan ta for å beskytte sky-kontoen din.
2. **Deling av filer og mapper:** Nettskyen gjør det veldig enkelt å dele, noen ganger for enkelt. I et verst tenkelig scenario kan det være at du tror at du kun deler filene dine med et spesifikt individ, men ved et uhell har du gjort filene eller kanskje hele mapper tilgjengelige for hele internettet. Den beste måten å beskytte seg på, er å ikke dele filer med noen som standard. Deretter kan man gi spesifikke individer eller grupper tilgang til spesifikke filer eller mapper etter behov. Fjern tilgangen når noen ikke lenger trenger tilgang. Skyleverandøren du velger burde gjøre det enkelt å for deg å se hvem som har tilgang til filene dine.
3. **Deling av filer og mapper med linker:** En funksjon som mange skytjenester har er muligheten til å lage linker som leder direkte til en fil eller mappe. Dette gjør det mulig å dele disse filene med noen ganske enkelt ved å gi dem linken. Det er imidlertid veldig lite sikkerhet forbundet med dette, alle som kjenner til linken har tilgang til de personlige filene. Selv om du kun sender linken til én person, kan den personen dele linken med andre, eller den kan dukke opp i søkemotorer. Når du deler informasjon ved bruk av en link, sørg for at du deaktiverer linken ved å sette en utløpsdato, eller beskytt den med et passord.



Nettskyen kan gjøre informasjonen din mer tilgjengelig og gjøre deg mer produktiv, men vær forsiktig med hvordan du behandler og deler informasjonen.

Sikker bruk av nettskyen

- 4. Innstillinger:** Det er viktig å forstå sikkerhetsinnstillingene hos skyleverandøren din. For eksempel, om du deler en mappe med en annen, vil de kunne dele den videre med andre uten at du får vite om det? Undersøk også om det er mulig å se hvem som har sett det delte innholdet ditt, og når. Har du mulighet til å begrense tilgangen til "lese" istedenfor "lese+skrive", som vil si at folk vil kunne se filene, men ikke endre på dem?
- 5. Antivirus:** Sørg for at det er oppdatert antivirus-programvare installert på datamaskinen din, og enhver annen maskin brukt til å dele filene dine. Om en fil du deler blir infisert, kan andre maskiner som har tilgang til den samme filen også bli infisert.

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

- Totrinns pålogging: <https://securingthehuman.sans.org/ouch/2015#september2015>
- Passordsetninger: <https://securingthehuman.sans.org/ouch/2015#april2015>
- Passordhåndterere: <https://securingthehuman.sans.org/ouch/2015#october2015>
- Hva er skadevare?: <https://securingthehuman.sans.org/ouch/2016#march2016>
- SEC524: Grunnleggende skysikkerhet: <https://sans.org/sec524>

OUCH! utgis av SANS Securing The Human, og er distribuert under [Creative Commons BY-NC-BD 4.0 lisensen](https://creativecommons.org/licenses/by-nc-bd/4.0/). Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på ouch@securingthehuman.org.

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



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus