OUCH! | September 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Bruke nettskyen sikkert

Oversikt

Gjesteredaktør

James og Keli Tarala (@isaudit / @kellitarala) er hovedkonsulenter hos Enclave Security og har vært forfatter av flere SANS-kurs, inkludert SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls og MGT 415: A Practical Introduction to Risk Assessments.

"Nettskyen" er en kraftig teknologi som både enkeltpersoner og organisasjoner tar i bruk. "Nettsky" kan bety forskjellige ting til forskjellige personer, generelt sett vil det bety at man bruker en tjeneste på Internettet for å lagre og prosessere dataene din for deg. En fordel med nettskyen er at du enkelt kan aksessere og synkronisere data mellom forskjellige enheter hvor som helst i verden. Du kan også dele denne informasjonen med andre. Grunnen til at vi kaller disse tjenesten nettskyen er at du ofte ikke vet hvor dataene fysisk lagres. Eksempler på tjenester vi kaller nettskyen er: Google Docs, deling av filer via Dropbox, sette opp din egen server hos Amazon Cloud eller lagring av musikk og bilder hos Apples iCloud. Disse tjenestene kan gjøre deg mer produktiv, men det tar også med seg noen unike risikoer. I dette nyhetsbrevet vil vi gå gjennom hvordan du kan benytte nettskyen sikkert.

Velge leverandør

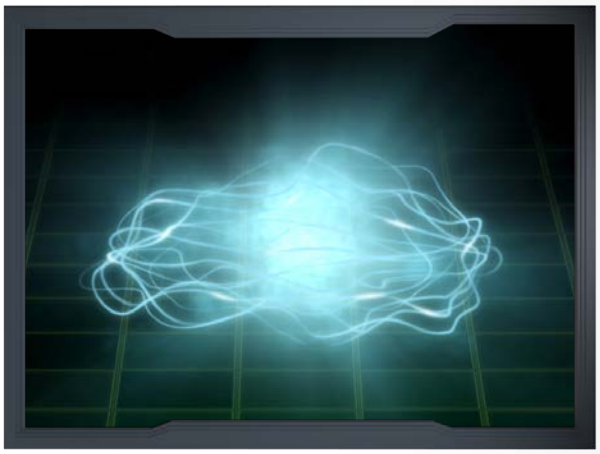
Nettsky, som en teknologi, er verken god eller dårlig, det er et verktøy for å få ting gjort, både på arbeidsplassen og privat. Likevel, når du bruker slike tjenester, så overleverer du dataene dine til fremmede og forventer at de både beskytter dataene og sørger for at de er tilgjengelig når du trenger de. Derfor er det viktig at du gjør et bra valg når du velger en skytjeneste. For arbeidsrelaterte enheter eller informasjon, sjekk med overordnet og hør om du kan bruke nettskytjenester. Hvis det er tillatt å bruke nettskytjenester, sjekk hvilke tjenester du kan bruke og hva retningslinjene er for bruk. Hvis du vurderer en nettskytjeneste for privat bruk, vurder følgende:

1. **Støtte**: Hvor enkelt er det å få hjelp eller å få spørsmål besvart? Finnes det telefonnummer du kan ringe eller e-postadresse du kan bruke? Finnes det andre muligheter for støtte, som forum eller vanlige problemsstillinger og spørsmål på deres side?
2. **Enkelhet**: Hvor enkelt er det å bruke tjenesten? Hvis tjenesten er vanskelig å bruke, så er det mer sannsynlig at

Bruke nettskyen sikkert

du begår feil og informasjonen kommer på avveier. Bruk en nettskytjeneste som du syns er enkel å forstå, konfigurere og bruke.

3. **Sikkerhet**: Hvordan blir informasjonen din overført fra din datamaskin til nettskyen, er tilkoblingen kryptert? Hvordan er dataen lagret i nettskyen, er den kryptert og hvis den er det, hvem kan dekryptere dataen?
4. **Bruksvilkår**: Gå gjennom bruksvilkårene for tjenesten (de er ofte ganske enkle å lese). Sjekk hvem som kan aksessere dataene dine og hva dine rettigheter er.



Nettskyen kan gjøre informasjonen din lettere tilgjengelig og hjelpe deg med å være mer produktiv, men vær forsiktig med hvordan du lagrer og deler informasjonen.

Sikre dine data

Etter at du har valgt en leverandør, så er neste steg å sørge for at du bruker tjenesten på en sikker måte. Hvordan du aksesserer og deler dine data kan ha en veldig stor innvirkning på sikkerheten din. Noen nøkkelpunkter du bør tenke på er:

1. **Autentisering**: Bruk et sterkt, unikt passord for autentisering til nettskykontoen. Hvis leverandøren støtter to-faktor autentisering, så er det absolutt anbefalt.
2. **Dele filer / mapper**: Nettskyen gjør det veldig enkelt å dele informasjon, noen ganger for enkelt. I verste fall gjør du filer og kanskje hele mapper tilgjengelig for alle på Internettet. Den beste måten du kan beskytte deg på er ved å ha “ikke del” som standardinnstilling. Deretter kan du dele etter hvert som det trengs. Når noen ikke lenger trenger tilgang til filene dine, så fjerner du tilgangen. Leverandøren burde tilby en lettvint måte å holde oversikt på.
3. **Dele filer / mapper ved å bruke lenker**: En vanlig funksjon hos mange tjenester er muligheten til å lage en link som peker til en fil eller en mappe. Dette lar deg deler filer bare ved å distribuere en link. Dette er likevel en funksjon som har veldig liten sikkerhet, alle som kjenner linken kan aksessere informasjonen. Hvis du sender linken til én person, så kan fortsatt denne personen videresende linken til andre, eller så kan kanskje linken vises i søkeresultater. Hvis du deler data ved å bruke en lenke, sørg for at du deaktiverer linken når du ikke trenger den lenger, hvis mulig, kan du også beskytte linken med et passord.
4. **Innstillinger**: Sett deg inn i og sørg for at du forstår innstillingene i tjenesten. For eksempel, hvis du deler en

Bruke nettskyen sikkert

mappe med noen andre, kan de dele denne videre med andre uten at du finner det ut?

5. **Antivirus**: Sørg for at din datamaskin og andre datamaskiner som brukes til å dele din informasjon har et oppdatert antivirus installert. Hvis en fil du deler blir infisert, så kan også andre datamaskiner som aksesserer denne filen bli infisert.
6. **Sikkerhetskopi**: Selv om nettskyleverandøren tar regelmessig sikkerhetskopi av dataene, vurder å ta egen sikkerhetskopi. Dette beskytter deg hvis dataene blir utilgjengelig fra leverandøren, kanskje ved at leverandøren går konkurs, blir stengt ned eller andre grunner som gjør dataene utilgjengelige. Det kan også være mye enklere å gjenopprette store mengder data fra en lokal sikkerhetskopi enn å hente de ned fra nettskyen. Sørg også for at du finner ut hvor ofte nettskyleverandøren tar sikkerhetskopi av filene dine, kan du gjenopprette en tidligere versjon av filen og hvor lenge lagrer de sikkerhetskopien?

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

Sterke passord:	http://www.securingthehuman.org/ouch/2013#may2013
Passordhåndterere:	http://www.securingthehuman.org/ouch/2013#october2013
Sikkerhetskopi:	http://www.securingthehuman.org/ouch/2013#september2013
Sikkerhetsleksikon:	https://norsis.no/sikkerhetspedia/

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