OUCH! | November 2016

Det månedlige nyhedsbrev om IT-sikkerhed

OUCH!

I DENNE UDGAVE...

- Overblik
- Hvordan vælger man en udbyder?
- Hvordan sikrer man sine data?

Hvordan bruger man “Skyen”sikkert?

Overblik

Begrebet “Skyen” kan betyde noget forskelligt fra person til person, men oftest betyder det, at man benytter sig af en internetservice til at gemme og håndtere sine computersystemer og/eller data. En fordel ved at bruge Skyen er, at det er let at få adgang til sine data fra flere forskellige enheder, det er let at synkronisere flere forskellige enheder og det er let at dele med personer i hele verden. Man kalder disse servicer for ”Skyen” fordi man oftest ikke ved, hvor ens data fysisk befinder sig. Eksempler på Skyen er: Google Docs, Dropbox, en server på Amazon Cloud, kundedata på Salesforce eller billeder og musik i Apples iCloud. Disse online muligheder kan gøre dig mere effektiv, men der er nogle sikkerhedsproblemer man skal være opmærksom på.

Gæsteredaktør

Dave Shackleford (**@daveshackleford**) er konsulent og ejer Voodoo Security. Han er desuden forfatter til flere SANS træningskurser blandt andet SANS Security 579: Virtualization and Private Cloud Security og Security 524: Cloud Security Fundamentals.

Hvordan vælger man en udbyder?

Skyen er hverken god eller ond, den er et redskab til at få ting gjort både hjemme og på arbejde. Du skal være opmærksom på, at når du bruger Skyen giver du dine private oplysninger til andre og forventer, at de sørger for, at de både er let tilgængelige og sikre. Du skal derfor være sikker på, at du vælger den rette udbyder. På din arbejdscomputer og ved arbejdsrelaterede informationer, skal du sikre dig, at din arbejdsplads tillader, at du bruger eksempelvis Google Docs eller Dropbox og at du overholder deres retningslinjer Hvis du vil bruge Skyen privat bør du overveje følgende:

1. **Support**. Hvor let er det at få hjælp eller få besvaret et spørgsmål. Er der en e-mailadresse du kan kontakte, et offentligt forum hvor du kan stille spørgsmål eller har deres hjemmeside en liste med ofte stillede spørgsmål?
2. **Enkelthed**. Hvor let er det at bruge den pågældende service? Jo mere kompliceret servicen er, des større er risikoen

Hvordan bruger man “Skyen”sikkert?

for, at du ved en fejl kommer til at offentliggøre eller miste dine informationer. Vælg en service der er let at forstå, let at sætte op og let at bruge

3. **Sikkerhed**. Find ud af, om der bliver indsamlet data om dig og hvilke data det drejer sig om. Hvordan kommer data fra din computer til Skyen og hvordan er data gemt i Skyen. Er dine data krypteret og hvis de er, hvem kan så dekryptere dem?
4. **Betingelser**. Brug et øjeblik på at sætte dig ind i betingelserne for at bruge servicen (de er ofte overraskende lette at læse). Få bekræftet hvem der har adgang til dine data og hvad dine juridiske rettigheder er. Undersøg hvilke sikkerhedsforanstaltninger udbyderen står for og hvilke, der er dit ansvar.

Skyen kan give let adgang til dine informationer og gøre dig mere produktiv, men pas på! Hvordan har du adgang til dine informationer? Hvordan du deler dem?

Hvordan sikrer man sine data?

Når du først har valgt din udbyder er det næste trin at sikre dig at du bruger Skyen på en sikker måde. Hvordan du har adgang til dine data og hvordan du deler dine data er ofte det, der har størst betydning for, hvor sikre dine filer er. Der er nogle forholdsregler du kan tage.

1. **Autentifikation**: Brug et stærkt og unikt password (gerne en passphrase) til din konto i Skyen. Hvis din udbyder tilbyder to-trinsbekræftelse anbefaler vi, at du benytter dig af det. To-trinsbekræftelse er en af de vigtigste måde til at beskytte din konto.
2. **Dele filer og mapper**: Skyen gør det let at dele, måske for let. I det værst tænkelige tilfælde kan du risikere at dele en fil eller folder med hele internettet i stedet for blot en enkelt person. Den bedste måde at beskytte dig mod det er at undlade at automatisk dele filer med nogen. Del kun filer eller foldere med udvalgte personer (eller grupper) og del kun det, der er nødvendigt at dele. Når en person ikke længere behøver at have adgang til dine filer bør du fjerne adgangen. Det bør være let at se hvem der har adgang til hvilke filer eller foldere.
3. **Dele filer eller foldere ved hjælp af link**: Det er ofte muligt at få lavet et link til dine filer eller foldere, som du ønsker at dele. Det er en let måde at dele på, men det er ikke en sikker måde. Alle der får fat i linket har adgang

Hvordan bruger man "Skyen"sikkert?

til dine filer. Selvom du deler linket med en enkelt person, kan du risikere at personen deler det med andre, du kan også risikere at det dukker op i søgemaskiner. Hvis du benytter dig af denne mulighed, bør du derfor beskytte dine filer ved at sætte en udløbsdato på linket eller ved at beskytte linket med et password.

4. **Indstillinger**: Sæt dig ind i, hvilke sikkerhedsindstillinger din udbyder tilbyder. Det kan eksempelvis være godt at vide, om den person du har delt en folder med, kan dele den med andre uden du ved det. Kan man se hvem der har læst dine filer og hvornår? Kan man sørge for at personer kun kan læse og ikke ændre filer?
5. **Antivirus**: Sørg for at der er den nyeste version af dit antivirusprogram på din computer og alle andre computere, der deler dine data. Hvis du deler en fil, der er inficeret kan andre computere, der har adgang til den fil også blive ramt.

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 (ikke oversat til dansk)

Totrinsbekræftelse (dansk udgave):	https://securingthehuman.sans.org/ouch/2015#september2015
Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Password Managers:	https://securingthehuman.sans.org/ouch/2015#october2015
What is Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

Licensinformation

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversat af: Mie Ljungberg Kristensen for WelcomeSecurity