Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

- Översikt
- Välja en molnleverantör
- Säkra dina data

Använd Molnet Säkert

Översikt

"Molnet" är en kraftfull teknik som både människor och organisationer har snabbt antagit. "Moln" kan betyda olika saker för olika människor, men i allmänhet innebär det att använda en tjänsteleverantör på Internet för att lagra och hantera dina data för dig. En fördel med molnet är inte bara att kan du enkelt komma åt och synkronisera dina data från flera enheter var som helst i världen, men du kan också dela din information med vem du vill. Anledningen till att vi kallar dessa tjänster "Molnet" är för att du ofta inte vet var dina data fysiskt lagras. Exempel på ett datormoln inkluderar att skapa dokument på Google Docs, dela filer via Dropbox, ställa in din egen server på Amazon Cloud, eller lagra din musik eller bilder på Apples iCloud. Dessa online-tjänster har potential att göra dig mycket mer produktiv, men de kommer också med unika risker. I detta nyhetsbrev täcker vi hur man säkert kan utnyttja molnet.

Gästredaktör

James och Kelli Tarala (**@isaudit** / **@kellitarala**) är huvud konsulter på Enclave säkerhet och har skrivit flera SANS utbildningar, bland annat SANS Audit 566: Genomförande och Revision av de Tjugo Kritiska Säkerhetskontrollerna och MGT 415: En Praktisk Introduktion till Riskbedömningar.

Välja en Molnleverantör

Molnet är varken gott eller ont, det är ett verktyg för att få saker gjorda, både på jobbet och hemma. Men när du använder dessa tjänster lämnar du över dina privata uppgifter till främlingar och man förväntar sig att de ska hålla det både säkert och tillgängligt. Som sådan, vill du vara säker på att du väljer klokt. För dina arbetsdatorer eller arbetsrelaterad information, kolla med din chef för att se om du kan använda molntjänster. Om du har rätt att använda molnet, vänligen se till att bekräfta vilka molntjänster du kan använda och vilken policy som förklara hur man använder dem. Om du funderar på en molntjänst för personligt bruk, överväga följande.

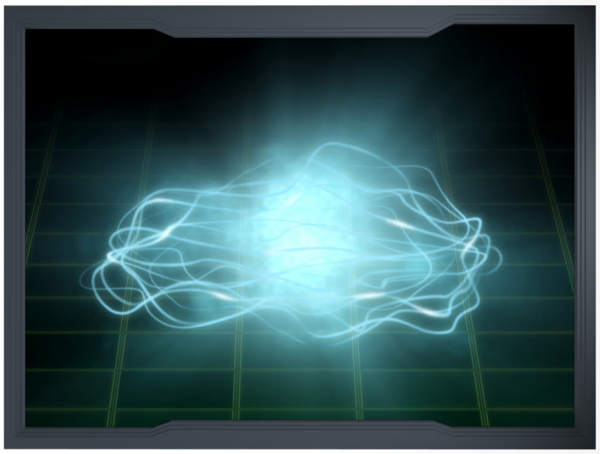
1. **Support**: Hur lätt är det att få hjälp eller få en fråga besvarad? Finns det ett telefonnummer som du kan ringa eller e-postadress kan du kontakta? Finns det andra alternativ för support, såsom offentliga forum eller vanliga frågor på deras hemsida?
2. **Enkelhet**: Hur lätt är det att använda tjänsten? Ju mer komplex tjänsten är, desto mer sannolikt att du kommer att

© The SANS Institute 2014

Använd Molnet Säkert

göra misstag och avslöja eller förlora din information. Använd en molnleverantör som du tycker är lätt att förstå, konfigurera och använda.

3. **Säkerhet**: Hur kommer dina data från datorn till molnet, är anslutningen säkras genom kryptering? Hur är data lagrat i molnet, är krypterat och i så fall vem som kan dekryptera dina data?
4. **Villkor**: Ta en stund att granska användarvillkoren (de är ofta förvånansvärt lätt att läsa). Bekräfta vem som kan komma åt dina uppgifter och vilka dina lagliga rättigheter är.



Molnet kan göra din information mer tillgänglig och bidra till att göra dig mer produktiv, men var försiktig med hur du lagrar och delar din information.

Säkra Dina Data

När du har valt en molntjänst, är nästa steg att se till att du använder dina molntjänster på rätt sätt. Hur du kommer åt och delar dina data kan ofta ha en mycket större inverkan på säkerheten för dina filer än något annat. Några viktiga saker du kan göra är:

1. **Autentisering**: Använd en stark, unik lösenord för att autentisera till ditt molnkonto. Om din molnleverantör erbjuder tvåstegsverifiering rekommenderar vi att du aktiverar den.
2. **Dela filer/mappar**: Molnet gör det mycket enkelt att dela, ibland för enkelt. I värsta fall kanske du råkar göra dina filer eller hela mappar offentligt tillgängliga för hela Internet. Det bästa sättet att skydda sig är som standard att inte dela några av dina filer med vem som helst. Då tillåts endast vissa personer (eller grupper av personer) tillgång till vissa filer eller mappar på en behovsenlig behörighet. När någon inte längre behöver tillgång till dina filer, ta bort dem. Din molnleverantör bör tillhandahålla ett enkelt sätt att spåra vem som har tillgång till dina filer och mappar.
3. **Dela filer/mappar med Länkar**: Ett gemensamt drag för vissa molntjänster är möjligheten att skapa en webblänk som pekar på dina filer eller mappar. Den här funktionen gör det möjligt att dela dessa filer med vem du vill genom att helt enkelt ge en webblänk. Men denna metod har mycket lite säkerhet, vem som helst som känner den här länken har tillgång till dina personliga filer eller mappar. Om du skickar länken till bara en person, kan den personen dela den länken med andra eller de kan visas upp på sökmotorerna. Om du delar data med hjälp av en länk, se till att du inaktiverar länken när den inte längre behövs eller om möjligt, skydda kopplingen med ett lösenord.
4. **Inställningar**: Förstå de säkerhetsinställningar som erbjuds av din molnleverantör. Till exempel, om du delar en mapp

med någon annan, kan de i sin tur dela dina data med andra utan din vetskap?

5. **Antivirus**: Se till att den senaste versionen av antivirusprogram är installerat på datorn och på någon annan dator som används för att dela data. Om en fil du delar blir smittad, kan andra datorer med tillgång till samma fil också bli smittad.
6. **Säkerhetskopiering**: Även om din molnleverantör gör säkerhetskopieringar av dina data, överväg att göra regelbundna säkerhetskopior själv. Inte skyddar bara detta dina data, men om din molnleverantör går i konkurs, stängs av, eller av någon anledning blir oåtkomlig, det kan vara mycket lättare att återvinna stora mängder data från dina lokala säkerhetskopieringar än att dra ner från molnet. Kontrollera också hur ofta din molnleverantör säkerhetskopierar dina filer, tillåter de dig att återställa tidigare versioner av dina filer, och hur länge behåller de dina säkerhetskopior?

LÄR DIG MER

Prenumerera på det månaltliga OUCH! nyhetsbrevet om säkerhetsmedvetenhet, ha tillgång till OUCH! arkiven, och lär dig mer om SANS lösningar inom säkerhetsmedvetenhet genom att besöka oss på http://www.securingthehuman.org

Swedish Version

OUCH! är översatt av Andreas Bohman och Marcus Andersson. Båda arbetar inom informationssäkerhetsbranchen och har många års erfarenhet i etablering av säkerhetsmedvetenhetsprogramm.

Resurser

Starka lösenord:	http://www.securingthehuman.org/ouch/2013#may2013
Lösenordshanterare:	http://www.securingthehuman.org/ouch/2013#october2013
Säkerhetskopior:	http://www.securingthehuman.org/ouch/2013#september2013
Säkerhet Villkor:	http://www.securingthehuman.org/resources/security-terms

OUCH! utgivs av SANS Securing the Human och är distribuerat under Creative Commons BY-NC-ND 4.0 licens.
Du kan fritt distrubera nyhetsbrevet eller andvända det i ditt interna medvetenhetsprogramm så länge du inte ändrar nyhetsbrevet.

För översättning eller mer information, vänligen kontakta ouch@securingthehuman.org.

Redaktion: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Översatt Av: Andreas Bohman och Marcus Andersson

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus