Det Månatliga Nyhetsbrevet Om Säkerhetsmedvetenhet för Datoranvändare

OUCH!

I DENNA UTGÅVA…

Kryptering

Vad är Kryptering?

Du kan höra folk som använder termen “kryptering” och hur du ska använda den för att skydda dig själv och din information. Men begreppet kryptering kan verka förvirrande. Dessutom kan kryptering inte skydda dig från allt, det har sina begränsningar. I detta nyhetsbrev förklarar vi i mycket enkla termer vad kryptering är, varför du bör använda den, och hur man ska genomföra det på rätt sätt.

Gästredaktör

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) är en konsult baserad i Washington, DC. Han är ledande instruktör för SANS Institute kursen Mobile Device och Ethical Hacking (SEC575) och författare till Incident Response Team Management (MGT535).

Du har en enorm mängd känslig information på dina enheter, till exempel ekonomiska dokument, bilder, e-post, eller journaler. Om du skulle ha en av dina enheter förlorade eller stulna, kan all denna mycket känsliga information nås av den som har den. Dessutom kan du utföra känsliga transaktioner på nätet, till exempel onlinebanker eller onlinebutiker. Om en cyber angripare skulle övervaka dina aktiviteter på nätet, kan de stjäla all din information, såsom dina ekonomiska konton eller kreditkortsnummer. Kryptering skyddar dig i dessa situationer genom att se till att obehöriga inte kan komma åt eller ändra dina uppgifter.

När informationen inte är krypterad, kallas det vanlig text. Detta innebär att vem som helst kan enkelt läsa eller komma åt den. Kryptering omvandlar informationen till ett icke-läsbart format som kallas chiffertext. Kryptering fungerar med hjälp av komplexa matematiska operationer och en unik nyckel för att omvandla informationen till chiffertext. Det viktiga är vad som låser eller låser upp din information, precis som en nyckel kan låsa eller låsa upp en dörr. Ett vanligt exempel på en nyckel är ett lösenord, bara människor som har det lösenordet kan dekryptera och komma åt din information. För att skydda din krypterade information behöver du skydda din nyckel. Generellt sett fungerar kryptering på två sätt, kan du kryptera data i vila (t.ex. data som lagras på din bärbara dator) och data i transit (till exempel överföring av information på nätet).

Kryptera Information i Vila

Det primära målet för kryptering i vila är att skydda information om din dator eller mobila enhet försvinner eller blir stulen. För femton år sedan var detta inte ett problem, eftersom de flesta datorer var stora, otypliga stationära enheter som var mycket

Kryptering

svåra att flytta runt. Idag väger många bärbara datorer endast ett par kilo medan en mobil enhet kan väga bara några gram. Dessa enheter är extremt kraftfulla och håll en enorm mängd information, men är också väldigt lätta att förlora. Dessutom kan andra mobila medier innehålla känslig information, till exempel USB-minnen eller CD-ROM. En vanlig teknik för att kryptera information på dessa enheter kallas Full Disk Encryption (FDE). Det innebär att allt på systemet krypteras automatiskt, du behöver inte bestämma vad eller vad man inte ska kryptera. De flesta operativsystem kommer numera med Full Disk Encryption inbyggd, du har bara att helt enkelt aktivera det. Till exempel innehåller Mac OS X Filevault medan vissa versioner av Windows inkluderar BitLocker. Om din dator har stöd för Full Disk Encryption, rekommenderar vi starkt att du aktiverar det. Dessutom har de flesta mobiltelefoner stöd för Full Disk Encryption för sina interna lagringsenheter. Till exempel iOS, operativsystemet för iPhone och iPads, tillämpas automatiskt Full Disk Encryption när ett lösenord har ställts in. Om du vill veta om din dator eller mobila enhet på jobbet stödjer Full Disk Encryption, fråga din helpdesk eller handledare. För din personliga datorer, kontakta datortillverkaren eller se online-dokumentationen.

Kryptering är ett kraftfullt sätt att säkra din information, men den är bara så stark som din nyckel.

Kryptera Information i Transit

Information är också sårbar när det är i transit. Om data inte är krypterad, kan den övervakas och fångas på nätet. Det är därför du vill se till att all känslig online kommunikation, t.ex. för onlinebanker, skicka e-post eller kanske till och med tillgång till sociala medier är krypterade. Den vanligaste typen av online-kryptering är HTTPS. Det innebär att all trafik mellan din webbläsare och en webbplats är krypterad. Leta efter https:// i webbadressen, ett lås i din webbläsare, eller ditt adressfält bli grönt. Dessa är alla tecken på att kommunikationen är krypterad. Beroende på din webbläsare och webbplatsen, kan du se alla tre på samma gång. Dessutom, när du ansluter till ett Wi-Fi-nätverk, se till att också använda kryptering när så är möjligt. Slutligen, när du skickar eller tar emot e-post se till att din e-postklient är inställd för att sända din e-post via en krypterad kanal. De flesta e-postklienter ger kryptering, dessutom kan din ISP kanske hjälpa dig att aktivera kryptering på din e-postklient.

Kryptering

Implementera Kryptering Korrekt

Oavsett vilken typ av kryptering du använder eller hur du använder den, delar nästan alla former av kryptering några vanliga steg i andvändning.

- Din kryptering är inte starkare än din nyckel. Om någon gissar eller äventyrar din nyckel, kommer de att ha tillgång till dina uppgifter. Du måste skydda din nyckel.
- Om du använder ett kåd eller lösenord för din nyckel, se till att det är ett långt, säkert lösenord och inte glömmer det. Om du har glömt det, kommer du att bli utelåst från din egen data.
- Din kryptering är inte starkare än säkerheten i din dator. Om datorn har äventyrats eller är infekterad kan cyber angripare kringgå din kryptering. Som sådan, se till att hålla din dator eller mobila enhet säker också.
- Om du får olika alternativ för kryptering, välj alltid den starkaste metoden.

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

Mac OS X Filevault: http://support.apple.com/kb/ht4790
iOS-kryptering: http://support.apple.com/kb/ht4175
Android-kryptering: http://www.androidauthority.com/how-to-encrypt-android-device-326700/
Windows Kryptering: http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
Skydda datorn: http://www.securingthehuman.org/ouch/2012#december2012
Lösenord Chefer: http://www.securingthehuman.org/ouch/2013#october2013

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

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