Payback Sverige

Hur du skyddar din information

Bakgrund

Ingen ifrågasätter att vi befinner oss i en utveckling där övervakningen av medborgarna kraftigt ökar för varje år som går. För lite övervakning anses ge problem i form av kriminalitet och otrygghet, för mycket övervakning ger problem i form av att inte få ha sitt privatliv ifred. **FN:s deklaration om de mänskliga rättigheterna, artikel 12** *(Universal declaration of human rights) Ingen får utsättas för godtyckligt ingripande i fråga om privatliv, familj, hem eller korrespondens och inte hel- ler för angrepp på sin heder eller sitt anseende. Var och en har rätt till lagens skydd mot sådana ingripanden och angrepp.*

Skälet till ovanstående deklaration, som är skrivet på samma nivå som rätten till liv, är att de flesta människor upplever det som ett mycket väsentligt värde att ha ett skyddat privatliv och att det helt enkelt är obehagligt att vara iakttagen. Det har ingenting med brottslig verksamhet att göra. En människa vill helt enkelt ha sina privata omständigheter ifred, och det behöver hon inte motivera. Vår tids digitala övervakningsåtgärder måste anses strida mot FN:s deklaration om mänskliga rättigheter och Europakonventionen. Dessa deklarationers underförstådda krav på att nödvändigheten av övervakning ska vara så uppenbar att den väger tyngre än grundprincipen om skydd för privatlivet, är inte uppfyllda när det gäller exempelvis:

Trafikdatalagringen (*lagring av information om vilka vi ringer och mailar, med mera*) och den föreslagna **FRA-övervakningen** (*möjlighet för Försvarets Radioanstalt att avlyssna/läsa kommunikation som passerar landets gränser, utan brotts- misstanke*).

Länk: http://sv.wikipedia.org/wiki/Trafikdatalagring
Länk: http://sv.wikipedia.org/wiki/Försvarets_radioanstalt
Länk: http://sv.wikipedia.org/wiki/Titan_(trafikdatabas)

Så att vi under de senaste åren mer och mer börjat få ett ”Storebror ser dig” samhälle är ganska uppenbart, men frågan är ju till vilket pris. Jag har redan belyst övervakningens konsekvenser i en tidigare publicerad artikel.
Länk:
http://www.mynewsdesk.com/se/view/pressrelease/oevervakningens-konsekvenser-del-2-470318

Och det är väl ganska självklart att man vill vara säker på att den information som man har i sin dator, sänder via mail eller pratar om i mobil endast är tillgänglig för dig själv eller de du väljer att delge informationen till och inga andra. Speciellt om det rör sig om känslig företags information m.m.

Säkert Internet

Vi börjar med det självklara och det är Internet. I Sverige har vi i dag en mängd av olika så kallade ISP:s (*Internet Service Providers*) som helt enkelt levererar Internet via telefonjacket, fiber, 3G eller numera 4G nätet även kallat Mobilt Bredband.

Den ISP man använder sig av oavsett leverantör som t.ex. Telia, Comhem, Tele2, Bahnhof, Bredbandsbolaget m.fl. levererar Internet och i vissa fall med antivirustjänster och ett säkert utrymme att lägga upp sina bilder på m.m. Och självklart så kostar allt extra de erbjuder mer pengar, så månadskostnaderna för en Internettjänst kan bli ganska dyr i slutänden.

När det gäller Internetleverantörer så finns det i dagsläget få som levererar Internet till dig som kund och som **INTE** sparar loggar på den trafik du skapar, och en sån leverantör är Bahnhof. Gå in på den ISP du har köpt Internet av och sök information om hur de hanterar trafik informationen som du skapar när du använder deras tjänster. Står det inget på deras hemsida så kontakta ISP:n och begär att få information, men räkna inte med att de säger som det är. Det är ju precis inget som dom vill skylta med, för då kommer dom att tappa många kunder.

Integritet

Bahnhof och några fler mindre leverantörer förespråkar Integritet på nätet och står bland annat bakom initiativ som http://www.integrity.st/ samt http://www.integritetskollen.se/ (*skulle öppna under våren 2010, men ännu har inget hänt vilket förmodligen beror på att de stora Internet drakarna inte vill lämna information om hur de handhar sina kunders information*). Bahnhof tillhandahåller även en tjänst där du som kund hanterar IP-adresstilldelningen själv och kan när du vill gå in och byta IP-adress via en kundsida. Det finns även en tjänst som man kallar för Anoine som döljer din IP-adress på Internet.

När det gäller de operatörer som är engagerade i Integritetssidan så gäller följande:

De operatörer som vill kunna använda Integrity-märkningen förbinder sig att:

1. Aldrig stänga av en hemsida, ta bort eller ändra information så länge innehållet inte strider mot svensk lag.
2. Aldrig lämna ut information om kunder till tredje part utöver vad som krävs enligt svensk lag.
3. Aldrig vidta andra åtgärder för övervakning eller informationslagring än vad som krävs av svensk lag.
4. Värna kundens lagstadgade rätt till sina åsikter och rätten att uttrycka dem offentligt – även på Internet.
5. Följa lagen om elektronisk kommunikation, som bland annat kräver att all kundinformation som inte är nödvändig för den dagliga driften raderas så fort som möjligt.

VPN-Tjänster

Steg två när det gäller säkert Internet är att använda sig av en lösning som fungerar klockrent och det är att använda sig av en så kallad VPN tjänst. En krypterad tunnel där man surfar på en helt annan IP-adress och i en krypterad tunnel över Internet. Då fungerar t.ex. inte ”traffic shaping” och leverantören kan inte heller logga den trafik du generar eftersom de inte kan se den. Och om det är någon myndighet som av någon anledning försöker låsa dig som person till en viss lokal IP-adress, så går inte det heller.

När det gäller VPN tjänster så finns det även här flera leverantörer och här kommer några exempel:
Strong VPN: http://www.stronvpn.com/ Strong VPN har flera olika tjänster beroende på ditt behov och du kan även välja vart i världen du kopplas upp. Kostar från 55-85 dollar per år. (360-555kr) Fördelen är en pålitlig tjänst och bra service där man vid problem kan chatta med supporten direkt dygnet runt. Har levererat tjänster sedan 1995 och är således ett väletablerat företag.

”*When analyzing other VPN companies, please be careful when choosing. Purchase your VPN service through an established company. There are many start up companies, and they could be using your information for other means.*”

Anonine: http://www.bahnhof.se/ Bahnhofs tjänst kostar 40 kr i månaden (480 kr per år)
VPNTUNNEL: www.vpntunnel.se kostar 49 euro per år (499kr)

Av ovanstående alternativ så rekommenderar jag Strong VPN som alltid fungerar och har bra service, dock på engelska. Har man svårt med engelskan så kan jag rekommendera Bahnhofs tjänst Anonine eller vpntunnel.se. Använder man sig av en VPN tjänst så kan man garanterat surfa helt fritt utan att någon har koll på vart man surfar och vilken trafik man genererar, vilket borde vara en självklarhet i dagens samhälle, Men så är icke fallet, tyvärr.Och här kommer några svenska leverantörer av VPN. Observera dock att dessa företag är sent etablerade och har således inte varit i branschen speciellt länge samt att man försöker sälja in sig med följande information på sin sida: ”*Med hänsyn till säkerheten används ingen amerikansk krypteringsteknik*” (de tre Relakks sidorna).

https://www.relakks.com/ Kostnad 449kr/år
https://www.ipredator.se/ (Samma som Relakks, bara ett annat namn) Kostnad 449kr/år
https://www.flashback.name/ (Samma som Relakks, bara ett annat namn)

VPN Tjänsten som erbjuds är ett svenskt bredbandsabonnemang över Internet vilket innebär att det regelverk som framför allt reglerar verksamheten är Lagen (2003:389) om elektronisk kommunikation. De uppgifter som svenska myndigheter kan begära förutom abonnentuppgifter är så kallade trafikuppgifter. Dessa är omgivna av ett mycket starkare legalt skydd. För att bryta sekretessen för trafikuppgift måste brottet vara föreskrivet ett straff om minst två år i fängelse.

Säker Mail

När det gäller säker mail så använder idag många gratisfunktioner som t.ex. hotmail, yahoomail, gmail m.m. vilket innebär att mailen sänds i ”cleartext”. Allt sker helt öppet för någon att ta del av om man har åtkomst till det nät man använder sig av hemma eller på jobbet. Jag rekommenderar att man lägger en liten slant per år och använder sig av en säker mail tjänst där man har möjligheten att kryptera det mail man vill att ingen annan skall kunna ta del av, än den man skickar mailet till.

Även mailtjänsterna som ISP levererar när man köper ett Internet abonnemang, är helt okrypterade och öppna.
Några av de kändaste tjänsterna och vad det kostar:
Hushmail: www.hushmail.com Är helt gratis men vill man ha mer mailutrymme och fler funktioner så kostar ett premiumkonto 48 dollar (305kr) för ett år.
S-mail: www.s-mail.com Även här är grundkontot gratis men vill man ha fler funktioner och mer utrymme så kostar det en slant, 14 dollar (89kr) för 3 månader.
4Secure Mail: www.4securemail.com Inget gratis konto utan den billigaste varianten kostar 40 dollar (254kr) för 1 år.

Av dessa tre så kan jag av egen erfarenhet varmt rekommendera Hushmail som är den tjänst som funnits längst och fungerar stabilast. Hushmail startade redan 1999 och har utvecklat sin produkt kontinuerligt. Det är dock viktigt att poängtera att självklart måste även den du mailar till använda samma tjänst annars funkar det inte. Använder man mailtjänsten och begår brott så lämnar leverantörerna ut information till polisen om de kräver detta.

Krypterad Chatt

Många använder sig av någon form av chatt tjänst dagligen som MSN, Yahoo, ICQ, Adium m.fl. Av dessa så är det väl i dagsläget MSN som väldigt många använder. Det man bör tänka på även här är att det du skriver sänds i cleartext precis som vanlig mail.
Adium är chatt programmet för Mac och fördelen med Adium är att du kan chatta med polare som har MSN, ICQ, Yahoo. Ja i stort sett alla andra chatt program som finns samt att det redan finns inbyggd kryptering.

Adium: http://adium.im/ Gratis open source produkt med inbyggd kryptering.
För att kunna köra övriga chatt tjänster krypterat så finns det lösningar på följande sidor:
Secway: http://www.secway.fr/us/products/simppro/home.php Kostnad 25 dollar (160kr)
Finns även en gratisversion: http://www.secway.fr/us/products/simplite_msn/

Operativsystem

Innan jag går in på kryptering av hårddisk så måste vi gå igenom valet av operativsystem. Och när det gäller operativsystem så rekommenderar jag i första hand en Mac dator med Mac OSX. Mac OSX är bland det säkraste som finns på marknaden och är enkelt att lära sig och fungerar utan problem. Självklart så finns det en massa olika Linux distributioner som Ubuntu, Red Hat, Mandrake, PC Linux OS m.fl. Men, det är lite mer pillande med dessa och det är självklart en vanesak vilket system man använder sig av och en kostnadsfråga.

Och varför då valet av Mac OSX? Jo, av den enkla anledningen att i OSX så är det du som användare som har fullständig kontroll över alla processer i datorn och således styr. Så är icke fallet med Windows, där är det bara gilla läget, att vara passageraren och åka med. Och är man lite mer van med datorer så finns det massor med programvaror gratis för Mac OSX samt programvara där man kan lära sig att koda program själv vilket tillhandahålls av Apple helt gratis, du behöver bara registrera en mailadress.

Länk**:** http://developer.apple.com/technologies/xcode.html

Eftersom att många av oss använder Windows XP, Vista och 7 så har jag gjort en djupdykning i Windows träsket och hittat Windows 7 Tiny som är en komprimerad version av det senaste Windows 7. Windows 7 Tiny är på endast 699 mb till skillnad mot 6-10 GB på en variant av Windows 7 Ultimate och en kostnad på 1800kr. (Red. kommentar: Skillnaden mellan Tiny och Windows 7 är att Tiny saknar drivrutiner för modem, scanners, och kameror. Vidare att Windows Media Player och codes för det är borta samt att Security Center och Bit Locker Drive Encryption är bortrensade)

Det utvecklarna har gjort är helt enkelt att rensa bort allt onödigt och på så vis få till ett väldigt snabbt operativsystem som även fungerar på äldre datorer och i bootcamp läget på en Mac. Bootcamp läget i Macen innebär att du kan ha både Mac OSX och t.ex. Windows 7 på en och samma burk. Jag har kört så sedan OSX kom.

Windows 7 Tiny är förstås inte en licensierad variant av Windows och således inte laglig, men det är ju upp till dig själv som användare vad du vill använda. Men vill man vara säker och har en slant i plånboken rekommenderar jag en Macbook Pro med Mac OSX som begagnade ligger runt 4000kr. Sen kör man in Windows Tiny XP eller Windows Tiny 7 och vips så har man två datorer i en.

Förutom ett bra operativsystem, säker mail och säkert Internet så är det självklart att man använder sig av ett antivirus och en brandvägg. Speciellt om man använder ett Windows system i sin dator. Brandvägg ingår oftast i det modem eller den router som man får av Internetleverantören. Och vill man inte lägga 4-500 kr per år så finns det ypperliga gratis produkter för Antivirus som t.ex.:
Avast Antivirus: www.avast.com Funkar perfekt och är på svenska.

Jag brukar även rekommendera Windows användare att installera Emsisoft Anti Malware 5.0 som du kan tanka ner gratis från http://www.emisoftcom

Det programmet kan du köra en gång i månaden för att hålla Windows rent från skräpfiler.

Krypterad hårddisk

När vi nu har gått igenom Internet, mail samt operativsystem så har vi kommit till en av de viktigaste aspekterna när det gäller att skydda sig från informationsförlust. Och det är kryptering av hårddisk, USB minnen m.m.

Att bli av med en bärbar dator är inte bara jobbigt p.g.a. den ekonomiska aspekten. Det är minst lika jobbigt att hårddisken är helt öppen och att informationen kan kommas åt av obehöriga. En bra krypterings programvara i datorn gör det omöjligt för obehöriga att ta del av innehållet på disken/minnet. Och, när det gäller destruktion av hårddisk och USB minne så är det total kross som gäller.

En hårddisk är uppbyggd av flera lager med skivor och slänger man den som den är, eller borrar ett hål i den, så kan ändå information plockas ur disken av duktiga tekniker. I Sverige har vi ett företag som heter IBAS och som har fått fram information ur diskar som har legat på havets botten i flera år eller som varit med om en brand. Så det tål att upprepas, total förstörelse eller helst nedmalning eller nedsmältning av en hårddisk. omöjliggör återskapandet av informationen. Det finns även såkallade överskrivningsverktyg, men det går inte att säkerställa till 100% att informationen inte går att plocka fram ändå.

Truecrypt: www.truecrypt.org Truecrypt är helt gratis och med tanke på det ett bra alternativ. Det pratas en hel del om att eftersom det är en såkallad ”open source” produkt så har myndigheter och polisväsendet koll på programvaran och kan knäcka den enkelt.
I USA kanske, men inte i Sverige med tanke på den undermåliga utrustning och brist på kompetens som läget är inom tidigare nämnda myndigheter. Men helt klart så är Truecrypt bättre än ingen kryptering alls. (*Fungerar på alla operativsystem*)

Men tydligen så har amerikanerna misslyckats med att knäcka Truecrypt:
Länk: http://news.techworld.com/security/3228701/fbi-hackers-fail-to-crack-truecrypt/

Drive Crypt Plus Pack: www.drivecrypt.com För ca 60 dollar (390kr) (*endast Windows system*) så krypteras hela disken med AES 256-bitars kryptering och enligt Amerikanska National Institute of Standards and Technology så torde det vara omöjligt att knäcka bara man har ett ordentligt lösenord. *”Assuming that one could build a machine that could recover a DES key in a second (255 keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key”*

Och betänk då att Drivecrypt Plus Pack använder sig av 256-bitars kryptering.
PGP Whole Disk Encryption: www.pgp.com/products/index.html Ett hårddisk krypto som fungerar på alla operativsystem för 149 dollar (970kr)

Och att observera när det gäller hårddisk krypto är att användaren måste skapa ett rejält lösenord, som i sig inte kan knäckas allt för enkelt, annars är det helt meningslöst. Och det finns en uppsjö med produkter på marknaden även här. Välj den produkt som du, som användare, tycker känns bäst för dig att använda.

Säker Mobiltelefoni

När det gäller säkra mobiler så har det under flera år varit väldigt osäkert på tillförlitligheten av produkterna på marknaden. Krypteringen har inte fungerat och strömförbrukningen har varit enorm. Men nu under de senaste åren har det kommit en hel del intressanta produkter som vi skall gå igenom.

Nummer ett är självklart det svenska säkerhetsföretaget Sectras telefon Sectra Tiger 7401 som används av b.la Försvarsmakten och har testats av flera säkerhetsföretag och statliga säkerhetsavdelningar. Godkänd av NATO och EU med en taltid på upp till 7 timmar.
Utöver telefonen 7401 så har företaget även släppt produkten Tiger XS som är ett personligt talkrypto som skyddar telefonsamtal från avlyssning över tele-, GSM-, 3G-, ISDN- och IP-nät samt via satellitsystem och som kan användas för krypterad telefontrafik, krypterad datatrafik, krypterad fax sams krypterade SMS. Fördelen med Tiger XS är att den kopplas till din vanliga telefon via Bluetooth. Så man kan använda vilken telefon som helst. Problemet är att Tiger XS kostar 5000euro (42.785kr).

Och den tidigare produkten Sectra Panthon ligger på ca 2500 euro (21.438kr).
Sen när det gäller Sectras produkter, som för övrigt produceras i Linköping, så lär det förmodligen vara svårt att som vanlig medborgare få tag i produkterna.
Nummer två på marknaden är Crypto AG:s mobil Crypto Mobile HC-9100. Men, det är samma problem här som med Sectras produkter. Den är väldigt dyr och ej för den civila marknaden.

Så vi får sänka ribban lite och kika på vad det finns för produkter för oss vanliga medborgare, och då är det mjukvaruprodukter som gäller, som du helt enkelt installerar i din vanliga mobil. Ett av dessa produkter är mobilecrypto och som enligt deras hemsida funkar på Nokia, iPhone, Blackberry och Symbian samt Windows system.

Mobilecrypto: www.mobile-crypto.com Hittade tyvärr ingen prisuppgift på deras hemsida men lite intressant information: (*No modern hacking/decryption techniques are capable of decrypting the Secure Lock™ signal in any way. Even the mathematicians who developed the Secure Lock™ encryption algorithms are not capable of decrypting your secure calls and messages. Secure Lock is the only system in the world with the proper certification and documentation to prove it.*)

Phonecrypt: www.phonecrypt.com Ytterligare en intressant produkt där man på deras hemsida kan kontrollera exakt vilka telefonmodeller som är kompatibla med programvaran. En väldigt informativ sida där man även kan tanka ner en testversion av Phonecrypt och testa. Phonecrypt varnar också användaren ifall någon försöker lyssna av eller bryta det krypterade samtalet.

Det finns även gratis produkter men frågan är om funktion och säkerheten kan garanteras. Gör er egen bedömning.
Whispersys: www.whispersys.com En produkt för Android telefoner och som är i Beta stadiet. Men, som sagt bättre än ingenting och gratis.

Säkert Trådlöst Nätverk

Vi hoppar tillbaks lite när det gäller hårdvara och nätverk eftersom att fler och fler går över till trådlösa nätverk eller WLAN som det kallas. Väldigt enkelt och snabbt att sätta upp när man har det behovet i en fastighet. Det finns självkart en mängd olika produkter men vi skall gå igenom några av de bästa och ge lite enkla tips hur man kan säkerställa ett WLAN. Självfallet så skall man slå på krypteringen och helst WPA2-AES kryptering. Absolut inte WEP, som kan knäckas på några minuter.

Utöver krypteringen så är det en fördel om man i routern sätter upp en behörighetslista på de datorer och telefoner som får tillgång till nätverket. Samt att man inte sänder ut nätverkets namn eller SSID som det kallas, vilket försvårar för andra vanliga användare att lokalisera ditt nätverk. Och, självklart så skall man ha ett ordentligt lösenord på basstationen.
Det finns fler tekniska lösningar att använda sig av om man vill säkerställa det trådlösa nätverket ännu mer som att t.ex. använda sig av en RADIUS autentisering. Men det går vi inte in något djupare på.

Aruba Networks: www.arubanetworks.com En leverantör av säkra produkter för trådlösa nätverk, amerikanska försvarsmakten använder i stort sett bara Aruba när de bygger WLAN. Och anledningen till att Aruba har en högre säkerhet i sina produkter än 3Com, D-link, Linksys, Netgear och Zyxel är att man har konstruerat ett eget operativsystem som baseras på UNIX, ArubaOS samt en del annan unik teknik i nätverksmiljön som övriga leverantörer ej kan erbjuda. Därav är också Aruba Networks den enda trådlösa nätverksprodukten som är säkerhets certifierad, enligt FIPS-140 standarden.

Länk: http://www.arubanetworks.com/company/news/release.php?id=194

Övriga tillverkare som levererar bra produkter till överkomliga priser, bara och kika in på länkarna och kolla:

Cisco/Linksys:
http://homestore.cisco.com/en-us/products/linksys-other-products_stcVVcatId552009VVviewcat.htm

Apple Airport Extreme:
http://store.apple.com/se/product/MC340Z/A/AirPort-Extreme?fnode=MTY1NDA0Mg&mco=MTM5NDczMzc

Netgear:
http://www.netgear.com/business/products/access-points-wireless-controllers/access-points/default.aspx

Skydda sig mot Buggning

Enligt lag så är buggning, eller ”Hemlig rumsavlyssning” som det så fint heter i lagen, tillåtet endast om det kan ge ett straff på 4 år eller mer. Men ändå så förekommer det mer än man kan tro. Ett bra sätt att skydda sig är att införskaffa en scanner som reagerar om det finns utrustning i rummet som avger sändande signaler.

Länk: http://www.notisum.se/rnp/sls/lag/20070978.htm
Länk: http://sverigesradio.se/sida/artikel.aspx?programid=83&artikel=3852089

Och när det gäller bugg scanners så finns det en hel del modeller att välja mellan. Här är några av de bästa som finns på Spy Chest hemsida:
Spy Chest: www.spytechs.com/bug_sweep_equip/default.htm

Den billigaste ”Wireless Signal Detector” och den minsta som även har ett ”Vibration Mode” vilket gör att du kan scanna utan att någon annan är medveten om det, den kostar 80 dollar (508kr) (Scannar från 50 Mhz till 6 GHz)

Den lite mer avancerade ”Frequency Scanner” även den med ”Vibration Mode” och även ”Signal Strength Graph” kostar 200 dollar (1270kr) (Scannar från 1 MHz till 6GHz)
Och till sist den mest avancerade ”Bug Sweeper” som inte bara detekterar buggen utan även visar på vilken frekvens den sänder signalen, kostar 300 dollar (1905kr)

Utöver Spy Chest så finns det flera leverantörer av bugg scanners produkter, bara och söka på Internet och bilda sig en egen uppfattning om funktionalitet och kostnad.

Agerande vid en Rättegång

Rent allmänt så har rättsväsendet väldigt dålig kompetens när det gäller IT. Åklagare, advokater, domare och nämndemän har ingen som helst teknisk kompetens vilket gör att de vid en rättsförhandling måste förlita sig på polisens forensiska utredare eller inlånad, teknisk expertis.

Det som är väldigt viktig att veta om man hamnar i en sådan situation, är att teknikerna jobbar efter ”Chain of Custody” metoden när de genomfört sin tekniska utredning. Vilket innebär att de skall bevisas att materialet som utretts, som t.ex. en hårddisk i en dator, har hanterats i en obruten kedja och att hela hanteringen har dokumenterats noggrant. Det vill säga att ingen har kunnat manipulera de eventuella bevisen på hårddisken. Har så icke skett bedöms rent tekniskt hårddisken vara värdelös som bevis.

Detta är det självklart många som inte vet. Så när en åklagare lägger fram bevisning, med hjälp av teknisk expertis, så sväljer man allt de säger för att man helt enkelt inte vet vad som gälleroch hur det fungerar. I USA är rättsväsendet extremt noggranna när det gäller COC, men i Sverige så är fortfarande inte rättsväsendet med på banan. Och en annan intressant aspekt är att rätten måste kunna bevisa vem som satt framför tangentbordet när det eventuella brottet har begåtts. Värt att tänka på i vissa fall.

Sammanfattning

Nu har jag gått igenom en hel del om hur man kan säkra den information, som man vill skydda på olika sätt, och förhoppningsvis så har ni fått en hel del nya tips och funderingar. Jag har försökt att gå igenom de viktigaste aspekterna när det gäller att skydda sin information. Sen är det upp till dig som läser detta, vilket behov du eller ditt företag har. En viktig sak att tänka på är att många av programmen kan man få en testperiod på. Det skall man självklart utnyttja och testa om programmet fungerar som det ska. Och, det bästa är ju att själv testa om det går att knäcka en kryptering eller ta sig in i ett nätverk t.ex.

Jag är medveten om att mycket av det jag har skrivit är helt ny information för många och att en del kanske är svårt att förstå. Men, sök gärna själva på Internet och lär er mera. Kunskap kostar inte pengar, men i slutänden kan du tjäna pengar på att veta.

Och sen finns det massor med tekniska prylar på marknaden som jag inte radat upp i artikeln. Sök information om produkten och försök bilda dig en uppfattning om det är vad du söker, och om produkten kan lösa ditt problem. Sedan är det också en smaksak vilken produkt eller system man använder sig av. Till exempel. när det gäller säker mail, är man oftast van vid ett visst utseende på mail programmet.

Har ni några funderingar eller behöver hjälp så ta kontakt med mig via mail så ska jag hjälpa er så gott jag kan, och när jag har tid.

Tack för att ni läst och tagit till er artikeln, och hoppas den kan hjälpa er framöver.

Teddy ”Blue” Roswall (Informationssäkerhets Specialist), *för Nättidningen Payback / Payback Sverige*
securityhelp@nym.hush.com

Payback Sverige
C/o Schjerva
Kommendantsvägen 38
291 36 KRISTIANSTAD

Hemsida: www.payback.name
E-post: peter@payback.name