För att skydda sig mot oönskade intrång och risk för datastöld är det viktigt att tänka ha en god datasäkerhet i botten. Vi använder själva verktyg för krypterad trafik, som ssh för avlyssningssäker kommunikation med våra servrar och PGP för signering och kryptering av epost.

Vid programmering är det också viktigt att tänka på att kontrollera indata m.m. för att inte applikationen skall utsätta sig själv eller hela driftmiljön för onödiga risker.

Här delar vi med oss av några steg på vägen mot säkrare användning av Internet:

Säker webb

För webbtjänster som hanterar känslig information skall man skydda dataöverföringen mellan webbläsaren och webbservern med kryptering. Det gör man med https som skyddar mot avlyssning när data transporteras över Internet. Servern utrustas med ett SSL-certifikat som identifierar den och innehåller kryptonycklar. Klienter, som webbläsare, kan verifiera att servern är rätt motpart för kommunikationen samt använda kryptering för att skydda data som utväxlas med servern mot avlyssning.

Vi hjälper Dig gärna att uppgradera till en skyddad webbplats.

Säker epost

Vanlig epost är som att skicka vykort utan kuvert då de passerar ett antal servrar och nätverk i klartext på väg mellan avsändare och mottagare.Två saker man kan göra med enkla medel:

- skydda överföringen mellan epost-program och epost-server
- skicka krypterad epost genom att använda certifikat

Tyvärr är det inte helt enkelt och därför alldeles för många som fortsätter att "skicka öppna vykort" istället för säker epost.

Några konkreta tips:

- De flesta epost-program kan använda TLS för skydd av kommunikation mellan epost-program och epost-server (både SMTP och POP/IMAP). Det ger ett skydd mot lyssnare som annars kan snappa upp login och lösenord för Din epost, samt skydd av innehållet i meddelanden. Dock skyddas inte meddelandet när det lämnar epost-servern och går över Internet till mottagarens epost-server.
- 

Genom att installera PGP eller GnuPG kan man kryptera och signera meddelanden. Krypteringen ger skydd "end-to-end", alltså under hela överföringen från Din dator till mottagarens dator. Signering är också en viktig funktion för att säkerställa att avsändaren verkligen är den det ser ut som (då det är enkelt att skicka epost med falsk avsändare).

Själva använder vi epost-programmet Mozilla ThunderBird (kompis med webbläsaren FireFox) som med tillägget EnigMail och GnuPG ger smidig kryptering och signering av epost. För Outlook kan TLS ställas in. För kryptering och signering i Outlook rekommenderas den kommersiella produkten PGP.

En förhoppning är att fler installerar stöd för skyddad kommunikation då bägge parter måste ha skyddet installerat för att det skall fungera.

Kort om tekniken

Modern kryptering är oftast asymmetrisk och bygger på två nycklar (ett nyckelpar):

- En hemlig nyckel som endast nyckelns ägare skall ha tillgång till
- En publik nyckel som kan skickas till dem ägaren vill kommunicera med eller ännu bättre laddas upp på nyckelserver där andra kan ta del av den

Nyckelparet kallas ofta certifikat.

Poängen med de två delarna i nyckeln är att den publika delen används för att kryptera och den hemliga för att dekryptera. För att skicka ett krypterat meddelande till en mottagare behöver man alltså dennes publika nyckel, vilket enklast hämtas från en nyckelserver med mottagarens

epost-adress som sökbegrepp. Med mottagarens publika nyckel krypteras meddelandet och kan sedan enbart dekrypteras av mottagaren med certifikatets andra del: mottagarens hemliga nyckel.

Signering funkar åt andra hållet: avsändaren använder sin hemliga nyckel för att skapa en signatur till meddelandet. Mottagaren som har avsändarens publika nyckel kan med den säkerställa att meddelandet verkligen är från avsändaren och att meddelandet inte förändrats under överföringen. Det är mycket enkelt att förfalska avsändaradressen så signering borde användas i all viktig kommunikation.

Trådlös säkerhet

Det är väldigt smidigt att använda trådlösa accesspunkter med bärbara datorer, men om man inte konfigurerar nätet på rätt sätt riskerar man att öppna för både obehörig användning av anslutningen och för avlyssning av känslig trafik. Vi rekommenderar att man skyddar sig genom att aktivera WEP eller hellre WPA med ett lagom krångligt lösenord. Vill man öka säkerheten ytterligare rekommenderas MAC-filtrering och att nätverkets namn inte annonseras ut.

Våra tjänster

Vi assisterar Dig gärna med att säkra Din kommunikation, både webb, epost och trådlösa nätverk. Tveka inte att kontakta oss , någon kanske redan lyssnar på Din kommunikation.

Se Webbhotell | Webbportal