



Svårt avlyssna IP-telefoni

Okunnigt i TV: IP-telefoni inte lättare att avlyssna än vanlig telefoni. IP-telefoni kan dessutom göras omöjlig att avlyssna! I ett Rapportinslag om IP-telefoni 060129 påstår säkerhetsexperten André Rickardsson att IP-telefoni är osäkert, för att vem som helst med en Internetanslutning kan avlyssna samtalen.



I en TV-intervju påstår en säkerhetsexpert att vem som helst kan avlyssna IP-telefoni - vilket är helt felaktigt.

Påståendet är både okunnigt och felaktigt och det är tråkigt att fakta inte kontrollerats innan inslaget sändes. Precis som med vanlig telefoni måste man vid IP-telefoni ha tillgång till någon ledning som transporterar just det samtal som man vill avlyssna. Det sprids inte över hela Internet och inte ens över hela det interna företagsnätet. Det dataprogram som visades i TV gör bara att man nu kan avlyssna ett okrypterat IP-telefonisamtal på samma sätt som man kan koppla in en hörlur i kopplingskåpet där ett vanligt analogt telefonisamtal passerar!

När det gäller trådlös nätverksutrustning, så innehåller även den billigaste utrustningen kryptering av all trafik. Det gör IP-telefonisamtal är ytterst svåra att avlyssna den vägen, eftersom det både kräver lokal närvaro och att krypteringen knäcks (så länge krypteringen inte är avslagen förstås). Om det nu vore så enkelt att avlyssna IP-telefonisamtal, så kan man undra varför det diskuteras lagstiftning som tvingar IP-telefonioperatörer att installera extrautrustning för att polisen i brottsutredningar över huvud taget ska kunna känna till eller avlyssna IP-telefonisamtal.

I TV-inslaget nämndes tyvärr inte alls den intressanta utveckling som skett: Att IP-telefoni nu har standardiserats och kan göras helt omöjlig att avlyssna! En flora av IP-telefonilösningar ersätts snabbt av system som följer den sk SIP-standarden. SIP är inte bara Internetvärldens IP-telefonistandard, utan kommer att användas för all form av direkt person till person-kommunikation, t ex direkt-meddelanden, presence (närvaro) och videokonferenser, både på de privata näten och globalt över Internet.

På samma sätt som Internetstandarder gjort att vi idag inte kan vara utan e-post och webben, så kommer SIP att göra direkt personkommunikation över Internet lika oumbärlig. Med SIP behöver inte IP-telefoni vara isolerade öar som talar med varandra över det gamla telenätet utan trafiken sammankopplas över Internet. Då är det viktigt att säkerhet är på plats och sekretess kan upprätthållas då det behövs. Vis av tidigare Internetsstandarder har IETF - Internetvärldens standardiseringsorganisation - redan definierat en mängd säkerhetsfunktioner i SIP-standarden och några av dessa berör just avlyssning.



Inte i någon tidigare Internetstandard har det lagts ned så mycket möda på just säkerhetsfrågorna som i SIP. Orsaken är att SIP förväntas skapa nästa stora Internet-användning, precis som SMTP gav oss e-post och HTTP gav oss webben. Med SIP vill man inte behöva täppa till säkerhetsluckor i ett senare skede. Eftersom SIP är så välstandardiserat, finns redan idag brandväggar (eller tillsatsutrustning till som inte bara möjliggör global SIP-kommunikation, utan låter även brandväggen ha kontroll över vad som ska komma in till och ut från det privata nätet. Säkerhetsmedvetna företag, organisationer och myndigheter tillåter bara säkra applikationer som använder välkända protokoll att passera sin brandvägg.

Med SIP-kunniga brandväggar kan man använda IP-telefoni globalt över Internet och samtidigt behålla en mycket strikt säkerhetspolicy. Om man vill omöjliggöra för obehöriga att avlyssna samtal, så standardiserar SIP både hur samtalen och signaleringen som initierar samtalen kan krypteras. Det ger ett starkt avlyssningsskydd som vida överstiger skyddet för vanliga telefonsamtal. Man kan förvänta sig att dessa metoder kommer att finnas i fler och fler utrustningar allteftersom de efterfrågas. Få har dock behov att göra avlyssning ännu svårare än vad det är idag, vare sig det gäller vanliga samtal eller IP-samtal.

Sammantaget betyder det att IP-telefoni kan göras betydligt säkrare än det vanliga telefonnätet, om man gör det på rätt sätt och använder de säkerhetsmekanismer som finns i SIP.

Källa: Intertex