SÄKERHET &
SKADLIG KOD

Vi har information andra vill ha. En del försöker komma åt den genom att luras. Och vissa av dem är väldigt skickliga.

Försvarsmakten har it-system med hög säkerhet, men för att det ska fungera måste alla ta ansvar.

För inga säkerhetsåtgärder i världen kan skydda oss mot den mänskliga faktorn. Och det är den som oftast ställer till det.

Att ta sig in i säkerhetsklassade nätverk är svårt, men det blir enklare om man kan lura någon på insidan.

Ett vanligt sätt att luras är att förmå andra att föra in digital information som innehåller skadlig kod.

Skadlig kod är en datorkod som utnyttjar säkerhetshålen i din dator. Syftet är att ta kontroll över datorn och därefter resten av it-systemet.

VAD KAN HÄNDA DÅ?

1. Hemlig och sekretessbelagd information kan förvanskas, stjälas eller raderas.
2. Samtal kan lyssnas av och spelas in.
3. Datorer som är uppkopplade mot internet kan fjärrstyras så att mikrofon och kamera aktiveras.
4. Nätverket kan kartläggas för att kunna saboteras vid ett senare tillfälle.

Och det är lätt att trilla dit. Till exempel genom att använda en smittad usb-sticka.

Eller klicka på okända länkar och bilagor.

För även om alla vet att man ska vara försiktig, händer det ändå.

Det beror på att de som luras ofta är väldigt skickliga och på att metoderna för att sprida skadlig kod hela tiden ändrar skepnad.

Spam, eller massmejl, är till exempel inte längre det vanligaste sättet att sprida skadlig kod.

Istället blir det allt vanligare med skräddarsydda meddelanden som anpassas utifrån mottagaren. Avsändaren kan se väldigt trovärdig ut och se ut att komma från en myndighet eller till och med en kompis.

Det gör den svår att upptäcka.

ETT EXEMPEL – CLOUD HOPPER

Cloud Hopper var en hackergrupp som riktade in sig på it-leverantörer.

För att vara så trovärdiga som möjligt gjordes en ordentlig research om varje person som skulle kontaktas. På det sättet kunde de mejl som skickades anpassas till varje enskild mottagare.

En anställd som var fotbollstränare åt ett knattelag på fritiden fick ett mejl med rubriken *Ny speluppställning*.

Han öppnade mejlet med en bilaga om fotbollstaktik på felfri norska, men också en skadlig programkod som tog över hans dator, utan att han märkte det.

Genom att lura en anställd att öppna ett mejl med en infekterad bilaga kunde man alltså ta sig in i ett säkerhetsklassat nätverk.

Ingen säkerhetslösning står emot om någon från insidan håller upp dörren.

Öka ditt säkerhetsmedvetande på **forsvarsmakten.se/saker**

FÖRSVARSMAKTEN
MILITÄRA UNDERRÄTTELSE- OCH SÄKERHETSTJÄNSTEN