Snacka om IT-säkerhet!

www.sharp.se

SHARP
Be Original.

Komplicerade säkerhetuttryck på ett enkelt sätt

Cyberbrottslighet kan se ut på många olika sätt och konsekvenserna om ett företag blir utsatt ska inte underskattas.

För att verkligen kunna skydda dig, är det bra att förstå innebörden av begrepp och uttryck.

Nätverkssäkerhet

Hänglåset som skyddar din information

Precis som du låser in dina mest värdefulla saker i ett kassaskåp och kedjar fast cykeln, skyddar nätverkssäkerheten ditt företags känsliga information. Det är viktigt för alla affärsnätverk att ditt säkerhetsskydd inkluderar ett intrångsdetekteringssystem (IDS), som är utformat för att hålla utkik efter och identifiera potentiella hot, misstänkta aktiviteter, obehöriga åtkomstförsök på anslutna enheter, som bärbara datorer och skrivare.

Dataintrång

När känslig information från företaget eller kunden stjäls av cyberkriminella.

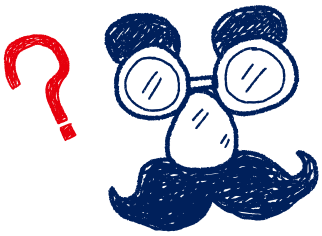
Du kanske inte vet om att det har hänt förrän mobilen och korten redan är i fel händer. Ett dataintrång är när känslig information, oavsett om den tillhör företaget eller en kund, stjäls av cyberkriminella. Ett dataintrång kan i slutändan leda till förlorat förtroende från kunder och användare, skadat varumärkesrykte och till och med höga böter.

Nätfiske, falska sms och samtal

En hackare som låtsas vara din chef, kund, bästa vän eller favoritbutik

De här attackerna är kanske inte uppenbara för ögat, men de är vanliga. Faktum är att omkring 90 % av cyberattackerna börjar med nätfiske (e-post), medan frekvensen av smishing (SMS) och vishing (röstsamtal) också ökar. Vi har alla fått e-post som dyker upp i vår skräppostmapp. Nätfiske, smishing och vishing är cyberattacker som lurar användare att klicka på e-post, svara på meddelanden och samtal.

Om attacken lyckas, kommer medarbetare omedvetet att luras att lämna ut känslig information som nätverkslösenord.



Malware

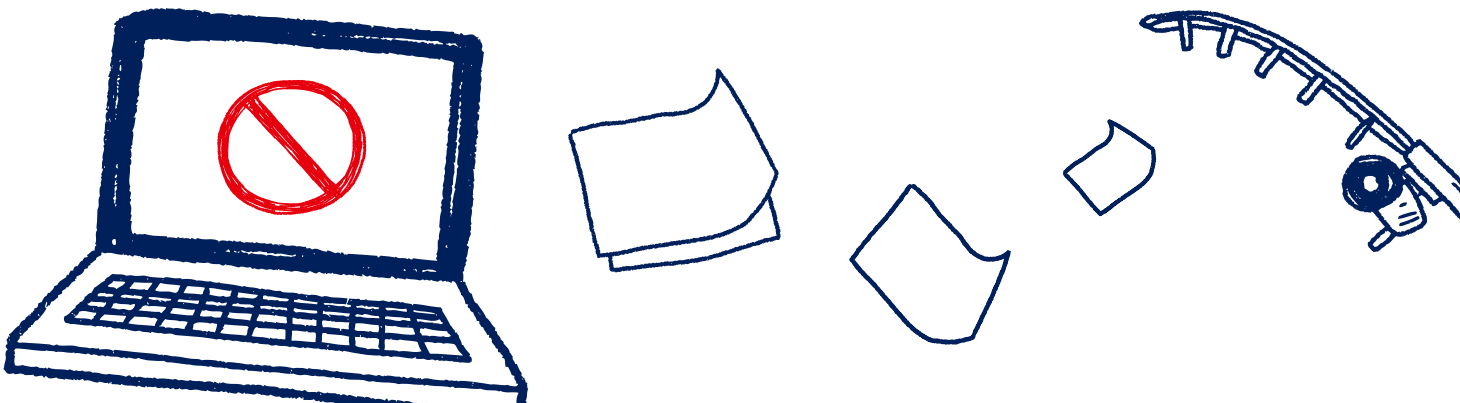
Elak programvara som är gjord med onda avsikter

“Malware” är en skadlig programvara som är designad för att skada ditt företags nätverkssystem – och hindra dig från att kunna använda dem. Som ett resultat av att öppna ett e-postmeddelande, klicka på en misstänkt länk eller besöka en osäker webbplats, kan skadlig programvara infiltrera ditt system. När det är gjort kan information som lagras i ditt nätverk tas över av hackare, vilket i sin tur leder till en ökad attack.

Ransomware

När data hålls som gisslan

Skadlig programvara - ransomware används vid cyberattacker för att förhindra ett företag att ha tillgång till kritisk affärsinformation genom att kryptera och låsa datan. Alla företag äger data, från finansiella register till testresultat från patienter och konfidentiella juridiska dokument. Att ha tillgång till sin egen data är avgörande, men när ransomware har infiltrerat ditt nätverk förlorar företaget sina viktigaste tillgångar. För att få tillbaka det måste lösensummor på ofta höga belopp, betalas ut till hackaren.



End-point security

Se till att alla dina enheter är lika säkra

Ditt digitala försvar börjar och slutar inte med din dator. Slutpunktssäkerhet innebär att det finns en process som säkerställer alla dina “slutpunkter”; från surfplattor till smartphones och andra internetanslutna enheter - som dina skrivare, har säkerhetsskydd. De bör hanteras centralt och övervakas för att garantera att det finns en realistisk bild av din cybersäkerhetsställning.

Kryptering

Din data mixas till en enda röra av siffror och bokstäver

Hur hindrar man att någon obehörig läser ett meddelande? Du mixar bokstäver och siffror. Det är vad kryptering gör. Den kodar oformaterad text - din känsliga data - till “cybertext”, vilket gör den oläslig för alla utan en “dekrypteringsnyckel”, det vill säga; lösenordet för att komma åt ett säkert trådlöst nätverk. Kryptering bör tillämpas på alla enheter, som din mobil och laptop, då kan innehållet inte läsas om enheten tappas bort eller blir stulen.

Patch management

Tänk på att uppdatera mobilen till senaste operativsystemet

Vi har alla stött på programuppdateringar på våra mobiler: “uppdatera nu till Windows 10” eller “installera iOS 9,999”. Dessa uppdateringar är en avgörande säkerhetsåtgärd. Patchhantering är processen för att uppdatera programvara, drivrutiner och firmware för att skydda sårbarheter i nätverket. Detta innebär övervakning av efterlevnad, hantering av de applikationer som ditt företag använder och att säkerställa att dina system fungerar till sin fulla potential.

Incidentrapport

Din handlingsplan för att avvärja en attack

Vad är det första du gör när ditt företag riskerar en cyberattack? En incidentrapport (IR) är det systematiska sätt för organisationer som vill planera hur de ska reagera på och hantera cybersäkerhetsincidenter effektivt. Att ha en tydlig handlingsplan på plats när ett hot dyker upp, kan förhindra attacker – och kan vara avgörande för att upprätthålla integriteten, konfidentialitet och tillgängligheten för känslig affärsdata.

Var säker hela tiden

Även om säkerhet är komplext är det viktigt att förstå innebörden. Sharp erbjuder ett heltäckande utbud av skräddarsydda säkerhetstjänster och lösningar, vilket gör det lättare för dig att hantera riskerna.

Sharp säkerhetshub