Ciscos problemlösarguide

Utnyttja IT fullt ut – tio viktiga råd om säkerhet för ditt företag

Säkerhet en del av allt företagande. Att kunna garantera att information, kunduppgifter och lokaler hanteras säkert är förmodligen en viktig fråga för dig – även om den inte är en del av din huvudsakliga inriktning. Problemet är att det finns så mycket information – men väldigt lite som ger den hjälp du behöver. Icke-experten ska ständigt ta beslut som att ”Jag måste ha en brandvägg, men den är väl inbyggd i Windows?” Behöver jag verkligen en?

I den här guiden hjälper vi dig igenom ett antal frågor och ger dig den information du behöver. Vi tar också upp frågor som snarare har med företagsledning än teknik att göra. Frågor du ställs inför om du tycker det är viktigt att skydda ditt företag.

Tio viktiga råd

1. Virusskydd:

Antiviruspaket är bra, men långt ifrån alla ger tillräckligt skydd. Du känner säkert till att virusskydd fungerar genom en databas, som innehållermed uppgifter om olika hot vid en given tidpunkt (det är därför det är så viktigt att se till att virusskyddet hela tiden uppdateras).

Det betyder att om ditt virusskydd inte ”känner till” ett visst virus är du oskyddad. Det är därför Cisco® rekommenderar både virusskydd och intrångsskydd (IPS). Skillnaden är att skydden verkar i två steg: 1) Först granskas all information av en IPS-detektor, som letar efter sådant den inte gillar, och 2) därefter kontrolleras eventuella avvikelser via ett program i din dator. Med andra ord letar den inte bara efter virus den känner till, utan sätter även stopp för koder som börjar göra otrevliga saker – tar bort filer, söker igenom din kunddatabas eller liknande. Det här kallar säkerhetsexperter för nolldagsattack – svagheter eller brister i program eller system utnyttjas innan tillverkaren själv känner till dem. Genom att hålla utkik efter sådant som avviker snarare än sådant vi redan känner till kan vi stoppa attacken.

IPS-systemen arbetar på olika nivåer – som värdbaserade eller nätverksbaserade. Ett nätverksbaserat IPS-system sitter i ingångspunkten till ditt nätverk. Ett värdbaserat IPS-system sitter på din bärbara dator och inte i ditt nätverk – när du kopplar upp dig mot andra nätverk är du fortfarande skyddad.

2. Brandvägg:

En brandvägg är så mycket mer än en kryssruta där det står ”Jag har en brandvägg”. Vissa är inbyggda i operativsystemet, andra ligger på separata datorer i nätverket.

En viktig fråga är vad brandväggen ska leta efter. Flera av dem letar efter vad som uppfattas som en attack mot nätverket, vilket är en viktig del av det skydd du behöver. På Cisco erbjuder vi också skydd på tillämpningsnivå. Det betyder att om en del av en kod försöker få ett enskilt program att uppföra sig konstigt kommer det att upptäckas. Det är viktigt att brandväggen inte finns på din egen dator utan på en annan dator, router eller utrustning som fungerar som nätport till ditt nätverk. Om det är den enda nätporten som passeras för att komma in i ditt datorsystem är det lämpligt att installera någon form av skydd på den. Cisco erbjuder säkerhetssystem på flera olika nivåer.

3. Medarbetarna:

Innan vi går djupare in i tekniska detaljer är det lämpligt att fundera över hur stor del av riskerna ett företag ställs inför som inte har med teknik att göra. Här följer några exempel där medarbetare förlorat data eller fått sina uppgifter förvanskade:

- I en genomarbetad policy beskrevs vem som hade rätt att se vad i elektroniskt lagrad data – men det stod inget om vad som gällde för utskrifter som glömts kvar på tåg, hotell, osv.
- Om du inte lyckas få medarbetarna att förstå att de måste släcka ned skärmen när de lämnar skrivbordet kan besökare läsa – och läser – konfidentiellt material på skärmen (skärmsparare drar el i onödan och skyddar inte längre skärmen som förr).
- Vi måste ta upp en annan sak eftersom det fortfarande förekommer: din hunds eller partners namn, eller namnet på gatan där du bor. De är inte säkra lösenord precis som ordet ”lösenord”.
- Det är i sig en säkerhetsrisk att inte ha en tydlig policy om hur nätverket ska göras säkert, vem som ska göra det och vilka påföljderna blir om man inte följer policyn. Alla som behandlar sina medarbetare som vuxna, intelligenta individer märket hur samarbetet fungerar bättre.
- Lägg till i policyn att det inte är tillåtet att ladda ned program hur som helst. Oftast är det ingen fara men du måste ha koll på programlicenser och skydda dig mot risker med eventuella sabotageprogram.

4. Utrustningen:

Utrustning som tas med in i och ut från en byggnad: Om du arbetade för försvarsmakten skulle du vara tvungen att lämna in din mobiltelefon eller musikspelare vid entrén och få tillbaka den först när du lämnade byggnaden. Det beror inte på att man inte litar på att folk gör sitt jobb i tid utan på att mobiler, kameror och liknande utrustning kan innehålla data. En iPhone 3G (vi valde den eftersom den är populär) har i vissa fall ett minne på 16 Gb. Den kan anslutas till datorns USB-port och vem som helst kan råka lämna kontoret och få med sig hela din kundlista. En annan risk är att någon överför virus till ditt datasystem.

Du kanske inte vill gå så långt att du förbjuder alla former av bärbar, personlig datautrustning på din arbetsplats, men du kan vidta vissa åtgärder:

- Datorer kan konfigureras så att de inte accepterar USB-utrustning.
- Intelligenta övervakningsprogram, som det som ingår i Ciscos samtliga produkter, upptäcker avvikande aktivitet i ditt nätverk och rapporterar det till dig.
- Om du har besökare som loggar in på ditt nätverk är det nödvändigt att se till att utrustningen (om besökaren använder egen bärbar dator) är virusskyddad och lika säker som din egen. Den utrustning som Cisco erbjuder kontrollerar datorer och annan utrustning i samband med inloggningen och identifierar både virus och avvikande aktivitet.

5. Dataskydd för hem- och distansarbete:

Det är givetvis ingen vits att skydda ditt interna nätverk om det börjar läcka information utanför kontoret. Det innebär flera saker. Först och främst måste du se till att varje länk till ditt nätverk från Internet går genom ett lämpligt sk VPN (Virtual Private Network) med alla de säkerhetsfunktioner som hör till. För det andra måste du se till att samma säkerhetskrav gäller för varje icke-teknisk del av medarbetarnas aktiviteter som när de är på kontoret. Om medarbetarna inte får skriva ut dokument, spara uppgifter på USB-minne osv. när de är på kontoret är det inte okej att göra det hemma.

Mycket av ovanstående kan du uppnå om du installerar ett intelligensstyrt nätverk på kontoret och skyddar nätporten med rätt produkter från Cisco.

6. Trådlöst nätverk:

En förutsättning för att garantera dataskydd för hem- och distansarbete är att undersöka det trådlösa nätverket, både internt och externt. Lita inte på ett nätverk som påstås vara ”säkert” när en bärbar dator eller en smarttelefon hittar det – det kanske bara har WEP-säkerhet, vilket är föråldrat och enkelt för hackare att ta sig förbi.

På kontoret har all nätverksutrustning som Cisco levererar ett inbyggt säkerhetssystem som standard och kan konfigureras av våra sakkunniga partner. Utanför kontoret kan dina medarbetare använda egen trådlös utrustning. Det är viktigt att utrustningen skyddas på följande sätt:

- Om den har WEP-kryptering behöver den uppgraderas till WPA.
- Lösenord som används rutinmässigt i hemutrustningen bör bytas ut.
- Routern till datorn och nätverket har ett nätverksnamn som kallas SSID, som du hittar i routerns inställningsmeny. Ändra det och se även till att SSID-namnet inte sprids så att andra ser din dator om de är ute efter ett nätverk att hacka.
- Stäng av autoanslutningen till WiFi-nätverk så att användarna bara kopplar upp sig mot nätverk du litar på.
- Bestäm en statisk IP-adress för din utrustning. Alternativet är att ditt nätverk slumpmässigt bestämmer adress, vilket kan bli problematiskt om du vill koppla bort en viss utrustning.
- Du har förmodligen en brandvägg på din router – kontrollera att den är aktiverad eftersom många normalt levereras i avstängt läge.
- Stäng av nätverket om du inte ska använda det en längre tid.

7. Hackare – hur stor är risken?

Hittills har vi tagit upp hur man undviker hackare och hur man förhindrar oönskat intrång i datornätverket. Men hur troligt är det att någon försöker ta sig in i ditt system? Många av Ciscos kunder är mindre företag som undrar om någon verkligen kan vara intresserad.

Tidigare var hackaren alltid en person och då var frågan mer relevant. Problemet nu är att många ”hack” och intrång numera sker med automatik. Tänk på hackaren som en ledare för flera brottslingar som måste bryta sig in i oövervakade hus för att ta reda på om det finns något värt att stjäla. I det här fallet är husen istället datorer som ser likadana ut. Enda sättet att ta reda på om de har något av värde är att ta sig in och se efter.

Det görs genom ”bottar” som sprids automatiskt på Internet och som gör något som kallas för ”portskanning” – de kommer till ”porten” till ditt nätverk på Internet och ser efter om porten är låst. Det ligger helt klart i ditt intresse att se till att det är låst.

Och glöm inte dina riktiga dörrar. Cisco erbjuder kameror som kan länkas till Internet så att du kan se vad som händer på kontoret oavsett var du befinner dig. Vissa av dem aktiveras av rörelse och skickar en varning till dig om någon tagit sig in.

8. Internetförsäljning:

Om du har försäljning på Internet måste du absolut vidta åtgärder för att skydda både kunddata och lagerinformation. Samtliga åtgärder som vi nämnt bidrar till ett sådant skydd, men det finns några fler – återigen vill vi betona att de här åtgärderna är en ledningsfråga i lika hög grad som en teknisk angelägenhet och innebär till exempel att man inte bör glömma en CD med dekrypterade filer på bussen! (Kom ihåg att kryptera dina CD-skivor – då kan ingen läsa den information som finns där även om någon lyckas komma över ditt lösenord).

9. Hur kan säkerhet löna sig?

Många småföretagare måste, särskilt i ekonomiska orostider, se till att varje teknisk investering betalar sig. Det är svårare när det gäller något så abstrakt som säkerhet. Förmodligen har du någon gång betalat för att installera lås hemma, men du har aldrig räknat på hur lång tid det tar innan investeringen betalar sig. Du vet bara vad du kan förlora om någon bryter sig in.

I vissa fall är det däremot enkelt att prata om avkastning på gjorda säkerhetsinvesteringar. Om du driver ett e-handelsföretag och till exempel inte kan säkra kundernas uppgifter riskerar du att få se din verksamhet tyna bort. Om du har besök av en kund som ansluter sig till ditt nätverk och åker hem med ett datavirus, har du förmodligen sett din kund för sista gången. Det finns fler exempel.

Det är värt att tänka på att det sällan är grundutrustningen som kostar en förmögenhet. Ett litet kontor med en handfull medarbetare kan få en bra trådlös router med brandvägg och fullgod säkerhet för mindre än 2 000 kronor.

10. Outsourca säkerhet:

Om du fortfarande tycker säkerhet verkar besvärligt kan det vara värt att fundera på att outsourca företagets infrastruktur för säkerheten. Flera av Ciscos partner har specialiserat sig på att hjälpa mindre företag bli säkrare. Alla har en gedigen expertkunskap som det knappast är värt mödan för dig att uppnå. Många mindre företag väljer att lägga ut datahanteringen externt hos ett specialiserat företag som en extra säkerhetsåtgärd.

Som vi sa i början är du som företagare, oavsett inriktning, även en del av säkerhetsbranschen. Lyckligtvis är startkostnaderna för ett säkert nätverk låga. Våra experter står redo att hjälpa dig komma igång.

Lycka till!