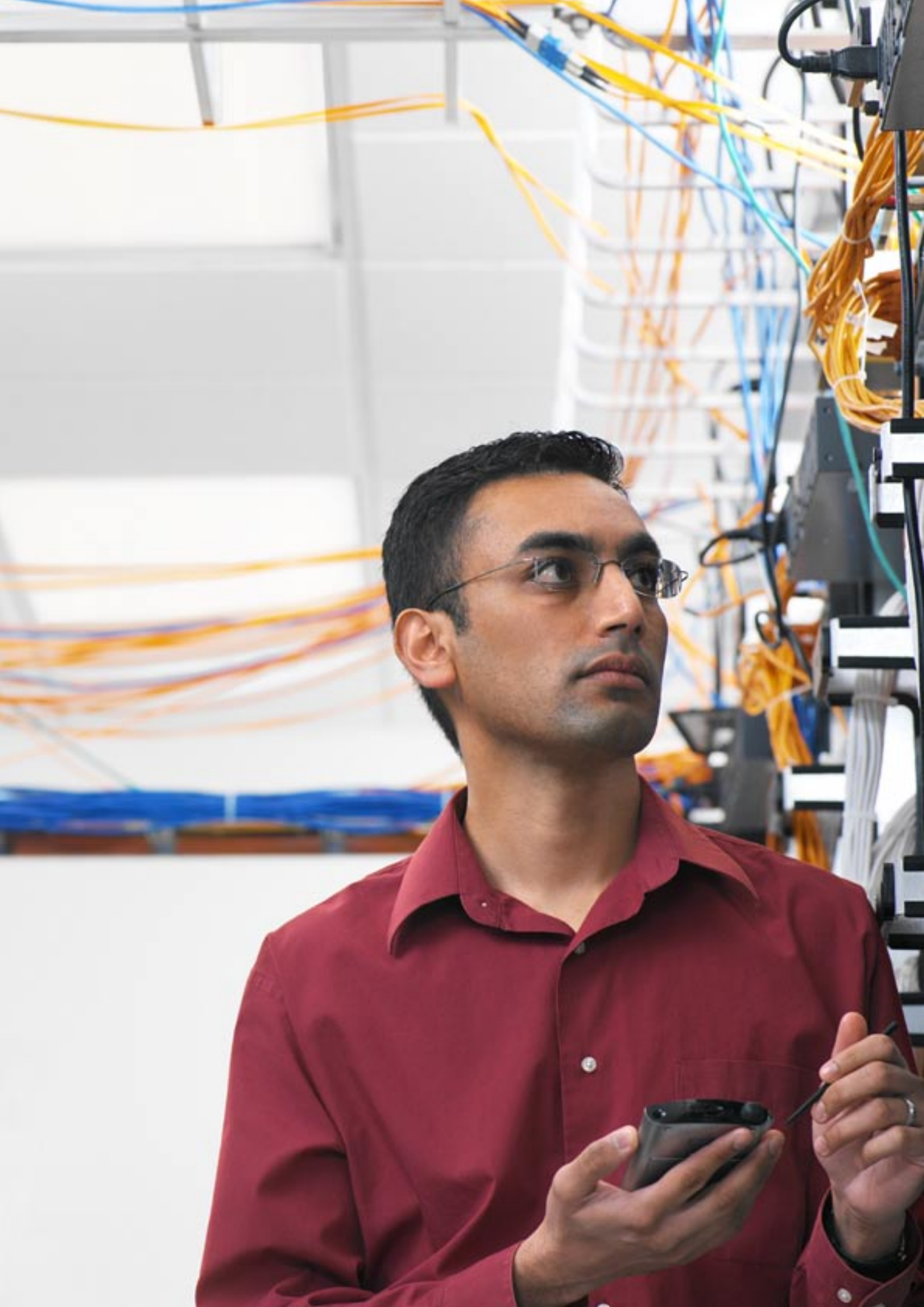
Säkerhet.

Hoten mot informationsnäten – att bedöma och hantera risker.



Hur skapar du det säkra nätverket?

IT-säkerhet är en fråga om att bedöma och hantera den risk som företaget utsätts för – det som vanligtvis kallas Risk Management.

Hur mycket säkerheten för ditt företag får kosta beror på organisationen och vad ni riskerar att förlora. För en samhällsviktig myndighet eller t.ex. en bank, som har mycket stora värden att försvara, kan väsentliga investeringar i säkerhetsinfrastrukturen motiveras.

Hur utnyttjar du effektivt de möjligheter som nya tekniker kan ge? Hur minimerar du riskerna på ett kostnadseffektivt sätt? Hur skapar du det säkra nätverket?

Hackers, maskar, trojaner och andra hot. Varje dag läser vi i tidningarna om ständigt återkommande attacker mot vår IT-infrastruktur. Ord som hackers, virus, spam och belastningsattacker blir allt vanligare och du känner säkert igen företeelser som dessa:

- En virusmask har invaderat det interna nätverket och sprider sig blixtsnabbt från dator till dator. Infekterade datorer börjar fylla nätet med trafik för att smitta så många andra datorer som möjligt. Efter några sekunder är infrastrukturen så hårt belastad att alla legitima applikationer har slutat att fungera.
- En hacker har skickat ett e-postmeddelande med en bilaga till en av våra anställda. Den anställdes maskin beter sig till synes helt normalt, men i bakgrunden samlar trojanen – som fanns dold i bilagan – information från datorn och kopierar obemärkligt filerna till en server på Internet.
- En missnöjd anställd är på väg att säga upp sig. Först vill han dock ta med sig användbar information till sin nästa arbetsgivare. I det tysta installerar han en ”sniffer” på sin dator för att försöka fånga upp lösenord på nätverket. Med hjälp av ett av dessa lösenord kan han sedan ta sig in på exempelvis en filserver han normalt inte har access till.
- En utpressare hotar ett webbaserat företag – som är helt beroende av sin webbplats. Om man inte betalar kommer tusentals zombies (hackade maskiner som fjärrstyrs av utpressaren) att börja generera en så hög last mot webbplatsen, att de legitima kunderna stängs ute.

Priset som det drabbade företaget får betala blir ofta högt, oavsett om det handlar om förlorade intäkter, missnöjda kunder, datorer som måste installeras om – eller något ännu kostsammare.

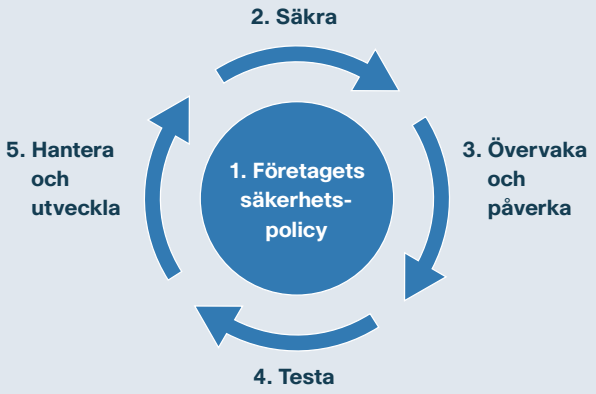
Hur hanterar du risken?

Att upprätta en säkerhetsplan är ett viktigt steg för alla företag som på ett metodiskt sätt vill arbeta med den egna IT-säkerheten.

I en säkerhetsplan bör man först definiera vilka risker man löper och är villig att löpa, t.ex. i produktionsbortfall, eller stulen eller förfalskad information. I säkerhetsplanen bestämmer man sedan den process som ska användas för att hantera riskerna.

En effektiv metod att beskriva den löpande säkerhetsprocessen är det s.k. säkerhetshjulet.

Säkerhetshjulet är en metod för att beskriva företagets löpande säkerhetsprocess.



Allt cirklar kring säkerhetspolicyn där man noga har definierat situationen. Vilka risker kan vi ta? Vilka risker vill vi minimera? Vad ska vara tillåtet? Etc.

- Man säkrar systemet med tillgängliga verktyg som t.ex. brandväggar, antivirus-skydd och system för engångslösenord, men även – som vi ska se – med nät-verksutrustning.
- Man övervakar systemet kontinuerligt, identifierar eventuella avvikelser och sätter vid behov in motåtgärder.
- Man testar systemet regelbundet och då även ansvarig personal för att testa hur snabbt man upptäcker en attack. Tester sker ofta med hjälp av externa konsulter, men även med automatiserade analys-verktyg.
- Man hanterar systemet och utvecklar det efterhand som kraven och hoten förändras.

Skalförsvar eller säkerhet på djupet?

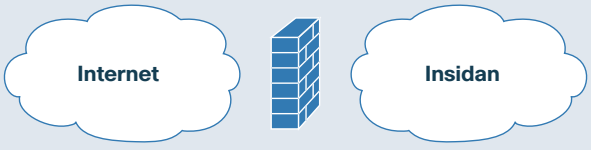
Under mitten av 1990-talet var brand-väggen företagens centrala verktyg för att säkra IT-systemen. Likt byggandet av en traditionell försvarsmur placerade man en brandvägg mellan det interna nätet och Internet för att stoppa hackers från att nå in i det interna nätverket.

Även om brandväggen fortfarande är ett mycket funktionellt verktyg för att höja säkerheten, har allt fler företag insett att denna typ av skalförsvar inte är tillräcklig. Och några av anledningarna till detta är:

- Ökad mobilitet. En bärbar – och oskyddad – dator, som ena dagen var uppkopplad mot Internet via ett bred-bandsabonnemang utanför företaget, kan nästa dag kopplas upp på företagets interna nätverk.
- Sofistikerade attacker. Många av dagens attacker från hackare och virus gömmer sig i applikationer – t.ex. webb och e-post – som brandväggen tillåter.
- Dynamiska relationer. När företags-uppköp, fusioner, partnerskap och nya affärsrelationer gör det interna nätet alltmer komplext blir utgångarna mot Internet lätt fler än man har kontroll över.

När brandväggen inte räcker till för att trygga infrastrukturen, ligger lösningen istället i en ny syn på de ingående kompo-nenterna i nätverket.

Klassiskt skalförsvar med brandvägg.



Höj säkerheten i nätverket.
Att etablera ett betydligt mer robust och djupgående försvar än ett skalförsvar är inte komplicerat. Lösningen ligger i att utnyttja säkerhetsfunktionerna i nätverksutrustningen innanför brandväggen.

Att nyttja redan befintliga funktioner är dessutom mycket kostnadseffektivt. Utrustning som routrar, switchar och accesspunkter finns redan på plats för att forsla trafik och förmodligen övervakas de redan av övervakningssystemen. Att addera säkerhetsfunktioner till existerande utrustning minimerar både kapital- och driftskostnader.

Ciscos SAFE-modell är en heltäckande säkerhetsstrategi för nätverk och omfattar såväl utformning som införande och underhåll. SAFE-modellen är indelad i moduler, som motsvaras av de moduler som normalt används vid nätverksdesign.

Det säkra nätverket bygger på att vissa funktioner och principer för säkerhet fastställs och tillämpas. Några av de viktigaste reglerna är:

Kontrollera användarna och deras datorer.
Säkerheten måste vara lika hög oavsett hur man ansluter sig – fjärranslutning från en distansarbetare, från en filial eller från huvudkontoret, via kabel eller trådlöst.

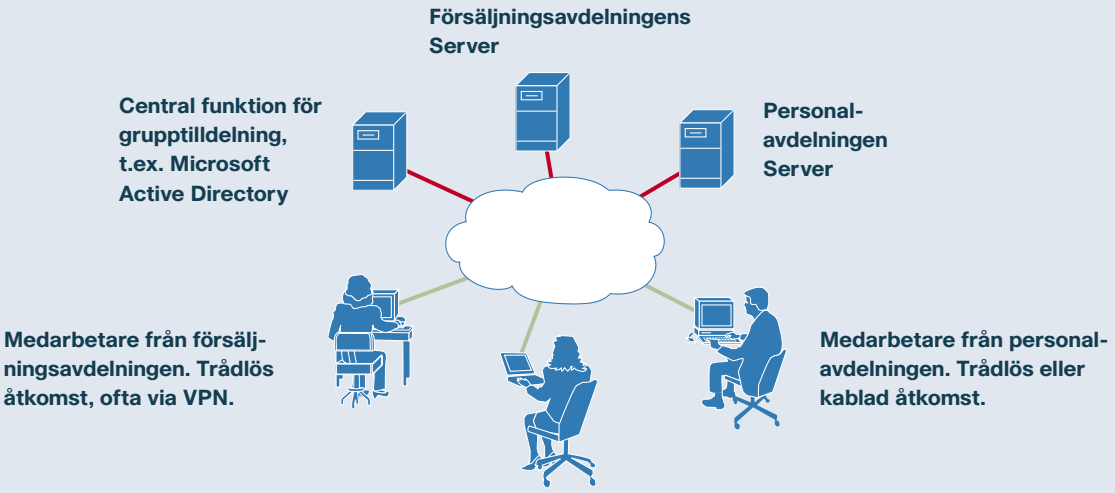
Det säkra nätverket måste kunna identifiera de användare som ansluter sig, och begränsa respektive användares rättigheter. Förutom att användarna identifieras bör säkerhetsnivån på deras datorer fastställas, t.ex. om antivirusprogrammet är uppdaterat, och tilldela rättigheter därefter.

Låt oss illustrera detta med några praktiska exempel:

- Åsa tillhör personalavdelningen. Hennes dator har de senaste antivirusuppdateringarna och de rekommenderade ”Hotfixarna” från Microsoft. Därför ska hon ha full åtkomst till Internet, men även till gemensamma servrar och till personalavdelningens lönesystem.
- Ylva är säljchef och borde ha tillgång till såväl Internet som filservern med säljavdelningens offerter. Men eftersom hon inte har uppdaterat sitt antivirusprogram efter semestern har hennes dator satts i karantän. Den får endast tillgång till en server från vilken hon kan ladda ned de senaste uppdateringarna. När uppdateringarna är installerade återfår hon automatiskt sina rättigheter.
- Ulf är konsult och har inte tillgång till det interna nätet. Däremot får han komma åt Internet och han tillåts också koppla upp sig med VPN mot sitt företag.

För att kunna erbjuda dessa och ytterligare en mängd säkerhetsfunktioner, har Cisco utvecklat Cisco Network Admission Control (Cisco NAC), en arkitektur som ingår i Ciscos nätverksutrustning (routrar, switchar, trådlösa accesspunkter) och som även fungerar med produkter från flera andra leverantörer, t.ex. antivirusprogram från Trend Micro, Mcafee och Symantec samt en rad andra leverantörer.

Här jobbar personalavdelningen mot personalavdelningens servrar, samtidigt som personal från försäljningsavdelningen jobbar mot försäljningsavdelningens servrar. Ingen avdelning kommer åt den andra avdelningens resurser.



Skydda datorerna.
Cisco NAC säkerställer att alla maskiner som ansluter sig till nätverket har en tillräcklig säkerhetsnivå. Kraven varierar beroende på verksamheten. Antivirusprogram med aktuella uppdateringar installerade och en personlig brandvägg är dock ett baskrav.

Men även det bästa virusskydd kan svikta vid en s.k. Day Zero-attack – en attack som inträffar innan virusskydd eller uppdatering finns tillgängliga.

För att stoppa Day Zero-attacker har Cisco utvecklat Cisco Security Agent (CSA) som, istället för att utgå från kända signaturer, använder avancerad beteendeanalys för att identifiera och stoppa nya attacker. I CSA finns hundratals beteenderegler fördefinierade, men dessa kan naturligtvis modifieras och nya, egna regler kan adderas. Så här kan reglerna se ut:

- Ett program som laddats ned från nätet öppnar upp utgående sessioner mot flera andra maskiner. Detta skulle kunna vara ett virus och stoppas därför.
- En webbläsare vill plötsligt modifiera en viktig systemfil – förmodligen beroende på ett säkerhetshål i webbläsaren. Detta stoppas eftersom beteendet inte är normalt.
- En webbserverprocess börjar skriva filer i stället för att läsa dem. Detta stoppas då det är ett onormalt beteende för en webbserver som tyder på att den har blivit angripen.

Begränsa trafikflödena.
Nätverket måste också kunna begränsa trafikflödena, alla behöver ju inte komma åt hela nätverket. Exempelvis ska endast personalavdelningen och ledningen kunna komma åt personalavdelningens servrar.

Detta kan åstadkommas på olika sätt, t.ex. genom att nätverket separeras i olika Virtuella LAN (VLAN – Virtual Local Area Network).

En stor fördel är att denna separering inte kräver extra nätverksutrustning, då man tillämpar logisk separering. En annan fördel är att full mobilitet kan behållas. När personer på olika avdelningar ska byta plats, måste inte nätverksenheterna konfigureras om – det säkra nätverket kan dynamiskt tilldela användarna deras rättigheter. Vanligt är att återanvända Microsoft Active Directory-katalogen, och dess gruppering av användarna – t.ex. i olika avdelningar – för att definiera deras olika rättigheter.

- Privata Virtuella LAN (Private VLAN eller Private VLAN Edge) är ett annat sätt att separera nätverket. Funktionen förhindrar direkt IP-kommunikation (Internet Protocol) mellan två användare, även om de sitter på samma VLAN. Därmed minskar risken för att t.ex. en användare ska smitta en annan via en mask.

Naturligtvis kan alla användare fortfarande kommunicera med varandra via e-post eller instant messaging-applikationer, men genom att trafikflödena begränsas är det möjligt att kontrollera exakt hur denna kommunikation sker.

Inspektera trafiken.
För att upptäcka onormala trafikmönster och hackerangrepp innehåller Ciscos nätverksutrustning flera funktioner som inspekterar trafiken, oftast på olika nivåer. Så är t.ex. switchar väl lämpade för att inspektera trafiken på nivå 2 och 3, där de kan verifiera att avsändaradresser och protokoll som används är rimliga.

En kritisk funktion i ett nätverk är utdelandet av IP-adresser. Nätverket måste kunna kontrollera att IP-adresser delas ut endast av vissa dedicerade DHCP-servrar (Dynamic Host Configuration Protocol). En falsk eller felkonfigurerad DHCP-server kan orsaka mycket stor skada och i princip stänga en del av nätet.

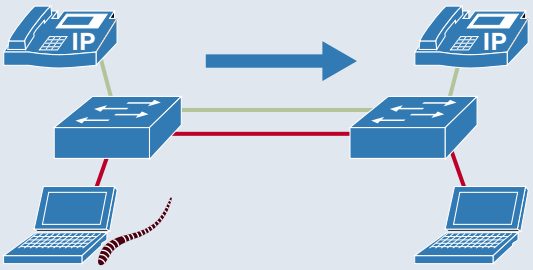
Nätverket måste också kontrollera att ingen utrustning förfalskar sin IP-adress. Förfalskade avsändaradresser utnyttjas ofta av hackers, vilket försvårar felsökning och spårbarhet, t.ex. när man vill finna en maskinfekterad maskin.

Att hacker- och virusangrepp använder samma protokoll som legitim trafik skapar stora problem. Så kan t.ex. webb- och e-postprotokollen utnyttjas av hackers och maskar för intrång i servrar. Tack vare IPS (Intrusion Prevention Systems) kan dock trafiken analyseras på applikationsnivån och därmed kan otillåten trafik, som hacker- och maskangrepp, stoppas. Ciscos IPS-system finns såväl fristående som integrerade i brandväggar, VPN-utrustning, routrar och switchar.

Prioritera affärskritiska applikationer.
Vissa situationer, exempelvis ett utbrott av en virusmask, leder till onormala trafikmönster i nätverket. Eftersom virusmasken vill sprida sig så fort som möjligt genererar den extremt mycket trafik. Exempel visar att bara ett dussintal infekterade maskiner kan konsumera alla tillgängliga nätverksresurser även för större företag.

Det säkra nätverket bör därför tillämpa prioritering, vilket innebär att den affärskritiska trafiken alltid kommer fram – även i en överbelastningssituation. Vilka applikationer som är kritiska för verksamheten varierar från företag till företag. Det väsentliga är att denna trafik prioriteras, och att nätverkutrustningen konfigureras därefter, innan en överbelastningssituation uppstår.

En verksamhetskritisk applikation, i det här fallet IP-telefoni, prioriteras och fortsätter att fungera även under ett maskutbrott.



Internetuppkopplingen.
Kopplingen mot Internet används vanligtvis för flera ändamål, främst utgående och inkommande e-post, utgående surfning mot Internet, inkommande surfning mot den egna organisationens publika webbservrar samt för att ge distansarbetare möjlighet att koppla upp sig via VPN.

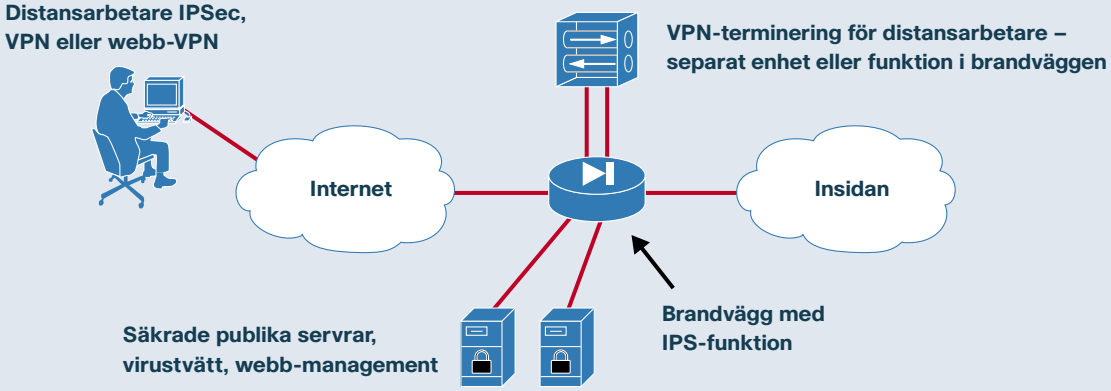
Brandväggen är och förblir en mycket viktig komponent för kontroll av Internettrafiken, men det innebär också att kraven är många.

För att kunna hantera en ökning i såväl trafikvolym som antalet säkerhetszoner bör brandväggen vara skalbar. Dess prestanda bör vara dimensionerad för att även hantera abnorma situationer. Brandväggen bör också kunna kompletteras med avancerade funktioner för att stoppa attacker på applikationsnivå (Intrusion Prevention System). Övervakning är en annan viktig funktion, därför bör alarm från brandväggen kunna bevakas av samma utrustning som övervakar samtliga säkerhetsrelaterade alarm.

VPN-uppkopplingar, för t.ex. distansarbetare, kan hanteras av antingen brandväggen eller en separat VPN-utrustning. I bägge fallen krävs stöd för stark kryptering i hårdvara och starka identifieringsmetoder som t.ex. certifikat. För distansarbetare finns två olika tekniker: VPN baserade på IPSec (Internet Protocol Security), som kräver en IPSec-klient på datorn, och webbaserade VPN, som inte kräver en förinstallerad klient på datorn. Eftersom båda uppkopplingsformerna har för- och nackdelar, är det ett stort plus om VPN-utrustningen kan hantera båda.

I anslutning till Internetuppkopplingen finns också företagets publika servrar, ofta webb- och e-postservrar. Dessa servrar ska naturligtvis säkras upp på bästa sätt

En typisk Internetuppkoppling.



för respektive operativsystem och applikation. Genom att installera en speciell säkerhetsprogramvara som Cisco Security Agent (CSA) är det möjligt att höja säkerheten ytterligare.

Den typ av attack som kanske är svårast att försvara sig emot är belastningsattacken. En sådan utförs av en angripare som fjärrkontrollerar ett mycket stort antal datorer (ofta bredbandsanslutna datorer som blivit hackade). Dessa s.k. zombies används sedan för att generera enorma mängder trafik mot den attackerade webbplatsen.

Det som gör en sådan attack så allvarlig är att den kan drabba trånga resurser i operatörens nät – t.ex. genom att fylla all tillgänglig bandbredd – och att det då redan är för sent för brandväggen att stoppa attacken. Bästa sättet att hantera detta är att välja en operatör som förstår riskerna – och som har investerat i utrustning och personal för att bekämpa och stoppa denna typ av attacker.

Övervakning.

Det säkra nätverket måste också kunna övervakas på ett kostnadseffektivt, men ändå säkert, sätt. Detta innebär att man från en central punkt kan definiera de policies som gäller i nätverket. Dessa appliceras sedan på all nätverksutrustning – routrar, switchar, brandväggar, VPN-system och IPS-system.

Lika viktigt som att definiera dessa policies, är det att kontrollera att de efterföljs. Man bör därför centralt kunna bearbeta information (larm och loggar) som är relevanta för säkerheten i nätverket.

Trots att säkerhetsinformationen kommer från olika typer av utrustning (routrar, switchar, brandväggar, IPS-system, datorer, servrar och applikationer) är det möjligt att redan på ett tidigt stadium upptäcka attacker och vidta åtgärder tack vare automatisk och intelligent bearbetning av dessa data.

Cisco MARS (Monitoring Alarm Resonse System) kan ta emot loggar från vitt skilda typer av utrustning (inklusive andra leverantörers säkerhetssystem och loggar från Windows och Unix system). Genom att Cisco MARS känner till nätverkstopologin kan information summeras och presenteras grafiskt på ett överskådligt sätt. Vilken maskin har attackerats? Har attacken lyckats? Varifrån kom attacken?

En säkrare framtid.

Samtidigt som hoten mot företagens IT-säkerhet och nätverk blir fler, blir också motåtgärderna i form av nya tekniker och utrustning fler och effektivare.

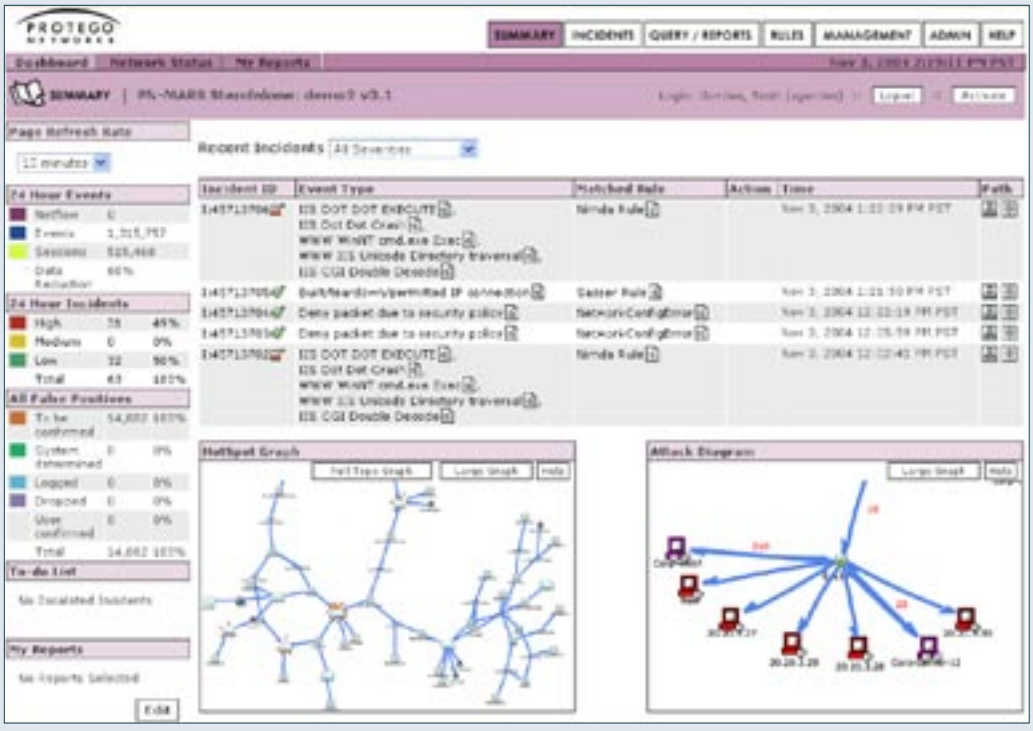
Effektiv IT-säkerhet idag handlar om kunskap och förutseende, om att hantera och minska riskerna på ett kostnadseffektivt sätt samt att välja leverantör av säkerhetsutrustningen med omsorg.

Det traditionella skalförsvaret är inte längre tillräckligt. I en tid då både användare och nya samarbetsformer kräver allt större mobilitet och öppenhet, ställs företagen inför allt mer avancerade hotbilder.

Genom att komplettera skalskyddet med säkerhetsfunktioner i det egna nätverket kan varje företag få ett mer djupgående skydd och därmed dramatiskt förbättra sin säkerhet. Detta kan göras mycket kostnadseffektivt, tack vare minimala kostnader för köp av extra utrustning, utbildning av personal, supportavtal och övervakningssystem.

Cisco Sverige har lång erfarenhet av att utforma säkra nätverk. Oavsett nätverkens komplexitet och organisationens storlek kan vi erbjuda ditt företag en säkerhetslösning som är både effektiv och kostnadseffektiv.

Övervakningen bör bearbeta säkerhetslarm från alla säkerhetsfunktioner och presentera informationen på ett överskådligt sätt.



Cisco Systems är världsledande på nätverkslösningar för Internet. Våra hård- och mjukvarubaserade produkter och tjänster används för att skapa Internetlösningar för kommunikation med data, tal och video mellan personer, företag och länder oavsett skillnader i tid och plats.

Så skulle nog många, helt korrekt, beskriva oss. Men frågar du våra kunder, kan svaret bli helt annorlunda: ”Cisco hjälper oss att arbeta smartare, säkrare och effektivare.”

Hela vår verksamhet kretsar kring teknik och teknikutveckling. Och tekniken kommer alltid att vara viktig för oss – men aldrig som ett mål, utan ett verktyg.

Vår tekniska vision är det intelligenta informationsnätet som kommer att förändra sättet vi arbetar, leker och lär på. Vi drivs av övertygelsen om det intelligenta informationsnätet som en strategisk resurs – att det mer än något annat kan bidra till att arbeta säkert, optimera verksamheter och skapa tillväxt.

Vi grundades 1984 och har utvecklats till att bli ett av världens högst värderade och snabbast växande företag.

www.cisco.se

Cisco Systems