Anders Berndt

Arena College
Höstterminen 2002

Introduktion till

Informationssäkerhet

Sammanfattning

Den här rapporten belyser olika faktorer inom informationssäkerhet. Utvecklingen rusar framåt, systemen blir alltmer komplicerade och svåra att administrera. Risken för egna misstag ökar och utanför knuten väntar spioner och sabotörer på att knäcka våra lösenord och riva ner våra brandväggar. Hur är det ställt med säkerhetsarbetet egentligen?

Vi ska gå igenom olika aspekter på ämnet, såväl hårda som mjuka. De datortekniska byggstenarna som används beskrivs, människans egenheter framför skärmen och hur man kan undvika att det leder till bristande säkerhet behandlas, och goda råd till säkrare datahantering ges.

Innehållsförteckning, del 1

1. Inledning

"Pålitlig information skall finnas tillgänglig för den person eller dator som är behörig att få ta del av den, och som efterfrågar den på ett korrekt sätt."

Meningen ovan sammanfattar de tre grundförutsättningar som man arbetar med inom informationssäkerhet:

1. Sekretess - att information är tillgänglig endast för dem som har behörighet till den.

2. Riktighet - att information förblir korrekt och fullständig.

3. Tillgänglighet - att behöriga användare vid behov har tillgång till information.

Sekretess är traditionellt en säkerhetsfråga, men om riktighet och tillgänglighet fallerar ses det ofta som ett problem med datadriften. Alla tre är dock förutsättningar som måste vara uppfyllda om det ska anses råda informationssäkerhet i ett system. Det räcker inte med att hantera och skydda servrar, klienter och nätverk, man måste också titta på hur information hanteras i sin helhet i en organisation.

Vi har valt att titta på informationssäkerhet från i huvudsak tre håll: yttre säkerhet, inre säkerhet och fysisk säkerhet. Hoten utifrån får ofta stort utrymme i debatten, medan de inre svagheterna sällan berörs. Vi ska försöka reda ut vilka de största farorna mot informationssäkerhet egentligen är och hur man bör arbeta för att minska riskerna.

Redogörelsen består av två delar. I den första behandlas inre och fysisk säkerhet, i den andra följer en mer detaljerad teknisk beskrivning av skydd mot yttre hot. För att läsaren ska få en bättre överblick har vi valt att ha två innehållsförteckningar, en för varje del.

2. Metod och begränsning

Vi har huvudsakligen funnit vårt material på Internet, i form av artiklar, avhandlingar och guider om säkerhet. Tillsammans med våra kunskaper och erfarenheter i ämnet har det hela sammanställts till ett slutresultat.
Vi har varit tvungna att begränsa oss. Ett viktigt ämne i allt säkerhetsarbete, men som vi inte har med i den här redogörelsen, är det som behandlar virus och virusskydd.

3. Resultat

Inre säkerhet

Säkerhet verkar ofta handla om att skydda sig mot yttre hot som blixtnedslag, hackerattacker eller illasinnade virus. Den gängse uppfattningen av hot är just att det är någon eller något utifrån den stora stygga världen som försöker nästla sig in. Eller? Tyvärr är det inte alls det största problemet.
Anställda som av misstag eller okunnighet raderar väsentlig information är det största problemet när det gäller datasäkerhet.
Intern säkerhet handlar om att skydda sina system mot inre hot, oavsett om de uppstår av slarv eller om det är kriminella handlingar. Intern säkerhet är också att utbilda, och framför allt motivera sina anställda att ta till sig säkerhetstänkandet, och att tillämpa det på sitt område inom organisationen. Vad hjälper det med sekretess om informationen inte också är tillgänglig och - ännu viktigare - korrekt.
Den information som de flesta sysslar med är inte hemlig. Däremot är den ofta viktig för företagets verksamhet. Om den av någon anledning ändras eller försvinner kan det innebära att verksamheten lamslås. Där finns det stora hotet.

Lite statistik

I en examensrapport från Handelshögskolan som citeras av Karl Jóhannson i hans Projektarbete i datasäkerhet framkommer följande:
Tre av fyra datachefer inom tillverkningsindustrin anser att det finns väsentliga hot mot företagets information. Drygt 40 procent av datacheferna anser att felaktig förändring eller radering av information är det enskilt största hotet, och 48,1 procent anser att det är anställda som genom misstag eller okunskap utgör detta hot.

I praktiken handlar datasäkerhet ofta om funktionerna i systemet, till exempel att skrivarna och e-postsystemet fungerar som det ska. En viktig del är också dataintegriteten, det vill säga att det som lagras i systemet är korrekt.
Få datachefer upplever något reellt hot från hackers som obehörigt försöker att ta sig in i företagets datasystem. Dock finns en skillnad mellan mindre och större företag. Företag med mer än 200 anställda uppger i mycket större utsträckning hackers som ett väsentligt hot.
Värt att notera är också att hela 92,6 procent av de tillfrågade uppger att man inte har någon speciell post för datasäkerhet i budgeten.

Problemet kan egentligen sägas vara detsamma som en av förtjänsterna med ett bra datasystem: det ska vara så lättillgängligt för användarna som möjligt.

Vad göra?

Det gäller att bestämma sig för vad det är som ska skyddas. Vad kan någon tänkas vilja ha eller förstöra, vad kan tänkas gå sönder eller försvinna? Gör det något?
Man måste ta fram en hotbild.
Ett företag som tillverkar något som de är ensamma om vill inte att andra ska få nys om hemliga uppgifter. Det största hotet för dem är förmodligen att någon försöker spionera och stjäla information. Ett annat företag kanske inte har några hemligheter alls men skulle skadas

mycket om deras kundregister försvann. Ett tredje företag, t.ex. en bank, skulle nog lida allvarliga men om systemen gick ner aldrig så korta perioder under kontorstid.
Det är alltså minst lika viktigt med säkerhetskopiering och jämn strömförsörjning som att skydda sig mot spioner och sabotörer.

Det viktigaste för den interna informationssäkerheten är att redan från början ha ordning och reda. Först och främst måste det finnas en säkerhetspolicy. Hur den ska se ut bestäms av ledningen och måste genomsyra hela organisationen, från golv till tak. Den måste också vara i rörelse, aldrig stanna till och slå sig till ro, utan ständigt ses över och revideras.

Riskanalysen görs genom att analysera vilka faror det som ska skyddas kan utsättas för, hur troligt det är att det händer, vilka konsekvenser det skulle få, och vad det skulle kosta att skydda (eller inte skydda) sig. När den är klar ska man ha en klar bild av vad som behöver göras för att få bästa möjliga skydd.

Hot/Brist	**Sannolikhet**	**Konsekvens**	**Summa**	**Kostnad** (t.ex.)
Brand	3	5	15	10.000.000
Inbrott	4	3	12	500.000
Sabotage	2	2	4	3.000.000

Exempel på enkel riskanalys

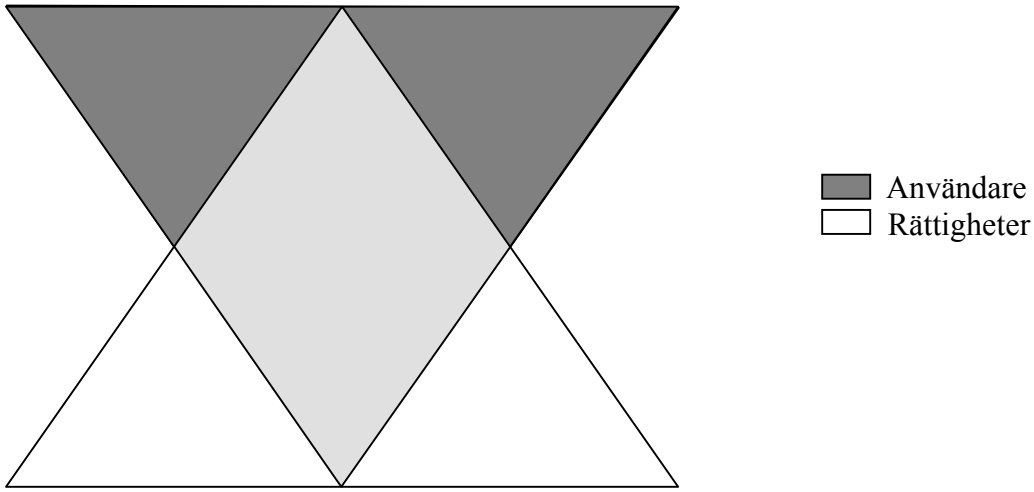
Om säkerhetssystemen blir för abstrakta och krångliga kommer folk att – i bästa fall – sluta använda dem. I sämsta fall kommer företaget att ta skada. Ett typexempel är kodlåsta dörrar som helt enkelt ställs upp för att det är så besvärligt att hålla på med koder och kort varje gång man ska förflytta sig. Till slut är det naturligtvis ingen som orkar göra det. Det får heller inte bli så att datasäkerheten lever sitt eget liv, att den upprätthålls för sin egen skull. Då kan det sluta med att inte ens säkerhetsansvariga vet vad som skyddas och varför. Den totala säkerheten är det viktigaste. Optimerad, inte maximerad.

Ett exempel på bristande helhetssyn kan vara att du har en dator som lagrar vissa uppgifter och det bredvid står en pärm som innehåller samma information. Då är det inte mycket vits att skydda datorn med någon oknäckbar algoritm.

För att kunna begränsa möjligheterna att påverka informationssäkerheten upprättar man någon form av modell över användarna och deras tänkta behörigheter och rättigheter.
Modellen behöver inte vara någon direkt spegling av rättigheterna och behörigheterna i operativsystemet, även om det bör finnas likheter mellan dem. Man måste inte heller skapa en väldigt detaljerad och komplett modell. Den ska vara en hjälp i säkerhetsarbetet helt enkelt, inte något som känns jobbigt att behöva hålla på med och som får en att ledsna på alltihop.

En bild av hur rättigheter (behörigheter) generellt sätts följer på nästa sida.

Längst upp: många användare, få rättigheter.
Längst ner: få användare, mycket rättigheter.



I varsin ände av figuren har vi alltså: de anställda som har rättigheter enbart i sina hemkataloger, och administratören som har fullständiga rättigheter i hela systemet.

Men, som alltid: varje system har sitt system. På ett litet företag kanske det är bra om servern står framme så att alla kan lära sig att exempelvis säkerhetskopiera. På ett större företag bör den vara inlåst i något rum där folk inte springer och ”geggar” i onödan – inte ens för att hämta en ny nätkabel. Det senare är en klar rekommendation i de flesta fall.

Ett särskilt problem att tänka på är bärbara datorer. Det är lätt att glömma bort dem, och missa att ha dem med i säkerhetsarbetet. Traditionellt har det kanske inte funnits så många i en organisation, men plötsligt står man där med några hundra användare som varje dag går iväg utanför låsta dörrar och brandväggar med känslig information. Det viktigaste torde vara att se till att det finns någon form av krypteringsskydd på dem. Dock: helhetssyn! Har alla de bärbara datorerna viktig information på sina hårddiskar? Vissa har det säkert och behöver ha smarta kort för att släppa in någon, andra kanske klarar sig med mjukvarukryptering som visserligen går att knäcka för en kommersiell spion, men är mycket billigare. Mjukvarukryptering går att skaffa till ett pris av 500-600 kronor per dator medan smarta kort kräver läsare för minst ett par tusen kronor och dessutom behöver en administrativ apparat för att korthanteringen.

En stor risk för säkerhetsarbetet, såväl det interna som det externa, är att bli för produktinriktad. Säkerhet ska vara resultatet av ett fortlöpande arbete och en förståelse för hur systemen och människorna fungerar. Hur går man bäst tillväga för att lyckas med det?

Kreativitet och enkelhet

Det har experimenterats med en del olika metoder. Det bästa tycks vara om man spånar ostrukturerat och avslappnat i ämnet, och om representanter för olika personalgrupper finns

med. Är det bara ett antal tekniker som sätter sig ner finns det en risk att de begraver sig i tekniska detaljer. Det leder till två problem: dels kan deras idéer bli omöjliga att ro i hamn, dels missar de kanske hotbilder som dyker upp på mer icke-tekniska håll.

Det krävs kreativitet för att tänka sig in i alla varianter av problem och deras lösningar.
Ett exempel på okonventionell men effektiv intern säkerhet finns i Huddinge Kommuns datanät, som bland annat omfattar kommunens alla skolor. Där har man valt att lägga alla administrativa system – inklusive det för betygssättningen – i ett Token Ring-nät, medan eleverna får hålla till godo med ett Ethernet-nät. Vill en elev ta sig in i systemet måste han alltså inte bara lista ut lösenord och andra mjukvaruspärrar, utan också ta med sig ett Token Ring-nätverkskort och installera det i elevdatorn.

Den mjuka vägen är stundom hård…

Grunden i det praktiska säkerhetsarbetet är alltså någon form av modell för hur rättigheter och behörigheter sätts. Grunden i det långsiktiga och mer informella arbetet för att förbättra den interna säkerheten är ”mjukare”. Det handlar om saker som utbildning, förståelse, ansvar, samhörighet och lojalitet. Den bästa hjälpen man kan få som säkerhetsansvarig är förstås att de anställda förstår problemen, varför de bör och hur de kan undvikas. Och det bästa sättet att undvika insiderbrott är förstås att få de anställda att känna sig delaktiga och, tycka om företaget de arbetar på.

Inom intern säkerhet används ibland policyregler som ska fastställas och skrivas under av de anställda. Vissa företag har kanske också infört straff för olika typer av interna brott eller internt slarv, även om det inte är så vanligt i Sverige. Men det finns all anledning att vara skeptisk till den typen av tillvägagångssätt:
Det är ganska uppenbart att det inte fungerar. Vi har numera lärt oss att tänka själva och att misstro auktoriteter. Det anses idag som ett uttryck för kreativitet att gå sin egen väg.

Men ibland måste man vara stenhård: Internet och e-post är typexempel på vad du som säkerhetsansvarig måste ta tag i på skarpen om du inte lyckas på det ”mjuka” viset. Och eftersom användarna inte lär acceptera att stängas ute från Internet någon längre tid är du så illa tvungen att få över dem på din sida…

Internet har visserligen inneburit en ökning för de yttre hoten, men fortfarande är de inte i närheten av andelen interna brott.
Banker och försäkringsbolag medger att de interna brotten ett mycket större problem än inkräktare utifrån. Det är dock vanligt att man inte talar om det eller ens vill kännas vid det när man blir tillfrågad, eftersom det anses ge företaget dålig publicitet. Som när flygbolagen målar över firmanamnet på havererade flygplan. Rimligen borde öppenhet kring det hela ge intrycket av ett företag som har koll på läget och tar säkerhetsproblemen på allvar.

Hur ser skurken ut?

Vem är det då vi ska leta efter när vi försöker hitta levande potentiella faror. Brottsforskaren Leif GW Persson har i ett utredningsmaterial om IT-brott i Sverige delat in IT-brottslingen i fyra kategorier: Bror Duktig, Hackern, Spionen och Bedragaren.

Bror Duktig kan ställa till enorm skada för företaget, men han gör det inte för personlig vinnings skull. Han har ofta företagets bästa för sina ögon, men problemet är att han går utöver sitt mandat.
Han är i regel en ung och välutbildad man. Det kan t.ex. vara valutahandlare inom ett företag. Det mest kända exemplet är Nick Leeson på Barings bank, men det finns också svenska exempel. Enligt Leif GW Persson kännetecknas den här personen av ett stort behov av att visa vilken klipsk klippare han är.

Det kan också vara kreativa personer som har till uppgift att utveckla de produkter eller tjänster som företaget livnär sig på. För att dessa personer ska kunna gör sitt jobb så måste de ha tillgång till all information inom företaget. Till de kreativa personernas egenskaper hör att de gärna vill prata om sina idéer med andra och det spelar ofta ingen roll om det är personer inom företaget eller hos konkurrenter.
Problemet är att om dessa personer åläggs alltför hårda restriktioner så hämmas deras kreativitet och de kan hamna i konflikt med sina uppdragsgivare.

Hackern förekommer inte ofta. Målet för honom är det tekniska systemet. Ju svårare det är att ta sig förbi spärrarna, desto större utmaning är det.

Spionen vill komma över information. Det kan vara en anställd som slutar på ett företag och tar med sig kundregistret. Det finns i den här gruppen också en kategori som söker ”nyfikenhetsinformation”. Det finns t.ex. polisaspiranter som missbrukat sin behörighet till polisväsendets Person- och belastningsregister.

Bedragaren är enligt Persson den vanligaste IT-brottslingen. Det är en som helt enkelt vill komma över pengar. Han har funnits i alla tider och att det han sysslar med kallas för databrott beror helt enkelt på att transaktioner och finansiell hantering numera sker i digital form.

Det finns ingen typisk IT-brottsling, men ofta handlar det om en person som är i någon slags konflikt med sin arbetsplats, eller med sig själv.

Fysiskt säkerhet

Stöld

Stöld innebär inte bara att någon stjäl din dator med tillhörande kringutrustning utan kan också innebära att information följer med, vilket ofta kan ha ett större ekonomiskt värde för ägarna än vad hårdvaran är värderad till.

Följden av stöld blir att du

- förlorar utrustningen.
- riskerar att förlora den tillgängliga informationen.
- riskerar att informationen sprids till obehöriga.
- riskerar att den tillgängliga informationen är inaktuell eftersom det kanske inte finns någon kopia på de senast gjorda ändringarna av informationen.

Praktiska råd

När du säkerhetskopierar kan du välja på att enbart kopiera de förändringar du gjort under dagen eller att kopiera alla data. Det senare brukar benämnas totalbackup. Vilket du väljer beror på volymen av information och vilka tekniska hjälpmedel du har skaffat dig. Har du möjlighet att skaffa dig nödvändig teknik så är alltid en totalbackup det bästa alternativet.

- Oberoende av ditt datorberoende bör du regelbundet ta en total säkerhetskopia som innehåller all information och alla program som finns på din dator. Ett sådant förfarande effektiviserar och säkrar återstarten vid långa avbrott.
- Din säkerhetskopia kan du antingen lagra på disketter eller på band. För stora mängder information bör du utnyttja band eller CD-skivor för att erhålla en rationell och säker hantering.
- Om du tänker köpa ett säkerhetsskåp för att förvara dina säkerhetskopior, välj då ett skåp som också skyddar mot brand. Kom ihåg att det traditionella kassaskåpet är ett dåligt skydd mot brand.
- Att förvara säkerhetskopior och originalprogram i bostaden kan vara ett enkelt och billigt alternativ för dig som arbetar i näringslivet. Kom dock alltid överens med din chef innan du tar hem kopiorna. Ta aldrig med hemligt material i okrypterad form utanför arbetsplatsen.
- Förvara inte nycklarna till låsta utrymmen och säkerhetsskåp öppet i samma rum som skåpet, eller i ett synligt nyckelskåp.

Brand

Brand kan medföra inte bara att datorn med tillhörande kringutrustning förstörs utan även att informationen försvinner. Det betyder att branden och inte minst brandröken även kan påverka och förstöra t.ex. disketter, CD-skivor och band som finns i samma rum som datorutrustningen eller i närheten av datorutrustningen.

Följden av en brand blir att du

- förlorar dina arbetsredskap och kan få stora svårigheter och kostnader för att återanskaffa informationen.
- riskerar att inte kunna använda din arbetsredskap och därmed inte kan utföra dina arbetsuppgifter.
- riskerar att förlora informationen.
- riskerar att den tillgängliga informationen i form av säkerhetskopia eller papperskopia är inaktuell. Orsaken kan vara att det kanske inte finns någon kopia på de senast gjorda ändringarna av informationen.

Praktiska råd

När du planerar ditt skydd mot brand så glöm inte:

- Förutom själva branden och röken så kan även strålningsvärme, vatten och annat släckningsmedel skada din utrustning.
- Slå om möjligt alltid av utrustningen vid arbetstidens slut för att minska brandrisken.
- Genomför halvårsvis egna inspektioner av brandbelastningen i de lokaler som du har datorutrustning i.
- Lämna räddningstjänsten en karta/förteckning över var datorutrustingen finns, så att den kan prioriteras vid eventuella släckningsinsatser.
- Ta en papperskopia av speciellt viktig information och förvara den på lämpligt ställe, kan vara ett billigt alternativ för att hjälpligt kunna utföra nödvändigt arbete vid förlust av informationen.
- Kombinera gärna arbetet med att upprätta inventarieförteckning med en fysisk märkning av utrustningen.
- Din första säkerhetskopia skall alltid vara en totalbackup.

- Din säkerhetskopia kan du antingen lagra på diskett, CD-skiva, löstagbar hårddisk, band eller optisk disk beroende på informationsmängden.
- Överväg möjligheten att kombinera ditt inbrottslarm med ett brandindikeringslarm.
- Samråd med räddningstjänsten om t.ex. placering av datamediaskåp och val av släckningsutrustning.
- Ett alternativ till datamediaskåp ar brandklassade diskettboxar placerade i säkerhetsskåp. Därmed erhålls också ett inbrottsskydd.
- Kom ihåg att disketter och datakassetter bara tål cirka 55°C, band, hårddisk cirka 75°C och papper 175°C innan mediet blir oanvändbart.
- Att förvara säkerhetskopior i bostaden kan vara ett billigt och enkelt alternativ för dig som arbetar i näringslivet. Diskutera dock alltid med din chef om lämpligheten i att du tar hem kopiorna.

Vattenskada

Med vattenskada avses störningar som kan uppstå i datordrift eller datorstödd verksamhet på grund av vätska och fukt.

Orsaken till skadan kan vara:

- Hög fuktighet (kondens) från t.ex. ett kylaggregat.
- Översvämning på grund av t.ex. sönderfryst vattenledningsrör, glömd vattenkran, takläckage i egna eller kringliggande lokaler.
- Översvämning i avloppssystemet eller kraftig vårflod.
- Släckning av brand i omkringliggande utrymmen.
- Läckande yttertak, särskilt vid snösmältning.

Följden av en skada kan bli att datorn med tillhörande utrustning skadas och inte kan användas och att du:

- riskerar att förlora informationen.
- riskerar ett längre stillestånd i datoranvändningen och därmed stora störningar i den datorstödda verksamheten.
- kan få stora svårigheter och kostnader för att återanskaffa informationen.
- riskerar att den tillgängliga informationen i form av säkerhetskopia eller papperskopia är inaktuell. Orsaken kan vara att det kanske inte finns någon kopia på de senast gjorda ändringarna av informationen.
- riskerar stora kostnader för att återställa datorutrustningen eller delar därav.

Praktiska råd

- Kontakta ditt försäkringsbolag och diskutera med deras experter vilka risker för översvämningar som du bör ta hänsyn till i din verksamhet.
- Undersök vilka risker för vattenskada som finns genom verksamheter i din omgivning eller som kan uppstå genom dina lokalers geografiska placering.
- Anskaffa material som kan användas för övertäckning av din utrustning vid risk för vattenskada. Förvara detta material i direkt anslutning till utrustningen och se till att berörd personal vet hur det används.

Innehållsförteckning, del 2

5. Teknisk beskrivning av skydd mot yttre säkerhetshot

Systemstrippning

Ett av många sätt att försvåra angrepp mot sin verksamhet, är att minska på antalet funktioner i systemet. Genom att lyfta bort dessa onödiga funktioner och tjänster optimeras säkerheten. Det kallas för att strippa systemet.
Strippningen kan även omfatta komponenter i ett system. En känslig informationsserver ska exempelvis inte alltid ha alla moderna gränssnitt mot Internet installerade.

Skydda sin webbserver

Vad kan man göra för att skydda sig och sin verksamhet?

- Öppna minsta möjliga antal tjänster och portnummer.

- Lägg verksamhetens webserver på ett eget firewall-segment.
- Låt inte verksamhetens server ha någon annan uppgift, undvik s.k. "kompletta Internetservrar".
- Undvik så långt det går all användning av cgi-bin script.
- Om scripts ändå måste användas, tillåt ej kommandotolkar (typ perl, perl.exe) i cgi-bin katalogen.
- Använd helst bara tillfälliga skrivtillstånd på webserverns filutrymme.
- Begränsa webprogrammets rättigheter i filsystemet så långt det bara går.
- Avinstallera nfs från verksamhetens webserver.
- Ta bort alla onödiga program och funktioner.

Förstå hur angriparen arbetar

Först hämtar angriparen information om vilka portar och tjänster som är öppna, vilka maskiner som ligger på samma nätsegment som servern, vilka programvaror som används och hur dessa är konfigurerade.

Angripare läser också alla filer de kommer åt i servern, både genom länkar i websidor och genom att lista innehållet i kataloger. De försöker även på många olika sätt läsa konfigurationsfiler, scriptfiler och systemfiler.

De provar sedan via anonym FTP om de har skriv- eller lästillstånd på webserverns filsystem eller om de via cgi-bin script kan anropa någon typ av kommandotolk.

Därefter söker angriparen efter de programvaror de identifierat. Detta kan bestå av att man utnyttjar buggar eller vanliga konfigurationsfel i serverns program, cgi-bin script, FTP- eller SMTP-program. Många av dessa program svarar alltid med olika versionsnummer, antingen vid uppkopplingen eller när de får ett kommando de inte kan tolka.

I den sista fasen sätts samma program upp i en egen dator för att jämföra konfigurationerna med hjälp av olika tester.

Sniffer-program

Ett sniffer-program fångar upp alla IP-paket och letar igenom dem och dess uppgifter/innehåll. Det enda sättet att skydda sig är att kryptera alla IP-paket som skickas över Internet.

Vad gör man då om ett angrepp har lyckats?

Det bästa man kan göra är att följa ordinarie rutiner inom företaget och låta den pressansvarige besvara frågor. Tillåt inte tekniker att besvara frågor eller föra diskussioner i ämnet på Internet. Förutsätt alltid att angriparen lämnat en eller flera bakdörrar efter sig, nyinstallera därför i största möjliga mån operativsystem och serverprogramvara. Byt alla lösenord.
Anmäl alltid det inträffade. Försök att ytterligare öka säkerheten i mån av att det går stegvis, flytta servern till ett eget nätsegment.

Stöld av krypterade lösenord via Internet

När kontonamn och krypterade lösenord överförs via Internet kan de avlyssnas eller stjälas på många olika sätt. Man bör därför använda starka lösenord som är minst åtta tecken långa och inte går att hitta i en ordlista. Självklart är användarens och företagets namn bannlysta som lösenord, likaså ord som kan associeras med användaren.

Hemlig källkod - bra eller dåligt?

När det gäller de allra flesta krypteringsalgoritmer, anser upphovsmännen att det gynnar säkerheten att ge ut källkoden. Användarna kan då gå igenom koden för att granska hur säker eller osäker den egentligen är. När det gäller Windows operativsystem hålls koden hemlig, men inte Unix.
Tanken med att hålla källkoden hemlig är naturligtvis att det ska bli svårare för hackers att skriva program som knäcker de olika säkerhetssystemen.

Proxyservern

Proxyservern har fått en allt starkare position i takt med att allt fler tillämpningar flyttas till Internet. Proxyn passar lika bra som vakthund i brandväggen som cache-vaktmästare hos Internet-operatören. Bland de mest omdiskuterade Internet-tillämpningarna idag märks brandväggar, virtuella privata nät och olika effektivitetshöjande verktyg för webbtrafik.
De bygger alla på ett ingripande i det normala trafikflödet - på att det finns en proxy mellan klient och server.

Proxyn fungerar som ett filter mellan verksamhetens nätverk, och omvärlden (Internet), som även kan vara ett annat nätverk inom företaget och verksamheten.
Ordet "proxy" betyder enligt lexikonet "fullmakt", "ombud" eller "ställföreträdare".
Precis det är vad proxy-servern är också. Den fungerar som ett ombud mellan två parter.
Meningen med en proxy-server är att utföra någon typ av tjänst, så att kommunikationen mellan parterna – klient och server – fungerar enligt systemadministratörens önskemål.
De flesta förknippar oftast ordet "proxy-server" med antingen cache-funktioner för webbsidor eller brandväggar. I de fallen är det fråga om proxy-servrar för webbtjänster (HTTP) respektive webb- och liknande trafik (FTP, e-post, o.s.v.). Det finns emellertid ingenting som begränsar en proxy-tjänst till webben. För sakligheten skull ska vi börja med att tala om proxy-tjänster i allmänna termer.

Även Routrar är Proxy

Proxyn fungerar som ombud för en viss typ av trafik, på en viss nivå i nätverksmodellen. En brygga eller växel, fungerar som en proxy på länknivå (nivå två), och en router fungerar som en proxy på nätverksnivå (nivå tre). Växlar och routrar är mycket enkla proxy, som enbart mixtrar en del med adresserna.

För brandväggsfunktioner finns så kallade säkerhetsroutrar eller filtrerande routrar, som gör mer avancerade överväganden innan trafiken vidarebefordras. Paketfiltrering brukar sådana proxyfunktioner kallas, och de kräver av naturliga skäl topprestanda, vilket oftast innebär att filterfunktionen är implementerad i hårdvaran. Nästa steg uppåt i hierarkin blir nätverksnivån, det vill säga nivå 4, där protokoll som TCP och UDP agerar. I ett brandväggs/proxy-sammanhang kallas nivå 4 ofta för kretsnivå (circuit level), för att trycka på det faktum att protokollen är mer förbindelseorienterade. Många proxy-servrar har även funktioner för att filtrera trafiken på kretsnivå.

En paketfiltrerande proxy är också begränsad. En kretsnivå-proxy är eventuellt begränsad till TCP och UDP, vilket antagligen inte gör så mycket, men som trots allt inte klarar all tänkbar IP-trafik. Den tredje och sista varianten kallas applikations-proxy. Det innebär inte riktigt att den agerar på OSI-modellens högsta nivå, men dock att den ingriper i de tillämpningsorienterade protokollen, exempelvis HTTP för webbtrafik, FTP för filöverföringar, SMTP och POP3 för e-post.

Proxyn stegar in mellan klient och server

Proxy-servern är alltså en funktion som stegar in mellan klient och server, och på så sätt modererar trafiken enligt de regler som nätverksadministratören anger. När klienten tror att han har direktkontakt med den önskade servertjänsten, är det istället proxyn som svarar på anropet. Så snart proxyn fått klart för sig vad klienten vill, och om klienten är behörig att utföra tjänsten, kontaktar proxyn den aktuella servern. Under hela förloppet agerar proxyn som mellanhand.

Proxyn är internt uppbyggd av en server-, respektive klientdel. Serverdelen har hand om kontakten med klienten medan klientdelen pratar med den aktuella servern. Mellan dessa sitter de funktioner som är själva syftet med anordningen.

Det ger alltså oanade möjligheter till trafikstyrning. För att nämna några exempel kan en proxy användas för:

- lagring i cache-minnen av vanliga webbsidor, vilket ökar prestandan för slutanvändarna och minskar belastningen i nätet.
- filtrering av IP-paket så att obehöriga inte kan komma igenom (låg nivå).
- autenticering av användare så att inte obehöriga personer får tillträde till känslig information och tjänster (hög nivå).
- loggning av trafikinformation så att den nätverksansvarige kan studera belastning, fördelning mellan trafiktyper, m.m.
- loggning av händelser så att den nätverksansvarige kan analysera händelser i efterhand, exempelvis om något gått fel eller någon brutit sig in.
- filtrering av webbmaterial, exempelvis så att vissa användare inte får tillgång till vissa typer av webbsidor.
- filtrering av e-post, exempelvis så att reklam sorteras bort eller att olika bilagor viruskontrolleras.
- kryptering av trafiken så att publika förbindelser (som Internet) kan användas för privata länkar, s.k. virtuella privata nät (VPN).

En skyddad frizon (DMZ)

Ett vanligt upplägg för avancerade brandväggslösningar är att ha två filtrerande routrar (paketfilterproxy i hårdvara) och en uppsättning applikationsproxy, som vanligen körs på en dedikerad Unix- eller Windows NT-maskin. En av routrarna placeras mellan Internet och applikationsproxy-datorn medan den andra sitter mellan det interna nätverket och proxy-datorn.
På detta sätt skapas ett ingenmansland, ett litet mininät där proxy-datorn är skyddad från både externa och interna attacker. Dessutom förbättras applikationsproxy-servrarnas prestanda, eftersom de bara behöver ha hand om trafik som faktiskt passerar genom arrangemanget. Ofta placeras även webbservern i detta lilla mellannät. Förutom de vanligaste TCP/IP-tillämpningarna HTTP, FTP, SMTP, POP3, SNMP, TELNET, SSL m.fl., krävs proxy-tjänster för strömmad multimedia (Realaudio, Realvideo, Vivo m.fl.) eller andra nymodigheter. Detta skapar förstås problem i takt med att Internet-tekniken utvecklas.

Om vi undersöker Microsofts och Netscapes produkter närmare ser vi att båda sedan inte lång tid tillbaka hanterar specifikationerna Carp och Socks. Carp är ett Microsoft-initierat standardförslag till förbättring av protokollet ICP, en IETF-standard som låter en grupp proxy-cache-servrar samarbeta distribuerat för att skapa bättre prestanda, skalbarhet och feltolerans.

Mellan Internet och webbservern

Omvänd proxy innebär att proxy-servern sitter mellan Internet (”det andra nätet”) och webbservern. Den är alltså proxy åt de som försöker komma åt din webbserver, vilket kan användas både för att styra vem som kommer åt vad eller för att kunna erbjuda bättre prestanda – genom cachning – åt omvärlden. En variant av omvänd proxy är en s.k. ”virtual host”, en virtuell värd, vilket innebär att proxy-servern binder ett flertal interna webbservrar till en enda externt synlig server. Det ger förbättrad flexibilitet vid webbpubliceringen.

Sammanfattningsvis är proxy-funktionen som sådan mycket allmän och har en mängd olika användningsområden. Grundprincipen är att en viss trafik, på en viss nivå, får passera genom en funktion som på det ena eller andra viset bearbetar flödet enligt nätverksansvariges inställningar. Högre nivå ger bättre säkerhet, men krångliga handhavande. Lägre nivå är enkelt, men kräver bra prestanda, ofta i form av skräddarsydd hårdvara. Ofta kombineras olika produkter för att uppnå den säkerhet och den prestanda som är önskvärd.

Slutligen krävs som alltid en noggrann analys av det egna nätet och de egna behoven innan man bestämmer sig för hur lösningen ska se ut.

Brandväggar och filter

Säkerhetsmurar byggs för att skydda intern kommunikation från obehörig insyn och intrång, samtidigt som åtkomst till externa funktioner tillåts att fungera ostört. En rätt konfigurerad brandvägg är en effektiv kontrollant av in- och utgående trafik i en verksamhet.
En felkonfigurerad brandvägg är en katastrof för säkerheten.
Du installerar brandväggar för att skydda ditt företag och verksamhet från dataintrång och angrepp av olika slag. Det krävs kunskap och erfarenhet för att göra en riktig och korrekt installation, precis som för all annan typ av säkerhetsutrustning.

Internet har snabbt blivit en positiv nödvändighet, men samtidigt utgör kopplingen mellan ett internt nät och Internet en allt större fara i dagens samhälle.
En bra brandvägg kan stoppa oönskade intrång, men det är samtidigt viktigt att inse att dess skydd aldrig blir hundraprocentigt. En genomtänkt säkerhetspolicy är A och O.

Styr valet av brandvägg

Säkerhetspolicyn måste styra valet av vilken typ av brandvägg man ska använda sig av i sin verksamhet. En brandvägg kan vara allt från en ganska enkel router, till en lösning med paketfiltrering eller en proxy. En proxy är säkrare, men för det mesta långsammare än filtrering av paket och dessutom måste en proxy oftast vara specialskriven för ett specifikt protokoll till exempel HTTP eller FTP. Om det dyker upp nya protokoll, eller sker förändringar i de gamla måste nya specialskrivna proxys installeras. Fler och fler brandväggar är i dagens läge en blandning av paketfiltrering och proxys för att både ge optimal säkerhet och en hög funktionalitet.
Valet av brandvägg är också ett val av operativsystem och ett val av hårdvaru-, respektive mjukvarulösningar.

Var sitter oftast brandväggen?

Den vanligaste brandväggslösningen är en dator försedd med tre nätverkskort och ett brandväggsprogram. På första kortet finns Internet, det andra rymmer en så kallad demilitariserad zon (DMZ) med webb-, FTP- och e-post-servrar och på det tredje kortet ligger det interna nätet. Om du tillåter något protokoll som anses vara mindre säkert än de andra kan den funktionen sättas på en server med ett fjärde nätverkskort och för att ytterligare höja säkerheten kan en eller flera routrar installeras på den ena eller den andra sidan om brandväggen.

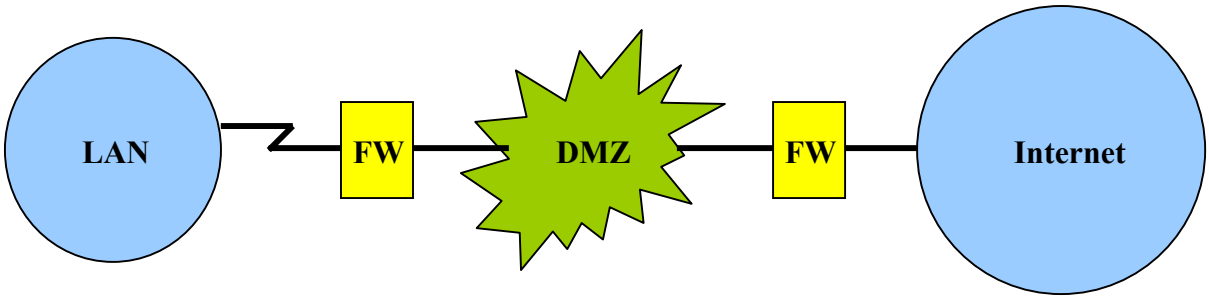


Bild över vanlig brandväggslösning.

Principen för hur en brandvägg ska konfigureras borde vara att inte tillåta någon trafik alls, och där du efter hand tillåter fler och fler funktioner, till exempel HTTP (port 80), FTP (port 21), e-post (port 25) och news (port 119), om säkerhetspolicyn tillåter detta. Samtidigt bör du även om möjligt undvika funktioner som kan vara mycket praktiska men som många gånger anses osäkra, till exempel telnet (port 23), eller som kan ge en angripare värdefull information, t.ex. finger (port 79). Att göra det omvända, det vill säga att ha en öppen lösning där funktionerna en efter en täpps igen, är både svårare och mer tidskrävande och risken för fel ökar markant.

Förutom program som installeras på en vanlig dator finns det även skräddarsydda hårdvarulösningar där det underliggande operativsystemet har strippats och där maskinen är dedikerad som brandvägg. Den typen av lösningar förbises ofta av brandväggsexperter, men de kan definitivt vara prisvärda för en rad företag och myndigheter. Det är ju inte alltid så att den dyraste och mest tekniskt avancerade lösningen är nödvändig om hotbilden uppfattas som relativt låg. Se bara till att brandväggen är skyddad från de vanligaste typerna av attacker som IP-spoofing, Denial of Service och liknande, samt att den har möjlighet att rapportera när den utsätts för så kallad port scanning.

Testa säkerheten

På samma sätt som en utomstående revisor går igenom ekonomiavdelningens arbete måste någon utomstående granska dataavdelningen. Vare sig du själv har konfigurerat brandväggen eller haft konsulter hos dig, bör någon icke inblandad testa säkerheten och funktionaliteten. Om du av ekonomiska skäl måste avstå från en extern kontroll så finns det flera brandväggslösningar med så kallat självtest.

Liten checklista om säkerhet

I och med att du installerat en brandvägg har du minskat osäkerheten avsevärt. Men tro inte att skyddet är komplett för det.

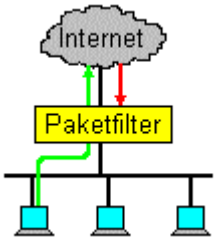
- För det första är den lösning du har skapat en **färskvara**. Operativsystemet och brandväggsprogrammet måste uppdateras och underhållas. Nya patchar måste installeras kontinuerligt.
- För det andra måste all aktivitet loggas och kontrolleras på ett intelligent sätt. Den kan exempelvis finnas användare på det lokala nätverket som av misstag eller okunnighet gör saker som kompromitterar säkerheten.

Viktigt är att införskaffa någon form av ”Intrusion Detection System” om detta inte följer med brandväggen. Du måste omedelbart få veta om någon försöker ta sig in i det interna nätet. Brandväggen ska framför allt skydda mot intrång utifrån. Det betyder ofta att skyddet inte är tillräckligt mot trojanska hästar eller fientliga Java- eller ActiveX-script. Därför måste du ha extra skydd i form av antivirusprogram.

Se alltid till att underhålla din kunskap om det operativsystem och den brandvägg du använder, och hämta även in annan relevant information. Försäkra dig om att respektive leverantör alltid håller dig uppdaterad om nya hot och patchar. Prenumerera därför på e-postlistor och följ de diskussionsgrupper som täcker dina intresseområden, markera de webbsiter som är relevanta och knyt kontakter med andra användare som du kan lita på.

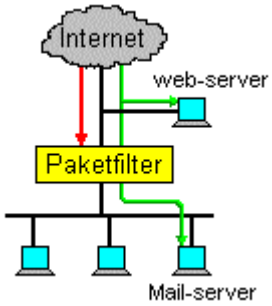
Sist, men inte minst, var alltid beredd att ompröva tidigare beslut. Vad som var den bästa lösningen igår är inte alltid den bästa i morgon. Hotbilden förändras med verksamheten, nya angreppsmetoder dyker upp, och naturligtvis bidrar leverantörerna med nya sofistikerade säkerhetslösningar.

Exempel på filter och brandväggar



Paketfilter

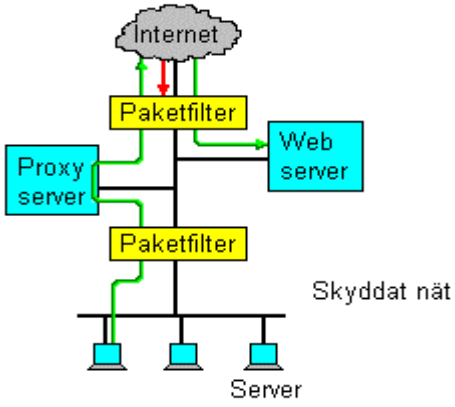
Filtret ansluts mellan ett yttre nät och ett inre nät, t.ex. mellan Internet och ett LAN.
I paketfiltret sker filtrering både på IP- och TCP-nivå. Filterfunktionen är dubbelriktad så att olika filterregler kan sättas upp för utgående och inkommande paket. Man kan dels begränsa de adresser och tjänster som omvärlden kan komma åt i det skyddade nätet, dels begränsa de egna användarnas tillgång till adresser och tjänster i världen utanför.



Servrar

Servrar för www, e-post, FTP o.s.v. kan placeras antingen utanför filtret eller som en ”screened host” inne på det skyddade nätet för att kunna erbjuda sina tjänster till Internet samtidigt som åtkomsten till andra datorer på det lokala nätet hindras.

Paketfiltret kan som extra tillval kompletteras med Proxy-servers för t.ex. e-post och www. I många sammanhang förekommer beteckningen "brandvägg" på denna lösning, men säkerhetsmässigt finns mer att göra.



Brandvägg

Den högsta säkerhetsnivån erhåller man genom att använda två paketfilter och placera servrarna mellan dessa. Utgående trafik förmedlas genom proxy-servers.
På det interna nätet i brandväggen sitter en ”bastion host” som innehåller en roxy-server för varje typ av tjänst som erbjuds in eller ut genom brandväggen. Här placeras också servrar som erbjuder tjänster ut mot Internet. Inga paket tillåts gå direkt från det yttre till det inre filtret eller vice versa. Ytterligare servrar kan finnas på brandväggens interna nät, t.ex. företagets intranet web-server. Paketfiltren sätts upp så att dessa servrar inte kan nås från Internet.

Paketfiltrering eller proxy

De flesta brandväggar bygger på den ena av två grundprinciper och ibland på en kombination av dem: paketfiltrering eller proxy.
Proxy är engelska för "fullmakt" eller "ställföreträdare" och det är precis vad det handlar om. Separata program, eller "proxys", för varje protokoll tar emot förfrågningar från klienterna i

det lokala nätverket och skickar sedan förfrågningarna vidare till rätt maskin på Internet, väntar på svar, och skickar svaret till klienten i det lokala nätet som ursprungligen begärde det. Proxyn tillämpar alltså regler på TCP-sessionen och övervakar dataflödet för att avgöra om varje kommando i sessionen ska tillåtas. Proxy är grundligare än paketfilter och mer effektivt för TCP-trafik.

Proxyns svaghet är att den måste kunna hantera alla protokoll som ska släppas igenom brandväggen. Om det kommer ett nytt protokoll behöver brandväggen nästan alltid uppgraderas för att kunna hantera det.
Proxy har också svårt att hantera UDP-trafik eftersom det är ett lägeslöst protokoll, men det går att ha en generell proxy som hanterar UDP mellan fasta, fördefinierade portar.
En proxy översätter förfrågningar mellan maskiner. Ett paketfilter filtrerar paket.
Brandväggen (ofta en separat maskin) skyddar det interna nätverket mot intrång från Internet.
Paketfilter tillämpar regler baserade på sändarens och mottagarens adresser samt de portar kopplingarna görs på.
Paketfilter arbetar på en lägre nivå (nivå tre, Network, i OSI-modellen) jämfört med proxy som kan arbeta på nivåerna fyra till sju och därför kallas proxys också ofta för tillämpningsgateway.

Stateful inspection eller filtering

En tredje teknik är det som kallas "stateful inspection", "stateful filtering", "stateful multi-layer inspection", "cut-through proxy" eller "adaptive security algorithms". Stateful inspection består huvudsakligen av två komponenter: Mönstermatchning (pattern matching) och lägeskontroll (state maintnance).
Mönstermatchning innebär att brandväggen kontrollerar informationen i paketen för att få veta mer om paketen än bara avsändare och mottagare. Lägeskontroll betyder att brandväggen upprätthåller lägesinformation om pågående datautbyten.
Stateful inspection arbetar mellan nivå två (Data Link) och tre (Network) i OSI-modellen och det innebär att brandväggen tar hand om paketen innan de kommer i kontakt med operativsystemet som körs på brandväggsmaskinen.

Svagheter en hacker letar efter

- Telnet och FTP: Telnet och FTP är protokoll som låter användare logga på andra datorer i ett TCP/IP-nätverk. Det enda åtkomstskyddet är i regel användar-ID och lösenord och många användare väljer lösenord som är enkla att gissa. En hacker som är ansluten till nätverket kan dessutom köra ett sniffer-program som undersöker alla paket på nätet och på det viset komma åt lösenord.
- FTP: FTP eller File Transfer Protocol används för att överföra filer. FTP är en säker och nyttig tjänst som dessvärre lider av samma svagheter som Telnet. Anonym FTP kan, om den konfigureras fel, leda till att hela servern blir åtkomlig utifrån.
- SMTP: Simple Mail Transfer Protocol är ett mycket användbart protokoll som används för att skicka e-post mellan maskiner på TCP/IP-nätverk. Den vanligaste SMTP-servern heter Sendmail och den är ökänd på grund av sina omfattande säkerhetsproblem. Många Sendmail-hack består i att lura Sendmail att köra innehållet i e-postmeddelandet som ett shell-skript på maskinen.

- WWW: Att ta hand om indata från formulär på www via CGI-skript är en potentiell säkerhetsrisk. Många webservrar kommer med en uppsättning standardprogram som ligger i CGI-BIN-biblioteket. Program som inte behövs för organisationens websatsning bör raderas snarast.
- NFS: Network File System är en mekanism för att dela hårddiskvolymer mellan servrar i ett TCP/IP-nätverk. NFS kan vara användbart, men det har vissa designfel som gör det sårbart för hackare. Om möjligt bör NFS stängas av helt och hållet. Alternativet är att använda starkare versioner av NFS som Secure-NFS. När Telias hemsida hackades häromåret togs sig hackarna in via NFS.
- NIS: Network Information Service (tidigare känd som Yellow Pages) låter flera Unixmaskiner dela på samma lösenords-, grupp- och host-filer över nätverket. Hackers brukar försöka stjäla NIS-filerna för att kunna komma åt alla servrar i en NIS-domän. Bör undvikas helt och hållet.

6. Slutsats

Informationssäkerhet är ett komplext ämne, inte minst för att det inte finns någon given definition av vad det är, eller mall för hur man ska ta itu med det. Varje organisation måste bestämma sig för vad säkerhet innebär, och hur mycket arbete och pengar den vill lägga ner på det.

De flesta i beslutsfattande positioner är på det klara med att det största hotet kommer från den egna personalen, något som inte brukar framkomma i t.ex. media, där den stora stygga hackern brukar gälla som den största säkerhetsrisken.
Dock är det många företag som inte har någon beredskap alls, och många som har en bristfällig sådan, ifall något allvarligt skulle inträffa.

Det finns teknik och metoder för att säkra information, de flesta både enkla och billiga. Kunskap och medvetenhet hos personalen är en av de viktigaste resurserna ett företag kan investera i. Det, tillsammans med teknisk utrustning som sköts av kvalificerad personal, torde borga för ett lyckat utförande av ett företags säkerhetspolicy.

7. Källförteckning

Källor på Internet

http://www.excedo.se/infosakerhet.asp

http://www.isecurity.se/forpres.htm

http://home8.swipnet.se/~w-81425/secsv

http://www.packetstorm.com/products.htm

http://www.securiteam.com/