

# *Viktiga tips för en säker och stabil IT-miljö på ditt företag!*

*Att upprätta, underhålla och bibehålla en säker och stabil IT-miljö är inte så omständligt som man kan tro. På ett mindre företag handlar mycket om att vara tydlig med vad som får och inte får göras. Du har också stor nytta av att känna till vilka verktyg och resurser som finns till hands. I denna broschyr ger vi dig handfasta råd, samt tips på åtgärder som hjälper dig att upprätta och bibehålla en stabil IT-miljö.*

# Sju steg för en säker och stabil IT-miljö.

I denna broschyr ger vi dig handfasta tips på hur du upprättar och bibehåller en säker och stabil IT-miljö på företaget, bland annat genom dessa sju steg.

1. Skydda företagets samtliga datorer	Sid. 3
2. Säkerhetskopiera och skydda information	Sid. 5
3. Surfa säkert och informera om riskerna	Sid. 6
4. Skydda företagets nätverk	Sid. 7
5. En säker server = en säker verksamhet	Sid. 8
6. Säkra affärskritiska program	Sid. 9
7. Administrera alla datorer från servern	Sid. 10

## Mer om risker, hot och skydd

Nätfiske (Phishing)	Sid. 11
Att upprätta en policy för informationssäkerhet	Sid. 12
Ordlista	Sid. 14
Mer information	Sid. 15

## 1. Skydda företagets samtliga datorer

Tre grundläggande saker för ett företags IT-säkerhet är att; 1) Hålla mjukvaran uppdaterad, 2) Skydda datorerna mot skadlig kod och 3) Installera en brandvägg. Dessa åtgärder kommer inte att ge dig ett komplett skydd mot säkerhetshot eller minskad effektivitet, men tillsammans utgör de en kraftfull första försvarslinje.

### 1. Håll mjukvaran uppdaterad

Inkräktare gillar att hitta och utnyttja buggar och kryphål i populär mjukvara, vilket såklart kan ställa till med problem. När Microsoft eller ett annat företag upptäcker exempelvis en sårbarhet i mjukvaran, publiceras normalt sett en säkerhetsuppdatering som kan laddas hem över Internet. Uppdateringen åtgärdar sedan kryphålet eller buggen i samband med att den installeras. Besök webbplatsen **Windows Update** för att hämta de senaste uppdateringarna till din dator. Se "Mer information på Microsofts webbplatser" på sid. 15 i denna broschyr.

Uppdateringarna kan även hanteras per automatik om du använder funktionen **Automatiska uppdateringar** i Windows XP med Service Pack 2 (SP2). Du kan justera inställningarna för denna funktion i **Säkerhetscenter**.



### Tips!

Gör så här för att ställa in skräppostfunktionen i Office Outlook 2003:

1. Klicka på menyn **Åtgärder**
2. Välj **Skräppost** och klicka på **Skräppostalternativ**
3. Välj vilken skyddsnivå du vill ha
4. Klicka **OK**

### Tänk på att...

Håll antivirusprogrammet uppdaterat och låt det söka igenom företagets datorer regelbundet.

### 2. Skydda datorerna mot skadlig kod

Virus, liksom maskar och trojanska hästar, är olika typer av skadlig kod som körs på en dator. Skadlig kod kan exempelvis radera eller ändra filer, förbruka datorns resurser eller ge utomstående tillgång till information. Vissa typer kan replikera, kopiera eller skicka sig själva vidare till e-postadresser i en kontaktlista.

Infekterade datorer kan sprida den skadliga koden vidare till datorer inom och utanför ditt företag och orsaka stora förluster av tid och information. Ett antivirusprogram som kan kontrollera alla filer och inkommande e-post bör finnas på samtliga datorer.

Du bör även försäkra dig om att alla dina medarbetare är medvetna om att de ska radera, utan att öppna, alla filer som är bifogade till e-postmeddelanden från okända, misstänkta eller opålitliga avsändare. Ni kan också använda er av de säkerhetsfunktioner som finns i de flesta e-postprogram, exempelvis blockering av bifogade filer. Detta hjälper ytterligare till att upptäcka och rensa bort e-post som kan vara infekterad.

### 3. Installera och aktivera en brandvägg

De flesta företag har tillgång till Internet. Har ni en fast uppkoppling ökar risken att ditt företags nätverk hittas och attackeras av inkräktare. Med en brandvägg minskas risken för detta avsevärt.

#### Det finns två grundtyper av brandväggar:

- **Dedikerade brandväggar** blockerar all trafik som inte är uttryckligen tillåten mellan Internet och ditt nätverk och har som enda uppgift att vara just en brandvägg. Dessa brandväggar kan vara både av såväl hårdvarutyp som mjukvarutyp (exempelvis Microsoft Internet and Acceleration Server (ISA) 2004). Det är en vanligt förekommande missuppfattning att en hårdvarubrandvägg är säkrare än en mjukvarubrandvägg, det som är avgörande är istället att den skall vara av så kallad applikationsfiltrerande typ och inte paketfiltrerande. Detta ger möjligheter att stoppa exempelvis trafik som är "förklädd" att se ut som något annat än det egentligen är.
- **Personliga brandväggar** kan även de vara av både hårdvarutyp och mjukvarutyp. Oftast är de dock av mjukvarutyp, som exempelvis Windows-brandväggen som är inbyggd i Windows XP med Service Pack 2. Denna brandvägg är aktiverad som standard och ger ett fullgott skydd för de enskilda datorerna som de körs på.

#### Visste du att...

Microsoft filtrerar bort 3 miljarder spam varje dag och skyddar mer än 200 miljoner användares brevlådor världen över.

### Hur väljer man rätt brandvägg?

Gemensamt för båda dessa typer är att de undersöker den trafik som passerar i den skyddade datormiljön, och stoppar den trafik som inte uppfyller rätt kriterier. I en nätverksmiljö är en dedikerad brandvägg att föredra eftersom den kan övervaka och skydda samtliga datorer i nätverket från trafik utifrån. En personlig brandvägg skyddar enbart den dator som den används på. För att uppnå bästa resultat så rekommenderar vi att man använder sig av en dedikerad brandvägg i kombination med personlig brandvägg.



**Säkerhetscenter – alla säkerhetsinställningar på ett ställe**

Med hjälp av den enhetliga vyn som finns i **Säkerhetscenter**, kan du snabbt och enkelt hantera och få information om dina inställningar för såväl uppdateringar som brandväggs- och antiviruskydd.

**Säkerhetscenter** hittar du på **Kontrollpanelen**.

## 2. Säkerhetskopiera och skydda information

Att skapa rutiner för regelbunden säkerhetskopiering är ett enkelt sätt att skydda sig mot förlust av information. Vill ni skydda filer eller viss information från att ses och nås av obehöriga kan kryptering eller att sätta olika rättighetsnivåer komma väl till pass.

Förlust av information kan inträffa oavsett hur väl du skyddar den. Detta kan orsakas av trasig hårdvara, eldsvådor, säkerhetsintrång eller att någon helt enkelt råkar radera en viktig fil. Att vara beredd på att detta kan hända är som en försäkring om att din verksamhet snabbt kommer igång igen. Oavsett problemets orsak.

Det finns ett flertal olika sätt för att skydda sin information. Här får du tre grundläggande tips som hjälper dig att komma igång.

### 1. Skapa rutiner för säkerhetskopiering

Att säkerhetskopiera innebär att kopiera information från ett ställe till ett annat. I sin enklaste form kan det innebära att bränna ned viktiga filer på en CD, eller lägga dem på en andra hårddisk. Den bästa lösningen för ett företag är dock att använda en funktion eller ett program som automatiskt sköter säkerhetskopieringen. I Microsoft Windows Server 2003, exempelvis, finns funktioner för detta.

Det finns två grundtyper av säkerhetskopiering; fullständig och inkrementell. Vid fullständig säkerhetskopiering skapas en komplett kopia av all vald information på ett annat media. Vid en inkrementell säkerhetskopiering kopieras endast det innehåll som har lagts till eller ändrats sedan den senaste fullständiga säkerhetskopieringen genomfördes.

En fullständig säkerhetskopiering som kompletteras med inkrementella säkerhetskopieringar är oftast den lösning som är snabbast

och tar upp minst lagringsutrymme. Det kan vara lämpligt att genomföra en fullständig säkerhetskopiering en gång i veckan, följt av dagliga inkrementella säkerhetskopieringar.

### 2. Anpassa rättigheter

Såväl Windows XP som de flesta serverlösningarna och operativsystemen erbjuder skydd mot dataförluster, tack vare avancerade möjligheter att tilldela användare olika anpassade rättighetsnivåer. Åtkomstbehoven varierar förstås kraftigt, beroende på personernas roller och ansvarsområden inom organisationen.

### 3. Kryptera känslig information

Kryptering innebär att du omvandlar information till en form, som endast de du satt rättigheter för, kan läsa. Kryptering används för att skydda känslig information såväl inom ett nätverk som i "vanliga" dokument vi skickar mellan varandra. Windows XP och Microsoft Windows Small Business Server 2003 stödjer krypteringsfunktioner för filer och mappar.

#### Tänk på att...

Testa dina säkerhetskopior ofta genom att återskapa innehållet till en testmiljö. Detta hjälper dig att upptäcka eventuella problem i processen samt vara väl förberedd om olyckan skulle vara framme.

### 3. Surfa säkert och informera om riskerna

Om ditt företag inte har en policy när det gäller användandet av Internet – skaffa en. Webben kan vara ett otroligt kraftfullt verktyg på arbetsplatsen, men den kan också orsaka allvarliga problem som kan resultera i förlorad tid och effektivitet.

Det är lätt att "råka" installera ett program eller ett tillägg om man inte tänker sig för. Riskerna finns också alltid att dina anställda inte vet, eller inte bryr sig om vad man bör göra och inte göra på Internet. Vissa aktiviteter som kan vara direkt sårbara för verksamheten, kanske en ovan användare bara ser det som en "kul grej".

Att upprätta en policy för hur Internet ska användas på arbetsplatsen är därför till stöd och hjälp både för verksamheten och de anställda.

#### Vad er Internet-policy kan innehålla;

- Huruvida anställda har rätt att surfa för personliga ändamål och (i den mån det går) definitioner av vad som är tillåtet i arbetet.
- När får de anställda surfa för personliga ändamål? Exempelvis i samband med lunch eller efter kontorstid.
- Om, och i så fall hur, företaget övervakar användandet av Internet och i vilken grad de anställda kan förvänta sig att vara övervakade.
- Vilka aktiviteter tillåts? Fastställ vilka betenden som inte är accepterade i detalj. Hos många företag inkluderar detta:
  - Nedladdning av stötande innehåll
  - Våldsamt eller hotfullt beteende
  - Kommersiell användning som inte är kopplad till jobbet

Se till att det finns två kopior av policyn; en som de anställda ska behålla och en som de ska skriva under och ge tillbaka till dig.



#### Tips!

##### Tips för att surfa säkert

Utöver Internet-policyn, kan följande rekommendationer vara bra att ha till hands på företaget:

- Besök endast sajter som ni litar på.
- Surfa inte från en server.
- Se till att brandväggen är rätt konfigurerad, för att blockera trafik till och från skadliga webbplatser.
- Vill ni filtrera Internet-användandet finns det flera företag som tillhandahåller mjukvara för detta.
- Hämta bara filer från pålitliga källor.



#### Se även...

Avsnittet "Att upprätta en policy för informationssäkerhet" på sidan 12.

### 4. Skydda företagets nätverk

Fjärråtkomst till nätverket är förträffligt vid exempelvis arbete hemifrån, men det medför även en säkerhetsrisk. Speciellt försiktig bör man vara om man arbetar i ett trådlöst nätverk. Här får du tips på enkla åtgärder som minskar säkerhetsriskerna i ditt nätverk markant.

#### 1. Använd en brandvägg

Som du kunde läsa i det första steget, "Installera och aktivera en brandvägg", kontrollerar brandväggen den interna och externa åtkomsten till nätverket. En brandvägg blockerar inkräktare och kan reglera vad dina anställda ska ha tillgång till om de befinner sig utanför nätverket. Att använda en rätt konfigurerad brandvägg är med andra ord en mycket viktig del i ett säkert nätverk, då denna kommer att förhindra kommunikationen på portar som inte används och därigenom minska attackytan för en potentiell inkräktare.

#### 2. Använd starka lösenord

De flesta företag använder lösenord för att logga in på nätverket, men hanteringen av dessa är tyvärr inte alltid den bästa. Lösenorden ska förvaras på ett bra sätt, inte vara för enkla och ändras ofta. Ett lösenord är lika viktigt att hålla koll på som en nyckel till kontoret.

#### 3. Trådlöst nätverk? Använd trådlösa säkerhetsfunktioner!

Trådlösa nätverk använder en radiolänk istället för kablar för att koppla samman datorer. Som en följd av detta, kan vem som helst inom rätt avstånd teoretiskt sett övervaka eller använda nätverket. Det finns inbyggda säkerhetsfunktioner i de så kallade Wi-Fi-produkterna, men tillverkarna låter ofta dessa vara avstängda som standard, eftersom det förenklar installationen av nätverket. Om du använder ett trådlöst nätverk bör du vid minsta tveksamhet kring hur det ska sättas upp säkert, kontakta någon firma som kan assistera. Trådlösa nätverk som inte är rätt konfigurerade är en väldigt enkel dörr in i många företagsnätverk och vikten

av att låsa denna dörr kan nog inte understrykas tillräckligt.

#### 4. Stäng onödiga nätverksportar

Nätverksportarna möjliggör kommunikation mellan datorer och servrar i nätverket. Oanvända eller onödiga portar bör stängas genom att använda brandvägg eller filter, men tänk på att produkter inom Microsoft Windows Server System använder ett flertal olika numrerade nätverksportar och protokoll i sin kommunikation.



#### Tips!

##### Tips för starka lösenord

- Undvik lösenord som är lätta att gissa sig till. Detta kan till exempel vara lösenord som utgörs av deras användarnamn, formuleringar som "password", "1234" eller att ersätta till exempel "i" med "!" eller "s" med "\$".
- Tänk på en "lösenfras". Oftast när man tänker på ett lösenord så blir det väldigt kort och komplext och kanske inte alltid särskilt logiskt att komma ihåg. Om man däremot tänker på en mening som exempelvis "Jag skall på semester till Norge sommaren 2008" så blir det ganska hopplöst att som utomstående försöka gissa sig till detta men det blir väldigt logiskt att komma ihåg. Även om lösenordet är långt.
- En lösenordspolicy bör se ut enligt följande:
  - Minst åtta tecken långt.
  - Kombinera gemener, versaler, siffror och symboler.
  - Förändras åtminstone var 90:e dag, till något som skiljer sig markant från tidigare lösenord.
  - En serveradministratör kan skapa regler centralt som till exempel styr hur gamla de vanliga användarnas lösenord får bli innan de tvingas byta. På så sätt kan ni försäkra er om att de viktigaste inslagen i er lösenordspolicy efterlevs.

## 5. En säker server = en säker verksamhet

Företagets server (eller servrar) är nätverkets kommandocentral. Att hålla efter en modern server är relativt enkelt och ett mycket smidigt sätt att se till att verksamheten hålls säker och stabil.

På ett mindre företag är en server ofta kärnan för lagring, säkerhetskopiering, nätverksövervakning och e-post. I vissa fall kan den också användas för att köra vissa program, eller för att hantera företagets webbplats.

Många av de åtgärder som redan har diskuterats hjälper till att skydda även dina servrar. Så om du inte redan gjort följande, se till att prioritera:

- **Steg 1** – Skydda företagets samtliga datorer
- **Steg 2** – Säkerhetskopiera och skydda information
- **Steg 3** – Surfa säkert och informera om riskerna
- **Steg 4** – Skydda företagets nätverk

Man kan aldrig skydda sin server (eller sina servrar) för mycket. Här får du ytterligare tips, utöver ovanstående.

### 1. Förvara servrarna på en säker plats

Placera servern i ett säkert, välventilerat rum, aldrig i en korridor eller under ett skrivbord där någon kan komma åt den. Det kan handla om något så enkelt som att av misstag råka sparka till eller spilla kaffe på den men även en direkt möjlighet för någon att manipulera servern. Vi rekommenderar starkt att serverrummet inte har några fönster och att det skall gå att låsa. Även serverns chassi bör vara låst och den IT-ansvarige bör ha god koll på vem eller vilka som har nyckel till serverrummet. Förvara gärna en lista över servrarnas serienummer på ett säkert ställe, samt märk dem med information om företaget, så att de kan identifieras och återlämnas om de skulle bli stulna.

### 2. Ange inte onödiga rättigheter

För att bibehålla en säker IT-miljö bör servern användas för att hantera företagets datorer centralt, och att endast administratören har administratörsåtkomst till servern. Windows-baserade servrar kan konfigureras för att enbart ge enskilda användare tillgång till specifika program och att definiera vilka åtgärder som är tillåtna på servern.

Detta säkerställer att användarna inte kan förändra sådant som är nödvändigt för att servern eller den egna datorn ska fungera korrekt. Det förhindrar dessutom användare från att installera programvara som kan vara infekterad med skadlig kod eller som på annat sätt hotar nätverkets säkerhet.

### 3. Ha kunskap om de säkerhetsalternativ som finns

Dagens servrar är säkrare än någonsin, men de kraftfulla säkerhetsfunktioner som du finner i produkter inom Microsoft Windows Server System är bara till nytta om de används på ett lämpligt sätt och övervakas ordentligt. Om ditt företag inte har en IT-ansvarig med rätt kunskaper och tid bör ni överväga att anlita en konsult eller ett externt företag för att skydda servern och företaget, på ett lämpligt sätt.

#### Tänk på att...

Säkerhet uppnår man inte en gång för alla, det kräver löpande och kontinuerligt arbete.

## 6. Säkra affärskritiska program

Många företag använder program avsedda för exempelvis hantering av ekonomi, försäljning eller kundhantering. Dessa typer av program körs vanligtvis på en server och arbetar mot en databas. Här är det viktigare än någonsin att ha en policy för att skydda sin information.

### 1. Skydda det fundamentala

Att skydda databaser från oönskade intrång och andra hot, inleds med att genomföra grundläggande datasäkerhetsåtgärder på arbetsplatsen. Installation av en brandvägg, viruskydd och mjukvaruuppdateringar är som sagt nödvändigt. Liksom säkerhetskopiering och användandet av säkra lösenord.

### 2. Reglera åtkomsten till information

Alla bör inte ha åtkomst till allting på arbetsplatsen. Med lösningar inom Windows Server System kan ni centralt och enkelt möjliggöra eller förhindra användarnas tillgång till dokument och program. Du kan bland annat ange om en användare enbart har läsrättigheter, eller om hon även har rätt att redigera en fil. Här finns möjlighet att gruppera användarkonton och ange rättigheter baserat på grupptillhörigheter snarare än att konfigurera säkerheten för varje enskild användare. Detta kan spara mycket tid i samband med administration av åtkomstmöjligheterna.

### 3. Skydda informationen i databasen

Var noga med databassäkerheten, inte minst eftersom affärsspecifika program vanligtvis arbetar mot en eller flera databaser. Här nämns några av de åtgärder som du kan genomföra:

- Installera de senaste uppdateringarna och Service Packs som finns tillgängliga för serveroperativsystemet och dess applikationer.
- Fastställ din servers säkerhet med **Microsoft Baseline Security Analyzer**

(MBSA), ett verktyg som söker efter vanliga konfigurationsbrister i många av Microsofts produkter.

- Använd Windows-autentisering vid arbetet mot Microsoft SQL Server. Databaserna skyddas mot de flesta Internet-baserade attacker om åtkomsten begränsas till Windows- och domän-användarkonton.



#### Vill du ha hjälp?

Microsoft erbjuder ett enkelt verktyg helt på svenska för att arbeta med den här formen av frågor. Verktyget heter Microsoft Security Risk Self-Assessment och kan hittas på <http://securityguidance.com>

Fler tips på läsning, resurser och verktyg hittar du i avsnittet "Mer information på Microsofts webbplatser" på sidan 15.

## 7. Administrera alla datorer från servern

Att administrera alla datorer centralt från servern är ett enkelt sätt att få kontroll och överblick av nätverket och vad som är installerat på de enskilda datorerna.

Om varje användare själv sköter sina program-uppdateringar, finns det alltid en ökad risk att någon laddar hem otillåten och potentiellt skadlig mjukvara. Genom att administrera företagets samtliga datorer från servern minskas risken att genomtänkta säkerhetsåtgärder misslyckas. I de flesta fall medför det också betydelsefulla besparingar i tid och pengar eftersom såväl den som sköter servern som de enskilda användarna kan koncentrera sig på det de gör bäst – och göra det rätt.

### Fördelar med central administration

- **Korrekt grundinstallation.** Du kan säkerställa att korrekta versioner av operativsystem och programvara installeras på alla datorer – stationära som bärbara. Detta säkrar också att licensavtal åtlöds och att allting fungerar konsekvent i samband med hantering av delade filer eller liknande.
- **Uppdateringar i rätt tid.** Säkerhets-uppdateringar och bugg-fixar, samt nya versioner av mjukvara, kan installeras från servern till användarnas datorer. På så sätt vet du att uppdateringarna har genomförts på rätt sätt och du behöver inte förlita dig på att användarna ska komma ihåg att göra det själva. För detta finns kostnadsfria verktyg som kan hjälpa dig. Se "Mer information på Microsofts webbplatser" på sidan 15.
- **Särskilda konfigurationer.** Om företaget vill ha särskilda inställningar för operativsystemet eller de program som används kan dessa hanteras, uppdateras och genomdrivas från servern. Du kan dessutom förhindra att användare installerar otillåtna program genom att begränsa

deras möjlighet att köra program från exempelvis CD-skivor eller Internet.

- **Övervakning.** Om det förekommer otillåten åtkomst till en dator, eller om det uppstår ett systemfel av något slag på en enskild dator, kan detta upptäckas omedelbart genom övervaknings-möjligheterna som finns i en kontrollerad datormiljö.

I serverlösningar och serveroperativsystem inom Windows Server System finns omfattande administrationsmöjligheter och säkerhetsfunktioner. Står ni inför att köpa er första server kan helhetslösningen **Microsoft Windows Small Business Server 2003 (SBS 2003)** vara ett bra val.



### Tips!

#### SBS 2003 – en praktisk helhetslösning

Serverlösningen SBS 2003 är anpassad för företag med upp till 75 användare och ger en kostnadseffektiv, smidig och säker lösning för såväl lagring, samarbete, e-post som säkerhet.

Hitta fler serverlösningar på

[www.microsoft.se/windowsserversystem](http://www.microsoft.se/windowsserversystem)

Läs mer om SBS 2003 på:

[www.microsoft.se/sbs2003](http://www.microsoft.se/sbs2003)

## Nätfiske (Phishing)

Phishing är en sorts bedrägeri som går ut på att stjäla din identitet. Vid phishing försöker en illvillig person att få information såsom kreditkortsnummer, lösenord, kontoinformation eller annan personlig information genom att få dig att lämna ut den under falska premisser.

Phishing kommer vanligtvis via skräppost eller popup-fönster. Phishing fungerar på så sätt att den som vill lura dig och stjäla din identitet skickar ett falskt e-postmeddelande (ofta som massutskick) som ser ut att komma från en webbplats du litar på och ofta besöker, exempelvis din bank eller ditt kreditkortsföretag.

För att få dessa falska e-postmeddelanden att verka ännu mer korrekta kan de som skickar dem bifoga en länk som går till den riktiga webbplatsen, men som i verkligheten tar dig till en falsk webbplats eller ett popup-fönster som ser ut exakt som den officiella webbplatsen.



### Tips!

På Microsofts webbplats om säkerhet hittar du kontinuerligt uppdaterad information om phishing och andra säkerhetshot. Här finns även information om de senaste säkerhets-uppdateringarna du rekommenderas att installera.

[www.microsoft.se/security](http://www.microsoft.se/security)

### Följ de här fem enkla stegen för att skydda dig och företaget

- Svara aldrig på frågor om personlig information via e-post. Om du är tveksam, ring upp företaget som säger sig ha skickat brevet.
- Besök webbplatser genom att du själv skriver in webbadressen i adressfältet.
- Granska regelbundet dina kreditkorts- och kontoutdrag.
- Om du har utsatts för phishing bör du omedelbart anmäla det till företaget vars webbplats har blivit förfalskad eller till relevant myndighet.
- Kontrollera att webbplatsen använder kryptering.

För att kontrollera att webbplatsen använder kryptering kan du dubbelklicka på låsikonen (hänglåset) för att se säkerhetscertifikatet för webbplatsen. Det namn som följer efter "Utfärdat till" ("Issued to") ska överensstämma med den webbplats du tror att du besöker. Om namnet skiljer sig är du med största sannolikhet på en falsk webbplats. Om du inte är säker på att ett certifikat är riktigt ska du inte ange någon personlig information. Ta det säkra före det osäkra och lämna webbplatsen.



Dubbelklicka på hänglåset då du vill se säkerhetscertifikatet för webbplatsen.

## Att upprätta en policy för informationssäkerhet

I Microsofts arbete med säkerhetsfrågor har vi tydligt utgått ifrån att god informationssäkerhet utgår ifrån individers och organisationers kompetens att själva bedöma vilken säkerhetsnivå som eftersträvas. Först därefter kommer investeringar i organisation, tjänster och produkter.

Här ger vi dig några tankar, idéer och tips på hur du lättast kommer igång med att definiera ditt företags acceptabla risknivå, samt hur ni kan formulera er policy för informationssäkerhet.

### Hur är vi organiserade och vad gör vi?

En tumregel för att arbeta effektivt med informationssäkerhet är att göra det så enkelt som möjligt. Einstein har rätt i följande uttalande: "Allting bör göras så enkelt som möjligt, men inte enklare". Det är grundtesen i arbetet med att definiera en policy för informationssäkerhet.

Den allra första frågan att tänka på är hur just ditt företag ser ut. Vilka produkter/tjänster gör ditt företag unikt, hur det är organiserat och vilka samarbetspartners har ni för att ta verksamheten framåt. Det här är självklarheter som ibland glöms bort för att många tenderar att endast fokusera på tekniken.

När du har skapat dig en färdig bild av ovanstående är det dags att börja titta på vilka potentiella risker som är förknippade med företaget så som det ser ut. I det här läget är det dags att skapa en riskprofil som därefter utgör en mät punkt mot vilken alla insatser för informationssäkerhet mäts. I skapandet av riskprofilen är det viktigt att täcka in följande delar:

- **Människor och processer.** Har ni egen IT-kompetens eller anlitas extern kompetens? Hur hanteras känslig information utanför företagets lokaler? Har företaget någon form av medvetenhets-

höjande program på plats? Hur teknikmogna är medarbetarna? Finns tydliga roller/ansvar för att hantera informationens tillgänglighet och kvalitet?

- **Infrastruktur.** Hur ser företagets nätverk ut? Vilka in- och utgångar finns inom nätverket? Finns det någon form av extern tjänst på samma nätverk som det interna? Får anställda själva installera exempelvis program i nätverket?
- **Applikationer och information.** Vilka är de kritiska tillämpningarna och är ni beroende av data som lagras utanför företaget? Finns det åtkomstskydd för känsliga tillämpningar? Finns det Internetåtkomst till företagets kritiska applikationer? Vilken information är den mest kritiska för företaget?

I det här läget har du en ganska god bild över företagets målsättningar, organisation och vilka faktorer som är kritiska för att stötta företaget framåt.

### Nu till det praktiska

Nu börjar det riktigt roliga – att införa en policy för informationssäkerhet och få med alla medarbetare i processen. En sådan policy kan vara stor, genomarbetad och enormt detaljrik. Huvudsaken är dock att den används och gynnar verksamheten, därför rekommenderar vi en kortfattad, informativ och lättillgänglig policy. Exempel på innehåll, i korthet:

- Företaget AB vill skydda sina tillgångar mot otillbörlig användning av utomstående. Följande information är kritisk för

företagets fortlevnad: ( lista på det ni kommit fram till ) Den informationen vill vi skydda genom; regelbunden säkerhetskopiering och halvårsvis återställning av information, förvaring av datamedia på avsedd plats, åtkomstkontroll, uppföljning av loggar med mera.

- Medarbetaransvaret är kritiskt för framgången. Företaget förstår att ansvar kommer från självförtroende och tillit. Företaget kommer därför att ha kontinuerliga utbildningar och uppföljningar för att säkerställa att varje medarbetare är trygg med den policy som är fastställd.
- Samverkan med extern tredje part kommer att ske för att regelbundet göra en revision kring målbild och efterlevnad.



### Tips!

Lansera företagets policy för informationssäkerhet på ett festligt sätt för att få samtliga medarbetare att uppmärksamma den. Exempel på aktiviteter kan vara;

- En kick-off där ni redogör för hur policyn följs upp, revideras och kommuniceras.
- Dagliga meddelanden om IT-säkerhet på företagets intranät.
- Veckovisa e-postmeddelanden med information om er IT-säkerhet.

### Visste du att...

Det tar i genomsnitt 20 minuter för en PC som ansluts till Internet att bli smittad av något slags elakartat program, exempelvis en mask.

Enligt Internet Storm Center som ingår i Sans Institute.



# Ordlista

<b>Bakdörr</b>	En bakväg in i ett datorsystem utan att administratören eller användaren vet om det. Blockeras i de flesta fall av en rätt inställd brandvägg.
<b>Beta</b>	En beta-version av ett program är en version som inte är fullständigt färdig och släppt. De flesta beta-versioner körs på egen risk, utan möjlighet till support.
<b>BotNET</b>	BotNET är ett nätverk av datorer som har tagits över via någon form av skadlig kod. De infekterade datorerna ingår därefter i ett dolt nätverk som ofta kommunicerar via Internet Relay Chat (IRC). En hacker kan tack vare detta utlösa avståndsattacker eller e-postutskick från massor av maskiner utspridda över hela Internet.
<b>Hackare</b>	Svenska för engelskans "hacker". Person som är mycket skicklig i att göra egna program eller ändra i andras program.
<b>Hoax</b>	En varning om ett virus som inte finns, det vill säga ett rykte som du uppmanas att skicka vidare till alla du känner.
<b>Internet Relay Chat (IRC)</b>	En av de tidigaste formerna, och än idag en av de vanligaste för interaktion mellan användare över Internet.
<b>Knäckare</b>	Svenska för engelskans "cracker". Person som försöker forcera datorsystems säkerhets spärrar i syfte att sabotera programvara eller att komma åt skyddad information.
<b>Mask</b>	Ett program som försöker sprida kopior av sig självt från dator till dator, vanligen via e-postmeddelanden.
<b>Nätfiske (phishing)</b>	Vid phishing försöker en illvillig person att få information såsom kreditkorts-nummer, lösenord, kontoinformation eller annan personlig information genom att få dig att lämna ut den under falska premisser. Phishing drabbar dig vanligtvis via skräppost eller popup-fönster.
<b>RC</b>	RC står för Release Candidate. Efter att en beta släppts och feedback samlats in från de som testat kan en RC1 släppas, och efter det en RC2 och så vidare tills den färdiga produkten finns att tillgå.
<b>Rootkit</b>	En programvara som helt tar över det infekterade systemet. Detta görs så grundligt att det därefter är Rootkitet som avgör vad man ser på sin maskin, även om man är administratör. Även backuper kan vara infekterade.
<b>Service Packs</b>	Service Packs är större serviceuppdateringar som regelbundet släpps för program. Ett Service Pack är kumulativt, det vill säga innehåller samtliga korrigeringar som släppts separat eller i tidigare Service Packs.
<b>Skadlig kod</b>	Samlingsnamn för bakdörrar, maskar, spionprogram, trojanska hästar, virus med mera.
<b>Social manipulation</b>	Svenska för engelskans "Social Engineering". Kanske den form av dataintrång som är svårast att skydda sig emot. Det handlar om att en hacker utnyttjar människans naturliga instinkt att försöka hjälpa till, genom att manipulera till sig information via exempelvis telefon eller som en vän.
<b>Spam</b>	Oönskat massutskick av skräppostmeddelanden via Internet, med reklam för olika företag och tjänster.
<b>Spionprogram</b>	Program som samlar in information om dig och ditt beteende på Internet utan att du vet om det.

<b>Spoof</b>	Spoofing är när någon förfalskar en avsändaradress för att lura mottagaren. Spoofing är en typ av identitetsstöld.
<b>Säkerhetscenter</b>	En funktion i Microsoft Windows XP med Service Pack 2 där du kan hantera datorns samtliga säkerhetsinställningar.
<b>Säkerhetsuppdatering</b>	Microsofts programuppdateringar som åtgärdar kända problem och skyddar mot dataintrång. Installeras via Windows Update eller funktionen Automatiska Uppdateringar i Microsoft Windows.
<b>Trojansk häst</b>	Ett program som utger sig för att ha en viss funktion, men som även har andra dolda och skadliga funktioner. De dolda delarna aktiveras vid en viss inmatning eller tidpunkt och kan ställa till problem.
<b>Virus</b>	Ett datorprogram som sprider sig själv genom att lägga till sig på andra objekt.

## Mer information på Microsofts webbplatser

### Läs, lär och hitta information

Microsofts säkerhetswebb  
[www.microsoft.se/security](http://www.microsoft.se/security)

Microsofts webbplats för småföretagare  
[www.microsoft.se/smb](http://www.microsoft.se/smb)

TechNet, Microsofts webbplats för IT-proffs  
[www.microsoft.se/technet](http://www.microsoft.se/technet)

### Hämta och installera uppdateringar

Windows Update (Microsoft Update)  
[windowsupdate.microsoft.com](http://windowsupdate.microsoft.com)

Office Update (Microsoft Update)  
[office.microsoft.com/sv-se/officeupdate](http://office.microsoft.com/sv-se/officeupdate)

Microsoft Download Center  
[www.microsoft.com/downloads](http://www.microsoft.com/downloads)

### Verktyg och resurser

Software Update Services (SUS)  
Microsoft Windows Update Services (WUS)  
Microsoft Baseline Security Analyzer (MBSA)  
Malicious Software Removal Tool  
Microsoft Windows AntiSpyware

Hitta dessa och fler verktyg på  
[www.microsoft.se/security](http://www.microsoft.se/security)

### Kostnadsfri virussupport

Microsoft erbjuder kostnadsfri support på frågor och problem som rör virus.  
Tel: 08-752 09 29

[www.microsoft.se/support](http://www.microsoft.se/support)

### Nyhetsbrev

**Anmäl dig till nyhetsbrevet för småföretagare och få tipsen via e-post. Självklart ger vi dig också det senaste om kurser, seminarier och aktuella erbjudanden.** [www.microsoft.se/smb](http://www.microsoft.se/smb)

### Microsoft Security Update

Information om säkerhetsuppdateringar och hot för småföretag (på engelska).

### Security Notification Service

Information om säkerhetsuppdateringar och hot för IT-proffs (på engelska).

Hitta dessa och fler nyhetsbrev på  
[www.microsoft.se/security](http://www.microsoft.se/security)

### Småföretagare?

På Microsofts webbplats för småföretagare finns användbar information och tips på arbetsätt och lösningar. Här hittar du bland annat inköpsråd, utförliga artiklar och handfasta tips på hur du löser ett problem här och nu.

### Nyhetsbrev

Anmäl dig till nyhetsbrevet för småföretagare och få tipsen via e-post. Självklart ger vi dig också det senaste om kurser, seminarier och aktuella erbjudanden.

[www.microsoft.se/smb](http://www.microsoft.se/smb)

## Varför är det så viktigt med säkerhet?

Vi hoppas att du som innan du läste denna broschyr tänkte "Vem skulle vilja angripa mitt företag när det finns mycket större företag att ge sig på?", nu istället tänker "Klart vi ska satsa på säkerhet och se till att alla är medvetna om riskerna". För visst stämmer det att mindre företag inte attackeras lika ofta som större företag, men det händer. Och det händer ofta. Och det är extremt onödigt, eftersom det är förhållandevis enkelt att undvika.

Att återställa datorsystemet tar tid, och tid är som vi alla vet pengar. Tänk över hur det skulle vara att inte kunna använda datorn på en vecka, eller att förlora all information ni har lagrad. Handeln på hjärtat – är det värt det? Vi vet att det kan verka krångligt och att vissa experter har en tendens att få grundläggande säkerhet att verka vara komplicerat och svårt. Vi vet också att det INTE är så – att skydda sitt företag är enklare än man tror. Förhoppningsvis har du fått flera tips och hjälp på vägen i denna broschyr.

På Microsoft webbplats för småföretagare finns avdelningen **Security Guidance Center**, där du förutom länkar till mer information, resurser och verktyg hittar en repetition av de sju stegen i denna broschyr. Tillammans med webbplatsen **Säkerhet** hoppas vi här kunna ge dig all den vägledning du behöver för att säkra din IT-miljö. Om inte, är du alltid välkommen att kontakta oss på telefon eller via e-post.

[www.microsoft.se/smb](http://www.microsoft.se/smb)  
[www.microsoft.se/security](http://www.microsoft.se/security)  
[www.microsoft.se/contact](http://www.microsoft.se/contact)

**Microsoft kundservice, tel 08 - 752 56 30**