HANTERING
AV
IT-INCIDENTER
- vem gör vad och hur?

CSIRC

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY

ADMINISTRATIV VÄGLEDNING

Förord

Den omfattande användningen av informationsteknik (integration av datateknik, telekommunikation och mikroelektronik) för insamling, lagring, utsökning, bearbetning och distribution av information har medfört att en hög nivå av IT-säkerhet är en nödvändig förutsättning för verksamheten.

Hundraprocentig säkerhet är en illusion medan snabb och effektiv hantering av IT-incidenter, dvs. IT-relaterade säkerhetsincidenter, har blivit lika viktig som snabb och effektiv hantering av andra typer av säkerhetsincidenter, t.ex. inbrott eller brand.

Denna rapport innehåller riktlinjer och råd för etablering och drift av s.k. CSIRC-funktioner (Computer Security Incident Response Capability), dvs. organisationsenheter för beredskap och operativ insats vid IT-incidenter.

Allvarligare IT-incidenter måste hanteras i lämpligt sammansatta grupper med specialkompetens. Sådana grupper kallas ofta CSIRT (Computer Security Incident Response Team) på lokal, t.ex. myndighets-, nivå och CERT (Computer Emergency Response Team) på övergripande, t.ex. sektoriell eller nationell, nivå.

Verksamheten inom en CSIRC påminner starkt om verksamheten inom en räddningstjänst: förmågan att snabbt reagera på en specifik, kritisk händelse måste kompletteras med förebyggande aktiviteter. Dessa aktiviteter ska dels minimera risken att något oönskat inträffar, dels garantera en beredskap i hela organisationen om något mot förmodan ändå inträffar.

Rapporten har utarbetats gemensamt av Statskontoret och IT-kommissionens observatorium för informationssäkerhet och i samråd med Rikspolisstyrelsen (RPS) genom Säkerhetspolisen (SÄPO) och, under det inledande skedet, Svenska Arbetsgivarföreningen (SAF).

Följande personer har deltagit i arbetet:
- Bengt Angerfelt, Säkerhetspolisen
- Anne-Marie Eklund-Löwinder, IT-kommissionen
- Robert Malmgren, Robert Malmgren AB
- István Orci, Statskontoret

Post- och telestyrelsen har, på regeringens uppdrag, utrett förutsättningar för att inrätta en särskild funktion för IT-incidenthantering på nationell nivå och föreslagit inrättandet av ett nationellt CERT under en försöksperiod om 2 år. Detta förslag, sett i ett större sammanhang, har också infogats i Sårbarhets- och säkerhetsutredningens nyligen presenterade betänkande (SOU 2001:41).

CERT-organisationer finns i de flesta industriländer sedan några år tillbaka. Det finns också ett väletablerat, internationellt samarbete mellan många av dessa inom ramen för FIRST (Forum of Incident Response and Security Teams). FIRST har ca 70 medlemmar från ett tjugotal länder världen över. Medlemsorganisationerna representerar såväl offentlig förvaltning och näringsliv som universitet och högskolor.

Statskontoret, IT-kommissionen och RPS menar att existensen av organisationsinterna, lokala CSIRC är en förutsättning för att globala CERT, t.ex. den föreslagna nationella CERT, ska fungera effektivt. Föreliggande rapport syftar till att underlätta etablering av sådana, organisationsinterna, lokala CSIRC.

Nils Qwerin
Statskontoret

Christer Marking
IT-kommissionen

Sammanfattning

Säkerhetsincidenter, såväl IT-relaterade som andra, skapar ”bad will”, tär på resurser, stjäl tid och kostar pengar. Dels kan de ekonomiska och andra konsekvenserna av en incident vara betydande, dels krävs det resurser för att

- utreda och eliminera orsakerna
- återgå till normal verksamhet

Vägledningen syftar till att underlätta en systematisk hantering av IT-relaterade säkerhetsincidenter (IT-incidenter) i enskilda organisationer. Den ger bl.a. råd och vägledning avseende ledning, organisation och administration av såväl CSIRC-funktionen som av insatsgrupper (CSIRT) för hantering av mera allvarliga IT-incidenter.

Det första avsnittet är en allmän inledning medan avsnitt 2 är en populär introduktion till incidenthantering. Avsnittet behandlar IT-intrång och är en omarbetad version av en artikel skriven av Robert Malmgren.

Avsnitt 3, Styrande regelverk, beskriver kort övergripande krav och restriktioner på IT-säkerhet, inkl. krav och restriktioner på incidenthantering.

Avsnitt 4 har rubriken Arbetsmodell för incidenthantering och presenterar en generell modell för incidenthantering. Modellen är en systematisering och strukturering av vad man vanligen gör (eller borde göra) när en IT-incident inträffar. Den bygger delvis på en modell utarbetad av SANS Institute (System Administration and Network Security) i ett samarbetsprojekt med AusCERT samt ett femtiotal företag och organisationer i USA.

Avsnitt 5, Ledning, organisation, administration, behandlar frågor som:
- motiv för etablering
- syfte och mål
- ansvarsområde
- personresurser
- organisation
- kompetens
- utrustning
- kommunikation

Avsnitt 6, Typiska aktiviteter, exemplifierar och ger en mera detaljerad beskrivning av vissa CSIRC/CSIRT-aktiviteter.

Avsnitt 7, Systemutveckling och -förvaltning, beskriver kort hur incidenter ska hanteras i den normala systemförvaltningsmiljön. Förutom frågor om inrapportering av incidenter och användaråtgärder vid en incident berörs sambandet mellan systemutveckling och incidenthantering.

I det avslutande avsnittet behandlas diverse frågor av intresse vid etableringen av en CSIRC.

Bilaga 1, IT-incidenter och polisanmälan, är råd från Rikspolisstyrelsen om vad som bör göras i samband med en polisanmälan.

Bilaga 2, Krisråd för vilsna, är praktiska råd i kortform om hur man bör agera om olyckan är framme.

Bilaga 3, IT-incidenter, beskriver de vanligaste typerna av IT-incidenter. Bilagan är hämtad från PTS:s utredningsrapport avseende förutsättningar för att inrätta en särskild funktion för IT-incidenthantering.

Bilaga 4, Kompetensområden CSIRC/CSIRT, är ett försök att beskriva de grundläggande kompetenskraven på medlemmar i en CSIRC eller ett CSIRT.

Innehållsförteckning

Introduktion

Hot och risker

Användningen av lokala och allmänt tillgängliga datanät i verksamhetskritiska system har ökat kraftigt och förväntas fortsätta att öka. Den utbyggda IT-infrastrukturen i form av nätverk, datorsystem och kritiska tillämpningar - i kombination med den ökade allmänna kompetensen om och användandet av informationsteknik - gör att risken för såväl interna som externa IT-attacker ständigt ökar.

Exempel på vanligt förekommande externa angrepp är datavirus, avsiktlig störning av tillgänglighet, avlyssning av datanät och fjärrstyrning av arbetsstationer. Exempel på vanligt förekommande interna angrepp är obehörig läsning av känslig information och spridning av elektroniska hatbrev. (För en mera omfattande förteckning av potentiella hot se bilaga 3.)

Den vanligaste angriparen i dag är en enskild hacker/cracker med syftet att briljera eller skada. Det finns dock misstänkta fall av organiserat industrispioneri, både nationellt och internationellt. Under senare tid har det även förekommit informationsoperationer med politiska syften riktade mot ekonomiska eller nationella intressen.

Skyddsåtgärder

För att minska sårbarheten, och därmed säkerhetsriskerna, kan vi vidta olika typer av åtgärder:

- proaktiva (förebyggande), t.ex. i form av införande av behörighetskontrollsystem eller incidentrapporteringssystem
- aktiva (operativa), t.ex. i form accesskontroll i realtid eller säkerhetsloggning
- reaktiva (detektiva och korrigerande), t.ex. i form av intrångsdetektering eller incidentrespons i realtid
- postaktiva (återställande), t.ex. i form av återstartsystem och återhämtningsprocedurer

En organisations samlade säkerhetsskydd - och deras samspel inbördes och med verksamheten - utgör ryggraden i organisationens säkerhetssystem. Både verksamhetssystem och säkerhetssystem är i de flesta fall komplexa och kan innehålla luckor och svagheter orsakade av konstruktionsmissar, programmeringsfel, installationsmissar, handhavandefel, etc. Detta inte minst på grund av den snabba tekniska utvecklingen på IT-området.

Dessa faktorer, bland andra, har framhävt betydelsen av reaktiva mekanismer i form av operativ beredskap hos organisationer att handskas med IT-incidenter på ett effektivt sätt.

Utredningar och polisanmälan

De flesta IT-incidenter är inte ett resultat av brottsligt uppsåt; de uppstår på grund av bristande kompetens, misstag, felaktig användardokumentation, etc. Icke desto mindre måste varje incident utredas om man ska kunna undvika händelser av samma slag i framtiden.

En del incidenter har emellertid kriminell bakgrund och kan medföra omfattande internutredningar, eventuellt med efterföljande polisanmälan. Att i dessa situationer agera på rätt sätt är viktigt; dels för att minska de egna utrednings- och återhämtningskostnaderna samt stilleståndstiderna, dels för att möjliggöra och underlätta polisens arbete.

Juridiska aspekter

Utredning av IT-incidenter ställer särskilda krav på juridisk kompetens både vid externa angrepp och interna oegentligheter. Det är därför av vikt att CSIRC-funktionen garanteras tillgång till juridisk expertis både i det operativa (t.ex. internutredning) och strategiska (t.ex. policyutformning) arbetet.

Vägledningens målgrupp

Vägledningen riktar sig till organisationer som driver, eller planerar att inrätta och driva, en lokal CSIRC. Den behandlar inte hantering av IT-incidenter på global nivå, annat än mycket summariskt när det gäller samarbetet mellan lokala CSIRC och globala CSIRC/CERT (Computer Emergency Response Team) på t.ex. nationell eller internationell nivå.

Grundläggande termer

För att underlätta förståelsen och undvika misstolkning förklaras här ett antal akronymer, begrepp och termer.

CERT	*Computer Emergency Response Team* global organisation för att hantera allvarligare IT-incidenter (används ibland som synonym till CSIRT)
CSIRC	*Computer Security Incident Response Capability* enhet med beredskap och förmåga att hantera IT-incidenter
CSIRT	*Computer Security Incident Response Team* insatsgrupp för att hantera IT-incidenter
FIRST	*Forum of Incident Response and Security Teams* internationellt forum för samarbete mellan såväl offentliga som privata CERT och CSIRC

fullständig jour	jour under hela den tid ett IT-system är nominellt tillgängligt för användning
informations-säkerhet	säkerhet vid hantering av information avseende sekretess, integritet, tillgänglighet, äkthet och oavvislighet
IT-säkerhet	säkerhet i IT-system
IT-incident	IT-relaterad säkerhetsincident
säkerhets-incident	oplanerad och icke-önskad händelse som innebär ett säkerhetshot

1 Incidenthantering i ett nötskal

Vad bör man tänka på vid ett intrång? Vad kan gå fel och hur gör man en bra utredning? Här ges exempel på förberedelser och praktiska tips att ta till vid en incident.

Frågan är inte om, utan när, eller snarare hur ofta, man blir drabbad. Statistik visar att antalet upptäckta säkerhetsluckor i de vanligaste operativsystemen har ökat drastiskt de senare åren. Med ett större antal möjliga säkerhetsluckor blir det lättare för en angripare att ta att sig in i ett system genom att hitta en svaghet som man missat eller inte tror sig ha.

Många gånger vidtas en mängd ogenomtänkta åtgärder vid en incident. Det kan vara driftspersonal som på eget bevåg, utan att informera någon ansvarig, tar kontakt med en inkräktare eller med någon i den organisation varifrån attackerna kommer. Det förekommer också att personal på eget bevåg gör motattacker eller klumpiga spårningsförsök. Dessutom är det vanligt att man inte dokumenterar iakttagelser, händelser och åtgärder i tillräcklig utsträckning.

Den typ av incident som tas upp här är IT-intrång i vid mening. Det kan vara manipulation av webbsidor, det kan vara en användare som går utöver sina befogenheter eller det kan vara någon som tar sig in via svagheter i nätverket. Andra typer av incidenter - virusangrepp, stöld av maskinvara, skadehändelser i form av brand eller översvämning, etc. - behandlas inte.

Förberedelser

Förbereder man sig - genom att ta fram riktlinjer för incidenthantering och ha rutiner - har man också möjlighet att bättre klara en situation. Tyvärr saknas det ofta en genomtänkt plan för hantering av IT-relaterade incidenter. När något inträffar får man i panik både försöka lösa problem och skapa metoder för problemlösningen. Om man istället hade tagit fram metoderna under lugnare förhållanden så hade de kanske blivit mer genomtänkta och sannolikt bättre. Utbildning i och övning av dessa metoder är viktiga inslag i föreberedelserna. Behovet av övning inför större incidenter är särskilt uttalat.

En annan fördel med att ha utarbetat och gjort förberedelser är att man också minskar möjligheterna för godtycke, felbedömningar och bristfälligt handlande. Planer och rutiner för olika typer av händelser och genomarbetade scenarion ger stöd för hur man ska hantera den uppkomna situationen. En ytterligare fördel är att framtida händelser av samma typ, eller samma händelser inom en annan del av organisationen, kommer att hanteras på ett likartat sätt.

För att effektivt hantera en allvarligare händelse behövs en insatsgrupp, ett incidenthanteringsteam (CSIRT), med olika kompetenser och befogenheter. Teamet behöver, bland annat:

- kunskap om gällande lagar och förordningar, civilrättsliga avtal samt organisationsspecifika regler och procedurer,
- kunskap om aktuell teknisk plattform, nätarkitektur och andra lokala förhållanden,
- kunskap om berörda applikationer,
- kunskap om säkerhet, särskilt informations- och IT-säkerhet,
- befogenheter att fatta beslut om de åtgärder som krävs.

Teamet kan vara en permanent sammansatt grupp men är, som regel, en dynamisk grupp med en fast kärntrupp där sammansättningen styrs av incidentens mål, typ och omfattning.

Ett CSIRT bör ledas av någon som har tillräckliga befogenheter och resurser att besluta om t.ex. driftstopp, polisanmälningar, eller användning av extra resurser, t.ex. i form av externa experter. Exempel kan vara IT-säkerhetschefen, säkerhetschefen eller någon ur organisationens ledning. Har man etablerat en CSIRC-funktion bör någon från denna stå för den operativa ledningen av incidenthanteringsteamet.

Andra nödvändiga resurser, inom eller i nära anslutning till CSIRT, kan vara:

- juridisk expertis,
- internrevisor,
- informations- och medieansvarig,
- teknisk skribent med huvuduppgift att se till att incidenten blir väl dokumenterad, att alla beslut dokumenteras, etc.

En annan typ av förberedelse är att initiera förebyggande tekniska säkerhetsåtgärder. T.ex. se till att installera programvara som loggar och eventuellt spärrar nätuppkopplingar, exempelvis TCP wrapper[1], eller se till att system- och säkerhetsloggning är aktiverad i tillräcklig utsträckning.

De verktyg som finns för att hjälpa till vid utredningar av ett intrång - såsom TCT, *The Coroners Toolkit*[2], (Unix), IRCR*, Incident Response Collection Report*[3], (Windows NT) eller *Corporate Incident Respons Suite*[4], (Windows) - kräver en del förkunskaper. Det gör att man bör bekanta sig med verktygen i förväg så att man kan använda dem effektivt när de behövs.

[1] ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
[2] http://www.fish.com/tct
[3] http://www.incident-response.org/IRCR.htm
[4] http://www.forensics-intl.com/tools.html

De tio budorden när något inträffar

1. Behåll lugnet, var eftertänksam inför varje handling
2. Analysera och förstå situationen och incidentens omfattning
3. Handla inte på eget bevåg
4. Var försiktig vid efterforskning och kontroll
5. Begränsa och kontrollera informationsspridning
6. För anteckningar och se till att alla viktiga steg och händelser dokumenteras
7. Prioritera arbetet efter vad som sägs i policy och andra kravdokument
8. Använd säkra kommunikationssätt
9. Lokalisera källorna till problemet, inte symptomen, och eliminera dessa
10. Utvärdera, analysera och lär av det inträffade

#1 Behåll lugnet

Behåll lugnet så att du kan tänka logiskt. Oavsett hur många incidenter du har varit med om så kommer du att drabbas av förhöjd adrenalinhalt. Därför är det viktigt att inte fatta några panikbeslut eller vidta panikåtgärder. När någon handlar i en stressad och upphetsad situation sker nästan alltid saker som inte löser grundproblemet och som dessutom kan ställa till med mer skada än nytta.

#2 Analysera och förstå situationen och incidentens omfattning

Det är viktigt att göra en grundlig och omfattande inledande genomgång av vad som inträffat. Det du behöver tänka på är:

- Vad är det som har inträffat?
- När inträffade det?
- Hur inträffade det?
- Var inträffade det?
- Hur omfattande är det? Är det ett eller flera system som har drabbats? Berör incidenten andra organisationer?
- Vad gör vi för att begränsa skadorna?

Är det en ”riktig” incident? Till en början måste man vara säker på det. Det kanske är en systemadministratör som gjort en förändring i systemet men glömt att dokumentera den? Det kanske är ett bakgrundsjobb som löpt amok och gjort fel? Kan det vara en replikering som felaktigt skrivit över data? Kan det vara hårdvaru- eller operativsystemsfel som gör att felaktiga datablock läses upp när man försöker komma åt en webbsida? Har någon via ett programfel förändrat en fil av misstag? Har säkerhetsavdelningen anlitat någon för att i tysthet kontrollera IT-säkerheten?

Vad är det för typ av incident? Är det ett fullständigt intrång där någon är inne i systemet eller exekverar kod i datorn? Är det en tillgänglighetsattack (DoS, Denial of Service)?

Stämmer den första analysen eller larmrapporten? Tänk på att incidenten kanske utvecklar sig till att vara något helt annat än vad man trodde i från

första början. Det som bara föreföll vara okynnigt kladd på webbsidan kan vara något större där någon även avlyssnar nätverket, läser all e-post eller använder systemet som språngbräda för att attackera andra.

#3 Handla inte på eget bevåg

Den som är system- eller nätverksadministratör, eller någon annan som arbetar med det angripna systemet, bör inte agera på eget bevåg. Vad du än gör, vilka åtgärder du än vidtar, kommer du sannolikt att kritiseras i efterhand. Det är bättre att se till att allt arbete är förankrat hos de aktuella verksamhetsansvariga och utförs enligt gällande policy och andra bestämmelser.

Det innebär att du ska informera ansvariga och låta dessa fatta beslut på det underlag du presenterar. Innan de ansvariga kontaktas bör du kontrollera:

- vad säger policyn, planer, instruktioner och rutiner?
- vem/vilka ska informeras?
- vilken information behöver tas fram?
- vad behöver skyddas?

#4 Var försiktig vid efterforskning och kontroll

Se till att inte förvärra det inträffade genom att vid efterforskning och kontroll vidta åtgärder som förvärrar situationen eller förstör information och möjligheter till spårning i systemet. Man kan förvanska information genom att vara oförsiktig i sin efterforskning. Dessutom, om angriparen finner att man är honom på spåren, kan det leda till ”uppstädning” eller att systemet medvetet skadas eller förstörs.

#5 Begränsa och kontrollera informationsspridning

Det är viktigt att rätt information når rätt personer och att man delger information endast då mottagaren behöver denna.

Det kan vara svårt att veta vem som ligger bakom incidenten. Det kan vara någon internt, det kan vara en konsult, det kan vara personal från ett serviceföretag som har tillgång till lokalerna, det kan också vara någon externt eller en kombination av detta. Att sprida information alltför frikostigt kan leda till att den skyldige blir förvarnad.

#6 För anteckningar och se till att alla viktiga steg och händelser dokumenteras

Att noggrant dokumentera alla händelser och åtgärder i kronologisk ordning är A och O i all incidenthantering.

#7 Prioritera arbetet efter vad som sägs i policy och andra kravdokument

Det förenklar arbetet om det på förhand finns en utstakad prioritet på vad som ska hanteras, i vilken ordning och hur det ska göras.

Schablonmässiga prioriteringslistor för incidenter inom IT-området brukar omfatta, i fallande prioritetsordning:

- skydda människoliv och –hälsa,
- skydda natur och miljö,
- skydda hemlig eller känslig information och förhindra spridning,
- skydda annan, företagsintern, information,
- skydda mot skador i systemet och minimera kostnader för incident,
- upprätthålla drift samt system- och nätverkstillgänglighet.

Exempel på andra frågor som kan vara aktuella är:

- Ska Internetanslutningen stängas av?
- Ska en klient frånkopplas från nätet?
- Ska någon server tas ner?
- Ska systemet installeras om?
- Ska nuvarande utrustning temporärt eller permanent bytas mot ersättningsutrustning?

#8 Använd säkra kommunikationssätt

Försök att undvika all form av datorbaserad kommunikation när ett intrång har inträffat. En inkräktare kan lätt söka igenom brevkorgar eller kontrollera om någon diskussion sker om intrång eller säkerhetsfrågor. Lika lätt kan man använda verktyg för att avlyssna e-post, eller annan e-kommunikation, t.ex. IRC (Internet Relay Chat). Att skicka krypterad e-post är inte heller problemfritt. Kan man garantera att den som är inne i systemet inte ersatt kryptoprogramvaran eller lagt in ett program som avlyssnar mitt tangentbord när jag skriver in lösenord eller kryptonycklar (t.ex. via ett trojanprogram av typen Back Orifice)?

Alternativ som används i praktiken är telefon, SMS, fax, internpost eller vanliga brev. Säkrare är givetvis att se till att all kommunikation sker ansikte mot ansikte, via budbärare eller via kurirpost.

#9 Lokalisera och eliminera källorna till problemet, inte symptomen

Det är lätt att ha fel fokus i en akut situation. Har intrånget verkligen gjorts på det sätt som vi tror? Om vi tätar luckan, har vi löst problemet? Finns det säkerhetsbrister kvar i systemet? Har bakdörrar installerats?

Det är viktigt att se till att problemet inte sprider sig, vare sig inom samma dator eller till andra datorer.

#10 Utvärdera, analysera och lär av det inträffade

Det finns mycket lärdom att ta vara på efter en incident. Med rätt återkoppling blir händelsen något som ger erfarenheter och kunskap som kanske kan förhindra framtida incidenter eller gör att man bättre kan hantera dom om de inträffar.

Säkerhetskopian - livlinan

Vid en incident är det viktigt att man tidigare har kontrollerat att de drabbade systemen har en fungerande säkerhetskopiering. Ofta är det först efter en incident som det blir känt om säkerhetskopieringen inte fungerat som den ska. Det kan vara felkonfigurerade program för säkerhetskopiering, fel på bandstationer eller kablar, överskrivning av magnetband av misstag, användning av magnetband som med tiden och efter flitig användning blivit dåliga, eller felaktiga antaganden i planering och körscheman.

Det är relativt vanligt att det inte finns säkerhetskopior av vissa system, t.ex. webb- och e-postservrar i brandväggsområdet. Anledningen är oftast att de anses vara lätta att återställa från distributionsmedia, eller, som i fallet med webbinformation, att det går snabbt att återskapa från publiceringsverktyg eller replikeringsservrar. Dessa antaganden är emellertid många gånger en förenkling av verkligheten. Det finns risk för att man missar en mängd småförändringar som sannolikt gjorts i systemet sedan ursprungsinstallationen, eller information som skapas av systemet själv, t.ex. loggar, temporära filer och konfigurationsfiler.

Säkerhetskopiorna är viktiga av flera anledningar, bl.a.:

- för att kunna återställa systemet,
- för att ha äldre filer att jämföra med när man letar efter modifierade filer,
- för att se vid vilka tidpunkter vissa saker har hänt, t.ex. inloggning, start av programexekvering, eller skapande, modifierande och raderande av filer,
- för att kunna dokumentera och rekonstruera vad som har hänt,
- för att få tillgång till dynamiska data som har skapats av systemet, t.ex. loggar och temporära filer.

Säkerhetskopior utgör värdefullt utredningsmaterial och kan vara viktiga som bevismaterial. Det är därför av stor vikt att de säkerställs på lämpligt sätt; dels för att förhindra överskrivning eller radering av misstag, dels för att förhindra obehörig påverkan.

Ett sätt att underlätta kommande utredningar är att ta särskilda säkerhetskopior på obegagnat datamedia med hjälp av beprövad kriminalteknisk programvara. Se till att dessa kopior märks väl och hålls separerade från ordinarie säkerhetsmedia. Dessa kopior ska tas tidsmässigt så nära incidenten som möjligt och sparas på ett säkert och kontrollerat sätt för att senare kunna användas vid en eventuell intern- eller polisutredning.

Det ställs speciella krav på den programvara som används för säkerhetskopiering enligt ovan. Den ska inte ändra metadata, t.ex. filåtkomst- och ändringstider, på originalsystemet, och den bör även kopiera skräputrymmen, arbetsareor för virtuellt minne, etc. Ett annat krav är att det ska gå att återskapa hela eller delar av systemet på en dator med delvis avvikande maskinvarukonfiguration. Det bästa sättet att få en fullständig säkerhetskopia utan att originaldata förändras är att göra en binär spegelkopiering från skivminne till skivminne.

En viktig sak att tänka på vid en incident är hur länge systemet kan ha varit angripet eller komprometterat. Det kan vara svårt att med säkerhet avgöra hur länge någon annan haft kontroll över systemet, eftersom den information på vilken det går att göra antaganden sannolikt är manipulerad. Finns säkerhetskopior så långt tillbaka att du har tillgång till data och program såsom det såg ut innan angreppet?

Det är också viktigt att gå igenom rutinerna för säkerhetskopiering för att undvika misstag som senare kan bli dyra. Det är bl.a. lätt att glömma att lyfta ut band ur körschemat och därmed löpa risk för överskrivning av misstag.

Simulering och verklighet

Något som man kan ha fördel av är att man känner sitt eget system bättre än den som angripit det. Har ansvarig personal tagit sig tid och lärt sig systemet och applikationerna är det lättare att upptäcka och analysera konstigheter. Många som gör angrepp är individer som saknar djupare kunskap om drift och system (s.k. ”script kiddies”). Dessa följer i regel ett angreppsschema ”mekaniskt” eller använder sig av hel- eller halvautomatiserade verktyg som systematiskt attackerar datorer. Detta gör att de troligen kommer att begå ett eller flera små eller stora misstag, som tex.:

- att de installerar och startar ett program som de döpt till ett programnamn som inte finns i det aktuella operativsystemet eller i den aktuella versionen,
- att de startar program som innehåller argument, eller ordning på argument, som du själv inte använder eller sett någon kollega använda,
- att de använder felaktiga kommandonamn, eller ovanliga kommandosekvenser som du inte känner igen.

Det är lärorikt att testa om planerna verkligen går att följa och att rutinerna fungerar som avsett. Det är inte alltid fallet, varför tester och attacksimuleringar i huvudsak bör genomföras i en laboratorie- eller utvecklingsmiljö för att inte störa produktionsprocesserna. (Vissa tester måste kanske göras också i produktionsmiljön.)

Man kan genom tester och simulerade attacker:

- samöva, skapa samsyn och därmed bli effektivare,
- upptäcka luckor i sina kunskaper,
- upptäcka misstag och felaktig hantering,
- hitta tekniska brister, t.ex. att det saknas reservkomponenter, att säkerhetskopieringen inte fungerar, att applikationer eller system loggar felaktigt eller bristfälligt eller att system slutar fungera i udda situationer,
- identifiera behov av bättre verktyg,
- se om den teoretiska prioriteringen och hanteringen enligt riskanalysen balanserar insatser och kostnader väl.

Denna kunskap kan leda till omprioriteringar, både uppåt och nedåt, eller att man omdefinierar vissa incidenter till kalkylerade risker som inte motiverar några omfattande insatser över huvud taget.

Ett av de första besluten som ska fattas vid ett intrång är om systemen ska fortsätta vara aktiva, om de ska stängas av, eller om de ska ersättas med utbytessystem, alternativt installeras om. Det bör finnas fastställda kriterier och regler för val mellan de olika alternativen i olika situationer.

Om systemen ska hållas aktiva bör man temporärt aktivera utökad kontroll och övervakning, t.ex. extra regler i brandväggar som loggar all trafik, eller program för protokoll- och nätanalys som spelar in viss eller all nättrafik.

Att ha testat, eller åtminstone analyserat, vad som egentligen händer när man stryper hela eller delar av Internetkopplingen är en viktig förberedelse. Åtgärden kan leda till allvarliga bieffekter: intern e-post slutar fungera, datorer hänger sig när de gör namnuppslagningar eftersom de inte kan få kontakt med externa namnservrar, dataöverföringar, som behövs för interna system, skickas inte eller tas inte emot, etc.

Vem kan man lita på?

Vid en incident finns i inledningsskedet ingen vetskap om vem som gjort vad. Är det en extern angripare? Är det en missbelåten anställd som vill ge igen? Är det en kombinerad (extern/intern) attack? Det är därför viktigt att i ett tidigt skede inte sprida alltför mycket information om vad som har hänt eller att i onödan avslöja hur mycket som är känt om det inträffade.

Förutom att det är svårt att veta vilka personer du kan lita på så är det näst intill omöjligt att lita på den information som finns i ett kompromitterat system. Har en inkräktare lyckats skaffa sig administratörsrättigheter, kan i princip vad som helst blivit ändrat:

- Operativsystemet eller dess konfiguration kan ha blivit manipulerat. Det är i vissa fall möjligt att modifiera ett exekverande operativsystem direkt och i flykten utan att man behöver installera filer och program som kan lämna spår.
- Programfiler kan ha blivit modifierade och innehålla bakdörrar, trojanska hästar eller andra mindre trevliga överraskningar.
- Loggar, historikfiler och spårdata kan ha blivit manipulerade.
- Data kan vara förändrade.

Det har länge funnits färdigutvecklade angreppspaket, s.k. ”rootkits”, till olika UNIX-dialekter. De är programpaket som innehåller modifierade systemprogram, t.ex. program för att lista filer och processer, program för att avlyssna login-processen, eller snifferprogram (program för avlyssning av nättrafiken). ”Rootkits” har sedermera blivit ett samlingsnamn för verktygslådor att manipulera operativsystem och systemprogram och finns numera även för t.ex. Windows NT. De ersatta programmen används ibland för att dölja en angripares närvaro; ersättningsprogrammen kan t.ex. skilja

sig från originalen genom att inte visa vissa filer, program, processer eller användare.

Ett system som fått programfiler ersatta kan vara osäkert ur mer än ett perspektiv. Förutom bakdörrar, trojaner och andra oönskade finesser är det inte ovanligt att de nyinstallerade programmen fungerar sämre än de ersatta. Orsaker till det kan vara att de är skapade ifrån källkod från en äldre version av systemet, att de är byggda av egenutvecklad och otillräckligt testad källkod, att de inte inkluderar senare installerade uppdateringar, etc. Detta kan leda till att driftssäkerheten i vissa avseenden blir sämre.

Personer som gör intrång har varierande syften och skiftande kunskaper om systemet i fråga. Det kan leda till att systemet drabbas av driftsstörningar på grund av angriparens misstag eller illvilja. Det har hänt att angripare raderat filer, eller på annat sätt förstört ett system, antingen för att dölja spår eller för att sabotera.

Kommunikation och kontakter

Det finns många fördelar med att peka ut enstaka kontaktpersoner inom incidentteamet och låta dessa sköta alla kontakter med omgivningen. Det man vinner är bl.a. kontroll över vilken information som lämnas ut och till vilka.

Innan kontakter med rättsväsendet eller andra externa parter sker bör man vara säker på att berörda verksamhetsansvariga är informerade och har givit klartecken. Det kan exempelvis vara viktigt att informations- och presskontakterna är tränade så att de kan hantera media professionellt. Det är inte sällan som polisanmälningar leder till att press och media får kännedom om det inträffade. Det är också viktigt att information som lämnas ut, t.ex. i en polisanmälan, hålls så kort och allmän som möjligt. Det är alltid möjligt att komplettera med mer material i efterhand.

En primär uppgift för kontaktpersonen är att se till att användarstöd och kundkontakter har klara budskap till användarna.

Tänkbara externa kontakter är bl.a.:

- incidenthanteringsorganisationer, t.ex. CERT/CC och dess svenska motsvarighet,
- organisationer varifrån attackerna kommer,
- organisationer dit spåren leder (t.ex. om man hittar adresser eller domännamn i loggfiler och programkod),
- andra som blivit drabbade,
- tele- och nätverksleverantörer.

Vid dessa kontakter måste det vara klart vilken information som kan lämnas ut. Det kan t.ex. vara känsligt att berätta om vilka andra som blivit drabbade eller beskriva i detalj hur den egna organisationen blivit angripen.

Om andra har blivit drabbade anses det som god sed och bra grannsämja i Internetvärlden att kontakta dem direkt. Inom vissa organisationer eller i samband med vissa typer av incidenter kan detta dock vara svårt eller till och med strida mot gällande regler.

Någon gång under det inträffade kan det bli nödvändigt att gå ut med information till en större krets, t.ex. de datoransvariga inom företaget eller alla anställda.

Vid all kommunikation gäller det att beakta hur informationen kan tolkas resp. misstolkas samt brukas i ett senare skede. Olämplig information kan eventuellt vändas mot organisationen i ett senare skede då man genomför en rättslig process mot den eller de som har gjort intrånget.

De flesta tele- och nätverksoperatörer har en e-kontaktfunktion (abuse-funktion) för säkerhetsfrågor. Det är dock klokt att vid en första kontakt endast be om telefonnummer och namn så att man kan etablera en personlig kontakt. För samarbete kräver operatörerna i vissa fall att man gjort en polisanmälan, och vissa aktiviteter, t.ex. spårningar och liknande efterforskningar, utförs normalt endast av polisen.

Spårning och efterforskning

Iakttag försiktighet vid spårningsförsök. Dels är det lätt att förstöra viktig information om incidenten dels kan du röja att intrånget har upptäckts. Framförallt, gör inget som kan leda till motanklagelser. Tänk efter, både en och två gånger, innan du inleder en direkt, aktiv kommunikation med den misstänkta källan t.ex. via:

- ping och traceroute,
- portscanning,
- nättjänster som finger, smtp och telnet.

Om man trots allt bestämmer sig för att göra någon form av efterforskningar, bör det göras från en dator eller nätkomponent som inte kan kopplas ihop med de attackerade systemen.

Det är fullt möjligt att attackerna kommer från ett system som i sin tur är angripet. De egna efterforskningarna kan i värsta fall leda till att systemansvariga, som inte upptäckt den tidigare attacken, upptäcker försöken till spårning. I det fallet kan man själv bli anklagad för intrångsförsök eller, i värsta fall, även för det aktuella intrånget.

Tänk på att även neutrala aktiviteter som förefaller harmlösa, t.ex. uppslagningar av domännamn eller IP-adresser, kan leda till loggar eller larm. Angriparen eller angriparna kan då inse att någon har börjat söka efter dem.

Ett oförsiktigt beteende kan dessutom förstöra information om incidenten. I sällsynta fall är attackerade system försåtsminerade så att kvarlämnade inkräktarverktyg raderar viss eller all information vid exempelvis ett spår-

ningsförsök. Om driften av systemet fortsätter kommer det att påverka en del lagrad information med potentiellt bevisvärde, t.ex. kan loggfiler tömmas på äldre innehåll, temporära filer kan raderas, slaskområden kan överskrivas och data- och programfiler kan få ändrade åtkomst- eller modifieringsdatum. En ytterligare riskfaktor vid fortsatt drift är att angriparen ges tillfälle att radera eller ändra i graverande filer, t.ex. intrångsverktyg eller loggfiler.

Vid allvarligare incidenter bör man därför ”konservera originalsystemet” genom att skapa binära spegelkopior av sekundärminnen. Har man möjlighet ska man också spara originalskivminnen och fortsätta driften med ersättningsenheter. Den efterföljande tekniska analysen ska utföras på fristående utrustning och, om så är möjligt, med hjälp av kriminalteknisk programvara.

Det är viktigt att den programvara som används vid analysen är beprövad och att de som använder den är välbekanta med den; bevisvärdet av analysen kan lätt ifrågasättas annars.

En viktig del av den tekniska utredningen är att identifiera avvikande eller osannolika händelser, alternativt kända angreppsmönster. Några exempel på händelser att leta efter är:

- osannolika inloggningar, till exempel på tider som är ovanliga för en viss användare,
- uppseendeväckande åtkomst- eller ändringstider på filer,
- förekomst av okända filer, program och processer,
- förekomst av nya användare, grupper eller roller,
- orimliga förändringar i behörighet och rättigheter,
- frånvaron av information, beroende på att någon städat undan spåren efter sig. Ett exempel kan vara att det saknas loggar från en hel dag; inkräktaren kan vid städningen ha kopierat tillbaka en äldre loggfil från tiden före intrånget skedde.

Tid är ofta en viktig aspekt när man gör efterforskningar och spårning. Ju snabbare man startar utredningen desto större är utsikterna till framgång. Tid är också av betydelse när det gäller kontakter med nätoperatörer; en del av dessa håller logg och spårdata tillgängliga endast under en begränsad tid.

En effektiv förebyggande säkerhetsmekanism för identifiering av obehöriga ändringar i filsystemet är kryptografisk kontrollsummering. Genom att jämföra en nyberäknad kontrollsumma med en lagrad går det att enkelt se om en fil har blivit modifierad. Här är det viktigt att använda algoritmer som ger en kryptografiskt stark kontrollsumma.

Dokumentera

Om det inte finns dokumenterat har det aldrig hänt sägs det. För att undvika missar i kommunikationen och för att få underlag i det akuta, men även framtida, arbetet bör man dokumentera alla händelser och allt runtomkring.

Dokumentera bl.a. alla kostnader som har uppstått i samband med en incident. För att senare kunna driva ett skadeståndsmål måste man kunna påvisa de extra kostnader som uppstått i samband med incidenten.

Det är viktigt att dokumentationen förvaras säkert och hanteras på ett sätt som gör att information inte kan läcka ut eller förvanskas. Spara ingen information om incidenten i elektronisk form på nätverksanslutna datorer eller i ett format som är ovanligt eller svårt att hantera.

Dokumentera extra noggrant all kommunikation med externa parter, t.ex. polis, åklagare, säkerhetsorganisationer. Se till att dokumenten innehåller tid och datum, vem man talade med samt anteckningar om samtalet.

Viktigare beslut bör tas i protokollförda möten så att det inte råder några tvivel om vad som har bestämts.

För att kunna driva en process mot den som gjort intrånget krävs det bra bakgrundsmaterial. Datera, numrera och signera viktiga dokument. Som en extra försiktighetsåtgärd kan man be någon att vidimera att datum och signatur stämmer.

Av stor vikt är att den s.k. beviskedjan (chain of custody), dvs. förvaltning av att kedjan för allt som ska användas som bevis är obruten och tillförlitlig. Detta gäller oavsett om bevisen ska användas i brottmål, civilmål eller internt i organisationen.

Analys och återkoppling

Genom att utvärdera situationen, analysera vad som har inträffat och hur man hanterade situationen går det att lära sig av incidenten och förbättra skyddet inför framtida händelser. Exempel på frågor man bör ställa är:

- Har vi vidtagit rätt åtgärder?
- Hade vi tillräckliga resurser, rätt kompetens, bra kommunikation inom gruppen, etc.?
- Är problemet eliminerat eller går det att fortsätta att missbruka systemet på samma eller liknande sätt?
- Finns motsvarande säkerhetsbrister i några andra av våra system?
- Vilka direkta kostnader är orsakade av incidenten?
- Vilka kostnader uppstod i samband med incidenthanteringen?
- Går det att i liknande fall få en lägre kostnad genom att införa bättre förebyggande säkerhetsåtgärder?
- Vad går att göra bättre, effektivare, etc.?

Erfarenheterna från händelsen bör analyseras för att se om de kan leda till att rutiner och planer uppdateras, omprioriteringar sker, nya rutiner utarbetas, etc.

För att organisationen och medarbetarna ska ta lärdom av det inträffade bör information om incidenten spridas, t.ex. i en avidentifierad och allmänt hållen form och som internutbildning.

Sammanfattning

Frågan är inte om, utan när och hur ofta någon IT-relaterad incident inträffar i en organisation. Ju bättre förberedd man är, desto bättre går det att hantera situationen. Planering, dokumenterade rutiner, programverktyg, stöd för beslut, utbildning och inte minst övning minskar misstag och godtycke.

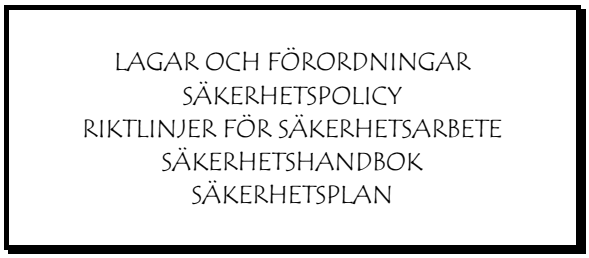
Stor försiktighet måste iakttas vid spårning och efterforskning då det är lätt att röja att intrånget upptäckts eller att förstöra eller förändra värdefull information av misstag.

Dokumentera incidenten, och den efterföljande analysen, så att händelser och beslut går att följa. Dokumentationen bör innehålla material som kan användas dels för internutredning och återkoppling, dels som bevisunderlag vid en rättegång eller i ett civilmål. Se till att hantera all information på ett restriktivt och säkert sätt.

Erfarenheterna ifrån säkerhetsincidenter bör tas om hand så att framtida säkerhetsproblem och incidenter av liknande slag kan elimineras eller hanteras på ett effektivt sätt.

2 Styrande regelverk

Säkerhetsarbetets uppläggning och struktur varierar från organisation till organisation; likaså sättet att beskriva säkerhetssystemet, säkerhetsreglerna, etc. I denna rapport har vi valt att arbeta med strukturen nedan.



Lagar och förordningar

Det är en mångfald av lagar och förordningar som reglerar eller påverkar agerandet vid incidenthantering. Vissa av dessa har allmän giltighet, vissa är generella men verksamhetsspecifika och vissa ska tillämpas enbart under speciella omständigheter. Bland de viktigaste lagarna, förutom relevanta delar av brottsbalken, kan nämnas:

- tryckfrihetsförordningen, yttrandefrihetsgrundlagen
- sekretesslagen
- säkerhetsskyddslagen
- säkerhetsskyddsförordningen
- personuppgiftslagen
- patientjournallagen
- lagen om skydd för företagshemligheter
- bokföringslagen
- bokföringsförordningen
- förvaltningslagen
- arkivlagen
- upphovsrättslagen
- patentlagen
- arbetsmiljölagen
- lagen om medbestämmande
- arbetstvistlagen
- lagen om anställningsskydd

Säkerhetspolicy

Varje organisation ska ha en säkerhetspolicy som uttrycker ledningens åsikt och vilja om hur säkerhetsarbetet ska bedrivas inom organisationen. Som regel är policyn av övergripande natur och riktar sig mot organisationen som helhet.

IT-säkerhetspolicyn är en del av säkerhetspolicyn och redovisar vad som gäller inom organisationen avseende IT-säkerhet; vad som betraktas som

tillgång, vilka hot som anses vara av särskild betydelse och hur tillgångar ska skyddas i princip.

Riktlinjer för säkerhetsarbete

Säkerhetspolicyn måste förfinas och detaljeras för att kunna tillämpas i det praktiska arbetet. Detta kan göras i form av riktlinjer, normer, föreskrifter, anvisningar, instruktioner eller arbetsrutiner beroende på syfte och abstraktionsnivå.

På samma sätt som säkerhetspolicyn är ett styrverktyg för organisationens ledning, är riktlinjerna för säkerhetsarbetet ett verktyg för säkerhetsledningen att övergripande styra säkerhetsarbetet.

Säkerhetshandbok

Säkerhetshandboken beskriver säkerhetssystemet och dess användning, dvs. hur policyn och riktlinjerna för säkerhetsarbetet tillämpas på olika organisatoriska och tekniska nivåer. Den reglerar krav och restriktioner på behörighetsadministration och -kontroll, accesskontroll, konfigurering av brandväggar och routrar, konfigurering av intrångsdetekteringssystem, incidenthantering, etc.

Säkerhetshandboken reglerar även CSIRC-verksamheten, dvs. incidenthantering, internutredningar, rutiner för polisanmälan, m.m. Det finns många olika typer av IT-incidenter och konsekvenserna av en incident kan variera från betydelselös kuriosa till ekonomisk kris eller organisatorisk katastrof. Hur incidenter ska hanteras bör framgå i detalj: Vilka typer av händelser ska rapporteras som IT-incidenter, vilka slag av åtgärder ska vidtas, vilka regler gäller för internutredningar, hur ska polisanmälan ske, etc.?

Även om termen ”säkerhetshandbok” associerar till ett enda dokument så bör det snarare uppfattas som ett samlingsnamn för en uppsättning säkerhetsrelaterade handböcker. Det är t.ex. lämpligt att ha skilda handböcker för systemanvändare, systemadministratörer och annan driftspersonal, IT-säkerhetsansvariga, etc. I fallet CSIRC är två skilda handböcker att föredra - en för ledning, organisation och administration av funktionen och en för teknisk handläggning.

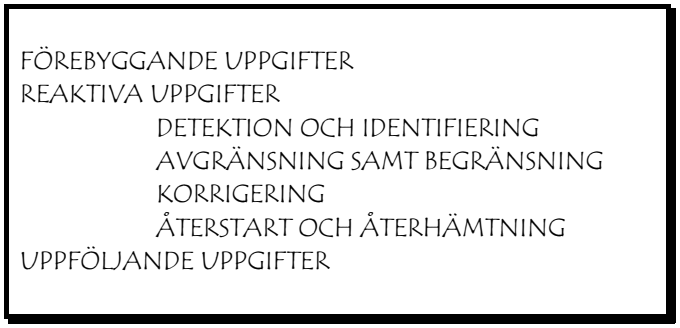
Säkerhetsplan

De flesta verksamheter bedrivs i en dynamisk och föränderlig omgivning där det krävs en kontinuerlig anpassning till nya krav och möjligheter. Detta påverkar såväl säkerhetssystemet som säkerhetsarbetet. Säkerhetspolicyn och säkerhetshandboken är därför levande dokument i ständig förändring och utveckling.

Införandet av nya eller anpassning av befintliga säkerhetsmekanismer kräver både resurser och planering. Säkerhetsplanen dokumenterar hur detta förändringsarbete är tänkt att bedrivas.

3 Arbetsmodell för incidenthantering

Arbetsmodellen är indelad i tre faser: förebyggande, reaktiv och uppföljande. Den förebyggande fasen omfattar incidenthanteringen i sin helhet medan de reaktiva och uppföljande faserna är mera orienterade mot hantering av enskilda incidenter. De förebyggande och uppföljande faserna är starkt relaterade till det löpande IT-säkerhetsarbetet medan den reaktiva fasen genomförs normalt av en, för ändamålet rätt bemannad, insatsgrupp CSIRT.



Fas 1 Förebyggande uppgifter

Att fatta rationella beslut i en krissituation är svårt om man inte är väl förberedd och tränad. Genom att i förväg etablera riktlinjer, handlingsplaner, samarbetsformer, kommunikationskanaler, etc. samt utforma och öva kritiska rutiner under realistiska former kan man undvika kostsamma misstag. Exempel på generellt tillämpliga, förebyggande aktiviteter är:

- utgående från verksamheten precisera ett legalt ramverk med hänsyn till verksamhetens art och med beaktande av de anställdas personliga integritet,
- utveckla ledningens och organisationens förtroende och stöd för incidenthantering,
- definiera och implementera klara regler för incidenthantering, inkl. ansvarsfördelning och samarbetsformer,
- implementera och driva en fullständig jourtjänst (Call Center) för handläggning av IT-incidenter,
- organisera information om incidenter i en databas och implementera och driva ett tekniskt stödsystem för hantering av denna,
- följa upp tillämpningen av regler och procedurer för incidenthantering kontinuerligt och anpassa dessa efter behov,
- implementera och driva ett tekniskt stödsystem - inkl. alternativa möjligheter vid störningar i ordinarie kommunikationskanaler - för snabb och säker kommunikation med avnämarna,
- medverka aktivt i utformning av kommunikationsplaner för intern och extern kommunikation vid allvarligare incidenter,

- införa ett varningssystem för systemanvändare, t.ex. genom varnings-flaggor och varningstexter i inloggningsprocedurer
- medverka aktivt i utformning och implementering av förebyggande (proaktiva) säkerhetsmekanismer av typ behörighets- och accesskontroll, brandväggar/filter, spårningsmekanismer, säkerhetsloggning, intrångs-detektering, viruskontroll, säkerhetskopiering, reservsystem, återstart, etc.,
- följa upp system- och säkerhetsloggar rutinmässigt,
- genomföra regelbundna sårbarhetsanalyser, säkerhetstester och angreppssimuleringar,
- aktivt och kontinuerligt söka och använda relevant information om säkerhetsluckor, korrigerande kod, illvilliga program, hackerverktyg, etc.,
- aktivt och kontinuerligt informera berörda organisationsenheter inom ansvarsområdet om relevanta säkerhetshändelser.

Fas 2 Reaktiva uppgifter

Reaktiva uppgifter avser aktiviteter som utförs när och omedelbart efter det att en incident inträffat. De omfattar bl.a. åtgärder för:

- detektion och identifiering av incidenter,
- avgränsning av incidenter samt begränsning av deras skadeverkan,
- korrigering,
- återstart och återhämtning.

Som gyllene regel gäller att:

ALLA ÅTGÄRDER I SAMBAND MED EN IT-INCIDENT
SKA UTGÅ IFRÅN ATT
INCIDENTEN SKA POLISANMÄLAS

innan beslut om motsatsen har fattats.

Självfallet polisanmäls inte alla incidenter, en incident kan ju visa sig vara av mindre allvarlig art och inte föranleda några kraftigare åtgärder. Men grundregeln är att man inte bör vidta åtgärder som kan komma att påverka en eventuell polisutredning i negativ riktning, t.ex. genom att påverka data-media, applikationsdata eller loggfiler på ett sådant sätt att deras bevisvärde reduceras.

De detaljerade operativa åtgärderna är i regel beroende av verksamhetens art och den underliggande tekniska plattformen. Det är dock möjligt att identi-fiera några generellt tillämpliga aktiviteter på en övergripande nivå.

Detektion och identifiering

- Analysera och dokumentera händelsen.
- Besluta om händelsen ska betraktas som en incident.
- Utse ansvarig person att hantera incidenten.
- Meddela berörda ansvariga i linjeorganisationen.
- Kontakta berörda externa organisationer.

Avgränsning

- Organisera lämplig insatsgrupp (CSIRT).
- Ta bevis- och utredningskopior.
- Ta återstartkopior.
- Analysera loggfiler, IDS-rapporter (IntrångsDetekteringsSystem) och annan relevant information.
- Besluta om internutredning och/eller polisanmälan och eventuella restriktioner på det fortsatta arbetet på grund av det.
- Besluta om (partiellt) driftstopp eller fortsatt (partiell) drift och eventuella speciella åtgärder i samband med detta.
- Informera berörda systemansvariga.

Korrigering

- Fastställa orsakerna till incidenten.
- Eliminera orsakerna till incidenten.
- Fastställa eventuella andra åtgärder.
- Fastställa (i tillämpliga fall) när och hur säker återstart ska ske.

Återstart och återhämtning

- Återstarta systemet (i tillämpliga fall).
- Validera återstarten.
- Preparera beslutsunderlag för återhämtning.
- Övervaka systemdrift under en lämplig tidsperiod.

Fas 3 Uppföljande uppgifter

Analysera och fastställa behovet av eventuella följdaktiviteter av typen systemändringar, internutredning, polisanmälan, externa kontakter, etc.

Analys och återkoppling

- Analysera behovet av ändringar till driftsmiljön.
- Analysera behovet av ändringar i säkerhetsarbetet.
- Föreslå eventuella följdprojekt.

Internutredning

- Genomför internutredning.
- Preparera beslutsunderlag till verksamhetsansvariga inkl. förslag till lämpliga åtgärder.

Polisanmälan

- Preparera och genomför polisanmälan.
- Medverka i polisutredning.

4 Ledning, organisation, administration

Detta avsnitt behandlar motiv och mål, ansvarsområde, organisation, administration, personal, utrustning, etc.

Motiv

- Den ökade tillämpningen av distribuerad informationsteknik för verksamhetskritiska system, tillsammans med en högre grad av systemsamverkan, har medfört att vi har blivit mera sårbara för såväl interna som externa angrepp samt interna missbruk och felgrepp.

- Bättre, billigare och snabbare hantering av inträffade incidenter är ekonomiskt fördelaktigt och har en hög ”good will”-effekt.

Mål

- Koordinera snabb och adekvat respons på IT-incidenter.
- Utforma ett välstrukturerat och väldokumenterat incidenthanteringssystem.
- Inför regler och procedurer för hantering av IT-incidenter hos berörda enheter/funktioner.
- Förbättra de förebyggande säkerhetsåtgärderna på berörda enheter/funktioner genom effektiv omvärldsbevakning och trendanalyser.
- Följa den tekniska utvecklingen och lansera förebyggande åtgärder i god tid .
- Ge stöd åt enheterna/funktionerna i användning av modern säkerhetsteknik och ”state-of-the-art”-säkerhetsprodukter.
- Öka medvetenheten av säkerhetsrisker och deras potentiellt negativa effekter, bl.a. genom att sprida aktuell säkerhetsinformation till berörda enheter/funktioner.
- Öka IT-säkerheten i allmänhet och nätverkssäkerheten i synnerhet, speciellt säkerheten i s.k. extranät.
- Öka organisationens säkerhetskompetens bl.a. genom att utbilda systemadministratörer, systemanvändare, etc. i modern säkerhetsteknik.
- Öka den allmänna IT-säkerheten genom att aktivt medverka i relevanta externa samarbetsprojekt och i det nationella/internationella samarbetet mellan olika CSIRC-organisationer.

Ansvarsområde

Det är nödvändigt att ansvarsområdet för CSIRC är strikt definierat organisatoriskt, beslutsmässigt och tekniskt. Ledningen för CSIRC måste t.ex. veta:

- vilka organisatoriska enheter/funktioner CSIRC ska betjäna,
- hur enheterna/funktionerna är lokaliserade geografiskt,
- vilken teknisk plattform (maskin- och programvaror) dessa enheter/funktioner använder,
- vem som fattar beslut i relevanta frågor samt hur dessa beslut fattas.

Beroende på de aktuella förhållandena måste det bl.a. slås fast:

- vilka skyldigheter/rättigheter CSIRC och resp. organisatorisk enhet/funktion har,
- vilken beslutsordning som gäller vid IT-incidenter,
- vilka tjänster ska tillhandahållas av CSIRC och i vilken utsträckning,
- hur olika geografiska regioner ska betjänas,
- hur samarbetet med aktuella ISP (Internet-operatörer) ska ske.

Organisation

Arbetet i en CSIRC kan indelas i olika typer av arbetsuppgifter:

- ledning av CSIRC,
- ledning och koordination av tillsatta CSIRT,
- tekniska utredningar,
- tekniskt och administrativt stöd.

Funktionen bör ha en platt organisation med klart definierat ansvar och befogenheter för de olika roller (CSIRT-ledare, teknisk expert, etc.) medarbetarna kan tilldelas i olika situationer.

Personalresurser

Den är önskvärt att antalet personer i CSIRC som organisatorisk enhet hålls nere. CSIRC ska bemannas så att de förebyggande och uppföljande uppgifterna samt ledning av reaktiva uppgifter kan genomföras med egen personal; flertalet medlemmar av en insatsgrupp CSIRT ska hämtas från andra organisatoriska enheter. Storleken på en CSIRT är beroende av den aktuella incidentens typ och omfattning och teammedlemmarnas speciella kompetens.

Alla organisationer oavsett storlek har behov av en organiserad CSIRC. I mindre organisationer kan denna funktion i vissa fall hanteras på deltid, t.ex. av den säkerhetsansvarige. Organisationer av medelstorlek, större organisationer och organisationer med särskilt känsliga eller kritiska IT-system har ofta behov av ett eller flera IT-säkerhetsspecialister med god kunskap om incidenthantering och internutredning.

Några saker att tänka på vid bemanning:

- CSIRC bör tillhandahålla fullständig jourberedskap,
- snabb och adekvat reaktion vid svårare incidenter är ett krav även om dessa inträffar under tillfälliga toppbelastningar,
- incidenthantering eventuellt med efterföljande internutredning och/eller polisanmälan kräver säkerhetskontroll av och sekretessavtal med inblandad personal; inte minst med hänsyn till den personliga integriteten.

Administrativa processer

Exempel på administrativa processer inom CSIRC som bör regleras i säkerhetshandboken är:

- utformning av formalia (rapportutseende, kontaktinformation, etc.),
- administration av incidenter (inrapportering, bekräftelse, klassning, lagring och utsökning, avrapportering, etc.),
- genomförande av aktiv säkerhetskontroll (sårbarhetsanalys, intrångsförsök, etc.),
- utfärdande av råd och anvisningar,
- hantering av känsliga, t.ex. icke autenticerade, kontakter,
- informationsspridning,
- formellt samarbete med externa organisationer,
- drift och förvaltning av säkerhetslaboratorium,
- genomförande av distansinsatser.

Kompetens och kompetensutveckling

Personalen i en CSIRC (liksom flertalet medlemmar i en CSIRT) bör besitta goda kunskaper om IT i allmänhet och det aktuella ansvarsområdet i synnerhet. Kunskaperna om det aktuella ansvarsområdet ska omfatta kunskaper om teknisk plattform, kommunikationsarkitektur och tillämpning. (Se Bilaga 4 för en mer detaljerad beskrivning.)

Kompetensutveckling kan bl.a. ske genom:

- rapporter från CERT/CC, FIRST, etc.,
- böcker, tidskrifter, konferensuppsatser, forskningsrapporter,
- WWW, FTP, USENET nyhetsgrupper, e-postlistor,
- deltagande i kurser, konferenser,
- samarbete med andra CSIRC, CERT, etc.

För att bibehålla hög teknisk kompetens är det nödvändigt att berörd teknisk expertis arbetar med närliggande frågor i sin dagliga gärning (system- och nätadministration, intrångsdetektering, etc.).

Utrustning

Exempel på grundutrustning är:

- utrustning för fullständig jour (Call Center),
- datorbaserat incidentrapporteringssystem,
- telefoner, mobiltelefoner, personsökare,
- (säker) fax och datorfax,
- laboratorium för test av t.ex. nya säkerhetsprodukter, nya programvaror, föreslagna systemändringar, alternativa skydd mot existerande hot, etc.,
- webbplats för intern och extern information,
- kryptering, digital signering, stark autenticering av CIRT-medlemmar (speciellt när arbetet bedrivs på distans),
- bärbara datorer,
- programvaror för aktiv kontroll, t.ex. för sårbarhetsanalys, teknisk riskanalys, ”Read Team”-verksamhet, etc.,
- program- och maskinvaror för teknisk utredning av incidenter (Computer Forensics Software),
- dokumentförstörare, datamediaförstörare,
- brand- och stöldsäkra datamediaskåp, kassaskåp, m.m.

Kommunikation

Interna kontakter

Aktuella kontaktlistor för olika typer av incidenter och för alla avnämare inom ansvarsområdet måste upprättas, innehållande:

- organisation
- ansvarig person
- adress
- telefon (direkt)
- telefon (mobil)
- fax
- e-post
- alternativ kontakt

Externa kontakter

Aktuell kontaktinformation med relevanta uppgifter (WWW-adress, kontaktperson, e-post, e-postlista, diskussionsgrupp, etc.) för externa organisationer, t.ex.:

- polisen (närpolisen, länspolisen, Rikskriminalens 24/7 Service, Säkerhetspolisen)
- CERT/CIAC
  - *FIRST (Forum of Incident Response & Security Teams)*
  - *CERT/CC (CERT Coordination Center)*
  - *SwedCERT (arbetsnamn på den av PTS föreslagna särskilda funktionen för incidenthantering)*
  - *Försvarsmaktens CERT*
  - *CERT hos aktuella ISP:er*
  - *branschspecifika CERT*
- leverantörer
- universitet, högskolor, forskningsinstitut
- olika former av e-postlistor för incidenter

5 Typiska aktiviteter

Avsnittet avser att exemplifiera och detaljera några typiska arbetsuppgifter för ett CSIRC eller CSIRT.

Omvärldsbevakning

En CSIRC ska bevaka säkerhetsområdet i allmänhet och vad som är relevant för de aktuella tekniska plattformarna i synnerhet. Omvärldsbevakningen omfattar:

- *insamling* av relevant information,
- *analys* av insamlad information,
- *delgivning* av analysresultat.

Informationsinsamlingen bör förutom rapporterade säkerhetsproblem och eventuella korrigeringar till dessa samt nya produktversioner och temporära system också omfatta ändringar (patchar), nya angreppsmetoder, nya hackerverktyg, nya program som kan användas för fientliga ändamål (virus, mask, ”rootkit”, etc.), nya säkerhetsprodukter och ny säkerhetsteknik.

Analysen ska identifiera behov av såväl omedelbara åtgärder och åtgärder på kort sikt som mer strategiska och långsiktiga åtgärder. Resultatet ska delges samtliga intressenter i organisationen.

En av dom viktigaste intressenterna är organisationens IT-funktion, speciellt den del av IT-funktionen som ansvarar för teknisk IT-säkerhet. När det gäller omvärldsbevakning har IT-funktionen och CSIRC delvis överlappande intressen och bör samordnas.

Larm- och informationscentral

Funktionen bör inkludera en larm- och informationscentral (Call Center) med fullständig jour. Exempel på arbetsuppgifter för Call Center är:

- ta emot rapporter om misstänkta incidenter,
- registrera händelser i en databas över incidenter,
- administrera och underhålla databasen över incidenter,
- besvara och registrera övriga inkommande telefonsamtal, fax, e-post,
- larma ansvariga befattningshavare inom CSIRC,
- sprida behovsstyrd information,
- distribuera periodisk information.

Call Center behöver inte vara bemannad under hela jourtiden. Inrapportering bör dock vara möjlig kontinuerligt (t.ex. genom e-post) och en effektiv larmfunktion för akuta händelser måste finnas.

En kostnadseffektiv praktisk lösning är att Call Center ingår som en integrerad del av IT-driftens hjälpfunktion. Allt löpande arbete sköts då inom

hjälpfunktionen som ska ha klara regler för när och hur CSIRC skall larmas i olika situationer.

För vissa, speciellt för mindre, organisationer kan en tredjepartslösning (outsourcing) av larm- och informationscentral vara ett lämpligt alternativ.

Tekniska analyser

Verksamheten i en CSIRC förutsätter kunskap och resurser dels om olika typer av incidenter och deras handläggning, dels om förebyggande åtgärder i form av aktiv säkerhetskontroll. Exempel på incidenttyper är:

- illvilliga program som virus, maskar eller trojaner,
- angrepp som intrång, DoS (Denial of Service), DDoS (DistributedDenial of Service) eller ”logisk” skadegörelse, t.ex. i form av radering av filer,
- obehörig användning av IT-resurser,
- olovlig kopiering av programvaror.

Exempel på aktiv säkerhetskontroll är:

- sårbarhetsanalyser med hjälp av externa eller interna analysverktyg (security scanners),
- intrångsförsök (”Red Team”-attacker),
- interna angrepp, t.ex. för att erhålla administratörsbehörighet.

Förutom metoder och modeller för teknisk hantering av incidenter och aktiv säkerhetskontroll krävs också tillgång till lämpliga verktyg för korrekta och effektiva tekniska analyser. Exempel på sådana verktyg är maskin- och programvaror för:

- binär spegelkopiering,
- filterprogram,
- fysisk editering av skivminnen,
- omvänd kompilering (reverse engineering),
- källkodsanalys,
- logganalys,
- selektiv systemövervakning,
- superloggning (riktad övervakning av enskilda användare),
- angrepp, t.ex. intrångsförsök,
- sårbarhets- och teknisk riskanalys,
- distansåtgärder (off-site operationer).

Användning av dessa verktyg förutsätter god kännedom om den aktuella tekniska plattformen (operativsystem, filhanteringssystem, kommunikationsprotokoll etc.) förutom om verktygen själva.

Avrapportering av den tekniska analysen kan ske på ett flertal sätt:

- information, t.ex. om konstaterade sårbarheter eller säkerhetsbrister,
- varningar, t.ex. om nya virus eller trojaner,
- problemlösning på berörda driftsställen,
- distribution av temporära systemändringar (patchar).

Internutredning

Internutredning ska genomföras vid misstanke om brott eller regelbrott efter beslut av ansvariga befattningshavare. Beslutet sker lämpligen i en säkerhetskommitté bestående av representanter för ledning, verksamhets- och säkerhetsansvariga. Det är viktigt att man i detta arbete har tillgång till kvalificerad juridisk vägledning avseende vad som får och inte för göras. Arbetet i säkerhetskommittén ska kunna bedrivas under slutna former.

Syftet med en internutredning är:

- att få ersättning för det ekonomiska eller annan skada brottet har medfört,
- att förhindra att brottet återupprepas,
- att så långt det är möjligt försöka slå fast vem eller vilka som kan misstänkas för brottet,
- att undanröja obefogade misstankar,
- att avskräcka andra från brottsliga gärningar.

Eftersom resultatet av en internutredning kan leda till ett brottmål eller civilmål är det viktigt att den genomförs på ett sätt som inte äventyrar bevisföringen i dessa sammanhang. Tillförlitliga, korrekta och väl underbyggda argument är för övrigt en fördel även om utredningen ”endast” resulterar i disciplinära åtgärder, ekonomiska eller andra uppgörelser. Internutredningen ska helt eller delvis besvara frågorna:

- Vad hände?
- Hur stor är skadans omfattning?
- Är det ett brott enligt brottsbalken, och i så fall enligt vilket lagrum?
- Är det ett avtalsbrott?
- Är det ett regelbrott, dvs. ett brott mot det interna regelverket?
- När utfördes det?
- Var utfördes det?
- Hur utfördes det?
- Vem utförde det?
- Varför utfördes det?

Utredningsarbetet ska bedrivas under sekretess. Detta dels av effektivitetsskäl, dels av sociala skäl. Dessutom är det ett brott enligt brottsbalken att utpeka någon som brottslig eller klandervärd eller på annat sätt utsätta någon för andras missaktning.

Bevisföringen i samband med IT-relaterade brott kan vara tekniskt krävande och förutsätter normalt särskilda hjälpmedel. Även den mest noggranna undersökningen av en brottsplats blir utan bevisvärde om man inte på ett övertygande sätt kan visa att bevisen har förvarats på ett sätt som garanterar att ingen (varken behörig eller obehörig) har kunnat manipulera dem (chain-of-custody), från att de har samlats in till dess de är framlagda i domstol.

Polisanmälan

Huvudregeln är att polisanmälan ska göras till närmaste polismyndighet, normalt närpolisen. Det är av stor vikt att det finns etablerade kommunikationskanaler mellan CSIRC och den aktuella polismyndigheten eftersom närpolisen inte alltid har den kunskap och de resurser som fordras för att hantera IT-relaterade brott. Inom många polismyndigheter finns dock specialutbildade poliser som kan kontaktas och länspolismyndigheterna hjälper gärna till med att ge råd samt att etablera lämpliga samarbetsformer.

Innan polisanmälan sker ska man:

- utse en ansvarig kontaktperson,
- sammanställa uppgifter om det drabbade systemet,
- dokumentera hur incidenten upptäcktes,
- dokumentera tillvaratagna föremål och deras handhavande efter tillvaratagandet,
- dokumentera systemtekniska bevis (säkerhetskopior, loggar, etc.) och deras handhavande efter incidenten,
- sammanställa dokumentation om vidtagna åtgärder.

En polisanmälan är en allmän handling och bör utformas på ett neutralt sätt. Den ska innehålla, förutom administrativa data, uppgifter om datum, tid och plats för brottet samt en gärningsbeskrivning. Resultatet från internutredningen ska bifogas som bilaga. Bilagan blir då arbetsmaterial i den polisiära förundersökningen och offentliggörs först om och när åtal väcks. Vissa uppgifter kan även sekretessbeläggas i förundersökningsprocessen.

Som målsägare behöver man inte göra en bedömning om det inträffade verkligen utgör ett brott; det är rättsväsendets uppgift. Misstanke om brott är tillräcklig.

6 Systemutveckling- och förvaltning

Systemutveckling

En förutsättning för säkra IT-system är att säkerhetsaspekter beaktas från första början och under hela utvecklingsprocessen.

Den tillämpade utvecklingsmetoden bör innehålla anvisningar, procedurer och hjälpmedel för specifikation, design, konstruktion och realisering av IT-system så att:

- verksamhetens säkerhetskrav på IT-systemet identifieras och uppfylls,
- revision, incidenthantering, internutredningar, polisutredningar, etc. underlättas.

Detta innebär bl.a. att säkerhetskraven - t.ex. krav på informationsklassning, auktorisering, behörighetskontroll, tillgänglighet och applikationsloggar - ska fastställas i början av ett utvecklingsprojekt.

Systemförvaltning

Ett fungerande samspel mellan CSIRC och verksamhetsorienterad systemförvaltning samt IT-drift är grunden för en fungerande incidenthantering.

IT-incidenter kan inträffa såväl inom den verksamhet som använder IT-systemet som inom IT-drift.

lakttagelser

Säkerhetsrelaterade händelser i verksamheten bör rapporteras som säkerhetsiakttagelser av användarna. Exempel på händelser av denna typ är avvikande systembeteenden (misslyckade inloggningar, konstiga systemmeddelanden, omotiverat långa svarstider, ”hängningar” av arbetsstationen, oförklarliga systemavbrott eller -låsningar, etc.) och andra ovanligheter (oönskad e-post, omotiverade ändringar av filskydd, etc.). Ett absolut krav är att inrapporteringen är enkel och snabb att genomföra, annars är risken stor att folk slarvar med den.

Dokumentation av de åtgärder inklusive rapportering som systemanvändarna ska vidta vid allvarligare IT-incidenter - såsom virussmitta, e-postbombning, skivminneskrasch, etc. - måste finnas lättillgängligt i både elektronisk och annan form.

Säkerhetsiakttagelser skall analyseras av CSIRC, IT-drift och förvaltningsansvarig (systemägaren). Berörd personal bör informeras om resultatet snarast möjligt - snabb återrapportering är ett måste. Systemanvändare ska uppleva att inrapporteringen är meningsfull och till nytta för den egna verksamheten.

IT-incidenter inom IT-drift

IT-incidenter, eller misstänkta sådana, som upptäcks av IT-driften kan ofta avhjälpas av IT-driften själv; det är dock av vikt att även sådana händelser rapporteras till CSIRC. Avsikten med detta är dels att använda informationen för statistiska ändamål, dels att få en helhetsbild av IT-säkerheten inom organisationen.

Allvarliga IT-incidenter, speciellt händelser med illvilligt uppsåt, får inte hanteras av IT-driften ensamt utan måste tas hand om av CSIRC. Dock får IT-driften vidta i förväg definierade krisåtgärder om så krävs.

Reglerna för samarbetet mellan IT-drift och CSIRC i situationer ovan ska fastställas och dokumenteras i säkerhetshandboken. Detsamma gäller för användning av tekniska hjälpmedel för driftsövervakning, intrångs- och missbruksdetektering, säkerhetsloggning, etc.

Standardiserad beskrivning av IT-incidenter

Det pågår arbete inom Internetsfären för att definiera en standard för beskrivning, arkivering och utbyte av information om IT-incidenter (Incident Object Description and Exchange Format Requirements). Standardförslaget är främst avsett för att underlätta samarbetet mellan globala CERT men kommer i praktiken, åtminstone till vissa delar, även att kunna tillämpas inom lokala CSIRC/CSIRT.

Sandia National Laboratories har dessutom föreslagit en modell - i form av ett abstrakt språk innehållande termer och taxonomier (klassificeringsregler) för insamling, utbyte och jämförelse av information avseende säkerhetsincidenter.

7 Övrigt

Inrättande av CSIRC

När en CSIRC inrättas bör så många som möjligt informeras både internt och externt. Det är centralt att denna information ger en korrekt bild av den planerade verksamheten samt att det klart framgår att funktionen aktivt har stöd från den högsta ledningen.

CSIRC är en tvärfunktionell verksamhet vars effektivitet är avhängig av hur väl den accepteras av den ”ordinarie linjestrukturen”. För en hög acceptans krävs att organisationen anser att CSIRC ”ger valuta för pengarna”.

Den interna introduktionen sker lämpligen genom någon form av internt meddelande med efterföljande presentationer för berörd personal. Press-release och elektronisk information (nyhetsmeddelande, webbsida, etc.) är lämpliga medel för allmän, extern introduktion.

Etablering av lämpligt samarbete med relevanta externa organisationer (andra CSIRC, polis, universitet och högskolor m.m.) bör initieras snarast möjligt, helst från första början.

Brottsförebyggande åtgärder

För närvarande utgör interna angrepp och IT-missbruk en relativt stor andel av IT-incidenter. Brottsförebyggande åtgärder, annat än explicita säkerhets-åtgärder, är inte en uppgift för CSIRC. Man bör dock aktivt arbeta för att öka medvetenheten om risken för intern brottslighet samt betydelsen av effektiva förebyggande åtgärder av typen god personalpolitik, positiv före-tagskultur, samhörighet och ”vi”-känsla.

Referenslitteratur

Arvidsson, Jimmy
Säkerhetsutredning - Lagar, avtal och metodik, Miniuppsats, DSV, SU/KTH, 1995.

Arvidsson, Jimmy
Incidentorganisation och incidenthantering, Master´s Thesis, DSV, SU/KTH, 2000.

Arvidsson, Jimmy et al.
IODEF Requirements, RFC 3067, 2001.

Brownlee, Nevil; Guttman, Erik
Expectations for Computer Security Incident Response, RFC 2350, 1998.

Fraser, Barbara Y
Site Security Handbook, RFC 2196, 1997.

Försvarsdepartementet
Säkerhet i en ny tid, Sårbarhets- och säkerhetsutredningens betänkande, SOU 2001:41.

Malmgren, Robert
Hantera incidenter rätt, *Säkerhet & Sekretess,* **2**, 6, 2000.

Post och Telestyrelsen
Förutsättningar för att inrätta en särskild funktion för IT-incident-hantering, 2000.

SANS Institute
Computer Security Incident Handling Step by Step, Version 1.5, 1998.

Smith, Danny:
Forming an Incident Response Team, AusCERT, University of Queensland, 1994 (FIRST 1994 Paper).

Schwartau, Wim:
Information Warfare, 2nd Edition, Thunder´s Mouth Press, 1996.

West-Brown, Moira J; Stikvoort, Don; Kossakowski, Klaus-Peter:
Handbook for Computer Security Incident Response Teams (CSIRTs), Software Engineering Institute, Carnegie Mellon, CMU/SEI-98-HB-001, 1998.

Wack, John P:
Establishing a Computer Security Incident Response Capability (CSIRC), NIST Special Publications 800-3, 1991.

Bilaga 1 IT-incidenter och polisanmälan

Källa: Rikspolisstyrelsen

Om en incident inträffar och det finns anledning att tro att den kan resultera i en polisanmälan finns ett antal principer att beakta så att man inte försvårar eller förhindrar möjligheterna att utreda händelsen. Givetvis bör man alltid följa dessa principer så långt man finner det lämpligt, eftersom man från början kanske inte kan avgöra om det kommer att bli aktuellt med en polisanmälan.

Huvudprincipen är att ”frysa” situationen och skapa en spegelkopia av drabbat system tidsmässigt så nära den aktuella händelsen som möjligt. Följande punkter utgör en vägledning men kan behöva anpassas beroende på händelsens art och typen av system.

1. *Drabbas ej av panik*, behåll lugnet.
2. *Begränsa skadan*.
3. *Dokumentera* hur problemet upptäcktes.
4. *Dokumentera* alla vidtagna åtgärder.
5. *Utse an ansvarig* kontaktperson.
6. *Ta en fullständig reservkopia* av systemet (helst en *spegelkopia*, dvs en binär kopia av skivminnets samtliga sektorer oavsett om de tillhör någon fil eller ej). Om en spegelkopia ej kan göras bör man om möjligt skapa en vanlig reservkopia och plocka bort det drabbade skivminnet för vidare utredning. Reservkopian laddas sedan till ett nytt skivminne för att om så önskas återuppta driften.
7. Om *egna analyser* ska göras, gör det mot en egen kopia av det drabbade skivminnet. Att arbeta med ett skivminne som kan komma att bli föremål för polisutredning innebär att man riskerar påverka information som kan ha betydelse för utredningens resultat.
8. *Säkra reservkopiorna*. Reservkopior ingår ofta i en cyklisk användning med veckoband, månadsband, etc. Det är viktigt att plocka ut och säkra dessa så att de inte återanvänds.
9. *Säkra systemtekniska loggar*. Det är extra viktigt i miljöer där man inte kan göra en spegelkopia av systemet och då man inte kan stoppa verksamheten för en längre tid. Loggar kan finnas i många olika former: säkerhetslogg, systemlogg, transaktionslogg, databaslogg, applikationslogg, Internetrelaterade loggar, mm.
10. *Sammanställ uppgifter* om det drabbade systemet. I fall det är ett Internetrelaterat problem - sammanställ även uppgifter om typ av anslutning, nätoperatörer, Internetleverantörer, etc.
11. Kopiera alltid e-post och dylikt i *fullständig form* så att alla administrativa uppgifter (brevhuvud mm) kommer med.
12. *Kontakta polisen*. Huvudprincipen är att anmälan ska göras till närmaste polismyndighet. Notera dock att närpolisen inte alltid har kunskap om IT-relaterade brott varför man kan behöva beskriva det inträffade med hänsyn till detta. Det finns även personal vid länspolismyndigheterna som kan ge råd beträffande IT-relaterade brott.

Bilaga 2 Krisråd för vilsna

Källa: ÖCB och Statskontoret

Steg 1 Behåll lugnet

En lugn sinnesnärvaro underlättar effektiv kommunikation och samarbete. En upprörd stämning förorsakar ofta dyrbara misstag.

Steg 2 Ta utförliga anteckningar

Adekvat dokumentation av incidenter är en förutsättning för framtida förbättringar av säkerhetsskyddet. Tänk på att dina anteckningar kan utgöra bevismaterial efter en polisanmälan. Försök att besvara frågorna VAD, VAR, NÄR, VEM, HUR och VARFÖR. Dokumentera kontinuerligt under hela utredningen.

Steg 3 Informera berörda befattningshavare och skaffa hjälp

Informera berörd linjechef samt säkerhetsansvarig. Be att få hjälp av en eller flera kollegor vid den fortsatta hanteringen av incidenten. Se till att alla medverkande har tillgång till den senaste versionen av den interna telefonkatalogen. Se till att alla i incidentgruppen utförligt dokumenterar vad de gör.

Steg 4 Inför regler för informationsspridning

Endast en mindre grupp medarbetare behöver känna till detaljerna kring incidenten. Kräv diskretion vid behöv. Be högre chef besluta hur media och andra externa kommunikationskanaler ska hanteras om frågan blir aktuell.

Steg 5 Använd säkra kommunikationskanaler

Skicka ingen okrypterad e-post, använd inte ”chat” eller organisationens intranät vid t.ex. dataintrång. Använd telefon, SMS eller fax.

Steg 6 Avgränsa problemet

Vidta nödvändiga åtgärder för att problemet inte ska förvärras. Vid dataintrång på en värddator koppla t.ex. bort värddatorn från nätet.

Steg 7 Ta säkerhetskopia

Skapa en binär spegelkopia i två exemplar på nya, oanvända media. Den ena kan användas som bevismaterial vid en eventuell polisanmälan, den andra som underlag för tekniska analyser.

Steg 8 Avlägsna problemet

Vidta åtgärder, om möjligt, för att undvika problemet i framtiden, eller i varje fall för tillfället.

Steg 9 Sammanställ all dokumentation

Sammanställ all dokumentation, inkl. allt arbetsmaterial, som har använts under utredningen.

Steg 10 Återgå till arbetet

Återstarta systemet från den senaste ej komprometterade säkerhetskopian. Testa om systemet fungerar korrekt. Övervaka systemet noggrant under en tidsperiod.

Bilaga 3 IT-incidenter

Källa: Post- och telestyrelsen

Vad är IT-incidenter?

Ordet incident har skilda tolkningar beroende på sammanhanget. Begreppet IT-incident har heller ingen bestämd innebörd. Begreppet torde ha uppkommit därför att man länge inom IT-området använt ordet ”incident” för att beteckna vissa typer av oönskade händelser. IT-incident har sedan utan närmare precisering kommit att användas bl.a. i utredningar och direktiv. I Internetsammanhang kopplas ”incident” ofta till olika slags angrepp eller förberedelser för angrepp på datorer eller datornät. FIRST (ett samarbetsorgan för organisationer för incidenthantering) beskriver exempelvis en incident som “an event that has actual or potentially adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information. Examples include penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software”.

Beteckningen IT-incident används i resten av denna sammanställning för Händelser

- som drabbar eller påverkar IT-system (inklusive system för datakommunikation)
- där IT-system utnyttjas för angrepp, brott eller annan oönskad verksamhet
- som är oönskade och oplanerade (ur ägarens, förvaltarens eller användarnas perspektiv)
- direkt eller indirekt medför eller kan medföra allvarliga negativa konsekvenser för ägare, användare eller andra

För att en händelse ska kallas en IT-incident krävs också att påverkan på eller utnyttjande av IT-systemet är en viktig del av händelsen. Händelser som utgör steg i en händelsekedja som leder fram till en faktisk IT-incident, eller som utgör förberedelser för en sådan, kan också omfattas av beteckningen. Alla sådana händelser är dock inte IT-incidenter (då skulle t.ex. anskaffning av ett datasystem kunna vara en IT-incident). Denna beskrivning och avgränsning är inte invändningsfri, och heller inte särskilt precis, men kan tjäna som utgångspunkt för fortsatta resonemang.

De IT-incidenter som beskrivs nedan är avsedda att exemplifiera IT-incidenter enligt ovanstående beskrivning och avgränsning. Exempelsamlingen är varken fullständig eller strikt systematisk.

Tekniska fel och fysiska skador

Avbrott i försörjningssystem

IT-incidenter kan orsakas av avbrott i elförsörjning, telekommunikation, kylvattenförsörjning och liknande. Sådana IT-incidenter kan medföra omfattande konsekvenser om avbrotten är långvariga. Kortare incidenter kan normalt hanteras med befintliga skyddsåtgärder (reservkraft, etc).

Tekniska fel

IT-incidenter kan orsakas av tekniska fel i datautrustning, utrustning för datakommunikation, operativsystem och andra stödsystem, tillämpningsprogram, kablage m.m. Tekniska fel är relativt vanliga, men genom lämpliga skyddsåtgärder (säkerhetskopiering, redundans, serviceavtal m.m.) kan konsekvenserna lindras.

Fysisk skada, stöld m.m.

IT-incidenter kan orsakas av brand, översvämning, vatteninströmning, avgrävning av kablar eller andra fysiska skador. De kan också orsakas genom att datautrustning stjäls. IT-incidenter orsakade av vatten- eller brandskador kan orsaka mycket omfattande konsekvenser.

Vandalisering, sabotage m.m.

IT-incidenter kan orsakas av vandalisering, sabotage och andra avsiktliga handlingar. Dessa kan vara riktade mot IT-systemet, mot andra system som IT-systemet är beroende av (el, tele, etc.) eller mot något helt annat mål (ett exempel på det senare är när vandalisering av ett toalettutrymme leder till översvämning i en datorhall). IT-incidenter orsakade av vandalisering eller sabotage kan medföra mycket omfattande konsekvenser. Smärre sabotageincidenter, orsakade exempelvis av missnöjda anställda eller f.d. anställda, ger normalt mer begränsade konsekvenser.

Handhavandefel m.m.

Handhavandefel

Merparten problem i IT-system orsakas av handhavandefel. Normalt medför de endast små konsekvenser. Enstaka händelser kan också medföra allvarliga konsekvenser och bör då benämnas IT-incidenter.

Fel vid service

Många IT-incidenter orsakas av fel vid service, installation eller underhåll av IT-system. Exempel på detta är oavsiktlig radering eller förändring av viktiga data samt längre funktionsavbrott på grund av fel vid service eller installation.

Felaktigt utvecklade eller införda system

Felaktigt utvecklade, upphandlade eller införda IT-system kan orsaka mycket omfattande negativa konsekvenser för såväl ägare och användare som för andra. Med den beskrivning av IT-incident som finns ovan kan dessa händelser ses som IT-incidenter. Det finns skäl såväl för som emot att behandla dem som IT-incidenter i utredningen. Säkerhetskritiska fel i kommersiella programsystem möjliggör merparten avsiktliga IT-incidenter, men felen i sig kan knappast ses som IT-incidenter. Ett funktionskritiskt fel i en kommersiell programvara kan däremot ses som en potentiell IT-incident (2000-felen i program är ett exempel på detta). Det är svårt att låta bli att på-

peka att denna kategori IT-incidenter troligen totalt sett orsakat de största kostnaderna för systemägarna och användarna.

Användarinstallerade program

Vid anslutning av t.ex. företagsnät till Internet får användarna ofta möjlighet att själva ladda ner och installera program av skilda slag i sina datorer, inklusive nya eller ändrade versioner av drivrutiner m.m. Sådana egeninstallerade program kan orsaka stora problem, om de inte fungerar tillsammans med andra program. De kan också försvåra eller fördyra programunderhåll och användarstöd.

Datavirus och trojaner

Datavirus

Datavirus är sällan riktade mot någon enskild organisation, men kan i sällsynta fall spridas avsiktligt för att drabba en viss grupp mottagare. Datavirus är mycket vanliga, men motmedlen (antivirusprogram m.m.) är effektiva. IT-incidenter som orsakas av datavirus (med undantag för e-postvirus, se nedan) kan medföra omfattande konsekvenser, särskilt i större organisationer. Enstaka virusangrepp kan oftast klaras av med enkla åtgärder.

E-postvirus

E-postvirus utnyttjar kopplingar mellan e-postprogram och t.ex. ordbehandlare för att sprida viruset vidare via e-post. Den angripna datorns epostadresslista utnyttjas för detta. E-postvirus kan får mycket snabb spridning, vilket gör att antivirusprogrammen kanske inte hunnit anpassas. Epostvirus kan därför få omfattande spridning innan motåtgärder hinner vidtas. IT-incidenter som orsakas av e-postvirus (Melissa är ett känt exempel) kan medföra omfattande konsekvenser. Kostnaderna för att rensa datorer efter omfattande virusangrepp kan i stora organisationer blir betydande.

Maskar

En ”mask” är ett program som startar kopior av sig självt i andra nätanslutna datorer. Till skillnad från ett virus behöver en mask inte kopiera sig till något datamedium. Ett av de mest omfattande angreppen på Internet var Morris mask (skriven av Robert T. Morris Jr.) som 2-3 november1988 slog ut en betydande del av de Internetanslutna datorerna. Program som är kombinationer av e-postvirus och maskar har tillfälligt uppnått omfattande spridning bland användare av specifika programprodukter (t.ex. VBS/LoveLetter 4-5 maj 2000).

Trojaner

Trojaner (dvs. program med en avsiktligt dold och vanligen skadlig funktion) är en angreppsmetod snarare än en särskild kategori av IT-incidenter. Trojaner kan ha funktioner som underlättar intrång, eller som medför direkt skada. Program för fjärrstyrning av PC (BackOrifice, NetBus, Sub-7 m.fl.) installeras ofta som trojaner genom att distribueras tillsammans med t.ex. spelprogram. Trojaner kan användas för angrepp som kan orsaka allvarliga konsekvenser (intrång, stöld av data, etc.), men används oftast för slumpmässiga angrepp.

Webbtrojaner

Med en webbtrojan avses här en webbsida som angriper den dator som används för att ladda ner (titta på) webbsidan. Webbtrojaner kan idag framför

allt bestå av program skrivna i Java eller ActiveX. En webbtrojan kan utnyttja säkerhetshål i den webbläsare som används. Webbtrojaner har i praktiken inte orsakat några omfattande skador. Däremot har webbtrojaner enligt uppgift använts för att göra motangrepp mot aktivister som lamslagit webbplatser genom samordnad överbelastning.

Missbruk, intrångsförsök och dataintrång

Detta delområde beskrivs i något större detalj än övriga områden, eftersom det stått i fokus i de tidigare utredningarna kring IT-incidenter.

Missbruk av IT-system

Missbruk av IT-system används här för att beteckna att någon utnyttjar sina möjligheter att använda ett IT-system på ett olämpligt eller otillåtet sätt. Mindre missbruk av IT-system är vanliga (privat användning av företags IT-system och Internetanslutningar, okynnesåtkomst till data som inte har med arbetsuppgiften att göra etc). Mindre missbruk av IT-system utgör knappast IT-incidenter med den definition som används här. Grovt missbruk av IT-system, för att möjliggöra exempelvis industrispionage eller ekonomiska brott, kan dock medföra allvarliga konsekvenser för det drabbade företaget eller myndigheten.

Portscanning

Portscanning (svensk term saknas) yttrar sig som försök till uppkoppling mot utvalda portar, eller mot ett stort antal portar, på nätanslutna datorer. Avsikten med uppkopplingarna är ofta att hitta kända svagheter i systemen, eller kontrollera om någon känd programvara för ”missbruk” (BackOrifice, Sub-7 e.d.) är installerad. Avsikten kan också vara att ta reda på vilket operativsystem e.d. som är installerat för att förbereda för intrång. Portscanningen medför i sig ingen skada, men är ofta första steget i ett intrång.

Okomplicerade dataintrång

Dataintrång innebär i sin enklaste form att någon olovligen utnyttjar en dator eller t.ex. en användaridentitet i en dator. (Alternativt utgör denna handling olovligt brukande av IT-resurser.) Ett enkelt exempel är när anställdas anhöriga utnyttjar företagets modempool och Internetkoppling för att surfa gratis på Internet. Ett allvarligare exempel är när någon utnyttjar en arbetskamrats användaridentitet för att exempelvis betala ut bidrag åt närstående. Okomplicerade dataintrång behöver inte medföra allvarliga konsekvenser, och kostnaderna för att återställa efter dem är vanligtvis låga. De kan också vara ett hjälpmedel för dataintrång, stöld av data, industrispionage eller andra brott som medför avsevärda konsekvenser.

Förstörande dataintrång

Med förstörande dataintrång avses dataintrång där angriparen avsiktligt förändrar styrdata, lösenord, programfiler eller annat i den angripna datorn. Sådana dataintrång innebär normalt att angriparen skaffar sig administratörsbehörighet (root-behörighet e.d.) och utnyttjar denna för att få kontroll över den angripna datorn. Ofta innebär de också att angriparen raderar loggar och vidtar andra åtgärder för att dölja intrånget. Det är vanligt att angriparen installerar ”bakdörrar” till systemet som gör det möjligt för honom/henne att komma tillbaka och åter få administratörsbehörighet.

Det finns idag många välkända och lätt tillgängliga hjälpmedel för att göra intrång och därefter skaffa sig administratörsbehörighet. Det finns också verktygssamlingar (rootkits) för att dölja intrången och öppna bakvägar.

Intrången kan göras utan särskilt syfte, eller för att göra det möjligt för angriparen att utnyttja datorn, till exempel för att ”hoppa vidare” för att försvåra spårning, avlyssna datakommunikation, installera en server eller installera DoS-verktyg. Intrången kan också göras för att kopiera (stjäla) data eller program för utnyttjande eller för utpressning e.d. Kostnaderna för att återställa efter intrång av detta slag är relativt stora och kräver hög kompetens. Intrången i sig åstadkommer sällan stor skada, annat än om de utnyttjas för stöld av data eller andra brott eller angrepp. Intrången kan däremot medföra avsevärd förlust av goodwill (t.ex. om servrar med olagligt eller oetiskt material sätts upp hos ett företag eller en myndighet). Förstörande dataintrång kan vara en förberedelse för andra former av angrepp eller brott, som sedan kan medföra omfattande konsekvenser.

Fjärrstyrning

Det finns ett antal väl utvecklade program, med vilka det går att fjärrstyra en PC från någon annan dator. Till de mest kända hör BackOrifice, Sub-7 och Netbus. Med hjälp av program av detta slag kan en angripare bland annat läsa av tangentnedslag, kopiera filer, installera program och avlyssna samtal (om datorn har inbyggd mikrofon). Programmen består av en del som måste installeras i den dator som ska angripas, och en annan del som körs av angriparen. Installationen i den angripna datorn görs ofta som en trojan, men skulle kunna göras i form av ett datavirus. Program för fjärrstyrning har fått en omfattande spridning, framför allt bland ungdomar. De kan användas för att förbereda eller underlätta intrång och andra angrepp.

Avlyssning av datanät

Otillåten avlyssning av datanät görs oftast genom ett förstörande dataintrång i en nätansluten dator, där man sedan installerar programvara för nätavlyssning och lagring eller vidaresändning av den avlyssnade trafiken. Avsikten med avlyssningen är oftast att få tillgång till datoradresser, användaridentiteter och lösenord för att kunna genomföra ytterligare dataintrång. Avlyssningen i sig medför inte mer allvarliga konsekvenser än andra förstörande dataintrång. Om ett stort antal lösenord avlyssnats, kan kostnaderna för att rensa angripna datorer och byta lösenord däremot blir mycket stora (flera miljoner kronor i större organisationer).

Avsiktlig störning av tillgänglighet

DoS-attacker

Med DoS-attacker (Denial of Service) avses avsiktliga IT-incidenter som är avsedda att förhindra användning av ett system, ett nät eller en tjänst. Attackerna genomförs vanligen genom att målsystemet överbelastas på något sätt, men kan också genomföras genom att målsystemet fås att sluta fungera (”hänga”, ”krascha” e.d.). Det finns ett flertal kända och effektiva sätt att överbelasta eller avbryta funktionen i system och nät. Några av dem utnyttjar kända svagheter i systemen. Attackerna genomförs ofta som sabotage, men kan också göras för att t.ex. öppna ett system för intrång. DoS-attacker kan stänga ett system eller en tjänst för lång tid, och kan därmed orsaka omfattande konsekvenser.

Distribuerade DoS-attacker

Distribuerade DoS-attacker genomförs med hjälp av ett stort antal ”attack-program”, som placerats ut i datorer där man gjort förstörande intrång. DoS-attackerna från samtliga program samordnas mot ett fåtal målsystem. Genom de samordnade attackerna blir det i praktiken omöjligt att skydda målsystemet. Distribuerade DoS-attacker kan överbelasta även mycket stora målsystem, med omfattande konsekvenser som resultat. Distribuerade DoS-attacker som görs manuellt genom samordning av många ”användare” kan vara relativt enkla att organisera, och kan medföra stora problem eller kostnader om de utförs mot viktiga system (till exempel bankernas Internet-tjänster i slutet av en månad).

Angrepp på DNS

Genom att en angripare för in felaktig information i en eller flera domännamnservrar (DNS-servrar) kan användare dirigeras om till en ”falsk” adress eller server. Alternativt kan de dirigeras om till obefintliga adresser. I båda fallen förhindras användning av den avsedda tjänsten. En falsk server kan användas för bedrägerier eller spridande av falsk information e.d.

Personalbrist

Nyckelpersonsberoende bedöms ofta vara en av de största säkerhetsriskerna i IT-system. Om så är fallet måste händelser som innebär att en nyckelperson slutar eller skadas e.d. kunna utgöra IT-incidenter enligt definitionen ovan. Massuppsägningar eller strejker skulle då också kunna vara IT-incidenter. Det är oklart om personalproblem av dessa slag ska ses som IT-incidenter.

IT-relaterade brott

BRÅ påpekar i sin senaste rapport om IT-relaterad brottslighet att allt fler brott kommer att vara IT-relaterade enbart i kraft av att IT-användningen i samhället ökar. Man påpekar också att Internet är ett effektivt hjälpmedel för organiserad brottslighet och kriminella nätverk. Gränsdragningen mellan IT-incidenter och annan IT-relaterad brottslighet är inte enkel. Data kopierade vid ett dataintrång (en typisk IT-incident) kan utnyttjas för brott som exempelvis utpressning, bedrägeri eller industrispionage. Omvänt kan ett ”okomplicerat” kontorsinbrott, där datautrustning stjäls, bli en IT-incident om data som är kritiska för företaget försvinner.

Civila informationsoperationer

”Information Operations” har ersatt ”Information Warfare” som begrepp bl.a. inom USA:s försvar. Det finns ingen entydig definition av vad man avser med informationsoperationer. I detta avsnitt diskuteras några exempel på informationsoperationer som innebär organiserade åtgärder för att åstadkomma IT-incidenter hos en motståndare eller motpart. Beteckningen informationsoperationer används i andra sammanhang för många fler typer av åtgärder, inklusive militära operationer.

Aktionsgrupper

Grupper med ideologiska eller andra motiv kan utnyttja Internet och datasystem för att skada motståndare, men också för att få uppmärksamhet. De militanta veganernas e-postbombning av Karolinska Institutet är ett exempel. Aktionsgrupper kan använda olika slags avsiktligt framkallade IT-inci-

denter för sina syften. DoS-attacker är vanliga, men även t.ex. intrång i webbservrar för att förändra webbplatser.

Massaktioner

Det är möjligt att på Internet mobilisera ett mycket stort antal personer för angelägna syften. Om tiotusentals eller hundratusentals användare och systemadministratörer världen över enas om samordnade aktioner, är det fullt möjligt att under mycket lång tid blockera ett företags eller till och med ett mindre lands Internetförbindelser. Mindre sådana aktioner har förekommit, liksom hot om aktioner. I samband med folkomröstningen om Östtimor i Indonesien i augusti 1999 uttalades ett hot om att genom ”samordnade hackerattacker” stänga Indonesiens IT-system om valet inte gick rätt till. Hotet verkställdes inte. Massaktioner kan genomföras som DoS-attacker av olika slag (e-postbombning, rå överbelastning e.d.). Även andra typer av attacker är möjliga. Det är i många fall så gott som omöjligt att skydda sig mot denna typ av massaktioner.

Motattacker

Användare, systemadministratörer, operatörer eller nätägare som utsätts för störningar kan - avsiktligt eller oavsiktligt - utsätta ”oskyldiga” för motattacker. Ett banalt exempel på detta är att om en e-postserver hos en ”oskyldig” utnyttjas för massutskick av e-post, kan de klagobrev som detta resulterar i överbelasta den ”oskyldiges” egen e-posttjänst.

Bortkoppling

Inom Internet har man av hävd utnyttjat bortkoppling av störande nät eller system både som en skyddsåtgärd och något som kan liknas vid en bestraffning. Den tydligaste formen av bortkoppling innebär att ett system, ett delnät eller ett helt land kopplas bort från resten av Internet. En annan form av bortkoppling innebär att ett delnät e.d. avsiktligt stänger ute något annat delnät (detta kan göras genom att inte acceptera vissa avsändaradresser i den egna accessroutern). Den senaste tidens distribuerade DoS-attacker har aktualiserat bortkoppling som skyddsåtgärd och hot. Bortkoppling innebär för den bortkopplade en IT-incident som kan medföra allvarliga konsekvenser, om bortkopplingen är långvarig eller kommer olämpligt.

Informationsattacker

Med informationsattacker (termen är lånad från Ag IW:s rapport) avses här avsiktlig desinformation publicerad på eller distribuerad över Internet. Avsiktlig desinformation på Internet har använts bl.a. i syfte att påverka aktiekurser. Attacker av detta slag kan medföra stora ekonomiska konsekvenser. De kan också användas för att påverka opinionen, etc.

Det är en öppen fråga om informationsattacker ska betecknas som IT-incidenter eller inte.

Underrättelseverksamhet

Det är möjligt att utnyttja dataintrång, avlyssning av datakommunikation och liknande IT-incidenttekniker för underrättelseverksamhet.

Militära informationsoperationer

Här avses informationsoperationer använda av militära organisationer, gerillaorganisationer, terroristorganisationer eller liknande organisationer (eller individer), eller utnyttjade mot sådana organisationer.

Kvalificerade informationsoperationer

Hit hör såväl offensiva som defensiva informationsoperationer. Informationsoperationer används här i mycket vid bemärkelse (men begränsade till operationer som är IT-incidenter).

Sabotage

Det är möjligt att genomföra sabotageoperationer med IT-incidentteknik, eller med stöd av sådan teknik.

Fysiskt destruktiva informationsoperationer

Till denna grupp informationsoperationer hör fysisk förstöring av IT-system, inklusive system för kommunikation (oavsett teknik för förstöringen).

Nya typer av IT-incidenter

Nya typer av IT-incidenter uppkommer allt eftersom tekniken utvecklas och användningen av tekniken ökar.

Teknikrelaterade IT-incidenter

Ny teknik kommer att medföra nya typer av fel och felfunktioner. Ny teknik kommer med all sannolikhet också att kunna utnyttjas för att åstadkomma avsiktliga IT-incidenter (på samma sätt som makrofunktionerna i Word och kopplingarna till e-postprogram gjorde e-postvirusen möjliga).

IT-relaterade brott

Nya typer av IT-relaterade brott kommer att utvecklas, både därför att ny teknik tas i bruk och därför att nya ”innovationer” görs inom brottsområdet.

Användningsrelaterade IT-incidenter

Ny eller ökad användning av IT-system och IT-kommunikation kan resultera i nya typer av IT-incidenter, där konsekvenserna blir omfattande på grund av det sätt som IT-tekniken används (på samma sätt som informationsförmedlingen via Internet gjort desinformation via Internet möjlig).

Bilaga 4 Kompetensområden för CSIRC/CSIRT

Efterföljande förteckning illustrerar lämplig specialkompetens för medlemmar i ett CSIRC eller CSIRT. Förteckningen gör inga anspråk på fullständighet.

Generell kompetens inom IT och säkerhet

Goda kunskaper avseende:
- TCP/IP
- IT-säkerhet
- källkodsanalys
- internutredning

Grundläggande kunskaper avseende:
- systemutveckling
- systemdrift
- systemförvaltning
- säkerhetsjuridik
- förhandling och avtal
- Risk Management

Teknisk kompetens

Goda kunskaper avseende:
- maskinvaror
- operativsystem och hjälpprogram
- nätoperativsystem, nätövervakningssystem
- Internetprotokoll
- standardprogram
- tillämpningssystem
- program för IT-säkerhet
  - accesskontrollsystem
  - brandväggar
  - intrångsdetekteringssystem
  - antivirusprogram

Expertkunskaper avseende:
- hjälpmedel för Risk Management
- hjälpmedel för incidentanalys
- intrångsdetektering
- kriminaltekniska programvaror (Computer Forensics Software)
- program för omvänd kompilering (reverse engineering) av programvara
- program för ”statisk” sårbarhetsanalys
- program för aktiv kontroll
- ”Read Team”-attacker
- superloggning (riktad individövervakning)

Administrativ kompetens

Expertkunskaper avseende:
- behörighetskontrollsystem
- procedurer för incidentrapportering
- hantering av incidentdatabas

- externa och interna kommunikationsprocedurer
- utredningsdokumentation och -procedurer
- procedurer för distansinsatser (off site operations)