EN TRINVIS VEJLEDNING I OPRETTELSE AF ET CSIRT

Dokument WP2006/5.1(CERT-D1/D2)

Indholdsfortegnelse

1 Resumé

I denne publikation beskrives processen med at oprette et it-sikkerheds- og udrykningsteam (Computer Security and Incident Response Team (CSIRT) ud fra alle relevante synsvinkler, f.eks. virksomhedsledelse, processtyring og tekniske perspektiver. Med publikationen gennemføres to af de opgaver, der beskrives i ENISA's arbejdsprogram 2006, kapitel 5.1:

- Dette dokument: *Skriftlig rapport om den trinvise vejledning i oprettelse af en it-alarmtjeneste CERT (Computer Emergency Response Team) eller lignende faciliteter, med eksempler* (**CERT-D1**)
- Kapitel 12 og eksterne filer: *Uddrag af en køreplan i punktform, som gør det let at anvende køreplanen i praksis.* (**CERT-D2**)

2 Juridisk meddelelse

3 Tak

ENISA ønsker at takke alle institutioner og personer, der har bidraget til dette dokument. En særlig "Tak" skal gå til følgende bidragydere:

- Henk Bronk, der som konsulent udarbejdede den første udgave af dette dokument.
- CERT/CC og især CSIRT-udviklingsteamet, der bidrog med særdeles nyttigt materiale og eksemplerne på kursusmateriale i bilaget.
- GovCERT.NL, der har leveret *CERT-in-a-box.*

- TRANSITS-teamet, der har bidraget med eksemplerne på kursusmateriale i bilaget.
- Kollegerne fra kontoret for sikkerhedspolitikker i den tekniske afdeling, der har bidraget med kapitel 6.6.
- De utallige mennesker, der har gennemlæst dette dokument.

4 Indledning

Kommunikationsnet og informationssystemer er blevet en væsentlig faktor i den økonomiske og sociale udvikling. Informationsteknologi og net er nu ved at blive en alment tilgængelig ressource på lige fod med f.eks. vand og elektricitet.

Sikkerheden i kommunikationsnet og informationssystemer, og navnlig deres tilgængelighed, får derfor stigende betydning for samfundet. Det skyldes risikoen for problemer i centrale informationssystemer som følge af systemernes kompleksitet, uheld, fejl og angreb mod de fysiske infrastrukturer, som sikrer tjenesteydelser af stor betydning for EU-borgernes velfærd.

Den 10. marts 2004 blev der oprettet et europæisk agentur for net- og informationssikkerhed (ENISA)[1]. Det havde til formål at sikre et højt og effektivt net- og informationssikkerhedsniveau i Fællesskabet og udvikle en net- og informationssikkerhedskultur til gavn for borgere, forbrugere, virksomheder og organisationer under den offentlige sektor i Den Europæiske Union og dermed bidrage til et velfungerende indre marked.

I flere år har en række sikkerhedsfællesskaber i Europa som CERT/CSIRT'er, "Abuse Team" og WARP'er (Warning, Advice and Reporting Points, advarsels-, rådgivnings- og rapporteringspunkter), nu samarbejdet om at skabe et mere sikkert internet. ENISA ønsker at støtte disse fællesskaber i deres bestræbelser ved at levere information om foranstaltninger til at sikre et passende servicekvalitetsniveau. Endvidere ønsker ENISA at styrke sin evne til at rådgive EU-medlemsstaterne og EU-organerne i spørgsmål om, hvordan bestemte grupper af it-brugere dækkes ind med passende sikkerhedstjenester. På grundlag af resultaterne fra ad hoc-arbejdsgruppen CERT Cooperation and Support, der blev nedsat i 2005, skal denne nye arbejdsgruppe behandle spørgsmål om tilvejebringelse af relevante sikkerhedstjenester ("CERT-tjenester") til bestemte (kategorier eller grupper af) brugere.

ENISA støtter etableringen af nye CSIRT'er ved at udgive denne ENISA-rapport "*En trinvis vejledning i oprettelse af et CSIRT med supplerende tjekliste"*, som kan være en hjælp ved oprettelse af et CSIRT.

[1] Europa-Parlamentets og Rådets forordning (EF) nr. 460/2004 af 10. marts 2004 om oprettelse af et europæisk agentur for net- og informationssikkerhed. Et "EU-agentur" er et organ, der oprettes af EU for at udføre en helt specifik teknisk, videnskabelig eller ledelsesmæssig opgave inden for EU's "fællesskabsområde" ("første søjle").

4.1 Målgruppe

De primære målgrupper for denne rapport er statslige og andre institutioner, der beslutter at oprette et CSIRT med henblik på at beskytte deres egen eller de implicerede parters it-infrastruktur.

4.2 Hvordan bruger man dette dokument?

Dokumentet indeholder oplysninger om, hvad et CSIRT er, hvilke tjenester det kan levere, og hvilke skridt der skal tages for at komme i gang. Det skulle give læseren et godt og praktisk overblik over, hvordan man opbygger et CSIRT, og hvad det skal indeholde.

Kapitel 4 *"Indledning"*
Introduktion til denne rapport

Kapitel 5 *"Overordnet strategi for planlægning og oprettelse af et CSIRT"*
Første afsnit giver en beskrivelse af, hvad et CSIRT er. Det indeholder også information om de forskellige miljøer, CSIRT'er kan fungere i, og hvilke tjenester de kan levere.

Kapitel 6 *"Udarbejdelse af forretningsplan"*
Dette kapitel beskriver virksomhedsledelsens strategi for oprettelsesprocessen.

Kapitel 7 *"Fremme af forretningsplanen"*
Dette kapitel omhandler forretningsplanen og finansieringsspørgsmål.

Kapitel 8 *"Eksempler på operationelle og tekniske procedurer"*
I dette kapitel beskrives proceduren med at skaffe information og oversætte den til en sikkerhedsbulletin. Kapitlet indeholder også en beskrivelse af et arbejdsflow for håndtering af sikkerhedshændelser.

Kapitel 9 *"CSIRT-uddannelse"*
Dette kapitel giver et resumé af den tilgængelige CSIRT-uddannelse. Til illustration er der samlet eksempler på kursusmateriale i bilaget.

Kapitel 10 *"Øvelse: fremstilling af en bulletin"*
Dette kapitel indeholder en øvelse i, hvordan man gennemfører en af de grundlæggende CSIRT-ydelser, eller kerneydelser: fremstilling af en sikkerhedsbulletin (eller rådgivende bulletin).

Kapitel 12 "Beskrivelse af projektplanen"
Dette kapitel indeholder den supplerende projektplan (tjekliste), der følger med denne vejledning. Planen sigter mod at være et let anvendeligt værktøj til gennemførelse af vejledningen.

4.3 Konventioner i dette dokument

For at gøre det lettere for læseren begynder hvert kapitel med et resumé af de skridt, vi indtil nu har taget i processen med at oprette et CSIRT. Disse resuméer er indrammet som vist nedenfor:

Vi har taget det første skridt

Hvert kapitel afsluttes med et praktisk eksempel på de skridt, der er taget. I dette dokument vil det fiktive CSIRT være et lille uafhængigt CSIRT til en mellemstor virksomhed eller institution. Der findes et resumé i tillægget.

Det fiktive CSIRT

5 Overordnet strategi for planlægning og oprettelse af et CSIRT

For at sikre en vellykket start på oprettelsen af et CSIRT er det vigtigt at have et klart billede af de mulige tjenester, teamet kan yde sine kunder, der i "CSIRT-verdenen" er bedre kendt som "konstituenter". Derfor er det nødvendigt at vide, hvilke behov konstituenterne har, for at kunne levere de relevante ydelser til rette tid og i den rette kvalitet.

5.1 Hvad er et CSIRT?

CSIRT står for Computer Security Incident Response Team, der er et it-sikkerheds- og udrykningsteam. Forkortelsen CSIRT bruges overvejende i Europa for det beskyttede udtryk CERT, der er registreret i USA af CERT-koordinationscentret (CERT Coordination Center, CERT/CC).
Der findes forskellige forkortelser for den samme type team:

- CERT eller CERT/CC (Computer Emergency Response Team / Coordination Center, som på dansk bliver it-alarmtjeneste)
- CSIRT (Computer Security Incident Response Team), der er et it-sikkerheds- og udrykningsteam
- IRT (Incident Response Team), udrykningsteam i forbindelse med sikkerhedshændelser
- CIRT (Computer Incident Response Team), it-udrykningsteam i forbindelse med sikkerhedshændelser
- SERT (Security Emergency Response Team), it-alarmtjeneste

Det første store udbrud af orm i den globale it-infrastruktur skete i slutningen af 1980'erne. Ormen blev kaldt Morris[2], og den spredte sig hurtigt og inficerede effektivt en lang række it-systemer rundt omkring i verden.

Den hændelse virkede som en øjenåbner, for pludselig blev folk opmærksomme på et stærkt behov for samarbejde og koordinering mellem systemadministratorer og it-chefer for at takle tilfælde som dette. Eftersom tid var en kritisk faktor, var det nødvendigt at opstille en mere organiseret og struktureret strategi til håndtering af it-sikkerhedshændelser. Så et par dage efter "Morris-hændelsen" oprettede Defence Advanced Research Projects Agency (DARPA) det første CSIRT: CERT-koordinationscentret, (CERT/CC[3]), der blev placeret på Carnegie Mellon University i Pittsburgh (Pennsylvania, USA).

Denne model blev snart indført i Europa, og i 1992 lancerede den nederlandske akademiske udbyder SURFnet det første CSIRT i Europa under navnet SURFnet-CERT[4]. Mange team fulgte, og på nuværende tidspunkt omfatter ENISA's opgørelse

[2] Mere information om Morris-ormen http://en.wikipedia.org/wiki/Morris_worm

[3] CERT-CC, http://www.cert.org

[4] SURFnet-CERT: http://cert.surfnet.nl/

over CERT-aktiviteter i Europa, *Inventory of CERT activities in Europe*[5], over 100 kendte team i Europa.

I årenes løb har CERT'erne udvidet deres kapacitet fra blot at være udrykningsteam til at blive en komplet sikkerhedsserviceudbyder, der også kan tilbyde forebyggende tjenesteydelser, såsom varslinger, sikkerhedsbulletiner samt uddannelses- og sikkerhedsstyringstjenester. Udtrykket "CERT" blev snart anset for utilstrækkeligt. Som følge heraf blev det nye udtryk "CSIRT" indført i slutningen af 1990'erne. I øjeblikket bruges begge udtryk (CERT og CSIRT) synonymt, men CSIRT er det mest præcise.

5.1.1 Udtrykket *"konstituent"*

Fra nu af vil det (i CSIRT-kredse) velkendte udtryk "konstituent" blive brugt om et CSIRT's kundegrundlag. En enkelt kunde vil blive omtalt som "konstituent", en gruppe som "konstituenter".

5.1.2 Definition af et CSIRT

Et CSIRT er et team af it-sikkerhedseksperter, hvis hovedopgave er at reagere på it-sikkerhedshændelser. Det leverer de tjenesteydelser, der er nødvendige for at håndtere dem, og støtter deres konstituenter med at sikre genoprettelse efter brud.

Med henblik på at mindske risici og minimere antallet af nødvendige indgreb leverer de fleste CSIRT'er også tjenesteydelser af forebyggende og uddannelsesmæssig karakter til deres konstituenter. De udsender bulletiner om sårbarheder i den soft- og hardware, der bruges, og informerer også brugerne om exploits og vira, der udnytter disse smuthuller, således at konstituenterne hurtigt kan patche og opdatere deres systemer. Se en komplet liste over mulige tjenester i kapitel *5.2 Mulige tjenester*.

5.1.3 Fordelene ved at have et CSIRT

Når en organisation har et særligt it-sikkerhedsteam, medvirker det til at mindske og forebygge større hændelser og til at beskytte værdifulde aktiver.

Andre mulige fordele:

- at have en centraliseret koordinering af it-sikkerhedsspørgsmål inden for organisationen (kontaktpunkt (Point of Contact, PoC)).
- at have en centraliseret og specialiseret håndtering af og reaktion på it-sikkerhedshændelser
- at have eksperter ved hånden, der kan støtte og bistå brugerne, så de hurtigt får sikret genoprettelse efter sikkerhedshændelser
- at have folk, der kan håndtere juridiske spørgsmål og bevare bevismateriale i tilfælde af en retssag
- at følge med i udviklingen på sikkerhedsområdet
- at stimulere samarbejdet mellem konstituenterne om it-sikkerhed (bevidstgørelse).

Det fiktive CSIRT (trin 0)

[5] ENISA Inventory http://www.enisa.europa.eu/cert_inventory/

Forståelse for, hvad et CSIRT er:
Vores fiktive CSIRT skal betjene en mellemstor institution med 200 medarbejdere. Institutionen har sin egen it-afdeling og to andre lokalafdelinger i samme land. It spiller en afgørende rolle for virksomheden, fordi den bruger it til intern kommunikation, datanet og e-business 24 timer i døgnet, 7 dage om ugen (24x7). Institutionen har sit eget net og har en ekstra forbindelse til internettet via to forskellige internetudbydere.

5.1.4 Beskrivelse af de forskellige former for CSIRT-miljøer

Vi har taget det første skridt

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.

>> Næste skridt er at få svar på spørgsmålet: ”Hvilken sektor skal have leveret CSIRT-tjenester?”

Når man opretter et CSIRT, er det (som med enhver anden virksomhed) særdeles vigtigt meget hurtigt at få et klart billede af, hvem konstituenterne er, og hvilken type miljø CSIRT-tjenesterne skal udvikles til. I øjeblikket skelner vi mellem følgende ”sektorer” opført i tilfældig rækkefølge:

- CSIRT til den akademiske sektor
- Kommercielt CSIRT
- CSIRT til sektorer med kritisk infrastruktur/kritisk informationsinfrastruktur
- CSIRT til den statslige sektor
- Internt CSIRT
- CSIRT til den militære sektor
- Nationalt CSIRT
- Smv-CSIRT
- Leverandør-CSIRT

CSIRT til den akademiske sektor
Fokus
Et CSIRT til den akademiske sektor leverer CSIRT-tjenester til akademiske institutioner og uddannelsesinstitutioner, såsom universiteter eller forskningsfaciliteter og deres internetmiljøer på campus.

Konstituenter
Typiske konstituenter for denne type CSIRT er medarbejdere og studerende på universiteter.

Kommercielt CSIRT
Fokus
Et kommercielt CSIRT leverer CSIRT-tjenester til deres konstituenter på kommerciel basis. Hvis der er tale om en internetudbyder, leverer CSIRT for det meste misbrugstjenester til slutbrugerkunder (indvalg, adsl) og CSIRT-tjenester til deres erhvervskunder.

Konstituenter
Kommercielle CSIRT’er leverer normalt deres tjenester til konstituenter, der betaler for dem.

CSIRT til sektorer med kritisk infrastruktur/kritisk informationsinfrastruktur
Fokus
CSIRT'er i den sektor fokuserer hovedsagelig på kritisk informationsbeskyttelse og/eller kritisk informations- og infrastrukturbeskyttelse. I de fleste tilfælde har dette specialiserede CSIRT et tæt samarbejde med en statslig styrelse for informationsinfrastrukturbeskyttelse. Det dækker alle kritiske it-sektorer i landet og beskytter det pågældende lands borgere.

Konstituenter
Staten, kritiske it-virksomheder, borgere.

CSIRT til den statslige sektor
Fokus
Et statsligt CSIRT leverer tjenester til statslige organer og i nogle lande til borgerne.

Konstituenter
Staten og statslige organer; i nogle lande leveres der også varslingstjenester til borgerne (f.eks. i Belgien, Ungarn, Nederlandene, Det Forenede Kongerige eller Tyskland).

Internt CSIRT
Fokus
Et internt CSIRT leverer kun tjenester til sin værtsorganisation. Der er snarere tale om en funktion end om en sektor. F.eks. driver mange telekommunikationsorganisationer og banker deres egne interne CSIRT'er. De driver normalt ikke et websted for offentligheden.

Konstituenter
Værtsorganisationens interne medarbejdere og it-afdeling.

CSIRT til den militære sektor
Fokus
Et CSIRT i den sektor leverer tjenester til militære organisationer med ansvar for den it-infrastruktur, der er nødvendig til forsvarsformål.

Konstituenter
Medarbejdere i militære institutioner eller tæt tilknyttede enheder, f.eks. forsvarsministeriet.

Nationalt CSIRT
Fokus
Et CSIRT med et nationalt fokus, der anses for at være et sikkerhedskontaktpunkt for et land. I nogle tilfælde fungerer det statslige CSIRT også som et nationalt kontaktpunkt (som UNIRAS i Det Forenede Kongerige).

Konstituenter
Denne type CSIRT har normalt ikke direkte konstituenter, da det nationale CSIRT kun spiller en formidlende rolle for hele landet.

CSIRT for små og mellemstore virksomheder (smv'er)

Fokus
Et selvorganiseret CSIRT, der leverer sine tjenester til sin egen branche eller sine egne brugergrupper.

Konstituenter
Disse CSIRT'ers konstituenter kan være smv'er og deres medarbejdere eller særlige interessegrupper som et lands sammenslutning af byer og kommuner.

Leverandør-CSIRT
Fokus
Et leverandør-CSIRT fokuserer på support i forbindelse med leverandørspecifikke produkter. Formålet med det er normalt at udvikle og levere løsninger for at fjerne sårbarheder og mindske de potentielle negative virkninger af smuthuller.

Konstituenter
Produktejere

Som beskrevet i afsnittet om de nationale CSIRT'er er det muligt for et team at betjene mere end én sektor. Det betyder noget for f.eks. analysen af konstituenterne og deres behov.

Det fiktive CSIRT (trin 1)
Startfase I startfasen planlægges det nye CSIRT som et internt CSIRT, der leverer tjenester til værtsvirksomheden, den lokale it-afdeling og medarbejderne. Det støtter og koordinerer også håndteringen af it-sikkerhedsrelaterede hændelser mellem de forskellige lokalafdelinger.

5.2 Mulige tjenester, et CSIRT kan levere

Vi har taget de første tro skridt

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?

>> Næste trin er at svare på spørgsmålet, *hvilke tjenester skal der leveres til konstituenterne?*

Et CSIRT kan levere mange tjenester, men indtil videre er der ingen eksisterende CSIRT, som leverer dem alle. Så det er en afgørende beslutning at udvælge de relevante tjenester. Nedenfor findes en kort oversigt over alle kendte CSIRT-tjenester, som de defineres i håndbogen for CSIRT'er "Handbook for CSIRT's", der er udgivet af CERT/CC[6].

[6] CERT/CC CSIRT handbook http://www.cert.org/archive/pdf/csirt-handbook.pdf

Reaktive tjenester	**Proaktive tjenester**	**Håndtering af artefakter**
• **Varslinger og advarsler** • **Håndtering af sikkerhedshændelser** • **Analyse af hændelser** • **Support til incident response** • **Koordinering af incident response** • Incident response på stedet • Håndtering af sårbarhed • Analyse af sårbarhed • Respons mod sårbarhed • Koordinering af responsen mod sårbarhed	• **Meddelelser** • Teknologiovervågning • Sikkerhedsaudit eller -vurdering • Konfiguration og vedligeholdelse af sikkerhed • Udvikling af sikkerhedsværktøjer • Tjenester til detektering af uautoriseret adgang • Formidling af sikkerhedsrelateret information	• *Artefaktanalyse* • *Artefaktrespons* • *Koordinering af artefaktrespons* ***Sikkerhedskvalitetsstyring*** • *Risikoanalyse* • *Fortsættelse af driften og genetablering efter en katastrofe* • *Sikkerhedsrådgivning* • *Bevidstgørelse* • *Uddannelse/Træning* • *Produktevaluering eller -certificering*

Fig. 1 Liste over CSIRT-tjenester fra CERT/CC[7].

Kernetjenester (fremhævet med fed): der skelnes mellem reaktive og proaktive tjenester. Proaktive tjenester sigter mod at forebygge sikkerhedshændelser gennem bevidstgørelse og uddannelse, mens reaktive tjenester sigter mod at håndtere sikkerhedshændelser og mindske den deraf følgende skade.

Artefakthåndtering omfatter analyse af en fil eller et objekt, der findes på et system, og som måske indgår i ondsindede handlinger såsom rester af vira, orme, scripts, trojanske heste osv. Den omfatter også håndtering og distribution af oplysningerne til leverandører og andre interesserede parter for at forebygge en yderligere spredning af ondsindet software og for at mindske risiciene.

Sikkerheds- og kvalitetsstyringstjenester er tjenester med mere langsigtede mål og omfatter rådgivning og uddannelsesforanstaltninger.

Se tillægget for at få en detaljeret forklaring af CSIRT-tjenesterne.

Det er et vigtigt skridt at vælge de rette tjenester til dine konstituenter, og det vil blive behandlet nærmere i kapitel 6.1. *Definition af den finansielle model*.

De fleste CSIRT'er begynder med at udsende "varslinger og advarsler", udarbejde "meddelelser" og levere "håndtering af sikkerhedshændelser" for deres konstituenter. Disse kerneydelser giver normalt en god profil og har en opmærksomhedsskabende værdi hos konstituenterne og anses hovedsagelig som reel "merværdi".

[7] Liste over CSIRT-tjenester fra CERT/CC: http://www.cert.org/CSIRT's/services.html

Det er en god ide at starte med en lille gruppe "pilotkonstituenter", levere kerneydelserne i en pilotperiode og herefter anmode om feedback.
Interesserede pilotbrugere giver sædvanligvis konstruktiv feedback og hjælper med at udvikle skræddersyede tjenester.

Det fiktive CSIRT (trin 2)
Valg af de rette ydelser I startfasen bliver det besluttet, at det nye CSIRT især skal fokusere på at levere nogle af kerneydelserne til medarbejderne. Det bliver besluttet, at man efter en pilotfase kan overveje at udvide ydelsesporteføljen og måske tilføje nogle "sikkerhedsstyringstjenester". Den beslutning vil blive truffet på grundlag af feedback fra pilotkonstituenterne og i nært samarbejde med kvalitetssikringsafdelingen.

5.3 Konstituentanalyse og mission statement

Vi har taget de første tre skridt:

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?

>> Det næste skridt er at svare på spørgsmålet, *hvilken fremgangsmåde skal vi vælge for at starte CSIRT'et?*

Det næste skridt er at se nøjere på konstituenterne med det hovedformål at vælge de rette kommunikationskanaler:

- definition af kommunikationsstrategien i forhold til konstituenterne
- formulering af mission statement
- udarbejdelse af en realistisk gennemførelses-/projektplan
- definition af CSIRT-tjenesterne
- fastlæggelse af organisationsstruktur
- opstilling af informationssikkerhedspolitik
- ansættelse af de rette medarbejdere
- anvendelse af CSIRT-kontor
- vurdering af samarbejdsmuligheder mellem andre CSIRT'er og mulige nationale initiativer

Disse skridt vil blive beskrevet nærmere i de følgende afsnit og kan bruges som inspiration til forretnings- og projektplanen.

5.3.1 Kommunikationsstrategi i forhold til konstituenterne

Det er som nævnt meget vigtigt at kende både konstituenternes behov og sin egen kommunikationsstrategi, bl.a. hvilke kommunikationskanaler der er de mest hensigtsmæssige for at få information ud til dem.

Ledelsesteorien rummer flere mulige metoder til at analysere en målgruppe. I dette dokument vil vi beskrive to af dem: SWOT- og PEST-analysen.

SWOT-analyse
En SWOT-analyse er et strategisk planlægningsværktøj, der bruges til at vurdere styrker (**S**trengths), svagheder (**W**eaknesses), muligheder (**O**pportunities) og trusler (**T**hreats) i forbindelse med et projekt eller etablering af en virksomhed eller i alle andre situationer, der kræver en beslutning. Teknikken tilskrives Albert Humphrey, der ledede et forskningsprojekt ved Stanford University i 1960'erne og 1970'erne og anvendte data fra virksomheder på Fortune 500-listen.[8]

Styrker	**Svagheder**
Muligheder	**Trusler**

Fig. 2 SWOT-analyse

[8] SWOT-analyse på Wikipedia: http://da.wikipedia.org/wiki/SWOT-analyse

PEST-analyse

PEST-analysen er et andet vigtigt og udbredt værktøj til at analysere konstituenter med det formål at forstå de politiske (**P**olitical), økonomiske (**E**conomic), sociokulturelle (**S**ocio-cultural) og teknologiske (**T**echnological) forhold, et CSIRT opererer under. Den vil bidrage til at fastslå, hvorvidt planlægningen stadig er i overensstemmelse med miljøet og hjælper formentlig til at undgå, at der træffes foranstaltninger ud fra de forkerte formodninger.

Politiske	**Økonomiske**
• Økologiske/miljømæssige spørgsmål • Nuværende lovgivning hjemmemarked • Fremtidig lovgivning • Europæisk/international lovgivning • Tilsynsorganer og -processer • Statslige politikker • Regeringsperiode og -ændring • Handelspolitikker • Finansiering, bevillinger og initiativer • Hjemmemarked lobbying/pressionsgrupper • Internationale pressionsgrupper	• Den nationale økonomiske situation • Nationale økonomiske tendenser • Oversøiske økonomier og tendenser • Generelle beskatningsspørgsmål • Særlig beskatning af produkt/tjenesteydelse • Sæsonbetonethed/vejrproblemer • Markeds- og handelscykler • Særlige erhvervsfaktorer • Markedsveje og distributionstendenser • Drivkræfter hos kunder/slutbrugere • Rente- og valutakurser
Sociale	**Teknologiske**
• Livsstilstendenser • Demografi • Kundeholdninger og -meninger • Mediernes synspunkter • Lovændringer, der påvirker sociale faktorer • Brand-, virksomheds-, teknologiimage • Kundernes indkøbsmønstre • Mode og rollemodeller • Større begivenheder og påvirkninger • Købsadgang og -tendenser • Etniske/religiøse faktorer • Annoncering og reklame	• Konkurrerende teknologiudvikling • Forskningsfinansiering • Tilknyttede/afhængige teknologier • Erstatningsteknologi/-løsninger • Teknologimodenhed • Fremstillingsmodenhed og -kapacitet • Information og kommunikation • Kundernes købsmekanismer/-teknologi • Teknologilovgivning • Innovationspotentiale • Teknologiadgang, licenser, patenter • Spørgsmål om intellektuel ejendomsret

Fig. 3 PEST-analysemodel.

En deltaljeret beskrivelse af PEST-analysen kan ses på Wikipedia[9].

Begge værktøjer giver et omfattende og velstruktureret overblik over, hvad konstituenternes behov er. Resultaterne vil supplere forretningsforslaget og hermed bidrage til at opnå finansiering til at oprette et CSIRT.

Kommunikationskanaler

Et vigtigt emne, der skal indgå i analysen, er mulige kommunikations- og informationsdistributionsmetoder (”Hvordan skal man kommunikere med konstituenterne?”).

[9] PEST-analyse på Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Hvis det er muligt, bør regelmæssige personlige besøg hos konstituenterne overvejes. Det er et faktum, at personlige møder letter samarbejdet. Hvis begge sider er villige til at arbejde sammen, vil disse møder føre til et mere åbent forhold.

Normalt bruger CSIRT'er en række kommunikationskanaler. Følgende har vist sig nyttige i praksis og er værd at overveje:

- offentligt websted
- lukket medlemsområde på et websted
- web-formularer til at rapportere sikkerhedshændelser
- mailinglister
- personlige e-mail
- telefon/telefax
- sms
- "gammeldags" papirbreve
- månedlige eller årlige rapporter

De fleste CSIRT'er bruger e-mail, web-formularer, telefon eller fax til at lette håndteringen af sikkerhedshændelser (for at modtage hændelsesrapporter fra konstituenterne, koordinere med andre team eller give feedback og support til ofret), og derudover udgiver de deres sikkerhedsbulletiner på et offentligt tilgængeligt websted og via en mailingliste.

! Information bør om muligt distribueres på en sikker måde. En e-mail kan f.eks. underskrives digitalt med PGP, og følsomme data om hændelser bør altid sendes krypteret.

For yderligere oplysninger jf. kapitel 8.5 *Tilgængelige CSIRT-værktøjer*. Se også kapitel 2.3 i *RFC2350*[10].

Det fiktive CSIRT (trin 3a)
Udarbejdelse af en analyse af konstituenterne og de relevante kommunikationskanaler En brainstorm med nogle centrale personer fra ledelsen og konstituenterne gav tilstrækkeligt input til en SWOT-analyse. Det førte til den konklusion, at der er behov for kerneydelserne: • varslinger og advarsler • håndtering af sikkerhedshændelser (analyse, responssupport og koordinering af respons) • meddelelser Der skal sikres en velorganiseret distribution, så informationen når ud til den størst mulige del af konstituenterne. Derfor tager man den beslutning, at varslinger, advarsler og meddelelser i form af sikkerhedsbulletiner skal offentliggøres på et dedikeret websted

[10] http://www.ietf.org/rfc/rfc2350.txt

og distribueres via en mailingliste. CSIRT faciliterer e-mail, telefon og telefax til at modtage rapporter om sikkerhedshændelser. Der planlægges en samlet web-formular til næste trin.

Se et eksempel på en SWOT-analyse på næste side.

Styrker • Der er et vist kendskab i virksomheden. • De kan lide planen og er villige til at samarbejde. • Støtte og finansiering fra direktionen	**Svagheder** • Ikke megen kommunikation mellem de forskellige afdelinger og lokalafdelinger • Ingen koordinering med it-hændelser • Mange ”små afdelinger”
Muligheder • Enorm strøm af ikke-strukturerede sårbarheds-informationer • Stærkt behov for koordinering • Nedbringelse af tab som følge af hændelser • Mange løse ender i forbindelse med it-sikkerhed • Uddannelse af medarbejdere i it-sikkerhed	**Trusler** • Ikke mange penge til rådighed • Ikke mange medarbejdere • Høje forventninger • Kultur

Fig. 4 Eksempel på SWOT-analyse.

5.3.2 Mission statement

Efter at have analyseret konstituenternes behov for og ønsker til CSIRT-tjenester bør næste skridt være at udfærdige en mission statement.

En mission statement beskriver organisationens grundlæggende funktion i samfundet med hensyn til de produkter og tjenesteydelser, den leverer til sine konstituenter. Den gør det muligt at kommunikere det nye CSIRT's eksistens og funktion klart og tydeligt.

Det er en god ide at gøre sin mission statement kompakt, men ikke for stram, for den vil normalt forblive uændret i nogle år.

Her er nogle eksempler på mission statements fra fungerende CSIRT'er:

"<Navn på CSIRT> giver information og yder bistand til sine <konstituenter (definer dine konstituenter)> ved at gennemføre proaktive foranstaltninger for at nedbringe risici for it-sikkerhedshændelser samt ved at reagere på disse hændelser, når de opstår.

"At yde support til <Konstituenter> i forbindelse med forebyggelse af og respons på it-relaterede sikkerhedshændelser[11]*.*
Det er et meget vigtigt og nødvendigt skridt at starte med sin mission statement. Se en mere detaljeret beskrivelse af, hvilke informationer et CSIRT bør offentliggøre, i kapitel *2.1 i RFC2350*[12].

Det fiktive CSIRT (trin 3b)
Ledelsen af det fiktive CSIRT har udarbejdet følgende mission statement: *"Det fiktive CSIRT leverer information og bistand til medarbejderne i sin værtsvirksomhed for at nedbringe risici for it-sikkerhedshændelser og reagere på sådanne hændelser, når de opstår."* Hermed gør det fiktive CSIRT det klart, at det er et internt CSIRT, og at dets kerneopgave er at varetage spørgsmål i forbindelse med it-sikkerhed.

[11] Mission statement fra Govcert.ni: http://www.govcert.nl

[12] http://www.ietf.org/rfc/rfc2350.txt

6 Udarbejdelse af forretningsplan

Vi har taget følgende skridt:

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?
4. Analyse af miljø og konstituenter
5. Formulering af mission statement

>> Det næste skridt er at definere forretningsplanen.

Resultatet af analysen giver et godt overblik over konstituenternes behov og (formodede) svagheder, så det bruges som input til det næste skridt.

6.1 Definition af den finansielle model

Efter analysen blev der valgt nogle kerneydelser til at begynde med. Det næste skridt er at se på den finansielle model: hvilke serviceparametre er både egnede og rentable?

I en perfekt verden ville finansieringen blive tilpasset konstituenternes behov, men i virkeligheden skal den portefølje af tjenesteydelser, der kan leveres, tilpasses et givet budget. Så det er mere realistisk at begynde med planlægningen af den finansielle side af sagen.

6.1.1 Omkostningsmodel

De to vigtigste faktorer, der påvirker omkostningerne, er fastlæggelsen af tjenestetid og antallet af medarbejdere, der skal ansættes (og disses kvalitet). Er der behov for incident response og teknisk support 24x7, eller skal disse tjenester kun ydes inden for almindelig kontortid?

Alt efter den ønskede tilgængelighed og kontorudstyret (er det f.eks. muligt at arbejde hjemmefra?) kan det være en fordel at arbejde med en tilkaldevagtplan eller en fast vagtplan.

Et muligt scenario er at levere både proaktive og reaktive tjenester inden for almindelig kontortid. Uden for kontortid vil der kun blive leveret begrænsede tjenester af medarbejdere med tilkaldevagt, f.eks. kun i tilfælde af større katastrofer og sikkerhedshændelser.

En anden mulighed er at se på internationalt samarbejde mellem andre CSIRT-team. Der er allerede eksempler på fungerende samarbejde, der ”følger solen”. F.eks. har samarbejde mellem europæiske og asiatiske team vist sig fordelagtige og har været en god måde at dele hinandens kapacitet på. F.eks. leverer Sun Microsystems’ CSIRT, der har mange lokalafdelinger i forskellige tidszoner rundt omkring i verden (men alle er

medlemmer af samme CSIRT-team), 24x7-tjenester ved konstant at have vagtskifter mellem teamene over hele verden. Det begrænser faktisk omkostningerne, fordi teamene altid kun arbejder inden for normal kontortid og også leverer tjenesteydelser til den "sovende del" af verden.

Det er en god ide navnlig at analysere konstituenternes behov for 24x7-tjenester til bunds. Varslinger og advarsler, der udsendes om natten, er ikke til megen gavn for modtageren, der først læser dem om morgenen. Der er forskel på at "have behov for en tjeneste" og "ønske en tjeneste", men især arbejdstiden gør en stor forskel på, hvor mange medarbejdere og faciliteter der er nødvendige, og har dermed store følger for omkostningsmodellen.

6.1.2 Indtægtsmodel

Når man kender omkostningerne, er det godt som næste skridt at tænke på de mulige indtægtsmodeller: hvordan kan de planlagte tjenesteydelser finansieres? Her er nogle mulige scenarier til vurdering:

Anvendelse af eksisterende ressourcer
Det kan altid betale sig at vurdere de ressourcer, der allerede er til stede i andre dele af virksomheden. Er der allerede egnede medarbejdere ansat (f.eks. i den eksisterende it-afdeling) med den nødvendige baggrund og ekspertise? Der kan formentlig laves aftaler med ledelsen om at udlåne disse medarbejdere til CSIRT i startfasen, eller de kan yde støtte til CSIRT på ad hoc-basis.

Medlemsgebyr
En anden mulighed er at sælge sine tjenesteydelser til konstituenterne mod et medlemsgebyr, der betales årligt eller hvert kvartal. Supplerende ydelser kan betales efter brug, f.eks. konsulenttjenester eller sikkerhedsauditter.

Et andet muligt scenario: ydelser til de (interne) konstituenter leveres gratis, mens der betales for ydelser til eksterne kunder. En anden ide er at offentliggøre sikkerheds- og informationsbulletiner på det offentlige websted og have en sektion "Kun for medlemmer" med særlig, mere detaljeret eller skræddersyet information.

Det er i praksis bevist, at "abonnement pr. CSIRT-ydelse" kun i begrænset omfang sikrer tilstrækkelig finansiering, især i startfasen. Der er f.eks. faste grundomkostninger til teamet og udstyret, som skal forudbetales. Det er vanskeligt at finansiere disse omkostninger ved at sælge CSIRT-ydelser, og det kræver en meget detaljeret finansiel analyse at finde "balancepunktet".

Støtte
En anden mulighed, der er værd at overveje, kunne være at ansøge om projektstøtte fra regeringen eller et statsligt organ, da de fleste lande nu om dage har midler til it-sikkerhedsprojekter. Det kan være en god begyndelse at kontakte indenrigsministeriet.

Det er naturligvis muligt at blande de forskellige indtægtsmodeller.

6.2 Fastlæggelse af organisationsstruktur

Hvilken organisationsstruktur der er egnet for et CSIRT, afhænger i høj grad af værtsorganisationens og konstituenternes eksisterende struktur. Den afhænger også af, hvor let det er at få kompetente eksperter ansat fast eller på ad hoc-basis.

Et typisk CSIRT definerer følgende roller inden for teamet:

Overordnet
- direktør

Medarbejdere
- kontorchef
- bogholder
- kommunikationskonsulent
- juridisk konsulent

Driftsteknisk team
- teknisk teamleder
- teknikere med speciale i CSIRT, der leverer CSIRT-ydelserne
- forskere

Eksterne konsulenter
- ansættes efter behov

Det er særdeles nyttigt at have en juridisk ekspert på holdet, især i CSIRT's startfase. Det øger omkostningerne, men vil i sidste ende spare tid og juridisk besvær.

Alt efter hvor forskelligartet ekspertise konstituenterne selv har til rådighed, men også når CSIRT har en høj medieprofil, har det vist sig meget nyttigt også at have en kommunikationsekspert i teamet. Disse eksperter kan fokusere på at oversætte vanskelige tekniske problemer til mere forståelige budskaber til konstituenter eller mediepartnere. Kommunikationseksperten kan også give feedback fra konstituenterne til de tekniske eksperter, så han/hun kan fungere som "oversætter" og "formidler" mellem disse to grupper.

Her følger nogle få eksempler på organisationsmodeller, der bruges af fungerende CSIRT'er.

6.2.1 Den uafhængige forretningsmodel

CSIRT oprettes og fungerer som en uafhængig organisation med sin egen ledelse og egne medarbejdere.

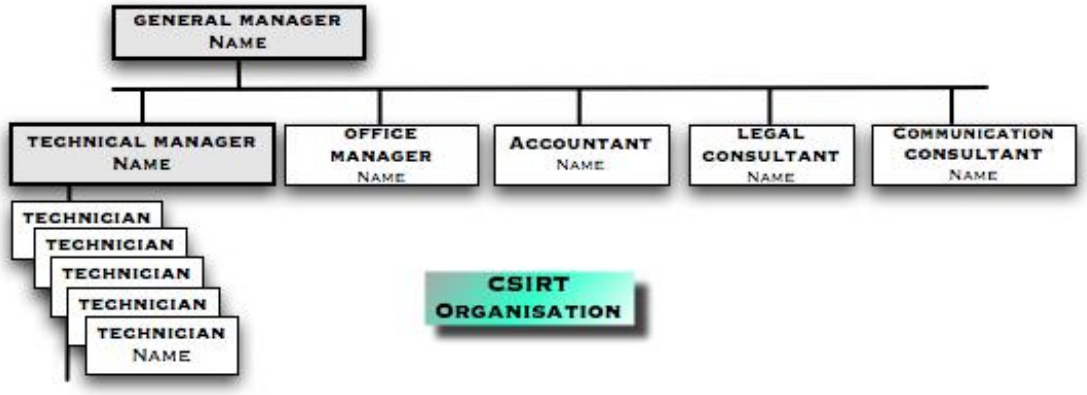


Fig. 5 Uafhængig forretningsmodel.

6.2.2 Den indbyggede model

Denne model kan bruges, hvis der skal oprettes et CSIRT inden for en eksisterende organisation, f.eks. ved at bruge en eksisterende it-afdeling. CSIRT ledes af en teamleder, der får ansvar for CSIRT-aktiviteterne. Teamlederen samler de nødvendige teknikere, når der skal løses problemer med sikkerhedshændelser eller arbejdes med CSIRT-aktiviteter. Han/hun kan anmode om ekspertbistand hos den eksisterende organisation.

Denne model kan også tilpasses særlige situationer, når de opstår. I så fald får teamet tildelt et fast antal ansatte eller et antal omregnet til fuldtidsbeskæftigede. Det er helt bestemt et fuldtidsjob for én eller (i de fleste tilfælde) mere end én fuldtidsbeskæftiget at passe en ”abuse desk” hos f.eks. en internetudbyder.

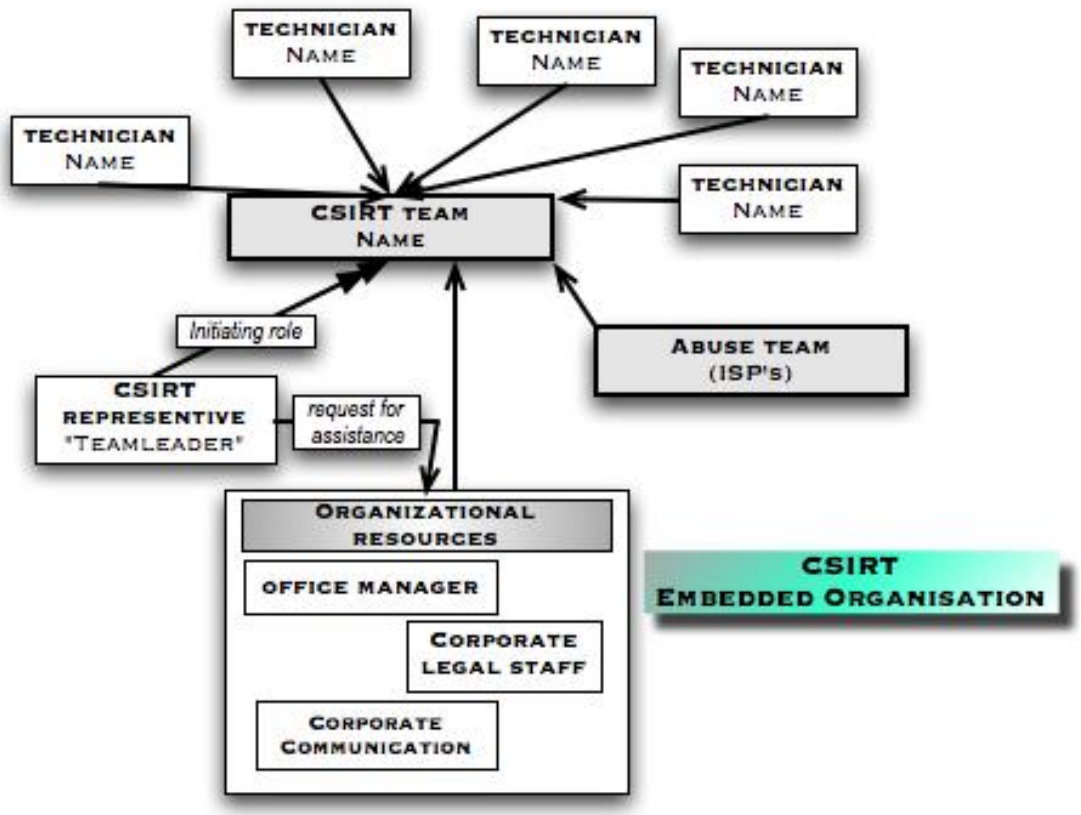


Fig. 6 Organisatorisk indbygget model.

6.2.3 Campus-modellen

Campus-modellen bruges, som navnet antyder, mest af akademiske og forskningsrelaterede CSIRT'er. De fleste akademiske institutioner og forskningsorganisationer består af flere universiteter og campus-faciliteter forskellige steder, spredt ud over en region eller endog hele landet (som i tilfældet med de nationale forskningsnet, NREN (National Research Networks). Disse organisationer er normalt uafhængige af hinanden, og de driver ofte deres eget CSIRT. Disse CSIRT'er er normalt organiseret under et "moder-CSIRT" eller centralt CSIRT. Det centrale CSIRT varetager koordinationen og er det eneste kontaktpunkt for verden udenfor. I de fleste tilfælde vil det centrale CSIRT også yde centrale CSIRT-tjenester og udsende information om hændelser til det relevante campus-CSIRT.

Nogle CSIRT'er udveksler deres centrale CSIRT-tjenester med de øvrige campus-CSIRT'er, hvilket giver lavere faste omkostninger for det centrale CSIRT.

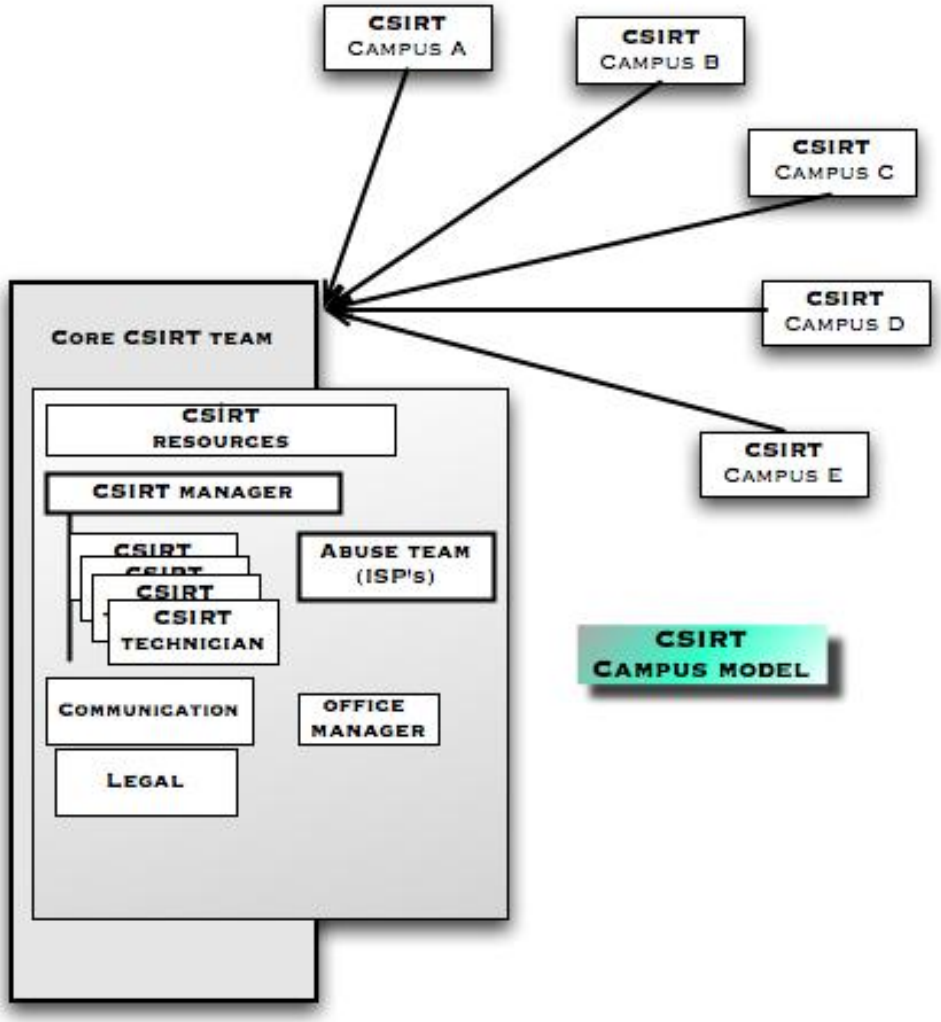


Fig. 7 Campus-modellen.

6.2.4 Den frivillige model

Denne organisationsmodel beskriver en gruppe mennesker (specialister), der går sammen for at yde rådgivning og support til hinanden (og andre) på frivillig basis. Det er et løst fællesskab, som er særdeles afhængigt af deltagernes motivation.

Denne model bruges f.eks. af WARP-fællesskabet[13].

6.3 Ansættelse af de rette medarbejdere

Når man har besluttet, hvilke tjenester og hvilket support-niveau der skal leveres, og har valgt en organisationsmodel, er næste skridt at finde den rette mængde kvalificerede personer til jobbet.

Det er næsten umuligt at sige præcist, hvor mange tekniske medarbejdere der er brug for, men følgende nøgleværdier har vist sig at være nyttige:

- For at levere to kerneydelser, nemlig udsendelse af rådgivende bulletiner samt håndtering af hændelser: minimum **4** FTE.
- Til et fuldservice-CSIRT i almindelig kontortid og vedligeholdelse af systemer: minimum **6-8** FTE.
- Til et fuldt bemandet 24x7-skift (2 skift uden for kontortid) er minimum ca. **12** FTE.

Disse tal omfatter også dubleringer i tilfælde af sygdom, ferier osv. Det er også nødvendigt at tjekke de lokale kollektive overenskomster. Hvis folk arbejder uden for kontortid, kan det føre til ekstra omkostninger i form af ekstra godtgørelse.

[13] WARP-initiativet http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#12

Her følger en kort oversigt over nøglekompetencer for de tekniske eksperter i et CSIRT

Punkter til jobbeskrivelse for generelle tekniske medarbejdere:

Personlige kompetencer

- fleksibel, kreativ og en god samarbejdsånd
- stærke analytiske færdigheder
- evne til at forklare vanskelige tekniske problemer i et let sprog
- en god fornemmelse for fortrolighed og for at arbejde procesorienteret
- gode organisatoriske færdigheder
- modstandsdygtig over for stress
- solide kommunikative evner og skrivefærdigheder
- åben og villig til at lære

Tekniske kompetencer

- bredt kendskab til internetteknologi og protokoller
- kendskab til Linux- og Unix-systemer (alt efter konstituenternes udstyr)
- kendskab til Windows-systemer (alt efter konstituenternes udstyr)
- kendskab til netværksinfrastrukturudstyr (router, switches, DNS, proxy, mail osv.)
- kendskab til internet-applikationer (SMTP, http'er, FTP, telnet, SSH, osv.)
- kendskab til sikkerhedstrusler (DDoS, Phishing, Defacing, sniffing, osv.)
- kendskab til risikovurdering og praktiske gennemførelser

Supplerende kompetencer

- villig til at arbejde 24x7 eller med tilkaldevagt (alt efter servicemodellen)
- maksimal afstand til arbejde (hvis man skal kunne være på kontoret med kort varsel, maksimal rejsetid)
- uddannelsesniveau
- erfaring med at arbejde på it-sikkerhedsområdet

Det fiktive CSIRT (trin 4)

Udarbejdelse af forretningsplan

Finansiel model

Da virksomheden har 24x7 e-business og også har en 24x7 it-afdeling, bliver det besluttet at yde fuld service i kontortiden og have en tilkaldevagt uden for kontortid. Ydelserne til konstituenterne bliver leveret gratis, men muligheden for at levere ydelser til eksterne kunder vil blive vurderet i pilot- og evalueringsfasen.

Indtægtsmodel

I start- og pilotfasen vil CSIRT blive finansieret gennem værtsvirksomheden. I pilot- og evalueringsfasen vil der blive drøftet supplerende finansiering, bl.a. muligheden for at sælge tjenesteydelser til eksterne kunder.

Organisationsmodel

Værtsorganisationen er en lille virksomhed, så derfor vælger man den indbyggede model.

I kontortiden vil en medarbejderstab på tre levere kerneydelserne (udsendelse af sikkerhedsbulletiner og håndtering/koordinering af hændelser).

Virksomhedens it-afdeling beskæftiger allerede mennesker med egnede kvalifikationer. Der indgås en aftale med it-afdelingen, således at det nye CSIRT kan anmode om støtte på ad hoc-basis, når der er behov for det. Deres tilkaldeteknikere i anden række kan også bruges.
Der bliver et kerne-CSIRT-team med fire fuldtidsansatte og fem supplerende CSIRT-teammedlemmer. Et af medlemmerne er også til rådighed på roterende skift.

Medarbejdere
CSIRT-teamlederen har erfaring med sikkerhed og support på 1. og 2. niveau og har udført arbejde inden for resiliens og krisestyring. De tre andre teammedlemmer er sikkerhedsspecialister. De CSIRT-teammedlemmer fra it-afdelingen, der arbejder på deltid, er specialister i hver deres del af virksomhedens infrastruktur.

6.4 Anvendelse og udstyring af kontoret

Udstyring og anvendelse af kontorområdet og den fysiske sikkerhed er meget brede emner, og der kan derfor ikke gives nogen udtømmende beskrivelse i dette dokument. Dette kapitel har til formål at give et kort overblik over emnet.

Der kan fås mere information om fysisk sikkerhed på:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

"Sikring af bygningen"
Da CSIRT'er normalt håndterer meget følsomme oplysninger, er det en god ide at lade teamet kontrollere kontorets fysiske sikkerhed. Den vil afhænge meget af de eksisterende faciliteter og infrastruktur og af værtsvirksomhedens eksisterende informationssikkerhedspolitik.

Regeringsmyndigheder arbejder f.eks. med klassificeringsordninger og ser meget strengt på, hvordan fortrolige oplysninger skal håndteres. Tjek lokale regler og politikker hos din virksomhed eller institution.

Normalt er et nyt CSIRT afhængig af samarbejdet med sin værtsorganisation for at lære om lokale regler, politikker og andre juridiske spørgsmål.

En udtømmende beskrivelse af alt det udstyr og alle de sikkerhedsforanstaltninger, der er nødvendige, ligger uden for dette dokuments rammer. Nedenfor følger dog en kort liste over dit CSIRT's grundlæggende faciliteter:

Generelle regler for bygningen
- brug adgangskontroller
- sørg for, at der i hvert fald til CSIRT-kontoret kun er adgang for CSIRT-medarbejdere
- overvåg kontorer og indgange med kameraer
- arkiver fortrolig information i aflåste skabe eller bokse
- brug sikre it-systemer

Generelle regler for it-udstyr
- brug udstyr, som medarbejderne kan supporte
- styrk alle systemer
- patch og opdater alle systemer, før de logges på internettet
- brug sikkerhedssoftware (firewalls, mange antivirusscannere, anti-spyware osv.)

Opretholdelse af kommunikationskanaler
- offentligt websted
- lukket medlemsområde på webstedet
- web-formularer til at rapportere sikkerhedshændelser
- e-mail (PGP / GPG / S/MIME support)
- software til mailingliste
- hav et dedikeret telefonnummer til konstituenterne:
    - telefon
    - fax
    - sms

Registrer tracking-system(er)
- kontaktdatabase med oplysninger om teammedlemmer, andre team osv.
- CRM-værktøjer
- billetsystem til hændelseshåndtering

Brug "virksomhedens stil" fra begyndelsen til
- layout til standard e-mail og rådgivende bulletin
- "gammeldags" papirbreve
- månedlige eller årlige rapporter
- blanket til rapportering af hændelser

Andre spørgsmål
- sørg for at kunne kommunikere uden for båndet i tilfælde af angreb
- sørg for at have flere internettilslutninger

Se yderligere oplysninger om specifikke CSIRT-værktøjer i kapitel 8.5 *Tilgængelige CSIRT-værktøjer*.

6.5 Udvikling af en informationssikkerhedspolitik

Man skal have en informationssikkerhedspolitik, der passer til det CSIRT, man opretter. Ud over at beskrive de ønskede operationelle og administrative processer og procedurer skal en sådan politik være i overensstemmelse med lovgivning og standarder, især med hensyn til CSIRT'ets ansvar. CSIRT er normalt bundet af nationale love og regler, der ofte gennemføres inden for rammerne af EU-lovgivningen (sædvanligvis direktiver) og andre internationale aftaler. Standarder er ikke nødvendigvis direkte bindende, men kan være påbudt eller anbefalet ved love og regler.

Nedenfor følger en kort liste over mulige love og politikker:

Nationale
- forskellige love om informationsteknologi, telekommunikation, medier
- love om databeskyttelse og privatlivets fred
- love og regler om dataopbevaring
- lovgivning om finans- og regnskabsforhold samt virksomhedsledelse
- adfærdskodekser for "corporate governance" og it-forvaltning

Europæiske
- direktiv om elektroniske signaturer (1999/93/EF)
- direktiver om databeskyttelse (1995/46/EF) og privatlivets fred i elektronisk kommunikation (2002/58/EF)
- direktiver om elektroniske kommunikationsnet og -tjenester (2002/19/EF-2002/22/EF)
- direktiver om selskabsret (f.eks. det 8. selskabsretsdirektiv)

Internationale
- Basel II-aftalen (især med hensyn til styring af driftsrisiko)
- Europarådets konvention om it-kriminalitet
- Europarådets konvention om menneskerettigheder (artikel 8 om privatlivets fred)
- internationale regnskabsstandarder (IAS, som til en vis grad påbyder it-kontrol)

Standarder
- British Standard BS 7799 (informationssikkerhed)
- internationale standarder ISO2700x (informationssikkerhedsstyringssystemer)
- den tyske IT-Grundschutzbuch, den franske EBIOS og andre nationale variationer

Spørg din juridiske rådgiver til råds for at fastslå, om dit CSIRT overholder national og international lovgivning.

De mest grundlæggende spørgsmål, dine informationshåndteringspolitikker skal besvare, er:

- Hvordan "tagges" eller "klassificeres" indkommende information?
- Hvordan håndteres information, især med hensyn til eneret?

- Hvilke overvejelser skal der gøres med hensyn til offentliggørelse af information, især hvis information i forbindelse med en hændelse videregives til andre team eller virksomheder?
- Er der juridiske forhold, der skal tages hensyn til i forbindelse med informationshåndtering?
- Har du en politik for brug af kryptografi til beskyttelse af eneret og integritet i arkiver og/eller datakommunikation, især e-mail?
- Omfatter denne politik mulige betingelser for juridiske grænser såsom nøgledeponering eller håndhævelse af dekryptering i tilfælde af retssager?

Det fiktive CSIRT (trin 5)

Kontorudstyr og placering

Eftersom værtsvirksomheden allerede har en effektiv fysisk sikkerhed på plads, er det nye CSIRT godt dækket ind i den retning. Der indrettes et såkaldt "kommandorum", hvor koordineringen kan foregå i tilfælde af en nødsituation. Der indkøbes en boks til krypteringsmateriale og følsomme dokumenter. Der blev etableret en separat telefonlinje med et omstillingsbord til facilitering af en hotline i kontortiden og tilkaldevagtens mobiltelefon uden for kontortid med samme telefonnummer.

Det eksisterende udstyr og virksomhedens websted til CSIRT-relaterede meddelelser kan også bruges. Der installeres og vedligeholdes en mailingliste med en begrænset del til kommunikation mellem teammedlemmerne og med andre team. Alle kontaktoplysninger om medarbejderne lagres i en database, og en udskrift opbevares i boksen.

Regler

Da CSIRT er indbygget i en virksomhed, der allerede har informationssikkerhedspolitikker, er de tilsvarende politikker for CSIRT blevet udarbejdet med hjælp fra virksomhedens juridiske rådgiver.

6.6 Muligheder for samarbejde med andre CSIRT'er og eventuelle nationale initiativer

Vi har allerede nogle gange i dette dokument nævnt, at der findes andre CSIRT-initiativer, og at der er et stærkt behov for samarbejde mellem dem. Det er en god ide at kontakte andre CSIRT'er så tidligt som muligt for at få den nødvendige kontakt med CSIRT-fællesskaberne. Normalt er andre CSIRT'er meget åbne over for at hjælpe nyoprettede team med at komme i gang.

ENISA's *Inventory of CERT activities in Europe*[14] (oversigt over CERT-aktiviteter i Europa) er et godt udgangspunkt for søgningen efter andre CSIRT'er i landet eller efter nationale CSIRT-samarbejdsaktiviteter.

Hvis du ønsker hjælp til at finde en egnet kilde til CSIRT-information, kan du kontakte ENISA's CSIRT-eksperter:

CERT-Relations@enisa.europa.eu

[14] ENISA's oversigt: http://www.enisa.europa.eu/cert_inventory/

Her følger en oversigt over CSIRT-fællesskabsaktiviteter. Se en mere omfattende beskrivelse og yderligere oplysninger i oversigten, *Inventory*.

EU's CSIRT-initiativ

TF-CSIRT[15]
TF-CSIRT Task Force fremmer samarbejdet mellem CSIRT'er i Europa. Denne task forces hovedmål er at skabe et forum, hvor der kan udveksles erfaringer og viden, at oprette pilottjenester for europæiske CSIRT'er og bistå med oprettelse af nye CSIRT'er.

Task forcens vigtigste mål er:
- at skabe et forum for udveksling af erfaringer og viden
- at oprette pilottjenester til det europæiske CSIRT-fællesskab
- at fremme fælles standarder og procedurer for respons på sikkerhedshændelser
- at bistå ved oprettelse af nye CSIRT'er og uddannelse af CSIRT-medarbejdere
- aktiviteterne under TF-CSIRT fokuserer på Europa og nabolandene i overensstemmelse med kommissoriet, der blev godkendt af TERENA's tekniske udvalg den 15. september 2004.

Det globale CSIRT-initiativ

FIRST[16]
FIRST er den førende organisation og anerkendte globale leder inden for incident response. Medlemskab af FIRST giver et it-sikkerheds- og responseteam mulighed for at reagere mere effektivt på sikkerhedshændelser – reaktivt så vel som proaktivt.

FIRST samler mange forskellige CSIRT'er fra statslige og kommercielle organisationer samt uddannelsesinstitutioner. FIRST har til formål at skabe samarbejde om og koordinering af forebyggelse af sikkerhedshændelser, tilskynde til hurtig reaktion på sikkerhedshændelser og fremme informationsdeling blandt medlemmerne og fællesskabet som helhed.

FIRST danner et "trust network" i det globale incident response-fællesskab, men leverer derudover også værdiforøgende tjenester.

Det fiktive CSIRT (trin 6)
Muligheder for samarbejde Ved at bruge ENISA's Inventory hurtigt blev der fundet og kontaktet nogle CSIRT'er i samme land. Der blev aftalt et besøg hos et af dem for den nyansatte teamleder. Han hørte om nationale CSIRT-aktiviteter og deltog i et møde. Dette møde var særdeles nyttigt med hensyn til at indsamle eksempler på arbejdsmetoder og få støtte fra nogle andre team.

7 Fremme af forretningsplanen

[15] TF-CSIRT: http://www.enisa.europa.eu/cert_inventory/pages/04_01_02.htm#06

[16] FIRST: http://www.enisa.europa.eu/cert_inventory/pages/05_02.htm

Vi har indtil nu taget følgende skridt:

1. Forståelse af, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?
4. Analyse af miljø og konstituenter
5. Formulering af mission statement
6. Udvikling af forretningsplan
    a. Definere den finansielle model
    b. Definere organisationsstrukturen
    c. Begynde at ansætte medarbejdere
    d. Anvende og udstyre kontoret
    e. Udarbejde en informationssikkerhedspolitik
    f. Se på samarbejdspartnere

>> Det næste skridt er at indsætte ovenstående punkter i en projektplan og komme i gang!

En god start på formuleringen af dit projekt er at udarbejde en forretningsplan. Denne plan skal bruges som grundlag for projektplanen og skal også bruges til at søge om ledelsens støtte og få budget- eller andre ressourcer.

Det har vist sig nyttigt til stadighed at rapportere til ledelsen for at sikre en høj bevidsthed om it-sikkerhedsproblemer og dermed stadig støtte til eget CSIRT.

Planlægningen begynder med at analysere problemer og muligheder ved hjælp af en analysemodel, som beskrevet i kapitel *5.3 Konstituentanalyse*, og søge tæt kontakt til de potentielle konstituenter.

Som tidligere beskrevet er der meget at tænke på, når man starter et CSIRT. Det er bedst at justere ovenstående materiale efter CSIRT's behov i takt med udviklingen.

Ved rapportering til ledelsen er det en god ide at ajourføre sin egen plan så meget som muligt ved at bruge nye artikler fra aviser eller internettet og forklare, hvorfor en CSIRT-tjeneste og intern koordinering af sikkerhedshændelser er afgørende for sikre forretningsaktiver. Det er også nødvendigt at gøre det klart, at kun stadig support i it-sikkerhedsspørgsmål fører til en stabil forretning, især for en virksomhed eller en institution, der er afhængig af it.

(En berømt sætning af Bruce Schneier understreger denne pointe: *"Sikkerhed er ikke et produkt, men en proces*[17]*!"*)

Et berømt værktøj, der illustrerer sikkerhedsproblemer, er følgende figur fra CERT/CC:

[17] Bruce Schneier: http://www.schneier.com/

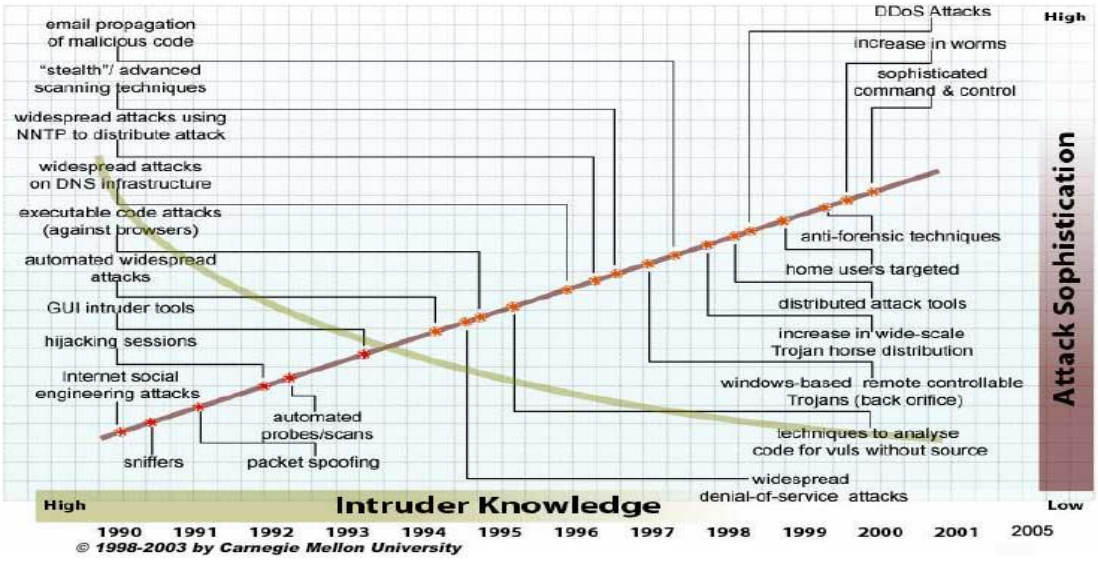


Fig. 8 Den indtrængendes viden i forhold til angrebsniveau (kilde CERT-CC[18])

Den viser tendenserne inden for it-sikkerhed, navnlig at det kræver stadigt mindre avancerede færdigheder at gennemføre stadigt mere avancerede angreb.

Det skal også nævnes, at der går stadigt kortere tid mellem det øjeblik, hvor softwareopdateringer til sårbarheder bliver tilgængelige, og angrebene mod dem bliver sat ind:

Patch -> Exploit		**Spredningstakt**	
Nimda:	11 måneder	Code red:	Dage
Slammer:	6 måneder	Nimda:	Timer
Nachi:	5 måneder	Slammer:	Minutter
Blaster:	3 uger		
Witty:	1 dag (!)		

Indsamlede data over sikkerhedshændelser, potentielle forbedringer og indhøstede erfaringer giver også en god præsentation.

[18] http://www.cert.org/archive/pdf/info-sec-ip.pdf

7.1 Beskrivelse af forretningsplaner og argumentation over for ledelsen

Et oplæg til ledelsen med en salgstale for CSIRT alene er ikke en forretningsplan, men hvis det gennemføres på passende vis, kan det i de fleste tilfælde føre til, at ledelsen støtter CSIRT. Planen skal på den anden side ikke kun opfattes som en ledelsesøvelse, men bør også bruges som kommunikation til teamet og konstituenterne. Udtrykket forretningsplan kan måske lyde meget kommercielt og langt væk fra den daglige CSIRT-praksis, men den sikrer fokus og styring, når man opretter et CSIRT.

Svarene på følgende spørgsmål kan bruges til at opstille en god forretningsplan (de anførte eksempler er hypotetiske og bruges kun som illustration). De "virkelige" svar afhænger i høj grad af de "virkelige" omstændigheder).

- Hvad er problemet?
- Hvad vil du gerne opnå med dine konstituenter?
- Hvad sker der, hvis du ikke gør noget?
- Hvad sker der, hvis du gør noget?
- Hvad vil det koste?
- Hvad kommer der ind?
- Hvornår starter du, og hvornår er det slut?

Hvad er problemet?
I de fleste tilfælde opstår ideen til at oprette et CSIRT, når it-sikkerhed er blevet en vital del af en virksomheds eller institutions kerneforretning, og når it-sikkerhedshændelser bliver en erhvervsrisiko, hvilket gør risikoreduktion til en normal forretningsoperation.

De fleste virksomheder eller institutioner har en regulær support-afdeling eller en helpdesk, men i de fleste tilfælde håndteres sikkerhedshændelser utilstrækkeligt og ikke så struktureret, som de burde. I de fleste tilfælde kræver arbejdet med sikkerhedshændelser særlige kvalifikationer og opmærksomhed. En mere struktureret fremgangsmåde vil også være gavnlig og vil mindske forretningsrisici og skader for virksomheden.

Problemet er i de fleste tilfælde, at der mangler koordinering, og at den eksisterende viden ikke bruges til at håndtere sikkerhedshændelser, hvilket ellers kunne forhindre, at de skete i fremtiden, og forebygge mulige finansielle tab og/eller skader på en institutions rygte.

Hvilke mål skal der nås med konstituenterne?
Som forklaret tidligere skal dit CSIRT betjene sine konstituenter og bistå dem med at løse it-sikkerhedshændelser og -problemer. En højnelse af vidensniveauet om it-sikkerhed og indførelse af en sikkerhedsbevidst kultur er supplerende mål.

Denne kultur tilstræber at træffe proaktive og forebyggende foranstaltninger fra starten og dermed reducere driftsomkostningerne.

Det kan i de fleste tilfælde øge effektiviteten generelt at indføre denne samarbejds- og bistandskultur i en virksomhed eller institution.

Hvad sker der, hvis der ikke gøres noget?
En ustruktureret måde at håndtere it-sikkerhed på kan føre til yderligere skade, ikke mindst på institutionens rygte. Finansielle tab og juridiske følger kan være andre resultater.

Hvad sker der, hvis der gøres noget?
Bevidstheden om sikkerhedsproblemer øges. Det hjælper med til at løse dem mere effektivt og forebygge fremtidige tab.

Hvad vil det koste?
Alt efter organisationsmodellen vil det koste lønningerne til medlemmerne af CSIRT-teamet og organisation, udstyr, værktøjer og softwarelicenser.

Hvad kommer der ind?
Afhængig af forretningen og tidligere tab vil det skabe mere åbenhed i procedurer og sikkerhedspraksis og vil dermed beskytte vigtige forretningsaktiver.

Hvad er tidsplanen?
Se en beskrivelse af et eksempel på projektplan i kapitel *12*. *Beskrivelse af projektplanen*.

Eksempler på eksisterende planer og strategier
Her er nogle eksempler på CSIRT-planer, som det er værd at se nærmere på:

- http://www.cert.org/CSIRT's/AFI_case-study.html
  Creating a Financial Institution CSIRT: A Case Study (oprettelse af et CSIRT i en finansinstitution: en casestudy).

  Formålet med dette dokument er at dele erfaringer fra en finansinstitution (der i dette dokument omtales som AFI), mens de både udviklede og gennemførte en plan til løsning af sikkerhedsproblemer og oprettede et CSIRT.

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Summary of the business case of CERT POLSKA (slideshow in PDF format) (resumé af CERT POLSKAs plan (diasshow i PDF-format).

- http://www.auscert.org.au/render.html?it=2252
  Det kunne være en afskrækkende opgave at oprette et Incident Response Team (IRT) i 1990'erne. Mange mennesker, der oprettede et IRT, havde ingen erfaring med det. I dette indlæg undersøges det, hvilken rolle et IRT kan spille i samfundet, og hvilke spørgsmål der skal tages stilling til både under oprettelsen og efter påbegyndelsen af driften. Det kan være til gavn for eksisterende IRT'er, da det kan øge bevidstheden om problemer, der ikke tidligere har været behandlet.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Case Study in Information Security, Securing the Enterprise, af: Roger Benton.

  Det er en praktisk case om et forsikringsselskabs overgang til et virksomhedsdækkende sikkerhedssystem. Formålet med casen er at vise, hvordan man kan gribe det an, når man opretter eller migrerer til et sikkerhedssystem. Oprindelig var et primitivt onlinesikkerhedssystem den eneste mekanisme til at kontrollere adgangen til selskabets data. Eksponeringen var alvorlig – der var ingen integritetskontrol uden for onlinemiljøet. Enhver med basale programmeringsfærdigheder kunne tilføje, ændre og/eller slette produktionsdata.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Marriott's e-security strategy: business-IT collaboration (Marriotts e-sikkerhedsstrategi: erhvervssamarbejde om it).

  Ifølge de erfaringer, Chris Zoladz fra Marriott International Inc. har gjort, er e-business-sikkerhed en proces, ikke et projekt. Det var budskabet fra Zoladz på den seneste e-sikkerhedskonference og -udstilling i Boston, der blev sponsoreret af Intermedia Group. Som vicedirektør for informationsbeskyttelse hos Marriott rapporterer Zoladz gennem den juridiske afdeling, selv om han ikke er advokat. Hans funktion er at afdække, hvor Marriotts mest værdifulde forretningsinformation lagres, og hvordan den bevæger sig inden for og uden for virksomheden. Marriott har defineret et særskilt ansvar for den tekniske infrastruktur, der understøtter sikkerheden, og som pålægges it-sikkerhedsarkitekten.

Det fiktive CSIRT (trin 7)

Fremme af forretningsplanen

Det besluttes at samle fakta og tal fra virksomhedens historie. Det er særdeles nyttigt for at få et statistisk overblik over it-sikkerhedssituationen. Man bør fortsætte med at samle data, når CSIRT'et er kommet i gang, for at holde statistikkerne ajour.

Andre nationale CSIRT'er blev kontaktet og interviewet om deres forretningsplaner. De ydede støtte ved at samle nogle dias med oplysninger om den seneste udvikling i it-sikkerhedshændelser og omkostningerne ved hændelserne.

I vores caseeksempel havde det fiktive CSIRT ingen presserende behov for at overbevise ledelsen om it-branchens betydning, så det var ikke svært at få grønt lys til det første skridt. Der blev udarbejdet en forretningsplan og en projektplan med bl.a. et skøn over etableringsomkostninger og driftsomkostninger.

8 Eksempler på operationelle og tekniske procedurer (workflow)

Vi har indtil nu taget følgende skridt:

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?
4. Analyse af miljø og konstituenter
5. Definition af mission statement
6. Udarbejdelse af forretningsplanen
   a. Definere den finansielle model
   b. Definere organisationsstrukturen
   c. Begynde at ansætte medarbejdere
   d. Anvende og udstyre kontoret
   e. Udarbejde en informationssikkerhedspolitik
   f. Se på samarbejdspartnere
7. Fremme af forretningsplanen
   a. få forretningsplanen godkendt
   b. indpasse det hele i en projektplan

>> Det næste skridt er: at gøre CSIRT'et operationelt

Det vil forbedre kvaliteten og den nødvendige tid pr. hændelse eller tilfælde af sårbarhed, hvis man har veldefinerede arbejdsgange på plads.

Som beskrevet i de indrammede eksempler vil det fiktive CSIRT tilbyde de grundlæggende CSIRT-kerneydelser:

- varslinger og advarsler
- håndtering af sikkerhedshændelser
- meddelelser

Dette kapitel giver eksempler på workflow, hvor et CSIRT's kerneydelser beskrives. Kapitlet indeholder også oplysninger om, hvordan man indsamler information fra forskellige kilder, kontrollerer den med hensyn til relevans og ægthed og videreformidler den til konstituenterne. Og endelig indeholder dette kapitel eksempler på de mest grundlæggende procedurer og specifikke CSIRT-værktøjer.

8.1 Vurdering af konstituenternes installationsgrundlag

Det første skridt er at danne dig et overblik over de it-systemer, dine konstituenter har installeret. Hermed kan CSIRT vurdere de indkommende informationers relevans og filtrere dem, før de sendes videre, således at konstituenterne ikke bliver oversvømmet med information, som de grundlæggende ikke kan bruge til noget.

Det er en god ide at begynde enkelt, f.eks. ved at bruge et Excelark som det følgende:

Kategori	Applikation	Software -produkt	Version	OS	OS version	Konstituent
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A
Netværk	Router	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Ydelser	Webserver	Apache		Unix	x-x-x	B

Med filterfunktionen i Excel er det meget let at udvælge den rigtige software og se, hvilke konstituenter der bruger hvilken slags software.

8.2 Generering af varslinger, advarsler og meddelelser

Genereringen af varslinger, advarsler og meddelelser følger alle samme workflow:

- indsamling af information
- vurdering af informationen med hensyn til relevans og kilde
- risikovurdering baseret på den indsamlede information
- udsendelse af information

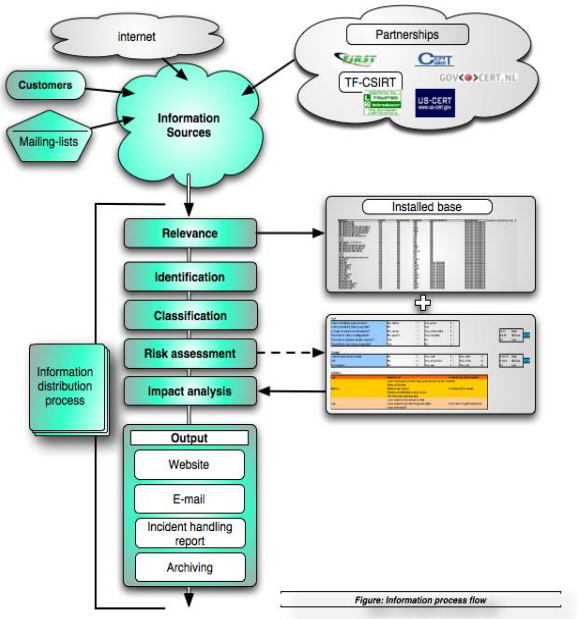


Fig. 9 : Informationsprocesflow.

I de følgende afsnit beskriver vi dette workflow nærmere.

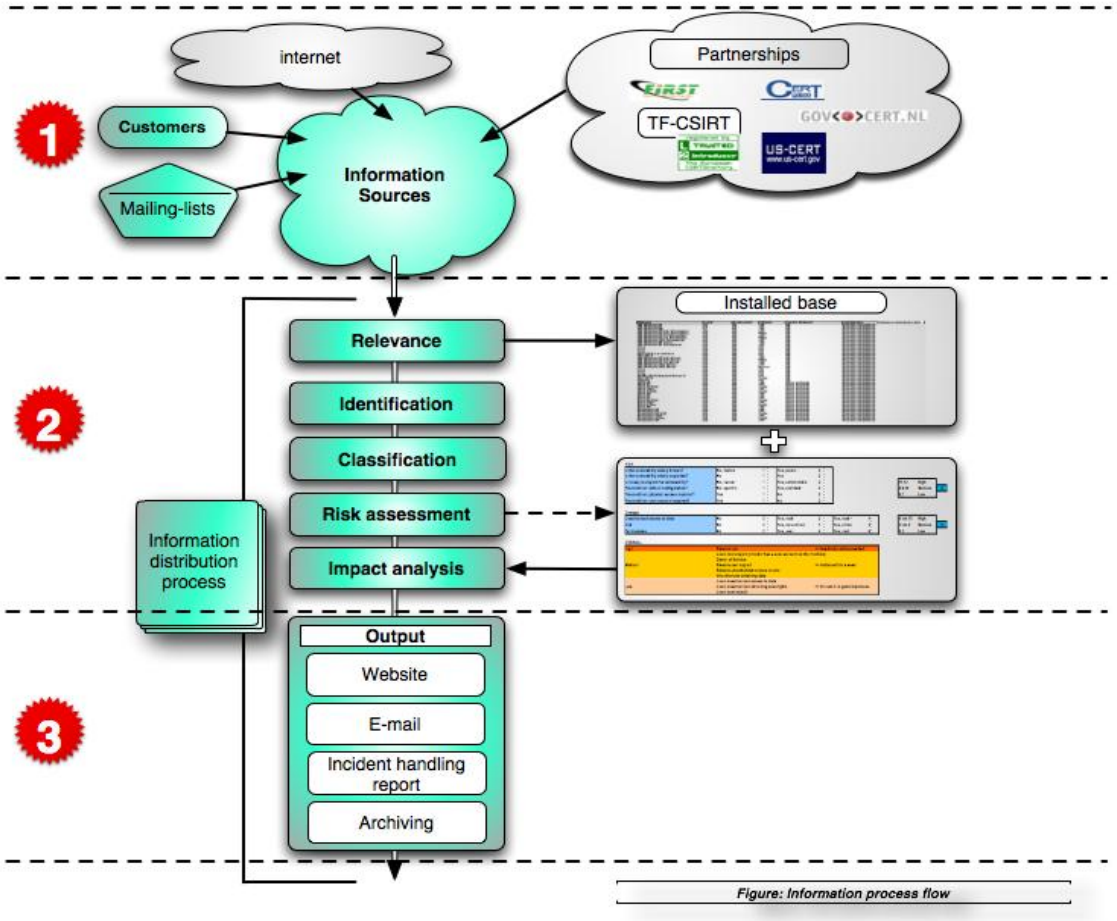


Figure: Information process flow

1 Trin 1: Indsamling af information om svagheder.

Der findes normalt to hovedtyper af informationskilder, som bidrager med information som input til tjenesterne:

- information om svagheder i (dine) it-systemer
- hændelsesrapporter

Alt efter branche og it-infrastruktur findes der mange offentlige og lukkede kilder til information om sårbarheder:

- offentlige og lukkede mailinglister
- produktinformation om sårbarheder hos leverandører
- websteder
- information på internettet (Google osv.)
- offentlige og private partnerskaber, der leverer information om sårbarheder (FIRST, TF-CSIRT, CERT-CC, US-CERT osv.)

Al denne information bidrager til vidensniveauet om specifikke sårbarheder i it-systemer.

Som før nævnt er der masser af gode og lettilgængelige sikkerhedsinformationskilder til rådighed på internettet. ENISA's ad hoc-arbejdsgruppe "CERT services" for 2006 er i skrivende stund ved at udarbejde en mere omfattende liste, der forventes færdig ved udgangen af 2006[19].

Trin 2: Evaluering af information samt risikovurdering

Dette trin vil føre til en analyse af virkningerne af en specifik sårbarhed for konstituenternes it-infrastruktur.

Identifikation
Indkommende sårbarhedsinformation skal altid identificeres via sin kilde, og det skal afgøres, om kilden er troværdig, før der gives informationer videre til konstituenterne. Ellers kan folk blive udsat for falsk alarm, hvilket kan føre til unødvendige forstyrrelser i forretningsprocesser og i sidste ende skade CSIRT'ets omdømme.

[19] Ad hoc-arbejdsgruppen om CERT-ydelser:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

Følgende procedure viser et eksempel på afdækning af, om en meddelelse er ægte:

Procedure for, hvordan man afdækker en meddelelses ægthed og dens kilde

Generel tjekliste
1. Er kilden kendt og registreret som sådan?
2. Kommer informationen via en regulær kanal?
3. Indeholder den "mærkelig" information, som "føles" forkert?
4. Følg din fornemmelse, og hvis du er i tvivl om en information, så lad være med at gøre noget, men kontroller den igen!

E-mail-kilder
1. Er kildeadressen kendt i organisationen og kendt på kildelisten?
2. Er PGP-signaturen korrekt?
3. Tjek hele meddelelsens hoved, hvis du er i tvivl.
4. Brug "nslookup" eller "dig" for at verificere afsendernes domæne[20], hvis du er i tvivl.

WWW-kilder
1. Kontroller browser-certifikater, når du logger på et sikkert websted (https://).
2. Kontroller kilden med hensyn til indhold og validitet (teknisk).
3. Lad være med at klikke på links eller downloade software, hvis du er i tvivl.
4. Få foretaget et "lookup" og et "dig" på domænet, og lav en "traceroute", hvis du er i tvivl.

Telefon
1. Lyt nøje til navnet.
2. Genkender du stemmen?
3. Bed om et telefonnummer, og sig, du vil ringe tilbage, hvis du er i tvivl.

Fig. 10 Eksempel på en procedure for informationsidentifikation.

Relevans
Oversigten over installeret hard- og software, som blev lavet tidligere, kan bruges til at filtrere den indkommende sårbarhedsinformation efter relevans med det formål at få besvaret følgende spørgsmål: "Bruger konstituenterne denne software?", "Er informationen relevant for dem?"

Klassificering
Noget af den information, der kommer ind, kan klassificeres eller tagges som "kun til tjenestebrug" (f.eks. indkommende hændelsesrapporter fra andre team). Al information skal håndteres i overensstemmelse med afsenderens krav og med egen informationssikkerhedspolitik. En god grundregel er *"Lad være med at distribuere information, hvis det ikke er klart, om det er meningen; når du er i tvivl, så bed om afsenderens tilladelse til det."*

[20] Værktøjer til kontrol af identiteter i CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Risikovurdering og konsekvensanalyse
Der er flere metoder til at fastslå risikoen ved og konsekvenserne af en (potentiel) sårbarhed.

Risiko defineres som den potentielle mulighed for, at sårbarheden kan udnyttes. Der er flere vigtige faktorer (bl.a.):

- Er sårbarheden velkendt?
- Er sårbarheden udbredt?
- Er det let at udnytte sårbarheden?
- Kan udnyttelsen af sårbarheden fjernstyres?

Alle disse spørgsmål giver en god fornemmelse for sårbarhedens alvor.
En meget enkel metode til at beregne risikoen er følgende formel:

konsekvens = risiko X potentiel skade

Den potentielle skade kan være:

- uautoriseret adgang til data
- Denial of Service (DoS)
- opnåelse eller udvidelse af tilladelser

(Se mere detaljerede klassificeringsordninger i slutningen af dette kapitel).

Når disse spørgsmål er besvaret, kan der tilføjes en samlet score til den rådgivende bulletin med information om den potentielle risiko og skade. Ofte bruges der enkle udtryk som LAV, MIDDEL og HØJ.

Andre, mere omfattende, risikovurderingsskemaer er:

GOVCERT.NL rating system[21]

Det statslige nederlandske CSIRT GOVCERT.NL har udviklet en matrix til risikovurdering, som blev udviklet i startfasen af Govcert.nl og stadig opdateres med de seneste tendenser.

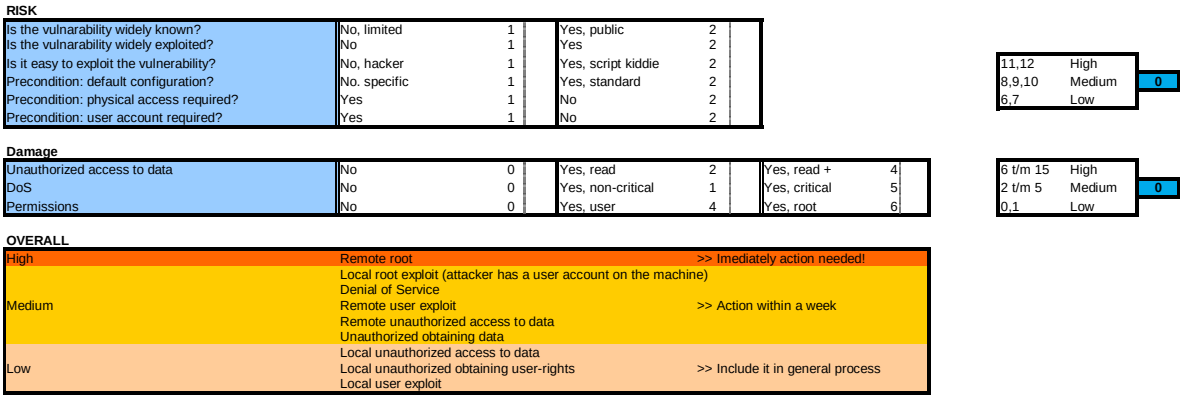


Fig. 11 Ratingsystemet GOVCERT.NL

EISPP Common Advisory Format Description[22]

Det europæiske program til fremme af informationssikkerhed (European Information Security Promotion Programme, EISPP) er et projekt, der medfinansieres af Det Europæiske Fællesskab under det femte rammeprogram. EISPP-projektet sigter mod at udvikle europæiske rammer, ikke blot for at dele sikkerhedsviden, men også for at definere indholdet og de måder, hvorpå man kan formidle sikkerhedsinformation til smv'er. Hvis de europæiske smv'er får de nødvendige it-sikkerhedstjenester, vil det øge deres tillid til og brug af e-handel, hvilket vil føre til flere og bedre muligheder for ny omsætning. EISPP er en pioner i Europa-Kommissionens vision for oprettelse af et europæisk netværk af ekspertise i EU.

DAF Deutsches Advisory Format[23]

Initiativet til DAF blev taget af det tyske CERT-Verbund, og det er en central bestanddel af en infrastruktur for forskellige teams generering og udveksling af sikkerhedsbulletiner. DAF er specielt skræddersyet til tyske CERT'ers behov; standarden udvikles og vedligeholdes af CERT-Bund, DFN-CERT, PRESECURE og Siemens-CERT.

Trin 3: Udsendelse af information

Et CSIRT kan vælge mellem flere distributionsmetoder afhængigt af konstituenternes ønsker og din kommunikationsstrategi.

---

[21] Sårbarhedsmatrix: http://www.govcert.nl/download.html?f=33

[22] EISSP: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#03

[23] DAF: http://www.enisa.europa.eu/cert_inventory/pages/04_03.htm#02

- websted
- e-mail
- rapporter
- arkivering og forskning

De sikkerhedsbulletiner, et CSIRT udsender, bør altid følge samme disposition. Det vil gøre dem lettere at læse, og læseren vil hurtigt finde alle de relevante oplysninger.

En bulletin bør som minimum indeholde følgende oplysninger:

Bulletinens titel ……
Referencenummer …… **Berørte systemer** **-** …… **-** …… **Tilknyttet OS + version** …… **Risiko** (Høj-Middel-Lav) …… **Konsekvenser/potentiel skade** (Høj-Middel-Lav) …… **Eksterne id'er:** (CVE, id'er for sårbarhedsbulletin) ……
Oversigt over sårbarhed …… **Konsekvenser** …… **Løsning** …… **Beskrivelse (detaljer)** …… **Tillæg** ……

Fig. 12 Eksempel på bulletinskema.

Se et eksempel på en hel sikkerhedsbulletin i kapitel *10. Øvelse*.

8.3 At arbejde med håndtering af sikkerhedshændelser

Som nævnt i indledningen til dette kapitel er processen med informationshåndtering under håndteringen af sikkerhedshændelser meget lig den, der bruges under kompilering af varslinger, advarsler og meddelelser. Men informationssamlingsdelen er sædvanligvis anderledes, da den normale måde at få hændelsesrelaterede data på enten er ved at modtage hændelsesrapporter fra konstituenter eller andre team eller ved at få feedback fra involverede parter under selve hændelseshåndteringen. Informationen flyder i reglen pr. (krypteret) e-mail; undertiden er det nødvendigt at bruge telefon eller fax.

Når man får information over telefonen, er det en god ide at notere selv den mindste detalje med det samme enten ved hjælp af et hændelseshåndterings-/rapporteringsværktøj eller ved at skrive et memo. Det er nødvendigt straks (før opringningen er slut) at generere et hændelsesnummer (hvis der ikke allerede findes et for denne hændelse) og give det til rapportøren i telefonen (eller i en opsummerende e-mail bagefter) som reference i den videre kommunikation.

I resten af dette kapitel beskrives den grundlæggende proces for håndtering af sikkerhedshændelser. En tilbundsgående analyse af hele processen for hændelsesstyring og alle de hertil knyttede workflow og del-workflow kan ses i CERT/CC's publikation om definition af hændelsesstyringsprocesser for CSIRT'er, *Defining Incident Management processes for CSIRT's*[24].

[24] Definition af hændelsesstyringsprocesser: http://www.cert.org/archive/pdf/04tr015.pdf

Helt basalt følger hændelseshåndtering følgende workflow:

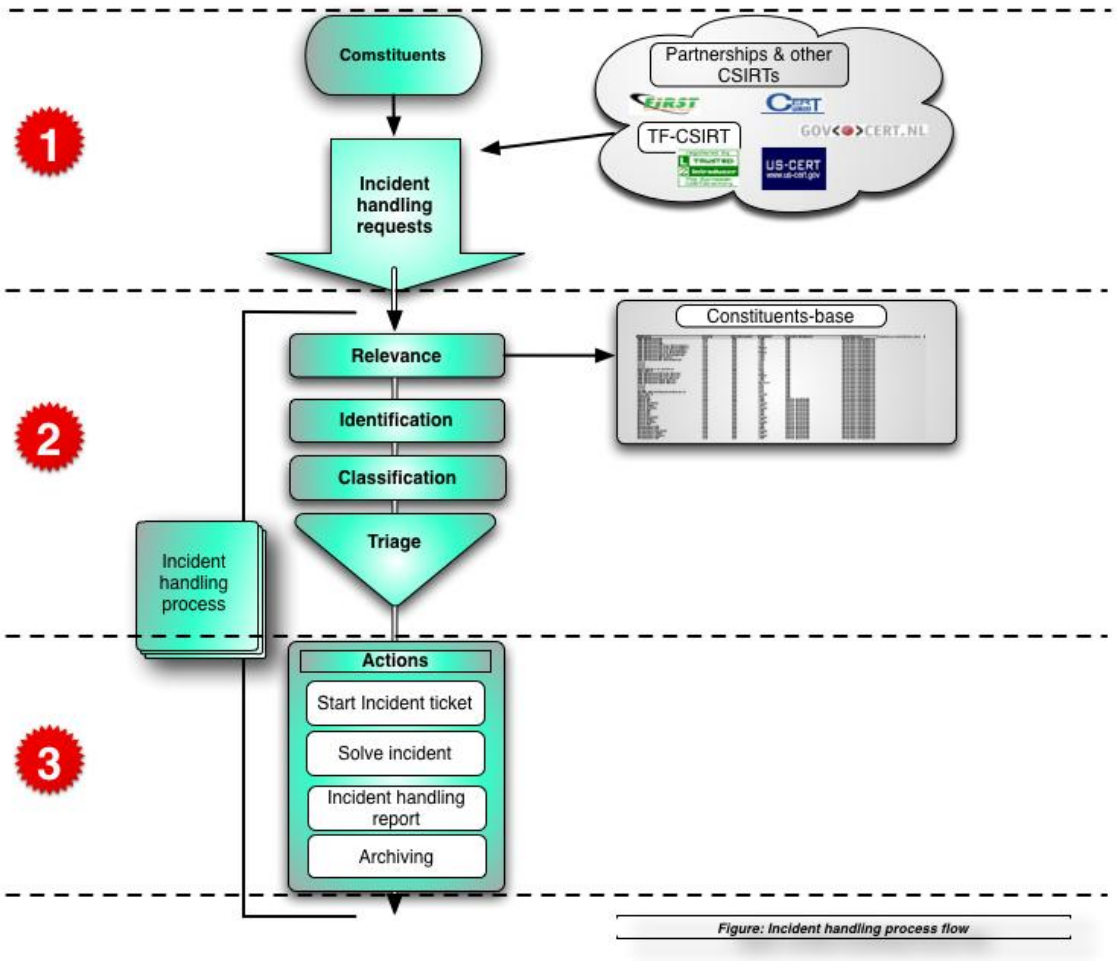


Fig. 13 Hændelsesprocesflow.

Trin 1: Modtagelse af hændelsesrapporter

Som nævnt når hændelsesrapporter frem til et CSIRT ad flere kanaler, for det meste e-mail, men også telefon eller fax.

Det er en god ide at notere alle oplysninger i et fast format, mens man modtager en hændelsesrapport. Dermed sikrer man, at der ikke udelades afgørende information. Nedenfor ses et eksempel på et skema:

BLANKET TIL HÆNDELSESRAPPORTERING

Udfyld venligst denne blanket, og send den pr. fax eller e-mail til: ……..
*Linjer markeret med * skal udfyldes.*

Navn og organisation
1. Navn*:
2. Organisationens navn*:
3. Branche:
4. Land*:
5. By:
6. E-mailadresse*:
7. Telefonnummer*:
8. Andet:

Berørt(e) vært(er)
9. Antal værter:
10. Værtsnavn & IP*:
11. Værtens funktion*:
12. Tidszone:
13. Hardware:
14. Operativsystem:
15. Berørt software:
16. Berørte filer:
17. Sikkerhed:
18. Værtsnavn & IP:
19. Protokol/port:

Hændelse
20. Referencenummer
21. Hændelsestype:
22. Hændelse startet:
23. Det er en igangværende hændelse: JA NEJ
24. Tidspunkt og opdagelsesmetode:
25. Kendte sårbarheder:
26. Mistænkelige filer:
27. Modforanstaltninger:
28. Detaljeret beskrivelse*:

Fig. 14 Indholdet af en hændelsesrapport.

Trin 2: Hændelsesvurdering

I løbet af dette trin bliver en rapporteret hændelses ægthed og relevans kontrolleret, og hændelsen klassificeres.

Identifikation

For at forebygge unødvendige foranstaltninger er det en god vane at kontrollere, om ophavsmanden er pålidelig, og om ophavsmanden er en af dine egne eller et andet CSIRT's konstituenter. Der gælder lignende regler som dem, der er beskrevet i kapitel *8.2 Generering af varslinger.*

Relevans

Med dette skridt tjekker du, om anmodningen om hændelseshåndtering stammer fra CSIRT'ets konstituenter, eller om den rapporterede hændelse involverer it-systemer fra konstituenterne. Hvis ingen af delene er tilfældet, omdirigeres rapporten normalt til det rette CSIRT[25].

Klassificering

Med dette skridt klassificeres hændelsens alvor som forberedelse af triagen. Det ligger uden for denne publikations rammer at gå i detaljer med hændelsesklassificering. Det er en god start at bruge CSIRT-skemaet til hændelsesklassificering (eksempel på virksomheds-CSIRT):

Incident Categories

All incidents managed by the CSIRT should be classified into one of the categories listed in the table below.

Incident Category	Sensitivity*	Description
Denial of service	S3	• DOS or DDOS attack.
Forensics	S1	• Any forensic work to be done by CSIRT.
Compromised Information	S1	• Attempted or successful destruction, corruption, or disclosure of sensitive corporate information or Intellectual Property.
Compromised Asset	S1, S2	• Compromised host (root account, Trojan, rootkit), network device, application, user account. This includes malware-infected hosts where an attacker is actively controlling the host.
Unlawful activity	S1	• Theft / Fraud / Human Safety / Child Porn. Computer-related incidents of a criminal nature, likely involving law enforcement, Global Investigations, or Loss Prevention.
Internal Hacking	S1, S2, S3	• Reconnaissance or Suspicious activity originating from inside the Company corporate network, excluding malware.
External Hacking	S1, S2, S3	• Reconnaissance or Suspicious Activity originating from outside the Company corporate network (partner network, Internet), excluding malware.
Malware	S3	• A virus or worm typically affecting multiple corporate devices. This does not include compromised hosts that are being actively controlled by an attacker via a backdoor or Trojan. (See Compromised Asset)
Email	S3	• Spoofed email, SPAM, and other email security-related events.
Consulting	S1, S2, S3	• Security consulting unrelated to any confirmed incident.
Policy Violations	S1, S2, S3	• Sharing offensive material, sharing/possession of copyright material. • Deliberate violation of Infosec policy. • Inappropriate use of corporate asset such as computer, network, or application. • Unauthorized escalation of privileges or deliberate attempt to subvert access controls.
* - Sensitivity will vary depending on circumstances. Guidelines are provided.		

Fig. 15 Skema til hændelsesklassificering (kilde: FIRST)[26]

[25] Værktøjer til kontrol af identiteter i CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

[26] CSIRT hændelsesklassificering http://www.first.org/resources/guides/csirt_case_classification.html

Triage
Triage er et system, der bruges af lægelige medarbejdere eller nødhjælpspersonale til at rationere begrænsede lægelige ressourcer, når antallet af behandlingskrævende sårede overstiger de disponible behandlingsressourcer, således at der behandles så mange patienter som muligt[27].

CERT/CC giver følgende beskrivelse:

Triage er et væsentligt element i enhver hændelseshåndteringskapacitet, især for et CSIRT. Triage er afgørende for at forstå, hvad der rapporteres i hele organisationen. Det er det middel, der sikrer, at alle informationer flyder til et fælles kontaktpunkt, så man kan få et anvendelsesorienteret billede af den igangværende aktivitet og en omfattende sammenhæng mellem alle rapporterede data. Triage giver mulighed for en indledende vurdering af en indkommende rapport og sætter den i kø til videre håndtering. Det er også her, man påbegynder den indledende dokumentation og dataregistrering af en rapport eller en forespørgsel, hvis det ikke allerede er gjort i detektionsprocessen.

Triagefunktionen giver et øjebliksbillede af den aktuelle status for al rapporteret aktivitet – hvilke rapporter der er åbne eller lukkede, hvilke foranstaltninger der er i gang, og hvor mange af hver type rapport der er indkommet. Denne proces kan bidrage til at identificere potentielle sikkerhedsproblemer og prioritere arbejdsbyrden. De informationer, der indsamles under triagen, kan også bruges til at udlede tendenser for sårbarhed og sikkerhedshændelser samt generere statistikker herfor til den øverste ledelse[28].

Triage bør kun foretages af de mest erfarne teammedlemmer, fordi det kræver en dybtgående forståelse af hændelsernes potentielle følger for bestemte konstituenter samt evnen til at beslutte, hvem af teammedlemmerne der vil være egnet til at håndtere hændelsen.

[27] Triage i Wikipedia: http://en.wikipedia.org/wiki/Triage

[28] Definition af hændelsesstyringsprocesser: http://www.cert.org/archive/pdf/04tr015.pdf

Trin 3: Foranstaltninger

Normalt kommer triagerede hændelser ind i en forespørgselskø i et hændelseshåndteringsværktøj, der bruges af en eller flere personer, som håndterer sikkerhedshændelser, de såkaldte "incident handlers", der grundlæggende følger disse trin.

"Start incident ticket"
Nummeret på "hændelsesbilletten" kan allerede være blevet genereret i et tidligere trin (f.eks. når hændelsen blev rapporteret pr. telefon). Ellers er det første skridt at oprette sådan et nummer, der vil blive brugt i al videre kommunikation om hændelsen.

Hændelsens livscyklus
Når man håndterer en hændelse, følger man ikke en række af skridt, der til sidst fører til en løsning, men bevæger sig snarere i cirkler og foretager de samme skridt gentagne gange, indtil hændelsen endelig løses, og alle involverede parter har al den nødvendige information. Denne cirkel, der ofte omtales som "sikkerhedshændelsens livscyklus", omfatter følgende processer:

Analyse:	Alle detaljer ved den rapporterede hændelse analyseres,
Opnå kontaktinformation:	for at kunne videresende information i forbindelse med hændelsen til alle involverede parter, såsom andre CSIRT'er, ofre og formentlig ejerne af systemer, der kan være blevet misbrugt til et angreb,
Yde teknisk bistand:	hjælpe ofrene med hurtig genoprettelse efter følgerne af hændelsen og indsamle flere informationer om angrebet,
Koordinering:	informere andre involverede parter, såsom det CSIRT, der har ansvaret for it-systemet, som blev brugt til angrebet, eller andre ofre.

Denne opbygning kaldes en "livscyklus", fordi det ene skridt fører til det næste, og det sidste, koordineringsdelen, så igen kan føre til en ny analyse, og cyklussen starter igen. Processen slutter, når alle involverede parter har modtaget og rapporteret alle nødvendige oplysninger.

Se en mere detaljeret beskrivelse af sikkerhedshændelsens livscyklus i CERT/CC's CSIRT-håndbog[29].

Rapport over hændelseshåndtering
Vær forberedt på spørgsmål fra ledelsen om hændelserne ved at udarbejde en rapport. Det er også en god ide at skrive et dokument (kun til internt brug) om "indhøstede erfaringer", som medarbejderne kan lære af, og for at undgå fejl i håndtering af fremtidige hændelser.

[29] CSIRT-håndbogen: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Arkivering
Se arkiveringsreglerne, der er beskrevet i kapitel *6.6. Udvikling af en informationssikkerhedspolitik.*

Se bilaget, afsnit *A.1 Yderligere læsning* om omfattende vejledninger til hændelsesstyring og hændelseslivscyklus.

8.4 Eksempel på en tidsplan for svar

Det undlades ofte at definere svartider, men det skal indgå i enhver gennemarbejdet serviceniveauaftale mellem et CSIRT og dets konstituenter. Det er afgørende at give rettidig feedback til konstituenter under håndteringen af en hændelse, både af hensyn til konstituenternes egne forpligtelser og til teamets omdømme.
Svartiderne skal kommunikeres klart ud til konstituenterne for at undgå forkerte forventninger. Følgende helt grundlæggende tidsplan kan bruges som udgangspunkt for en mere detaljeret serviceniveauaftale med et CSIRT's konstituenter.

Her er et eksempel på en praktisk svartidsplan fra det tidspunkt, hvor en forespørgsel om assistance kommer ind.

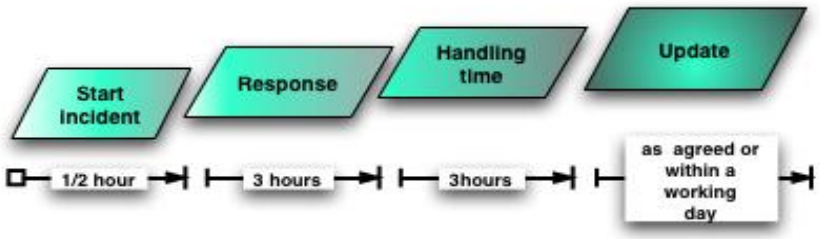


Fig. 16 Eksempel på svartidsplan.

Det er også en god ide at instruere konstituenterne om deres egne svartider, især hvornår de skal kontakte CSIRT i tilfælde af en nødsituation. I de fleste tilfælde er det bedre at kontakte deres CSIRT på et tidligt tidspunkt, og det er en god ide at opfordre konstituenterne til at gøre det, når de er i tvivl.

8.5 Tilgængelige CSIRT-værktøjer

I dette kapitel finder du oplysninger om almindelige værktøjer, der bruges af CSIRT'er. Der er kun tale om eksempler, og der kan findes flere i *Clearinghouse of Incident Handling Tools*[30] (CHIHT).

Software til kryptering af e-mail og meddelelser

- GNUPG http://www.gnupg.org/
  GnuPG er GNU-projektets fuldstændige og gratis implementering af den åbne PGP-standard som defineret af RFC2440. Med GnuPG kan du kryptere og underskrive dine data og din kommunikation.

- PGP http://www.pgp.com/
  Kommerciel variant

Hændelseshåndteringsværktøj

Til at administrere og følge op på hændelser samt holde styr på foranstaltninger.

- RTIR http://www.bestpractical.com/rtir/
  RTIR er et gratis open source hændelseshåndteringssystem, der er udviklet med henblik på CERT-teams og andre incident responseteams behov.

CRM-værktøjer

Når du har mange forskellige konstituenter og skal have styr på alle aftaler og oplysninger, er en CRM-database nyttig. Der er mange forskellige variationer, bl.a.:

- SugarCRM http://www.sugarcrm.com/crm/

- Sugarforce (Gratis, open source version) http://www.sugarforge.org/

Informationskontrol

- Website watcher http://www.aignes.com/index.htm
  Dette program overvåger websteder for opdateringer og ændringer.

- Watch that page http://www.watchthatpage.com/
  Tjenesten sender information om ændringer i websteder pr. e-mail (gratis og kommerciel).

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Hvordan finder man kontaktinformation?
Det er ikke nogen let opgave at finde den rette kontaktperson at rapportere hændelser til. Her er et par informationskilder, der kan bruges:

- RIPE[31]
- IRT-object[32]
- TI[33]

Endvidere har CHIHT en liste over værktøjer til at finde kontaktinformation[34].

Det fiktive CSIRT (trin 8)

Etablering af processtrømme og operationelle og tekniske procedurer
Det fiktive CSIRT fokuserer på at levere kerne-CSIRT-ydelser:

- varslinger og advarsler
- meddelelser
- håndtering af sikkerhedshændelser

Teamet har udviklet procedurer, der fungerer godt, og som er lette at forstå for alle teammedlemmer. Det fiktive CSIRT har også ansat en juridisk ekspert til at tage sig af ansvar og informationssikkerhedspolitik. Teamet har indført nogle nyttige værktøjer og har gennem diskussioner med andre CSIRT'er fundet nyttig information om operationelle spørgsmål.

Der er blevet genereret en fast model til sikkerhedsbulletiner og hændelsesrapporter. Teamet bruger RTIR til håndtering af hændelser.

[31] RIPE whois: http://www.ripe.net/whois

[32] IRT-object i RIPE-databasen: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

[33] Trusted Introducer: http://www.enisa.europa.eu/cert_inventory/pages/04_01_03.htm#07

[34] Værktøjer til kontrol af identiteter i CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 CSIRT-uddannelse

Vi har indtil nu taget følgende skridt:

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?
4. Analyse af miljø og konstituenter
5. Definition af mission statement
6. Udarbejdelse af forretningsplanen
   a. Definere den finansielle model
   b. Definere organisationsstrukturen
   c. Begynde at ansætte medarbejdere
   d. Anvende og udstyre kontoret
   e. Udvikle en informationssikkerhedspolitik
   f. Se på samarbejdspartnere
7. Fremme af forretningsplanen
   a. Få forretningsplanen godkendt
   b. Indpasse det hele i en projektplan
8. At gøre CSIRT'et operationelt
   a. Etablere workflow
   b. Implementere CSIRT-værktøjer

>> Det næste skridt er: at uddanne medarbejderne

Dette kapitel indeholder de to hovedkilder til særlig CSIRT-uddannelse: TRANSITS- og CERT/CC-kurser

9.1 TRANSITS

TRANSITS har været et europæisk projekt med det formål at få etableret it-sikkerheds- og udrykningsteam (CSIRT'er) og styrke eksisterende CSIRT'er ved at gøre noget ved problemet med manglen på kvalificerede CSIRT-medarbejdere. Dette mål har man arbejdet hen imod ved at udbyde specialistkurser for at uddanne medarbejdere i (nye) CSIRT'er i organisatoriske, operationelle, tekniske, markedsrelaterede og juridiske spørgsmål i forbindelse med ydelse af CSIRT-tjenester.

Gennem TRANSITS har man navnlig

- udviklet, opdateret og regelmæssigt revideret modulopbygget kursusmateriale
- afholdt uddannelsesworkshopper, inklusive kursusmateriale
- givet mulighed for, at medarbejdere i (nye) CSIRT'er kunne deltage i disse uddannelsesworkshopper med særlig vægt på deltagelse fra EU-tiltrædelsesstaterne
- formidlet kursusmaterialer og sikret udnyttelse af resultaterne[35].

[35] TRANSITS: http://www.enisa.europa.eu/cert_inventory/pages/04_02_02.htm#11

ENISA fremmer og støtter TRANSITS-kurserne. Hvis du vil vide mere om, hvordan man søger om kurser, og hvilke krav og omkostninger der er, kan du kontakte ENISA's CSIRT-eksperter:

CERT-Relations@enisa.europa.eu

I bilaget til dette dokument finder du eksempler på kursusmateriale!

9.2 CERT/CC

Computer- og netværksinfrastrukturers kompleksitet og den administrative udfordring gør det vanskeligt at styre netværkssikkerhed ordentligt. Netværks- og systemadministratorer har hverken folk nok eller tilstrækkelige sikkerhedspraksiser til at kunne forsvare sig mod angreb og minimere skader. Som følge heraf er antallet af computersikkerhedshændelser stigende.
Når der opstår computersikkerhedshændelser, skal organisationerne reagere hurtigt og effektivt. Jo hurtigere en organisation erkender, analyserer og reagerer på en hændelse, jo bedre kan den begrænse skaden, og jo mindre bliver omkostningerne. En god måde at sikre denne hurtige reaktionskapacitet på og også forebygge fremtidige hændelser, er ved at oprette et it-sikkerheds- og udrykningshold (CSIRT).

CERT-CC tilbyder kurser til ledere og tekniske medarbejdere inden for områder som oprettelse og styring af it-sikkerheds- og udrykningshold (CSIRT'er), reaktion på og analyse af sikkerhedshændelser og forbedring af netværkssikkerhed. Medmindre andet er anført, afholdes alle kurser i Pittsburgh, Pennsylvania. Vores medarbejdere afholder også kurser i sikkerhed på Carnegie Mellon University.

Særlige CERT/CC-kurser[36] for CSIRT'er

Creating a Computer Security Incident Response Team (CSIRT) (oprettelse af CSIRT)
Managing Computer Security Incident Response Teams (CSIRT's) (ledelse af CSIRT)
Fundamentals of Incident Handling (grundlæggende håndtering af sikkerhedshændelser)
Advanced Incident Handling for Technical Staff (avanceret håndtering af sikkerhedshændelser for tekniske medarbejdere)

I bilaget til dette dokument finder du eksempler på kursusmateriale!

Det fiktive CSIRT (trin 9)
Uddannelse af medarbejderne Det fiktive CSIRT beslutter at sende alle sine tekniske medarbejdere på de næste ledige TRANSITS-kurser. Teamlederen deltager desuden i CERT/CC's kursus om ledelse af et CSIRT, *Managing a CSIRT*.

[36] CERT/CC-kurser: http://www.sei.cmu.edu/products/courses

10 Øvelse: fremstilling af en bulletin

Vi har indtil nu taget følgende skridt:

1. Forståelse for, hvad et CSIRT er, og hvilke fordele det kan give.
2. Hvilken sektor skal det nye team levere sine tjenester til?
3. Hvilke former for tjenester kan et CSIRT levere til sine konstituenter?
4. Analyse af miljø og konstituenter
5. Definition af mission statement
6. Udarbejdelse af forretningsplanen
   a. Definere den finansielle model
   b. Definere organisationsstrukturen
   c. Begynde at ansætte medarbejdere
   d. Anvende og udstyre kontoret
   e. Udvikle en informationssikkerhedspolitik
   f. Se på samarbejdspartnere
7. Fremme af forretningsplanen
   a. Få forretningsplanen godkendt
   b. Indpasse det hele i en projektplan
8. At gøre CSIRT'et operationelt
   a. Etablere workflow
   b. Implementere CSIRT-værktøjer
9. Uddannelse af dine medarbejdere

>> Det næste skridt er at træne og blive klar til det rigtige arbejde!

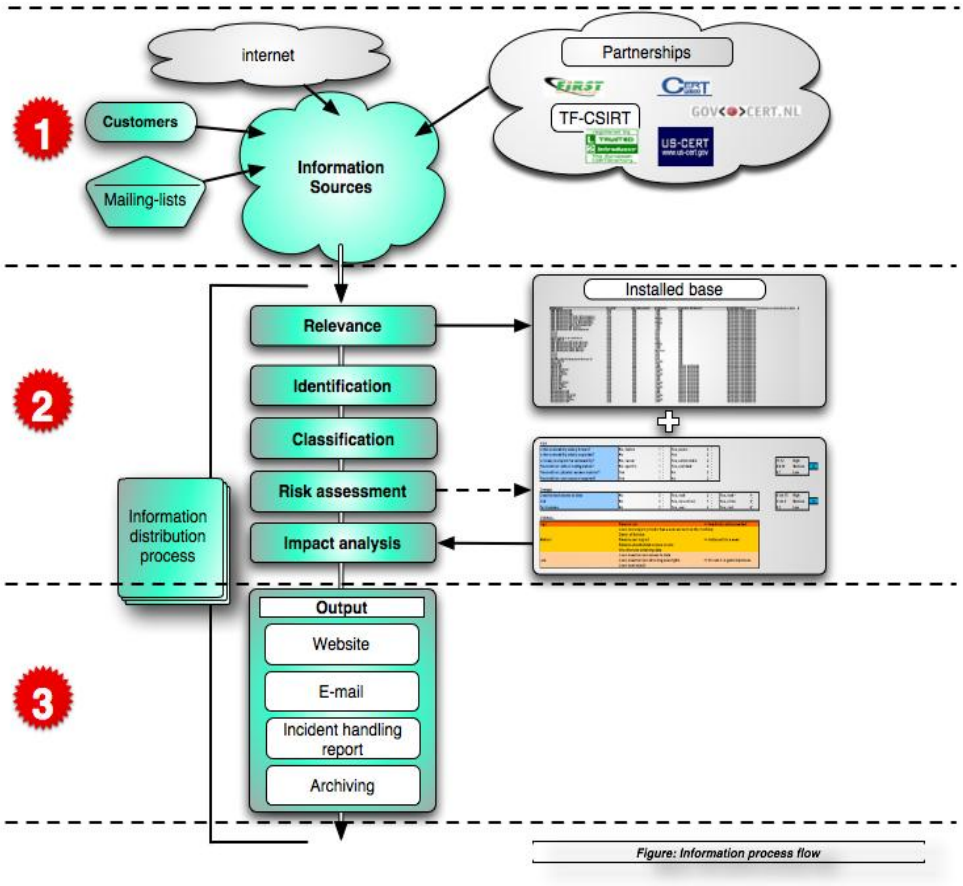
Til illustration beskriver dette kapitel et eksempel på en øvelse i en hverdagsopgave for et CSIRT: oprettelse af en sikkerhedsbulletin.

Udløseren var følgende originale sikkerhedsbulletin fra Microsoft:

Bulletin-id	**Microsoft Security Bulletin MS06-042**
Bulletintitel	**Cumulative Security Update for Internet Explorer (918899)**
Resumé	Denne opdatering løser flere svagheder i Internet Explorer, der kunne åbne mulighed for fjernstyret kodeudførelse.
Maksimal sværhedsgrad	Kritisk
Følger af sårbarheden	Fjernstyret kodeudførelse
Berørt software:	**Windows, Internet Explorer.** For yderligere information, se afsnittet Berørt software og Download locations.

Denne bulletin til leverandører behandler en nyligt opdaget sårbarhed i Internet Explorer. Leverandøren offentliggør mange fejlretninger til denne software til mange forskellige versioner af Microsoft Windows.

Efter at det fiktive CSIRT har modtaget denne sårbarhedsoplysning via en mailingliste, begynder det med workflowet, som er beskrevet i kapitel *8.2 Generering af varslinger, advarsler og meddelelser.*



1 Trin 1: Indsamling af information om svagheder.

Første skridt er at browse til leverandørens websted. Der kontrollerer det fiktive CSIRT, at informationen er ægte og samler yderligere oplysninger om sårbarheden og de berørte it-systemer.

Trin 2: Evaluering af information samt risikovurdering

Identifikation
Informationen er allerede blevet verificeret ved krydstjekning mellem den sårbarhedsinformation, der indløb med e-mail, og teksten på leverandørens websted.

Relevans
Det fiktive CSIRT tjekker listen på webstedet over berørte systemer med listen over de systemer, konstituenterne bruger. Det konstaterer, at mindst én af deres konstituenter bruger Internet Explorer, så sårbarhedsinformationen er absolut relevant.

Kategori	Applikation	Software produkt	Version	OS	OS Version	Konstituent
Desktop	Browser	IE	x-x-	Microsoft	XP-prof	A

Klassificering
Informationen er offentlig, så den kan bruges og videreformidles.

Risikovurdering og konsekvensanalyse
Besvarelsen af spørgsmålene viser, at risiko og konsekvenser er *høje* (Microsofts vurdering var *kritisk*).

RISIKO

Er sårbarheden velkendt?	J
Er sårbarheden udbredt?	J
Er det let at udnytte sårbarheden?	J
Kan udnyttelsen af sårbarheden fjernstyres?	J

SKADE
De mulige konsekvenser er fjernadgang og potentielt fjernstyret kodeudførelse. Denne sårbarhed rummer mange problemer, som gør skaderisikoen *høj*.

Trin 3: Distribution

Det fiktive CSIRT er et internt CSIRT. Det har e-mail, telefon og det interne websted til rådighed som kommunikationskanaler. CSIRT udarbejder denne bulletin ud fra modellen fra kapitel *8.2 Generering af varslinger, advarsler og meddelelser.*

Bulletinens titel
Mange sårbarheder fundet i Internet Explorer

Referencenummer
082006-1
Berørte systemer
- Alle desktopsystemer, der kører Microsoft

Tilknyttet OS + version
- Microsoft Windows 2000 Service Pack 4
- Microsoft Windows XP Service Pack 1 og Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 og Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 til Itaniumbaserede systemer og Microsoft Windows Server 2003 med SP1 til Itaniumbaserede systemer
- Microsoft Windows Server 2003 x64 Edition

Risiko (Høj-Middel-Lav)
HØJ
Konsekvenser/potentiel skade (Høj-Middel-Lav)
HØJ
Eksterne id'er: (CVE, id'er for sårbarhedsbulletin)
MS-06-42

Oversigt over sårbarhed
Microsoft har fundet flere kritiske sårbarheder i Internet Explorer, der kan føre til fjernstyret kodeudførelse.

Konsekvenser
En angriber kan få fuldstændig kontrol over systemet og installere programmer, tilføje brugere og konkurrere med, ændre eller slette data. Det er en formildende omstændighed, at ovenstående kun kan ske, hvis brugeren er logget på med administratorrettigheder. Virkningen for brugere, der er logget på med færre rettigheder, kan være mindre.

Løsning
Patch din IE omgående.

Beskrivelse (oplysninger)
Få mere information på ms06-042.mspx

Tillæg
Få mere information på ms06-042.mspx

Resultatet er nu klar til at blive udsendt. Da det er en kritisk bulletin, er det tilrådeligt også at ringe konstituenterne op, når det er muligt.

Det fiktive CSIRT (trin 10)
Træning I de første uger har det fiktive CSIRT brugt flere fiktive cases (som de fik som eksempler fra andre CSIRT'er), der blev brugt som øvelse. Endvidere har de udsendt nogle sikkerhedsbulletiner baseret på virkelig sårbarhedsinformation udsendt af hard- og softwareleverandører, som de finpudsede og tilpassede konstituenternes behov.

11 Konklusion

Her slutter vejledningen. Denne publikation har til formål at give et helt koncist overblik over de forskellige processer, der er nødvendige for at oprette et CSIRT. Den skal ikke opfattes som fuldstændig, og den går heller ikke for meget ned i specifikke detaljer. Se afsnit *A.1 Yderligere læsning* i bilaget, og find nævneværdig litteratur om det emne, du vil vide mere om.

De næste vigtige skridt for det fiktive CSIRT vil nu være at:

- få feedback fra konstituenterne for at finpudse de tjenester, der ydes
- få rutine i det daglige arbejde
- træne nødsituationer
- bevare en tæt kontakt med de forskellige CSIRT-fællesskaber med det formål en dag at bidrage til deres frivillige arbejde

12 Beskrivelse af projektplanen

NB: Projektplanen er et første skøn over den krævede tid. Afhængig af de disponible ressourcer kan projektets reelle varighed være anderledes.

Projektplanen foreligger i forskellige formater på cd og på ENISA's websted. Det dækker fuldstændig alle de processer, der er beskrevet i dette dokument.

Hovedformatet vil være Microsoft Project, så det direkte kan bruges i dette projektstyringsværktøj.

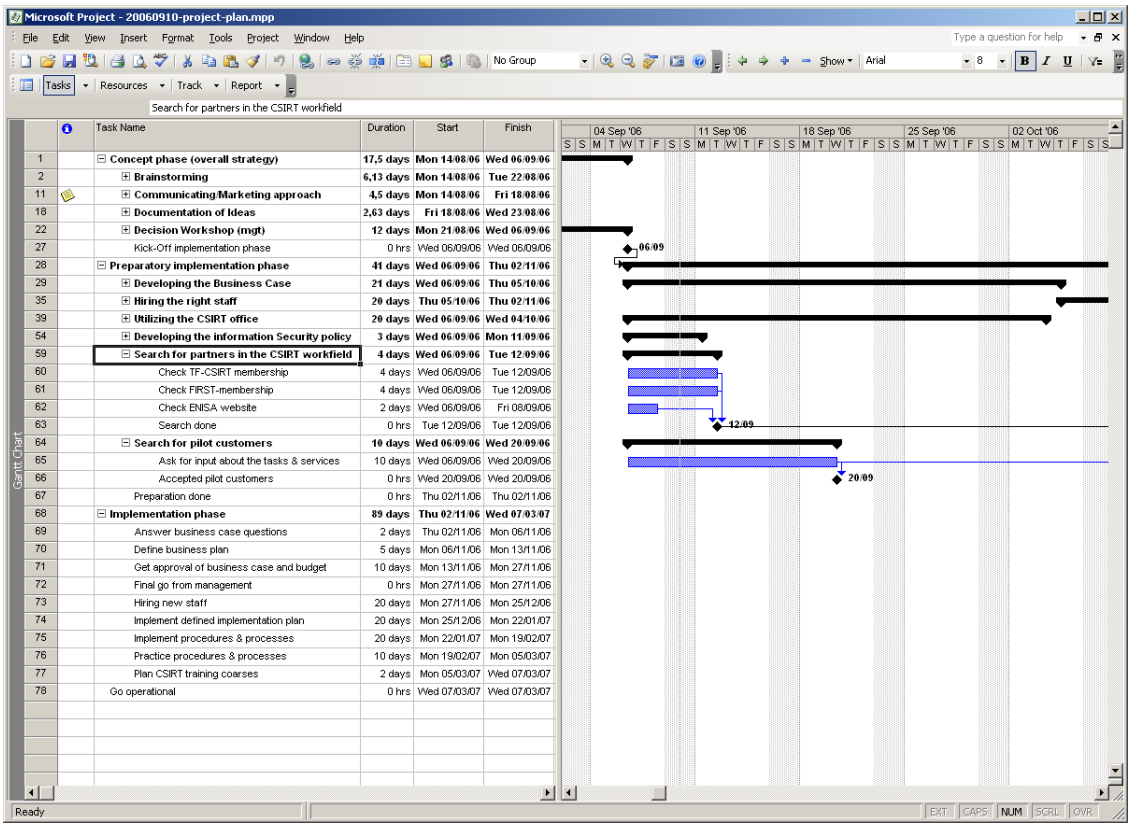
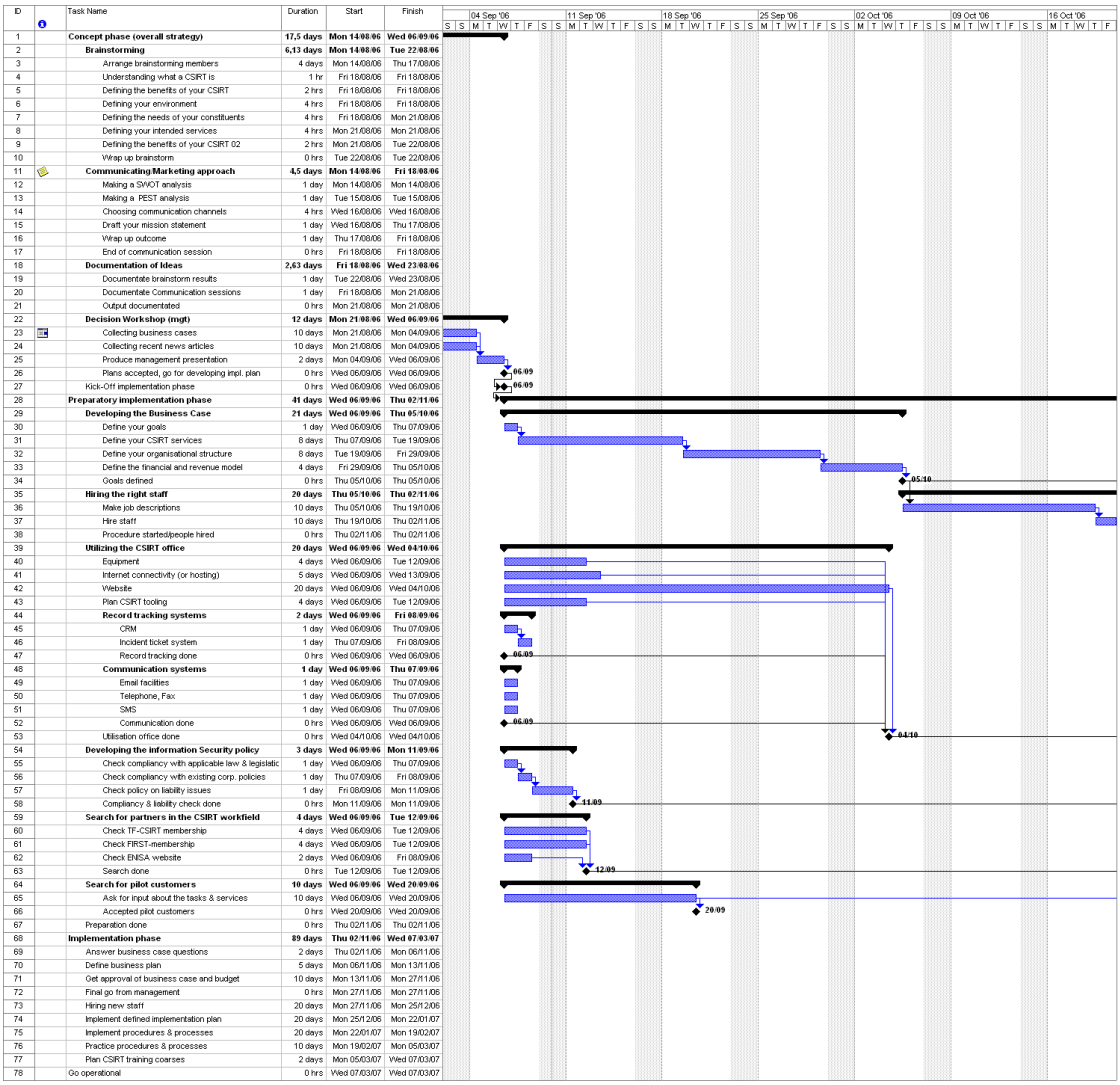


Fig. 17 Projektplan.



ID	Task Name	Duration	Start	Finish
1	**Concept phase (overall strategy)**	**17,5 days**	**Mon 14/08/06**	**Wed 06/09/06**
2	**Brainstorming**	**6,13 days**	**Mon 14/08/06**	**Tue 22/08/06**
3	Arrange brainstorming members	4 days	Mon 14/08/06	Thu 17/08/06
4	Understanding what a CSIRT is	1 hr	Fri 18/08/06	Fri 18/08/06
5	Defining the benefits of your CSIRT	2 hrs	Fri 18/08/06	Fri 18/08/06
6	Defining your environment	4 hrs	Fri 18/08/06	Fri 18/08/06
7	Defining the needs of your constituents	4 hrs	Fri 18/08/06	Mon 21/08/06
8	Defining your intended services	4 hrs	Mon 21/08/06	Mon 21/08/06
9	Defining the benefits of your CSIRT 02	2 hrs	Mon 21/08/06	Tue 22/08/06
10	Wrap up brainstorm	0 hrs	Tue 22/08/06	Tue 22/08/06
11	**Communicating/Marketing approach**	**4,5 days**	**Mon 14/08/06**	**Fri 18/08/06**
12	Making a SWOT analysis	1 day	Mon 14/08/06	Mon 14/08/06
13	Making a PEST analysis	1 day	Tue 15/08/06	Tue 15/08/06
14	Choosing communication channels	4 hrs	Wed 16/08/06	Wed 16/08/06
15	Draft your mission statement	1 day	Wed 16/08/06	Thu 17/08/06
16	Wrap up outcome	1 day	Thu 17/08/06	Fri 18/08/06
17	End of communication session	0 hrs	Fri 18/08/06	Fri 18/08/06
18	**Documentation of Ideas**	**2,63 days**	**Fri 18/08/06**	**Wed 23/08/06**
19	Documentate brainstorm results	1 day	Tue 22/08/06	Wed 23/08/06
20	Documentate Communication sessions	1 day	Fri 18/08/06	Mon 21/08/06
21	Output documentated	0 hrs	Mon 21/08/06	Mon 21/08/06
22	**Decision Workshop (mgt)**	**12 days**	**Mon 21/08/06**	**Wed 06/09/06**
23	Collecting business cases	10 days	Mon 21/08/06	Mon 04/09/06
24	Collecting recent news articles	10 days	Mon 21/08/06	Mon 04/09/06
25	Produce management presentation	2 days	Mon 04/09/06	Wed 06/09/06
26	Plans accepted, go for developing impl. plan	0 hrs	Wed 06/09/06	Wed 06/09/06
27	Kick-Off implementation phase	0 hrs	Wed 06/09/06	Wed 06/09/06
28	**Preparatory implementation phase**	**41 days**	**Wed 06/09/06**	**Thu 02/11/06**
29	**Developing the Business Case**	**21 days**	**Wed 06/09/06**	**Thu 05/10/06**
30	Define your goals	1 day	Wed 06/09/06	Thu 07/09/06
31	Define your CSIRT services	8 days	Thu 07/09/06	Tue 19/09/06
32	Define your organisational structure	8 days	Tue 19/09/06	Fri 29/09/06
33	Define the financial and revenue model	4 days	Fri 29/09/06	Thu 05/10/06
34	Goals defined	0 hrs	Thu 05/10/06	Thu 05/10/06
35	**Hiring the right staff**	**20 days**	**Thu 05/10/06**	**Thu 02/11/06**
36	Make job descriptions	10 days	Thu 05/10/06	Thu 19/10/06
37	Hire staff	10 days	Thu 19/10/06	Thu 02/11/06
38	Procedure started/people hired	0 hrs	Thu 02/11/06	Thu 02/11/06
39	**Utilizing the CSIRT office**	**20 days**	**Wed 06/09/06**	**Wed 04/10/06**
40	Equipment	4 days	Wed 06/09/06	Tue 12/09/06
41	Internet connectivity (or hosting)	5 days	Wed 06/09/06	Wed 13/09/06
42	Website	20 days	Wed 06/09/06	Wed 04/10/06
43	Plan CSIRT tooling	4 days	Wed 06/09/06	Tue 12/09/06
44	**Record tracking systems**	**2 days**	**Wed 06/09/06**	**Fri 08/09/06**
45	CRM	1 day	Wed 06/09/06	Thu 07/09/06
46	Incident ticket system	1 day	Thu 07/09/06	Fri 08/09/06
47	Record tracking done	0 hrs	Wed 06/09/06	Wed 06/09/06
48	**Communication systems**	**1 day**	**Wed 06/09/06**	**Thu 07/09/06**
49	Email facilities	1 day	Wed 06/09/06	Thu 07/09/06
50	Telephone, Fax	1 day	Wed 06/09/06	Thu 07/09/06
51	SMS	1 day	Wed 06/09/06	Thu 07/09/06
52	Communication done	0 hrs	Wed 06/09/06	Wed 06/09/06
53	Utilisation office done	0 hrs	Wed 04/10/06	Wed 04/10/06
54	**Developing the information Security policy**	**3 days**	**Wed 06/09/06**	**Mon 11/09/06**
55	Check compliancy with applicable law & legislatic	1 day	Wed 06/09/06	Thu 07/09/06
56	Check compliancy with existing corp. policies	1 day	Thu 07/09/06	Fri 08/09/06
57	Check policy on liability issues	1 day	Fri 08/09/06	Mon 11/09/06
58	Compliancy & liability check done	0 hrs	Mon 11/09/06	Mon 11/09/06
59	**Search for partners in the CSIRT workfield**	**4 days**	**Wed 06/09/06**	**Tue 12/09/06**
60	Check TF-CSIRT membership	4 days	Wed 06/09/06	Tue 12/09/06
61	Check FIRST-membership	4 days	Wed 06/09/06	Tue 12/09/06
62	Check ENISA website	2 days	Wed 06/09/06	Fri 08/09/06
63	Search done	0 hrs	Tue 12/09/06	Tue 12/09/06
64	**Search for pilot customers**	**10 days**	**Wed 06/09/06**	**Wed 20/09/06**
65	Ask for input about the tasks & services	10 days	Wed 06/09/06	Wed 20/09/06
66	Accepted pilot customers	0 hrs	Wed 20/09/06	Wed 20/09/06
67	Preparation done	0 hrs	Thu 02/11/06	Thu 02/11/06
68	**Implementation phase**	**89 days**	**Thu 02/11/06**	**Wed 07/03/07**
69	Answer business case questions	2 days	Thu 02/11/06	Mon 06/11/06
70	Define business plan	5 days	Mon 06/11/06	Mon 13/11/06
71	Get approval of business case and budget	10 days	Mon 13/11/06	Mon 27/11/06
72	Final go from management	0 hrs	Mon 27/11/06	Mon 27/11/06
73	Hiring new staff	20 days	Mon 27/11/06	Mon 25/12/06
74	Implement defined implementation plan	20 days	Mon 25/12/06	Mon 22/01/07
75	Implement procedures & processes	20 days	Mon 22/01/07	Mon 19/02/07
76	Practice procedures & processes	10 days	Mon 19/02/07	Mon 05/03/07
77	Plan CSIRT training coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Fig. 18 Projektplanen med alle opgaver og en del af et Gantkort.

Projektplanen foreligger også i CVS- og XML-format. ENISA's CSIRT-eksperter kan spørges til råds om yderligere brug: CERT-Relations@enisa.europa.eu

TILLÆG

A.1 Yderligere læsning

Handbook for CSIRTs (CERT/CC)
Håndbogen for CSIRT'er er et meget omfattende referenceværk om alle emner af relevans for et CSIRT's arbejde
Kilde: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Defining Incident Management Processes for CSIRTs: A Work in Progress
En tilbundsgående analyse af hændelsesstyring
Kilde: http://www.cert.org/archive/pdf/04tr015.pdf

State of the Practice of Computer Security Incident Response Teams (CSIRTs)
En omfattende analyse af den aktuelle situation i det verdensomspændende CSIRT-landskab, bl.a. historie, statistikker og meget mere
Kilde: http://www.cert.org/archive/pdf/03tr001.pdf

CERT-in-a-box
En omfattende beskrivelse af erfaringerne med oprettelse af GOVCERT.NL og den nederlandske nationale varslingstjeneste 'De Waarschuwingsdienst'.
Kilde: http://www.govcert.nl/render.html?it=69

RFC 2350: Expectations for Computer Security Incident Response
Kilde: http://www.ietf.org/rfc/rfc2350.txt

NIST[37] Computer Security Incident Handling Guide
Kilde: http://www.securityunit.com/publications/sp800-61.pdf

ENISA Inventory of CERT activities in Europe
ENISA's oversigt over CERT-aktiviteter i Europa er et referenceværk med information om CSIRT'er i Europa og deres forskellige aktiviteter
Kilde: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: National Institute of Standards and Technologies

A.2 CSIRT-tjenester

En særlig tak til CERT/CC, der har udarbejdet denne liste

Reaktive tjenester	***Proaktive tjenester***	***Håndtering af artefakter***
• Varslinger og advarsler • Håndtering af sikkerhedshændelser • Analyse af hændelser • Incident response på stedet • Support til incident response • Koordinering af incident response • Håndtering af sårbarhed • Analyse af sårbarhed • Indsats mod sårbarhed • Koordinering af indsatsen mod sårbarhed	• Meddelelser • Teknologiovervågning • Sikkerhedsaudit eller -vurdering • Konfiguration og vedligeholdelse af sikkerhed • Udvikling af sikkerhedsværktøjer • Tjenester til detektering af uautoriseret adgang • Formidling af sikkerhedsrelateret information	• Artefaktanalyse • Artefaktrespons • Koordinering af artefakt-respons ***Sikkerhedskvalitetsstyring*** • Risikoanalyse • Fortsættelse af driften og genetablering efter en katastrofe • Sikkerhedsrådgivning • Bevidstgørelse • Uddannelse/Træning • Produktevaluering eller -certificering

Fig. 19 CSIRT-tjenester fra CERT/CC.

Ydelsesbeskrivelser

Reaktive tjenester

Reaktive tjenester er udformet med henblik på at besvare anmodninger om bistand, rapporter om hændelser fra CSIRT's konstituenter og eventuelle trusler eller angreb mod CSIRT-systemerne. Nogle tjenester kan iværksættes ved at give meddelelse til tredjemand eller se på overvågnings- eller IDS-logger og varslinger.

Varslinger og advarsler

Denne tjeneste går ud på at formidle information med en beskrivelse af et angreb fra indtrængende, sikkerhedssårbarhed, indtrængningsvarsel, computervirus eller -hoax og på at anbefale en kortsigtet handlingsplan til takling af det deraf opståede problem. Varslingen, advarslen eller bulletinen sendes som en reaktion på det aktuelle problem for at underrette konstituenterne om aktiviteten og give vejledning til beskyttelse af deres systemer eller genoprettelse af systemer, der eventuelt er blevet påvirket. Informationen kan udarbejdes af CSIRT'et eller kan videreformidles fra leverandører, andre CSIRT'er eller sikkerhedseksperter eller andre af konstituenterne.

Håndtering af sikkerhedshændelser

Håndtering af sikkerhedshændelser går ud på at modtage, triagere og reagere på forespørgsler og rapporter samt analysere hændelser og begivenheder. Særlige responsaktiviteter kan omfatte

- at træffe foranstaltninger til at beskytte systemer og netværk, der er berørt eller truet af indtrængende aktivitet
- at levere løsninger og afbødningsstrategier fra relevante bulletiner eller varslinger
- at se efter uvedkommende aktivitet på andre dele af netværket
- at filtrere netværkstrafik
- at genopbygge systemer
- at patche eller reparere systemer
- at udvikle andre svar eller omgåelsesstrategier.

Eftersom forskellige typer CSIRT'er gennemfører hændelseshåndteringsaktiviteter på forskellige måder, kategoriseres denne tjenesteydelse yderligere på grundlag af den udførte aktivitetstype og ydede bistand:

Hændelsesanalyse

Hændelsesanalyse foregår på mange niveauer, og der er mange delydelser. I al væsentlighed er hændelsesanalyse en gennemgang af al tilgængelig information og støttedokumentation eller artefakter i forbindelse med en hændelse eller begivenhed. Formålet med analysen er at afdække hændelsens rækkevidde, omfanget af den skade, hændelsen har forvoldt, hændelsens art og tilgængelige responsstrategier eller workarounds. CSIRT kan bruge resultaterne af sårbarheds- og artefaktanalysen (der beskrives nedenfor) til at forstå og udarbejde den mest fuldstændige og ajourførte analyse af, hvad der er sket på et bestemt system. CSIRT ser på sammenhængen på tværs af hændelser for at fastslå eventuelle indbyrdes relationer, tendenser, mønstre eller indtrængendes underskrifter. To delydelser, der kan leveres som led i en hændelsesanalyse – afhængig af CSIRT'ets mission, mål og processer – er:

Indsamling af retsligt bevismateriale

Indsamling, bevaring, dokumentering og analyse af bevismateriale fra et skadet computersystem for at fastslå ændringer i systemet og bistå ved rekonstruktionen af de begivenheder, der førte til skaden. Denne indsamling af information og bevismateriale skal gøres på en måde, der dokumenterer en bevisbar effektstyring, som en domstol kan godkende i henhold til bevisreglerne. Opgaverne i forbindelse med indsamling af retsligt bevismateriale omfatter (men er ikke begrænset til) at tage en bit-image kopi af det berørte systems harddiskdrev, at kontrollere ændringer i systemet, f.eks. nye programmer, filer, tjenester og brugere, at se på kørende processer og åbne porte samt tjekke for trojanske heste og toolkot. CSIRT-medarbejdere, der udfører dette job, må også være forberedt på at skulle møde som ekspertvidner under retssager.

Tracking eller tracing

Sporing af en indtrængendes oprindelse eller afdækning af systemer, som den indtrængende havde adgang til. Denne aktivitet kan indebære tracking eller tracing af, hvordan den indtrængende kom ind i de ramte systemer og tilknyttede netværk, hvilke systemer der blev brugt til at få den adgang, hvor angrebet startede fra, og hvilke andre systemer og netværk der blev brugt som led i angrebet. Det kan også indebære, at man prøver at finde frem til den indtrængendes identitet. Dette arbejde kan gøres alene, men

normalt samarbejder man med politi eller retsvæsen, internetudbydere eller andre involverede organisationer.

Incident response på stedet

CSIRT yder direkte bistand på stedet for at hjælpe konstituenterne med genoprettelsen efter en hændelse. CSIRT analyserer selv fysisk de ramte systemer og udfører reparation og genoprettelse af systemerne i stedet for kun at yde support til genoprettelse efter en hændelse pr. telefon eller e-mail (jf. nedenfor). Denne tjeneste omfatter alle foranstaltninger på lokalt plan, der er nødvendige, hvis der er mistanke om en hændelse, eller hvis den opstår. Hvis CSIRT'et ikke er etableret i den ramte virksomhed/organisation, rejser teammedlemmerne til det pågældende sted og udfører genoprettelsen. I andre tilfælde kan der allerede være et lokalt team på stedet, som yder incident response som led i sit rutinearbejde. Dette gælder navnlig, hvis det er en del af system-, netværks- eller sikkerhedsadministratorernes normale jobfunktion at yde hændelseshåndtering i stedet for et etableret CSIRT.

Support til incident response

CSIRT bistår og vejleder ofret/ofrene for angrebet med genoprettelse efter en hændelse via telefon, e-mail, fax eller dokumentation. Her kan være tale om teknisk bistand med fortolkning af indsamlede data, levering af kontaktinformation eller viderebringelse af vejledning om afbødnings- og genoprettelsesstrategier. Det indebærer ikke direkte incident responsforanstaltninger på stedet som beskrevet ovenfor. CSIRT giver i stedet vejledning off-site, så personalet på stedet selv kan udføre genoprettelsen.

Koordinering af incident response

CSIRT koordinerer responsindsatsen mellem de parter, der er involveret i hændelsen. Det omfatter sædvanligvis ofret for angrebet, andre virksomheder, der har været udsat for angrebet, og virksomheder, som eventuelt behøver bistand til analyse af angrebet. Det kan også omfatte parter, der yder it-support til ofret, såsom internetudbydere, andre CSIRT'er samt system- og netværksadministratorer på stedet. Koordineringsarbejdet kan indebære indsamling af kontaktinformation, underretning af virksomheder om, at de måske er omfattet (som offer eller kilde til et angreb), indsamling af statistikker om antallet af involverede virksomheder samt fremme af informationsudveksling og analyse. En del af koordineringsarbejdet kan indebære underretning af og samarbejde med en organisations juridiske rådgiver samt HR- eller PR-afdelinger. Det kan også omfatte koordinering med politi og retsvæsen. Denne tjenesteydelse omfatter ikke direkte incident response på stedet.

Håndtering af sårbarhed

Håndtering af sårbarhed indebærer at modtage information og rapporter om sårbarheder i hardware og software, at analysere sårbarhedernes art, mekanik og virkninger samt at udvikle responsstrategier for detektering og reparation af sårbarhederne. Eftersom sårbarhedshåndteringsaktiviteter gennemføres på forskellige måder af forskellige typer CSIRT'er, kategoriseres denne tjeneste yderligere på grundlag af den udførte aktivitetstype og ydede bistand:

Sårbarhedsanalyse

CSIRT udfører teknisk analyse og undersøgelse af sårbarheder i hardware og software. Dette omfatter verifikation af mistænkte sårbarheder og teknisk gennemgang af sårbarhed i hardware eller software for at fastslå, hvor den sidder, og hvordan den kan

udnyttes. Analysen kan omfatte revision af kildekode, brug af en fejlretter for at fastslå, hvor sårbarheden opstår eller forsøg på at reproducere problemet i et testsystem.

Indsats mod sårbarhed

Denne tjeneste går ud på at finde frem til den relevante respons for at afbøde eller reparere sårbarheden Det kan betyde, at der skal udvikles eller søges efter ”patches”, ”fixes” og ”workarounds”. Det betyder også, at andre skal underrettes om afbødningsstrategien, muligvis ved at udarbejde og udsende bulletiner eller varslinger. Denne tjeneste kan omfatte udførelse af responsen ved at installere patches, fixes, eller workarounds.

Koordinering af indsatsen mod sårbarhed

CSIRT underretter de forskellige dele af virksomheden eller konstituenterne om sårbarheden og deler information om, hvordan sårbarheden kan rettes eller afbødes. CSIRT verificerer, at implementeringen af responsstrategien mod sårbarhed er vellykket. Denne tjeneste kan indebære kommunikation med leverandører, andre CSIRT’er, tekniske eksperter, konstituenter og de enkeltpersoner eller grupper, der oprindelig opdagede eller rapporterede sårbarheden. Aktiviteterne omfatter facilitering af analysen af en sårbarhed eller sårbarhedsrapport, koordinering af tidsplaner for frigivelse af tilsvarende dokumenter, patches eller workarounds og sammenfatning af tekniske analyser udført af forskellige parter. Tjenesteydelsen kan også omfatte opretholdelse af et offentligt eller privat arkiv eller en videnbase med information om sårbarhed og de tilhørende responsstrategier.

Artefakthåndtering

Et artefakt er en fil eller genstand fundet i et system, der kan være med til at sondere eller angribe systemer og netværk, eller som bruges til at nedbryde sikkerhedsforanstaltninger. Artefakter kan omfatte, men er ikke begrænset til, computervira, trojanske heste, orme, exploit scripts og toolkits.
Artefakthåndtering indebærer, at man modtager information om og kopier af artefakter, som bruges i uvedkommende angreb, rekognoscering og andre uautoriserede eller forstyrrende aktiviteter. Når artefaktet kommer ind, bliver det gennemgået. Det omfatter analyse af artefakternes art, mekanik, version og brug samt udvikling af (eller forslag til) responsstrategier til detektering og fjernelse af samt forsvar mod disse artefakter. Eftersom artefakthåndteringsaktiviteter gennemføres på forskellige måder af forskellige typer CSIRT’er, kategoriseres denne tjeneste yderligere på grundlag af den udførte aktivitetstype og ydede bistand:

Artefaktanalyse

CSIRT udfører en teknisk undersøgelse og analyse af et artefakt fundet på et system. Den udførte analyse kan omfatte afdækning af filtypen og artefaktets opbygning, sammenligning mellem et nyt artefakt og eksisterende artefakter eller andre versioner af samme artefakt for at se ligheder og forskelle eller gennemførelse af ”reverse engineering” eller ”disassembling” for at fastslå artefaktets formål og funktion.

Respons mod artefakter

Denne tjeneste indebærer, at man fastlægger passende foranstaltninger til at detektere og fjerne artefakter fra et system samt foranstaltninger til at forebygge installation af artefakter. Det kan betyde at oprette signaturer, der kan tilføjes til antivirussoftware eller IDS.

Koordinering af responsen mod artefakter

Denne tjeneste indebærer, at man deler og sammenfatter analyseresultater og responsstrategier, der er relevante for et artefakt, med andre forskere, CSIRT'er, leverandører og andre sikkerhedseksperter. Aktiviteterne omfatter, at man underretter andre og sammenfatter tekniske analyser fra en række forskellige kilder. Aktiviteterne kan også indebære, at man vedligeholder et offentligt arkiv eller et arkiv for konstituenter over kendte artefakter og deres virkninger samt tilhørende responsstrategier.

Proaktive tjenester

Proaktive tjenester er udformet til at forbedre konstituenternes infrastruktur og sikkerhedsprocesser, før en hændelse eller begivenhed indtræder eller detekteres. Hovedmålene er at undgå hændelser og nedbringe deres virkninger og rækkevidde, når de alligevel opstår.

Meddelelser

Det omfatter, men er ikke begrænset til, varslinger om indtrængen, advarsler om sårbarhed samt sikkerhedsbulletiner. Disse meddelelser informerer konstituenterne om nye udviklinger med mellem- til langsigtede virkninger, såsom nyligt fundne sårbarheder eller indtrængningsværktøjer. Meddelelserne giver konstituenterne mulighed for at beskytte deres systemer og netværk mod nye problemer, før de kan udnyttes.

Teknologiovervågning

CSIRT overvåger og observerer nye tekniske udviklinger, indtrængningsaktiviteter og tendenser i den forbindelse for at medvirke til at afdække fremtidige trusler. De emner, man ser på, kan udvides til at omfatte retsafgørelser og lovgivning, sociale eller politiske trusler og nye teknologier. Denne tjeneste indebærer, at man læser sikkerhedsmailinglister, sikkerhedswebsteder og aktuelle nyheds- og tidsskriftsartikler inden for områderne videnskab, teknologi, politik og forvaltning for at uddrage information af relevans for konstituenternes systemers og netværks sikkerhed. Det kan omfatte kommunikation med andre aktører, som er myndigheder på disse områder, for at sikre, at man får de bedste og mest præcise informationer eller fortolkninger. Resultatet af denne tjeneste kan være en form for meddelelse, retningslinjer eller anbefalinger orienteret mod mere mellem- til langsigtede sikkerhedsspørgsmål.

Sikkerhedsauditter eller -vurderinger

Denne tjeneste giver en detaljeret gennemgang og analyse af en organisations sikkerhedsinfrastruktur baseret på krav defineret af organisationen eller af andre gældende branchestandarder. Den kan også indebære en gennemgang af organisationens sikkerhedspraksis. Der kan ydes mange forskellige typer audit eller vurdering, bl.a.

Gennemgang af infrastruktur

Manuel gennemgang af hardware- og softwarekonfigurationer, routere, firewalls, servere og desktopanordninger for at sikre, at de svarer til organisationens eller branchens bedste praksis for sikkerhedspolitikker og standardkonfigurationer.

Gennemgang af god praksis

Interview med medarbejdere og system- og netværksadministratorer for at fastslå, om deres sikkerhedspraksis svarer til organisationens definerede sikkerhedspolitik eller nogen specifikke branchestandarder.

Scanning

Ved hjælp af sårbarheds- og virusscannere konstatere, om systemer og netværk er sårbare.

Indtrængningstest

Afprøvning af en virksomheds sikkerhed ved bevidst at angribe dets systemer og netværk.
Det kræver den øverste ledelses godkendelse, før man gennemfører en sådan audit eller vurdering. Nogle af disse metoder kan være forbudt i henhold til organisationens politik. Ydelse af denne tjeneste kan omfatte udvikling af en række fælles fremgangsmåder, som test eller vurderinger udføres efter, sammen med udvikling af en række nødvendige kvalifikationer eller certificeringskrav for medarbejdere, der udfører test, vurderinger, auditter eller revisioner. Denne tjeneste kan også outsources til en tredjepart eller en udbyder af ”managed security service” med den relevante ekspertise i gennemførelse af auditter og vurderinger.

Konfiguration og vedligeholdelse af sikkerhedsværktøjer, applikationer, infrastrukturer og tjenester

Denne tjeneste afdækker eller giver relevant vejledning i, hvordan man sikkert konfigurerer og vedligeholder de værktøjer og applikationer og den generelle computerinfrastruktur, der bruges af CSIRT's konstituenter eller af CSIRT selv. Ud over at give vejledning kan CSIRT udføre opdatering af konfigurationer og vedligeholdelse af sikkerhedsværktøjer og -tjenester, såsom IDS, netværksscanning eller overvågningssystemer, filtre, wrappere, firewalls, virtuelle private netværk (VPN) eller autentifikationssystemer. CSIRT kan endog yde disse tjenester som led i deres hovedfunktion. CSIRT kan også konfigurere og vedligeholde servere, stationære og bærbare computere, personal digital assistants (PDA'er) og andre trådløse anordninger, efter sikkerhedsretningslinjer. Denne tjeneste betyder, at alle spørgsmål eller problemer med konfigurationer eller brug af værktøjer og applikationer, som ifølge CSIRT kan gøre systemet sårbart over for angreb, skal meddeles ledelsen.

Udvikling af sikkerhedsværktøjer

Denne tjeneste omfatter udvikling af alle nye konstituent-specifikke værktøjer, der forlanges eller ønskes af konstituenterne eller af CSIRT selv. Den kan f.eks. omfatte udvikling af sikkerhedspatches til individuelt tilpasset software, der bruges af konstituenterne, eller sikret softwaredistribution, der kan bruges til at genopbygge kompromitterede værter. Den kan også omfatte udvikling af værktøjer eller scripts, der udvider funktionaliteten af eksisterende sikkerhedsværktøjer, såsom en ny plug-in til en

sårbarheds- eller netværksscanner, scripts, der letter brugen af krypteringsteknologi, eller automatiske patchdistributionsmekanismer.

Tjenester til detektering af uautoriseret adgang

CSIRT'er, der yder denne tjeneste, gennemgår eksisterende IDS-logs, analyserer og iværksætter en respons mod alle begivenheder, der opfylder deres definerede tærskel, eller fremsender varslinger ifølge en foruddefineret serviceniveauaftale eller eskaleringsstrategi. Detektering af uautoriseret adgang og analyse af de tilknyttede sikkerhedslogs kan være en dristig opgave – ikke blot med hensyn til at fastslå, hvor man skal placere følerne i miljøet, men med hensyn til at indsamle og derefter analysere de store mængder registrerede data. I mange tilfælde kræves der specialiserede værktøjer eller ekspertise for at sammenfatte og fortolke informationen for at afdække falske alarmer, angreb eller netværksbegivenheder og gennemføre strategier til at fjerne eller minimere sådanne begivenheder. Nogle organisationer vælger at outsource denne aktivitet til andre, der har mere ekspertise i at udføre disse tjenester, såsom udbydere af "managed security service".

Formidling af sikkerhedsrelateret information

Denne tjeneste giver konstituenterne en omfattende samling af nyttige informationer, der er lette at finde, og som bidrager til at forbedre sikkerheden. Disse informationer kan omfatte

- retningslinjer for rapportering og kontaktinformation til CSIRT
- arkiver over varslinger, advarsler og andre meddelelser
- materiale om aktuelt bedste praksis
- vejledning i generel computersikkerhed
- politikker, procedurer og tjeklister
- information om udvikling og distribution af patches
- leverandørlinks
- aktuelle statistikker og tendenser inden for rapportering af hændelser
- anden information, der kan forbedre den samlede sikkerhedspraksis

Denne information kan udvikles og offentliggøres af CSIRT eller af en anden del af organisationen (it, HR eller PR) og kan omfatte information fra eksterne kilder som f.eks. andre CSIRT'er, leverandører og sikkerhedseksperter.

Sikkerhedskvalitetsstyringstjenester

Tjenester inden for denne kategori er ikke enestående for hændelseshåndtering eller CSIRT'er i særdeleshed. De er velkendte, etablerede tjenester, der er udformet, så de forbedrer en organisations samlede sikkerhed. Et CSIRT kan – ved at udnytte de erfaringer, det har indhøstet gennem levering af de ovenfor beskrevne reaktive og proaktive tjenester – give disse kvalitetsstyringsafdelinger nogle enestående perspektiver, der ellers ikke ville have været tilgængelige. Disse tjenester skal samle feedback og erfaringer på grundlag af den viden, der udvikles ved at reagere på hændelser, sårbarheder og angreb. Hvis man fodrer de etablerede, traditionelle afdelinger (der beskrives nedenfor) med sådanne erfaringer som led i en sikkerhedskvalitetsstyringsproces, kan det forbedre den langsigtede sikkerhedsindsats i en organisation. Alt efter organisationens strukturer og ansvarsområder kan et CSIRT yde disse tjenester eller deltage som en del af en større organisatorisk teamindsats.
I følgende beskrivelser forklares det, hvordan CSIRT-eksperter kan udnytte hver af disse sikkerhedskvalitetsstyringstjenester.

Risikoanalyse

CSIRT'er kan være i stand til at øge værdien af risikoanalyse og -vurderinger. Dette kan forbedre organisationens evne til at vurdere reelle trusler, give realistiske kvalitative og kvantitative vurderinger af risici for informationsaktiver og evaluere beskyttelses- og responsstrategier. CSIRT'er, der udfører denne tjenesteydelse, gennemfører eller bistår ved risikoanalyseaktiviteter i forbindelse med informationssikkerhed for nye systemer og forretningsprocesser eller vurderer trusler og angreb mod konstituentens aktiver og systemer.

Planlægning af fortsættelse af driften og genoprettelse efter en katastrofe

På grundlag af tidligere oplevelser med og kommende prognoser for nye hændelses- eller sikkerhedstendenser har stadigt flere hændelser potentiale til at medføre alvorlig forringelse af erhvervslivets aktiviteter. Derfor bør man inddrage CSIRT'ernes erfaringer og anbefalinger i planlægningen, når man skal bestemme, hvordan man bedst kan reagere på sådanne hændelser for at sikre, at virksomhederne kan fortsætte deres drift. CSIRT'er, der udfører denne tjeneste, arbejder på, at virksomheden kan fortsætte sin drift og sikre genoprettelse efter en katastrofe i forbindelse med computersikkerhedstrusler og -angreb.

Sikkerhedsrådgivning

CSIRT'er kan bruges til at give råd og vejledning om bedste sikkerhedspraksis for gennemførelse af konstituenternes forretningsaktiviteter. Et CSIRT, der leverer denne tjeneste, arbejder med at udarbejde anbefalinger eller afdække krav til køb, installering eller sikring af nye systemer, netværksanordninger, softwareapplikationer eller forretningsgange i hele virksomheden. Tjenesten omfatter rådgivning og bistand i forbindelse med udvikling af sikkerhedspolitikker for organisationen eller konstituenten. Det kan også indebære, at man afgiver forklaring til eller rådgiver lovgivende myndigheder eller andre statslige organer.

Bevidstgørelse

CSIRT'er kan finde ud af, hvor konstituenter har brug for mere information og vejledning for at komme bedre i overensstemmelse med anerkendt sikkerhedspraksis og organisatoriske sikkerhedspolitikker. Hvis man øger den generelle bevidsthed om sikkerhed hos konstituentens medarbejdere, forbedrer det ikke blot deres forståelse for sikkerhedsspørgsmål, men hjælper dem også med at udføre deres daglige arbejde på en mere sikker måde. Det kan nedbringe forekomsten af vellykkede angreb og øge sandsynligheden for, at konstituenterne vil opdage og rapportere angreb og dermed nedbringe genoprettelsestiderne og fjerne eller minimere tab.
CSIRT'er, der udfører denne tjeneste, søger muligheder for at øge sikkerhedsbevidstheden ved at udarbejde artikler, plakater, nyhedsbreve, websteder eller andre informationsressourcer, der forklarer god sikkerhedspraksis og giver råd om, hvilke forholdsregler der bør tages. Aktiviteterne kan også omfatte planlægning af møder og seminarer for at holde konstituenterne ajour med igangværende sikkerhedsprocedurer og potentielle trusler mod organisatoriske systemer.

Uddannelse/træning

Denne tjeneste består i at informere konstituenterne om computersikkerhed gennem seminarer, workshopper, kurser og vejledning. Emnerne kan være retningslinjer for rapportering af hændelser, relevante responsmetoder, værktøjer til imødegåelse af hændelser, metoder til forebyggelse af hændelser og anden information, der er nødvendig for at beskytte, opdage, rapportere og reagere på computersikkerhedshændelser.

Produktevaluering eller -certificering

I forbindelse med denne tjeneste kan CSIRT gennemføre produktevalueringer af værktøjer, applikationer eller andre tjenester for at vurdere produkternes sikkerhed og sikre, at de lever op til anerkendt CSIRT- eller organisatorisk sikkerhedspraksis. De værktøjer og applikationer, der gennemgås, kan være open source eller kommercielle produkter. Denne tjeneste kan ydes som en vurdering eller gennem et certificeringsprogram, alt efter hvilke standarder der anvendes af organisationen eller af CSIRT.

A.3 Eksempler

Det Fiktive CSIRT

Trin 0 - Forståelse for, hvad et CSIRT er:

Vores fiktive CSIRT skal betjene en mellemstor institution med 200 medarbejdere. Institutionen har sin egen it-afdeling og to andre lokalafdelinger i samme land. It spiller en afgørende rolle for virksomheden, fordi den bruger it til intern kommunikation, datanet og e-business 24 timer i døgnet, 7 dage om ugen (24x7). Institutionen har sit eget net og har en ekstra forbindelse til internettet via to forskellige internetudbydere.

- -

Trin 1: Startfase

I startfasen planlægges det nye CSIRT som et internt CSIRT, der leverer tjenester til værtsvirksomheden, den lokale it-afdeling og medarbejderne. Det støtter og koordinerer også håndteringen af it-sikkerhedsrelaterede hændelser mellem de forskellige lokalafdelinger.

- -

Trin 2: Valg af de rette ydelser

I startfasen bliver det besluttet, at det nye CSIRT især vil fokusere på at levere nogle af kerneydelserne til medarbejderne.

Det bliver besluttet, at man efter en pilotfase kan overveje at udvide ydelsesporteføljen og måske tilføje nogle ”sikkerhedsstyringsydelser”. Den beslutning vil blive truffet på grundlag af feedback fra pilotkonstituenterne og i nært samarbejde med kvalitetssikringsafdelingen.

- -

Trin 3: Udarbejdelse af en analyse af konstituenterne og de relevante kommunikationskanaler

En brainstorm med nogle centrale personer fra ledelsen og konstituenterne gav tilstrækkeligt input til en SWOT-analyse. Det førte til den konklusion, at der er behov for kerneydelserne:

- varslinger og advarsler
- håndtering af sikkerhedshændelser (analyse, responssupport og koordinering af respons)
- meddelelser

Der skal sikres en velorganiseret distribution, så informationen når ud til den størst mulige del af konstituenterne. Derfor tager man den beslutning, at varslinger, advarsler og meddelelser i form af sikkerhedsbulletiner skal offentliggøres på et dedikeret websted og distribueres via en mailingliste. CSIRT faciliterer e-mail, telefon og telefax til at modtage rapporter om sikkerhedshændelser. Der planlægges en samlet web-formular til næste trin.

Trin 4: Mission statement

Ledelsen af det fiktive CSIRT har udarbejdet følgende mission statement:
"Det fiktive CSIRT leverer information og bistand til medarbejderne i sin værtsvirksomhed for at nedbringe risici for it-sikkerhedshændelser og reagere på sådanne hændelser, når de opstår."

Hermed gør det fiktive CSIRT det klart, at det er et internt CSIRT, og at dets kerneopgave er at varetage spørgsmål i forbindelse med it-sikkerhed.

- -

Trin 5: Udvikling af forretningsplan

Finansiel model
Da virksomheden har 24x7 e-business og også har en 24x7 it-afdeling, bliver det besluttet at yde fuld service i kontortiden og have en tilkaldevagt uden for kontortid. Ydelserne til konstituenterne bliver leveret gratis, men muligheden for at levere ydelser til eksterne kunder vil blive vurderet i pilot- og evalueringsfasen.

Indtægtsmodel
I start- og pilotfasen vil CSIRT blive finansieret gennem værtsvirksomheden. I pilot- og evalueringsfasen vil der blive drøftet supplerende finansiering, bl.a. muligheden for at sælge tjenesteydelser til eksterne kunder.

Organisationsmodel
Værtsorganisationen er en lille virksomhed, så derfor vælger man den indbyggede model.
I kontortiden vil en medarbejderstab på tre levere kerneydelserne (udsendelse af sikkerhedsbulletiner og håndtering/koordinering af hændelser).

Virksomhedens it-afdeling beskæftiger allerede mennesker med egnede kvalifikationer. Der indgås en aftale med it-afdelingen, således at det nye CSIRT kan anmode om støtte på ad hoc-basis, når der er behov for det. Deres tilkaldeteknikere i anden række kan også bruges.
Der bliver et kerne-CSIRT-team med fire fuldtidsansatte og fem supplerende CSIRT-teammedlemmer. Et af medlemmerne er også til rådighed på roterende skift.

Medarbejdere
CSIRT-teamlederen har erfaring med sikkerhed og support på 1. og 2. niveau og har udført arbejde inden for resiliens og krisestyring. De tre andre teammedlemmer er sikkerhedsspecialister. De CSIRT-teammedlemmer fra it-afdelingen, der arbejder på deltid, er specialister i hver deres del af virksomhedens infrastruktur.

Trin 5 Anvendelse af kontoret og informationssikkerhedspolitik
Kontorudstyr og placering
Eftersom værtsvirksomheden allerede har en effektiv fysisk sikkerhed på plads, er det nye CSIRT godt dækket ind i den retning. Der indrettes et såkaldt "kommandorum", hvor koordineringen kan foregå i tilfælde af en nødsituation. Der bliver indkøbt en boks til krypteringsmateriale og følsomme dokumenter. Der blev etableret en separat telefonlinje med et omstillingsbord til facilitering af en hotline i kontortiden og tilkaldevagtens mobiltelefon uden for kontortid med samme telefonnummer.

Det eksisterende udstyr og virksomhedens websted til CSIRT-relaterede meddelelser kan også bruges. Der installeres og vedligeholdes en mailinglistesoftware med en begrænset del til kommunikation mellem teammedlemmerne og med andre team. Alle kontaktoplysninger om medarbejderne lagres i en database, og en udskrift opbevares i boksen.

Regler
Da CSIRT er indbygget i en virksomhed, der allerede har informationssikkerhedspolitikker, er de tilsvarende politikker for CSIRT blevet udarbejdet med hjælp fra virksomhedens juridiske rådgiver.
- -
Trin 7 Vurdering af samarbejdsmuligheder
Ved at bruge ENISA's Inventory hurtigt kunne der findes og kontaktes nogle CSIRT'er i samme land. Der blev aftalt et besøg hos et af dem for den nyansatte teamleder. Han hørte om nationale CSIRT-aktiviteter og deltog i et møde.
Dette møde var særdeles nyttigt med hensyn til at indsamle eksempler på arbejdsmetoder og få støtte fra nogle andre team.
- -
Trin 8 Fremme af forretningsplanen

Det besluttes at samle fakta og tal fra virksomhedens historie. Det er særdeles nyttigt til at få et statistisk overblik over it-sikkerhedssituationen. Man bør fortsætte med at samle data, når CSIRT'et er kommet i gang for at holde statistikkerne ajour.

Andre nationale CSIRT'er blev kontaktet og interviewet om deres forretningsplaner. De ydede støtte ved at samle nogle dias med oplysninger om den seneste udvikling i it-sikkerhedshændelser og omkostningerne ved hændelserne.

I dette caseeksempel havde det fiktive CSIRT ingen presserende behov for at overbevise ledelsen om it-branchens betydning, så det var ikke svært at få grønt lys til det første skridt. Der blev udarbejdet en forretningsplan og en projektplan med bl.a. et skøn over etableringsomkostninger og driftsomkostninger.
- -

Trin 9 Etablering af processtrømme og operationelle og tekniske procedurer
Det fiktive CSIRT fokuserer på at levere kerne-CSIRT-ydelser:

- varslinger og advarsler
- meddelelser
- håndtering af sikkerhedshændelser

Teamet har udviklet procedurer, der fungerer godt, og som er lette at forstå for alle teammedlemmer. Det fiktive CSIRT har også ansat en juridisk ekspert til at tage sig af ansvar og informationssikkerhedspolitik. Teamet har indført nogle nyttige værktøjer og har gennem diskussioner med andre CSIRT'er fundet nyttig information om operationelle spørgsmål.

Der er blevet udviklet en fast model til sikkerhedsbulletiner og hændelsesrapporter. Teamet bruger RTIR til håndtering af hændelser.

- -

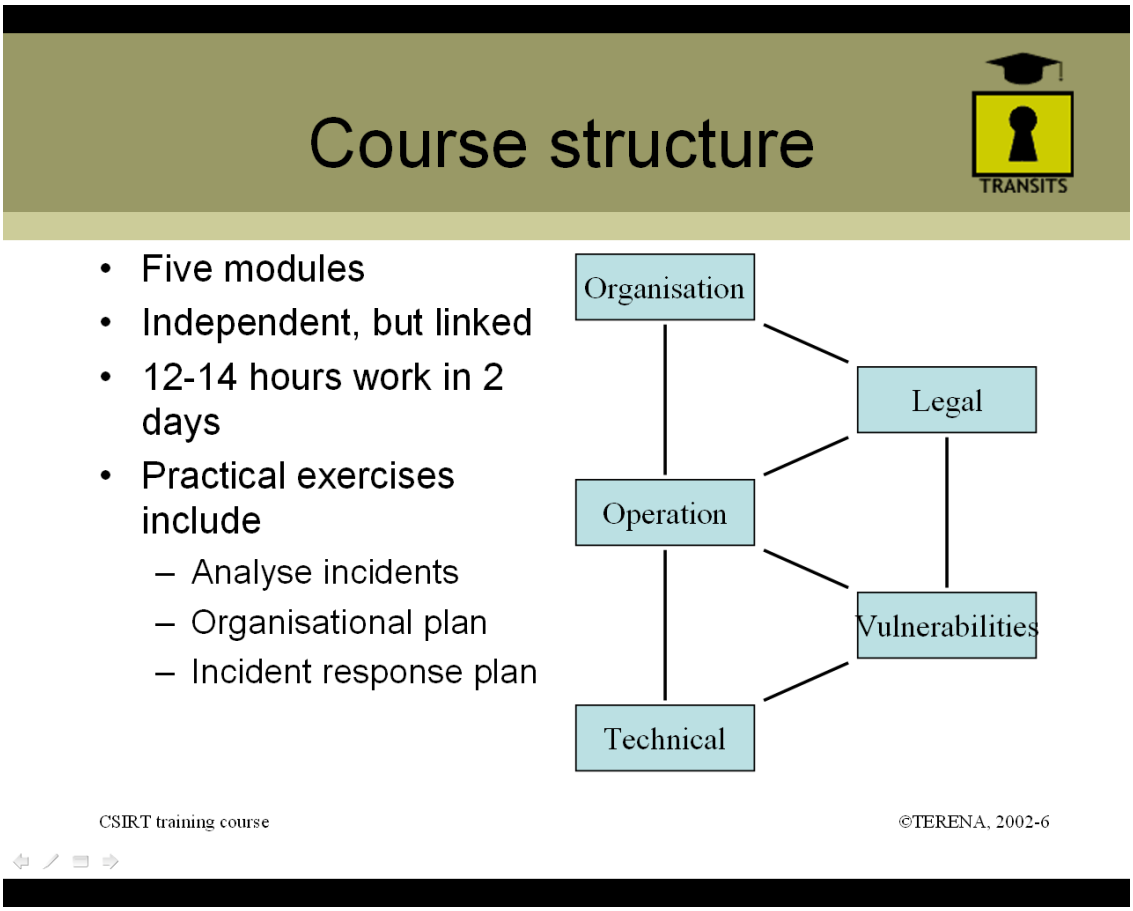
Trin 10 Uddannelse af medarbejdere
Det fiktive CSIRT beslutter at sende alle sine tekniske medarbejdere på de næste ledige TRANSITS-kurser. Teamlederen deltager desuden i CERT/CC's kursus om ledelse af et CSIRT, *Managing a CSIRT*.

- -

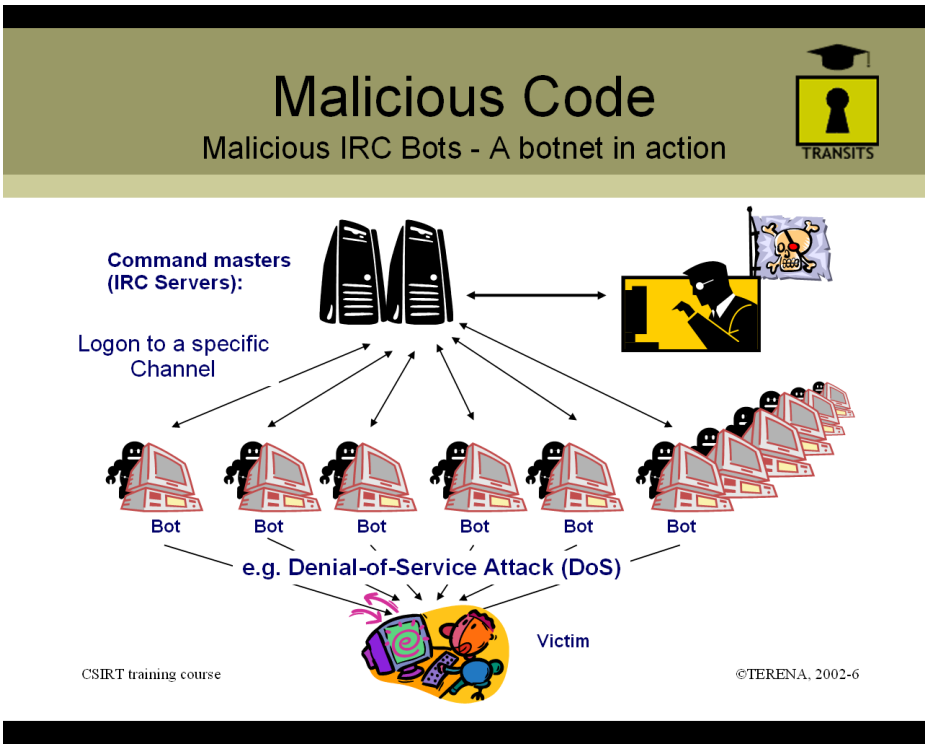
Trin 11: Træning
I de første uger har det fiktive CSIRT brugt flere fiktive cases (som de fik som eksempler fra andre CSIRT'er), der blev brugt som øvelse. Endvidere har de udsendt nogle sikkerhedsbulletiner baseret på virkelig sårbarhedsinformation udsendt af hard- og softwareleverandører, som de finpudsede og tilpassede konstituenternes behov.

A.4 Eksempel på materiale fra CSIRT-kurser

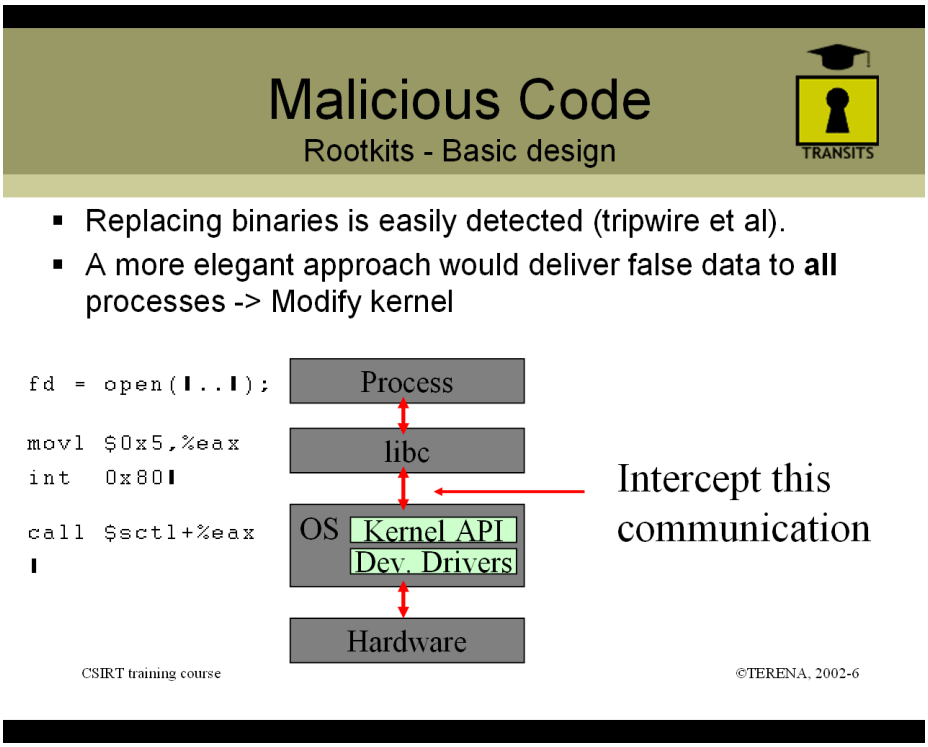
TRANSITS (Venligst stillet til rådighed af Terena, http://www.terena.nl)



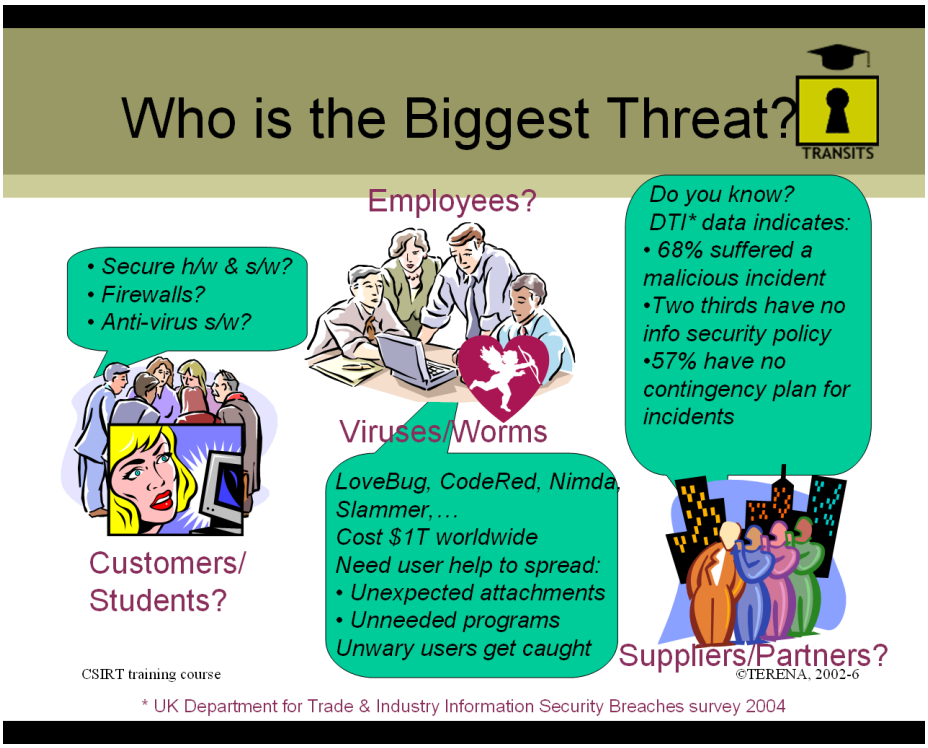
Oversigt: Kursusopbygning.



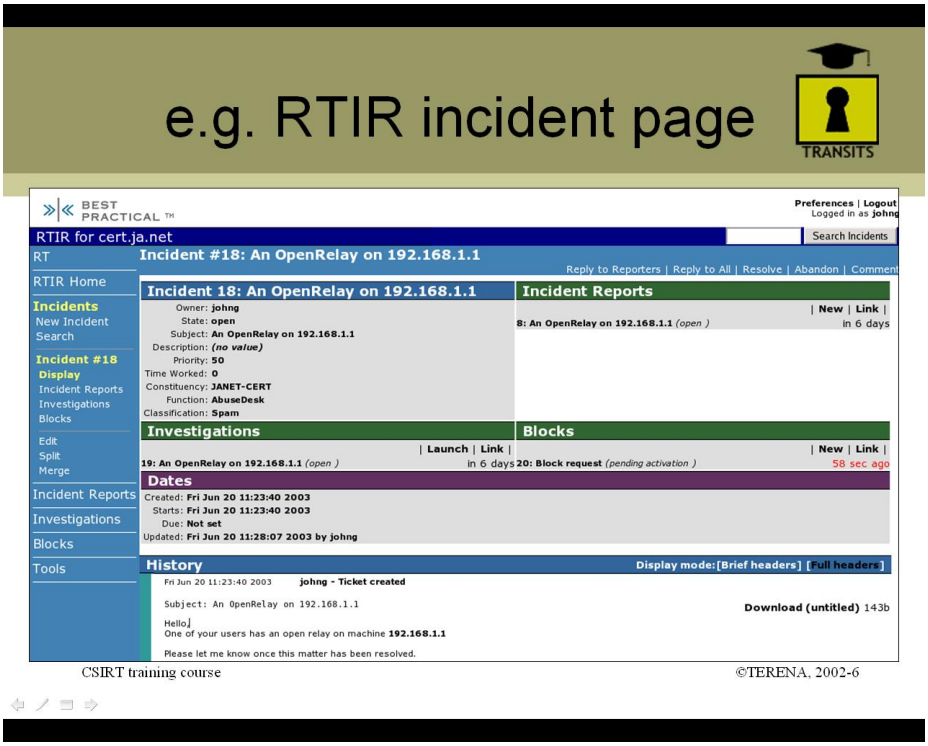
Fra det *tekniske modul*: Beskrivelse af et botnet.



Fra det *tekniske modul*: Grundlæggende opbygning af et rootkit.



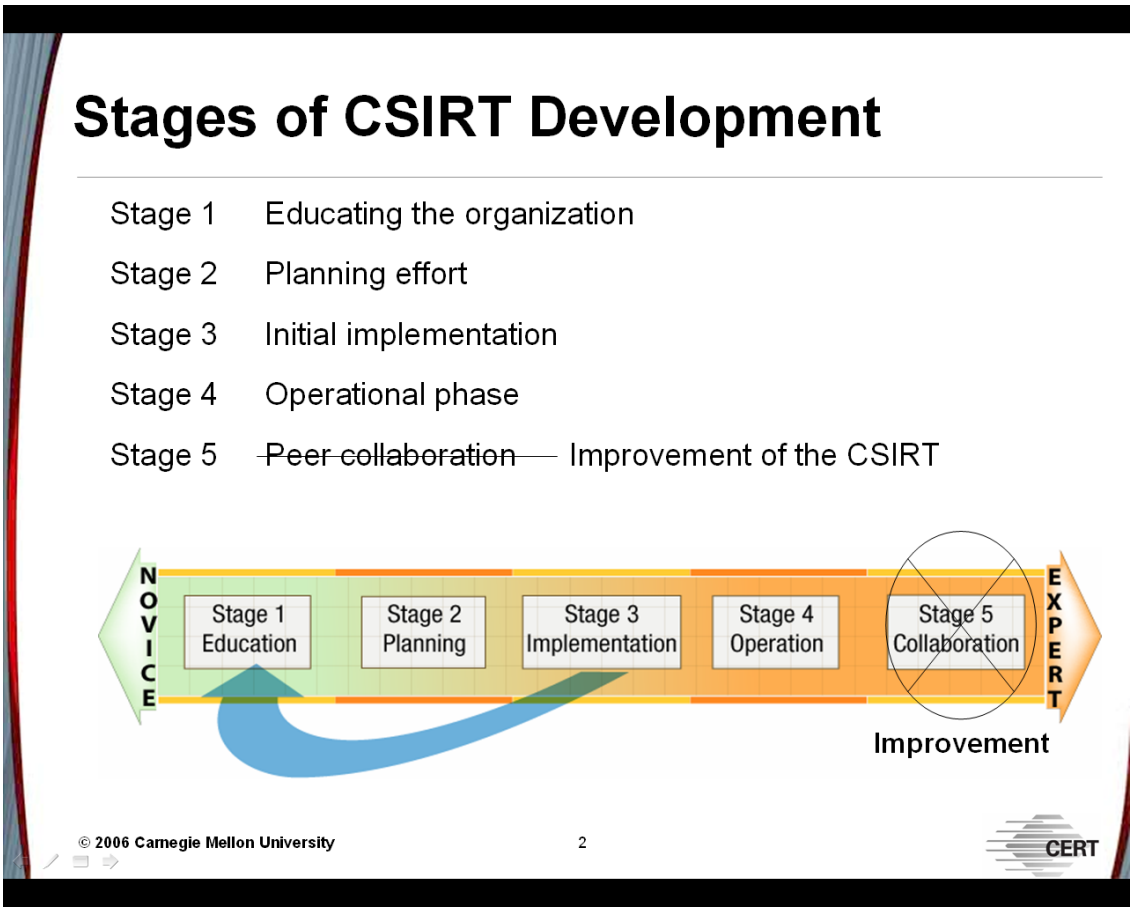
Fra *organisationsmodulet*: Hvor ligger den største trussel - i eller uden for virksomheden?



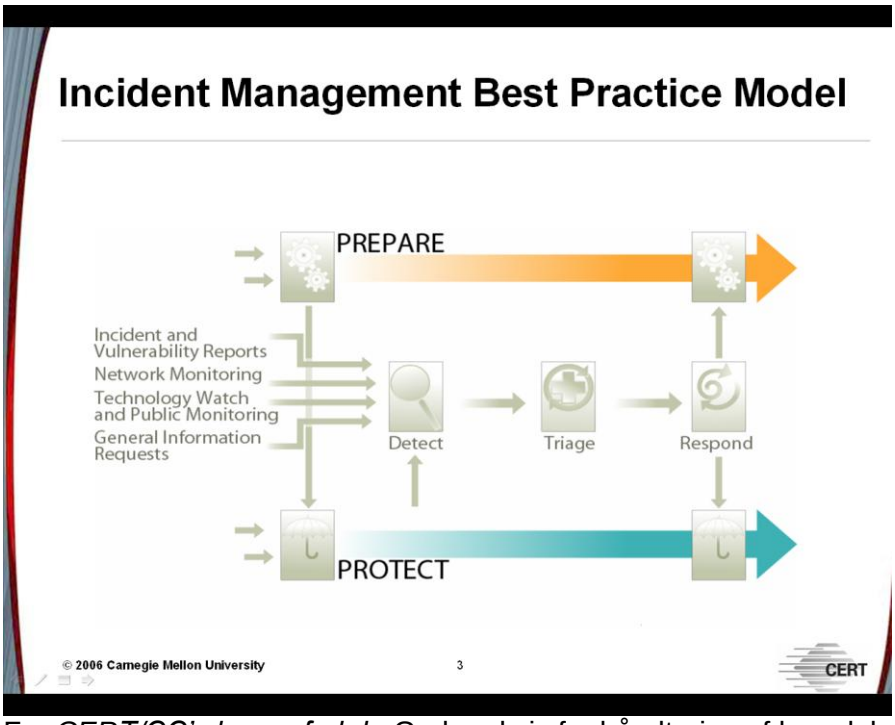
Fra *Operational track*: Request Tracker for Incident Response (RTIR)

"Oprettelse af et CSIRT" (venligst stillet til rådighed af CERT/CC, http://www.cert.org)

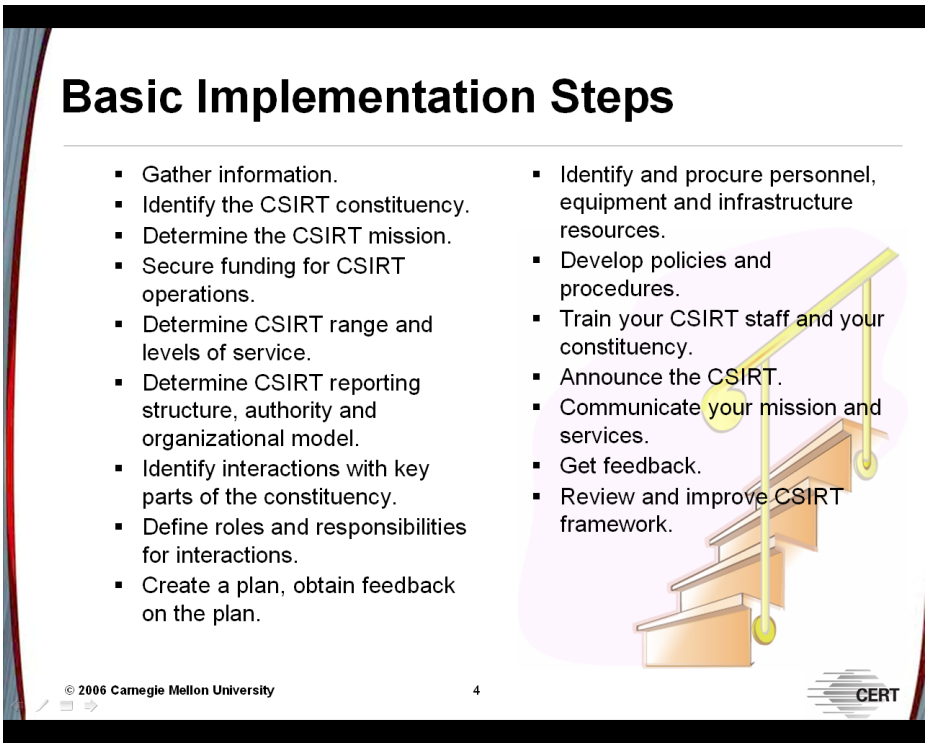
ENISA takker CSIRT-udviklingsteamet på CERT-programmet, som har ladet os bruge indhold fra deres kursusforløb!



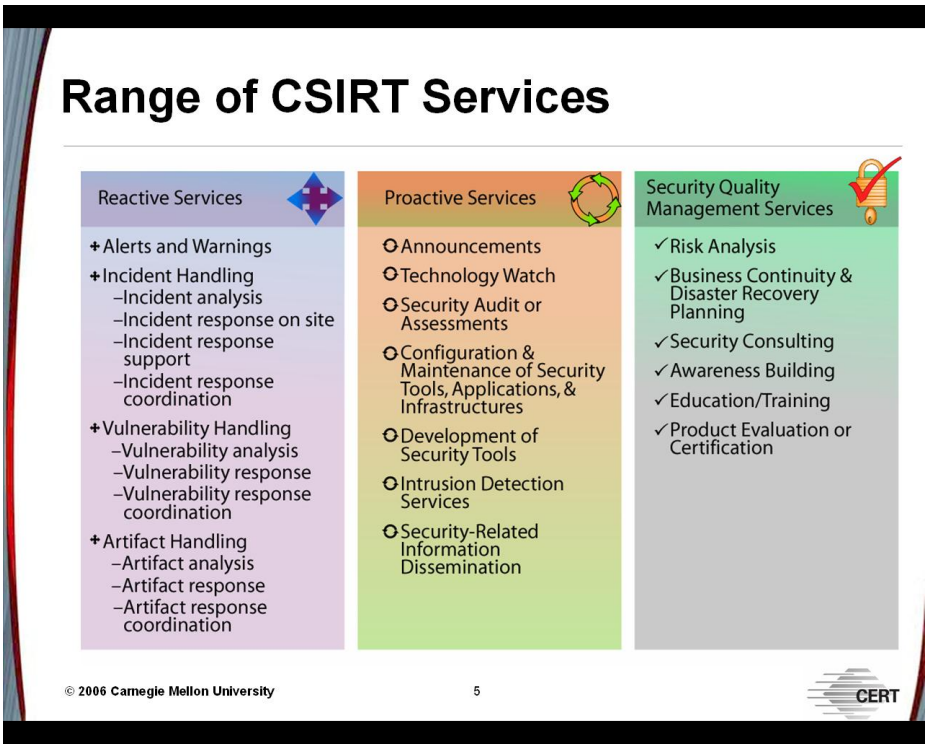
Fra *CERT/CC's kursusforløb*: De enkelte trin i udviklingen af et CSIRT.



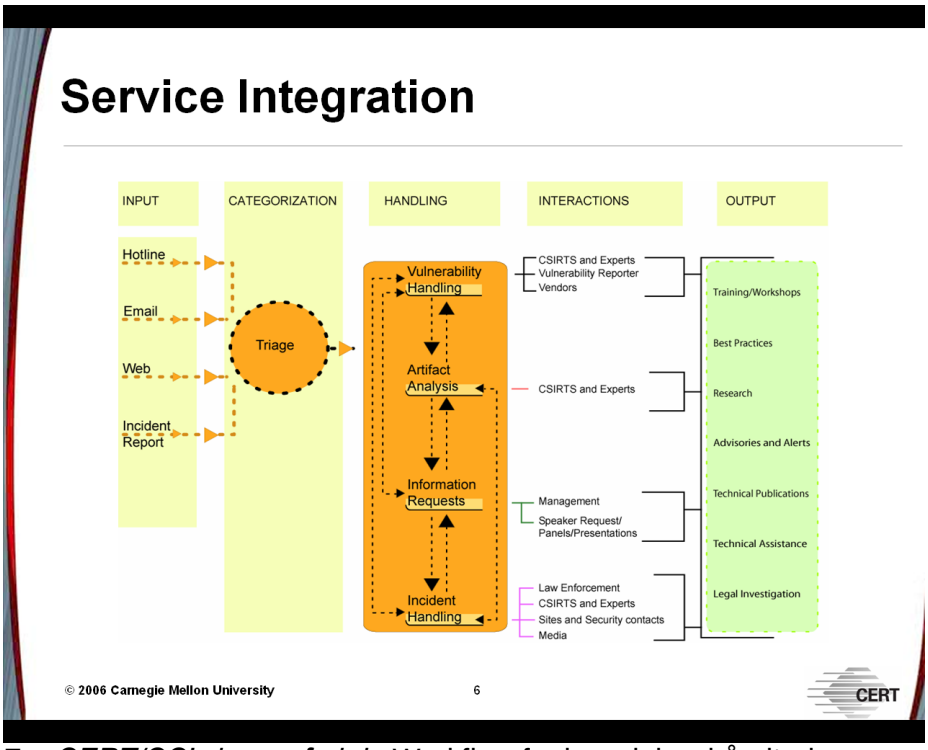
Fra *CERT/CC's kursusforløb*: God praksis for håndtering af hændelser.



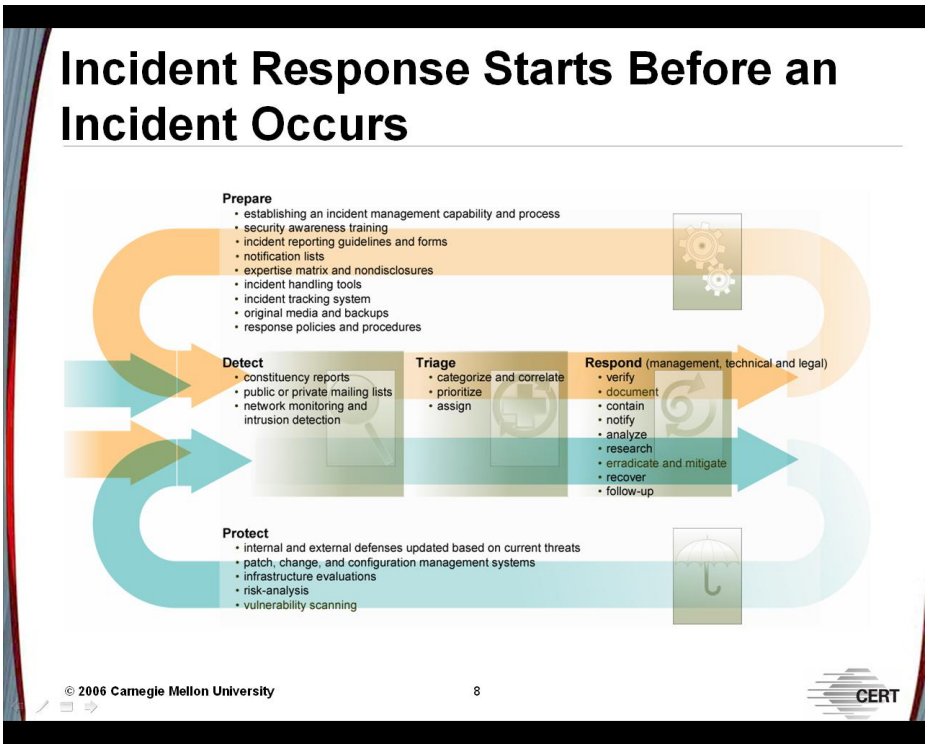
Fra *CERT/CC's kursusforløb*: Oprettelse af et CSIRT, trin for trin.



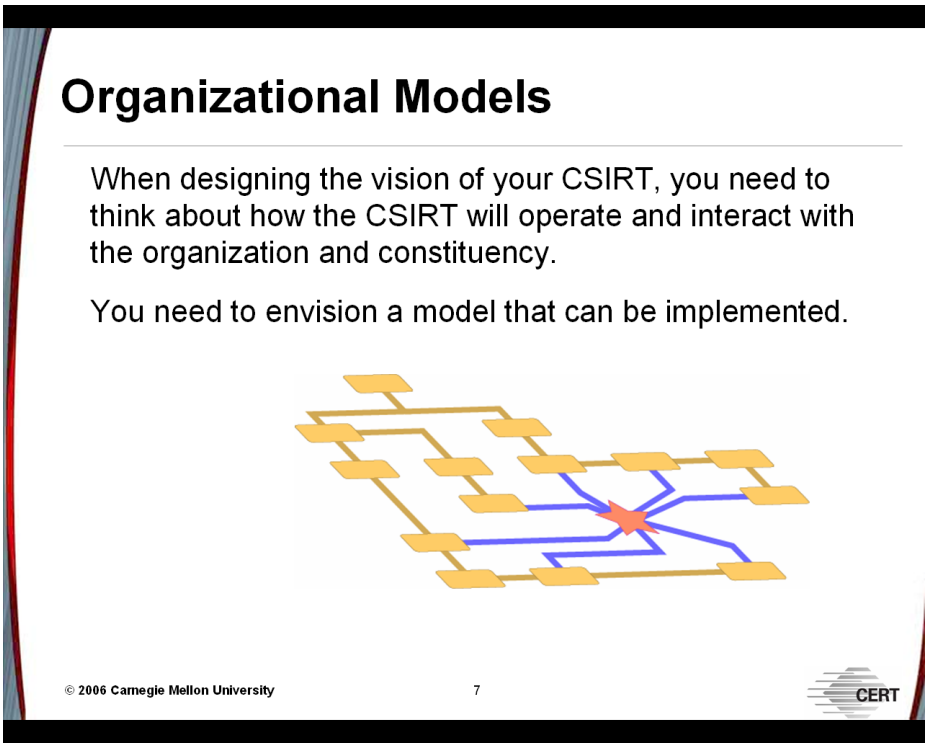
Fra *CERT/CC's kursusforløb*: De tjenester, et CSIRT kan levere.



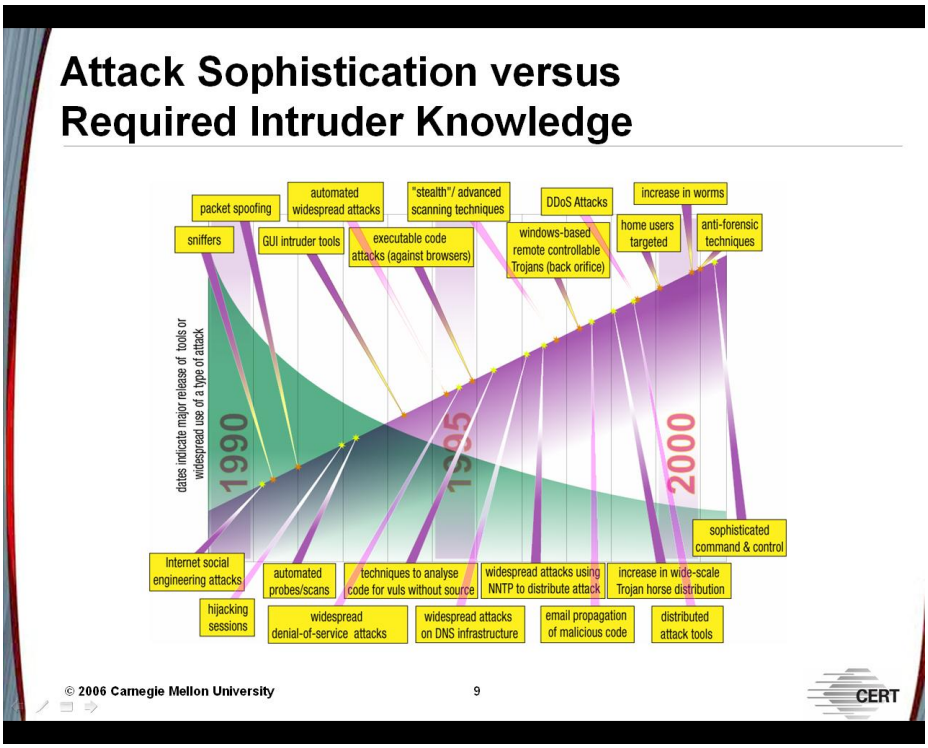
Fra *CERT/CC's kursusforløb*: Workflow for hændelseshåndtering.



Fra *CERT/CC's kursusforløb*: Incident response.



Fra *CERT/CC's kursusforløb*: Hvordan skal et CSIRT organiseres?



Fra *CERT/CC's kursusforløb*: Mindre viden, mere skade.