POSTUPNÝ PRÍSTUP K VYTVORENIU CSIRT

Predmet plnenia WP2006/5.1(CERT-D1/D2)

Obsah

1 Stručné zhrnutie

Tento dokument opisuje proces vytvorenia Tímu pre počítačovú bezpečnosť a reakciu na bezpečnostné incidenty – CSIRT *(Computer Security and Incident Response Team)* zo všetkých príslušných hľadísk, ako je obchodné riadenie, riadenie procesov a technické hľadisko. Tento dokument plní dve funkcie opísané v pracovnom programe Európskej agentúry pre bezpečnosť sietí a informácií – ENISA *(European Network and Information Security Agency)* na rok 2006, kapitola 5.1:

- Tento dokument: *Písomná správa o postupnom prístupe k vytvoreniu Tímu pre reakciu na počítačové útoky – CERT (Computer Emergency Response Team), vrátane príkladov (CERT-D1).* (**CERT-D1**)
- Kapitola 12 a externé súbory: *Výťah zo scenára v podrobnej forme, ktorý uľahčuje jeho použitie v praxi.* (**CERT-D2**)

2 Právne upozornenie

3 Poďakovanie

Agentúra ENISA by chcela poďakovať všetkým inštitúciám i jednotlivcom, ktorý sa na tomto dokumente podieľali. Zvláštne „Poďakovanie“ patrí nasledujúcim prispievateľom:

- Henkovi Bronkovi, ktorý ako konzultant spracoval prvú verziu tohto dokumentu.
- CERT/CC a najmä tímu pre rozvoj CSIRT, ktoré prispeli najužitočnejším materiálom a materiálom vzorového kurzu v prílohe.

- GovCERT.NL za poskytnutie CERT *in-a-box* (v jednom balíku).
- Tímu TRANSITS, ktorý prispel materiálom vzorového kurzu v prílohe.
- Kolegom z oddelenia pre bezpečnostné politiky v technickom odboru, ktorí sa podieľali na kapitole 6.6.
- a celému radu tých, ktorí tento dokument revidovali.

4 Úvod

Komunikačné siete a informačné systémy sa stali dôležitým faktorom v hospodárskom a sociálnom rozvoji. Programovanie a vytváranie sietí sa stávajú v súčasnosti všadeprítomnými verejnými službami rovnako ako dodávky elektrickej energie alebo vody.

Bezpečnosť komunikačných sietí a informačných systémov a najmä ich dostupnosť má preto čím ďalej tým väčšiu dôležitosť pre spoločnosť. Vyplýva to z rizika problémov pre kľúčové informačné systémy kvôli zložitosti, poruchám a chybám systému a útokom na fyzické infraštruktúry, ktoré dodávajú služby dôležité pre blahobyt občanov EÚEÚ.

Dňa 10. marca 2004 bola vytvorená Európska agentúra pre bezpečnosť sietí a informácií (ENISA)[1]. Jej cieľom bolo zaistiť vysokú a efektívnu úroveň bezpečnosti sietí a informácií v spoločenstve a rozvíjať kultúru bezpečnosti sietí a informácií na prospech občanov, spotrebiteľov, podnikov a organizácií verejného sektoru v rámci Európskej únie, a teda prispievať k plynulému fungovaniu vnútorného trhu.

Celý rad bezpečnostných organizácií v Európe ako CERT/CSIRT, tímy proti zneužívaniu a WARP už niekoľko rokov spolupracujú v záujme pre bezpečnejšieho Internetu. ENISA hodlá podporiť tieto organizácie v ich úsilí poskytovaním informácií o opatreniach pre zaistenie príslušnej úrovne kvality služieb. ENISA ďalej hodlá zvýšiť schopnosť poskytovať odborné rady členským štátom EÚ a orgánom EÚ v otázkach zaistenia príslušných bezpečnostných služieb pre špecifické skupiny užívateľov informačných technológií – IT *(Information Technology)*. Na základe záverov Pracovnej skupiny ad-hoc CERT pre spoluprácu a podporu vytvorenej v roku 2005 sa preto táto nová pracovná skupina bude zaoberať otázkami, ktoré sa týkajú poskytovania zodpovedajúcich bezpečnostných služieb („služby CERT“) pre špecifických užívateľov (kategórie alebo skupiny užívateľov).

ENISA podporuje vytvorenie nových tímov CSIRT uverejnením tejto svojej správy *„Postupný prístup k vytvoreniu CSIRT s doplňujúcim kontrolným zoznamom“,* ktorý Vám pomôže vytvoriť Váš vlastný tým CSIRT.

[1] Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií. Agentúra Európskeho spoločenstva“ je orgán zriadený EÚ pre plnenie veľmi špecifických technických, vedeckých alebo riadiacich úloh v „oblasti Spoločenstva“EÚ.

Cieľová skupina

Základné cieľové skupiny tejto správy sú štátne a iné inštitúcie, ktoré rozhodujú o vytvorení CSIRT s cieľom ochrany vlastnej infraštruktúry IT alebo infraštruktúry IT zainteresovaných strán.

Ako používať tento dokument

Tento dokument poskytuje informácie o tom, čo je CSIRT, aké služby môže zaistiť a aké nutné kroky treba urobiť pre začatie práce. Mal by dať čitateľovi dobrý a pragmatický prehľad o prístupe, štruktúre, a obsahu, ako vytvoriť CSIRT.

Kapitola 4 *„Úvod“*
Úvod k tejto správe

Kapitola 5 *„Celková stratégia pre plánovanie a vytvorenie CSIRT*“
Prvá časť uvádza opis, čo je CSIRT. Poskytne tiež informácie o rôznych prostrediach, v ktorých môžu tímy CSIRT pracovať, a o tom, aké služby môžu dodávať.

Kapitola 6 *„Vypracovanie obchodného plánu“*
Táto kapitola opisuje prístup obchodného vedenia k procesu vytvorenia týmu.

Kapitola 7 *„Podpora obchodného plánu“*
Táto kapitola sa zaoberá obchodným prípadom a otázkami financovania.

Kapitola 8 *„Príklady pracovných a technických postupov“*
Táto kapitola opisuje postup získavania informácií a ich prevedenia do bezpečnostného bulletinu. Táto kapitola tiež opisuje priebeh prác v riešení bezpečnostných incidentov.

Kapitola 9 *„Výcvik CSIRT“*
Táto kapitola poskytuje zhrnutie výcviku CSIRT, ktorý je k dispozícii. Pre ilustráciu je v prílohe uvedený materiál vzorového kurzu.

Kapitola 10 *„Cvičenie: poskytovanie poradenstva“*
Táto kapitola obsahuje cvičenie, ako uskutočňovať jednu zo základných (alebo kľúčových) služieb CSIRT: vytvorení bezpečnostného bulletinu (alebo poskytnutie poradenstva).

Kapitola 12 „Opis plánu projektu“
Tato kapitola poukazuje na doplňujúci plán projektu (kontrolný zoznam) uvedený v tejto príručke. Tento plán je zameraný na to, aby bol nástrojom, ktorý sa jednoducho použije pre zavedenie tejto príručky.

Obvyklé postupy používané v tomto dokumente

Aby sa čitateľovi poskytla pomoc, každá kapitola začína zhrnutím krokov urobených do daného momentu v procese vytvárania CSIRT. Tieto zhrnutia sú vysvetlené v rámčekoch, ako je nasledujúci:

Urobili sme prvý krok

Každá kapitola bude uzatvorená praktickým príkladom krokov, ktorými sa zaoberá. V tomto dokumente „Fiktívny CSIRT“ bude malý nezávislý CSIRT pre stredne veľkú spoločnosť alebo organizáciu. Zhrnutie možno nájsť v prílohe.

Fiktívny CSIRT

5 Celková stratégia pre plánovanie a vytvorenie CSIRT

Pre úspešné začatie procesu vytvorenia CSIRT je dôležité mať jasnú víziu o prípadných službách, ktoré môže tím poskytovať svojim zákazníkom, vo „svete CSIRT“ lepšie známe ako ‘zložky’. Z tohto dôvodu je nutné pochopiť, pre aké potreby zložiek sa majú poskytovať zodpovedajúce služby v príslušnej kvalite a včas.

Čo je CSIRT?

CSIRT znamená Tím pre reakciu na bezpečnostné incidenty počítačov *(Computer Security Incident Response Team)*. Termín CSIRT sa používa prevažne v Európe pre chránený názov CERT *(Computer Emergency Response Team* – Tím pre reakciu na počítačové útoky), ktorý si v USA zaregistrovalo Koordinačné stredisko CERT – CERT/CC *(CERT Coordination Center)*.
Existujú rôzne skratky používané pre rovnaký druh tímov:

- CERT alebo CERT/CC (Computer Emergency Response Team / Coordination Center – Tím pre reakciu na počítačové útoky /Koordinačné stredisko)
- CSIRT (Computer Security Incident Response Team – Tím pre reakciu na bezpečnostné incidenty počítačov)
- IRT (Incident Response Team – Tím pre reakciu na bezpečnostné incidenty)
- CIRT (Computer Incident Response Team – Tým pre reakciu na bezpečnostné incidenty počítačov)
- SERT (Security Emergency Response Team – Tím pre reakciu na ohrozenie bezpečnosti).

K prvému veľkému prieniku červa do celosvetovej infraštruktúry IT došlo koncom 80. rokov. Červ bol nazvaný Morris[2], rýchlo sa rozšíril a účinne infikoval veľký počet systémov IT po celom svete.

Tento bezpečnostný incident zapôsobil ako budík: ľudia si naraz uvedomili naliehavú potrebu spolupráce a koordinácie medzi správcami systémov a manažérmi IT, aby sa riešili také prípady ako tento. Keďže čas bol rozhodujúci faktor, musel sa vytvoriť organizovanejší a štruktúrovanejší prístup k riešeniu bezpečnostných incidentov IT. A tak niekoľko dní po „Bezpečnostnom incidente Morris“ Projekčná agentúra pre výskum zdokonalenej obrany – DARPA *(Defence Advanced Research Projects Agency)* vytvorila prvý tým CSIRT: Koordinačné stredisko CERT (CERT/CC[3]) so sídlom na Univerzite Carnegie Mellon v Pittsburghu (Pennsylvánia).

Tento model bol skoro prijatý v Európe a v roku 1992 holandský univerzitný prevádzkovateľ surfovacej siete SURFnet inicioval prvý tím CSIRT v Európe pod názvom SURFnet-CERT[4]. Potom nasledovalo mnoho tímov a v súčasnej dobe *Zoznam činností CERT v Európe* agentúry ENISA uvádza viac ako 100 známych tímov nachádzajúcich sa v Európe[5].

[2] Viacej informácií o červovi Morris http://en.wikipedia.org/wiki/Morris_worm

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

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

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

Tímy CERT po celé roky zdokonaľovali svoje schopnosti od iba reakčnej sily až po poskytovateľov komplexných bezpečnostných služieb, vrátane preventívnych služieb ako výstrahy, odborné rady v bezpečnosti a výcvik a služby manažmentu bezpečnosti. Po krátkom čase sa dospelo k názoru, že termín „CERT“ nie je dostačujúci. V dôsledku toho bol koncom 90. rokov vytvorený nový termín „CSIRT“. V súčasnej dobe sa obidva termíny (CERT a CSIRT) používajú ako synonymá s tým, že CSIRT je presnejší.

5..1 Termín zložka

Odteraz sa (v organizáciách CSIRT) dobre zavedený termín ‘zložka’ bude používať vo vzťahu k báze zákazníkov CSIRT. Jednotlivý zákazník sa bude uvádzať ako ‘zložka’ a skupina ako ‘zložky’.

5..2 Definícia CSIRT

CSIRT je tím expertov pre bezpečnosť IT, ktorých hlavnou úlohou je reagovať na bezpečnostné incidenty počítačov. Poskytuje potrebné služby pre ich riešenie a pre podporu svojich zložiek, aby sa zotavili z poruchy.

S cieľom znížiť riziká a minimalizovať počet potrebných reakcií, väčšina tímov CSIRT zaisťuje pre svoje zložky tiež preventívne a vzdelávacie služby. Dáva odborné rady týkajúce sa zraniteľnosti používaného softvéru a hardvéru a taktiež informuje užívateľov o zneužívaní a vírusoch, ktoré zneužívajú tieto chyby. Zložky môžu takto rýchle opraviť a aktualizovať svoje systémy. Úplný zoznam prípadných služieb pozri v kapitole 5.2 *Možné služby*.

5..3 Výhody existencie CSIRT

Keď má organizácia zanietený tím pre bezpečnosť IT, pomáha jej to znížiť veľké bezpečnostné incidenty, predchádzať im a chrániť svoj hodnotný majetok.

Ďalšie prípadné výhody sú:

- Centralizovaná koordinácia otázok bezpečnosti IT v rámci organizácie (kontaktné miesto – PoC *(Point of Contact))*.
- Centralizované a špecializované riešenie bezpečnostných incidentov IT a reakcia na ne.
- Odborné znalosti na podporu užívateľov a pre pomoc užívateľom, aby sa rýchle zotavili z bezpečnostných incidentov.
- Riešenie právnych otázok a uchovávanie dôkazov pre prípad súdneho sporu.
- Sledovanie rozvoja v oblasti bezpečnosti.
- Podnetná spolupráca v rámci zložky týkajúca sa bezpečnosti IT (vytváranie povedomia).

Fiktívny CSIRT (0. krok)

Pochopenie, čo je CSIRT:

Vzorový CSIRT bude slúžiť strednej organizácii, ktorá má 200 pracovníkov. Organizácia má vlastné oddelenie IT a dve ďalšie pobočky v tej istej krajine. IT hrá kľúčovú úlohu pre spoločnosť, lebo sa používa pre internú komunikáciu, dátovú sieť a elektronické obchodovanie 24 hodín denne, 7 dní v týždni. Organizácia má vlastnú sieť a disponuje redundantným pripojením k Internetu prostredníctvom dvoch poskytovateľov pripojenia do siete Internet – ISP *(Internet Service Provider)*.

5..4 Opis rôznych druhov prostredia CSIRT

Urobili sme prvý krok

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.

>> Ďalší krok je odpoveď na otázku: „Akému sektoru sa budú dodávať služby CSIRT?“

Keď sa začína s tímom CSIRT (rovnako ako s každou inou činnosťou), je veľmi dôležité rýchlo spracovať jasné stanovisko, kto sú zložky, a pre aký druh prostredia sa budú služby CERT rozvíjať. V tejto chvíli rozlišujeme nasledujúce ‘sektory’ uvedené v abecednom poriadku (pozn. prekl.: abecedný poriadok platí len pre anglický text):

- Akademický sektor CSIRT
- Komerčný CSIRT
- Sektor CIP/CIIP CSIRT
- Štátny sektor CSIRT
- Interný CSIRT
- Vojenský sektor CSIRT
- Národný CSIRT
- Malé a stredné podniky (SME) Sektor CSIRT
- CSIRT predajcov

Akademický sektor CSIRT

Zameranie

Akademický sektor CSIRT poskytuje služby CSIRT školským a vzdelávacím inštitúciám, ako sú vysoké školy alebo výskumné zariadenia a ich prostredie Internetu na školskej pôde.

Zložky

Typickými zložkami tohto typu CSIRT sú pracovníci a študenti vysokých škôl.

Komerčný CSIRT
Zameranie
Komerčný CSIRT poskytuje služby CSIRT svojim zložkám na komerčnej báze. V prípade ISP poskytuje CSIRT väčšinou služby koncovým užívateľom proti zneužívaniu (vykrúcané spojenie, ADSL) a služby CSIRT pre svojich profesionálnych zákazníkov.

Zložky
Komerčné CSIRT obvykle dodávajú svoje služby zložkám, ktoré za ne platia.

Sektor CIP/CIIP CSIRT
Zameranie
Tímy CSIRT v tomto sektore sa zameriavajú hlavne na ochranu dôležitých informácií a / alebo ochranu dôležitých informácií a infraštruktúry – CIP/CIIP *(Critical Information Protection / Critical Information and Infrastructure Protection)*. Tieto špecializované tímy CSIRT väčšinou úzko spolupracujú s vládnym oddelením CIIP. Ten pokrýva všetky rozhodujúce sektory IT v krajine a chráni jej občanov.

Zložky
Vláda; rozhodujúce podniky IT; občania

Štátny sektor CSIRT
Zameranie
Štátny CSIRT poskytuje služby štátnym orgánom a v niektorých krajinách aj občanom.

Zložky
Štátne orgány a orgány spojené s vládou; v niektorých krajinách sa služby vydávania výstrah poskytujú tiež občanom (napríklad v Belgicku, Maďarsku, Holandsku, Spojenom kráľovstve a Nemecku).

Interný CSIRT
Zameranie
Interný CSIRT poskytuje služby len pre svoju hostiteľskú organizáciu. Charakterizuje to skôr činnosť ako sektor. Napríklad veľa telekomunikačných organizácií a bánk používa vlastné interné tímy CSIRT. Obvykle neudržujú webovú stránku pre verejnosť.

Zložky
Interní pracovníci a oddelenie IT hostiteľskej organizácie

Vojenský sektor CSIRT
Zameranie
Tím CSIRT v tomto sektore poskytuje služby vojenským organizáciám zodpovedným za infraštruktúru IT potrebnú pre obranné účely.

Zložky
Pracovníci vojenských inštitúcii alebo úzko spojených orgánov, napr. ministerstvo obrany.

Národný CSIRT
Zameranie
CSIRT s národným zameraním považovaný za bezpečnostné kontaktné miesto pre danú krajinu. V niektorých prípadoch pôsobia štátne CISRT tiež ako národné PoC (ako UNIRAS v Spojenom kráľovstve).

Zložky
Tento druh CSIRT obvykle nemá priame zložky, pretože národný CSIRT hrá len úlohu sprostredkovateľa pre celú krajinu.

Malé a stredné podniky (SME) Sektor CSIRT
Zameranie
Samoorganizujúci sa tím, ktorý poskytuje svoje služby vo vlastnom odvetví podnikania alebo podobnej skupine užívateľov.

Zložky
Zložkami týchto CSIRT môžu byť SME a ich pracovníci alebo zvláštne záujmové skupiny ako „Združenie miest a obcí“ v krajine.

CSIRT predajcov
Zameranie
CSIRT predajcov sa zameriava na podporu produktov špecifických pre predajcov. Jeho cieľom je obvykle spracovať a poskytnúť riešenie, aby sa odstránila zraniteľnosť a znížili potenciálne negatívne vplyvy porúch.

Zložky
Vlastníci produktov

Ako to bolo popísané v odseku o národnom CSIRT, tím môže slúžiť viac ako jednému sektoru. Má to dopad napríklad na analýzu zložky a jej potrieb.

Fiktívny CSIRT (1. krok)
Počiatočná fáza V počiatočnej fáze je nový CSIRT plánovaný ako interný CSIRT, ktorý poskytuje svoje služby pre hostiteľskú spoločnosť, miestne oddelenie IT a pracovníkov. Tiež podporuje a medzi rôznymi pobočkami koordinuje riešenie incidentov súvisiacich s bezpečnosťou IT.

Možné služby, ktoré je CSIRT schopný poskytovať

Urobili sme prvé dva kroky.

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?

>> Ďalší krok je odpoveď na otázku, *aké služby sa majú poskytovať zložkám*.

Existuje mnoho služieb, ktoré môže CSIRT dodávať, ale dosiaľ žiadny CSIRT neposkytuje všetky z nich. Takže výber príslušného súboru služieb je zásadným rozhodnutím. Dole je uvedený stručný prehľad všetkých známych služieb CSIRT definovaných v „Príručke pre CSIRT“, ktorú vydal CERT/CC[6].

Reaktívne služby	**Aktívne služby**	**Zaobchádzanie s artefaktmi**
• **Výstrahy a varovania** • **Riešenie bezpečnostných incidentov** • **Analýza bezpečnostných incidentov** • **Podpora reakcie na bezpečnostné incidenty** • **Koordinácia reakcií na bezpečnostné incidenty** • Reakcia na bezpečnostné incidenty na mieste • Riešenie zraniteľnosti • Analýza zraniteľnosti • Reakcia na zraniteľnosť • Koordinácia reakcií na zraniteľnosť	• **Oznámenie** • Sledovanie techniky • Audity alebo hodnotenia bezpečnosti • Konfigurácia a udržiavanie bezpečnosti • Vývoj nástrojov bezpečnosti • Služby detekcie narušenia • Šírenie informácií týkajúcich sa bezpečnosti	• *Analýza artefaktov* • *Reakcia na artefakty* • *Koordinácia reakcií na artefakty* ***Manažment kvality bezpečnosti*** • *Analýza rizík* • *Kontinuita obchodu a obnovenie prevádzky po havárii* • *Poradenstvo v bezpečnosti* • *Vytváranie povedomia* • *Vzdelávanie/výcvik* • *Hodnotenie alebo certifikácia produktov*

Obr. 1 Zoznam služieb CSIRT od CERT/CC[7]

Kľúčové služby (označené tučným písmom): Rozlišujú sa reaktívne a aktívne služby. Aktívne služby sa zameriavajú na prevenciu bezpečnostných incidentov vytváraním povedomia a výcvikom, zatiaľ čo reaktívne služby sa zameriavajú na riešenie bezpečnostných incidentov a zníženie výsledných škôd.

Riešenie artefaktov zahŕňa analýzu každého súboru alebo objektu zisteného v systéme, ktorý by mohol byť zapojený do škodlivých aktivít ako zvyšky vírusov, červy, skripty, trojské kone a pod. Obsahuje tiež zaobchádzanie s výslednými informáciami a ich distribúciu predajcom a ďalším zainteresovaným stranám, aby sa zamedzilo ďalšiemu šíreniu škodlivých programov, a aby sa znížili riziká.

Služby manažmentu bezpečnosti a kvality sú služby s dlhodobejšími cieľmi a zahŕňajú poradenské a vzdelávacie opatrenia.

Podrobné vysvetlenie služieb CSIRT pozri prílohu.

Výber správnych služieb pre vaše zložky je dôležitý krok a ďalej bude uvedený v kap. 6.1 *Definovanie finančného modelu.*

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

[7] Zoznam služieb CSIRT od CERT/CC http://www.cert.org/csirts/services.html

Väčšina tímov CSIRT začína rozosielaním 'Výstrah a varovaní', robí 'Oznámenia' a zaisťuje 'Riešenie bezpečnostných incidentov' pre svoje zložky. Tieto kľúčové služby obvykle vykazujú u zložky dobrý profil a hodnotu upozornení a väčšinou sa považujú za skutočne „pridanú hodnotu".

Dobrá prax je začať s malou skupinou 'pilotných' zložiek, poskytovať kľúčové služby v priebehu pilotnej doby a potom požiadať o spätnú väzbu.
Zainteresovaní pilotní užívatelia zaisťujú konštruktívnu spätnú väzbu a pomáhajú rozvíjať služby prispôsobené potrebám.

Fiktívny CSIRT (2. krok)

Výber správnych služieb

V počiatočnej fáze sa rozhodne, že nový CSIRT sa zameria hlavne na poskytovanie niektorej z kľúčových služieb pre zamestnancov.

Urobí sa rozhodnutie, že po pilotnej fáze sa zváži rozšírenie portfólia služieb a doplnia sa niektoré 'Služby manažmentu bezpečnosti'. Toto rozhodnutie sa príjme na základe spätnej väzby od pilotných zložiek a v úzkej spolupráci s oddelením zaisťovania kvality.

Analýza zložky a poslanie

Urobili sme prvé tri kroky:

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. „Akému sektoru sa budú dodávať služby CSIRT?"
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.

>> Ďalší krok je odpoveď na otázku, *aký druh prístupu by sa mal zvoliť, aby CSIRT začal pracovať?*

Ďalší krok je hlbší náhľad do zložky s hlavným cieľom vybrať správne komunikačné kanály.

- Vymedzenie komunikačného prístupu k zložkám
- Stanovenie poslania.
- Vypracovanie realistického plánu realizácie/plánu projektu
- Stanovenie služieb CSIRT
- Určenie organizačnej štruktúry
- Stanovenie politiky bezpečnosti informácií
- Nábor správnych pracovníkov
- Využitie kancelárie vášho CSIRT
- Vyhľadávanie spolupráce medzi inými CSIRT a prípadnými národnými iniciatívami.

Tieto kroky budú podrobnejšie popísané v nasledujúcich bodoch a možno ich použiť ako vstup pre obchodní plán a plán projektu.

5..1 Prístup ku komunikácii so zložkou

Ako bolo uvedené skôr, je veľmi dôležité vedieť potreby zložky a tiež svoju vlastnú stratégiu komunikácie, vrátane komunikačných kanálov, ktoré sú najvhodnejšie na to, aby ste sa na ňu obrátili s informáciami.

Teória riadenia pozná niekoľko možných prístupov k tomuto problému analyzovania cieľovej skupiny. V tomto dokumente opisujeme dva z nich: analýzu SWOT a PEST.

Analýza SWOT
Analýza SWOT je nástroj strategického plánovania používaný na hodnotenie silných stránok (**S**trengths), slabých stránok (**W**eaknesses), príležitostí (**O**pportunities) a hrozieb (**T**hreats), ktoré sa týkajú projektu alebo obchodného podnikania, alebo ktoré si v akejkoľvek inej situácii vyžadujú rozhodnutie. Táto metóda sa pripisuje Albertovi Humpreymu, ktorý viedol výskumný projekt na Stanfordské univerzite v 60. a 70. rokoch s využitím údajov 500 najväčších korporácií USA zverejnených v časopise Fortune.[8]

Silné stránky	**Slabé stránky**
Príležitosti	**Hrozby**

Obr. 2 Analýza SWOT

[8] Analýza SWOT vo Wikipedia: http://en.wikipedia.org/wiki/SWOT_analysis

Analýza PEST

Analýza PEST je ďalší dôležitý nástroj, ktorý sa v širokom meradle používa pre analýzu zložky s cieľom pochopenia politických (**P**olitical), ekonomických (**E**conomic), sociálno-kultúrnych (**S**ocio-cultural) a technologických (**T**echnological) okolnosti prostredia, v ktorom pracuje CSIRT. Pomôže ustanoviť, či plánovanie je ešte v súlade s prostredím, a pravdepodobne prispeje k tomu, aby sa zamedzilo prijatiu opatrení na základe nesprávnych predpokladov.

Politické	**Ekonomické**
• Ekologické/environmentálne otázky • Legislatíva platná pre domáci trh • Budúca legislatíva • Európska/medzinárodná legislatíva • Zákonné orgány a procesy • Štátne politiky • Funkčné obdobie vlády a zmena • Obchodné politiky • Financovanie, granty a iniciatívy • Lobistické/nátlakové skupiny na domácom trhu • Medzinárodné nátlakové skupiny	• Vnútroštátna hospodárska situácia • Vnútroštátne hospodárske trendy • Zahraničné ekonomiky a trendy • Problematika všeobecného zdaňovania • Dane špecifické pre produkt/služby • Problémy sezónnosti/poveternostných podmienok • Tržné a hospodárske cykly • Faktory špecifické pre odvetvie • Smerovanie trhu a trendy distribúcie • Hybné sily zákazníka/konečného užívateľa • Úrokové sadzby a výmenné kurzy
Sociálne	**Technologické**
• Trendy životného štýlu • Demografia • Postoje a názory zákazníkov • Stanoviská médií • Malé zmeny ovplyvňujúce sociálne faktory • Obchodná značka, spoločnosť, technická povesť • Vzorce nakupovania zákazníkov • Modely spôsobu a úlohy • Dôležité udalosti a vplyvy • Dostupnosť a trendy nakupovania • Etnické/náboženské faktory • Reklama a propagácia	• Rozvoj konkurenčnej technológie • Financovanie výskumu • Pomocné/závislé technológie • Náhradné technológie/riešenie • Vyspelosť technológie • Výrobná vyspelosť a kapacita • Informácie a komunikácie • Mechanizmy/ technológia nakupovania zákazníkov • Technická legislatíva • Inovačný potenciál • Dostupnosť technológií, udeľovanie licencií, patenty • Otázky duševného vlastníctva

Obr. 3 Analýza modelu PEST

Podrobný opis analýzy PEST je uvedený vo Wikipedia[9].

Obidva nástroje poskytujú komplexný a štruktúrovaný prehľad o tom, aké sú potreby zložiek. Výsledky doplnia obchodný návrh a tým pomôžu získať finančné prostriedky pre vytvorenie CSIRT.

[9] Analýza PEST vo Wikipedia: http://en.wikipedia.org/wiki/PEST_analysis

Komunikačné kanály
Ako dôležitú tematiku možno do analýzy zahrnúť komunikáciu a metódy šírenia informácií („Ako komunikovať so zložkou?“)

Podľa možnosti by sa mali zvážiť pravidelné osobné návštevy zložiek. Je dokázané, že porady za osobnej účasti uľahčujú spoluprácu. Ak sú obidve strany ochotné pracovať spolu, tieto porady povedú k otvorenejšiemu vzťahu.

CSIRT obvykle používa súbor komunikačných kanálov. Nasledujúce z nich sa v praxi ukázali ako účelné a zasluhujú si posúdenie:

- Verejná webová stránka
- Uzavretá oblasť členov na webovej stránke
- Internetové formuláre pre hlásenie bezpečnostných incidentov
- Adresáre
- E-mail na meno
- Telefón / fax
- SMS
- ‘Zastarané’ písomné listy
- Mesačné alebo ročné správy

Okrem používania elektronickej pošty, internetových formulárov, telefónu alebo faxu s cieľom uľahčiť riešenie bezpečnostných incidentov (prijímanie správ o bezpečnostných incidentoch od zložky, koordinácia s ostatnými tímami alebo poskytovanie spätnej väzby a podpora obete) väčšina CSIRT publikuje svoje odborné rady týkajúce sa bezpečnosti na verejne prístupnej webovej stránke a za pomoci adresárov.

! Ak je to možné, informácie by sa mali rozosielať bezpečným spôsobom. Napríklad elektronickú poštu možno podpísať pomocou programu pre šifrovanie elektronickej pošty, freewarového šifrovacieho programu „veľmi dobré súkromie“ – PGP *(Pretty Good Privacy)* a citlivé údaje o bezpečnostnom incidente by sa mali vždy zasielať šifrované.

Viacej informácií pozri kapitolu 8.5 *Dostupné nástroje CSIRT*. Pozri tiež kapitolu *2.3 RFC2350*[10].

Fiktívny CSIRT (krok 3a)
Uskutočnenie analýzy zložky a vytvorenie vhodných komunikačných kanálov

Brainstormingová porada s niektorými kľúčovými osobami z vedenia a zo zložky generovala dostatočný vstup pre analýzu SWOT. Vedie to k záveru, že existuje potreba týchto rozhodujúcich služieb:

- Výstrahy a varovania
- Riešenie bezpečnostných incidentov (analýza, podpora reakcie a koordinácia reakcie)
- Oznámenie

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

Musí sa zaistiť, aby sa informácie rozosielali dobre organizovaným spôsobom s cieľom dostať ich k čo najväčšej časti zložky. Príjme sa teda rozhodnutie, že výstrahy, varovania a oznámenia vo forme poradenstva k bezpečnosti sa budú publikovať na vyhradenej webovej stránke a rozosielať pomocou adresára. Elektronická pošta, telefón a fax uľahčuje tímu CSIRT prijímať správy o bezpečnostných incidentoch. Ako ďalší krok sa plánuje unifikovaný webový formulár.

Vzorová analýza SWOT pozri ďalšiu stranu.

Silné stránky • Spoločnosť má určité znalosti. • Plán sa im páči a sú ochotní spolupracovať. • Podpora a financovanie zo strany riadiaceho tímu.	**Slabé stránky** • Rôzne oddelenia a pobočky medzi sebou príliš nekomunikujú. • Nie je koordinácia v bezpečnostných incidentoch IT • Je mnoho 'malých oddelení'.
Príležitosti • Veľké množstvo neštruktúrovaných informácií o zraniteľnosti. • Veľká potreba koordinácie. • Zníženie strát kvôli bezpečnostným incidentom. • Mnoho neurčitostí v otázke bezpečnosti IT. • Vzdelávanie pracovníkov v bezpečnosti IT.	**Hrozby** • Nie je k dispozícii veľa peňazí. • Nie je veľa pracovníkov. • Veľké očakávania. • Kultúra.

Obr. 4 Vzorová analýza SWOT

5..2 Poslanie

Po analýze potrieb a želaní zložky týkajúcich sa služieb CSIRT by ďalším krokom malo byť skoncipovanie poslania organizácie .

Definícia poslania opisuje hlavnú funkciu organizácií v spoločnosti z hľadiska produktov a služieb, ktoré poskytujú pre svoje zložky. Umožňuje to jasne oznámiť, že CSIRT existuje a akú má funkciu.

Dobrou praxou je skoncipovať výstižné definície poslania, ale nie príliš striktne stanovené, pretože obvykle zostane nezmenené po niekoľko rokov.

Dole je niekoľko príkladov definície poslania od fungujúcich tímov CSIRT:

"<Názov CSIRT> poskytuje informácie a pomoc svojim <zložkám (definujte svoje zložky)> v zavádzaní aktívnych opatrení s cieľom znížiť riziká bezpečnostných incidentov počítačov a tiež v reagovaní na tieto bezpečnostné incidenty, keď sa vyskytnú."

„Ponúkať pomoc <zložkám> v prevencii bezpečnostných incidentov týkajúcich sa IT

a v reakcii na ne."[11]

Prehlásenie o poslaní je veľmi dôležitý a potrebný krok pre začatie. Podrobnejší opis toho, aké informácie by mal CSIRT uverejniť, pozri kapitolu *2.1 RFC2350*[12].

Fiktívny CSIRT (krok 3b)
Vedenie fiktívneho CSIRT urobilo nasledujúce prehlásenie o poslaní: *„Fiktívny tím CSIRT poskytuje informácie a pomoc pracovníkom svojej hostiteľskej spoločnosti s cieľom znížiť riziká bezpečnostných incidentov počítačov a tiež s cieľom reagovať na tieto bezpečnostné incidenty, keď sa vyskytnú.“* Týmto fiktívnym CSIRT sa vysvetľuje, že ide o interný CSIRT, a že jeho hlavnou úlohou je zaoberať sa otázkami súvisiacimi s bezpečnosťou IT.

[11] Prehlásenie o poslaní Govcert.nl: http://www.govcert.nl

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

6 Vypracovanie obchodného plánu

Urobili sme nasledujúce kroky:

1. Pochopenie, čo je CSIRT a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.
4. Analýza prostredia a zložiek.
5. Stanovenie prehlásenia o poslaní.

>> Ďalší krok je stanovenie obchodného plánu.

Výstup z analýzy vám dáva dobrý prehľad o potrebách a (predpokladaných) slabých stránkach zložky, takže sa berie ako vstup pre ďalší krok.

Definovanie finančného modelu.

Po analýze bolo vybraných niekoľko rozhodujúcich služieb, s ktorými sa začne. Ďalší krok je uvažovanie o finančnom modeli: aké parametre poskytovania služieb sú vhodné, ako aj rentabilné.

V dokonalom svete by sa financovanie prispôsobilo potrebám zložky, ale v reálnom svete sa portfólio služieb, ktoré možno poskytovať, musí prispôsobiť danému rozpočtu. Je teda viac realistické začať s plánovaním otázok finančných prostriedkov.

6..1 Model nákladov

Existujú dva hlavné faktory, ktoré ovplyvňujú náklady, a to určenie pracovnej doby a počtu (kvality) pracovníkov, ktorí majú pracovať. Treba reagovať na bezpečnostné incidenty a poskytovať technickú podporu 24 hodín denne, 7 dní v týždni, alebo sa budú tieto služby zaisťovať len v pracovnej dobe?

V závislosti od žiaducej dostupnosti a kancelárskom vybavení (je napríklad možné pracovať z domu?) môže byť prospešné pracovať s rozvrhom služieb na zavolanie alebo s časovo plánovaným rozvrhom služieb.

Možným scenárom je dodávať počas pracovnej doby tak aktívne, ako aj reaktívne služby. Mimo pracovnej doby budú pracovníci poskytovať iba obmedzené služby na zavolanie, napríklad len v prípade veľkých havárií a bezpečnostných incidentov.

Ďalšia možnosť je vyhľadávanie medzinárodnej spolupráce medzi inými tímami CSIRT. Už existujú príklady fungovania spolupráce „Nasledovanie slnka“. Napríklad spolupráca medzi európskymi a americkými tímami sa ukázala ako prospešná a poskytuje dobrý spôsob zdieľania vzájomných pracovných kapacít. Napríklad CSIRT spoločnosti Sun Microsystems, ktorá má mnohé pobočky v rôznych časových pásmach po celom svete (ale všetky sú členmi rovnakého tímu CSIRT), uskutočňuje služby 24 hodín denne, 7 dní

v týždni, v nepretržitých zmenách tímov po celom svete. Neobmedzujú sa tým náklady, pretože tímy vždy pracujú len v normálnej pracovnej dobe a zaisťujú služby tiež pre „spiacu časť“ sveta.

Dobrou praxou je najmä hlboká analýza, či zložka potrebuje služby 24 hodín denne, 7 dní v týždni. Výstrahy a varovania vydávané v nočnej dobe nemajú veľký zmysel, keď ich príjemca bude čítať až ďalšie ráno. Existuje jemná deliaca čiara medzi „potrebovať službu“ a „chcieť službu“, ale najmä pracovná doba má veľký význam pre počet pracovníkov a potrebné vybavenie, čo má veľký dopad na model nákladov.

6..2 Model výnosov

Keď už poznáme náklady, ako ďalší vhodný krok je posúdenie možných modeloch výnosov: ako možno financovať plánované služby. Dole je niekoľko možných scenárov pre hodnotenie:

Využitie existujúcich zdrojov
Vždy je výhodné vyhodnotiť zdroje, ktoré už existujú v iných častiach spoločnosti. Pracujú tam už vhodní zamestnanci (napr. v existujúcom oddelení IT) s potrebným vzdelaním a odbornými skúsenosťami? Pravdepodobne je možné dospieť k dohode s vedením o podpore týchto pracovníkov v CSIRT v počiatočnej fáze alebo sa podpora pre CSIRT poskytuje na báze ad hoc.

Členský poplatok
Ďalšia možnosť je predávať svoje služby zložke za ročný/štvrťročný členský poplatok. Ďalšie služby by sa mohli platiť za každé ich využitie, napríklad konzultačné služby alebo audity bezpečnosti.

Iný možný scenár: služby pre (internú) zložku sa poskytujú bezplatne, ale za služby dodávané externým zákazníkom sa musí platiť. Ďalší nápad je publikovať odborné rady a informačné bulletiny na verejnej webovej stránke a mať časť "Len pre členov" so zvláštnymi, podrobnejšími informáciami alebo informáciami prispôsobenými danému účelu.

V praxi sa ukázalo, že „Predplatenie služieb CSIRT“ možno iba v obmedzenej miere využiť na zaistenie dostatočných finančných prostriedkov, a to najmä v počiatočnej fáze. Existujú napríklad fixné základné výdaje na tím a vybavenie, ktoré sa musia uhradiť vopred. Financovanie týchto výdajov predajom služieb CSIRT je ťažké a vyžaduje si veľmi podrobnú finančnú analýzu s cieľom zistiť „mŕtvy bod (prah rentability, kedy sa náklady rovnajú výnosom).

Dotácie
Ďalšia eventualita, ktorú stojí za to zvážiť, by mohla byť žiadosť o dotáciu na projekt poskytnutú od vlády alebo od štátneho orgánu, pretože v súčasnej dobe väčšina krajín má fondy, ktoré sú k dispozícii pre projekty bezpečnosti IT. Kontaktovanie ministerstva vnútra by mohlo byť dobrým začiatkom.

Samozrejme je možná kombinácia rôznych príslušných modelov.

Určenie organizačnej štruktúry

Vhodná organizačná štruktúra CSIRT značne závisí od existujúcej štruktúry hostiteľskej organizácie a zložky. Je taktiež závislá od dostupnosti kvalifikovaných odborníkov, ktorých treba najať nastálo alebo na báze ad hoc.

Typický CSIRT určuje nasledujúce úlohy v rámci tímu:

Hlavné
- Generálny riaditeľ

Pracovníci
- Office Manager
- Účtovník
- Poradca pre komunikáciu
- Právny konzultant

Prevádzkovo-technický tím
- Vedúci technického tímu
- Technici technického tímu CSIRT, ktorí dodávajú služby CSIRT
- Výskumníci

Externí konzultanti
- Prijímaní podľa potreby

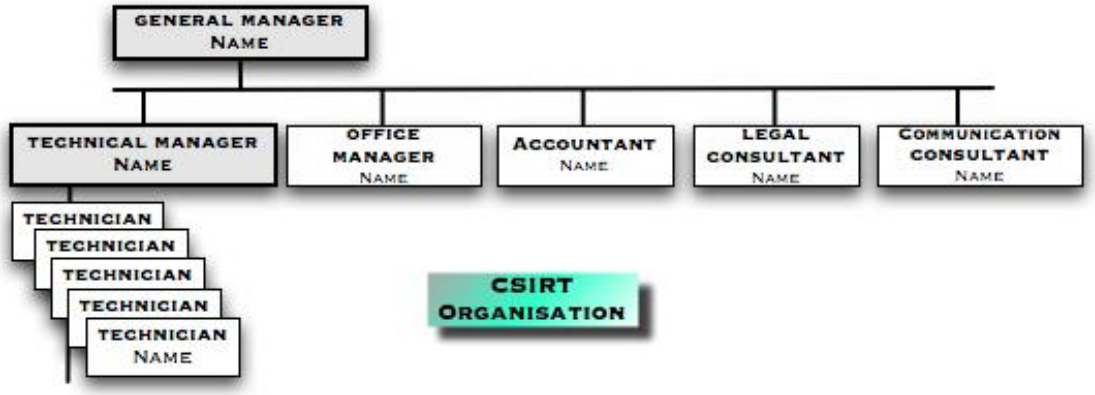
Je veľmi účelné mať k dispozícii právneho experta najmä v počiatočnej fáze CSIRT. Zvýšia sa tým síce náklady, ale nakoniec sa ušporí čas a zamedzí sa právnym problémom.

V závislosti od druhu odborných schopností v zložke, a tiež keď CSIRT má veľkú mediálnu propagáciu, ukázalo sa ako veľmi užitočné mať v tíme aj odborníka na komunikáciu. Títo odborníci sa môžu zamerať na prevádzanie ťažkých technických otázok do zrozumiteľnejších správ pre zložky alebo mediálnych partnerov. Odborník na komunikáciu bude takisto poskytovať spätnú väzbu zo zložky pre technických odborníkov, takže môže pôsobiť ako „prekladateľ“ alebo „uľahčovateľ“ medzi týmito dvoma skupinami.

Dole je niekoľko príkladov organizačných modelov používaných prevádzkovými tímami CSIRT.

6..1 Nezávislý obchodný model

CSIRT sa rozvíja a koná ako nezávislá organizácia s vlastným vedením a zamestnancami.



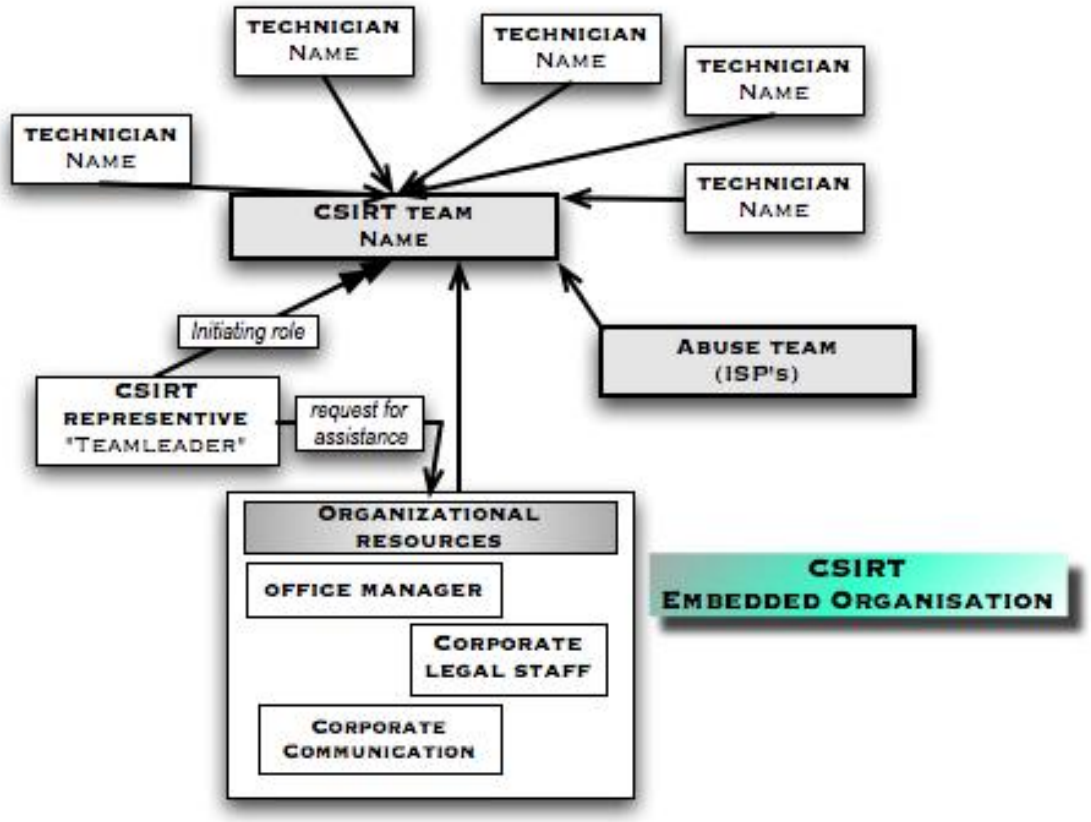
Generálny riaditeľ – meno
Technický riaditeľ – meno Office Manager – meno, účtovník – meno, právny poradca – meno, poradca pre komunikáciu – meno
technik, technik, technik, technik, technik – meno, organizácia CSIRT

Obr. 5 Nezávislý obchodný model

6..2 Vložený model organizácie

Tento model možno použiť, keď sa má CSIRT vytvoriť v rámci existujúcej organizácie, napríklad s využitím existujúceho oddelenia IT. Na čele CSIRT je vedúci tímu, ktorý zodpovedá za činnosti CSIRT. Vedúci tímu zhromaždí potrebných technikov, keď rieši bezpečnostné incidenty, alebo keď pracuje na činnostiach CSIRT. Môže požiadať o pomoc týkajúcu sa podpory odborníkov v rámci existujúcej organizácie.

Tento model možno tiež upraviť pre špecifické situácie, keď sa vyskytnú. V tomto prípade sa tímu pridelí pevný počet ekvivalentných pracovníkov na plný pracovný úväzok – FTE *(Full Time Equivalent)*. Napríklad zneužívanie desktopu u prevádzkovateľa služieb siete Internet – ISP (Internet Service Provider) je určite (vo väčšine prípadov) pracovné miesto na plný pracovný úväzok pre viacej ako jedného pracovníka FTE.



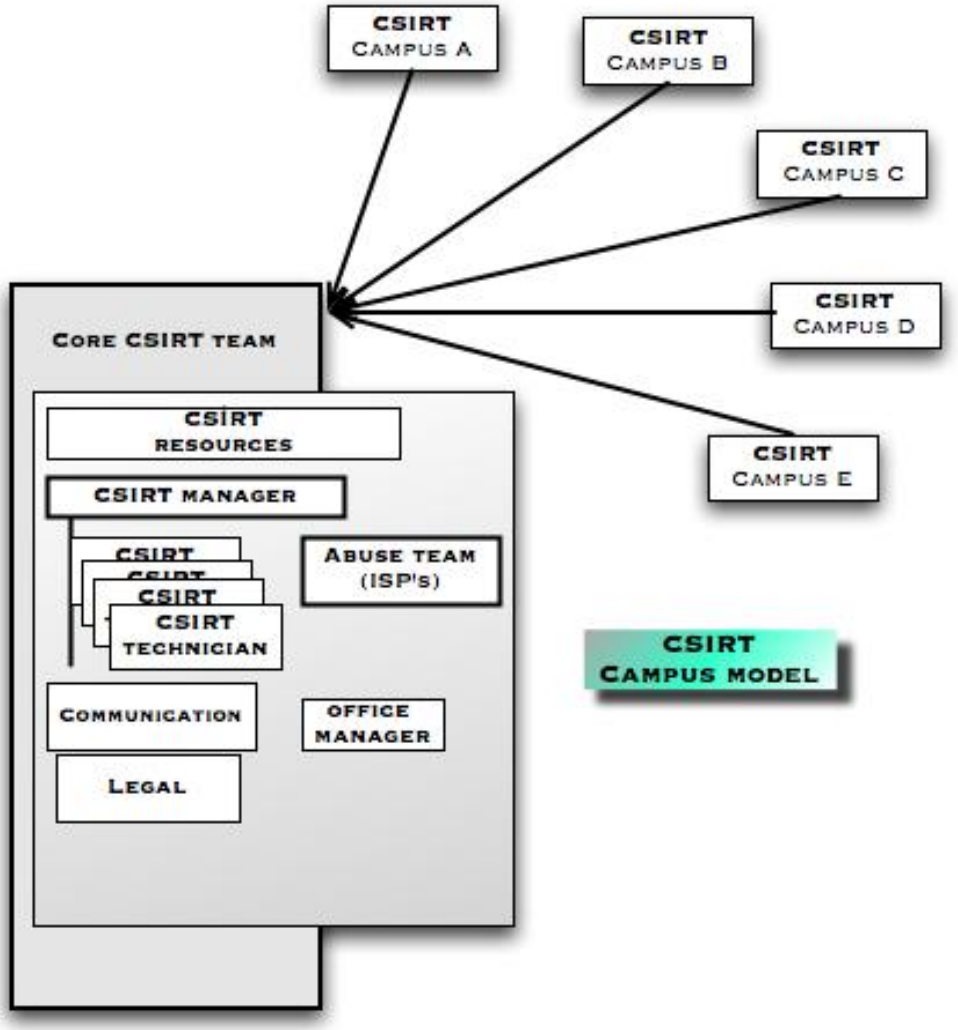
Technik – meno, technik – meno, technik – meno, technik – meno, technik – meno
Názov tímu CSIRT
Počiatočná úloha, Tím ISP proti zneužívaniu
Zástupca CSIRT, “vedúci tímu”, žiadosť o pomoc
Zdroje organizácie
Office Manager, vložená organizácia CSIRT
Podnikoví právnici
Podniková komunikácia

Obr. 6 Obr. 6 Vložený model organizácie

6..3 Vysokoškolský model

Vysokoškolský model, ako naznačuje jeho názov, prijímajú väčšinou vysokoškolské a výskumné CSIRT. Väčšina vysokoškolských a výskumných organizácií je zložená z rôznych vysokých škôl a univerzitných zariadení na rozličných miestach rozšírených po celom regióne alebo dokonca po celej krajine (ako v prípade Štátnych výskumných sietí – NREN *(National Research Networks)*. Obvykle sú tieto organizácie nezávislé jedna od druhej a často majú vlastný CSIRT. Tieto tímy CSIRT sú spravidla organizované pod záštitou 'materského' alebo hlavného CSIRT. Hlavný CSIRT koordinuje styk s vonkajším svetom a je jeho jediným kontaktným miestom. Hlavný CSIRT bude vo väčšine prípadov príslušnému vysokoškolskému CSIRT tiež poskytovať kľúčové služby CSIRT a aj rozosielať informácie o bezpečnostných incidentoch.

Niektoré CSIRT rozosielajú svoje kľúčové služby CSIRT spolu s inými vysokoškolskými CSIRT, čo vedie k nižším režijným nákladom pre hlavný CSIRT.



CSIRT – vysokoškolský areál A, CSIRT – vysokoškolský areál B, CSIRT – vysokoškolský areál C, CSIRT – vysokoškolský areál D, CSIRT – vysokoškolský areál E
Hlavný tím CSIRT
Zdroje CSIRT
Manažér CSIRT
Technik, technik, technik, technik, CSIRT, tím ISP proti zneužívaniu
Komunikácia
Právna
Office Manager
Vysokoškolský model CSIRT

Obr. 7 Vysokoškolský model

6..4 Dobrovoľný model

Tento organizačný model opisuje skupinu pracovníkov (odborníkov), ktorí sa spojili, aby dobrovoľne poskytovali jeden druhému (a ostatným) rady a podporu. Je to voľne zostavená skupina ľudí, ktorá je veľmi závislá od motivácie účastníkov.

Tento model napríklad prijala skupina WARP[13].

Nábor vhodných pracovníkov

Po rozhodnutí o službách a úrovni podpory, ktorá sa má poskytnúť, a po zvolení organizačného modelu, je ďalší krok zistenie správneho počtu kvalifikovaných pracovníkov pre danú prácu.

Je takmer nemožné ustanoviť pevný počet technických pracovníkov potrebných z tohto hľadiska, ale ako dobrý prístup sa osvedčili nasledujúce rozhodujúce počty:

- Pre dodávanie dvoch hlavných služieb, a to distribúcie poradenských bulletinov a tiež riešenia bezpečnostných incidentov: najmenej **4** pracovníci FTE.
- Pre úplné služby CSIRT v pracovnej dobe a systémy údržby: najmenej **6 až 8** pracovníkov FTE.
- Pre plne obsadenú zmenu 24 hodín denne, 7 dní v týždni (2 zmeny mimo pracovnej doby) je minimálny počet okolo **12** pracovníkov FTE.

Tieto počty zahŕňajú tiež nadpočetné stavy pre prípady choroby, dovoleniek a pod. Je taktiež nutné preveriť miestne kolektívne zmluvy. Ak zamestnanci pracujú mimo pracovnej doby, môže to viesť k mimoriadnym výlohám vo forme zvláštnych príplatkov, ktoré sa musia platiť.

Ďalej je uvedený stručný prehľad najdôležitejších schopností technických odborníkov pre CSIRT.

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

Body opisu práce hlavných technických pracovníkov:

Osobné schopnosti

- Flexibilný, tvorivý a s dobrým zmyslom pre tím
- Dobré analytické schopnosti
- Schopnosť vysvetliť zložité technické otázky jednoduchými slovami
- Dobrý cit pre dôvernosť a pre prácu na procedurálnych otázkach
- Dobré organizačné schopnosti
- Odolnosť voči stresu
- Dobré schopnosti komunikácie a písania
- Nezaujatý a ochotný učiť sa

Technické schopnosti

- Široké znalosti technológie Internetu a protokolov
- Znalosti systémov Linux a Unix (v závislosti od vybavenia zložky)
- Znalosti systémov Windows (v závislosti od vybavenia zložky)
- Znalosti vybavenia infraštruktúry siete (smerovač, prepínače, systém doménových mien – DNS *(Domain Name System)*, zástupca, pošta atď.)
- Znalosti internetových aplikácií (jednoduchý protokol transferu pošty – SMTP *(Simple Mail Transfer Protocol)*, hypertextové prenosové protokoly – HTTP *(HyperText Transfer Protocols)*, protokol pre prenos súborov – FTP *(File Transfer Protocol)*, telnet (protokol pre vzdialený prístup), zabezpečený protokol pre terminálovú emuláciu – SSH *(Secure Shell)* atď.)
- Znalosti ohrozenia bezpečnosti (distribuovaný útok typu odoprenia služby – DDoS *(Distributed Denial of Service)*, phishing (on-line krádež identity), poškodenie povrchovej úpravy *(defacing),* odpočúvanie sieťovej komunikácie *(sniffing)* atď.
- Znalosti hodnotenia rizík a praktických realizácií

Ďalšie schopnosti

- Ochota pracovať 24 hodín denne, 7 dní v týždni na zavolanie (v závislosti od modelu služieb)
- Maximálna cestovná vzdialenosť (v prípade havárie pohotovosť v kancelárii; maximálna cestovná doba)
- Úroveň vzdelania
- Skúsenosti v práci v oblasti bezpečnosti IT.

Fiktívny CSIRT (4. krok)

Stanovenie obchodného plánu

Finančný model
Keďže spoločnosť uskutočňuje elektronický obchod 24 hodín denne, 7 dní v týždni, a má tiež oddelenie IT, ktoré pracuje 24 hodín denne, 7 dní v týždni, rozhodla sa poskytovať počas pracovnej doby úplné služby a mimo pracovnej doby služby na zavolanie. Služby pre zložku sa budú poskytovať bezplatne, ale počas pilotnej a hodnotiacej fázy bude posúdená možnosť dodávania služieb externým zákazníkom.

Model výnosov
V priebehu počiatočnej a pilotnej fázy bude CSIRT financovaný prostredníctvom hostiteľskej spoločnosti. Počas pilotnej a hodnotiacej fázy bude prerokované ďalšie financovanie, vrátane možnosti predaja služieb externým zákazníkom.

Organizačný model
Hostiteľská organizácia je malá spoločnosť, takže bol vybraný vložený model.
Počas pracovnej doby bude personál zložený z troch pracovníkov poskytovať kľúčové služby (rozosielanie odborných rád k bezpečnosti a riešenie/koordinácia bezpečnostných incidentov).

Oddelenie IT spoločnosti už zamestnáva pracovníkov s vhodnými odbornými schopnosťami. S týmto oddelením je urobená dohoda, takže nový CSIRT môže v prípade potreby požiadať o podporu na báze ad hoc. Možno využiť tiež ich technikov na zavolanie 2. línie.
Hlavný tím CSIRT bude mať štyroch členov na plný pracovný úväzok a päť ďalších členov. Jeden z nich je k dispozícii tiež na striedavej zmene.

Pracovníci
Vedúci tímu CSIRT má vzdelanie v bezpečnosti a podporu 1. a 2. úrovne a vykonával prácu v oblasti riadenia pretrvávajúcich kríz. Ostatní traja členovia tímu sú odborníci na bezpečnosť. Členovia tímu CSIRT z oddelenia IT na čiastočný pracovný úväzok sú odborníci na infraštruktúru spoločnosti.

Používanie a vybavenie kancelárie

Vybavenie a využívanie kancelárskych priestorov a fyzická bezpečnosť sú veľmi široké problémy, preto v tomto dokumente nie je možné dať ich vyčerpávajúci opis. Táto kapitola hodlá poskytnúť stručný prehľad uvedenej problematiky.

Viacej informácií o fyzickej bezpečnosti možno nájsť na:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Zaistenie odolnosti budovy“
Pretože CSIRT obvykle zaobchádza s veľmi citlivými informáciami, dobrá praxe je nechať tým skontrolovať fyzickú bezpečnosť kancelárie. Bude to dosť závisieť od existujúceho vybavenia a infraštruktúry a od existujúcej politiky bezpečnosti informácií hostiteľskej spoločnosti.

Napríklad vlády pracujú so schémami klasifikácie a sú veľmi prísne v tom, ako zaobchádzať s dôvernými informáciami. Overte s vašou vlastnou spoločnosťou alebo organizáciou miestne pravidlá a politiky.

Nový CSIRT je obvykle závislý od spolupráce svojej hostiteľskej organizácie, aby sa dozvedel o miestnych pravidlách, politikách a iných právnych otázkach.

Vyčerpávajúci opis všetkého vybavenia a bezpečnostných opatrení, ktoré budú potrebné, vychádza za rámec tohto dokumentu. Dole je však uvedený stručný zoznam základného vybavenia pre váš CSIRT:

Všeobecné pravidlá pre budovu
- Používajte kontroly prístupu.
- Sprístupnite kancelárie CSIRT len pre pracovníkov CSIRT.
- Monitorujte kancelárie a vchody kamerami.
- Archivujte dôverné informácie v zamykateľných skrinkách alebo v trezore.
- Používajte zaistené systémy IT.

Všeobecné pravidlá pre vybavenie IT
- Používajte vybavenie, ktoré môžu obsluhovať pracovníci.
- Zaistite odolnosť všetkých systémov.
- Zaplátajte a aktualizujte všetky svoje systémy pred ich pripojením na Internet.
- Používajte bezpečnostný software (bezpečnostné rozhrania *(firewalls)*, početné antivírusové skenery, program proti spywaru atď.)

Udržovanie komunikačných kanálov
- Verejná webová stránka
- Uzavretá oblasť členov na webovej stránke
- Internetové formuláre pre hlásenie bezpečnostných incidentov
- Elektronická pošta (podpora PGP / GPG / S/MIME) (podpora „veľmi dobrého súkromia“ – PGP *(Pretty Good Privacy)* / ochrany súkromia GNU – GPG *(GNU Privacy Guard)* / „bezpečného viacúčelového rozšírenia pošty Internetu“ – S/MIME *(Secure Multimedia Internet Mail Extensions)*)
- Software adresárov
- Existencia vyhradeného telefónneho čísla, ktoré je k dispozícii zložke:
  - Telefón
  - Fax
  - SMS

Systém(y) sledovania záznamov
- Databáza kontaktov s podrobnosťami o členoch tímu, o iných tímoch atď.

- Nástroje riadenia starostlivosti o zákazníkov – CRM *(Customer Relationship Management)*
- Systém prukazov v riešení bezpečnostných incidentov

Používanie „firemného štýlu“ od samého začiatku pre
- štandardnú elektronickú poštu a usporiadanie poradenského bulletinu
- ‘Zastarané’ písomné listy
- Mesačné alebo ročné správy
- Formulár hlásenia bezpečnostného incidentu

Iné otázky
- Predvídanie mimo pásmovej komunikácie v prípade útokov
- Predvídanie redundácie internetového spojenia

Viacej informácií o konkrétnych nástrojoch CSIRT pozri v kapitole *8.5 Dostupné nástroje CSIRT*.

Vypracovanie politiky bezpečnosti informácií

V závislosti od druhu CSIRT si politiku bezpečnosti informácií upravíte podľa potrieb zákazníka. Okrem opisu želaného stavu pracovných a administratívnych procesov a postupov musí byť táto politika v súlade s legislatívou a normami, najmä čo sa týka zodpovednosti CSIRT. Tím CSIRT je obvykle viazaný vnútroštátnymi zákonmi a predpismi, ktoré sa často plnia v súlade s Európskou legislatívou (spravidla so smernicami) a inými medzinárodnými dohodami. Normy nemusia byť priamo záväzné, ale môžu byť nariadené alebo odporúčané na základe zákonov a predpisov.

Dole je stručný zoznam možných zákonov a politík:

Vnútroštátne
- Rôzne zákony o informačných technológiách, telekomunikáciách, médiách
- Zákony o ochrane údajov a súkromia
- Zákony a predpisy o uchovávaní údajov
- Legislatíva o finančníctve účtovníctve a podnikovom riadení
- Kódexy chovania pre podnikové riadenie a riadenie IT

Európske
- Smernica o elektronických podpisoch (č. 1993/93/ES)
- Smernica o ochrane údajov (č. 1995/46/ES) a súkromia v elektronických komunikáciách (č. 2002/58/ES)
- Smernice o sieťach a službách elektronickej komunikácie (č. 2002/19/ES – č. 2002/22/ES)
- Smernice o práve obchodných spoločností (napr. 8. smernica o práve obchodných spoločností).

Medzinárodné
- Bazilejská zmluva II (najmä pokiaľ ide o riadenie prevádzkového rizika)
- Dohor Rady Európy o internetovej kriminalite

- Dohovor Rady Európy o ľudských právach (čl. 8 o súkromí)
- Medzinárodné účtovné normy – IAS *(International Accounting Standards*; do určitej miery nariaďujú kontroly IT).

Normy
- Britská norma BS 7799 (Bezpečnosť informácií)
- Medzinárodné normy ISO 2700x (Systémy manažmentu bezpečnosti informácií)
- Nemecká IT-Grundschutzbuch (kniha o hlavnej ochrane IT), francúzsky EBIOS a iné národné varianty.

Uskutočnite konzultáciu so svojim právnym poradcom, aby ste zistili, či váš CSIRT postupuje v súlade s vnútroštátnou a medzinárodnou legislatívou.

Najdôležitejšie otázky, na ktoré musíte vo svojich politikách zaobchádzania s informáciami odpovedať, sú:

- Ako sa prichádzajúce informácie „označujú“ alebo „klasifikujú“?
- Ako sa s informáciami zaobchádza, najmä s ohľadom na exkluzivitu?
- Aké sú dôvody sprístupnenia informácií, najmä pokiaľ sa informácie súvisiace s bezpečnostným incidentom odovzdávajú iným tímom alebo miestam.
- Existujú nejaké právne dôvody, ktoré treba vziať do úvahy v zaobchádzaní s informáciami?
- Máte politiku šifrovania s cieľom ochrany exkluzivity a ucelenosti archívov a/alebo prenosu dát, najmä elektronickej pošty?
- Zahŕňa táto politika prípadné podmienky takých právnych hraníc, ako je spätné vygenerovanie kľúča alebo vynutiteľnosť dešifrovania v prípade právnych žalôb?

Fiktívny CSIRT (5. krok)

Vybavenie a umiestnenie kancelárie

Pretože hostiteľská spoločnosť už má zavedenú efektívnu fyzickú bezpečnosť, nový CSIRT je v tomto ohľade dobre chránený. Je zaistená takzvaná „spravodajská informačná sála“, aby bola umožnená koordinácia v prípade núdzového stavu. Bol zakúpený trezor pre šifrované materiály a citlivé dokumenty. Bola zriadená zvláštna telefónna linka, vrátane telefónnej ústredne pre uľahčenie horúcej linky počas pracovnej doby a zaistený mobilný telefón s rovnakým telefónnym číslom pre službu „na zavolanie“ mimo pracovnej doby.

Možno tiež využiť existujúce zariadenie a podnikovú webovú stránku pre oznamovanie informácií týkajúcich sa CSIRT. Adresár je nainštalovaný, udržuje sa a má vyhradenú časť pre komunikáciu medzi členmi tímu a s ostatnými tímami. Všetky podrobnosti o kontaktných pracovníkoch sa ukladajú do databázy, kópia sa bezpečne uchováva.

Predpisy

Keďže CSIRT je začlenený do spoločnosti, ktorá má politiky bezpečnosti informácií, boli za pomoci právneho poradcu spoločnosti vytvorené zhodné politiky pre CSIRT.

Vyhľadávanie spolupráce medzi inými CSIRT a prípadnými národnými iniciatívami.

Existencia iných iniciatív CSIRT a veľká potreba spolupráce medzi nimi už bola v tomto dokumente niekoľkokrát spomenutá. Dobrá prax je čo najskôr kontaktovať iné tímy CSIRT, aby sa získali potrebné kontakty so skupinami pracovníkov CISRT. Iné tímy CSIRT sú spravidla veľmi otvorené a poskytujú pomoc novo vytvoreným tímom v začatí práce.

Súpis činností CERT v Európe[14] agentúry ENISA je veľmi dobrý východiskový bod pre vyhľadávanie iných tímov CSIRT v krajine alebo aktivít pre spoluprácu národných CSIRT.

Aby ste získali podporu v nájdení vhodného zdroja informácií CSIRT, kontaktujte odborníkov na tímy CSIRT agentúry ENISA:

CERT-Relations@enisa.europa.eu

Dole je uvedený prehľad činností skupín CSIRT. Podrobnejší opis a ďalšie informácie pozri *Súpis.*

Európska iniciatíva CSIRT

TF-CSIRT[15]

Pracovná skupina TF-CSIRT podporuje spoluprácu medzi tímami pre reakciu na bezpečnostné incidenty počítačov (CSIRT) v Európe. Hlavným cieľom tejto pracovnej skupiny je poskytovať fórum pre výmenu skúseností a znalostí, vytvoriť pilotné služby pre Európsku skupinu tímov CSIRT a napomáhať vytváraniu nových CSIRT.

Hlavné ciele pracovnej skupiny sú:

- Poskytovať fórum pre výmenu skúseností a znalostí.
- Vytvoriť pilotné služby pre Európsku skupinu tímov CSIRT.
- Podporovať spoločné normy a postupy pre reagovanie na bezpečnostné incidenty.
- Napomáhať vytvoreniu nových CSIRT a výcviku pracovníkov CSIRT.
- Činnosť pracovnej skupiny CSIRT – TF-CSIRT *(Task Force CSIRT)* sa zameriava na Európu a susedné krajiny v súlade s právomocami schválenými 15. septembra 2004 Technickým výborom Trans-Európskeho združenia pre výskum a vytváranie vzdelávacích sietí – TERENA *(Trans-European Research and Education Networking Association).*

[14] Súpis ENISA : http://www.enisa.europa.eu/cert_inventory/

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

Celosvetová iniciatíva CSIRT

Fórum tímov pre reakciu na bezpečnostné incidenty a pre bezpečnosť – FIRST[16]
(Forum of Incident Response and Security Teams)

FIRST je prvotná organizácia a uznávaný celosvetový vodca v reakcii na bezpečnostné incidenty. Členstvo vo FIRST umožňuje tímom pre reakciu na bezpečnostné incidenty efektívnejšie reagovať na bezpečnostné incidenty – reaktívne a tiež aktívne.

FIRST spája rôzne tímy pre reakciu na bezpečnostné incidenty počítačov zo štátnych, komerčných a vzdelávacích organizácií. FIRST sa usiluje o podporu spolupráce a koordinácie v prevencii bezpečnostných incidentov, o stimulovanie rýchlej reakcie na bezpečnostné incidenty a o pomoc v zdieľaní informácií medzi členmi a spoločnosťou ako celkom.

Okrem siete dôvery, ktorú FIRST vytvára v celosvetovom spoločenstve pre reakciu na bezpečnostné incidenty, poskytuje tiež služby s pridanou hodnotou.

Fiktívny CSIRT (6. krok)
Vyhľadávanie spolupráce S využitím Súpisu agentúry ENISA bolo možné niektoré tímy CSIRT v tej istej krajine rýchle vyhľadať a kontaktovať. S jedným z nich bola pre novo prijatého vedúceho tímu zorganizovaná návšteva na mieste. Dozvedel sa o činnostiach národného CSIRT a zúčastnil sa na porade. Táto porada bola viac ako užitočná na to, aby sa zhromaždili príklady pracovných metód, a aby sa získala podpory niekoľkých iných tímov.

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

7 Podpora obchodného plánu

Doteraz sme urobili nasledujúce kroky:

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.
4. Analýza prostredia a zložiek.
5. Stanovenie prehlásenia o poslaní.
6. Vypracovanie obchodného plánu
    a. Definovanie finančného modelu.
    b. Určenie organizačnej štruktúry
    c. Začatie náboru pracovníkov
    d. Používanie a vybavenie kancelárie
    e. Vypracovanie politiky bezpečnosti informácií
    f. Vyhľadávanie partnerov pre spoluprácu

>> Ďalší krok je zahrnutie hore uvedeného do plánu projektu a začatie práce!

Dobrým začiatkom pre definovanie vášho projektu je navrhnúť obchodný prípad. Tento obchodný prípad sa použije ako základ pre plán projektu a uplatní sa tiež v podpore vedenia a v získaní finančných prostriedkov alebo iných zdrojov.

Ukázalo sa ako účelné, keď sa neustále podávajú správy vedeniu, aby sa udržovala dobrá informovanosť o problémoch bezpečnosti IT, a aby sa takto trvale podporoval vlastný CSIRT.

Začatie obchodného prípadu začína analýzou problémov a príležitostí s využitím modelu analýzy popísaného v kapitole *5.3 Analýza zložky* a vyhľadávaním úzkeho kontaktu na potenciálnu zložku.

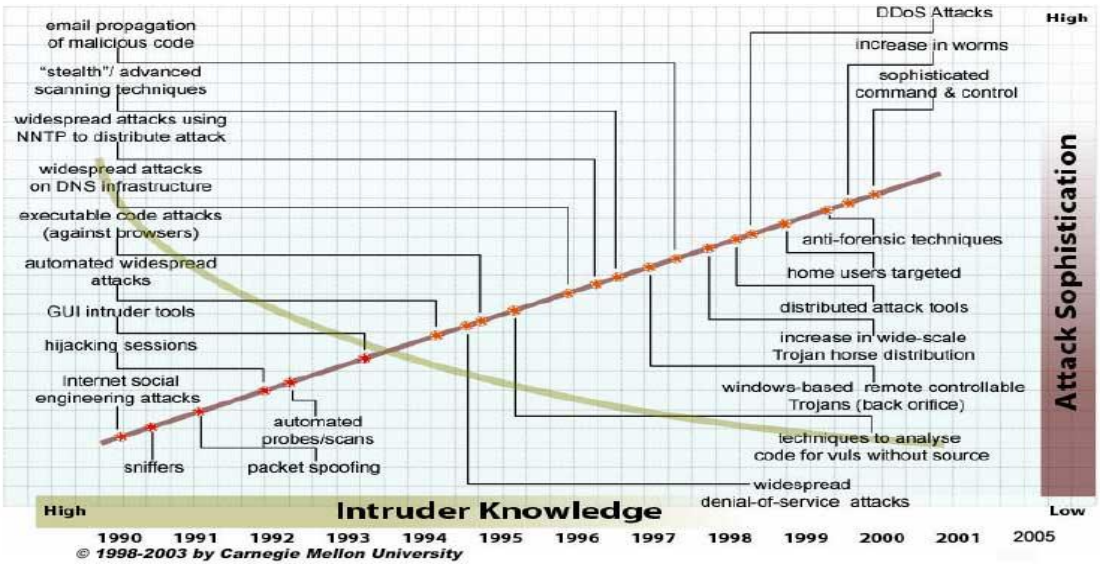
Ako bolo popísané skôr, keď sa začína s CSIRT, treba zvážiť mnohé otázky. Najlepšie je prispôsobiť vyššie uvedený materiál potrebám CSIRT, len čo potreby vzniknú.

Keď sa podávajú správy vedeniu, je dobrou praxou čo najviac aktualizovať vlastný prípad s využitím posledných článkov z novín alebo z Internetu a vysvetliť, prečo sú služby CSIRT a medzinárodnej koordinácie bezpečnostných incidentov rozhodujúce pre zaistenie obchodného majetku. Je taktiež dôležité vysvetliť, že len neustála podpora v otázkach bezpečnosti IT vedie k stabilnému obchodu, a to najmä v spoločnosti alebo organizácii, ktorá je závislá od IT.

(Poukazuje na to znamenitá veta Brucea Schneiera: *„Bezpečnosť nie je produkt, ale proces[17]!“)*

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

Veľmi známym nástrojom pre ilustráciu problémov bezpečnosti je nasledujúci graf poskytnutý tímom CERT/CC:



Šírenie škodlivého kódu elektronickou poštou

Pokrokové metódy skenovania "neviditeľných vírusov"

Rozsiahle útoky, ktoré na rozšírenie útoku využívajú štandardný protokol pre prevádzkovanie diskusných skupín – NNTP *(Network News* Transfer Protocol)

Rozsiahle útoky na systém doménových mien – DNS *(Domain Name System)*

Uskutočniteľné útoky na kódy (proti prehliadačom)

Automatizované rozsiahle útoky

Nástroje grafického užívateľského rozhrania narušiteľa – GUI *(Graphical User Interface)*

Únos presmerovaním prevádzky (únos relácie)

Internetové útoky na sociálne inžinierstvo (sociotechnický útok)

Automatizované prieskumy/skenovanie

Elektronické detekčné zariadenia pre odpočúvanie

Falšovanie paketov

Útoky DDoS

Zvýšenie počtu červov

Premyslený príkaz a kontrola

Antiforenzné metódy

Cieľoví domáci užívatelia

Nástroje rozosielaných útokov

Zvýšenie rozsahu rozosielania trojského koňa

Diaľkovo ovládateľné trojské kone založené na Windows (obslužný program)

Metódy analýzy kódu pre zraniteľnosť bez zdroja

Rozsiahle útoky typu odoprenia služby

Vysoká

Dômyselnosť útokov

Veľké Znalosti narušiteľa Malé

1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002

© 1998-2003 Univerzita Carnegie Mellon

Obr. 8 Znalosti narušiteľa verzus dômyselnosť útokov (zdroj CERT-CC[18])

Ukazuje trendy v bezpečnosti IT, najmä znižovanie potrebných schopností pre uskutočnenie čím ďalej tým dômyselnejších útokov.

Ďalší bod, o ktorom sa treba zmieniť, je neustále zmenšovanie časového rozpätia medzi okamžikom, kedy je k dispozícii aktualizácia softvéru na zraniteľnosť, a začatím útokov proti nemu:

Opravný balíček -> využitie		**Rýchlosť rozširovania**	
Nimda:	11 mesiacov	Redundancia kódu:	Dní
Slammer:	6 mesiacov	Nimda:	Hodín
Nachi:	5 mesiacov	Slammer:	Minút
Blaster	3 týždne		
Witty:	1 deň (!)		

Zhromaždené údaje o bezpečnostných incidentoch, potenciálne zlepšenie a získané poučenie vytvárajú tiež dobrú prezentáciu.

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

Opis obchodných plánov a hybných síl vedenia

Prezentácia pre vedenie, vrátane podpory CSIRT, sama o sebe nevytvára obchodný prípad, ale ak sa uskutoční vhodným spôsobom, vedie vo väčšine prípadov k podpore CSIRT zo strany vedenia. Na druhej strane by sa obchodný prípad nemal chápať ako čisto manažérske cvičenie, ale mal by sa použiť tiež pre komunikáciu s tímom a zložkou. Termínovaný obchodný prípad môže znieť veľmi komerčne a vzdialene od každodennej praxe CSIRT, ale poskytuje dobré zameranie a orientáciu, keď sa vytvára CSIRT.

Pre navrhnutie dobrého obchodného prípadu by sa mohli použiť odpovede na nasledujúce otázky (uvedené príklady sú hypotetické a používajú sa len pre ilustráciu. „Skutočné“ odpovede značne závisia od „skutočných“ okolností).

- Aký je problém?
- Čo by ste chceli u svojich zložiek dosiahnuť?
- Čo sa stane, keď nebudete robiť nič?
- Čo sa stane, keď urobíte opatrenie?
- Koľko to bude stáť?
- Čo sa získa?
- Kedy začnete a kedy to skončí?

Aký je problém?
Nápad vytvoriť CSIRT vo väčšine prípadov vznikne vtedy, keď sa bezpečnosť stane dôležitou súčasťou kľúčového podnikania spoločnosti alebo organizácie, a keď sa bezpečnostné incidenty IT stanú obchodným rizikom, ktoré zníži bezpečnosť obvyklej obchodnej činnosti.

Väčšina spoločností alebo organizácií má riadne oddelenie pre podporu alebo sekciu pre pomoc, ale vo väčšine prípadov sa bezpečnostné incidenty riešia nedostatočne a nie tak štruktúrovane, ako by to malo byť. Pracovné pole bezpečnostných incidentov si vo väčšine prípadov vyžaduje zvláštne odborné schopnosti a pozornosť. Mať štruktúrovanejší prístup je tiež výhodné a znižuje obchodné riziká a škody pre spoločnosť.

Problém väčšinou spočíva v tom, že koordinácia nie je dostatočná, a existujúce znalosti sa nepoužívajú na také riešenie bezpečnostných incidentov, ktoré by mohlo zamedziť ich výskytu v budúcnosti a predísť prípadným finančným stratám a / alebo poškodeniu povesti organizácie.

Aké ciele by sa mali u zložky dosiahnuť?
Ako bolo vysvetlené skôr, váš CSIRT bude slúžiť svojim zložkám a pomôže im v riešení bezpečnostných incidentov a problémov IT. Zvýšenie úrovne znalostí o bezpečnosti IT a dosiahnutie kultúry povedomia o bezpečnosti sú ďalšími cieľmi.

Táto kultúra sa usiluje o aktívne a preventívne opatrenia, ktoré sa prijímajú od začatia a znižujú tak prevádzkové náklady.

Zavedenie tejto kultúry spolupráce a pomoci v spoločnosti alebo organizácii môže vo väčšine prípadov všeobecne stimulovať efektívnosť.

Čo sa stane, keď sa nič neurobí?
Neštruktúrovaný spôsob zaobchádzania s bezpečnosťou IT môže viesť k ďalším škodám, v neposlednom rade k poškodeniu dobrého mena organizácie. Finančné straty a právne dôsledky môžu byť ďalšími následkami.

Čo sa stane, keď sa urobia opatrenia?
Povedomie o výskyte problémov bezpečnosti sa zvýši. To prispeje k ich efektívnejšiemu riešeniu a k zamedzeniu budúcim stratám.

Koľko to bude stáť?
V závislosti od organizačného modelu vzniknú náklady na platy členov tímu CSIRT a na organizáciu, vybavenie, nástroje a licencie softwaru.

Čo sa získa?
V závislosti od podnikania a strát v minulosti dosiahne sa viacej transparentnosti v postupoch a bezpečnostných praktikách, čím sa bude chrániť základný obchodný majetok.

Aká je aktuálnosť?
Opis vzorového plánu projektu pozri kapitole *12. Opis plánu projektu.*

Príklady existujúcich obchodných prípadov a prístupov
Dole je uvedených niekoľko príkladov obchodných prípadov CSIRT, ktoré má cenu skúmať.

- http://www.cert.org/csirts/AFI_case-study.html
  Vytvorení finančnej inštitúcie CSIRT: Prípadová štúdia

  Cieľom tohto dokumentu je zdieľať poučenie, ktoré získala finančná inštitúcia (v tomto dokumente uvádzaná ako AFI – *a financial institution*), keď spracúva a realizuje plán riešenia problému bezpečnosti a zavádza Tím pre reakciu na bezpečnostné incidenty počítačov – CSIRT *(Computer Security Incident Response Team).*

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Zhrnutie obchodného prípadu CERT POLSKA (premietanie diapozitívov vo formáte PDF).

- http://www.auscert.org.au/render.html?it=2252
  Vytvorenie Tímu pre reakciu na bezpečnostné incidenty – IRT *(Incident Response Team)* v 90. rokoch môže byť neľahká úloha. Mnoho pracovníkov, ktorí vytvárajú IRT, v tom nemá skúsenosti. Tento dokument skúma, akú úlohu môže IRT hrať v spoločnosti, a otázky, ktoré by sa mali riešiť tak v priebehu formovania tímu, ako aj po začatí jeho činností. Môže to byť prospešné pre existujúce tímy IRT, pretože sa môže zvýšiť povedomie o otázkach, ktoré sa skôr neriešili.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Prípadová štúdia o bezpečnosti informácií a zabezpečení podniku, od: Rogera Bentona.

  Toto praktické cvičenie je prípadovou štúdiou migrácie poisťovne do celopodnikového bezpečnostného systému. Zámerom tohto praktického cvičenia je poskytnúť cestu, ktorá sa má sledovať, keď sa vytvára bezpečnostný systém, alebo keď sa do neho migruje. Pôvodne bol jednoduchý bezpečnostný systém on-line jediným mechanizmom pre kontrolu prístupu k podnikovým údajom. Vystavenie riziku bolo veľké – neexistovali kontroly integrity mimo prostredia on-line. Každý so základnými schopnosťami programovania mohol dopĺňať, meniť a/alebo vymazávať výrobné údaje.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Stratégia elektronickej bezpečnosti v spoločnosti Marriot: spolupráca obchodných IT

  Skúsenosti Chrisa Zoladza z akciovej spoločnosti Marriot International, Inc., spočívajú v tom, že bezpečnosť elektronického obchodovania je proces, nie projekt. Táto správa Zoladza bola oznámená na poslednej Konferencii o elektronickej bezpečnosti a na Svetovej výstave elektronickej bezpečnosti v Bostonu, ktorú sponzorovala skupina Intermedia Group. Zoladz ako viceprezident pre ochranu informácií v Marriotte je podriadený právnemu oddeleniu, aj keď nie je právnik. Jeho úlohou je identifikovať, kde sú uložené najcennejšie obchodné informácie Marriotu, a ako sa pohybujú v rámci spoločnosti a mimo nej. V spoločnosti Marriott bola ustanovená zvláštna zodpovednosť za technickú infraštruktúru, ktorá podporuje bezpečnosť, a ktorá je zverená architektovi bezpečnosti IT.

Fiktívny CSIRT (7. krok)
Podpora obchodného plánu Bolo rozhodnuté zhromaždiť fakty a čísla z minulosti spoločnosti. Je to viacej ako účelné pre štatistický prehľad o situácii v bezpečnosti IT. Tento zber by mal pokračovať, keď je CSIRT vytvorený a pracuje, aby sa štatistický prehľad udržoval v aktuálnom stave. Boli kontaktované ďalšie národné tímy CSIRT a spytovali sa ich na ich obchodné prípady. Tímy poskytovali podporu zostavením určitých diapozitívov s informáciami o poslednom vývoji v bezpečnostných incidentoch IT a o nákladoch na bezpečnostné incidenty. V tomto vzorovom prípade fiktívneho CSIRT nebolo treba príliš presviedčať vedenie o dôležitosti problematiky IT, takže nebolo ťažké začať prvý krok. Bol spracovaný obchodný prípad a plán projektu, vrátane odhadu nákladov na prípravu a odhadu prevádzkových nákladov.

8 Príklady pracovných a technických postupov (priebeh prác)

Doteraz sme urobili nasledujúce kroky:

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.
4. Analýza prostredia a zložiek.
5. Stanovenie prehlásenia o poslaní.
6. Vypracovanie obchodného plánu
   a. Definovanie finančného modelu.
   b. Určenie organizačnej štruktúry
   c. Začatie náboru pracovníkov
   d. Používanie a vybavenie kancelárie
   e. Vypracovanie politiky bezpečnosti informácií
   f. Vyhľadávanie partnerov pre spoluprácu
7. Podpora obchodného plánu
   a. Schválenie obchodného prípadu.
   b. Začlenenie všetkého do plánu projektu.

>>Ďalší krok je: Zaistiť fungovanie CSIRT.

Keď sa zavedú dobre definované pracovné postupy, zlepší sa kvalita a zníži sa čas potrebný na prípad bezpečnostného incidentu alebo zraniteľnosti.

Ako bolo popísané vo vzorových rámčekoch, fiktívny CSIRT bude ponúkať základné kľúčové služby CSIRT:

- Výstrahy a varovania
- Riešenie bezpečnostných incidentov
- Oznámenia

Táto kapitola uvádza príklady pracovných postupov, ktoré opisujú kľúčové služby CSIRT. Obsahuje tiež informácie o zbere dát z rôznych zdrojov, ich overovanie z hľadiska dôležitosti a hodnovernosti a ich opätovné rozosielanie zložke. A nakoniec táto kapitola obsahuje príklady najdôležitejších postupov a špecifické nástroje CSIRT.

Hodnotenie inštalačnej bázy zložky

Prvý krok je získať prehľad o systémoch IT inštalovaných vo vašej zložke. CSIRT tak môže vyhodnotiť dôležitosť vstupných informácií a filtrovať ich pred opätovným rozoslaním, takže zložky nebudú zahltené informáciami, ktoré sú pre ne v podstate nadbytočné.

Dobrá prax je začať jednoducho, napr. s použitím listu v Excele ako nasledujúci:

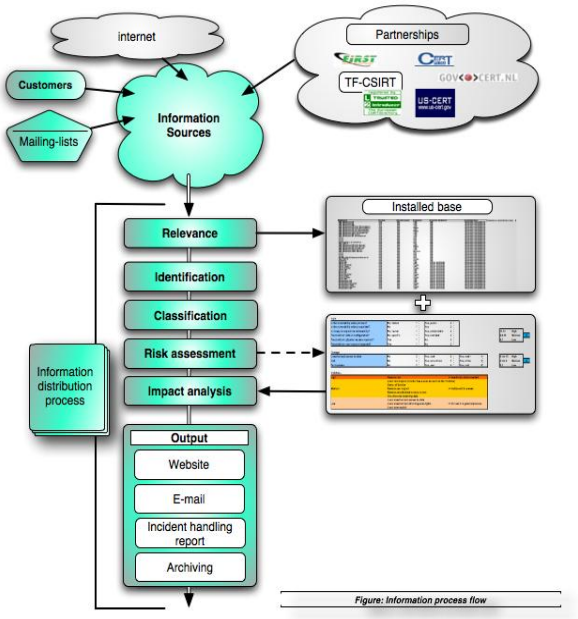
Kategória	Aplikácia	Produkt softvéru	Verzia	Operačný systém	Verzia operačného systému	Zložka
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Prehliadač	Internet Explorer	x-x-	Microsoft	XP-prof	A
Sieť	Smerovač	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Služby	Webový server	Apache		Unix	x-x-x	B

S funkciou filtru v Excele je veľmi ľahké vybrať vhodný softvér a zistiť, ktorá zložka aký druh softvéru používa.

Vytváranie výstrah, varovaní a oznámení

U vytvárania výstrah, varovaní a oznámení sa dodržujú rovnaké pracovní postupy:

- Zber informácií
- Hodnotenie informácií z hľadiska dôležitosti a zdroja
- Hodnotenie rizík založené na zhromaždených informáciách
- Rozoslanie informácií



Internet
Zákazníci, informačné zdroje
Adresáre
Dôležitosť
Identifikácia
Klasifikácia
Proces rozosielania informácií
Hodnotenie rizika
Analýza dopadu
Výstup
Webová stránka
Elektronická pošta
Správa o riešení bezpečnostných incidentov
Archivácia

Partnerstvo

Nainštalovaná báza

Obrázok: Postup procesov informácií

Obr. 9 Postup procesu informácií

V nasledujúcich bodoch bude tento pracovní postup popísaný podrobnejšie.

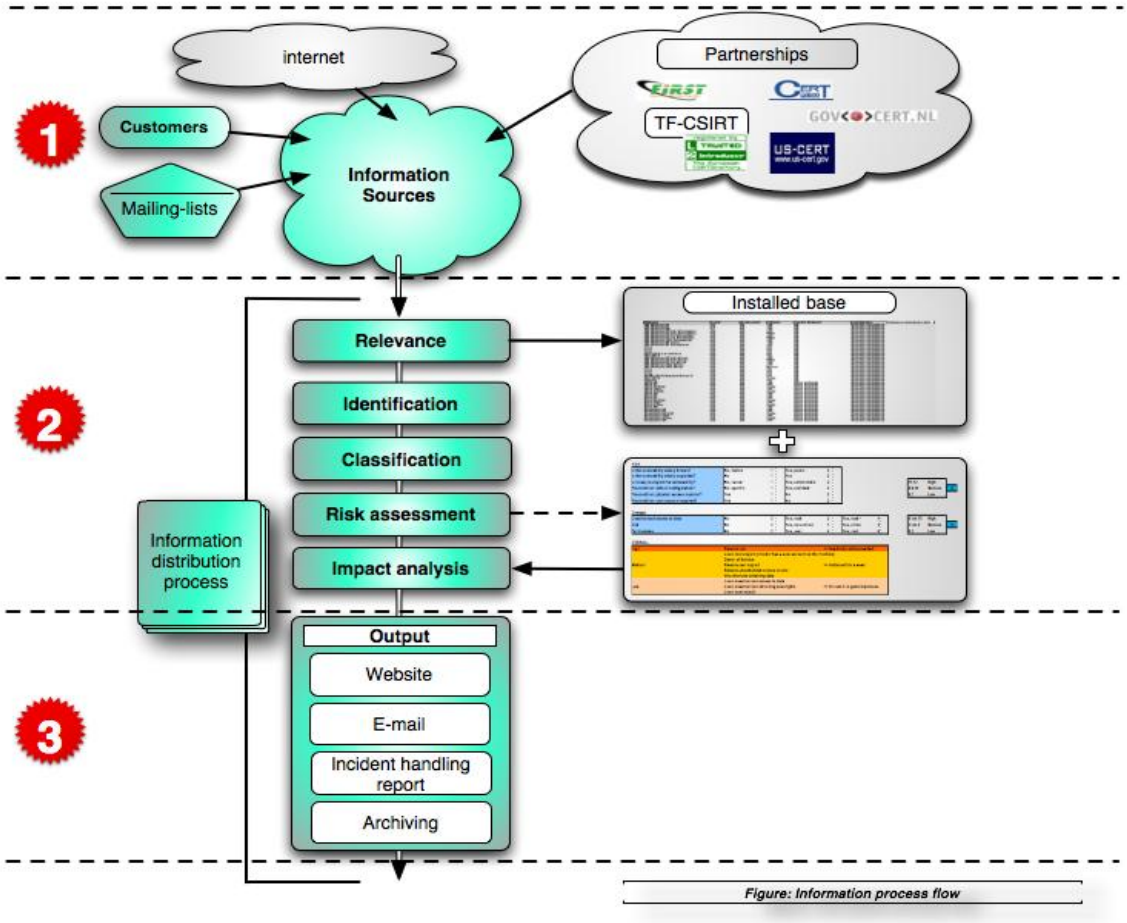


Figure: Information process flow

Internet
Zákazníci, informačné zdroje
Adresáre
Dôležitosť
Identifikácia
Klasifikácia
Proces rozosielania informácií
Hodnotenie rizika
Analýza dopadu
Výstup
Webová stránka
Elektronická pošta
Správa o riešení bezpečnostných incidentov
Archivácia

Partnerstvo

Nainštalovaná báza

Obrázok: Postup procesov informácií

1. krok: Zber informácií o zraniteľnosti.

Obvykle existujú dva hlavné druhy informačných zdrojov, ktoré prispievajú informáciami ako vstup pre služby:

- Informácie o zraniteľnosti (vašich) systémov IT
- Správy o bezpečnostných incidentoch

V závislosti od druhu podnikania a infraštruktúry IT existuje mnoho verejných a uzavretých zdrojov informácií o zraniteľnosti:

- Verejné a uzavreté adresáre
- Informácie o zraniteľnosti produktu predajcu
- Webové stránky
- Informácie na Internete (Google atď....)
- Verejné a súkromné partnerstvo, ktoré poskytuje informácie o zraniteľnosti (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

Všetky tieto informácie prispievajú k úrovni znalostí o špecifickej zraniteľnosti systémov IT.

Ako bolo uvedené skôr, na Internete je k dispozícii mnoho dobrých a ľahko dostupných zdrojov informácií o bezpečnosti. Pracovná skupina ad hoc agentúry ENISA „Služby CERT“ pre rok 2006 zostavuje v dobe spracúvania tejto správy podrobnejší zoznam, ktorý má byť hotový koncom roku 2006[19].

2. krok: Hodnotenie informácií a rizika

Výsledkom tohto kroku bude analýza dopadu špecifickej zraniteľnosti na infraštruktúru IT zložky.

Identifikácia
Prichádzajúce informácie o zraniteľnosti sa musia vždy identifikovať podľa ich zdroja, a než sa akákoľvek informácia odovzdá zložke, musí sa určiť, či je zdroj dôveryhodný. Inakšie by pracovníci mohli byť klamne varovaní, čo by mohlo viesť k zbytočným poruchám v podnikových procesoch a nakoniec poškodiť dobré meno CSIRT.

Nasledujúci postup ukazuje príklad identifikácie autentickosti správy:

Postup, ako identifikovať autentickosť správy a jej zdroja

Celkový kontrolný zoznam
1. Je zdroj ako taký známy a registrovaný?
2. Prichádza informácia bežným kanálom?
3. Je tam obsiahnutá „neobvyklá“ informácia, ktorá sa „zdá byť“ nesprávna?
4. Dajte na svoje dojmy, a ak máte pochybnosti o nejakej informácii, nerobte ďalej nič, ale znovu si ju overte!

Zdroje elektronickej pošty
1. Je zdrojová adresa organizácii známa a je známa v zdrojovom zozname?
2. Je podpis IPG správny?
3. V prípade pochybností overte celé záhlavie správy.

[19] Služby Pracovnej skupiny ad hoc CERT:
http://www.enisa.europa.eu/pages/ENISA_Working_group_CERT_SERVICES.htm

4. Ak máte pochybnosti, použite „nslookup“ (vyhľadávanie bezpečnosti siete) alebo „dig“ na overení domény odosielateľov[20].

Zdroje www
1. Overte certifikáty prehliadačov, keď sa napojujete na zaistenú webovú stránku (https://).
2. Overte zdroj z hľadiska obsahu a platnosti (technickej).
3. Ak máte pochybnosti, nekliknite na žiadne spojenia, ani si nestiahnite žiadny softvér.
4. Ak máte pochybnosti, majte aktivovaný „lookup“ (vyhľadávanie) a “dig“ na doméne a aktivujte „traceroute“ (sledovacia cesta).

Telefón
1. Pozorne počúvajte meno.
2. Rozoznávate hlas?
3. Ak máte pochybnosti, požiadajte volajúceho o telefónne číslo a o možnosť zatelefonovať mu späť.

Obr. 10 Príklad postupu identifikácie

Dôležitosť
Prehľad o nainštalovanom hardvéru a softvéru vytvorený skôr možno použiť na filtrovanie prichádzajúcich informácií o zraniteľnosti z hľadiska ich dôležitosti s cieľom nájsť odpoveď na otázky: „Používa zložka túto časť softvéru?“ „Je informácia pre ňu dôležitá?“

Klasifikácia
Niektoré prijaté informácie možno klasifikovať alebo označiť ako dôverné (napríklad správy o bezpečnostných incidentoch prichádzajúce od iných tímov). So všetkými informáciami sa musí zaobchádzať podľa požiadavky odosielateľa a v súlade s vlastnou politikou bezpečnosti informácií. Dobrým základným pravidlom je *„Nerozosielajte informáciu, ak nie je jasné, čo by mala znamenať; ak máte pochybnosti, požiadajte odosielateľa o súhlas s jej rozoslaním.“*

Hodnotenie rizika a analýza dopadov
Existuje niekoľko metód pre určení rizika a dopadu (potenciálnej) zraniteľnosti.

Riziko sa definuje ako potenciálna možnosť, že zraniteľnosť môže byť zneužitá. Je niekoľko dôležitých faktorov (okrem iných):

- Je zraniteľnosť dobre známa?
- Je zraniteľnosť značne rozšírená?
- Je ľahké zraniteľnosť zneužiť?
- Je zraniteľnosť zneužiteľná na diaľku?

Všetky tieto otázky poskytujú dobré povedomie o závažnosti zraniteľnosti.
Veľmi jednoduchou metódou výpočtu rizika je nasledujúci vzorec:

[20] Nástroje pre overenie identity v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Dopad = riziko x potenciálna škoda

Potenciálnou škodou by mohol byť

- Nepovolený prístup k údajom
- Odoprenie služby – DOS *(Denial of Service)*
- Získanie rozšírených povolení

(Prepracovanejšie schémy klasifikácie pozri koniec tejto kapitoly.)

Po zodpovedaní týchto otázok možno celkové hodnotenie doplniť do odbornej rady, ktorá informuje o potenciálnom riziku a škode. Často sa používajú jednoduché výrazy ako NÍZKE, STREDNÉ a VYSOKÉ.

Inou, komplexnejšou schémou hodnotenia rizika je:

Schéma hodnotenia GOVCERT.NL[21]
Holandský vládny CSIRT GOVCERT.NL spracoval maticu pre hodnotenie rizika, ktorá bola vyvinutá v počiatočnej fáze Govcert.nl, a stále sa aktualizuje podľa posledných trendov.

RISK

Is the vulnarability widely known?	No, limited	1	Yes, public	2				
Is the vulnarability widely exploited?	No	1	Yes	2				
Is it easy to exploit the vulnerability?	No, hacker	1	Yes, script kiddie	2				
Precondition: default configuration?	No. specific	1	Yes, standard	2				
Precondition: physical access required?	Yes	1	No	2				
Precondition: user account required?	Yes	1	No	2				

11,12	High	
8,9,10	Medium	0
6,7	Low	

Damage

Unauthorized access to data	No	0	Yes, read	2	Yes, read +	4		
DoS	No	0	Yes, non-critical	1	Yes, critica	5		
Permissions	No	0	Yes, user	4	Yes, root	6		

6 t/m 15	High	
2 t/m 5	Medium	0
0,1	Low	

OVERALL

High	Remote root	>> Imediately action needed!
Medium	Local root exploit (attacker has a user account on the machine) Denial of Service Remote user exploit Remote unauthorized access to data Unauthorized obtaining data	>> Action within a week
Low	Local unauthorized access to data Local unauthorized obtaining user-rights Local user exploit	>> Include it in general process

Obr. 11

RIZIKO										
Je zraniteľnosť známa v širokom meradle?	Nie, obmedzene	1	Áno, verejne	2						
Je zraniteľnosť rozsiahle znEÚžívaná?	Nie	1	Áno	2						
Je ľahké zraniteľnosť znEÚžiť?	Nie, hacker	1	Áno, script kiddie	2			11,12	Vysoká		
Predpoklad: vopred nastavená konfigurácia?	Nie, špecifická	1	Áno, štandardná				8, 9, 10	Stredná	0	
Predpoklad: Je nutný fyzický prístup?	Áno	1	Nie				8, 7	Nízka		
Predpoklad: Je nutný užívateľský účet?	Áno	1	Nie							
Škoda										
Nepovolený prístup k údajom	Nie	0	Áno, čítanie	4	Áno, čítanie +	4	6 t/m 15	Vysoký		
Odoprenie služby – DOS (Denial of Service)	Nie	0	Áno,	1	Áno,	5	02	Stred	0	

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

Povolenie	Nie	0	nevýznamné Áno, užívateľ	4	významné Áno, základné	6	t/m 5 0,1	ná Nízke
CELKOVÁ								
Vysoká	Vzdialený koreň (koreňový uzol)) Využitie miestneho koreňa (útočník má užívateľský účet v počítači) Odoprenie služby		>> Je nutné okamžité opatrenie					
Stredná	Diaľkové znEÚžitie užívateľa Diaľkový nepovolený prístup k údajom Nepovolené získanie údajov Miestny nepovolený prístup k údajom		>> Opatrenie do týždňa					
Nízka	Miestne nepovolené získanie užívateľských práv Miestne znEÚžitie užívateľa		>> Zaradenie do celkového procesu					

Obr. 12 Obr. Schéma hodnotenia GOVCERT.NL

Opis spoločnej formy poradenstva EISPP[22]

Európsky program podpory bezpečnosti informácií – EISIPP *(European Information Security Promotion Programme)* je projekt spolufinancovaný Európskym spoločenstvom na základe Piateho rámcového programu. Projekt EISIPP sa snaží rozvíjať Európsky rámec a nielen zdieľať znalosti o bezpečnosti, ale tiež vymedziť obsah a spôsoby šírenia informácií o bezpečnosti pre malé a stredné podniky – SME *(Small and Medium-Size Enterprises)*. Poskytovanie potrebných služieb bezpečnosti IT pre Európske SME ich podporí v rozvíjaní dôvery a v používaní elektronického obchodovania, ktoré vedie k väčším a lepším príležitostiam nových obchodov. EISPP je priekopníkom vo vízii Európskej komisie týkajúcej sa vytvárania Európskej siete odborných znalostí v rámci Európskej únie.

Nemecká forma poradenstva DAF *(Deutsches Advisory Format)*[23]

DAF je iniciatíva nemeckého Zväzu CERT *(CERT-Verbund)* a je základnou zložkou infraštruktúry pre vytváranie a výmenu odborných rád v bezpečnosti medzi rôznymi tímami. DAF je zvlášť prispôsobený potrebám nemeckých tímov CERT; normu spracoval a udržuje ju Zväz CERT *(CERT-Bund)*, DFN-CERT, PRESECURE a Siemens-CERT.

3. krok: Rozoslanie informácií

CSIRT si môže vybrať z niekoľkých metód rozosielania v závislosti od želaní zložiek a vašej stratégie komunikácie.

- Webová stránka
- Elektronická pošta
- Správy
- Archivácia a prieskum

[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

Odborné rady v bezpečnosti rozosielané tímom CSIRT by mali vždy dodržiavať rovnakú štruktúru. Zvýši sa tým ich zrozumiteľnosť a čitateľ rýchle nájde všetky dôležité informácie.

Odborná rada by mala obsahovať najmenej nasledujúce informácie:

Názov odbornej rady ……
Referenčné číslo …… **Dotyčné systémy** - …… - …… **Súvisiaci operačný systém + verzia** …… **Riziko** (Vysoké – Stredné – Nízke) …… **Dopad/potenciálna škoda** (Veľký – Stredný – Malý) …… **Vonkajšia identifikácia:** (Celková zraniteľnosť a vystavenie riziku – CVE *(Common Vulnerability and Exposure)*, Identifikácia bulletinu o zraniteľnosti) ……
Prehľad o zraniteľnosti …… **Dopad** …… **Riešenie** …… **Opis (podrobnosti)** …… **Príloha** ……

Obr. 13 Vzorová schéma odborných rad

Pozri kapitolu *10. Cvičenie na kompletný príklad odbornej rady v bezpečnosti*.

Riešenie bezpečnostných incidentov

Ako už bolo uvedené v úvode tejto kapitoly, proces zaobchádzania s informáciami v priebehu riešenia bezpečnostných incidentov je veľmi podobný procesu používanému počas zostavovania výstrah, varovaní a oznámení. Ale časť týkajúca sa zhromažďovania informácií je obvykle odlišná, pretože bežný spôsob získavania údajov o bezpečnostnom incidente spočíva buď v prijatí správ o bezpečnostných incidentoch od

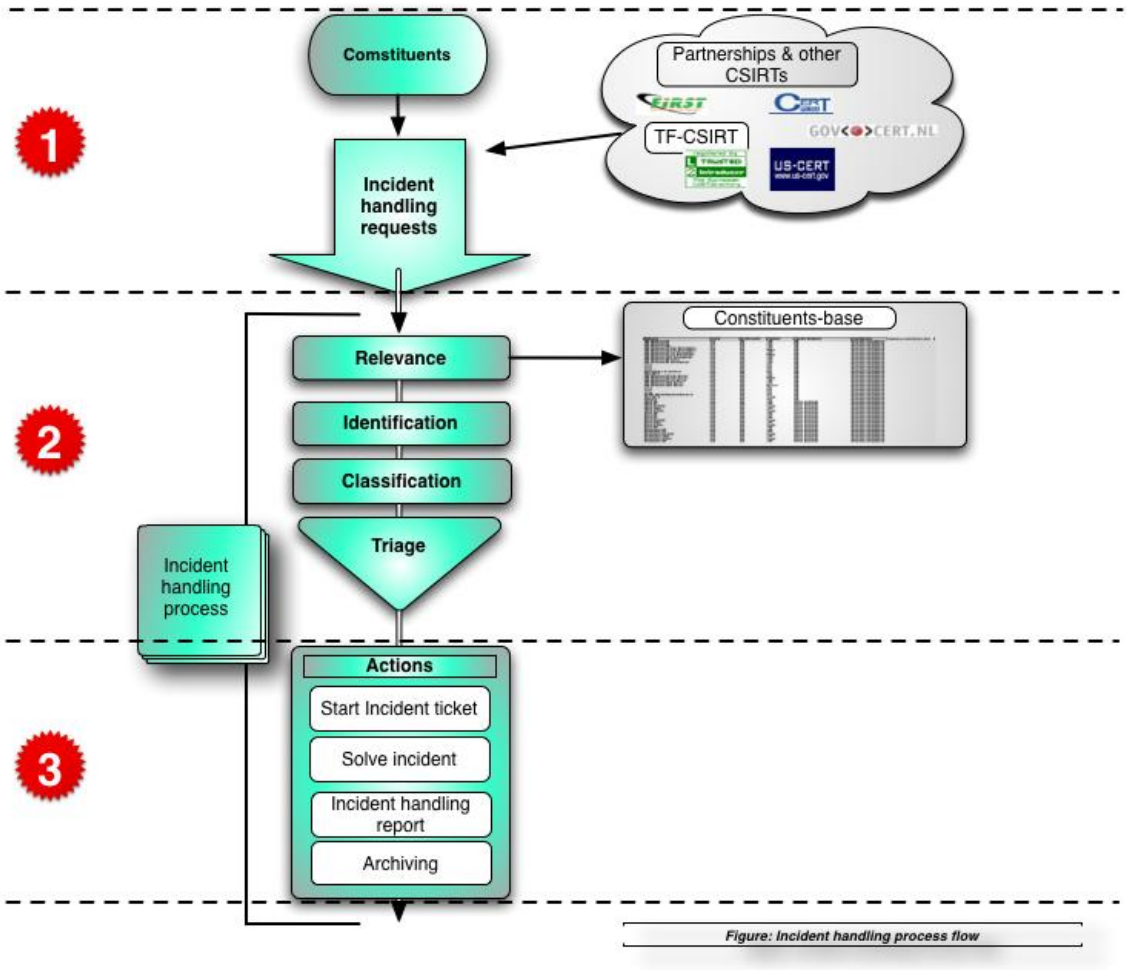
zložky alebo od iných tímov, alebo v prijatí spätnej väzby od zúčastnených strán počas procesu riešenia bezpečnostných incidentov. Informácie prichádzajú väčšinou (šifrovanou) elektronickou poštou; niekedy je nutné použiť telefón alebo fax.

Keď je informácia prijatá telefonicky, dobrou praxou je ihneď zaznamenať každú jednotlivú podrobnosť buď s použitím riešenia bezpečnostného incidentu/nástroja podávania správ, alebo vyhotovením krátkej písomnej správy. Je nutné ihneď (než telefonát skončí) vytvoriť číslo bezpečnostného incidentu (pokiaľ ho tento bezpečnostný incident doteraz nemá) a tomu, kto bezpečnostný incident ohlásil, ho dať telefonicky (alebo súhrnnou elektronickou správou zaslanou neskoršie) ako referenčné číslo pre ďalšiu komunikáciu.

Ostatná časť tejto kapitoly opisuje základný proces riešenia bezpečnostných incidentov. Hĺbková analýza úplného procesu riadenia bezpečnostných incidentov a všetkých používaných pracovných postupov a čiastkových pracovných postupov je uvedená v dokumentácii CERT/CC *Stanovenie procesov riadenia bezpečnostných incidentov pre tímy CSIRT*[24].

[24] Stanovenie procesov riadenia bezpečnostných incidentov: http://www.cert.org/archive/pdf/04tr015.pdf

Riešenie bezpečnostných incidentov v zásade dodržuje nasledujúci pracovný postup:



Zložka
Žiadosti o riešenie bezpečnostných incidentov
Dôležitosť
Identifikácia
Klasifikácia
Proces riešenia bezpečnostných incidentov
Triedenie
Opatrenie
Spustenie preukazov bezpečnostných incidentov
Riešenie bezpečnostných incidentov
Správa o riešení bezpečnostných incidentov
Archivácia

Partnerstvo a iné tímy CSIRT

Báza zložiek

Obrázok: Postup procesov informácií

Obr. 14 Postup procesu bezpečnostného incidentu

1. krok: Prijatie správ o bezpečnostných incidentoch

Ako už bolo uvedené skôr, správy o bezpečnostných incidentoch sa dostávajú do tímu CSIRT rôznymi kanálmi, väčšinou elektronickou poštou, ale tiež telefonicky a faxom.

Ako bolo spomenuté vyššie, keď sa prijíma správa o bezpečnostnom incidente, je dobrou praxou zaznamenať všetky podrobnosti v pevnom formáte. Tým sa zaistí, že sa nevynechá žiadna dôležitá informácia. Existuje nasledujúca vzorová schéma:

FORMULÁR HLÁSENIA BEZPEČNOSTNÉHO INCIDENTU

Vyplňte tento formulár a zašlite ho faxom alebo elektronickou poštou na: ……..
*Riadky označené hviezdičkou * sú povinné.*

Meno a organizácia
1. Meno*:
2. Názov organizácie*:
3. Druh sektoru:
4. Krajina*:
5. Mesto:
6. Elektronická adresa*:
7. Telefónne číslo*:
8. Iné:

Postihnutý hostiteľ (postihnutí hostitelia)
9. Počet hostiteľov:
10. Meno hostiteľa a internetový protokol – IP (Internet Protocol)*:
11. Funkcia hostiteľa*:
12. Časové pásmo:
13. Hardvér:
14. Operačný systém
15. Postihnutý softvér:
16. Postihnuté súbory:
17. Bezpečnosť:
18. Meno hostiteľa a IP:
19. Protokol/port:

Bezpečnostný incident
20. Referenčné číslo ref #:
21. Druh bezpečnostného incidentu:
22. Bezpečnostný incident začal:
23. Jedná sa o pokračujúci bezpečnostný incident: ÁNO NIE
24. Doba a spôsob zistenia:
25. Známa zraniteľnosť:
26. Podozrivé súbory:
27. Protiopatrenia:
28. Podrobný opis*:

Obr. 15 Obsah hlásenia bezpečnostného incidentu

2. krok: Hodnotenie bezpečnostného incidentu

Počas tohto kroku sa overuje autentickosť a závažnosť hláseného bezpečnostného incidentu a incident sa klasifikuje.

Identifikácia

Aby sa zamedzilo zbytočným krokom, dobrý zvyk je overiť si, či je odosielateľ správy dôveryhodný, a či je jedným z vás alebo spolupracovníkom zložiek tímov CSIRT. Uplatňujú sa podobné pravidlá ako tie, ktoré sú popísané v kapitole *8.2 Vytváranie výstrah*.

Závažnosť

Týmto krokom overujete, či žiadosť o riešenie bezpečnostného incidentu pochádza zo zložky tímov CSIRT, alebo či sa hlásený bezpečnostný incident týka systémov IT zložky. Ak neplatí nič z vyššie uvedeného, správa sa obvykle presmeruje na správny CISRT[25].

Klasifikácia

Týmto krokom sa spracúva triedenie na základe klasifikácie závažnosti bezpečnostného incidentu. Zaobchádzanie do podrobností klasifikácie bezpečnostných incidentov prekračuje rámec tohto dokumentu. Dobrým začiatkom je použitie schémy prípadovej klasifikácie CSIRT (príklad pre podnik 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.		

[25] Nástroje pre overenie identity v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

Kategórie bezpečnostných incidentov
Všetky bezpečnostné incidenty riadené tímom CSIRT by sa mali zaradiť do jednej z kategórií uvedených dole v tabuľke.

Kategória bezpečnostného incidentu	Citlivosť	Opis
Odoprenie služby	S3	• Útok DOS alebo DDOS.
Forenzná	S1	• Tím CSIRT nevykonal žiadnu forenznú prácu
Poškodené informácie	S1	• Pokus o porušenie alebo úspešné porušenie, poškodenie alebo sprístupnenie citlivých podnikových informácii alebo duševného vlastníctva.
Poškodený majetok	S1, S2	• Poškodený hostiteľ (základný účet, trojský kôň, rootkit), zariadenie siete, aplikácia, užívateľský účet. Zahŕňa to hostiteľov infikovaných škodlivým programom, kde útočník aktívne riadi hostiteľa.
Nezákonná činnosť	S1	• Krádež / podvod / ľudská bezpečnosť / detská pornografia. Bezpečnostné incidenty trestnej povahy týkajúce sa počítačov, ktoré pravdepodobne zahŕňajú vynucovanie práva, globálne vyšetrovanie alebo zábranu škôd.
Interné hackerstvo	S1, S2, S3	• Prieskum podozrivej činnosti pochádzajúcej zvonku, z miesta mimo podnikovej siete spoločnosti, okrem škodlivých programov.
Škodlivé programy	S3	• Vírus alebo červ, ktorý napadne mnohé podnikové zariadenia. Nezahŕňa to poškodených hostiteľov, ktorí sú aktívne riadení útočníkom prostredníctvom zadných vrátok alebo prostredníctvom trojského koňa. (Pozri poškodený majetok.)
Elektronická pošta	S3	• Predstieraná elektronická správa a iné udalosti týkajúce sa bezpečnosti elektronickej pošty.
Poradenstvo	S1, S2, S3	• Bezpečnostné poradenstvo, ktoré sa netýka žiadneho potvrdeného bezpečnostného incidentu.
Narušenie pravidiel v sieti	S1, S2, S3	• Zdieľanie škodlivého materiálu, zdieľanie/vlastnenie materiálu chráneného autorským právom. • Úmyselné porušenie politiky bezpečnosti informácií • Nevhodné používanie podnikového majetku ako počítač, sieť alebo aplikácia. • Nedovolené rozširovanie oprávnení alebo úmyselná snaha rozvrátiť riadenie prístupu.
* - Citlivosť sa bude meniť v závislosti od okolností. Poskytujú sa pokyny.		

Obr. 16 Schéma klasifikácie bezpečnostných incidentov (zdroj: Obr. 17 FIRST)[26]

Triedenie

Triedenie je systém používaný zdravotníckymi pracovníkmi alebo pracovníkmi záchrannej služby pre prideľovanie obmedzených zdravotníckych zdrojov, keď počet zranených, ktorí potrebujú ošetrenie, prekračuje disponibilné zdroje pre poskytovanie starostlivosti tak, aby bol ošetrený čo najväčší počet pacientov[27].

CERT/CC uvádza nasledujúci opis:

Triedenie je dôležitý prvok každé spôsobilosti riadenia bezpečnostných incidentov, a to najmä pre každý vytvorený CSIRT. Triedenie je na kritickej ceste k pochopeniu, o čom sa podávajú správy v celej organizácii. Slúži ako hybná sila, za pomoci ktorej všetky informácie postupujú do jedného kontaktného bodu, a ktorá umožňuje prehľad podniku o prebiehajúcej činnosti a uvádza všetky hlásené údaje do celkového vzájomného vzťahu. Triedenie umožňuje počiatočné hodnotenie prichádzajúcej správy a jej zoradenie pre ďalšie riešenie. Zaisťuje tiež miesto pre začatie zápisu počiatočnej dokumentácie a údajov správy alebo žiadosti, pokiaľ sa to už neurobilo v procese detekcie.

Funkcia triedenia poskytuje bezprostredný obraz súčasného stavu všetkých hlásených činností – aké správy sú otvorené alebo zatvorené, aké opatrenia sú dosiaľ otvorené a koľko správ od každého typu bolo prijatých. Tento proces môže pomôcť identifikovať potenciálne problémy bezpečnosti a stanoviť priority pracovných úloh. Informácie

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

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

zhromaždené počas triedenia možno tiež použiť na generovanie trendov zraniteľnosti a bezpečnostných incidentov a štatistických prehľadov pre vyššie vedenie[28].

Triedenie by mali uskutočňovať len najskúsenejší členovia tímov, pretože si vyžaduje hlboké chápanie možných dopadov bezpečnostných incidentov na konkrétne časti zložky a schopnosť rozhodovať, ktorý člen tímu by bol vhodný pre riešení tohto bezpečnostného incidentu.

[28] Stanovenie procesov riadenia bezpečnostných incidentov: http://www.cert.org/archive/pdf/04tr015.pdf

3. krok: Opatrenie

Triedené bezpečnostné incidenty sa obvykle zaraďujú do žiaduceho radu v nástroji pre riešenie bezpečnostných incidentov, ktorý používa jeden alebo viacej riešiteľov bezpečnostných incidentov dodržujúcich v zásade tieto kroky.

Spustenie preukazov bezpečnostných incidentov
Počet preukazov bezpečnostných incidentov už mohol byť generovaný v predchádzajúcom kroku (napríklad keď bol bezpečnostný incident nahlásený telefonicky). Pokiaľ nebol, prvý krok je vytvoriť taký počet, ktorý sa použije v ďalšej komunikácii o tomto bezpečnostnom incidente.

Životný cyklus bezpečnostného incidentu
Riešenie bezpečnostného incidentu nesleduje líniu krokov, ktoré nakoniec vedú k riešeniu, ale skôr cyklus krokov, ktoré sa opakovane používajú, dokiaľ sa bezpečnostný incident s konečnou platnosťou nevyrieši, a dokiaľ všetky dotknuté strany nemajú všetky potrebné informácie. Tento cyklus uvádzaný často ako „Životný cyklus bezpečnostného incidentu“ zahŕňa nasledujúce procesy:

Analýza: Analyzujú sa všetky podrobnosti o hlásenom bezpečnostnom incidente.

Získanie kontaktných informácií: Schopnosť odovzdať správu s informáciami o bezpečnostnom incidentu ďalej všetkým postihnutým stranám, ako sú iné tímy CSIRT, obete a najskôr vlastníci systémov, ktoré by boli mohli byť zneužité pre útok.

Poskytovanie technickej pomoci: Pomoc obetiam rýchle sa zotaviť z dôsledkov bezpečnostného incidentu a zhromaždiť viacej informácií o útoku.

Koordinácia: Informovanie iných postihnutých strán ako CSIRT zodpovedný za systém IT použitý pre útok alebo iné obete.

Táto štruktúra sa nazýva „životný cyklus“, pretože jeden krok vedie k druhému a k poslednému, ku koordinačnej časti, a potom môže zase viesť k novej analýze a cyklus začína znovu. Proces končí, keď všetky dotknuté strany dostanú a ohlásia všetky potrebné informácie.

Podrobnejší opis životného cyklu bezpečnostného incidentu pozri príručku CERT/CC CSIRT[29].

Správa o riešení bezpečnostných incidentov
Na otázky z vedenia o bezpečnostných incidentoch sa pripravte spracovaním správy. Dobrou praxou je tiež napísať dokument (len pre vnútornú potrebu) o „získanom

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

poučení“ s cieľom poučiť pracovníkov a vyhnúť sa chybám v procesoch budúceho riešenia bezpečnostných incidentov.

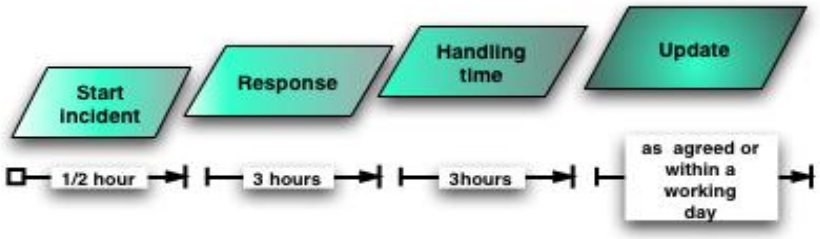
Archivácia
Podívajte sa na pravidlá archivácie popísané skôr v kapitole *6.6 Vypracovanie politiky bezpečnosti informácií.*

Podrobné pokyny k riadeniu a životnému cyklu bezpečnostných incidentov pozri časť prílohy A1 pod názvom *Ďalší výklad*.

Príklad časového harmonogramu reakcie

Na definíciu doby reakcie sa často zabúda, ale musí byť súčasťou každej dobre zostavenej zmluvy o úrovni služieb – SLA *(Service Level Agreement)* medzi CSIRT a jeho zložkou. Poskytovanie včasnej spätnej väzby zložkám počas riešenia bezpečnostných incidentov je veľmi dôležité tak pre vlastnú zodpovednosť zložiek, ako aj pre dobré meno tímu.
Doby reakcie sa musia zložke jasne oznámiť, aby sa zamedzilo mylným očakávaniam. Pre podrobnejšiu SLA so zložkou tímov možno ako východiskový bod použiť nasledujúci základný časový harmonogram.

Dole je príklad časového harmonogramu praktickej reakcie od okamžiku prijatia žiadosti o pomoc:



Začiatok bezpečnostného incidentu	Reakcia	Doba riešenia	Aktualizácia
½ hodiny	3 hodiny	3 hodiny	Podľa dohody alebo v pracovnej dobe

Obr. 17 Príklad časového harmonogramu reakcie

Dobrou praxou je tiež inštruovať zložku o jej vlastných dobách reakcie, najmä keď je CSIRT kontaktovaný v prípade núdzového stavu. Vo väčšine prípadov je lepšie kontaktovať jej CSIRT v rannom štádiu a dobrou praxou je podporiť zložku, aby tak urobila, ak má pochybnosti.

Dostupné nástroje CSIRT

Tato kapitola uvádza niekoľko pokynov k obvyklým nástrojom, ktoré používajú tímy CSIRT. Poskytuje len príklady, viacej pokynov je uvedených v *Informačnom centre nástrojov pre riešenie bezpečnostných incidentov (CHIHT - Clearinghouse of Incident Handling Tools)*[30].

Softvér pre šifrovanie elektronickej pošty a správ

- GNUPG http://www.gnupg.org/
  GnuPG je úplné a bezplatné zavádzanie projektu GNU normy OpenPGP podľa definície v RFC2440. GnuPG vám umožňuje šifrovať a podpisovať svoje údaje a oznámenia.

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

Nástroj riešenia bezpečnostných incidentov

Administratívne bezpečnostné incidenty a ich sledovanie, sledovanie opatrení.

- RTIR http://www.bestpractical.com/rtir/
  Sledovač žiadostí o reakciu na bezpečnostné incidenty – RTIR *(Request Tracker Incidence Response)* je bezplatný otvorený zdroj systému riešenia bezpečnostných incidentov vytvorený na základe potrieb tímov CERT a iných príslušných tímov pre reakciu na bezpečnostné incidenty.

Nástroje CRM

Ak máte veľa rôznych zložiek a potrebujete vysledovať všetky funkcie a podrobnosti, databáza CMR je užitočná. Existuje mnoho rôznych variant, tu je niekoľko príkladov:

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

- Sugarforce (bezplatná otvorená zdrojová verzia)
  http://www.sugarforge.org/

Overovanie informácií

- Internetová kontrola http://www.aignes.com/index.htm
  Tento program sleduje webové stránky z hľadiska ich aktualizácií a zmien.

- Sledovanie tejto stránky http://www.watchthatpage.com/
  Služba zasiela informácie o zmenách na webových stránkach elektronickou poštou (bezplatne a komerčne).

Vyhľadávanie kontaktných informácií

Vyhľadávanie správneho kontaktu pre hlásenie bezpečnostných incidentov nie je ľahká úloha. Tu je niekoľko informačných zdrojov, ktoré možno použiť:

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

- Organizácia RIPE[31]
- Objekt IRT[32]
- TI[33]

CHIHT okrem toho uvádza niektoré nástroje pre vyhľadávanie kontaktných informácií[34].

Fiktívny CSIRT (8. krok)

Vytvorenie pracovných postupov procesov a prevádzkových a technických postupov

Fiktívny CSIRT sa zameriava na poskytovanie týchto rozhodujúcich služieb CSIRT:

- Výstrahy a varovania
- Oznámenia
- Riešenie bezpečnostných incidentov

Tím spracoval postupy, ktoré dobre fungujú, a ktoré môže každý člen tímu ľahko pochopiť. Fiktívny CSIRT tiež najal právneho experta pre riešenie zodpovednosti a politiky bezpečnosti informácií. Tím schválil niekoľko užitočných nástrojov a v rámci rokovaní s inými tímami CSIRT zistil užitočné informácie o prevádzkových otázkach.

Bola vytvorená pevná šablóna pre poradenstvo v bezpečnosti a pre správy o bezpečnostných incidentoch. Na riešenie bezpečnostných incidentov tím používa sledovač žiadostí o reakciu na bezpečnostné incidenty – RTIR *(Request Tracker Incidence Response)*.

[31] Internetová služba organizácie RIPE zameraná na vyhľadávanie osôb a ich kontaktných údajov: http://www.ripe.net/whois

[32] Objekt IRT v databáze RIPE: http://www.enisa.europa.eu/cert_inventory/pages/04_02_01.htm#08

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

[34] Nástroje pre overenie identity v CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04

9 Výcvik CSIRT

Doteraz sme urobili nasledujúce kroky:

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.
4. Analýza prostredia a zložiek.
5. Stanovenie prehlásenia o poslaní.
6. Vypracovanie obchodného plánu
   a. Definovanie finančného modelu.
   b. Určenie organizačnej štruktúry
   c. Začatie náboru pracovníkov
   d. Používanie a vybavenie kancelárie
   e. Vypracovanie politiky bezpečnosti informácií
   f. Vyhľadávanie partnerov pre spoluprácu
7. Podpora obchodného plánu
   a. Schválenie obchodného prípadu.
   b. Začlenenie všetkého do plánu projektu.
8. Zaistenie fungovania CSIRT.
   a. Vytvorenie pracovných postupov
   b. Zavedenie nástrojov CSIRT

>> Ďalší krok je: výcvik pracovníkov.

Táto kapitola uvádza zoznam dvoch hlavných zdrojov pre vyhradený výcvik CSIRT: Výcvik v bezpečnosti sietí – TRANSITS *(Training of Network Security)* a CERT/CC.

TRANSITS

TRANSITS bol Európsky projekt na podporu vytvorenia tímov pre reakciu na bezpečnostné incidenty počítačov – CSIRT *(Computer Security Incident Response Teams)* a pre zdokonalenie existujúcich tímov CSIRT riešením problémov nedostatku odborne kvalifikovaných pracovníkov CSIRT. Tento cieľ sa riešil poskytovaním odborných výcvikových kurzov pre školenie pracovníkov (nových) CSIRT o organizačných, prevádzkových, technických, obchodných a právnych otázkach súvisiacich s poskytovaním služieb CSIRT.

TRANSITS najmä

- spracoval, aktualizoval a pravidelne revidoval modulárne školiace materiály kurzov
- organizoval školiace semináre, pre ktoré boli dodané materiály kurzov
- umožnil účasť pracovníkov (nových) tímov CSIRT na týchto školiacich seminároch so zvláštnym dôrazom na účasť zo štátov pristupujúcich k EÚ
- rozšíril školiace materiály kurzov a zaistil využitie výsledkov[35].

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

Agentúra ENISA uľahčuje a podporuje kurzy TRANSITS. Ak chcete vedieť, ako požiadať o kurzy, a ak chcete vedieť požiadavky a náklady, kontaktujte expertov CSIRT agentúry ENISA.

CERT-Relations@enisa.europa.eu

V prílohe tohto dokumentu sú vzorové materiály kurzov!

CERT/CC

Zložitosť počítačových infraštruktúr a infraštruktúr sietí a nároky na správu sťažujú náležité riadenie bezpečnosti sietí. Správcovia sietí a systémov nemajú dostatok pracovníkov a zavedených praktík bezpečnosti, aby sa bránili proti útokom a minimalizovali škody. V dôsledku toho sa počet bezpečnostných incidentov počítačov zvyšuje.
Ak sa vyskytnú bezpečnostné incidenty počítačov, organizácia musí rýchle a účinne reagovať. Čím rýchlejšie organizácia rozpozná, analyzuje a reaguje na bezpečnostný incident, tým viac môže obmedziť škody a znížiť náklady na obnovu. Vytvorenie tímu pre reakciu na bezpečnostné incidenty počítačov – CSIRT *(Computer Security Incident Response Team)* je vynikajúci spôsob, ako zaistiť túto schopnosť rýchle reagovať a tiež pomôcť predchádzať budúcim bezpečnostným incidentom.

CERT-CC ponúka kurzy pre manažérov a technických pracovníkov v takých oblastiach ako vytváranie a riadenie tímov pre reakciu na bezpečnostné incidenty počítačov (CSIRT), reagovanie na bezpečnostné incidenty a ich analyzovanie a zvyšovanie bezpečnosti sietí. Ak nie je uvedené inakšie, všetky kurzy sa konajú v Pittsburghu, PA. Naši pracovníci prednášajú v kurzoch o bezpečnosti tiež na Univerzite Carnegie Mellon.

Dostupné kurzy CERT/CC[36] venované tímom CSIRT

Vytvorenie tímu pre reakciu na bezpečnostné incidenty počítačov (CSIRT)
Riadenie tímov pre reakciu na bezpečnostné incidenty počítačov (CSIRT)
Zásady riešenia bezpečnostných incidentov
Pokročilé riešenie bezpečnostných incidentov pre technických pracovníkov

V prílohe tohto dokumentu sú vzorové materiály kurzov!

Fiktívny CSIRT (9. krok)
Výcvik pracovníkov Fiktívny CSIRT rozhodne vyslať všetkých svojich technických pracovníkov na nasledujúce kurzy TRANSITS, ktoré sú k dispozícii. Vedúci tímu sa okrem toho zúčastňuje na kurze *Riadenie CSIRT* z CERT/CC.

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

10 Cvičenie: Vytváranie odbornej rady

Doteraz sme urobili nasledujúce kroky:

1. Pochopenie, čo je CSIRT, a aké výhody môže poskytnúť.
2. Akému sektoru bude nový tím dodávať svoje služby?
3. Aký druh služieb môže CSIRT poskytovať svojej zložke.
4. Analýza prostredia a zložiek.
5. Stanovenie prehlásenia o poslaní.
6. Vypracovanie obchodného plánu
   a. Definovanie finančného modelu.
   b. Určenie organizačnej štruktúry
   c. Začatie náboru pracovníkov
   d. Používanie a vybavenie kancelárie
   e. Vypracovanie politiky bezpečnosti informácií
   f. Vyhľadávanie partnerov pre spoluprácu
7. Podpora obchodného plánu
   a. Schválenie obchodného prípadu.
   b. Začlenenie všetkého do plánu projektu.
8. Zaistenie fungovania CSIRT.
   a. Vytvorenie pracovných postupov
   b. Zavedenie nástrojov CSIRT
9. Výcvik vašich pracovníkov

>> Ďalší krok je precvičovanie a pripravenosť na skutočnú prácu!

Táto kapitola opisuje pre ilustráciu vzorové cvičenie na každodenné úlohy CSIRT: vytvorenie odbornej rady v bezpečnosti.

Podnetom bola nasledujúca pôvodná odborná rada v bezpečnosti rozoslaná Microsoftem:

Identifikátor bulletinu	**Bulletin Microsoftu o bezpečnosti MS06-042**
Názov bulletinu	**Cumulative Security Update for Internet Explorer (918899)** (Rozšírená aktualizácia bezpečnosti pre Internet Explorer (918899)
Celkové zhrnutie	Táto aktualizácia rieši rôznu zraniteľnosť vo webovom prehliadači Internet Explorer, ktorá by mohla umožniť uskutočňovanie diaľkového kódovania.
Najvyššie hodnotenie závažnosti	Critical (Rozhodujúca)
Dopad zraniteľnosti	Uskutočnenie diaľkového kódovania
Dotknutý softvér	**Windows, Internet Explorer.** Viacej informácií pozri časť Dotknutý software a adresy pre stiahnutie

Tento bulletin predajcu sa zaoberá zraniteľnosťou webového prehliadača Internet Explorer zistenou v poslednej dobe. Predajca uverejňuje mnohé opravné balíčky tohto softwaru pre početné verzie Microsoft Windows.

Po prijatí týchto informácií o zraniteľnosti prostredníctvom adresára začína fiktívny CSIRT s pracovným postupom popísaným v kapitole *8.2 Vytváranie výstrah, varovaní a oznámení*.

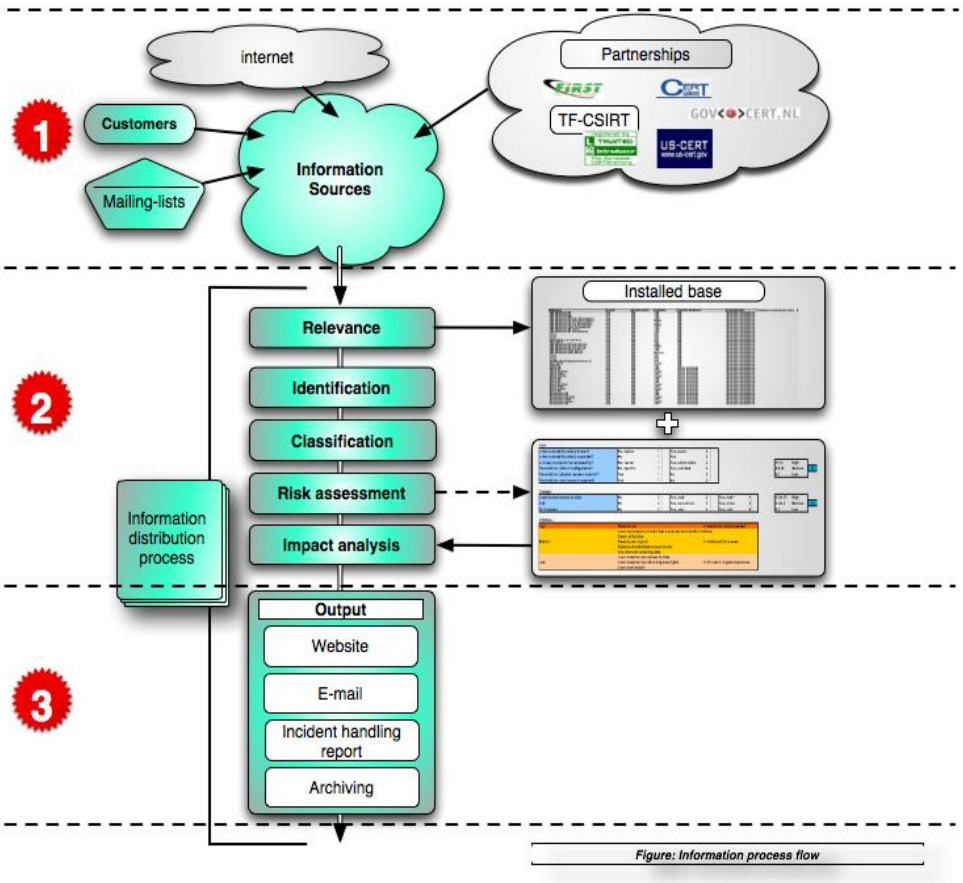


Figure: Information process flow

Internet
Zákazníci, informačné zdroje
Adresáre
Dôležitosť
Identifikácia
Klasifikácia
Proces rozosielania informácií
Hodnotenie rizika
Analýza dopadu
Výstup
Webová stránka
Elektronická pošta
Správa o riešení bezpečnostných incidentov

Partnerstvo

Nainštalovaná báza

Archivácia

Obrázok: Postup procesov informácií

1. krok: Zber informácií o zraniteľnosti.

Prvý krok je prezeranie webovej stránky predajcu. Fiktívny CSIRT overuje autentickosť informácii a zhromažďuje ďalšie podrobnosti o zraniteľnosti dotknutých systémov IT.

2. krok: Hodnotenie informácií a rizika

Identifikácia
Informácie už boli overené krížovou kontrolou informácií o zraniteľnosti prijatých elektronickou poštou s textom na webovej stránke predajcu.

Závažnosť
Fiktívny CSIRT kontroluje zoznam dotknutých systémov nájdený na webovej stránke so zoznamom systémov používaných v zložke. Zistí, že najmenej jedna z jeho zložiek používa Internet Explorer, takže informácie o zraniteľnosti sú skutočne relevantné.

Kategória	Aplikácia	Produkt softvéru	Verzia	Operačný systém	Verzia operačného systému	Zložka
Desktop	Prehliadač	Internet Explorer	x-x-	Microsoft	XP-prof	A

Klasifikácia
Informácie sú verejné, možno ich teda používať a znovu distribuovať.

Hodnotenie rizika a analýza dopadov
Zodpovedanie otázok ukazuje, že riziko a dopad sú *veľké* (hodnotené Microsoftom ako *rozhodujúce*).

RIZIKO

Je zraniteľnosť dobre známa?	Áno
Je zraniteľnosť značne rozšírená?	Áno
Je ľahké zraniteľnosť zneužiť?	Áno
Je zraniteľnosť zneužiteľná na diaľku?	Áno

ŠKODA
Možnými dopadmi sú vzdialená dostupnosť a potenciálne uskutočňovanie diaľkového kódovania. Táto zraniteľnosť zahŕňa početné problémy, ktoré spôsobujú, že riziko škody je vysoké.

3. krok: Distribúcia

Fiktívny CSIRT je interný CSIRT. Ako komunikačné kanály má k dispozícii elektronickú poštu, telefón a internú webovú stránku. CSIRT vydáva túto odbornú radu odvodenú zo šablóny z kapitoly *8.2 Vytváranie výstrah, varovaní a oznámení*.

Názov odbornej rady
Početná zraniteľnosť zistená v Internet Explorer

Referenčné číslo
082006-1
Dotknuté systémy
- Všetky systémy desktopu, ktoré používa Microsoft

Súvisiaci operačný systém + verzia
- Microsoft Windows 2000, 4. opravný balíček
- Microsoft Windows XP, 1. opravný balíček a Microsoft Windows XP, 2. opravný balíček
- Microsoft Windows XP Professional, vydanie x64
- Microsoft Windows Server 2003 a Microsoft Windows Server 2003, 1. opravný balíček
- Microsoft Windows Server 2003 pre systémy založené na Itaniu a Microsoft Windows Server 2003 s 1. opravným balíčkom – SP1 *(Service Pack 1)* pre systémy založené na Itaniu
- Microsoft Windows Server 2003, vydanie x64

Riziko (Vysoké—Stredné – Nízke)
VEĽKÉ
Dopad/potenciálna škoda (Veľký – Stredný – Malý)
VEĽKÝ
Vonkajšia identifikácia: (CVE, Identifikácia bulletinu o zraniteľnosti)
MS-06-42

Prehľad o zraniteľnosti
Microsoft zistil niekoľko závažných zraniteľností v prehliadači Internet Explorer, ktoré môžu viesť k uskutočňovaniu diaľkového kódovania.

Dopad
Narušiteľ by mohol prevziať úplnú kontrolu nad systémom, inštalovať programy, doplňovať užívateľov a osoby a meniť alebo mazať dáta. Zmierňujúcim faktorom je to, že k hore uvedenému môže prísť, keď sa užívateľ prihlási len s právami správcu. Dopad na užívateľov prihlásených s niekoľkými právami by mohol byť menší.

Riešenie
Nainštalujte ihneď opravný balíček na svoj Internet Explorer (IE).

Opis (podrobnosti)
Viacej informácií pozri ms06-042.mspx

Príloha
Viacej informácií pozri ms06-042.mspx

Tento výstup je teraz pripravený na rozoslanie. Pretože je to dôležitý bulletin, odporúča sa tiež zavolať zložky, keď je to možné.

Fiktívny CSIRT (10. krok)
Cvičenie: V priebehu prvých týždňov práce použil fiktívny CSIRT niekoľko fiktívnych prípadov (prijatých ako príklady od iných tímov CSIRT), ktoré sa použili ako cvičenie. Okrem toho vydal niekoľko odborných rád k bezpečnosti vychádzajúcich z informácií o skutočnej zraniteľnosti rozosielaných predajcami hardvéru a softvéru, ktoré doladil a prispôsobil potrebám zložky.

11 Záver

Tu návod končí. Dokument, ktorý je k dispozícii, je určený na poskytnutie veľmi stručného prehľadu o rôznych procesoch potrebných pre vytvorenie CSIRT. Dokument neobsahuje všetky informácie, ani príliš nezachádza do konkrétnych podrobností. Literatúru o tejto problematike, o ktorej sa oplatí dozvedieť viac, pozri v časti A.1 *Ďalší výklad*.

Pre fiktívny CSIRT by nasledujúcimi dôležitými krokmi mohli byť tieto::

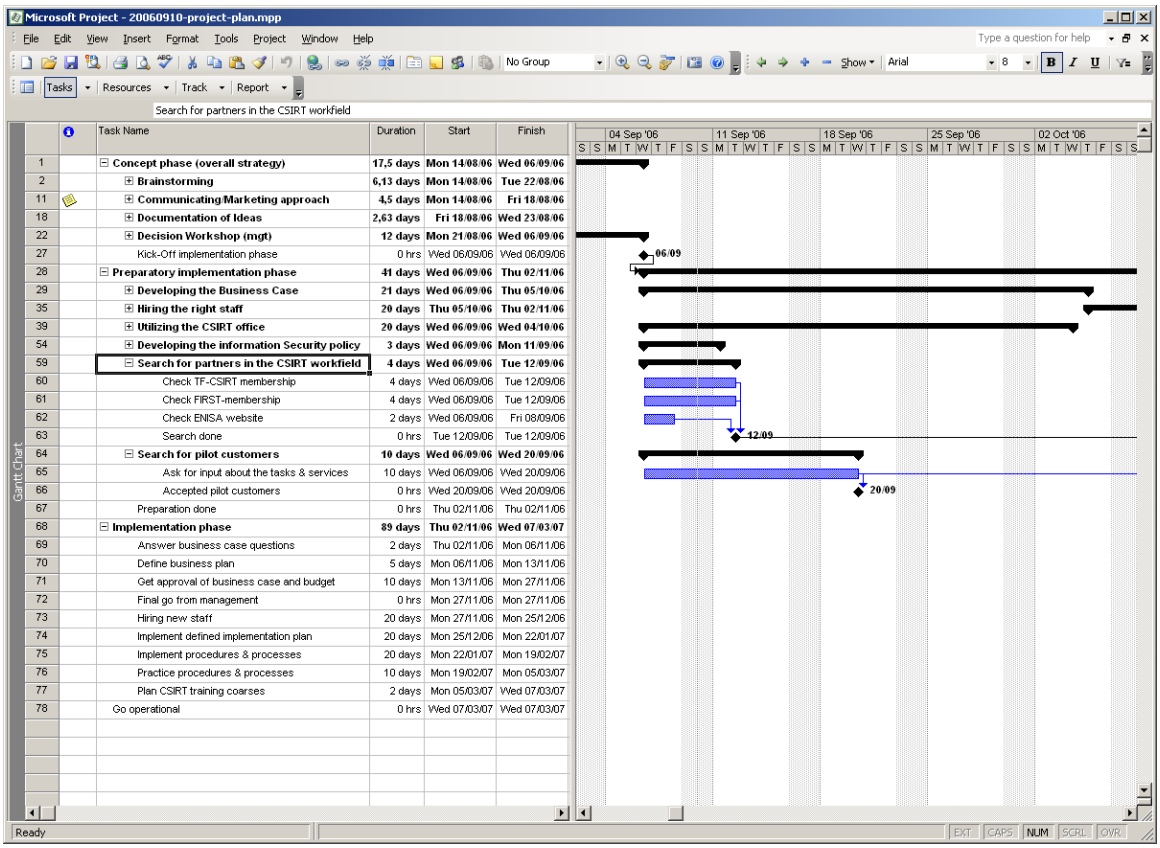
- Získať spätnú väzbu od zložky s cieľom doladiť poskytované služby.
- Získať rutinu v každodennej práci.
- Precvičiť si núdzové stavy.
- Zostať v blízkom kontakte s rôznymi skupinami CSIRT s cieľom prispieť raz k ich dobrovoľnej práci.

12 Opis plánu projektu

POZNÁMKA: Plán projektu je prvý odhad potrebného času. V závislosti od dostupných zdrojov môže byť skutočné trvanie projektu rôzne.

Plán projektu je k dispozícii v rôznych formátoch na CD a na webovej stránke agentúry ENISA. Úplne pokrýva všetky procesy popísané v tomto dokumente.

Hlavný formát bude Microsoft Project, môže sa teda priamo použiť v tomto nástroji riadenia projektu.



	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
11	Communicating/Marketing approach	4,5 days	Mon 14/08/06	Fri 18/08/06
18	Documentation of Ideas	2,63 days	Fri 18/08/06	Wed 23/08/06
22	Decision Workshop (mgt)	12 days	Mon 21/08/06	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
35	Hiring the right staff	20 days	Thu 05/10/06	Thu 02/11/06
39	Utilizing the CSIRT office	20 days	Wed 06/09/06	Wed 04/10/06
54	Developing the information Security policy	3 days	Wed 06/09/06	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

Projekt Microsoft

Vyhľadávanie partnerov v oblasti činnosti CSIRT

Názov úlohy

- Fáza koncepcie

+ Brainstorming

+ Oznámenie marketingovej koncepcie

+ Dokumentovanie nápadov

+ Seminár pre rozhodnutia (manažment)

Prechod do fázy realizácie

- Prípravná fáza realizácie

+ Vypracovanie obchodného prípadu

+ Nábor vhodných pracovníkov

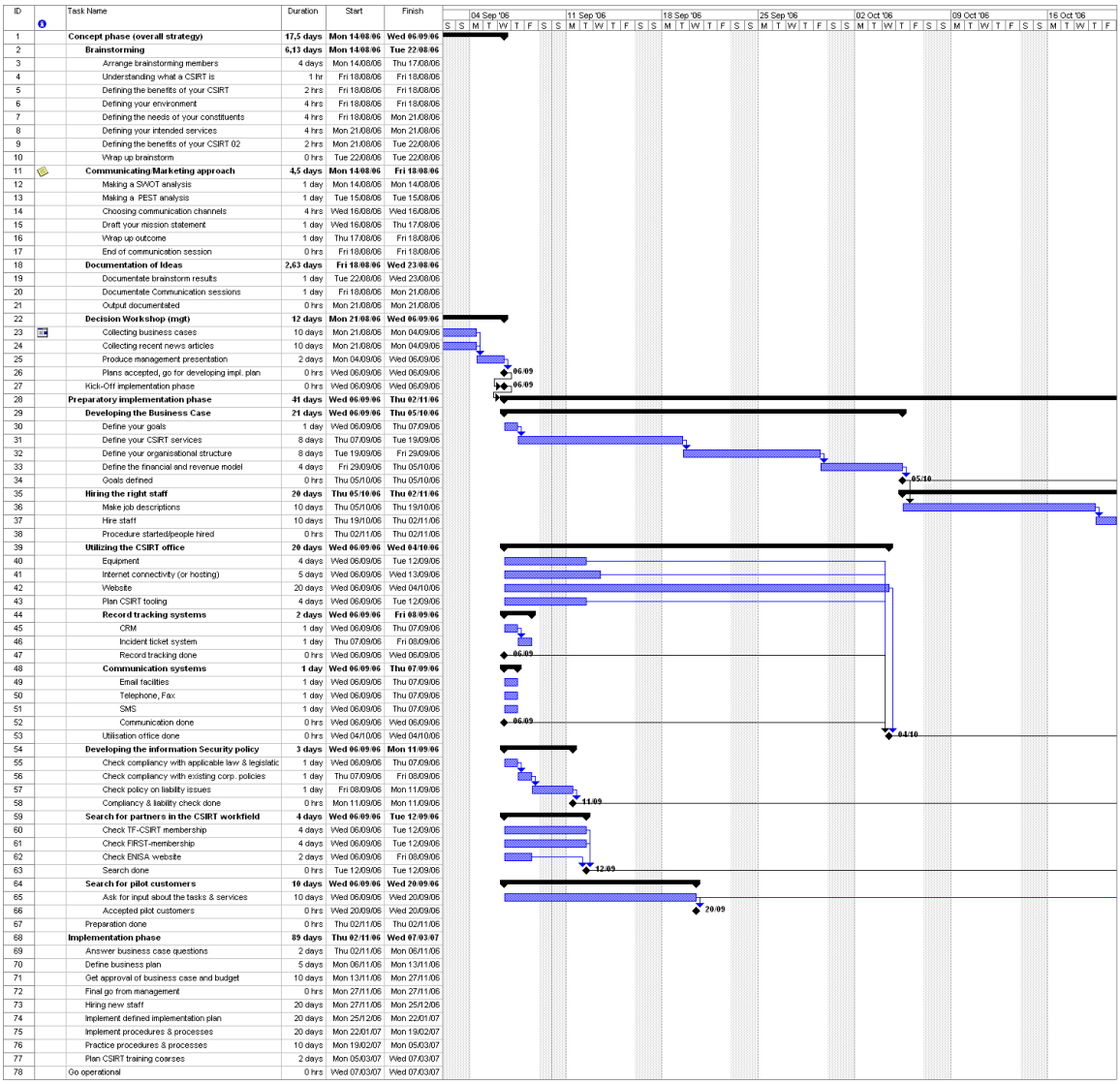
+ Používanie kancelárie CSIRT

- Vyhľadávanie partnerov v oblasti činnosti CSIRT

Overenie členstva v pracovnej skupine CSIRT

Overenie členstva vo FIRST
Overenie webovej stránky ENISA
Vyhľadávanie uskutočnené
- Vyhľadávanie pilotných zákazníkov
Žiadosť o vklad k úlohám a službám
Akceptovaní pilotní zákazníci
Príprava uskutočnená
- Fáza realizácie
Odpovede na otázky obchodného prípadu
Vytýčenie obchodného plánu
Získanie schválenia obchodného prípadu a rozpočtu
Záverečný východ z manažmentu
Nábor nových pracovníkov
Plnenie vytýčeného realizačného plánu
Zavedenie postupov a procesov
Používanie postupov a procesov
Plánovanie výcvikových kurzov CSIRT
Prechod na činnosť

Obr. 18 Plán projektu



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 courses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Názov úlohy
Fáza koncepcie
- **Brainstorming**
  - Zorganizovanie členov brainstormingu
  - Pochopenie, čo je CSIRT
  - Určenie výhod vášho CSIRT
  - Vymedzenie vášho prostredia
  - Určenie potrieb vašich zložiek
  - Určenie vašich predpokladaných služieb
  - Určenie výhod vášho CSIRT 02
  - Dokončenie brainstormingu
- **Oznámenie marketingovej koncepcie**
  - Uskutočnenie analýzy SWOT
  - Uskutočnenie analýzy PEST
  - Výber komunikačných kanálov
  - Vypracovanie definície poslania
  - Dokončenie výstupu
  - Ukončenie komunikačnej porady
- **Dokumentovanie nápadov**
  - Dokumentovanie výsledkov brainstormingu
  - Dokumentovanie komunikačnej porady

- Dokumentovaný výsledok
- **Seminár pre rozhodnutia (manažment)**
  - Spoločné obchodné prípady
  - Zhromažďovanie článkov o posledných novinkách
  - Vytvorenie prezentácie manažmentu
  - Plány schválené, prechod na vypracovanie realizačného plánu
  - Ukončenie realizačnej fázy
- **Prípravná realizačná fáza**
  - **Spracovanie obchodného prípadu**
    - Určenie vašich cieľov
    - Určenie služieb vášho CSIRT
    - Stanovenie vašej organizačnej štruktúry
    - Definovanie finančného modelu a modelu výnosov
    - Ciele stanovené
  - **Nábor vhodných pracovníkov**
    - Vypracovanie opisov práce
    - Nábor pracovníkov
    - Postup začatý/pracovníci najatí
  - **Používanie kancelárie CSIRT**
    - Zariadenie
    - Konektivita Internetu (možnosť pripojenia k Internetu) (alebo hosťovanie)
    - Webová stránka
    - Plánovanie nástrojov CSIRT
    - Systémy sledovania záznamov
      - CRM
      - Systémy preukazov bezpečnostných incidentov
      - Sledovanie záznamov uskutočnené
    - Systémy komunikácie
      - Vybavenie elektronickej pošty
      - Telefón, fax
      - SMS
      - Komunikácia uskutočnená
    - Využívanie kancelárie uskutočnené
  - **Vypracovanie politiky bezpečnosti informácií**
    - Overenie dodržiavania príslušných zákonov a legislatívy
    - Overenie dodržiavania existujúcich podnikových politík
    - Overenie politiky v otázkach zodpovednosti
    - Overenie právomocí a zodpovednosti uskutočnené
  - **Vyhľadávanie partnerov v oblasti činnosti CSIRT**
    - Overenie členstva v pracovnej skupine CSIRT
    - Overenie členstva vo FIRST
    - Overenie webovej stránky ENISA
    - Vyhľadávanie uskutočnené
  - **Vyhľadávanie pilotných zákazníkov**
    - Žiadosť o vklad k úlohám a službám
    - Akceptovaní pilotní zákazníci
  - Príprava uskutočnená
- **Fáza realizácie**
  - Odpovede na otázky obchodného prípadu
  - Vytýčenie obchodného plánu
  - Získanie schválenia obchodného prípadu a rozpočtu
  - Záverečný východ z manažmentu
  - Nábor nových pracovníkov
  - Plnenie vytýčeného realizačného plánu
  - Zavedenie postupov a procesov
  - Používanie postupov a procesov
  - Plánovanie výcvikových kurzov CSIRT
- Prechod na činnosť

Obr. 19 Plán projektu so všetkými úlohami a jedna časť Ganttovho diagramu

Plán projektu je k dispozícii tiež vo formáte CVS a XML. Ďalšie použitie si možno vyžiadať od expertov CSIRT agentúry ENISA: CERT-Relations@enisa.europa.eu

PRÍLOHA

A.1 Ďalší výklad

Príručka pre tímy CSIRT (CERT/CC)
Veľmi podrobné dielo s odkazmi na všetky otázky týkajúce sa práce CSIRT.
Zdroj: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Stanovenie procesov riadenia bezpečnostných incidentov pre tímy CSIRT: Prebiehajúce práce
Hĺbková analýza riadenia bezpečnostných incidentov
Zdroj: http://www.cert.org/archive/pdf/04tr015.pdf

Stav praxe tímov pre reakciu na bezpečnostné incidenty počítačov – CSIRT *(Computer Security Incident Response Teams)*.
Komplexná analýza aktuálnej situácie týkajúca sa celosvetového obrazu CSIRT, vrátane minulosti, štatistických prehľadov a mnohých ďalších otázok.
Zdroj: http://www.cert.org/archive/pdf/03tr001.pdf

CERT v rámčeku
Úplný opis poučenia získaného z vytvárania GOVCERT.NL a 'De Waarschuwingsdienst', holandskej štátnej služby pre vydávanie výstrah.
Zdroj: http://www.govcert.nl/render.html?it=69

RFC 2350: Očakávania od reakcie na bezpečnostné incidenty počítačov.
Zdroj: http://www.ietf.org/rfc/rfc2350.txt

Príručka pre riešenie bezpečnostných incidentov počítačov amerického Národného technického a normalizačného úradu – NIST *(National Institute of Standard and Technology)*[37]
Zdroj: http://www.securityunit.com/publications/sp800-61.pdf

Súpis agentúry ENISA týkajúci sa činností CERT v Európe
Príručka, ktorá uvádza informácie o tímoch CSIRT v Európe a ich rôzne aktivity
Zdroj: http://www.enisa.europa.eu/cert_inventory/

[37] NIST: Národný technický a normalizačný úrad *(National Institute of Standard and Technology)*

A.2 Služby CSIRT

Zvláštne poďakovanie patrí CERT/CC, ktorý poskytol tento zoznam.

Reaktívne služby	**Aktívne služby**	**Zaobchádzanie s artefaktmi**
• **Výstrahy a varovania** • **Riešenie bezpečnostných incidentov** • **Analýza bezpečnostných incidentov** • **Podpora reakcie na bezpečnostné incidenty** • **Koordinácia reakcií na bezpečnostné incidenty** • Reakcia na bezpečnostné incidenty na mieste • Riešenie zraniteľnosti • Analýza zraniteľnosti • Reakcia na zraniteľnosť • Koordinácia reakcií na zraniteľnosť	• **Oznámenie** • Sledovanie techniky • Audity alebo hodnotenia bezpečnosti • Konfigurácia a udržiavanie bezpečnosti • Vývoj nástrojov bezpečnosti • Služby detekcie narušenia • Šírenie informácií týkajúcich sa bezpečnosti	• *Analýza artefaktov* • *Reakcia na artefakty* • *Koordinácia reakcií na artefakty* ***Manažment kvality bezpečnosti*** • *Analýza rizík* • *Kontinuita obchodu a obnovenie prevádzky po havárii* • *Poradenstvo v bezpečnosti* • *Vytváranie povedomia* • *Vzdelávanie/výcvik* • *Hodnotenie alebo certifikácia produktov*

Obr. 20 Zoznam služieb CSIRT od CERT/CC

Opis služieb

Reaktívne služby

Reaktívne služby sú určené pre reakciu na žiadosti o pomoc, pre správy o bezpečnostných incidentoch zo zložky CSIRT a pre akékoľvek ohrozenie systémov CSIRT alebo útoky na ne. Niektoré služby môžu byť iniciované oznámením tretej strany alebo sledovaním monitoringu alebo súbormi log systému detekcie prieniku – IDS *(Intrusion Detection System)* a výstrahami.

Výstrahy a varovania

Táto služba zahŕňa šírenie informácií, ktoré opisujú útok narušiteľa, zraniteľnosť bezpečnosti, výstrahu narušenia, počítačový vírus alebo mystifikujúcu správu a zaistenie každého krátkodobého odporúčaného postupu konania pre riešenie vyplývajúceho problému. Výstraha, varovanie alebo odborná rada sa zasiela ako reakcia na aktuálny problém s cieľom oznámiť zložkám aktivitu a poskytnúť návod na ochranu ich systémov alebo na obnovu všetkých systémov, ktoré boli postihnuté. Informácie môže vytvoriť CSIRT alebo ich môžu opätovne rozoslať predajcovia, iné tímy CSIRT alebo experti na bezpečnosť či ostatné zložky.

Riešenie bezpečnostných incidentov

Riešenie bezpečnostných incidentov zahŕňa prijatie a triedenie žiadostí a správ a odpoveď na ne a analyzovanie bezpečnostných incidentov a udalostí. Konkrétne činnosti reakcie môžu zahŕňať

- prijímanie opatrení na ochranu systémov a sietí postihnutých alebo ohrozených rušivou činnosťou
- poskytnutie riešení a poskytnutie stratégií na základe príslušných odborných rád alebo výstrah
- pátranie po činnosti narušiteľov na iných častiach siete
- filtrovanie prevádzky na sieti
- systémy prestavby
- systémy zaplátania alebo opráv
- vypracovanie iných stratégií reakcie alebo stratégií dočasných opravných balíčkov *(workarounds)*.

Pretože činnosti riešenia bezpečnostných incidentov vykonávajú rôzne typy tímov CSIRT rozličnými spôsobmi, tieto služby sa ďalej kategorizujú na základe druhu vykonávaných činností a typu poskytovanej pomoci takto:

Analýza bezpečnostného incidentu

Existuje mnoho úrovní analýzy bezpečnostných incidentov a mnoho čiastkových služieb. Analýza bezpečnostných incidentov je v podstate skúška všetkých dostupných informácií a podporný dôkaz alebo artefakt týkajúci sa bezpečnostného incidentu alebo udalosti. Účelom analýzy je identifikovať rozsah bezpečnostného incidentu, rozsah škody spôsobenej bezpečnostným incidentom, povahu bezpečnostného incidentu a dostupné stratégie reakcie alebo dočasné opravné balíčky *(workarounds)*. CSIRT môže používať výsledky zraniteľnosti a analýzu artefaktov (popísanou dole) pre pochopenie a zaistenie komplexnejšej a aktuálnejšej analýzy toho, čo sa v konkrétnom systéme stalo. CSIRT uvádza do súladu činnosť naprieč bezpečnostnými incidentmi, aby určil akékoľvek vzájomné vzťahy, trendy, vzorce chovania alebo podpisy narušiteľov. Dve čiastkové služby, ktoré možno vykonávať ako súčasť analýzy bezpečnostných incidentov v závislosti od poslania, cieľov a procesov CSIRT, sú:

Zhromažďovanie súdnych dôkazov

Zhromažďovanie, uchovávanie, dokumentovanie a analyzovanie dôkazov z ohrozeného počítačového systému s cieľom určiť zmeny systému a pomôcť v rekonštrukcii udalostí vedúcich k ohrozeniu. Toto zhromažďovanie informácií a dôkazov sa musí uskutočňovať spôsobom, ktorý dokumentuje preukázateľný reťazec starostlivosti prípustný na súde podľa pravidiel dokazovania. Úlohy, ktoré sa týkajú zhromažďovania súdnych dôkazov, zahŕňajú (okrem iného) vyhotovenie kópie bitmapového obrázku pevného disku dotknutého systému; kontrolu zmien systému ako nové programy, súbory, služby a užívatelia; prezeranie prebiehajúcich procesov a otvorených portov; a kontrolu programov trojského koňa a súprav nástrojov. Pracovníci CSIRT, ktorí vykonávajú túto funkciu, sa môžu tiež pripraviť na to, že budú vystupovať ako znalecký svedkovia v súdnych konaniach.

Pátranie alebo sledovanie

Sledovanie pôvodu narušiteľa alebo identifikácie systémov, ku ktorým mal narušiteľ prístup. Táto činnosť môže zahŕňať pátranie alebo sledovanie, ako narušiteľ vstúpil do dotknutých systémov a súvisiacich sietí, ktoré systémy boli použité na získanie tohto prístupu, kde mal útok pôvod a aké iné systémy a siete boli použité ako súčasť útoku. Môže to tiež obsahovať snahu určiť totožnosť narušiteľa. Túto prácu môže niekto urobiť sám, ale obvykle ju vykonávajú pracovníci pre vynútenie práva, prevádzkovatelia internetových služieb alebo iné zainteresované organizácie.

Reakcie na bezpečnostné incidenty na mieste

CSIRT poskytuje priamu pomoc na mieste, aby pomohol zložkám zotaviť sa z bezpečnostného incidentu. CSIRT sám fyzicky analyzuje postihnuté systémy a vykonáva opravu a obnovenie systémov a neposkytuje podporu v reakcii na bezpečnostný incident len telefonicky alebo elektronickou poštou (pozri dole). Táto služba zahŕňa všetky opatrenia urobené na miestnej úrovni, ktoré sú nutné, keď je podozrenie na bezpečnostný incident, alebo keď k nemu príde. Ak sa CSIRT nenachádza na dotknutom mieste, členovia tímu by cestovali na toto miesto a zaistili by reakciu. V iných prípadoch môže byť miestny tím už na mieste a zaisťovať reakciu na bezpečnostný incident ako súčasť svojej rutinnej práce. Platí to najmä, keď riešenie bezpečnostného incidentu nezaisťuje vytvorený CSIRT, ale zaisťuje sa ako súčasť bežného pracovného fungovania systému, siete alebo správcov bezpečnosti.

Podpora reakcie na bezpečnostné incidenty

CSIRT pomáha obeti (obetiam) a vedie obeť (obete) útoku v zotavení sa z bezpečnostného incidentu za pomoci telefónu, elektronickej pošty, faxu alebo dokumentácie. Môže to zahŕňať technickú pomoc vo výklade zhromaždených údajov, v poskytovaní kontaktných informácií alebo v odovzdaní návodu na zmiernenie a stratégiu obnovy. Nezahŕňa to priame opatrenia týkajúce sa reakcie na bezpečnostný incident na mieste, ako je to popísané nižšie. CSIRT namiesto toho poskytuje návod na diaľku, takže pracovníci pôsobiaci na mieste môžu uskutočniť obnovu sami.

Koordinácia reakcií na bezpečnostné incidenty

CSIRT koordinuje snahy o reakciu medzi stranami, ktorých sa bezpečnostný incident týka. Obvykle to zahŕňa obeť útoku, iné miesta, ktorých sa útok týka, a všetky miesta, ktoré žiadajú o pomoc v analyzovaní útoku. Môže to taktiež zahŕňať strany, ktoré poskytujú podporu IT pre obeť, ako sú prevádzkovatelia služieb Internetu, iné tímy CSIRT a správcovia systémov a sietí na mieste. Koordinačná práca môže obsahovať zber kontaktných informácií, oznámenia miestam o ich možnom postihnutí (ako obeť alebo zdroj útoku), zber štatistických údajov o počte postihnutých miest a uľahčovanie výmeny a analýzy informácií. Časť koordinačnej práce môže obsahovať oznamovanie a spoluprácu s právnym poradcom organizácie, s oddeleniami pre ľudské zdroje alebo s oddelením pre styk s verejnosťou. Mohla by taktiež zahŕňať koordináciu s vynucovaním práva. Tieto služby nezahŕňajú priamu reakciu na bezpečnostný incident na mieste.

Riešenie zraniteľnosti

Riešenie zraniteľnosti zahŕňa prijímanie informácií a správ o zraniteľnosti hardwaru a softwaru; analyzovanie povahy, mechanizmov a dopadov zraniteľnosti a vypracovanie stratégií reakcie pre detekciu a opravu zraniteľnosti. Pretože činnosti riešenia zraniteľnosti realizujú rôzne typy tímov CSIRT rozličnými spôsobmi, tieto služby sa ďalej delia do kategórií na základe druhu vykonávaných činností a typu poskytovanej pomoci takto:

Analýza zraniteľnosti

CSIRT uskutočňuje technickú analýzu a kontrolu zraniteľnosti v hardvéru alebo v softvéru. Zahŕňa to overení podozrivej zraniteľnosti a technickú kontrolu zraniteľnosti hardvéru alebo softvéru, aby sa určilo, kde sa zraniteľnosť nachádza, a ako môže byť zneužitá. Analýza môže zahŕňať preskúmanie zdrojového kódu, použitie ladiaceho programu pre určenie, kde sa zraniteľnosť vyskytuje, alebo snahu o skopírovanie problémov na testovací systém.

Reakcia na zraniteľnosť

Táto služba zahŕňa určenie vhodnej reakcie pre zmiernenie alebo opravu zraniteľnosti. Môže sa to týkať vývoja prieskumných opravných balíčkov, záplat a dočasných opravných balíčkov *(workarounds)*. Zahŕňa taktiež oznamovanie zmierňujúcej stratégie pre iných, napríklad vytváraním a rozosielaním odborných rád alebo výstrah. Táto služba môže obsahovať zaisťovanie reakcie inštalovaním záplat, opravných balíčkov alebo dočasných opravných balíčkov.

Koordinácia reakcií na zraniteľnosť

CSIRT oznamuje zraniteľnosť rôznym častiam podniku alebo zložky a zdieľa informácie o tom, ako rýchle opraviť (zaplátať) alebo zmierniť zraniteľnosť. CSIRT overuje, či je stratégia reakcie na zraniteľnosť úspešne realizovaná. Táto služba môže zahŕňať komunikáciu s predajcami, inými tímami CSIRT, technickými odborníkmi, pracovníkmi zložky a s jednotlivcami alebo skupinami, ktorí zraniteľnosť pôvodne odhalili nebo nahlásili. Činnosti sa týkajú uľahčenia analýzy zraniteľnosti alebo správy o zraniteľnosti; koordinácie časových harmonogramov uvoľnenia zodpovedajúcich dokumentov, opravných balíčkov alebo dočasných opravných balíčkov; a syntézy odbornej analýzy uskutočnenej rôznymi stranami. Táto služba môže tiež zahŕňať udržovanie verejného alebo súkromného archívu alebo bázy znalostí informácií o zraniteľnosti a zodpovedajúcich stratégií reakcie.

Riešenie artefaktov

Artefakt je akýkoľvek súbor alebo objekt zistený v systéme, ktorý by mohol byť zapojený do prieskumu systémov a sietí alebo do útokov na ne, alebo ktorý sa používa na zmarenie bezpečnostných opatrení. Artefakty môžu okrem iného obsahovať počítačové vírusy, programy trojského koňa, červy, využívať skripty a súpravy nástrojov.

Zaobchádzanie s artefaktmi zahŕňa prijímanie informácií o artefaktoch a ich kópií, ktoré sa používajú v útokoch narušiteľov, v prieskume a v iných nepovolených alebo rušivých aktivitách. Keď už sa artefakt príjme, preskúma sa. Zahŕňa to analyzovanie povahy, mechanizmov, verzie a používania artefaktov; a vypracovanie (alebo navrhnutie) stratégií reakcie pre detekciu a odstránenie artefaktov a obranu proti nim. Pretože

aktivity riešenia artefaktov realizujú rôzne typy tímov CSIRT rozličnými spôsobmi, tieto služby sa ďalej delia do kategórií na základe druhu vykonávaných činností a typu poskytovanej pomoci takto:

Analýza artefaktov

CSIRT vykonáva technickú kontrolu a analýzu každého artefaktu zisteného v systéme. Uskutočnená analýza môže obsahovať identifikáciu druhu súboru a štruktúry artefaktu, porovnanie nového artefaktu s existujúcimi artefaktmi alebo s inými verziami toho istého artefaktu, aby sa zistili podobnosti a rozdiely, alebo reverzné (spätné) inžinierstvo alebo kód pre rozloženie s cieľom zistiť účel a funkciu artefaktu.

Reakcia na artefakt

Táto služba zahŕňa určenie príslušných činností pre detekciu a odstránenie artefaktov zo systému a tiež činností pre zamedzenie inštalácie artefaktov. Môže sa to týkať vytvorenia podpisov, ktoré možno doplniť do antivírového softwaru alebo IDS.

Koordinácia reakcií na artefakt

Táto služba zahŕňa zdieľanie a syntézu výsledkov analýzy a stratégie reakcie týkajúcej sa artefaktu s inými riešiteľmi, tímami CSIRT, predajcami a inými bezpečnostnými expertmi. Činnosti sa týkajú oznamovania technickej analýzy z rôznych zdrojov iným a jej syntézu. Činnosti môžu tiež obsahovať udržovanie verejného archívu alebo archívu zložky so známymi artefaktmi a ich dopadom a zodpovedajúcimi stratégiami reakcie.

Aktívne služby

Aktívne služby sú určené na zlepšenie infraštruktúry a procesov bezpečnosti zložky pred výskytom alebo detekciou bezpečnostného incidentu. Hlavným cieľom je zamedziť bezpečnostným incidentom a znížiť ich dopad a rozsah, keď k nim príde.

Oznámenia

Zahrnuje to okrem iného výstrahy týkajúce sa narušenia, varovania pred zraniteľnosťou a odborné rady v bezpečnosti. Tieto oznámenia informujú zložky o novom vývoji so strednodobým a dlhodobým dopadom, ako je novo zistená zraniteľnosť alebo nástroje narušiteľa. Oznámenia umožňujú zložkám chrániť svoje systémy a siete pred novo zistenými problémami skôr, než môžu byť použité.

Sledovanie techniky

CSIRT monitoruje a sleduje nový technický rozvoj a aktivity narušiteľov a súvisiace trendy, aby pomohol identifikovať budúce hrozby. Posudzované otázky možno rozšíriť o právne a legislatívne predpisy, sociálne alebo politické hrozby a vznikajúce technológie. Tieto služby zahŕňajú čítanie bezpečnostných adresárov, bezpečnostných webových stránok a aktuálnych článkov v novinách a časopisoch z oblasti vedy, techniky, politík a vlády s cieľom vybrať informácie týkajúce sa bezpečnosti systémov a sietí zložiek. Môže to zahŕňať komunikáciu s inými stranami, ktoré sú riadiacimi orgánmi v tejto oblasti, aby sa zaistilo, že sa získajú najlepšie a najpresnejšie informácie alebo výklad. Výsledkom týchto služieb by mohol byť určitý druh oznámení, návodov alebo odporúčaní zameraných na strednodobejšie až dlhodobé otázky bezpečnosti.

Audity alebo hodnotenia bezpečnosti

Tieto služby zaisťujú podrobné preskúmanie a analýzu bezpečnostnej infraštruktúry organizácie na základe požiadaviek ustanovených organizáciou alebo inými odvetvovými normami, ktoré sa aplikujú. Môže to tiež zahŕňať preskúmanie bezpečnostných praktík organizácie. Existuje mnoho rôznych druhov auditov alebo hodnotení, ktoré je možné poskytnúť, vrátane

Preskúmanie infraštruktúry

Manuálne preskúmanie konfigurácie hardvéru a softvéru, smerovačov, firewallov, serverov a prístrojov desktopu s cieľom zaistiť, aby zodpovedali najlepšej praxi v bezpečnostných politikách organizácie alebo odvetvia a štandardným konfiguráciám.

Preskúmanie najlepšej praxe

Rozhovory so zamestnancami a správcami systémov a sietí, aby sa zistilo, či ich bezpečnostné praktiky zodpovedajú ustanovenej bezpečnostnej politike organizácie alebo niektorým normám špecifickým pre dané odvetvie.

Skenovanie

Využitie skenerov zraniteľnosti alebo vírov s cieľom zistiť, ktoré systémy a siete sú zraniteľné.

Penetračné testovanie

Skúška bezpečnosti na mieste účelovým útokom na jeho systémy a siete.
Pred uskutočnením týchto auditov alebo hodnotení je nutné získať súhlas vyššieho vedenia. Niektoré z týchto metód môžu byť v politike organizácie zakázané. Poskytovanie týchto služieb môže zahŕňať vypracovanie spoločného súbor praktík, podľa ktorých sa uskutočňujú skúšky alebo hodnotenia, spolu s rozvojom potrebného súboru schopností alebo požiadaviek na certifikáciu pracovníkov, ktorí vykonávajú skúšky, hodnotenia, audity alebo preskúmania. Tieto služby možno tiež zadať dodávateľovi tretej strany alebo poskytovateľovi riadených bezpečnostných služieb, ktorý má príslušné odborné znalosti vo vykonávaní auditov a hodnotení.

Konfigurácia a udržiavanie nástrojov, aplikácií, infraštruktúr a služieb bezpečnosti

Tieto služby určujú a dávajú príslušný návod, ako bezpečne nastaviť a udržiavať nástroje, aplikácie a celkovú počítačovú infraštruktúru, ktorú používa tím CSIRT zložky alebo samotný CSIRT. Okrem poskytnutia návodu môže CSIRT uskutočňovať aktualizáciu konfigurácie a údržbu nástrojov a služieb bezpečnosti ako IDS, systémy skenovania alebo monitorovania siete, filtre, obtekanie *(wrappers)*, bezpečnostné rozhranie *(firewall)*, virtuálne privátne siete – VPN *(Virtual Private Network)* alebo mechanizmy overenia správnosti záznamov. CSIRT môže dokonca poskytovať tieto služby ako súčasť svojej hlavnej funkcie. CSIRT môže tiež nastavovať a udržiavať servery, desktopy, laptopy, osobných digitálnych asistentov – PDA *(Personál Digital Assistants)* a iné bezdrôtové zariadenia podľa smerníc o bezpečnosti. Tieto služby zahŕňajú predloženie všetkých otázok alebo problémov s konfiguráciou členom vedenia alebo používanie nástrojov a aplikácií, o ktorých je CSIRT presvedčený, že by mohli ponechať systém zraniteľný pre útok.

Vývoj nástrojov bezpečnosti

Táto služba zahŕňa vypracovanie všetkých nových nástrojov špecifických pre zložku, ktoré požaduje alebo chce zložka či samotný CSIRT. Môže to napríklad zahŕňať vypracovanie bezpečnostných opravných balíčkov pre softvér prispôsobený daným potrebám, ktorý používa zložka, alebo zaistené distribúcie softvéru, ktorý je možné použiť na obnovu narušených hostiteľov. Môže taktiež zahŕňať vývoj nástrojov alebo skriptov, ktoré rozširujú funkčnosť existujúcich nástrojov bezpečnosti ako nové zásuvné moduly (plug-in) pre skener zraniteľnosti alebo skener siete, skripty, ktoré uľahčujú používanie šifrovacej techniky alebo mechanizmy automatizovanej distribúcie opravných balíčkov.

Služby detekcie narušenia

Tímy CSIRT, ktoré vykonávajú tieto služby, preskúmavajú existujúce súbory log IDS, analyzujú a iniciujú reakciu na všetky udalosti, ktoré spĺňajú stanovenú prahovú hodnotu, alebo posielajú výstrahy podľa zmluvy o úrovni vopred definovaných služieb. Detekcia a analýza napadnutia súvisiacich bezpečnostných súborov log môže byť neľahká úloha – nielen v určení, kam v prostredí umiestniť snímač, ale aj v zbere a potom v analyzovaní veľkého množstva získaných údajov. V mnohých prípadoch sú nutné špecializované nástroje alebo odborné znalosti pre zhrnutie a výklad informácií s cieľom identifikovať falošné poplachy, útoky alebo udalosti na sieti a realizovať stratégie pre vylúčenie alebo minimalizovanie týchto udalostí. Niektoré organizácie sa rozhodnú zadať túto činnosť niekomu inému, kto má viacej odborných znalostí v poskytovaní týchto služieb, ako sú poskytovatelia riadených bezpečnostných služieb.

Šírenie informácií týkajúcich sa bezpečnosti

Tieto služby poskytujú zložkám komplexný súbor užitočných informácií, ktoré možno ľahko nájsť, a ktoré pomáhajú zvýšiť bezpečnosť. Tieto informácie môžu obsahovať

- návody pre podávanie správ a kontaktné informácie pre CSIRT
- archívy výstrah, varovaní a iných oznámení
- dokumentáciu o súčasných najlepších praktikách
- všeobecné návody k počítačovej bezpečnosti
- politiky, postupy a kontrolné zoznamy
- vypracovanie opravných balíčkov a informácií o distribúcii
- spojenie s predajcami
- aktuálne štatistické prehľady a trendy v hlásení bezpečnostných incidentov
- iné informácie, ktoré môžu celkovo zlepšiť bezpečnostné praktiky.

Informácie môže spracovávať a zverejňovať CSIRT alebo iná časť organizácie (IT, ľudské zdroje alebo oddelenie pre styk s médiami) a môžu obsahovať údaje z vonkajších zdrojov, ako sú iné tímy CSIRT, predajcovia a bezpečnostní experti.

Služby manažmentu kvality bezpečnosti

Služby, ktoré spadajú do tejto kategórie, nie sú špecifické predovšetkým pre riešenie bezpečnostných incidentov alebo pre CSIRT. Sú to dobre známe, zavedené služby určené na zvýšenie celkovej bezpečnosti organizácie. Zásluhou skúseností získaných v poskytovaní reaktívnych a aktívnych služieb popísaných vyššie môže CSIRT vniesť jedinečné hľadiská do týchto služieb manažmentu kvality, ktoré by inakšie nemuseli byť dostupné. Tieto služby sú určené na začlenenie spätnej väzby a získaného poučenia na základe znalostí nadobudnutých reagovaním na bezpečnostné incidenty a na

zraniteľnosť a útoky. Zahrnutie týchto skúseností do zavedených tradičných služieb (popísaných dole) ako súčasti procesu manažmentu kvality bezpečnosti môže zvýšiť dlhodobé úsilie v organizácii zamerané na bezpečnosť. V závislosti od štruktúr a zodpovedností organizácie môže tím CSIRT tieto služby poskytovať alebo sa môže podieľať na činnosti širšieho tímu organizácie.
Nasledujúce opisy vysvetľujú, ako môžu byť odborné znalosti CSIRT prospešné pre každú z týchto služieb manažmentu kvality bezpečnosti.

Analýza rizika

CSIRT môže pridať hodnotu k analýze a hodnoteniu rizika. Môže to zvýšiť schopnosť organizácie hodnotiť skutočné hrozby, aby sa zaistili realistické kvalitatívne a kvantitatívne hodnotenia rizík pre informační majetok a hodnotenie stratégií bezpečnosti a reakcie. Tímy CSIRT, ktoré zaisťujú tieto služby, by uskutočňovali analýzu rizika bezpečnosti informácií u nových systémov a podnikateľských procesov, alebo by u nich pomáhali, alebo by hodnotili hrozby a útoky na majetku a systémy zložiek.

Kontinuita podnikania a plánovanie obnovy po havárii

Na základe výskytov bezpečnostných incidentov v minulosti a budúcich predpovedí vznikajúceho bezpečnostného incidentu alebo trendov bezpečnosti môže čím ďalej tým viac bezpečnostných incidentov mať za následok znehodnotenie obchodných operácií. Preto by sa v činnostiach plánovania malo prihliadnuť k skúsenostiam a odporúčaniam CSIRT týkajúcim sa určenia, ako najlepšie reagovať na tieto bezpečnostné incidenty, aby sa zaistila kontinuita obchodných operácií. Tímy CSIRT, ktoré vykonávajú tieto služby, sú zapojené do súvislého podnikania a do plánovania obnovy po havárii u udalostí súvisiacich s hrozbami v bezpečnosti počítačov a s útokmi na ne.

Poradenstvo v bezpečnosti

CSIRT je možné využiť na poskytovanie rady a návodu k najlepším praktikám v bezpečnosti, aby sa realizovali obchodné operácie zložiek. CSIRT zaisťujúci tieto služby sa zúčastňuje v vypracovaní odporúčaní nebo v ustanovení požiadaviek na nakupovanie, inštaláciu alebo zaistenie nových systémov, zariadenia siete, aplikácie softwaru alebo celopodnikové podnikateľské procesy. Tieto služby zahŕňajú poskytovanie návodu a pomoci v vypracovaní politík organizácie alebo zložky týkajúcich sa bezpečnosti. Môžu tiež zahŕňať poskytovanie svedectva alebo odborných rád pre legislatívne alebo iné štátne orgány.

Vytváranie povedomia

Tímy CSIRT môžu identifikovať, kde zložky potrebujú viacej informácií a pokynov, aby lepšie spĺňali prijaté bezpečnostné praktiky a politiky organizácie týkajúce sa bezpečnosti. Zvyšovanie celkového povedomia ľudí zo zložky o bezpečnosti nielen zlepšuje ich chápanie otázok bezpečnosti, ale pomáha im tiež vykonávať každodenné operácie bezpečnejším spôsobom. Môže to znížiť výskyt úspešných útokov a zvýšiť pravdepodobnosť, že zložky zistia a ohlásia útoky a tým znížia doby obnovy a vylúčia alebo budú minimalizovať straty.
Tímy CSIRT, ktoré zabezpečujú tieto služby, vyhľadávajú príležitosti zvýšiť povedomie o bezpečnosti spracovaním článkov, plagátov, informačných bulletinov, webových stránok alebo iných informačných zdrojov, ktoré vysvetľujú najlepšie praktiky v bezpečnosti a poskytujú odborné rady alebo bezpečnostné opatrenia, ktoré sa majú

urobiť. Aktivity môžu tiež obsahovať časové plánovanie porád a seminárov, aby sa udržiavala aktuálna informovanosť zložiek o prebiehajúcich postupoch bezpečnosti a o potenciálnych hrozbách pre systémy organizácie.

Vzdelávanie/výcvik

Tieto služby zahŕňajú poskytovanie informácií zložkám o otázkach bezpečnosti počítačov za pomoci školení, seminárov, kurzov a cvičení. Otázky môžu obsahovať pokyny k hláseniu bezpečnostných incidentov, vhodné metódy reakcie, nástroje reakcie na bezpečnostné incidenty, metódy prevencie bezpečnostných incidentov a iné informácie potrebné pre ochranu, zisťovanie a hlásenie bezpečnostných incidentov počítačov a reagovanie na ne.

Hodnotenie alebo certifikácia produktov

U týchto služieb môže CSIRT uskutočňovať hodnotenie produktov z hľadiska nástrojov, aplikácií alebo iných služieb, aby sa zaistila bezpečnosť produktov a ich zhoda s prijateľnými bezpečnostnými praktikami CSIRT alebo organizácie. Preskúmavané nástroje a aplikácie môžu byť otvoreným zdrojom alebo komerčnými produktmi. Tieto služby možno poskytovať buď ako hodnotenie, alebo na základe programu certifikácie, a to v závislosti od noriem, ktoré organizácia alebo CSIRT aplikuje.

A.3 Príklady

Fiktívny CSIRT

0. krok – Chápanie, čo je CSIRT:
Vzorový CSIRT bude slúžiť strednej organizácii, ktorá má 200 pracovníkov. Organizácia má vlastné oddelenie IT a dve ďalšie pobočky v tej istej krajine. IT hrá kľúčovú úlohu pre spoločnosť, lebo sa používa pre internú komunikáciu, dátovú sieť a elektronické obchodovanie 24 hodín denne, 7 dní v týždni. Organizácia má vlastnú sieť a disponuje redundantným pripojením na Internet prostredníctvom dvoch prevádzkovateľov služieb siete Internet – ISP *(Internet Service Provider)*.

- -

1. krok: Počiatočná fáza
V počiatočnej fáze sa nový CSIRT plánuje ako interný CSIRT, ktorý poskytuje svoje služby pre hostiteľskú spoločnosť, miestne oddelenie IT a pracovníkov. Tiež podporuje a medzi rôznymi pobočkami koordinuje riešení incidentov súvisiacich s bezpečnosťou IT.

- -

2. krok: Výber správnych služieb
V počiatočnej fáze sa rozhodne, že nový CSIRT sa zameria hlavne na poskytovanie niektorej z kľúčových služieb pre zamestnancov.

Príjme sa rozhodnutie, že po pilotnej fáze by sa mohlo zvážiť rozšírenie portfólia služieb a doplniť služby manažmentu bezpečnosti. Toto rozhodnutie sa príjme na základe spätnej väzby od pilotných zložiek a v úzkej spolupráci s oddelením zaisťovania kvality.

- -

3. krok: Uskutočnenie analýzy zložky a vytvorenie vhodných komunikačných kanálov

Brainstormingová porada s niektorými kľúčovými osobami z vedenia a zo zložky generovala dostatočný vstup pre analýzu SWOT. Vedie to k záveru, že existuje potreba týchto rozhodujúcich služieb:

- výstrahy a varovania
- riešenie bezpečnostných incidentov (analýza, podpora reakcie a koordinácia reakcie)
- oznámenia.

Musí sa zaistiť, aby sa informácie rozosielali dobre organizovaným spôsobom s cieľom dostať ich k čo najväčšej časti zložky. Príjme sa teda rozhodnutie, že výstrahy, varovania a oznámenia vo forme bezpečnostných rád sa budú publikovať na vyhradenej webovej stránke a rozosielať pomocou adresára. Elektronická pošta, telefón a fax uľahčuje tímu CSIRT prijímať správy o bezpečnostných incidentoch. Ako ďalší krok sa plánuje unifikovaný webový formulár.

4. krok: Prehlásenie o poslaní

Vedenie fiktívneho CSIRT urobilo nasledujúce prehlásenie o poslaní:
"Fiktívny CSIRT poskytuje informácie a pomoc pracovníkom svojej hostiteľskej spoločnosti s cieľom znížiť riziká bezpečnostných incidentov počítačov a tiež reagovať na tieto bezpečnostné incidenty, keď sa vyskytnú."

Týmto fiktívnym CSIRT sa vysvetľuje, že sa jedná o interný CSIRT, a že jeho hlavnou úlohou je zaoberať sa otázkami súvisiacimi s bezpečnosťou IT.

- -

5. krok: Stanovenie obchodného plánu

Finančný model
Keďže spoločnosť uskutočňuje elektronický obchod 24 hodín denne, 7 dní v týždni, a má tiež oddelenie IT, ktoré pracuje 24 hodín denne, 7 dní v týždni, rozhodla sa poskytovať počas pracovnej doby úplné služby a mimo pracovnej doby služby na zavolanie. Služby pre zložku sa budú poskytovať bezplatne, ale v priebehu pilotnej a hodnotiacej fázy bude posúdená možnosť dodávania služieb externým zákazníkom.

Model výnosov
V priebehu počiatočnej a pilotnej fázy bude CSIRT financovaný prostredníctvom hostiteľskej spoločnosti. Počas pilotnej a hodnotiacej fázy bude prerokované ďalšie financovanie, vrátane možnosti predaja služieb externým zákazníkom.

Organizačný model
Hostiteľská organizácia je malá spoločnosť, takže bol vybraný vložený model.
Počas pracovnej doby bude personál zložený z troch pracovníkov poskytovať kľúčové služby (rozosielanie rád v bezpečnosti a riešenie / koordinácia bezpečnostných incidentov).

Oddelenie IT spoločnosti už zamestnáva pracovníkov s vhodnými odbornými schopnosťami. S týmto oddelením je urobená dohoda, takže nový CSIRT môže v prípade potreby požiadať o podporu na báze ad hoc. Možno využiť tiež ich technikov na zavolanie 2. línie.
Hlavný tím CSIRT bude mať štyroch členov na plný pracovný úväzok a päť ďalších členov. Jeden z nich je k dispozícii tiež na striedavej zmene.

Pracovníci
Vedúci tímu CSIRT má vzdelanie v bezpečnosti a podporu 1. a 2. úrovne a vykonával prácu v oblasti riadenia pretrvávajúcich kríz. Ostatní traja členovia tímu sú odborníci na bezpečnosť. Členovia tímu CSIRT z oddelenia IT na čiastočný pracovný úväzok sú odborníci na infraštruktúru spoločnosti.

6. krok: Používanie kancelárie a politiky bezpečnosti informácií

Vybavenie a umiestnenie kancelárie

Pretože hostiteľská spoločnosť už má zavedenú efektívnu fyzickú bezpečnosť, nový CSIRT je v tomto ohľade dobre chránený. Je zaistená takzvaná „spravodajská informačná sála“, aby bola možná koordinácia v prípade núdzového stavu. Bol zakúpený trezor pre šifrované materiály a citlivé dokumenty. Bola zriadená zvláštna telefónna linka, vrátane telefónnej ústredne pre uľahčenie horúcej linky počas pracovnej doby a zaistený mobilný telefón s rovnakým telefónnym číslom pre službu „na zavolanie“ mimo pracovnej doby.

Možno tiež využiť existujúce zariadenie a podnikovú webovú stránku pre oznamovanie informácií týkajúcich sa CSIRT. Softvér adresára je nainštalovaný, udržuje sa a má vyhradenú časť pre komunikáciu medzi členmi tímu a s ostatnými tímami. Všetky kontaktné podrobnosti pracovníkov sa ukladajú do databázy, kópia sa bezpečne uchováva.

Predpisy

Keďže CSIRT je začlenený do spoločnosti, ktorá má politiky bezpečnosti informácií, boli za pomoci právneho poradcu spoločnosti vytvorené zhodné politiky pre CSIRT.

- -

7. krok: Vyhľadávanie spolupráce

S využitím Súpisu agentúry ENISA bolo možné niektoré tímy CSIRT v tej istej krajine rýchle vyhľadať a kontaktovať. S jedným z nich bola pre novo prijatého vedúceho tímu zorganizovaná návšteva na mieste. Dozvedel sa o činnostiach národného CSIRT a zúčastnil sa na porade.

Táto porada bola viac ako užitočná na to, aby sa zhromaždili príklady pracovných metód, a aby sa získala podpora niekoľkých iných tímov.

- -

8. krok: Podpora obchodného plánu

Bolo rozhodnuté zhromaždiť fakty a čísla z minulosti spoločnosti. Je to viacej ako účelné pre štatistický prehľad o situácii v bezpečnosti IT. Tento zber by mal pokračovať, keď už je CSIRT vytvorený a pracuje, aby sa štatistické prehľady udržovali v aktuálnom stave.

Boli kontaktované ďalšie národné tímy CSIRT a spytovali sa ich na ich obchodné prípady. Tímy poskytli podporu zostavením určitých diapozitívov s informáciami o poslednom vývoji v bezpečnostných incidentoch IT a o nákladoch na bezpečnostné incidenty.

V tomto vzorovom prípade fiktívneho CSIRT nebolo treba príliš presviedčať vedenie o dôležitosti problematiky IT, takže nebolo ťažké podniknúť prvý krok. Bol spracovaný obchodný prípad a plán projektu, vrátane odhadu nákladov na prípravu a odhadu prevádzkových nákladov.

- -

9. krok: Vytvorenie pracovných postupov procesov a prevádzkových a technických postupov

Fiktívny CSIRT sa zameriava na poskytovanie týchto kľúčových služieb CSIRT:

- výstrahy a varovania
- oznámenia
- riešenie bezpečnostných incidentov

Tím spracoval postupy, ktoré dobre fungujú, a ktoré môže každý člen tímu ľahko pochopiť. Fiktívny CSIRT tiež najal právneho experta pre riešenie zodpovednosti a politiky bezpečnosti informácií. Tím schválil niekoľko užitočných nástrojov a v rokovaniach s inými tímami CSIRT zistil užitočné informácie o prevádzkových otázkach.

Bola vytvorená pevná šablóna pre poradenstvo v bezpečnosti a pre správy o bezpečnostných incidentoch. Pre riešenie bezpečnostných incidentov tím používa RTIR.

- -

10. krok: Výcvik pracovníkov

Fiktívny CSIRT rozhodne vyslať všetkých svojich technických pracovníkov na nasledujúce kurzy TRANSITS, ktoré sú k dispozícii. Vedúci tímu sa okrem toho zúčastňuje na kurze *Riadenie CSIRT* z CERT/CC.

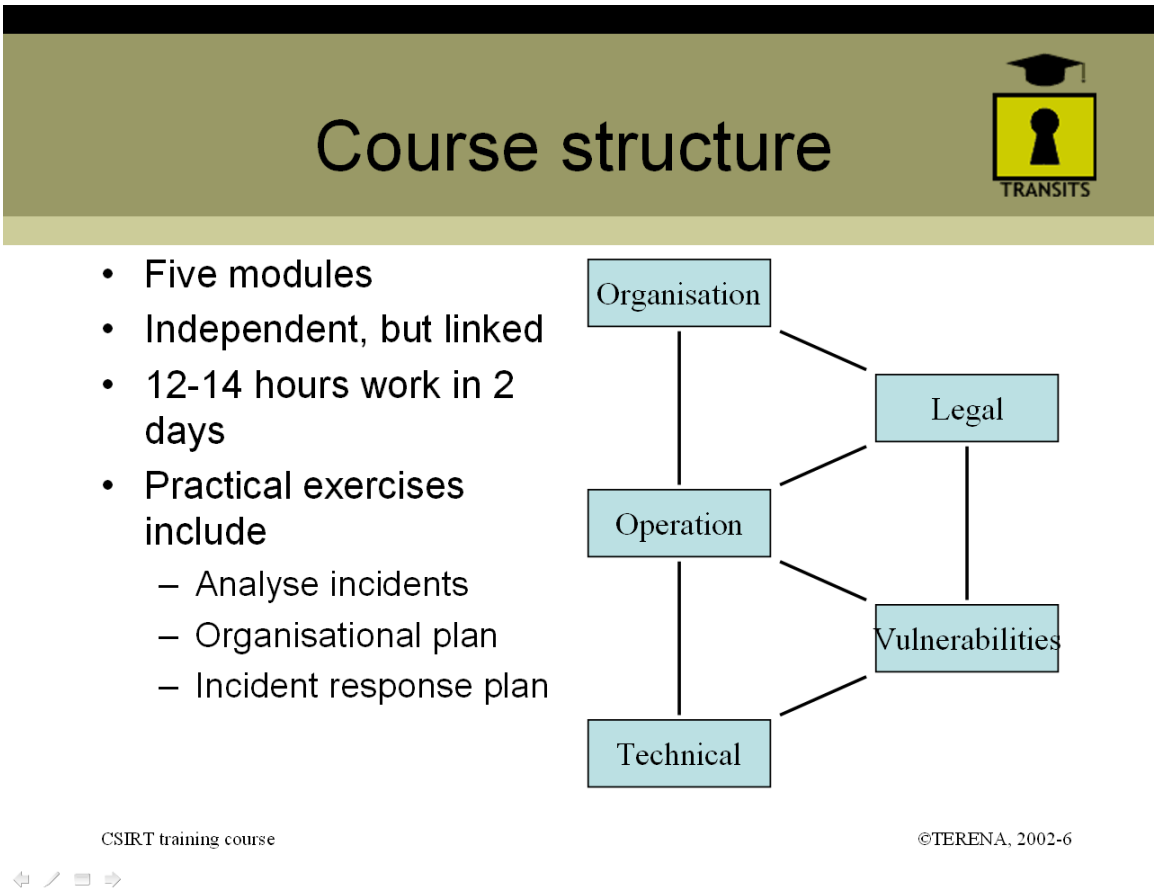
- -

11. krok: Cvičenie

V priebehu prvých týždňov práce použil fiktívny CSIRT niekoľko fiktívnych prípadov (prijatých ako príklady od iných tímov CSIRT), ktoré sa využili ako cvičenie. Okrem toho vydal niekoľko odborných rád k bezpečnosti vychádzajúcich z informácií o skutočnej zraniteľnosti rozosielaných predajcami hardvéru a softvéru, ktoré doladil a prispôsobil potrebám zložky.

A.4 Vzorový materiál z kurzov CSIRT

TRANSITS (s láskavým súhlasom spoločnosti Terena, http://www.terena.nl)



Prehľad: Štruktúra kurzu

Štruktúra kurzov

- Päť modulov
- Nezávislé, ale prepojené
- 12- 14-hodinová práca za 2 dny
- Praktické cvičenia zahŕňajú
  - Analyzovanie bezpečnostných incidentov
  - Organizačný plán
  - Plán reakcie na bezpečnostné incidenty

Organizácia

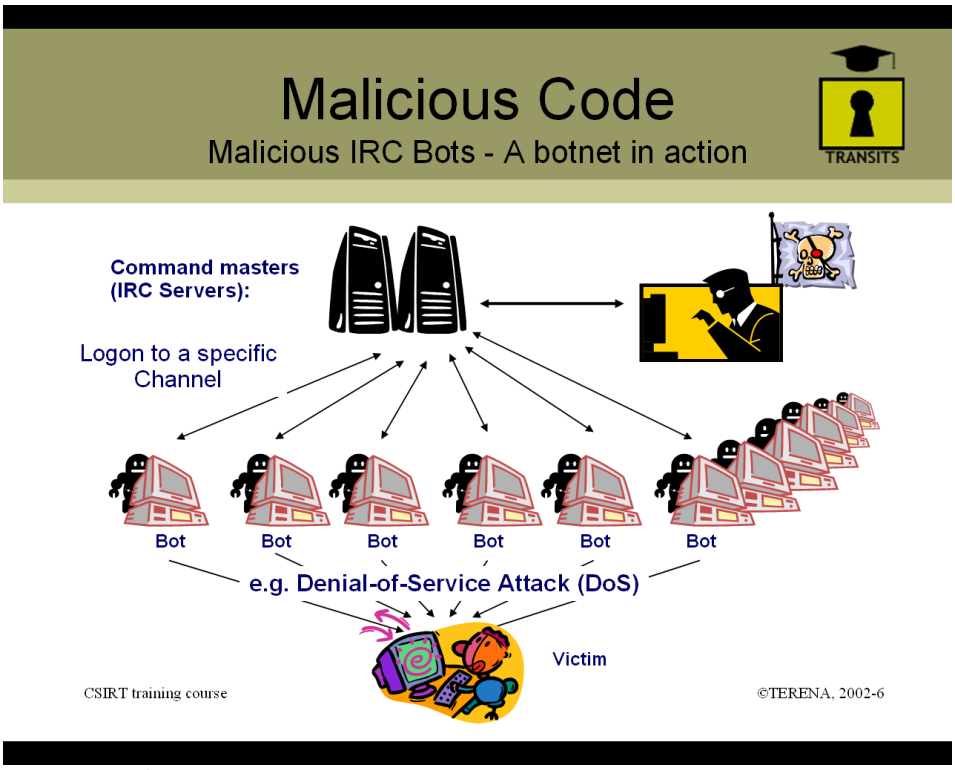
Právna

Činnosť

Zraniteľnosť

Technické

Výcvikový kurz CSIRT © TERENA, 2002-6



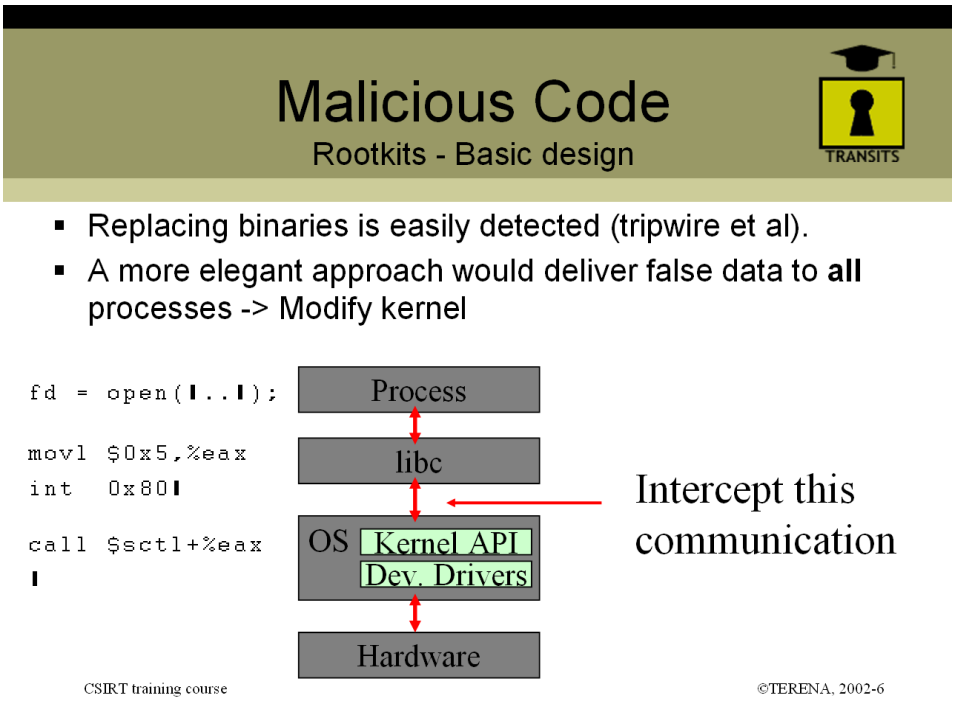
Z technického modulu: Opis siete internetových (vyhľadávacích) robotov

Škodlivý kód

Škodlivé roboty globálnej služby pre konverzáciu po sieti (chat) na Internete – IRC *(Internet Relay Chat*) sieť internetových (vyhľadávacích) robotov v činnosti

Matrica príkazov
(Servery IRC):
Prihlásenie na špecifický kanál
Internetový (vyhľadávací) robot – Internetový (vyhľadávací) robot – Internetový (vyhľadávací) robot – Internetový (vyhľadávací) robot – Internetový (vyhľadávací) robot – Internetový (vyhľadávací) robot
napr. útok typu odoprenia služby (DoS – Denial of Service)
Obeť

Výcvikový kurz CSIRT © TERENA, 2002-6



Z technického modulu: Základný návrh rootkitu

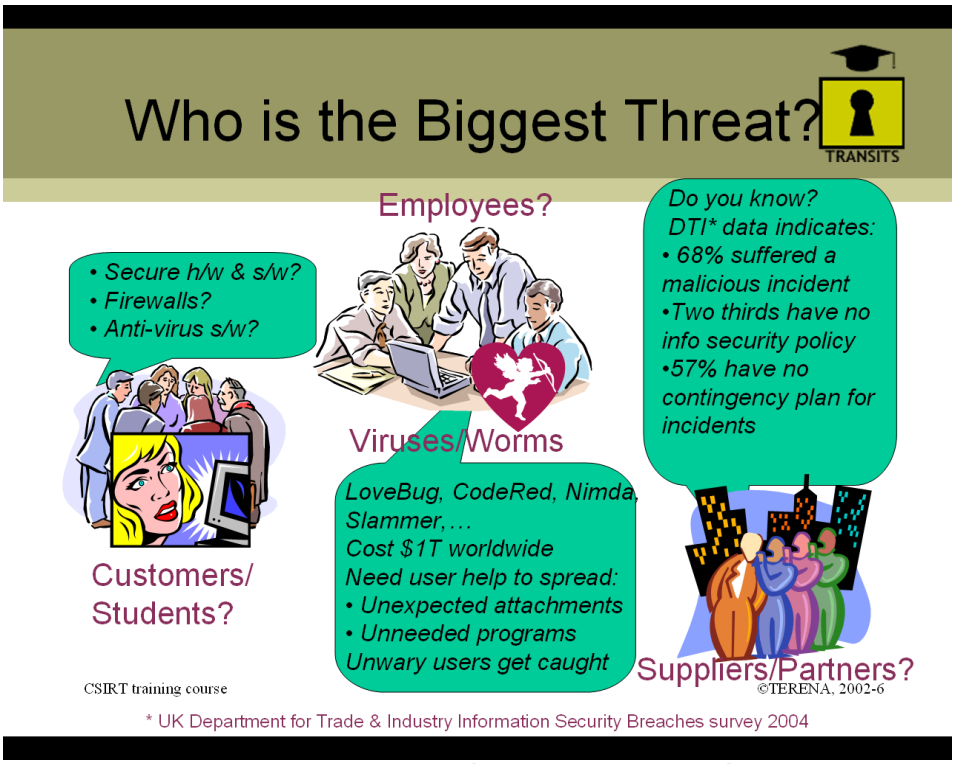
Škodlivý kód

Rootkyty (programy, ktoré skryjú po útočníkovi všetky stopy. úprava hackerských nástrojov, ktoré umožňujú získať a udržať práva administrátora) – základná štruktúra

- Náhrada binárnych zápisov sa ľahko zistí (nástražný drôt a i.)
- Uhladenejším prístupom by sa dodali falošné údaje do **všetkých** procesov -> modifikácia jadra

Proces
knižnica
- Zadržanie tejto komunikácie
Operačný systém aplikačného programového rozhrania zabezpečovacieho jadra – Kernel API *(Kernel Application Programming Interface)*
Ovládače zariadenia
Hardvér

Výcvikový kurz CSIRT © TERENA, 2002-6



Z organizačného modulu: Zasvätená alebo nezasvätená osoba – kde je väčšia hrozba?

Kto je najväčšou hrozbou?

Zamestnanci?

- *Bezpečný hardvér a softvér?*
- *Firewally?*
- *Antivírový softvér?*

Poznáte?
Údaje o zhoršení prenosu dát skreslením – DTI (Distortion Transmission Impairment) ukazujú, že:*

- *68 % je poškodených škodlivým bezpečnostným incidentom*
- *Dve tretiny nemajú žiadnu politiku bezpečnosti informácií*
- *57 % nemá žiadny núdzový plán pre bezpečnostné incidenty*

Vírusy/červy
LoveBug, CodeRed, Nimda, Slammer...
Cena na celom svete 1 tis. $ $.
Potreba pomôcť užívateľom v prípade rozšírenia:

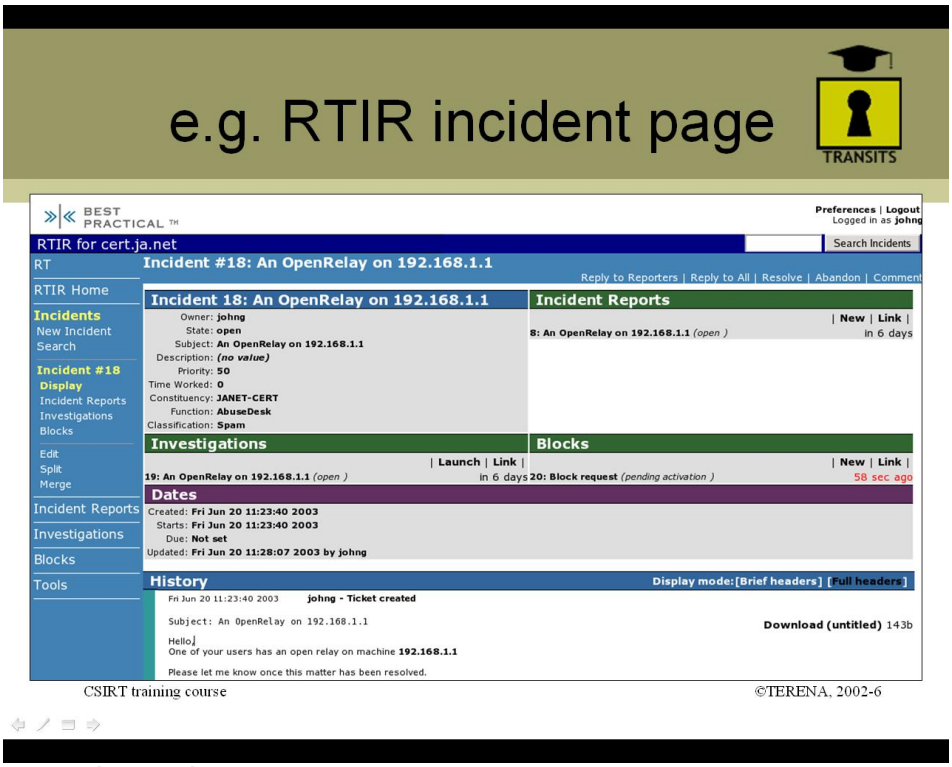
- *neočakávaných príloh*
- *zbytočných programov*

Neopatrní užívatelia sa chytili

Dodávatelia/partneri?

Výcvikový kurz CSIRT © TERENA, 2002-6

* Prieskum Ministerstva obchodu a priemyslu Spojeného kráľovstva týkajúci sa porušenia bezpečnosti informácií

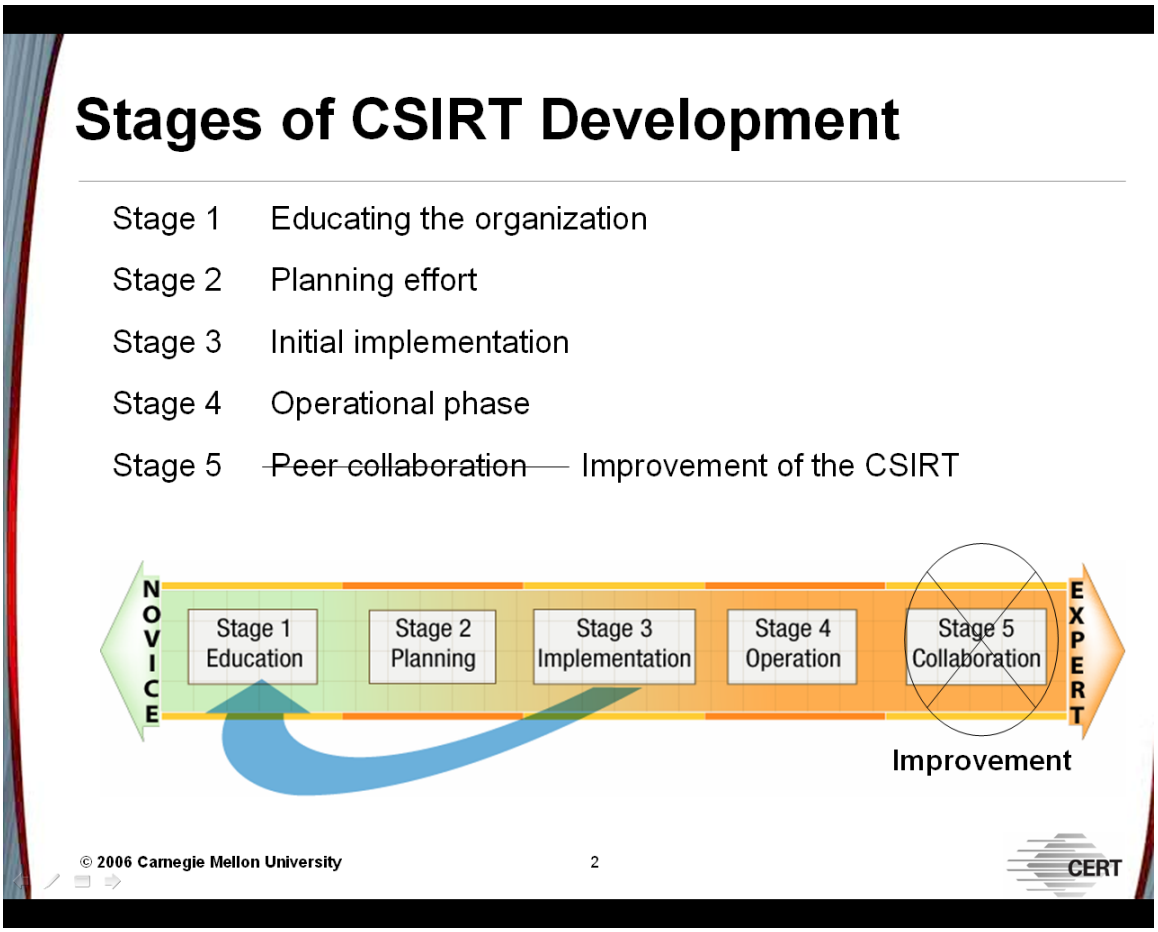


Z prevádzkového sledovania: Sledovač žiadostí o reakciu na bezpečnostné incidenty – RTIR *(Request Tracker for Incident Response)*

napr. strana bezpečnostných incidentov RTIRT

„Vytvorenie tímov CSIRT“ (s láskavým súhlasom CERT/CC, http://www.cert.org)

ENISA s vďačnosťou oceňuje Tím pre rozvoj CSIRT pri Programe CERT za to, že nám povolil využiť obsah jeho výcvikových kurzov!

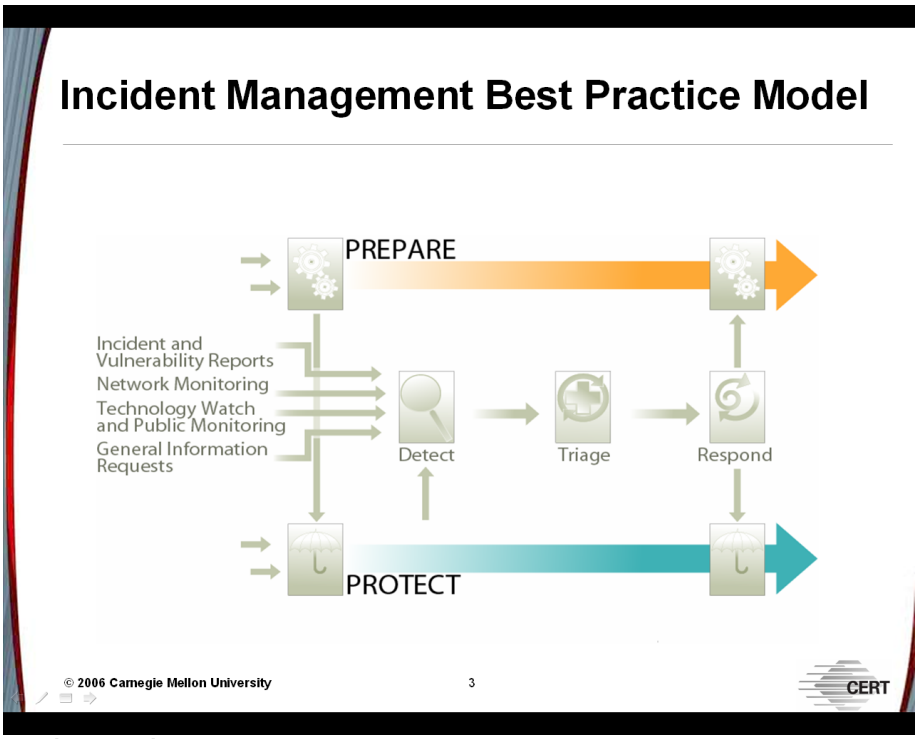


Z výcvikového kurzu CERT/CC: Fázy vývoja CSIRT

Fázy vývoja CSIRT

1. fáza Vzdelávanie organizácie
2. fáza Činnosť plánovania
3. fáza Počiatočná realizácia
4. fáza Pracovná fáza
5. fáza ~~Spolupráca kolegov~~ Zlepšenie CSIRT

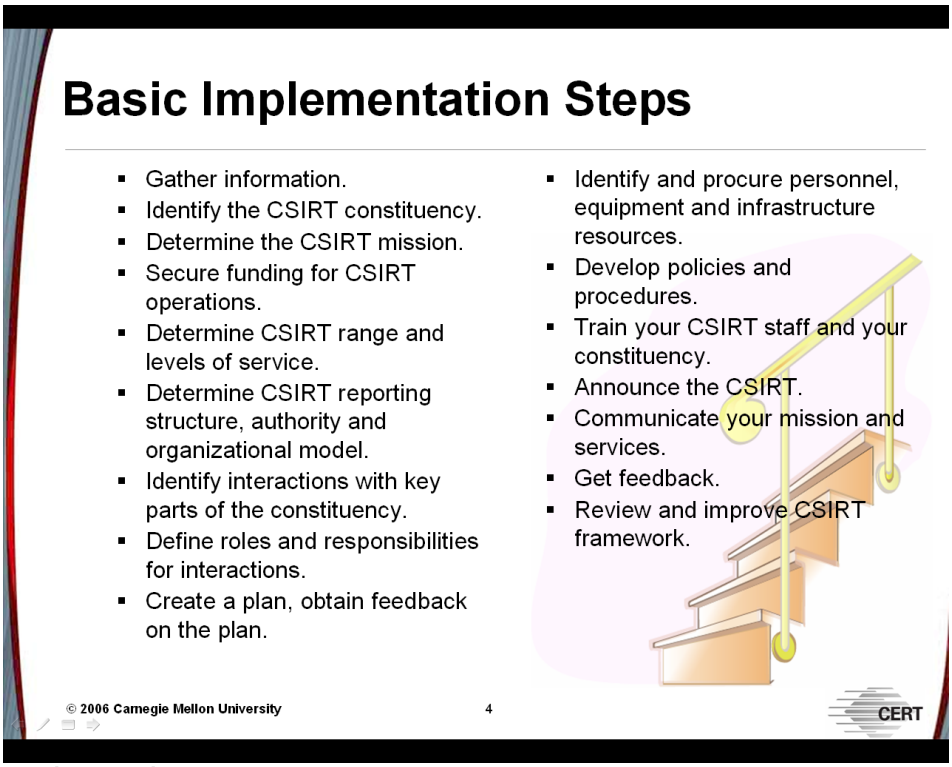
NOVÁČIK
1. fáza - vzdelávanie 2. fáza – plánovanie, 3. fáza – realizácia, 4. fáza – činnosť, ~~5. fáza - spolupráca~~
ODBORNÍK
Zlepšenie



Z výcvikového kurzu CERT/CC: Najlepšia prax v riadení bezpečnostných incidentov

Najlepšia prax v riadení bezpečnostných incidentov

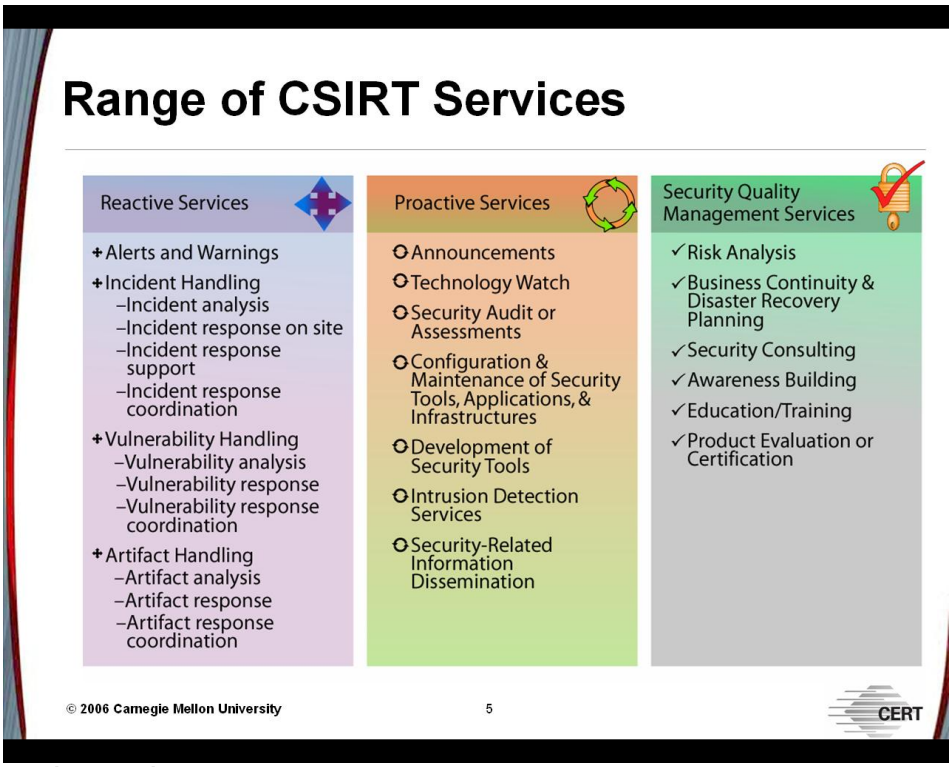
PRÍPRAVA
Správy o bezpečnostných incidentoch a zraniteľnosti
Monitorovanie siete
Sledovanie technológie a verejné monitorovanie
Žiadosti o všeobecné informácie
Detekcia Triedenie, Reakcia
OCHRANA



Z výcvikového kurzu CERT/CC: Kroky, ktoré sa majú dodržať, keď sa vytvára CSIRT

Základné kroky realizácie

- Zber informácií
- Identifikácia zložky CSIRT.
- Určenie poslania CSIRT.
- Zaistenie financovania pre činnosti CSIRT.
- Určenie rozsahu CSIRT a úrovní služieb.
- Určenie štruktúry hlásení CSIRT, kompetencie a organizačného modelu.
- Identifikácia vzájomnej súčinnosti s kľúčovými časťami zložky.
- Vymedzenie úloh a zodpovedností pre vzájomnú súčinnosť.
- Vytvorenie plánu, získanie spätnej väzby k plánu.
- Identifikácia a zaistenie pracovníkov, vybavenia a zdrojov infraštruktúry.
- Vypracovanie politík a postupov.
- Školenie vašich pracovníkov CSIRT a vašej zložky.
- Ohlásenie CSIRT
- Oznámenie vášho poslania a služieb.
- Získanie spätnej väzby.
- Preskúmanie a zlepšenie rámca CSIRT.



Z výcvikového kurzu CERT/CC: Služby, ktoré môže poskytovať CSIRT

Rozsah služieb CSIRT

Reaktívne služby

+ Výstrahy a varovania

+ Riešenie bezpečnostných incidentov
- Analýza bezpečnostných incidentov
- Reakcia na bezpečnostné incidenty na mieste
- Podpora reakcie na bezpečnostné incidenty
- Koordinácia reakcií na bezpečnostné incidenty

+ Riešenie zraniteľnosti
- Analýza zraniteľnosti
- Reakcia na zraniteľnosť
- Koordinácia reakcií na zraniteľnosť

+ Zaobchádzanie s artefaktmi
- Analýza artefaktov
- Reakcia na artefakty
- Koordinácia reakcií na artefakty

Aktívne služby

O Oznámenia

O Sledovanie techniky

O Audit alebo hodnotenie bezpečnosti

O Konfigurácia a udržiavanie bezpečnostných nástrojov, aplikácií a infraštruktúry

O Vývoj bezpečnostných nástrojov

O Služby detekcie útokov

Šírenie informácií týkajúcich sa bezpečnosti

Služby manažmentu kvality bezpečnosti

✓ Analýza rizika

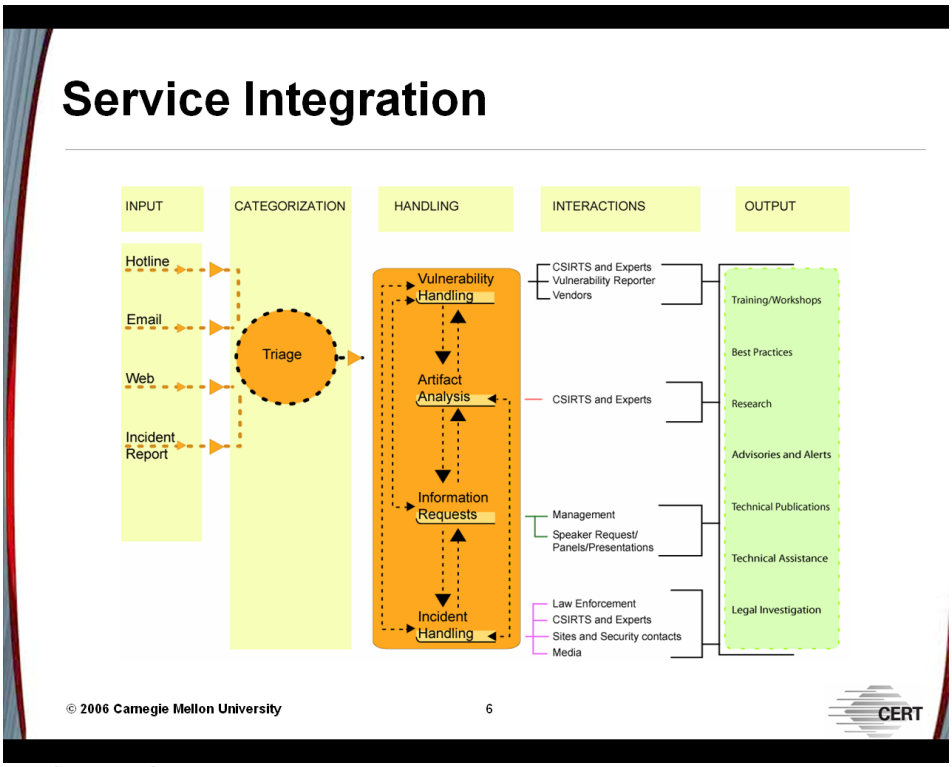
✓ Kontinuita podnikania a plánovanie obnovy po havárii

✓ Poradenstvo v bezpečnosti

✓ Vytváranie povedomia

✓ Vzdelávanie/výcvik

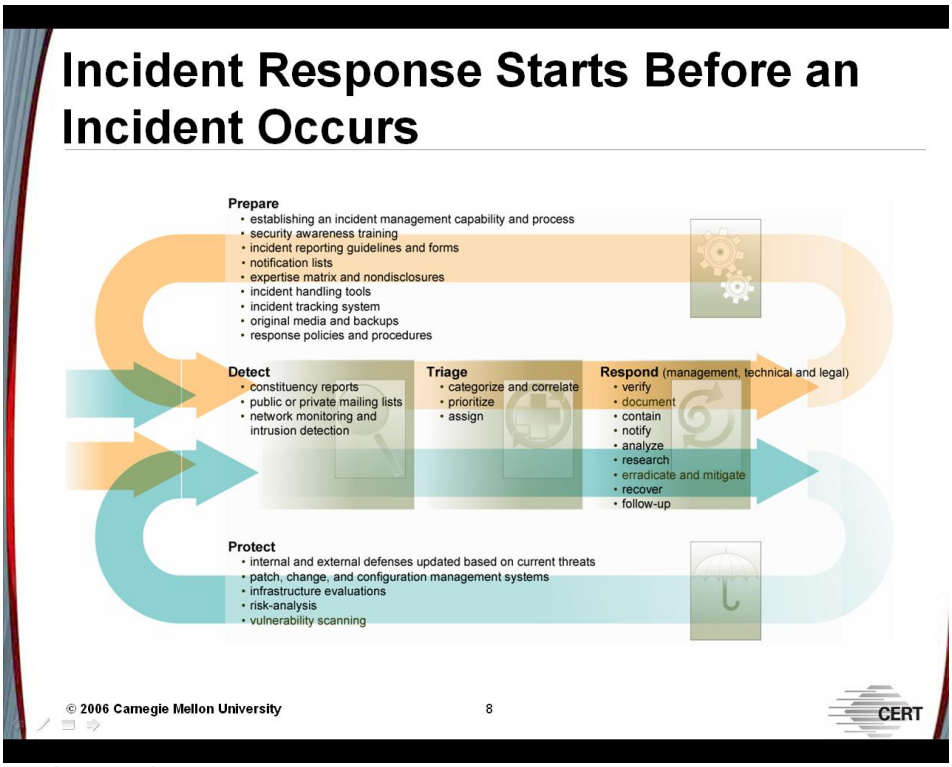
✓ Hodnotenie alebo certifikácia produktov



Z výcvikového kurzu CERT/CC: Pracovní postup riadenia bezpečnostných incidentov

Integrácia služieb

VSTUP	KATEGORIZÁCIA	RIEŠENIE	VZÁJOMNÁ SÚČINNOSŤ	VÝSTUP
Horúca linka		Riešenie zraniteľnosti	Tímy CSIRT a experti Osoby, ktoré hlásia zraniteľnosť Predajcovia	Výcvik/semináre
Elektronická pošta Internet Hlásenie bezpečnostných incidentov	Triedenie	Analýza artefaktov	Tímy CSIRT a experti	Najlepšie praktiky Prieskum Odborné rady a výstrahy
		Žiadosti o informácie	Manažment	Odborné publikácie
			Žiadosť zástupcov /partneri / prezentácia	Technická pomoc
		Riešenie bezpečnostných incidentov	Nízka vynútiteľnosť Tímy CSIRT a experti Miesta a bezpečnostné kontakty Média	Právne šetrenie



Z výcvikového kurzu CERT/CC: Reakcia na bezpečnostné incidenty

Reakcia na bezpečnostný incident začína pred jeho výskytom

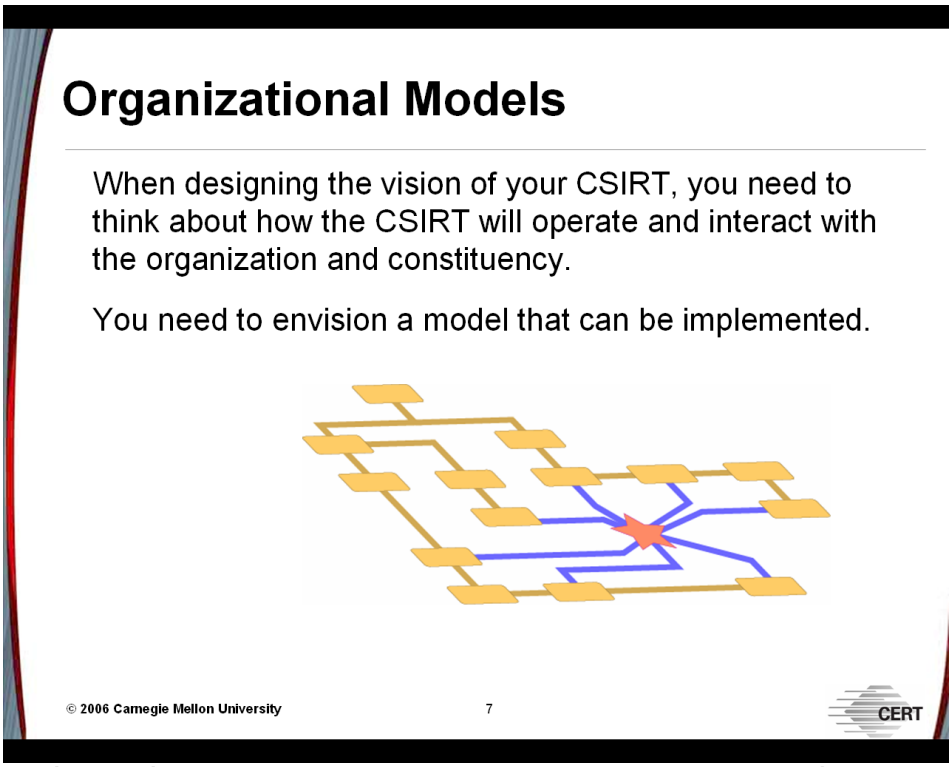
Príprava
- vytvorení spôsobilosti a procesu riadenia bezpečnostných incidentov
- výcvik v povedomí o bezpečnosti
- pokyny k hláseniu bezpečnostných incidentov a jeho formy
- zoznamy oznámení
- matica odbornej spôsobilosti a nesprístupnenie
- nástroje pre riešenie bezpečnostných incidentov
- systém sledovania bezpečnostných incidentov
- pôvodné média a zálohovanie
- politiky a postupy reakcie

Detekcia
- správy zložiek
- verejné a súkromné adresáre
- monitorovanie siete a detekcia útokov

Triedenie
- kategorizácia a uvedenie do vzájomného vzťahu
- ustanovenie priorít
- pridelenie

Reakcia (odborné a právne riadenie)
- overenie
- dokumentovanie
- zahrnutie
- oznámenie
- analyzovanie
- prieskum
- odstránenie a zmiernenie
- obnova
- sledovanie

Ochrana
- interná a externá aktualizovaná ochrana vychádzajúca z aktuálnych hrozieb
- opravný balíček, zmena a systémy riadenia konfigurácií
- hodnotenie infraštruktúry
- analýza rizika
- skenovanie zraniteľnosti

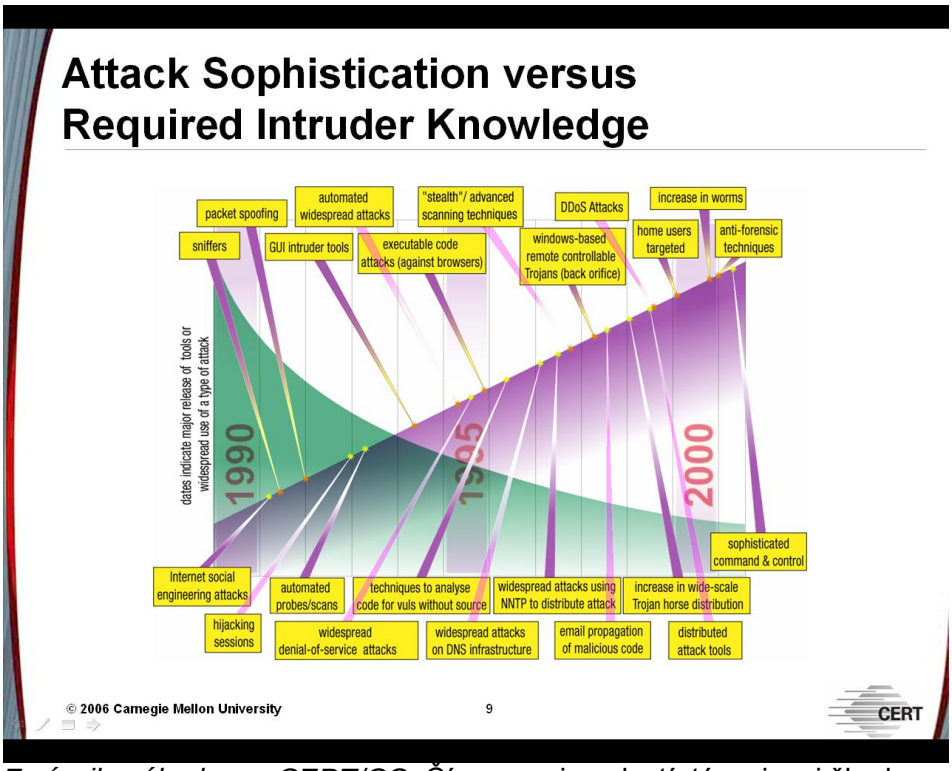


Z výcvikového kurzu CERT/CC: Ako bude CSIRT organizovaný?

Organizačné modely

Keď navrhujete víziu vášho CSIRT, musíte myslieť na to, ako bude CSIRT pracovať a uskutočňovať interakciu s organizáciou a zložkou.

Musíte si predstaviť model, ktorý je možné realizovať.



Z výcvikového kurzu CERT/CC: Čím menej znalostí, tým viacej škody

Dômyselnosť útoku verzus potrebné znalosti útočníka

Predstieranie paketu, automatizované rozsiahle útoky. krádež"/pokrokové metódy skenovania, útoky DDoS, zvýšenie počtu červov

Elektronické detekčné zariadenie, nástroje GUI útočníka, uskutočniteľné útoky na kód (proti prehliadačom), diaľkovo ovládateľné trojské kone založené na okne (obslužné programy), cieľoví domáci užívatelia, antiforenzné metódy.

Údaje ukazujú na veľké uvoľnenie nástrojov alebo široké využívanie druhu útoku, 1990, 1995, 2000

Premyslený príkaz a kontrola.

Útoky na internetové sociálne inžinierstvo, automatizované prieskumy/skenovanie, metódy analyzovania kódu na zraniteľnosť bez zdroja, rozsiahle útoky, ktoré na rozosielanie útoku využívajú štandardný protokol pre prevádzkovanie diskusných skupín – NNTP *(Network News Transfer Protocol)*, zvýšenie rozsahu rozosielania trojských koní.

Útok presmerovaním prevádzky (únos relácie), rozsiahle útoky typu odoprenia služby – DoS *(Denial of Service)*, rozsiahle útoky na infraštruktúru systému doménových mien – DNS *(Domain Name System)*, rozširovanie škodlivého kódu elektronickou poštou, nástroje rozosielaných útokov.