POSTUPNÉ VYTVÁŘENÍ CSIRT

Funkce WP2006/5.1 (CERT-D1/D2)

Obsah

1 Stručné shrnutí

Tento dokument popisuje proces ustavení týmu CSIRT *(Computer Security and Incident Response Team,* Týmu pro počítačovou bezpečnost a reakci na bezpečnostní incidenty*)* ze všech významných aspektů, jako je obchodní řízení, řízení procesů a technické hledisko. Tento dokument plní dvě funkce popsané v pracovním programu Evropské agentury pro bezpečnost sítí a informací – ENISA *(European Network and Information Security Agency)* na rok 2006, kapitola 5.1:

- Tento dokument: *Písemná zpráva o přístupu postupného vytváření tým CERT (Computer Emergency Response Team, týmu pro reakci na počítačové útoky), včetně příkladů.* (**CERT-D1**)
- Kapitola 12 a externí soubory: *Výtah ze scénáře v podrobné formě, který usnadňuje jeho použití v praxi.* (**CERT-D2**)

2 Právní upozornění

3 Poděkování

Agentura ENISA by chtěla poděkovat všem institucím i jednotlivcům, kteří se na tomto dokumentu podíleli. Zvláštní „Děkujeme“ patří následujícím přispěvatelům:

- Henku Bronkovi, který jako konzultant zpracoval první verzi tohoto dokumentu.
- CERT/CC, a zejména týmu pro rozvoj CSIRT, které přispěly nejužitečnějším materiálem a materiálem vzorového kurzu v příloze.
- GovCERT.NL za poskytnutí CERT *in-a-box (v jednom balíku)*.
- Týmu TRANSITS, který přispěl materiálem vzorového kurzu v příloze.

- Kolegům z oddělení pro bezpečnostní politiky v technickém odboru, kteří se podíleli na kapitole 6.6.
- a celé řadě těch, kdo tento dokument revidovali.

4 Úvod

Komunikační sítě a informační systémy se staly důležitým faktorem v hospodářském i společenském rozvoji. Zpracování údajů a vytváření sítí jsou teď stejně rozšířenými službami jako dodávky elektrické energie nebo vody.

Bezpečnost komunikačních sítí a informačních systémů a zejména jejich dostupnost má proto zvyšující se důležitost pro společnost. Vyplývá to z rizika problémů pro klíčové informační systémy kvůli složitosti, poruchám a chybám systému a útokům na fyzické infrastruktury, které dodávají služby důležité pro blaho občanů EU.

Dne 10. března 2004 byla vytvořena Evropská agentura pro bezpečnost sítí a informací (ENISA)[1]. Jejím cílem bylo zajistit vysokou a efektivní úroveň bezpečnosti sítí a informací ve společnosti a rozvíjet kulturu bezpečnosti sítí a informací ke prospěchu občanů, spotřebitelů, podniků a organizací veřejného sektoru v rámci Evropské unie a tedy přispívat k plynulému fungování vnitřního trhu.

Řada bezpečnostních organizací v Evropě jako CERT/CSIRT, týmy proti zneužívání a WARP už několik let spolupracovala pro bezpečnější Internet. ENISA hodlá podpořit tyto organizace v jejich úsilí poskytováním informací o opatřeních k zajištění příslušné úrovně jakosti služeb. ENISA dále hodlá zvýšit možnost poskytovat odborné rady členským státům EU a orgánům EU v otázkách zajištění příslušných bezpečnostních služeb pro specifické skupiny uživatelů informačních technologií – IT *(Information Technology)*. Na základě závěrů Pracovní skupiny ad-hoc CERT pro spolupráci a podporu vytvořené v roce 2005 se proto tato nová Pracovní skupina bude zabývat otázkami, které se týkají poskytování odpovídajících bezpečnostních služeb („služby CERT“) pro specifické uživatele (kategorie nebo skupiny uživatelů).

ENISA podporuje vytvoření nových CSIRT uveřejněním této své zprávy *„Postupný přístup k vytvoření CSIRT s doplňujícím kontrolním seznamem“*, který Vám pomůže vytvořit Váš vlastní tým CSIRT.

[1] Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací. Agentura Evropského společenství je orgán zřízený EU za účelem plnění velmi specifických technických, vědeckých nebo řídících úkolů v oblasti Společenství (tzv. první pilíř) EU.

Cílová skupina

Základní cílové skupiny této zprávy jsou státní a jiné instituce, které rozhodují o vytvoření CSIRT za účelem ochrany vlastní infrastruktury IT nebo infrastruktury IT zainteresovaných stran.

Jak používat tento dokument

Tento dokument poskytne informace o tom, co je CSIRT, jaké služby může zajistit a jaké nutné kroky je třeba učinit pro zahájení práce. Měl by dát čtenáři dobrý a pragmatický přehled o přístupu, struktuře a obsahu, jak vytvořit CSIRT.

Kapitola 4 *„Úvod“*
Úvod k této zprávě

Kapitola 5 *„Celková strategie pro plánování a vytvoření CSIRT“*
První část poskytuje popis, co je CSIRT. Uvede také informace o různých prostředích, v nichž mohou týmy CSIRT pracovat, a o tom, jaké služby mohou dodávat.

Kapitola 6 *„Zpracování obchodního plánu“*
Tato kapitola popisuje přístup obchodního řízení k procesu vytváření.

Kapitola 7 *„Podpora obchodního plánu“*
Tato kapitola se zabývá obchodním případem a otázkami financování.

Kapitola 8 *„Příklady pracovních a technických postupů“*
Tato kapitola popisuje postup získávání informací a jejich převedení do bezpečnostního bulletinu. Tato kapitola rovněž popisuje průběh prací v řešení bezpečnostních incidentů.

Kapitola 9 *„Výcvik CSIRT“*
Tato kapitola poskytuje shrnutí výcviku CSIRT, který je k dispozici. Pro ilustraci je v příloze uveden materiál vzorového kurzu.

Kapitola 10 *„Cvičení: poskytování poradenství“*
Tato kapitola obsahuje cvičení, jak uskutečňovat jednu ze základních (nebo klíčových) služeb CSIRT: vytvoření bezpečnostního bulletinu (nebo poskytnutí poradenství).

Kapitola 12 „Popis plánu projektu“
Tato kapitola poukazuje na doplňující plán projektu (kontrolní seznam) uvedený v této příručce. Tento plán je zaměřen na to, aby byl nástrojem, který se jednoduše použije k zavedení této příručky.

Obvyklé postupy používané v tomto dokumentu

V zájmu snadné orientace čtenáře každá kapitola začíná shrnutím dosavadních kroků v procesu vytváření CSIRT. Tato shrnutí jsou vysvětlena v rámečcích, jako je následující:

Učinili jsme první krok

Každá kapitola bude uzavřena praktickým příkladem kroků, kterými se zabývá. V tomto dokumentu „Fiktivní CSIRT“ bude malý nezávislý CSIRT pro středně velkou společnost nebo instituci. Shrnutí lze najít v příloze.

Fiktivní CSIRT

5 Celková strategie pro plánování a vytvoření CSIRT

Pro úspěšné zahájení procesu vytvoření CSIRT je důležité mít jasnou vizi o případných službách, které může tým poskytovat svým zákazníkům, ve „světě CSIRT“ lépe známé jako složky. Z toho důvodu je nutné pochopit, pro jaké potřeby složek se mají poskytovat příslušné služby v odpovídající jakosti a včas.

Co je CSIRT?

CSIRT znamená Tým pro reakci na bezpečnostní incidenty počítačů *(Computer Security Incident Response Team)*. Termín CSIRT se používá převážně v Evropě pro chráněný název CERT (Computer Emergency Response Team – Tým pro reakci na počítačové útoky*)*, který si v USA zaregistrovalo Koordinační středisko CERT – CERT/CC *(CERT Coordination Center)*.
Existují různé zkratky používané pro stejný druh týmů:

- CERT nebo CERT/CC (Computer Emergency Response Team / Coordination Center – Tým pro reakci na počítačové útoky /Koordinační středisko)
- CSIRT (Computer Security Incident Response Team – Tým pro reakci na bezpečnostní incidenty počítačů)
- IRT (Incident Response Team – Tým pro reakci na bezpečnostní incidenty)
- CIRT (Computer Incident Response Team – Tým pro reakci na bezpečnostní incidenty počítačů)
- SERT (Security Emergency Response Team – Tým pro reakci na ohrožení bezpečnosti)

K prvnímu velkému narušení celosvětové infrastruktury IT došlo koncem 80. let. Šlo tzv. červ Morris[2], který rychle se rozšířil a účinně infikoval velký počet systémů IT po celém světě.

Tento bezpečnostní incident zapůsobil jako studená sprcha: Lidé si najednou uvědomili naléhavou potřebu spolupráce a koordinace mezi správci systémů a manažery IT, aby se řešily takové případy jako tento. Protože čas byl rozhodující faktor, musel se vytvořit organizovanější a strukturovanější přístup k řešení bezpečnostních incidentů IT. A tak několik dnů po „Bezpečnostním incidentu Morris“ Projekční agentura pro výzkum zdokonalené obrany – DARPA *(Defence Advanced Research Projects Agency)* ustavila první tým CSIRT: Koordinační středisko CERT (CERT/CC[3]) se sídlem na Univerzitě Carnegie Mellon v Pittsburghu (Pensylvánie).

Tento model byl brzy přijat v Evropě a v roce 1992 holandský univerzitní poskytovatel surfovací sítě SURFnet zahájil první tým CSIRT v Evropě pod názvem SURFnet-CERT[4]. Pak následovalo mnoho týmů a v současné době *Seznam činností CERT v Evropě* agentury ENISA uvádí více než 100 známých týmů nacházejících se v Evropě[5].

[2] Více informací o červu Morris http://en.wikipedia.org/wiki/Morris_worm

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

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

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

Týmy CERT celá léta zdokonalovaly své schopnosti od pouhé reakce až po poskytovatele komplexních bezpečnostních služeb, včetně preventivních služeb jako výstrahy, odborné rady v bezpečnosti a výcvik a služby managementu bezpečnosti. Termín „CERT“ byl brzy považován za nedostačující. V důsledku toho byl koncem 90. let vytvořen nový termín „CSIRT“. V současné době se oba termíny (CERT a CSIRT) používají jako synonyma s tím, že CSIRT je přesnější.

5..1 Termín *složka*

Nadále se (v organizacích CSIRT) zavedený termín ‘složka’ bude používat ve vztahu k bázi zákazníků CSIRT. Jednotlivý zákazník se bude uvádět jako ‘složka’ a skupina jako ‘složky’.

5..2 Definice CSIRT

CSIRT je tým expertů pro bezpečnost IT, jejichž hlavním úkolem je reagovat na bezpečnostní incidenty počítačů. Poskytuje potřebné služby pro jejich řešení a pro podporu svých složek, aby se zotavili z poruchy.

S cílem snížit rizika a minimalizovat počet potřebných reakcí, většina týmů CSIRT zajišťuje pro své složky také preventivní a vzdělávací služby. Dává odborné rady týkající se zranitelnosti používaného softwaru a hardwaru a rovněž informují uživatele o zneužívání a virech, které využívají tyto závady. Tak mohou složky rychle opravit a aktualizovat své systémy. Úplný seznam případných služeb viz kapitola 5.2 *Možné služby*

5..3 Výhody existence CSIRT

Když má organizace nadšený bezpečnostní tým IT, pomáhá jí to snížit velké bezpečnostní incidenty, předcházet jim a chránit svůj hodnotný majetek.

Další případné výhody jsou:

- Centralizovaná koordinace otázek bezpečnosti IT v rámci organizace (kontaktní místo – PoC *(Point of Contact)*).
- Centralizované a specializované řešení bezpečnostních incidentů IT a reakce na ně.
- Odborné znalosti na podporu uživatelů a pro pomoc uživatelům, aby se rychle zotavili z bezpečnostních incidentů.
- Řešení právních otázek a uchování důkazů pro případ soudního sporu.
- Sledování rozvoje v oblasti bezpečnosti.
- Podnětná spolupráce v rámci složky týkající se bezpečnosti IT (vytváření povědomí).

Fiktivní CSIRT (0. krok)
Chápání, co je CSIRT: Vzorový CSIRT bude sloužit střední organizaci, která má 200 pracovníků. Organizace má vlastní oddělení IT a dvě další pobočky ve stejné zemi. IT hraje klíčovou roli pro společnost, protože se používá k interní komunikaci, datovou síť a elektronické obchodování 24 hodin denně, 7 dní v týdnu. Organizace má vlastní síť a disponuje redundantním připojením k Internetu prostřednictvím dvou provozovatelů služeb sítě Internet – ISP *(Internet Service Provider)*.

5..4 Popis různých druhů prostředí CSIRT

Učinili jsme první krok

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.

>> Další krok je odpověď na otázku: „Jakému sektoru se budou dodávat služby CSIRT?“

Když se začíná s týmem CSIRT (stejně jako s každou jinou činností), je velmi důležité rychle zpracovat jasné stanovisko, kdo jsou složky, a pro jaký druh prostředí se budou služby CSIRT rozvíjet. V této chvíli rozlišujeme následující ‘sektory’ uvedené v abecedním pořádku (pozn. překl.: abecední pořádek platí jenom pro anglický text):

- Akademický sektor CSIRT
- Komerční CSIRT
- Sektor CIP/CIIP CSIRT
- Státní sektor CSIRT
- Interní CSIRT
- Vojenský sektor CSIRT
- Národní CSIRT
- Malé a střední podniky (SME) Sektor CSIRT
- CSIRT prodejců

Akademický sektor CSIRT
Zaměření
Akademický sektor CSIRT poskytuje služby CSIRT školským a vzdělávacím institucím, jako jsou vysoké školy nebo výzkumná zařízení a jejich prostředí Internetu na školní půdě.

Složky
Typickými složkami tohoto typu CSIRT jsou pracovníci a studenti vysokých škol.

Komerční CSIRT
Zaměření
Komerční CSIRT poskytuje služby CSIRT svým složkám na komerční bázi. V případě ISP poskytuje CSIRT většinou služby koncovým uživatelům proti zneužívání (vytáčené spojení, ADSL) a služby CSIRT pro své profesionální zákazníky.

Složky
Komerční CSIRT obvykle dodávají své služby složkám, které za ně platí.

Sektor CIP/CIIP CSIRT
Zaměření
Týmy CSIRT v tomto sektoru se zaměřují hlavně na ochranu důležitých informací a / nebo ochranu důležitých informací a infrastruktury – CIP/CIIP *(Critical Information Protection / Critical Information and Infrastructure Protection)*. Tyto specializované týmy CSIRT většinou úzce spolupracují s vládním oddělením CIIP. Ten pokrývá všechny rozhodující sektory IT v zemi a chrání její občany.

Složky
Vláda; rozhodující podniky IT; občané

Státní sektor CSIRT
Zaměření
Státní CSIRT poskytuje služby státním orgánům a v některých zemích i občanům.

Složky
Státní orgány a orgány spojené s vládou; v některých zemích se služby vydávání výstrah poskytují také občanům (například v Belgii, Maďarsku, Nizozemí, Spojeném království a Německu).

Interní CSIRT
Zaměření
Interní CSIRT poskytuje služby pouze své hostitelské organizaci. Charakterizuje to spíše činnost než sektor. Například mnoho telekomunikačních organizací a bank používá vlastní interní týmy CSIRT. Obvykle neudržují webovou stránku pro veřejnost.

Složky
Interní pracovníci a oddělení IT hostitelské organizace

Vojenský sektor CSIRT
Zaměření
Tým CSIRT v tomto sektoru poskytuje služby vojenským organizacím odpovědným za infrastrukturu IT potřebnou pro účely obrany.

Složky
Pracovníci vojenských institucí nebo úzce spojených orgánů, např. ministerstvo obrany.

Národní CSIRT
Zaměření
CSIRT s národním zaměřením považovaný za bezpečnostní kontaktní místo pro danou zemi. V některých případech působí státní CISRT také jako národní PoC (jako UNIRAS ve Spojeném království).

Složky
Tento druh CSIRT obvykle nemá přímé složky, protože národní CSIRT hraje pouze roli zprostředkovatele pro celou zemi.

Malé a střední podniky (SME) Sektor CSIRT
Zaměření

Samoorganizující se tým, který poskytuje své služby ve vlastním oboru podnikání nebo podobné skupině uživatelů.

Složky
Složkami těchto CSIRT mohou být SME a jejich pracovníci nebo zvláštní zájmové skupiny jako „Sdružení měst a obcí“ v zemi.

CSIRT prodejců
Zaměření
CSIRT prodejců se zaměřuje na podporu produktů specifických pro prodejce. Jeho cílem je obvykle zpracovat a poskytnout řešení, aby se odstranila zranitelnost a snížily potenciální negativní dopady závad.

Složky
Vlastníci produktů

Jak to bylo popsáno v odst. o národním CSIRT, tým může sloužit více než jednomu sektoru. Má to dopad například na analýzu složky a jejich potřeb.

Fiktivní CSIRT (1. krok)
Počáteční fáze V počáteční fázi je nový CSIRT plánován jako interní CSIRT, který poskytuje své služby pro hostitelskou společnost, místní oddělení IT a pracovníky. Také podporuje a mezi různými pobočkami koordinuje řešení incidentů spojených s bezpečností IT.

Možné služby, které je CSIRT schopen poskytovat

Učinili jsme první dva kroky.

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým dodávat své služby?“

>> Další krok je odpověď na otázku, *jaké služby se mají poskytovat složkám.*

Existuje mnoho služeb, které může CSIRT dodávat, ale dosud žádný CSIRT neposkytuje všechny. Výběr příslušného souboru služeb je tudíž zásadním rozhodnutím. Níže je uveden stručný přehled všech známých služeb CSIRT definovaných v „Příručce pro CSIRT“, kterou vydal CERT/CC[6].

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

Obr. 1 Seznam služeb CSIRT od CERT/CC[7]

Reaktivní služby	**Aktivní služby**	**Zacházení s artefakty**
• **Výstrahy a varování** • **Řešení bezpečnostních incidentů** • **Analýza bezpečnostních incidentů** • **Podpora reakce na bezpečnostní incidenty** • **Koordinace reakcí na bezpečnostní incidenty** • Reakce na bezpečnostní incidenty na místě • Řešení zranitelnosti • Analýza zranitelnosti • Reakce na zranitelnost • Koordinace reakcí na zranitelnost	• **Oznámení** • Sledování techniky • Audity nebo hodnocení bezpečnosti • Konfigurace a udržování bezpečnosti • Vývoj nástrojů bezpečnosti • Služby detekce narušení • Šíření informací týkajících se bezpečnosti	• *Analýza artefaktů* • *Reakce na artefakty* • *Koordinace reakcí na artefakty*
		Management jakosti bezpečnosti
		• *Analýza rizik* • *Kontinuita obchodu a obnovení provozu po havárii* • *Poradenství v bezpečnosti* • *Vytváření povědomí* • *Vzdělávání/výcvik* • *Hodnocení nebo certifikace produktů*

Klíčové služby (označené tučným písmem): Rozlišují se reaktivní a aktivní služby. Aktivní služby se zaměřují na prevenci bezpečnostních incidentů vytvářením povědomí a výcvikem, zatímco reaktivní služby se zaměřují na řešení bezpečnostních incidentů a snížení výsledných škod.

Řešení artefaktů zahrnuje analýzu jakéhokoli souboru nebo objektu zjištěného v systému, který by mohl být zapojen do škodlivých činností jako zbytky virusů, červy, skripty, trojské koně apod. Obsahuje také zacházení s výslednými informacemi a jejich distribuci prodejcům a jiným zainteresovaným stranám, aby se zamezilo dalšímu šíření škodlivých programů, a aby se snížila rizika.

Služby managementu bezpečnosti a jakosti jsou služby s dlouhodobějšími cíli a zahrnují poradenská a vzdělávací opatření.

Podrobné vysvětlení služeb CSIRT viz příloha.

Výběr správných služeb pro vaše složky je důležitý krok a dále bude uveden v kap. 6.1 *Definování finančního modelu.*

Většina týmů CSIRT začíná rozesíláním Výstrah a varování, dělá Oznámení a zajišťuje Řešení bezpečnostních incidentů pro své složky. Tyto klíčové služby obvykle vykazují u složky dobrý profil a hodnotu upozornění a většinou se považují za skutečnou „přidanou hodnotu“.

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

Dobrá praxe je začít s malou skupinou pilotních složek, poskytovat klíčové služby během pilotní doby a pak požádat o zpětnou vazbu.
Zainteresovaní pilotní uživatelé zajišťují konstruktivní zpětnou vazbu a pomáhají rozvíjet služby přizpůsobené potřebám.

Fiktivní CSIRT (2. krok)
Výběr správných služeb V počáteční fázi se rozhodne, že nový CSIRT se zaměří hlavně na poskytování některé z klíčových služeb pro zaměstnance. Učiní se rozhodnutí, že po pilotní fázi se zváží rozšíření portfolia služeb a doplní se některé Služby managementu bezpečnosti. Toto rozhodnutí se učiní na základě zpětné vazby od pilotních složek a v úzké spolupráci s oddělením zajišťování jakosti.

Analýza složky a madnátu

Učinili jsme první tři kroky:

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.
2. „Jakému sektoru se budou dodávat služby CSIRT?“
3. Jaký druh služeb může CSIRT poskytovat své složce.

>> Další krok je odpověď na otázku, *jaký druh přístupu by se měl zvolit, aby CSIRT začal pracovat?*

Další krok je hlubší náhled do složky s hlavním cílem vybrat správné komunikační kanály.

- Vymezení komunikačního přístupu ke složkám
- Stanovení prohlášení o poslání.
- Zpracování realistického plánu realizace/plánu projektu
- Stanovení služeb CSIRT
- Určení organizační struktury
- Stanovení politiky bezpečnosti informací
- Nábor správných pracovníků
- Využití kanceláře vašeho CSIRT
- Vyhledávání spolupráce mezi jinými CSIRT a případnými národními iniciativami.

Tyto kroky budou podrobněji popsány v následujících bodech a lze je použít jako vstup pro obchodní plán a plán projektu.

5..1 Přístup ke komunikaci se složkou

Jak bylo řečeno dřív, je velmi důležité znát potřeby složky a také svou vlastní strategii komunikace, včetně komunikačních kanálů, které jsou nejvhodnější k tomu, abyste se na ni obrátili s informacemi.

Teorie řízení pozná několik možných přístupů k tomuto problému analyzování cílové skupiny. V tomto dokumentu popisujeme dva z nich: analýzu SWOT a PEST.

Analýza SWOT
Analýza SWOT je nástroj strategického plánování používaný k hodnocení silných stránek (**S**trengths), slabých stránek (**W**eaknesses)**,** příležitostí (**O**pportunities) a hrozeb (**T**hreats), které se týkají projektu nebo obchodního podnikání, nebo které si v jakékoli jiné situaci vyžadují rozhodnutí. Tato metoda se připisuje Albertu Humpreymu, který vedl výzkumný projekt na Stanfordské univerzitě v 60. a 70. letech s využitím údajů 500 největších korporací USA zveřejněných v časopise Fortune.[8]

Silné stránky	**Slabé stránky**
Příležitosti	**Hrozby**

Obr. 2 Analýza SWOT

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

Analýza PEST

Analýza PEST je další důležitý nástroj, který se v širokém měřítku používá pro analýzu složky za účelem pochopení politických (**P**olitical), ekonomických (**E**conomic), společensko-kulturních (**S**ocio-cultural) a technologických (**T**echnological) okolnosti prostředí, v němž pracuje CSIRT. Pomůže stanovit, zda plánování je ještě v souladu s prostředím, a pravděpodobně přispěje k tomu, aby se zamezilo přijetí opatření na základě nesprávných předpokladů.

Politické	**Ekonomické**
• Ekologické/environmentální otázky • Legislativa platná pro domácí trh • Budoucí legislativa • Evropská/mezinárodní legislativa • Zákonné orgány a procesy • Státní politiky • Funkční období vlády a změna • Obchodní politiky • Financování, granty a iniciativy • Lobbyistické/nátlakové skupiny na domácím trhu • Mezinárodní nátlakové skupiny	• Vnitrostátní hospodářská situace • Vnitrostátní hospodářské trendy • Zahraniční ekonomiky a trendy • Problematika všeobecného zdaňování • Daně specifické pro produkt/služby • Problémy sezónnosti/povětrnostních podmínek • Tržní a hospodářské cykly • Faktory specifické pro odvětví • Směrování trhu a trendy distribuce • Hybné síly zákazníka/konečného uživatele • Úrokové sazby a směnné kursy
Společenské	**Technologické**
• Trendy životního stylu • Demografie • Postoje a názory zákazníků • Stanoviska médií • Změny zákonů ovlivňující sociální faktory • Obchodní značka, společnost, technická pověst • Vzorce nakupování zákazníků • Modely způsobu a role • Důležité události a vlivy • Dostupnost a trendy nakupování • Etnické/náboženské faktory • Reklama a propagace	• Rozvoj konkurenční technologie • Financování výzkumu • Pomocné/závislé technologie • Náhradní technologie/řešení • Vyspělost technologie • Výrobní vyspělost a kapacita • Informace a komunikace • Mechanizmy/technologie nakupování zákazníků • Technická legislativa • Inovační potenciál • Dostupnost technologií, udělování licencí, patenty • Otázky duševního vlastnictví

Obr. 3 Analýza modelu PEST

Podrobný popis analýzy PEST je uveden ve Wikipedii[9].

Oba nástroje poskytují komplexní a strukturovaný přehled o tom, jaké jsou potřeby složek. Výsledky doplní obchodní návrh a tím pomohou získat finanční prostředky pro ustavení CSIRT.

Komunikační kanály

Jako důležitou tématiku lze do analýzy zahrnout komunikaci a metody šíření informací („Jak komunikovat se složkou?“)

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

Podle možnosti by se měly zvážit pravidelné osobní návštěvy složek. Je prokázáno, že porady za osobní účasti usnadňují spolupráci. Jsou-li obě strany ochotny pracovat spolu, tyto porady povedou k otevřenějšímu vztahu.

CSIRT obvykle používá soubor komunikačních kanálů. Následující z nich se v praxi ukázaly jako účelné a zasluhují si posouzení:

- Veřejná webová stránka
- Uzavřená oblast členů na webové stránce
- Internetové formuláře pro hlášení bezpečnostních incidentů
- Adresáře
- E-mail na jméno
- Telefon / fax
- SMS
- „Zastaralé“ psané dopisy
- Měsíční nebo roční zprávy

Kromě používání elektronické pošty, internetových formulářů, telefonu nebo faxu s cílem usnadnit řešení bezpečnostních incidentů (přijímání zpráv o bezpečnostních incidentech od složky, koordinace s ostatními týmy nebo poskytování zpětné vazby a podpora oběti) většina CSIRT publikuje své odborné rady týkající se bezpečnosti na veřejně přístupné webové stránce a za pomoci adresářů.

! Je-li to možné, informace by se měly rozesílat bezpečným způsobem. Například elektronickou poštu lze podepsat pomocí programu pro šifrování elektronické pošty, freewarového šifrovacího programu „velmi dobré soukromí“ – PGP *(Pretty Good Privacy)* a citlivé údaje o bezpečnostním incidentu by se měly vždy zasílat šifrované.

Více informací viz kapitola *8.5 Dostupné nástroje CSIRT.* Viz také kapitola *2.3 RFC2350*[10]*.*

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

Fiktivní CSIRT (krok 3a)

Uskutečnění analýzy složky a vytvoření vhodných komunikačních kanálů

Brainstormingová porada s některými klíčovými osobami z vedení a ze složky generovala dostatečný vstup pro analýzu SWOT. Vede to k závěru, že existuje potřeba následujících rozhodujících služeb:

- Výstrahy a varování
- Řešení bezpečnostních incidentů (analýza, podpora reakce a koordinace reakce)
- Oznámení

Musí se zajistit, aby se informace rozesílaly dobře organizovaným způsobem s cílem dostat je k co největší části složky. Přijme se tedy rozhodnutí, že výstrahy, varování a oznámení ve formě poradenství k bezpečnosti se budou publikovat na vyhrazené webové stránce a rozesílat pomocí adresáře. Elektronická pošta, telefon a fax usnadňuje týmu CSIRT přijímat zprávy o bezpečnostních incidentech. Jako další krok se plánuje unifikovaný webový formulář.

Vzorová analýza SWOT viz další strana.

Silné stránky • Společnost má určité znalosti. • Plán se jim líbí a jsou ochotni spolupracovat. • Podpora a financování ze strany řídícího týmu.	**Slabé stránky** • Různá oddělení a pobočky mezi sebou příliš nekomunikují. • Neexistuje koordinace v bezpečnostních incidentech IT • Je mnoho ‘malých oddělení’.
Příležitosti • Velké množství nestrukturovaných informací o zranitelnosti. • Velká potřeba koordinace. • Snížení ztrát kvůli bezpečnostním incidentům. • Mnoho neurčitostí v otázce bezpečnosti IT. • Vzdělávání pracovníků v bezpečnosti IT.	**Hrozby** • Není dostatek finančních prostředků. • Není dostatek pracovníků. • Velká očekávání. • Kultura.

Obr. 4 Vzorová analýza SWOT

5..2 Mandát

Po analýze potřeb a přání složky týkajících se služeb CSIRT by dalším krokem mělo být zpracování mandátu.

Mandát popisuje hlavní funkci organizací ve společnosti z hlediska produktů a služeb, které poskytují pro své složky. Umožňuje to jasně sdělit, že CSIRT existuje a jakou má funkci.

Dobrou praxí je zpracovat výstižný mandát, ale ne příliš striktně stanovený, protože obvykle zůstane nezměněn po několik let.

Zde je několik příkladů madnátů od fungujících týmů CSIRT:

“<Název CSIRT> poskytuje informace a pomoc svým <složkám (definujte své složky)> v zavádění aktivních opatření za účelem snížení rizik bezpečnostních incidentů počítačů a také v reagování na tyto bezpečnostní incidenty, když se vyskytnou.”

„Nabízet pomoc <složkám> v prevenci bezpečnostních incidentů týkajících se IT a

v reakci na ně ."[11]

Mandát je velmi důležitý a potřebný krok k zahájení. Podrobnější popis toho, jaké informace by měl CSIRT zveřejnit, viz kapitola *2.1 RFC2350*[12]*.*

Fiktivní CSIRT (krok 3b)
Vedení fiktivního CSIRT vytvořilo tento mandát: *"Fiktivní CSIRT poskytuje informace a pomoc pracovníkům své hostitelské společnosti za účelem snížení rizik bezpečnostních incidentů počítačů a také za účelem reagování na tyto bezpečnostní incidenty, když se vyskytnou."* Tímto fiktivním CSIRT se vysvětluje, že se jedná o interní CSIRT, a že jeho hlavním úkolem je zabývat se otázkami souvisejícími s bezpečností IT.

[11] Prohlášení o poslání Govcert.nl: http://www.govcert.nl

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

6 Zpracování obchodního plánu

Učinili jsme následující kroky:

1. Pochopení, co je CSIRT a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým poskytovat své služby?
3. Jaký druh služeb může CSIRT poskytovat své složce.
4. Analýza prostředí a složek.
5. Stanovení mandátu.

>> Další krok je stanovení obchodního plánu.

Výstup z analýzy vám dává dobrý přehled o potřebách a (předpokládaných) slabých stránkách složky, takže se bere jako vstup pro další krok.

Definování finančního modelu

Po analýze bylo vybráno několik rozhodujících služeb, s nimiž se začne. Další krok je uvažování o finančním modelu: jaké parametry poskytování služeb jsou vhodné, jakož i rentabilní.

V dokonalém světě by se financování přizpůsobilo potřebám složky, ale v reálném světě se portfolio služeb, které lze poskytovat, musí přizpůsobit danému rozpočtu. Je tedy více realistické začít s plánováním otázek finančních prostředků.

6..1 Model nákladů

Existují dva hlavní faktory, které ovlivňují náklady, a to stanovení pracovní doby a určení počtu (kvality) pracovníků, kteří mají pracovat. Je třeba reagovat na bezpečnostní incidenty a poskytovat technickou podporu 24 hodin denně, 7 dní v týdnu, nebo se budou tyto služby zajišťovat pouze v pracovní době?

V závislosti na žádoucí dostupnosti a kancelářském vybavení (je například možné pracovat z domu?) může být prospěšné pracovat s rozvrhem služeb na zavolání nebo s časově plánovaným rozvrhem služeb.

Možný scénář je dodávat během pracovní doby jak aktivní, tak i reaktivní služby. Mimo pracovní dobu budou pracovníci poskytovat jenom omezené služby na zavolání, například pouze v případě velkých havárií a bezpečnostních incidentů.

Další možnost je vyhledávání mezinárodní spolupráce mezi jinými týmy CSIRT. Už existují příklady fungování spolupráce „Následování slunce“. Například spolupráce mezi evropskými a americkými týmy se ukázala jako prospěšná a skýtá dobrý způsob sdílení vzájemných pracovních kapacit. Kupříkladu CSIRT společnosti Sun Microsystems, která má mnohé pobočky v různých časových pásmech po celém světě (ale všechny jsou členy stejného týmu CSIRT), uskutečňuje služby 24 hodin denně, 7 dní v týdnu,

v nepřetržitých směnách týmů po celém světě. Náklady tím nejsou omezeny, protože týmy vždy pracují pouze v normální pracovní době a zajišťují služby také pro „spící část“ světa.

Dobrou praxí je zejména hluboká analýza, zda složka potřebuje služby 24 hodin denně, 7 dní v týdnu. Výstrahy a varování vydávaná v noční době nemají velký smysl, když je příjemce bude číst až příští ráno. Existuje jemná dělící čára mezi „potřebovat službu“ a „chtít službu“, ale zejména pracovní doba má velký význam pro počet pracovníků a potřebné vybavení, což má značný dopad na model nákladů.

6..2 Model výnosů

Když už známe náklady, jako další vhodný krok je posouzení možných modelů výnosů: jak lze financovat plánované služby. Zde je několik možných scénářů pro hodnocení:

Využití existujících zdrojů
Vždy je výhodné vyhodnotit zdroje, které už existují v jiných částech společnosti. Pracují tam už vhodní zaměstnanci (např. v existujícím oddělení IT) s potřebným vzděláním a odbornými zkušenostmi? Pravděpodobně lze dospět k dohodě s vedením o podpoře těchto pracovníků v CSIRT v počáteční fázi nebo se podpora pro CSIRT poskytuje na bázi ad hoc.

Členský poplatek
Jiná možnost je prodávat své služby složce za roční/čtvrtletní členský poplatek. Další služby by se mohly platit za každé jejich využití, například konzultační služby nebo audity bezpečnosti.

Jiný možný scénář: služby pro (interní) složku se poskytují bezplatně, ale za služby dodávané externím zákazníkům se musí platit. Jiný nápad je publikovat odborné rady a informační bulletiny na veřejné webové stránce a mít část „Pouze pro členy“ se zvláštními, podrobnějšími informacemi nebo informacemi přizpůsobenými danému účelu.

V praxi se ukázalo, že „Předplacení služeb CSIRT“ lze pouze v omezené míře využít k zajištění dostatečných finančních prostředků, a to zejména v počáteční fázi. Existují například fixní základní výdaje na tým a vybavení, které se musí uhradit předem. Financování těchto výdajů prodejem služeb CSIRT je obtížné a vyžaduje si velmi podrobnou finanční analýzu za účelem zjištění „mrtvého bodu“ (prahu rentability, kdy se náklady rovnají výnosům).

Dotace
Další eventualita, kterou stojí za to zvážit, by mohla být žádost o dotaci na projekt poskytnutou od vlády nebo od státního orgánu, protože v současné době většina zemí má fondy, které jsou k dispozici pro projekty bezpečnosti IT. Kontaktování ministerstva vnitra by mohlo být dobrým začátkem.

Samozřejmě je možná kombinace různých příslušných modelů.

Určení organizační struktury

Vhodná organizační struktura CSIRT značně závisí na existující struktuře hostitelské organizace a složky. Je rovněž závislá na dostupnosti kvalifikovaných odborníků, které je třeba najmout nastálo nebo na bázi ad hoc.

Typický CSIRT určuje následující role v rámci týmu:

Hlavní
- Generální ředitel

Pracovníci
- Office Manager
- Účetní
- Poradce pro komunikaci
- Právní konzultant

Provozně-technický tým
- Vedoucí technického týmu
- Technici technického týmu CSIRT, kteří dodávají služby CSIRT
- Výzkumníci

Externí konzultanti
- Najímaní podle potřeby

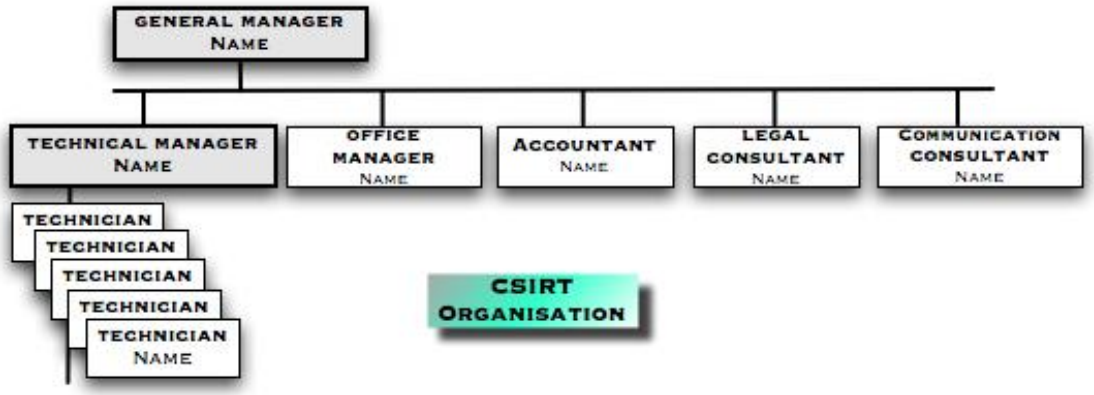
Je velmi účelné mít k dispozici právního experta, a to zejména v počáteční fázi CSIRT. Zvýši se tím sice náklady, ale nakonec se ušetří čas a zamezí se právním problémům.

V závislosti na druhu odborných schopností složky, a také když CSIRT má velkou mediální propagaci, ukázalo se jako velmi užitečné mít v týmu rovněž odborníka na komunikaci. Tito odborníci se mohou zaměřit na převádění obtížných technických otázek do srozumitelnějších zpráv pro složky nebo pro mediální partnery. Odborník na komunikaci bude rovněž poskytovat zpětnou vazbu ze složky pro technické odborníky, takže může působit jako „překladatel“ nebo „usnadňovatel“ mezi těmito dvěma skupinami.

Níže je několik příkladů organizačních modelů používaných provozními týmy CSIRT.

6..1 Nezávislý obchodní model

CSIRT se rozvíjí a jedná jako nezávislá organizace s vlastním vedením a zaměstnanci.

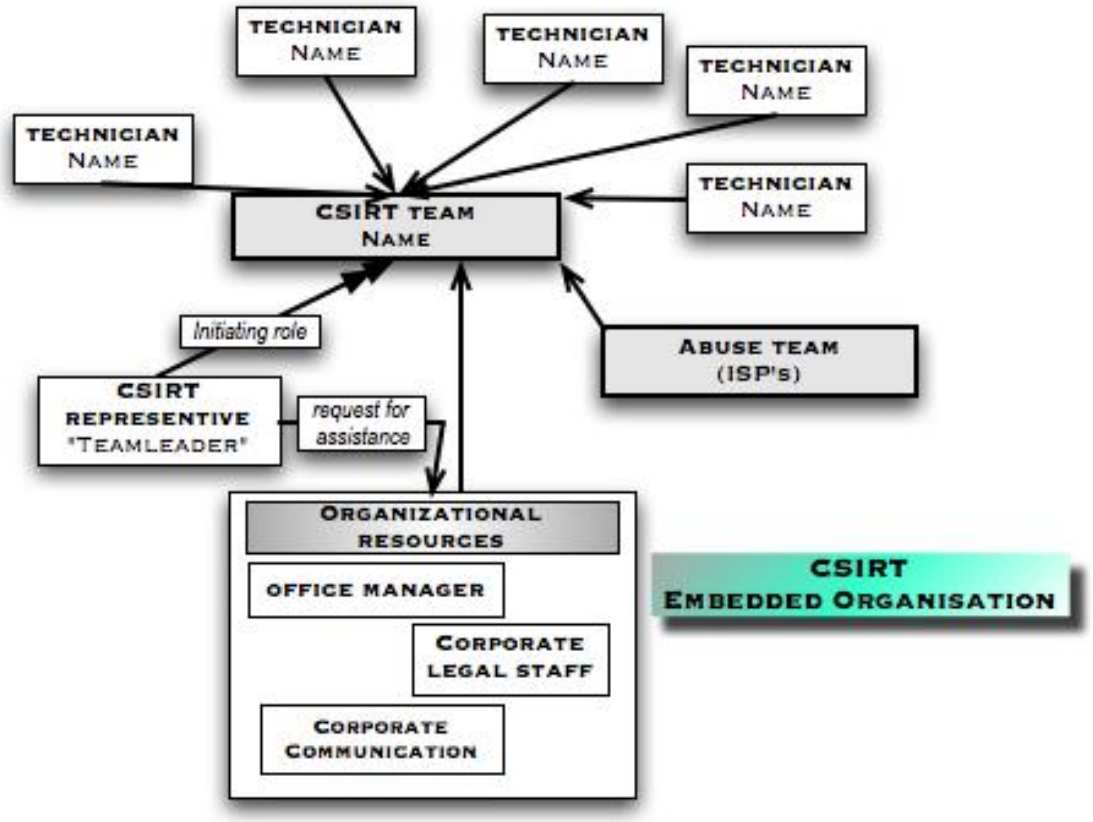


Obr. 5 Nezávislý obchodní model

6..2 Vložený model organizace

Tento model lze použít, když se má CSIRT vytvořit v rámci existující organizace, například s využitím existujícího oddělení IT. Na čele CSIRT je vedoucí týmu, který odpovídá za činnosti CSIRT. Vedoucí týmu shromáždí potřebné techniky, když řeší bezpečnostní incidenty, nebo když pracuje na činnostech CSIRT. Může požádat o pomoc týkající se podpory odborníků v rámci existující organizace.

Tento model lze rovněž upravit pro specifické situace, když se vyskytnou. V tomto případě se týmu přidělí pevný počet ekvivalentních pracovníků na plný pracovní úvazek – FTE *(Full Time Equivalent).* Například zneužívání desktopu u provozovatele služeb sítě Internet – ISP *(Internet Service Provider)* je určitě (ve většině případů) pracovní místo na plný pracovní úvazek pro více než jednoho pracovníka FTE.

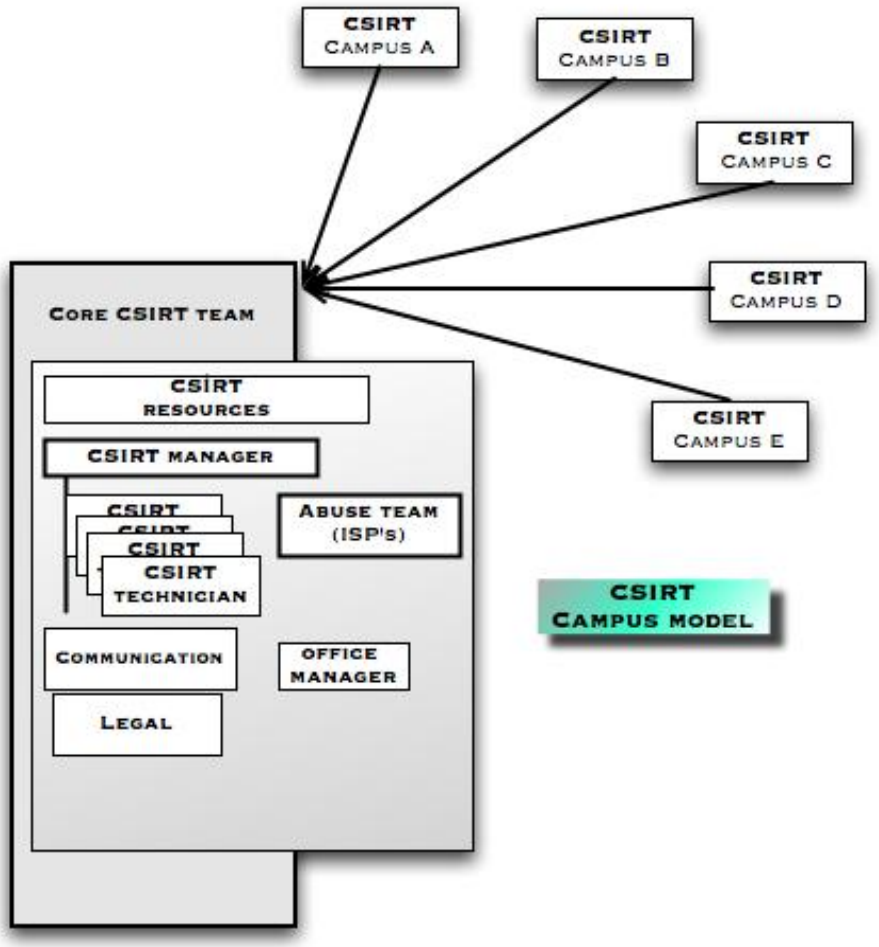


Obr. 6 Vložený model organizace

6..3 Vysokoškolský model

Vysokoškolský model, jak napovídá jeho název, přijímají většinou vysokoškolské a výzkumné CSIRT. Většina vysokoškolských a výzkumních organizací je složena z různých vysokých škol a univerzitních zařízení na různých místech rozšířených po celém regionu nebo dokonce po celé zemi (jako v případě Státních výzkumních sítí – NREN *(National Research Networks).* Obvykle jsou tyto organizace nezávislé jedna na druhé a často mají vlastní CSIRT. Tyto týmy CSIRT jsou zpravidla organizovány pod záštitou 'mateřského' nebo hlavního CSIRT. Hlavní CSIRT koordinuje styk s vnějším světem a je jeho jediným kontaktním místem. Hlavní CSIRT bude ve většině případů příslušnému vysokoškolskému CSIRT také poskytovat klíčové služby CSIRT a rovněž rozesílat informace o bezpečnostních incidentech.

Některé CSIRT rozesílají své klíčové služby CSIRT spolu s jinými vysokoškolskými CSIRT, což vede k nižším režijním nákladům pro hlavní CSIRT.



Obr. 7 Vysokoškolský model

6..4 Dobrovolný model

Tento organizační model popisuje skupinu pracovníků (odborníků), kteří se spojili, aby dobrovolně poskytovali jeden druhému (a ostatním) rady a podporu. Je to volně sestavena skupina lidí, která je velmi závislá na motivaci účastníků.

Tento model například přijala skupina WARP[13].

Nábor vhodných pracovníků

Po rozhodnutí o službách a úrovni podpory, která se má poskytnout, a po zvolení organizačního modelu, je další krok zjištění správného počtu kvalifikovaných pracovníků pro danou práci.

Je téměř nemožné stanovit pevný počet technických pracovníků potřebných z tohoto hlediska, ale jako dobrý přístup se osvědčily následující rozhodující počty:

- Pro dodávání dvou hlavních služeb, a to distribuce poradenských bulletinů a také řešení bezpečnostních incidentů: nejméně **4** pracovníci FTE.
- Pro plné služby CSIRT v pracovní době a systémy údržby: nejméně **6 až 8** pracovníků FTE.
- Pro plně obsazenou směnu 24 hodin denně, 7 dní v týdnu (2 směny mimo pracovní dobu) je minimální počet kolem **12** pracovníků FTE.

Tyto počty zahrnují také nadstavy pro případy nemoci, dovolených apod. Je rovněž nutné prověřit místní kolektivní smlouvy. Pracují-li zaměstnanci mimo pracovní dobu, může to vést k mimořádným výlohám ve formě zvláštních příplatků, které se musí platit.

Dále je uveden stručný přehled nejdůležitějších schopností technických odborníků pro CSIRT.

Body popisu práce hlavních technických pracovníků:

Osobní schopnosti

- Flexibilní, tvořivý a s dobrým smyslem pro tým
- Dobré analytické schopnosti
- Schopnost vysvětlit složité technické otázky jednoduchými slovy
- Smysl pro důvěrnost a pro práci na procedurálních otázkách
- Dobré organizační schopnosti
- Odolnost vůči stresu
- Dobré schopnosti komunikace a psaní
- Nezaujatost a ochota učit se

Technické schopnosti

- Široké znalosti technologie Internetu a protokolů
- Znalosti systémů Linux a Unix (v závislosti na vybavení složky)

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

- Znalosti systémů Windows (v závislosti na vybavení složky)
- Znalosti vybavení infrastruktury sítě (směrovač, přepínače, systém doménových jmen – DNS *(Domain Name System),* zástupce, pošta atd.)
- Znalosti internetových aplikací (jednoduchý protokol transferu pošty – SMTP *(Simple Mail Transfer Protocol),* hypertextové přenosové protokoly – HTTP *(HyperText Transfer Protocols),* protokol pro přenos souborů – FTP *(File Transfer Protocol),* telnet (protokol pro vzdálený přístup), zabezpečený protokol pro terminálovou emulaci – SSH *(Secure Shell)* atd.)
- Znalosti ohrožení bezpečnosti (distribuovaný útok typu odepření služby – DDoS *(Distributed Denial of Service),* phishing (on-line krádež identity), poškození povrchové úpravy *(defacing)*, odposlech síťové komunikace *(sniffing)* atd.
- Znalosti hodnocení rizik a praktických realizací

Další schopnosti

- Ochota pracovat 24 hodin denně, 7 dní v týdnu na zavolání (v závislosti na modelu služeb)
- Maximální cestovní vzdálenost (v případě havárie pohotovost v kanceláři; maximální cestovní doba)
- Úroveň vzdělání
- Zkušenosti v práci v oblasti bezpečnosti IT.

Fiktivní CSIRT (4. krok)

Stanovení obchodního plánu

Finanční model

Jelikož společnost uskutečňuje elektronický obchod 24 hodin denně, 7 dní v týdnu, a má také oddělení IT, které pracuje 24 hodin denně, 7 dní v týdnu, rozhodla se poskytovat během pracovní doby plné služby a mimo pracovní dobu služby na zavolání. Služby pro složku se budou poskytovat bezplatně, ale během pilotní a hodnotící fáze bude posouzena možnost dodávání služeb externím zákazníkům.

Model výnosů

V průběhu počáteční a pilotní fáze bude CSIRT financován prostřednictvím hostitelské společnosti. Během pilotní a hodnotící fáze bude projednáno další financování, včetně možnosti prodeje služeb externím zákazníkům.

Organizační model

Hostitelská organizace je malá společnost, takže byl vybrán vložený model.
Během pracovní doby bude personál složený ze třech pracovníků poskytovat klíčové služby (rozesílání odborných rad k bezpečnosti a řešení/koordinace bezpečnostních incidentů).

Oddělení IT společnosti už zaměstnává pracovníky s vhodnými odbornými schopnostmi. S tímto oddělením je udělána dohoda, takže nový CSIRT může v případě potřeby požádat o podporu na bázi ad hoc. Lze využít také jejich techniky na zavolání 2. linie.

Hlavní tým CSIRT bude mít čtyři členy na plný pracovní úvazek a pět dalších členů. Jeden z nich je k dispozici také na střídavé směně.

Pracovníci
Vedoucí týmu CSIRT má vzdělání v bezpečnosti a podporu 1. a 2. úrovně a vykonával práci v oblasti řízení přetrvávajících krizí. Ostatní tři členové týmu jsou odborníci na bezpečnost. Členové týmu CSIRT z oddělení IT na částečný pracovní úvazek jsou odborníci na infrastrukturu společnosti.

Používání a vybavení kanceláře

Vybavení a využívání kancelářských prostor a fyzická bezpečnost jsou velmi široké problémy, proto v tomto dokumentu nelze dát jejich vyčerpávající popis. Tato kapitola hodlá poskytnout stručný přehled uvedené problematiky.

Více informací o fyzické bezpečnosti lze najít na:
http://en.wikipedia.org/wiki/Physical_security
http://www.sans.org/reading_room/whitepapers/physcial/
http://www.infosyssec.net/infosyssec/physfac1.htm

„Zajištění odolnosti budovy“
Protože CSIRT obvykle zachází s velmi citlivými informacemi, dobrá praxe je nechat tým zkontrolovat fyzickou bezpečnost kanceláře. Bude to dost záviset na existujícím vybavení a infrastruktuře a na existující politice bezpečnosti informací hostitelské společnosti.

Například vlády pracují s klasifikačními schémat a jsou velmi přísné v tom, jak zacházet s důvěrnými informacemi. Ověřte s vaší vlastní společností nebo organizací místní pravidla a politiky.

Nový CSIRT je obvykle závislý na spolupráci své hostitelské organizace, aby se dozvěděl o místních pravidlech, politikách a jiných právních otázkách.

Vyčerpávající popis veškerého vybavení a bezpečnostních opatření, která budou nutná, vychází za rámec tohoto dokumentu. Níže je však uveden stručný seznam základního vybavení pro váš CSIRT:

Všeobecná pravidla pro budovu
- Používejte kontroly přístupu.
- Zpřístupněte kanceláře CSIRT pouze pro pracovníky CSIRT.
- Monitorujte kanceláře a vchody kamerami.
- Archivujte důvěrné informace v uzamykatelných skříňkách nebo v trezoru.
- Používejte zajištěné systémy IT.

Všeobecná pravidla pro vybavení IT
- Používejte vybavení, které jsou schopni obsluhovat samotní pracovníci.
- Zajistěte odolnost všech systémů.
- Záplatujte a aktualizujte všechny svoje systémy před jejich připojením na Internet.

- Používejte bezpečnostní software (bezpečnostní rozhraní *(firewalls)*, mnohočetné antivirové skenery, program proti spywaru atd.)

Udržování komunikačních kanálů

- Veřejná webová stránka
- Uzavřená oblast členů na webové stránce
- Internetové formuláře pro hlášení bezpečnostních incidentů
- Elektronická pošta (podpora PGP / GPG / S/MIME) (podpora „velmi dobrého soukromí“ – PGP *(Pretty Good Privacy)* / ochrany soukromí GNU – GPG *(GNU Privacy Guard)* / „bezpečného víceúčelového rozšíření pošty Internetu“ – S/MIME *(Secure Multimedia Internet Mail Extensions)*)
- Software adresářů
- Existence vyhrazeného telefonního čísla, které je k dispozici složce:
  - Telefon
  - Fax
  - SMS

Systém(y) sledování záznamů

- Databáze kontaktů s podrobnostmi o členech týmu, o jiných týmech atd.
- Nástroje řízení péče o zákazníky – CRM *(Customer Relationship Management)*
- Systém průkazů v řešení bezpečnostních incidentů

Používání „firemního stylu“ od samého začátku pro

- standardní elektronickou poštu a uspořádání poradenského bulletinu
- ‘Zastaralé’ písemné dopisy
- Měsíční nebo roční zprávy
- Formulář hlášení bezpečnostního incidentu

Jiné otázky

- Předvídání mimopásmové komunikace v případě útoků
- Předvídání redundance internetového spojení

Více informací o konkrétních nástrojích CSIRT viz kapitola *8.5 Dostupné nástroje CSIRT*.

Zpracování politiky bezpečnosti informací

V závislosti na druhu CSIRT budete mít politiku bezpečnosti informací upravenou podle potřeb zákazníka. Kromě popisu žádoucího stavu pracovních a administrativních procesů a postupů musí být tato politika v souladu s legislativou a normami, zejména co se týče odpovědnosti CSIRT. Tým CSIRT je obvykle vázán vnitrostátními zákony a předpisy, které se často plní v souladu s evropskou legislativou (zpravidla se směrnicemi) a jinými mezinárodními dohodami. Normy nemusí být přímo závazné, ale mohou být nařízeny nebo doporučeny na základě zákonů a předpisů.

Níže je stručný seznam možných zákonů a politik:

Vnitrostátní
- Různé zákony o informačních technologiích, telekomunikacích, médiích
- Zákony o ochraně údajů a soukromí
- Zákony a předpisy o uchovávání údajů
- Legislativa o finančnictví, účetnictví a podnikovém řízení
- Kodexy chování pro podnikové řízení a řízení IT

Evropské
- Směrnice o elektronických podpisech (1993/93/ES)
- Směrnice o ochraně údajů (1995/46/ES) a soukromí v elektronických komunikacích (č. 2002/58/ES)
- Směrnice o sítích a službách elektronické komunikace (2002/19/ES – 2002/22/ES)
- Směrnice o právu obchodních společností (např. 8. směrnice o právu obchodních společností).

Mezinárodní
- Basilejská smlouva II (zejména pokud jde o řízení provozního rizika)
- Úmluva Rady Evropy o internetové kriminalitě
- Úmluva Rady Evropy o lidských právech (čl. 8 o soukromí)
- Mezinárodní účetní normy – IAS *(International Accounting Standards;* do určité míry nařizují kontroly IT).

Normy
- Britská norma BS 7799 (Bezpečnost informací)
- Mezinárodní normy ISO 2700x (Systémy managementu bezpečnosti informací)
- Německá IT-Grundschutzbuch (kniha o hlavní ochraně IT), francouzský EBIOS a jiné národní varianty.

Uskutečněte konzultaci se svým právním poradcem, abyste zjistili, zda váš CSIRT postupuje v souladu s vnitrostátní a mezinárodní legislativou.

Nejdůležitější otázky, na které musíte ve svých politikách zacházení s informacemi odpovědět, jsou:

- Jak se příchozí informace „označují“ nebo „klasifikují“?

- Jak se s informacemi zachází, zejména s ohledem na exkluzivitu?
- Jaké jsou důvody zpřístupnění informací, zejména pokud se informace související s bezpečnostním incidentem předávají jiným týmům nebo místům.
- Existují nějaké právní důvody, které je třeba vzít v úvahu v zacházení s informacemi?
- Máte politiku šifrování za účelem ochrany exkluzivity a ucelenosti archivů a/nebo přenosu dat, zejména elektronické pošty?
- Zahrnuje tato politika případné podmínky takových právních hranic, jako je podmíněné sdílení soukromí nebo vynutitelnost dešifrování v případě právních žalob?

Fiktivní CSIRT (5. krok)

Vybavení a umístění kanceláře

Protože hostitelská společnost už má zavedenou účinnou fyzickou bezpečnost, nový CSIRT je v tomto ohledu dobře chráněn. Je zajištěn takzvaný „zpravodajský informační sál“, aby byla možná koordinace v případě nouzového stavu. Byl zakoupen trezor pro šifrované materiály a citlivé dokumenty. Byla zřízena zvláštní telefonní linka, včetně telefonní ústředny pro usnadnění horké linky během pracovní doby, a zajištěn mobilní telefon se stejným telefonním číslem pro službu „na zavolání“ mimo pracovní dobu.

Lze rovněž využít existující zařízení a podnikovou webovou stránku pro sdělování informací týkajících se CSIRT. Adresář je nainstalován, udržuje se a má vyhrazenou část pro komunikaci mezi členy týmu a s ostatními týmy. Všechny podrobnosti o kontaktních pracovnících se ukládají do databáze, kopie se bezpečně uchovává.

Předpisy

Jelikož CSIRT je začleněn do společnosti, která má politiky bezpečnosti informací, byly za pomoci právního poradce společnosti vytvořeny shodné politiky pro CSIRT.

Vyhledávání spolupráce mezi jinými CSIRT a případnými národními iniciativami.

Existence jiných iniciativ CSIRT a velká potřeba spolupráce mezi nimi už byla v tomto dokumentu několikrát zmíněna. Dobrá praxe je co nejdříve kontaktovat jiné týmy CSIRT, aby se získaly potřebné kontakty se skupinami pracovníků CISRT. Jiné týmy CSIRT jsou zpravidla velmi otevřené a poskytují pomoc nově vytvořeným týmům v zahájení práce.

Soupis činností CERT v Evropě[14] agentury ENISA je velmi dobrý výchozí bod pro vyhledávání jiných týmů CSIRT v zemi nebo aktivit pro spolupráci národních CSIRT.

Abyste získali podporu v hledání vhodného zdroje informací CSIRT, kontaktujte odborníky na týmy CSIRT agentury ENISA:

CERT-Relations@enisa.europa.eu

Níže je uveden přehled činností skupin CSIRT. Zevrubnější popis a další informace viz *Soupis*.

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

Evropská iniciativa CSIRT

TF-CSIRT[15]
Pracovní skupina TF-CSIRT podporuje spolupráci mezi týmy pro reakci na bezpečnostní incidenty počítačů (CSIRT) v Evropě. Hlavním cílem této pracovní skupiny je poskytovat fórum pro výměnu zkušeností a znalostí, vytvořit pilotní služby pro evropskou skupinu týmů CSIRT a napomáhat vytváření nových CSIRT.

Hlavní cíle pracovní skupiny jsou:
- Poskytovat fórum pro výměnu zkušeností a znalostí.
- Vytvořit pilotní služby pro evropskou skupinu týmů CSIRT.
- Podporovat společné normy a postupy pro reagování na bezpečnostní incidenty.
- Napomáhat ustavení nových CSIRT a výcviku pracovníků CSIRT.
- Činnost pracovní skupiny CSIRT – TF-CSIRT *(Task Force CSIRT)* se zaměřuje na Evropu a sousední země v souladu s pravomocemi schválenými dne 15. září 2004 Technickým výborem Trans-evropského sdružení pro výzkum a vytváření vzdělávacích sítí – TERENA *(Trans-European Research and Education Networking Association.)*

Celosvětová iniciativa CSIRT

Fórum týmů pro reakci na bezpečnostní incidenty a pro bezpečnost – FIRST[15] ***(Forum of Incident Response and Security Teams)***[16]

FIRST je přední organizace a uznávaný celosvětový vůdce v reakci na bezpečnostní incidenty. Členství ve FIRST umožňuje týmům pro reakci na bezpečnostní incidenty efektivněji reagovat na bezpečnostní incidenty – reaktivně a také aktivně.

FIRST dává dohromady různé týmy pro reakci na bezpečnostní incidenty počítačů ze státních, komerčních a vzdělávacích organizací. FIRST usiluje o podporu spolupráce a koordinace v prevenci bezpečnostních incidentů, o stimulování rychlé reakce na bezpečnostní incidenty a o pomoc ve sdílení informací mezi svými členy a společností jako celkem.

Kromě sítě důvěry, kterou FIRST vytváří v celosvětovém společenství pro reakci na bezpečnostní incidenty, poskytuje také služby s přidanou hodnotou.

Fiktivní CSIRT (6. krok)
Vyhledávání spolupráce S využitím Soupisu agentury ENISA bylo možné některé týmy CSIRT ve stejné zemi rychle vyhledat a kontaktovat. S jedním z nich byla pro nově najatého vedoucího týmu zorganizována návštěva na místě. Dozvěděl se o činnostech národního CSIRT a zúčastnil se porady. Tato porada byla více než užitečná k tomu, aby se shromáždily příklady pracovních metod, a aby se získala podpora několika jiných týmů.

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

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

7 Podpora obchodního plánu

Dosud jsme učinili následující kroky:

1. Pochopení, co je CSIRT a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým poskytovat své služby?“
3. Jaký druh služeb může CSIRT poskytovat své složce.
4. Analýza prostředí a složek.
5. Stanovení mandátu.
6. Zpracování obchodního plánu
    a. Definování finančního modelu
    b. Určení organizační struktury
    c. Zahájení náboru pracovníků
    d. Používání a vybavení kanceláře
    e. Zpracování politiky bezpečnosti informací
    f. Vyhledávání partnerů pro spolupráci

>> Další krok je zahrnutí výše uvedeného do plánu projektu a zahájení práce!

Dobrým začátkem pro definování vašeho projektu je navrhnout obchodní případ. Tento obchodní případ se použije jako základ pro plán projektu a uplatní se také v podpoře vedení a v získání finančních prostředků nebo jiných zdrojů.

Ukázalo se jako účelné, když se neustále podávají zprávy vedení, aby byla udržována dobrá informovanost o problémech bezpečnosti IT, a aby se tím trvale podporoval vlastní CSIRT.

Zahájení obchodního případu začíná analýzou problémů a příležitostí s využitím modelu analýzy popsaného v kapitole *5.3 Analýza složky* a vyhledáváním úzkého kontaktu na potenciální složku.

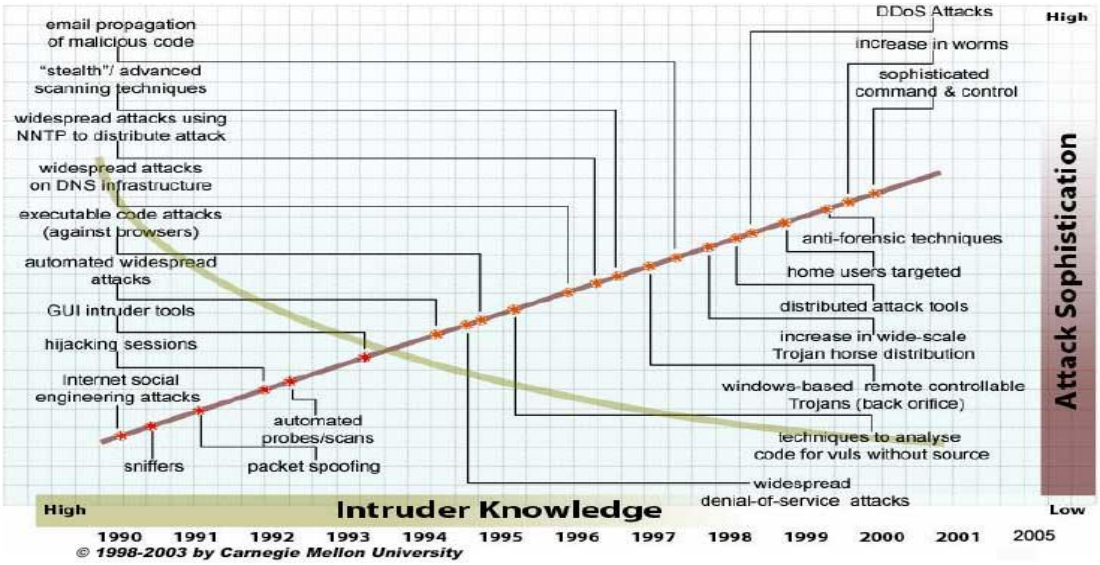
Jak bylo popsáno dřív, když se začíná s CSIRT, je třeba zvážit mnohé otázky. Nejlepší je přizpůsobit výše uvedený materiál potřebám CSIRT, jakmile tyto potřeby vzniknou.

Když se podávají zprávy vedení, je dobrou praxí co nejvíce aktualizovat vlastní případ s využitím posledních článků z novin nebo z Internetu a vysvětlit, proč jsou služby CSIRT a mezinárodní koordinace bezpečnostních incidentů rozhodující pro zajištění obchodního majetku. Je rovněž důležité vysvětlit, že pouze neustálá podpora v otázkách bezpečnosti IT vede ke stabilnímu obchodu, a to zejména ve společnosti nebo organizaci, která je závislá na IT.

(Poukazuje na to znamenitá věta Brucea Schneiera: *„Bezpečnost není produkt, ale proces[17]!“)*

Proslulým nástrojem pro ilustraci problémů bezpečnosti je následující graf poskytnutý týmem CERT/CC:

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



Obr. 8 Znalosti narušitele versus důmyslnost útoků (zdroj CERT-CC[18])

Ukazuje trendy v bezpečnosti IT, zejména snižování potřebné způsobilosti pro uskutečnění čím dál tím důmyslnějších útoků.

Další bod, o němž je třeba se zmínit, je neustálé zmenšování časového rozpětí mezi okamžikem, kdy je k dispozici aktualizace softwaru na zranitelnost, a zahájením útoků proti němu:

Opravný balíček -> využití		**Rychlost rozšiřování**	
Nimda:	11 měsíců	Redundance kódu:	Dní
Slammer:	6 měsíců	Nimda:	Hodin
Nachi:	5 měsíců	Slammer:	Minut
Blaster	3 týdny		
Witty:	1 den (!)		

Shromážděné údaje o bezpečnostních incidentech, potenciální zlepšení a získané poučení vytvářejí rovněž dobrou prezentaci.

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

Popis obchodních plánů a hybných sil vedení

Prezentace pro vedení, včetně podpory CSIRT, sama o sobě nevytváří obchodní případ, ale uskuteční-li se vhodným způsobem, vede ve většině případů k podpoře CSIRT ze strany vedení. Na druhé straně by se obchodní případ neměl chápat jako čistě manažerské cvičení, ale měl by se použít také pro komunikaci s týmem a složkou. Termínovaný obchodní případ může znít velmi komerčně a vzdáleně od každodenní praxe CSIRT, ale poskytuje dobré zaměření a orientaci, když se CSIRT vytváří.

Pro navržení dobrého obchodního případu by se mohly použít odpovědi na následující otázky (uvedené příklady jsou hypotetické a používají se pouze pro ilustraci. „Skutečné“ odpovědi značně závisí na „skutečných“ okolnostech).

- Jaký je problém?
- Čeho byste chtěli u svých složek dosáhnout?
- Co se stane, když nebudete dělat nic?
- Co se stane, když učiníte opatření?
- Kolik to bude stát?
- Co se získá?
- Kdy začnete a kdy to skončí?

Jaký je problém?
Nápad vytvořit CSIRT ve většině případů vznikne tehdy, když se bezpečnost stane důležitou součástí klíčového podnikání společnosti nebo organizace, a když se bezpečnostní incidenty IT stanou obchodním rizikem, které sníží bezpečnost obvyklé obchodní činnosti.

Většina společností nebo organizací má řádné oddělení pro podporu nebo sekci pro pomoc, ale ve většině případů se bezpečnostní incidenty řeší nedostatečně a ne tak strukturovaně, jak by tomu mělo být. Pracovní pole bezpečnostních incidentů si ve většině případů vyžaduje zvláštní odborné schopnosti a pozornost. Mít strukturovanější přístup je také výhodné a snižuje obchodní rizika a škody pro společnost.

Problém většinou spočívá v tom, že koordinace není dostatečná, a existující znalosti se nepoužívají k takovému řešení bezpečnostních incidentů, které by mohlo zamezit jejich výskytu v budoucnosti a předejít případným finančním ztrátám a / nebo poškození pověsti organizace.

Jakých cílů by se mělo u složky dosáhnout?
Jak bylo vysvětleno dřív, váš CSIRT bude sloužit svým složkám a pomůže jim v řešení bezpečnostních incidentů a problémů IT. Zvýšení úrovně znalostí o bezpečnosti IT a dosažení kultury povědomí o bezpečnosti jsou dalšími cíli.

Tato kultura usiluje o aktivní a preventivní opatření, která se přijímají od zahájení a snižují tak provozní náklady.

Zavedení této kultury spolupráce a pomoci ve společnosti nebo organizaci může ve většině případů obecně stimulovat efektivnost.

Co se stane, když se nic neudělá?
Nestrukturovaný způsob zacházení s bezpečností IT může vést k dalším škodám, v neposlední řadě k poškození dobrého jména organizace. Finanční ztráty a právní důsledky mohou být dalšími následky.

Co se stane, když se učiní opatření?
Povědomí o výskytu problémů bezpečnosti se zvýší. To přispěje k jejich efektivnějšímu řešení a k zamezení a k zamezení budoucím ztrátám.

Kolik to bude stát?
V závislosti na organizačním modelu vzniknou náklady na platy členů týmu CSIRT a na organizaci, vybavení, nástroje a licence softwaru.

Co se získá?
V závislosti na podnikání a ztrátách v minulosti dosáhne se více transparentnosti v postupech a bezpečnostních praktikách, čímž se bude chránit základní obchodní majetek.

Jaká je aktuálnost?
Popis vzorového plánu projektu viz kapitola *12. Popis plánu projektu.*

Příklady existujících obchodních případů a přístupů
Níže je uvedeno několik příkladů obchodních případů CSIRT, které má cenu zkoumat.

- http://www.cert.org/csirts/AFI_case-study.html
  Vytvoření finanční instituce CSIRT: Případová studie

  Účelem tohoto dokumentu je sdílet poučení, které získala finanční instituce (v tomto dokumentu uváděna jako AFI – *a financial institution*), když zpracovává a realizuje plán řešení problému bezpečnosti a zavádí Tým pro reakci na bezpečnostní incidenty počítačů – CSIRT (*Computer Security Incident Response Team).*

- http://www.terena.nl/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf
  Shrnutí obchodního případu CERT POLSKA (promítání diapozitivů ve formátu PDF).

- http://www.auscert.org.au/render.html?it=2252
  Vytvoření Týmu pro reakci na bezpečnostní incidenty – IRT *(Incident Response Team)* v 90. letech může být nelehký úkol. Mnoho pracovníků, kteří ustavují IRT, v tom nemá zkušenosti. Tento dokument zkoumá, jakou úlohu může IRT hrát ve společnosti, a otázky, které by se měly řešit jak během formování týmu, tak i po zahájení jeho činností. Může to být prospěšné pro existující týmy IRT, protože se může zvýšit povědomí o otázkách, které se dřív neřešily.

- http://www.sans.org/reading_room/whitepapers/casestudies/1628.php
  Případová studie o bezpečnosti informací a zabezpečení podniku od: Rogera Bentona.

  Toto praktické cvičení je případovou studii migrace pojišťovny do celopodnikového bezpečnostního systému. Záměrem tohoto praktického cvičení je poskytnout cestu,

která se má sledovat, když se vytváří bezpečnostní systém, nebo když se do něj migruje. Původně byl jednoduchý bezpečnostní systém on-line jediným mechanizmem pro kontrolu přístupu k podnikovým údajům. Vystavení riziku bylo velké – neexistovaly kontroly integrity mimo prostředí on-line. Každý se základními schopnostmi programování mohl doplňovat, měnit a/nebo mazat výrobní údaje.

- http://www.esecurityplanet.com/trends/article.php/10751_688803
  Strategie elektronické bezpečnosti ve společnosti Marriot: spolupráce obchodních IT

  Zkušenosti Chrisa Zoladze z akciové společnosti Marriot International, Inc., spočívají v tom, že bezpečnost elektronického obchodování je proces, ne projekt. Tato zpráva Zoladze byla oznámená na poslední Konferenci o elektronické bezpečnosti a na Světové výstavě elektronické bezpečnosti v Bostonu, kterou sponzorovala skupina Intermedia Group. Zoladz jako viceprezident pro ochranu informací v Marriottu je podřízen právnímu oddělení, ačkoli není právník. Jeho úkolem je identifikovat, kde jsou uloženy nejcennější obchodní informace Marriotu, a jak se pohybují v rámci společnosti a mimo ní. Ve společnosti Marriot byla stanovena zvláštní odpovědnost za technickou infrastrukturu, která podporuje bezpečnost, a která je svěřena architektovi bezpečnosti IT.

Fiktivní CSIRT (7. krok)
Podpora obchodního plánu Bylo rozhodnuto shromáždit fakta a čísla z minulosti společnosti. Je to více než účelné pro statistický přehled o situaci v bezpečnosti IT. Tento sběr by měl pokračovat, když už je CSIRT vytvořen a pracuje, aby se statistický přehled udržoval v aktuálním stavu. Byly kontaktovány další národní týmy CSIRT a dotazovány na jejich obchodní případy. Týmy poskytly podporu sestavením určitých diapozitivů s informacemi o posledním vývoji v bezpečnostních incidentech IT a o nákladech na bezpečnostní incidenty. V tomto vzorovém případě fiktivního CSIRT nebylo nutné příliš přesvědčovat vedení o důležitosti problematiky IT, takže nebylo těžké zahájit první krok. Byl zpracován obchodní případ a plán projektu, včetně odhadu nákladů na přípravu a odhadu provozních nákladů.

8 Příklady pracovních a technických postupů (průběh prací)

Dosud jsme učinili následující kroky:

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým poskytovat své služby?
3. Jaký druh služeb může CSIRT poskytovat své složce.
4. Analýza prostředí a složek.
5. Stanovení mandátu.
6. Zpracování obchodního plánu
   a. Definování finančního modelu
   b. Určení organizační struktury
   c. Zahájení náboru pracovníků
   d. Používání a vybavení kanceláře
   e. Zpracování politiky bezpečnosti informací
   f. Vyhledávání partnerů pro spolupráci
7. Podpora obchodního plánu
   a. Schválení obchodního případu.
   b. Začlenění všeho do plánu projektu.

>> Další krok je: Zajistit fungování CSIRT.

Když se zavedou dobře definované pracovní postupy, zlepší se jakost a sníží se čas potřebný na případ bezpečnostního incidentu nebo zranitelnosti.

Jak bylo popsáno ve vzorových rámečcích, fiktivní CSIRT bude nabízet tyto základní klíčové služby CSIRT:

- Výstrahy a varování
- Řešení bezpečnostních incidentů
- Oznámení

Tato kapitola uvádí příklady pracovních postupů, které popisují klíčové služby CSIRT. Obsahuje rovněž informace o sběru dat z různých zdrojů, jejich ověřování z hlediska důležitosti a hodnověrnosti a jejich opětovné rozesílání složce. A nakonec tato kapitola obsahuje příklady nejdůležitějších postupů a specifické nástroje CSIRT.

Hodnocení instalační báze složky

První krok je získat přehled o systémech IT instalovaných ve vaší složce. CSIRT tak může vyhodnotit důležitost vstupních informací a filtrovat je před opětovným rozesláním, takže složky nebudou zahlceny informacemi, které jsou pro ně v podstatě nadbytečné.

Dobrá praxe je začít jednoduše, např. s použitím listu v Excelu jako následující:

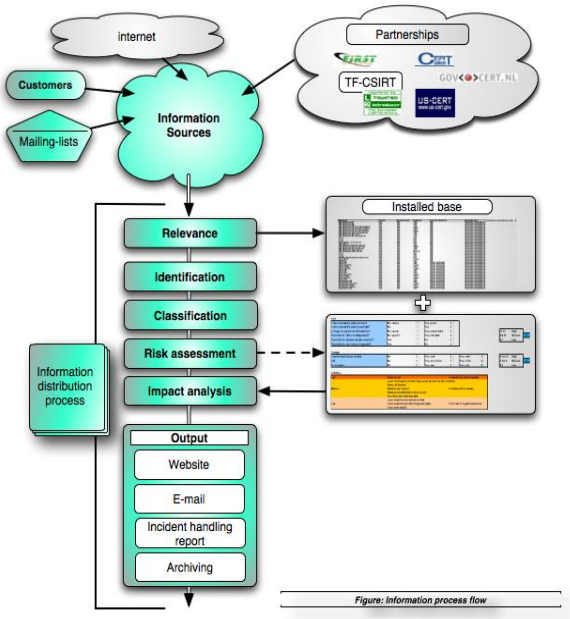
Kategorie	Aplikace	Produkt softwaru	Verze	Operační systém	Verze operačního systému	Složka
Desktop	Office	Excel	x-x-x	Microsoft	XP-prof	A
Desktop	Prohlížeč	Internet Explorer	x-x-	Microsoft	XP-prof	A
Síť	Směrovač	CISCO	x-x-x	CISCO	x-x-x-	B
Server	Server	Linux	x-x-x	L-distro	x-x-x	B
Služby	Webový server	Apache		Unix	x-x-x	B

S funkcí filtru v Excelu je velmi snadné vybrat vhodný software a zjistit, která složka jaký druh softwaru používá.

Vytváření výstrah, varování a oznámení

U vytváření výstrah, varování a oznámení se dodržují stejné pracovní postupy:

- Sběr informací
- Hodnocení informací z hlediska důležitosti a zdroje
- Hodnocení rizik založené na shromážděných informacích
- Rozeslání informací



Obr. 9 Postup procesu informací

V následujících bodech bude tento pracovní postup popsán podrobněji.

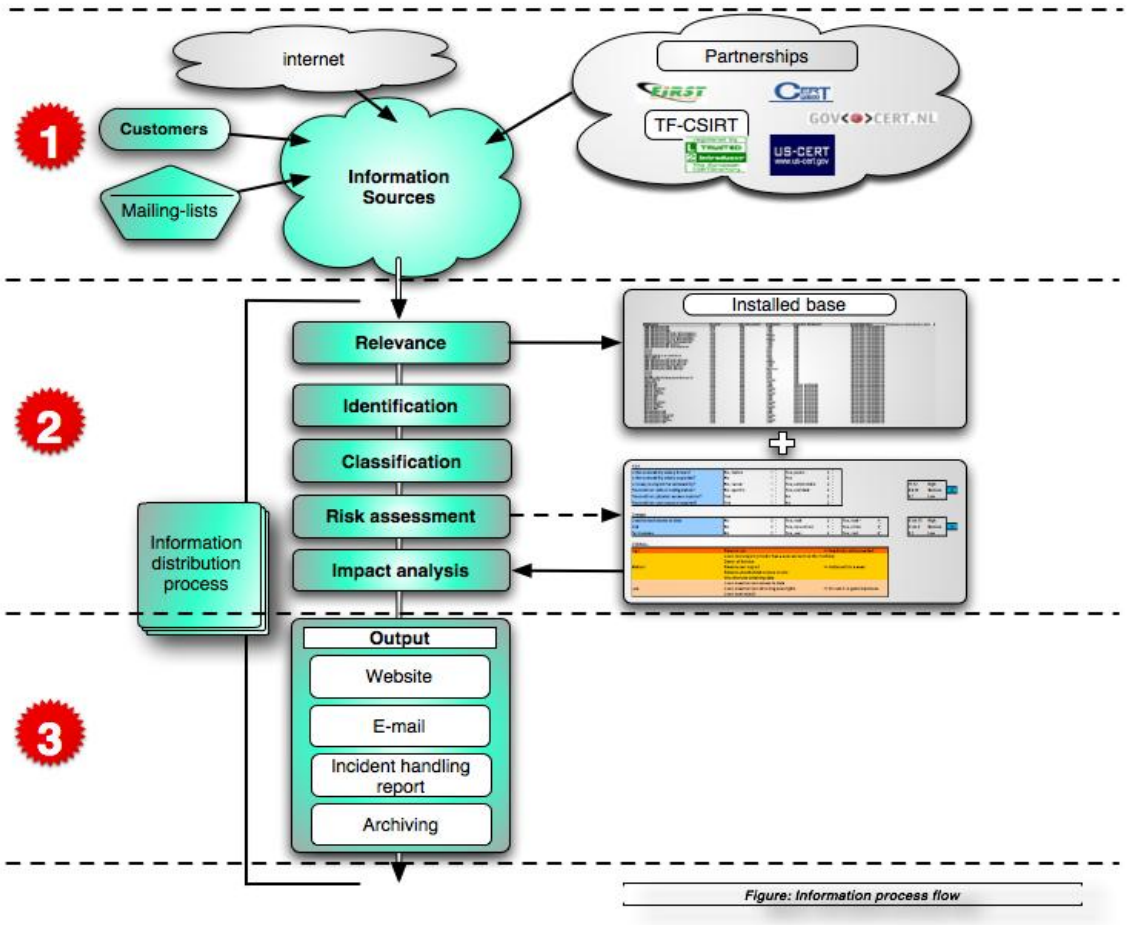


Figure: Information process flow

1. krok: Sběr informací o zranitelnosti.

Obvykle existují dva hlavní druhy informačních zdrojů, které přispívají informacemi jako vstup pro služby:

- Informace o zranitelnosti (vašich) systémů IT
- Zprávy o bezpečnostních incidentech

V závislosti na druhu podnikání a infrastruktuře IT existuje mnoho veřejných a uzavřených zdrojů informací o zranitelnosti:

- Veřejné a uzavřené adresáře
- Informace o zranitelnosti produktu prodejce
- Webové stránky
- Informace na Internetu (Google atd....)
- Veřejné a soukromé partnerství, které poskytuje informace o zranitelnosti (FIRST, TF-CSIRT, CERT-CC, US-CERT….)

Všechny tyto informace přispívají k úrovni znalostí o specifické zranitelnosti systémů IT.

Jak bylo uvedeno dřív, na Internetu je k dispozici mnoho dobrých a snadno dostupných zdrojů informací o bezpečnosti. Pracovní skupina ad hoc agentury ENISA „Služby CERT“ pro rok 2006 sestavuje v době zpracovávání této zprávy podrobnější seznam, který má být hotový koncem roku 2006[19].

2. krok: Hodnocení informací a rizika

Výsledkem tohoto kroku bude analýza dopadu specifické zranitelnosti na infrastrukturu IT složky.

Identifikace
Přicházející informace o zranitelnosti se musí vždy identifikovat podle jejich zdroje, a než se jakákoli informace předá složce, musí se určit, zda je zdroj důvěryhodný. Jinak by pracovníci mohli být klamně varováni, což by mohlo vést ke zbytečným poruchám v podnikových procesech a nakonec poškodit dobré jméno CSIRT.

Následující postup ukazuje příklad identifikace autentičnosti zprávy:

Postup, jak identifikovat autentičnost zprávy a jejího zdroje

Celkový kontrolní seznam
1. Je zdroj jako takový známý a registrovaný?
2. Přichází informace běžným kanálem?
3. Je tam obsažena „neobvyklá“ informace, která se „zdá být“ nesprávná?
4. Dejte na své dojmy, a máte-li pochybnosti o nějaké informaci, nedělejte dál nic, ale znovu si ji ověřte!

Zdroje elektronické pošty
1. Je zdrojová adresa organizaci známa a je známa ve zdrojovém seznamu?
2. Je podpis PGP správný?
3. V případě pochybností ověřte celé záhlaví zprávy.
4. Máte-li pochybnosti, použijte „nslookup“ (vyhledávání bezpečnosti sítě) nebo „dig“ k ověření domény odesílatelů[20].

Zdroje www
1. Ověřte certifikáty prohlížečů, když se napojujete na zajištěnou webovou stránku (https://).
2. Ověřte zdroj z hlediska obsahu a platnosti (technické).
3. Máte-li pochybnosti, neklikněte na žádná spojení, ani si nestáhněte žádný software.
4. Máte-li pochybnosti, mějte aktivovaný „lookup“ (vyhledávání) a “dig“ na doméně a aktivujte „traceroute“ (sledovací cesta).

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

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

Telefon
1. Pozorně poslouchejte jméno.
2. Rozeznáváte hlas?
3. Máte-li pochybnosti, požádejte volajícího o telefonní číslo a o možnost zatelefonovat mu zpátky.

Obr. 10 Příklad postupu identifikace

Důležitost
Přehled o nainstalovaném hardwaru a softwaru vytvořený dříve lze použít k filtrování přicházejících informací o zranitelnosti z hlediska jejich důležitosti s cílem najít odpověď na otázky: „Používá složka tuto část softwaru?“ „Je informace pro ni důležitá?“

Klasifikace
Některé obdržené informace lze klasifikovat nebo označit jako důvěrné (například zprávy o bezpečnostních incidentech přicházející od jiných týmů). Se všemi informacemi se musí zacházet podle požadavku odesílatele a v souladu s vlastní politikou bezpečnosti informací. Dobrým základním pravidlem je *„Nerozesílejte informaci, není-li jasné, co by měla znamenat; máte-li pochybnosti, požádejte odesílatele o souhlas s jejím rozesláním.“*

Hodnocení rizika a analýza dopadů
Existuje několik metod pro určení rizika a dopadu (potenciální) zranitelnosti.

Riziko se definuje jako potenciální možnost, že zranitelnost může být zneužita. Je několik důležitých faktorů (kromě jiných):

- Je zranitelnost dobře známá?
- Je zranitelnost značně rozšířena?
- Je snadné zranitelnost zneužít?
- Je zranitelnost zneužitelná na dálku?

Všechny tyto otázky poskytují dobré povědomí o závažnosti zranitelnosti.
Velmi jednoduchou metodou výpočtu rizika je následující vzorec:

Dopad = riziko x potencionální škoda

Potencionální škodou by mohl být

- Nepovolený přístup k údajům
- Odepření služby – DOS *(Denial of Service)*
- Získání rozšířených povolení

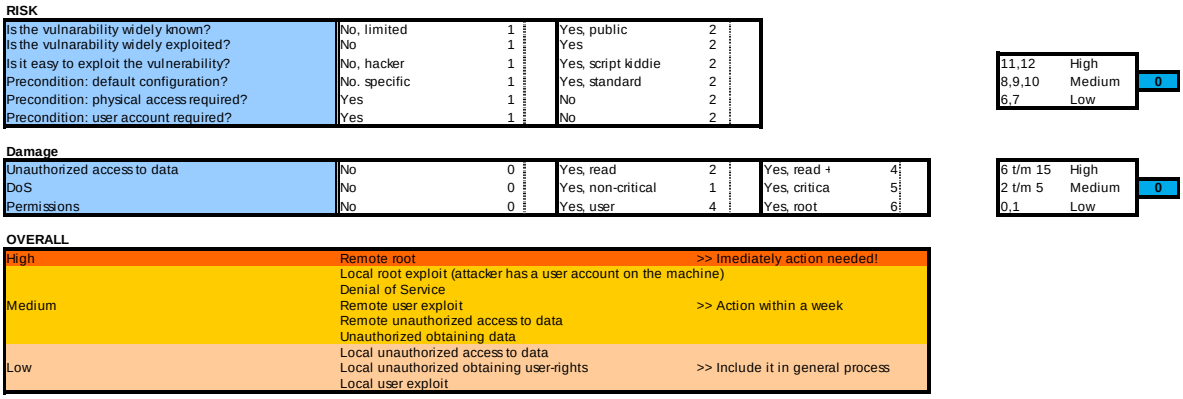
(Propracovanější schémata klasifikace viz konec této kapitoly.)

Po zodpovězení těchto otázek lze celkové hodnocení doplnit do odborné rady, která informuje o potenciálním riziku a škodě. Často se používají jednoduché výrazy jako NÍZKÉ, STŘEDNÍ a VYSOKÉ.

Jiným, komplexnějším schématem hodnocení rizika je:

Schéma hodnocení GOVCERT.NL[21]

Holandský vládní CSIRT GOVCERT.NL zpracoval matici pro hodnocení rizika, která byla vyvinuta v počáteční fázi Govcert.nl, a stále se aktualizuje podle posledních trendů.



Obr. 11 Schéma hodnocení GOVCERT.NL

Popis společné formy poradenství EISPP[22]

Evropský program podpory bezpečnosti informací – EISIPP *(European Information Security Promotion Programme)* je projekt spolufinancovaný Evropským společenstvím na základě Pátého rámcového programu. Projekt EISIPP se snaží rozvíjet evropský rámec a nejenom sdílet znalosti o bezpečnosti, ale také vymezit obsah a způsoby šíření informací o bezpečnosti pro malé a střední podniky – SME *(Small and Medium-Size Enterprises)*. Poskytování potřebných služeb bezpečnosti IT pro evropské SME je podpoří v rozvíjení jejich důvěry a v používání elektronického obchodování, které vede k větším a lepším příležitostem nových obchodů. EISPP je průkopníkem ve vizi Evropské komise týkající se vytváření evropské sítě odborných znalostí v rámci Evropské unie.

Německá forma poradenství DAF *(Deutsches Advisory Format)*[23]

DAF je iniciativa německého Svazu CERT *(CERT-Verbund)* a je základní složkou infrastruktury pro vytváření a výměnu odborných rad v bezpečnosti mezi různými týmy. DAF je zvlášť přizpůsoben potřebám německých týmů CERT; normu zpracoval a udržuje ji Svaz CERT *(CERT-Bund)*, DFN-CERT, PRESECURE a Siemens-CERT.

3. krok: Rozeslání informací

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

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

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

CSIRT si může vybrat z několika metod rozesílání v závislosti na přáních složek a vaši strategii komunikace.

- Webová stránka
- Elektronická pošta
- Zprávy
- Archivace a průzkum

Odborné rady v bezpečnosti rozesílané týmem CSIRT by měly vždy dodržovat stejnou strukturu. Zvýší se tím jejich srozumitelnost a čtenář rychle najde všechny důležité informace.

Odborná rada by měla obsahovat nejméně následující informace:

Název odborné rady
……

Referenční číslo
……
Dotyčné systémy
- ……
- ……

Související operační systém + verze
……
Riziko (Vysoké – Střední – Nízké)
……
Dopad/potenciální škoda (Velký – Střední – Malý)
……
Vnější identifikace: (Celková zranitelnost a vystavení riziku – CVE *(Common Vulnerability and Exposure)*, Identifikace bulletinu o zranitelnosti)
……

Přehled o zranitelnosti
……

Dopad
……

Řešení
……

Popis (podrobnosti)
……

Příloha
……

Obr. 12 Vzorové schéma odborných rad

Viz kapitolu *10. Cvičení na kompletní příklad odborné rady v bezpečnosti.*

Řešení bezpečnostních incidentů

Jak už bylo uvedeno v úvodu této kapitoly, proces zacházení s informacemi během řešení bezpečnostních incidentů je velmi podobný procesu používanému v průběhu sestavování výstrah, varování a oznámení. Ale část týkající se shromažďování informací je obvykle odlišná, protože běžný způsob získávání údajů o bezpečnostním incidentu spočívá buď v obdržení zpráv o bezpečnostních incidentech od složky nebo od jiných týmů, nebo v získání zpětné vazby od zúčastněných stran během procesu řešení bezpečnostních incidentů. Informace přicházejí většinou (šifrovanou) elektronickou poštou; někdy je nutné použít telefon nebo fax.

Když je informace přijata telefonicky, dobrou praxí je ihned zaznamenat každou jednotlivou podrobnost buď s použitím řešení bezpečnostního incidentu/nástroje

podávání zpráv, nebo vyhotovením krátké písemné zprávy. Je nutné ihned (než telefonát skončí) vytvořit číslo bezpečnostního incidentu (pokud ho tento bezpečnostní incident dosud nemá) a tomu, kdo bezpečnostní incident ohlásil, ho dát telefonicky (nebo souhrnnou elektronickou zprávou zaslanou později) jako referenční číslo pro další komunikaci.

Zbylá část této kapitoly popisuje základní proces řešení bezpečnostních incidentů. Hloubková analýza úplného procesu řízení bezpečnostních incidentů a všech používaných pracovních postupů a dílčích pracovních postupů je uvedena v dokumentaci CERT/CC *Stanovení procesů řízení bezpečnostních incidentů pro týmy CSIRT*[24].

[24] Stanovení procesů řízení bezpečnostních incidentů: http://www.cert.org/archive/pdf/04tr015.pdf

Řešení bezpečnostních incidentů v zásadě dodržuje následující pracovní postup:

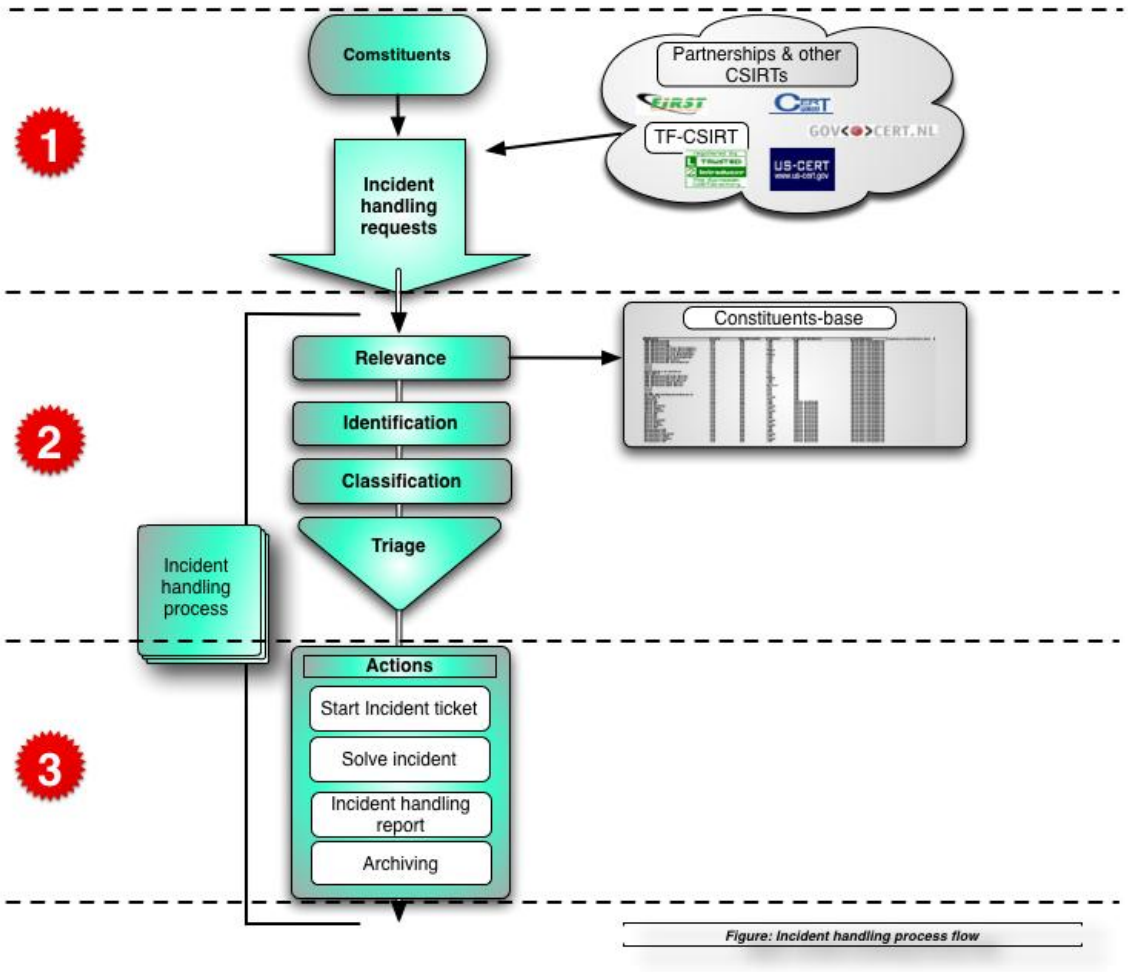


Figure: Incident handling process flow

1. krok: Přijetí zpráv o bezpečnostních incidentech

Jak bylo uvedeno dřív, zprávy o bezpečnostních incidentech se dostávají do týmu CSIRT různými kanály, většinou elektronickou poštou, ale také telefonicky a faxem.

Jak bylo zmíněno výše, když se přijímá zpráva o bezpečnostním incidentu, je dobrou praxí zaznamenat všechny podrobnosti v pevném formátu. Tím se zajistí, že se nevynechá žádná důležitá informace. Existuje následující vzorové schéma:

FORMULÁŘ HLÁŠENÍ BEZPEČNOSTNÍHO INCIDENTU
Vyplňte tento formulář a zašlete ho faxem nebo elektronickou poštou na: …….. *Řádky označené hvězdičkou * jsou povinné.* *Jméno a organizace* 1. Jméno*: 2. Název organizace*: 3. Druh sektoru: 4. Země*: 5. Město: 6. Elektronická adresa*: 7. Telefonní číslo*: 8. Jiné: *Postižený hostitel (postižení hostitelé)* 9. Počet hostitelů: 10. Jméno hostitele a internetový protokol – IP *(Internet Protocol)**: 11. Funkce hostitele*: 12. Časové pásmo: 13. Hardware: 14. Operační systém: 15. Postižený software: 16. Postižené soubory: 17. Bezpečnost: 18. Jméno hostitele a IP: 19. Protokol/port: *Bezpečnostní incident* 20. Referenční číslo ref #: 21. Druh bezpečnostního incidentu: 22. Bezpečnostní incident začal: 23. Jedná se o pokračující bezpečnostní incident: ANO NE 24. Doba a způsob zjištění: 25. Známá zranitelnost: 26. Podezřelé soubory: 27. Protiopatření: 28. Podrobný popis*:

Obr. 14 Obsah hlášení bezpečnostního incidentu

2. krok: Hodnocení bezpečnostního incidentu

Během tohoto kroku se ověřuje autentičnost a závažnost hlášeného bezpečnostního incidentu a incident se klasifikuje.

Identifikace

Aby se zamezilo zbytečným krokům, dobrý zvyk je ověřit si, zda je odesílatel zprávy důvěryhodný, a zda je jedním z vás nebo spolupracovníkem složek týmů CSIRT. Uplatňují se podobná pravidla jako ta, která jsou popsaná v kapitole *8.2 Vytváření výstrah.*

Závažnost

Tímto krokem ověřujete, zda žádost o řešení bezpečnostního incidentu pochází ze složky týmů CSIRT, nebo zda se hlášený bezpečnostní incident týká systémů IT složky. Neplatí-li nic z výše uvedeného, zpráva se obvykle přesměruje na správný CISRT[25].

Klasifikace

Tímto krokem se zpracovává třídění na základě klasifikace závažnosti bezpečnostního incidentu. Zacházení do podrobností klasifikace bezpečnostních incidentů překračuje rámec tohoto dokumentu. Dobrým začátkem je použití schématu případové klasifikace CSIRT (příklad pro 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.		

Obr. 15 Schéma klasifikace bezpečnostních incidentů (zdroj: Obr. 17 FIRST)[26]

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

Třídění

Třídění je systém používaný zdravotnickými pracovníky nebo pracovníky záchranné služby pro přidělování omezených zdravotnických zdrojů, když počet zraněných, kteří potřebují ošetření, překračuje disponibilní zdroje pro poskytování péče tak, aby byl ošetřen co největší počet pacientů[27].

CERT/CC uvádí následující popis:

Třídění je důležitý prvek každé způsobilosti řízení bezpečnostních incidentů, a to zejména pro každý vytvořený CSIRT. Třídění je na kritické cestě k pochopení, o čem se podávají zprávy v celé organizaci. Slouží jako hybná síla, pomocí které všechny informace postupují do jednoho kontaktního bodu, a která umožňuje přehled podniku o probíhající činnosti a uvádí všechny hlášené údaje do celkového vzájemného vztahu. Třídění dává možnost počátečního hodnocení přicházející zprávy a její seřazení pro další řešení. Zajišťuje rovněž místo pro zahájení zápisu počáteční dokumentace a údajů zprávy nebo žádosti, pokud se to už neudělalo v procesu detekce.

Funkce třídění poskytuje bezprostřední obraz současného stavu všech hlášených činností – jaké zprávy jsou otevřeny nebo zavřeny, jaká opatření jsou dosud otevřena a kolik zpráv od každého typu bylo obdrženo. Tento proces může pomoci identifikovat potenciální problémy bezpečnosti a stanovit priority pracovních úkolů. Informace shromážděné během třídění lze také použít ke generování trendů zranitelnosti a bezpečnostních incidentů a statistických přehledů pro vyšší vedení[28].

Třídění by měli uskutečňovat pouze nejzkušenější členové týmů, protože si vyžaduje hluboké chápání možných dopadů bezpečnostních incidentů na konkrétní části složky a schopnost rozhodovat, který člen týmu by byl vhodný pro řešení tohoto bezpečnostního incidentu.

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

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

[28] Stanovení procesů řízení bezpečnostních incidentů: http://www.cert.org/archive/pdf/04tr015.pdf

3. krok: Opatření

Tříděné bezpečnostní incidenty se obvykle zařazují do žádoucí řady v nástroji pro řešení bezpečnostních incidentů, který používá jeden nebo více řešitelů bezpečnostních incidentů dodržujících v zásadě následující kroky.

Spuštění průkazů bezpečnostních incidentů
Počet průkazů bezpečnostních incidentů už mohl být generován v předcházejícím kroku (například když byl bezpečnostní incident nahlášen telefonicky). Pokud nebyl, první krok je vytvořit takový počet, který se použije v další komunikaci o tomto bezpečnostním incidentu.

Životní cyklus bezpečnostního incidentu
Řešení bezpečnostního incidentu nesleduje linii kroků, které nakonec vedou k řešení, ale spíše cyklus kroků, které se opakovaně používají, dokud se bezpečnostní incident s konečnou platností nevyřeší, a dokud všechny dotčené strany nemají všechny potřebné informace. Tento cyklus uváděný často jako „Životní cyklus bezpečnostního incidentu“ zahrnuje následující procesy:

Analýza:	Analyzují se všechny podrobnosti o hlášeném bezpečnostním incidentu.
Získání kontaktních informací:	Schopnost předat zprávu s informacemi o bezpečnostním incidentu dál všem postiženým stranám, jako jsou jiné týmy CSIRT, oběti a nejspíše vlastníci těch systémů, které by byly mohly být zneužité pro útok.
Poskytování technické pomoci:	Pomoc obětem rychle se zotavit z důsledků bezpečnostního incidentu a shromáždit více informací o útoku.
Koordinace:	Informování jiných postižených stran jako CSIRT odpovědný za systém IT použitý pro útok nebo jiné oběti.

Tato struktura se nazývá „životní cyklus“, protože jeden krok vede ke druhému a k poslednímu, ke koordinační části, a pak může opět vést k nové analýze a cyklus začíná znovu. Proces končí, když všechny dotčené strany obdrží a ohlásí všechny potřebné informace.

Podrobnější popis životního cyklu bezpečnostního incidentu viz příručka CERT/CC CSIRT[29].

Zpráva o řešení bezpečnostních incidentů
Na otázky z vedení o bezpečnostních incidentech se připravte zpracováním zprávy. Dobrou praxí je také napsat dokument (pouze pro vnitřní potřebu) o „získaném poučení“

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

s cílem poučit pracovníky a vyhnout se chybám v procesech budoucího řešení bezpečnostních incidentů.

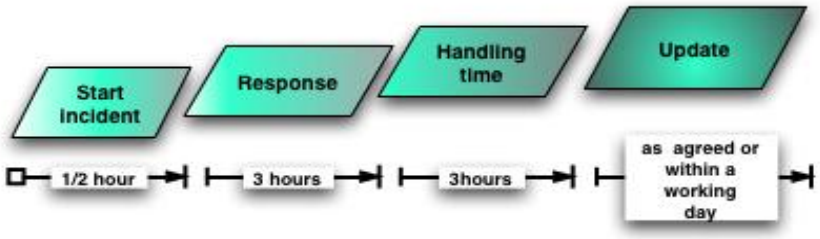
Archivace
Podívejte se na pravidla archivace popsaná dříve v kapitole *6.6 Zpracování politiky bezpečnosti informací.*

Podrobné pokyny k řízení a životnímu cyklu bezpečnostních incidentů viz část přílohy *A1* pod názvem *Další výklad.*

Příklad časového harmonogramu reakce

Definice doby reakce se často opomíjí, ale musí být součástí každé dobře sestavené smlouvy o úrovni služeb – SLA *(Service Level Agreement)* mezi CSIRT a jeho složkou. Poskytování včasné zpětné vazby složkám během řešení bezpečnostních incidentů je velmi důležité jak pro vlastní odpovědnost složek, tak i pro dobré jméno týmu.
Doby reakce se musí složce jasně oznámit, aby se zamezilo mylným očekáváním. Pro podrobnější SLA se složkou týmů CSIRT lze jako výchozí bod použít následující základní časový harmonogram.

Zde je příklad časového harmonogramu praktické reakce od okamžiku přijetí žádosti o pomoc:



Obr. 16 Příklad časového harmonogramu reakce

Dobrou praxí je také instruovat složku o jejich vlastních dobách reakce, zejména když je CSIRT kontaktován v případě nouzového stavu. Ve většině případů je lépe kontaktovat její CSIRT v ranném stádiu a dobrou praxí je podpořit složku, aby tak učinila, jestliže má pochybnosti.

Dostupné nástroje CSIRT

Tato kapitola uvádí několik pokynů k obvyklým nástrojům, které používají týmy CSIRT. Poskytuje pouze příklady, více pokynů je uvedeno v *Informačním centru nástrojů pro řešení bezpečnostních incidentů – CHIHT (Clearinghouse of Incident Handling Tools)*[30].

Software pro šifrování elektronické pošty a zpráv

- GNUPG http://www.gnupg.org/
  GnuPG je úplné a bezplatné zavádění projektu GNU normy OpenPGP podle definice v RFC2440. GnuPG vám umožňuje šifrovat a podepisovat svoje údaje a oznámení.

- PGP http://www.pgp.com/
  Komerční varianta

Nástroj řešení bezpečnostních incidentů

Administrativní bezpečnostní incidenty a jejich sledování, sledování opatření.

- RTIR http://www.bestpractical.com/rtir/
  Sledovač žádostí o reakci na bezpečnostní incidenty – RTIR *(Request Tracker Incidence Response)* je bezplatný otevřený zdroj systému řešení bezpečnostních incidentů vytvořený na základě potřeb týmů CERT a jiných příslušných týmů pro reakci na bezpečnostní incidenty.

Nástroje CRM

Máte-li hodně různých složek a potřebujete-li vysledovat všechny funkce a podrobnosti, databáze CRM je užitečná. Existuje mnoho různých variant, zde je několik příkladů:

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

- Sugarforce (bezplatná otevřená zdrojová verze) http://www.sugarforge.org/

Ověřování informací

- Internetový hlídač http://www.aignes.com/index.htm
  Tento program sleduje webové stránky z hlediska jejich aktualizací a změn.

- Sledování této stránky http://www.watchthatpage.com/
  Služba zasílá informace o změnách na webových stránkách elektronickou poštou (bezplatně a komerčně).

Vyhledávání kontaktních informací

Vyhledávání správného kontaktu pro hlášení bezpečnostních incidentů není snadný úkol. Zde je několik informačních zdrojů, které lze použít:

- Organizace RIPE[31]

[30] CHIHT: http://www.enisa.europa.eu/cert_inventory/pages/04_02.htm#04
[31] Internetová služba organizace RIPE zaměřená na vyhledávání osob a jejich kontaktních údajů: http://www.ripe.net/whois

- Objekt IRT[32]
- TI[33]

CHIHT kromě toho uvádí některé nástroje pro vyhledávání kontaktních informací[34].

Fiktivní CSIRT (8. krok)
Vytvoření pracovních postupů procesů a provozních a technických postupů Fiktivní CSIRT se zaměřuje na poskytování následujících rozhodujících služeb CSIRT: • Výstrahy a varování • Oznámení • Řešení bezpečnostních incidentů Tým zpracoval postupy, které dobře fungují, a které může každý člen týmu snadno pochopit. Fiktivní CSIRT také najal právního experta pro řešení odpovědnosti a politiky bezpečnosti informací. Tým schválil několik užitečných nástrojů a v rámci jednání s jinými týmy CSIRT zjistil užitečné informace o provozních otázkách. Byla vytvořena pevná šablona pro poradenství v bezpečnosti a pro zprávy o bezpečnostních incidentech. K řešení bezpečnostních incidentů tým používá sledovač žádostí o reakci na bezpečnostní incidenty – RTIR *(Request Tracker Incidence Response)*.

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

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

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

9 Výcvik CSIRT

Dosud jsme učinili následující kroky:

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým poskytovat své služby?“
3. Jaký druh služeb může CSIRT poskytovat své složce.
4. Analýza prostředí a složek.
5. Stanovení mandátu.
6. Zpracování obchodního plánu
   a. Definování finančního modelu
   b. Určení organizační struktury
   c. Zahájení náboru pracovníků
   d. Používání a vybavení kanceláře
   e. Zpracování politiky bezpečnosti informací
   f. Vyhledávání partnerů pro spolupráci
7. Podpora obchodního plánu
   a. Schválení obchodního případu.
   b. Začlenění všeho do plánu projektu.
8. Zajištění fungování CSIRT.
   a. Vytvoření pracovních postupů
   b. Zavedení nástrojů CSIRT

>> Další krok je: výcvik pracovníků.

Tato kapitola uvádí seznam dvou hlavních zdrojů pro vyhrazený výcvik CSIRT: Výcvik v bezpečnosti sítí – TRANSITS *(Training of Network Security)* a CERT/CC.

TRANSITS

TRANSITS byl evropský projekt na podporu vytvoření týmů pro reakci na bezpečnostní incidenty počítačů – CSIRT *(Computer Security Incident Response Teams)* a pro zdokonalení existujících týmů CSIRT řešením problému nedostatku odborně kvalifikovaných pracovníků CSIRT. Tento cíl se řešil poskytováním odborných výcvikových kurzů pro školení pracovníků (nových) CSIRT o organizačních, provozních, technických, obchodních a právních otázkách souvisejících s poskytováním služeb CSIRT.

TRANSITS zejména

- zpracoval, aktualizoval a pravidelně revidoval modulární školící materiály kurzů
- organizoval školící semináře, pro které byly dodány materiály kurzů
- umožnil účast pracovníků (nových) týmů CSIRT na těchto školících seminářích se zvláštním důrazem na účast ze států přistupujících k EU
- rozšířil školící materiály kurzů a zajistil využití výsledků[35].

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

Agentura ENISA usnadňuje a podporuje kurzy TRANSITS. Chcete-li vědět, jak požádat o kurzy, a chcete-li znát požadavky a náklady, kontaktujte experty CSIRT agentury ENISA.

CERT-Relations@enisa.europa.eu

V příloze tohoto dokumentu jsou vzorové materiály kurzů!

CERT/CC

Složitost počítačových infrastruktur a infrastruktur sítí a nároky na správu ztěžují náležité řízení bezpečnosti sítí. Správci sítí a systémů nemají dostatek pracovníků a zavedených praktik bezpečnosti, aby se bránili proti útokům a minimalizovali škody. V důsledku toho se počet bezpečnostních incidentů počítačů zvyšuje.
Vyskytnou-li se bezpečnostní incidenty počítačů, organizace musí rychle a účinně reagovat. Čím rychleji organizace rozpozná, analyzuje a reaguje na bezpečnostní incident, tím více může omezit škody a snížit náklady na obnovu. Vytvoření týmu pro reakci na bezpečnostní incidenty počítačů – CSIRT *(Computer Security Incident Response Team)* je vynikající způsob, jak zajistit tuto schopnost rychle reagovat a také pomoci předcházet budoucím bezpečnostním incidentům.

CERT-CC nabízí kurzy pro manažery a technické pracovníky v takových oblastech jako vytváření a řízení týmů pro reakci na bezpečnostní incidenty počítačů (CSIRT), reagování na bezpečnostní incidenty a jejich analyzování a zvyšování bezpečnosti sítí. Není-li uvedeno jinak, všechny kurzy se konají v Pittsburghu, PA. Naši pracovníci přednášejí v kursech o bezpečnosti také na Univerzitě Carnegie Mellon.

Dostupné kurzy CERT/CC[36] věnované týmům CSIRT

Vytvoření týmu pro reakci na bezpečnostní incidenty počítačů (CSIRT)
Řízení týmů pro reakci na bezpečnostní incidenty počítačů (CSIRT)
Zásady řešení bezpečnostních incidentů
Pokročilé řešení bezpečnostních incidentů pro technické pracovníky

V příloze tohoto dokumentu jsou vzorové materiály kurzů!

Fiktivní CSIRT (9. krok)
Výcvik pracovníků Fiktivní CSIRT rozhodne vyslat všechny své technické pracovníky na příští kursy TRANSITS, které jsou k dispozici. Vedoucí týmu se kromě toho účastní kursu *Řízení CSIRT* z CERT/CC.

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

10 Cvičení: Vytváření odborné rady

Dosud jsme učinili následující kroky:

1. Pochopení, co je CSIRT, a jaké výhody může poskytnout.
2. Jakému sektoru bude nový tým poskytovat své služby?“
3. Jaký druh služeb může CSIRT poskytovat své složce.
4. Analýza prostředí a složek.
5. Stanovení mandátu.
6. Zpracování obchodního plánu
   a. Definování finančního modelu
   b. Určení organizační struktury
   c. Zahájení náboru pracovníků
   d. Používání a vybavení kanceláře
   e. Zpracování politiky bezpečnosti informací
   f. Vyhledávání partnerů pro spolupráci
7. Podpora obchodního plánu
   a. Schválení obchodního případu.
   b. Začlenění všeho do plánu projektu.
8. Zajištění fungování CSIRT.
   a. Vytvoření pracovních postupů
   b. Zavedení nástrojů CSIRT
9. Výcvik vašich pracovníků

>> Další krok je procvičování a připravenost na skutečnou práci!

Tato kapitola popisuje pro ilustraci vzorové cvičení na každodenní úkoly CSIRT: vytvoření odborné rady v bezpečnosti.

Podnětem byla následující původní odborná rada v bezpečnosti rozeslaná Microsoftem:

Identifikátor bulletinu	**Bulletin Microsoftu o bezpečnosti MS06-042**
Název bulletinu	**Cumulative Security Update for Internet Explorer (918899)** (Rozšířená aktualizace bezpečnosti pro Internet Explorer (918899)
Celkové shrnutí	Tato aktualizace řeší různou zranitelnost ve webovém prohlížeči Internet Explorer, která by mohla umožnit provádění dálkového kódování.
Nejvyšší hodnocení závažnosti	Critical (Rozhodující)
Dopad zranitelnosti	Provádění dálkového kódování
Dotčený software	**Windows, Internet Explorer.** Více informací viz část Dotčený software a adresy pro stažení

Tento bulletin prodejce se zabývá zranitelností webového prohlížeče Internet Explorer zjištěné v poslední době. Prodejce uveřejňuje mnohé opravné balíčky tohoto softwaru pro četné verze Microsoft Windows.

Po obdržení těchto informací o zranitelnosti prostřednictvím adresáře začíná fiktivní CSIRT s pracovním postupem popsaným v kapitole *8.2 Vytváření výstrah, varování a oznámení.*

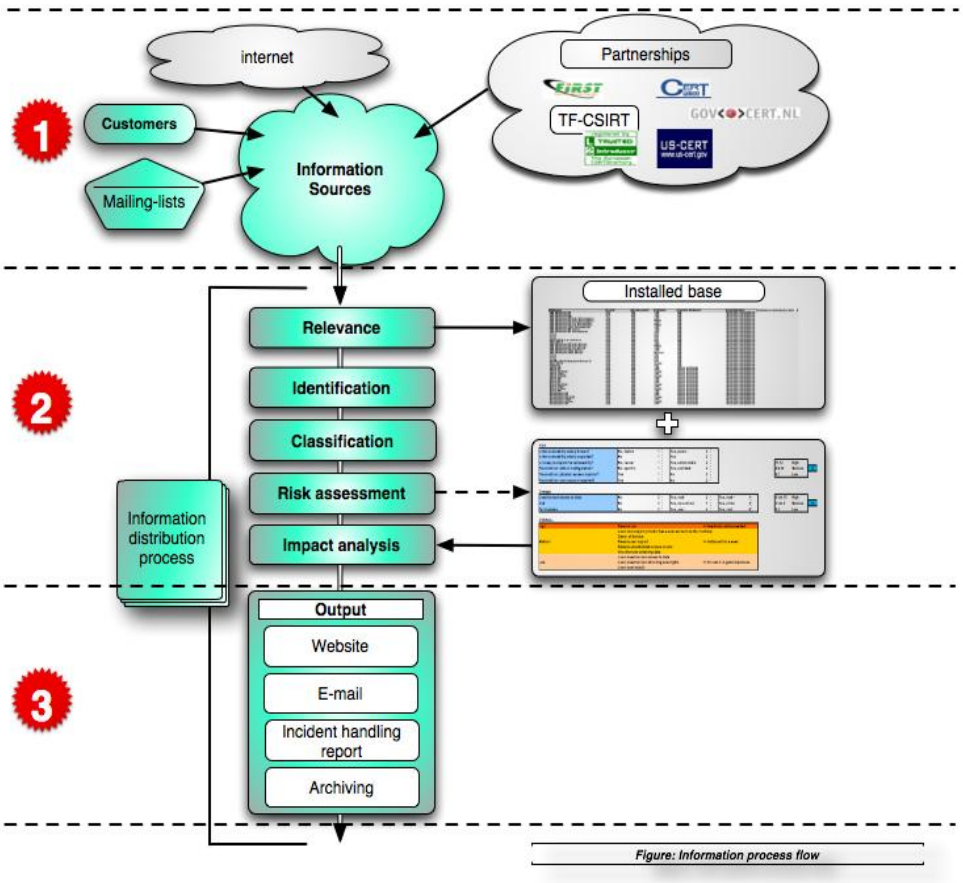


Figure: Information process flow

1. krok: Sběr informací o zranitelnosti.

První krok je prohlížení webové stránky prodejce. Fiktivní CSIRT ověřuje autentičnost informací a shromažďuje další podrobnosti o zranitelnosti a o dotčených systémech IT.

2. krok: Hodnocení informací a rizika

Identifikace
Informace už byly ověřeny křížovou kontrolou informací o zranitelnosti obdržených elektronickou poštou s textem na webové stránce prodejce.

Závažnost
Fiktivní CSIRT kontroluje seznam dotčených systémů nalezený na webové stránce se seznamem systémů používaných ve složce. Zjistí, že nejméně jedna z jeho složek používá Internet Explorer, takže informace o zranitelnosti jsou skutečně relevantní.

Kategorie	Aplikace	Produkt softwaru	Verze	Operační systém	Verze operačního systému	Složka
Desktop	Prohlížeč	Internet Explorer	x-x-	Microsoft	XP-prof	A

Klasifikace
Informace jsou veřejné, lze je tedy používat a znovu distribuovat.

Hodnocení rizika a analýza dopadů
Zodpovězení otázek ukazuje, že riziko a dopad jsou *velké* (hodnocené Microsoftem jako *rozhodující).*

RIZIKO

Je zranitelnost dobře známá?	Ano
Je zranitelnost značně rozšířená?	Ano
Je snadné zranitelnost zneužít?	Ano
Je zranitelnost zneužitelná na dálku?	Ano

ŠKODA
Možnými dopady jsou vzdálená dostupnost a potencionální provádění dálkového kódování. Tato zranitelnost zahrnuje mnohočetné problémy, které způsobují, že riziko škody je *vysoké*.

3. krok: Distribuce

Fiktivní CSIRT je interní CSIRT. Jako komunikační kanály má k dispozici elektronickou poštu, telefon a interní webovou stránku. CSIRT vydává tuto odbornou radu odvozenou ze šablony z kapitoly *8.2 Vytváření výstrah, varování a oznámení.*

Název odborné rady
Mnohočetná zranitelnost zjištěna v Internet Explorer

Referenční číslo
082006-1

Dotčené systémy

- Všechny systémy desktopu, které používá Microsoft

Související operační systém + verze

- Microsoft Windows 2000, 4. opravný balíček
- Microsoft Windows XP, 1. opravný balíček a Microsoft Windows XP, 2. opravný balíček
- Microsoft Windows XP Professional, vydání x64
- Microsoft Windows Server 2003 a Microsoft Windows Server 2003, 1. opravný balíček
- Microsoft Windows Server 2003 pro systémy založené na Itaniu a Microsoft Windows Server 2003 s 1. opravným balíčkem – SP1 *(Service Pack 1)* pro systémy založené na Itaniu
- Microsoft Windows Server 2003, vydání x64

Riziko (Vysoké—Střední – Nízké)
VELKÉ

Dopad/potenciální škoda (Velký – Střední – Malý)
VELKÝ

Vnější identifikace: (CVE, Identifikace bulletinu o zranitelnosti)
MS-06-42

Přehled o zranitelnosti
Microsoft zjistil několik závažných zranitelností v prohlížeči Internet Explorer, které mohou vést k provádění dálkového kódování.

Dopad
Narušitel by mohl převzít úplnou kontrolu nad systémem, instalovat programy, doplňovat uživatele a osoby a měnit nebo mazat data. Zmiňujícím faktorem je to, že k výše uvedenému může dojít, když se uživatel přihlásí pouze s právy správce. Dopad na uživatele přihlášené s několika právy by mohl být menší.

Řešení
Nainstalujte ihned opravný balíček na svůj Internet Explorer (IE).

Popis (podrobnosti)
Více informací viz ms06-042.mspx

Příloha
Více informací viz ms06-042.mspx

Tento výstup je teď připraven k rozeslání. Protože je to důležitý bulletin, doporučuje se také zavolat složky, když je to možné.

Fiktivní CSIRT (10. krok)
Cvičení Během prvních týdnů práce použil fiktivní CSIRT několik fiktivních případů (obdržené jako příklady od jitých týmů CSIRT), které se použily jako cvičení. Kromě toho vydal několik odborných rad k bezpečnosti vycházejících z informací o skutečné zranitelnosti rozesílaných prodejci hardwaru a softwaru, které doladil a přizpůsobil potřebám složky.

11 Závěr

Tady návod končí. Dokument, který je k dispozici, je určen k poskytnutí velmi stručného přehledu o různých procesech nutných k vytvoření CSIRT. Nečiní si nárok být úplný, ani příliš nezachází do konkrétních podrobností. Literaturu o této problematice, která si zasluhuje přečíst, viz část *A.1 Další výklad.*

Dalšími důležitými kroky pro fiktivní CSIRT by teď bylo:

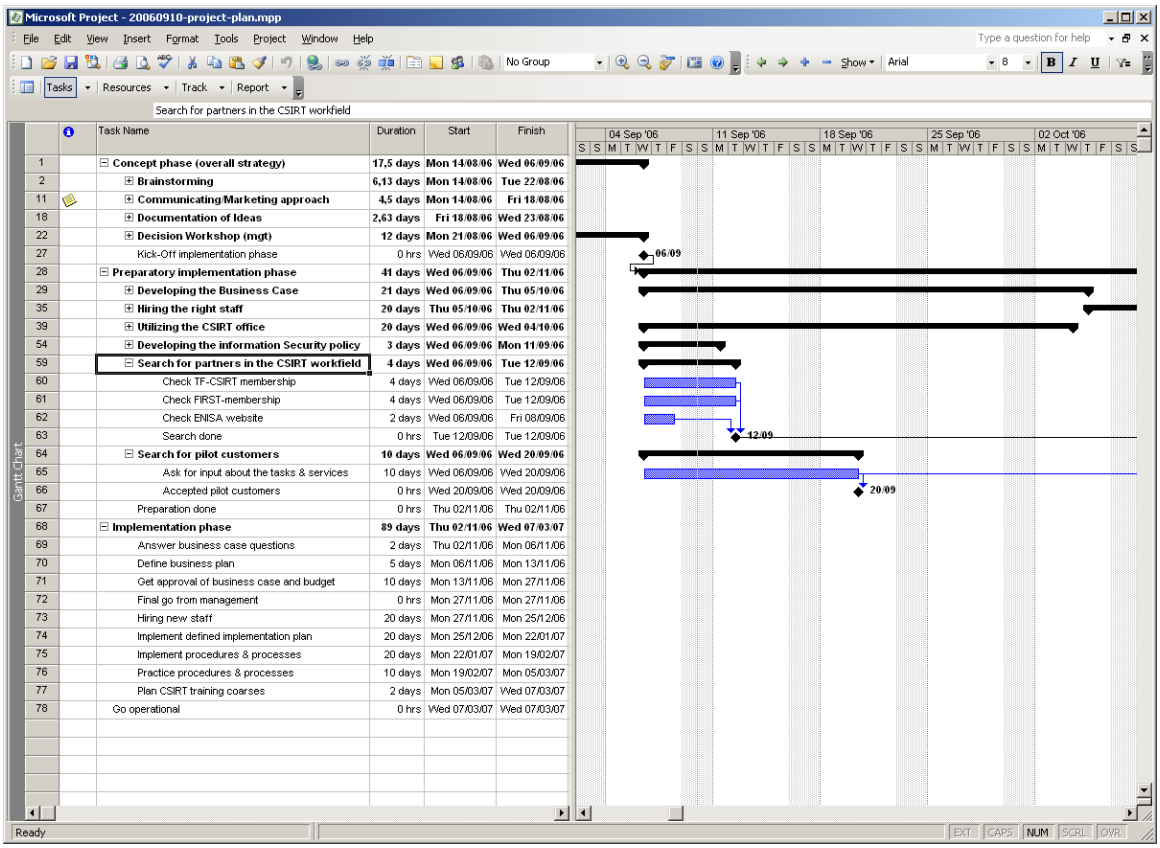
- Obdržet zpětnou vazbu od složky za účelem doladění poskytovaných služeb.
- Získat rutinu v každodenní práci.
- Procvičit si nouzové stavy.
- Zůstat ve styku s různými skupinami CSIRT s cílem přispět jednou k jejich dobrovolné práci.

12 Popis plánu projektu

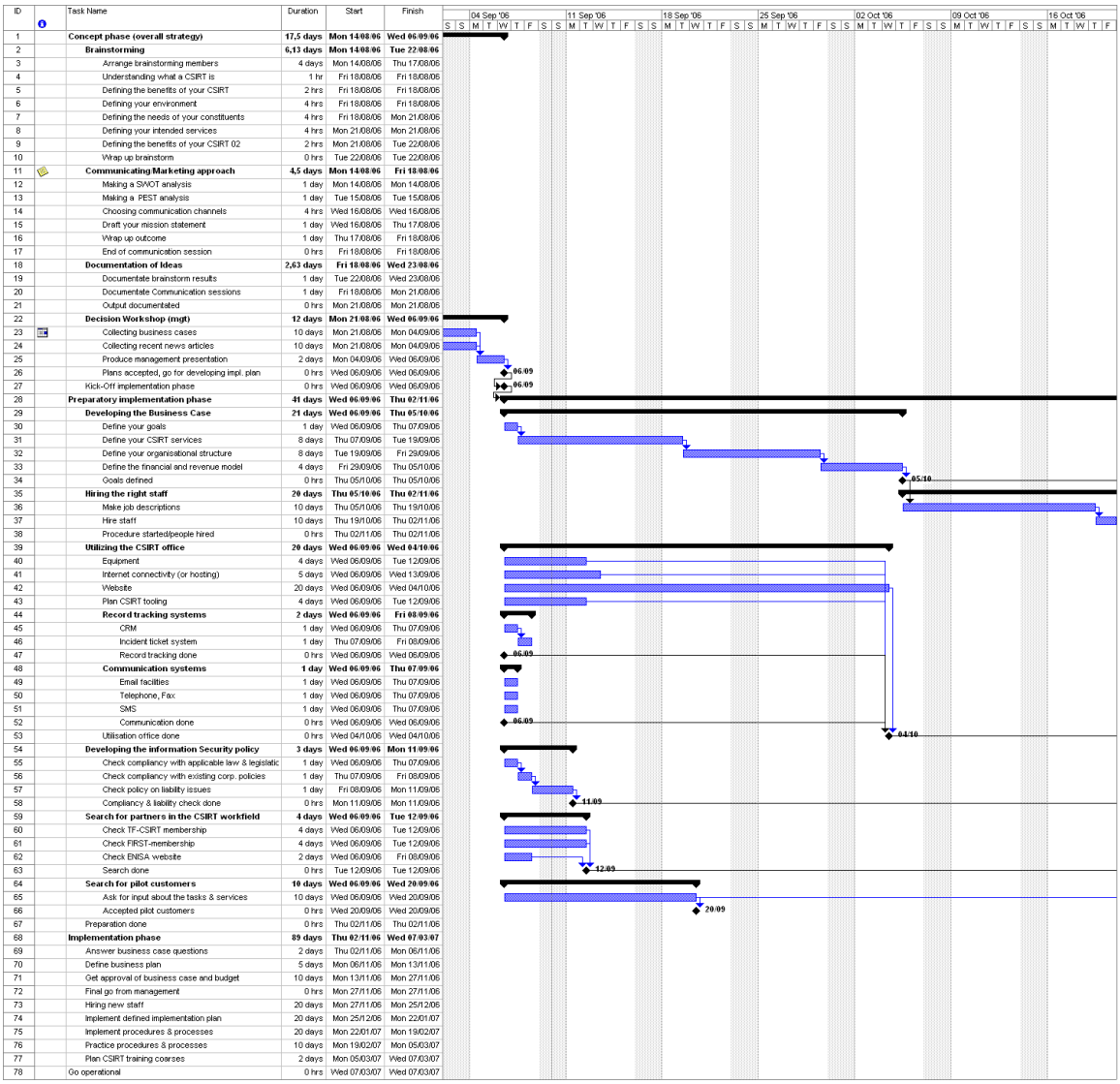
POZNÁMKA: Plán projektu je první odhad potřebného času. V závislosti na dostupných zdrojích může být skutečné trvání projektu různé.

Plán projektu je k dispozici v různých formátech na CD a na webové stránce agentury ENISA. Plně pokrývá všechny procesy popsané v tomto dokumentu.

Hlavní formát bude Microsoft Project, může se tedy přímo použít v tomto nástroji řízení projektu.



Obr. 17 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 coarses	2 days	Mon 05/03/07	Wed 07/03/07
78	Go operational	0 hrs	Wed 07/03/07	Wed 07/03/07

Obr. 18 Plán projektu se všemi úkoly a jedna část Ganttova diagramu

Plán projektu je k dispozici rovněž ve formátu CVS a XML. Další použití si lze vyžádat od expertů CSIRT agentury ENISA: CERT-Relations@enisa.europa.eu

PŘÍLOHA

A.1 Další výklad

Příručka pro týmy CSIRT (CERT/CC)
Velmi podrobné dílo s odkazy na všechny otázky týkající se práce CSIRT.
Zdroj: http://www.cert.org/archive/pdf/csirt-handbook.pdf

Stanovení procesů řízení bezpečnostních incidentů pro týmy CSIRT: Probíhající práce
Hloubková analýza řízení bezpečnostních incidentů
Zdroj: http://www.cert.org/archive/pdf/04tr015.pdf

Stav praxe týmů pro reakci na bezpečnostní incidenty počítačů – CSIRT *(Computer Security Incident Response Teams)*.
Komplexní analýza aktuální situace týkající se celosvětového obrazu CSIRT, včetně minulosti, statistických přehledů a mnohých dalších otázek.
Zdroj: http://www.cert.org/archive/pdf/03tr001.pdf

CERT v rámečku
Úplný popis poučení získaného z vytváření GOVCERT.NL a 'De Waarschuwingsdienst', holandské státní služby pro vydávání výstrah.
Zdroj: http://www.govcert.nl/render.html?it=69

RFC 2350: Očekávání od reakce na bezpečnostní incidenty počítačů.
Zdroj: http://www.ietf.org/rfc/rfc2350.txt

Příručka pro řešení bezpečnostních incidentů počítačů amerického Národního technického a normalizačního úřadu – NIST *(National Institute of Standard and Technology)*[37]
Zdroj: http://www.securityunit.com/publications/sp800-61.pdf

Soupis agentury ENISA týkající se činností CERT v Evropě
Příručka, která uvádí informace o týmech CSIRT v Evropě a jejich různé aktivity
Zdroj: http://www.enisa.europa.eu/ENISA%20CERT/index.htm

[37] NIST: Národní technický a normalizační úřad *(National Institute of Standard and Technology)*

A.2 Služby CSIRT

Zvláštní poděkování patří CERT/CC, který poskytl tento seznam.

Reactive Services	Proactive Services	Artifact Handling
• Alerts and Warnings • Incident Handling • Incident analysis • Incident response on site • Incident response support • Incident response coordination • Vulnerability Handling • Vulnerability analysis • Vulnerability response • Vulnerability response coordination	• Announcements • Technology Watch • Security Audits or Assessments • Configuration and Maintenance of Security • Development of Security Tools • Intrusion Detection Services • Security-Related Information Dissemination	• Artifact analysis • Artifact response • Artifact response coordination **Security Quality Management** • Risk Analysis • Business Continuity and Disaster Recovery • Security Consulting • Awareness Building • Education/Training • Product Evaluation or Certification

Reaktivní služby	Aktivní služby	Zacházení s artefakty
• Výstrahy a varování • Řešení bezpečnostních incidentů • Analýza bezpečnostních incidentů • Podpora reakce na bezpečnostní incidenty • Koordinace reakcí na bezpečnostní incidenty • Reakce na bezpečnostní incidenty na místě • Řešení zranitelnosti • Analýza zranitelnosti • Reakce na zranitelnost • Koordinace reakcí na zranitelnost	• **Oznámení** • Sledování techniky • Audity nebo hodnocení bezpečnosti • Konfigurace a udržování bezpečnosti • Vývoj nástrojů bezpečnosti • Služby detekce narušení • Šíření informací týkajících se bezpečnosti	• Analýza artefaktů • Reakce na artefakty • Koordinace reakcí na artefakty **Management jakosti bezpečnosti** • Analýza rizik • Kontinuita obchodu a obnovení provozu po havárii • Poradenství v bezpečnosti • Vytváření povědomí • Vzdělávání/výcvik • Hodnocení nebo certifikace produktů

Obr. 19 Seznam služeb CSIRT od CERT/CC

Popis služeb

Reaktivní služby

Reaktivní služby jsou určeny k reakci na žádosti o pomoc, pro zprávy o bezpečnostních incidentech ze složky CSIRT a pro jakékoli ohrožení systémů CSIRT nebo útoky na ně.

Některé služby mohou být iniciovány oznámením třetí strany nebo sledováním monitoringu nebo soubory log systému detekce napadení – IDS *(Intrusion Detection System)* a výstrahami.

Výstrahy a varování

Tato služba zahrnuje šíření informací, které popisují útok narušitele, zranitelnost bezpečnosti, výstrahu narušení, počítačový virus nebo mystifikující zprávu a zajištění každého krátkodobého doporučeného postupu jednání pro řešení vyplývajícího problému. Výstraha, varování nebo odborná rada se zasílá jako reakce na aktuální problém, aby se složkám oznámila aktivita a poskytl návod na ochranu jejich systémů nebo na obnovu všech systémů, které byly postiženy. Informace může vytvořit CSIRT nebo je mohou opětovně rozeslat prodejci, jiné týmy CSIRT nebo experti na bezpečnost či ostatní částí složky.

Řešení bezpečnostních incidentů

Řešení bezpečnostních incidentů zahrnuje obdržení a třídění žádostí a zpráv a odpověď na ně a analyzování bezpečnostních incidentů a událostí. Konkrétní činnosti reakce mohou zahrnovat

- přijímání opatření na ochranu systémů a sítí postižených nebo ohrožených rušivou činností
- poskytnutí řešení a poskytnutí strategií zmírnění na základě příslušných odborných rad nebo výstrah
- pátrání po činnosti narušitelů na jiných částech sítě
- filtrování provozu na síti
- systémy přestavby
- systémy záplatování nebo oprav
- zpracování jiných strategií reakce nebo strategií dočasných opravných balíčků *(workarounds).*

Protože činnosti řešení bezpečnostních incidentů vykonávají různé typy týmů CSIRT rozličnými způsoby, tyto služby se dále kategorizují na základě druhu vykonávaných činností a typu poskytované pomoci takto:

Analýza bezpečnostního incidentu

Existuje mnoho úrovní analýzy bezpečnostních incidentů a mnoho dílčích služeb. Analýza bezpečnostních incidentů je v podstatě zkouška všech dostupných informací a podpůrný důkaz nebo artefakt týkající se bezpečnostního incidentu nebo události. Účelem analýzy je identifikovat rozsah bezpečnostního incidentu, rozsah škody způsobené bezpečnostním incidentem, povahu bezpečnostního incidentu a dostupné strategie reakce nebo dočasné opravné balíčky *(workarounds)*. CSIRT může používat výsledky zranitelnosti a analýzu artefaktů (popsanou níže) k pochopení a zajištění komplexnější a aktuálnější analýzy toho, co se v konkrétním systému stalo. CSIRT uvádí do souladu činnost napříč bezpečnostními incidenty, aby určil jakékoli vzájemné vztahy, trendy, vzorce chování nebo podpisy narušitelů. Dvě dílčí služby, které lze provádět jako součást analýzy bezpečnostních incidentů v závislosti na poslání, cílech a procesech CSIRT, jsou

Shromažďování soudních důkazů

Shromažďování, uchovávání, dokumentování a analyzování důkazů z ohrozeného počítačového systému za účelem určení změn systému a pomoci v rekonstrukci událostí vedoucích k ohrožení. Toto shromažďování informací a důkazů se musí uskutečňovat způsobem, který dokumentuje prokazatelný řetězec péče přípustný u soudu podle pravidel dokazování. Úkoly, které se týkají shromažďování soudních důkazů, zahrnují (kromě jiného) vyhotovení kopie bitmapového obrázku pevného disku dotčeného systému; kontrolu změn systému jako nové programy, soubory, služby a uživatelé; prohlížení probíhajících procesů a otevřených portů; a kontrolu programů trojského koně a sad nástrojů. Pracovníci CSIRT, kteří vykonávají tuto funkci, se mohou také připravit na to, že budou vystupovat jako znalečtí svědci v soudních jednáních.

Pátrání nebo sledování

Sledování původů narušitele nebo identifikace systémů, ke kterým měl narušitel přístup. Tato činnost může zahrnovat pátrání nebo sledování, jak narušitel vstoupil do dotčených systémů a souvisejících sítí, které systémy byly použity k získání tohoto přístupu, kde měl útok původ a jaké jiné systémy a sítě byly použity jako součást útoku. Může to rovněž zahrnovat snahu určit totožnost narušitele. Tuto práci může někdo udělat sám, ale obvykle ji vykonávají pracovníci pro vynucení práva, provozovatelé internetových služeb nebo jiné zainteresované organizace.

Reakce na bezpečnostní incident na místě

CSIRT poskytuje přímou pomoc na místě, aby pomohl složkám zotavit se z bezpečnostního incidentu. CSIRT sám fyzicky analyzuje postižené systémy a provádí opravu a obnovení systémů a neposkytuje podporu v reakci na bezpečnostní incident pouze telefonicky nebo elektronickou poštou (viz níže). Tato služba zahrnuje veškerá opatření učiněna na místní úrovni, která jsou nutná, když je podezření na bezpečnostní incident, nebo když k němu dojde. Nenachází-li se CSIRT na dotčeném místě, členové týmu by cestovali na toto místo a zajistili by reakci. V jiných případech může být místní tým už na místě a zajišťovat reakci na bezpečnostní incident jako součást své rutinní práce. Platí to zejména, když řešení bezpečnostního incidentu nezabezpečuje vytvořený CSIRT, ale zajišťuje se jako součást běžného pracovního fungování systému, sítě nebo správců bezpečnosti.

Podpora reakce na bezpečnostní incidenty

CSIRT pomáhá oběti (obětem) a vede oběť (oběti) útoku v zotavení se z bezpečnostního incidentu za pomoci telefonu, elektronické pošty, faxu nebo dokumentace. Může to zahrnovat technickou pomoc ve výkladu shromážděných údajů, poskytování kontaktních informací nebo předání návodu na zmírnění a strategií obnovy. Nezahrnuje to přímá opatření týkající se reakce na bezpečnostní incident na místě, jak je to popsáno níže. CSIRT namísto toho poskytuje návod na dálku, takže pracovníci působící na místě mohou uskutečnit obnovu sami.

Koordinace reakcí na bezpečnostní incidenty

CSIRT koordinuje snahy o reakci mezi stranami, kterých se bezpečnostní incident týká. Obvykle to zahrnuje oběť útoku, jiná místa, kterých se útok týká, a všechna místa, která žádají o pomoc v analyzování útoku. Může to rovněž zahrnovat strany, které poskytují

podporu IT pro oběť, jako jsou provozovatelé služeb Internetu, jiné týmy CSIRT a správci systémů a sítí na místě. Koordinační práce může obsahovat sběr kontaktních informací, oznámení místům o jejich možném postižení (jako oběť nebo zdroj útoku), sběr statistických údajů o počtu postižených míst a usnadňování výměny a analýzy informací. Část koordinační práce může obsahovat oznamování a spolupráci s právním poradcem organizace, s odděleními pro lidské zdroje nebo s oddělením pro styk s veřejností. Mohla by rovněž obsahovat koordinaci s vynucováním práva. Tyto služby nezahrnují přímou reakci na bezpečnostní incident na místě.

Řešení zranitelnosti

Řešení zranitelnosti zahrnuje přijímání informací a zpráv o zranitelnosti hardwaru a softwaru; analyzování povahy, mechanizmů a dopadů zranitelnosti; a zpracování strategií reakce pro detekci a opravu zranitelnosti. Protože činnosti řešení zranitelnosti realizují různé typy týmů CSIRT rozličnými způsoby, tyto služby se dále dělí do kategorií na základě druhu vykonávaných činností a typu poskytované pomoci takto:

Analýza zranitelnosti

CSIRT uskutečňuje technickou analýzu a kontrolu zranitelnosti v hardwaru nebo v softwaru. Zahrnuje to ověření podezřelé zranitelnosti a technickou kontrolu zranitelnosti hardwaru nebo softwaru, aby se určilo, kde se zranitelnost nachází, a jak může být zneužita. Analýza může zahrnovat přezkoumáni zdrojového kódu, použití ladícího programu k určení, kde se zranitelnost vyskytuje, nebo snahu o zkopírování problémů na testovací systém.

Reakce na zranitelnost

Tato služba zahrnuje určení vhodné reakce pro zmírnění nebo opravu zranitelnosti. Může se to týkat vývoje průzkumných opravných balíčků, záplat a dočasných opravných balíčků *(workarounds)*. Zahrnuje rovněž oznamování zmírňující strategie pro jiné subjekty, třeba vytvářením a rozesíláním odborných rad nebo výstrah. Tato služba může obsahovat zajišťování reakce instalováním záplat, opravných balíčků nebo dočasných opravných balíčků.

Koordinace reakcí na zranitelnost

CSIRT oznamuje zranitelnost různým částem podniku nebo složky a sdílí informace o tom, jak rychle opravit (záplatovat) nebo zmírnit zranitelnost. CSIRT ověřuje, zda je strategie reakce na zranitelnost úspěšně realizována. Tato služba může zahrnovat komunikaci s prodejci, jinými týmy CSIRT, technickými odborníky, pracovníky složky a s jednotlivci nebo skupinami, kteří zranitelnost původně odhalili nebo nahlásili. Činnosti se týkají usnadnění analýzy zranitelnosti nebo zprávy o zranitelnosti; koordinace časových harmonogramů uvolnění odpovídajících dokumentů, opravných balíčků nebo dočasných opravných balíčků; a syntézy odborné analýzy uskutečněné různými stranami. Tato služba může také zahrnovat udržování veřejného nebo soukromého archivu nebo bázi znalostí informací o zranitelnosti a odpovídajících strategií reakce.

Řešení artefaktů

Artefakt je jakýkoli soubor nebo objekt zjištěný v systému, který by mohl být zapojen do průzkumu systémů a sítí nebo do útoku na ně, nebo který se používá ke zmaření

bezpečnostních opatření. Artefakty mohou kromě jiného obsahovat počítačové viry, programy trojského koně, červy, využívat skripty a sady nástrojů.

Zacházení s artefakty zahrnuje přijímání informací o artefaktech a jejich kopií, které se používají v útocích narušitelů, v průzkumu a v jiných nepovolených nebo rušivých aktivitách. Když už se artefakt přijme, přezkoumá se. Zahrnuje to analyzování povahy, mechanismů, verze a používání artefaktů; a zpracování (nebo navržení) strategií reakce za účelem detekce a odstranění artefaktů a obrany proti nim. Protože aktivity řešení artefaktů realizují různé typy týmů CSIRT rozličnými způsoby, tyto služby se dále dělí do kategorií na základě druhu vykonávaných činností a typu poskytované pomoci takto:

Analýza artefaktů

CSIRT vykonává technickou kontrolu a analýzu každého artefaktu zjištěného v systému. Uskutečněna analýza může obsahovat identifikaci druhu souboru a struktury artefaktu, porovnání nového artefaktu s existujícími artefakty nebo s jinými verzemi téhož artefaktu, aby se zjistily podobnosti a rozdíly, nebo reverzní (zpětné) inženýrství nebo kód pro rozložení za účelem zjištění účelu a funkce artefaktu.

Reakce na artefakt

Tato služba zahrnuje určení příslušných činností pro detekci a odstranění artefaktů ze systému a také činností pro zamezení instalace artefaktů. Může se to týkat vytvoření podpisů, které lze doplnit do antivirového softwaru nebo IDS.

Koordinace reakcí na artefakt

Tato služba zahrnuje sdílení a syntézu výsledků analýzy a strategie reakce týkající se artefaktu s jinými řešiteli, týmy CSIRT, prodejci a ostatními bezpečnostními experty. Činnosti se týkají sdělování technické analýzy z různých zdrojů jiným subjektům a její syntézu. Činnosti mohou také obsahovat udržování veřejného archívu nebo archivu složky se známými artefakty a jejich dopadem a odpovídajícími strategiemi rekce.

Aktivní služby

Aktivní služby jsou určeny ke zlepšení infrastruktury a procesů bezpečnosti složky před výskytem nebo detekcí bezpečnostního incidentu. Hlavním cílem je zamezit bezpečnostním incidentům a snížit jejich dopad a rozsah, když k nim dojde.

Oznámení

Zahrnuje to kromě jiného výstrahy k narušení, varování před zranitelností a odborné rady v bezpečnosti. Tato oznámení informují složky o novém vývoji se střednědobým a dlouhodobým dopadem, jako je nově zjištěna zranitelnost nebo nástroje narušitele. Oznámení umožňují složkám chránit své systémy a sítě před nově zjištěnými problémy dřív, než mohou být použity.

Sledování techniky

CSIRT monitoruje a sleduje nový technický rozvoj a aktivity narušitelů a související trendy, aby pomohl identifikovat budoucí hrozby. Posuzované otázky lze rozšířit o právní a legislativní předpisy, sociální nebo politické hrozby a vznikající technologie. Tyto služby zahrnují čtení bezpečnostních adresářů, bezpečnostních webových stránek a aktuálních článků v novinách a časopisech z oblasti vědy, techniky, politik a vlády

s cílem vybrat informace týkající se bezpečnosti systémů a sítí složek. Může to zahrnovat komunikaci s jinými stranami, které jsou řídícími orgány v této oblasti, aby se zajistilo, že se získají nejlepší a nejpřesnější informace nebo výklad. Výsledkem těchto služeb by mohl být určitý druh oznámení, návodů nebo doporučení zaměřených na střednědobější až dlouhodobé otázky bezpečnosti.

Audity nebo hodnocení bezpečnosti

Tyto služby zajišťují podrobné přezkoumání a analýzu bezpečnostní infrastruktury organizace na základě požadavků stanovených organizací nebo jinými odvětvovými normami, které se aplikuji. Může to také zahrnovat přezkoumání bezpečnostních praktik organizace. Existuje mnoho různých druhů auditů nebo hodnocení, které lze poskytnout, včetně

Přezkoumání infrastruktury

Manuální přezkoumání konfigurace hardwaru a softwaru, směrovačů, firewallů, serverů a přístrojů desktopu, aby se zajistilo, že budou odpovídat nejlepší praxi v bezpečnostních politikách organizace nebo odvětví a standardním konfiguracím.

Přezkoumání nejlepší praxe

Rozhovory se zaměstnanci a správci systémů a sítí, aby se zjistilo, zda jejich bezpečnostní praktiky odpovídají stanovené bezpečnostní politice organizace nebo některým normám specifickým pro dané odvětví.

Skenování

Využití skenerů zranitelnosti nebo virů za účelem zjištění, které systémy a sítě jsou zranitelné.

Penetrační testování

Zkouška bezpečnosti na místě účelovým útokem na jeho systémy a sítě.
Před uskutečněním těchto auditů nebo hodnocení je nutné získat souhlas vyššího vedení. Některé z těchto metod mohou být v politice organizace zakázané. Poskytování těchto služeb může zahrnovat zpracování společného souboru praktik, podle kterých se uskutečňují zkoušky nebo hodnocení, spolu s rozvojem potřebného souboru schopností nebo požadavků na certifikaci pracovníků, kteří vykonávají zkoušky, hodnocení, audity nebo přezkoumání. Tyto služby lze rovněž zadat dodavateli třetí strany nebo poskytovateli řízených bezpečnostních služeb, který má příslušné odborné znalosti ve vykonávání auditů a hodnocení.

Konfigurace a udržování nástrojů, aplikací, infrastruktur a služeb bezpečnosti

Tyto služby určují a dávají příslušný návod, jak bezpečně nastavit a udržovat nástroje, aplikace a celkovou počítačovou infrastrukturu, kterou používá tým CSIRT složky nebo samotný CSIRT. Kromě poskytnutí návodu může CSIRT provádět aktualizace konfigurace a údržbu nástrojů a služeb bezpečnosti jako IDS, systémy skenování nebo monitorování sítě, filtry, obtékání *(wrappers)*, bezpečnostní rozhraní *(firewall)*, virtuální privátní sítě – VPN *(Virtual Private Network)* nebo mechanismy ověření správnosti záznamů. CSIRT může dokonce poskytovat tyto služby jako součást své hlavní funkce. CSIRT může také nastavovat a udržovat servery, desktopy, laptopy, osobní digitální asistenty – PDA *(Personál Digital Assistants)* a jiná bezdrátová zařízení podle směrnic

o bezpečnosti. Tyto služby zahrnují předložení všech otázek nebo problémů s konfigurací členům vedení nebo používání nástrojů a aplikací, o nichž je CSIRT přesvědčen, že by mohly ponechat systém zranitelný pro útok.

Vývoj nástrojů bezpečnosti

Tato služba zahrnuje zpracování všech nových nástrojů specifických pro složku, které požaduje nebo chce složka či samotný CSIRT. Může to například zahrnovat zpracování bezpečnostních opravných balíčků pro software přizpůsobený daným potřebám, který používá složka, nebo zajištěné distribuce softwaru, který lze použít k obnově narušených hostitelů. Může rovněž zahrnovat vývoj nástrojů nebo skriptů, které rozšiřují funkčnost existujících nástrojů bezpečnosti jako nové zásuvné moduly (plug-in) pro skener zranitelnosti nebo skener sítě, skripty, které usnadňují používání šifrovací techniky nebo mechanismy automatizované distribuce opravných balíčků.

Služby detekce narušení

Týmy CSIRT, které vykonávají tyto služby, přezkoumávají existující soubory log IDS, analyzují a iniciují reakci na všechny události, které splňují stanovenou prahovou hodnotu, nebo posílají výstrahy podle smlouvy o úrovni předem definovaných služeb. Detekce a analýza napadení souvisejících bezpečnostních souborů log může být nelehký úkol – nejenom v určení, kam v prostředí umístit snímač, ale i ve sběru a pak v analyzování velkého množství získaných údajů. V mnoha případech jsou nutné specializované nástroje nebo odborné znalosti ke shrnutí a výkladu informací za účelem identifikace falešných poplachů, útoků nebo událostí na síti a realizace strategie pro vyloučení nebo minimalizování těchto událostí. Některé organizace se rozhodnou zadat tuto činnost někomu jinému, kdo má více odborných znalostí v poskytování těchto služeb, jako jsou poskytovatelé řízených bezpečnostních služeb.

Šíření informací týkajících se bezpečnosti

Tyto služby poskytují složkám komplexní soubor užitečných informací, které lze snadno najít, a které pomáhají zvýšit bezpečnost. Tyto informace mohou obsahovat

- návody pro podávání zpráv a kontaktní informace pro CSIRT
- archivy výstrah, varování a jiných oznámení
- dokumentaci o současných nejlepších praktikách
- všeobecné návody k počítačové bezpečnosti
- politiky, postupy a kontrolní seznamy
- zpracování opravných balíčků a informací o distribuci
- spojení s prodejci
- aktuální statistické přehledy a trendy v hlášení bezpečnostních incidentů
- jiné informace, které mohou celkově zlepšit bezpečnostní praktiky.

Informace může zpracovávat a zveřejňovat CSIRT nebo jiná část organizace (IT, lidské zdroje nebo oddělení pro styk s médii) a mohou obsahovat údaje z vnějších zdrojů, jako jsou jiné týmy CSIRT, prodejci a bezpečnostní experti.

Služby managementu jakosti bezpečnosti

Služby, které spadají do této kategorie, nejsou specifické především pro řešení bezpečnostních incidentů nebo pro CSIRT. Jsou to dobře známé, zavedené služby určené ke zvýšení celkové bezpečnosti organizace. Zásluhou zkušeností získaných v poskytování reaktivních a aktivních služeb popsaných výše může CSIRT vnést

jedinečná hlediska do těchto služeb managementu jakosti, která by jinak nemusela být dostupná. Tyto služby jsou určeny k začlenění zpětné vazby a získaného poučení na základě znalostí nabytých reagováním na bezpečnostní incidenty a na zranitelnost a útoky. Zahrnutí těchto zkušeností do zavedených tradičních služeb (popsaných níže) jako součásti procesu managementu jakosti bezpečnosti může zvýšit dlouhodobé úsilí v organizaci zaměřené na bezpečnost. V závislosti na strukturách a odpovědnostech organizace může tým CSIRT tyto služby poskytovat nebo se může podílet na činnosti širšího týmu organizace.
Následující popisy vysvětlují, jak mohou být odborné znalosti CSIRT prospěšné pro každou z těchto služeb managementu jakosti bezpečnosti.

Analýza rizika

CSIRT může přidat hodnotu k analýze a hodnocení rizika. Může to zvýšit schopnost organizace hodnotit skutečné hrozby, aby se zajistila realistická kvalitativní a kvantitativní hodnocení rizik pro informační jmění a hodnocení strategií bezpečnosti a reakce. Týmy CSIRT, které zajišťují tyto služby, by uskutečňovaly analýzu rizika bezpečnosti informací u nových systémů a podnikatelských procesů, nebo by u nich pomáhaly, nebo by hodnotily hrozby a útoky na majetek a systémy složek.

Kontinuita podnikání a plánování obnovy po havárii

Na základě výskytů bezpečnostních incidentů v minulosti a budoucích předpovědí vznikajícího bezpečnostního incidentu nebo trendů bezpečnosti může čím dál tím více bezpečnostních incidentů mít za následek znehodnocení obchodních operací. Proto by se v činnostech plánování mělo přihlížet ke zkušenostem a doporučením CSIRT týkajícím se určení, jak nejlépe reagovat na tyto bezpečnostní incidenty, aby se zajistila kontinuita obchodních operací. Týmy CSIRT, které vykonávají tyto služby, jsou zapojeny do souvislého podnikání a do plánování obnovy po havárii u událostí souvisejících s hrozbami v bezpečnosti počítačů a s útoky na ně.

Poradenství v bezpečnosti

CSIRT lze využít k poskytování rady a návodu k nejlepším praktikám v bezpečnosti za účelem realizace obchodních operací složek. CSIRT zajišťující tyto služby se účastní zpracování doporučení nebo stanovení požadavků na nakupování, instalaci nebo zajištění nových systémů, zařízení sítě, aplikace softwaru nebo celopodnikové podnikatelské procesy. Tyto služby zahrnují poskytování návodu a pomoci ve zpracování politik organizace nebo složky týkajících se bezpečnosti. Mohou také zahrnovat poskytování svědectví nebo poradenství pro legislativní nebo jiné státní orgány.

Vytváření povědomí

Týmy CSIRT mohou identifikovat, kde složky potřebují více informací a pokynů, aby lépe splňovaly přijaté bezpečnostní praktiky a politiky organizace týkající se bezpečnosti. Zvyšování celkového povědomí lidí ze složky o bezpečnosti nejenom zlepšuje jejich chápání otázek bezpečnosti, ale pomáhá jim také vykonávat každodenní operace bezpečnějším způsobem. Může to snížit výskyt úspěšných útoků a zvýšit pravděpodobnost, že složky zjistí a ohlásí útoky a tím sníží doby obnovy a vyloučí nebo budou minimalizovat ztráty.

Týmy CSIRT, které zabezpečují tyto služby, vyhledávají příležitosti zvýšit povědomí o bezpečnosti zpracováním článků, plakátů, informačních bulletinů, webových stránek nebo jiných informačních zdrojů, které vysvětlují nejlepší praktiky v bezpečnosti a poskytují odborné rady nebo bezpečnostní opatření, která se mají učinit. Aktivity mohou také obsahovat časové plánování porad a seminářů, aby se udržovala aktuální informovanost složek o probíhajících postupech bezpečnosti a o potenciálních hrozbách pro systémy organizace.

Vzdělávání/výcvik

Tyto služby zahrnují poskytování informací složkám o otázkách bezpečnosti počítačů za pomoci školení, seminářů, kurzů a cvičení. Otázky mohou obsahovat pokyny k hlášení bezpečnostních incidentů, vhodné metody reakce, nástroje reakce na bezpečnostní incidenty, metody prevence bezpečnostních incidentů a jiné informace potřebné pro ochranu, zjišťování a hlášení bezpečnostních incidentů počítačů a reagování na ně.

Hodnocení nebo certifikace produktů

U těchto služeb může CSIRT uskutečňovat hodnocení produktů z hlediska nástrojů, aplikací nebo jiných služeb, aby se zajistila bezpečnost produktů a jejich shoda s přijatelnými bezpečnostními praktikami CSIRT nebo organizace. Přezkoumávané nástroje a aplikace mohou být otevřeným zdrojem nebo komerčními produkty. Tyto služby lze poskytovat buď jako hodnocení, nebo na základě programu certifikace, a to v závislosti na normách, které organizace nebo CSIRT aplikuje.

A.3 Příklady

Fiktivní CSIRT
0. krok – Chápání, co je CSIRT: Vzorový CSIRT bude sloužit střední organizaci, která má 200 pracovníků. Organizace má vlastní oddělení IT a dvě další pobočky ve stejné zemi. IT hraje klíčovou roli pro společnost, protože se používá pro interní komunikaci, datovou síť a elektronické obchodování 24 hodin denně, 7 dní v týdnu. Organizace má vlastní síť a disponuje redundantním připojením k Internetu prostřednictvím dvou provozovatelů služeb sítě Internet – ISP *(Internet Service Provider)*. - **1. krok: Počáteční fáze** V počáteční fázi se nový CSIRT plánuje jako interní CSIRT, který poskytuje své služby pro hostitelskou společnost, místní oddělení IT a pracovníky. Také podporuje a mezi různými pobočkami koordinuje řešení incidentů spojených s bezpečností IT. - **2. krok: Výběr správných služeb** V počáteční fázi se rozhodne, že nový CSIRT se zaměří hlavně na poskytování některé z klíčových služeb pro zaměstnance. Příjme se rozhodnutí, že po pilotní fázi by se mohlo zvážit rozšíření portfolia služeb a doplnit služby managementu bezpečnosti. Toto rozhodnutí se učiní na základě zpětné vazby od pilotních složek a v úzké spolupráci s oddělením zajišťování jakosti. - **3. krok: Uskutečnění analýzy složky a vytvoření vhodných komunikačních kanálů** Brainstormingová porada s některými klíčovými osobami z vedení a ze složky generovala dostatečný vstup pro analýzu SWOT. Vede to k závěru, že existuje potřeba následujících rozhodujících služeb: • Výstrahy a varování • Řešení bezpečnostních incidentů (analýza, podpora reakce a koordinace reakce) • Oznámení Musí se zajistit, aby se informace rozesílaly dobře organizovaným způsobem s cílem dostat je k co největší části složky. Přijme se tedy rozhodnutí, že výstrahy, varování a oznámení ve formě bezpečnostních rad se budou publikovat na vyhrazené webové stránce a rozesílat za pomoci adresáře. Elektronická pošta, telefon a fax usnadňuje týmu CSIRT přijímat zprávy o bezpečnostních incidentech. Jako další krok se plánuje unifikovaný webový formulář.

4. krok: Mandát

Vedení fiktivního CSIRT vytvořilo tento mandát:
"Fiktivní CSIRT poskytuje informace a pomoc pracovníkům své hostitelské společnosti za účelem snižování rizik bezpečnostních incidentů počítačů a také reagování na tyto bezpečnostní incidenty, když se vyskytnou."

Tímto fiktivním CSIRT se vysvětluje, že se jedná o interní CSIRT, a že jeho hlavním úkolem je zabývat se otázkami souvisejícími s bezpečností IT.

- -

5. krok: Stanovení obchodního plánu

Finanční model
Jelikož společnost uskutečňuje elektronický obchod 24 hodin denně, 7 dní v týdnu, a má také oddělení IT, které pracuje 24 hodin denně, 7 dní v týdnu, rozhodla se poskytovat během pracovní doby plné služby a mimo pracovní dobu služby na zavolání. Služby pro složku se budou poskytovat bezplatně, ale během pilotní a hodnotící fáze bude posouzena možnost dodávání služeb pro externí zákazníky.

Model výnosů
V průběhu počáteční a pilotní fáze bude CSIRT financován prostřednictvím hostitelské společnosti. Během pilotní a hodnotící fáze bude projednáno další financování, včetně možnosti prodeje služeb externím zákazníkům.

Organizační model
Hostitelská organizace je malá společnost, takže byl vybrán vložený model.
Během pracovní doby bude personál složený ze třech pracovníků poskytovat klíčové služby (rozesílání rad v bezpečnosti a řešení / koordinace bezpečnostních incidentů).

Oddělení IT společnosti už zaměstnává pracovníky s vhodnými odbornými schopnostmi. S tímto oddělením je udělána dohoda, takže nový CSIRT může v případě potřeby požádat o podporu na bázi ad hoc. Lze využít také jejich techniky na zavolání 2. linie.
Hlavní tým CSIRT bude mít čtyři členy na plný pracovní úvazek a pět dalších členů. Jeden z nich je k dispozici také na střídavé směně.

Pracovníci
Vedoucí týmu CSIRT má vzdělání v bezpečnosti a podporu 1. a 2. úrovně a vykonával práci v oblasti řízení přetrvávajících krizí. Ostatní tři členové týmu jsou odborníci na bezpečnost. Členové týmu CSIRT z oddělení IT na částečný pracovní úvazek jsou odborníci na infrastrukturu společnosti.

6. krok: Používání kanceláře a politiky bezpečnosti informací
Vybavení a umístění kanceláře
Protože hostitelská společnost už má zavedenou efektivní fyzickou bezpečnost, nový CSIRT je v tomto ohledu dobře chráněn. Je zajištěn takzvaný „zpravodajský informační sál“, aby byla možná koordinace v případě nouzového stavu. Byl zakoupen trezor pro šifrované materiály a citlivé dokumenty. Byla zřízena zvláštní telefonní linka, včetně telefonní ústředny pro usnadnění horké linky během pracovní doby, a zajištěn mobilní telefon se stejným telefonním číslem pro službu „na zavolání“ mimo pracovní dobu.

Lze rovněž využít existující zařízení a podnikovou webovou stránku pro sdělování informací týkajících se CSIRT. Software adresáře je nainstalován, udržuje se a má vyhrazenou část pro komunikaci mezi členy týmu a s ostatními týmy. Všechny kontaktní podrobnosti pracovníků se ukládají do databáze; kopie se bezpečně uchovává.

Předpisy
Jelikož CSIRT je začleněn do společnosti, která má politiky bezpečnosti informací, byly za pomoci právního poradce společnosti vytvořeny shodné politiky pro CSIRT.
- -

7. krok: Vyhledávání spolupráce
S využitím Soupisu agentury ENISA bylo možné některé týmy CSIRT ve stejné zemi rychle vyhledat a kontaktovat. S jedním z nich byla pro nově najatého vedoucího týmu zorganizována návštěva na místě. Dozvěděl se o činnosti národního CSIRT a zúčastnil se porady.
Tato porada byla více než užitečná k tomu, aby se shromáždily příklady pracovních metod, a aby se získala podpora několika jiných týmů.
- -

8. krok: Podpora obchodního plánu

Bylo rozhodnuto shromáždit fakta a čísla z minulosti společnosti. Je to více než účelné pro statistický přehled o situaci v bezpečnosti IT. Tento sběr by měl pokračovat, když už se CSIRT vytvořil a pracuje, aby se statistické přehledy udržovaly v aktuálním stavu.

Byly kontaktovány další národní týmy CSIRT a dotazovány na jejich obchodní případy. Týmy poskytly podporu sestavením určitých diapozitivů s informacemi o posledním vývoji v bezpečnostních incidentech IT a o nákladech na bezpečnostní incidenty.

V tomto vzorovém případě fiktivního CSIRT nebylo nutné příliš přesvědčovat vedení o důležitosti problematiky IT, takže nebylo těžké zahájit první krok. Byl zpracován obchodní případ a plán projektu, včetně odhadu nákladů na přípravu a odhadu provozních nákladů.
- -

9. krok: Vytvoření pracovních postupů procesů a provozních a technických postupů

Fiktivní CSIRT se zaměřuje na dodávání následujících klíčových služeb CSIRT:

- výstrahy a varování
- oznámení
- řešení bezpečnostních incidentů.

Tým zpracoval postupy, které dobře fungují, a které může každý člen týmu snadno pochopit. Fiktivní CSIRT také najal právního experta pro řešení odpovědnosti a politiky bezpečnosti informací. Tým schválil několik užitečných nástrojů a v jednáních s jinými týmy CSIRT zjistil užitečné informace o provozních otázkách.

Byla vytvořena pevná šablona pro poradenství v bezpečnosti a pro zprávy o bezpečnostních incidentech. K řešení bezpečnostních incidentů používá tým RTIR.

- -

10. krok: Výcvik pracovníků

Fiktivní CSIRT rozhodne vyslat všechny své technické pracovníky na příští kurzy TRANSITS, které jsou k dispozici. Vedoucí týmu se kromě toho účastní kurzu *Řízení CSIRT* z CERT/CC.

- -

11. krok: Cvičení

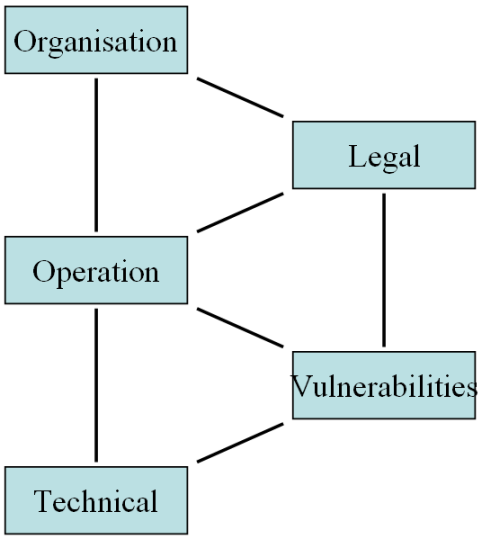
Během prvních týdnů práce použil fiktivní CSIRT několik fiktivních případů (obdržených jako příklady od jiných týmů CSIRT), které se využily jako cvičení. Kromě toho vydal několik odborných rad k bezpečnosti vycházejících z informací o skutečné zranitelnosti rozesílaných prodejci hardwaru a softwaru, které doladil a přizpůsobil potřebám složky.

A.4 Vzorový materiál z kursů CSIRT

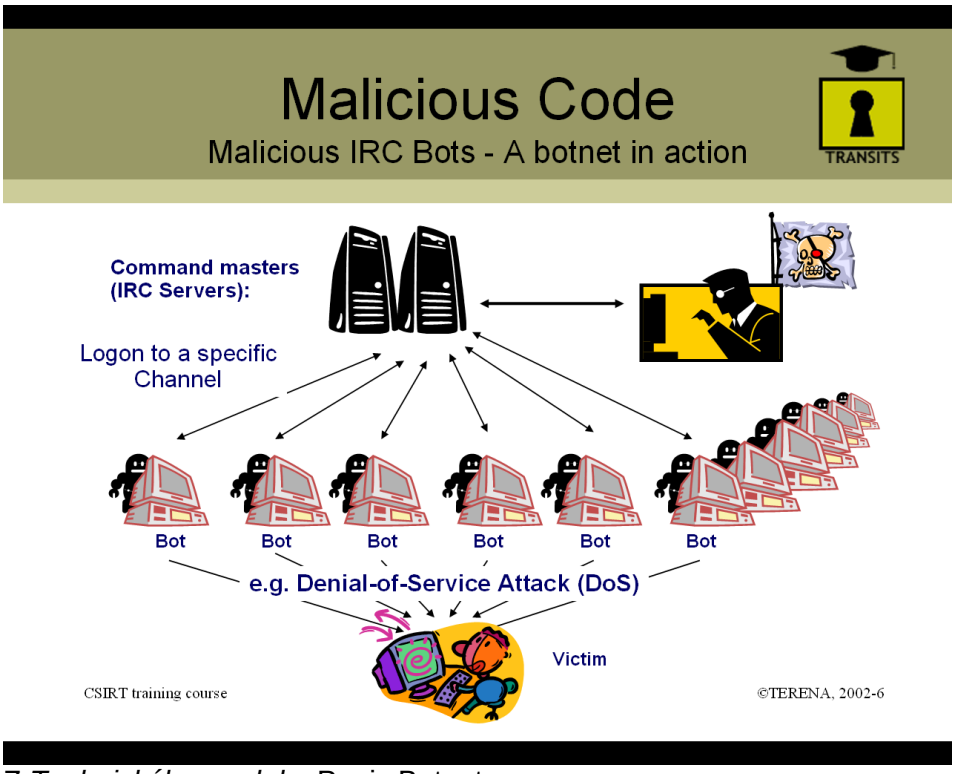
TRANSITS (s laskavým souhlasem společnosti Terena, http://www.terena.nl)

Course structure

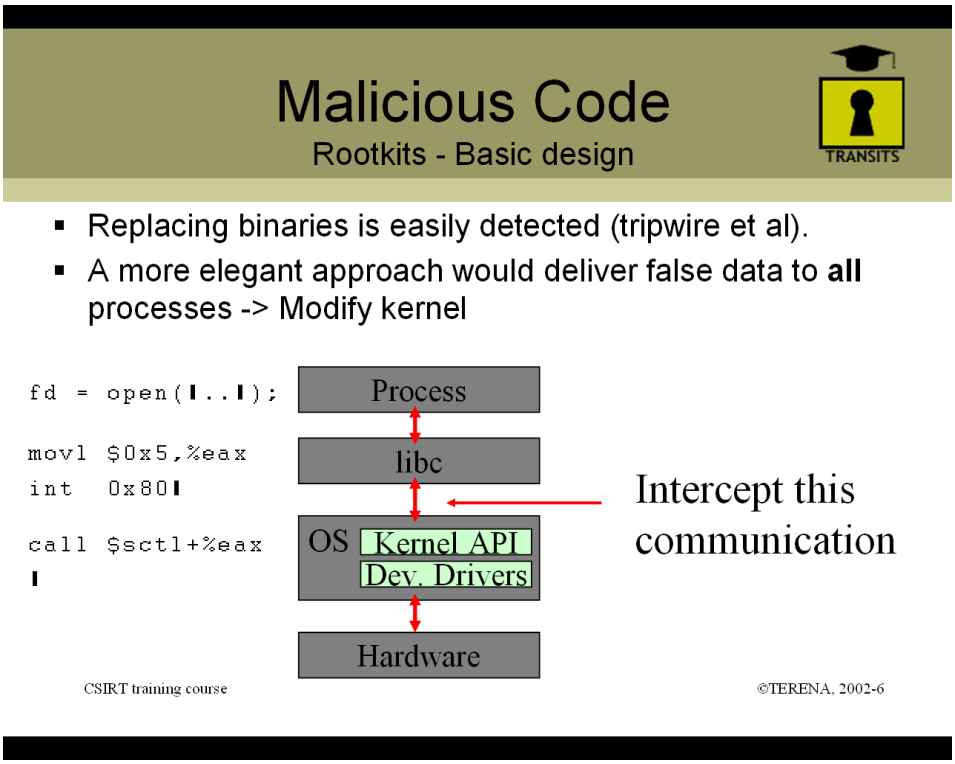
- Five modules
- Independent, but linked
- 12-14 hours work in 2 days
- Practical exercises include
  - Analyse incidents
  - Organisational plan
  - Incident response plan



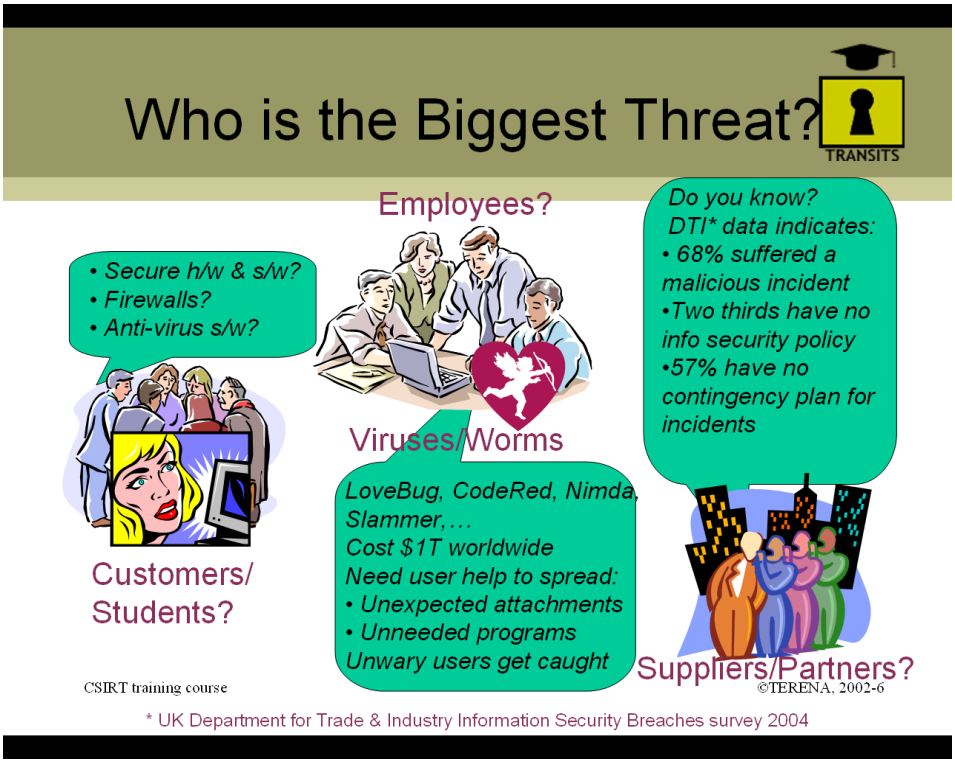
CSIRT training course ©TERENA, 2002-6



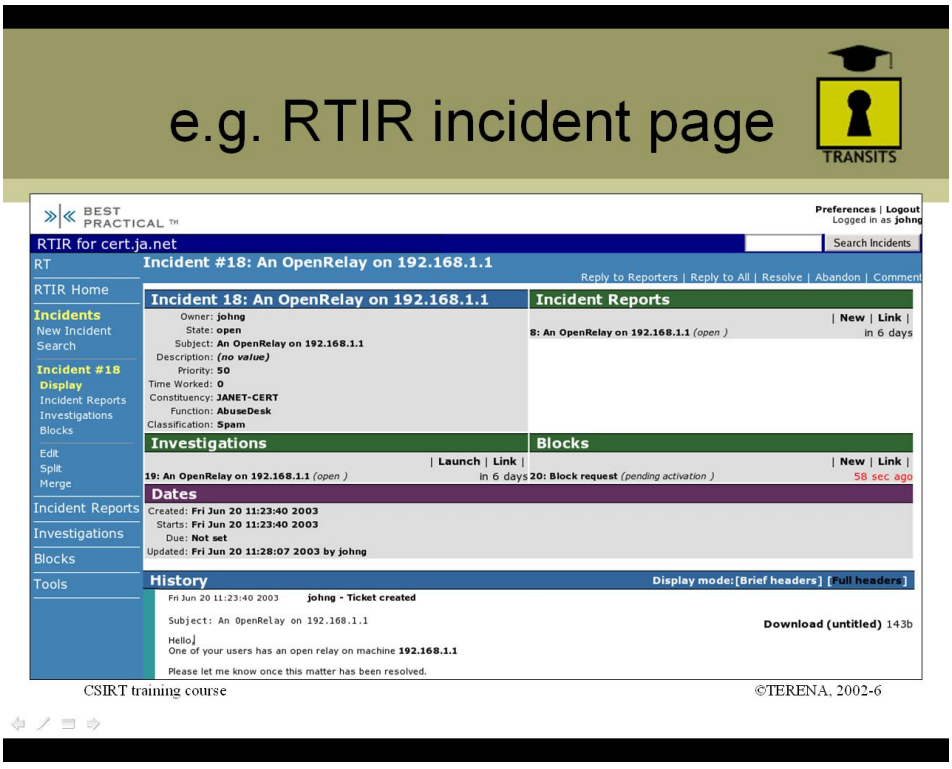
Z *Technického modulu*: Popis Botnetu



Z *technického modulu*: Základní návrh rootkitu



Z *organizačního modulu*: Zasvěcená nebo nezasvěcená osoba – kde je větší hrozba?

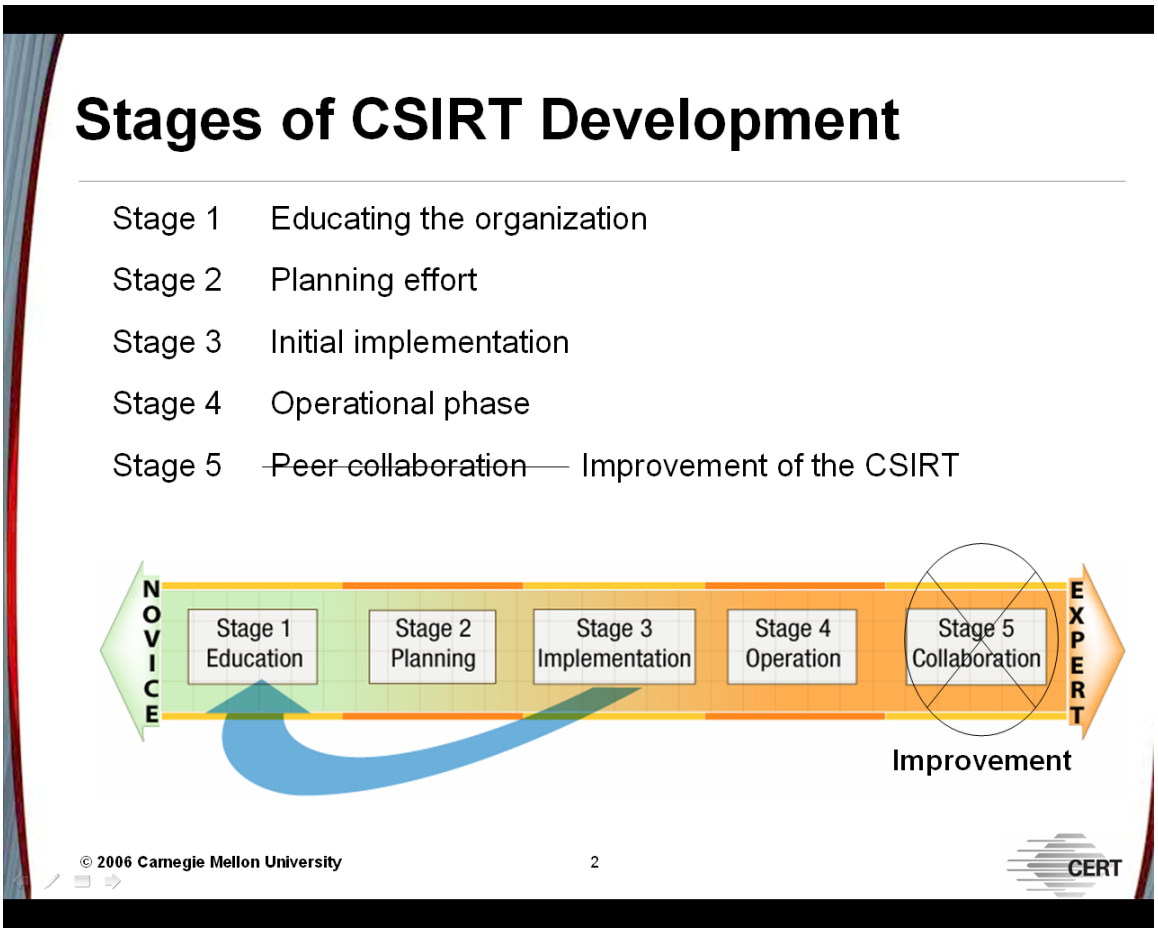


Z provozního sledování: Sledovač žádostí o reakci na bezpečnostní incidenty – RTIR *(Request Tracker for Incident Response)*

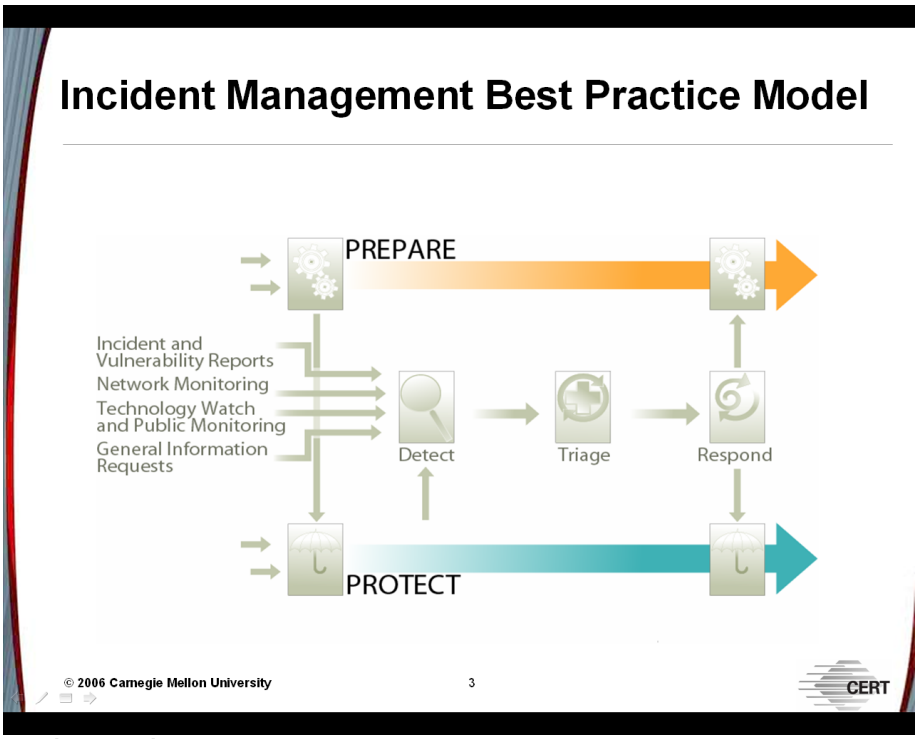
např. strana bezpečnostních incidentů RTIRT

„Ustavení týmů CSIRT“ (s laskavým souhlasem CERT/CC, http://www.cert.org)

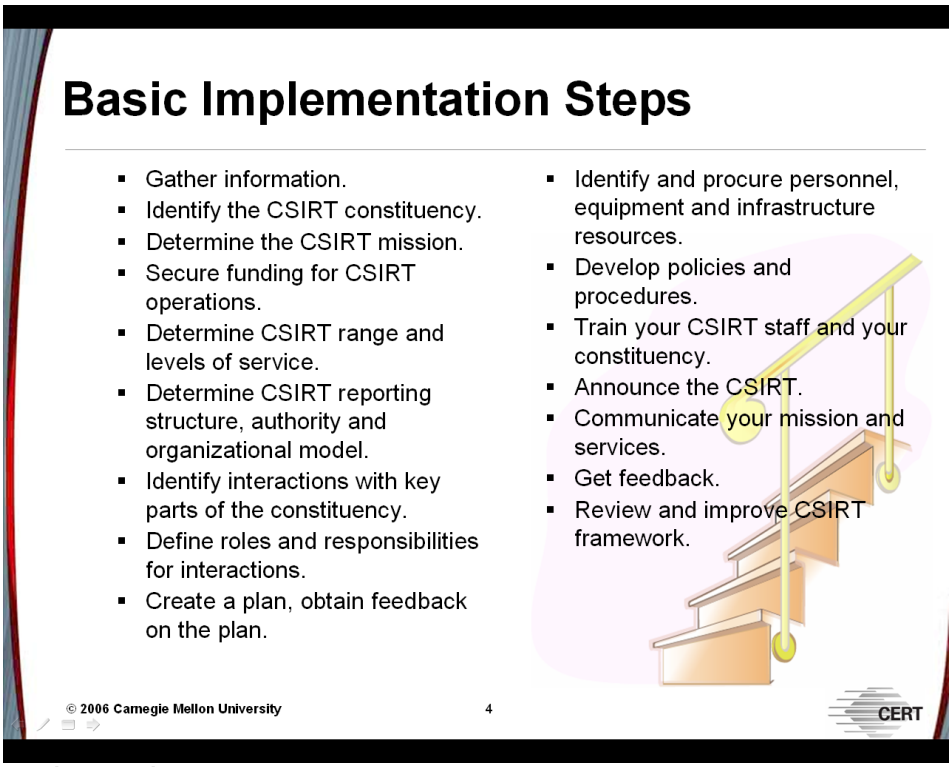
ENISA s povděkem oceňuje Tým pro rozvoj CSIRT u Programu CERT za to, že nám povolil využít obsah jeho výcvikových kursů!



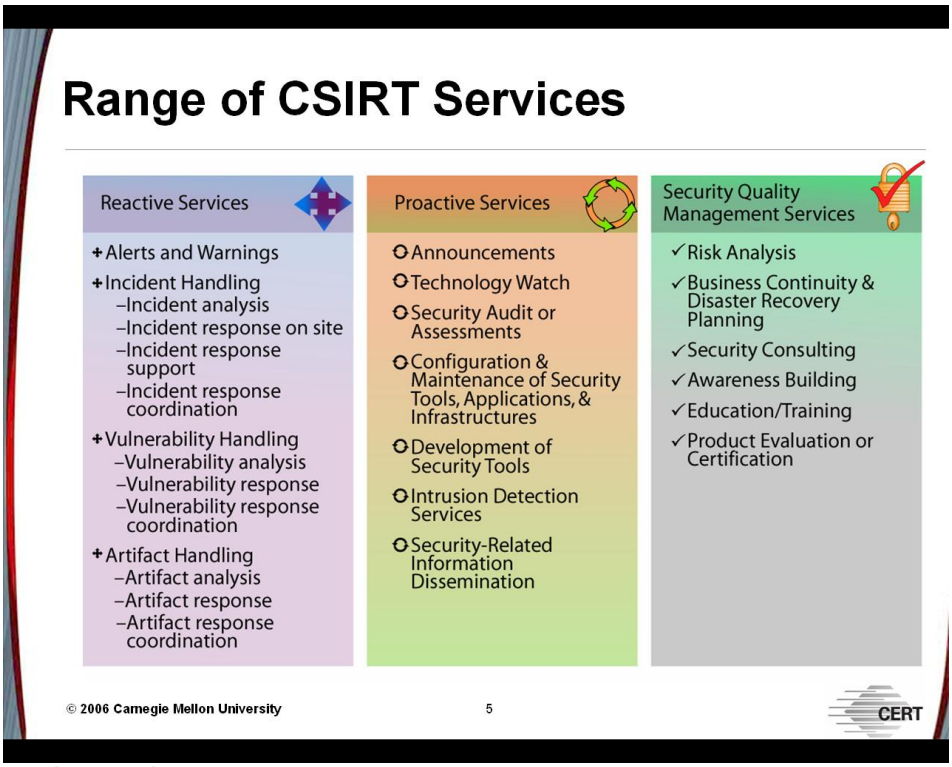
Z výcvikového kursu CERT/CC: Fáze vývoje CSIRT



Z výcvikového kursu CERT/CC: Nejlepší praxe v řízení bezpečnostních incidentů

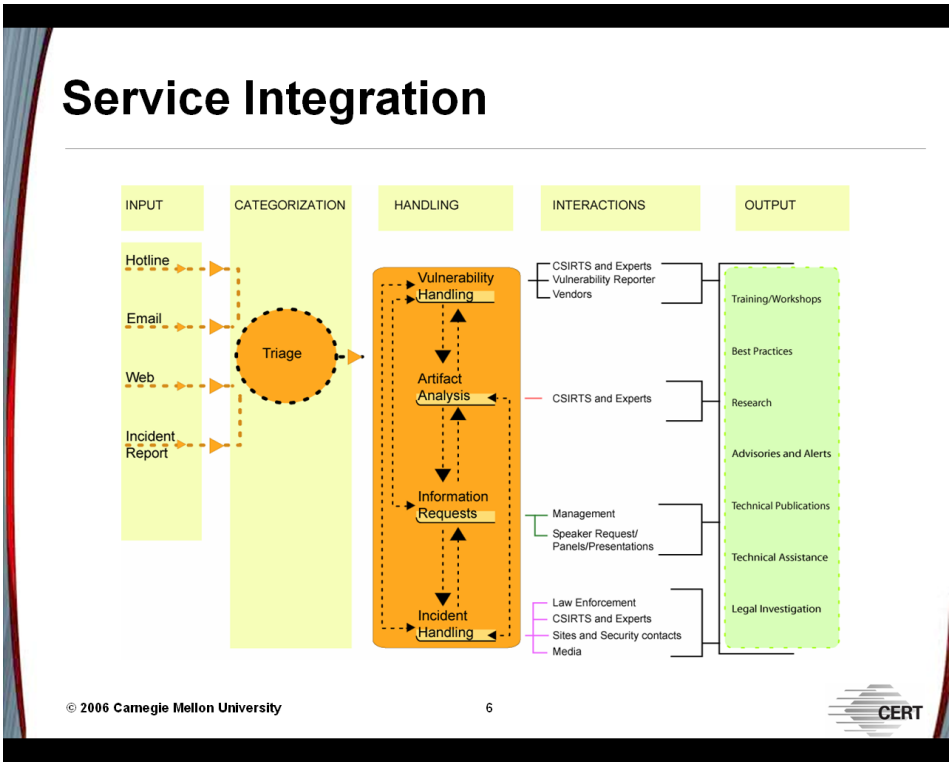


Z výcvikového kursu CERT/CC: Kroky, které se mají dodržet, když se ustavuje CSIRT

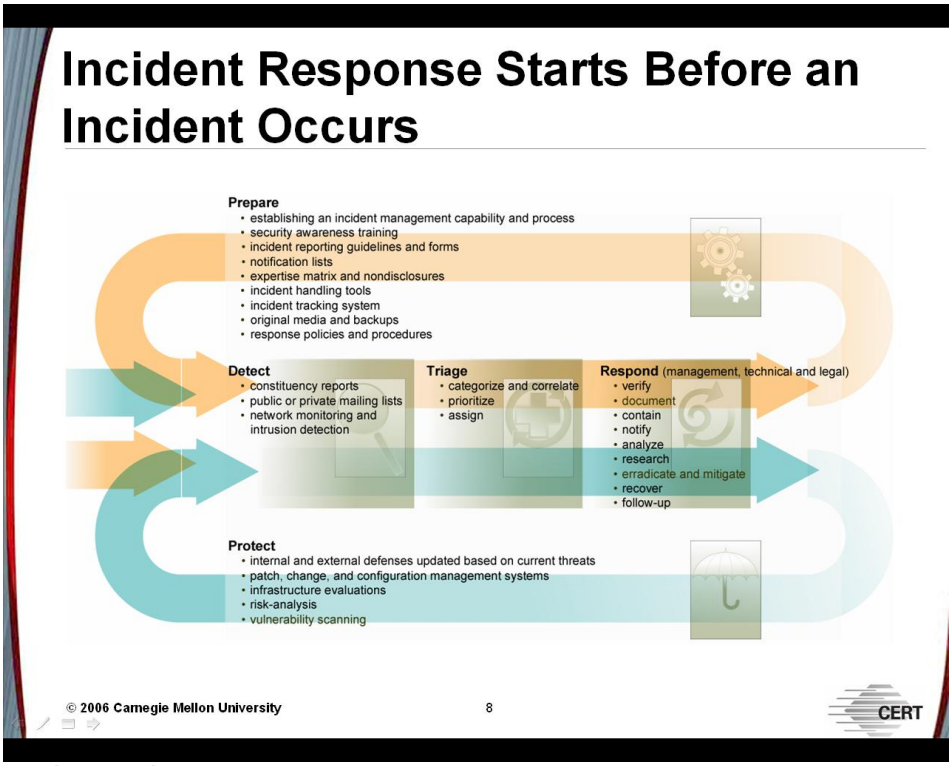


Z výcvikového kursu CERT/CC: Služby, které může poskytovat CSIRT

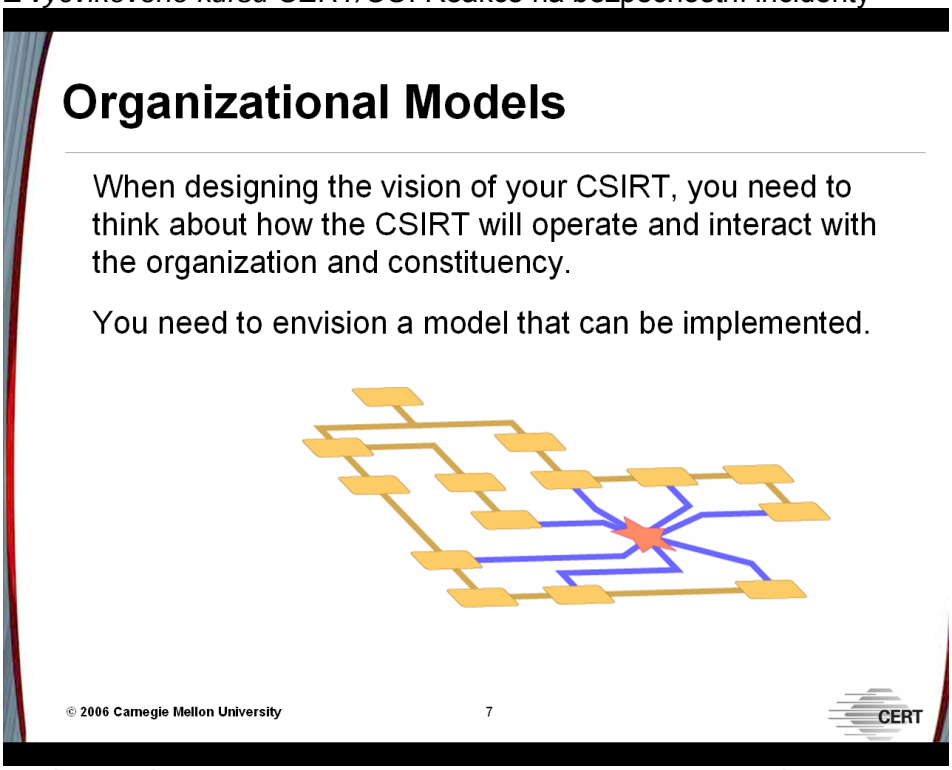
Rozsah služeb CSIRT



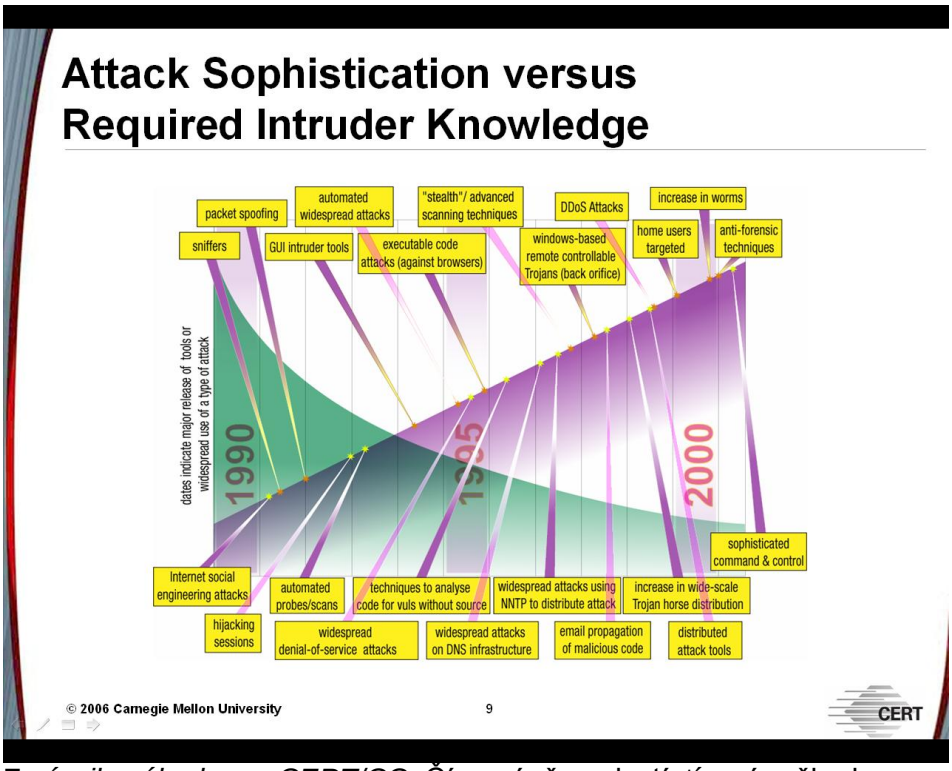
Z výcvikového kursu CERT/CC: Pracovní postup řízení bezpečnostních incidentů



Z výcvikového kursu CERT/CC: Reakce na bezpečnostní incidenty



Z výcvikového kursu CERT/CC: Jak bude CSIRT organizován?



Z výcvikového kursu CERT/CC: Čím méně znalostí, tím více škody