CSIRT.cz - jak zvládnout bezpečnostní incidenty?

Vložil/a cm3l1k1 [1], 8 Duben, 2008 - 20:57

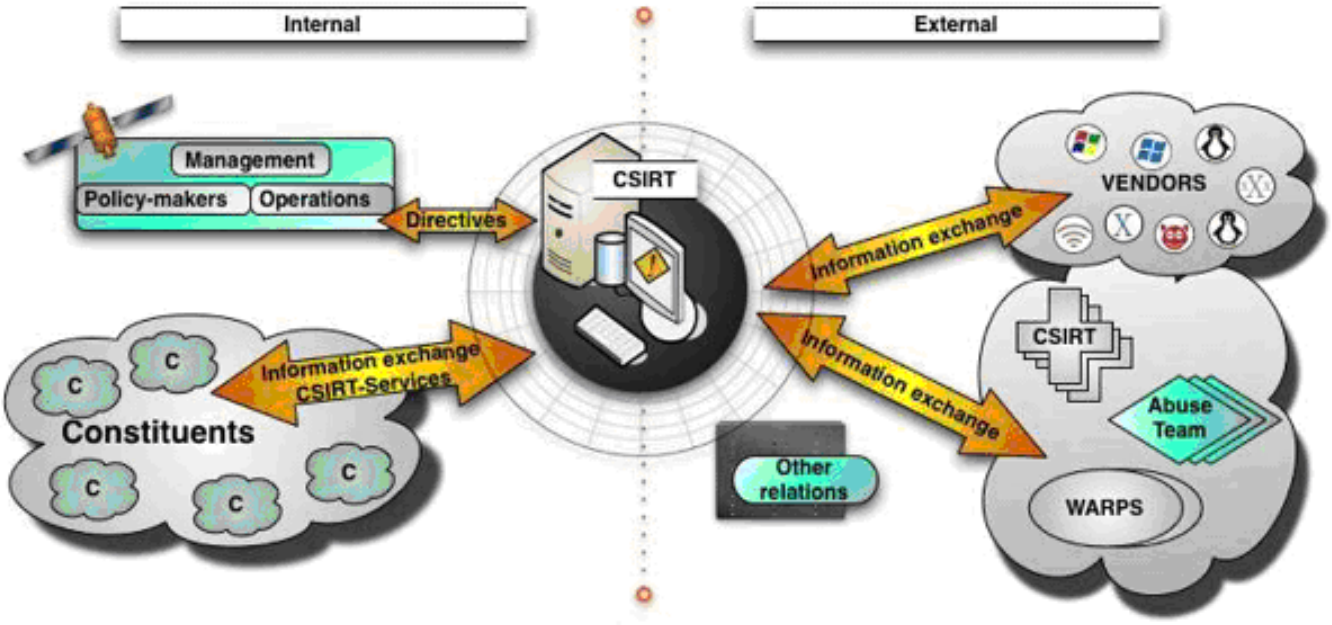
- Security [2]
- Tisková zpráva [3]

Nedílnou součástí preventivní a aktivní ochrany počítačů a počítačových sítí je důsledné a efektivní řešení bezpečnostních incidentů včetně odstraňování jejich příčin a následků. Je nanejvýš nutné, aby na možnost narušení bezpečnosti sítě a počítačů byli jejich správci a uživatelé připraveni a měli k dispozici funkční struktury, efektivní postupy, pravidla a technické prostředky vedoucí k co nejrychlejšímu odstranění problémů při minimalizaci škod.

Problematika zvládání incidentů je obecně řešena tzv. CSIRT týmy – Computer Security Incident Response Team (případně CERT – Computer Emergency Response Team) na níž staví i **předmět dílčího úkolu bezpečnostního výzkumu Ministerstva vnitra, kterým je vybudování distribuované hierarchie pro systematické plošné řešení bezpečnostní problematiky v sítích prostřednictvím CSIRT týmů, kde základem je vybudování modelového zastřešujícího CSIRT týmu a jeho pilotní provoz.**

Při řešení úkolu se spolupracuje s nadnárodními organizacemi TERENA (Trans European Research and Education Networking Association) a FIRST (Forum for Incident Response and Security Teams) a bude se využívat zkušenosti a know-how jediného oficiálního CSIRT týmu v České republice, který působí nad sítí národního výzkumu CESNET2 provozovanou sdružením CESNET z.s.p.o.

Na níže uvedeném obrázku je zobrazeno obecné postavení CSIRT v kontextu okolí a to směrem dovnitř organizace primárně reprezentované uživateli CSIRT (Constituents), představující pole působnosti CSIRT a směrem ven primárně reprezentované jinými CSIRT, případně WARPS (subjekty včasného varování).



Zdroj: ENISA (European Network and Information Security Agency)

Z hlediska cílů (role) je možné CSIRT obecně rozdělit na:

1) Interní CSIRT – řeší bezpečnostní incidenty a poskytuje služby v oblasti zvládání počítačových bezpečnostních incidentů pro vlastní organizaci (CSIRT bank, CSIRT poskytovatelů telekomunikačních služeb, provozovatelů sítí apod.)
2) Koordinační CSIRT – koordinuje a pomáhá zvládat počítačové bezpečnostní incidenty tam, kde je o jeho služby zájem
3) Kombinace interního a koordinačního CSIRT

CSIRT přináší reaktivní a proaktivní činnost v oblasti zvládání počítačových incidentů. Jeho snahou je, pokud je to možné, incidentům předejít nastavením vhodných protiopatření, přičemž pro CSIRT je nezbytná spolupráce s dalšími CSIRT a to hlavně za účelem sdílení varování a znalostí (zkušeností).

Existence alespoň jednoho oficiálního CSIRT týmu je žádoucí v každé provozované síti, obzvláště pak v těch rozsáhlých. Ve světě existují stovky CSIRT týmů a drtivá většina z nich vznikla a funguje v úzké spolupráci s nadnárodními organizacemi TERENA [4] (Trans European Research and Education Networking Association) a FIRST [5] (Forum for Incident Response and Security Teams), které poskytují vhodnou platformu pro rozvoj spolupráce a pravidelná setkávání. V České Republice v současné době existuje jediný oficiální CSIRT tým. Byl ustanoven v roce 2004 a je provozován sdružením CESNET. Tento tým nazývaný CESNET-CERTS (www.cesnet.cz/csirt [6]) operuje nad sítí národního výzkumu CESNET2.

Žádné bezpečnostní opatření nemůže stoprocentně zamezit vzniku bezpečnostních incidentů. Nové typy bezpečnostních incidentů se objevují zároveň s novými technologiemi. Řešení a předcházení bezpečnostních incidentů není úkolem pouze pro správce sítě (nebo IT oddělení), ale podílí se na něm všichni uživatelé. Je proto nutné, aby každý uživatel Internetu věděl o možných hrozbách, svých povinnostech a právech a znal základní postup při objevení podezřelé situace. **Při výskytu incidentu je čas na „spuštění“ plánu, ne čas na přemýšlení o incidentu a jak s ním naložit!**

CSIRT nemá pevně daný rozsah poskytovaných služeb. CSIRT reflektuje praxi a potřeby dané organizace a vhodným způsobem doplňuje její řešení informační bezpečnosti.

Rozdělení služeb CSIRT:
1. Reaktivní služby:
- které se spouští na základě nějakého podnětu (událost, požadavek).

2. Proaktivní služby:
- poskytují informační pomoc uživatelům, přičemž cílem těchto služeb je přímo snížení počtu incidentů, nebo zmírnění jejich dopadů.

3. Ostatní služby v oblasti informační bezpečnosti:
- představují služby vylepšující celkovou bezpečnost organizace.

Pokud v organizaci chybí schopnost zvládání incidentů, která zahrnuje nejen technologie, ale i procesy a lidi, může být investice do bezpečnostních opatření v podstatě zbytečná.

Odkazy:

CSIRT.cz [7]

Prezentace CSIRT ke stažení [8]

URL článku:
https://security-portal.cz/clanky/csirtcz-jak-zvl%C3%A1dnout-bezpe%C4%8Dnostn%C3%AD-incidenty

Odkazy:
[1] https://security-portal.cz/users/cm3l1k1
[2] https://security-portal.cz/category/tagy/security
[3] https://security-portal.cz/category/tagy/tiskov%C3%A1-zpr%C3%A1va
[4] http://www.terena.nl/

[5] http://www.first.org
[6] http://www.cesnet.cz/csirt
[7] http://www.csirt.cz
[8] http://data.security-portal.cz/clanky/141/Prezentace_-_CSIRT.pdf