

Vybudování bezpečnostního týmu

14. 11. 2005

Andrea Kropáčová

7275 7E6F 39E4 261D FF15 8973 BE2B 53A7 D874 7FE5

Bezpečnostní tým

Základní otázky:

- co je bezpečnostní tým?
- proč potřebujeme bezpečnostní tým?
- co by měl bezpečnostní tým dělat?
- jak máme začít?
- co je "Incident Response Policy"?
- kdo by měl vytvořit CSIRT?
- kolik členů musí mít bezpečnostní tým?
- co potřebuji znát?
- kde najdu kontakt na ostatní bezpečnostní týmy?

Bezpečnostní tým

Proč potřebujeme bezpečnostní tým?:

- roste počet uživatelů a připojených stanic, bezpečnostních incidentů
- incidenty jsou sofistikovanější a roste motivace
- počet odborníků moc ne, jen musí zvládnout více
- uživatelé jsou nezkušení, mít počítač je daleko dostupnější
- hrozí ztráta citlivých dat
- vznikají nové a nové zákony, které řeší počítačovou kriminalitu
- dobré jméno = peníze

Bezpečnostní tým

Otázky, které je třeba si zodpovědět na začátku

- definování základní strategie
- definování response capability, RFC 2350
- co jsou základní podmínky pro zřízení bezpečnostní skupiny?
- jaký typ bezpečnostní skupiny potřebujeme?
- jaký typ služeb budeme provozovat (nabízet)
- kolik členů musí mít bezpečnostní tým?
- na jaké pozici by bezpečnostní tým měl být ve své dom. organizaci
- kolik bude asi stát vytvoření a provoz bezp. týmu?
- jaké jsou základní kroky ke zřízení bezpečnostního týmu?

Bezpečnostní tým

Základní kroky ke zřízení bezpečnostního týmu:

- Získat podporu vedení a kolegů
- Stanovit si strategii vybudování týmu
- Získat co nejvíce užitečných informací
- Vyhodnotit získané informace
- Stanovit pole působnosti a zodpovědnost
- Vytvoření týmu
- Zveřejnění existence týmu
- Zhodnocení dosažených úspěchů a efektivitu týmu

Zřízení bezpečnostního týmu

Získat podporu vedení a kolegů:

- kolegové – čas, ochota a schopnosti prosazovat nové věci
- vedení – finanční a personální zázemí

Stanovit si strategii vybudování týmu:

- kdo bude členem týmu a proč
- jakou roli bude tým v organizaci hrát

Zřízení bezpečnostního týmu

Získejte co nejvíce užitečných informací:

- jaká je incident response organizace
- jaká je architektura naší sítě, použité prvky, služby, kdo má přístup ke zdrojům sítě
- kdo za co zodpovídá
- jaké typy incidentů jsou nám hlášeny
- jak se řeší bezp. incidenty v naší organizaci
- co jsou naše největší slabiny
- koho dále potřebujeme mít v týmu (správce, specialista, právník, manager ...)
- jsou někde v našem okolí již existující bezpečnostní týmy? Jak fungují?

Zřízení bezpečnostního týmu

Vyhodnocení shromážděných informací:

- získané informace mohou sloužit k rozhodnutí, kdo by se měl stát členem týmu a s kým bude tým úzce spolupracovat
- jeho vztah k dané organizaci
- jaké činnosti bude tým dělat
- jaké služby bude tým nabízet
- je nutné, aby vize týmu byla shodná s vizí vedení dané organizace
- personální kapacity

Zřízení bezpečnostního týmu

Stanovit pole působnosti a zodpovědnost:

- role týmu v dané organizaci (autoritativní, výkonný, informační, ...)
- zodpovědnost a pole působnosti
- definovat cíle, poslání, úkoly a časové horizonty naplnění vize
- stanovit strukturu týmu a určit role jeho členů
- základní pravidla fungování

Zřízení bezpečnostního týmu

Vytvoření týmu:

- zvolení členů a jejich zaškolení
- stanovení rolí
- zvolit prostředky a základní nástroje, se kterými budou členové operovat
- definování základních procedur a pravidel
- definování vizí a cílů

Zveřejnění existence týmu

- **webová stránka se základními informacemi**
- **diskusní el. listy**
- **lokální zpravodaj**
- **konference, setkání a semináře**
- **ve výroční, či jiné zprávě dané organizace**

Bezpečnostní tým

Zhodnocení dosažených úspěchů a efektivitu týmu:

- postup plnění cílů v porovnání s původními představami
- přínos týmu pro danou organizaci
- názory členů týmu na činnost, kterou se zabývají

Zřízení bezpečnostního týmu

Obecná doporučení:

- některé kroky mohou běžet paralelně
- je vhodné stanovit si reálné cíle a časové milníky
- zmíněné kroky jsou závislé na aktuální situaci v dané organizaci, na technickém stavu sítě a služeb, schopnostech zaměstnanců a na zdrojích dané organizace
- je nutné postupovat opatrně, postupně
- trpělivost růže přináší

Bezpečnostní tým

Jak na to v síti CESNET2:

- v síti CESNET2 by **bezpečnostním týmem** mohla být defacto každá skupina správců, např. příjemci **abuse** adres
- zvolit si dosažitelný cíl, pro začátek např. pouze ***incident***

handling:

- střídání s kolegy ve vyřizování incidentů
- vytvoření vhodného pracovního prostředí pro příjem a řešení incidentů
- odstranění původce incidentu
- odpověď autorovi stížnost
- archivace přijatého incidentu a jeho řešení