Zásady managementu incidentů

Obsah prezentace

- Úvod, základní pojmy
- ISO/IEC TR 18044

ISO/IEC TR 18044

- ISO/IEC TR 18044 – Information technology – Security techniques – Information security incident management

Základní pojmy

- Plánování kontinuity činností organizace
- Bezpečnostní událost (BU)
- Bezpečnostní incident (BI)
- ISIRT (Information Security Incident Response Team) – tým „reagující" na bezpečnostní incidenty

Cíle

- BU jsou detekovány a efektivně řešeny, především v identifikaci, zda musí být kategorizovány jako BI nebo ne.
- Identifikované BI jsou hodnoceny a řešeny nejvhodnějším a nejefektivnějším způsobem.
- Nepříznivé dopady BI na organizaci a její „business" jsou minimalizovány.
- Z BI a jejich vypořádání získat poučení.

Procesy

- Plánuj a připrav
- Používej
- Přezkoumej
- Zlepši

- Obdoba PDCA modelu

Plánuj a připrav

- Politika řízení bezpečnostních incidentů
- Schéma řízení BI
- Bezpečnost systémů, služeb a sítí
- Analýza a řízení rizik
- Aktualizace politiky
- Ustanovení ISIRT
- Vytváření povědomí o řízení BI a školení
- Testování schématu řízení BI

Používej

- Odhalování a hlášení BU
- Hodnocení a rozhodování o BI
- Reakce na BI, včetně forenzních analýz

  (Forenzní analýza ICT slouží jako prostředek k získání důkazů o spáchání nebo nespáchání trestného činu.)

Přezkoumej

- Další forenzní analýzy
- Identifikace ponaučení
- Identifikace zlepšení bezpečnosti
- Identifikace zlepšení schématu řízení bezpečnostních incidentů

Zlepši

- Zlepšit systém na základě analýzy rizik a výsledků přezkoumání
- Iniciovat zlepšení bezpečnosti
- Zlepšit schéma řízení bezpečnostních incidentů

Přínosy

- Zlepšení bezpečnosti informací
- Redukce nepříznivých dopadů na obchod (finančních ztrát)
- Posílení prevence BI
- Ospravedlnění rozpočtu a zdrojů
- Zlepšení aktualizace výsledků analýzy a řízení rizik
- Zajištění podkladů pro školení
- Zajištění vstupů pro přezkoumání bezpečnostní politiky a souvisejících dokumentů.

Klíčové problémy

- Závazek vedení
- Povědomí
- Zákonné a regulační aspekty
- Provozní efektivita a kvalita
- Anonymita
- Důvěrnost
- Věrohodné operace
- Typologie

Příklady bezpečnostních incidentů a jejich příčiny

- Odepření služby - Denial of Service (DoS)
  - Pingování adres k zaplnění šířky pásma
  - Zaslání dat v neočekávaném formátu za účelem zhroucení systému/služby nebo sítě, popř. narušení normálního provozu
  - Otevření mnohonásobných relací s jednotlivým systémem/službou nebo sítí za účelem „vyčerpání" zdrojů

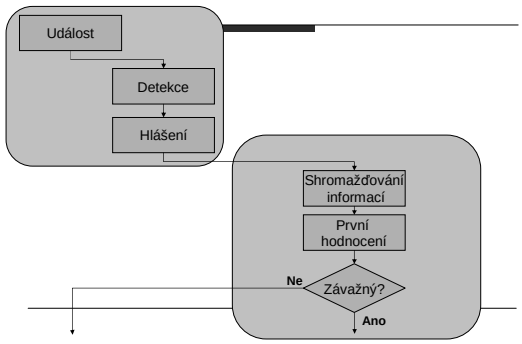
Příklady bezpečnostních incidentů a jejich příčiny

- Sběr informací (podkladů pro případný útok)
  - Skenování portů
  - Testování, který ze systémů je „naživu"
  - Zkoušení známých zranitelností napříč rozsahem síťových adres
  - Vyzrazení nebo modifikace informací
  - Krádež duševního vlastnictví uložených v elektronické podobě
  - Zneužití informačního systému
  - ……..

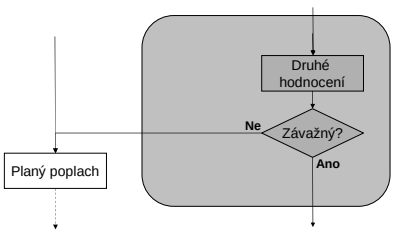
Příklady bezpečnostních incidentů a jejich příčiny

- Neautorizovaný přístup
  - Pokusy o získání souborů s hesly
  - Využití přetečení bufferu k získání privilegovaného přístupu k cíli
  - Využití zranitelností protokolů k napadení nebo přesměrování síťových spojení
  - …..

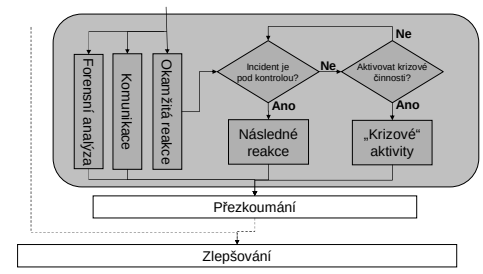
Vývojový diagram bezpečnostní události a incidentu



Vývojový diagram bezpečnostní události a incidentu



Vývojový diagram bezpečnostní události a incidentu



Záznam BU

- Detaily hlásící osoby
  - Jméno, adresa, organizace, telefon, mail …
- Popis BU
  - Co, jak a proč nastalo
  - Ovlivněné komponenty
  - Nepříznivé dopady
  - Identifikované zranitelnosti

Záznam BU

- Detaily BU
  - Datum a čas výskytu BU
  - Datum a čas zjištění BU
  - Datum a čas nahlášení BU
  - BU skončila? (ANO/NE)
  - Délka trvání BU (v případě, že skončila)

Záznam BI

- 1. část společná s BU
- Typ incidentu
  - Skutečný / nepodařený / podezřelý
  - Úmyslný / neúmyslný / chyba / neznámý (konkrétní typy)
- Ovlivněná aktiva
  - informace, HW, SW, komunikace, dokumenty
  - Způsob poškození, hodnota, náklady

Záznam BI

- Řešení incidentu
- Zapojená osoba / pachatel
  - Popis pachatele
  - Motivace
- Přijatá opatření k řešení incidentu
- Plánovaná opatření k řešení incidentu
- Další opatření (např. šetření další osobou)

Záznam BI

- Závěr (závažný / bezvýznamný)
- Informovaní jedinci / entity
- Zapojení jedinci (jméno, role, datum, podpis)

Metody auditu zaměřené na bezpečnost informací

Typy auditů

- Interní
- Zákaznický
- Třetí stranou (např. certifikační)

Stupně certifikačního auditu

- Vedený minimálně ve dvou stupních, oba k prokázání shody s ISO/IEC27001
- Audit 1. stupně – Přezkoumání dokumentace
- Může ale nemusí být vedený na místě, přezkoumání hlavních prvků ISMS
- Audit 2. stupně – Audit implementace
- Vedený na místě, přezkoumání účinnosti politik, postupů a cílů

Audit 1. stupně Přezkoumání dokumentace

Cíl

- Získat přehled pro plán auditu 2. stupně pochopením ISMS v kontextu bezpečnostní politiky a cílů organizace; zejména pak stupně připravenosti na audit

Audit 1. stupně Přezkoumání dokumentace

Klíčové činnosti

- Přezkoumání systému řízení ISMS
- Posouzení rozsahu ISMS
- Hodnocení a management rizik
- Prohlášení o aplikovatelnosti
- Bezpečnostní politika a podpůrné klíčové postupy
- Formální kontrola pořizování záznamů
- Vysvětlení 2. stupně organizaci

Audit 2. stupně Audit implementace

Cíl

- Potvrdit, že organizace dodržují vlastní politiky, cíle a postupy
- Potvrdit, že ISMS je v souladu se všemi požadavky ISMS standardu a tyto požadavky jsou organizací plněny
- Prověřit efektivnost systému ISMS

Audit 2. stupně Audit implementace

Klíčové činnosti

- Pohovor s vlastníky a uživateli ISMS
- Přezkoumání vysoce, středně a/nebo nízko rizikových oblastí
- Bezpečnostní cíle
- Přezkoumání bezpečnosti (interní audity) a přezkoumání vedením
- Souvislost mezi hlavními dokumenty uvnitř systému
- Záznamy a jejich využívání pro zlepšení

Odpovědnosti vedoucího auditora

Vymezené před 1. stupněm

- Plánovat a řídit všechny fáze auditu
- Vést 1. stupeň auditu
- Pomáhat při výběru týmu a instruovat tým
- Řídit konflikty a zvládat složité situace
- Vést a řídit všechny schůzky týmu a auditovaných

Odpovědnosti vedoucího auditora

- Rozhodovat v záležitostech auditu a ISMS
- Oznámit výsledky auditu bez odkladu
- Oznámit závažné překážky, s kterými se setká
- Bezprostředně oznámit kritické neshody
- Užívat efektivní komunikační dovednosti

Odpovědnosti auditora

- Podporovat vedoucího týmu
- Být připravený
- Účastnit se úvodní a závěrečné schůzky
- Provést přidělené úkoly
- Držet se časového plánu a rozsahu auditu

Odpovědnosti auditora

- Dokumentovat všechna zjištění
- Informovat auditované
- Chránit všechny dokumenty
- Dodržovat důvěrnost
- Být objektivní a etický
- Ověřit nápravná opatření

Role auditora

- Nezávislé a objektivní zhodnocení ISMS
- Bez zaujatosti a ovlivnění
- Efektivnost ISMS
- Stupeň implementace
- Plánování a řízení auditu
- Záznam a oznámení zjištění
- Všechny zainteresované strany auditu musí respektovat bezúhonnost a nezávislost auditorů

Vlastnosti auditora

- Být realistický
- Chápat situace komplexně
- Chápat vnitřní vztahy organizace
- Všímat si požadavků na důvěrnost
- Profesionální
- Nezávislý

Vlastnosti auditora

- Být otevřený názorům
- Být vyzrálý
- Mít zdravé mínění
- Mít analytické schopnosti
- Být houževnatý
- Být vnímavý

Přínosy bezpečnostních auditů

- Klíčový zdroj informací pro přezkoumání bezpečnosti
- Demonstruje závazek vrcholového vedení
- Zlepšuje povědomí, zapojení a motivaci zaměstnanců
- Poskytuje příležitosti pro průběžné zlepšování
- Zlepšuje důvěru a spokojenost zákazníků
- Zlepšuje provozní výkonnost

Cíle auditu

- Posouzení shody systému ISMS s ČSN ISO/IEC 27001
- Posouzení stupně implementace
- Posouzení efektivnosti a přiměřenosti systému ve vztahu k politice a cílům
- Identifikace bezpečnostních děr a slabin
- Zajištění příležitosti ke zlepšení ISMS

Cíle auditu

- Splnění smluvních požadavků
- Splnění zákonných požadavků
- Získání certifikace

Účelnost (rozpaky auditora)

- ČSN ISO/IEC 27001 uvádí, že ne všechny opatření budou relevantní každé situaci.
- Organizace bude normu interpretovat tak, aby vyhovovala jejím vlastním cílům.
- Rozhodnutí vedení pramení z důvodů uvedených na předchozím slidu
- Proto, kdo rozhoduje, zda je ISMS uzpůsoben účelu?

Proces certifikace

- Dotaz o informace
- Žádost
- Předaudit (volitelný)
- 1. stupeň
- 2. stupeň
- Certifikace
- Pravidelné dozorové audity
- Recertifikace každé 3 roky