BEZPEČNOST IS P8

2008-04-10

BEZPEČNOST IS/IT:

Standard BS 7799 – Plan-Do-Check-Act:

- ✓ **Plan:**
  - Definice rozsahu ISMS (Information Security Management Systems)
  - Definice politiky ISMS
  - Definice přístupu k posuzování rizik
  - Identifikace rizik
  - Posouzení rizik
    - Výběr metody AR vhodné pro typ organizace a rozsah ISMS
    - Označení rizik podle dopadu na organizaci a pravděpodobnost výskytu
    - Určení „oblasti platných rizik“, která zahrnuje rizika vyžadující ošetření pro jejich eliminaci nebo vyloučení mimo tuto oblast
  - Identifikace a hodnocení podmínek pro ošetření rizik výběr bezpečnost opatření a jejich cílů příprava dokumentu SOA (Statement of Applicability)
    - Identifikace všech zvolených opatření
    - Odůvodnění výběru (pozitivní i negativní) vzhledem k posouzení rizik
- ✓ **Do:**
  - Formulace plánu k ošetření rizik
  - Implementace plánu k ošetření rizik
  - Implementace bezpečnostních opatření
  - Implementace personálních opatření (školení, budování povědomí uživatelů apod.)
  - Řízení činností
  - Řízení zdrojů
  - Implementace procedur pro detekci incidentů a reakce na incidenty
- ✓ **Check:**
  - Provádění monitoringu
  - Pravidelné revize efektivity ISMS
  - Revize úrovně přijatelných a zbytkových rizik
  - Provádění interních ISMS auditů
  - Správa revizí efektivity a úrovně rizik
  - Provádění záznamů o dějích a událostech s dopadem na ISMS
- ✓ **Act:**
  - Implementace identifikovaných vylepšení
  - Provádění opravných nebo preventivních akcí
  - Využívání zprostředkovaných zkušeností
  - Komunikace se zúčastněnými stranami nad výsledky
  - Zaručit, že implementovanými vylepšeními bylo dosaženo požadovaného cíle

BEZPEČNOST DAT NA KONCOVÝCH ZAŘÍZENÍCH:

Rozdělení/kroky:

- ✓ **Monitoring uživatelových aktivit** – podrobné zaznamenávání aktivit + upozornění na nežádoucí aktivity
- ✓ **Restrikce pro některé operace** – nastavení omezení práce s aplikacemi, soubory nebo výměnnými médii
- ✓ **Ochrana dat šifrováním** – šifrování ukládaných souborů

Monitorování:

- ✓ Podrobný záznam činností zaměstnance při práci na pracovní stanici
- ✓ Získání přesného časového snímku pracovní doby zaměstnance

- ✓ Informace využitelné více způsoby

Záznam činností:
- ✓ Speciální software běžící na každé pracovní stanici organizace
- ✓ Vytváření detailního lokálního záznamu o činnostech zaměstnance
- ✓ Alertový systém na nebezpečné akce
- ✓ Přesun do databáze pro hromadné vyhodnocení

Nežádoucí/nebezpečné aktivity:
- ✓ Ne vždy lze přístup zcela zablokovat
- ✓ Uživatelé zneužívají možností, které jim nemohly být odebrány
- ✓ Koncové zařízení zůstává jedním z největších rizik pro vnitrofiremní síť
- ✓ Je třeba využít alertovací systém

Upozornění na nebezpečné aktivity:
- ✓ Okamžité upozornění na nežádoucí aktivitu
- ✓ Podrobné definování podmínek alertu tak, aby nebyl využíván zbytečně
- ✓ Různé operace:
  - Zaslání zprávy
  - Spuštění procesu
  - Odhlášení uživatele
  - Zablokování uživatelova účtu
  - Zápis do Event logu

Použití záznamů:
- ✓ Evidence vytížení výpočetní techniky, benchmarking
- ✓ Personální audit
- ✓ Bezpečnostní hledisko – zcizení dat, upozornění na nekalé aktivity

Bezpečnostní hledisko:
- ✓ Záznamy o potenciálních bezpečnostních incidentech ze strany zaměstnanců
- ✓ Tvorba a ověření funkčnosti bezpečnostní politiky
- ✓ Okamžité upozornění na nebezpečné akce nebo ztrátu dat

Restriktivní opatření:
- ✓ Nastavení na základě informací o využívání stanic
- ✓ Ne vše je možné/vhodné řešit politikou operačního systému
- ✓ Ideálně kombinace politiky OS a externího produktu
- ✓ Průběžné ověřování dodržování a kvality

Typické restrikce nad rámec politiky OS:
- ✓ Připojování/využívání externích zařízení
- ✓ Výčet aplikací dostupných uživateli
- ✓ Omezení počtu instancí aplikace
- ✓ Restrikce v uživatelově adresáři (restrikce pro využívání souborů určitých typů)
- ✓ Obnova souborů/registrů při restartu
- ✓ Dočasné změny v politice

Ochrana obsahu:
- ✓ Jedinou kvalitní ochranou dat je šifrování, všechny ostatní omezení pouze prodlužují dobu prolomení
- ✓ S daty může pracovat jen oprávněný uživatel - není v práci omezen, firemní data jsou chráněna
- ✓ Šifrování musí být na uživateli nezávislé

On-line šifrování:
- ✓ Nejuniverzálnější způsob šifrování souborů – ze všech způsobů šifrování chrání data před největším množstvím útoků

- ✓ Citlivé soubory jsou na disku vždy uloženy v zašifrovaném tvaru
- ✓ Využívá se symetrická kryptografie

Šifrování souborů:

- ✓ Převedení srozumitelného tvaru do nesrozumitelného
- ✓ Soubory navenek vypadají standardně, obsah je chráněn
- ✓ Šifrování musí být maximálně transparentní
- ✓ Téměř nikomu nebyla data odcizena během jejich přenosu, ale vždy přímo z místa, kde byla uložena.
- ✓ Libovolný soubor na lokálním, síťovém a výměnném disku může být šifrován
- ✓ Ochrana proti všem možným útokům a souborovým hrozbám
- ✓ Uživatel a aplikace pracují ve standardním prostředí, on-line šifrování dat – data jsou šifrována v případě potřeby do paměti, na disku stále šifrována

Šifrování – organizační procesy:

- ✓ Šifrování dat není jen o SW
- ✓ Šifrování výměnných médií vyžaduje obdobné procesy jako kompletní šifrování v organizaci
- ✓ Vhodné je využití čipových karet nebo USB tokenů
- ✓ Software by měl obsahovat podporu

Důležité organizační procesy:

- ✓ Management šifrovacích klíčů
- ✓ Management HW tokenů
- ✓ Nastavení s aplikováním bezpečnostní politiky šifrování souborů
- ✓ Distribuce šifrovacích klíčů k uživatelům v rámci rozsáhlého prostředí
- ✓ Zpětná kontrola používání a nastavení šifrování souborů
- ✓ Zálohování a obnova
- ✓ Nutná podpora při běžném provozu
- ✓ Řešení nouzových stavů