# ČESKÁ TECHNICKÁ NORMA

ICS 35.040

**Červenec**

**2005**

| Informační technologie - Bezpečnostní techniky - Struktura detekce průniku do IT | **ČSN 36 9796** |
|---|---|

idt ISO/IEC TR 15947:2002

Information technology - Security techniques - IT intrusion detection framework

Technologies de l´information - Techniques de sécurité - Cadre de détection de l´intrusion dans les systèmes
des technologies de l´information





Obsah

Strana

---

Předmluva

Tato norma obsahuje technickou zprávu typu 3 přijatou v souladu s částí 3 Směrnic ISO/IEC s označením ISO/IEC TR 15947. Technickou zprávu zpracovala ISO/JTC1 *Informační technologie*, subkomise SC 27 - *IT bezpečnostní techniky*.

Vypracování normy

Zpracovatel: Ing. Alena Hönigová, IČ 61470716

# 1 Předmět normy

Toto je technická zpráva (TR) typu 3, která definuje strukturu detekce průniků do systémů IT. Zvažovalo se mnoho tříd průniků. Mezi ně patří například průniky úmyslné nebo neúmyslné, zákonné nebo nezákonné, škodlivé nebo neškodné a neautorizovaný přístup vnitřních nebo vnějších vetřelců. TR se zaměřuje na:

- ustavení společných definicí pro termíny a pojetí spojené se strukturou detekce průniku do IT
- popis generického modelu detekce průniku
- poskytnutí bohatých příkladů pokusů o využití zranitelností systémů
- diskusi o obecných typech vstupních dat a zdrojů, potřebných k efektivní schopnosti detekce průniku
- diskusi o různých metodách a kombinacích metod analýzy detekce průniku
- popisu aktivit/akcí, které jsou odezvou na indikace průniků.

Tento rámec vysvětluje termíny a pojetí detekce průniku a popisuje vztahy mezi nimi. Zabývá se také možným uspořádáním úkolů detekce průniku a souvisících aktivit.

Tato TR poskytuje základ pro obecné pochopení detekce průniku. Cílem tohoto materiálu je pomoci manažerům zavést v organizacích systémy detekce průniku (IDS), které na sebe vzájemně působí a pracují spolu. Tato TR by měla usnadnit spolupráci mezi organizacemi na celém světě tam, kde je tato spolupráce vyžadována a/nebo je nezbytná při obraně proti pokusům o průnik.

Tento rámcový dokument není určený k tomu, aby se zabýval všemi podrobnostmi obsaženými v detekci průniku, např. podrobnými vzorci útoků nebo statistickými anomáliemi nebo mnoha uspořádáními, která by IDS mohl mít.

**-- Vynechaný text --**