

**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



© Český normalizační institut, 2005

**73637**

Podle zákona č. 22/1997 Sb. smějí být české technické normy rozmnožovány a rozšiřovány jen se souhlasem Českého normalizačního institutu.

Strana 2

Obsah

Strana

**1** Předmět  
normy

.....  
.. 5

**2** Normativní  
odkazy

.....	5
<b>3</b> Termíny a definice	5
.....	5
<b>4</b> Úvod do detekce průniku.....	6
<b>4.1</b> Potřeba detekce průniku.....	6
6	
<b>4.2</b> Typy útoků	
.....	
..... 7	
<b>4.2.1</b> Útoky založené na hostitelských systémech.....	7
<b>4.2.2</b> Útoky založené na sítích.....	7
<b>5</b> Generický model procesu detekce průniku.....	7
<b>5.1</b> Zdroje dat	
.....	
..... 8	
<b>5.2</b> Detekce událostí	
.....	
9	
<b>5.3</b> Analýza	
.....	
..... 9	
<b>5.4</b> Odezva	
.....	
..... 9	
<b>5.5</b> Uložení dat	
.....	
..... 10	
<b>6</b> Charakteristiky detekce	

průniku.....	10
<b>6.1</b> Zdroj dat.....	10
<b>6.1.1</b> Datové zdroje založené na hostitelském počítači.....	11
<b>6.1.2</b> Datové zdroje založené na sítích.....	11
<b>6.2</b> Četnost detekce a analýzy událostí.....	11
<b>6.2.1</b> Nepřetržitá/v čase blízkém reálnému času.....	11
<b>6.2.2</b> Periodicky/dávkově zpracovávané.....	11
<b>6.2.3</b> Iniciované pouze při speciálních okolnostech.....	11
<b>6.3</b> Analýza detekce průniku.....	12
<b>6.3.1</b> Založená na zneužití.....	12
<b>6.3.2</b> Založená na anomáliích.....	12
<b>6.4</b> Chování odezvy.....	12
<b>6.4.1</b> Pasivní.....	12
<b>6.4.2</b> Aktivní.....	12
<b>7</b> Role.....	

architektury

.....  
13

**8** Řízení  
IDS

.....  
..... 14

**8.1** Řízení  
konfigurace

..... 14

**8.1.1** Funkce  
detekce

.....  
14

**8.1.2** Funkce  
odezvy

.....  
.. 14

**8.2** Řízení bezpečnostních  
služeb.....

..... 14

**8.3** Integrace s jinými systémy  
řízení.....

..... 14

**8.4** Bezpečnost operací  
řízení.....

..... 14

**8.4.1**  
Autentizace

.....  
..... 15

**8.4.2**  
Integrita

.....  
..... 15

**8.4.3**  
Důvěrnost

.....  
..... 15

**8.4.4**  
Dostupnost

.....  
..... 15

**8.5** Model

řízení

..... 15

Strana 3

Strana

**9** Analýza detekce  
průniku.....  
16

**9.1** Analýza  
signatury  
.....  
16

**9.2** Statistický  
přístup  
.....  
16

**9.3** Expertní  
systémy  
.....  
17

**9.4** Analýza stavových  
přechodů..... 17

**9.5** Neuronové  
sítě  
.....  
. 17

**9.6** Identifikace anomálního chování  
uživatele..... 17

**9.7** Hybridní  
analýza  
.....  
17

**9.8**  
Ostatní  
.....  
..... 17

**10** Problémy implementace a  
nasazení..... 18

<b>10.1</b>	Efektivnost	
.....	18	
<b>10.2</b>	Funkčnost	
.....	18	
<b>10.3</b>	Personál pro nasazení a činnost IDS.....	18
<b>10.4</b>	Další úvahy o implementaci.....	19
<b>11</b>	Problémy detekce průniku.....	20
<b>11.1</b>	Detekce průniku a soukromí.....	20
<b>11.2</b>	Sdílení dat při průnicích .....	20
<b>11.3</b>	Další normalizace .....	21
<b>12</b>	Shrnutí .....	22
	Bibliografie .....	23

Strana 4

---

## 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 souvisejících 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 --