

MEZINÁRODNÍ NORMA

**Informační technologie – Směrnice
pro řízení bezpečnosti IT –
Část 3: Techniky pro řízení bezpečnosti IT**

ISO/IEC TR 13335-3

První vydání

1998-6-15

ICS 35.040

Deskriptory: data processing, information interchange, network interconnection, communication procedure, security techniques, management, rules (instructions).

Obsah

Předmluva.....	5
Úvod	6
1 Předmět normy	7
2 Normativní odkazy	7
3 Definice	7
4 Struktura	7
5 Účel.....	7
6 Techniky pro řízení bezpečnosti IT	7
7 Cíle, strategie a politika řízení bezpečnosti IT	9
7.1 Cíle a strategie bezpečnosti IT	9
7.2 Bezpečnostní politika IT celé společnosti	10
8 Volby strategie analýzy rizik celé společnosti	12
8.1 Základní přístup	12
8.2 Neformální přístup	13
8.3 Podrobná analýza rizik.....	13
8.4 Kombinovaný přístup	14
9 Kombinovaný přístup	14
9.1 Analýza rizik na hrubé úrovni	14
9.2 Základní přístup	15
9.3 Podrobná analýza rizik.....	15
9.3.1 Stanovení hranic revize	16
9.3.2 Identifikace aktiv	17
9.3.3 Ohodnocení aktiv a stanovení závislostí mezi aktivy	17
9.3.4 Odhad hrozeb	18
9.3.5 Odhad zranitelností.....	19
9.3.6 Identifikace existujících/plánovaných ochranných opatření	20
9.3.7 Odhad rizik.....	20
9.4 Výběr ochranných opatření.....	21
9.4.1 Identifikace ochranných opatření.....	21

Sp 260
 ODD. VĚDECKÝCH INFORMACÍ při MZČR
 Palackého nám. 4, 128 01 Praha 2 (34)
 detašované pracoviště NLK Praha 2
 DIČ CZ00023825 IČO 00023825

11 759

Bř. 305/2005 Strana

	Strana
9.4.2	Architektura bezpečnosti IT 22
9.4.3	Identifikace/Revize omezení 23
9.5	Přijetí rizik 24
9.6	Politika bezpečnosti systému IT 24
9.7	Plán bezpečnosti IT 25
10	Implementace plánu bezpečnosti IT 26
10.1	Implementace ochranných opatření 26
10.2	Povědomí o bezpečnosti 27
10.2.1	Analýza potřeb 28
10.2.2	Předání programu 28
10.2.3	Monitorování programů dosažení povědomí o bezpečnosti 28
10.3	Bezpečnostní školení 28
10.4	Odsouhlasení systémů IT 29
11	Sledování 30
11.1	Aktualizace ochranných opatření 30
11.2	Kontrola bezpečnostní shody 31
11.3	Řízení změn 32
11.4	Monitorování 32
11.5	Řešení incidentů 34
12	Shrnutí 35
Příloha A	Příklad obsahu politiky bezpečnosti IT celé společnosti 36
Příloha B	Ohodnocení aktiv 38
Příloha C	Seznam možných typů hrozeb 40
Příloha D	Příklady obecných zranitelností 42
Příloha E	Typy metod analýzy rizik 45

