

Obsah

Úvod	7
1. Hodnocení současné situace	10
1.1 Produkty společnosti Microsoft	11
2. Prognóza do budoucnosti – rok 2000	14
2.1 Viry v 32bitových prostředích	15
2.2 Nové trendy v oblasti makrovirů	20
Makroviry – úvod do problematiky – představení maker	20
Činnost makrovirů	20
Replikace makrovirů	23
Vývoj makrovirů	24
3. Předpokládaný vývoj ochranných prostředků	27
3.1 Vliv šifer na možnost antivirové ochrany	29
3.2 Příklady antivirové ochrany druhé generace	30
3.3 Hardware v antivirové ochraně	32
4. Kryptovirologie – nové nebezpečí	33
4.1 Kryptoviry	34
Virus One_Half	34
Virus KOH	34
Virus LZR	34
Trojský kůň AIDS Information	35
4.2 Útok kryptoviru	35
4.3 Doporučená protipatření	37
5. Definice infiltrací	38
5.1 Hackerství a průniky	38
5.2 Trojské koně	38
5.3 Červi	39
5.4 Počítačové viry	40
6. Druhy virů	42
6.1 Klasifikace podle způsobu umístění do paměti	42
Rezidentní viry	42
Nerezidentní viry (viry přímé akce)	42

6.2 Klasifikace podle napadených oblastí.....	43
Bootové viry.....	43
Souborové viry.....	45
Retroviry.....	49
Klastrové viry ⁶	50
Makroviry.....	50
6.3 Klasifikace podle chování a možností detekce	53
Viry typu stealth a sub-stealth	53
Polymorfní viry	54
Tunelující viry.....	56
Pomalé/rychlé infektory.....	56
Obrněné viry.....	56
„Sparse“ viry	56
6.4 Mutační generátory virů	57
7. Některé projevy působení virů v počítači.....	58
7.1 Úbytek kapacity pevného disku	58
7.2 Změna atributů infikovaných souborů	58
7.3 Zpomalení chodu systému	59
7.4 Náhodné poruchy	59
7.5 Změna operační paměti	59
7.6 Hlášení na obrazovce	59
7.7 Speciální projevy	60
8. Způsoby ochrany výpočetní techniky.....	61
8.1 Zdroje a vstupní body infekce.....	61
Standardní zdroje	61
Prodejci a výrobci softwaru	61
Nelegální a neověřený software.....	62
Internet	62
Úmyslné poškození	64
8.2 Prevence a její zásady	64
8.3 Antivirová opatření.....	70
• Skenery	71
• Monitorovací programy (Generic Behaviour Recognition)	80
Programy pro řízení přístupu (antivirové blokery).....	82
Kontroléry integrity (detektory změn).....	82
Vytváření speciálního MBR	84
Vytváření ochranných plotů.....	84
Bezpečnostní šifrovací programy	84
Antivirový hardware	85
Kombinovaná řešení	86
Rejstřík.....	88