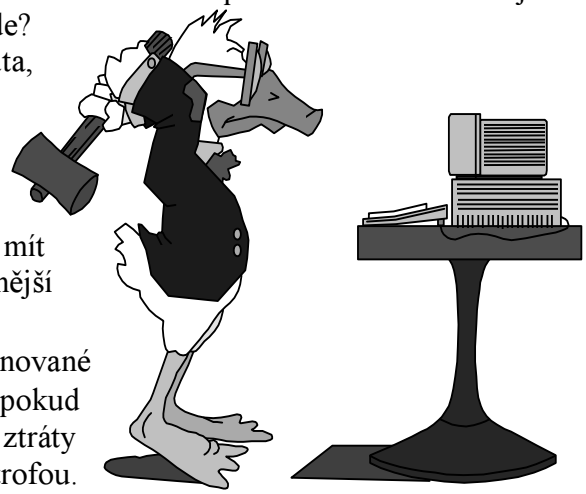
Počítačová bezpečnost

Vysvětlovat vzdělaným uživatelům, že důvěrná data je dobré chránit, by bylo v dnešní době nošením dříví do lesa. Ví ale každý, kde přesně číhá riziko např. zneužití dat a jak k němu může dojít? O co v ochraně dat vlastně jde? Pokud vlastníme nějaká cenná či důvěrná data, v zásadě se mohou stát dvě věci, z nichž lze mít strach. Můžeme o data přijít, nebo je může získat někdo, kdo si naši důvěru nezaslouží, případně se nám může stát obojí, tj. naše důvěrné informace bude mít někdo jiný a my nebudeme mít nic. Mezi první případ můžeme počítat nejrůznější havárie disků, virová napadení…



Na tyto rány je nejlepší *zálohování*. Dobře plánované a provedené zálohování nám umožní dobře spát, pokud se bojíme nechtěného smazání dat nebo jejich ztráty způsobené technickou chybou či přírodní katastrofou. Zálohu je dobré uchovat na jiném místě než zálohovaná data. Doporučuje se mít dvě zálohy jedněch dat, rozmístěné na geograficky odlehlých místech.

Pokud však jde o zabránění přístupu nepovolaných k důvěrným datům, jedinou spolehlivou ochranou souborů je kvalitní šifrování. *Šifrování* totiž jako jediná metoda dokáže oddělit uživatele vlastnícího klíč od osob, které klíč nevlastní. Pokud vlastníte klíč, získáte po rozšifrování souboru důvěrná data, pokud ne, dostanete maximálně nesmyslnou změť znaků, v odborném slangu známou jako „rozsypaný čaj“. Není však šifra jako šifra a není snadné bez odborných znalostí oddělit silnou kvalitní šifru od slabých a snadno rozluštitelných.

Prameny:

Softwarové noviny	čísla 2/99, 4/99 a 7/99
časopis PC WORLD	čísla 1/99 a 5/99
časopis CHIP	číslo 3/99
časopis Počítač pro každého	číslo 11/99

Nejpoužívanější antivirové programy

1	Antiviral Toolkit Pro (AVP)
2	F-Secure® Anti-Virus
3	Avast32
4	NOD 32
5	AVG

1 Antivirové programy

Počátky počítačových virů

Počítačové viry představují vážnou hrozbu pro uživatele od konce osmdesátých let. První funkční vir byl vytvořen v roce 1981 pro platformu Apple, ale vzhledem k poměrně malému rozšíření osobních počítačů v tehdejší době se nedočkal větší „popularity“. Po pěti letech,

s rozšířením PC, se objevují i první viry pro tuto platformu a přes počáteční „nesmělost“ se po dvou letech stávají skutečnou hrozbou, jak ostatně uvádí následující příklad. Dne 2. září 1988 kolem 18. hodiny místního času vypouští postgraduální student Cornellovy univerzity Robert Morris do rozvíjející se sítě Internet svůj síťový program Worm (Červ), který napadl velké množství počítačů v celých Spojených státech od východního k západnímu pobřeží. Následkem tohoto „útoku“ je pád asi 6000 počítačů (pro srovnání v tehdejší době to bylo něco kolem osmi procent uživatelů Internetu). V následujících hodinách se formuje zvláštní skupina VirusNet, jíž se po 24 hodinách hektické práce daří Červa zastavit. Dohra tohoto případu se odehrávala v soudní síni a Roberta Morrise stál jeho Červ tři roky vězení podmíněně, pokuta 10 000 amerických dolarů a 400 hodin veřejných prací. K podobnému případu došlo také 13. května 1988, kdy několik univerzit a velkých společností napadl vir Jeruzalém, který se projevoval likvidací souborů, které se jejich uživatelé pokoušeli spustit. Tento vir napadl množství počítačů po celém světě.

Základní druhy počítačových virů

- **Rezidentní viry** – při spuštění PC se nelegálně umístí do paměti a i po skončení své činnosti zůstane jeho část v paměti. Pak je schopen napadat každý nově spuštěný program, může se libovolně množit a narušovat činnost počítače a následně souborů a dat.
- **Souborový virus** – je uložen ve spustitelném s příponami COM, EXE, BIN, SYS. Může přepsat některou jejich část tak, aby funkčnost původního programu zůstala zachována. Virus se pak aktivuje při každém spuštění aplikace (souboru).
- **Bootovací virus** – boot je část pevného disku, ovládající start systému při zapnutí PC. Boot sektorový virus nahradí originální boot sektor disku a většinou také tabulku rozdělení disku svým vlastním programem a načte virus do paměti. Poté se může tento virus samovolně šířit na další disky (diskety) i bez kopírování souborů.
- **Worm (červ)** – program, který se sám rozmnožuje na počítači obvykle tak, že se zapíše do operační paměti. Může se sám zkopírovat na jednom počítači tolikrát, že nakonec způsobí jeho zhroucení tak, že se naplní paměti počítače, až v nich není žádný prostor pro další programy.

Č.	Název ochranné organizace	Díla, která chrání
1.	Ochranný svaz autorský pro práva k dílům	Psaná díla
2.	Intergram	Díla hudební
3.	Ochranná organizace autorská	Výtvarné umění, obrazové složky audiovizuálních děl
4.	Dilie	Díla divadelní (dramatická)

Možnosti ochrany proti počítačovým virům

Podle určitých příznaků lze rozpoznat virovou nákazu dříve, než se sám začne projevovat. Programy se zavádějí déle, pracují pomaleji, odzkoušené programy přestávají fungovat, aj. hlavním opatřením pro ochranu proti virům je prevence. Každý uživatel by měl dodržovat určité zásady jako nevyměňovat bez kontroly další diskety s jinými, pravidelně zálohovat data a kontrolovat pevný disk a všechny používané diskety antivirovým programem (AVG), nikdy nespouštět neznámé programy na počítači s pevným diskem, na němž jsou důležitá data, nenechávat zbytečně disketu v disketové mechanice a další.

Počítačová kriminalita

Informační technologie se neustále rozvíjejí, což má za následek, že zpracování informací a dat se stává dostupnější stále většímu počtu uživatelů. To však také způsobuje, že se informace stávají zbožím. Objevuje se také nový druh trestné činnosti – počítačová kriminalita. S tím souvisí útoky proti datům, útoky proti programovému vybavení, proti výpočetní a komunikační technice.

Na závěr trochu složitější tabulka

	I	II	III
3	🗁 You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather. 🗁 You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the intent is to exercise the right to control the distribution of derivative or collective works based on the Program 🗁 If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way. In addition, mere aggregation of another work not based on the Program.		
2			
1			

3 **Trochu složitější tabulka**

Seznam tabulek

Křížové odkazy

V tabulce 1 na straně 1 jsme uvedly některé antivirové programy. České organizace na ochranu práv autorských jsou uvedeny v tabulce 2 na straně 3. Tabulka s názvem *Trochu složitější tabulka* ukazuje, jak lze měnit tok textu a slučovat buňky.