SOC706

3. povinný úkol

Robert Beneš, 144474
Radim Kameník, 144332
Vojtěch Kozubík, 144416

Předmět výzkumu: Počítačová kriminalita a její předcházení

Cíl výzkumu

Vzhledem k rostoucí komplikovanosti a společenské nebezpečnosti počítačových zločinů je nutné zaměřit se na prevenci, obranu počítačů a informačních systémů, neboť jedině tak je možno se účinně bránit proti tomuto druhu trestné činnosti. Prevence je zde prakticky jediným obranným mechanismem, jelikož působení represe při vyšetřování této trestné činnosti je velmi omezené.

Cílem tohoto výzkumu proto bude přispět k rozvoji metodologie boje proti počítačové kriminalitě, představit tento druh kriminality veřejnosti a zjistit, jaké metody prevence jsou dnes institucemi běžně užívány.

Tyto informace také slouží jako podklady pro realizování programu Ministerstva Vnitra ČR na podporu boje proti počítačové kriminalitě.

Výzkumná otázka: ¨

Snižuje použití obranných mechanismů u finančních institucí a bank počet útoků v oblasti počítačové kriminality?

Odvozené otázky:

1) Jaké prostředky vynakládají finanční instituce a banky na tyto obranné mechanismy vzhledem ke svému ročnímu obratu?
2) Jak často dochází k aktualizaci obranných mechanismů?

3) Byly tyto obranné mechanismy někdy v minulosti již prolomeny?
4) Jsou společnosti více napadány zvenčí, nebo zevnitř společnosti?
5) Jaká je charakteristika nejvíce napadaných společností?

Kontext tématu

Počítačová kriminalita zahrnuje trestné činy namířené proti integritě, dostupnosti nebo utajení počítačových systémů, případně trestné činy v tradičním smyslu, při kterých je použito moderních informačních či telekomunikačních technologií. Jako taková se objevila s nástupem počítačového věku, v České Republice v 70.letech. V dnešní době na našem území neexistuje jediná instituce, která by se počítačovou kriminalitou systematicky zabývala. Vyšetřování jakékoliv trestné činnosti je doménou Policie a tak jedinou výjimkou na tomto poli je útvar Informační kriminality ředitelství služby kriminální policie při Policejním prezidiu v Praze.

V ČR je chronický nedostatek publikací zabývajících se tímto tématem, což znamená, že prakticky jediným existujícím zdrojem informací je internet (ověření relevance dat je nemožné), většinou však v cizojazyčné podobě. Chybí zde tedy jakákoliv možnost široké veřejnosti, ale i odborníků, seznámit se s tímhle celosvětovým fenoménem a s jeho předcházením.

Provedení výzkumu

Všechny finanční instituce a banky působící v ČR musí být podle zákona zaregistrovány. Populaci tedy budou tvořit všechny zaevidované finanční instituce a banky v ČR.
V našem výzkumu budeme vycházet z informací Českého statistického úřadu, jež vede statistiku finančních institucí a ze statistik a analýz těchto institucí.

V tomto případě tedy použijeme náhodný stratifikovaný výběr. Populaci (finanční instituce) rozdělíme do několika

homogenních skupin (realitní kanceláře, investiční fondy, penzijní fondy apod.) a tyto skupiny budou posléze do vzorku náhodně rozděleny technikou systematického výběru.

Tento kvantitativní výzkum bude proveden formou dotazníku hlavně z důvodu velkého počtu institucí a také proto, že forma odpovědí je z větší části jednoslovná.

Příklad:

1) Používáte firewall? Ano-ne
2) Vaše náklady na obranu proti napadení z vnější sítě jsou: menší, větší než 5 apod.…

Z důvodu malé návratnosti dotazníků použijeme metodu zvanou follow-ups. Po 3 týdnech pošleme těm institucím,které neodpověděly „upomínku" na korespondenčním lístku a pokud ani po dalších dvou týdnech neodpoví, pošleme jim další exemplář dotazníku.

Zkoumaná populace

Výzkumnou jednotkou zde budou finanční instituce a banky zaevidované v ČR, respektive správci počítačových sítí či jiní zaměstnanci odpovídající za zabezpečení výpočetní techniky, přičemž bude využito také záznamů a statistik institucí, zejména u problematiky prolomení obranných mechanismů. Vzhledem ke specifické problematice a nízkému počtu finančních institucí a bank bude základní vzorek obsahovat 300 jednotek.

Operacionalizace

Finanční instituce- jiná právnická osoba než banka podle zákona o bankách, která v rámci svého podnikání jako svou rozhodující či podstatnou činnost nabývá podíly na jiných právnických osobách nebo provádí některou z činností uvedených v § 1 odst. 1 a 3 zákona o bankách, a dále investiční společnost, investiční fond, penzijní fond a pojišťovna, které vykonávají činnosti podle zvláštních zákonů, to vše včetně osob se sídlem v zahraničí a s obdobnou náplní činnosti.

Indikátory: spořitelny, úvěrové společnosti, penzijní fondy, investiční společnosti, pojišťovací společnosti, makléřské společnosti, realitní kanceláře a burzy.

Banka - právnická osoba se sídlem v České republice založená jako akciová společnost, která
a) přijímá vklady od veřejnosti a
b) poskytuje úvěry
a která k výkonu činností má bankovní licenci.
Indikátory: komerční banky, investiční banky, poštovní banky

Obranné mechanismy-všechny mechanismy, které zabraňují pachatelům počítačové trestné činnosti neoprávněně využít počítače a jeho komunikačních zařízení k soukromým účelům, neoprávněně využít počítače a jeho komunikačních zařízení k páchání jiné trestné činnosti a znemožnit tvorbu a rozšiřování počítačových virů.
Indikátory - registrační číslo, antivirové programy, kódování programů, zabezpečovací certifikáty,přístupová hesla, registrační soubory a šifrovací protokoly

počítačová trestná činnost-Trestný čin namířený buďto proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je použito moderních informačních či telekomunikačních technologií
Indikátory: hacking, carding, phreaking, padělání, penězokazectví, spamming, warez, sniffing a šíření virů.

Zdůvodnění zájmu o zkoumanou otázku
Tato problematika je popsána v Cíl výzkumu a Kontext tématu.

Doba provedení výzkumu
Výzkum bude proveden v lednu 2005 a po zpracování dat bude uveden ve známost v září 2005.

Nějak mi uniká sociologická dimenze výzkumu. Jeví se to ryze technicky. Navíc to zní trochu jako marketingový průzkum o používaném softwaru, informovanosti firem ohledně možného zabezpečení atd.

Literatura k tématu:

Matějka, Michal, Počítačová kriminalita, Praha, Computer Press 2002

Červeň, Pavol, Cracking a jak se proti němu bránit, Praha, Computer Press 2001

Papke, Jerry, Combating Computer Crime, New York, McGraw-Hill, Inc 1992

Dastych, Jiří, „Co přináší IT do současného bankovnictví…", *Bankovnictví*, 21.11. 2002, s. 29-30

Dastych, Jiří, „Český internet a kriminalita", *Computerworld*, 1.10. 2001, s. 11-12

Smejkal, Vladimír, „Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku", *Trestněprávní revue*, červen 2003: 161-167

Ewans, Paul, „Computer Fraud-The Situation, Detection and Training", *Computers and Security*, 1991, s. 325-327

Belden, Menkus, „Eight Factors Contributing to Computer Fraud", *Internal Auditor*, 1990, s. 71-73

Syrowik, David, „Patent Protection for Software Technology-A Powerful New Form of Protection", *Michigan Bar Journal*, 1988, s. 968-974

Budka, Ivan, Dvořák, Vratislav, Bosák, Jan, „Zneužívání výpočetní techniky pro bankovní podvody a možnosti Kriminální policie při jejich odhalování", in Kol., *Kriminalistická problematika při odhalování, vyšetřování a prevenci počítačové kriminality*, Sborník odborných sdělení ze semináře uskutečněného na PA ČR, Praha, 23.prosince 1996, red. Suchánek Jaroslav, Praha, PA ČR, s. 97-101

Krošlák, Pavol, „Právní ochrana počítačových programů a boj proti počítačovému pirátství“ in Kol., *Ochrana výpočetní techniky a dat, počítačová kriminalita*, Sborník referátů a sdělení ze seminářů, Praha, 8.listopadu a 13.prosince 1990, red. Jan Hlaváček, Praha, Ringo, s. 26-35
Koubský, Petr „Zaklínadla postmoderního věku: uhlídat bezpečnost informačních systémů je téměř nemožné“, *Respekt*, 23.2. 2004, s. 18
ČTK, „Státy nezvládají kyberdžungli: jen v Německu počítačová kriminalita přesáhla polovinu veškeré trestné činnosti“, *MF Dnes* (Praha), 20.9. 2004