# ROZHOVOR PRO ČASOPIS CONNECT

**Karel Miko – DCIT, s.r.o.**
http://www.dcit.cz

**Michal Hroch – Connect**
http://cpress.cz

Zveřejněno v čísle 4/2003

**MH: Co považujete v současnosti za nejvě tší bezpečnostní hrozbu pro firemní sektor?**

KM: Myslím, že zcela jednoznačně je ve většině případů největší hrozbou lidský faktor – tj. vlastní zaměstnanci. Jelikož v běžném provozu nelze vše vynutit technickými opatřeními, je nutno řadu věcí řešit organizačně a spoléhat na kázeň zaměstnanců. Pokud jde o klasické hrozby, kam pravděpodobně míříte svou otázkou, hodnotím relativně vysoko hrozbu červů a jiného škodlivého software – v této oblasti očekávám, že nejhorší teprve přijde.

**MH: Kde jsou dnes subjekty z tohoto segmentu nejzranitelnější?**

KM: Pokud bych to měl vzít čistě na základě mého empirického pozorování z různých prostředí našich zákazníků, je z hlediska konvečních hrozeb relativně vysoká zranitelnost vůči vnitřním útokům, poněvadž v případě interních systémů je obvykle kladen důraz především na jejich funkčnost nikoli však na bezpečnost. Pokud se opět vrátím k lidskému faktoru a nekázni uživatelů, jsou firmy hodně zranitelné různými formami social hackingu (využití sociálního inženýrství). Dále se v praxi často také setkávám se zranitelnostmi, jež plynou z překotného zavádění nových, nevyzkoušených technologií.

**MH: Domníváte se například stejně jako pan Kaspersky, že by měl se měl každý člověk přistupující na Internet identifikovat?**

KM: Předpokládám, že pravděpodobně narážíte na výroky pana Kasperskeho z letošního CeBITu. Můj názor je NE a jsem hluboce přesvědčen, že tudy cesta nevede. Z hlediska bezpečnosti by povinná identifikace nepřinesla žádný přímý posun k lepšímu. Byl by to víceméně jen zastrašující nástroj, realita by velmi pravděpodobně dopadla tak, že běžní „nevinní“ uživatelé by byli pod policejním dozorem a ti, kteří hodlají provádět nekalosti, by zcela jistě brzy přišli na způsob, jak si pořídit falešnou nebo zneužít cizí identitu. Do jisté míry je to filozofická otázka, poněvadž je to zcela nepochybně vpád do soukromí a podle mého názoru zapadá do současných politických tendencí omezování osobních svobod jednotlivců pod záminkou boje proti terorismu či jiným negativním jevům. Myslím si, že přiměřená míra anonymity je součástí filozofie Internetu (koneckonců podobně jako v běžném životě). Pokud jde o zhroucení Internetu, které pan Kaspersky v důsledku rostoucí anarchie předvídá, jsem optimista, neboť Internet už několik podobných očekávaných kolapsů přežil.

**MH: Co je podle Vašeho názoru ideální nosič identifikace uživatele a proč?**

KM: Prokazování totožnosti má dva základní kroky, a to identifikaci (dotaz: „kdo jsi?“) a autentizací (dotaz: „dokaž, že jsi ten, za koho se vydáváš“). Pokud bych měl popsat ideální způsob uchovávání identifikačních a autentizačních informací, mělo by to být něco, co může uživatel mít neustále při sobě (HW předmět), použití tohoto nosiče musí být chráněno (např. PINen), nosič s identifikací uživatele musí být odolný vůči zkopírování a pozměnění údajů, u citlivých údajů typu certifikáty by mělo být zaručeno, že nikdy neopustí nosič.

**MH: Jak pohlížíte na projekty Identifikace přímo na internetu (project Liberty Alliance a MS Passport)?**

KM: Pohlížím na ně s odstupem. Obě technologie přináší spíše ulehčení života uživatelům a provozovatelům různých služeb (WWW aj.) než že by přispívaly ke zvýšení bezpečnosti. Osobně jsem díky své profesi člověk opatrný až paranoidní, tudíž pokud byste se mě zeptali, zda-li bych svá osobní data (včetně např. čísla platební karty, jak optimisticky zamýšlí tvůrci některých těchto technologií) uložil na nějaký identity server, tak dnes rozhodně ne. Kumulace osobních údajů, kterou tyto technologie přinášejí, představuje nemalá rizika a není mi zcela jasné, jakým způsobem si chtějí provozovatelé získat důvěru uživatelů.

**MH: V čem spatřujete do budoucna největší pole působnosti, který bezpečnostní trh se bude nejlépe vyvíjet (antiviry, firewally, antispamová ochrana, ...)?**

KM: Klasické technologie jako firewally či antiviry si nepochybně svůj význam udrží, pokud bych měl odhadnout, ve kterých oblastech lze očekávat výraznější rozvoj (z hlediska odbytu), vsadil bych na IDS systémy a systémy na monitoring a zpracování logů.

**MH: Existuje systém, který by se nedal prolomit? Pokud ano, jaké musí mít vlastnosti?**

KM: Já rozhodně nehlásám názor, že každý systém lze napadnout. Nicméně při dnešní rostoucí složitosti systémů vám bezchybnost není schopen garantovat ani sám výrobce, tudíž jistotu bezpečí nemůžete mít nikdy. Naopak četnost odhalovaných bezpečnostních slabin nás ujišťuje o tom, že v každém systému ještě minimálně jedna nezveřejněná slabina existuje. Přesto lze s využitím současných běžně dostupných technologií navrhnout a postavit systém, o kterém jsem schopen prohlásit, že je bezpečný (v daném čase). Jaké by měl mít vlastnosti je na delší diskuzi, zjednodušeně řečeno, je potřeba postavit dostatečné množství překážek na všech frontách a už v návrhu počítat s tím, že některé z nich mohou být prolomeny.

**MH: Dá se někdy předpokládat vyrovnání neustálého boje mezi antiviry a viry, když viry jsou neustále napřed.**

KM: Zcela jistě ne, neboť to není v zájmu ani jednoho z aktérů tohoto souboje. Nutno si uvědomit, že „nahrávky na smeč“ tvůrcům virů přichází vesměs od výrobců jednotlivých systémů či aplikací nikoli od tvůrců antivirů. Pokud tedy je někdo schopen sebrat vítr z plachet autorům virů, jsou to právě tito výrobci.

**MH: Co si lze představit pod pojmem Security Service Providing? Jedná se pouze o pojem, nebo se stává trendem?**

KM: Jedná se specifickou formu outsourcingu, kdy předmětem poskytovaných služeb je zajištění bezpečnosti provozovaných technologií – tj. kombinace dohledové služby, administrace a údržby systémů, detekce a řešení bezpečnostních incidentů. Netroufám si tvrdit, že to je dnes jednoznačný trend, ovšem díky rostoucí složitosti provozovaných systémů bude pro řadu firem s postupem času této typ služeb výhodnější než zaměstnávání vysoce specializovaných odborníků.

**MH: Co všechno může očekávat firma od dodávky komplexní služby bezpečnosti?**

KM: Jednak je třeba si uvědomit, že bezpečnost není něco, co lze jednou koupit a tím problém definitivně vyřešit. Osobně komplexnost dodávky vidím především v tom, že spolu s technologií je dodána také patřičná znalost (odborná instalace, školení) a kromě technického řešení je součástí dodávky rovněž nastavení patřičných organizačních opatření a interních procesů souvisejících s provozem dodané technologie.

**MH: Jakým způsobem se dá bojovat proti nedůvěře zákazníků v závislost/nezávislost bezpečnostních auditů.**

KM: Osobně se ve své praxi nesetkávám s pochybnostmi ohledně (ne)závislosti, v praxi je to spíše tak, že řada společností považuje bezpečnostní audit za něco zcela zbytečného a postradatelného – tudíž bojujeme spíše na této frontě. Pokud se firma pro bezpečnostní audit rozhodne, většinou jeho přínosy vyplynou z jeho výsledků poměrně přímočaře.

**MH: Jaký je dle Vašeho názoru stav bezpečnosti v mobilních komunikacích?**

KM: Technologie používané v mobilních komunikacích obsahují poměrně širokou škálu bezpečnostních mechanizmů (šifrování apod.). Osobně očekávám rostoucí rizika spojená s čím dál sofistikovanějšími telefony, u kterých je jen otázkou času, kdy začne vznikat ve větším měřítku škodlivý SW napadající právě mobilní telefony – což je v současnosti hrozba téměř nepokrytá.