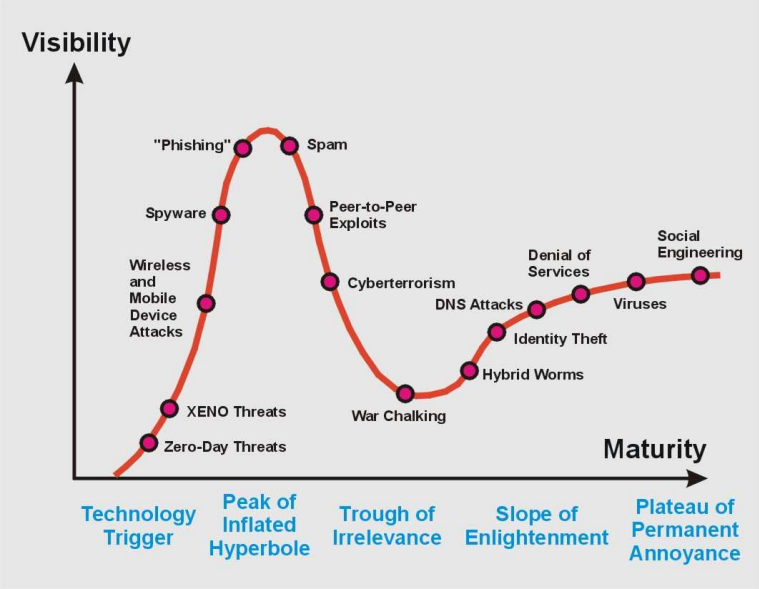
Pohled na bezpečnostní hrozby v informatice a telekomunikacích na přelomu roku 2004/2005

Roman Rak - Policejní akademie ČR v Praze
Viktor Porada - Policejní akademie ČR v Praze

Magické gartnerovské kvadranty vyjadřující dokonalost či perspektivy nejrůznějších výrobků zná ve světě ICT snad každý, kdo stál před rozhodnutím vybrat či doporučit pro svou instituci nový, perspektivní SW či jiný produkt, srovnat mezi sebou různé výrobce apod. Koncem roku 2004 jsou v odborné literatuře publikovány různé kybernetické hrozby, které lze nejlépe dokumentovat novým, zatím ne na veřejnosti příliš známým typem grafu – pomocí tzv. Hype Cycle diagramu, který Gartner nyní velmi hojně využívá pro dynamické srovnání specifických trendů.

Tento příspěvek si klade proto za cíl dva úkoly. Prvním úkolem je seznámit čtenáře s časovým vývojem základních trendů bezpečnostních hrozeb v oblasti ICT na přelomu roku. Druhým cílem je tento vývoj prezentovat pomocí HypeCycle diagramu a na základě zcela konkrétních a aktuálních bezpečnostních hrozeb vysvětlit jeho universální podstatu.



Obr. 1 Kybernetické hrozby ke konci roku 2004 znázorněné pomocí Hype Cycle diagramu společnosti Gartner.

Na svislé ose (*y*) diagramu (viz Obr. 1) je vyjádřena míra výskytu dané hrozby (její „viditelnost“, publicita, věnovaná odborná pozornost), na ose horizontální (*x*) pak vyspělost hrozby (u produktů vyspělost technologie, řešení). Jinými slovy – v levé části osy *x* nalezneme zcela nové hrozby (obecně produkty), které se teprve začínají objevovat v praxi (na trhu) nebo se o nich začíná diskutovat. V pravé části se nachází „ustálené“, velmi vyspělé hrozby, hrozby „stálice“, které se již staly součástí každodenního života. Jestliže bychom srovnávali SW produkty např. ERP systémy, na pravé části diagramu bychom našli řešení mySAP.

Každá hrozba (či produkt) zpravidla ve svém historickém vývoji prochází postupně grafem zleva doprava. Nejprve se objevuje s nějakou novou technologií, aby se nakonec za nějakou dobu „ustálila“ a stala se stálou, vyspělou hrozbou, které je nezbytně nutné věnovat neutuchající pozornost. Některé hrozby ale nemusejí projít všemi oblastmi, mohou se „ztratit“, přestat existovat a v druhé polovině pravé části grafu se nemusejí pak již dále objevovat.

Křivka grafu je pak rozdělena do pěti základních, logických oblastí, které mají svá specifika:

Oblast první - Technology Triger („*technologičtí spouštěči*“**)** – oblast zcela nových hrozeb, které se objevují s novými, perspektivními technologiemi, které se teprve začínají objevovat na trhu. Obecně novinky na trhu nebo ve sledované oblasti. Patří sem hrozby typu:

a. „*Zero-Day*“ – cílené útoky na technologické chyby výrobců SW nebo HW produktů ještě před tím, než výrobce distribuje opravné nástroje (např. SW patche). V okamžiku, kdy někdo zjistí slabinu technologie nebo zařízení, začne ji masově a cíleně napadat.
b. *XENO* (*eXtended Enterprise Networks Overseas*) hrozby se začínají objevovat v důsledku outsourcingů v oblasti IT, kdy není dostatečně zajištěna ICT bezpečnost, nejsou vyjasněny vztahy a odpovědnosti mezi outsourcovaným a outsourcujícím subjektem.
c. *Útoky na mobilní zařízení a bezdrátové (WiFi) produkty*. V těchto zařízeních se vyskytují viry podobně jako v klasické výpočetní technice.

Oblast druhá - Peak of Inflated Hyperbole („*vrchol zvýšeného zájmu*“ nebo též překládáno jako „*vrchol očekávání*“). Sem zařazujeme hrozby (produkty), o kterých se nejvíce hovoří, je jim věnována maximální odborná pozornost, směřováno maximální úsilí na ochranu. Oblast usilovných „marketingových“ aktivit výrobců ochranných prvků. Je to často i záležitost určitých módních trendů, jejichž oprávněnost se časem může zcela rozplynout.

a. *Spyware (špionážní programy)***,** monitorující chování uživatele, jeho činnost v počítači bez jeho vědomí a souhlasu. Krádeže znalostí nebo vlastnictví a jejich přenos k útočníkovi – soubory, technologická-know, průmyslová špionáž apod.
b. „*Phishing*“ *(„rybaření“)* – zcizování digitální identity uživatele, jeho loginů, hesel, čísel bankovních karet a účtů apod. za účelem jejich následného zneužití – výběr hotovosti z konta, neoprávněný přístup k funkcionalitám programů, datům atd.
c. *Spam (zahlcování)* – omezování prostoru, výkonnosti technologických zařízení, ztráta času uživatele (nebo jiné negativní dopady) rozesíláním nevyžádaných informací, datových souborů.
d. *Peer-to-peer Exploits* – zneužívání slabin komunikace typu peer-to-peer („rovný s rovným“).

Oblast třetí - Trough of Irrelevance někdy též **Trough of Disillusionment** (*„dno irelevantnosti či rozčarování*“). Hrozby (či produkty ve světě komerčním), o kterých se již přestává mluvit, mají svůj vrchol pozornosti již za sebou. Oblast nenaplněných nadějí, očekávání, tj. původní předpoklady se nestaly skutečností. Hrozba není již v módě. Tlak na opuštění iniciativ, spojených s touto hrozbou. Může se zdát, že hrozba je v této etapě nereálná.

a. *Kybernetický terorismus* – po útocích na světové obchodní centrum v New Yorku 11. září 2001 se předpokládalo, že kybernetický terorismus se stane novou hroznou zbraní útočníků. Nebyly ale zaznamenány žádné významné aktivity v této oblasti, takže se o dané problematice (dočasně?) přestává hovořit. Ostražitost bezpečnostních specialistů v tomto případě ale neklesá.
b. *War Chalking.* Skupina hrozeb průniku do bezdrátového WiFi počítačového spojení. Původně hackeři v městech označovali křídou (angl. *chalk*) na

chodníku místa, kde byl dobře zachytitelný WiFi signál, ke kterému měli bezproblémový přístup. V širším slova smyslu se pod tímto názvem dnes skrývá řada hackerských technik, pomocí kterých lze proniknout do nechráněné WiFi sítě. Nástup WiFi technologií byl provázen obrovskou fascinací uživatelů. Technologie WiFi byla z hlediska možných odposlechů silně zranitelná a více jak 90% komunikace bylo otevřené. V současnosti se zabezpečení WiFi technologií věnuje značná pozornost, takže War Chalking ustupuje z „módní vlny".

Oblast čtvrtá - Slope of Enlightenment („*svah znovurození, renesance*"). Hrozba, nebo technologie (produkt) se postupně, nenápadně stává běžnou realitou, začíná se denně vyskytovat ve velké míře. Ztrácí se módnost, nastupuje tvrdá realita.

a. *Hybridní červi* **–** specifické, těžko odhalitelné formy virů, které se dokáží skrývat, modifikovat sami sebe.
b. *Krádeže identity* – krádeže identity uživatele v digitálním prostředí. Pachatel pak vystupuje pod ochranou zcizené identity a minimalizuje odhalení své skutečné identity, která pak nemůže být spojována s jeho nelegální činností.
c. *Útoky DNS (Domain Name System).* Útoky na distribuovanou datovou službu s replikací, zajišťující decentralizovaným způsobem překlad jména hostitele (počítače) na jeho IP adresu a naopak.
d. *Denial of Service (odmítnutí služby)* – Typ útoku proti počítačovému systému. Útok zabrání autorizovanému přístupu ke zdrojům, nebo způsobí zpoždění časově kritických operací. Útočník zatíží server tolika požadavky, že dojde k vyčerpání všech volných zdrojů a následně k havárii služby nebo dokonce ke zhroucení celého serveru.

Oblast pátá, poslední - Plateau of Permanent Annoyance *(„rovina neustálých zlobičů"- u technologických produktů hovoříme o vyzkoušených, stabilních a jistých řešeních)* – hrozba se reálně projevuje v běžné praxi, je masově rozšířena a způsobuje závažné problémy (extremně vysoké škody) svou vysokou technologickou nebo sociologickou vyspělostí.

a. *Viry* **–** díky Internetu se dnes šíří obrovskou rychlostí, za několik hodin dokáží zamořit celý svět. Způsobují obrovské ekonomické ztráty napadených institucím i jednotlivcům.
b. *Sociální inženýrství* - je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využít lidí, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace. Technologická úroveň zabezpečení výpočetní a komunikační techniky neustále roste a stává se poměrně vyspělou. Proto pozornost útočníků je věnována na nejslabší článek řetězce a tím je člověk – uživatel, který nechtěně vyzrazením určitých informací degraduje celou technologicky orientovanou ochranu informačních systémů.

Závěr

HypeCycle diagram je intuitivním grafickým nástrojem pro zobrazení vývojových trendů jakéhokoliv lidského produktu či stavu a zcela jistě se s ním budeme v praxi stále více setkávat. Můžeme jej použít pro výstižnou charakteristiku SW produktů, stejně jako určitých typů bezpečnostních hrozeb či stavů našeho zájmu.

Literatura

[1] Matoušková, I.: *Psychologie a taktika prosazování investic do informační bezpečnosti ve firemní sféře*. Security Magazín, č.4/2004, str. 48-49

[2] Porada,V., Nečas, S.: *Bankovní bezpečnost jako součást bezpečnostní politiky organizace.* Bezpečnostní teorie a praxe, zvl. číslo. Praha : PA ČR, 2001 s. 437-448

[3] Spurný, J.: *O psychologickém přístupu k ochraně informací*. In. Psychologie v ekonomické praxi, 1999, roč. XXXIV. Č.3-4. s 199-203

Doc. Ing. Roman Rak, Ph.D., externí spolupracovník katedry kriminalistiky Policejní akademie ČR Praha, Lhotecká 559/7, Praha 4, E-mail: roman.rak@ct.cz

Dr.h.c. prof. JUDr. Ing. Viktor Porada, DrSc, Policejní akademie ČR Praha, Lhotecká 559/7, Praha 4, E-mail: porada@polac.cz