

Security Upgrade 1 konference 0

Závěrečná zpráva z konference Security Upgrade 2010

Základní data:

- **Termín konání:** 4. listopadu 2010
- **Místo konání:** hotel Diplomat, Praha
- **Účastníci:** IT odborníci, IT manažeři, IT konzultanti, CIO a CEO manažeři, ředitelé, management a ostatní pozice z řad českých firem, úřadů a institucí
- **Počet účastníků:** 72

Partneři:

Seznam.cz, S&T CZ, RSA, Kernum, VERGILIUS IT Expert, Zyxel, McAfee, Symantec, Belkin,

Mediální partneři:

Svět Hardware, System online, Parlament–Vláda–Samospráva

Report:

Svět informační bezpečnosti se mění ze dne na den, často dokonce z hodiny na hodinu. Takovou dynamiku nemá žádná jiná oblast IT. A tak není divu, že společnost 4U SUPPORT pořádá konference věnované otázkám informační bezpečnosti dvakrát do roka – vždy před zaplněným sálem a za velkého zájmu partnerů.

Abychom pochopili pravdivost výše uvedeného tvrzení o dynamických proměnách informační bezpečnosti, stačí jen zmínit škodlivý kód Stuxnet. Ten se stal noční můrou všech bezpečnostních firem i lidí za zajištění bezpečnosti přímo zodpovědných. Přitom v době konání jarní konference Security Forum 2010 se světem nade vši pochybnost šířil (jeho vznik je datovaný do roku 2008 nebo 09; přesněji to nejsme schopni zjistit). Přitom o něm nikdo neměl ani potuchy. V rámci konference Security Upgrade 2010 pak byl zmiňovaný snad v každé druhé přednášce – a pokaždé ve zcela jiné souvislosti (takže to nebylo tím, že by prezentující neměli o čem hovořit).

Konference Security Upgrade 2010 proběhla ve čtvrtek 4. listopadu 2010 v tradičních prostorách pražského hotelu Diplomat – před zcela zaplněným posluchačským sálem. Zahajovací přednáška konzultanta a publicisty Tomáše Příbyla nesla název **Staré i nové hrozby** a představovala průřez aktuálními trendy stejně jako netradičními a netypickými hrozbami (které by se ovšem velmi rychle mohly stát tradičními a typickými). Přinesla průřez od nových metod phishingu (whaling, TagNabbing) přes záměrné chyby v počítačových programech a nebezpečné bezpečnostní programy až po hardwarovou špionáž (na úrovni výrobců, nikoliv různých hardwarových „udělátek“ s key-loggery) nebo nebezpečí geografické lokace. Na závěr pak upozornil i a skutečnost, že kybernetičtí útočníci rychle pochopili význam nových technologií jako je cloud computing a virtualizace pro svoji činnost.

Druhá prezentace „**Jak jednoduše vybudovat základy Security Operation Center?**“ měla svoji teoretickou (na svá bedra si ji vzal Ivan Svoboda) i praktickou část (David Matějů, oba RSA Security). Věnovala se čím dál aktuálnějšími otázkám monitoringu, který má mnohem větší přesah, než pouze řešení bezpečnosti: zajišťuje např. soulad (compliance) s legislativou nebo normami. Prezentace se zaměřila na možnosti vybudování a provozování Security Operation Center v malých a středních firmách, které podobné řešení často považují za luxus a doménu „těch velkých“.

Ryze praktickou přednáškou bylo následné vystoupení Petra Koudelky (ZyXEL) „**Bezpečnost až na prvním místě aneb Podniková bezpečnost jednoduše.**“ Představil možnosti zabezpečení podnikového systému s pomocí „klasických“ technologií jako je VPN, IDP, antivirová ochrana, filtr spamu či obsahu. (Je zajímavé, že i přednášející představující pokročilá řešení pro zajištění bezpečnosti, se vzácně shodovali na tom, že přestože jsou tyto komponenty dnes už přežitě a nedostačující, tvoří základ a neobejdeme se bez nich.)

Po krátké přestávce pokračoval program konference Security Upgrade 2010 vystoupením Petera Pecha (Trusted Network Solutions) „**Chytré řešení pro filtrování českého webu.**“ Upozornil na to, že spoléhat bezhlavě a automaticky na velká globální řešení nemusí být až tak dobrý nápad, jak by se na první pohled mohlo zdát. Důvod je poměrně prozaický: čeští uživatelé typicky navštěvují české stránky (v rámci přednášky zazněla i konkrétní čísla: o návštěvu domény .cz se jedná v 75 procentech případů!), přičemž univerzální řešení obřích firem právě tyto nemají kategorizované. A zatímco domény třídy .com jsou kategorizované zhruba v devíti případech z deseti, u českých je to z necelé poloviny.

Poslední přednáškový slot před obědem se mikrofonu chopil Kamil Doležel (AdvalCT) a vystoupil na téma

„Přehled technologií pro bezpečnost sítí“. Představil dostupná řešení i služby a u každého názorně uvedl jejich výhody a nevýhody (resp. možnosti a omezení). Seznámil zvláště s bezpečnostním monitoringem sítí, který nevyužívá klasické přístupy a postupy, ale který pracuje v širokém kontextu s podezřelými jevy a událostmi. Má tak vysokou schopnost odhalit slabá místa systému nebo neznámé útoky.

Následoval oběd formou bohatého švédského stolu a konference se „přehoupala“ do své odpolední části.

„Bezpečnost jako náklad nebo byznysový přínos?“ byl název vystoupení Petra Hněvkovského (S&T CZ), který se zaměřil na problematiku bezpečnostního monitoringu – ovšem z hlediska ekonomických nákladů. Aneb s pomocí jasných argumentů vyvracel často omílané tvrzení, že bezpečnost je drahá a nákladná – a že nemá žádný hmatatelný ekonomický přínos pro organizaci. Navíc představil způsob (např. technologii ArcSight), s jehož pomocí lze velmi dramaticky redukovat provozní náklady na bezpečnost.

Přednáška věnovaná problematice spamu, kterou si připravili Mirek Chocholouš a Jakub Alimov ze společnosti Seznam.cz se stala jednou z nejzajímavějších událostí předchozí konference Security Forum 2010. Proto se pořadatelé ve spolupráci s jejími autory rozhodli připravit druhý díl: přednášku **„Spam útočí“**. Z úst nejpovolanějších zazněla slova o boji se spamem, o metodách spammerů, o snahách vyhnout se filtrům apod. Celá prezentace se nesla v duchu „poznej svého nepřítele“ a skončila se lehce neradostným konstatováním, že spam zde byl, je a ještě opravdu hodně dlouho bude.

Po odpolední přestávce se mikrofonu chopil poslední prezentující, Boris Mutina (lektor hackingových kurzů ve společnosti Vergilius IT Expert). Ve své prezentaci **„Hračky vs. zbraně“** se podíval jak do historie, tak do přítomnosti kyberútoků. S tím, že velmi kriticky zhodnotil jak dnešní útočníky (skutečné znalosti a schopnosti se vytrácejí, opisují staré škodlivé kódy, nepřicházejí s ničím novým, využívají univerzálních nástrojů), tak „obránce“ (kteří svou laxností zapříčiňují, že úspěchy mají právě čím dál horší agresori – i to je vizitka osob zodpovědných za zajištění bezpečnosti).

Celou konferenci Security Upgrade 2010 uzavřelo losování velmi bohaté a hodnotné (včetně ochrany přepětí, bezpečnostních síťových bran nebo poukazů na kurzy etického hackingu) tomboly. A příslib organizátorů, že se opět sejdem na konferenci Security Forum na jaře 2011.

Kontakty:

Tomáš Příbyl, odborný garant konference (tomas.pribyl@4us.cz)

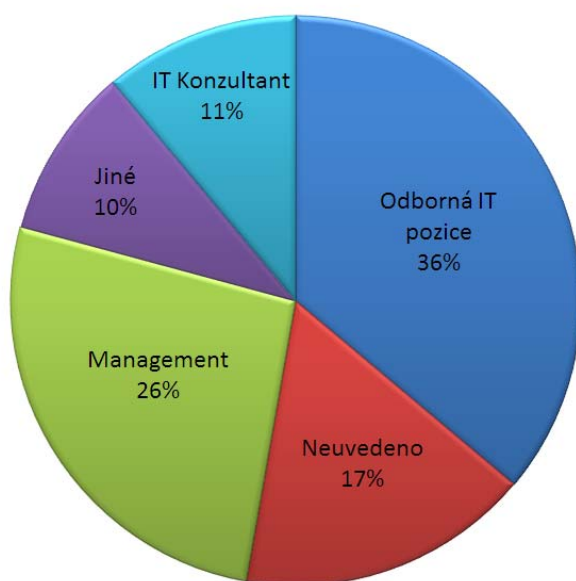
Michael Hurych, ředitel a jednatel společnosti 4U SUPPORT

s.r.o. (michael.hurych@4us.cz)

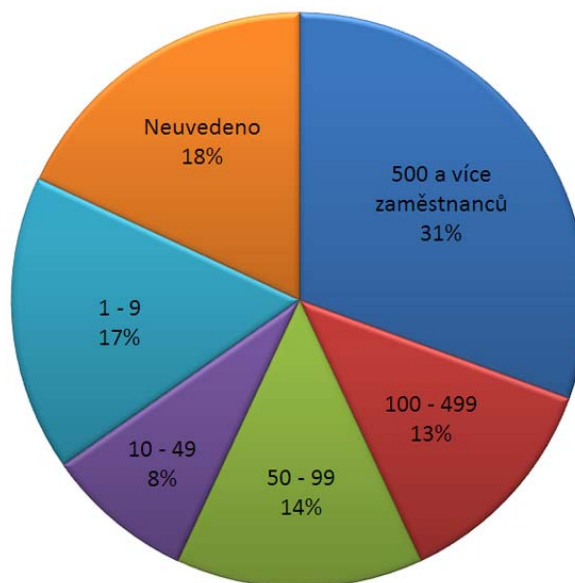
Další informace naleznete na adrese: http://www.konferenceit.cz/html/su_10.html.

Grafy

Pozice posluchačů konference



Velikost společností tvořící auditorium



Klíčové momenty konference Security Upgrade 2010:

- Představení řešení pro filtrování českého webu (který není globálními hráči kategorizován, protože je z celosvětového hlediska příliš malý), které měl Peter Pecho (Trusted Network Solutions).
- Představení BI (Business Intelligence) řešení ArcSight v security, dohledu, provozu a shodě (Petr Hněvkovský, S&T).
- Přesné statistiky ohledně spamu a jeho původu v rámci prezentace „Spam útočí“ Mirka Chocholouše a Jakuba Alimova (Seznam.cz).
- Rozbor aktuálních hrozeb včetně „superčerva“ Stuxnet v podání „etického hackera“ Borise Mutiny (Vergilius IT Expert).

Fotogalerie:



