Současné problémy bezpečnosti ve firmách

Lukáš Mikeska
Ernst & Young

17. února 2010

ERNST & YOUNG
Quality In Everything We Do

O čem budeme mluvit

- **Představení průzkumů v oblasti řízení informační bezpečnosti**
  - Průzkum stavu informační bezpečnosti v ČR 2009 (PSIB'09)
  - E&Y Global Information Security Survey 2009 (GISS'09)
- **Hlavní zjištění průzkumů – podobnosti a rozdíly**
- **Vybraná zjištění a jejich srovnání**
- **Co to pro nás znamená…**

PSIB'09

- 10 let průzkumů – 1999-2009 (každý lichý rok)
- Partneři
- Zaměření - střední a velké organizace v ČR, 100+ zaměstnanců
- Forma - anonymně formou dotazníků od dubna do července 2009
- Dotazník – 12 okruhů
- Výsledky - založené na 280 vrácených dotaznících

E&Y GISS'09

- 12. ročník
- 1,865 organizací v 61 zemích napříč hlavními odvětvími
- On-line i papírový dotazník v červnu a červenci 2009
- Účastník obdrží po vyhodnocení průzkumu report se srovnáním vlastních odpovědí s ostatními respondenty

HLAVNÍ ZJIŠTĚNÍ - ČR

- Očekávaný minimální dopad ekonomické krize na oblast informační bezpečnosti
- Hrozba útoku je stále na špici důvodů, proč rozvíjet řízení bezpečnosti
- Bezpečnostní povědomí vnímáno jako největší překážka rozvoje informační bezpečnosti a také jako hlavní oblast, která může přinést úspory nákladů
- Většina společností nemá dostatečně zpracované postupy reakce na bezpečnostní incidenty
- Aktuálními výzvami jsou „virtualizace serverů“ a bezpečnost přenosných médií
- Většina společností monitoruje a omezuje činnost svých zaměstnanců na Internetu

Hlavní zjištění - svět

- Největší nárůst IT výdajů půjde na zlepšení systémů řízení rizik, implementaci DLP technologií a virtualizaci
- Bezpečnostní aspekty virtualizace a „cloud computing“ nejsou adekvátně řešeny
- Roste výskyt externích a interních útoků
- Dostupnost kvalitních pracovníků je hlavním problémem při realizaci bezpečnostních projektů a iniciativ
- Regulace hraje důležitou roli při řízení informační bezpečnosti a zvyšuje celkové náklady na bezpečnost
- Šifrování koncových stanic a zařízení není příliš rozšířeno

Používané standardy

Vybrané standardy pro řízení bezpečnosti (součet netvoří 100%)	Svět	ČR
ISO/IEC 27001:2005	27%	27%
ISO/IEC 27002:2005	15%	N/A*
CobIT	13%	5%
Information Technology Infrastructure Library (ITIL)	13%	14%

*V ČR otázka sledovala celkové využití ISO 2700x řady standardů

Co se v bezpečnosti outsourcuje

Bezpečnostní aktivity	Outsorcujeme	Zvažujeme me /plánujeme	Neplánujeme
Bezpečnostní audity	44%	16%	40%
Penetrační testování	55%	18%	27%
Testování aplikací	21%	12%	67%
Bezpečnostní školení	12%	15%	73%
Vulnerability/patch management management	17%	8%	75%
Disaster recovery/business continuity recovery/business continuity continuity	15%	12%	73%
Forenzní vyšetřování	14%	13%	73%
Incident response	10%	6%	84%
Help desk	23%	7%	70%
Správa firewall ů a podobná zařízení	30%	9%	61%

Dopady ztráty dat na společnosti

Důsledky	Nejméně ě významné	2	3	4	Nejvíce e významné
Poškození pověsti/značky	2%	4%	10%	20%	64%
Ztráta výnosů	5%	11%	18%	29%	37%
Ztráta zákazníků	6%	9%	14%	27%	44%
Ztráta důvěry investorů/trhů apod.	3%	6%	17%	32%	42%
Soudní spory	3%	6%	22%	32%	37%
Poškození vztahů se zaměstnanci	5%	17%	34%	29%	15%
Postih od regulačních orgánů	4%	9%	20%	29%	38%
Ztráta konkurenční výhody	8%	11%	20%	28%	33%

Které technologie používáte/zvažujete - svět

Technologie	Používáme	Plánujeme do 1 roku	Zvažujeme	Nepoužíváme
Biometriky	22%	5%	27%	46%
Cloud computing	9%	8%	36%	47%
Nástroje na filtrování /monitorování obsahu	69%	9%	10%	12%
DLP nástroje	25%	22%	28%	25%
Šifrování koncových stanic	15%	12%	34%	39%
Digital rights management	14%	10%	31%	45%
Šifrování emailů	35%	15%	25%	25%
Šifrování přenosných médií	25%	19%	29%	27%
Zlepšená autentikace (802.1x, tokeny)	49%	12%	18%	21%
Governance, risk and compliance aplikace	36%	17%	24%	23%
Grid computing	7%	5%	31%	57%
IAM produkty	31%	15%	25%	29%
Šifrování notebooků	41%	17%	23%	19%
Konvergence fyzické a logické bezpečnosti	24%	9%	26%	41%
Radio Frequency Identifiers (RFID) Identifiers (RFID)	15%	4%	29%	52%
Virtualizace serverů	67%	11%	12%	10%
SAN/NAS	80%	5%	6%	9%
Voice over IP	63%	9%	15%	13%
Wireless	69%	6%	10%	15%

Co je největší výzvou bezpečnosti - ČR

Technologie	% respondentů	Horizont
Teleworking	1%	Řešíme
Radio Frequency Identifiers (RFID) Identifiers (RFID)	4%	Do 1 roku
Digital rights management	4%	Do 1 roku
Kryptování emailů	5%	Do 1 roku
Virtualizace desktopů	5%	Do 1 roku
Integrace logické a fyzické bezpečnosti	11%	Do 1 roku
Voice-over-IP (VoIP)	12%	Do 1 roku
Změna SW platformy	12%	Do 1 roku
Kryptování disků	12%	Do 1 roku
Mobilní komunikace (PDA, smart phones) smart phones)	14%	Do 1 roku
Webové aplikace	19%	Řešíme
Bezdrátové služby (wifi)	23%	Řešíme
Elektronická komunikace (instant messaging, email) (instant messaging, email) email)	29%	Řešíme
Přenosná média (např. USB flash disky)	40%	Do 1 roku

Co z toho pro nás plyne?

- Vyplatí se investovat do „měkkých“ částí řízení informační bezpečnosti
- Virtualizace a „cloudy“ mají své bezpečnostní dopady a musíme se s nimi naučit pracovat/řídit je
- Regulace je na západ od našich hranic silnější nebo silněji prosazovaná – a dříve nebo později se to dotkne i nás
- Útoky budou pokračovat a stanou se sofistikovanější s větším využitím technik „sociálního inženýrství“; zvyšuje se pravděpodobnost interních útoků od nespokojených zaměstnanců
- Postupy a technologie v oblasti řízení informační bezpečnosti se budou muset stále více orientovat na ochranu samotné informace, ne pouhé zabezpečení jejího nositele/obalu

Diskuse

Děkuji za pozornost

Lukáš Mikeska
Lukas.mikeska@cz.ey.com