SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Měření a metriky ISMS na České poště

Petr Slavík, Martin Tobolka

Česká pošta, s.p., AEC, spol. s r.o.

Proč jsme začali měřit bezpečnost

- Česká pošta má některé stěžejní odbory certifikovány dle ISO/IEC 27001
  - kde je ISMS certifikováno, tam víme jak na tom jsme očima auditorů
  - kde ISMS certifikováno není, je úroveň bezpečnosti různá
  - Ředitel odboru bezpečnost ICT odpovídá za bezpečnost informací na celé ČP

- Zahájení měření informační bezpečnosti
  - využit normativní rámec ISMS jako srovnávací základ pro celou ČP
  - získání informací kde a jak se změnila úroveň bezpečnosti ICT na celé ČP
  - jaký je přínos zavedených opatření
  - měřitelná identifikace slabých a silných míst
  - získání měřitelných podkladů pro podporu obhájení investic do ICT bezpečnosti

- Zahájení prací na vývoji metrik pro bezpečnost ICT
  - využito nové normy ISO/IEC 27004 pro tvorbu metrik
  - sestaveny pilotní metriky pro měření úrovně ochrany proti malware a měření úrovně fyzické bezpečnosti
  - problematika sběru dat pro metriky, matice odpovědností v rámci metrik

Jak měření bezpečnosti probíhá

Česká pošta

Měření shody bezpečnosti informací dle ČSN/ISO IEC 27001 (ISMS)

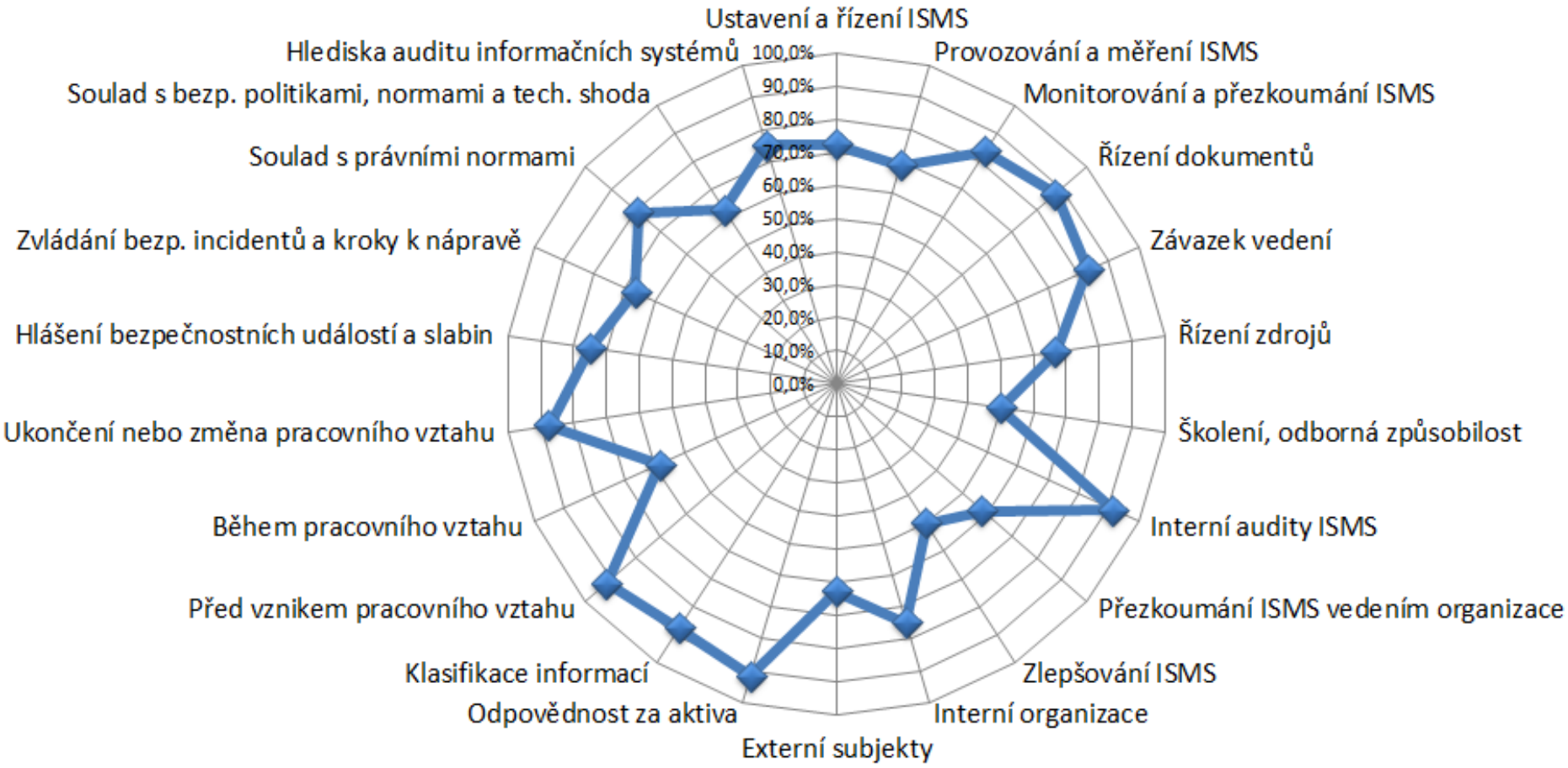
Stav k: 27.1.2012 - fiktivní data

Dosažená úroveň ve vztahu k normě

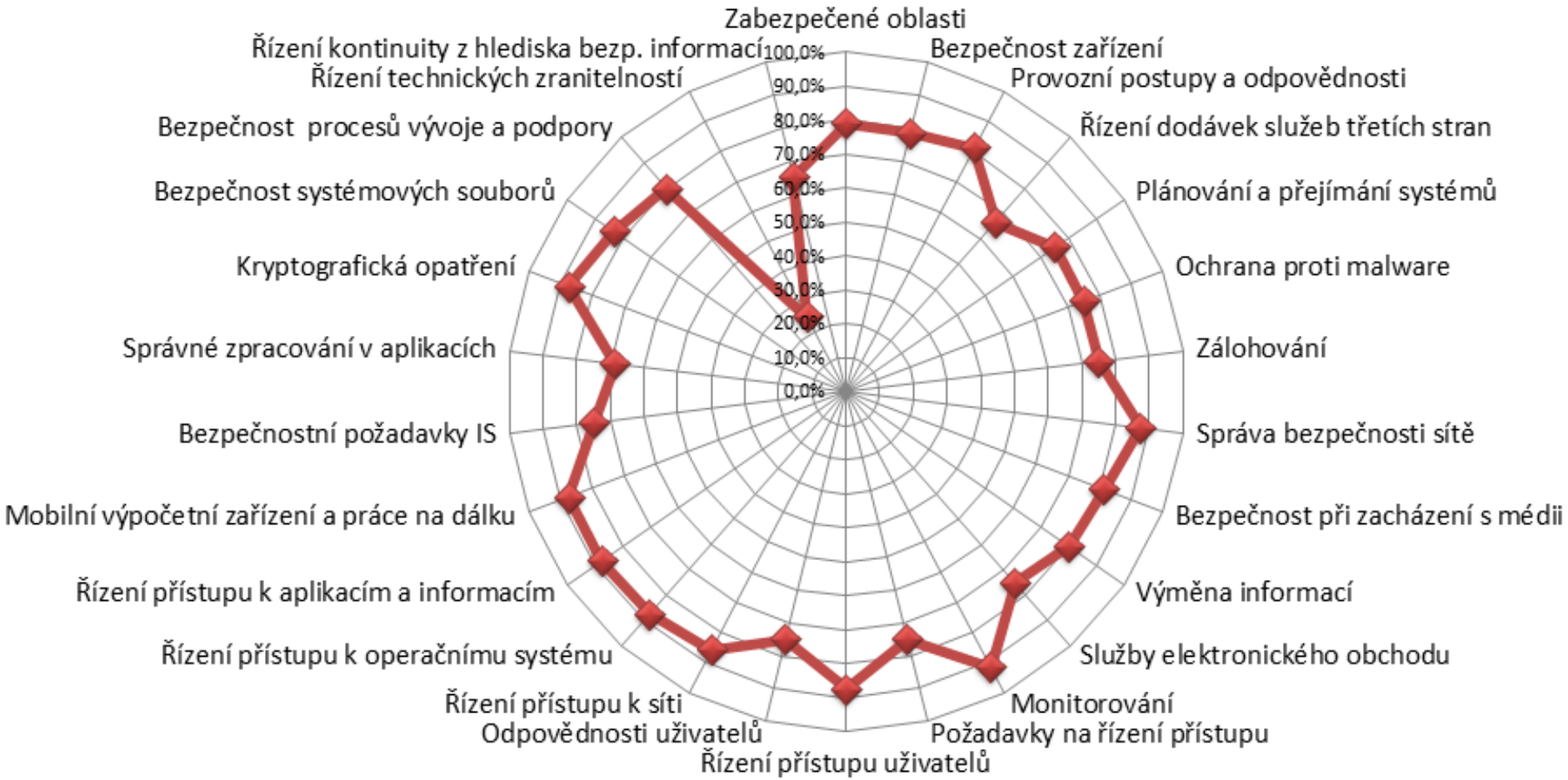
Index shody s ISMS	77,17 %
Prováděné záznamy dle ISMS	77,0 %
Dokumentované postupy	82,4 %
Neúplné postupy	16,2 %

	Prvek - oblast	článek normy	Dosažená úroveň	Vedení záznamů		Dokum. postup	
9	**Zvládání bezpečnostních incidentů**		**70,0%**	**75 %**		**60 %**	
9.1	**Hlášení bezpečnostních událostí a slabin**		**75,0%**				
9.1.1	- Existuje postup pro hlášení incidentů, slabých míst v bezpečnosti, selhání SW apod.? Pro hlášení bezp. incidentů musí existovat formalizovaný postup (včetně postupu reakce na incidenty a jejich eskalace) definující činnosti, které budou provedeny po nahlášení.Uživatelé seznámeni s povinností hlášení bezp. incidentů.	A.13.1.1 - Hlášení bezpečnostních událostí	75%		x	Ano	
9.1.2	- Všichni zaměstnanci, smluvní strany a ost. uživatelé musí zaznamenávat a hlásit jakékoliv bezp. slabiny nebo podezření na bezp. slabiny v systémech nebo službách. Uživatelé nesmí slabiny „prověřovat" = zneužití systému.	A.13.1.2 - Hlášení bezpečnostních slabin	75%	Ano		Ano	
9.2	**Zvládání bezpečnostních incidentů a kroky k nápravě**		**66,7%**				
9.2.1	- Jsou stanoveny odpovědnosti a postupy pro zvládání bezp. incidentů? Postupy musí být odsouhlaseny vedením a zodpovědné osoby musí být seznámeny s prioritami pro zvládání bezp. incidentů	A.13.2.1 - Odpovědnosti a postupy	100%	Ano		Ano	
9.2.2	- Existují mechanizmy pro kvantifikaci a monitorování typu, rozsahu a nákladů bezp. incidentů? Informace z vyhodnocení slouží jako podklad k analýze rizik nebo zavedení nových opatření.	A.13.2.2 - Ponaučení z bezpečnostních incidentů	50%	Ano		Ne+	
9.2.3	- V případě, že bezp. incident má charakter „trestného činu" , musí být sbírány, uchovávány a soudu předkládány důkazy.	A.13.2.3 - Shromažďování důkazů	50%	Ne		Ne+	

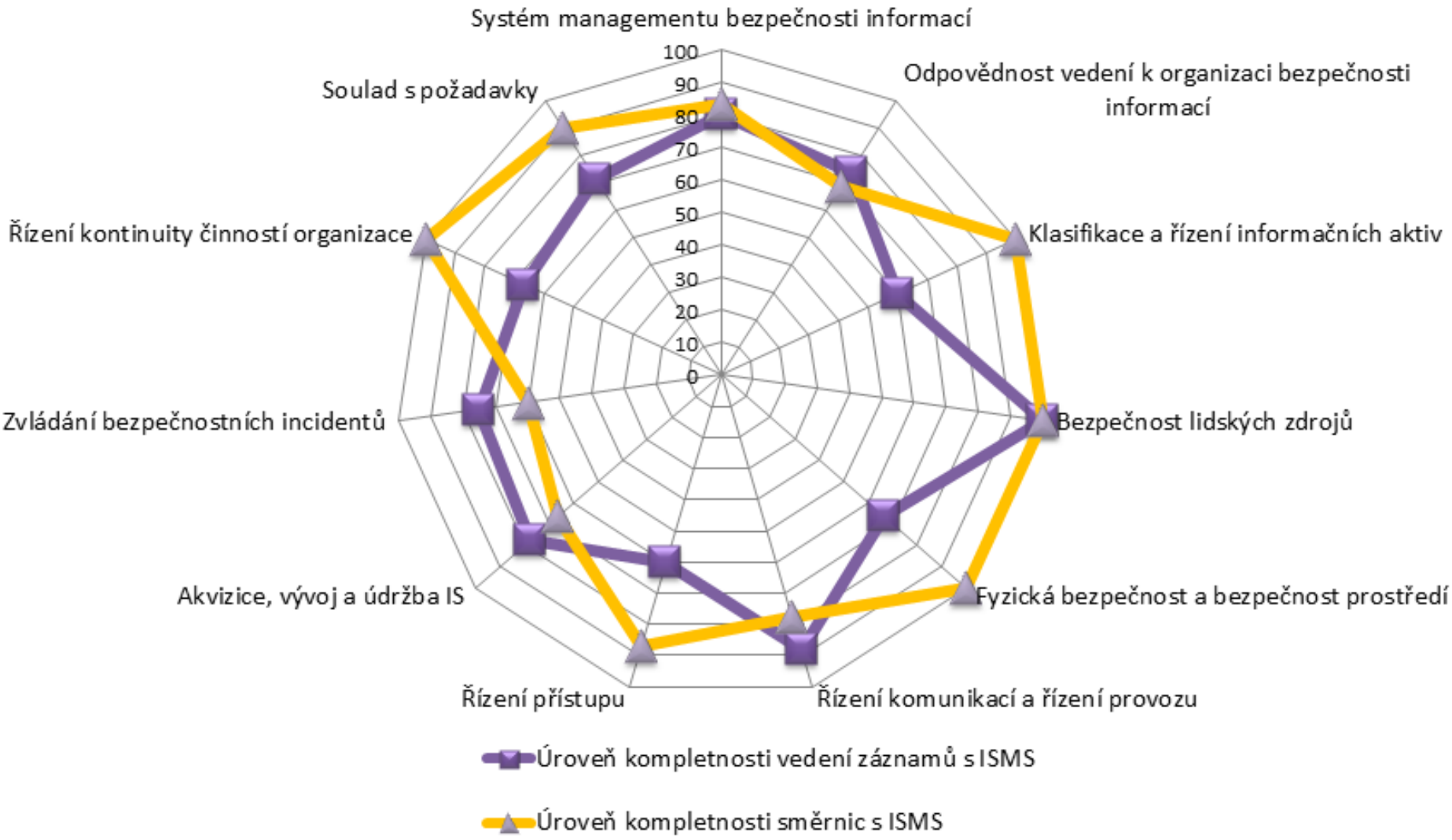
Měření ISMS - kapitoly 4-8, A5-A8, A13 a A15



Měření ISMS – kapitoly A9-A12 a A14

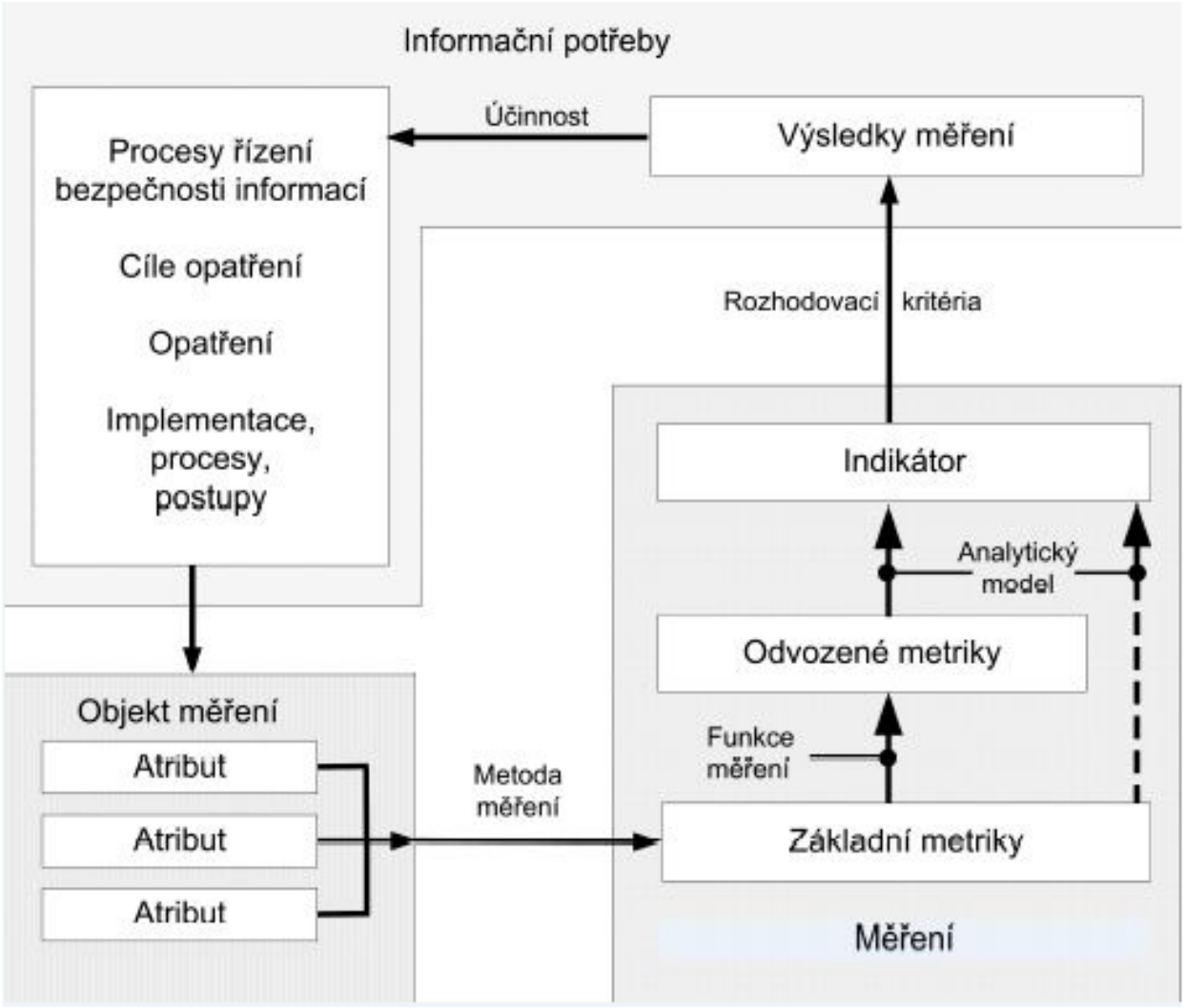


Měření úrovně rozsahu směrnic a tvorby záznamů



Jak na metriky

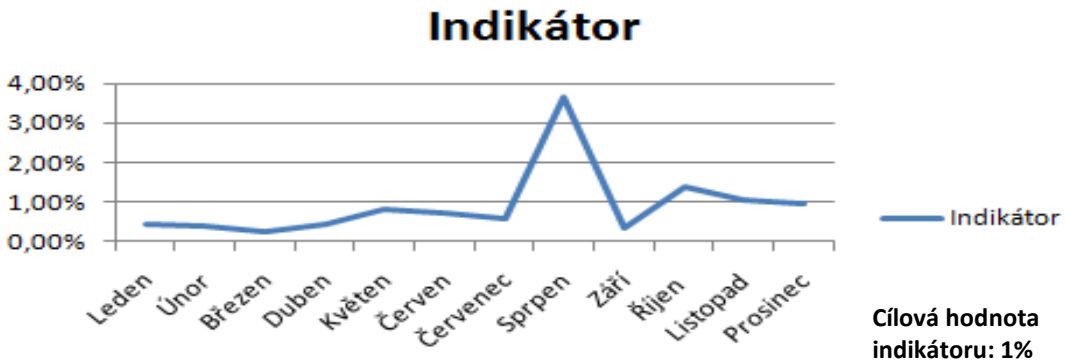
Model měření bezpečnosti informací



Zdroj: ISO/IEC 27004

Metriky – Příklad: ochrana proti malware

Účel konceptu měření	Ohodnotit účinnost ochrany systémů proti útokům škodlivých programů.
Cíl opatření	Cíl opatření A.10.4 Chránit integritu programového vybavení a dat. proti škodlivým programům.
Opatření	Na ochranu proti škodlivým programům musí být implementována opatření na jejich detekci, prevenci a obnovu a zvyšování odpovídajícího bezpečnostního povědomí uživatelů.
Objekt měření	1 Hlášení incidentů 2 Logy antivirových programů
Atribut	Incident způsobený škodlivým kódem
Interpretace indikátoru	Vzrůstající trend ukazuje zhoršující se shodu, klesající trend indikuje zlepšující se shodu. Pokud trend nápadně vzrůstá, bylo by potřebné prozkoumat příčinu a zavést další opatření proti malware.
Formy hlášení	Spojnice trendu, která popisuje poměr detekce a prevence škodlivých programů, překrytá spojnicemi trendu vytvořených v předcházejících periodách hlášení.



Cílová hodnota indikátoru: 1%

Měsíc	Incidenty	Blokace	Indikátor
Leden	12	2621	0,46%
Únor	14	3524	0,40%
Březen	10	4122	0,24%
Duben	8	1830	0,44%
Květen	16	1989	0,80%
Červen	18	2459	0,73%
Červenec	22	3859	0,57%
Srpen	156	4257	3,66%
Září	25	6852	0,36%
Říjen	36	2569	1,40%
Listopad	42	4036	1,04%
Prosinec	29	3012	0,96%

Přínos projektu

- Výstupy projektu měření a metriky ISMS
  - byl stanoven výchozí index bezpečnosti celé ČP dle ISMS
  - byl získán přehled o kompletnosti bezpečnostní dokumentace
  - byla změřena úroveň vedení záznamů dle požadavků směrnic
  - byly sestaveny pilotní metriky
  - existuje srozumitelná grafická interpretace výsledků měření pro Top management

- Jak dál?
  - pravidelné nezávislé přezkoumání úrovně ISMS
  - rozvoj metrik
  - selektivní zlepšování ISMS v nejslabších oblastech bezpečnosti na ČP
  - investice vynakládat efektivně a pouze tam, kde je to skutečně na základě výsledků měření bezpečnosti nezbytné

SECURITY 2012

20. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Petr Slavík, Martin Tobolka
Česká pošta, s.p., AEC
Email: martin.tobolka@aec.cz