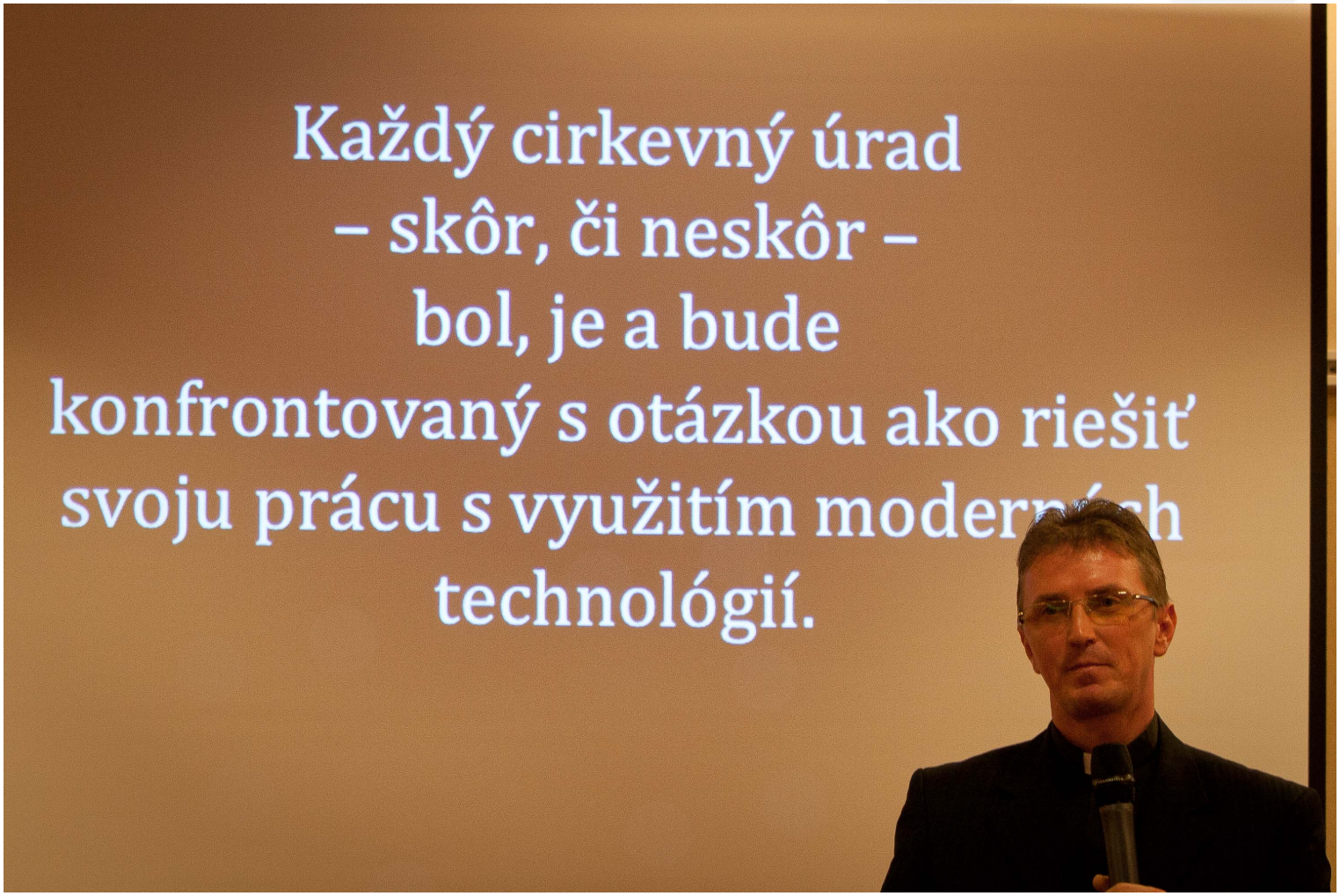
Aktuálny stav elektronizácie a informačnej bezpečnosti v cirkevnom prostredí

Peter Šantavý, Mario Minarovský
psantavy@abuba.sk, mminarovsky@ecclesia.sk

ecclesia


Každý cirkevný úrad
– skôr, či neskôr –
bol, je a bude
konfrontovaný s otázkou ako riešiť
svoju prácu s využitím moderných
technológií.

ecclesia


ecclesia

Zásady elektronizácie procesov

- Hlavné princípy
  - 🕮 ľudský (kultúra organizácie a organizačný aspekt)
  - 🕮 procesný (spôsob organizácie a kontroly práce)
  - 🕮 technologický (IKT).

ecclesia

Zásady elektronizácie procesov

- Má umožniť „bezpapierový“ obeh dokumentov
- Urýchliť priebeh procesu automatizáciou krokov
- Zvýšiť efektivitu
- Znížiť chybovosť
- Znížiť náklady

ecclesia

Zásady elektronizácie procesov

- Spoľahlivá infraštruktúra
- Bezpečnosť
- Koncepcia

ecclesia

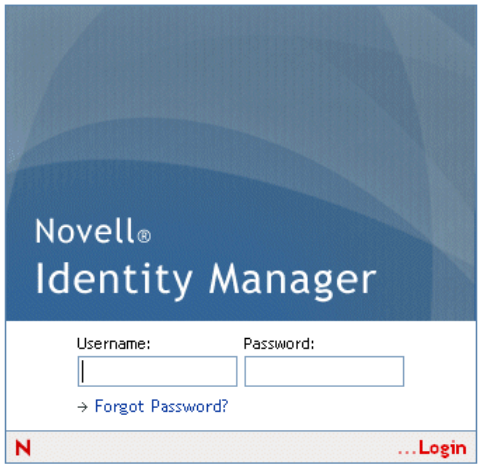
Zásady elektronizácie procesov

- Procesy
  - Kódex kanonického práva
  - Interné predpisy
  - Legislatíva

ecclesia

Zásady elektronizácie procesov

- Štandardizácia a konsolidácia
  - Umožňuje zdieľanie a efektívne využitie dostupných zdrojov
  - Prináša nižšie náklady pri nasadzovaní a prevádzke
- Základ tvorí IDM a RBAC
  - Vieme „kto je kto“
  - Vieme „na čo má právo“



ecclesia

Elektronický výkon verejnej moci (e-Government)

- §305/2013
  - Čo fara to IČO
  - Čo IČO to datová schránka
  - Čo datová schránka to prijaté/odoslané elektronické dokumenty
    - Spracovať
    - Udržiavať
    - Archivovať

ecclesia


ecclesia

Aktuálny stav elektronizácie procesov

Informačná bezpečnosť v cirkevnom prostredí

Peter Šantavý, Mario Minarovský
psantavy@abuba.sk, mminarovsky@602.sk

ecclesia

Prečo informačná bezpečnosť?

- pracujeme s citlivými údajmi
  Od osobných údajov až po forum internum...
- riziko zneužitia IKT a realita informačnej kriminality
  Zlyhanie ľudského faktora i možnosť kompromitácie techniky.
  Od zneužitia prostriedkov až po OÚ, sledovanie a ohrozenie životov.
- legislatívne požiadavky
  Zákon č. 122/2013 Z. z. o ochrane osobných údajov.
  Zmena a doplnenie niektorých zákonov v znení zákona č. 84/2014 Z. z.
  GDPR a nový Zákon o ochrane osobných údajov.
- sme viazaní právnymi normami Cirkvi

ecclesia

Zneužitie prostriedkov – ako?

- chyby v systémoch
  – systémy IKT sú čoraz komplexnejšie (v súčasnosti od operačných systémov a aplikácií až po technológie umelej inteligencie)
  – existencia chýb v prostriedkoch informačných a komunikačných technológií (IKT)
  – umožňujú prevzatie vlády nad systémom a únik dát
- zlyhanie ľudského faktora
  – ľudské chyby a neznalosť
  – sociálne inžinierstvo
  – zámerná sabotáž z ideologických, osobných, ekonomických... dôvodov
-

ecclesia

Informačná kriminalita

- kriminalizácia zneužívania prostriedkov
  - kriminalizácia zneužívania chýb v systémoch a zlyhania ľudského faktora
  - jedna z troch najvýnosnejších oblastí kriminality
  - oblasti zneužívania chýb
    - krádeže identity, OÚ a podvody
    - vykrádanie obsahu počítačov
    - botnety (nelegálny obsah, spam, DDOS)
    - vydieranie (ransomware, revenge acts)
  - masívne rozšírenie zneužívania chýb (automatizácia -> AI)
    - unifikované a neochraňované systémy
- riziko zneužitia IKT ako nástroja moci
  - monitorovanie a sledovanie
  - perzekúcia, odopieranie a blokovanie prostriedkov IKT
  - kybernetický terorizmus a oblasť elektronického boja

ecclesia

Bežný prístup k bezpečnosti

- nedostatočný stav zabezpečenia IKT
  – neaktuálnosť operačných systémov a softvérového vybavenia
  – zložitosť bezpečnej konfigurácie techniky
  – mýtus black box je bezpečný
- rizikové správanie vo virtuálnom svete
  – absentujúce alebo nedostatočné bezpečnostné povedomie
  – mýtus anonymity a bezpečia – kto by mal o mňa/nás záujem?
- chýba koncepčnosť
  – riešenie problémov až po incidentente, resp. kompromitácii
  – neexistuje zodpovedná osoba, záväzné pravidlá a dokumentácia
  – nevykonáva sa monitoring a detekcia, školenia
- fatalistický prístup – nemá to význam

ecclesia


ecclesia

Rôznorodosť IS

- interné IS biskupských úradov/organizácií
  – komplexná a rôznorodá agenda biskupského úradu
  – registratúra, archív, napojenie na externé systémy
  – pracovníci úradu + externí spolupracovníci
  – interné informačné systémy
- farnosti
  – uzatvorená množina informačných systémov
  – jednotlivci, ktorí prichádzajú do styku s IS a OÚ
  – rôznorodé technológie/technika, ktoré nemusia byť v požadovanom stave
- verejné služby a samostatné projekty
  – verejne prístupné front-endy interných IS
  – verejné webové stránky a sociálne médiá
  – informačné služby a aplikácie pre veriacich i širokú verejnosť

ecclesia

Verejné služby a samostatné projekty – apríl 2017

Médium	Zabezpečenie	Médium	Zabezpečenie
SSV		TV Lux	
Katolícke noviny		Rádio Lumen	
Vydavateľstvo Lúč		MojaKomunita	polofunkčné
Vydavateľstvo Don Bosco		Christ-Net.Sk	
Kumran		Web Závislosť od internetu	
Zachej		Cesta+	
FarskyUrad.Sk	naviac dáta v zahraničí (USA)!!!	Fara.Sk	čiastočne (časť je zabezpečená)

Stav informačnej bezpečnosti niektorých médií z kategórie vo vlastníctve Cirkvi, resp. hlásiacich sa k Cirkvi – apríl 2017.

ecclesia

Verejné služby a samostatné projekty – november 2017

Médium	Zabezpečenie	Médium	Zabezpečenie
SSV		TV Lux	
Katolícke noviny		Rádio Lumen	
Vydavateľstvo Lúč		MojaKomunita	
Vydavateľstvo Don Bosco		Christ-Net.Sk	
Kumran	nefunkčné	Web Závislosť od internetu	
Zachej		Cesta+	
FarskyUrad.Sk	naviac dáta v zahraničí (USA)!!!	Fara.Sk	okrem starších webov

Aktuálny stav informačnej bezpečnosti niektorých médií z kategórie vo vlastníctve Cirkvi, resp. hlásiacich sa k Cirkvi – november 2017.

ecclesia

Vonkajšie služby diecéz, 04/2017

Súčasť	Web TLS	Vlastníctvo domény	Uloženie dát	Webmail TLS	Privátna zóna
KBS					
Bratislavská arc.					
Trnavská d.	*				
Nitrianska d.	*				
Žilinská d.	*		*	*	
Banskobystrická d.	*		*		N/A[1]
Košická arc.	*				N/A[1]
Spišská d.	*		*		
Rožňavská d.	*				
Košická ep.	*				
Prešovská arc.	*				
Bratislavská ep.	*				N/A[1]
Ordinariát OS a OZ	*		N/A[2]	N/A[2]	N/A[2]

ecclesia

Stav vonkajšej informačnej bezpečnosti KBS a diecéz – apríl 2017.

Vonkajšie služby diecéz, 11/2017

Súčasť	Web TLS	Vlastníctvo domény	Uloženie dát	Webmail TLS	Privátna zóna
KBS					
Bratislavská arc.					
Trnavská d.	*				
Nitrianska d.	*				
Žilinská d.	*		*	*	
Banskobystrická d.	*		*	*	N/A[1]
Košická arc.	*				N/A[1]
Spišská d.	*		*		
Rožňavská d.	*				
Košická ep.	*				
Prešovská arch.	*				
Bratislavská ep.	*				N/A[1]
Ordinariát OS a OZ			N/A[2]	N/A[2]	N/A[2]

ecclesia

Stav vonkajšej informačnej bezpečnosti KBS a diecéz – november 2017.

Vysvetlivky – legenda

Web TLS	prístup na webové stránky je zabezpečený šifrovaným spojením
Vlastníctvo domény	TLD doména 2. stupňa je vo vlastníctve Cirkvi
Uloženie dát	privádne dáta a informácie sú uložené na cirkevných serveroch
Webmail TLS	prístup k elektronickej pošte (webmail alebo IMAP/SMTP) je zabezpečený šifrovaným spojením
Privátna zóna	prístup do privátnej zóny je zabezpečený šifrovaným spojením
N/A[1]	informácie o privátnej zóne nie sú k dispozícii, resp. privátna zóna neexistuje
N/A[2]	údaj nie je relevantný, ordinariát má tieto oblasti spravované ministerstvom obrany na štátnych serveroch
	plne vyhovujúci stav – bezpečné
*	plne vyhovujúci stav – bezpečné, nevzťahuje sa to ale na všetky farnosti!
	čiastočne vyhovujúci stav – existuje určité bezpečnostné riziko (napr. self-signed certifikáty, u ordinariátu štátne servery a pod.)
	nevyhovujúci stav – praktická možnosť úniku dát, resp. ďalších škodlivých aktivít (napr. dáta dostupné externej firme, nešifrované spojenie, zlá implementácia certifikátov umožňujúca MITM útok)
*	nezabezpečené spojenie, pričom bezpečnosť bežnej prevádzky nie je ohrozená (v konkrétnych scenároch však určité bezpečnostné riziko existuje)

ecclesia

K aktuálnemu stavu...

- neuvádzame stav interných systémov
  – stav viacerých diecéz vieme na vyžiadanie kompetentných komunikovať
  – vieme popísať viaceré bezpečnostné incidenty z posledných rokov
- v 50% uvádzaných problémov je technické riešenie nápravy triviálne
  – problémom je koncepčnosť, procesy alebo ľudský faktor
- náročnosť bezpečných riešení rastie
  – musia byť koncepčné a komplementárne s legislatívou a normami
  – musia byť odborne navrhnuté
  – musia byť profesionálne realizované a následne spravované
  – musia byť používané

ecclesia


ecclesia

Čo navrhujeme (1)

- koncepčnosť
  – principiálna – informačná, nielen kybernetická bezpečnosť!
  – technologická – security and privacy by design and by default
  – organizačná – zodpovedné vedenie, normy/zákony, týka sa všetkých
- bezpečnostná politika (BP) organizácie
  – koncepcia informačnej bezpečnosti v organizácii
  – BP znamená:
  – povedať každému zamestnancovi organizácie čo môže, čo nesmie, čo musí a za čo je zodpovedný
  – poveriť vhodného človeka zostavením pracovnej skupiny a vypracovaním zásad BP
  – BP schvaľuje vedenie a vydáva ako vnútorný predpis
- informačná bezpečnosť je trvalý proces!

ecclesia

Čo navrhujeme (2)

- legislatíva a normy
  – GDPR, eIDAS, NIS
  – Zákon o ochrane osobných údajov, Zákon o kybernetickej bezpečnosti
  – ISO 27002
- STN ISO/IEC 27002:2013
  – informačné technológie, bezpečnostné metódy
  – pravidlá dobrej praxe riadenia informačnej bezpečnosti
  – manažment kontinuity činnosti; riešenie bezpečnostných incidentov; obstarávanie, vývoj a údržba systémov; riadenie prístupu; manažment aplikačných sieťových služieb; prevádzka systémov a komunikácie; manažment vzťahov s dodávateľmi/poskytovateľmi služieb; fyzická bezpečnosť; personálna bezpečnosť; správa aktív; organizácia IB; bezpečnostná politika
  – množina štandardov ISO/IEC 27000

https://www.csirt.gov.sk/informacna-bezpecnost/standardy-a-legislativa/isoiec-814.html

ecclesia

ĎAKUJEM ZA POZORNOSŤ

INFO@ECCLESIA.SK

ecclesia


ecclesia