

„Prodloužená ruka“ bezpečnosti aneb co vše chtít od elektronické podatelny

Marek Prchal
SECURITY 2010
17. 02. 2010



Co Vás čeká a nemine?

- 4 pohledy na bezpečnost z hlediska koloběhu zprávy
- ilustrativní příklad „bezpečné“ podatelny
- zkušenosti a požadavky Vás uživatelů
- případy z praxe
- Váš výběr kritérií a nároků

„Prodloužená ruka“ bezpečnosti



17. 02. 2010 Prezentaci pro konferenci SECURITY 2010 připravil Marek Prchal

AEC

DATA SECURITY

Bezpečná aplikace je základem

- vyzrazení nejcitlivějších informací a zpráv
- provázanost s DMS
- nedodržení právních lhůt
- předcházení právním sporům (zjednodušení)
- ochrana investic do bezpečnostní politiky

Bezpečná aplikace je základem

- součinnost vývoje s bezpečnostní politikou
- stanovení priorit pro zabezpečení
- testování a prověření aplikace
- testování a prověření umístění aplikace, především její frontendové části
- výběr vhodné aplikace splňující kritéria ISMS
- odolnost vůči sociálnímu hackingu



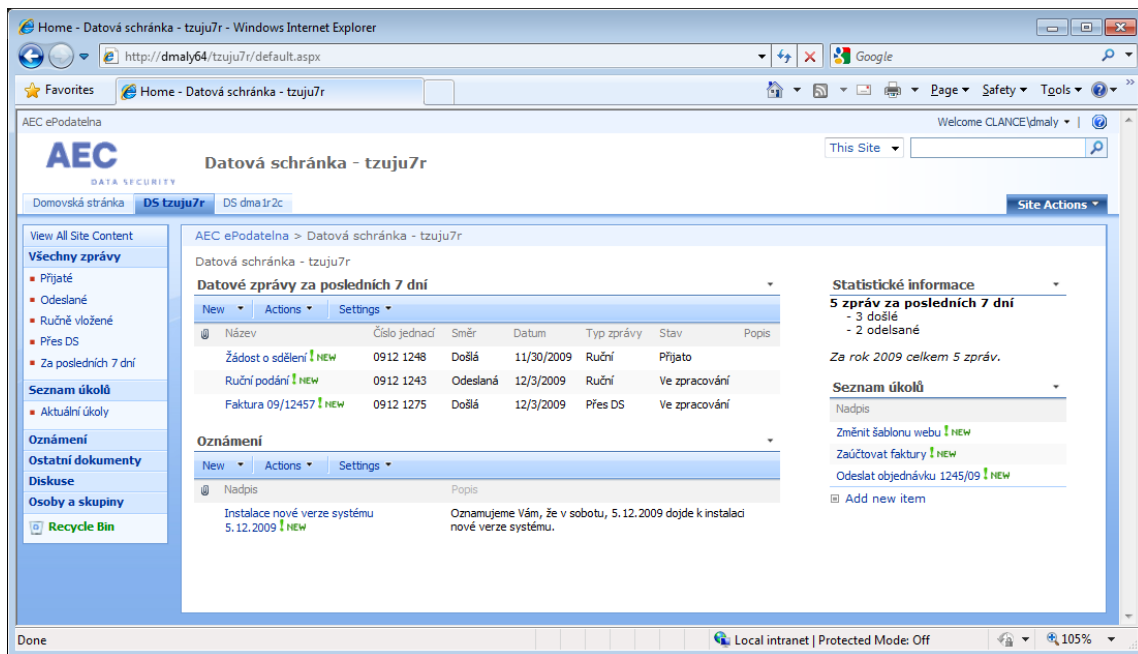
Příjem a předávání zpráv

- kontrola veškerých obsažených podpisů
- kontrola důvěryhodnosti CA (vlastní seznam)
- kontrola platnosti na certifikační autoritě
- kontrola správnosti certifikátu
- přenos zprávy kryptovaným kanálem z ISDS
- vytvoření protokolu a jeho přiložení k DS



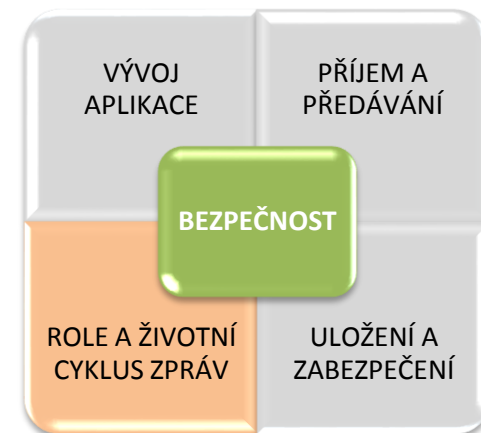
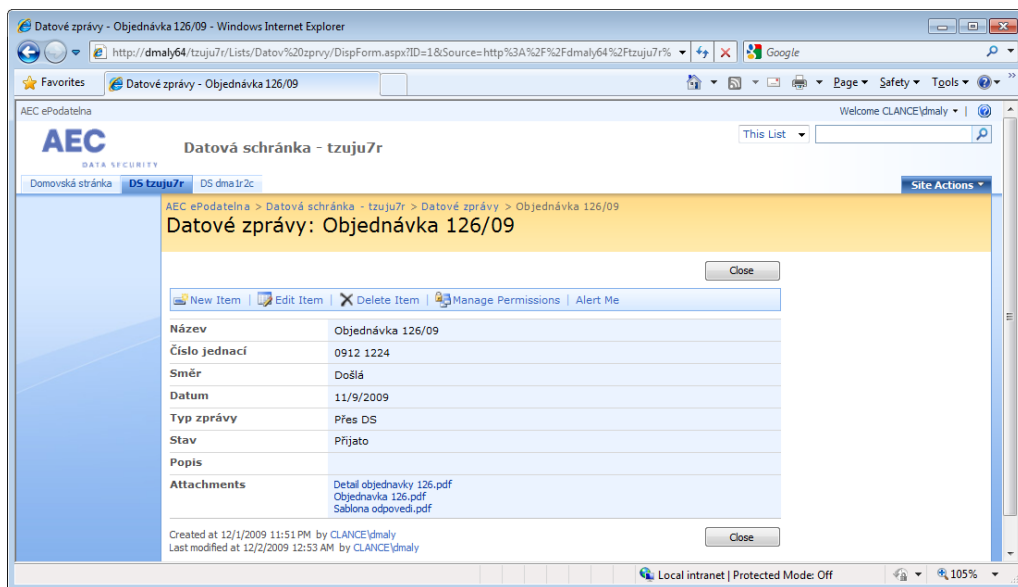
Příjem a předávání zpráv

- pokračování bezpečného kanálu
- předávání do e-mailu pomocí šifrovaného provozu
- šifrované předání do spisových služeb
- dodržení bezpečnostních zásad organizace



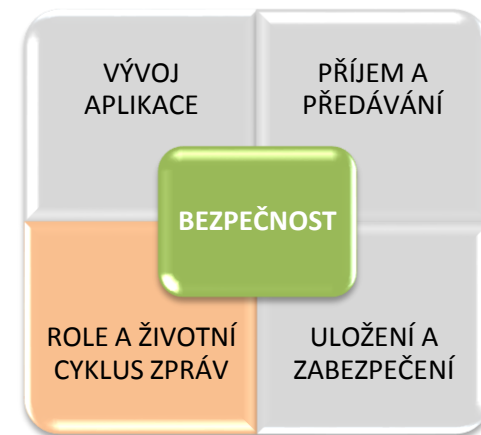
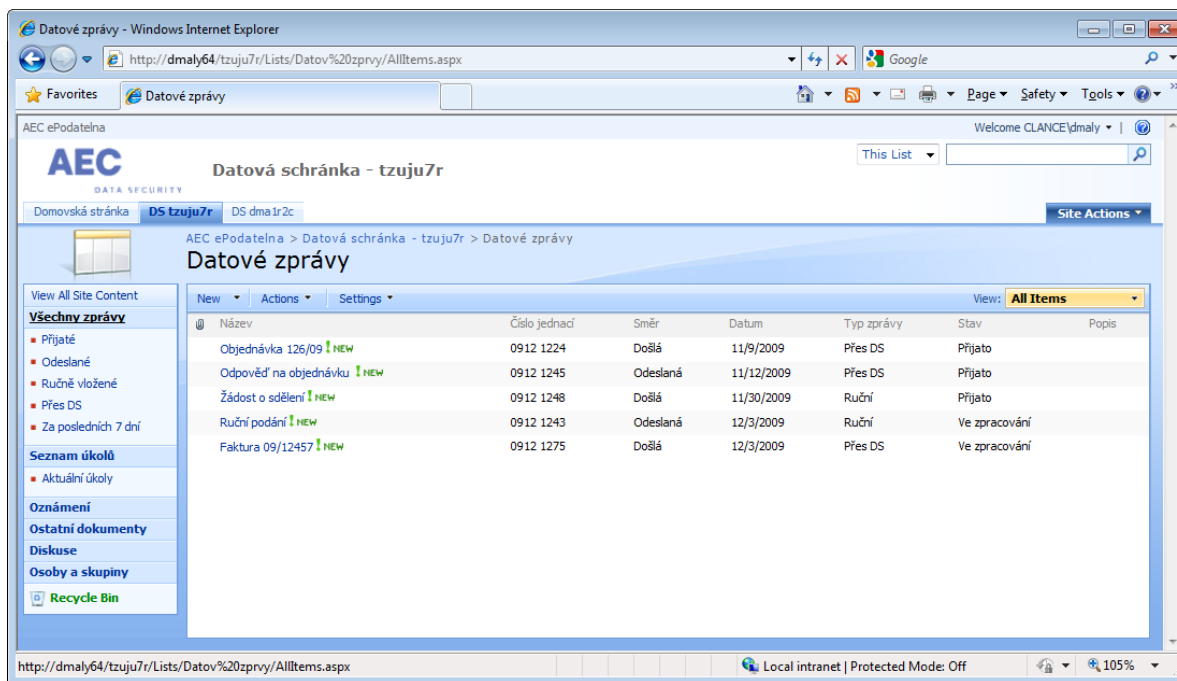
Uživatelské role, životní cyklus

- správa rolí, nakládání se zprávou a přílohami dle úrovně
- viditelnost a možnost otevření příloh
- příprava odchozích zpráv pověřenými pracovníky
- kontrola a podepsání zprávy (eSign Pro)
- znemožnění přístupu administrátora do obsahu DS



Uživatelské role, životní cyklus

- spuštění životního cyklu zprávy v organizaci
- přehledné zobrazení stavu zprávy
- upozorňování na vypršení lhůty pro zpracování
- vyžádaná kontrola stavu doručení



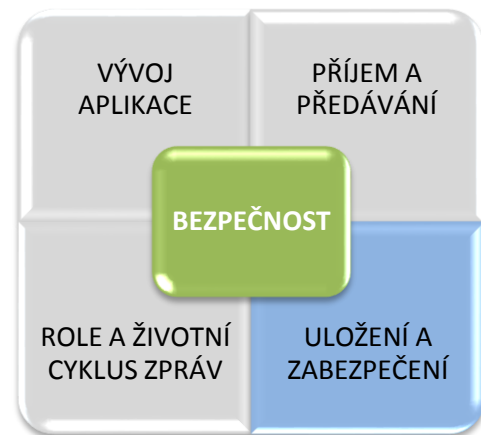
Uložení a zabezpečení

- nemožnost ukládat DS v šifrované podobě
- ukládání rozšifrovaných zpráv ve formátu .zip
- přístup k uloženým souborům dle rolí
- návaznost na ISMS



Uložení a zabezpečení

- data při příjmu opatřena systémovou značkou a razítkem
- uložení pro archivaci zabezpečí pouze po dobu platnosti certifikátu
- hrozba prolomení privátního klíče – za současných technických podmínek cca 1 rok
- zajištění, že zpráva nebyla modifikována při prolomení PKI
- prokázání „nemanipulace“ se zprávou po dobu uložení



AEC

DATA SECURITY

Děkuji za pozornost!

Marek Prchal
marek.prchal@aec.cz

AEC, spol. s r.o. · Spielberk Office Centre
Holandská 878/2 · 639 00 · Brno · Czech Republic
Phone: +420 541 235 466 · Fax: +420 541 235 038

AEC, spol. s r.o. · European Business Center
Dukelských hrdinů 34 · 170 00 Praha 7 · Czech Republic
Phone: +420 267 311 402 · Fax: +420 266 177 155

www.aec.cz