

O tom, jak vybírat bezpečnostní řešení pro informační systémy veřejné správy, na co nezapomenout a co by tato řešení měla splňovat, s námi hovořil Karim Ifrah ze společnosti Comguard.

Karim Ifrah,

Channel Sales Manager, Comguard karim.ifrah@comguard.cz



Při budování e-Governmentu nezapomínejme na oblast bezpečnosti IT

Na co při budování e-Governmentu nezapomínat z hlediska řízení bezpečnosti?

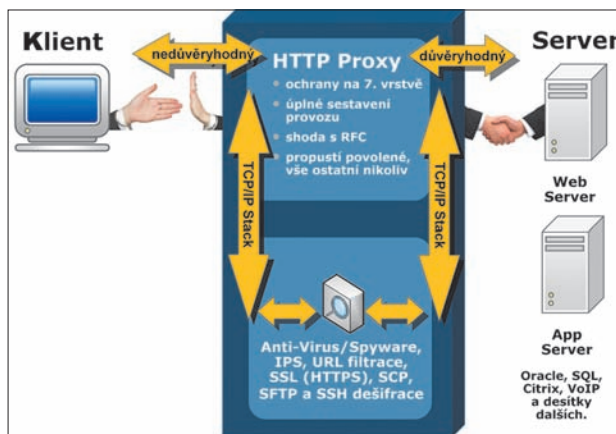
E-Government už přestává být tématem a začíná být „hitem“, ale ne každý přesně ví, co to znamená. Díky této situaci se orgány veřejné moci pustily do elektronizace výkonu služeb veřejné moci. Budují datová centra spolu s metropolitními sítěmi, implementují aplikace spisovou službou počínaje a správou místních poplatků konče. Hlavní činností, táhnoucí se jako červená nit všemi projekty, je digitalizace, což zatím představuje nákup skenerů, čteček čárových kódů, tiskáren a dalšího vybavení s tímto souvisejícího a „začínáme digitalizovat“. Dost bylo nadsázky a teď vážněji. Zkusme nastavit stěžejní body problematiky.

Díky platnosti zák. 300/2008 Sb. orgány veřejné moci „musí“ komunikovat elektronicky, a to představuje revoluční změnu v jejich práci. Času na přípravu bylo poměrně málo a rozsah informací o tom, co to vlastně pro úřad znamená, ještě mívá. V rychlosti úřady činí kroky k vlastní elektronizaci a splnění legislativy, ale tak zásadní téma, jako je bezpečnost, ustupuje do pozadí a bude ho tedy nutno řešit až ex-post. Pravidla budování e-Governmentu nehovoří o bezpečnosti informací taxativně, ovšem zmiňují ji jako automatickou záležitost. Tady narážíme na naprosto odlišný přístup pro oběh, zpracování a archivaci dokumentů. Náhle se úředník ocitá ve světě, kde razítko je elektronické, podpis zašifrovaný a klade si otázky typu, která verze dokumentu je platná, kdo editoval dokument poslední a kdy vlastně dokument přišel mailem. Pro svět ICT běžné. Doporučujeme tedy vzít v úvahu vhodný DMS (Document Management System), kde je možno nastavit např. workflow shodné s interními procesy a zpracovat šablony dokumentů, využít maximálně technologie xml a začít pracovat s digitálním dokumentem. V kombinaci s DMS je vhodné nasadit systém DLP (Data Loss Prevention), který dokáže monitorovat a chránit informace před jejich neoprávněným užitím ze strany vlastních uživatelů. V tomto ohledu je vhodný DLP systém **McAfee Data Loss Prevention**, který dokáže pokrýt nejen síťovou komunikaci (např. e-mail, FTP atd.), ale i fyzická zařízení (např. tiskárny, USB zařízení, CD/DVD-RW) a zaručit, že informace jsou stále pod dohledem.

Pro digitální podpis úředníka zvolíme některý z vhodných nosičů, kterými jsou dnes Token nebo elektronická karta. Vhodný token je například **USB token ActivKey SIM USB od společnosti ActivIdentity**, který dokáže na sobě uchovávat různé certifikáty či elektronické podpisy. V případě, že je třeba kombinovat uložení certifikátu s generátorem jednorázových hesel pro přístup do LAN či do různých aplikací, tak vhodným řešením může být token **ActivKey Display USB**. Pro případ, že je třeba kombinovat uložení certifikátu s generátorem jednorázových hesel a s bezdotykovým čipem, např. pro přístup

do budov, je bezesporu vhodným řešením **ActivIdentity Smart DisplayCard**.

Při zavedení tohoto elektronického nosiče je dobré zamyslet se nad tím, zda-li by nebylo vhodné využít jeho funkcionalitu pro více účelů. Je velice elegantně využitelný jako médium pro elektronický podpis, kartu lze využít jako elektronický klíč pro docházkový systém a kontrolovaný vstup (třeba na parkoviště), můžete ji použít jako elektronickou stravenku do jídelny a díky tomu, že obsahuje aktivní generátor hesel, i pro autentikaci do počítačové sítě či jiných systémů (např. RSA). Docílíte toho, že zaměstnanec úřadu nenosí u sebe několik barevných tokenů a karet, ale má jednu „slušivou“ kartu se jménem a fotografií (chceme-li). Pochopitelně to vše souvisí s centrálním managementem a provázaností na IDM. Chceme-li mít jistotu, že nedochází k únikům formou neoprávněných tisků či skenů, nasadíme aplikaci tzv. tiskové řešení a opět v návaznosti na IDM provádíme monitoring. Zní to poměrně jednoduše, ovšem nutno podotknout, že bez kvalitní rizikové analýzy se jen pokoušíte o zabezpečení a účinnost vynaložených prostředků se limitně blíží k nule. Doporučená cesta k budování systému řízení bezpečnosti dat začíná u analýzy prostředí, rizikové analýzy, a pokud není k dispozici procesní analýza, tak alespoň



Unikátní systém aplikačních proxy bran uplatňuje skutečný proxy přístup.

dokumentace k aplikacím a popisy pracovních náplní včetně provozního řádu. Další postup je doporučen v normě ISO 27000 a je vhodné se ho přidržet.

Jaké bezpečnostní standardy musí splňovat informační systémy samosprávy a jaká bezpečnostní řešení doporučujete nasadit?

Většina systémů pro VS vlastní atestaci podle platné legislativy, ovšem tato skutečnost nezaručuje, že jsou opravdu bezpečné. Nechci tím říci, že jsou špatné či nevyhovující, ale nelze spoléhat na standard zabezpečení

aplikace samé. Je téměř nutně řešit bezpečnost jinými nástroji. Zvláště pak, pracuje-li aplikace se supertenkým klientem a přistupuje-li do ní uživatel prostřednictvím browseru, a to libovolně z internetu či v prostředí intranetu. Zde je vhodné nasadit UTM bránu s aplikačními proxy bránami, jako je **McAfee Firewall Enterprise (Sidewinder)**, který dokáže nekompromisně kontrolovat celý provoz a kombinovat antivirovou, antispýwarovou ochranu, IPS, URL Filtraci, SCP, SFTP a SSH dešifraci. Správu uživatelů je potřeba řešit prostřednictvím IDM v kombinaci se správou rozhraní pro Remote Access tzv. Active Identity. Funkce tohoto rozhraní umožňuje organizacím řešit různé scénáře zabezpečení přístupu uživatelů, jako jsou vzdálený přístup přes VPN, přístup k aplikacím přes webové rozhraní či přístup k aplikacím a datům v LAN.

Většina technologií se dá účinně chránit, nicméně při výběru aplikace je vhodné konzultovat výběr aplikace s bezpečnostním expertem, neboť řešení se liší nejvíce v cenách a asi není cílem nasadit aplikaci a stejnou cenu prostředky na její zabezpečení. Naopak je dobré vybrat aplikaci, kterou lze ochránit standardem, který již existuje. V této oblasti je výjimečným tématem systém datových schránek, neboť správcem je stát, potažmo Česká pošta, ochrana je zajištěna formou hesla na přístupu. Ovšem o úrovni zabezpečení nepochybují jen odborníci, ale také tzv. poučená veřejnost. Proto je nutné zabezpečit na své straně alespoň obsah před neoprávněnou modifikací.

Proč a jak nejlépe chránit veřejně dostupné informace?

Pokud si prostudujete zák. 106/1999 Sb., o svobodném přístupu k informacím, tak zjistíte, že nejsnadnější cesta vede k informacím přes žádost v duchu jeho ustanovení. Kde je tedy riziko a proč chránit systémy, sítě a data úřadů? Riziko je v neoprávněné modifikaci dokumentů, získání údajů o vnitřní komunikaci a veškerých záležitostech, které předcházejí schvalovacím procesům ve volených orgánech veřejné správy. Proto je vhodné chránit perimetr komplexně a hlavně účinně. Portfolio společnosti McAfee nabízí jak **aplikační UTM firewall McAfee Firewall Enterprise**

(**Sidewinder**), tak komplexní ochranu **Email a Web komunikace McAfee Total Protection for Internet Gateways**, která v sobě kombinuje tři sofistikované bezpečnostní McAfee řešení, jež jsou dlouhodobě špičkou ve svém oboru. Jsou to: **McAfee Web Gateway** (dříve Webwasher), **McAfee Email Gateway** (dříve IronMail) a **McAfee Network DLP Prevent** (dříve Reconnex iGuard Prevent). Kombinace těchto tří produktů přináší maximum výkonu při minimalizaci nároků na administraci.

Zmiňovaná řešení v oblasti bezpečnosti nabízí společnost Comguard.