Prípadová štúdia nasadzovania KERBERu

Mesto VEĽKÝ KRTÍŠ

Prvé písomné zmienky o meste **Veľký Krtíš** pochádzajú už z 13. storočia a v dnešnej dobe je centrom Hontiansko-novohradského regiónu.
Mesto Veľký Krtíš patrí do Banskobystrického samosprávneho kraja s počtom **13 120 obyvateľov**.
Orgánmi mesta sú mestské zastupiteľstvo a primátor mesta. Ich výkonným orgánom je mestský úrad, ktorý zabezpečuje chod mesta a aplikovanie nariadení do praxe.

Organizácia :
Mesto Veľký Krtíš
www. velky-krtis.sk

Odvetvie :
Verejná správa

Požiadavky :
Zabezpečiť bezpečné pripojenie na Internet

Riešenie :
Kerber – 50 užívateľov

Požiadavky zákazníka

Mestský úrad v rámci svojej činnosti pracuje s rôznymi druhmi informácií, ktoré majú rôzny stupeň dôvernosti. Preto je nutné s niektorými údajmi pracovať obozretne a zabezpečiť, aby sa nedostali do nepovolaných rúk. Pri realizácii týchto cieľov je potrebné sa riadiť výnosom Ministerstva financií MF/013261/2008-132 o štandardoch pre informačné systémy verejnej správy.

V tejto súvislosti bolo potrebné zabezpečiť :

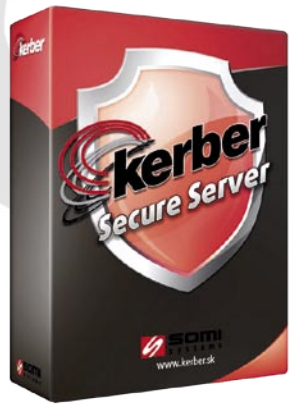
- riadenie informačnej bezpečnosti,
- zabezpečenie realizácie a dodržiavania bezpečnostnej politiky,
- implementáciu systému riadenia a monitorovania rizík v súvislosti s informačným systémom verejnej správy, a to najmä podľa relevantných technických noriem a pravidelné zbieranie relevantných údajov súvisiacich s rizikami a možnými hrozbami
- identifikáciu, analýzu a hodnotenie rizík spojených s využívaním aktív a informačného systému úradu mimo priestorov úradu,

kerber

Požiadavky zákazníka

- zavedenie ochrany informačného systému úradu pred škodlivým kódom najmä v rozsahu:
  1. detekcie prítomnosti škodlivého kódu na všetkých používaných zariadeniach informačného systému verejnej správy,
  2. kontroly súborov prijímaných zo siete Internet a odosielaných do siete Internet na prítomnosť škodlivého softvéru,
  3. detekcie prítomnosti škodlivého kódu na všetkých webových sídlach,
- zabezpečenie ochrany vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (firewall) pre informačný systém,
- zabezpečenie existujúcich záložných kapacít informačného systému, zabezpečujúcich funkčnosť alebo náhradu informačného systému úradu,
- periodické hodnotenie zraniteľnosti,
- zavedenie identifikácie používateľa a následnej autentizácie pri vstupe do informačného systému úradu,
- určenie bezpečnostných zásad pre mobilné pripojenie do informačného systému a pre prácu na diaľku; mobilným pripojením je najmä prenosný počítač a personal digital assistant (PDA),
- zabezpečenie proti používaniu informačného systému úradu na nelegálne účely.

Nasadené riešenie



Z požiadaviek zákazníka vyplynulo, že požadovaný produkt musí vysoko spĺňať bezpečnostné štandardy na komunikáciu v Internete a všeobecne v počítačových sieťach.

Tieto požiadavky v plnej miere ponúka produkt **KERBER**. Jedná sa o modulárny softvérový produkt, určený na ochranu firemných sietí pred rôznymi typmi útokov, či už z Internetu , alebo zvnútra siete. Celé riešenie je postavené nad operačným systémom Linux s jednoduchým a prehľadným grafickým rozhraním, ktoré umožní každému administrátorovi komplexne nastaviť funkcionalitu požadovanej ochrany.

Ďalšou požiadavkou zákazníka bolo, aby nasadzovanie systému čo najmenej obmedzilo prevádzku na úrade a bolo maximálne plynulé.

Štandardom našej spoločnosti je aj možnosť využitia bezplatnej testovacej prevádzky na našom hardvéri. Túto možnosť využil aj MsÚ Veľký Krtíš a testovacia prevádzka bola spustená na testovacom serveri našej spoločnosti HP ML150 G5, kde boli nainštalované všetky moduly systému okrem modulu SAS. Primárne zameranie je na moduly IDS (Intrusion Detection System), HTTP filtrovanie a Bandwidth Monitoring (monitorovanie šírky pásma). Testovacia prevádzka trvala takmer tri týždne, kedy boli aktívne zbierané logy, ktoré sa následne vyhodnotili a boli prezentované vedeniu MsÚ v spolupráci s informatikom p. Gregušom.

Na základe týchto údajov sa vedenie mestského úradu rozhodlo pre zakúpenie systému KERBER a inštaláciu na vlastný server. Tento server sa ešte počas behu testovacej prevádzky presunul k nám do spoločnosti, kde sa identicky nainštaloval a nakonfiguroval. Následná výmena na mieste prebiehala jednoducho a bezproblémovo, kde odstávka pre lokálnych užívateľov úradu nepresiahla 5 minút.

kerber

Nasadené riešenie

Jednotlivé moduly systému KERBER :

- **VPN tunel**, ktorý poskytuje bezpečný prístup k firemnej infraštruktúre z ktoréhokoľvek miesta na svete. Samozrejmosťou je šifrovaný prenos využívajúci najmodernejšie technológie šifrovania. Grafické rozhranie obsahuje plnohodnotnú konfiguráciu klientskych certifikátov a kľúčov s ich jednoduchým exportom smerom k používateľovi.
- **HTTP filtrovanie** poskytuje transparentný a konfigurovateľný proxy server, ktorý je optimalizovaný pre potreby konkrétnej siete. Zabezpečuje ochranu pred malware. Súčasťou HTTP filtra je tiež redirector, vďaka ktorému môže administrátor určovať používateľom podmienky pre surfovanie na webe, či už na základe času, cieľovej domény, alebo zdrojovej IP adresy. Obsahuje tiež predkonfigurované a obsahovo bohaté cieľové blacklisty rôzneho zamerania (napr. porn, jobsearch, chat a pod.).
- **Stavový firewall,** pomocou ktorého administrátor dokáže na jeho základe riadiť sieťovú komunikáciu alebo prístup do Internetu. Povoľuje prístupy k svojim sieťovým službám alebo aktivuje ich ochranu. Firewall slúži ako kontrolný bod, ktorý určuje pravidlá komunikácie medzi sieťami.
- **IDS (Intrusion Detection System)** čiže technika odhaľovania neoprávnenej či nezvyklej aktivity v počítačovom systéme alebo v sieti. Modul IDS chráni pred sieťovými útokmi na nezabezpečené služby, útokmi na aplikácie, neautorizovaným prihlásením, neoprávneným prístupom k citlivým dátam ako aj pred malware (vírusy, trójske kone a červy, ...).
- **P2P modul** obsahuje funkciu na úspešné blokovanie takzvanej peer-to-peer komunikácie, ktorou zákazník dokáže ušetriť vyše 50 % celkovej Internetovej prevádzky.
- **Bandwidth Monitoring**, ktorý sleduje využitie linky na pripojenie do Internetu. Ponúka prehľad o spotrebe prenosovej kapacity linky podľa jednotlivých používateľov pristupujúcich na Internet.
- **KERBER antivír** – antivírový softvér vyvíjaný komunitou antivírových odborníkov zvaný **ClamAV** a antivírové riešenie **NOD32** od nášho partnera Eset.

Prínosy riešenia

„Nasadenie systému Kerber v našej organizácií, ako prvé prinieslo zefektívnenie pripájania pracovníkov na Internet. Vďaka početným blacklistovým databázam sme úspešne dokázali obmedziť využívanie internetu na súkromné účely. Pozitívne hodnotím aj to, že pomocou VPN tunelov sa môžu naši pracovníci bezpečne pripájať na informačný systém úradu z akéhokoľvek miesta. Tak isto sa do značnej miery zvýšila aj bezpečnosť pripájania sa do internetu vďaka výkonnému stavovému firewallu. Celá činnosť systému je ešte podčiarknutá profesionálnou hotline podporou a nepretržitou kontrolou funkčnosti systému. Napriek tomu že Kerber ja na našom úrade ešte len pár mesiacov, môžem objektívne povedať, že boli naplnené naše očakávania o činnosti takéhoto systému“.

Pavel Greguš

Správca siete MsÚ Veľký Krtíš