kerber

Prípadová štúdia nasadzovania KERBERu

Remeslo skupina s.r.o.

REMESLO skupina je značka, pod ktorou vystupuje niekoľko spoločností, ktoré rozvíjajú svoje podnikateľské aktivity v stavebníctve, doprave, strojárstve a cestovnom ruchu. Skupina REMESLO spoločností zamestnáva viac ako **500 ľudí**.

Spoločnosť :
REMESLO skupina s.r.o.

Odvetvie :
Stavebníctvo, strojárstvo, doprava, obchodná činnosť, stolárska výroba, cestovný ruch

Požiadavky :
Komplexné zabezpečenie podnikovej siete

Riešenie :
KERBER (80 užívateľov) nasadený na serveri IBM System X3200 M2

Požiadavky zákazníka

Remeslo, ako skupina zastrešujúca viacero firiem pôsobiacich v priemysle a cestovnom ruchu v rámci svojich podnikateľských aktivít pracuje s veľkým množstvom informácií a dát. Tie sú do vysokej miery duševným vlastníctvom týchto spoločností, a preto je nutné s týmito údajmi pracovať obozretne a vo vysokej miere ich zabezpečiť, aby sa nedostali do nepovolaných rúk. Toto bola jedna z požiadaviek nášho zákazníka.

V tejto súvislosti bolo potrebné zabezpečiť :

- zabezpečenie realizácie a dodržiavania bezpečnostnej politiky,
- pravidelné zbieranie relevantných údajov súvisiacich s rizikami a možnými hrozbami,
- riadenie informačnej bezpečnosti,
- zavedenie ochrany spoločnosti pred škodlivým kódom a to najmä v rozsahu:
  1. kontroly súborov prijímaných zo siete Internet a odosielaných do siete Internet na prítomnosť škodlivého kódu,
  2. detekcia škodlivého kódu na všetkých internetových sídlach,
  3. kontroly prichádzajúcej elektronickej pošty na prítomnosť škodlivého kódu a nepovolených príloh,

kerber

Požiadavky zákazníka

- zabezpečenie ochrany vonkajšieho a vnútorného prostredia prostredníctvom nástroja sieťovej bezpečnosti (firewall) pre informačný systém,
- rozčlenenie podnikovej siete na zóny,
- začlenenie VPN privátnych sietí pre obchodných zástupcov,
- bezpečné a funkčné prepojenie medzi pobočkami,
- nastavenie prístupových práv pre používateľov na web,
- prideľovanie adries v DMZ pomocou DHCP,
- periodické hodnotenie zraniteľnosti.

Nasadené riešenie

Z požiadaviek zákazníka vyplynulo, že požadované riešenie musí spĺňať vysoké bezpečnostné štandardy nie len v komunikácii na Internete, ale aj všeobecne vo všetkých počítačových sieťach spoločnosti Remeslo.

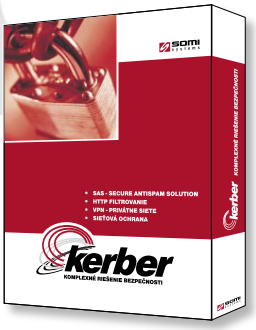
Tieto požiadavky v plnej miere ponúka produkt **KERBER**. Jedná sa o modulárny softvérový produkt určený pre ochranu firemných sietí pred rôznymi typmi útokov, či už z Internetu alebo zvnútra siete. Celé riešenie je postavené nad operačným systémom Linux s jednoduchým a prehľadným grafickým rozhraním,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

Spoločnosť Remeslo sa rozhodlo pre inštaláciu celého systému KERBER so všetkými jeho modulmi. Primárne zameranie inštalácie je na moduly SAS (Secure Antispam Solution), http filtrovanie a VPN - privátne siete.

Osadenie, premigrovanie a počítačové nastavenie bolo realizované v priebehu jedného dňa, bez akýchkoľvek problémov. Pri inštalácii bol premigrovaný Mail Server aj s existujúcimi adresami od poskytovateľa mailov na lokálny server a dodatočne sa po pár mesiacoch prevádzky premigrovala aj ďalšia nezávislá doména. V DMZ zóne bolo umiestnené wifi v rokovacej miestnosti a fyzicky oddelené od lokálnej siete. Pomocou troch sieťových kariet v Kerber Serveri bola firemná sieť logicky rozčlenená na Internet, Intranet a DMZ. Adresy v DMZ zóne sú prideľované pomocou DHCP umiestneného na Kerber Serveri. Prístup na Internet bol rozčlenený a následne boli nastavené rôzne prístupové práva, pre rôzne skupiny používateľov (napr. riaditelia, IT staff, bežní používatelia).

Ďalšou požiadavkou bolo nastavenie transparentného proxy, čo po spustení zabezpečilo, že ľubovoľný systém vo vnútornej sieti má automatický prístup na net aj bez konfigurácie proxy serveru.

Systém KERBER bol nainštalovaný na samostatný nový Kerber Server IBM System x3200 M2.



Jednotlivé moduly systému KERBER:

- **SAS (Secure Antispam Solution)**, je produkt vyvinutý spoločnosťou SOMI Systems a.s. na základe voľne dostupných opensource nástrojov. Na trhu je úspešne predávaný už niekoľko rokov a bol implemetovaný vo viacerých významných spoločnostiach. Integráciou do systému KERBER získal SAS grafické používateľské rozhranie, cez ktoré je možná konfigurácia jednotlivých funkcií, ako sú nastavenie príjmu a odosielania elektronickej pošty, zapnutie jednotlivých filtrov pre analýzu a kontrolu pošty.

Nasadené riešenie

SAS zohľadňuje požiadavky na flexibilný, vysoko výkonný, ľahko škálovateľný a manažovateľný produkt, zameraný na komplexnú ochranu pred nevyžiadanou elektronickou poštou. Je to riešenie, ktoré eliminuje problémy so SPAMom a jeho odstraňovaním na čo najnižšiu úroveň.

- **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.
- **DHCP (Dynamic Host Control Protocol)** - jednou z možností, ako zabrániť kolíziám IP adries v sieti spolu s uľahčením konfigurácie klientskych zariadení je použiť DHCP Protokol. DHCP slúži k dynamickému nastaveniu vlastnej IP adresy, masky siete, IP adries DNS serverov a brány. Počítač kontaktuje DHCP server a vyžiada si potrebné informácie. DHCP server pridelí adresy na základe uvedeného rozsahu adries a z neho rozdáva a berie späť. Jednou z možností je, aby DHCP server prideľoval IP adresy na základe fyzických MAC adries sieťových kariet.

Prínosy riešenia

„Systém Kerber, v plnom rozsahu splnil naše požiadavky ohľadom bezpečnosti podnikovej siete. Od jeho spustenia, už prakticky nemáme žiadny problém s nevyžiadanou elektronickou poštou. V jeho prehľadnom grafickom rozhraní, je jednoduchá administrácia a zadávanie pravidiel pre jednotlivé skupiny užívateľov pohybujúcich sa po Internete. To pre nás znamená, ochranu pracovných staníc a tak isto aj zamedzenie používaniu Internetu na súkromné účely v pracovnom čase zamestnancov. Výhodná a zaujimavá sa mi javí aj možnosť vytvárania vlastných blacklistov a whitelistov, a v prípade akýchkoľvek náznakov problémov mám k dispozícii podrobné štatistiky o behu celého systému. Na vysokej profesionálnej úrovni je aj váš hotline a celkovo komunikácia s oddelením technickej podpory. Rozhodnutie zakúpiť Kerber, bolo určite správnym rozhodnutím.“

Ing. Richard Ševčík
IT Manažér