

# Soitron chráni mailové schránky spoločnosti SPP



## Spoločnosť

Slovenský plynárenský priemysel, a.s.

## Zameranie

Dodávka zemného plynu a elektrickej energie

## Počet zamestnancov

985 (počet zamestnancov k 31.12.2012)

## Požiadavky

- \* Zabrániť neželanému a potenciálne nebezpečnému zahlcovaniu firemných mailových schránok spamom.
- \* Znížiť náklady, ktoré spam prináša v podobe zahlcovania prenosových kapacít a diskových priestorov.
- \* Zvýšiť ochranu firemnej počítačovej siete a firemných dát eliminovaním bezpečnostných rizík, keďže spam máva často podobu podvodných emailov alebo obsahuje škodlivý softvér.

## Riešenie

- \* Posúdenie dizajnu celej podnikovej siete.
- \* Nasadenie hardvérovo-sofтверového riešenia Cisco IronPort, ktoré je výkonné, vysoko dostupné a škálovateľné podľa budúcich potrieb podniku.

## Výsledok

- \* Odbremenenie IT oddelenia. Vďaka karanténe sa informatici nemusia zaoberať dopytmi používateľov, ktorí nevedia nájsť očakávané e-mail

a nezaťažuje ich ani prevádzka IronPortu, ktorý je vo veľkej miere autonómny.

- \* Odľahčenie celej IT infraštruktúry, ktorá nie je zahltená spamom.
- \* Zníženie bezpečnostných rizík, či už v podobe prieniku škodlivého softvéru do firemnej siete alebo úniku podnikových dát.

Zamestnanci spoločnosti Slovenský plynárenský priemysel, a.s. (SPP) mesačne prijmu a odošlú vyše 200 tisíc mailov. Keďže vyše tri štvrtiny celosvetovej mailovej premávky tvorí nevyžiadaná pošta (spam), je prirodzené, že firma sa snaží, aby mailové servery a tým aj beztak preplnené schránky zamestnancov nezahľovali neželané a potenciálne nebezpečné správy. Obzvlášť keď náklady na spam – či v už v podobe zníženia produktivity zamestnancov, ale aj zvýšených nákladov na potrebné prenosové kapacity či úložný priestor – sú enormné. Podľa Journal of Economic Perspectives uvaluje spam na celú globálnu spoločnosť náklady 20 mld. USD ročne.

## Pôvodný stav

Manažéri SPP si vysokú cenu a riziká spamu uvedomujú a záleží im na tom, aby ich eliminovali. Keďže spameri sú čoraz sofistikovanejší a antispam, ktorý spoločnosť v minulosti využívala prestával vyhovovať a nemal ani podporu na požadovanej úrovni, bolo rozhodnutie vybrať nové riešenie jednoduché a priamočiare.

Hlavná požiadavka bola zabezpečiť vyše päť tisíc firemných schránok proti spamu a malwaru pomocou výkonného, vysoko dostupného a škálovateľného systému, ktoré zvládne nielen súčasné technologické hrozby, ale bude pripravené aj na budúcnosť.

SPP sa rozhodol pre hardvérovo-sofтверové riešenie Cisco IronPort, ktoré implementuje spoločnosť Soitron. Hlavným dôvodom pre voľbu tohto antispamového systému bolo, že už niekoľko rokov využíva neustále



*„Ideálny bezpečnostný systém je taký, o ktorom zákazník ani nevie, že ho má.“*

Maroš Rajnoch  
Produktový manažér Soitron, a.s.

aktualizované reputačné databázy bežiacie v cloude. Systém si v nich preveruje, akú reputáciu má server, ktorý žiada o komunikáciu – a podľa toho rozhoduje, ako daný mail vyhodnotí. Energetikov tiež presvedčilo, že riešenie používajú na Slovensku viaceré podniky a napokon aj sám dodávateľ Soitron. „Vedeli sme pri výberovom konaní predložiť detailné náhľady do prevádzky, vrátane rôznych štatistík,“ hovorí Juraj Audi, projektový manažér spoločnosti Soitron.

## Nové riešenie

Okrem reputačných databáz a viacerých referencií, zaujali SPP aj ďalšie kľúčové vlastnosti IronPortu.

- \* Obsahuje široké spektrum rozličných bezpečnostných modulov. Napríklad pre monitorovanie úniku citlivých informácií z firmy, alebo na šifrovanie mailovej komunikácie. Hoci si SPP nezakúpil licencie

pre všetky z nich, v budúcnosti má možnosť kedykoľvek ľubovoľnú funkcionality jednoducho odomknúť. Napríklad, ak sa SPP rozhodne poslať klientom elektronické faktúry, môžu ich s pomocou IronPortu jednoducho šifrovať.

- \* Je mimoriadne výkonný. IronPort nie je iba softvér – je to zariadenie, ktoré dokáže spracovať obrovské objemy pošty v priebehu niekoľkých sekúnd. A to je pre podnik veľkosti SPP dôležité. Navyše, vďaka robustnosti možno odvrátiť riadené útoky, ktoré môžu odstaviť celý mailový server.
- \* Dá sa jednoducho a rýchlo nasadiť. „Raz nám zavolał zákazník, že má úplne zahltené poštové servery, ktoré začali spamovať medzi sebou,“ hovorí Maroš Rajnoch, produktový manažér spoločnosti Soitron. „Ešte v ten deň sme im IronPort priniesli a nainštalovali. Problém sa okamžite vyriešil, hoci neskôr sme samozrejme systém doladzovali a prispôbovali požiadavkám klienta.“ V spoločnosti SPP nebol potrebný takýto akútny zásah, keďže firma antispamovú ochranu mala. Výhodou však bolo, že IronPort nasadil Soitron bez toho, aby bolo potrebné prerušiť prevádzku predošlého antispamového riešenia.
- \* Prevádzka je bezstarostná. „IronPort má vysoký účinok aj bez detailnej konfigurácie a nastavovania,“ poznamenáva M. Rajnoch. Vďaka dopytovaniu na neustále aktualizované reputačné databázy v cloude je celé riešenie do veľkej miery autonómne a nevyžaduje príliš veľkú pozornosť a údržbu. „Ideálny bezpečnostný systém je taký, o ktorom zákazník ani nevie, že ho má,“ podotýka M. Rajnoch.

Pre úspech projektu bola dôležitá najmä analytická časť, kedy bolo treba špecifikovať celý sieťový návrh a navrhnuť ideálny spôsob implementácie IronPortu. „Pre optimálne nasadenie je dôležité posúdiť existujúci dizajn celej podnikovej siete a špecifické požiadavky firmy, napríklad jej zámery pre budúce rozširovanie,“ vysvetľuje J. Audí prečo je dôležitý výber skúseného dodávateľa.

### Výsledky

Keď sa dnes zamestnanec SPP vracia z dovolenky, nemusí sa báť, že ho po príchode do práce čaká mailbox zahltený stovkami či tisíckami neželaných správ. Ak si systém nie je istý či prichádzajúci mail je alebo nie je spam, prípadne ak spĺňa niektoré z vopred nadefinovaných kritérií

(napríklad obsahuje zašifrovanú časť), zaradí ho do karantény. K nej má zamestnanec prístup, takže ak mu očakávaný mail nechodí, nemusí poslať požiadavky na IT oddelenie a zdĺhavo čakať, pokiaľ mu príde informácia či náhodou systém dotýčný mail nezablokoval. „Pri piatich tisícoch používateľov by IT oddelenie vybavovanie podobných otázok časovo nezvládlo,“ podotýka M. Rajnoch.

Keďže IronPort je vo veľkej miere autonómny, nemá IT oddelenie veľké starosti ani s jeho prevádzkou a údržbou.

Prínosom IronPortu nie je len odbremenenie IT oddelenia, ale aj celej podnikovej IT infraštruktúry. Spam zahlučuje komunikačné linky aj diskový priestor. Navyše, často je nositeľom malwaru, čiže škodlivého softvéru, ktorý narušuje prevádzku počítača, snaží sa získať citlivé informácie, alebo prístup do informačného systému. „Niekdedy nemusí byť malware priamo obsahom spamu, ale v správe môže byť odkaz na web, kde sa malware nachádza,“ dodáva M. Rajnoch.

IronPort nezvyšuje iba bezpečnosť vnútropridávateľskej siete tým, že ju chráni pred škodlivým kódom, ale zabráňuje tiež úniku citlivých informácií z firmy. Systém obsahuje modul DLP (Data Loss Protection), ktorý dokáže robiť hĺbkovú inšpekciu obsahu mailov. Inými slovami, monitoruje mailovú komunikáciu a hľadá slová, čísla alebo iné vopred zadefinované reťazce znakov a čísiel, ktoré by mohli indikovať že ide citlivé dáta. Potom je na zvolenej politike či sa takáto správa predtým ako z firmy odíde zašifruje, alebo či napríklad dostane zodpovedný pracovník upozornenie.

### Použité technológie

CISCO IronPort Email Security Appliance – ESA

- \* Bezpečnostná politika AntiSpam
- \* Reputačná databáza SensorBase a SDN v. 3
- \* Bezpečnostná politika Sophos AntiVirus
- \* Obsahový filter
- \* Virus Outbreak

CISCO IronPort Security Management Appliance – SMA

- \* Karanténa
- \* Reporting

### Slovenský plynárenský priemysel, a.s. (SPP)

SPP je nadnárodná energetická spoločnosť s významným postavením medzi plynárenskými hráčmi v Európe. Spoločnosť priamo nadväzuje na viac ako 155-ročnú tradíciu plynárenstva na Slovensku. Jej hlavné pôsobenie spočíva v dodávke dvoch komodít - zemného plynu aj elektrickej energie. SPP je lídrom na trhu dodávky zemného plynu a spoľahlivým partnerom pre takmer 1,3 mil. slovenských domácností a mnohých komerčných zákazníkov, vrátane popredných podnikov slovenského hospodárstva.

### Soitron

Naša spoločnosť dlhodobo pôsobí na európskom trhu ako systémový integrátor v oblasti IT Infrastructure, Unified Communications, Customer Interaction, Content Management a Security. Už viac ako 20 rokov pomáhame firmám ako Tatra banka, Slovenská sporiteľňa, Orange, E-On, J&T, Hewlett Packard a mnohým ďalším rozvíjať ich biznis. Našou filozofiou je snaha neustále napredovať, preto sme lídrom v zavádzaní unikátnych technológií a inovatívnych riešení. Svedčia o tom aj naše ocenenia ako IT firma roka 2010, Cisco Best Partner of the Year 2012 či zaradenie medzi Veľkú päťku podľa Deloitte Technology Fast 50 (2011). V skupine Soitron pracuje viac ako 600 medzinárodných odborníkov, medzi ktorých patria aj profesionálne tímy v Českej republike, Rumunsku a Turecku.

Pre viac informácií navštívte našu stránku [www.soitron.sk](http://www.soitron.sk)