SOPHOS
Cybersecurity made simple

Microsoft Azure

trizma
accelerate beyond

Postavka Azure Sophos XG Firewall uređaja sa modulom za email zaštitu

Korisnik
Trizma d.o.o.
www.trizma.com

Poslovno okruženje
Kompanija poseduje većinu svojih produkcionih servisa hostovnih na Azure Cloud platformi kao i na Office 365. Poseduje i sigurnosna rešenja koja su bazirana na onpremise hardverskim rešenjima u svom data centru (uglavnom na virtualnoj VMware esxi).

Zahtev
Povećati nivo zaštite bez prekida email saobraćaja, radi smanjenja faktora rizika zbog kojih je moguće narušavanje visoke dostupnosti email saobraćaja.

Rešenje
Kompanija Smart d.o.o. kako bi odgovorila poslovnim zahtevima kompanije Trizma d.o.o. i smanjila rizik za poslovanje, predložila je postavljanje Azure Sophos XG Firewall uređaja sa modulom za email zaštitu.

Profil korisnika

Trizma d.o.o. je osnovana 2002. godine u Beogradu, kao prvi nezavisan Contact Center Outsourcer u Srbiji. Kao rezultat posvećenosti razvoju, konstantnom rastu ljudskog kapitala i poboljšanju poslovnih procersa, 2011. godine Trizma d.o.o. se transformisala u kompletnog BPTO (Business Process Outsourcing and Technology Outsourcing) provajdera, kao i u BPS (Business Process Service) provajdera 2016. godine. Tako je Trizma d.o.o. danas prepoznata kao siguran provajder za vodeće kompanije na globalnom tržištu, u industrijama kao što su finansijske usluge, IT, zdravstvena zaštita i aero-svemirska industrija. U cilju izgradnje dugoročnih odnosa sa klijentima, Trizma d.o.o. je unapredila svoj pristup tako što je ojačala svoju konsultantsku uslugu isporučujući inovativna rešenja koja će klijentima biti od ključne važnosti.

Izazov

Kompanija koristi visoko dostupan cloud email servis Office 365 za sve svoje zaposlene koji se nalaze na više geografskih lokacija u Beogradu, kao i u Banja Luci. Kompanijska email zaštita je onpremise, na koju utiče više faktora rizika zbog kojih je moguće narušavanje visoke dostupnosti email saobraćaja. Potrebno je rešenje koje je moguće postaviti na Azure cloud servis kako bi se povećao nivo zaštite od poznatih i budućih pretnji koje se propagiraju putem email saobraćaja i da kao takav nije vezan za geografsku lokaciju.

Rešenje

Nakon detaljnih razgovora, inspekcije i analize trenutnog rešenja, u saradnji sa IT timom kompanije Trizma d.o.o. izabrano je Azure Sophos XG Firewall appliance rešenje. Sophos je trenutno lider u proizvodnji cloud sigurnosnih uređaja i u okviru porodice mrežno/sigurnosnih uređaja poseduje unapređen model svog virtualnog uređaja koji je moguće postaviti na Azure platformu putem „Azure Marketplace“.

Sophos XG Firewall on Microsoft Azure

Sophos inženjeri iz Smarta uspeli su da postave rešenje u veoma kratkom roku. Sophos Appliance omogućava da se kompletno postavi i konfiguriše bez narušavanja trenutno produkcijske konfiguracije. Tako da prilikom postavke rešenja nije bila narušena email komunikacija kompanije Trizma d.o.o. niti je imala prekida. Nakon kompletno završene konfiguracije klijent je morao samo da preusmeri email saobraćaj promenom javnog MX DNS zapisa.

"Saradnja sa kompanijom Smart je na vrlo visokom nivou. Svi su bili vrlo raspoloženi da odgovore na sve naše zahteve i pruže nam podršku i savete"

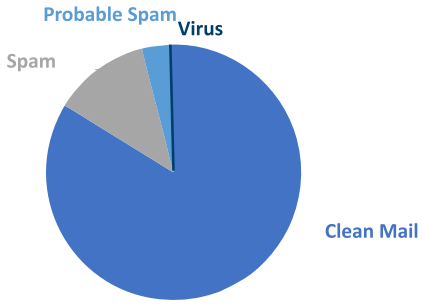
Petar Samardžić, IT specialist, Trizma

Tokom prvog meseca rada Smartovi Sophos inženjeri su zajedno sa IT timom kompanije Trizma d.o.o. nadgledali rad uređaja i vršili dodatna fina podešavanja kako bi zaštita bila na najvišem mogućem nivou.

Sophos Email statistika

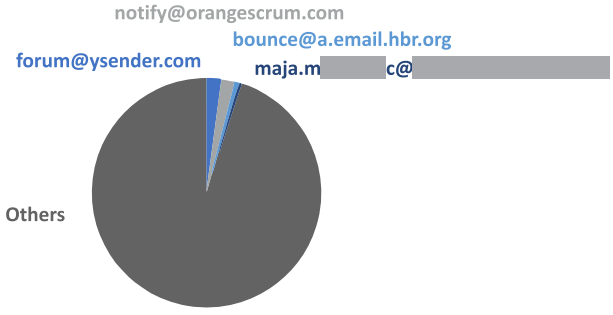
Tokom prvog meseca produkcije implementiranog rešenja, dobili smo sledeće rezultate:

Mail Traffic Summary



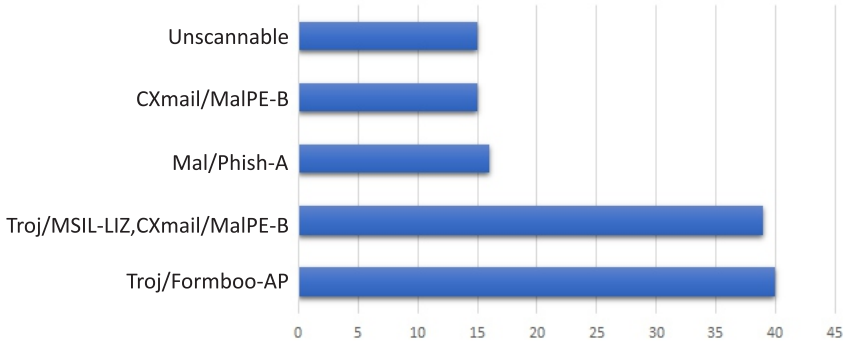
Traffic	Mail Count	Percent
Clean Mail	48197	83,73%
Spam	7024	12,21%
Probable Spam	2101	3,65%
Virus	199	0,35%

Spam Senders



Sender	Mail Count	Percent
forum@ysender.com	190	2,08%
notify@orangescrum.com	167	1,83%
bounce@a.email.hbr.org	62	0,68%
maja.m c@	39	0,43%
Others	8667	87,45%

Mail Virus



CPU Usage

CPU	Max	Min	Average
User	4.45%	0.00%	2.75%
SystemConfiguration	0.78%	0.00%	0.30%
Idle	99.37%	94.77%	96.94%

Disk Usage

Partition	Max	Min	Average
Signature	17.67%	0.00%	14.06%
Config	16.00%	0.00%	14.51%
Reports	6.00%	0.00%	3.47%
Temp	1.10%	0.00%	0.86%

Memory Usage

Memory	Max	Min	Average
Free	4,70 GB	0	4,15 GB
Used	6,28 GB	2,11 GB	2,65 GB
Total	6,80 GB	6,80 GB	6,80 GB

“Sophos XG rešenje je vrlo dobro radilo u našem okruženju. Sophos je odsecao skoro sve spam poruke čak i one koje su bile validne, ali koje su poslate sa domena koji nisu imali odgovarajuće DNS zapise. Ono što je nama u jednom trenutku predstavljalo problem je to što je Sophos blokirao poruke sa zaštićenim prilogom i sa domena koji je bio na listi dozvoljenih pošiljalaca. Ovo je generalno dobro rešenje jer Sophos kontroliše prilog emaila i sa dozvoljenih domena, što znači da i ako bi neko iz te kompanije slučajno ili namerno, poslao zaražen prilog, Sophos bi to blokirao"

Petar Samardžić, IT specialist, Trizma

Sophos XG Firewall on Microsoft Azure

Tehničke karakteristike

Email Protection and Control

- Email scanning with SMTP, POP3, and IMAP support
- Reputation service with spam outbreak monitoring based on patented RecurrentPattern-Detection technology
- Block spam and malware during the SMTP transaction
- Spam greylisting
- Recipient verification for mistyped email addressed
- Second independent malware detection engine (Avira) for dual-scanning
- Live Protection real-time, in-the-cloud lookups for the latest threat intelligence
- Automatic signature and pattern updates
- Smart host support for outbound relays
- File-Type detection/blocking/scanning of attachments
- Accept, reject or drop over-sized messages
- Detects phishing URLs within emails
- Use pre-defined content scanning rules or create your own custom rules based on a variety of criteria with granular policy options and exceptions
- TLS Encryption support for SMTP, POP, and IMAP
- Append signature automatically to all outbound messages
- Email archiver
- Individual user-based block and allow sender lists maintained through the user portal

Email Quarantine Management

- Spam quarantine digest and notification options
- Malware and spam quarantines with search and filter options by date, sender, recipient, subject, and reason with option to release and delete messages
- Self-serve user portal for viewing and releasing quarantined messages

Azure VM specifikacija i potrošnja na mesečnom nivou

Specifikacija Azure VM: Standard D2 VM
CPU: 2 vCPUs
Memorija: 7GB
Potrošnja/mesec: 99,57$

SMART
new frontier group

21000 Novi Sad
Kralja Aleksandra 12
021/ 47 28 200
office@smart.rs
www.smart.rs

Smart d.o.o.

Kompanija Smart d.o.o. je osnovana 2000. godine kao informatički edukativni centar. Danas predstavlja jednu od vodećih Solution & Service kompanija u Srbiji koja svojim korisnicima usluga obezbeđuje konstantan kvalitet. Svoje poslovanje zasniva na područjima konsaltinga, rešenja, edukacije, podrške i licenciranja.

Dugogodišnjim radom i usavršavanjem poslovnih procesa, kompanija Smart je ostvarila značajna partnerstva, između kojih su i Microsoft Gold Partnerstvo, kao i Regionalna Distribucija i Partnerstvo sa kompanijom Sophos. Od 2003. godine, Smart u svom timu ima sertifikovane stručnjake za pružanje kvalitetne tehničke 24/7 podrške korisnicima Sophos rešenja u regionu.