SOPHOS
Cybersecurity made simple

Microsoft Azure

trizma
accelerate beyond

Deploying Azure Sophos XG Firewall Appliance with email protection module

User

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

Business environment

The company have most of its own production services hosted at Azure Cloud platform as well at Office 365. It also has security solutions based on on-premise hardware solutions in its data centar (mainly on virtual VMware esxi).

A request

Increase the level of protection without interruption email traffic, to reduce risk factors which could be disturbe high availability (HA) email traffic.

Solution

In order to responded to business demands of company Trizma d.o.o. and reduced risks, company Smart d.o.o. suggested setting up Azure Sophos XG Firewall Appliance with module for email protection.

User profile

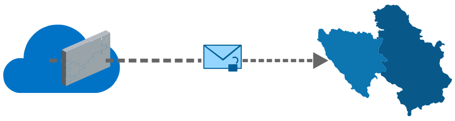
Trizma d.o.o. was founded in Belgrade in 2002 as the first independent Contact Center Outsourcer in Serbia. As a result of commitment to development, continuous growth of human capital and business processes improvement, in 2011 Trizma d.o.o. was transformed into a full Business Process Outsourcing and Technology Outsourcing (BPTO) provider and to a Business Process Service provider (BPS) in 2016. Today, Trizma d.o.o. is recognized as a secure provider for leading companies in the global market, in industries such as financial services, IT, health care and aero-space industry. In order to build long-term relations with clients, Trizma d.o.o. has improved its approach by making it strengthened its consulting service by delivering innovative solutions that will be crucial to the customers.

Challenge

The company uses a highly available cloud email service Office 365 for all employees who are in different geographical locations in Belgrade, as well as in Banja Luka. Company email protection is on-premise, to which affects more risk factors for possible high distortion availability of email traffic. It takes a solution that can be set up on the Azure cloud service to increase the level of protection against known and unknown, future threats which has been propagated through email traffic, without geographic location.

Solution

After detailed interviews, inspections and analysis of the current solution, in cooperation with the IT team of the company Trizma d.o.o., Azure Sophos XG Firewall appliance solution was chosen. Sophos is currently the leader in production cloud security devices. Within the family of network/security devices, Sophos has an upgraded model of its virtual device which could be set up on the Azure platform through the "Azure Marketplace".



Sophos XG Firewall on Microsoft Azure

Sophos engineers from company Smart managed to set up solution in a very short time. Sophos Appliance allows to be complete set up and configure without breaking current production configurations. During the solution deployment email communication of the company Trizma d.o.o. were not disturb and had no breaks. After the configuration has been completed, client only had to redirect email traffic by changing public MX DNS records.

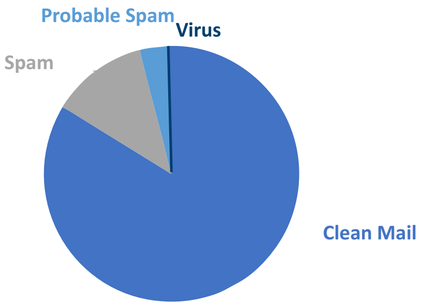
> *"Cooperation with Smart is at a very high level. They were all very acessible to respond to all our requests and to give us support and tips"*
>
> Petar Samardžić, IT specialist, Trizma

During the first month of work, Sophos engineers from Smart are together with the IT team of the company Trizma d.o.o. supervised the operation of the appliance and performed additional fine settings for highest possible protect.

Sophos Email Statistics

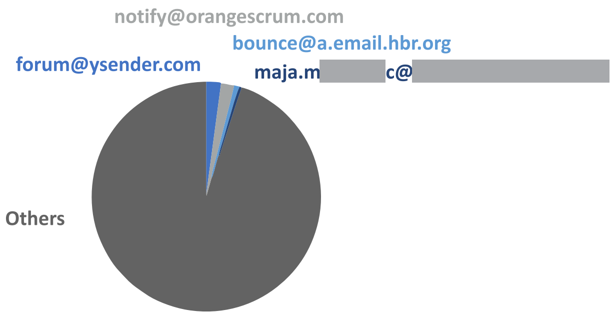
During the first month of production implemented solutions, we got the following results:

Mail Traffic Summary



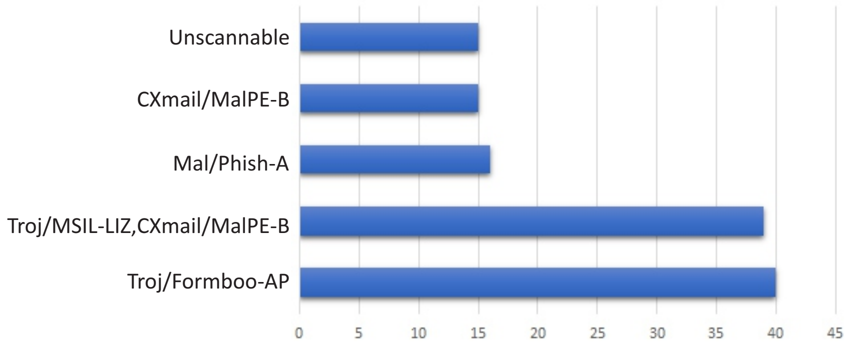
Traffic	Mail Count	Percent
Clean Mail	48197	83,73%
Spam	7024	12,21%
Probable Spam	2101	3,65%
Virus	199	0,35%

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[redacted]c@[redacted]	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

“The Sophos XG solution worked very well in our environment. Sophos cut off almost all spam messages, even those that were valid, but which are sent from domains that did not have the appropriate DNS records. At one point, the problem was that Sophos blocked messages with protected attachment and from the domain that was on the list of allowed senders. This is generally a good solution because Sophos controls the email attachment even from allowed domain, which means that if someone from these companies accidentally or intentionally send infected attachment, Sophos would block it"

Petar Samardžić, IT specialist, Trizma

Sophos XG Firewall on Microsoft Azure

Technical Specifications

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 specification and consumption on monthly level

Specification Azure VM: Standard D2 VM
CPU: 2 vCPUs
Memory: 7GB
Consumption/month: 99,57$

SMART
new frontier group

21000 Novi Sad
Kralja Aleksandra 12
+381 21 47 28 200
office@smart.rs
www.smart.rs

Smart d.o.o.

Company Smart d.o.o. was founded in 2000 as an IT educational centar. Today it is one of the leading Solution & Service companies in Serbia which provides to its users constant quality. Our business is based on areas of consulting, solutions, education, support and licensing.

Thanks to many years of working and developing business processes, Smart has made significant partnerships, among which are the Microsoft Gold Partnership and Regional Distribution and Partnership with Sophos. Since 2003, company Smart has a team of certified security experts in providing quality technical 24/7 support for users of Sophos solutions in the EE region.