Securing Data Through Network Segmentation in Modern Enterprises

A TrendLabs℠ Primer

We began this series on data protection by discussing the need to understand and implement **data classification** in the primer ***Data Classification in Hybrid Clouds: An Overlooked but Critical Step in Data Protection***. We also went through upcoming regulations that would impact enterprises, as well as methods that can help deter threats.

To provide further information on the importance of data classification, we will be sharing another defense strategy: network segmentation. Focusing on network segmentation is the next logical step for enterprises to continue improving security after data is classified, distributed, and given appropriate security measures.

Corporate environments, which get bigger and bigger as they take in more functions, are more difficult to protect. The application of network segmentation, however, provides IT administrators a solid foundation in effectively maintaining and improving security in a growing network.

Standards, Function, and Results of Network Segmentation

Network segmentation, in a general sense, means clustering systems that work in a similar capacity and isolating them from other clusters. Dividing systems gives enterprises the ability to prioritize the security of networks containing highly sensitive data over those with low or even moderately sensitive data. Thus, having a segmented network makes it difficult for attackers and/or unauthorized people to navigate through networks carrying sensitive data. Traditionally, network segmentation was difficult to achieve, since maintaining and updating networks in large corporate environments is time consuming and tedious. However, the availability of software-defined segmentation today has made network segmentation much easier to implement and maintain.

As enterprises handle different types of data across varying network environments, network segmentation could be done in several ways. Over the years, different industries have developed a number of models that work best in their field. Here are some examples of popular models and how they help protect data:

Purdue Model of Control Hierarchy – is a guide for Industrial Control Systems (ICS) network and is known to make use of zones that include systems that have similar functions or requirements. The framework for this model identifies six zones and five levels and is built upon the hierarchy of security devoted to networks and the corresponding data stored within each network. Meanwhile, access and communication to users beyond the network, which are usually vulnerable to attacks, are done through demilitarized zones in order to protect the rest of the network in the event of an attack.

Payment Card Industry Data Security Standard (PCI DSS) – is a global data security standard adopted by payment card companies that process, store, or transmit cardholder data. Along with enterprises that employ network segmentation in ICS networks, this strategy is used to limit access to highly sensitive data. For enterprises that utilize payment data and operate with third party vendors or affiliates, it is necessary to create a secure network that stores highly sensitive data such as customer account information.

Infosec Institute Network Segmentation with virtual local area networks (VLANS) – this model creates a collection of isolated networks within a data center, with each network as a separate broadcast domain. This model provides protection for networks and data centers and even cloud storage facilities.

Micro Segmentation – this strategy protects the network by breaking down the network into smaller chunks through the use of firewalls, host firewalls, VLANs, virtual private networks (VPN), and network administrator or access. Adding such complexity to the network slows down the progress of attacks and increases the visibility of unauthorized use or entry into a network.

What's common across the aforementioned examples is the creation of multiple levels or layers into the enterprise network. Besides creating separate, small networks, specific privileges are also applied to these networks to limit access. This procedure is used to effectively keep unauthorized persons from accessing highly sensitive files. Aside from limiting access, networks containing sensitive information may also require whitelisting to specifically define acceptable communication paths and block everything else not included in the whitelist.

This particular way of protecting data isn't focused on highly sensitive data alone, as it was originally designed to protect all kinds of data and to mitigate the damage of known threats like data breach and ransomware. For IT administrators, data segmentation provides them with visibility over every network. Data segmentation also gives IT administrators a boost in their capability to protect each segment since they can control access and communication among segments and monitor suspicious communication and movement. With this, IT administrators can also quarantine threats and thus protect each segment adequately.

Nefarious Network Threats

As discussed, network segmentation can help deter threats. If, for example, every system is connected to a single network, and one unpatched system is exploited to download malware, cybercriminals may access every machine in the network, including servers and data storage centers. With the application of network segmentation, however, the damage of a downloaded malware is limited. For example, even if the ransomware variant Locky has the capacity to infect every file on the network after it has been executed, the effects of the ransomware variant won't go beyond the segmented network. With this, the threat is stopped from spreading.

In the case of data breaches, segmented networks with varying degrees of security can slow down a threat's attempts of lateral movement. Preventing lateral movement is ideal in stopping a threat since there is a bigger chance for a threat to be spotted if the threat stays in the system longer. In general, network segmentation is capable of creating an environment that's safer for enterprise data and is also effective in making it harder for attackers to pursue their motives.

Network Segmentation on Site

Setting up a secure segmented network is especially crucial for various enterprise environments. In an enterprise that has volumes of communication within its own networks, setting up parameters to secure highly sensitive data is crucial. Doing so prevents unauthorized access of these networks by malicious actors, employees, or even partners. This strategy also gives IT admins more control in finding and getting rid of a threat that has made its way into the network.

In the past, we produced research papers on different environments that demonstrated how the applied network segmentation helps in securing different types of environments. In our paper, ***Defending Against PoS RAM Scrapers***, enterprises that used Point of Sale (PoS) machines can utilize this strategy to deter PoS RAM Scraper attacks. The application of the strategy involves placing all PoS systems on a dedicated network that is separate from the corporate network. In the paper, we also identified how network segmentation works as a deterrent against the lateral movement of the threat.

Meanwhile, our paper titled ***Cyber Threats to the Mining Industry*** discussed intricacies of large scale environments that utilized ICS in running day-to-day functions. These enterprises cannot afford to get their systems bogged down with attacks that tamper with physical instruments.

Network segmentation was among our top five security strategy recommendations for the mining industry. Applying such a strategy helps isolate critical networks from facilities that are more likely to get attacked. Given the scale of each operation, this makes it easier to manage and maintain the networks.

Implementing Data Protection in the Near Future

In April 2016, the Council and the European Parliament approved the European Union General Data Protection Regulation (GDPR) and had agreed to enforce it on May 2018. The EU GDPR defines the rights of an individual and sets the obligations of organizations responsible for processing data of individuals. Once the GDPR is implemented, enterprises will have to spend a great amount of time and resource to make the necessary changes in their system in order to continue doing business in the EU. Several provisions of the regulation have already been introduced to give enterprises ample time to assess and improve their data protection capabilities.

From a legal standpoint, enterprises that don't have a secure network may clash with the new the EU GDPR. Among the directives is an article stating that an appropriate level of security must be ensured by taking into account the nature of the data to be secured, as well as the inherent risks. When this law is enacted, enterprises that do not meet the qualification may find themselves unable to do business with entities in the EU.

Enterprises handling EU-related customer data must adapt a security solution that can provide data protection that follows the EU GDPR standard and can achieve PCI DDS compliance.

Protection Beyond Segmentation

Similar to data classification, network segmentation can make it difficult for attackers to succeed. However, the application of network segmentation is not a guarantee that threats will be completely deterred. This strategy is best employed alongside additional security such as malware-blocking capabilities or the ability to detect suspicious communication or movement.

The best protection that can complement network segmentation is having a reliable security solution for the network and the server. An important strength in network security is its capability to shield vulnerabilities from being exploited. An enterprise's network grows with the number of endpoints, and so the risk of vulnerabilities being exploited increases as well. Aside from the rising number of vulnerabilities through endpoints, a network is also susceptible to attacks when using products that no longer receive patch updates.

Another important security capability necessary in segmented networks is system security. This enables IT admins to monitor the integrity of each network and it also provides visibility in terms of changes across the network that may represent malicious behavior. Besides networks, servers should also be shielded from vulnerabilities since there are several known malware that target servers directly instead of entering through common endpoints like desktops.

Created by:

TrendLabs

The Global Technical Support and R&D Center of Trend Micro

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years of experience, we deliver top ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**

Securing Your Journey to the Cloud

www.trendmicro.com

©2016 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.