BIZCOMMUNITY

Lay the foundation for advanced cyber security tech

By Simeon Tassev

7 Jun 2016

It's safe to say that doing business in a digital world without cyber security is not a smart move. Obviously all businesses have some sort of online presence and, whether email or e-commerce, companies are exposed to more risks than they were in the past.

Many business and commercial transactions and interactions now take place online but despite opening up the possibility of collaborating with partners and clients across the globe, these same connections could also potentially provide access to malicious individuals that want to hack your company's network and compromise its position.

While the technology that enables digital commerce and mobile productivity evolves constantly, the malicious technologies designed to compromise business systems evolve just as quickly. From phishing and whaling attacks to ransomware, hackers are always thinking up new ways to compromise critical systems and so organisations need to think about improving their security monitoring and vulnerability management, which often involves advanced security solutions.

In light of the fact that each organisation is unique, with its own specific requirements and working processes, advanced security solutions cannot be called to task like a silver bullet. Before new technology can be implemented to prevent cybercrime, certain foundations must first be laid in order to effectively leverage advanced cyber security technology. Organisations first need to reach a certain level of maturity in terms of security, which means they must have the basics in place first.

Start at the beginning

The first step in addressing security monitoring and vulnerability management is the development of a cyber security strategy. This strategy should consist of various controls and technologies that can allow potential risks and attacks to be identified timeously. One of the biggest problems with detection of cyber attacks in the past was that the company might not know that they’d been hacked or even when it happened and that intruders were stealing information and had been doing so for months, even years, without their knowledge.

With today's technology it is possible to develop a strategy that allows us to actively and proactively monitor all systems, and detect any intrusions as easily as possible to allow for quick response and effective reaction. From a preventative point of view, it's important to look at controls like intrusion prevention systems, advanced threat protection, as a first line of defense.

Additional technologies assume that these first controls did not work. For example, a vulnerability program will check the systems to ensure that there are no weaknesses as research shows that most breaches occur through known vulnerabilities. While there is still the risk of exploiting new vulnerabilities (undocumented, zero knowledge attacks) there might be legacy vulnerabilities that could be exploited further down the line if unchecked.

Having first line systems that generate intrusion or exception alerts is pointless without having the systems that act on those alerts to actively analyse the various stats and possible risks. This technology is known as security information and event management systems, but such technology requires a security system that is mature, in order to effectively analyse and deal with alerts and events, before its too late.

Get the basics right

The biggest prerequisite that companies need to address before implementing advanced cyber security solutions, is to have a clear definition of what they are protecting. Therefore, companies should take a full inventory of all systems, and preferably implement a level of security categorisation. By classifying these systems, you can identify which systems are business-critical and which are back office and non-critical.

Once there's a clear picture of what you're protecting, it's time to put the relevant policies and procedures into place that tell you how protection must be done. For example, it's not enough to say that data must be encrypted to protect it. A policy is required that stipulates how to encrypt data and how to deal with it.

Build the right protection

As soon as the inventory has been done and the policies are in place, only then is it possible to start building the security-technology stack by going through all of your systems and infrastructure. Starting with physical security, the physical controls (access cards, keys, biometrics, etc.) must be assessed before moving to the next level of network access control (how do devices connect to your network?) and then moving to identification management (how do you connect, how do you authenticate?)

This process is stacked, and it's essential to take care of the physical before you can get to the logical. Obviously every single one of those systems needs to be configured and must be be able to provide a level of information – whether it's logging or alerts – that can be used by the identifying system to determine what actions to take.

Data loss prevention is intrinsically connected to advanced cyber security, given that hackers will try to take, compromise, delete or damage your data or hold it to ransom. Your security strategy must extend to your environment and not only protect against people getting to the information, but from extracting data, which means having controls in place that prevent confidential information being emailed, copied or leaked.

Furthermore, companies need to be able to enforce the controls that they have selected to implement around the strategy. There’s no point in having a policy against copying data and emailing confidential information, if you don’t have the tools in place to prevent that action. Without such controls, a system cannot be said to be mature.

Successful cyber security depends on a strategy that has been designed with clear goals in mind. These objectives must be implemented through clearly articulated policies and made effective with the right balance of control and enforcement in order to manage and mitigate the risks that come with doing business in cyberspace.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...