Stopping Breaches with Agile Security by Eccuni

Article published on December 13th 2011 | Internet

It is very important for the network security to improve so that they can address the rapidly changing environment they are in. Unfortunately, many companies suffered damaging and also embarrassing attacks on their network. It has also dealt a devastating blow to the security industry because it has exposed their technologies, systems, services and procedures, which most people rely on. Nowadays, the traditional in IT security is not enough in protecting the IT network.

The traditional security measures and tools we used to have are made to deal with a slow changing setting. In fact, they weren't built to deal with the fast changing resources, applications as well as systems that are now too common nowadays. They weren't built to quickly react against the changing attacks. Computer forensics believes that there are hundreds of millions of new malware in the Web each day and many of these can be seen attempting to breach security systems of companies. These fast evolving threats means that the defense are slowly getting left behind.

As the reality has shown, traditional security tools lose their edge and capabilities to protect the systems quickly. Thus it is important for security to evolve so that they can react to the fast changing environment. It is safe to say that the security must become more mature and agile. Agile security can deliver a much better and effective protection because of the four core elements.

Unlike traditional security that is blind to the changing attacks and environment, agile security can see much better. Because of it, agile security can provide better access to all the unprecedented amount of information; they yield more visibility on the assets of the network, the operating systems, the applications, protocols, users, services, network behavior and also network attacks like viruses and malware.

Since there is visibility, it thus generates data. With data, security can make effective decisions, which requires learning. The learning of security includes the application of data that is generated both locally and from larger communities. Agile security will correlate the events with the knowledge they have gathered, which is an important avenue to understand and make decisions, thus enabling prioritized, informed and automated response.

The only constant thing in the world is change and it also applies in network security. Networks, targets and attacks will change and security must respond to that by changing as well. Agile security can automatically adapt and modify its defenses to provide better protection in the changing environment.

The most important responsibility of security systems is protecting the sensitive data and assets of companies or individuals. Security systems must have policies on allowed applications, prohibited activities and supported devices. Suspicious events must be prioritized and must be reported to security officials like digital computer forensics. Agile security must be flexible in responding to events, risk prioritizing and distributing threat intelligence to deliver the best possible protection and solution.

Agile security's four important elements, seeing, learning, adapting and acting will deliver a much more effective protection because these elements provides the ability of responding to the continues change in the environment.

Nowadays, if you want to see if the security solutions you have can really adapt to the changing environment in the world, you have to look for these important features or essential functions that are built into the agile security.

Agile security must have defense optimization or the ability to tune their security policies automatically to keep with the changes in their environment. No guesswork, but instead an optimized and ensured protection. Agile security must be able to enforce policy compliance and the ability to lock or support networks; preventing undesirable or unauthorized changes, thus reducing the available vulnerabilities in the system. Last but not the least, agile security must have an open structure, which makes it able to support customization as well as modification in their capabilities, but it has to be done only by experts in security or individuals who have completed computer forensics training.

It is important for organizations to have agile security that has the capabilities to adapt to their environment to ensure better protection for their assets and data. Indeed, traditional defenses have been refined and improved to do well today, but they are still nothing compared to agile security.

Article Source:
http://www.articleside.com/internet-articles/stopping-breaches-with-agile-security.htm - Article Side

Eccuni - About Author:

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in cybersecurity and e-commerce. It is the owner and developer of 20 security certifications. EC-Council has trained over 90,000 security professionals and certified more than 40,000 members. These certifications are recognized worldwide and have received endorsements from various government agencies. They also offer trainings in computer forensics.

More information about EC-Council is available at www.eccouncil.org, a Computer forensics, a digital computer forensics, a computer forensics training

Article Keywords:
Breaches, Agile Security, computer forensics, computer forensics training, digital computer forensics, security tools, network security, security industry, traditional security, network behavior, virus, malware, vulnerabilities, E-Commerce, security profe