Article published on December 29th 2011 | Internet

Nowadays, many industries are being haunted by serious and sophisticated threats from cybercriminals. Sadly, most existing security tools and defenses like pen testing are slowly falling behind and being left in the dust by criminals, and even the technologies and methods used to keep pace with the criminals lack the right communications and management skills. These skills would have been necessary in influencing the attitudes of the staff, suppliers and customers of security tools.

Millions of malware appeared a year before and most likely this number would increase more exponentially in the near future. Yet, most security tools become less and less effective against these sophisticated threats. Together with the poor coordination among the security personnel as well as incident handling team, no wonder cybercriminals can compromise any target - we can say the defense is on its heels because of the offense.

In order to address all the threats, industries must have an organization who can improve the security of the industry by using a better strategic value for its customers and employees. There are basically 3 important characteristics that could influence this; the first thing is using more intelligent resource models that have specialized skills, technologies and processes in performing cyber security methods like pen test in a complex network structure. Second is by extracting better value from the existing investments and selecting new technology. Lastly, understanding data whether, internal and external, and the intelligence to learn and know where to act.

To achieve this setting, industries must develop a model, which will allow industries to view their progress according to the different factors like security policy, security monitoring, tracking, malware detection and also intrusion detection. These would help industries understand their security system and how they can further improve these.

Advanced analytics will help security experts to see what is coming and optimize the courses of action that they can use to respond immediately and effectively. Since, cyber attacks become more and more sophisticated and that they are initiated by more determined criminals; the pressure is slowly mounting on industries - to recognize these attacks and respond immediately before even the damage has begun. Security driven by analytics uses statistics; data mining as well as other techniques that would help industries understand the right patterns and attitudes that would deter attacks even before the attack happened.

Security operation has to respond faster by employing automation with the help of human workflow. Automation, when it is properly applied will reduce the need for manpower. When attacks happen and the damage has been done, only human intervention can determine the damage as well as the data loss, but automation can help individuals by supporting them with technologies that will reduce the number of errors a human may make when he is sifting through the thousands of events that happened in an hour. It is a critical key in maintaining the stability in operation, even amidst the new threats that are more sophisticated and more frequent as well as the fast changing technological environment. It can also reduce the number of the steps in the system's workflow in a response as well as the noise from unimportant events that are presented to the operators; plus it helps the industry in the making important decision - decisions in budget, policy, acquisition, operations and also compliance.

The ability to immediately access the virtual assets will provide the security operation with the needed computing resources, processes as well as staff that are required so that they can rapidly meet the imminent dangers from cyber threats. Once the danger has passed, then the system can return to the steady and ready state. Industries aren't limited to the available staff only, with virtualization sourcing for the infrastructure and the applications that are demanded will offer various benefits for the industry - benefits like cost reduction. The flexibility and elasticity of security operation can also be applied in hardware, security software and bandwidth requirements. With virtualization industries can collaborate personally with researchers in reverse-engineering malware, simulate the cyber attack and sharing important knowledge like pen test training.

Industries nowadays, who never knew that they would serve as target from coordinated criminals, are now finding that their important data, intellectual property and key strategies are at risk. The stakes are even higher, thus it is important to transform the security features and systems of industries in order to adapt with changing threats and form a better security.

Article Source:
http://www.articleside.com/internet-articles/creating-and-operating-a-highly-efficient-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 penetration testing.

More information about EC-Council is available at www.eccouncil.org, a pen testing, a pen test, a pen test training.

Article Keywords:
pen test, pen test training, pen testing, cyber threats, security, cybercriminals, security tools, security personnel, cyber security, malware detection, intrusion detection, security system, security software, cyber attack, security features, E-Commerce