Article published on December 8th 2011 | Internet

Without a doubt, hackers are very persistent and that they have the advantage against their victims. However, hackers are still human and if we are aware of their methods, then it is possible to defend the sensitive data of the company. The knowledge on how the company can defend their data could possibly deter any future attacks. If the companies could determine how hackers work, then they could make the right countermeasures against them.

The bright minds behind the maintenance and security of company networks are familiar with DDoS attacks, spear phishing and also defacements on company websites. They have a clear understanding about some methods of hackers such as foot-printing and others that are used in stealing important data. In fact, they are aware the danger hackers pose; a risk of losing millions of dollars that could damage the company's reputation and economical structure. Thus it is important to have knowledge and of course action.

Security Information and Event Management

There are some indispensable tools that could determine how serious or severe the real-time threats in the network of the company are. These are the Security and Event Management software and they work round the clock, providing the latest reports regarding the activities in the system and these could assist those responsible for network security. These tools will report events, such as the alerts regarding the TCP port scan on firewalls, suspicious anomalies on the system as well as the intrusions. All of these reports will be passed to those responsible individuals like those masters degree in information security graduates who will take action.

SIEM can even detect suspicious activities with their employees. For example the company has a swipe ID card system used for identification and an employee entered the business premises after regular business hours and the same identification is used to enter other facility miles away. SIEM can surely tell that something is really off like the ID was cloned and used unknowingly by the owner of the ID. Such events will be detected in short notice and it can be used to investigate on what happened.

Intrusion Detection

We know the importance of security cameras on company premises and on how they can help the security of the company. Intrusion detection systems work the same way and the only difference is that they keep watch on the network of the company. If security cameras watch the people going in and out inside the company premises, IDS will inspect any network activity, whether it is inbound or outbound. These systems can catch hackers or even disgruntled employees, which will automatically lead to the cut-off of the access to the network system of the company and alert the ms in information security officials.

Basically, there are two types of IDS; the Network-based and host-based. Network-based is responsible for the network, while the host-based examines the desktops of employees. Furthermore, these types of IDS are divided in 2 types the passive system that detects problems and signals and alert; the reactive system that reacts to any suspicious activities and shutting down or logging off the user. Sometimes, IDS can reprogram firewall to deter intrusions.

Sharing the Knowledge

Companies may choose one strategy over the other to deter hackers, but it can still suffer attacks from hackers. Even if the attack has been discovered and investigations take place, it would be too late since the hacker has erased all his presence and is hidden.

However, security officials of a company may have knowledge upon certain knowledge against certain cyber attacks and one could have knowledge against another one. Then it would be much better to pool their knowledge together and share the information they have to different companies as well. This can be called sharing or intelligence sharing and it is to gather and collect as much data and information against such attacks. Together, companies can learn more against hackers and make better defenses for their networks.

Security officials of companies believe the importance of information gathering and intelligence sharing, since hackers are getting more and more persistent and they have the advantage against their victims. In fact, most masters degree information security graduates and security experts believe that sooner or later, companies who haven't experienced being hacked must prepare themselves against potential attacks and join the sharing of information.

It is important to share the knowledge between companies so that they are always prepared and ahead against attackers.

Article Source:
http://www.articleside.com/internet-articles/the-power-of-knowledge-against-hackers.htm - Article Side

Eccuni - About Author:

EC-Council University is a licensed university that offers degrees and master's degrees on Security Science online. The degrees are recognized worldwide and may be used in any employment worldwide as well as the graduate certificates that they offer. With excellence and dedication as the core values, many professionals and degree holders have benefitted from undergoing the programs in this university.

More information about master's degrees in information security available at www.eccuni.us, a masters degree in information security, a ms in information security, a masters degree information security

Article Keywords:
ms in information security, masters degree information security, masters degree in information security, Hackers, cyber attacks, Security officials, security experts, company networks, victims, sensitive data, future attacks, DDoS attacks, spear phishing,

You can find more free articles on Article Side. Sign up today and share your knowledge to the community! It is completely FREE!