Cyber Security for Beginners: Stay Safe!

Presented by Michael Gardner, Technology Consulting

Define CyberSecurity: the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this.

"some people have argued that the threat to CyberSecurity has been somewhat inflated"

Guaranteeing CyberSecurity requires coordinated efforts throughout an information system.

Elements of CyberSecurity include:

- Application security
- Information security
- Network security
- Disaster recovery / business continuity planning
- Operational security
- End-user education

One of the most problematic elements of CyberSecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment. Adam Vincent, CTO-public sector at Layer 7 Technologies (a security services provider to federal agencies including Defense Department organizations), describes the problem:

"The threat is advancing quicker than we can keep up with it. The threat changes faster than our idea of the risk. It's no longer possible to write a large white paper about the risk to a particular system. You would be rewriting the white paper constantly..."

To deal with the current environment, advisory organizations are promoting a more proactive and adaptive approach. The National Institute of Standards and Technology (NIST), for example, recently issued updated guidelines in its risk assessment framework that recommended a shift toward continuous monitoring and real-time assessments.

According to Forbes Magazine, the global CyberSecurity market reached $75 billion in 2015 and is expected to hit $170 billion in 2020.

CyberSecurity awareness can reduce infection risk up to 70%

A new study from Wombat Security and Aberdeen Group, a recognized leader in security awareness and training**,** shows that boosting CyberSecurity awareness and education among employees can reduce enterprise security risks and cost.

According to a pair of organizations behind a newly released study, CyberSecurity awareness and education is important, not just for IT professionals but for all employees of every organization, from management to the general rank-and-file of an organization's workforce.

However, it can be difficult for security officers to effectively communicate this importance to senior management.

Wombat Security Technologies Inc. and the Aberdeen Group hope to change that with new research released this week, which suggests that security awareness and changing employee behavior can reduce the risk of a breach by up to 70%.

While companies tend to spend a lot on security technologies, Wombat and Aberdeen found these controls are not 100% effective and may not account for one of the biggest threats to security: the errant behavior of end users.

Investing in awareness and training to teach employees how to effectively deal with common threats from social media or phishing can quantifiably reduce security-related risk by 45% to 70%, according to the companies, when accounting for both the likelihood and business impacts of security infections due to employee behavior.

Security education may lower malware costs

Research, assembled in Q4 2014, details how education could significantly reduce the costs associated with potential malware infections.

Wombat and Aberdeen sought to estimate the cost of infections resulting from employee behavior, and found that for an organization with $200 million in annual revenue, there is an 80% chance of these infections costing $2.5M per year and a 20% chance of the damages exceeding $8M.

In a statement, Joe Ferrara, president and CEO of Pittsburgh-based Wombat, acknowledged many organizations struggle to justify the cost of security awareness training. The study, he said, is intended to support the risk analysis security officers need to build a compelling business case.

Cyber Security Awareness Tips

Given the complexity of the attacks now perpetrated by malicious hackers, the variety of possible targets and of ways to penetrate systems, there is no single effective prevention measure to implement. A holistic and synergic approach is necessary to secure systems with technology, prevent vulnerabilities caused by users' actions and creatively anticipate possible attacks.

Tip No. 1: Promote security by training employees

Staff training is a good place to start. Everyone must be aware of security issues related to computer threats/attacks/scams. Users are often the weakest link in the cyber security chain and any good cyber security program should start with increasing the knowledge of end users. Cyber Security awareness training can help employees and executives recognize signs of phishing and spear phishing as well as avoid common mistakes like downloading files without proper checking and changing security settings.

Particular care must be given to sensitizing employees not only to the dangers of being the target of phishing, but also to the proper use of social media which are now increasingly been used not

only as a personal communication means but also as an effective work tool. Employees should also be made aware of watering hole techniques: this is another attack that exploits users and is carried out by observing which websites a particular organization or group of people most often visits and infecting those with malware to affect the intended targets.

Promoting security education has to be a priority! The best defense against cyber security threats is knowledge, and that comes with training. Joe Ferrara, President and CEO of Wombat Security Technologies, in fact, believe that organizations "can reduce their risk of security infections between 45% and 70% by implementing effective security awareness training programs that include assessments, education, reinforcement, and measurement."

Tip No. 2: Exploit the latest technological innovations

Awareness is also keeping informed on latest technology developments. Investing in technology is imperative; one must embrace its capability to combat and prevent cybercrime, in addition to help secure computers and protect privacy. To defend IT systems, while constructing substantial defenses to meet current and future cyber threats, it is important to make the most of the **6 D's of Cyber Security** — Deter, Detect, Defend, Deflect, Document, and Delay — as they may help drastically to reduce an organization's risk.

It is also important to keep up-to-date with current releases and make sure to update often as software companies continuously research and implement fixes to common security flaws in their products. Closing any backdoors before they are exploited is a basic safety measure for any environment.

Tip No. 3: Develop a cyber-defense strategy

Take a holistic approach to the security strategy for network-based detection; it helps to detect threats and block exploit attempts. An integrated hardware and software solution, such as Firewalls, an IDS, and Encryption, to name a few, that can be both hardware- or software-based, is essential to defend against and remove cyber threats. A holistic approach helps being constantly aware of any changes in the network and makes it easy to spot disturbances and variations in normal patterns of behavior.

Tip No. 4: Prepare, Implement and Clearly Communicate a Strict Security Policy

Today's IT environments are not just made of servers and end user workstations, as they also comprise mobile devices, BYOD, remote workstations and cloud storage. Protecting this type of configuration is no longer possible by simply segregating the network and protecting it from the outside cyberspace; much of the information is stored and processed outside of the confined perimeters of a company office and through a variety of different operating systems, hardware and software.

If employees are not using the same devices, software, and are not even co-located, they have at least to follow the same guidance. It is important that rules are well defined and the perimeters within which each user can move are clearly established.

Rules for strong passwords, for e-mailing or downloading files, for using peripherals and connection methods (wireless, Bluetooth, hotspots…) need to be established and enforced to prevent confusion and chaos in managing the entire cyber infrastructure.

Tip No. 5: Employ intelligence tools and engage in proactive cyber-security

Network information/intelligence gathering can be applied in the information security world. Awareness includes being also able to understand signs that something is about to happen even when there are no clear indications of malfeasance. Commence by analyzing behaviors and analyze normal patterns in your system; try to anticipate what indicators you could expect to see in case of stealth attacks.

As Orla Cox, a long-standing member of Symantec Security Response, said, in a blog post, "Corporations need to get ahead of the attacker and embrace Proactive CyberSecurity." She explains, "Proactive CyberSecurity puts you firmly in control of your network security. Spence Witten, Lunarline's Director of Federal Sales, wrote in a blog, "A proactive cyber security approach is a necessity to stay protected against aggressive cyber criminals."

When you consider proactive cyber security, consider the following points:

- Identifying security control gaps (raised through self-assessment)
- Pinpointing vulnerabilities in the IT environment
- Examining level of preparedness against cyber-attacks
- Formulating threat detection and incident response methods
- Reviewing cyber risk management policies
- Determining effective cyber security practices
- Establishing specific guidance
- Incorporating appropriate cyber security controls

As there are many paths for exposing data and applications within the corporate cyber infrastructure, it is vital to discover where the organization is most vulnerable to risks. Aside from searching for cyber security vulnerabilities, when you anticipate potential problems and potential indicators that can lead to the spotting of intrusions, it is quite easy to deploy the necessary countermeasures and train employees to recognize and report signs of suspicious activity.

Conclusion

When you venture into cyberspace, you could indeed be vulnerable to hackers, phishers, and cybercriminals who are upping their game in mobile scams and attacks. By implementing CyberSecurity measures, companies will be able to protect their users and assets from the attacks of hackers looking for ways to steal sensitive information or just wreak havoc on systems.

Any technical defense measure, however, would be useless without cyber-awareness. By providing end users with knowledge and giving them the tools to prevent cybercrime and attacks, businesses will be able to sustain vigilance efforts regarding cyber readiness and resilience.

Sources: eForensics Magazine & Wombat Security and Aberdeen Group