CONNSTEP
a CBIA affiliate

Cybersecurity Starts with Your Employees

October 04, 2018

By Pat Toth

We're all familiar with Smokey the Bear and the "Only You Can Prevent Wildfires" slogan. In 2015, Smokey got an update and the new "Receive a Bear Hug" ads ran nationwide. In the ad, Smokey runs out of the woods and gives a big bear hug to a camper for properly checking camp fire embers. The new, more huggable version of Smokey rewards campers for making responsible decisions rather than scolding them to prevent wild fires. Fear and anxiety are not always the best motivators, and many people respond better to positive motivation through awareness activities.

October is National Cybersecurity Awareness Month. In 2003, it was created to ensure that Americans have the resources they need to stay safe and secure online. October is a great time for small and medium-sized manufacturers (SMMs) to educate employees about the vital role they play in protecting the business against cyber-attacks while providing a positive cybersecurity message. A good way to do this is to create a Cybersecurity Incident Response Plan and communicate the critical role that each employee plays in preventing and responding to an incident.

A cybersecurity incident is defined as “an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.” Examples include:

- Attempts from unauthorized sources to access systems or data
- Unplanned disruption to a service or denial of a service
- Unauthorized processing or storage of data
- Unauthorized changes to system hardware, firmware, or software

An Incident Response Plan is a set of written instructions or procedures for your company to detect, respond to, and limit the consequences of a malicious cyber-attack. The plan includes preparation, detection and analysis, containment, and eradication and recovery. An Incident Response Plan should be put in place before an attack occurs to limit the damage that is done. It will also help reduce the time and cost of recovering from an attack.

1. Preparation

A good rule of thumb when it comes to cybersecurity is to plan for the worst. The number of cyber-attacks is on the rise and SMMs are prime targets of cybercriminals given that many such companies do not have adequate preventative measures in place.

Your ability to respond quickly (and appropriately) can help mitigate damage. You will want to identify key people who need to be notified and each person should understand and be trained on his or her roles and responsibilities when an incident occurs.

You will also want to create and maintain a list of assets – the people, processes, and technology that help your company maintain its daily operations.

2. Detection and Analysis

It’s important to install and regularly update anti-virus, anti-spyware, and other anti-malware programs because computers are regularly threatened by new viruses and cybercriminal tactics.

Also, you should maintain and monitor logs, which automatically document operations of a computer and its user, such as accessing websites and creating and modifying files. Logs provide a detailed record of activities that can be used to reconstruct the sequence of a network or system that has been compromised. The timeline, source of contamination, and contaminated devices or servers can be traced and analyzed using these log files. Not only will this help you detect an incident, it will help you identify any potential vulnerabilities and remedy them.

3. Containment

Using the information that you have gathered, you will want to contain and combat the incident. Someone will need the authority to make quick decisions on the necessary steps to contain the incident. This will be easier to manage if you have already identified key people who should be notified that an incident has occurred. Be sure to regularly update contact information and make sure it's easily accessible to necessary staff. Normal operating activities may need to be temporarily paused until the incident has been resolved.

4. Eradication and Recovery

Now that you have contained the incident, you will want to remove the cause and restore systems to their normal functionality. This could be as simple as removing a virus from a server or device, or it could mean restoring data from a back-up. Systems may need to be brought back online in stages. For this reason, it's important to schedule incremental backups as an incident can occur at any time.

You should also consider lessons learned after an incident and make any improvements to processes, procedures, or technologies.

Incident Response Plan in Action

Recently, an SMM experienced a spear phishing attack. Spear phishing is an attack that seeks to steal sensitive company information, like financial data, or access a company's network through an email that seems innocuous.

An employee at the manufacturer received an email from a supplier that contained malware disguised in a PDF file. The email appeared legitimate and was in response to actual emails the company employee had sent the day before. The attackers used social engineering to tailor the email to the employee in the accounting department who had responsibility for paying invoices. When the company employee opened the PDF file, malicious code was introduced into the company network.

Thankfully, the manufacturer had just worked with their local MEP Center to improve their cybersecurity. The company had developed and implemented an Incident Response Plan. They had trained their employees to recognize phishing attacks and what to do if a cybersecurity incident occurred. The company detected the threat from the malicious code and with the new Incident Response Plan in place, was able to respond immediately. Employees knew what they were supposed to do, pulled out the plan and sprang into action. Since only one computer had been infected, the IT Team removed it from the network and the malicious code was stopped.

The Critical Role Employees Play

Your employees are your first line of defense against cyber-attacks. Having an Incident Response Plan in place and training your employees on how to respond provides a positive cybersecurity approach. Many SMMs are still unaware of and unconcerned about their cyber risks.

Thirty-four percent of all documented attacks targeted manufacturers, and SMMs are especially vulnerable. Cyber criminals often view these companies as easy entryways into the supply chain. Over 90 percent of malware is delivered via email and all it takes is one wrong click to compromise your business. Cyber criminals know if they hack into your system they can access your network and gather sensitive information about your customers.

While you may not think criminals are after your company information, you can be sure they are interested in the sensitive information you have about your customers and their customers. While statistics and awareness events that highlight threats to your systems may build fear among SMMs, they don't always result in action. I believe we need to move toward a more positive cybersecurity message for your employees. Just like Smokey, let's move away from the scary bear and toward the big bear hug.

To learn more on this subject, connect with CONNSTEP, your local MEP National Network Center, 800.266.6672 or info@connstep.org.

ABOUT THE AUTHOR

Pat Toth
Pat is a Computer Scientist at NIST MEP and serves as the Cybersecurity Program Manager. Pat has over 30 years of experience in Cybersecurity and worked on various NIST Cybersecurity guidance documents.