Cyber Action Plan – Focus on the basics first, it is a *Process* not a *Product*

Cyber-Security is now a regular topic in the news and in our meetings and conferences. Even in the Engineering & Operations or the Finance & Accounting meetings, Cyber-something is still a regular topic of discussion. This week, at the TVPPA meeting in Chattanooga, there was a session about Cyber Security and CIP compliance. There are benefits for smaller organizations to follow the NIST and CIP standards, which puts good security in place, but it is a big undertaking and most of the audience reading this article are not required to be CIP compliant. To confuse matters even more, technology vendors are investing millions of dollars into marketing and advertising to convince you to buy their widget that will handle all of your security needs. But guess what? Even security products have vulnerabilities that hackers take advantage of. Products are required to add layers of security, but it is the *process* around these that keep you secure. They must be updated and maintained. If you do not check on their performance, you have no idea of whether they are still functioning properly.

Basic Blocking and Tackling

Studies show that over 90% of breaches happen because something simple was missed. So, before you run out and invest in some of the newer security solutions, it is important to make sure the basics are covered by solid products and the processes supporting them. Making sure these basics are covered reduces much of your risk:

1. **Security patching for *all* hardware/software.** This is where most of your vulnerabilities lie. Windows computers are just the start. All of their applications (office, adobe, browsers, etc.) need to be up to date. Switches, routers, firewalls, and SCADA systems need updates too. You need to independently check to make sure that this is happening – a patching report from a Microsoft Console typically only tells you about Microsoft products and does not cover all of the others.
2. **Endpoint protections - Antivirus/Malware solutions.** Make sure these are working. Pull a report and do an inventory of systems. Not the most glamorous thing in the world, but simple and effective.
3. **Review all accounts and passwords regularly.** I don't have to hack if I can just log in. You should also limit the number of privileged accounts and not use shared accounts.
4. **Constant inventory devices on your network.** If you don't know what is on the network, how do you know whether it is allowed or protected?
5. **Encrypt all portable devices**. Smartphones, tablets, laptops – anything that may have sensitive data on it.
6. **Provide security training for users and IT staff**. Your users are the target and need to make good decisions. As for IT, yes they are smart, but typical IT training does not always include security *processes* (there is that word again…). And what IT folks hear most is faster, cheaper, and more reliable. Oh, and by the way, can you make it secure too?
7. **Review firewall, remote access/VPN, and wireless solutions regularly**. Another way to get in…

david@securit360.com

8. **Implement a proactive monitoring/logging/alerting solution.** There are millions of log events produced in your network each day. They need to be collected and analyzed. There are many options available that will tell you when something bad is happening and you can react.
9. **Check your email gateway (Spam filter)**. Make sure it has virus and malware capability. Email is one of the most common attack vectors. Most of you should have this, but you need to double-check that this is in place and functioning.
10. **Additional basic perimeter protections.** Make sure that your firewall has IDS/IPS capabilities – not all do. Internet content filtering software also keeps users from going to dangerous websites. Some firewalls include both of these features, but they may require additional licensing or products *AND* you need to make sure they are updated and functioning properly. You need to ask if you are not sure.

What do leaders need to do?

Leaders do not need to become experts or spend millions on cyber security to protect their organizations and customers. BUT, you do need to know enough to oversee and carry on the conversation.

Where to start:

1. **Educate yourself** – The buck stops with you. When something happens, answers will be demanded. Get in the conversation and ask questions of those that you trust to handle cyber security for you.
2. **Measure your status** - Measure against accepted standards. This is more than asking your IT guys to check the firewall. Standards are multi-dimensional, covering all areas. CIP, NIST, or ISO 27000 are good standards to compare yourself to – AFTER you have covered the basics.
3. **Develop a plan to close holes –** There is no such thing as 100% security which always leaves room for improvement. The gaps should be ranked by risk and prioritized. Regular meetings and documented progress against risks will show the level of commitment to security.
4. **Develop a security program –** The rapid pace of change does not allow you to set-it-and-forget-it. Policies need to be written and responsibilities assigned. The program will require monitoring and regular reporting.

A Note to the CFO: You may want to remind your finance committee that breaches can cause serious reputational damage and be very expensive. Cyber Liability insurance is not enough. In today's world, the expectation is that there are measureable efforts (and funds) devoted to keeping information safe.

david@securit360.com