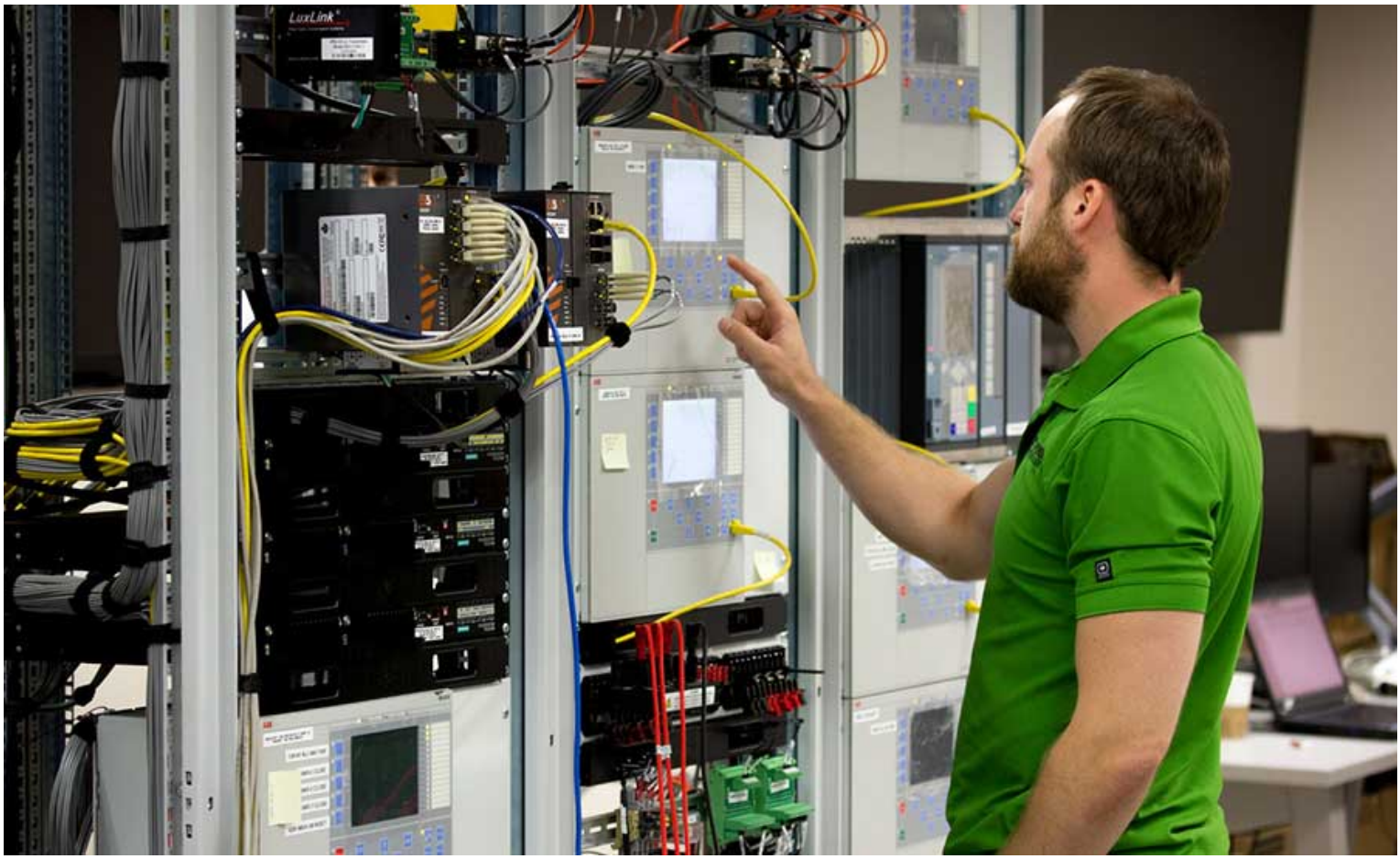
ENR
Engineering News-Record

4 Priority Steps That Will Help You Successfully Prepare For a Cybersecurity Attack



When it comes to industrial controls for water, power and transportation, cybersecurity can be more critical than most business functions. An engineered, strategic approach can help stop an attack.

Photo Credit: Jared Haskett

November 1, 2017

Jeff Pack

It starts with something that just doesn't seem right. Something on your information or operational technology system is not behaving as it should, and you're trying to troubleshoot the issue.

Your phone suddenly starts ringing. You answer. The person on the other end, clearly someone from outside your organization, says that your system is compromised and begins threatening to either damage similar systems or remove control from you and your operators. Now what?

This scenario is unfortunately happening all too frequently to all types of businesses and systems. We've all heard about the big data breaches including Target, Home Depot and the U.S. Office of Personnel Management. There's also the threat of ransomware and losing access to your valuable information. For the industrial control system world, Ukraine's power outages in 2015 and 2016 demonstrate that critical infrastructure is actively under attack.

All utility owners and operators need to be able to defend their systems and networks against cybersecurity threats. Here are some important steps to take to protect your systems:

Priority #1: Know what you have to defend

The first step in defending is knowing what you have. An accurate asset inventory is critical in helping design the appropriate detection, response and recovery processes to use.

As an example, let's look at an electrical power plant. There are many different types of control equipment and devices in any type of power plant, regardless of the energy source. Some controls measure and control environmental factors, such as temperature, pressure and humidity. Other controls measure and protect equipment from electrical damage, such as over or under voltage and current. Still others detect status of power delivery elements such as lines, transformers and breakers.

Some controls are deemed more important than others based on what equipment they are monitoring, so certain controls are considered higher risk and require more protection from cybersecurity threats. An accurate asset list, prioritized by risk, gives you the basis to design effective detection, response and recovery processes.

Priority #2: Know how to detect bad things

Now that you know what you are defending and which assets may require some more attention, you have to design and implement an intrusion detection system. With the wide variety of cybersecurity threats, this isn't a one-box or one-vendor solution. Your ability to detect multiple threats against a diverse set of equipment and software depends on having multiple detection locations and technologies.

For example, continuing our power plant theme, the operational technology network is pretty static and should not have somewhat random network traffic. Therefore, the network firewall rule set should be highly deterministic and any outbound traffic should be analyzed for suspicious traffic. The network security monitoring system should flag any traffic that doesn't conform to well-known operational technology protocols and data flow for collection.

A temperature sensor should not be initiating a connection to the distributed control system (DCS). The DCS servers and human machine interface (HMI) workstations should also be static and flag any new or modified files that are not involved in data collection and processing using file integrity or whitelisting programs.

Design your intrusion detection system with your high-risk assets and their associated data flows in mind.

Priority #3: Develop and test an incident response plan

Most organizations have an incident response plan sitting on a shelf somewhere so they can demonstrate that they are ready for a cybersecurity incident. Fewer organizations test their plan annually with a minimum of a tabletop exercise so the people with roles and responsibilities remember that they are part of the plan. Even fewer have quarterly or monthly exercises of the plan, with a mix of tabletop exercises and live tests during a scheduled outage.

The only way to have any level of confidence that your organization will respond well during a cybersecurity incident is to test, measure and revise the plan on a frequent basis. Be one of the few that takes this plan to heart and has the training, skills and resources to respond effectively when things start breaking bad.

Priority #4: Recovery—keeping the lights on

The true measure of defending your assets is how quickly can you recover and bring your critical assets back online. Attackers have many different motives, but ultimately the prize is to disrupt your operation and keep your system down.

For the power plant we've used as an example, it's all about availability. Electric utilities are all focused on availability and keeping the lights on. They have to deal with a constantly fluctuating supply and demand of power, severe weather, sabotage and cybersecurity threats.

Electric utilities have an extensive emergency response plan including mutual support with neighboring utilities to help them recover quickly when bad things happen. Response to a cybersecurity incident should use the same types of processes to recover, including manual control of substations to restore power. Leverage the experience in emergency response and recovery to improve the cybersecurity recovery plan.

Summary

The notion that a single device such as a network firewall will protect your system from attack is dead. Defending your system requires active participation from multiple areas of responsibility in your organization.

Start with an accurate list of risk prioritized assets so you know what has to be defended. Design an intrusion detection system that addresses all areas of exposure, including network, operating system and application interfaces. Test and improve your incident response plan so you'll be ready for the eventual attack, and learn from existing recovery processes to minimize downtime.

Jeff Pack specializes in cybersecurity services for POWER Engineers, Inc. He has over 28 years of experience in electric utilities, energy research & development and information security solutions. He is an experienced leader and subject matter expert in the cybersecurity field, including program development, consulting and operations. He has also provided executive and team leadership for numerous projects related to cybersecurity and operations. He has bachelor's degrees in engineering and computer science from Montana Tech and an MBA from Boise State University.

Recent Articles By Jeff Pack

Make Cybersecurity One of Your Engineering and Design Goals