SMART manufacturing

A publication of sme

August 2022

sme.org

2022 SME AM Industry Achievement Award Winner Slade Gardner:

“Put AM into factories—now.”

IMTS2022

POWERED BY AMT

- Cybersecurity Update
- Robots as a Service
- SMX Experienced

ALSO INSIDE:

VOICES AMplified

The Mutating Cyber Threat

Cybersecurity practices must continue to adapt as attacks and attackers evolve

Karen Haywood Queen
Contributing Editor

As cybercriminals and their attacks evolve—with ransomware currently the greatest threat—cybersecurity best practices must evolve to keep up. Some of the most critical best practices to thwart cybercriminal attacks include an accurate inventory of accounts, software, and patches. Beyond that, manufacturers need malware and virus protection/safe listing, patch management, a backup and recovery processes, and prepared incident response.

Some best practices to ward off threats can be implemented immediately, while others require funding for updated software. To address the ongoing threats head on, it is necessary to change the manufacturing culture.

"In the last three years, the greatest threat and therefore the greatest risk has been ransomware," said John Cusimano, a Deloitte managing director specializing in industrial cybersecurity.

"Most manufacturers don't even know what they have so they have no clue to their exposure—let alone have the tools to remediate an event or better yet, to proactively protect and reduce exposure," added Rick Kaun, vice president for solutions at

Verve Industrial. "It's about awareness and scope, which they seem to be lacking."

In some cases, Cusimano and Kaun agreed, manufacturers are just starting to look for vulnerabilities in systems that are 10, 20, 30, and even 40 years old.

An important first step is to determine what vulnerabilities to prioritize. "Which do you address first? Typically, only 20 percent of the vulnerabilities represent high risk," Cusimano said. "In operations, the key is finding that 20 percent."

Getting leadership buy in on investments also is important, Kaun added. "I had an OT program manager tell me the other day that they had never spent a dime on cybersecurity—now they need to show management they need X more dollars and Y more people and it's an eye opener."

Low-Hanging Fruit

For companies looking at near-term solutions, best practice starting points include:

Close unused accounts, add missing patches, and eliminate out-of-date or unnecessary software. "These can be cleaned up immediately and reduce risk by up to 50 percent," Kaun said. "Don't think a passive or cursory approach to inventory will be enough. You need an accurate inventory to get to these details."

Anti-virus/anti-malware/safe listing software. "A lot of things are easy to fix if you have the funding," Cusimano said. "This is software you purchase that is effective at preventing malware from running."

Risk management software. "This is a key factor in making and maintaining progress," Kaun said. "We have seen our clients reduce time and effort by over 70 percent while driving 100 percent visibility and awareness into specific risk by deploying an end point risk-management software."

Training. Hacks and ransomware often begin with a click on an email containing a virus or other malware. "Awareness training is relatively easy to do," Cusimano noted. "It's a matter of resources, spending the money for the training, and allocating people's time for the training."

Backup and recovery. Assume the system will be breached, Cusimano advised, and plan to easily recover from in-house backup systems rather than paying the demanded ransom.

Incident response. Train people at every level on actions to identify and respond to incidents. "Responding effectively to incidents doesn't just happen; you need to conduct drills and exercises," Cusimano said.

Fixes that Require More Effort

Once a manufacturer accomplishes those early practices, it's time to move on to the more difficult, but still important best practices, which include:

Inventory and tracking of operations assets. "Operations technology is besieged by risk but can't always patch like IT," Kaun said. "If IT pushes a patch to an automation station, the patch might not be compati-

ble with the automation OT is using. Instead, they have to have many compensating controls and the ability to track them." As noted above, managing risk is key, especially on the operations side, Cusimano added. "In some cases, the risk of patching could outweigh the risk of not patching."

Inventory and tracking of software. It is not uncommon for a manufacturer to purchase software without fully understanding its embedded capabilities, Cusimano said. Without this knowledge, the manufacturer may not even know they need to respond to an alert.

Ongoing patch management. Once missing patches are identified and fixed, manufacturers must make sure all systems that can be patched continue to be patched. This is challenging, but doable, Cusimano asserted.

John Cusimano, managing director and industrial cybersecurity specialist at Deloitte.

"USUALLY THE PROBLEMS ARE NOT BECAUSE [IT AND OT] PEOPLE ARE NOT WILLING TO WORK TOGETHER. IT'S A MATTER OF NOT SPEAKING THE SAME LANGUAGE, NOT UNDERSTANDING EACH OTHER'S POSITIONS. WE ENCOURAGE PEOPLE TO MINGLE. WE ENCOURAGE THOSE CONVERSATIONS."

Network segmentation. "The more you can segment your network, the more you've reduced the likelihood of ransomware spreading," Cusimano said, adding that while it is an effective prevention tool, it takes time to implement.

IT/OT cooperation. "Many debate the value of this approach and even the label," Kaun said. "But IT knowledge of specific risk and OT awareness and ownership of what can or can not be done is the only way to reduce risk." Some best practices are as simple as seating operations technology and IT people side by side during training and incident response simulation exercises, Cusimano said. "Usually the problems are not because people are not willing to work together," he said. "It's a matter of not speaking the same language, not understanding each other's positions. We encourage people to mingle. We encourage those conversations."

Remote access control. "Remote access can be a big cost savings to manufacturers, particularly during the pandemic," Cusimano said. This allows people to enter the system remotely to investigate potential problems, access data, and monitor operations without expanding the attack surface. This one is technically easy but, because of the human element, not easy to fix, Cusimano cautioned.

"In recent years, industry has confidently expanded the use of remote access and given even more people remote access," he continued. The easy fix would be to remove all remote access or cut it back to a handful of people, he said. However it is an unpopular solution that limits the advantages listed above. Alternatively, manufacturers can implement privileged, granular, layers of access control based on the problem, the user, and where the user is working from.

Real Victory Comes with Change and Culture Shifts

Although each best practice is important, having a programmatic approach is essential for success, Kaun said. "Too many organizations look at security as a list of individual tasks such as perimeter protection and patching, but in reality they all have to work together."

As best practices mature and become part of corporate culture, and as people become educated and equipped to apply those best practices, true change and improved security begins to evolve.

"A common adage in security is 'people, processes, and technology,' Cusimano noted. "Two of those involve people because people have to adhere to the processes."

The human element is the ultimate toolset, including awareness, collaboration, support, and maintenance. "A proper security program is properly educated and equipped people applying best practice policy and procedures, aided by technology," Kaun said. "While the right technology will accelerate the effort, if you do not have the global view, the appropriate people, and contextual data to act upon, you will struggle."

Establishing that culture is critical but won't happen overnight, Cusimano said. He recalled the transition to a safety-first culture in many manufacturing plants. "You can't go into a manufacturing facility now without seeing signage and reminders about safety: 'Wear a hard hat, wear steel-toed shoes, grab the handrails,'" he noted. "It took decades for manufacturers to embrace a zero-accident culture. We can do the same with security. It starts with training. People have to understand why it's so important and how it applies to them on a day-to-day basis."

That training should be role-based, not one-size-fits-all, Cusimano said, with different training for front-line operators, engineers, supervisors, and other managers. For example, engineering people need more technical training on controls and how they're implemented, while managers and supervisors need general training on security terminology concepts, technical controls, and how they work.

"The front-line operators can be your first line of defense," he said. "They're going to notice when something is not right. Something that is out of the ordinary might be an early indicator of some kind of cyber compromise. Training operators to identify and properly report those things is critical."

Rick Kaun, vice president for solutions at Verve Industrial

In one incident, a water plant operator noticed the setpoint for a certain chemical had been increased dramatically, which could have allowed dangerous levels of that chemical into the water, Cusimano said. The operator noticed the discrepancy, restored the correct set point, and reported the incident, he said.

"This is where our clients are making the most impact," Kaun said. "They build the visibility, truly understand the end points, and more importantly, their context." He explained that best practices drive details about assets, about risk, about reviewing access and status. Then, the deployment of best practices around remote access, network segmentation, end point, and management are how clients start to rapidly mature their OT cyber defense.

In conclusion, Kaun advised: "While the right technology will accelerate the effort, if you do not have the global view, the appropriate people, and contextual data to act upon, you will struggle."