

<http://www.darkreading.com/vulnerabilities---threats/look-but-dont-touch-one-key-to-better-ics-security--/d/d-id/1328987?>

Look, But Don't Touch: One Key to Better ICS Security

6/26/2017

09:00 AM



[Sara Peters](#)

Better visibility is essential to improving the cybersecurity of industrial control systems and critical infrastructure, but the OT-IT cultural divide must be united.

How do we fix industrial control systems cybersecurity?

Experts say better visibility is essential to improving ICS/SCADA security. But infosec teams will never gain that visibility until they stop trying to observe ICS environments through the eyes of IT professionals.

There are fundamental differences in IT and OT (operational technology) gear, processes, and people, say experts.

"Overall, IT has no idea what goes into operating an OT environment," says Paul Brager, senior staff product security leader, cybersecurity and risk, for GE Oil and Gas.

"The success of the Internet has made computer people kind of smug," says Chris Blask, chair of the ICS-ISAC and global director of industrial control systems for Unisys. Industrial workers, however, he says, "know how society works," like what keeps raw sewage out of your drinking water supply.

So while cybersecurity professionals worry about nation-states knocking out the power grid with ICS malware attacks, OT engineers know that their generating stations and production lines can be disrupted by much

more than hackers. They're so aware of this that they adhere to extensive process safety management controls, hazard analysis, change management, emergency response, incident investigation rules, and more, to deal with such threats early and swiftly.

The introduction of anything new to the operational environment - a new pump, a software patch, an upgrade, a new security tool - is approached with caution, because any disruption in availability or integrity could have irreversible, expensive, even dangerous physical impacts.

It isn't just the worst-case scenarios of sustained blackouts, broken dams, nuclear meltdowns, and poisoned public water systems, either: it's economic impacts as well. If part of a chemical plant's system malfunctions or goes offline during a production run even very briefly because an insufficiently tested software patch misbehaves once it's released into the live environment, the chemicals could be corrupted. "That might be \$100,000 of product that they dump," Brager says.

"No CEO is going to sign something that says 'Okay we're going to stop extracting oil from the ground for a week,'" to fix something that doesn't appear to be broken, like an unsupported operating system, explains Galina Antova, co-founder of OT security firm Claroty and former global head of industrial security services for Siemens. Convincing them that cybersecurity is a threat at all, much less one worth spending money on, is a challenge, she says.

Enterprise IT environments will withstand more iteration and downtime than OT environments. If the OT environment appears to be stable, operational and efficient, then why make a change that might make it unstable?

Many of the physical and cyber-physical systems in use today have been in use "literally for generations," explains Eddie Habibi, CEO of PAS.

As these experts say, the attitude is generally If it ain't broke, don't fix it. So infosec professional's challenge therefore is: to convince the OT side of the house that something is broken and then to fix it without breaking it further. And that takes a lighter touch than infosec pros and their tools are used to.

Seeing What No One Else can See

As Blask says, ICS is "the system put in place to provide visibility into physical processes. The one thing that they don't have visibility into is the [ICS] system itself."

"Visibility is a big deal. And we typically don't have a lot of visibility down there," on the cyberphysical systems says Brager. When something goes wrong, "You don't necessarily know if it's a cyber thing or a human thing."

Unfortunately, says Habibi, "These systems are not easily discoverable." As he explains, industrial environments are often a heterogenous conglomerate of highly complex, proprietary systems, communicating on different protocols, requiring specialized expertise to run.

Brager adds, many of these systems are no longer supported and the vendors may no longer exist. Many of them only communicate on one protocol, if they communicate at all.

"It continues to get worse," says Habibi, "because people continue to add automation."

This IT-OT "convergence" adds more sensors, more I/O cards, more endpoints, more protocols, more interconnections, and more complexity to an environment, making the picture even murkier.

"Unless you can visually see [an asset]," says Brager, "it's really hard to interrogate it ... But if you don't know which ones you have, you don't know how vulnerable you are."

Plus, he notes, a significant amount of industrial environments are generally managed by third parties with privileged access. Documentation - who runs what, where - is the last thing done, if it's done at all, says Brager.

However, calling these third-party contractors and managed service providers and asking them for a manual count would be "worse than doing nothing," says Habibi, because of the scale of the challenge.

How to Do it

According to Brager, whenever terms like "sniffing" or "actively interrogating" are suggested by security teams or companies, "the people in those plants get real nervous."

What may seem like a very gentle gesture to an enterprise IT manager, he explains, may be seen as a dangerous intrusion to an operational

engineer. The industrial processes cannot tolerate new latency that might be introduced and if some mechanical system is damaged and cannot be recovered, it will need to be replaced.

"If you say, 'we're going to install an agent,' they'll say 'No you won't install an agent,'" says Brager.

That doesn't change the fact that improved visibility is necessary. Without it, attackers hiding in plain sight may be a greater threat than some OT teams realize -- because attackers may be better at achieving visibility than operators are.

Take the [CrashOverride/Industroyer malware](#), which researchers discovered was responsible for the December 2016 attacks on the Ukrainian power grid. It's designed to map, target, and attack grid operations by exploiting ICS communication protocols. The malware actually employs those protocols just the way they were designed so that it flies under the radar.

ICS security team's goal, therefore, says Antova, is "improving visibility in a passive way. ... This is something I can do that the engineers will allow me to do without impacting their processes." It also provides the most benefit for minimum investment, she says.

Habibi urges the same practice. Passively take stock of all the components in an environment, then check them all for vulnerabilities, present that information to the operator, and allow them to act (or not). "You want to fix those broken windows and broken locks," he says, "Then implement a very tight change management process."

But, Brager cautions, test products carefully, because some vendors that promise "passive monitoring" are less passive than they claim.

As ICS relates to safety processes and change management, it's is an opportunity for OT and IT groups to come together.

"A lot of this comes down to having manners," says Blask. "What you don't do is what security teams often do, is say 'your baby is ugly.' ... And then they complain to their friends why they don't get invited to the meetings anymore."

http://www.darkreading.com/author-bio.asp?author_id=524

Profile of Sara Peters

Senior Editor at Dark Reading

Member Since: 3/12/2014

Author

News & Commentary Posts: 434

Comments: 646

Sara Peters is Senior Editor at Dark Reading and formerly the editor-in-chief of Enterprise Efficiency. Prior that she was senior editor for the Computer Security Institute, writing and speaking about virtualization, identity management, cybersecurity law, and a myriad of other topics. She authored the 2009 CSI Computer Crime and Security Survey and founded the CSI Working Group on Web Security Research Law -- a collaborative project that investigated the dichotomy between laws regulating software vulnerability disclosure and those regulating Web vulnerability disclosure.