Regardless of the headlines, most cyber security events are unintentional

Kristen Poulos 8/8/18 Industrial Cyber Security

Let's face it, we Operations Technology (OT) folks can sometimes get a little bit smug when the news of the latest IT cyber security event hits the airwaves. “We don't store credit card information or social security numbers,” some might be thinking, “so no one would be interested in targeting us.”

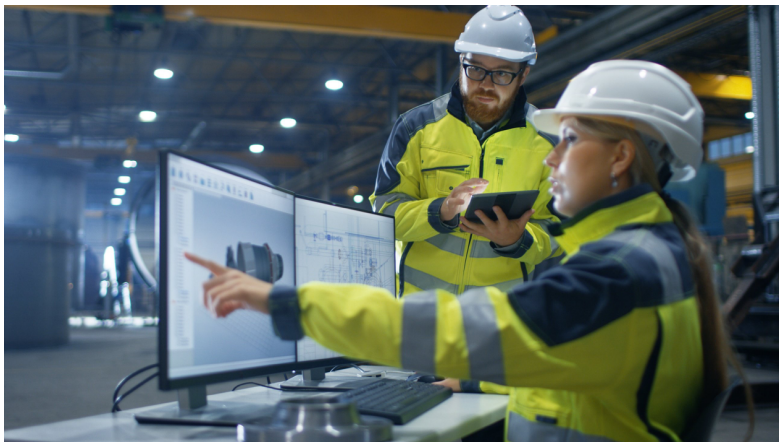
Unfortunately, this can be a false—and dangerous—sense of optimism. In the OT world, spear phishing or even malicious targeted cyber destruction just for its own sake (whether from a disgruntled insider or state-sponsored or other outsider) is becoming an ever-increasing reality.

However, while I hope that the awareness of this fact is improving, that is not the focus of this particular blog post. In fact, I'm here to point out that, while the anonymous hacker working out of a basement in a faraway country is a very real threat, far more menacing statistically is the day-to-day threat posed by Fred, Mary or any of your other friendly, hardworking colleagues right there in the plant.

Related Posts

When it comes to zero-day threats, we’re all just sitting ducks. Or are we?

April 18th, 2018



Remember that, as a practical matter, a cyber security event is anything that negatively impacts the ability to view, monitor or control an industrial process, regardless of source or intention. And, in fact, some 80% of cyber security incidents are unintentional as opposed to targeted, such as a random malware attack inadvertently set in motion by an unwitting colleague, a non-malicious accidental error, or a bug in software or hardware device dutifully purchased. Consider these scenarios:

- An operator finds a new flash drive in the parking lot, not realizing that it's one of the most common vehicles a virus developer uses to send his malicious code randomly out into the world, and it ends up infecting your network
- An operator accidentally miskeys and programs a PLC to deliver 10x the amount of fuel needed to sustain a process, shutting down the line
- A controller on break uses a plant PC that regulates an operational process to check personal email, falls victim to a broadcast phishing campaign and inadvertently downloads a worm or other malware into the OT network
- Your newly purchased software package or device contains exploitable security flaws or vulnerabilities
- An operator connects his internet-enabled laptop to an isolated industrial device to check the configuration, creating an exploitable link to the outside world

Any of these scenarios can have devastating consequences on an industrial operation. And, with these types of threats still making up some 80% of the cyber security event landscape, you are significantly more likely

How Plant Operators Can Overcome the Language Barrier to Securing OT Environments

March 7th, 2018

Evaluating Deep Packet Inspection Technology: Six Essential Elements

October 18th, 2017

Topics

ICS Security

SCADA Security

Industrial Cyber Security

Industrial Security

PLC Security

Industrial Networking

IoT Security

Industrial Firewall

Industrial Network Security

Stuxnet

View More

security event landscape, you are significantly more likely to experience one of these unintentional scenarios than a targeted hack. In fact, depending on the size of your facility, number of people and devices and level of protection in place, it could be highly likely that you experience one of these issues in the near future – if you haven't already.

Of course, when something is costing you tens or hundreds of thousands of dollars or more every hour, the immediate priority is to fix it as quickly as possible, regardless of who might be responsible. Just ask the oil pipeline that had to shut down for six hours when someone accidently uploaded software to the plant network instead of the test network. Or the automotive manufacturer that had to shut down 13 processing plants while they mitigated a "simple" random worm that was unwittingly unleashed into their network. Estimated cost: $14 million.

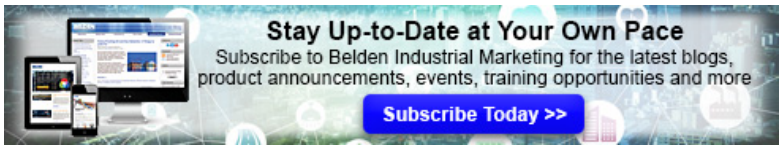
Or, better yet, work to ensure that your cyber security defense takes these scenarios into account so that they are less likely to happen to you at all. Indeed, a smart cyber security strategy anticipates all of these and more.

Protect your "castle"

How? The answer is to create a "defense in depth" strategy. Simply put, it means that you put into place multiple layers of protection to thwart the malicious as well as accidental threats that are all around us. I liken it to defending a castle—successful fortresses didn't simply rely upon one single form of protection. Castle guardians knew that if that was breached, all was lost. Instead, they scouted the best strategic location and built on a high hill. Then they surrounded the structure with a moat. They built up high, thick walls. They limited entrances and built a retractable drawbridge. Armed forces kept watch from high perches at all times, and archers and other fighters were always at the ready.

While I don't suggest that you post archers at your facility, the multiple layer approach is apt. Networks, like castles, should be strategically built and maintained, with multiple zones and segments so that the entire plant doesn't consist of one big network that can be fully exploited. Each should be individually protected and firewalled to regulate what is coming in and out of each zone. Data and

information should be collected from devices and the traffic and analyzed. Rules and parameters should be established and monitored. Robust reporting dashboards should be generated and carefully and proactively observed. Cyber security metrics should be continually assessed and measured against published standards and best practices for continual improvement and updating. And more.



As with castles, network threats are diverse, multi-faceted and ever-changing. And so, defenses have to be so also, with a strong security posture featuring a diverse continuum of protections and regular hygiene updates that are never static, but work to continually strengthen the network against any kind of attack.

For more on the risks that face OT networks in the emerging connected world, read our free white paper —"Industrial Cyber Security—Essential to Assure Availability, Safety and Resilience." It's daunting information, but it's a reality that we all have to face head on. Fortunately, no one has to go it alone. Many organizations stand ready to help. Belden and Tripwire, for example, offer significant in-house expertise as well as a robust portfolio of cyber security devices such as Tofino Xenon security appliances, Hirschmann EAGLE firewalls, GarrettCom secure routers and Tripwire Data Collector. Give us a call—we can help you keep your castle safe from marauders both intentional and unintentional.

Download White Paper

Related Blogs

- The Human Attack Surface: The Weakest Link in Your ICS Security
- IT/OT Convergence Means Better Resources for Both
- 70 Percent of Energy Security Pros Fear Digital At-

tacks Could Produce a “Catastrophic Failure”

- How Plant Operators Can Overcome the Language Barrier to Securing OT Environments

---

PREVIOUS POST
IT/OT Convergence Means Greater Resources for Both

Kristen Poulos

Kristen is the Vice President of Marketing for the Enterprise Platform and has previously held roles within the product line management team and Mohawk brand. She started with Belden as a summer intern in 2010 and joined full time in 2011. In her spare time, she enjoys outdoor activities with family and two Australian Shepherds.

CONNECT WITH ME

Comments

First Name*

Last Name

Email*

Website

Comment*

Yes, I would like to receive marketing information from Belden Inc. and its affiliates, subsidiary companies and brands indicated below. I therefore provide my consent to the use of the personal information submitted here for the purpose of providing me marketing information related to Belden and its subsidiaries' products, services and marketing events. I understand that I may withdraw my consent at any time.
Belden Inc. affiliates, subsidiary companies and brands include: Alpha Wire; Belden Deutschland GmbH; Coast Wire & Tech; Hirschmann Automation and Control GmbH; GarrettCom; Grass Valley; Lumberg Automation, Poliron; PPC Broadband; ProSoft Technology; S-A-M (Snell Advanced Media); Softel Ltd.; Thinklogical; Tofino Security; Tripwire; and West Penn Wire.

Additional information regarding Belden's data privacy policies, including how to withdraw consent, is available at Belden.com/about/privacy.

By clicking subscribe below, you consent to allow www.belden.com to store and process the personal information submitted above to provide you the content requested.

protected by reCAPTCHA
Privacy - Terms

Submit Comment

Overall, how would you rate your experience on Belden.com?

0 1 2 3 4 5 6 7 8 9 10

Poor Excellent

© Copyright 2018 Belden Inc.