WHAT IF YOU CAN'T PATCH?

By Scott Coleman, Director of Product Management – Owl Cyber Defense Solutions

ICS networks and IT networks are becoming increasingly entangled (or more politely, "converging"). Workstations and servers on the ICS networks using standard IT operating systems, such as Windows, is becoming more and more common. Unfortunately, and as many ICS operators are all too aware, these changes are making ICS networks more vulnerable than ever to hacking, especially malware and ransomware attacks.

The latest rash of NotPetya and WannaCry ransomware proved cyber attacks are certainly not slowing down, but simply patching systems and device applications can go a long way in preventing them. These two attacks relied on the EternalBlue NSA exploit[1] – a security flaw within multiple versions of the Windows operating system – to infiltrate and lock down vital systems, charging a ransom to get them unlocked. However, the patch to prevent these attacks[2] was already available months before they took place. So why didn't many major organizations patch their vulnerable systems?

DOWNTIME = $$$

The first complication is that large industrial, infrastructure, and commercial networks are usually

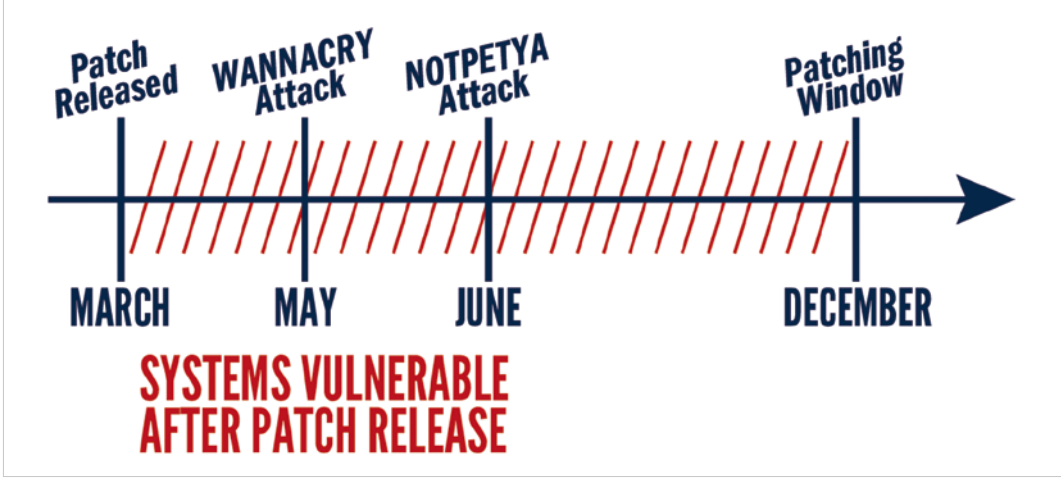


Figure 1: Delay from patch release to patching window.

tuned to operate at peak performance (or very near it), and often involve the production of a product, whether it's electricity for the power grid or a children's toy. So, when the systems go down and production stops, there is a financial impact to the operators/owners.

Not surprisingly, this means operators don't want to take the systems down very often, which is required to install patches. Downtime is planned far in advance, and often it may be months, or even over a year until the next patching window. So, while the Microsoft patch was available in March, they may still not have gotten to the patch window when the first attack occurred in May.

TO RISK OR NOT TO RISK

In other cases, operators may run the risk/benefit analysis and choose not to patch. This is to completely ignore that many modern attacks can completely destroy entire ICS networks[3], and that it's not really a matter of if your network will get attacked, but when.

Regardless, the most common reason given is simply because the systems work as is, and no one wants to perform change management, deal with any downtime, or risk infection or disruption. While illogical, there are many operators who assume the costs of breach remediation will be less than that of the downtime required to patch or upgrade systems. Needless to say, this practice is not recommended.

NO CAN DO

Or ultimately, they just can't do it. There are often critical systems, devices, and applications that cannot be patched because they are outdated and no longer supported, or they may have no free memory to install a patch.

Even being "up-to-date" doesn't necessarily mean that all software vulnerabilities have been patched. It's possible that a vulnerability exists that is unknown to anyone outside of a few elite hackers – a so-called "zero-day" exploit, as EternalBlue was before it was revealed to the public. Zero-days can be weaponized by hackers, and because even the company that makes the software doesn't know about it, there is no way to patch them.

There are also instances where third parties which own or manage equipment within operational networks neglect to update these systems in a timely fashion. These third parties might also have connections into the ICS network. In such cases, operators may have no control over whether the systems are kept up to date, but operate under SLAs (service level agreements) that require data to be shared with the third party.

WHAT DO YOU DO IF YOU CAN'T PATCH?

Taking into consideration the variety of reasons that patches may not be possible, there are still options available to protect your valuable ICS operations and devices:

Internal Audit

The first important step is to take an internal inventory or audit of connected systems, to identify potential threat vectors and define your risk level. A lot of companies don't have accurate maps of data flows or system architectures, but they are extremely helpful for effective cybersecurity. Unless you know where you are vulnerable, there's no way to mitigate the possibility of cyber attack.

An audit can be performed manually, or with the assistance of an automated network device mapping tool, although many organizations shy away from the use of automated tools, as they could potentially disrupt operations by adding even a tiny extra load on the network.

You don't usually have to look far to find connected systems and devices that have known or potential unpatched vulnerabilities, but finding *all of them* can prove challenging. However, a device or system that may become infected can still be limited from impacting the entire ICS network.

Remove Unnecessary Connections

Frankly, sometimes devices are connected to external networks without any good reason to do so. Whether through flawed network architecture, lack of clearly defined security procedures, urgent requests for data access, or just doing it because it can be done,

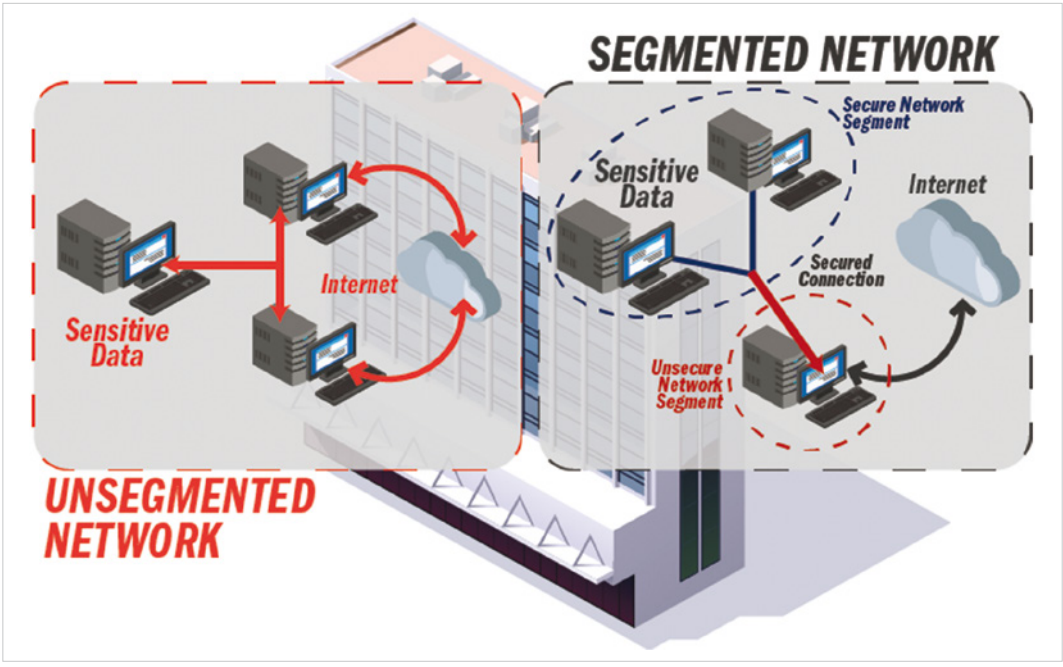


Figure 2: Network segmentation.

unnecessarily connected systems and equipment is a top cause of malware infections and proliferation.

Among the best practices outlined in the U.S. Department of Homeland Security's invaluable white paper, "Seven Steps to Effectively Defend Industrial Control Systems[4]," perhaps the most important is to create a more easily defendable environment. First, by removing any unnecessary connections. This also includes connections to third parties that do not require access to your ICS network.

Every connection to an external network, no matter how well monitored, is a potential avenue for an attack into the ICS network. Many ICS operators are stretched thin on cybersecurity, to begin with – some don't even have a single dedicated role for it – so for each connection that is removed, it is one less requiring protection, attention, and vigilance from a shorthanded group.

Creating a defendable environment also means segmenting the ICS network itself, and creating layers of security within it.

By creating multiple network segments, each one can be assigned its own level of security and trust, and the flow of data between each segment can be limited and monitored. Segmentation can also help to mitigate penetration test-style "lateral traversal", where hackers or malware jump from one device/system/workstation to the next. Think of network segments as compartments on a ship. If the ship is attacked and starts taking on water, each compartment can be closed off from the rest to stop it from spreading.

Implement Hardware-Based Security

Quite often, proposing severing connections to the ICS network, no matter how trivial, will result in heavy pushback, as end users in business or IT roles, or third parties want access to ICS data. In these cases, the DHS recommends that operators change as many of these connections to one-way as possible[5], with the use of a data diode or similar hardware-based cybersecurity device.

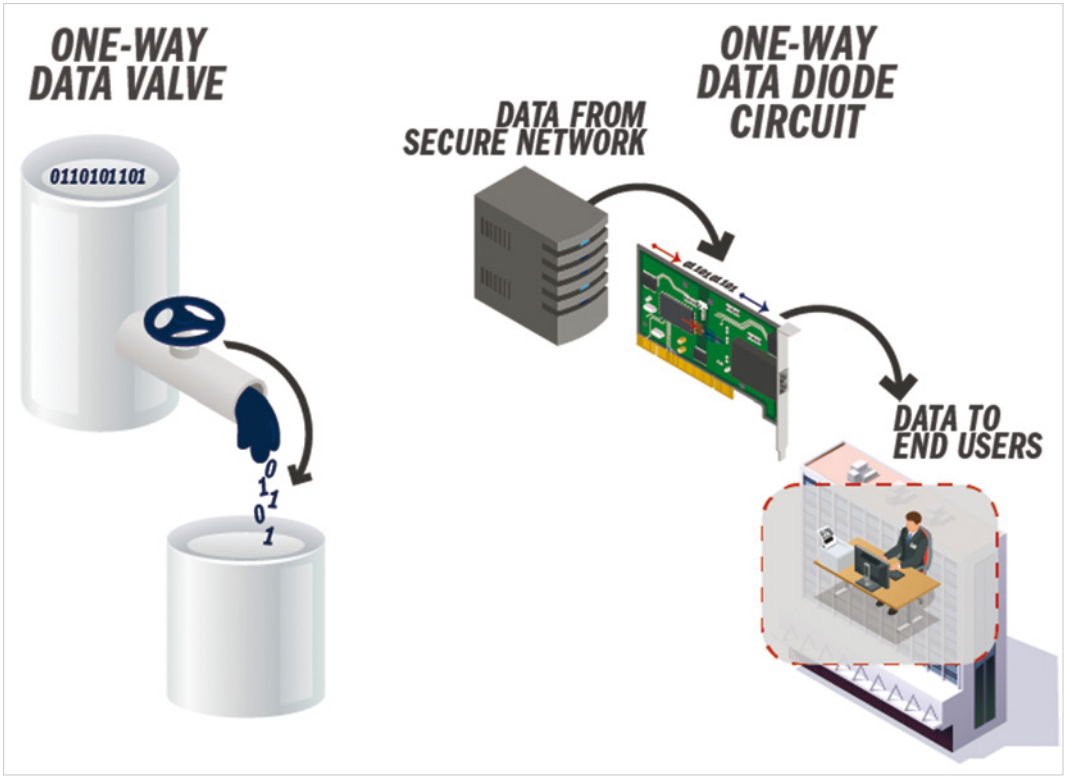


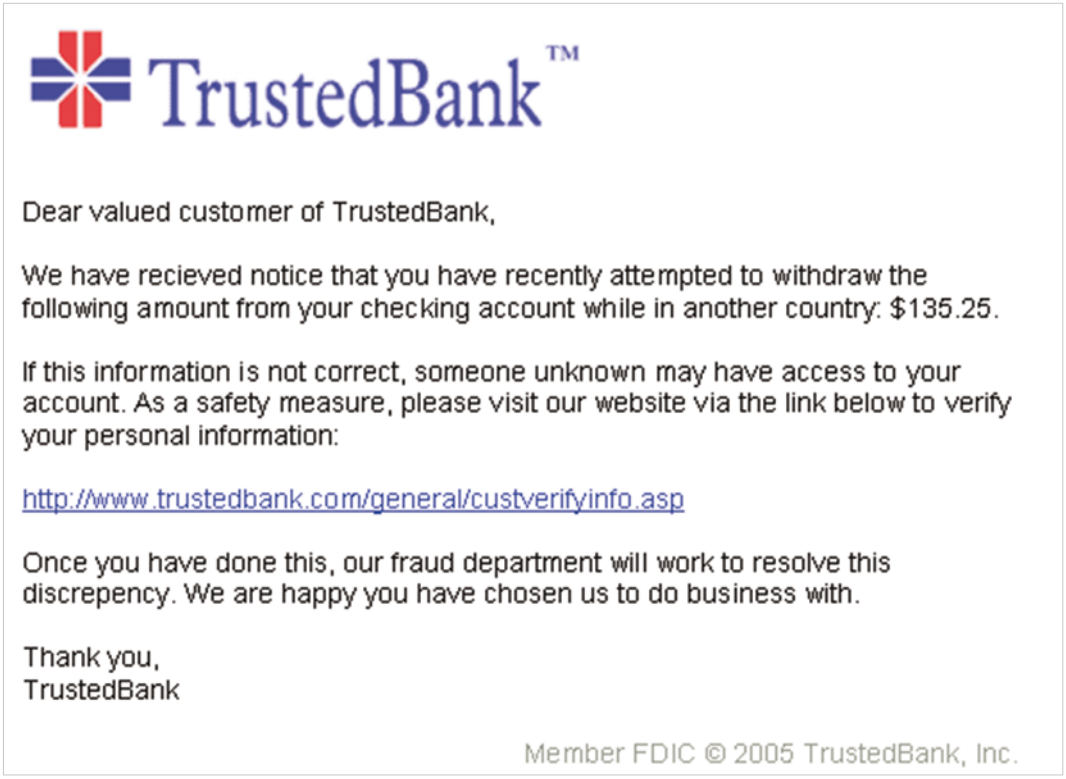
Figure 3: Data diode as a one-way data valve.

A data diode is a hardware-based device that physically enforces a one-way flow of data. To borrow from the ship metaphor, it's perhaps simplest to think of them as one-way valves for data, allowing it to flow from one compartment to the next, but not back.

As one-way data transfer systems, data diodes are used as cybersecurity tools to segment and protect networks from external cyber threats and prevent penetration from any external sources. They allow data to flow out to users that need it, without allowing access back in, which can be extremely useful for unpatched or otherwise closed networks. Data diodes effectively sustain an "air-gapped" architecture from the outside, while enabling data flows out of the ICS network to continue.

Firewalls and software-based cybersecurity tools are usually the first line of defense, and the first to mind when considering building a wall of security around sensitive networks. Unfortunately, in addition to having their own issues with zero-day attacks, firewalls mean heavy, ongoing change management, configuration, and (*you guessed it!*) more patching.

In contrast, data diodes often do not require any change management, as they also usually do not require much, if any reconfiguration, upgrade, or replacement of industrial control systems or settings – including legacy systems. As hardware-based devices, they are not vulnerable to software attacks, and thus do not require any regular patching, although patches to improve functionality may be available from time to time. Data diodes also assist in network segmentation and creating layers of defense between trusted and untrusted networks.


TrustedBank™

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Figure 4: Example of a phishing email.

Thoroughly Vet Portable Media

Given that the prudent approach should be to maintain as disconnected an architecture as possible for unpatched ICS networks, the majority of data that comes in, and thus the most likely vector of attack, will be from portable media – USB drives, laptops, test equipment, etc. Therefore, it is vital that all portable media be subject to thorough vetting, including antivirus, hash checksums, and other file authentication.

Typically this screening is performed with a security kiosk, where the portable media is first plugged in and scanned before it is allowed to be connected anywhere in the ICS network. These security kiosks may also be used in conjunction with data diodes, firewalls, and authentication tools to provide additional security. Ideally, no laptops or other sophisticated media that have been connected to the internet should be allowed to enter the ICS network, but if it is necessary, they must also be subject to the same thorough vetting.

Institute/Pay for Cybersecurity Training

The reality is, all of the strongest cybersecurity technology and best practices in the world won't prevent one human from rendering it all useless. It's vital to minimize the human element as much as possible, especially in an environment where known vulnerabilities exist. Not to mention that human error accounts for over half of all cyber incidents and breaches[6]. Unless your staff is extensively (or at least adequately) trained in cybersecurity procedures, all your security efforts, large or small, are at risk.

Nowhere is this more apparent than in phishing attacks – where an attacker sends an email that appears to be legitimate but instead links to malicious software.

Once one employee is compromised, the attacker can then utilize all of that person's personal and professional information to compromise the next employee (so-called "social engineering"), jumping from one to the next until they get the access that they need to do real damage. The BlackEnergy Ukrainian grid attack[7] in particular, showed the devastation of a sophisticated phishing and social engineering campaign could accomplish.

Developing an internal training program is ideal, as it builds security into the routine of your operators and employees. If an internal training program is not possible, reach out to a reputable company for phishing training, and to develop a comprehensive program that can be taught and repeated on a regular schedule.

SUMMARY

While applying patches that are readily available sounds simple in theory, in practice, especially in ICS networks, it can get complicated very quickly. Whatever your organization's reasons for not patching, all hope of implementing adequate security and preventing a successful cyber attack is not lost.

With the use of various techniques and technologies, such as data diodes, operators may even be able to avoid performing change management, which can come with loads of paperwork, limit the need for downtime, which can be costly, and keep a connection between the ICS network and the IT network while reducing or eliminating the risk that comes with it.

Following the guidelines above, in combination with best practices from the DHS and industry regulatory bodies, as well as implementing a comprehensive training program, can provide a strong basis to prevent cyber attack against your unpatched systems. ■

REFERENCES

1 https://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch

2 https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

3 https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

4 https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

5 https://ics-cert.us-cert.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

6 https://www.dataprivacymonitor.com/cybersecurity/deeper-dive-human-error-is-to-blame-for-most-breaches/

7 https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

ABOUT THE AUTHOR

Scott Coleman has a strong technical background with 25+ years of experience working in high tech as a programmer, marketing and product manager, and now as Director of Product Management at Owl Cyber Defense. His experience in real-time network solutions covers a number of industries including healthcare, telecommunications, power and water utilities, wiretapping, and cybersecurity for both the private and public sectors. He has authored many articles, hosted numerous webinars on advanced technology and cybersecurity, and is a frequent invited speaker at conferences.