Podcast Episode

Public Sector
Embracing Digital Transformation

A Holistic Approach to Critical Infrastructure Security

Darren W Pulsipher, Dr. Anna Scott, Steve Orrin – Dec 15, 2022

Time to leverage IT best practices in securing your OT critical infrastructure.

In this episode, Darren talks about the convergence of OT and IT cybersecurity with Security expert Steve Orrin and Industrial OT expert Dr. Anna Scott.

Video: Youtube Channel

Podcast: SoundCloud

Keywords: EDT116, EmbracingDigital, OT/IT,CyberSecurity, CriticalInfrastructure, OTSecurity,RiskAsssessment

There is a real threat to Critical Infrastructure

According to Dr. Scott, OT organizations still use the traditional Purdue Model, which leverages air-gapped and firewalled-off networks. However, this model is starting to fall apart as IT and OT networks converge. Businesses are trying to get better insight into what is happening in their operational infrastructure. As a result, they punch holes in the previously well-isolated networks, exposing them to cyber threats. Additionally, cybercriminals are finding ways to circumvent air-gapped and firewalled networks.

Steve argues that leveraging IT best practices can help, but OT professionals and IT professionals have different motivators and operating models. Continuing to isolate your network is still a good strategy but should be one of many tools used in critical infrastructure cybersecurity protection. OT security should look at IT cybersecurity best practices for ideas to improve their networks and infrastructure.

IT and OT differences impeding Best Practices

IT systems are traditionally updated quickly or continuously based on security profiles. One of the primary tools to improve security is basic security hygiene through patching operating systems firmware and software in the IT infrastructure. However, as Dr. Scott enlightens us, OT systems managing critical infrastructure cannot have downtime, and the window to update these systems is measured in years, not days. It is not uncommon in OT infrastructure devices that machines run for 5 to 10 years with no downtime, meaning no patch updates.

For example, in the oil and gas industry, refineries operate continuously for four to five years, have a one to three-week downtime for upgrades, and then operate again for four to five years. These operating models are not conducive to the traditional continuous security patching that IT organizations typically use. However, Steve elaborates on many other cybersecurity tools that should be leveraged when cybersecurity patches cannot be applied to existing devices due to their critical controlling infrastructure.

Best Practice Risk Assessment

the primary cybersecurity best practice is risk assessment. Even though risk remediation may be different, the risk assessment process can be leveraged equally across OT and its environments. Steve argues that the first step of the risk assessment process is getting a complete inventory of hardware, firmware, and software assets in your OT environment. This first step is critical in evaluating your cyber threat position and assessing the risk your organization is willing to take. The next step is to evaluate CVEs against your known inventory.

It is critical to recognize that this is a continuous process and not to be done just once or periodically. Some OT professionals have argued that their OT environments are static and do not require ongoing risk assessment evaluation. However, Steve points out that even though OT environments may be fixed, the threat environment constantly changes, and business factors can change the organization's risk position. Therefore continuous risk assessment must be done to protect critical infrastructure from bad cybersecurity actors.

Dealing with OT Vendors

Another interesting factor in OT infrastructure is the shared security model with device vendors. In many cases, these embedded devices controlling multimillion-dollar critical infrastructure are managed to buy the vendor, not the OT professional. The vendor can only make cyber security patches and updates to the devices. This can sometimes lead to vulnerabilities in your OT environment, increasing the risk of cyber infiltration. Steve brings additional cyber security tools to help protect assets that cannot be patched with critical cyber security patches, including increased isolation of affected devices, deploying watchdog devices, and canary design patterns into the OT infrastructure. These tools can help protect and isolate the device to prevent the spread and access to compromised assets.

What to do when you are compromised

So what do you do when you have a critical infrastructure that has been compromised? Can the organization handle shutting down the infected infrastructure? What business continuity plans are in place when hazardous situations occur? Can this be used when a cyber security event happens as well?

The key here is to isolate the infection as quickly as possible to minimize the impact on the critical infrastructure. I am decreasing the effect on the operating reliability of the necessary infrastructure. The goal is to reduce the impact and protect the safety of people and the infrastructure involved.

Find out more

Continue to look for more podcasts on OT cybersecurity. Additionally, a whitepaper describes the challenges of converging OT and IT cybersecurity environments.

.