BIZCOMMUNITY

The specialised security concerns of OT networks

By Doros Hadjizenonos

13 Nov 2018

As with traditional IT networks, Operational Technology (OT) networks are undergoing a digital transformation process of their own. The goal is to improve productivity, efficiency, uptime, and flexibility through better monitoring.

Source: pixabay.com

To do this, online sensors and connected systems are replacing traditional serial connections, proprietary protocols, and programmable logic controllers to better manage and control industrial environments.

At the same time, the integration of automation, communications, and networking in industrial environments is an integral part of the growing Industrial Internet of Things (IIoT).

Specialised security concerns of OT networks

As with IT, the most important – and often overlooked – consideration during this transformation process is security. Many OT systems were never designed for remote accessibility, so the risks associated with connectivity were never considered when the OT architecture was originally engineered.

Rather than completely redesigning these environments, OT networks have begun to utilise solutions such as strong segmentation and specialised analytics to ensure the safety and reliability of physical processes and devices.

This helps organisations apply some measure of their larger IT cybersecurity practices into their OT environments to address new security risks targeting multi-vector threat landscapes.

However, as cybercriminals begin to more aggressively target OT devices and systems, these basic security measures are increasingly inadequate. OT networks need to evolve to address increasing cyber risk.

One challenge is that many OT networks are especially delicate, and taking even one sensor or device offline can have serious if not devastating consequences. Even something as basic as actively scanning an OT device or system looking for vulnerabilities or malware can cause them to fail. Which means that many of the traditional tools and protocols used to protect the IT network simply don’t translate over to OT. Instead, it requires specialised security technologies and solutions designed to provide protection without impacting the function of sensitive and highly regulated equipment and systems.

Creating a unified security strategy

This convergence of IT, OT and IoT has sent many security practitioners back to the drawing board to rethink security practices and redefine security architectures so that they can align to evolving environments, without compromising the overall integrity of the distributed network.

What is becoming apparent, especially as OT emerges as a new target for cybercriminals, is that organisations not only need to be able to apply specialised security solutions and strategies to their OT environment, but they need to also be able to tie them into their larger security framework. This requires a single, cohesive Security Fabric platform that enables security teams to establish true, single-pane-of-glass visibility and control.

This approach enables them to seamlessly see and address security risk across multi-vector threat landscapes without overburdening security staff resources or impacting their highly differentiated networked environments.

3 Key considerations

Approaching the development of a unified security strategy that addresses both IT and OT requirements includes the following considerations:

1. The first place to start is by choosing a security vendor that specifically addresses the cybersecurity, safety, and reliability challenges being faced by the OT industry. Not all security solutions are the same, especially when it comes to securing OT.

   You need a vendor that offers a full range of specialised tools and protocols designed for OT environments, and that has established strategic partnerships with the industry’s leading OT security specialists. And these solutions need to be field tested and proven. Unlike IT environments, OT systems and devices cannot afford to be taken offline by an inappropriate security solution.

2. These OT security solutions also need to be able to be seamlessly integrated into a centralised and integrated security platform that spans the larger network. Data, applications, and workflows need to move where they will, from the core to the cloud, including IoT devices, branch offices, and distributed OT networks. And a truly effective security solution needs to be able to track and monitor that traffic, automatically correlate threat intelligence, and orchestrate a unified response to detected threats through a single management console.

   This requires a degree of integration most security vendors struggle to provide.

3. Finally, your security solution needs to be flexible enough to easily accommodate and integrate with a large number of

partners to provide truly comprehensive security coverage. No single vendor can provide all of the resources you need to secure your distributed and evolving networked environment, including OT.

So, in addition to providing specialised OT security solutions and deep integration between security elements, you need solutions that supports an open security ecosystem. Common standards, open APIs, and a commitment to meaningful integration are essential for any tool being added to your security arsenal. In fact, interoperability may be more important than specific features, as an integrated, collaborative and adaptive security system will always be more effective than any functionality provided by any single device.

Key takeaway

In today's new digital economy, the stakes are high. Consumers and end users demand instant access to data and other resources, combined with pervasive protection of their personal data. And for organisations involved in securing operational environments, that risk extends to the personal as well as cybersecurity of employees and citizens.

As a result, organisations can no longer afford to be implementing security silos built around isolated legacy security tools that can't function as an integral component of a larger security strategy. You need specialised OT tools that can be integrated into a comprehensive security strategy. That needs to include a rich ecosystem of technologies from an array of specialised partners.

Only this approach will enable you to develop different networking environments, each with their own, unique business functions, that can be secured through a comprehensively integrated security strategy.

This strategic approach ensures the confidentiality, integrity, availability, and performance of today's increasingly complex and interconnected digital networks, while controlling the overhead associated with other approaches to digital transformation.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...