SPONSORED FEATURE

Centralized, Model-Driven Visibility Key to IT-OT Security Management

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2Eqo6Or

The threat landscape has changed significantly for operational technology (OT) environments as their connectivity to IT networks and the Internet has exponentially increased. Today, Internet of Things (IoT) devices such as remote sensors transmitting data over Wi-Fi have introduced millions of new access points in organizations responsible for utilities, energy, manufacturing and more. Additionally, there is a greater need to connect OT computer, control and inventory systems to corporate IT networks to better manage the business and production.

Challenges

While connectivity has been a boon to efficiency, it has introduced new risk to both IT and OT environments. In the first half of 2017, an average of 20 percent of industrial control system computers were attacked worldwide each month.[1] As the knowledge, tools and services to carry out these attacks become more widely available, this figure will only increase.

But an even bigger challenge to secure hybrid IT/OT networks is internal. First, the scale and complexity of such networks are immense. Second, their management teams are generally disconnected, working with different processes, technologies and objectives. The gap created between the security management demands of IT/OT networks and the resources available to meet them are where attackers find their opportunity.

To overcome these challenges while maximizing uptime and maintaining safety, organizations need to gain seamless visibility of their entire attack surface. While visibility solutions are available for OT networks, they are not widely in use and not integrated with the IT security program, leaving a large and high-risk blind spot of cyberrisk. To unify IT and OT security management, organizations need to have a centralized solution that gives all teams a common view of the entire network and its risk scenarios.

Threats to OT on the Rise

For attackers, limited visibility and organizational vulnerabilities create a perfect storm. Security experts and governments worldwide are warning of the increased threat to OT networks, including to critical infrastructure.[2] Traditionally, advanced persistent threat (APT) groups or nation-states have given OT engineers the biggest headaches, but the democratization of attack tools and increasing organization of cybercrime are expanding the variety of threats to these networks. Using attack methods commonly seen in IT networks, such as phishing and ransomware, hackers have set their sights on notoriously unpatched—or unpatchable—OT assets to disrupt operations, cause damage, perform reconnaissance or profit the attacker.

In the last two years, there have been major incidents demonstrating what the new threat to OT looks like. WannaCry forced hospitals to turn away patients and brought production lines to a halt.[3, 4] NotPetya disrupted radiation monitoring systems at the Chernobyl nuclear site, and cost Maersk alone US $300 million.[5] And Industroyer is largely credited with taking a Kiev transmission substation offline, causing a power outage in the middle of winter.[6]

Ingredients for Unified IT/OT Security Management

Considering these events, boards want to reduce business and operational risk; IT teams want to reduce cyberrisk across all networks; and OT teams want to keep production running smoothly—and safely—without becoming full-time security experts. To meet these objectives, organizations need to have the right tools and processes in place.

First, security teams need to be able to automatically and nonintrusively collect data from various levels

Ron Davidson
Is a 30-year IT veteran who has worked with many of today's leading minds in the security industry. As chief technology officer and vice president of research and development at Skybox Security, Davidson is responsible for advancing product innovation and leading the Skybox Research Lab intelligence group.

of the connected environments, including IT and OT assets, OT protocols, network devices, and firewalls. To make sense of these data, they should be built into a comprehensive, visual and interactive model spanning physical IT and OT, virtual and cloud networks.

An offline model gives IT teams access to the OT network to troubleshoot connectivity, analyze network paths, and simulate potential attack paths between and within different networks, without disrupting production. Understanding the connections between IT and OT gives visibility to the state of the perimeter and whether the appropriate security controls are in place. For instance, the model can show Internet connections to the OT network—a major source of risk, but increasingly common in OT networks where the convenience of IoT devices has outweighed security concerns.

> "THE GAP BETWEEN THE SECURITY MANAGEMENT DEMANDS OF IT/OT NETWORKS ARE WHERE ATTACKERS FIND THEIR OPPORTUNITY."

The model can also be used to assess vulnerability status on demand without an active scan, which is difficult to run in OT environments requiring constant uptime. Scanless assessments utilize other data repositories (patch and asset management systems, network device data and system information). That information is correlated with Common Vulnerabilities and Exposures (CVE) listings, manufacturer advisories and other public vulnerability databases to discover vulnerabilities on demand—even in systems where scanning is not an option.

By combining vulnerability data and threat intelligence with the network model and attack simulations, IT teams have an accurate view of their attack surface and can spot security issues attackers are most likely to target, such as vulnerabilities exposed in the network or actively being exploited in the wild. For example, vulnerabilities used in WannaCry, NotPetya or Industroyer should be top priorities. Intelligent vulnerability prioritization can better facilitate the workflow between IT and OT. During planned production downtime, IT teams can make informed recommendations of patching priorities or other mitigation measures that can cut off vulnerabilities from attack paths.

Take the Holistic Approach

A holistic security management program is one that balances objectives: reducing cyberrisk without sacrificing uptime, availability or safety. To create this kind of program, visibility is the first step. Seamless visibility across IT and OT networks lays the foundation for centralized security management that can mature and adapt even as the organization and the threat landscape evolve.

Endnotes

1 Kaspersky Lab ICS CERT, "Threat Landscape for Industrial Automation Systems in H1 2017," 28 September 2017, *https://ics-cert.kaspersky.com/wp-content/uploads/sites/6/2017/10/KL-ICS-CERT-H1-2017-report-en.pdf*

2 Ashford, W.; "Industrial Control Systems Under Attack, Warns MIT Researcher," *ComputerWeekly.com*, 11 October 2017, *www.computerweekly.com/news/450428010/Industrial-control-systems-under-attack-warns-MIT-researcher?utm_medium=EM&asrc=EM_EDA_83784149&utm_campaign=20171011_Government%20proposes%20changes%20to%20make%20Britain%20safer%20online&utm_source=EDA*

3 Brandom, R.; "UK Hospitals Hit With Massive Ransomware Attack," *The Verge*, 12 May 2017, *https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin*

4 Reuters Staff, "Honda Halts Japan Car Plant After WannaCry Virus Hits Computer Network," *Reuters.com*, 21 June 2017, *https://www.reuters.com/article/us-honda-cyberattack/honda-halts-japan-car-plant-after-wannacry-virus-hits-computer-network-idUSKBN19C0EI*

5 Burton, G.; "Maersk Pins $300m Cost on NotPetya Ransomware," *Computing*, 7 November 2017, *https://www.computing.co.uk/ctg/news/3020561/maersk-pins-usd300m-cost-on-notpetya-ransomware*

6 Greenberg, A.; "'Crash Override': The Malware That Took Down a Power Grid," *Wired*, 12 June 2017, *https://www.wired.com/story/crash-override-malware/*