Control Networks:
Maintain Their Availability During a Cyberattack

What You Will Learn

Control networks and industrial control systems manage the generation and delivery of electricity, automate production lines, control environmental systems in large commercial buildings and hospitals, and manage many other vital processes. They also face a unique set of complications when it comes to cybersecurity. Cisco understands this and helps protect control networks before, during, and after an attack without sacrificing reliability.

Control networks are targeted by the same cybersecurity threats that typical corporate networks face, but many industrial control systems in operation today were designed during a time when it was sufficient for networks to be physically separated (“air-gapped”) from their corresponding corporate networks. It was assumed that a system on the control network was explicitly authorized to be there. It followed that there was no reason to specifically authorize communications between systems. But amid the sensationalism that the Stuxnet worm generated for its ability to sabotage an air-gapped control network was an important lesson: Air gaps as a cybersecurity technique are no longer effective.

At the same time, it is important to recognize that IT cybersecurity solutions in use on the corporate network can’t be deployed interchangeably to protect the control network. The two management teams have different priorities. The IT team is typically focused on the triad of confidentiality, integrity, and availability, in that order. The control network operations technology (OT) team is focused on availability first, then integrity and confidentiality. When control networks fail, there are real risks posed to human life and environmental safety. Availability and reliability are paramount and must be maintained at all times.

Another consideration is ease of use. It is not uncommon to find cybersecurity as one of many functions for which OT engineers are responsible. Therefore, cybersecurity solutions deployed in control environments must be intuitive with minimal management requirements.

The Attack Continuum and Defense in Depth

For many years, conventional wisdom focused solely on a perimeter-based defense with the mission to keep out all attackers. Little attention was paid to what happened within the walls of the enterprise, to the detriment of more than one organization. For all of the effectiveness of a good, solid wall, it protects against only certain types of attack. All it takes is one door left open, intentionally or not, to render the thickest of walls useless.

Today, the conventional wisdom is to expect a successful attack, and to design and defend a network with a defense-in-depth approach to mitigate the damage. This approach involves a multi-layered, multi-technology strategy to protect an organization’s most critical assets as determined by asset inventories, business continuity reviews, and risk analyses.

Another important shift in thinking is to recognize that cybersecurity is not a point-in-time exercise. Rather, it must be thought of as a continuous process, constantly evolving. Cisco's strategy, therefore, focuses on the full attack continuum.

The full attack continuum can be broken into three phases—before, during, and after an attack—and each phase consists of a number of activities. For instance, for the attacker the "before" phase consists of surveying the targeted network and planning the attack, while the exfiltration or destruction of data will, logically, occur in the "during" phase. What is sometimes overlooked is the "after" phase, when attackers can remain hidden for days, weeks, or months while they complete their mission and establish a beachhead for subsequent attacks. But if we are to prevent history from repeating itself, thwarting attacks can't focus only on detection and blocking. Ongoing analysis after an attack is vital to mitigate damage and adapt defenses before the next attack. Cisco offers protection along all phases of the attack continuum through research, real-time monitoring and response, and continuous event and traffic analysis to detect trends and evasion techniques.

Applying Cybersecurity to Control Networks

Before

The adage "forewarned is forearmed" is a key tenet in Cisco's strategy. The Cisco Talos Security Intelligence and Research Group analyzes millions of pieces of malware annually and updates rule content regularly to keep customers up to date to defend against the latest threats to keep our customers up to date to defend against the latest threats. Our rule library includes industrial control system (ICS)-specific content for common industrial protocols. Custom content may be created by our customers and by other third parties and then be imported into our rule library, regardless of whether that content was created on our commercial product or our open-source Snort® product. This flexibility makes it easy to share content within the community rather than requiring each customer to build custom content from scratch.

To put this research to use, you first have to know what it is you're protecting and where it is, but that isn't as easy as it may seem in a control network. Industrial control systems such as remote terminal units (RTUs) and programmable logic controllers (PLCs) are typically built to perform a specific task and many run proprietary operating systems with the minimum amount of processing power and memory. Therefore, even the most basic discovery methods, such as a port scan, could conceivably take these industrial control systems down. Cisco is able to passively profile control networks without being inline. This capability means that we will not introduce communications latencies between control systems, and we do not need to aggressively scan the control network. Baselines of behavior and communications patterns may then be established in whitelists where only anomalous traffic is inspected and approved communications are allowed to flow freely, as is commonly desired in control networks.

Commercial operating systems such as Microsoft Windows XP have made inroads into the control system world over the past few years, particularly with human-machine interface (HMI) systems and historians. The use of commercial operating systems has provided a benefit to manufacturers. They do not need to devote effort into developing proprietary operating systems, and asset owners enjoy the increased interoperability between vendors' equipment. But these control systems face increased security vulnerabilities due to the complexity of the operating system code base. The interconnectivity itself creates another attack vector. Although commercial vendors regularly release security patches, patching systems in a control network is not the same as patching systems in an IT network. Control system patching cycles are a great deal longer and require extensive testing in order to protect the reliability of the control network. Cisco provides compensating controls and increased security focus on these systems while they are unpatched and vulnerable.

During

A nation-state probes your corporate network looking for access to your control network. A smartphone is plugged into a management system to recharge the battery, and malware is released onto the network. A new device in a substation begins communicating with a management system, which in turn begins communicating with other systems it hadn’t communicated with previously. A teen hacker uses a specialized search engine to find a system that was inadvertently connected to the Internet and tries a brute-force attack to take control of the system.

Attacks can be swift and blatant, or they can be slow and subtle. They can be direct, or an unknowing middleman can facilitate them. Attacks may endanger physical safety just as much as they endanger network reliability.

Cisco monitors your perimeter and internal network for attacks, anomalous behavior, role violations, advanced malware, and so on, from a single appliance platform. Appliances are available as hardware or virtual appliances. Endpoints and mobile devices may also be monitored for advanced malware. You determine which capabilities you wish to enable based on your requirements, budget, and timelines. You don’t need to add more hardware, and you can evolve your deployment over time. When anomalies, policy violations, or indicators of compromise are detected, Cisco security solutions can respond in an alert-only mode or automatically take action to contain the threat upon detection. The choice is yours. You can also have the control to set response policies based upon network segment so that responses on vital segments require human approval before being executed. All monitoring, reporting, and management are performed through a single central console.

After

It has been said that no plan survives contact with the enemy. The reality is that attackers’ tactics evolve quickly and defenses must keep pace just as quickly. What may appear innocuous today may be later discovered to have been a cleverly disguised attack. How does one defend vulnerabilities that are not yet known? Cisco’s threat-centric approach to security includes a continuous capability, always analyzing event and network data and searching for patterns and anomalies. When they are discovered, our retrospective security capability determines the source and scope of compromise, contains the outbreak, and remediates the malware. With this intelligence you can update protections to reduce the chance of reinfection.

Conclusion

Air gaps are no longer insurance against intrusion. And the increased connectivity that brings operational efficiencies to control networks has also brought a host of vulnerabilities and a larger attack surface. Although these threats are like those faced by corporate IT networks, the unique requirements of control networks means that cybersecurity solutions are not one-size-fits-all. Cisco understands this. Our advanced cybersecurity portfolio helps protect your networks before, during, and after an attack without sacrificing reliability.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA 11/14