betanews

Priorities for data center OT security in the cloud era

- By Jose Seara
- Published May 2024

The decentralized nature of the cloud provides great flexibility for users, but it also introduces great vulnerabilities for data center operators. As an abundant source of valuable data, the modern data center has become a prime target for cybercriminals, from small business facilities to the huge hyperscale colocation data centers run by Amazon, Google, and Microsoft.

Protecting these interconnected facilities and the hardware and software systems that they physically host provides a perpetual job for security teams. But it’s important to recognize the clear distinction between securing information technology (IT) inside a data center facility, versus securing the operational technology (OT), or what’s called “cyber-physical systems” needed to run the facility itself. IT and OT involve two complementary but distinct categories of security and risk.

IT cybersecurity is managed through security software platforms, network firewalls, and scanning technologies. While the cybersecurity of OT systems involves similar solutions, additional constraints limit how quickly cybersecurity measures can be deployed. Maintenance windows require advanced planning for the OT systems that focus on physical buildings and handle electricity, heating, cooling, and access control.

In addition, these interrelated subsystems increase the risk that successful cyberattacks could spread across multiple parts of a data center. Some types of exploits by bad actors include hiding backdoors in equipment to install malware that can later compromise other systems and devices, or cutting off sources of power to shut down the cooling system, leading to hardware damages.

More than half of data center operators (55 percent) reported some kind of outage over the past three years, according to the Uptime Institute’s Global Data Center Survey 2023.

And 20 percent of survey respondents cited concerns about data center operations, architecture, or resiliency as their reasons for not utilizing public clouds.

Right-Sizing OT Security Protections and Barriers

Protecting an entire data center facility is a complicated problem. In this treacherous geopolitical climate, it’s tempting for data center operators to focus on the security of hardware and software deployed in their facilities and overlook the physical assets within the data center. They need to develop clear plans to ensure continual uptime. This includes hardening critical systems for infrastructure management, electrical management, building management, and security management.

Infrastructure Management Systems: Data center infrastructure management systems include tools and dashboards that are used to monitor, analyze, and manage a facility’s power and cooling systems, along with server utilization, asset tracking, and other vital functions.

Standard security procedures such as regularly updating and patching software are not always feasible in a timely manner, if at all, in OT environments. That is why, whenever possible, data center OT networks should be segmented apart from IT networks to increase security. OT networks use dedicated OT communications protocols and redundant systems to maintain reliability and resilience.

Many operators are also adopting new tools to prevent cyberattacks from harming data center networks. Unidirectional gateway technology solutions are encased in hardware to ensure a unidirectional transfer of data between two networks. The software stores copies of active servers and devices from the OT network to share with the enterprise network in real-time. Because the hardware can only send the data in one direction, attacks can never be propagated back into the network through the gateway server.

Electrical Management Systems: Electrical power and distribution systems provide the lifeblood of any data center. Attacks on the EMS can cause serious power-related problems including disruptions to power supplies or failures in power distribution. Such issues can lead to expensive data losses, service interruptions, and damages to electrical hardware.

Building Management Systems: Every data center facility must have BMS controls to manage their physical environment, including temperature, humidity, airflow, and fire suppression. All these systems present potential threats for unauthorized access and manipulation that can result in downtime or damages to equipment.

Security Management Systems: Physical security assets include access controls, video surveillance, and threat detection systems. Problems involving disabled cameras or breaches to access controls can allow intruders to infiltrate restricted areas of the facility without authorization.

Newer approaches such as cyber risk quantification and management (CRQM) tools can give data center operators an advantage by assessing the full range of business damages that could be triggered by vulnerabilities. CRQM tools help by thoroughly analyzing the impacts of any potential cyber incidents, and then prioritizing the top sources of risk for mitigation.

Data center OT will continue to provide a rich target for large scale attacks on critical infrastructure well into the future. The stakes could not be higher, as the bad actors include state-sponsored threat actors and global adversaries seeking a geopolitical advantage in times of crisis. Data center operators can only achieve their uptime goals and secure their capital-intensive assets by first securing their OT networks. That is why it is so important to update aging cybersecurity infrastructure and deploy emerging technologies to keep pace with these attackers' ever-shifting attack vectors and threat surfaces.

Image credit: achirathep/depositphotos.com

Jose Seara is Founder and Chief Executive Officer, DeNexus.