Five Basic Considerations to Prevent Server Attacks for Good

CHATSWORTH PRODUCTS

Global businesses experienced a radical change in 2020 as many had to shift to a remote and distributed workforce quickly and without much preparation. In the cybersecurity segment, these circumstances were seen as opportunities by cyber attackers.

Not surprisingly, besides an overall increase in ransomware, phishing and malware attacks, server access was the third most common type of attack in 2020, according to the 2021 IBM X-Force Threat Intelligence Index, an annual report published by the Security arm of IBM. The report defines a server attack as a "threat actor gaining unauthorized access to a victim's server, either by exploiting stolen server credentials, exploiting a vulnerability, or other means."

In a reality where data has become the world's most valued asset, privacy and ethical management of data must be a top priority for organizations and data centers, particularly during times when remote work is becoming the norm rather than the exception.

Chatsworth Products (CPI), an expert in intelligent power management solutions and information and communications technology (ICT) infrastructure, recommends for data centers to include a robust access control system measure as part of their comprehensive cybersecurity framework.

Although data privacy standards and regulations require physical access control measures for data processing and storage equipment, it is up to each organization to decide which specific method of technology to use.

In general, compliance to regulations requires a method to:

Physically secure data processing and storage equipment

Identify and manage authorized accessors

Manage access to the physically secure space

Keep records of access to the physically secure space

Five Basic Considerations When Building an Access Control System

Physical Security: First Line of Defense

For an enterprise-owned, single-tenant site, room-level security could be considered sufficient. Particularly in multitenant data centers (MTDCs), also known as colocation facilities, and remote sites, physical access control at the cabinet level simplifies management and prevents unauthorized users to access the servers and switches in which data is stored.

Electronic locks and access control systems automate monitoring, documenting and control of access and allow fast reprogramming if access rights change or if a credential is lost or stolen.

Key and Rights Management

When keyed locks are used to secure equipment cabinets, companies must have a strong and effective key management program. Regardless how the cabinets are keyed, a strong system for documenting access is required.

In contrast, electronic locking can be reprogrammed quickly with new access codes, and no hardware modification is required. Each user can have different rights, and the setup of rights in the software is simultaneously documenting the assigned access codes (keys).

Logging Reports and Auditing

Having users sign in at controlled front building access ensures there's documented record of the person's presence in the building but not their access to individual cabinets.

Electronic locking and access control systems automate the logging of access at the cabinet level and enable automated reporting by user or cabinet. This speeds preparation for an audit and helps narrow the scope of event investigations.

Event Response

When a data breach occurs, immediate event response is critical. With a keyed lock system, IT teams must manually check the condition of doors and locks. If a key is lost or stolen, they must rekey the lock.

Electronic locking and access control systems simplify, shorten and in some cases, automate these responses. Additionally, these systems allow IT teams to remotely manage access attempts and door status remotely, from a software interface.

Jurisdiction: IT or Facilities Management?

In most data center facilities, security is deployed via a building management system platform, owned and managed by facilities management. When it comes to data center cabinets and systems, security is most often controlled by IT, which oversees data protection and equipment security.

Electronic locking systems support both connection to a building management system or installation as a separate system with a separate authentication database.

These considerations and capabilities outlined above are a wise place to start, but there are other important elements that, when combined, create a wholly future-proof, intelligent cabinet ecosystem. To learn more, watch the video at chatsworth.com/data-centers.

CHATSWORTH PRODUCTS