Secure Data Center Racks & Cabinets

Access Cards, Biometrics Seen As Key Elements In Overall Plan

Randomly poll stakeholders about what they feel their enterprise's most valuable asset is, and the answer will most likely be related to data. It makes sense then that data center managers go to great lengths to protect that asset. Traditionally, one means of securing data centers has been the use of security access cards, including at the individual rack and cabinet level. The question, however, is whether access cards still are the best option for securing racks and cabinets or if a security upgrade is in order.

Understand The Limitations Of Access Cards

According to David Orischak, CEO of Digitus Biometrics (www.digitus-biometrics.com), security experts agree that card-access systems are less secure than manual key-based systems. Still, are there data center scenarios in which access cards can prove sufficient?

"Whenever I'm asked this question, my response is the same: What level of risk are you willing to live with in the data center?," Orischak says. As he sees it, card-based systems are still only used because enterprises have legacy card systems installed at building and room access points, and they want to prolong their investment.

Typically, Orischak says, data centers embrace a military-style, reduced-concentric circle, card-based security scheme with the idea being to reduce the speed of an attack before it reaches the core, or the data center. An intruder who does reach the core, he says, will usually find server cabinets unprotected. Orischak points to last year's security breach at the Health Net data center in Rancho Cordova, Calif., as an example. "In the Health Net case, the card access control system proved ineffective," he says. Such a system doesn't show "who is passing through the access point; it only tells you what card is passing through the access point."

See The Big Security Picture

Info-Tech Research Group analyst Jenna Maertz says two primary issues typically prevent greater adoption of rack- and cabinet-level security. First, many server OEMs design cabinets so that it's incredibly difficult to close the cabinet's back. "The cabinets comply with width standards, but we have customers that are unable to secure the back of the cabinet because of the length being

Key Points

- Many experts consider access card-based security systems as less secure than other systems, including manual key-based solutions.
- Attacks perpetrated by employees possessing access cards, or those who can obtain access cards, pose one of the biggest risks to enterprises.
- Security systems based on biometrics are a viable option to access cards. Costs of solutions have come down considerably in recent years.

introduced by some server OEMs," she says. Enterprises, she says, "might not be able to retroactively install security at this level on existing infrastructure." Second, many enterprises view data center security from a top-down, entire-footprint perspective as opposed to securing individual pieces. The mentality, she says, is "why secure each part individually when you could secure the whole?"

Orischak says the majority of malicious attacks on data centers are conducted by insiders, which is why no enterprise can ignore the security risk created by insiders, including where racks and cabinets are concerned. Beyond having greater access to cards, insiders' mobility is seldom questioned, he says. This fact "neuters the idea of perimeter-based, reduced concentric circle access control," he says. "The attackers are already on the inside." Maertz says Info-Tech advises its customers to review employee access rights as often as possible but at least annually. A risk specific to access cards, she says, is the possibility of approved employees bringing guests into secure locations, which is a "huge security breach."

Equip Yourself

Jeff Clark, president and general manager of Lindy USA (888/865-4639; www.lindy-usa.com), says "real" data center security consists of multiple layers and starts by defining who has access to the server room. Start with a locking mechanism at the door, he says, whether it's a key-coded system, badge scanner, fingerprint recognition system, iris scanner, or other device. "Much of this is dictated by budget," he says. Clark notes that rack-mountable cameras are also available. Once a server cabinet is opened, the camera snaps network-distributable shots to identify who is inside the cabinet. Additionally, most server room-level KVM switches provide additional security via the OSD system, which prevents keyboard/mouse access without a password.

Orischak says most experts agree that biometrics is the best alternative for securing mission-critical facilities. Biometric solutions are now less expensive to purchase and operate than card-based systems, he says. Maertz points out that many newer access cards can be programmed to include biometrics. "The employee swipes her card and then places her hand on a biometric reader," she says. "This helps ensure that they didn't just pass off the access card to another employee." Biometrics technology, she says, is becoming more commonplace, and some options, such as fingerprint readers, can be installed fairly inexpensively.

Overall, cabinet-level security costs have dropped dramatically in the past year, Orischak says. "With the appearance of energy efficient bus-based systems, the cost to biometrically secure a cabinet can be less than $500," he says. "In situations where the cabinets are already installed, there may be some costs associated with modification of the lock opening on the cabinet door and/or the modification or replacement of the door." P

Top Tips

✔ **Use this equation.** For all organizations, securing data center racks starts with assessing how much risk the organization is willing to live with, says David Orischak, CEO of Digitus Biometrics (www.digitus-biometrics.com). He says the standard risk equation is: Risk = Threat x Cost x Vulnerability, and vulnerability is the only variable a data center manager can control. "If a data center manager is uncomfortable with the current level of risk, he must try to reduce vulnerability," Orischak says. "Dollars spent on cabinet-level security reduce vulnerability more so than dollars spent elsewhere in the data center."

✔ **Guard USB ports.** Jeff Clark, president and general manager of Lindy USA (888/865-4639; www.lindy-usa.com), says that in addition to racks and cabinets, data center managers need to consider guarding USB ports in an effort to protect enterprise data. USB port blockers can prevent authorized access. "Keep in mind that your network is protected from the outside by your firewall. With a thumb drive, a person can easily introduce unwelcome software applications into a network through the USB port," he says. "Not only that, they can retrieve and save sensitive data such as credit card numbers, classified documents, etc."

✔ **Make certain that upgrades make sense.** Info-Tech Research Group analyst Jenna Maertz advises small to midsized enterprises to take caution before investing money and effort into upgrading rack/cabinet security, as "there may be use cases in which this is appropriate and sufficient," but for some enterprises, it may make sense to focus attention on securing the entire data center.

Action Plan

■ Determine if security is needed more at the rack/cabinet-level or entire data center.

■ If an upgrade is necessary, determine what your budget is.

■ Know what your regulatory and compliance requirements are and ensure the potential solution meets them.

■ Ensure you can centrally manage cabinet access in real-time, produce and communicate alerts, and generate audit trails related to cabinet access.

■ Determine which type of rack/cabinet security solution best suits your data center.

■ Compare the solutions' initial and ongoing costs.

Get Started

Before choosing a cabinet-level security solution, make sure to ask several questions first, says David Orischak, CEO of Digitus Biometrics (www.digitus-biometrics.com). Questions include: What is the initial purchase price, how secure is the solution, what are the ongoing system operating costs (cards, powering the system, maintenance, etc.), can the system meet regulatory and compliance needs, is it easy to operate, and is it compatible with the operating environment?