Electronic locks: Intelligent access enhances datacenter security

Steve Spatig, General Manager, Electronic Access Solutions, Southco

The information stored within datacenters has become the foundation on which many organizations today conduct daily business and operations, and in many cases, is considered to be their most valuable asset. From the facility down to the cabinet level, security is a key concern of datacenter engineers. The increasing dependence on network-based electronic equipment is leading engineers to look beyond traditional mechanical locks to electronic locking solutions for securing valuable IT equipment and data.

For datacenter managers, the threat of loss is a constant concern – whether it’s damage to racks and hardware such as servers, switches and routers, or the loss or corruption of data. Loss affects IT productivity, resulting in data reconstruction, IT infrastructure repair or the replacement or retrofitting of security measures. Loss often translates to downtime in areas outside of IT as well, such when an organization must repair or rebuild their reputation or brand due to a disruption in business or services provided.

In order to increase the level of protection for cabinets housing network equipment and other critical hardware, many engineers are choosing to incorporate electromechanical locks or latches (EMLs) into enclosure designs. When combined with an access control device, such as a digital keypad or card reader, EMLs provide datacenter managers with a secure method of locking cabinets and the ability to control and track user activity through an existing networked access control system. This complete Electronic Access Solution (EAS) can also accept existing access control credentials, allowing datacenter personnel to use their current credentials to unlock and open cabinets outfitted with EMLs.

Designing for security

An EASis composed of three primary components: an access control or input device, an electromechanical lock and a system for monitoring the status of the access point. The EML is the most critical element of the system, providing the physical security and intelligence that remote systems rely on for access control and

monitoring. When designing an EAS, it is important that the appropriate EML is designed for the specific enclosure and provides the intelligence, flexibility and security needed at the rack level.

Electronic locks are actuated by external access control devices, which validate user credentials and produce a signal that initiates the EML unlock cycle. Appropriate EMLs can be combined with any access control device from keypads to radio frequency (RF)proximity card systems, biometrics or wireless systems. The access control device can also be integrated into the EML for a streamlined, integrated solution that requires minimal installation preparations.

Each time an EML is actuated, an electronic “signature” is created which can be captured to monitor access –either locally with visual indicators or audible alarms, or remotely over a computer network. The electronic signatures can be stored to create audit trails that can be viewed at any time, whether on- or off-site, to forensically reconstruct a series of access events. This electronic record can store cabinet access activity including location, date, time, duration of access and specific user credentials, allowing security breaches to be dealt with immediately. The remote monitoring capability of an EAS can streamline security administration and reduce risk.

Electromechanical locks provide security down to the rack level, protecting valuable data and IT equipment.

Simplified integration

Electronic access solutions provide datacenters with improved security, increased

convenience and simplified integration with existing electronic control systems. EAS can be designed to suit a variety of retrofit options and enables a simple transition from traditional mechanical locks to electronically engineered locking solutions.

The ability to seamlessly integrate an electronic access solution into an existing access control network extends the datacenter's physical security system down to server racks and IT cabinetry. By managing access privileges electronically, costs associated with complex mechanical key distribution, tracking and replacement can be significantly reduced.

EAS integration provides additional benefits to the datacenter as well. When designing a new cabinet security system or retrofit that incorporates electronic locks and access control devices, current facility security systems can be used to control access to both secure areas and cabinets by using credentials already assigned to datacenter personnel.

EMLs can be linked to security and environmental systems such as IP video cameras and rack monitoring systems to provide additional security and oversight. Additionally, electronic access solutions can be equipped with a mechanical override system to enable access to enclosures in the event of a power failure. A back up power supply, or a simple connection port for an external battery can also be used as an alternative means to operate an EAS.

Conclusion
The threat of unauthorized access and loss continues to be a challenge for datacenter managers. To help eliminate physical and network security concerns, facility managers are turning to engineers, who are meeting demands for more secure locking mechanisms in datacenters by integrating electronic access solutions into cabinet designs.

Electronic locks and latches, combined with appropriate access control devices are an efficient, secure method to safeguard data and IT assets from potential security breaches. The remote monitoring and control capabilities that a rack level electronic access solution provides allows facility security personnel to effectively record physical access to valuable information, resulting in a detailed audit trail to demonstrate security to the organization whose information the datacenter manager must protect.

Southco.com [1]

Electronic Access Solutions (EAS) provide datacenter managerswith a secure means to manage enclosure access. As the human interface of EAS, the electronic access control device is the first line of defense against potential security threats. This chart provides an overview of the relative advantages of each.

Electronic Access Controllers

Technology	Advantage
Keypads	No credential to carry
RF proximity reader	Building integration, good security
Electronic keys	Easy transition, familiarity
Biometrics	No credential to carry, nothing to recall, high security, indisputable link to the user
Remote control	High security with more control over access
Stand-alone systems	Simplified set-up, no software
Network-wired, wireless systems	Simultaneous remote management of multiple access points and credentials

About the author
Steve Spatig is the General Manager for Southco's Electronic Access Solutions (EAS) division. He has worked in the electronics packaging and engineered access industry for over 15 years and holds three patents for engineeredaccess solutions.

Source URL (retrieved on *10/22/2014 - 7:04pm*):
http://www.ecnmag.com/articles/2012/09/electronic-locks-intelligent-access-enhances-datacenter-security?qt-recent_content=0

Links:
[1] http://www.Southco.com