White Paper

Biometric Access Control in Data Centers:

Bullet-Proof Physical Security from the Front Door to Server Cabinets

First Quarter, 2011

Overview

In the quest to protect mission-critical business assets and to satisfy government regulations, data centers are often on the leading edge of security measures. In terms of physical security, data centers within corporate buildings typically feature multiple access control solutions designed to keep most employees out. Private data centers often resemble military installations, with security guards and extensive surveillance in addition to access control at multiple points of passage.

The access control methods used to secure these facilities usually include a mixture of unrelated devices, from palm readers to proximity card readers to mechanical keyed or combination locks. Palm readers, which are too large for server cabinet applications, are commonly found only on doors; server cabinets are most often accessed with keys or key cards.

The use of mixed access control devices that are meant to protect actually creates significant security issues and challenges:

- <u>Complexity of security administration</u>. The use of proximity readers and keyed or combination locks requires careful management of key cards, keys, and combinations. Tracking which users have which access enablers, and reassigning/retrieving them when access needs or personnel change, is a sizable task in large facilities.
- <u>Increased opportunities for breaches</u>. The existence of multiple keys and key cards makes a facility less secure by increasing the number of access enablers that can become separated from their intended carriers, representing an opportunity for access by unauthorized personnel.
- <u>Lack of reliable audit trails</u>. The use of mixed access control devices can make it very difficult, if not impossible, to identify the culprit when a breach occurs, as there is no comprehensive audit trail covering all access points. While palm

Copyright © 2011 Digitus Biometrics

readers can produce audit trails for doors, the use of keys or combination locks on cabinets and elsewhere means some access points have no audit trail at all.

This white paper describes a cost-effective platform and methodology that can greatly simplify security administration, eliminate opportunities for physical security breaches, and provide an indisputable audit trail of access throughout an entire facility, or even multiple facilities, to physically secure business assets and ensure regulatory compliance. The solution involves uniform, networked biometric access control at every critical access point within a data center, from front door to interior doors to server cabinets.

Why Take Uniform Security All the Way to the Server Cabinet?

Data center operators have long understood the need for physical access control on server cabinets. In corporate facilities, where data centers are potentially exposed to a significant number of employees, mission-critical servers must be protected from thumb-drive data theft and from theft of a server itself. Those same considerations apply to colocation facilities, which must also reassure customers that their servers are individually secure within a generally secured facility.

Yet these server cabinets are rarely protected with the same level of security as facility doors. The most common method of physical access control at the server is to enclose it with a cage or cabinet featuring a mechanical keyed lock. Less common are enclosures that feature proximity readers. Both create significant risks.

Keys and keycards can be forgotten, lost, or stolen, and any key or keycard separated from an authorized user represents a potential, undetected security breach. The only thing that's known for sure in cabinet access is that an authorized person's key or keycard, but not necessarily the authorized person, opened the cabinet.

While proximity readers offer an advantage over mechanical keyed locks in that they can produce audit trails, those audit trails are not indisputable. Again, they show only which card opened the lock – but not whose hand held it.

U.S. Air Force Drove Need for Better Access Control at Server Cabinet

In 2010, the U.S. Air Force, which has long used Digitus Biometrics' db Nexus access control units to secure the doors of multiple key facilities and their communications closets, asked Digitus to extend its biometric approach to server cabinets in multiple installations.

The key features of db Nexus units that were to be retained in the server solution included:

- Two-part architecture, with the scanner outside the door connected only to the lock control inside the door, eliminating the possibility of clipping external wires and electrically spoofing the lock.
- Network interface, which enables remote control from a centralized location.
- Real-time monitoring and alerts to computers and phones in the event of an attempted breach.
- 100% accurate audit (log) reports showing exactly who gains access through each unit, and when.

The server cabinet solution Digitus created, db ServerRack, appears to the Digitus Access Software that controls the system as simply another biometric access point on the network. db ServerRack is the functional equivalent of db Nexus; the difference is that rather than mounting on a door, db ServerRack mounts on the server cabinet.

Advantages Specific to Data Centers

In addition to providing extremely accurate identification for access control, db ServerRack offers several key advantages relative to the rack itself and, when paired with db Nexus, to the task of securing the entire data center:

- Simplified security administration. With biometric access control, administration is greatly simplified compared to the mixed-solution environment found in most data centers. There are no keys or keycards to assign, track, retrieve, and reassign. Removing all access privileges is a matter of a few keystrokes within the Digitus Access Software, as is reassigning access to specific areas facility-wide, or even among multiple geographies.
- Reduced opportunities for breaches. Because biometrics eliminates the user of access enablers that can become separated from their authorized users, there are far fewer opportunities for security breaches. The authorized user absolutely must be present for access to be granted at any biometrically controlled checkpoint.
- Indisputable audit trail. Especially of interest in demonstrating compliance with government regulations concerning data storage, biometric access control produces an indisputable audit trail. db ServerRack extends that indisputable

audit trail to the server cabinet. When paired with db Nexus, that audit trail can cover the entire enterprise, recording and reporting each instance of each individual's access from door to door to cabinet, and the exact time of each access – indisputably.

Conclusion: Secure Your Entire Data Center with a Single, Unified Access-Control Platform

Certainly, there are many ways of securing data centers, and many solutions have evolved over time to address access control at doors and server cabinets. The problem is that those solutions evolved separately to address individual access points, rather than addressing the overall needs of the data center. In contrast, db ServerRack and db Nexus were designed with an eye toward overall facility needs, and today are unique in their ability to serve as a single, networked platform to completely secure every access point throughout a data center – from the front door to the server cabinets.

About Digitus Biometrics

Since its founding in 2005, Digitus Biometrics has become the market leader in access security solutions via the application of its highly advanced fingerprint recognition technology, operating software, and unique system configurations.

Today, the company's third generation fingerprint recognition technology provides unparalleled access security solutions in various high-profile installations including government, military, healthcare, educational, and commercial facilities.

Contact:
912.231.8175
info@digitus-biometrics.com
www.digitus-biometrics.com

Qualifying data center professionals can order an evaluation unit directly from Digitus Biometrics and test-drive it for 30 days with no purchase obligation. For more information go to:

http://info.digitus-biometrics.com/testdrive.html

Copyright © 2011 Digitus Biometrics