

Best Practices for Data Center Security - IO



Copyright © 2013 IO Data Centers

IO Blog



Best Practices for Data Center Security

June 28th, 2010 / Sarah / 0 comments

SHARE 

It's time to get physical—as in physically protecting a data center and all of its assets.

The need for ironclad virtual security measures, such as managed firewalls, is well known. Yet physical security is often placed on the back burner, largely forgotten about until an unauthorized party manages to break into or sneak onto a site and steals or vandalizes systems.

As with virtual security, physical protection requires building a multi-layer defense using a variety of tools and techniques. Here's a look at the basic measures employed by a state of the art data center:

External Measures

Entry point. Data centers are generally designed with a central access point that's used to filter employees and visitors into the data center. All requests are vetted by a security guard with an intercom link to ensure that they have a legitimate reason for entering the premises.

Automatic bollards. As an alternative to a guard-controlled gate, automatic bollards can be used at entry points. These short vertical posts pop out of the ground to prevent unauthorized vehicles from driving onto the site. When a vehicle's occupants are verified by a guard, an access card or other secure process, the bollards are quickly lowered to allow the vehicle to enter. When in the lowered position, the top of each bollard is flush with the pavement or asphalt and completely hidden. The bollards move quickly and are designed to prevent more than one vehicle from passing through at any one time.

Closed-Circuit TV. External video cameras, positioned in strategic locations, including along perimeter fencing, provide efficient and continuous visual surveillance. The cameras can detect and follow the activities of people in both authorized and "off limits" locations. In the event someone performs an unauthorized action or commits a crime, digitally stored video can supply valuable evidence to supervisors, law enforcement officials and judicial

authorities. For added protection, the video should be stored off-site on a digital video recorder (DVR).

Internal Measures

Lobby area. A staffed reception desk, with one or more security guards checking visitors' credentials, creates an invaluable first line of access control.

Closed circuit TV. Like their external counterparts, internal cameras provide constant surveillance and offer documented proof of any observed wrongdoing.

Biometric screening. Once the stuff of science fiction and spy movies, biometric identification now plays a key role in premises security. Biometric systems authorize users on the basis of a physical characteristic that doesn't change during a lifetime, such as a fingerprint, hand or face geometry or retina or iris features.

Mantrap. Typically located at the gateway between the lobby and the rest of the data center, mantrap technology consists of two interlocking doors positioned on either side of an enclosed space. The first door must close before the second one opens. In a typical mantrap, the visitor needs to first "badge-in" and then once inside must pass a biometric screening in the form of an iris scan.

Access Control List. Defined by the data center customer, an access control list includes the names of individuals who are authorized to enter the data center environment. Anyone not on the list will not be granted access to operational areas.

Badges and cards. Visually distinctive badges and identification cards, combined with automated entry points, ensure that only authorized people can access specific data center areas. The most common identification technologies are magnetic stripe, proximity, barcode, smart cards and various biometric devices.

Guard staff. A well-trained staff that monitors site facilities and security technologies is an essential element in any access control plan.

Loading and receiving. For full premises security, mantraps, card readers and other access controls located in public-facing facilities also need to be duplicated at the data center's loading docks and storage areas.

Operational areas. The final line of physical protection falls in front of the data center's IT resources. Private cages and suites need to be equipped with dedicated access control systems while cabinets should have locking front and rear doors for additional protection.

Tags: data center, Data Center Access, Data Center Security

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment

You may use these HTML tags and attributes: <abbr title=""> <acronym title=""> <blockquote cite=""> <cite> <code> <del datetime=""> <i> <q cite=""> <strike>

POST COMMENT



www.io.com