Data center physical hacks: How to safeguard equipment in cabinets

Paul Mott, Raritan

Paul Mott is global technical product manager of power solutions at Raritan, Legrand,

If cabinets are not secured, it's akin to paying for a home security service and leaving the family jewelry out on the kitchen table instead of in a safe.

October 10, 2018

On any given day data center managers go through their mental checklists. Security, invariably, makes it to the top of the list:

- The network is secure; assets are shielded from cyberattacks. **Check**. **Check**.
- No one can come into the data center without a smart card or biometrics authentication scan. **Check**.
- There is an audit trail of data center comings and goings. **Check**.
- Alerts are programmed to notify the team if there are security breaches. **Check**.

Security is all about layers of protection, and most data centers do an excellent job of applying layers of defense to protect virtual access and the physical perimeter. But what about the actual equipment sitting inside the data center? Are the servers residing in cabinets protected from physical access?

If cabinets are not secured, it's akin to paying for a home security service and leaving the family jewelry out on the kitchen table instead of in a safe.

Raising the bar at the rack

the entrance. As long as you could reasonably ensure that no unauthorized persons had access to your sensitive digital infrastructure, and as long as you could provide proof of those reasonable measures to auditors - you'd be OK.

Escalating regulatory requirements - such as HIPAA, SOX, PCI DSS 3.2, and SSAE 16 - now require that sensitive systems and data be subject to their own specific protections.

Then there are the risks from within. Internal threats - including human errors - continue to be one of the major causes of downtime in data centers. To help eliminate internal threats requires giving only trusted users access to the specific cabinets that they are authorized to work on.

Most of the security today is focused on keeping people out, but not necessarily focused on tracking what happens inside the data center after the initial security layers at entry.

So it's no longer enough to ensure that only authorized persons enter the data center. You must track and monitor their access to specific sensitive systems and ensure they have the correct rights to a particular area. And you must be able to provide an extensive audit trail regarding who touched those systems when - and what they did each time.

In response, data centers are shoring up rack-level physical security and compliance using a number of approaches:

- Electronic Enclosure Locks that can be administered remotely so that appropriate permissions can be mapped between the right people and the right systems using enterprise security policy and/or ad hoc administration.
- Proximity card authentication that makes it easy for authorized personnel to quickly gain access to enclosures for which they are authorized.
- In-rack cameras that capture live video and photos automatically tagged with relevant data (time, date, user ID, system data, actions, etc.) for audit documentation and forensics.
- Integration with DCIM and/or other access and building control systems to facilitate single point-of-control and easy consolidation of all security/compliance-related audit trails.
- Encryption and detection safeguards to ensure the integrity of rack-level security protections and audit systems.
- Real-time alerting/alarming that notifies appropriate parties of events requiring immediate attention.

It's also important to recognize that your rack-level controls don't exist in a vacuum. They are part of your data center infrastructure management workflows. They feed into your SIEM analytics and forensics. They support delivery of compliance documentation to your organization's internal and external auditors. They can even play a role in other processes - such as the capture and analysis of activity-based data center costs.

Rack-level tools should integrate well with a wide range of associated hardware and software. And the diverse stakeholders in rack-level management - from your front-line tech staff to outside regulators - must have a high level of confidence in the data and controls you provide through those integrations. So, in addition to effectively integrating rack-level tools into your broader security and compliance processes from a technical

Installation of your new cabinet controls should ideally retrofit easily with existing locks and be plug-and-play with existing rack infrastructure, such as PDUs, so that you can leverage existing data center infrastructures - eliminating the cost to install a separate security system, wiring, and network cabling. And, of course, you'll need software that works with your existing DCIM applications, asset tracking systems, LDAP/AD directory services, etc. so that data can be shared. ID badge credentials used with proximity card systems for building access, for example, can be used to establish access privileges down to the cabinet level.

You don't have to engage in a "boil the ocean" overhaul of your data center enclosures to start on the road to better rack-level control and audit. A good pilot program on select enclosures can give you the hands-on insight you need to ensure your success when you're ready to execute a more complete rollout.

Related Stories

- DCD>London: Minkels and Legrand launch Nexpand cabinet
- Virtu files complaint over microwave equipment on NYSE data center roof
- Google Cloud us-east1 data centers disrupted due to "physical damage to multiple fiber bundles"

0 Comments **DatacenterDynamics** 1 **Login**

♡ **Recommend** Tweet f Share **Sort by Best**

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS ?

Name

Be the first to comment.

✉ **Subscribe** 🔒 **Disqus' Privacy PolicyPrivacy PolicyPrivacy**

*Email:

*Country:

Select...

Get the latest news in your inbox:

□ Global (Daily)
□ EMEA (Weekly)
□ North America (Weekly)
□ Asia (Every two weeks)

*I have read and agree to the Terms and Conditions and Privacy Policy

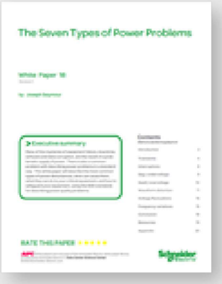
□ Yes, I agree

Submit

Trending Stories

Power consumption in data centers is a global problem	1
Discrimination prevents electrical failures	2
Apex Legends: How a video game supported a million concurrent players on its second day	3
Data center predictions for 2019	4
What you need to know about Azure's Hybrid Use Benefit	5

Resources



The Seven Types of Power Problems

The seven types of power problems

Accelerate Your Energy Strategy With PPAs

01 Feb 2020

Avoiding costs from oversizing data center and network room infrastructure

01 Feb 2020

Data center interconnects reach 400G speeds

29 Jan 2020

More

Data Centre Dynamics Ltd.
102-108 Clifton Street
London EC2A 4HW

Tel. +44 (0)207 377 1907
Fax. +44 (0)207 377 9583
Email.info@datacenterdynamics.com

Products

Conferences // Training // Awards // Certification // Webinars // Magazine

DCD

Management Team // Advertise With Us // Office Locations // Work For Us // Environmental Management // Event News