

Data Center Physical Security

Total Security Means Protecting Your Data Virtually & Physically

WHEN IT COMES TO SECURITY, enterprises tend to focus their efforts on viruses, information leakage, and similar cybersecurity issues, as opposed to physical security issues that focus on protecting the data center and its servers. However, physical security of a data center is as vital as the virtual security.

Why is it so important? “If the data goes, the company goes,” says Shane MacDougall, principal partner at Tactical Intelligence. “That data is a company’s primary asset. Even though data is ethereal that you can’t see or touch, if somebody can schmooze their way into the facility and then walk out with several of your drives or one of your servers, your company just walked out the door.”

In addition, there are a growing number of lawsuits regarding stolen or lost data. “With the increasing data breaches, if your data is stolen and you get sued, chances are you’re going to lose,” MacDougall says. “Maybe 20 years ago, it was unheard of for someone to steal stuff from data centers. Now you hear about it happening too frequently.”

Hide In Plain Sight

MacDougall has designed several data centers, including one for the largest identity theft protection provider in the world. In his experience, the best first step a data center can take toward physical security is to take measures to blend into the surroundings. That means no outdoor signage announcing the data center’s presence or

anything too conspicuous around the building, such as barbed wire fencing, which makes people curious about what might be inside the building. The building itself should also be non-descript.

It’s also wise to keep street addresses and other identifying information off of Web sites, MacDougall believes.

“A great example of a top-notch data center is Oracle’s Austin data center, [which] has all the bells and whistles,” MacDougall says. “Unfortunately, Oracle, in its desire to push how secure its site is, has leaked pretty much every piece of information about all the protections in place. That in itself reduces the security of the site significantly.”

Implement Security Layers

The physical security of the data center should be in rings or layers, according to Mike Clemson, senior director of facilities at Carpathia Hosting (www.carpathia.com). “The outermost ring is often a fence,”

who passes through. For example, Clemson says, “At Carpathia, you can’t park inside the fence line unless you are an employee or a contractor who has to bring equipment into the building.”

The next layer is actual access into the facility. MacDougall recommends that there should be a minimal number of entrances into the facility. Ideally, he says, there will be only one entrance where all access is verified and monitored, preferably by a guard. “This access point should involve a man trap of some sort,” he says. A man trap is a fairly low-tech but highly effective means of security: two sets of doors very close together that only one person can go through at a time. This prevents a second person without proper credentials from sneaking in when the doors are open.

Although man traps may be low-tech security, data centers are also utilizing some very high-tech security methods, such as smartcards and biometrics or a

Key Points

- A data center’s physical security is as vital as its virtual security.
- The physical security of the data center should be in rings or layers.
- The proprietary cage may be the best piece of security within the data center.

means we don’t have to go through videotape to find a particular bit of footage.”

Protect The Equipment Itself

Although there may be several layers of security before anyone can even get to the server rooms, both Clemson and MacDougall recommend taking extra security measures for the servers themselves.

“Servers can be put in cages,” says MacDougall. “In a lot of data centers, you’ll see shared cabinets and racks, and a lot will have sections where they are

“With the increasing data breaches, if your data is stolen and you get sued, chances are you’re going to lose.”

- Tactical Intelligence’s Shane MacDougall

he says. But what and who you let inside the fence needs to be taken into consideration. Some data centers have gated parking lots with a security guard monitoring

combination of the two. Proximity smartcards or biometric scanners can be used not only at entrances onto the property, but also throughout the facility to ensure that only authorized personnel are allowed into specific areas. And because the price of using biometrics has become so reasonable, MacDougall says there is no reason not to use the technology. “Biometrics is the most secure method of authentication that you can put out there for physical security,” he says.

Using CCTV (closed-circuit television) to monitor doors, hallways, and the facility’s grounds has long been a staple in data center security, but as Clemson says, it is the area of security that has seen the most change in recent years. “Old CCTV systems were analog,” Clemson says. “Now they use digital feeds. That enables playback to be handled more cleanly and

caged off, where you need a special key or a proximity card to get in and out of the cage.”

MacDougall especially suggests that individual clients within a hosted data center have their own security systems within the locked cage. “That way, you aren’t just depending on the facility, but you have your own backup security system,” he says.

In fact, the cage may be the best piece of security within the data center. “The reality is, once someone is able to socially engineer their way inside a center, all bets are off,” MacDougall says. Once inside, the person is going to find a way to get access to unprotected servers. However, a server locked in a cage is usually set up so that the data center staff needs to contact the client before accessing the server and get permission. ■

Test Your Access Control

Above all, access control is the most critical part of the physical security plan. “The data center manager has to have a solid procedure in place when it comes to visitors or granting access into the facility,” says Mike Clemson, senior director of facilities at Carpathia Hosting (www.carpathia.com). “They have to have a security team that does not make exceptions or allow people to socially engineer their way into the facility.”

Clemson says he has hired someone who is scheduled to break into his site several times a year. He doesn’t have any idea when it is happening, but rather, he gets a report from his security team that a breach has been attempted.

“If you don’t have a tight policy and you don’t test your people,” Clemson says, “you don’t know if you can actually keep your data center safe.”

Broadband Carriers Providing Service That’s Closer To Advertised Speeds

U.S. broadband providers are measurably more accurate in the speeds they’ve been advertising lately, according to a new report from the Federal Communications Commission.

This year’s “Measuring Broadband in America” study focused on 13 of the country’s biggest ISPs serving 86% of U.S. wireline broadband subscribers. It polled users on their actual home download and upload speeds as measured by standard testing mechanisms. The goal was to scientifically ascertain real-world broadband speeds for comparison with carriers’ advertised data rates.

“During the FCC’s development of the National Broadband Plan, we reported evidence from 2009 that actual broadband speeds significantly lagged behind advertised speeds. That’s why, as part of the FCC’s Consumer Empowerment Agenda, we’ve been working to arm consumers with information to help them make smart choices about the broadband service that’s right for them,” said FCC chairman Julius Genachowski in his remarks on the new report.

“First, we found that most major ISPs are providing service close to what they’re advertising. This represents a

significant improvement over the findings from two years ago,” Genachowski said. “While there are some differences between technologies, DSL, cable, and fiber-to-the-home are all delivering quality service generally consistent with what they advertise.”

On average, and during peak hours, fiber-to-the-home services provided 114% of advertised download speeds and 112% of advertised upload speeds, the report says. Cable broadband supplied 93% download and 108% upload advertised speeds, and DSL provided 82% download and 95% upload speeds.

“Another finding was that during peak hours—7 p.m. to 11 p.m.—broadband performance generally decreases somewhat,” Genachowski said. “But most services still provide actual speeds that are 80 to 90% of advertised speeds or better.”

Making Informed Decisions

The FCC also announced a new online guide to walk consumers through the process of choosing a broadband service to fit their needs. The guide also explains important broadband terminology in plain English, according to the chairman. Of course, the guide can also bring new IT

decision-makers up to speed when it’s time to evaluate the broadband needs of branch offices and the like.

“The more consumers know about broadband speeds and the more they know about the speeds they receive, the more able they are to let providers know what they really want,” Genachowski said. “Information for consumers enhances competition among providers of broadband Internet access services and increases the likelihood that consumers will be better served and receive greater value.”

