Selecting a Co-Location Facility:

Ensuring Physical Security in a Shared Environment

Michael A. Pease

GIAC Security Essentials Project

9 September 2000

Introduction

The demand for space in internet data centers is growing at an exponential rate. The US hosting market alone is expected to grow from almost $1 Billion in 1999, to over $19 Billion in 2003[1]. This growth can bring tremendous benefits to web based businesses in the form of reduced operating expenses. However, these savings do not come without a certain degree of risk. Before placing your company's equipment in any facility, make sure you are satisfied with the level of protection offered. The market growth will attract all types of people, and not all telco hotels will be the Ritz Carlton.

It would not be realistic to expect to find a completely risk free environment, but steps can be taken that will minimize the risks to your corporate assets. When protecting a network, defense-in-depth is a common strategy. By providing multiple layers of protection, you are able to defend the confidentiality, integrity, and availability of your systems. The same strategy can also be applied in a co-location facility.

Availability

Often, the greatest concerns when selecting a co-location facility relate to availability and the physical environment. Prior to installing your equipment in any hosting facility, you should conduct a thorough site survey. Is there a clean, redundant power supply with emergency backup? Are temperature and humidity kept at levels that are acceptable? These concerns are addressed in a relatively uniform fashion through out the industry, but there are other factors that can impact availability too. How do your internet connections get into the facility? Is the carrier's equipment secure, or can anyone get access to it? Does the carrier have more than one path into the building? It won't do you much good to have generators in the event of a power loss, if the same backhoe that caused the power outage also severed the only fiber that feeds the building. Ideally, the carrier should have secure, diverse paths into the facility. There is a growing trend in deploying "Neutral" hosting facilities, where the customer has more than one carrier available to provide the needed bandwidth[2]. Now you can order your circuits from separate providers, eliminating a single point of failure.

Another facility related issue that can impact availability is the fire suppression system. If it is a water-based system, is it dry or wet? In a wet system, there is water in the sprinkler pipes all the time. If a sprinkler head is accidentally triggered or broken, equipment will get wet. A dry, pre-action system, offers a safer alternative. If there are portable fire extinguishers, are they dry chemical or a halon-type agent? A dry chemical extinguisher discharges a cloud of fine particles that can be very damaging to electronic equipment. Many facilities are being built in former warehouses that were equipped with deluge sprinkler systems, meaning that all the sprinkler heads were open all the time. If the system was activated, everything got wet. Was the old sprinkler system upgraded? Finally, if there is a water-based system, is it designed to provide effective coverage without damaging equipment not directly affected by the fire?

Confidentiality

"Confidentiality, the act of keeping things hidden or secret, is one of the primary goals of computer security practioners."[3] Maintaining confidentiality in a shared facility can be difficult. Access control could be a little as pulling open a door, or as elaborate as using biometric devices to confirm an individual's identity prior to granting access. Access control should be done in layers. A primary component in any access control system should be an Access Control List. The ACL should specify who is permitted to access your equipment, along with any restrictions on that access. The ACL should also state who is allowed to make changes to the list, and under what circumstances. If you are in a common area with other customers, how will your cabinets be secured? There are many types of locks available now, including models that keep an internal log that can be audited on a regular basis. All entry points into the facility should be alarmed, and there should be video monitoring, with recording, throughout the building. Finally, look at the site staff that works there. Are they familiar with their own security policies and procedures? Do they leave doors propped open and tools and equipment unprotected? How they treat their own equipment could be a good indication of how they will treat yours. These are the people that are going to be around your equipment on a daily basis, make sure that thought isn't going to keep you up at night.

Integrity

Now that we've secured our equipment, and limited who has access to it, we should be pretty safe, right? Wrong! How are your circuits getting from the provider to you? If someone were able to access your circuits, they may not even need to get to your equipment. If you are in a raised-floor environment, ask if the floor panels are alarmed. Also, find out who will have access to the cabling. Do you really want your competitor crawling over your connections? "Accidents" can happen, leaving connections cut, unplugged, or even moved. Use the site staff to help you maintain the integrity of your system. Develop a professional relationship with them. Keep them update on issues that may impact them, such as personnel changes. Talk to them, discuss any concerns you may have with them. The better run facilities will welcome customer feed back, and through these discussions you will build a good working relationship with them. That may just pay off when they happen to notice an unknown face tinkering with your equipment. Finally, look at your own operations. Your own personnel can present the greatest threat to your systems' integrity. This also applies to any contractors that may be working for you. Make sure your staff isn't inadvertently giving away critical information to anyone who walks by. If I'm looking at someone's equipment as I walk past, and see an IP address on a label over their sever, and a login name on a monitor that wasn't turned off, I won't have very much work to do to access that system. To bad they didn't leave their password. What's on that Post-It note on the floor?

Conclusion

The current trend in Internet co-location facilities could have a tremendous impact on electronic commerce. There will always be people who will look for an easy dollar. There are no risk free endeavors, but if the same principles that are used to secure our networks in our own companies are applied to co-location facilities, the risks can be minimized. Military strategists have used defense-in-depth for centuries, and we use the same principles when securing our networks. These techniques can be applied quite effectively in a co-location environment. Avoid facilities that don't provide the level of protection that you expect for your mission critical assets. Make sure your concerns and questions are addressed prior to installation. Develop a professional, working relationship with site staff. The key to securing your assets in an open environment is to take a coordinated approach in planning and providing security.[4] An effective security program is dynamic, don't forget to re-evaluate on a regular basis and make any changes that may be necessary.

[1] "IDC Expects US Companies to Increase Their Web Hosting Services Revenues by Almost $1 Billion in 1999." 4 January 2000. URL http://www.idc.com/communications/press/pr/CM010400PR.stm (9 Sept. 2000)

[2] Masud, Sam. "Neutral Internet Exchanges on the Rise." Telecommunications Online. July 2000. URL http://www.telecommagazine.com/issues/200007/tcs/neutral.html (9 Sept. 2000)

[3] Hollbrook, P., and Reynolds, J. "Site Security Handbook." RFC 1244. July 1991. URL http://www.ietf.cnri.reston.va.us/rfc/rfc1244.txt?number=1244 (9 Sept. 2000)

[4] Zyskowski, John. "A need for commitment." 4/10/2000 URL http://www.fcw.com/fcw/articles/2000/0410/sec-edit-4-10-00.asp (2 Sept. 2000)