GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Data Center Physical Security Checklist
Sean Heare
December 1, 2001

Abstract

This paper will present an informal checklist compiled to raise awareness of physical security issues in the data center environment. Information Security Specialists should use this checklist to ascertain weaknesses in the physical security of the data centers that their organization utilizes.

In a "Defense-in-Depth" security model, physical threat vectors are often the most vulnerable and overlooked (Schneier, 284). Physical penetration offers the hacker or malicious user access to sensitive data with less technical acumen making it a tempting attack method (Schwartau, 112). Social engineering, Shoulder surfing and physical access to console ports are all facilitated (118-119). Dumpster diving by definition involves a breach of physical security.

People are not the only physical threat. Disaster recovery also falls under the purview of physical security. In other words, e-mail should not be lost because there is a flood in the basement (Mason, 1).

Definitions and Assumptions

According to searchdatabase.com:

"[A] data center (sometimes spelled datacenter) ... is a specialized facility that houses Web sites and provides data serving and other services for other companies.

This kind of data center may contain a network operations center (NOC), which is a restricted access area containing automated systems that constantly monitor server activity, Web traffic, and network performance and report even very slight irregularities to engineers so that they can spot potential problems before they happen...In a company, data center is a term sometimes used to describe the central data processing facility."

The NCSC Glossary of Computer Security Terms defines physical security as "[t]he application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information."

A more verbose definiton of physical security is:

*"[T]he protection of building sites and equipment (and all **information** and **software** contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee). It requires solid building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders." (Safeguarding, 5:1)*

Both these definitions fail to bring site location in as a factor in determining how physically secure a site is from threats to the "sensitive information" contained therein. For the purposes of this checklist consider the definition of Physical Security to encompass both the above definitions with some attention paid to site location as a physical security factor.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 (Bradner, 1).

Caveats

Information Security Specialists and their management teams will need to ascertain their organizations need for physical security versus the costs involved. A small enterprise will have to either lease space from a data center or place data center space in a building with other offices.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Furthermore some risks on this list may not be relevant to the particular data center being tested. For example a fence around the perimeter of the building is not practical in an urban setting. The checklist items listed as MUSTs are therefore few and far between, and are only listed because without them very few other security measures would be of much use. Information Security Specialists will put different weight on different items in the checklist according to their own organizations needs. This checklist is not a comprehensive physical security checklist. It merely provides a reasonable starting point in regards to physical security for a data center.

Always obtain written permission from proper management before performing security testing of any kind. Ensure that all the testing peformed (physical penetration, fire control, social engineering) is outlined explicitly in the permission received from management.

Data Center Management may require that a Non-Disclosure Agreement be signed because of the potential exposure of security procedures. This checklist, as designed, only covers the physical aspects of your security setup. You will need other checklists to secure networks, operating systems, applications and other potential targets.

Using the checklist

The checklist is broken into two sections, property and people. Property includes, but is not limited to the building, infrastructure, servers, laptops and data. People is further broken down into users and outsiders. Users are employees, clients and others who need access to business data. Outsiders are those who are not directly employed by the business. Cleaning crews, security guards, and service engineers are examples of outsiders.

Property Section - Place a check by each item that passes.

1.1 Site Location

____ 1.1.1 Natural Disaster Risks
The site location SHOULD be where the risk of natural disasters are acceptable. Natural Disasters include but are not limited to forest fires, lightning storms, tornadoes, hurricanes, earthquakes and floods. ComputerSite Engineering, Inc. has compiled a Natural Disaster Risk Profile Map for Data Centers.

____ 1.1.2 Man-Made Disaster Risks
The Site Location SHOULD be located in an area where the possibility of man-made disaster is low. Man-made disasters include but are not limited to plane crashes, riots, explosions, and fires. The Site SHOULD NOT be adjacent to airports, prisons, freeways, stadiums, banks, refineries, pipelines, tank farms, and parade routes.(Newton, par. 4-6), (Natural, par. 21-23)

____ 1.1.3 Infrastructure
The electrical utility powering the site SHOULD have a 99.9% or better reliability of service. Electricity MUST be received from two separate substations (or more) preferably attached to two separate power plants. Water SHOULD be available from more than one source. Using well water as a contingency SHOULD be an option. There MUST be connectivity to more than one access provider at the site.(Natural, par. 27)
____ 1.1.4 Sole purpose
A data center SHOULD NOT share the same building with other offices, especially offices not owned by the organization. If space must be shared due to cost then the data center SHOULD not have walls adjacent to other offices. (Harrison, 12)

1.2 Site Perimeter

____ 1.2.1 Perimeter
There SHOULD be a fence around the facility at least 20 feet from the building on all sides. There SHOULD be a guard kiosk at each perimeter access point. There SHOULD be an automatic authentication method for data center employees (such as a badge reader reachable from a car). The area surrounding the facility MUST be well lit and SHOULD be free of obstructions that would block surveillance via CCTV cameras and patrols. Where possible, parking spaces should be a minimum of 25 feet from the building to minimize damage from car bombs. There SHOULD NOT be a sign advertising

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

that the building is in fact a data center or what company owns it.
____ 1.2.2 Surveillance
There SHOULD be CCTV cameras outside the building monitoring parking lots and neighboring property. There SHOULD be guards patrolling the perimeter of the property. Vehicles belonging to data center employees, contractors, guards, and cleaning crew should have parking permits. Service engineers and visitor vehicles should be parked in visitor parking areas. Vehicles not fitting either of these classifications should be towed.
____ 1.2.3 Outside Windows and Computer Room Placement
The Site Location MUST NOT have windows to the outside placed in computer rooms. Such windows could provide access to confidential information via Van Eck Radiation and a greater vulnerability to HERF gun attacks. (Schwartau, 138-147, 184-189) The windows also cast sunlight on servers unneccesarily introducing heat to the computer rooms. Computer rooms SHOULD be within the interior of the data center. If a computer room must have a wall along an outside edge of a data center there SHOULD be a physical barrier preventing close access to that wall.

____ 1.2.4 Access Points
Loading docks and all doors on the outside of the building should have some automatic authentication method (such as a badge reader). Each entrance should have a mantrap (except for the loading dock), a security kiosk, physical barriers (concrete barricades), and CCTV cameras to ensure each person entering the facility is identified. Engineers and Cleaning Crew requiring badges to enter the building MUST be required to produce picture ID in exchange for the badge allowing access. A log of equipment being placed in and removed from the facility must be kept at each guard desk listing what equipment was removed, when and by whom.

Security Kiosks SHOULD have access to read the badge database. The badge database SHOULD have pictures of each user and their corresponding badge. Badges MUST be picture IDs.

1.3 Computer Rooms

____ 1.3.1 Access
There SHOULD be signs at the door(s) marking the room as restricted access and prohibiting food, drink, and smoking in the computer room. There SHOULD be an automatic authentication method at the entrance to the room (such as a badge reader). Doors should be fireproof. There SHOULD only be two doors to each computer room (one door without windows is probably a violation of fire code).

Access should be restricted to those who need to maintain the servers or infrastructure of the room. Access should be restricted to emergency access only during moratoriums for holidays. Service Engineers MUST further go to the NOC to obtain access to computer room badges.

____ 1.3.2 Infrastructure
Computer Rooms should be monitored by CCTV cameras. Each computer room SHOULD have redundant access to power, cooling, and networks.
There should be at least an 18" access floor to provide for air flow and cable management. Computer rooms should have air filtration. Computer rooms should have high ceilings to allow for heat dispersal.(Level, 1)
____ 1.3.3 Environment
Each computer room SHOULD have temperature between 55 and 75 degrees farenheit and a humidity of between 20 and 80 percent.(Safeguarding, 5:2) Environmental sensors should log the temperature and humidity of the room and report it to the NOC for monitoring and trend analysis(Level, 1).
____ 1.3.4 Fire Prevention
There SHOULD be a Halon or other total flooding agent solution in place in each computer room. There MUST be fire extinguishers located in each computer room. There MUST be emergency power off switches inside each computer room. There MAY be respriators in computer rooms. There MUST NOT be wet pipe sprinkler systems installed.
____ 1.3.5 Shared Space
If the space is being leased then the computer room will probably be shared space. A clause should be entered into the lease stating that competitors of the business may not have equipment located in the same computer room. Lists of clients utilizing the same room should be monitored to ensure compliance. Computer equipment in shared spaces MUST at a minimum be in a locked cabinet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1.4 Facilities

____ 1.4.1 Cooling Towers
There MUST be redundant cooling towers. Cooling towers MUST be isolated from the Data Center parking lot.
____ 1.4.2 Power
There MUST at least be battery backup power onsite with sufficient duration to switch over to diesel power generation. If there is no diesel backup then there should be 24 hours of battery power. There SHOULD be diesel generators on site with 24 hours of fuel also on site. A contract SHOULD be in place to get up to a week of fuel to the facility.
____ 1.4.3 Trash
All papers containing sensitive information SHOULD be shredded on site or sent to a document destruction company before being discarded. Dumpsters SHOULD be monitored by CCTV.
____ 1.4.4 NOC
The NOC MUST have fire, power, weather, temperature, and humidity monitoring systems in place. The NOC MUST have redundant methods of communication with the outside. The NOC MUST be manned 24 hours a day. The NOC MAY monitor news channels for events which effect the health of the data center.

1.5 Disaster Recovery

____ 1.5.1 Disaster Recovery Plan
The data center MUST have a disaster recovery plan. Ensure that the plan addresses the following questions:
What constitutes a disaster? Who gets notified regarding a disaster and how? Who conducts damage assessment and decides what back-up resources are utilized? Where are backup sites located and what is done to maintain them on what schedule? How often and under what conditions is the plan updated?
If the organization does not own the data center what downtime does the service level agreement with the center allow?
A list of people within the organization to notify MUST be maintained by the NOC of the data center including pager, office, home, and cell numbers and Instant Message Names if available (Derbort, Gallagher, Girard, et al., par 3). How often are those people updated? (MIT, 7-9)
____ 1.5.2 Offsite Backup
There MUST be regular offsite backups of essential information. There must be a backup policy in place listing the procedure for restoring from backup and allowing for the scheduling of practice runs to test that the backups work.(Windows, 24-25)
____ 1.5.3 Redundant Site
Redundant servers MAY be set up in another data center. If these are set up then they must be tested during a "dry run" to ensure that they will switch over properly during a disaster. (Derbort, Gallagher, Girard, et al., par 7)

People Section - Place a check by each item that passes.

2.1 Outsiders

____ 2.1.1 Guards
Security guards SHOULD submit to criminal background checks. Guards SHOULD be trained to follow and enforce physical security policy strictly (for example ensuring that everyone in the facility is wearing a badge).
____ 2.1.2 Cleaning Staff
Cleaning crews SHOULD work in groups of at least two. Cleaning crew SHOULD be restricted to offices and the NOC. If cleaning staff must access a Computer Room for any reason they MUST be escorted by NOC personnel.
____ 2.1.3 Service Engineers
Service Engineers MUST log their entering and leaving the building at the entrance to the building. The NOC SHOULD log their badge exchange to access a computer room.
____ 2.1.4 Visitors
Visitors MUST be escorted by the person whom they are visiting at all times. Visitors MUST NOT be allowed access to a computer room without written approval from data center management. All visitors who enter Computer Rooms must sign Non Disclosure Agreements.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2.2 Users

____ 2.2.1 Education
Users must be educated to watch out for potential intruders who may shoulder surf or directly attempt social engineering. Users should be educated on securing workstations and laptops within the facility and laptops outside the facility (Palmer, 1), awareness of surroundings, and emergency procedures.
____ 2.2.2 Policy
All users at the facility must sign Non Disclosure Agreements. A Physical Security Policy SHOULD be signed by each user and enforced by security guards.

2.3 Disaster Recovery

____ 2.3.1 Organizational Chart
An organizational chart should be maintained detailing job function and responsibility (Derbort, Gallagher, Girard, et al. [2], par. 7). Ideally the org chart would also have information on which functions the worker has been cross trained to perform.
____ 2.3.2 Job Function Documentation
"It's not enough to document only what your current employees know at the moment about existing systems and hardware. All new work, all changes, must be documented as well."(Derbort, Gallagher, Girard, et al., par 7)
____ 2.3.3 Cross Training
Data Center employees should be cross trained in a number of other job functions. This allows for a higher chance of critical functions being performed in a crisis. (Derbort, Gallagher, Girard, et al., par. 7)
____ 2.3.4 Contact Information
A contact database MUST be maintained with contact information for all Data Center employees. (Derbort, Gallagher, Girard, et al., par. 3)
____ 2.3.5 Telecommuting
Data Center employees should regularly practice telecommuting. If the data center is damaged or the ability to reach the data center is diminished then work can still be performed remotely. (Derbort, Gallagher, Girard, et al. [2], par. 3)
____ 2.3.6 Disparate Locations
If the organization has multiple Data Centers then personnel performing duplicate functions should be placed in disparate centers. This allows for job consciousness to remain if personnel at one center are incapacitated. (Derbort, Gallagher, Girard, et al. [2], par. 3)

Works Cited

Bradner, S. "Key words for use in RFCs to Indicate Requirement Levels." IETF RFC Repository. Mar. 1997. <http://www.ietf.org/rfc/rfc2119.txt?number=2119>.
"Data Center." SearchDatabase.com. 14 Nov. 2000 <http://searchdatabase.techtarget.com/sDefinition/0,,sid13_gci332661,00.html>.
Derbort, Gallagher, Girard, et al. "The People Principles: 10% Solution". Baseline. 29 Oct. 2001. 30 Nov. 2001 <http://www.baselinemag.com/article/0,3658,s%253D25064%2526a%253D16921,00.asp>.
---. "The People Principles: 25% Solution". Baseline. 29 Oct. 2001. 30 Nov. 2001 <http://www.baselinemag.com/article/0,3658,s%253D25064%2526a%253D16922,00.asp>.
Harrison, H. The Stainless Steel Rat. New York: Ace, 1961.
Level 3 Design Characteristics. Ellerbe Becket. 3 May 2000. <http://www.eb-datacenters.com/dtf/level3.html>.
MIT Recovery Plan Master. Massachusetts Institute of Technology. 1995 <http://web.mit.edu/security/www/pubplan.htm>.
Natural Disaster Risk Profiles for Data Centers. ComputerSite Engineering, Inc. 30 July 1998 <http://207.201.136.39/csepages/csemap.html>
Mason, I. "UK Lab out of Contact Due to Flood". bionet.organisms.zebrafish. 3 Nov. 1999. 30 Nov 2001 <http://groups.google.com/groups?q=basement+flood+server+water&hl=en&rnum=10&selm=7vqgu6%24so9%40net.bio.net>
Newton, J. "Designing a Data Center". WebTechniques 30 Aug. 2000, 30 Nov. 2001 <http://www.webtechniques.com/archives/1999/08/newton/>

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Palmer, T. "Basic Travel Security Revisited". Sans Institute Information Security Reading Room 6 Aug. 2001. 30 Nov. 2001 <http://www.sans.org/infosecFAQ/travel/sec_revisited.htm
Safeguarding Your Technology, NCES Publication 98-297. National Center for Education Statistics. 18 Nov. 1998.<http://nces.ed.gov/pubs98/safetech/chapter5.html>.
Schneier, B. Secrets and Lies: Digital Security in a Networked World. New York: Wiley and Son, 2000.
Schwartau, W. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth, 1994.
Substitutes for Halon 1301 as a Total Flooding Agent as of November 11, 2000. Environmental Protection Agency. 11 Nov. 2000. <http://www.epa.gov/docs/ozone/title6/snap/lists/flood.html>
United States. Department of Defense. National Computer Security Center. Glossary of Computer Security Terms. Washington: GPO, 1988.
Windows Backups. The Sans Institute. 3 August 2001.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.