Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Building the Ideal Web Hosting Facility: A Physical Security Perspective

Defense in Depth is a wonderful ideal, but it's also a costly one, particularly when dealing with Physical Security. While it is easy to maintain high standards when using a hypothetical model, Physical Security implementations in the real world generally fall well short of this ideal. Compromises are made regarding the site, the building, and the desired security measures. Lesser devices are substituted for the desired ones, all in the name of keeping to the budget. At the worst extreme, you may find that you're not e...

Copyright SANS Institute

Author Retains Full Rights

AD

Building the Ideal Web Hosting Facility:

A Physical Security Perspective

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Abstract

Introduction

Choosing a Site

Building Design and Construction

External Security

Internal Security

Personnel

Disaster Recovery

Conclusion: The Ideal vs. The Real

References

© SANS Institute 2001, Author retains full rights

Abstract

[Return to Table of Contents]

Defense in Depth is a wonderful ideal, but it's also a costly one, particularly when dealing with Physical Security. While it is easy to maintain high standards when using a hypothetical model, Physical Security implementations in the real world generally fall well short of this ideal. Compromises are made regarding the site, the building, and the desired security measures. Lesser devices are substituted for the desired ones, all in the name of keeping to the budget. At the worst extreme, you may find that you're not even able to fully control access to your facility.

Natural or man-made disasters can always be counted on to bring Physical Security to the forefront of everyone's minds, and it is to be hoped that many companies will then begin the process of reviewing, creating and implementing better Physical Security standards. Past history, however, has shown that once the initial event recedes further into the past, companies go back to their old ways and forget these hard-learned lessons. Perhaps now, with the recent effects and threats of global terrorism all too obvious, this will change and comprehensive physical security implementations will become as commonplace as firewalls

Introduction

[Return to Table of Contents]

The purpose of this paper is to provide a comprehensive look at Physical Security by means of building an ideal web hosting facility. By viewing this design and construction process from a Physical Security perspective, we will identify and describe the measures needed to make our facility fully secure. Along with this we should, as an end product, have a comprehensive Physical Security Primer that can be used in many types of facilities and circumstances.

First, it would be best to define Physical Security. The following, from Garfinkel's and Spafford's Practical Unix and Internet Security, is my preferred definition. Physical Security is not something that can be easily and strictly defined, and their definition demonstrates this well.

> "'Physical Security' is almost everything that happens before you (or an attacker) start typing commands on the keyboard. It's the alarm system that calls the police department when a late-night thief tries to break into your building. It's the key lock on the computer's power supply that makes it harder for unauthorized people to turn the machine off. And it's the surge protector that keeps a computer from being damaged by power surges."[1]

With that wide-open definition in mind, we'll begin our journey through the design and construction of our facility. Along with identifying the pertinent Physical Security requirements at each step, we'll also look at some of the commercially available products that'll fit our evolving physical security specifications. Finally, with our ideal web hosting facility completed, we'll discuss some real world Physical Security implementations, focusing on where and why they fell short as compared to our ideal.

Choosing a Site

[Return to Table of Contents]

The first Physical Security consideration is the building site. Long before any concrete is poured, we must have ensured that our site meets all Physical Security specifications. Any proposed site must meet the following minimum requirements:

[1] Garfinkel, Simson and Spafford, Gene, Practical Unix & Internet Security, O'Reilly and Associates, 1996, page 357

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Conveniently Available Utilities (Electricity, Water, Sewer, Gas, Telephone, Fiber).
- The facility must not be located in a flood, earthquake, hurricane, or tornado prone area.
- Interstate Highways, Railroads, Landfills, Feedlots, & Lakes must be at least two miles away.
- It must be built as a freestanding building on a lot sized to provide adequate buffer space between it and any outlying buildings or roads.
- Any Nuclear Plants must be a minimum of ten miles away (preferably 50 miles away).
- Military Bases, Munitions, Embassies, & Research Labs must be at least five miles away.
- Gas Stations, Self-Storage Facilities, Water Towers, & Substations must be a minimum of one mile away.
- Emergency Services must be within five miles (Police, Fire, Medical, Etc.).
- No Subsurface Soil Contamination.
- Limited Fire Hazards (No Dry Forest/Grass Lands or Periodic Hot, Dry Winds) and no Other Limited Hazard Exposures (No Nearby Wetlands, Protected Habitats, Etc).
- Moderate Temperature/Climatic Extremes (20-95°F, $\leq$ 4 Days/Yr Freezing Rain)

Only when our site has met all of these requirements, can we move on to the Design and Construction phase.

Building Design and Construction

[Return to Table of Contents]

The building design as well as the required construction materials must be chosen with Physical Security as a prime requirement, particularly as regards the walls, roof, windows, and entrances. Form must follow function — the building's appearance must be secondary to its security requirements. Indeed, the less the building calls attention to itself, the better.

A good source of guidance in selecting our design, is "The Director of Central Intelligence Directive 1/21: Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF)", which provides the government's specifications for constructing disaster and blast resistant facilities. A comprehensive Physical Security Checklist can be found at http://www.eb-datacenters.com/tech/sec1198-list.html. Some of the design elements we must include in our Design and Construction considerations are:

- Full-Height, One-Hour Fire-Rated Walls Around Complete Perimeter
- Penetration Resistant Perimeter Wall Construction
- Windowless Perimeter or Interior Barriers at External Windows
- RFI/EMI Shielding (TEMPEST)
- Anti-Concealment Landscaping and Architecture
- Physical Barriers for Site Perimeter and External Facility Environmental Equipment

The design must provide the maximum protection to the server farms. To this end, we will use a building within a building design wherein the server farms are placed at the center of the building, with office or utility areas surrounding them on all sides. The server farms will be built in a bunker style, with reinforced, lead filled concrete walls, which will prevent any computer electrical signals from getting outside of the building. All doorways will be constructed with concrete block above and below. In any areas where concrete block isn't feasible, hardened steel

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

mesh will be placed within the construction material, e.g. drywall. This mesh will also be installed at regular intervals under the raised floors and in the space between the server farm ceiling and the building roof. The server farm ceiling will be made of the same material as the roof and there will be nothing intervening between the ceiling and floor.

As mentioned earlier, the utility areas will form one of buffers surrounding the server farms. Here is we'll find our main electrical systems, diesel generators and plumbing. Additionally, utility shafts will also be located between each server farm to house the fire suppression and environmental equipment. This points up another basic Physical Security design principle—to completely segregate any ancillary equipment from the server farms. Electricians, plumbers, and other utility technicians will access their equipment without ever entering the server farm. The only exception to this are the Power Distribution Units, which by design, must be located inside the server farm with the computer equipment.

Another value of this design is that we can sandwich the server farms with redundant environmental and fire suppression equipment within the utility shafts. Should one shaft become disabled, the other side will continue providing an N + 1 level of protection.

Finally, within the utility area we will build two loading areas. This will allow a separate area for those vendors with clearance and another for those without it. The security arrangements for these areas will be discussed in more detail in the Internal Physical and Environmental Security section.

The remainder of our buffer area will be provided by office space for the engineers.

External Security

[Return to Table of Contents]

We've got our facility built, but now we need to turn our attention to its defenses. We'll begin with our external security requirements. We want to create multiple layers of security, e.g. Defense in Depth. A good choice for our outermost layer is a fence such as the INNO-FENCE from Magal Security Systems Ltd. (http://www.magal-ssl.com/pages/innofence.asp), so named for its innocent looks. An alarm will be sounded if a force of 88 pounds or more is applied to the fence; or if a gap of 8.7 inches or more is created between any of the vertical bars.

An intrusion detection system will provide our next barrier. Magal Security Systems provides us a good example with their Permitrax product, (http://www.magal-ssl.com/pages/Perimitrax.asp), an intrusion detection sensor that generates an invisible electromagnetic field around buried sensor cables.

A camera system covering the entire exterior of the facility and, in particular, recording all license plate numbers of vehicles entering the facility, is also required. Turning again to Magal Security Systems, we find the DTS-1000, (http://www.magal-ssl.com/pages/DTS1000.asp), an advanced digital video intrusion detection and tracking system specifically designed for outdoor applications and capable of detecting and tracking several targets per camera.

Only delivery and security vehicles will be allowed within the security perimeter. Staff and visitors will have a separate parking area located outside of the fence.

All entrances must be secured. This can best be done using a combination of smart cards, biometric devices, and man-traps. Each employee is issued an ID card and a Personal Identification Number (PIN). The first entry level then requires that you swipe your card through the reader and then enter your PIN, generally within a proscribed length of time. These systems will also provide an audit trail of all entering and will allow a limited number of failed attempts before locking the card out.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

As this method is prone to the unauthorized use of cards, the next level uses biometrics for authentication. These offer a choice of fingerprint readers, palm readers, retinal scans, and voice identification. As fingerprints alone can be copied, my preference is either a palm reader or retinal scanner. The palm reader needs a live hand to provide the necessary amount of pressure for authentication and the retinal scanner requires the correct eye to be scanned. While both can be hoaxed, the degree of difficulty is quite high.

There is still one major gap in our entrance security. Neither of the previous methods will stop an unauthorized person from piggybacking in with or without the cooperation of an employee. A man-trap, an arrangement of two locked doors with only enough space between for one person, will close this gap nicely. A card reader and a biometric device will be used at both the entrance and the exit to the man-trap along with constant camera observation. Additional sensors may be considered to detect an extra set of feet, the presence of metal or explosives, etc. If the building is small enough, only one entrance should be available for employees and visitors alike, manned by a permanent guard station. If there are additional entrances, the combination of card reader, biometric device, and man-trap should be used, but, if the entrance is in a low security zone, a card reader alone may suffice.

Our final barrier, which should never be underestimated, is that essential human touch – roving guards along with permanently manned stations.

A good source of more information regarding biometrics can be found at http://www.biopassword.com/home/technology/biometrics.asp. Information concerning man-traps can be found at http://www.jasperinc.com/english/products/side-p.htm.

Internal Security

[Return to Table of Contents]

Many of the same external security techniques are used as well for internal security. A camera surveillance system will be installed throughout the facility along with roving guards and a permanent guard station at the main entrance. A combination of card readers and biometric devices will handle authentication and where required man-traps will be installed.

The building will be partitioned into different security levels. Low security areas may only require a card reader for access, while the highest security areas will have a combination of card readers, biometrics, and man-traps. At the least, the server farms and utility areas will be classified at the highest level of security. Both the entrances and exits of the server farms will require auditing and authentication of all who pass through. The exit devices in the server farms will be programmed to reject any card and PIN that was not used to enter the center. This will require that every person in a group authenticate themselves one at a time. Use of man-traps at all doorways will make this requirement unavoidable. (The question of whom to give access will be addressed in the following section.)

In the case of extremely secure rooms or centers, it may be necessary to require authentication and auditing of the server cabinets. (Go to http://www.smcplus.com/products/SmartCabinet.htm for an excellent example of this.) Additionally, this type of room will require a permanently manned guard station and manual logging of all entries and exits.

Temperature, Smoke and Humidity sensors will be installed throughout the facility, in various zones. In particular, there will be separate fire zones below the floor and above the ceiling. Fire extinguishing will be handled by FM-200. FM-200 has replaced Halon as the industry standard, as it is more environmentally and data systems friendly. The gas will be stored in the utility

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

shafts with air-sampling sensors inside the center used to release the gas. Air-charged, dry pipe sprinkler systems will also be installed.

The farms will be kept at 68 degrees Fahrenheit and 50% humidity. Water-cooling systems (aka chillers) will be located within the utility shafts. A 2 x (N + 1) redundancy formula will be used to determine the necessary quantity of the FM-200 and chillers. Electricity will be supplied from two separate grids. Even better is if each is from a different vendor.

Personnel

[Return to Table of Contents]

Access is the key issue with personnel security. All staff will be issued a Photo ID and PIN. These will be keyed to the different access levels discussed in the previous section. Only those who can demonstrate a need for access to a high security area will have it granted and that access must be held only as long as needed. The security team will maintain a record of all personnel with the highest access and will run regular audits to ensure that all IDs are accounted for and that justifications for high security access remain valid.

Requirements for this level of access should include at a minimum a background check, and very likely periodic drug and polygraph tests. As discussed in Building Construction and Design, our facility is designed correctly, it'll allow repairmen to do their work without entering a farm repairmen, custodians, etc. are denied access to any of farms. This goes back to the building design. There is no way to justify having custodial workers in such areas, which means the engineers will have to be responsible for maintaining a clean environment. Vendor support engineers will have to be accompanied at all times by a staff engineer with the proper clearance. It is possible that vendor engineers may wish to go through the clearance process as well, which would then negate the need for anyone to accompany them.

All staff must sign a statement that they have been informed of the security policy, which will cover such areas as laptop security, maintenance and disposal of sensitive documents, and access levels. All must be held strictly accountable for any security breaches with misuse of one's access rights being grounds for dismissal. This policy must be supported and vigorously endorsed from the executive staff down if it is to be taken seriously. The guards will be instructed to sweep work areas as they patrol and confiscate and report any unsecured equipment or sensitive documents.

Disaster Recovery

[Return to Table of Contents]

Now we need to address the possibility of things going wrong. We've already touched on some of this in the section on Internal Physical and Environmental Security, e.g. FM-200 and electrical power being supplied from two grids. We need to do much more, however.

To counter the loss of electricity to any of the server farms we have Uninterruptible Power Supplies (UPS). We will again double the standard N + 1 redundancy rule and as a further precaution will separate the UPS in two rooms. If we lose power from one grid, we have the second power grid to fall back on. If this is out as well, we will have diesel generators ready to supply power. To keep the generators running, we will contract with a minimum of two vendors and will have storage capacity on-hand sufficient to run the facility for several days. At least once per month we will test the generators by switching the facility off of the grids, using the diesel generators as the sole source of power.

We will again double the N + 1 redundancy rule in planning our Internet connections. Our extensive Physical Security measures would be for naught should we lose the very function the

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

facility is meant to provide—web hosting, which means we must have multiple Internet connections provided by at least two different vendors.

All servers will have their data backed up through a central backup system. This system will follow a standard rotation of full and differential backups. The backup logs will be audited on a daily basis to ensure that all systems were completely backed up. Tapes will be duplicated, with one copy being sent offsite for secure storage. Random test restores will occur on a weekly basis to ensure the integrity of the tapes.

Finally, to protect the data even if the facility is destroyed, fail-over sites will be maintained for those clients with no downtime tolerance. These will be tested on a monthly basis.

Conclusion: The Ideal vs. The Real

[Return to Table of Contents]

To build a facility that meets all of these requirements is an expensive proposition. For a Web Hosting Company, it's a question of how much of this cost they can pass on to their clients. With a corporate data center, it's more about convincing senior management that all of this is necessary. Physical Security implementations in the real world generally fall well short of the ideal.

From the start, your attempts to promote this high a standard of security will be compromised, with the site of the facility the first of many more compromises to come. In the ideal scenario, our facility is built where we want it and how we want it. In reality, the budget may only allow you to use an existing building, or the location may be too close to streets or railways. The ripple effect begins. If you're in an existing building and particularly if your data center is on the tenth floor, fencing, as well as some of the other external measures are out of the question. You will have to live with the exterior walls that are highly unlikely to meet DoD standards. You likely will have no control on the choice of neighbors and no buffer to offer you some protection.

Biometric devices are, you discover, quite expensive, as are man-traps. How will you ever convince your senior management that these are necessities and not luxuries? Perhaps you'll even end up convincing yourself that security won't suffer if you only use smart cards and standard doors. It can get even worse; you may not even be able to control the number of people with access to the server farm. I remember one building where the only way to reach another work area was through the server room. This same company also had cleaning crews working in the server room every night. On at least one occasion, the crew unplugged a key device so they could plug in the vacuum. I did some work at one web hosting company for one of their clients and was essentially given the run of the place simply by giving them my driver's license. No escort and no accountability. Of course they also weren't doing any background checks on their own personnel either.

A web hosting company, I've worked with, operates out of the third floor of a restored 18th Century factory. This site choice alone has been the cause of numerous compromises in Physical Security. In many areas there weren't any doors at all, much less a card reader, biometric device, or man-trap. Other centers I've been in were much closer to the ideal. One in particular served as the basis for much of this paper. They, however, made their compromises as well – no man-traps and no fence. Few, if any companies, will compromise on the minimal requirements such as environmental monitors, fire extinguishers, and UPSs. But will they go the extra mile and double their N+1 requirements in deciding on the numbers of such devices purchased. (This is assuming they used N+1 requirements in the first place. Redundant Internet connections are also

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

a major budget issue. These can be quite costly and hard to justify to upper management unless you've put together the numbers on lost productivity because of the loss of Internet connectivity.

Backups are another area I've often found lacking in the various companies I've worked in over the years. When web hosting, you've got to check that this is included. Otherwise it's your responsibility. Often, though, backups are not even being done or tapes being sent off-site. Many web-hosting companies and IT departments just go along hoping that no one will ask for any data to be restored. Finally, fail-over sites are still a luxury for all but a relative few. This is definitely an expensive service and most companies never consider the cost of losing not only their data, but their workplace as well. If they did the math, the cost of a fail-over site might seem a lot more reasonable.

Physical Security isn't rocket science. The standards exist and there're many good checklists and examples for other companies to follow. The reason Physical Security is an often ignored or under-implemented piece of Information Security is quite simply the cost. There're simply is no cheap or easy ways to good physical security. Natural or man-made disasters can always be counted on to bring Physical Security to the forefront of everyone's minds, and it is to be hoped that many companies will then begin the process of reviewing, creating and implementing better Physical Security standards. Past history, however, has shown that once the initial event recedes further into the past, companies tend to go back to their old ways, forgetting these hard-learned lessons. Perhaps now, with the recent effects and threats of global terrorism all too obvious, this will change and a complete physical security implementation will become as commonplace as firewalls.

References

[Return to Table of Contents]

1. Ellerbe Becket Physical Security Primer, http://www.eb-datacenters.com/tech/sec1198.html
2. Ellerbe Becket Physical Security Check List, © 1998, 1999 Ellerbe Becket, http://www.eb-datacenters.com/tech/sec1198-list.html
3. Digex SmartCenters[SM], © 2001 Digex Inc., http://www.digex.com/leverage/smartcenters04.htm#dc
4. Premier Data Centers, Copyright © 1996-2001 Verio Inc., http://home.verio.com/products/datacenter/premier.cfm
5. Shelter From the Storm, By: G. Beato Business 2.0, Issue: June 2000, Copyright © 2001 Business 2.0 Inc., http://www.business2.com/articles/mag/print/0,1643,13782,00.html
6. Internet Data Centers, © 1999-2001 Exodus Communications, Inc., http://www.exodus.net/idc/idc_diagram.html
7. FM-200 Fire Protection Systems, http://www.reliablefire.com/fm200/fm200.html
8. CSU3000, Constant Protection For Water-Cooled Medical & Industrial Equipment, Copyright © 2001 Liebert Corporation, http://www.liebert.com/products/english/products/env/csu3000/60Hz/bro_4pg/html/SL_11730.asp
9. Generator Packages, Power Solutions & Sizing Your System, http://www.caterpillar.com/industry_solutions/shared/electric_power/products/products.html
10. Communications, Reliable Power for a Demanding Industry, http://www.caterpillar.com/industry_solutions/shared/electric_power/markets_we_power/04_communications/communications.html

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

11. Dmitry Eroshenko, From Zero To Maximum Security In 180 Days, Web Hosting Magazine, Copyright © 1998-2001 Infotonic, Inc., http://www.whmag.com/content/0401/security/
12. SIDE-P Secure IDentification Entry Portal, http://www.jasperinc.com/english/products/side-p.html
13. Biometrics, Copyright © 2001 Net Nanny Software Inc, http://www.biopassword.com/home/technology/biometrics.asp
14. DTS-1000 for WINDOWS-Video Motion Detection and Tracking System, © 2001 Magal Security Systems Ltd., http://www.magal-ssl.com/pages/DTS1000.asp
15. Perimitrax - Buried Cable Intrusion Detection Sensor, © 2001 Magal Security Systems Ltd., http://www.magal-ssl.com/pages/Perimitrax.asp
16. The Innocent-Looking Detection system - INNO-FENCE, © 2001 Magal Security Systems Ltd., http://www.magal-ssl.com/pages/innofence.asp
17. Director of Central Intelligence Directive 1/21: Manual for Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF), http://www.fas.org/irp/offdocs/dcid1-21.htm#4
18. SmartCabinet I: http://www.smcplus.com/products/SmartCabinet.htm
19. National Industrial Security Program Operating Manual Supplement, December 24, 1994, http://nsi.org/Library/Govt/NISPOMSU.txt
20. Walter Cooper and Robert DeGrazio, *Progressive Architecture*, March 1995, pp. 78-83, http://jya.com/archsec.htm,
21. Alexander, Michael, The Underground Guide to Computer Security, Addison-Wesley, 1996
22. Winkler, Ira, Corporate Espionage, Prima Publishing, 1997
23. Garfinkel, Simson and Spafford, Gene, Practical Unix & Internet Security, O'Reilly and Associates, 1996

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: March 9th, 2014

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

9th Annual ICS Security Summit	Lake Buena Vista, FLUS	Mar 12, 2014 - Mar 23, 2014	Live Event
SANS Northern Virginia 2014	Reston, VAUS	Mar 17, 2014 - Mar 22, 2014	Live Event
Secure Canberra 2014	Canberra, AU	Mar 17, 2014 - Mar 22, 2014	Live Event
ICS 410@ Sydney 2014	Sydney, AU	Mar 24, 2014 - Mar 28, 2014	Live Event
SANS Munich 2014	Munich, DE	Mar 31, 2014 - Apr 05, 2014	Live Event
SANS 2014	Orlando, FLUS	Apr 05, 2014 - Apr 14, 2014	Live Event
FOR518 Mac Forensic Analysis	Vienna, VAUS	Apr 22, 2014 - Apr 27, 2014	Live Event
SANS Abu Dhabi 2014	Abu Dhabi, AE	Apr 26, 2014 - May 04, 2014	Live Event
US Cyber Crime Conference	Leesburg, VAUS	Apr 27, 2014 - Apr 28, 2014	Live Event
SANS Austin 2014	Austin, TXUS	Apr 28, 2014 - May 03, 2014	Live Event
Security Leadership Summit 2014	Boston, MAUS	Apr 29, 2014 - May 07, 2014	Live Event
SANS Security West 2014	San Diego, CAUS	May 08, 2014 - May 17, 2014	Live Event
SANS Secure Europe 2014	Amsterdam, NL	May 10, 2014 - May 24, 2014	Live Event
SANS Melbourne 2014	Melbourne, AU	May 12, 2014 - May 17, 2014	Live Event
SANS ICS410 London 2014	London, GB	May 12, 2014 - May 16, 2014	Live Event
SANS Malaysia @MCMC 2014	Cyberjaya, MY	May 12, 2014 - May 24, 2014	Live Event
SANS Bahrain May 2014	Manama, BH	May 17, 2014 - May 22, 2014	Live Event
SANS Delhi 2014	New Delhi, IN	May 19, 2014 - May 31, 2014	Live Event
SANS Secure Thailand	Bangkok, TH	May 26, 2014 - May 31, 2014	Live Event
Digital Forensics & Incident Response Summit	Austin, TXUS	Jun 03, 2014 - Jun 10, 2014	Live Event
Secure Singapore 2014	OnlineSG	Mar 10, 2014 - Mar 15, 2014	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced