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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Disaster Recovery: A Security Exploit

Michael Courton

October 5, 2000

Introduction

Disaster Recovery is the function of planning for the recovery and restoration of the data processing function of an organization. In general, disaster recovery plans are developed for a worst case scenario. This scenario is defined as the facility is totally damaged and there is NO access to it or its contents whatsoever.

In this paper we will focus on the disaster recovery planning process, the inherent security vulnerabilities within the process and the possible exploitation of these vulnerabilities. Outside of the plan development we will also look at the vulnerabilities inherent in the testing of those plans.

For many organizations disaster recovery planning is a regulatory requirement. Furthermore, many corporations have started requiring that vendors they deal with have disaster recovery plans as well. So there is no option to NOT do it.

According to research done by Contingency Planning Research (CPR) the disaster recovery business is expected to be a billion+ dollar industry by 2000, with continued growth of 15% annually.

Process

Lets take a look at how the process of disaster recovery planning is performed so we can have a better idea of how these vulnerabilities arise. We will not get into a lot of detail but briefly outline the major steps in developing and testing a plan.

First there is the risk and impact analysis phase. The employees (analysts) responsible for writing the plan must uncover all the possible ways that the company is vulnerable to a disastrous event happening. After these risks are identified, then the financial impact to the business should one of these events happen must be determined. And the probability of any of these events happening must be determined.

The next step would be to determine which risks are acceptable, and which would have such a negative impact that you should perform due diligence and implement some mitigation to lessen the chance of them occurring. The next step is that options on how to deal with the interruptions are identified, investigated and selected. Procedures are then written on how to respond to an event, establish communication between all parties involved, coordinate the implementation of the strategic options selected, and document detailed actions on how to recover critical functions and resources.

Furthermore, single points-of-failure in the recovery process are identified and eliminated. A good example of this could be to eliminate reliance on a single individual as the sole source of knowledge of a particular function by minutely documenting all that person knows about that function including how to get it back .

Vulnerabilities

- Social Engineering
- Physical Access
- Data Integrity
- Third Party Authentication
- System Integrity

Social Engineering

Because disaster recovery planning is such a people intensive endeavor, many of the social engineering techniques commonly used by hackers would be successful in gathering information. Like calling someone up in the middle of the night and pretending to be someone else. Or perhaps posing as an employee, so that he/she can walk around the organization looking for opportunity.

For emergency communications, a lot of personal information is gathered from critical individuals in the planning process. This information would include telephone numbers, alternate addresses, personal details and even family information. Armed with just a small amount of this type of information, hackers could have a field day.

© SANS Institute 2000 - 2005 Author retains full rights.

Physical Access

The dissemination of the documentation of a disaster recovery plan is central to its effectiveness. However, distributing the information in various forms creates a security risk. Paper binders are conspicuously labeled and given out to designated personnel who most often keep them on a open shelf in their office or cubicle where anyone walking by can just pick it up

Another form of documentation is online databases, where third party software is purchased and installed on the corporate system. This software comes in LAN varieties so that personnel from all over the company can have access to it. This software is based on very common SQL engines. An even more vulnerable variety is internet-based, where a vendor assumes the role of an ASP. Many of these vendors are inexperienced in network security.

Data Integrity

Another form of documentation is done on some database software. There are versions of these products that are LAN connected and can be accessed from anywhere in the company or even remotely. Additionally, this database or online system is often replicated and synchronized on laptop PCs for members of the management team.

As often happens when employees are issued a company laptop, they use it for all kinds of things not related to the business function, like getting online, and downloading software and such from the internet. Afterwards, these same employees then follow regular procedures for transferring information from the laptop directly to a synchronized application on their desktop system at work. Or better yet, due to the increased popularity of tele-commuting, these laptops are used in place of desktop systems and are setup to connect directly directly to the corporate LAN from almost anywhere. Now you have opportunity for the introduction of malicious software.

Another area where data integrity can become a major concern is producing and storing backup system data. In many companies there is a hoge-poge of employees that have access to critical records. I audited a facility once where as many as 125 people had access to the tape storage library. This kind of access should be on a need only basis.

Third Party Authentication

It has been proven over and over again that a person’s main concern at the time of some regional type event is to their family and immediate safety. Which means that for certain functions within a recovery you will have to use temporary employees, and given the circumstances you would not have the time to screen these temps prior to putting them to work. A hacker could easily be hired in this situation.

According to Sharon Spontak of the Rehabilitation Institute of Chicago, "almost eighty percent of all computer security breaches involve someone inside the company".

Another exposure that exists is that when you contract with a vendor for disaster recovery services, you have no idea of the personnel policies that vendor may have for hiring employees. You can be certain of one thing though. There will be disgruntled employees or someone who feels they are under-compensated. That leaves your company open to direct contact by someone who may be looking for an opportunity to exploit.

If you’re located in an area that is prone to regional events, then best practices in recovery planning and testing requires you to use personnel that are geographically distant enough that they would not be affected. This requirement leaves you susceptible to including people in your testing that you’re not familiar with. You have to rely on second and third hand evaluation as to their competency and dedication to the company as well as not knowing what their current history with the company is.

System Integrity

Perhaps the most dangerous vulnerability is that when systems are initially rebuilt, normal User IDs, passwords and group definitions are replaced with User-IDs that grant SU privileges to anyone that logs in. The reason for this is the time factor. A premium is put on getting the system back up as soon as possible. And these IDs are not limited to systems administrators but often include support personnel for critical applications as well.

Testing is most often performed at a commercially available facility run and operated by another company. During testing or recovery the procedure is to go into your vendor’s site and begin to restore your basis operating system. You then reboot the system with your software, but what is to stop someone, a technician, from loading sniffers and such on the generic machine, which then captures information from you as you restore and rebuild your system. Additionally, because of the amount of personnel resources it takes to conduct testing, there is almost always a

© SANS Institute 2000 - 2005 Author retains full rights.

telcom link back to the ‘home-office’ for support.

Companies that perform sophisticated testing do more than just test recovery plan elements, they often conduct software patch testing or new procedure testing. The results of which are then transferred back to the ‘home-office’ environment.

Conclusion

These are just some of the more common vulnerabilities that exist within the process. Due to nature of disaster recovery planning it would be impossible to eliminate all vulnerabilities but perhaps incorporating security awareness within the process most of these exposures could be plugged.

References

Market Analysis and Forecast, Eagle Rock Alliance/Contingency Planning Research, 1998

The Business Continuity Institute, "The Ten Certification Standards for Business Continuity Practitioners" 2000 http://thebci.org/frametrial.html

Winkler, Ira S. "Social Engineering and Reverse Social Engineering"
Data Security Management – Auerbach Publications CRC Press

Rothstein, P. "When a Virus creates Disaster"
http://www.rothstein.com/virus.html (1995)

Spontak, Sharon "Oops, you did it again" 2000

Schranz A. "Disaster Recovery" IWorks 98 Conference Slide Presentations
http://www.erpnews.com/conference/IWorks98/sessions/sn087/sld001.html 1999

Arnold, R.L. "The San Francisco Earthquake" The Disaster Recovery Journal Winter 1998
http://www.drj.com/special/sfquake.html

Chamberlain, Ronald "The Restoration Vendor’s Perspective" Disaster Recovery Testing: Exercising Your Contingency Plan 1995

Kirvan Paul F., Rothstein Phillip J. "Local Area Network Recovery Testing" Disaster Recovery Testing: Exercising Your Contingency Plan 1995

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event