Corporate Security Vulnerabilities in e-Business

By

L. N. Papke

Table of Contents

Abstract

This paper will assess the current state of corporate security vulnerabilities in e-Business, by discussing, analyzing the risks of both hardware and software, along with the problems associated with physical storage and handling, and then proceed to offer recommendations and then pull everything together in a conclusion. It is by no means a total and exhaustive examination of the problem, but it is a starting point for anyone who wishes to know more about this problem and what is being done about it in today's corporate world.

Introduction

The world of today is vastly different from that of a hundred years of even fifty years ago when it comes to the way in which the security and vulnerability of the way corporations do business. Gone are the times when records were kept on paper and could easily be kept track of, gone are the days when the number of people that had access to any records could be put on a short list.

Now, with the advent of databases and the use of the Social Security Number (SSN) as a common identifier, the ability of a thief to steal massive amounts of data at one time is tremendous. The personal credit history of millions of customers can be contained in the space of one large capacity hard drive, or on several reels of magnetic tape.

This is just one aspect of the problems that are faced today when it comes to e-Business. There are also numerous problems when one puts a web server up on the Internet, for there the hackers are every vigilant to try and break in to steal whatever they can. There is also the possibility of a disgruntled employee or former employee who has access or the capability of hacking into the network to do untold economic and social harm to the company and all of its customers.

Therefore, it should be made mandatory that all companies take stock of their vulnerability to any of these scenarios and prepare plans to close any holes in their security matrix, and provide ways in which minimize any damage that could possibly come forth from any type of security problem. To do any less would be a great disservice to not only the company but the customers and others who rely on it for the security of their data.

Risks

Hardware

If a company has shoddy hardware in their network, or neglects to keep pace with the latest technologies, then the hardware that they are using will become outdated and susceptible to intruders. One of the first links in the armor of security is that of the hardware, and so it must be kept up to date.

Hardware that has been on the market for some time is studied by the criminal element for any and all vulnerabilities that can be found and exploited. Hardware vendors constantly strive to improve their products, both in functionality and security, so it behooves the companies that buy the product to do the same. By keeping up with the increases in the computing world, the companies that rely on the hardware to help keep the network protected will have a better chance of doing that.

Since the lawless keep up with the latest in technology, shouldn't the lawful do the same thing? It would be foolish to not do so. The administrator of the network must be alert for any new changes in the hardware that comprises the network, and bring to the attention of the proper personnel what must be done to protect the company and the data that it holds from any attacks.

Software

In addition to the hardware that the company must purchase and maintain on a regular basis, there is also the software that runs on the computers. If the operating system and other applications that the company uses are not kept patched and up to date, then any security risks that have been discovered and exploited by a malicious person will exist on the network and leave a gaping hole for the attacker to come in through.

It is not enough to worry about this on a monthly or yearly basis, protecting the software that the company uses is a security item that must be monitored on a constant basis. One of the main advantages of the computer is the ability to perform repetitious tasks. Intruders have often taken advantage of this, by using both software and hardware attacks to see where a network might be vulnerable. Because of this, the software that a company uses must be maintained properly and not installed then left alone on the computers.

According to Gregory Toto (2005), here is a list of problems:

> Failure to maintain current security configuration and patch levels because the computer wasn't in the office or on the network at the right time to receive them
>
> Corrupted patches, which can occur if a current version of a Dynamic Link Library is overwritten by an older vulnerable version when the user installs or reinstalls software
>
> "Weak" security settings, which are often the result of a user changing settings when attempting to get the computer to communicate with the Internet on a home network or a customer's internal network
>
> The growing number of mobile workers, which can compound problems -- and compromise your network -- when communication is re-established with the network.

One is able to see from this that not patching and setting the proper security settings allow for a multitude of problems on the network.

Storage

As a corporation accumulates data, it must be stored in some form (or destroyed). When the data is stored, the responsibility for security is not any less than when it was on the server. Even though the data might be older, or not currently in use for whatever reason, does not make it less useful to an intruder.

> "Enterprises should be careful not to get too fancy about their storage security, since some solutions could create their own problems" (Hirsh, 2002).

Careful thought and planning must also be given to what way the data will be stored, where it will be stored, the length of time that is has to be stored, and who will be responsible for it while it is stored.

If the company chooses an outside facility for the storage of the data, there is also the matter of how to transport the data to the storage facility, what party will do the transporting, and when the storage facility becomes responsible for the storage of the data.

Internet

> "Attacks on web-connected servers are becoming more common. Every day there is news of another major corporation whose security has been breached. Attackers stole credit card numbers from Western Union's site and a computer hacker broke into a

> Walt Disney Company computer, stealing sensitive guest information" (Sima, 2004, p. 5).

Businesses need to be made more aware of the dangers that they face when they connect their networks to the Internet, and especially if critical information is stored on any servers that can be accessed from the outside, such as credit card information or other personal data.

As shown earlier, as soon as a computer is connected to the Internet the unscrupulous are ready to start their attacks, and there are enough out there to ensure that all servers are attacked on a constant basis. When a web site has an application that passes sensitive data from the customer's computer over the line to the corporate server, this is the time that great care must be taken to ensure that the data is not compromised in any way.

By ensuring that the proper security protocols are put in place from the start, administrators can go a long way in minimizing their problems with data loss to any intruders.

Recommendations

There are many people out in the world who have come up with various solutions to protect the data that resides on corporate networks, but no one has found a perfect system as of today. When companies move from the offline world to the online world too often the idea of protecting and securing the servers is down on the list of priorities, and usually because the management does not understand the needs and risks involved in connecting to the Internet. According to Berinato & Scalet (2002), there are 10 key components of good information security, listed below:

> 1. *Identify your risks*. Determine what your company's most critical information assets are, and spend your time and energy protecting what's most important.
>
> *2. Get the CEO involved*. Good security has to start from the top, with executives who help create a corporate culture that values security.
>
> *3. Put someone in charge*. Security is a complex job, so make sure someone is in charge of coordinating security efforts.
>
> *4. Develop and implement a security policy*. Establish guidelines for how your company handles and protects its data—from who makes sure software patches are installed to how employees access their e-mail on the road, to how often passwords should be changed.
>
> *5. Educate employees and raise awareness*. Make security awareness an ongoing project. Employees need to understand why their role is so critical.
>
> 6. *Have a security audit done*. Hire an independent third party to evaluate your security posture, and then use the recommendations made by the auditor.
>
> 7. *Incorporate physical security into the plan*. The best security technology in the world won't do any good if a well-meaning employee lets the wrong person into the server room.
>
> 8. *Remember internal threats*. Most attempted hacks come from the outside, but most successful ones start with people who have inside knowledge. First and foremost, have a process in place to delete users accounts when employees quit or are let go.
>
> 9. *Stay tuned in*. Make sure someone keeps track of new developments in information security, including new vulnerabilities and attacks.
>
> 10. *Prepare for the worst*. Create an incident response plan to help you save time in the event of a security problem. This will lay out who needs to be involved, what their jobs are, and how you'll minimize the damage.

By following this list, one would be able to create a good policy for protecting and securing the network and data that the company is in charge of. There is also the suggestion by Eric Ogren (2003) that companies should also observe the following:

> “Mandate DoS protection from service providers in future service-level agreements. Service providers have defenses against bandwidth-consuming attacks such as SQL Slammer. Do business with service providers that can guarantee greater availability and will accept financial incentives for extended e-business.
>
> Make network intrusion prevention mandatory in front of critical data centers and Web-facing application zones. The cost of a service disruption merits extra attention. The technology can be deployed as widely as IT feels comfortable administering it in larger scale deployments.
>
> Know what security problem you are trying to solve and choose solutions accordingly. Evaluate products against specific needs. Crosscheck references with peers within the industry to avoid being swayed by vendor marketing hype.
>
> If manual control over the network and protocol exploits is important, use a network intrusion-detection system. Large enterprises should choose from among Cisco, ISS, Sourcefire, and Symantec. A monitoring system, such as the one provided by Securify, also allows IT to defend the network against security vulnerabilities.
>
> If DoS attacks against revenue-generating application zones are a concern, focus on intrusion-prevention products strong in flow-based algorithms. Consider vendors such as Arbor Networks and Mazu Networks.
>
> If freedom to evolve the solution as the technology matures is a priority, focus on blended solutions that provide the best of both worlds. Vendors such as IntruVert, NetScreen, TippingPoint, and Top Layer deserve attention.”

One can see that the recommendations are simple and fairly easy to implement, along with being of low cost if done properly. Training of the proper personnel is also needed, for the software must have someone that can interpret the results and determine the correct couse of action that must be taken if there are any problems. Personnel must also know how to create the web sites and the applications that will be exposed to the Internet so that a poorly designed web site is not the starting point for an invasion by anyone into the corporate servers.

Conclusion

As one can see from this paper, most of the problems that have risen from companies moving their business to the Internet are because of the lack of knowledge of the risks that are to be found, and of a lack of consensus of what a company should do in order to protect their network from intruders.

By using some common sense and realizing that the business of e-Business is just like that of every other business, only the medium that it is transacted over has changed, but the application of good, sound protocols for protecting the entire system, from the physical connection to the customer’s computer is what is important.

Taking the time to develop a sound policy of what to do to protect and secure the data of the business and that of the customer’s, any company will be able to enter the world of e-Business with confidence that they are able to protect themselves and their customers.

The cost of not doing anything to safeguard the company and the customer will be far greater than the cost of implementing any of these solutions to this growing problem that has been created by the mad dash onto the Internet by the corporate world.

References

Berinato, Scott & Scalet, Sarah. (March 20, 2002). The ABCs of Security. Retrieved May 25, 2005 from http://www.cio.com/security/edit/security_abc.html

Burleson, Donald K. (February 21, 2005). An Enterprise Database Security Primer. Retrieved May 23, 2005 from http://www.dbazine.com/oracle/or-articles/burleson-sec1

Harrison, Reed. (April 9, 2003). Why your company needs a security audit. Retrieved May 22, 2005 from http://www.computerworld.com/printthis/2003/0,4814,80167,00.html

Hirsh, Lou. (October 11, 2002). Safeguarding Corporate Data. Retrieved May 22, 2005 from http://www.ecommercetimes.com/story/19651.html

Hurwitz Group, Inc. (October 2000). Managing e-Business Risks. Retrieved May 23, 2005 from http://www.globalwatchtech.net/resources/hurwitz_riskmgt_wp.pdf

Neeley, DeQuendre. (July, 2000). The Hacker Files. Retrieved May 24, 2005 from http://www.securitymanagement.com/library/000884.html

Ogren, Eric. (October 1, 2003). Preventive Steps for Securing the Corporate Network. Retrieved May 21, 2005 from http://www.csoonline.com/analyst/report1784.html

Otuteye, Eben. (No Date). Framework for E-Business Information Security Management Retrieved May 23, 2005 from http://ecommerce.mit.edu/papers/ERF/ERF136.pdf

Siemens Corporation. (2001). Comprehensive Security for Your e-Business Infrastructure. Retrieved May 23, 2005 from http://www.sbs-usa.siemens.com/portfolio/docs/SBS-NSS.pdf

Sima, Caleb. (2004). Are your web applications vulnerable? Retrieved May 21, 2005 from http://www.spidynamics.com/whitepapers/webappwhitepaper.pdf

Toto, Gregory. (January 13, 2005). Seven signs of trouble in endpoint security. Retrieved May 20, 2005 from http://itreports.computerworld.com/securitytopics/security/story/0,10801,98905,00.html?SKC=mobile-98905

Tuesday, Vince. (September 24, 2001). Wireless Network Fails Corporate Security Test. Retrieved May 23, 2005 from http://www.computerworld.com/mobiletopics/mobile/story/0,10801,64098,00.html

Addendum

Annotated Bibliography

Berinato, Scott & Scalet, Sarah. (March 20, 2002). The ABCs of Security. Retrieved May 25, 2005 from http://www.cio.com/security/edit/security_abc.html

This article defines what information security is, who should be responsible for it, what can be done to implement it, legal aspects of security, and several other items. It is a good article since it covers so much of what security is all about, it even has a section on wireless and then concludes with a list of the 10 key components of good information security.

Burleson, Donald K. (February 21, 2005). An Enterprise Database Security Primer. Retrieved May 23, 2005 from http://www.dbazine.com/oracle/or-articles/burleson-sec1

The author of this article writes about the different type of security that is faced by system administrators and others in the IT departments. He covers server access security, Internet access security, database access security, and data privacy security. These are all very important parts of the total security puzzle that the administrator must solve, and make sure that the security of all is up to date and correct at the same time. The needs of the users must also be taken into consideration, and balanced with the needs of the company and of the customers.

Harrison, Reed. (April 9, 2003). Why your company needs a security audit. Retrieved May 22, 2005 from http://www.computerworld.com/printthis/2003/0,4814,80167,00.html

The author writes about the problems of hackers attacking a network, and that the solution for many of these is a security audit of where the network is at. He covers some of the basic hacker attacks, and lists a few of the areas that a security audit will cover and then be able to point out where there are problems and what can be done to solve them.

Hirsh, Lou. (October 11, 2002). Safeguarding Corporate Data. Retrieved May 22, 2005 from http://www.ecommercetimes.com/story/19651.html

The author of this article writes about the problems that corporations face when it comes to storing and protecting their data, and describes some of the most common methods of protecting and storing corporate data today. He also mentions some of the problems that a corporation can run into when it stores the data, and how further protection of stored data can also cause problems for employees at different locations.

Hurwitz Group, Inc. (October 2000). Managing e-Business Risks. Retrieved May 23, 2005 from http://www.globalwatchtech.net/resources/hurwitz_riskmgt_wp.pdf

This paper is about the risks that business faces as it moves to the Internet, and what a company should do in order to minimize it potential of falling victim to the hackers that are constantly on the lookout for networks to break into. It covers the various ways that a network can connect to the Internet, the risks involved, and the steps that should be taken in order to implement a strong security policy in order to protect the corporate data and that of the customers that the business deals with.

Neeley, DeQuendre. (July, 2000). The Hacker Files. Retrieved May 24, 2005 from http://www.securitymanagement.com/library/000884.html

This article covers the latest hacker attack mechanisms, from DDoS to software vulnerabilities, which it states are usually just updates on old attacks that were successful. The author goes on to examine some of them in greater detail, and covers aspects of what a system administrator can do to help protect the network, as well as some places that one can turn to for further resources in need be.

Ogren, Eric. (October 1, 2003). Preventive Steps for Securing the Corporate Network. Retrieved May 21, 2005 from http://www.csoonline.com/analyst/report1784.html

This article focuses on network intrusion-detection systems, and that the corporate security system needs to be moved both backwards and forwards, from the supply line chain to the consumer's computers. In this way, it will help with defeating those who are out to institute DoS attacks on various networks that are in place around the world. This would also have the effect of beefing up the security for the e-business of the Internet, since DoS attacks are a major problem.

Otuteye, Eben. (No Date). Framework for E-Business Information Security Management Retrieved May 23, 2005 from http://ecommerce.mit.edu/papers/ERF/ERF136.pdf

This paper is about the start of the Internet and that security concerns were an afterthought in the beginning. The author then goes on to describe how this changed over the years to where now security has become one of the top priorities for every aspect of the Internet and the computers that are connected to it, from businesses to individuals. He also writes about how security should be implemented, from what is needed to what is possible at this time.

Siemens Corporation. (2001). Comprehensive Security for Your e-Business Infrastructure. Retrieved May 23, 2005 from http://www.sbs-usa.siemens.com/portfolio/docs/SBS-NSS.pdf

This is an assessment from the Siemens Corporation about the needs of businesses on the Internet, and what Siemens can do for them when it comes to the security of their network and computers. The company details exactly what they offer, and provides some facts from the FBI and others about what the latest crime figures are for security problems.

Sima, Caleb. (2004). Are your web applications vulnerable? Retrieved May 21, 2005 from http://www.spidynamics.com/whitepapers/webappwhitepaper.pdf

This paper is about the lack of application security on the web; it details various types of applications and proposes different solutions that can be used to secure the applications. The author is very through in detailing all of these types of problems and the solutions that one can use to protect the applications that the company runs on the servers from the hackers that are out there searching for networks to attack. He also goes into what the company can provide the customer and some background about the company so that one can see if they will be useful to them or not.

Toto, Gregory. (January 13, 2005). Seven signs of trouble in endpoint security. Retrieved May 20, 2005 from http://itreports.computerworld.com/securitytopics/security/story/0,10801,98905,00.html?SKC=mobile-98905

This article covers seven points about security in a network. The author writes about the costs to business and government, and then uses the list to point out where a corporation should be looking to take care of any security problems that might exist in the network.

Tuesday, Vince. (September 24, 2001). Wireless Network Fails Corporate Security Test. Retrieved May 23, 2005 from http://www.computerworld.com/mobiletopics/mobile/story/0,10801,64098,00.html

This article covers the aspect of wireless computing security, and details the experiences of one company as it tried to setup an overseas office using wireless networks and the problems and difficulties that they encountered, as well as the solutions that were put into place. A nice reference to make one think that not only is security have to be thought of for wired computers, but also the wireless that have to be taken care of also.