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

Mitigating Risks to the Insider Threat within your Organization

Harry Krimkowitz

October 24, 2000

At a regional headquarters of an international energy company, a MIS contractor effectively captures and closes off the UNIX based telephonic switching system for the entire complex. Subsequent investigation uncovers that the contractor had been notified a week earlier that he was being terminated. Further investigation reveals that the employee has two prior felony convictions.

As this case shows, malicious actions on the part of insiders within your organization can have very serious consequences. Today when most everyone focuses on the threat your network from external sources such as hackers, crackers and malicious code, in reality, you are much more likely to suffer compromise of your network or loss of proprietary information by people inside your own organization. Insiders continue to pose a more serious risk then outsiders. Security breaches such as electronic sabotage, equipment theft, theft of corporate resources and access abuses are ever increasing. According to the Computer Security Institute/FBI and Ernst and Young, nearly 50% of all network attacks come from the inside, often from unhappy workers. In fact in Survey 2000 conducted by ICSA, at least half of all respondents experienced insider security breaches related to unauthorized installation of computing tools, misuse of company resources and abuse of access controls. This confirms that the insider threat represents at least as much risk as to corporate assets as external crackers and virus writers.

So, what actions can you take to mitigate the risk from loss to your organization from the insider threat?

The Insider and the Threat

Before we look at the recommended actions for mitigating risk to the insider threat, let us identify who the insider is. Although all employees in your organization potentially are a threat for computer security breaches, organizations should focus on the information technology specialist. These personnel design, maintain or manage critical information systems. They are of primary concern in your efforts to mitigate the risks to the insider threat because they are the personnel who usually hold the keys to your information kingdom. They also possess the necessary skills and access to engage in serious abuse or harm to your information systems. These information technology specialists may be regular full-time or part-time staff employees, contractors, consultants or even temporary workers. Remember that a well-placed insider can pinpoint key data quickly and that none of the operating systems used in organizations today are immune to root compromise from an existing user account.

Now that we have defined who the insider is and established the fact that your insider can pinpoint the critical information within your organization with which to perform malicious acts, what are the prudent steps that your organization can take to mitigate the risk of this threat?

Risk Mitigation steps to the Insider Threat

Each company should start their risk mitigation process against the insider threat by seriously looking at their hiring processes and procedures. I would highly recommend that a company take a serious look at paying the price to conduct some type of pre-employment screening/background checks on their prospective employees before they make an offer to hire. Although this may be a challenge in our tight labor market, there are companies that can perform these background checks very quickly. If you cannot perform background checks on all your potential hires, ensure that you do this at a minimum for your information technology specialists.

The next, thing that your organization should do is to set a structured coordinated effort with the HR, and IT departments within your organization for new personnel in-processing and for personnel out-processing. I believe that organizations don't combine in a comprehensive way, information security and physical security. For example, one of the major reasons for physical theft is the lack of asset control. With PCs, peripherals, external drives and so on so easy to acquire, companies in many cases do not know what has been acquired and as a result, asset tags are never attached to devices. Physical inventories of assets are rarely conducted and as employees come and go, or move from department to department, these small devices just get lost in the shuffle. This coordinated and structured effort must be established in the initial in processing of each individual into your organization. Your HR Department should ensure that each new employee receive:

- A briefing on the computer security policies within the organization
- An indoctrination on security awareness

© SANS Institute 2000 - 2005 Author retains full rights.

Of course, everything with respect to computer security starts with your organization's security policy. By having established policies and ensuring that all employees are aware of the consequences for failure to comply with these established policies will go a long way in mitigating some of your insider risk.

Also, it would be prudent that each individual have their access privileges and or limits established by their immediate supervisor/manager and that these privileges be verified with the supervisor/manager by the system administrators prior the end of the employee's first day.

I also believe that each new employee should be required to sign a proper receipt for the equipment that they will operate and maintain.

Finally, all users should be required to sign an acceptable use policy stating that they are responsible for protecting information used or stored in their accounts.

My reasoning for the measures detailed above are because, I believe that the most common management errors/ommissions when it comes to computer security lapses are: failure to have clear standardized rules governing the use of information systems with explicit consequences for misuse and failure to punish rule violators.

As for employee out-processing, it is essential that all user accounts be terminated before the employee's last day. The number of cases that separated employees have returned to extract revenge on their former employers indicates a need for improved management of the termination process. Policy and procedures should be in place to define the steps that must be taken by HR, IT support and Security to provide prompt notification of changes in the status of your personnel.

Some Additional Actions

Organizations should require that their personnel use password protected screen savers that activate after 15 minutes or less of idle time because this can help to reduce the opportunities for unauthorized access to unattended terminals

Use of file encryption to protect your company's sensitive files stored on servers is another approach to effectively manage at-risk employees.

Also, it may be wise to install programs that monitor your employee's at-work electronic communications. However, it would be wise to consult with your legal consul before initiating any type of monitoring activities

Your security policy should only allow software to be installed by authorized members of the IT staff.

Finally, you should require system administrators to perform comprehensive information security audits. You should require that audit logs be stored and reviewed at least weekly. Of course, you must allocate your system administrators sufficient time and resources to adequately review these logs.

All of the above actions are focused on the insider threat. This list is not intended to be inclusive but to highlight those actions that I believe to be the most beneficial against this threat. Understand that your organization must also deploy other standard protective measures such as firewalls and intrusion detection systems. Companies with layered defenses detect a far greater number of both insider and outsider breaches.

Conclusion

A major factor in the rise in corporate computer fraud and computer crime is the fact that most companies have failed to establish sufficient security policies, procedures and controls on their computer systems. In addition, because of down sizing, process re-engineering and other efficiency moves, internal controls may not be adequate to deter insider abuse. Disgruntled employees and other insiders pose a tremendous threat to companies and organizations. These individuals usually know what controls are in place, and may have the ability to circumvent these controls or exploit weaknesses found in applications, systems and networks. Your information technology specialists will definitely possess the requisite skills. Only by adapting a comprehensive approach to applying technological and human factors to information security can an organization adequately protect itself from both the outside threat and the inside threat. If your organization takes to heart and effectively implements the actions delineated above, you will at least have taken prudent steps to mitigate the risk of computer security breaches from your employees. In short, when it comes to mitigating insider risk it pays to sweat the small stuff.

© SANS Institute 2000 - 2005 Author retains full rights.

Sources

Berst, Jesse. "The Biggest Threat to Your Network's Security. (It Isn't What You think)". April 7,1998. URL: http://www.zdnet.com/anchordesk/story/story_1959.html.

Post, Jerrold M., Ruby, Keven G., and Shaw, Eric D. "The insider threat to Information Systems". URL: http://www.smdc.army.mil/SecurityGuide/Treason/Infosys.htm.

"Security Focus 2000", Information Security Magazine, September 2000.

Para-Protect, Monthly Checklist for May 2000, "Protecting Your Company from a Bad Insider". URL: http://www.para-protect.com/monthly-checklist/May2000_checklist.html

© SANS Institute 2000 - 2005, Author retains full

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: October 26th, 2016

Upcoming Training

Click Here to {Get CERTIFIED!}

SANS Sydney 2016	Sydney, Australia	Nov 03, 2016 - Nov 19, 2016	Live Event
SANS Gulf Region 2016	Dubai, United Arab Emirates	Nov 05, 2016 - Nov 17, 2016	Live Event
Community SANS Detroit SEC401	Detroit, MI	Nov 07, 2016 - Nov 12, 2016	Community SANS
SANS Miami 2016	Miami, FL	Nov 07, 2016 - Nov 12, 2016	Live Event
SANS London 2016	London, United Kingdom	Nov 12, 2016 - Nov 21, 2016	Live Event
Healthcare CyberSecurity Summit & Training	Houston, TX	Nov 14, 2016 - Nov 21, 2016	Live Event
SANS San Francisco 2016	San Francisco, CA	Nov 27, 2016 - Dec 02, 2016	Live Event
SANS Dublin	Dublin, Ireland	Dec 05, 2016 - Dec 10, 2016	Live Event
Community SANS San Diego SEC401	San Diego, CA	Dec 05, 2016 - Dec 10, 2016	Community SANS
Community SANS St Louis SEC401	St Louis, MO	Dec 05, 2016 - Dec 10, 2016	Community SANS
Community SANS Richmond SEC401	Richmond, VA	Dec 05, 2016 - Dec 10, 2016	Community SANS
SANS Cyber Defense Initiative 2016	Washington, DC	Dec 10, 2016 - Dec 17, 2016	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201612,	Dec 13, 2016 - Feb 02, 2017	vLive
SANS Security East 2017	New Orleans, LA	Jan 09, 2017 - Jan 14, 2017	Live Event
Community SANS Virginia Beach SEC401	Virginia Beach, VA	Jan 09, 2017 - Jan 14, 2017	Community SANS
Community SANS Marina del Rey SEC401	Marina del Rey, CA	Jan 09, 2017 - Jan 14, 2017	Community SANS
Mentor Session - SEC401	Philadelphia, PA	Jan 10, 2017 - Feb 21, 2017	Mentor
Community SANS New York SEC401	New York, NY	Jan 16, 2017 - Jan 21, 2017	Community SANS
Community SANS Chantilly SEC401	Chantilly, VA	Jan 23, 2017 - Jan 28, 2017	Community SANS
SANS Las Vegas 2017	Las Vegas, NV	Jan 23, 2017 - Jan 30, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201701,	Jan 30, 2017 - Mar 08, 2017	vLive
Community SANS Albany SEC401	Albany, NY	Feb 06, 2017 - Feb 11, 2017	Community SANS
SANS Southern California - Anaheim 2017	Anaheim, CA	Feb 06, 2017 - Feb 11, 2017	Live Event
Community SANS Seattle SEC401	Seattle, WA	Feb 13, 2017 - Feb 18, 2017	Community SANS
SANS Munich Winter 2017	Munich, Germany	Feb 13, 2017 - Feb 18, 2017	Live Event
SANS Scottsdale 2017	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	Live Event
SANS Scottsdale 2017 - SEC401: Security Essentials Bootcamp Style	Scottsdale, AZ	Feb 20, 2017 - Feb 25, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Feb 20, 2017 - Feb 25, 2017	Community SANS
SANS Dallas 2017	Dallas, TX	Feb 27, 2017 - Mar 04, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Feb 27, 2017 - Mar 04, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Mar 06, 2017 - Mar 11, 2017	Community SANS