: How can managers improve security for decision support applications?

by Daniel J. Power

Editor, DSSResources.COM

Decision support security is important. Managers and Information Systems staff must understand and examine the stages involved with improving security for information systems, especially decision support applications. Improving security is a continuous and ongoing task that should be assigned to staff trained for and sensitive to security concerns. Anticipating problems and preventing security breaches is a major goal. Improving security can be examined in a continuous cycle of four stages.

The four major stages are 1) evaluating security needs (evaluation), 2) remedying problems and implementing solutions (implementation), 3) observing and monitoring the operation of the system (monitoring and feedback), and finally 4) staying informed on security issues (cf., Jones, 1998). Each of these stages is discussed in more detail in subsequent paragraphs:

Stage 1. Evaluation

Before implementing any form of security one must decide how important security is in the situation and identify any security problems that need attention. This section examines these two tasks, looks at some of the possible threats and introduces some ways to evaluate security problems.

Decision support capabilities can be made very secure if enough effort and resources are expended. Some capabilities and the associated data are more important than others. Any decision support application deemed "mission critical" should receive the highest priority for enhanced security. Security does inconvenience authorized users. So managers and Systems Administrators must balance the need for convenience in using the application against the need for security.

To evaluate the need for security for a system one should first identify the possible threats to the system. There are three major types of threats to a computer system: physical threats, unauthorized access, and denial of service (DoS). Physical threats include fire, theft of equipment, and vandalism. Unauthorized access is the feared hacker or a former employee breaking into a company’s computers or Web Site. Denial of service means people are unable to use a system because of a security breach.

: How can managers improve security for decision support applications?

Not all attacks on computer systems rely on expert knowledge of computer hardware and software. The quickest way of denying service is to steal or destroy the physical hardware. Mechanisms should be in place to prevent access to the physical hardware of a system. Network cables are also a security risk. The simplest way to disable a computer network is to take a shovel and dig up a few of the cables used for a computer network. This problem may occur by design or accident.

Logical security threats are caused by problems and errors in computer software. These problems are caused either by misuse, by hardware incompatibilities, by people, by mistakes in programs, or by program interactions with other programs. IS professionals need to evaluate the possibilities of technical and programming problems.

To break into a computerized system a hacker will generally go through a number of steps. The **first step** is information gathering. During this phase a hacker is trying to gather as much information about your site as possible, for example, what are the user's names, their phone numbers, office locations, what machines are there. **Second**, using the information gathered about a decision support application or transaction processing system a hacker tries to get a login account. It usually doesn't matter whose account. At this point the hacker is just interested in getting onto the system. In the **third step**, a criminal tries to get administrator privileges for the system. Criminals exploit flaws in programs or badly configured systems. Finally in **step four**, a criminal hacker makes changes to gain access and control of the application/system.

Social engineering, manipulating people, is one of the most used methods for gaining access and it generally requires very little computing knowledge. The most common form of social engineering manipulation is for a criminal hacker to impersonate an employee, usually a computer support employee, and obtain passwords or other security related information over the phone. Criminal hackers may also sift through the trash of an organization looking for passwords or other information. Some criminal hackers actually get a job on the site, for example a job as a temporary janitor. Criminals recognize that people are the weakest link in security.

What can be done? Passwords are the first barrier to provide security for a computer system. Also, passwords are usually the single biggest security hole. The main reason for password security problems is that users compromise the privacy of passwords including:

1. writing a password on a slip of paper and then leaving it on the desk,

2. typing a password slowly while someone is watching,

3. choosing simple passwords like "password" or a person's own first name, and

4. logging into an account using an unsecured Internet interface.

These thoughtless actions make it easier for criminal hackers to obtain passwords and bypass this important initial security barrier.

What happens next? If a person has managed to crack someone's password and break into an account, the next step is to obtain a user account with more access. The Systems Administrator is responsible for initially setting up file permissions correctly and then maintaining them. Breaching a password negates user permissions.

Stage 2. Implementation

Once managers decide on an appropriate level of security for an application and once having identified security problems at a site System Administrators now have to fix the problems and implement the security policy. This section examines tools and methods that can be used to improve security with passwords, the file system, the network and policies.

Improving password security. There are a number of schemes Managers and Systems Administrators can use to help make passwords more secure including: user education, shadow passwords, proactive password programs, password generators, password aging, regular password cracking, and one-time passwords.

User education. Users do not want other people breaking into their accounts. If the users of a system are educated in the dangers of using bad passwords most will choose good passwords. How you perform user education will depend on your users. Different users respond to different methods. System administrators must always remember that it is important not to alienate users.

: How can managers improve security for decision support applications?

Firewalls. The Internet creates access for hackers, spies and saboteurs who would like nothing more than to break into your DSS. By connecting to the Internet you basically open the doors for them. A firewall is a concept designed to shut those doors. Basically a firewall is a collection of hardware and software that forces all in-coming and out-going Internet data to go through one gate. Everything going in and out, but especially in, of that gate is evaluated. If it doesn't fulfill a certain criteria it is shut out. Having a firewall results in the following four advantages: 1) protects vulnerable or strategic services, 2) concentrates security on the most important systems, 3) enhances privacy, and 4) provides logging and statistics on network use.

Encryption. Another measure is to have a secure server and use encryption. A Web address (the Uniform Resource Locator) for a secure server is displayed in a web browser's location field beginning with "https" rather than "http" when one enters a secure area. Most browsers also show either a closed lock or a solid key symbol in the status bar at the bottom of the screen. Companies should have a secure server for decision support applications. Encryption involves coding data so that unauthorized users can not easily use or read the data. Encrypt means to put into a code or use a cipher to transform data.

Computer Security Policy. A company/organization needs a *Computer Security Policy* (CSP) to ensure the safe and organized use of computing, decision support and information resources. A *Computer Security Policy* is a written document of rules and principles related to how an organization approaches security problems. A company should specify security policy for major, specific decision support capabilities.

Examples of Computer Security Policy Statements

- Computer Applications should be built using a standardized application lifecycle. At a minimum, the process must include a testing phase. Updates, patches, and feature changes should follow the same phases and processes as if the application were being developed from concept.

- Each individual user should have specific credentials for accessing a Decision Support Application. A generic user should not be created. Each user role should be specified and not be linked with a single user.

- Only authenticated users should have access to a Decision Support Application. Each user should be restricted to access only the information they require. Establishing and changing access for a user or group should be approved by the Application's data owner.

- Developers should follow best practices for creating secure applications to minimize the impact

of attacks. A code validation process should be followed to discover and remedy any code errors before an application is approved for production. The validation process must include peer review and application code scanning.

- The production data source should not be used to develop or test a Decision Support application. Development and testing databases should be significantly disguised if copied from production data sources. Production data sources must be stored in an encrypted format. Data in transit to and from the application should also be encrypted.

- Web-based Decision Support applications shall be hosted on secure, robust servers with multi-layered security. Application and web services error messages should be altered to prevent exposure of coding errors, directory structure, or other information about the application or server.

- Logs for the server, application, and web services should be collected and maintained in a readily viewable format for a reasonable period of time (may be specified by applicable state and/or federal regulation).

(See http://technology.iusm.iu.edu/security-policies-procedures-and-standards/application-security-policy)

Stage 3. Monitoring and Feedback

Once a decision support application has been secured, a security professional's task is not completed. Managers and System Administrators must continually monitor what people are doing with the decision support application and whether or not someone may have compromised the security of the system. Ongoing maintenance and monitoring of security solutions is important. An operating system or decision support application can develop "security holes" that are discovered and then solutions need to be implemented. Feedback from logs and observation of application use is important to closing the loop and engaging in ongoing evaluation. Feedback insures that security is continuously improved and that optimum control of the system occurs.

Stage 4. Staying Informed

Managers must also stay informed about security needs and issues. The Web is the best source of current, timely Internet security and computer security information. Check the CERT Coordination Center at http://www.cert.org. CERT is a security watch-dog and reporting group that studies how to prevent, detect, and respond to security threats. Staying informed is increasingly difficult for people responsible for security of computing systems. The amount of information continues to expand:

read technical material and more general material, attend conferences, discuss security issues with experts, be skeptical and don't neglect low probability threats.

Conclusions

The advent of networks, especially global networks such as the Internet has increased the likelihood that a network accessible decision support or BI system will be attacked. Security experts must protect against unauthorized access by people on site and all of the people on the Internet.

Being proactive and vigilant and following a systematic process are especially important to maintaining the security of important computing applications and systems. Professionals in the field of computing security need to focus more on protecting internally-facing decision support, analytics and business intelligence applications.

Security issues associated with the Internet, Cloud and decision support are being addressed proactively and the Internet is now an integral part of distributing decision support capabilities to users. Architecture, network and security issues must be examined together during the planning for new decision support capabilities.

References

Frisch, A., Essential System Administration. Sebastopol, CA: O'Reilly & Associates, Inc., 1995.

Hunt, C., TCP/IP Network Administration. Sebastopol, CA: O'Reilly & Associates, Inc., 1992.

Jones, D., "A University Course on Systems Administration", Department Math and Computing, Central Queensland University, The Study Guide, 1998 at URL: http://www.infocom.cqu.edu.au/Units/aut98/85321/Study_Material/Text_Book. (See http://davidtjones.wordpress.com/publications/teaching-systems-administration-ii/).

Power, D. J., Decision Support Systems Hyperbook. Cedar Falls, IA: DSSResources.COM, HTML version, 2000, accessed on 3/7/2012 at URL

http://dssresources.com/subscriber/password/dssbookhypertext.

Power, D.J., Decision Support Systems: Concepts and Resources for Managers, Quorum, 2002.

Power, D. J. "How can managers and technology staff secure decision support data and decision support systems?" DSS News, Vol. 8, No. 11, June 3, 2007 at URL http://dssresources.com/newsletters/191.php .

Power, D. J. "Is security important for decision support applications?" Decision Support News, Vol. 14, No. 07, March 31, 2013 at URL http://dssresources.com/faq/index.php?action=artikel&id=266.

Cite as:

Power, D. J. "How can managers improve security for decision support applications?" Decision Support News, Vol. 14, No. 08, April 14, 2013.

Author: Daniel Power
Last update: 2013-04-14 03:40