2013

System/Application Domain

A Training Document for James C. Childress Elementary School

The System/Application Domain is the seventh layer of James C. Childress Elementary School’s IT infrastructure. This domain consists of all school, student, and faculty private information, thus it is important that we secure it. This document outlines the common vulnerabilities associated with the system/application domain and methods to reduce the risk of falling victim to such vulnerabilities.

Alex When, Jacklyn Truong, Nick Poczynek
Silver Consulting
4/4/2013

Table of Contents

1. The System/Application Domain

The system/application domain consists of all of a business's mission-critical systems, applications, and data. It is important to ensure that this domain is secure at all times, otherwise a business could easily lose large amounts of sensitive information as well as face the threat of having productivity come to a halt. Common targeted systems and applications are operating systems (desktop, server, and network), e-mail applications and servers, Enterprise Resource Planning (ERP) applications and systems, and web browsers. System/application attacks are generalized into three categories: denial or destruction, alteration, and disclosure. This paper will cover the seven common system/application domain vulnerabilities: unauthorized physical and logical access to resources, weaknesses in server operating system and application software, and data loss from errors, failures, and disasters.

2. Unauthorized Physical Access

Unauthorized physical access can be defined as gaining access to a physical entity or area without permission from an administrative figure. It is considered a threat because if an individual with malicious intentions were to attain unauthorized physical access to an area containing sensitive systems, they could steal, alter, or destroy the systems and the data found on those systems. This threat is especially dangerous when the targets are sensitive areas such as computer rooms, data centers, or wiring closets because they contain a vast amount of sensitive information. However, it is also important to keep in mind that physical entities such as important documents can be targets to this threat.

Businesses can prevent falling victim to unauthorized physical access by developing and implementing simple policies, standards, procedures, and guidelines for employees as well as guests to follow. For example, require all guests to be escorted by an employee at all times. Make sure that every employee has an ID badge that they have visible at all times so that other employees can easily notice when a guest is present. Encourage staff to report any suspicious activities they may see. Secure all areas containing sensitive systems and/or data. Security can be as simple as ensuring the door is locked to assigning a security guard to each secured area. Require staff to follow entrance procedures when entering a secured area. For example, an employee could be required to check in with a valid ID badge before entering a secured area, or RFID readers could be installed for each secured doorway. Also ensure that physical data such as important documents are secured. Require employees to store sensitive documents in locked drawers and make sure that the drawers are locked when an employee leaves his desk.

3. **Unauthorized Logical Access**

   Unauthorized logical access is nearly identical to unauthorized physical access, except it is not limited to tangible data. It can be considered even more dangerous than unauthorized physical access because it can be carried out by a naïve staff member as well as an experienced attacker. A staff member with access to data that they do not need to perform their daily work could accidently alter or destroy said data. Additionally, an attacker who can gain access to a business's systems could destroy, alter, and/or disclose any information that they find. This could result in a denial of service attack on an important system required for the business to continue running.

   In order to mitigate the risk of falling victim to the attacks corresponding to unauthorized logical access, a business should first limit which staff members have access to certain data. For example, the nurse should not have access to payroll information. Classify data and roles and correlate these data and roles. Also, in order to ensure that only authorized individuals have access to sensitive information, all information should be encrypted and access to such data should require second-level authentication. A business should also develop and implement data handling standards. For example, staff members should know not to store sensitive information on a personal thumb drive or unnecessarily disclose sensitive information. Sensitive information could be anything from payroll data to accounting information to student information.

4. **Software Vulnerabilities**

   A software vulnerability is a flaw that exists in the programming of a software component or system that allows a malicious attacker to gain unauthorized access to that system through an exploit. These vulnerabilities can be exploited through malicious software (known as malware) that is accidentally executed on the system by a user, or more directly exploited by an attacker. Weaknesses in software that lead to vulnerabilities can occur in any software that is running on a system, including the operating system itself. Many common applications such as Adobe Flash or Internet Explorer may contain software vulnerabilities. Even custom built in-house software is not immune to software vulnerabilities.

   Software vulnerabilities can allow an attacker to steal, alter, or destroy sensitive data. It is even possible for software vulnerabilities to be exploited to allow for long term monitoring of a system, providing the attacker with large amounts of sensitive data. This type of long term monitoring could be achieved with keyloggers or other similar types of malicious software.

   Ensuring that security updates are performed regularly is one of the best ways to mitigate the impact of software vulnerabilities. By performing security updates software vulnerabilities can be corrected shortly after they are discovered, minimizing the window of time that they can be exploited. Systems should also be monitored for suspicious or abnormal behavior in order to detect intrusions.

5. **Server Vulnerabilities**

Server software vulnerabilities are similar to software vulnerabilities on non-server systems with the exception that software vulnerabilities that exist on servers have the potential to be even more damaging. Server vulnerabilities can exists in the software that the server uses to provide services (FTP, SSH,PHP) or in the operating system of the server itself.

Mitigating software vulnerabilities on servers allows for more options than software vulnerabilities in general. With servers, the option exists to virtualize aspects of the server, even entire operating systems. Virtualization serves the purpose of separating the logical components of the server from the physical components of the server. This separation helps to mitigate the risk of software vulnerabilities in a single component of the system. It is also important for system administrators to be aware of any new exploits and should quickly apply any security patches that are required.

6. **Data Loss**

Data, for the purposes of this document, includes any information stored digitally on a computing system or network. Data can be in the form of an email, a document or spreadsheet, images, database records, or other formats.

Data loss occurs when any stored data is destroyed. Loss can occur during storage, transmission, or processing. These losses are considered the greatest risk to the system/application domain, because the goal of these systems is to allow users to create, store, retrieve, and manipulate data.

The most common preventative measure is to perform backups of all data. Complete system images are stored in case a computer needs to be formatted and brought back to a known good state. Daily backups to an off-site or physically separated storage medium will allow nearly full data recovery in the event of data loss.

There are various guidelines that should be followed when implementing a data backup and recovery system. Generally, daily backups will be archived monthly onto a more permanent digital storage medium. Backup policies should be compatible with an organization's BCP (business continuity plan) and DRP (disaster recovery plan). Data recovery should be configured to meet any specified RTO (recovery time objective). Sensitive data should be stored appropriately in different databases and encrypted. Long term backups are often encrypted to prevent major data breaches.

Users should be aware of what data needs to be backed up and/or encrypted. Work should not be saved to a drive that is not regularly backed up, for example. Attention should be paid during large data transfers that the transfer completes successfully. Backups should be checked for integrity on a regular basis. If backup files are corrupted, recovery from a data loss event may not be possible.

7. Reducing Risks

In summary, the following suggestions should be taken into consideration in order to reduce risks associated with the system/application domain:

- Physically secure areas containing sensitive systems
- Implement encryption and data handling standards
- Minimize data access
- Backup data
- Develop a BCP and DRP
- Be aware of all applications on the network
- Plan, configure, maintain, and improve network servers
- Develop and implement standards
- Read and understand your provided Acceptable Use Policy
- Report suspected IT policy violations to your supervisor

The Director of IT Security is responsible for maintaining the system/application domain security policies, standards, procedures and guidelines. The Director of System and Applications and the Director of Software Development are responsible for maintaining production systems and its uses. If a staff member needs more information on any of these above topics, they should contact the appropriate director. Otherwise, the staff member is encouraged to call the help desk.