Improving Cyberdyne System Cybersecurity with Defense-in-Depth Strategies

Date: 05/04/2018

Author Name: Arpit Khandekar(A20409171)

Database Security Engineer

Table of Contents

Contents

1. EXECUTIVE SUMMARY

Manufacture based organization called Cyberdyne Systems. It is one of the biggest manufacturers of a microprocessor, microcomputer, and robotics-based technology. By this document, we are trying to address logical issues of the current security challenges of Cyberdyne. We have explained an approach which helps in shielding against cybersecurity threats and vulnerabilities that could affect the Cyberdyne systems. This type of approach is called as Defense in Depth approach. It is also called a multilayer approach to security.

Defense in Depth is used use of multiple security countermeasures to protect the integrity of the information assets in an enterprise. The strategy is based on the military principle that it is more difficult for an enemy to defeat a complex and multi-layered defense system than to penetrate a single barrier. This approach has been used by many other organizations previously or currently using to secure their systems. It has been observed that threats of an intrusion by malicious actors on Cyberdyne system have increased recently. As per the report from testing and auditing team, it is becoming difficult for those teams to handle such attack, thus Cyberdyne system has taken a decision to use Defense-in-depth approach to secure their systems from attackers.

This document helps in understanding how to deal with such threats from attackers and implement multilayer security approach Defense in Depth to increase the system security. Documents information is divided into six parts which are as follows:

1) Background and overview: It will give an insight knowledge of the current state of Cyberdyne systems and will provide the proper better understanding of what Defense in Depth approach is all about.
2) Cyberdyne Defense in Depth Strategies: It will define the strategies for database environments.
3) Security Vulnerabilities: Impact to Cyberdyne network system and its network.
4) Recommendations for Securing Environment: Based on latest methods, how we can secure Cyberdyne database.
5) Conclusion: It concludes the topics which are discussed in this document.
6) References: It describes the references which are used in the entire document.

2. BACKGROUND AND OVERVIEW

Manufacturer of Microprocessor, Microcomputer and robotics-based technology company called Cyberdyne Systems based in California. The organization has currently a 15 database engineers and 5 developers a total of 20 information technology resources. Cyberdyne initially begins as a manufacturing corporation at 18144 El Camino Real,[1] Sunnyvale, California. Founded on January 17, 1984, its products are unclear, possibly computers or processors, but from the equipment in its factory and its high tech-sounding name, it seems possible that Cyberdyne might have been some sort of smaller parts producer for larger manufacturers of high tech equipment. A closer look at how Defense in Depth evolved and how it was made to fit within Information Technology is important to help better understand the trends seen today. Knowing that Defense in Depth, as practiced, renders the organization more vulnerable is vital to understanding that there must be a shift in attitudes and thinking to better address the risks faced in a more effective manner.

The company is getting data from outside the company which fed into the system via a web application(s) that take in user input and stores it into the back-end systems. Back-end developers have noticed that there were some data that has been modified, changed, or deleted without warning. The IT department that manages Cyberdyne's data systems has grown in the capacity as demand and the amount of data into the system has increased. The report having the strategy called Defense-in-Depth which helps in providing the recommendations for the secure environment. Also, with this report, we can find out the loopholes in the system. The report helps in figuring out the problem which can be encountered in the future of Cyberdyne existing system. Also, this report gives an insight knowledge of the security measures in the report so that they can be implemented in the right manner by the developers. To sum up, the important point of this report is that after looking at memo and software in a right manner it shows the brief strategy of how to protect the system from hacking.

3. CYBERDYNE DEFENSE-IN-DEPTH STRATEGIES

Defense in depth is the concept of protecting a computer network with a series of defensive mechanisms such that if one mechanism fails, another will already be in place to thwart an attack. Because there are so many potential attackers with such a wide variety of attack methods available, there is no single method for successfully protecting computer networks. Utilizing the strategy of defense in depth will reduce the risk of having a successful and likely very costly attack on a network.

3.1 TRAINING AND EDUCATION:

To enhance the awareness about the security measures, training and education sessions should be conducted within the Cyberdyne employees. These training and Education will ultimately help the organization to grow. Also, training and more information about security measures will help employees to add new skills, ideas, tools and experience.

3.2 POLICIES AND PROCEDURES:

At its most basic, policy is "a course or principle of action, adopted or proposed by a government, party, business or individual". The term is used in many different ways, varying from institution to institution, organization to organization and sometimes within institutions and organizations as well. Policies and Procedures clearly defines "Rules of the Road" set of instructions for users and it helps in explaining consequences of violating policies. Successfully Policy creation is what when Policies are created when IT employees and management teams sit together.

3.2.1 **Clean Desk Policies:** It is one of the top strategies to utilize when trying to reduce the risk of security breaches in the workplace. This policy ensures that all sensitive/confidential materials are removed from an end user workspace and locked away when the items are not in use or an employee leaves his/her workstation. This policy also helps in increasing the employee's awareness about protecting sensitive information.

3.2.2 **Data Breach response Policy:** This policy helps in define to whom it applies and under what circumstances. Also, it includes definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.

3.2.3 **Digital Signature Acceptance Policy:** The Digital signature can act as a substitute for traditional “wet” signatures, within the organization. This signature acceptance requires specific action on both employee signing the document or correspondence. The goal of Organization like Cyberdyne which is having most of business digital should implement digital signature for every digital files which they are dealing with to ensure the security of the documents.

3.2.4 **Email Policy:** Nowadays, Electronic mail (Email) which is primary communication and awareness method within almost every organization. All the email should be consistent with the Company name policies and procedures of ethical conduct, safety, compliance with applicable laws and proper business practices. Organization may monitor messages without prior notice. Employees are prohibited from automatically forwarding Organization email to a third-party email system.

3.2.5 **Password Protection Policy:** This policy helps in establishing a standard for creating strong passwords, the protection of those passwords, the frequency of change. It is very important to save confidential files with strong passwords; otherwise unauthorized users can access important confidential Organization files.

3.3 SYSTEM AUDITING:

This auditing is considered as one of the key management tools for achieving the objectives set out in the policy of the organization. System Auditing helps in verifying elements within the systems are effective and suitable in achieving the stated objectives. In this auditing it helps in defining the effectiveness of the implemented system in meeting the specified objectives.

3.3.1 DATA ASSETS:

A data asset is a result of taking the raw material from the run-the-business data and producing higher-quality-data end products to integrate the business and monitor the business. To identify patterns and predict upcoming outcomes within Cyberdyne Systems having real-time data. Optimized data can be used for better customer performance. Information which is readily available is immensely helpful for the customer. Following are the data type:

Types of Data are as follow:

1. Sets of master data.
2. Metadata
3. Sensitive data

4. Acquired data.

3.3.2 TECHNOLOGY ASSETS:

Technology assets play a crucial role in enabling the competitiveness of companies in most industries. Data which is stored using encryption technology in the organization system which cannot be read simply, it needs to decrypt with help of encryption key. Encrypted data is stored in databases, the cloud, computer hard drives, or mobile devices.

3.3.3 PEOPLE ASSETS:

- **Data owner**: In an organization every data object is own by an owner. Intellectual property rights and copyright of data are normally understood by the Data owner.
- **Security Management**: Security practices within the organization are taken care by security management.
- **Security Advisory Group**: Security issues are reviewed by these group with chief security officer.
- **Chief Security Officer**: Security of the organization and its critical issues on daily basis are the responsibilities of Chief Security Officers.
- **User**: They are responsible to make sure requirements laid out in policies and procedure are meet properly.
- **Developers**: Within the program it is the responsibility of developers that the program is secured with proper security controls.
- **Auditor**: To provide the effectiveness of the organization’s security controls is the main job of Auditor.

4. SECURITY VULNERABILITIES

4.1 MAN IN THE MIDDLE ATTACK(MITM)

This type of attack can be done on Cyberdyne database security by attackers attacking between two targets. While transmission of Cyberdyne was going there was man in the middle attack(MITM) which can be sensed as there was data loss and data manipulation occurred which are the symptom of MITM attack. This means that attackers have easy access to Cyberdyne database. The goal of MITM attack is to steal the personal information like account information, personal information and credit card numbers. Recently, Cyberdyne System failure occurred, illegal data manipulation and deletion of data were found by which we can conclude that it was MITM attack.

Man in the Middle attack:

- Sniffer could be present in the network who have accessed the Cyberdyne network and has accessed them.
- Security level protocols like digital keys, certificates and secured HTTP for sending and receiving data should be used properly.
- Also, there is a possibility of virus which is present in Cyberdyne database because of which data migration took to wrong or faulty users.
- In Cyberdyne system, there could be a possibility of session hijacking attacker, which can be pulled off by using tools, for example, ssls trip which strips the website of its SSL protocols.

4.2 SQL INJECTIONS:

Cyberdyne system security is more prone to get attacked by attackers through SQL injections, as it contains a large amount of data from the various source. Whenever there is huge data it is directly proportional to data attacks. In our firm when application developer was trying to fetch the data, but the system was behaving repeatedly illogical, which could be a sign of SQL injections. Attackers could attack the Cyberdyne system easily if:

- Password not changed since long time.
- Using old technologies software's like old PHP-My-Admin.
- From insider to attackers using error handling techniques.
- Poor SQL commands which are utilized by Cyberdyne is to check username and password which gives an opportunity to the attackers to attack the system without having previous knowledge of the password.

Following are the types of SQL injections(SQLi) are as follows:

1) **In-band SQLi (Classic SQLi)**: In-band SQL Injection is the most common and easy-to-exploit of SQL Injection attacks. In-band SQL Injection occurs when an attacker is able to use the same communication channel to both launch the attack and gather results. It has two types Error-based SQLi and Union-based SQLi.
2) **Inferential SQLi (Blind SQLi):** In an inferential SQLi attack, no data is actually

transferred via the web application and the attacker would not be able to see the result of an attack in-band (which is why such attacks are commonly referred to as "blind SQL Injection attacks"). It has two types Blind-boolean-based SQLi and Blind-time-based SQLi.

3) **Out-of-band SQLi:** Out-of-band SQL Injection occurs when an attacker is unable to use the same channel to launch the attack and gather results. Out-of-band SQLi techniques would rely on the database server's ability to make DNS or HTTP requests to deliver data to an attacker.

4.3 UNAUTHORIZED ACCESS

Due to this unauthorized access, only attackers were able to access the Cyberdyne database servers. In Cyberdyne, organization users were given access to almost every other role which is not required. Allocation of access should be done based on the roles of employees, hence by this, we can restrict the unauthorized access to some point. This can be identified by the following:

- Website having HTTP are easy to attack and also consider as improper usage of web links. It should be modified to https, to make the website more secure.
- Privileges should be given to employees based on the roles, otherwise, it could be the threat to data security. If same privileges are given to all employees then there is a chance of attack which can be done by outsider or insider.
- Data integrity can be hampered if all the access are provided to the employees as they can access the base file and change it which leads to the data leak.

5. RECOMMENDATIONS FOR SECURING ENVIRONMENT:

Security is the process which focusses on CIA (Confidentiality, Integrity and availability)

5.1 MONITORING AND LOGGING:

Every security appliances, business critical system, noncritical servers and endpoint in Cyberdyne organization generates and extensive even logs daily which must be managed to provide an early warning system for fast response to security events. By observing the administrator movement and obligation issues, it works as a repaying control for privileged Cyberdyne users.

Log Retention: This service helps in offloading the management and maintain burden while retaining full access to the appliances. There are several log retention tools which are used to satisfy security, compliance requirements for log creation, storage and reporting through the capture and aggregation of million logs generated every day by disparate assets and data sources.

Log Monitoring: Log monitor analyzes security logs and alerts virtually any security technology and critical information assets in Cyberdyne environment. It helps in responding to threats in real-time. Benefits for Log Monitoring are as follow:

- It protects systems and data 24x7 and provides alerts for threats before the damage is done.
- Using fewer resources, it satisfies regulatory requirements.
- It helps in capturing millions of logs generated everyday by disparate assets.

5.2 ACCESS CONTROL:

Access Control is a security technique which can be used to regulate who or what can view or use resources in computing Cyberdyne environment. There are mainly two types of access control, they are as follows:

Physical access Control: It is limited to Cyberdyne campuses, buildings, rooms and physical IT assets.

Logical access Control: It is limited to Cyberdyne connections to computer networks, system files and data.

5.3 ROLES, PERMISSION, PRIVILEGES:

To control access to information Cyberdyne security team, must sort out the roles of the employees, team must restrict the roles or should give permissions to the employees based on the work they are doing. Cyberdyne have many numerous security roles.

Permission are security qualities of records that associate a role with a capability. Following are the capability:

a) Read

b) Insert

c) Update

d) Node-update

e) Execute

5.4 PROPER CODING TECHNIQUES:

Cyberdyne system developer should focus on below coding techniques are as follow:

a) Input Validation:

- Data validation is conducted on a system.
- Segregate them into trusted and untrusted information sources. Get approval from

untrusted sources.

b) **Output Encoding:**

- Encoding on trusted system is conducted.
- For each sort of outbound encoding standard is utilized.
- Encoded all the information which is returned to the customer, that started outside the application's trust limit.

c) **Authentication and Password Management:**

- Those which are planned to be public it requires authentication for all the pages.
- Authorization should be done on all the authentication controls.

d) **Session Management:**

- Application should perceive these session identifiers as valid.
- It should check calculations which assure adequately random session identifiers.

e) **Access Control:**

- For settling authorization decisions, we should trust system objects like server-side session objects.
- To check access authorization, use a single site wide component.

f) **Cryptographic Practices:**

- To protect insider facts from the application client executed on a trusted system, Cryptographic functions are used.
- With such practice, it helps in protecting master secrets from unauthorized access.

g) **Error Handling and Logging:**

- Error messages give an attacker great insight into the inner workings of an application.
- Error Handling code is to assure the application fails safely under all possible error conditions, expected and unexpected.
- Passwords are encrypted while remotely logging in to the database (Data in Transit).

h) **Data Protection:**

- It is a process of safeguarding important information from corruption, compromise or loss.
- Data protecting is used to describe both operational backup of data and business continuity/disaster recovery.

5.5 FIREWALLS, SOFTWARE, OTHER PROTECTION:

5.5.1 Firewalls:

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. A firewall can be hardware, software, or both.

Types of Firewalls:

Proxy firewall: Proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network.

Stateful inspection firewall: Stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed.

Unified threat management (UTM) firewall: UTMs focus on simplicity and ease of use. It typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and antivirus.

Next-generation firewall (NGFW): Next-generation firewalls are used to block modern threats such as advanced malware and application-layer attacks.

Threat-focused NGFW: With complete context awareness it helps in understanding which assets most at risk are. Also, it provides ease administration and reduce complexity with unified policies that protect across the entire attack continuum.

5.5.2 Software’s:

Antivirus and Anti Malware Software: Viruses are a specific type of malware (designed to replicate and spread), while malware is a broad term used to describe all sorts of unwanted or malicious code. Malware can include viruses, spyware, adware, nagware, trojans, worms, and more.

Application Security: Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application.

5.5.3 Other Protection:

Web Security: A website is always prone to malware attacks. Hence website security includes scanning websites, servers and applications for malware and vulnerabilities, and includes timely detection and prevention of threats and vulnerabilities including malware threats, zero-day vulnerabilities, DDoS attacks, brute-force attacks etc. The focus is on data protection and includes sensitive personal data of customers as well.

VPNs and Private Networking: VPNs, or Virtual Private Networks, allow users to securely access a private network and share data remotely through public networks. Much like a firewall protects your data on your computer, VPNs protect it online.

5.6 DBMS SPECIFIC SAFEGUARDS:

a) **Data entry:** It is considered as one of the most specific safeguards. Encryption level which was OK two years prior to Cyberdyne is not more adequate. One approach is to physically keep the theft of the PC where the database resides keeping the server or PC in a territory of considerable protection.

b) **Passwords:** To approach certain areas in the PC/servers software passwords helps in enabling certain security faculty. Database should be isolated into levels of authorization.

c) **Backups:** To ensure the security system, backing up the database is required. Due to multiple changes occurring every day backup should be performed daily.

d) **Viruses and worms:** Once the attacks done on the system, which alerts to the clients and patches are conveyed to them to mitigate the effect of those virus.

5.7 PROTECTION AGAINST THREATS:

a) **SQL injections:** SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. Following ways Cyberdyne mitigate SQL injection

Prepared statements with parameterized queries. Use of prepared statements with parameterized queries is a strong control to mitigate an attack. Instead of writing dynamic queries—which fails to differentiate between application code and data—prepared statements force developers to use static SQL query and then pass in the external input as a parameter to query.

Stored Procedures: Developer can generate dynamic SQL queries inside stored procedures. Implement stored procedures safely by avoiding dynamic SQL generation inside.

Input validation: A common source of SQL injection is maliciously crafted external input. As such, it’s always a good practice to only accept approved input—an approach known as input validation.

Principle of least privilege: This is a standard security control that helps minimize the potential damage of a successful SQL injection attack. Application accounts shouldn't assign DBA or admin type access onto the database server.

b) Man in the Middle preventions:

Organization like Cyberdyne can prevent from Man in the middle with the following preventions:

- Make sure that the websites you visit have HTTPS in front of the URL
- Before clicking on emails, check the sender of the email
- If you're a website admin, you should implement HSTS
- DO NOT make a purchase or send sensitive data on a public Wi-Fi network.
- Make sure your website doesn't have any mixed content
- If your website is using SSL, make sure you have disabled insecure SSL/TLS protocols. You should only have enabled TLS 1.1 and TLS 1.2
- Don't click on malicious links or emails
- Do not download pirated content
- Secure your home/work network
- Have proper security tools installed on your systems.

c) Unauthorized Access Protections:

Organization like Cyberdyne can prevent the unauthorized Access protections by following methods are as follows:

Database Auditing: It is the monitoring and recording of selected user database actions. It can be based on individual actions, such as the type of SQL statement executed, or on combinations of factors that can include user name, application, time, and so on.

Fine-Grained Audit: It enables audit policies to be associated with columns in application tables along with conditions necessary for an audit record to be generated. Fine grained audit policies can be used to create audit records when a table is accessed during specific periods or specific columns are accessed.

Transparent Data Encryption: Transparent Data Encryption (TDE) enables you to encrypt sensitive data, such as Personally Identifiable Information (PII), that you store in tables and tablespaces. It also prevents access to the documents from the hard drive or reinforcement media.

Encode Database Backups: To encode the files encryption comes handy which is main defense with regards to secure the business documents when it is transferred on tape to storage location for protection.

Virtual Private Database: Virtual Private Database (VPD) is a database security feature that is built into an Oracle database server, as opposed to being part of an application that is accessing the data. The user is only allowed to see the data they have been given permission to see.

Roles: Roles are important feature in Database security, it helps in adding the privileges to a role and then grant/revoke the role based on the work which he/she is performing. Also, it is considered as one of the powerful method for managing privileges in Oracle database.

Proxy Authentication: On the command line Proxy authentication is supported by thin and thick JDBC connections. For example, this feature allows the identity of a user using a web application (also known as a "proxy") to be passed through the application to the database server.

6. CONCLUSION

We can conclude that it is recommended that Cyberdyne should properly implement all the security measures properly within their organizations. On daily basis, Cyberdyne is expanding to different business and different networks the security and risk associated with it are also growing. Defense in depth provides a comprehensive structure for managing information security within Cyberdyne organization environment.

It has been understood that no single security measure can fully protect the network, there is simply too many methods available for attackers and hackers for this to work. By implementing a strong approach or strategy called defense in depth will hopefully try to win over all kinds of attackers. Firewalls, intrusion detection systems, well-trained users, policies, and procedures, switched networks, strong password, and good physical security are examples of some of the things that go into an effective security plan. Each of these mechanisms by themselves is of little value but when implemented together become much more valuable as part of an overall security plan.

Defense in Depth is an approach which is used to protect the minimize the impact on Cyberdyne system done by an attacker, it cannot protect all the weakness and vulnerabilities in Cyberdyne systems.

7. REFERENCES USED

1. http://terminator.wikia.com/wiki/Cyberdyne_Systems
2. https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525
3. http://sydney.edu.au/legal/policy/what/index.shtml
4. https://www.sans.org/security-resources/policies/general/pdf/clean-desk-policy
5. http://www.dummies.com/programming/big-data/engineering/data-warehousing-what-is-a-data-asset/
6. https://www.acunetix.com/websitesecurity/sql-injection2/
7. https://www.secureworks.com/capabilities/managed-security/security-monitoring/log-management
8. https://searchdatabackup.techtarget.com/definition/data-protection
9. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html
10. https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277
11. https://searchsoftwarequality.techtarget.com/definition/application-security
12. https://www.comodo.com/website-security-platform/cwatch.php
13. https://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one
14. https://www.synopsys.com/software-integrity/resources/knowledge-database/sql-injection.html
15. https://www.thesslstore.com/blog/man-in-the-middle-attack/
16. https://docs.oracle.com/cd/B19306_01/network.102/b14266/auditing.htm#CHDJBDHJ
17. http://www.oracle.com/technetwork/database/security/index-083815.html
18. https://docs.oracle.com/cloud/latest/db121/ASOAG/asotrans.htm#ASOAG10270