The European Proceedings of
Social & Behavioural Sciences
EpSBS

ISSN: 2357-1330

https://doi.org/10.15405/epsbs.2019.12.03.27

ICLTIBM 2017
7th International Conference on Leadership, Technology, Innovation and Business Management

PENETRATION TOOLS TO PREVENT ORGANIZATIONAL DATA SECURITY BREACHES

Onurhan Yılmaz (a), Arif Sarı (a, b)*
*Corresponding author

(a) Girne American University, Üniversite Yolu Sk, Karaman 99320
(b) Gazi Üniveristesi, Emniyet mah, Gazi Üniversitesi, 06560, Ankara, email: arif.sari@gazi.edu.tr

Abstract

Nowadays, technology development and undergo modernization and the expansion of public and private institutions, the information on the basis of actual information as a result of exposure to war, the need to ensure the security of corporate information has emerged to reconstruct. This study, examine the enterprises's information security policy and information security prevention. So, examining threat of enterprise information security elements, determine present type of attacks and explain the the vulnerability analysis with penetration tools. This article examine the respectively, enterprise information security, enterprise information security policy, measures take for the enterprise information security and tools of the information security. This study shows that the public and have concluded private institutions of information security to ensure the purpose of the opinion that not enough alone measures taken by, in order to prevent various security vulnerabilities, intrusion detection system, it is emphasized that security scanners and firewall technology system, it is important that it needs to work in sync with each other.

© 2019 Published by Future Academy www.FutureAcademy.org.UK

Keywords: Cyber attack, security, enterprise information security, cyber secucity policy, state.

The Author(s) 2019. This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (https://creativecommons.org/licenses/by-nc-nd/4.0/).

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

Information security is very important for enterprises. If, information undergoes the modification it can be disaster. For example, the change departure or arrival time of military war plane by enemies, the result will reach the very dangerous situation.

Organizations use several methods to prevent these types of problems. Take security measures by several tools. Some of these tools duty intrusion detection and report when happen the attack of the system.

This article examine the respectively, enterprise information security, enterprise information security policy, measures take for the enterprise information security and tools of the information security.

2. Enterprise Information Security

Nowadays, people can obtain the information easily. So, information can undergo modification, fabrication and steal from the attackers. The enterprise information security, is taking the necessary measures to protect the institution of the information being accessed by attackers (Maliye Bakanlığı ISO27001 raporu, 2009).

There are many factors that affect the security of enterprise information. These are some of the technology, education and human factors. Therefore, information security is not just Information Technology or Information Systems. For this purpose, it is necessary approval and support of corporate management. To be effective, to be reflected in the corporate culture, information technology, security solutions need to be implemented fully supported and with the business processes and policies. Otherwise, the proposed solutions will remain unaffected (Maliye Bakanlığı ISO27001 raporu, 2009).

2.1. Enterprise Information Security Policy

In corporate security policies that help to determine the level of safety required, the whole staff and the whole of the rules must comply with the joint efforts made by other organizations (Kalman, 2003). This policy includes all information security activities to ensure the security of information in the organization and is directing instructions are documents containing the rules to be complied with by all personnel with the authority to reach these sources of information. These policies may vary for each institution. However, the responsibilities of staff, audit tools, goals and objectives of the management of enterprise information assets, including distribution and protection rules and important functions are defined in general terms.

In the following table 1 shows in the policy reasons and noted the risk, the application of the covers that information being responsible for the policies and personnel rules and should do, and these rules are located in sections that define the sanctions to be applied in case of violations (Kalman, 2003).

Table 01. Part of Security Policy

Section Name	Content
Overview	For the policy reasons, and includes a description of the related risks.
Purpose	The purpose of writing the policy and explain why such a policy is needed.
Scope	Policy compliance required working groups (all related to a group or organization) and determine their information assets.
Policy	Implementation and compliance with regulations or policies should include.
Criminal Sanctions	Policy violations explain the criminal sanctions to be applied.
Definitions	Technical terms are explained by non-public listed and expression.
Correction History	Changes made in politics, as well as date and reason.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Corporate security policies on information security needs of the organization can focus on creating the basic security elements in mind. For example, in military institutions, privacy, security and integrity of information is extremely important.

A security policy is created, the user must pull the response should not be difficult to work, and should be considered applicable. The policy should consist of users and of the rules with adequate sanctions in facilities owned by the system administrator. Authorized person to implement these measures and policies should have adequate administrative and technical authority. Which will be implemented within the policy legal and moral confidentiality requirements with electronic messages and access the contents of files, supervision and procedures for monitoring such as the registration to be followed users how to do, and they should be explained how to protect personal rights while person (Vural & Sağıroğlu, 2007).

Enterprises are threatening some elements. For example, the human factor are examples of this case. Enterprise in order to avoid some of the tools they use. The next section on the measures taken by institutions, enterprise information security threats to the security of the institution and used to ensure that the vehicle will be examined.

2.2. Measures Take for the Enterprise Information Security

Security threat is increasing for the enterprise with technology development. In order to ensure the security of systems, security mechanisms such as authentication and access control of unauthorized persons to enter the system to prevent the seizure of information entering the system has been developed. So, enterprises need to new mechanism for the information security. Firewall, intrusion detection systems and vulnerability scanner creates the second step security mechanism. But, these mechanisms are not sufficient alone. Because, each of them focuses the different point for the security mechanism.

2.2.1 Intrusion Detection Systems

Intrusion detection systems, integrity of the system is the system used to determine the functioning and privacy-threatening attacks. These systems fall into two categories; anomaly detection and misuse detection.

To detect abuse, plans designed before considering a breach of the policies initiated earlier. These plans are then reduced to the attack signature. After the creation of the signature attack signatures, it provided the system to understand Translation to machine language (Ilgar, 1995). The following table 2 lists the advantages and disadvantages of intrusion detection systems.

Table 02. Advantages and disadvantages of intrusion detection systems

Advantages	Disadvantages
It is the very helpful for finding attacks and blocking.	It has to manually coded and definition the novel attacks when detection the attack of the system.
It is making actively reporting, prevention and learning.	The approach is based anomaly detection is not possible to establish the relation between the events.
They are not passive safety devices such as firewalls and routers.	Intrusion detection systems produce significantly false alarms
It can be found security weaknesses of the attack behavior. At which point they may need to be strengthened.	Attack to be made on data mining can not work as much data when the system is active.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

In the following section examine the vulnerability scanner security mechanism advantages and disadvantages.

2.2.2. Vulnerability Scanner

The purpose of the vulnerability scanner, find the any vulnerability on the system. These; computers, servers, classified as examining the network or communication infrastructure. In addition, as a result of this analysis, the proposed countermeasures are evaluated by estimating the effectiveness of how it works better. There are advantages and disadvantages of security scanners in the table below ("An Overview of Vulnerability Scanners", 2008).

2.2.3. Vulnerability Scanner

The purpose of the vulnerability scanner, find the any vulnerability on the system. These; computers, servers, classified as examining the network or communication infrastructure. In addition, as a result of this analysis, the proposed countermeasures are evaluated by estimating the effectiveness of how it works better. There are advantages and disadvantages of security scanners in the table 3 below ("An Overview of Vulnerability Scanners", 2008)

Table 03. Advantages and disadvantages of security scanners

Advantages	Disadvantages
It is determine the problem earlier.	Scanning can occur new vulnerabilities or system configuration changes, such as introducing new vulnerabilities, it needs to be done regularly.
A vulnerability malicious machines that could endanger the overall system and network security scanner that can help you determine.	Human reasoning is required.
A vulnerability scanner helps to verify the inventory of all devices on the network. Inventory device type, operating system version and patch level, includes hardware configurations and other relevant system information. This information is useful for security management and monitoring.	A vulnerability scanner is designed only to discover known vulnerabilities.

In the following sections, providing information about the next-generation firewalls, various corporate firewall preferences and those preferences are discussed indicate the level of success in securing corporate information in line.

2.2.4. Firewall

The another method is firewall used by corporate for information security. A firewall is not a particular piece of software or hardware. Which can be used for protecting the system from outside attack against hardware or software solution. The firewall is the main aim to control access to the system or to protect.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Firewalls protects against threats that might systems by filtering system. There are three different types of firewall. These; packet filtering, application level gateways, and circuit-level gateway. There are advantages and disadvantages of the method of the firewall in the following table 4 (Stallings, 1995).

Table 04. Advantages and disadvantages of the method of the firewall

Firewall	Advantages	Disadvantages
Static Package Filtering	Low Cost Efficient Performance According transparent to users	Limited control capabilities. They are not hidden the inside network structure. They can only understand the network protocols.
Dynamic Package Filtering	The attacks are blocked at the top level. According transparent to users. Included all OSI models.	It is difficult to make advanced user registration. It is difficult to make the filters of complex applications.
Proxy Servers	Setting and programming is easy. It has control and user recording tools. They can understand the protocols in the application layer.	Low performance. According transparent to users

Today, a new generation of firewall species were also introduced. Palo Alto Networks firewall is a new generation will be examined below.

Palo Alto Networks

The development of technology users want to access different applications, but consideration of the security risks. There were two basic options for security technology in the past; business interests or to enable everything to prevent anything in terms of network security. Palo Alto Networks firewalls, while also allowing access while preventing the threat of cyber security application that allows you to enable your users require in a safe manner.

Palo Alto Networks is designed to address the most developed attacks every aspect of enterprise security platform is the basis. Also, it examines all traffic, type of location or device connects as separate users.

This platform helps addressing the security requirements of a number of institutions based on common principles. Corporates, on the one hand while supporting business initiatives by using a balanced combination of the global threat information with network security and endpoint protection also improves the overall security posture and security incident will reduce the response time (Palo Alto Networks).

2.3. Elements of Enterprise Information Security Threats

There are many factors that threaten the security of the enterprise. It may be both internal and external. Internal threats can be given as an example uninformed and irresponsible use or misuse of the. Ignorant and irresponsible use, you can delete the database if an employee is receiving enough training and may cause information to be lost. The malicious acts, an employee of the network "sniffer" e-mails or read information about the corporation's staff who have been dismissed are examples of reasons to change the network.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

The external attacks are divided directed target attacks and into the attacks indiscriminately. Attacking the server or changing the studies mentioned website as an example of target attacks indiscriminately virus attacks, worms and trojan attacks are examples of the backdoors (Özavcı, 2015).

2.4. Type of Attacks

The attacks against the information of the enterprises, being dominated by the methods and techniques for the removal characteristics of the attack and is extremely important in terms analyzing of the aggressive profile (Canbek & Sağıroğlu, 2007). Attackers who violated security of the systems, they achieve these goals by using different methods. These attacks are divided into four categories (Allen, 2001). These are, Interruption, Intercept, Modification, Fabrication (see table 5).

Table 05. Type of Attacks

Interruption:	The purpose of this attacks, interrupt the exchange of information between target systems. DoS, DDoS as an example of this attacks.
Intercept:	It is listening between source and computers communication. Network sniffing is example of this attack.
Modification:	The data sent to the target computer during the exchange of information captured by the attackers changed the destination is sent to the user. Safety integrity principle in this type of attack are being violated.
Fabrication:	This attack has a new data generated by the attackers. Attack will occur with fake data sent to the target.

Attack analysis are divided five catogories, these; discovery, scanning, providing access, maintain and access tracks (Burlu, 2013). The purpose is information gathering about the target. For example, capture the e-mail corporate's personnel. In the scannig part, based on the information obtained during the discovery phase before the attacks made final preparations are made for a variety of scanning. Attackers are using vulnerability into the system gained at this stage. The purpose of the attackers, access the system share the unauthorized people with using exploits. In the part of continued access, attackers aim to benefit from the openness of the systems that have been seized. Thus, it can be captured through the system that provides access to other systems connected to the system. So, attackers use malicious software like trojan horse, backdoor and rootkit teams. The traces of the cleaning step, to eliminate the traces of others in order to avoid detection side attack made targets. Its aim is to leave evidence of the crimes it has committed.

2.5. Providing Enterprise Information Security Tools

Many studies have been carried to ensure the security of computer systems. These systems generally; To set up a firewall, to set up intrusion detection system, such solutions can provide secure communication protocols. However, it can be deficit the system to the benefit of the attacker. In order to avoid these uses various security tools. In addition, these tools also provide a system of monitoring (see Table 6). The main objective here is to take the necessary measures to detect before the offensive system is turned on. The main objective here is to take the measure to detect deficit of the system before attackers (Gündüz, 2013).

Computer security is occur during hiding or transport of data in the electronic media distortions and all the measures taken to protect it from unauthorized access. For this relevant determination of the security policy and must be applied. These policies, examining the effectiveness evaluation by keeping records of

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

different, there might be some usage patterns, such as limiting the access of monitoring and deletion (Gündüz, 2013).

Table 06. Type of information penetration tools

Sniffer	Vulnerability Scanner	Intrusion Detection Systems	Password Cracking	Rootkit Scanner	Port Scannner	Exploit Vulnerability Scanner	Web Vulnerability Scanner
Nmap	Nessus	Snort	John The Ripper	Tripware	Superscan	Metasploit	Burb Suite
TCP dump	GFI Life	Honeyd	Cain&Abel	AIDE		W3af	SQLMAP
Dsniff	Core Impact	OSSEC HIDS	Aircrack			Core Impact	W3af
Ettercap	Open VAS		THC Hydes			Sqlmap	Skip Fish
Wireshark	Nespose					Canvas	
	Retina						
	PSI						

Snort

Snort makes real-time traffic analysis for IP networks and is a means of determining a leak can save packages. It can detect attacks or threats by several studies. Snort is permitted or denied traffic to a flexible rule authoring language for defining and has a modular detection engine. Furthermore, it alerts the user after detecting attacks through the alarm mechanism.

TCP dump

TCP dump is the oldest network analysis and data mining program that allows network monitoring. It used to examine the network move. It can show the information in a packet network interface by mapping the given statements. Wireshark is more preferred moment in this process.

WIRESHARK

Wireshark is an analysis program that allows network monitoring such as TCP dump. Users can get information about the data analyzed in detail in an interactive way. The most prominent feature of the program is that Wireshark has a rich filtering language. Moreover, nowadays the preferred program for this purpose.

NMAP

Nmap is a program used in security monitoring and network research. Sending IP packets indicate computers that are active on the network. Also, the network can identify available applications on computers nmap can run on many operating systems.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

DSNIFF

Dsniff is a tool that allows teams to penetration testing. Dsniff includes filesnarf, mailsnarf, msgsnarf, urlsnarf and webspy tools. These programs are listening the networks passive style. Also, it is capture the important information such as password, email.

SUPERSCAN

Superscan is windows based programs. It is making port scan based on IP port range. Also, it is making tcp and udp scan successfully.

METASPLOIT

This is the most popular tool for penetration test. It is based on Exploit style for the enter the system. If ıt is successful on the target machine, it runs an excellent code for penetration testing. It is available web applications, networks and servers.

BURP SUITE

Burp suite is a very powerful platform that can be used for web attacks and to facilitate and accelerate Web attacks include a variety of interfaces and tools.

JOHN THE RIPPER

John the Ripper is a powerful password cracking tool, because multiple features for password cracking program is compatible with many platforms. It is working, DOS together with each version of the Linux operating system now, BeOS, OpenVMS, and can run on Windows.

Aircrack-ng

Aircrack one of the most popular tool for WEP/WPA/WPA2 cracking. Aircrack-ng Suite in the package and agreements seize / catch, depending on the user to give permission to remove permissions, create traffic, "Brute Force" and a variety of tools are available to do dictionary-based attacks.

TRIPWIRE

Tripwire is the oldest tools according the other rootkit scanners. It examines the detect files and directories. In the meantime there is a change system files by checking the warning system administrator. Although Linux is a free to paid software for other platforms.

CAIN & ABEL

Cain & Abel program developed for security experts, developers and network administrators. It is making package analysis, password information, Brute Force and Cryptanalysis methods for the target. It is one of the most popular tool for ARP Poison area. Cain & Abel program format used in Linux systems is Dsniff program.

https://doi.org/10.15405/epsbs.2019.12.03.27
Corresponding Author: Arif Sarı
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

SCAPY

Scapy a powerful interactive packet manipulation, packaging manufacturer, network discovery and listening tool package. Scapy is a low level tool, it can interact with the Python language. Scapy package or create the package sets, manipulate them, send over the line, the rest of the other packages on the line, allows classes to match the questions and answers (Baykara, Dastan, & Karadoğan, 2013).

2.6. Importance of Penetration Test- Dropbox Case

This section elaborates the importance of penetration tests for cloud storage services through discussing the latest data security breach event of Dropbox.

On 31st August 2016, unknown hackers leaked 68 million Dropbox user accounts including login emails and encrypted passwords from a breach that took place in 2012. Initially, the leaked data was accessible to several breach notification sites such as Hacked-DB, LeakedSource, and HaveIbeenPwned, but now a vendor going by the online handle of "DoubleFlag" is selling the sameDropBox data on a dark web marketplace known as TheRealDeal. In the following figure 1 shows DropBox usage by industry.

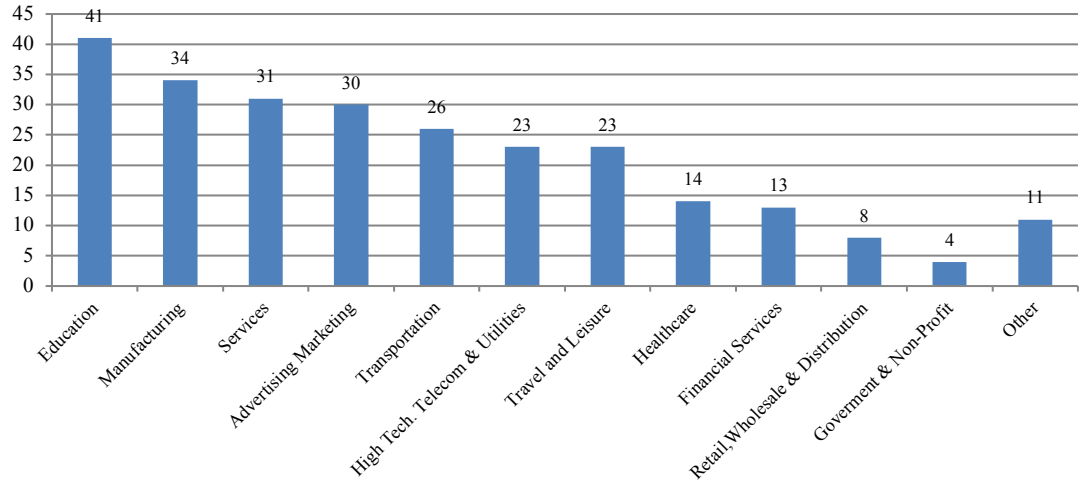

Figure 01. DropBox Usage by Industry

The data is being sold for 1209.38 US Dollar. The total number of accounts offered for sale are 68,679,804 which includes emails and encrypted passwords. There are 36,814,524 passwords that are encrypted with Secure Hash Algorithm 1 (SHA-1), 36,814,524 passwords are Brute force salt while 31,865,280 are encrypted with Blowfish encryption algorithm.

Hacked user credentials can be very valuable among data traders. Email and password data is typically bought and sold on the darknet, a tier of anonymous and largely untraceable Internet access that is often used for illegal activity such as drug or firearms trading. Large numbers of stolen user data can be integrated with software that automatically cycles though email/password combinations to hack into different websites. Given that many people reuse the same passwords on multiple websites, this can be a very effective method. Dropbox actually points to an employee's reused password hacked from another website as the cause of the 2012 Dropbox breach, according to a blogpost that year on its website. Dropbox

has a several big company clients such as Hyatt, HP Enterprise and Spotify. It can be very dangerous for these companies, because they can storage the important data in the DropBox cloud services.

3. Conclusion

Today, enterprise information technology as a result of increased attacks along with growing security needs have emerged. Enterprise takes the prevention with intrusion detection systems, vulnerability scanner and firewall. In this study, the advantages and disadvantages of the measures used to ensure safety were investigated. Snort intrusion detection tool in the system it is most preferred penetration tool. The Nessus vulnerability scanner is the most popular tool. Palo Alto Networks next-generation technology is a tool that is engineered with the highest level of firewalls. This study showed that the public and have concluded private institutions of information security to ensure the purpose of the opinion that not enough alone measures taken by, in order to prevent various security vulnerabilities, intrusion detection system, it is emphasized that security scanners and firewall technology system, it is important that it needs to work in sync with each other. But, human factor is most important things. As you can see, even if organizations have a best penetration tools can not block the human mistakes such as DropBox case.

References

Allen J. H. (2001). *The CERT Guide to System and Network Security Practices.* Addison-Wesley Professional.

An Overview of Vulnerability Scanners. (2008). Retrieved on 2008, February from https://www.infosec.gov.hk/english/technical/files/vulnerability.pdf

Baykara, M., Dağ, R., & Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi. 1st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, Elazığ, Turkey

Burlu, K. (2013). Bilişimin Karanlık Yüzü [Disinformatics: The Dark Side of Informatics]. Nirvana Yayınları.

Canbek, G., & Sağıroğlu, Ş. (2007). Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme. [Attacks Agaınst Computer Systems And Their Types: A Review Study]. *Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, *23*(1-2), 1-12.

Gündüz M. Z. (2013). Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti [IP-Based Evidence Detection]. (Master Thesis). Fen Bilimleri Enstitüsü, Fırat Üniversitesi. Retrieved from http://hdl.handle.net/11508/17376

Kalman, S. (2003). *Web Security Field Guide.* Indianapolis: Cisco Press.

Maliye Bakanlığı ISO27001 Raporu (2009). Retrieved from https://ms.hmb.gov.tr/uploads/2019/05/ISO27001.pdf

Özavcı, F. (2015). Bilgi Güvenliği–Temel Kavramlar [Information Security Basic Concepts]. Retrieved from https://seminer.linux.org.tr/wp-content/uploads/bgtk-210902.pdf

Palo Alto Networks® Yeni Nesil Güvenlik Duvarı Genel Tanıtım [Palo Alto Networks® Next generation Firewall Overview]. (2014). Retrieved from https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/datasheets/firewall-features-overview/firewall-features-overview-tu.pdf

Stallings, W. (1995). *Network and Internetwork Security*. New Jersey: IEEE press.

Vural, Y., & Sağıroğlu Ş. (2007). Kurumsal bilgi güvenliği: güncel gelişmeler. [Enterprise information security: Current Developments]. Proceedings of Information Security & Cryptology Conference with International Participation.