SETSCI conference proceedings

SETSCI Conference Proceedings
13 , 93-99, 2022

5th International Symposium on Innovative Approaches in Smart Technologies

28-29 May 2022, Turkey

ISAS 2022

https://doi.org/10.36287/setsci.5.1.018
eISSN: 2687-5527/

A Survey of Cyber-Threats for the Security of Institutions

Mehmet KARAKAYA[1*], Abdullah SEVİN[2+]

[1,2]*Department of Computer Engineering, Sakarya University, TURKEY.*
[*]*Corresponding author: mehmet.karakaya4@ogr.sakarya.edu.tr*
[+]*author: asevin@sakarya.edu.tr*

Abstract – Cyber security is an important concept, and its importance is increasing daily in every aspect of our daily lives. The increase in technology usage areas and rate in online platforms is one of the most important reasons for the security requirement. Today, the active use of information technologies is seen in many sectors, such as health, tourism, education, transportation, communication, and banks. Companies operating in these sectors may suffer severe financial losses, and their reputations may be damaged in case of possible cyber-attacks. This situation makes corporate information security an important topic. Cyber-attacks on companies can be implemented with various methods and techniques. It can be grouped as social engineering, physical attacks, and web application attacks. In this study, cyber-attack threats that institutions are exposed to were examined. The study aims to investigate the possible attacks that can be carried out on institutions. As a result of these examinations, it is a resource that provides an understanding of the importance of cyber security.

Keywords – Cyber Security, Corporate Information Security, OWASP

I. INTRODUCTION

The usage of information systems is increasing globally, and their establishment as an indispensable element in our lives presents the issue of ensuring the security of these systems as a vital topic. The systems can be captured by malicious people and rendered inoperable due to many reasons such as software failures, vulnerabilities in the technologies, unconscious users, and organized attacks. As a result, sensitive data such as credit card information and identity information can be stolen. With ransomware, systems can be disabled and material damage can be occurred. The interruption of systems that require continuity may cause the loss of life or property, such as health, military, and communication. Cyber-attacks can compromise the security of military systems. Today, cyber security emerges as a critical component of national security [1].

Cyber-attacks are defined as an increasingly complex attack method for institutions and companies. It should be taken into account that hackers also have increased their advanced capabilities and programs during technology development. Institutions should have a cyber defense plan that can respond to the attack before or in the event of an attack. Reputation and customer loss are more important than material damage. It has become necessary for institutions to create a cyber security action plan for the worst possible scenarios before, during, and after the attack. Institutions that do not have a cyber security plan or pay attention to cyber-attacks are easy targets for cyber hackers [2].

Raising awareness of cyber-attacks and recognizing threats is critical for information security. But to contend with cyber-attacks, there is a need for the main elements; attack detection and attack prevention. Taking action beforehand for attacks and the ability of the relevant employees are essential issues in terms of cyber security. However, no matter how many precautions are taken, it should be remembered that there is no such thing as absolute security. The ultimate goal is to make it difficult for cyber hackers to reach the target and intimidate the attackers [3].

The remaining sections are; literature research is mentioned in the second section. In the third section, corporate information security and its principles are presented. The types of cyber threats are detailed in the fourth section. The fifth chapter discusses the examples of cyber-attacks on institutions. In the last section, the results and general evaluations are given.

II. LITERATURE

There are many types of research and studies on corporate cyber security. Yasar [4] discussed the possible threats to corporate security and methods of struggle. The corporate cyber security action plans are emphasized. Yilmaz [5] examined the importance of software quality processes in providing cyber security. The questionnaire studies show that awareness of information security and secure software development is high. However, despite the increased attention, most institutions do not implement the necessary software quality processes. It has been proposed to make quality process certificates legitimate for institutions to solve this situation. Yildirim [6] analyzed the cyber security reports and questionnaires applied by different institutions. According to the observed results of the questionnaires, it was concluded that most institutions do not have a specific plan in case of a possible cyber attack. Most of them do not have cyber security experts, and they do not provide the necessary training to their employees. Senturk [7] presented the current attack methods and the most commonly used penetration test tools in his study. He showed active information gathering, passive information gathering, scanning for security vulnerabilities, web application attacks, and many similar attack methods. The article also includes a section on certificates and exams that can be taken in cyber security. Ozbay [8] presented active cyber defense techniques in his study with applications. He has realized tests in a lab setting to demonstrate how active cyber

defense can improve security in institutions. With these tests, it was concluded that active cyber defense techniques increase security. Aytekin [9] evaluated the national importance of cyber security in his study and examined Turkey's National Cyber Security Strategy and 2013-2014 action plans. As a result of his investigations, he identified the areas where the existing laws were insufficient. There are deficiencies in the training that need to be given in the fight against cybercrime, and improvements should be performed on budgeting and setting standards. Aydogdu and Gunduz [10] investigated the OWASP (Open Web Application Security Project) Top 10 2013 vulnerability list in their study. They researched and evaluated security solutions for vulnerabilities. Their work concluded that most of the vulnerabilities are caused by code flaws, and end-users and developers should be trained to prevent vulnerabilities. Also, intrusion detection methods should be used, and it is crucial to follow up on up-to-date vulnerabilities.

The studies aim to inform the relevant institutions about the importance of cyber security and the risks of a possible attack and raise awareness. In addition, it is desired that awareness-raising institutions take the necessary precautions to prevent possible attacks or minimize the damage.

III. Corporate Information Security

The security of information systems starts from the weakest point. Considering this principle, corporations should consider all assets that play a role in the cyber world as a risk and create a cyber action plan accordingly. An unconscious user move can compromise a heavily guarded system. This state is an example of a situation that summarizes the need and importance of cyber security. Corporations and companies are most exposed to cyber-attacks. The concept of corporate cyber security ensures increasing corporate information security awareness, data security, business continuity of critical corporate information, and secure communication system infrastructures. Figure 1 shows the percentages of vulnerabilities in web applications in different areas.

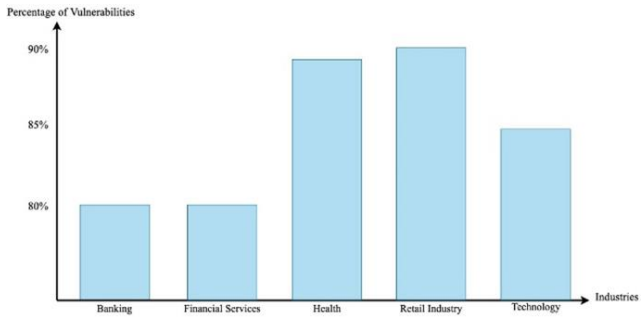

Fig. 1 Percent of vulnerabilities in web applications in different areas [10]

To ensure corporate cyber security, hardware, personnel, and all kinds of software mustn't pose a security problem. Critical analyses should be carried out adequately and periodically to prevent possible attacks. Figure 2 shows the categorization of cyber threats. Threats to corporate cyber security are divided into human and natural origins. Human-made threats consist of internal and external fragments. Unconscious users, spies, malicious personnel, system administrator errors, and developer errors can be internal threats to corporations. On the other hand, external threats generally include malicious attackers who resort to unauthorized access and data stealing from the Internet. Threats originating from nature mainly include floods, fires, and earthquakes that will cause the servers that are not correctly protected/backed up to be affected and damaged [4].

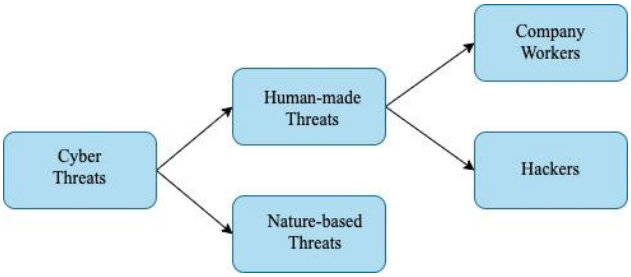

Fig. 2 Classification of cyber threats [4]

There are some challenges to implementing cyber-security for organizations. Lack of human resources, framework selection, awareness, dedicated budgets, management commitments, maturity of the organization, and security by compliance are some of the challenges given in Figure 3 according to institutions.

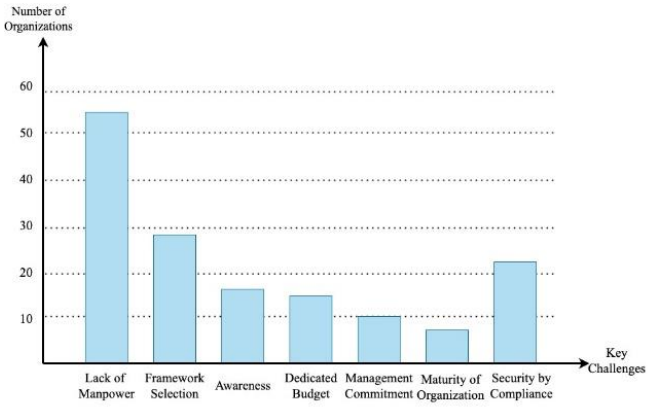

Fig. 3 Challenges for implementing cybersecurity for the organizations [11]

Cyber security for institutions and organizations is to provide the three basic principles of cyber security; confidentiality, integrity, and accessibility. Each element should not be considered independently of the others. The confidentiality of inaccessible information and the integrity of externally accessed information does not indicate that they are secure [12].

Confidentiality: It is the protection of information against unauthorized access. Only those who have permission to access the data should access it. Generally, institutions create specific rules and laws to ensure this principle.

Integrity: Information is not changed by unauthorized persons. This principle aims to ensure that data is protected completely. Even the damage to a small part of the information can mislead the decision-making mechanisms and cause significant problems.

Accessibility: It is the access and use of the information by authorized persons. It needs to be configured correctly and securely [13].

IV. Cyber Threats

A. Cyber-Physical Attack

The first thing that comes to mind is remote, network-based attacks regarding cyber-attacks. However, many cyber attacks

can be carried out using physical tools. USB ports on computers or phones can be used in physical attacks. There are some methods as port protection systems incorporate companies to prevent cyber attacks carried out by physical methods. These systems avoid devices capable of entering data into the ports. These ports only allow input/output units such as the keyboard and mouse to reach the computer. It completely prevents data exchange from being made by physical means [4].

B. Social Engineering

Various software and hardware precautions are available as a solution to cyber attacks. However, there may be a type of cyber-attack that falls outside of all precautions. This type is called social engineering. Social engineering means capturing sensitive and private information of a specific institution or person using human relations [3]. It is carried out by persuading, influencing, deceiving, and taking advantage of carelessness. For example, a company receives software support from an institution and constantly communicates via e-mail. If the attackers have this information, they can reach the institution's employee who did the interviews with the company through an e-mail address that looks as if it belongs to the company but has a different extension. The employee's inattention and failure to notice the error in the e-mail at that time will cause him to share sensitive data with the attacker or fulfill the attacker's demands without question. [4]

Social engineering attacks can be examined under two main methods: human-based and software-based attacks, summarized in table 1. In human-based attacks, a limited number of users are affected, as there is an attack on the target directly. The success rate is high in this method. In software-based attacks, attacks are carried out by using devices such as computers and mobile phones. Multiple targets can be affected in a short time. There are special add-ons for these attacks [14].

Table 1 Comparison of human-based and software-based attack types [14]

Attack Technique	Advantages	Disadvantages
Human-based	- Easy to raise awareness of people - Low number of affected people - High efficiency	- Easily affect people emotionally - Benefiting from a sense of trust - Take advantage of the tendency to want more
Software-based	- High efficiency	- High system costs - Doesn't work if the user is conscious

In addition, within the scope of this study, a phishing attack was simulated using SeToolKit (SET) tool in the Kali Linux environment. Within the scope of the attack, we imitated an e-mail environment. It is aimed for the target user to log in to this address with his user information. As a result, this information has been obtained. The mail application environment and results are shown in Figures 4 and 5.

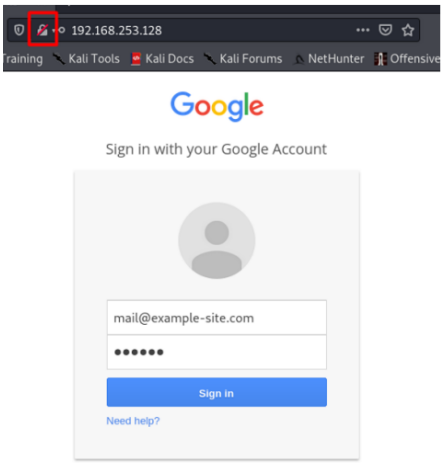

Fig. 4 Image of the mail application used for the phishing attack

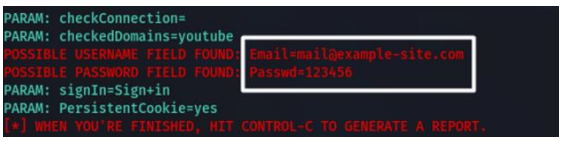

Fig. 5 Displaying user information on the SeToolKit terminal screen after the phishing attack

It is necessary to provide periodic cyber security courses to employees in institutions, disseminate software using natural language processing techniques within the institution, prevent harmful content as much as possible with various software, or show warnings to users. On the other hand, individuals should take extra care and attention, especially in the transactions where they send sensitive information.

C. Web Application

In this section, the OWASP Top 10 vulnerabilities list is referenced to assess cyber threats in detail. OWASP stands for Open Web Application Security Project. OWASP is a free community that aims to eliminate web application vulnerabilities and ensure security in these applications [15]. OWASP collects information from many companies and people who work on web application penetration testing. Afterward, it analyzes this information, provides the statistics of the ten most risky security vulnerabilities for the relevant year, and offers them free. Figure 6 shows the attack level for various organizations.

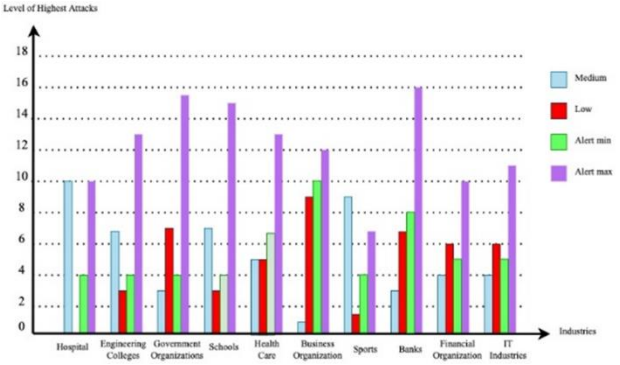

Fig. 6 Attack levels for different organizations [16]

Broken authentication is an attacker impersonates users who have access to the system and compromises the system (Figure 7). Attackers can carry out this attack in various ways. For

example, several attacks can be performed for uncomplicated, easily guessed passwords, or passwords not stored securely pose a threat. For instance, SQL (Structured Query Language) injection attacks can compromise passwords kept openly in databases. Again, passwords and credentials supported openly on the URL (Uniform Resource Locator) structure pose a significant risk [17].

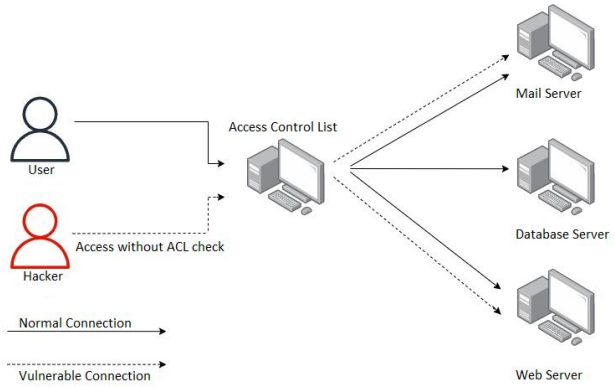

Fig. 7 Broken Access Control

Cryptographic failures can be defined as capturing sensitive and protected data using insufficient or unsafe encryption methods. Situations like keeping data in the database unencrypted and using weak encryption keys can cause this vulnerability. Considering large-scale systems, the importance of protection against this vulnerability increases even more [17]. For example, passwords, credit card numbers, health data, personal information, and trade secrets are sensitive data that require extra protection. According to the GDPR (General Data Protection Regulation) of the European Union, necessary institutional and technical precautions must be taken to protect such sensitive data. These data cannot be processed or shared without permission.

Injection attacks can be studied in a wide area. These attacks occur when attackers find a weakness at any of the entry points in the system and send malicious code from that point. They can directly damage the system or capture confidential data. There are many types of SQL injection attacks. For example, in error-based attacks, the attacker using the SQL error message generated by the system captures confidential data. Another type of SQL injection is Union-based attacks. In these attacks, the attacker uses the union key, which can pull data from two different tables and accesses other tables and data through the existing SQL query. Code injection attacks are carried out by reaching the main server computer of the system and executing malicious codes. These attacks; can be prevented by verifying user logins and completely blocking processes that will affect the system [17].

In order to create the attack environment, a virtual machine that has SQL injection vulnerability was established. HTTP-based injection attack, one of the most common attack forms, was organized on this installed machine. After the attack, it was observed that the relevant records came from the database, as shown in Figure 8.

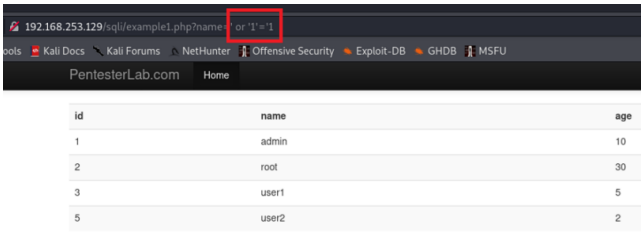

Fig. 8 SQL Injection Attack

The insecure design focuses on the risks associated with design flaws. The use of design patterns, threat modeling, and reference architectures should be given due importance and should be included in the systems to protect from attacks. Accurate security controls and identifications are more difficult in a system with design flaws. However, it is easier to provide security in systems with a secure structure by design. Developing a secure system; requires a secure software development lifecycle, a specific design pattern, certain components, and threat modeling. In other words, support should be obtained from experts in security at every stage of the software [15].

Security misconfiguration refers to when security configurations are misconfigured to expose them to threats. Misconfigurations in the firewall and open ports that allow remote attacks can cause these attacks. Some of the precautions that can be taken to prevent such attacks are passing the configurations through a specific quality assurance process, testing, and verifying the changes made in a controlled manner [17].

Today, almost every system has a dependency on specific components. Known, existing vulnerabilities in these outdated components can cause vulnerabilities. Attackers prioritize using existing vulnerabilities rather than discovering new vulnerabilities. The dependencies of the current system should always be kept under control to protect against such types of attacks. Deprecated dependencies that are outdated or unused components should be removed. The monitoring and updating of the dependent components should be included in the maintenance life cycle of the existing system and should be followed within specific procedures [17].

Areas such as authentication and session management are critical points in these attacks. It can occur when there is no protection against brute force attacks in the system, default usernames or passwords, insecure designed password forget/renew processes, and cryptographic vulnerabilities in session data. Passwords should be forced to be complex, session data should not be displayed in URLs, session duration should be limited, error messages given in faulty login attempts should be checked, and the number of attempts at system logins should be limited to prevent such these attacks [17].

Software and data integrity failures related to code and infrastructures do not protect against integrity breaches. An example is that the system relies on libraries, plug-ins, and modules obtained from insecure sources. In addition, many systems today have automatic update features. This process may pose the risk of being updated without adequate integrity verification. Attackers can upload their malicious code to a widely used plug-in, and systems with this plug-in can be automatically attacked [15].

It is vulnerable when the recording and control of security-related situations are insufficient. In this case, attack attempts

by attackers may continue undetected. This state complicates detection and defense against possible attacks and slows down operations [17]. Some of the situations include logs of transactions like login; failed login attempts are not logged, error messages in log records containing insufficient information, and local storage of log records only.

In the Server-Side request forgery attack, attackers send requests on behalf of the system, as shown in Figure 9. The attacker can change the requests to the target server and enter the desired data in the parameters. Failure to check the allowed domains and protocols in recommendations made by the server to remote resources causes this vulnerability [15].

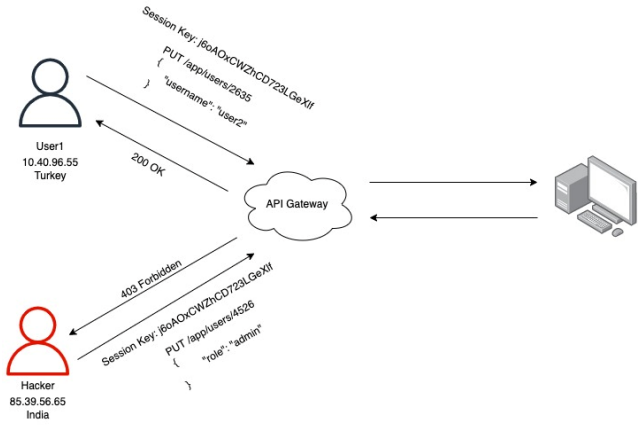

Fig. 9 Server-side Request Forgery

DDoS (Distributed Denial of Service) attacks can be divided into two groups bandwidth-consuming and resource-consuming attacks. In bandwidth-consuming DDoS attacks, unnecessary and large numbers of packets are sent to the target computer. In resource-consuming DDoS attacks, it aims to consume the target computer's resources.

An Apache2 web server based on Ubuntu was chosen as the target system in the example scenario to test. Slowloris tool developed with python was used for DDoS attacks. Slowloris tool primarily sends too many HTTP requests. It then sends header information every 15 seconds to keep connections open. As soon as the server closes the connection, it creates a new connection and tries to consume the server's connection socket resource. When the attack is analyzed with Wireshark, it is observed that a large number of TCP packets are sent periodically and simultaneously, as shown in Figure 10.

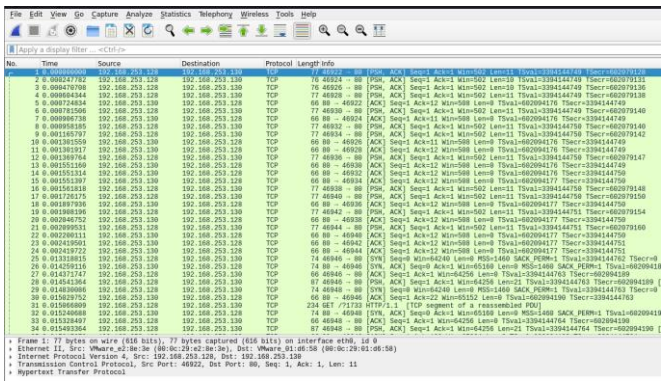

Fig. 10 Examining DDoS attack packets with Wireshark

D. Web Application Attacks Statistics

OWASP also includes many CWE (Common Weakness Enumeration) data in the list of vulnerabilities it publishes. CWE is an organization that lists, classifies, and measures software and hardware vulnerabilities to help with software security and reduce vulnerabilities (Figure 11). Another data frequently encountered in OWASP documents is the CVE (Common Vulnerabilities Enumeration) list. The goal of the CVE is to identify, determine and categorize publicly available cybersecurity vulnerabilities [18].

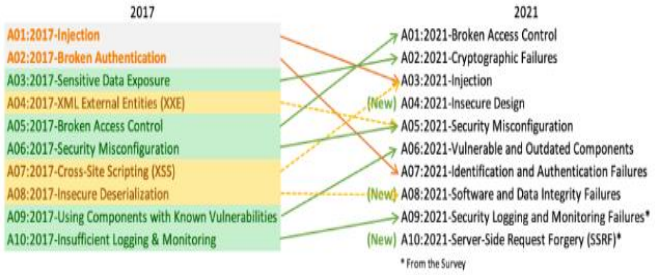

Fig. 11 OWASP Top 10 chart and change over the last four years [15]

In the Top ten vulnerabilities list made available by OWASP, some data factors are given for each category in table 2. Their descriptions are as follows:

- Mapped CWEs: The number of CWEs matching the relevant category.
- Incidence Rate: Percentage of CWE-vulnerable applications tested by that organization for the year.
- Weighted Exploit: Exploit sub-score of CVSSv2(Common Vulnerability Scoring System) of CVEs and CVSSv3 scores.
- Weighted Impact: Impact subscore of CVSSv2 and CVSSv3 scores of CVEs.
- Coverage: Number of applications tested by all organizations for a given CWE.
- Total Occurrences: The total number of applications where CWEs are mapped to the relevant category.
- Total CVEs: Total number of CVEs in the National Vulnerability Database mapped to CWEs mapped to the relevant category [15].

Broken authentication vulnerability ranks first in the OWASP Top 10 list for 2021. In the data set made by OWASP, over 318 thousand samples are analyzed; this vulnerability was found at a rate of 94%. Unauthorized access to sensitive information and cross-site request forgery are some of the vulnerabilities under this heading [15].

In the list, some vulnerabilities cover each other. For example, security misconfiguration includes injection, broken access control, identification and authentication failures, and many vulnerabilities. At the same time, broken access control and identification and authentication failures also overlap to a certain extent [19].

Table 2 OWASP Top 10 data factors

OWASP Top 10	CWE's Mapped	Avg. Incidence Rate	Avg. Weighted Exploit	Avg. Weighted Impact	Avg. Coverage	Total Occurrences	Total CVE's
Broken Access Control	34	3,81	6,92	5,93	47,72	318,487	19,013
Cryptographic Failures	29	4,49	7,29	6,81	34,85	233,788	3,075
Injection	33	3,37	7,25	7,15	47,90	274,228	32,078
Insecure Design	40	3,0	6,46	6,78	42,51	262,407	2,691
Security Misconfiguration	20	4,51	8,12	6,56	44,84	208,387	789
Vulnerable and Outdated Components	3	8,77	5,0	5,0	22,47	30,457	0
Identification and Authentication Failures	22	14,84	7,40	6,50	2,55	132,195	3,897
Software and Data Integrity Failures	10	2,05	6,94	7,94	45,35	47,972	1,152
Security Logging and Monitoring Failures	4	6,51	6,87	4,99	39,97	53,615	242
Server Side Request Forgery (SSRF)	1	2,72	8,28	6,72	67,72	9,503	385

V. Examples of Cyber Attacks on Companies

A. Sony

Some attackers hacked 77 million Playstation users and 24.6 million Sony online users in April 2011. People's passwords, credit card information, order history, and addresses are among the stolen data. Sony facilities were severely affected by the earthquake in Japan in March of the same year. This situation allowed the attack in April to cause even more casualties. The total estimated loss is $171 million. However, this loss does not include compensations, losses due to misuse of stolen credit card data, or a decrease in the brand's market value [20].

B. JP Morgan

In 2014, JP Morgan Chase, one of the largest U.S. banks, reported that some of its servers had been accessed by hackers for administrative access. The account holders' names, phone numbers, and addresses were seized in this attack. Seventy-six million households and 7 million small businesses were affected. JP Morgan has updated its security systems and hired many new employees. In addition to financial losses, it lost its reputation in the market. Many users have fallen victim to e-mail scams due to compromised contact data [20].

C. Aramco Oil Company

On August 15, 2012, a group close to Iran attacked Aramco, one of the vital oil companies of Saudi Arabia. The attack on the company, which has a market value of around 2 trillion, was carried out with an attack transmitted by an employee's USB inserted into the computer. It was aimed to delete data with the virus called Shamoon and Distract. The attackers, who carried out the attack, published the I.P. (Internet Protocol) addresses of the infected computers on the Internet. The damage caused by the attack could be brought under control in 2 weeks with the joint work of the USA, Israel, and Russia. About 30 thousand computers belonging to the company became unusable due to the attack. As a result of the attack, material damage, and loss of reputation, the country also suffered significant damage [5].

D. Ashley Madison

In July 2015, people's account data registered with Ashley Madison, a dating site, were stolen. Personal data of 33 million accounts were leaked. The attack on the site, whose most crucial principle is privacy and security, damaged its reputation to a great extent. A lot of lawsuits were filed against Ashley Madison after the attack. In the leaked personal data, it was seen that many members had e-mail addresses with the ".mil" domain name found in people serving in the U.S. military. Many members went to jail as dating sites were a crime in the U.S. military. In addition, many well-known personalities got divorced or discredited due to the disclosure of their memberships [20].

As seen in exemplary cyber-attacks, corporate companies have suffered in many ways. These can be listed as material damages, loss of reputation, psychological effects, loss of employees, etc.

VI. CONCLUSION

It has been observed that some methods can be performed very simply to avoid cyber-attacks. In addition, robust and various tools can provide for the attackers. Although organizations are doing their work in cyber security, the number of devices that receive I.P. addresses is generally very high. The higher the number of devices increased the potential target for hackers. It should be kept in mind that a misconfiguration, a forgotten port, or a loaded vulnerability can endanger the entire system's security. With the developing technology, cyber hackers are also developing new attack methods. It is necessary to identify the risks, intervene in the identified risks, and use the ISMS (Information Security Management System) within the scope of specific standards. At this point, penetration tests are performed as an essential tool. With the penetration tests carried out before the attack, existing security vulnerabilities in applications and services can be detected, and precautions can be taken. It should not be forgotten that the most critical element in cyber security is people. Institutions should first create a cyber security action plan within the organization and provide cyber security courses to their employees at regular periods as specified in this plan. The sites that employees try to access download files and input or output devices should be kept under control with the appropriate software. Application development units should use secure software development methodologies in software development processes. If there are critical points in the developed application, the approval of the cyber security units should be obtained.

The concept of 'national' is essential in all fields, but this concept has come to an equivalent point with independence nowadays in technology. The fact that the technologies used are not national makes our country depend on the countries producing technology. Still, it will not provide us with one hundred percent confidence in how the data used by these technologies are processed. The use of the national operating system, the support of technology companies and Research-

Development studies, the preference for open-source software, and the training of qualified personnel are essential in this regard.

REFERENCES

[1] Akyıldız, M.A., Evaluation of Penetration Tests with Applications in Cyber Security. Süleyman Demirel University, Graduate School of Natural and Applied Sciences, Department of Electronic Communication Engineering, Master Thesis, 2013.

[2] Aytekin, A., Evaluation of Turkey's cyber security strategy and action plan, Gazi University, Institute of Informatics, Department of Information Systems, Master Thesis, 2015.

[3] Arda, E., A Real-Time System Proposal on Awareness, Detection and Prevention of Attack Threats in the Cyberspace Environment. Baskent University, Graduate School of Natural and Applied Sciences, Department of Computer Engineering, Master Thesis, 2020.

[4] Yaşar, H., Threats to Corporate Cyber Security and Fighting Methods: An Action Plan Example. Gazi University, Institute of Informatics, Department of Management Information Systems, Master Thesis, 2014.

[5] Yılmaz, S., The Importance of Software Quality Processes in Providing Cyber Security. Gazi University, Informatics Institute, Department of Computer Science, Master Thesis, 2015.

[6] Yıldırım, Y.E., Cyberattacks on information systems and providing cyber security. International Occupational Sciences Symposium, Ankara University, 2018.

[7] Şentürk, M.Y., Current Cyber Attack Methods, Penetration Testing Tools and Application on a Representative Corporate Network. Turkish Aeronautical Association University, Department of Electrical and Computer Engineering, Electrical and Computer Engineering Program, Master Thesis, 2018.

[8] Özbay, R., Active cyber defense techniques and performance analysis. Afyon Kocatepe University, Graduate School of Natural and Applied Sciences, Department of Internet and Information Technologies Management, Master Thesis, 2015.

[9] Aytekin, A., Evaluation of Turkey's cyber security strategy and action plan, Gazi University, Institute of Informatics, Department of Information Systems, Master Thesis, 2015.

[10] Aydoğdu, D., Gündüz, M., A Research on Web Application Security Vulnerabilities and Security Solutions, International Journal of Information Security Engineering, Volume 2, 1-7, 2016.

[11] Bahuguna, A., Bisht, R.K., Pande, J., Roadmap amid chaos: cyber security management for organizations. 9th International Conference on Information Processing, Communication and Network Technologies, 1-6, 2018.

[12] Fussell, R.S., Protecting Information Security Availability via Selfadapting Intelligent Agents. Military Communications Conference, IEEE, 2005.

[13] Aşan, H., Gökşen, Y., A Tool for Security and Process Efficiency in Web Applications: DEBSA. Atatürk University, Journal of Economics and Administrative Sciences, 2020.

[14] Salahdine, F., Kaabouch, N., Social Engineering Attacks: A Survey, Future Internet, MDPI, 2019.

[15] www.owasp.org/www-project-top-ten., Accessed time: 18.11.2021.

[16] https://vulners.com/d0znpp/D0ZNPP: BB56737687F42F8AF85734B9ECA05C33., Accessed time: 28.12.2021.

[17] Bach-Nutman, M., Undestanding the Top 10 OWASP Vulnerabilities, Bournemounth University, United Kingdom, 2020.

[18] www.cve.org/About/Overview., Accessed 07.12.2021.

[19] Devi, R., Kumar, M., Testing for Security Weakness of Web Applications using Ethical Hacking. Fourth International Conference on Trends in Electronics and Informatics (ICOEI 2020).

[20] Agrafiotis, I., Nurse, J., Goldsmith, M., Creese, S., Upton, D., A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, 2018.