IMPLEMENTATION OF TECHNIQUES TO AVOID CYBER ATTACKS

Dr. Neelam Naik, Assistant Professor
SVKM's Usha Pravin Gandhi College of Arts, Science, and Commerce
Vile Parle, Mumbai
neelamnaik08@gmail.com

Ms. Sneha Nathwani, Student
MScIT Part I, SVKM’s Usha Pravin Gandhi College of Arts, Science and Commerce
Vile Parle, Mumbai
Sneha.Nathwani@svkmmumbai.onmicrosoft.com

ABSTRACT

It has been observed that there is an increase in cyber-attacks in today's world. This attack causes a lot of losses to companies and on a personal level. Several measures need to be taken care of by the user as well while developing the app or website. The practice of defending programs, systems, and networks from online threats is known as cyber security. These assaults typically aim to gain access to, alter, or destroy sensitive data, demand money from users, or obstruct regular business operations. Attacks can take many different forms. Only during the software development process, the method for preventing cyberattacks can be taken into consideration. The present study aims to focus on gathering cyber-attack-related information from software developers who are there in this domain for a long. The information gathered was related to cyber-attacks that the developers were aware of. Special techniques are needed to be considered to avoid cyber-attacks while developing any application or website. The survey focuses on gathering information about the techniques used to avoid cyber-attacks, the possibility of prevention of attacks after the implementation of these techniques, the stage of the software development lifecycle in which implementation of such techniques is taken care of, and the effect of implementing these techniques on the performance of the System.

Keywords: Cyber Security, Cyber Threats, Cyber Attacks, Website Development, SQL Injection

Introduction

Life has become more and more comfortable with the spread of various digital devices and the Internet. All good things have a downside, and that is true in today’s digital world as well. The Data-Internet service has brought about great changes in our lives today, but it also poses great challenges in securing data. This leads to cyber-attacks. Defenders must cover all potential weaknesses, whereas attackers only need to discover one. Attackers can take unorthodox routes, take advantage of system confidence, or employ destructive methods because they are not bound by any regulations. Defenders must try to protect their assets, do little damage, and incur little expenses. Security infrastructure downgrades attackers to the weakest link. Attackers typically progress from the simplest level to the most severe level of compromise. The weakest link attracts the most attacks. Each security measure should complement the others and be just as effective.

When a third-party gains access to a system or network without authorization, it is called a cyberattack. Cyberattacks have several negative effects. Attacks may result in data breaches that cause data loss or data modification. Financial losses, a decline in customer trust, and reputational harm are the results for organizations. The practice of preventing unwanted digital access to networks, computer systems, and the parts that make them up is known as cybersecurity. Attackers will target any device that is connected to the Internet. Attackers and malicious software will continuously investigate it to find flaws. There are several types of cyber-attacks as shown in figure 1

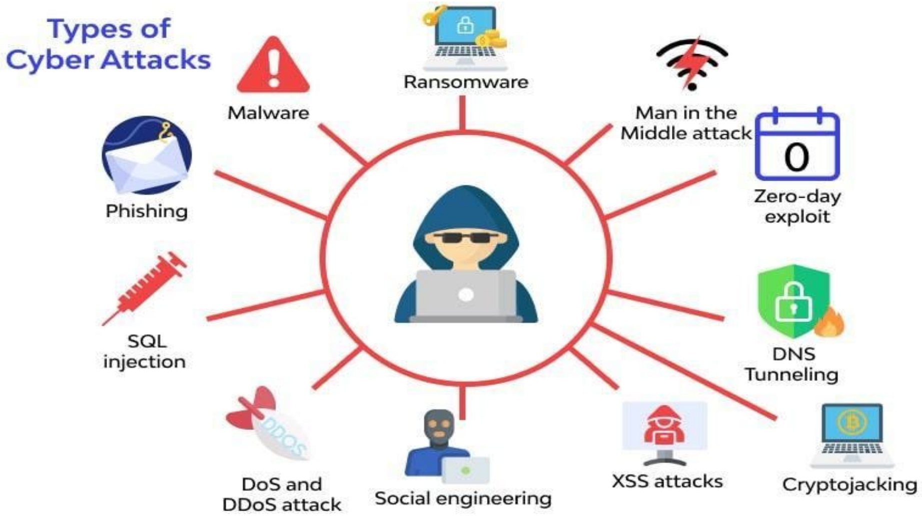


Figure 1: Types of cyber-attacks (Source: https://www.wallarm.com)

Malware attack - An example of a malware attack is when malicious software (malware) is introduced into a computer system or network to cause harm, steal data, or gain unauthorized access. Malware can take on many different shapes, such as viruses, worms, Trojan horses, ransomware, spyware, and adware. Malware assaults can be launched via a few channels, like phishing emails, corrupted websites, or malicious software downloads. Once installed, the virus may cause a variety of issues, including interrupting system performance, stealing sensitive information, encrypting data, and granting the attacker illegal access. To avoid malware assaults, maintain software and security systems up to date, use strong passwords, and exercise caution when opening email attachments or clicking on links from unfamiliar sources

Phishing attack - Phishing is a sort of cyber-attack in which an attacker poses a reputable business, such as a bank, online merchant, or social networking platform, to dupe a victim into supplying personal information or clicking on a dangerous link. Phishing assaults are commonly conducted via email, instant messaging, or social media. A phishing assault attempts to persuade the target to perform a certain action, such as entering login credentials or supplying personal information that can be exploited for identity theft or other illicit reasons. Phishing attacks frequently include social engineering techniques, such as haste or fear, to create a sense of urgency or panic and raise the victim's probability of falling for the hoax. To avoid phishing attempts, be cautious when clicking on links or opening attachments from unfamiliar sources, and double-check the legitimacy of any request for personal or sensitive information before delivering it. This may be accomplished by inspecting the website's address, searching for the padlock icon in the browser, and contacting the organization directly to confirm the request.

Password attack - In a password attack, an attacker attempts to figure out or crack a user's password to access their account or system. Password assaults can take several forms, including brute force, dictionary, and phishing attacks. The attacker uses software to guess every conceivable combination of characters until the right password is determined in a brute-force assault. A dictionary attack tries guessing the password using a collection of common passwords and variants. A phishing assault includes duping the victim into providing their password via a bogus login page or email. It is critical to choose strong, using passwords that are challenging to crack to safeguard against password assaults. A strong password is at least 12 characters long and comprised of uppercase and lowercase letters, numbers, and symbols. Employing two-factor authentication, which needs an additional form of verification in addition to a password, can also offer an extra degree of protection.

Man-in-the-Middle attack - When an attacker intercepts communication between two parties, such as a user and a website, and eavesdrops on or modifies the communication without the parties' knowledge, the attack is known as a man-in-the-middle (MITM) cyberattack. To do this, the attacker may employ a variety of techniques, such as session hijacking, DNS spoofing, or Wi-Fi eavesdropping. If the attacker has obtained access to the communication, they can eavesdrop on it to collect sensitive information such as login passwords or financial information, or they can change it to implant malware or divert the user to a bogus website. To avoid MITM attacks, utilize secure communication protocols such as HTTPS, which encrypt communications and protect against eavesdropping and alteration. A virtual private network (VPN) can also provide further security by encrypting all communication between the user and the internet, making it more difficult for attackers to intercept.

SQL Injection - SQL injection is a sort of cyber-attack that specifically targets websites or programs that use a SQL database. To manipulate the database and steal or change sensitive information, malicious SQL code is inserted into a website's input fields, such as search boxes or login forms. SQL injection can be used by the attacker to extract information such as usernames and passwords or to manipulate data in the database. This can lead to data loss, illegal access, or even a total takeover of the targeted system. To prevent SQL injection attacks, developers must use safe coding standards such as input validation and parameterized queries to prevent unauthorized database access. Moreover, frequent security audits and upgrades to software and online applications can aid in the prevention of SQL injection vulnerabilities.

Denial of service attack - A Denial of Service (DoS) assault is a form of cyber-attack that seeks to overload a website, application, or network with traffic or requests to impair its availability. This is accomplished by flooding the target system with a huge number of traffic or requests from various sources, rendering the system incapable of responding to genuine requests. A DoS attack causes the target system to become unresponsive or crash, rendering it inaccessible to users. This may lead to considerable financial losses for enterprises as well as user annoyance and irritation. It is critical to have suitable network security measures in place to guard against DoS assaults, such as firewalls and intrusion prevention systems. Furthermore, by lowering the volume of malicious traffic that reaches the target system, rate limiting, or traffic filtering methods can assist to lessen the impact of a DoS assault.

Insider Threat -An insider threat is a cyber security danger that originates within a company. It is committed by a current or former employee, contractor, or another trusted individual who has allowed access to the organization's systems, data, or network and utilizes that access to cause harm or perform malicious activities. Insider threats can take many different forms, such as stealing sensitive information, sabotaging systems or data, or gaining unauthorized access to networks or accounts. Insider threats can be purposeful, such as an employee motivated by monetary gain or retribution, or inadvertent, such as an employee who unintentionally reveals critical information due to negligence or human error. Organizations can establish access restrictions and monitoring, security awareness training, and background checks for workers and contractors to prevent insider risks. Moreover, frequent audits and incident response planning can aid in the detection and response to insider threats.

Crypto-jacking - Crypto-jacking is a sort of cyber-attack in which an attacker mines cryptocurrency on a victim's computer or device without their knowledge or consent. The attacker often does this by infecting the victim's machine with malware, such as a browser-based mining script that mines bitcoin for the attacker using the system's computing power. The victim may notice that their system is functioning slower than normal, or that their electricity bill has increased because of higher processing power utilization. The victim, on the other hand, may be unaware that their system is being exploited to mine bitcoin.

Cyber-attacks and their Impact on Business

A successful cyberattack could have disastrous effects on your company. This may have an impact on your revenue as well as the confidence of customers and the reputation of your company.

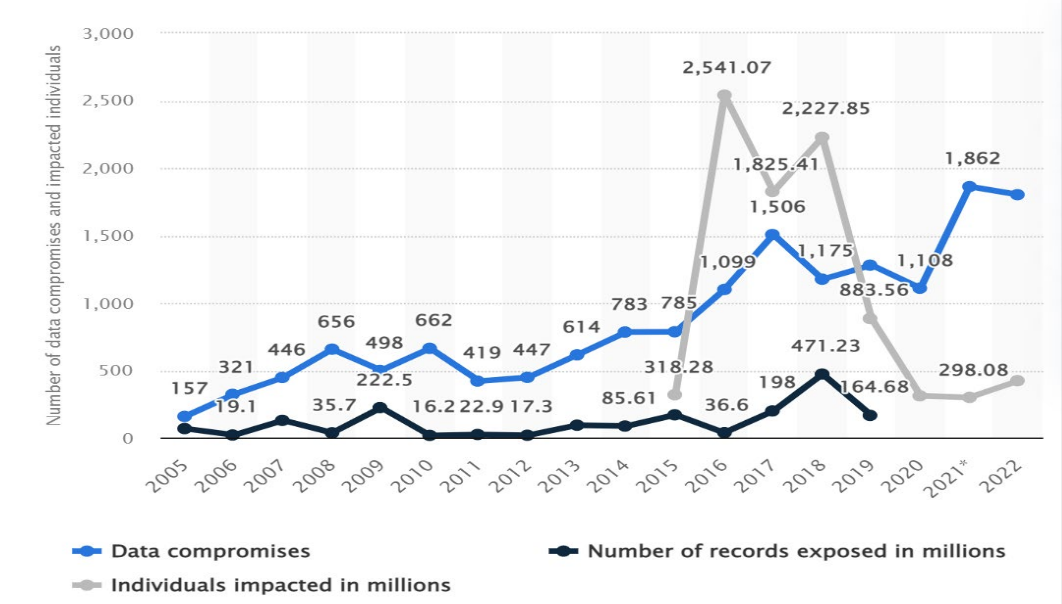


Figure 2: Cost of data loss and individuals impacted in the U.S. from 2005 to 2022 (Source: https://www.statista.com)

A security breach's effects can be broadly divided into three types: financial, reputational, and legal. The economic cost of cyber-attack is associated with data theft from companies, financial information theft (for example bank details, payment card details), interference with business transactions (for example online transactions), business - or loss of contract, and dealing with the breach. While doing so, businesses often also foot the bill for fixing broken systems, networks, and tools.

According to the most recent UK government survey on cyber security breaches, 39% of UK businesses have reported experiencing a cyberattack in the previous 12 months. Within this group, according to 31% of firms, attacks occur at least once every week and one in five, claim that an assault has harmed them 444 April costs £4,200. However, this amount increases to £19,400 for the category of medium and large businesses. Figure 2 shows annual number of cost of data loss and individuals impacted in the United States from 2005 to 2022 because of cybercrimes. A poll of US IT decision-makers in 2022 revealed that close to a quarter of businesses that have been the target of cyberattacks had suffered losses of between $50,000 and $99,999. Another 22% of the surveyed businesses disclosed suffering a financial loss of between $100,000 and USD 499,999.

Techniques to Avoid Cyber Attacks

Secure Coding Practices: Security should be built into the code at every step. Buffer overflows, SQL injection, and cross-site scripting are vulnerabilities that can be avoided with the use of secure coding techniques. The application of techniques and industry standards known as safe coding practices helps to ensure that programmers are developed securely and are not exposed to harmful assaults. These procedures aid in making sure that code is trustworthy, secure, and attack resistant. Some of the practices include using secure coding standards, using encryption, using secure authentication methods, using secure coding frameworks, avoiding insecure coding practices, and using source code analysis tools. By following these secure coding practices, developers can aid in making sure their code is safe and resilient to malicious attacks.

Test Application Security: Regular security testing should be carried out to find any potential flaws. This can include penetration testing, source code reviews, threat modeling, and static analysis. Application security is the practice of designing, developing, and testing applications to protect them from malicious attacks. It ensures that an application is secure enough to protect data, assets, and user information from unauthorized access and manipulation. Application security includes authentication and authorization, encryption, data protection, input validation, and monitoring. It also includes secure coding practices, secure development lifecycle (SDLC), secure communication, and secure deployment. With application security, organizations and developers can better protect their applications from cyber threats.

Use Appropriate Authentication and Authorization: Proper authentication and authorization should be used to control access to resources and make sure that only authorized users can access them. Two-factor authentication is one option, as password policies, and role-based access control.

- Use strong passwords: Strong passwords are a must when it comes to authentication and authorization. Passwords should be at least 8 characters in length and should include a combination of upper- and lower-case letters, numbers, and special characters. Additionally, passwords should be changed regularly, and unique passwords should be used for each service or website.
- Use multi-factor authentication: multi-factor authentication requires more than just a username and password for authentication. It usually involves a combination of something you know (such as a password), something you have (such as a security token or code sent to your mobile phone), or something you are (such as biometric data).
- Use encryption: Encryption is a powerful tool for protecting data. Encrypting data becomes unreadable to anyone who does not have the encryption key. This helps to protect data from unauthorized access.
- Implement access control lists: Access control lists (ACLs) are used to specify who has access to what resources. By configuring ACLs, you can control who can access specific resources and limit their access to those resources.
- Use role-based access control: Role-based access control (RBAC) is used to assign specific access rights to users based on their roles. This helps to ensure that users can only access the resources that they need for their job and cannot access resources that are not relevant to their roles.

Implement Security Controls: Firewalls, intrusion detection systems, and antivirus software are examples of security measures that can help protect against malicious activity.

- Implement TLS/SSL encryption: Use TLS/SSL (Transport Layer Security/ Secure Sockets Layer) encryption on all website or application traffic to protect data in transit.
- Use Strong Passwords: Use strong passwords to protect user accounts and access sensitive data.

- Enforce Access Controls: Use access controls to limit users' access to data and resources to only what is necessary for them to perform their duties.
- Implement a Firewall: Use a firewall to protect the system from external attacks.
- Perform Regular Security Audits: Audit the system regularly for security vulnerabilities and take steps to remediate any issues that are found.
- Educate Users: Educate users on the importance of security and the risks associated with inadequate security.
- Use Anti-Malware Solutions: Use anti-malware solutions to protect the system from malicious software.
- Monitor Logs: Monitor system and application logs for suspicious activity and take steps to address any issues that are found.
- Update Software Regularly: Ensure all software is updated regularly to address any security vulnerabilities that may exist.
- Backup Data: Backup data regularly to protect against data loss.

Monitor and Log Activity: Logging and monitoring activities on the system can help detect suspicious behavior. This can include network traffic, user logins, and system events.

- Monitor and log any changes to the codebase: Track which files have been modified, and who modified them.
- Monitor and log user activity: Log which users have accessed the application, when, and for how long.
- Monitor and log application performance: Monitor response times, server load, and other performance metrics.
- Monitor logs for security breaches: Log any attempts to access the application, and alert on suspicious activity.
- Monitor and log errors and exceptions: Log any errors that occur while the application is running.
- Monitor and log database operations: Log any database operations, such as queries and updates, that occur while the application is running.
- Monitor and log network traffic: Monitor any incoming and outgoing network traffic, and alert on any suspicious activity.

Secure Storage of Sensitive Data: Sensitive data should be encrypted and stored in secure locations. This can include databases, file systems, and cloud storage. There are several ways to securely store sensitive data while developing a website or application. Here are some of them:

- Encryption: Encryption is the process of transforming information into an unreadable format, making it difficult for unauthorized users to access it. When dealing with sensitive data, it is important to encrypt the data both in transit and at rest. This ensures that even if an unauthorized user gains access to the data, they will not be able to read or use it.
- Data Masking: Data masking is a process of obscuring sensitive data by replacing it with a synthetic, but still realistic, version of the data. This makes it impossible for an unauthorized user to gain any useful information from the data.
- Access Control: Access control is a process of restricting access to sensitive data to only those individuals who need it. This prevents unauthorized users from viewing or using data they do not have permission to view or use. Access control can be set up at the user level or on a more granular level, such as restricting access to a specific field within a database.
- Data Leakage Prevention: Data leakage prevention is a process of preventing data from leaving or entering an organization without authorization. It is important to have processes in place that detect and monitor data leakage, such as data loss prevention (DLP) solutions.
- Audit Logging: Audit logging is a process of recording information about user activity. This allows organizations to track and monitor user activity, as well as to detect any unusual or suspicious activity. Audit logging is an important tool for increasing the security of sensitive data.

Use Secure Communication Protocols: Web traffic should be protected using secure protocols such as SSL/TLS. This will ensure that data is encrypted while in transit.

- Utilize SSL/TLS: Secure Socket Layer (SSL) and its successor TLS (Transport Layer Security) are protocols that provide secure communications between two points (client and server) over the internet. It provides encryption and authenticity, meaning that the data is kept private and can be trusted to be from the intended source.
- Use SSH: Secure Shell (SSH) is an encrypted communication protocol that can be used for remote login, file transfers, and port forwarding. It uses public-key cryptography for authentication and encryption, making it a secure and reliable method for protecting data in transit.

- Implement HTTPS: Hypertext Transfer Protocol Secure (HTTPS) is a secure version of the HTTP protocol used for web communication. It uses SSL/TLS to encrypt data, ensuring that any information transmitted is kept private.
- Utilize IPsec: IPsec (Internet Protocol security) is a suite of protocols designed to provide secure communications over IP networks. It provides authentication, confidentiality, and integrity for data, making it a good choice for secure communication.
- Use VPNs: Virtual Private Networks (VPNs) provide a secure tunnel between two points on the internet. They use encryption and authentication to ensure that data remains private and only accessible by authorized users.

Keep Software and Operating System Up to Date: All software and operating systems should be kept up to date with the latest security patches. This can help mitigate known vulnerabilities.

- Install and use an antivirus software
- Enable automatic updates for software and operating system
- Stay informed about the latest security and software updates
- Use a firewall to protect network traffic
- Follow the latest security industry best practices
- Regularly scan your systems for malware and viruses
- Secure your web server against known vulnerabilities
- Perform regular backups of your website or application
- Regularly audit your code and configuration files
- Use trusted 3rd-party libraries and plugins

Objectives of the Study

The objectives of the study are:

- To elaborate the strategies for organizations to save their information from cyber-attacks and implementation of these strategies.
- To study the implementation of security measures such as user authentication, encryption, securing web applications, monitoring system and network activities, updating software, and creating disaster recovery plans.
- To check the awareness of software developers about techniques to be implemented while building website itself to protect from cyber-attacks.

Literature review

(Mosteanu, 2020) because of cyberattacks, there is always a need for awareness to subdue fear when examining cutting-edge technology employed in the business. Any internet-connected gadget that stores data may at any time become a target of a cyberattack. Cybersecurity is used to safeguard businesses while also providing examples of risk management from Malta. (Anwar, 2017) Even though it is challenging to fight against the more potent attacks on systems, advanced artificial intelligence techniques improve traditional security systems' overall security performance and protect against an increasing variety of sophisticated cyber threats. (Dorn, 2019) principles and methods of cyber-peacekeeping techniques decides their effectiveness in physical space. The framework helps in preventing global attacks and if the attack happens. The cyber-peacekeeping technique helps in the recovery process and impartial investigations to find the perpetrators. (Ghelani, 2022) deploying multiple strategies across an organization achieves a combined, balanced, and optimized security system. A preventive approach keeps technology services always available. (Jamil, 2018) there are loopholes in the web system due to which hacking becomes possible. The countermeasures to prevent hacking attacks must be performed in experiments to detect cyber-attacks. These tested countermeasures are used and implemented by software developers. (Ping-Chen, 2011) The principles and ideas of SOL injection attacks are introduced in the publication. It recognizes SQL injection attacks and lists all available strategies for preventing them. Examples of ASP website platform system injection attack prevention technology are examined, and the technology is used as a means of preventing SQL injection in real-world web security applications.

(Anakath, 2018) different methods are used to analyze various SQL injection attacks protect the software system from these cyber-attacks. (Shabut, 2016) the most recent cyber security attacks, defenses, and safeguards for typical online activities are linked together. The framework is defined to frame useful taxonomy and classification of cyberattacks that aid in the identification of attacks and countermeasures for cybersecurity. (Jackson, 2008) ForceHTTPS is a straightforward browser security technique that websites or users utilizes to opt into stricter error handling by avoiding network attacks that take advantage of the browser's loose error handling. It enables knowledgeable users to seamlessly retrofit security onto some unsafe sites that support HTTPS by supplying the browser with a library of unique URL rewriting rules.

(Yunus, 2018) various techniques are used for preventing SQL injection. The Blockchain concept is also used to prevent SQL injection attacks on the database management system. (Nunez, 2020) an innovative and preventive technique can be implemented to achieve security by default throughout the whole software life cycle. With the model, the overall number of vulnerabilities is decreased by 68,42%, and security and quality are increased. The more secure software is provided by the new, emerging technique. (Zhang, 2018) technical support for SQL injection testing offers a strong warranty for web-based information systems in SQL injection protection. Ingale, Anute (2020) all new technology tools, payment banks, artificial intelligence, block chain, cyber security and RPA have high effectiveness. (Li, 2021) complete investigation and assessment of standard breakthroughs produced in the field of cyber security look into the challenges, advantages, and disadvantages of the suggested solutions. The new descendant cyber-attacks emerge day by day, but their thorough investigation is always required. (Voitovych, 2016) a software tool is created that makes it possible to defend Web applications against SQL injection vulnerabilities. It enables the user to utilize SQL to defend their web application against an attack. (Sirohi, 2016) the SSL/TLS protocol secures communication over networks by guaranteeing data confidentiality, data integrity, and party-to-party authenticity. During SSL/TLS protocol evolution, security flaws were discovered thorough historical listing of SSL/TLS protocol assaults during the previous 22 years is recorded for the reference.

Research Methodology

The existing literature was studied to have a look at the implementation of technologies to protect the software from cyber-attacks. The review focuses on identifying the different types of technologies used in cyber-attacks, their characteristics, their impact on the victims, and how these technologies can be used to perpetrate attacks.

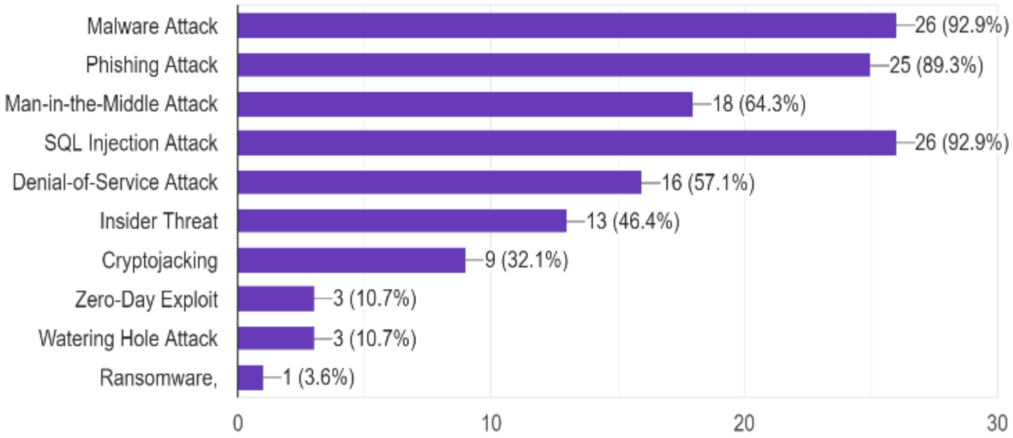
Data Collection: The data was collected from various sources such as online forums, open-source databases, and organizations specialized in cyber security. The collected data includes information about the various technologies used in cyber-attacks.

Data Analysis: The collected data was analyzed to determine the types of technologies used in cyber-attacks, their implementations, and the impact and effects on victims.

Survey: A survey was conducted to understand the opinions of the software developers about the different technologies that they are aware of to avoid cyber-attacks and implementation of these technologies. The questionnaire was passed to the software developers and received responses from them. The questionnaire consists of various questions to understand their opinions about the cyber-security and its implementation. Around 62 responses were collected from software professionals working in various organizations and having exhaustive and comprehensive software development experience. On average the experience of the respondents in their work field was in the range of 15-20 years. Various graphs are drawn to analyze the collected data and these graphs are interpreted. The major analysis is done to find awareness of cyber-attack prevention techniques among software developers and the techniques they use to prevent these cyber-attacks.

Result and Discussion

The survey of software is conducted to get some information about how they deal with cyber security and what they use to avoid cyber crimes. The initial few questions were to gather demographic information such as the name of the organization and the number of years of experience in the software development field. The question was asked to judge the awareness of software developers about different types of cyber-attacks. From graph 1 it is clear that the majority of software developers are aware of malware attacks, phishing attacks, SQL injection attacks, man-in-the-middle attacks, and denial-of-service attacks.



Graph 1: Awareness among developers about various cyber-attacks

The question was asked to find awareness of the techniques to be considered to avoid cyber-attacks. Around 82.1% of software developers are aware of various techniques used during the implementation phase of software development to avoid cyber-attack.

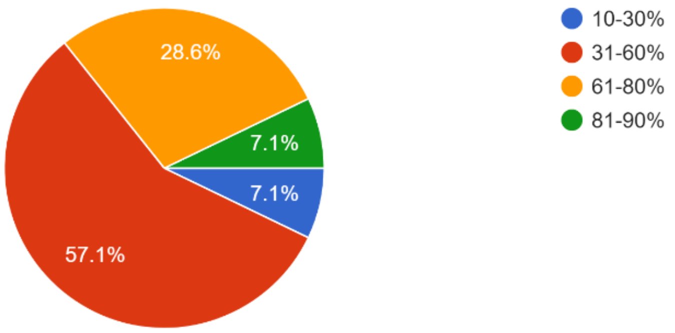
The responses to the open-ended question "What are the techniques that should be considered while developing an application or website to avoid cyber-attacks?" were interesting. The techniques mentioned were use of firewall, backing-up data from time-to-time basis, security access to authorized data, software should be up to date, follow the best coding practices, avoid passing values in URLs, validate inputs before using them to fetch data, check for secure network connections, learn how to detect a potential social engineering attack and also choose very strong passwords, securing the devices by keeping strong passwords, using multi-factor authentication, secure website with http cookies only enabled, use of secure database and network, store all the passwords in #### (encrypted) format, building an attack proof software, malware detection, function call injection, session management, activities tracker, provision of SSL certification, data should be encrypted, user data should be properly validated, authentication should done while developing any application, use of proper data transferring methods, applying injections and proper input validation, decentralization of database, use of advance cypher attacks proof advanced login system, safe hosting of the website, auditing and logging at multiple levels, quality assurance and regression testing, improved security configurations, validations on user input, blocking of spyware attacks, regular vulnerability scanning, use of SQL database with strict constraints so that database won't get corrupted and scripting security which help to only accept per IP request after every 10 seconds. Some other suggestions to avoid cyber-attack were also given by software developers. These are:

- Not to use third-party APIs (Application Programming Interfaces) which are not secured
- Not to allow access through unsecured websites
- Also, updating oneself about modern-day cyber-attacks and updating the security measures on one's end as well as the hosting is important

The strong recommendation was suggested by developers not to go for dynamic SQL. For example, the use of SQL queries such as:
'UPDATE table SET column=' + web form.column + 'WHERE something=something'
Where query inputs are accepted from web form directly then it may breach the security of the SQL environment. Again, acceptance of query parameters must be done in actual format only. For example, if the query parameter is an integer then input from the user must be restricted to an integer only. If the query parameter is in date format, in that case, user input must be accepted in date format only.

To protect the software from SQL injection vulnerability, it was suggested by one of the surveyed developers that write a query in the following form:

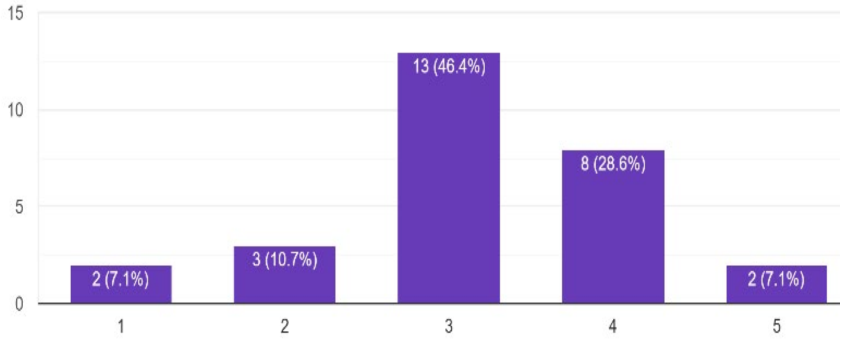
'IF EXISTS (SELECT * FROM users WHERE username=%form.username% AND password=%form.password%)'



Graph 2: Percentage of protection after implementing cyber-attack-proof techniques.

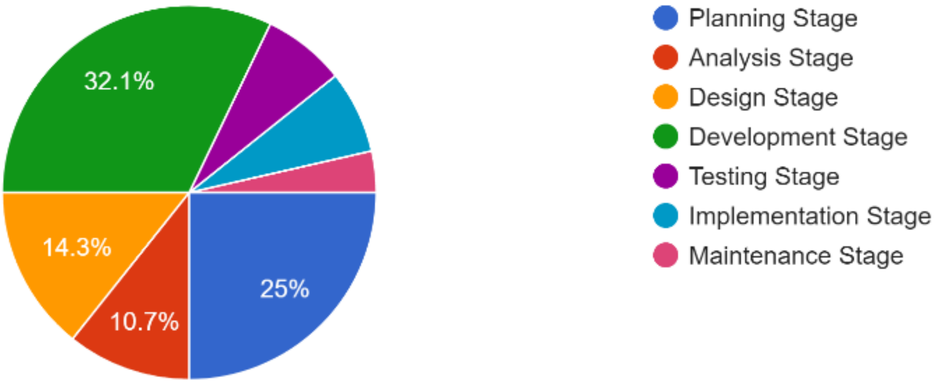
It is also suggested to pursue the best practice is to run the query explicitly and do a row count to ensure rowcount=1 (or whatever it is supposed to be in the developer's environment). The question was also asked to find the possibility of the level of protection after implementation of the above-discussed techniques. The various opinions of the developers are mentioned in Graph 2.

Majority of the developers which is around 57.1% think that only 31-60% of attacks can be avoided while using these cyber-attack-proof techniques. 28.6% of them think that 61-80% of attacks can be avoided and only 10-30% of them think that 81-90% of attacks can be avoided. Software developers were also asked to rate the existing techniques for avoiding cyber-attack on a scale of 1 to 5.



Graph 3: Rate the existing techniques for avoiding cyber-attack.

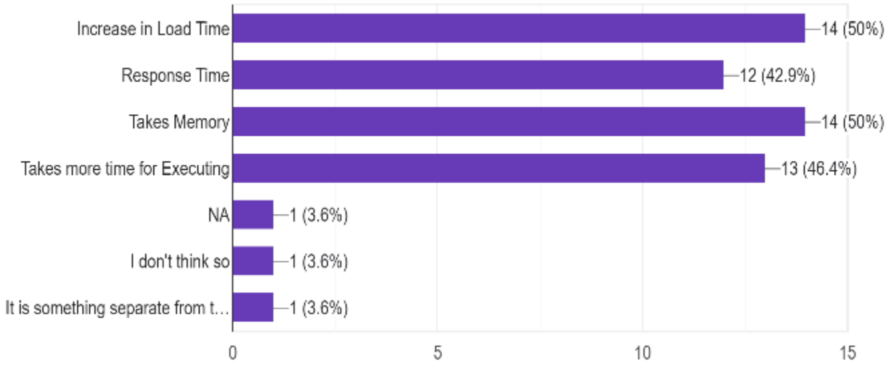
As shown in graph 3, around 46.4% have rated these techniques as average-performing techniques while 28.6% of software developers have rated these techniques as above-average performing techniques to avoid cyber-attacks.



Graph 4: Stages of SDLC where cyber-attack proof techniques are implemented

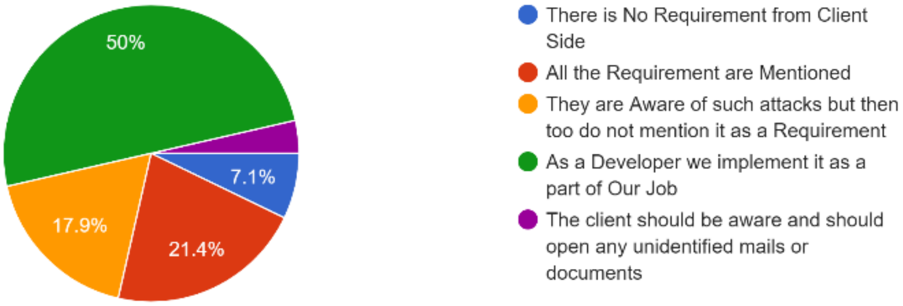
The opinion was taken to understand the stage of the software development life cycle (SDLC), where cyber-attack proof techniques are implemented. Around 25% of the software developers think that it should be done during the planning stage itself. Around 32% of them think that it should be done during the development stage, while 14% believe in the right time for implementation of these techniques is during the designing stage and 10% prefer it at analyzing stage as shown in Graph 4.

The implementation of cyber-attack-proof techniques in website development affects the performance of the website. As shown in graph 5, the major effects are an increase in the loading time of the website at the client end, a high response time of the website, high utilization of memory, and an increase in the execution time.



Graph 5: Effect on the performance of the website or app

Graph 6 shows the opinion about the preventive measures to be taken from the client end to avoid cyber-attacks on the websites. 50% of software developer believes in implementing these techniques at the developer stage itself, 21% believes in mentioning these safety requirements as the part of requirement gathering stage, while around 18% believes in not mentioning these safety requirements as a part of overall software requirements but the responsibility of the developer itself.



Graph 6: Preventive measures need to be taken from the client's end.

The constructive suggestions given by the software developers to avoid cyber-attacks during the period of implementation are as follows.

- As a software developer, one has to create any custom code with the input data validation in mind to make the software application to be resilient against injection attacks
- Before the beginning of software development, one should make the client aware of cyber security and the risks associated with it. Also, these points need to be budgeted in software cost estimation.

In general, it is believed that if there is data or financial loss due to a cyber-attack then it will affect the reputation of the organization. This may lead to a damaged reputation for the organization and the organization may lose the faith of the customers. Cyber-attacks can also cause a slowdown in business operations as employees may have to spend time dealing with the attack instead of attending to other tasks.

As per the overall observation, the following are the major measures to be taken by any organization to prevent cyber-attacks.

- **Use an Authentication System:** Implementing an authentication system is an important step in protecting the application from cyberattacks. A strong authentication system can help prevent access to sensitive information by unauthorized users and limit the chances of successful attacks.

- **Secure Database Connections**: Database connections are some of the most vulnerable points of the application and should be secured to the highest level. Use secure protocols like TLS/SSL to encrypt all database connections and use the latest security protocols.
- **Use Encryption:** This is the best way to protect sensitive data and ensure that only users with proper authentication can use it. The use of strong encryption algorithms such as AES (Advanced Encryption Standard) and RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) and the choice of the right key length are the recommendations to protect from cyber-attacks.
- **Perform Regular Security Audits:** It is important to perform regular security audits to identify any potential vulnerabilities in your application. Security audits should be conducted by an experienced security team or an outside security consultant to ensure maximum security.
- **Use Web Application Firewall:** A web application firewall can help to protect the application from cyberattacks by filtering malicious traffic and preventing unauthorized access. It should be ensured install a reliable web application firewall and keep it up to date.
- **Monitor User Activity:** Monitoring user activity can help detect suspicious activities and prevent malicious attacks. It is important to monitor user activity and keep track of user logins, access attempts, and other suspicious activities.
- **Use Secure Protocols:** Using secure protocols like TLS/SSL can help protect user data from being intercepted by malicious attackers. It needs to be assured to use the latest security protocols and ensure that all connections are encrypted.

Conclusion

Cyberattack prevention is an essential part of any website or application development process. In today's digital world, cyberattacks have become one of the most serious threats to businesses and individuals. With the increasing use of technology, the number of cyberattacks has also increased significantly. Therefore, it is essential to take the necessary steps to protect against these malicious activities.

Many developers are aware of cyber-attacks and the techniques to avoid these attacks. Many techniques need to be considered while developing the website itself to avoid the majority of cyber-attacks. But after the implementation of these techniques, it is believed that by the implementation of these techniques, only 31-60% of cyber-attacks can be avoided. Most software developers prefer to take care of the implementation of these techniques in the development stage of the software development life cycle. After the implementation of these techniques, the website may get affected by an increase in loading time, response time, execution time, and memory utilization of the website. Many software developers believe in providing security measures in the developed software even though the client does not specify it during the requirement-gathering stage. The main emphasis is to be given to taking preventive measures beforehand by implementing these techniques throughout the software development life cycle itself.

The first step to prevent cyberattacks while developing a website or application is to use secure coding practices. This includes secure writing code, using secure authentication and authorization methods, and following coding best practices. Additionally, developers should use defensive coding techniques such as input validation, output encoding, and encryption to prevent attackers from accessing sensitive information. It is also important to regularly monitor the application and website for any suspicious activity or unusual behavior. Using a Web Application Firewall (WAF) is also a good way to protect against cyberattacks. A WAF acts as a barrier between the application and malicious actors, by blocking malicious requests and alerting the developer to any attempts to access or modify the application or website. It is also important to ensure that all users are authenticated and authorized before accessing any data or application. This can be done by using two-factor authentication and implementing access control policies. Finally, it is important to use robust logging and monitoring systems to detect suspicious activity. Logging and monitoring systems should be set up to track events such as failed logins, suspicious network traffic, and other suspicious activities. These systems should also be set up to alert the developer to any suspicious activity so that it can be investigated. By following these steps, developers will be able to avoid the risk of cyberattacks while developing a website or application.

References

Anakath A., Kannadasan R. & Ambika S. (2018), “Prevention of SQL Injection and Penetrating Attacks”, International Journal of Research and Analytical Reviews, Volume 5 I Issue 3 I July– Sept 2018, E-ISSN 2348 –1269, Print ISSN 2349-5138

Anwar A. , Hassan S. I. (2017), “Applying Artificial Intelligence Techniques to Prevent Cyber Assaults”, International Journal of Computational Intelligence Research, ISSN 0973-1873 Volume 13, Number 5, pp. 883-889

Dorn A. W. , Webb S. (2019), "Cyber peacekeeping: New Ways to Prevent and Manage Cyberattacks”, International Journal of Cyber Warfare and Terrorism, Volume 9, Issue 1, January-March 2019

Ghelani D. (2022), Cyber Security, Cyber Threats, Implications and Future Perspectives: A Review. Authorea. September 22, 2022, DOI: 10.22541/au.166385207.73483369/v1

Jackson C., Barth A. (2008), “Forcehttps: protecting high-security web sites from network attacks”, Proceedings of the 17th international conference on World Wide Web, April 2008 Pages 525–534https://doi.org/10.1145/1367497-1367569

Ingale D, Anute N (2020) A Study on Adoption of New Technology tools in Indian Private Banking Sector, Studies in Indian Place Names, ISSN: 2394-3114 Vol-40-Issue-70- 2020, Page no- 3873-3879.

Jamil A., Asif K., Ashraf R., Mehmood S & Mustafa G., "A comprehensive study of cyber-attacks & countermeasures for web systems”, ICFNDS '18: Proceedings of the 2nd International Conference on Future Networks and Distributed Systems, June 2018 Article No.: 50, Pages 1–7, https://doi.org/10.1145/3231053.3231116

Li Y. and Liu Q. (2021), “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, Elsevier, Energy Reports Volume 7, November 2021, Pages 8176-8186

Mosteanu, N. R. (2020), “Artificial Intelligence and Cyber Security – Face to Face with Cyber Attack – A Maltese Case of Risk Management Approach”, Ecoforum Journal, 2020. 9 (2).

Nunez J. C. , Caro A. (2020), “A Preventive Secure Software Development Model for a Software Factory: A Case Study”, IEEE Access PP(99):1-1, DOI:10.1109/ACCESS.2020.2989113

Ping-Chen X. (2011), “SQL injection attack and guard technical research”, Elsevier, Procedia Engineering, Volume 15, 2011, Pages 4131-4135

Shabut A. M., Lwin K. T. and Hossain M. A. (2016), "Cyber-attacks, countermeasures, and protection schemes — A state of the art survey," 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA), Chengdu, China, 2016, pp. 37-44, doi: 10.1109/SKIMA.2016.7916194.

Sirohi P., Agarwal A., Tyagi S. (2016), "A comprehensive study on security attacks on SSL/TLS protocol", International Conference on Next Generation Computing Technologies (NGCT), Dehradun, India, IEEE Xplore, pp. 893-898, doi: 10.1109/NGCT.2016.7877537.

Voitovych O., Yuvkovetskyi O., Kupershtein L. (2016), “SQL injection prevention system”, International Conference on "Radio Electronics & Info Communications" (UkrMiCo), DOI:10.1109/UkrMiCo.2016.7739642

Yunus Mh. A., Brohan M., Nawi N., Surin E., Najib N., Liang C. (2018), “Review of SQL Injection: Problems and Prevention”, International Journal on Informatics Visualization, Vol 2, No. 3-2, e-ISSN: 2549-9904 ISSN:2549-9610

Zhang H., Zhang X. (2018), “SQL Injection Attack Principles and Preventive Techniques for PHP Site”, International Conference on Computer Science and Application Engineering, October, Article No.: 187, Pages 1–9, https://doi.org/10.1145/3207677.3277958