E-BOOK | EDITION 1

Information Security

Coordination

Ricardo Barretto Ferreira da Silva
Ingrid Bandeira Santos
Isabella da Penha Lopes Santana

Azevedo Sette
ADVOGADOS

INTRODUCTION

Dear readers,

The digital world we live in brings countless opportunities, but it also presents significant challenges in terms of cybersecurity. As a team specialized in technology, we are concerned about the risks that companies face daily. Therefore, we decided to compile this E-book to help you protect yourself and your Company.

In this material, we address the main types of cyberattacks that affect organizations, from malware and phishing to system intrusions and data leaks. Each chapter details the characteristics, attack vectors, and impacts of these incidents, as well as offering practical guidance on how to prevent and mitigate them.

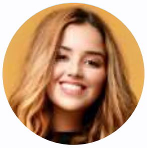
Our goal is to equip your company with the knowledge needed to identify threats, strengthen security, and be prepared to deal with possible incidents. Cybersecurity is an ongoing challenge, but with the information gathered here, you can take effective steps to protect your digital assets and the continuity of your business.

We invite you to explore this E-book and contact us if you need specialized legal advice on technology. Together, we can build a safer digital environment for everyone.

Best regards,
Technology, Media, and Telecommunications (TMT) team of Azevedo Sette Advogados

barretto@azevedosette.com.br

isantos@azevedosette.com.br



ilsantana@azevedosette.com.br

Ricardo is a senior partner in the areas of TMT, Privacy and Data Protection, IP, and Life Sciences, and Ingrid and Isabella are lawyers of the TMT team of Azevedo Sette Advogados and, together, they coordinate this project.

TABLE OF CONTENTS

DIGITAL, TMT, INTERNET

SOCIAL ENGINEERING

Social Engineering in the context of cybersecurity refers to the psychological manipulation of people into revealing confidential information or taking actions that compromise security. Rather than exploiting technical vulnerabilities in systems, social engineering attacks take advantage of human nature, such as curiosity, fear, or trust, to deceive victims.

SOME EXAMPLES INCLUDE:

- An attacker pretending to be a trusted coworker to gain access to network resources
- Phishing messages that appear to be from a legitimate source asking for confidential information
- Tempting offers of riches or prizes in exchange for personal information

ATTACKS USUALLY HAPPEN IN STEPS:

1. Victim investigation to identify security weaknesses

2. Gaining the victim's trust with emotional stimuli

3. Persuading the victim to reveal confidential data or grant access

Social engineering is dangerous because it is easier to exploit human error than to find technical vulnerabilities. Even with sophisticated security systems, it only takes a single employee to fall victim to a scam to compromise the entire network.

SOME PROTECTIVE MEASURES INCLUDE:

- Social engineering awareness training for employees
- Strict access control policies and multi-factor authentication
- Use of security technologies such as spam filters and firewalls

In short, social engineering is a cyber threat that exploits trust and human nature to steal information and compromise systems. Training employees and implementing robust security policies and technologies are essential to protect against these attacks.

PHISHING ATTACK

A phishing attack is an attempt to trick people into revealing personal information such as passwords, credit card numbers, or login details through malicious emails, SMS, or websites. Examples:

Fake Email or Message: A phishing attack usually starts with the sending of an email or message that appears to be legitimate. It may look like it came from a bank, online service, or even a friend or colleague.

Mistake: The email or message usually contains alarming or tempting information. For example, it might say that there has been suspicious activity on your account and that you need to verify your login information immediately.

Malicious Link or Attachment: The email often includes a link to a fake website that looks very similar to a real company's website. This site may ask you to enter your personal information such as username, password, credit card number, etc. Alternatively, it may contain a malicious attachment that, if downloaded and opened, could infect your computer with malware.

Obtaining Information: If you enter your information on the fake website or open the malicious attachment, hackers can gain access to your online accounts, steal your money, or even compromise your identity.

HOW DOES THIS HAPPEN?

You receive an email that appears to be from, for example, your banking institution. The email says that there has been suspicious activity on your account and that for security reasons, you need to verify your login information immediately. The email looks official, with the bank's logo and a layout that resembles the legitimate emails you receive from your bank.

CHARACTERISTICS

Deceptive Sender: The email may come from an address that looks legitimate at first glance, such as "info@yourbank.com", but upon closer inspection, you notice slight variations in the domain name (for example, "yourbank-info@phishing.com").

Alarming Content: The email might say something like: "We have detected an attempt to access your account without authorization. To protect your funds, please click the link below to verify your security information."

Fake Link: The email includes a button or link that supposedly takes you to your bank's website to verify your information. However, if you hover your mouse over the link (without clicking), you will notice that the address the link points to does not correspond to the bank's official website. It could be something like: “http://yourbank-phishing.com.br".

Request for Confidential Information: The website the link takes you to will ask you to enter your username, password, credit card number, and perhaps other personal or security information.

PHISHING ATTACK

CONSEQUENCES

The consequences of falling for a phishing attack can range from financial loss to compromised personal and corporate security. Hackers can use your information to commit fraud, steal your identity, or even access corporate systems if you are logged into them. [1]

OTHER FORMS OF PHISHING

Spear Phishing
It involves targeting a specific individual within an organization to try to obtain their login credentials. The attacker usually obtains detailed information about the person, such as name, title, and contact details, before launching the attack.

Vishing
Vishing, short for "voice phishing," occurs when someone uses the telephone to try to obtain personal information. The attacker can pretend to be someone you know, such as a friend or relative, or impersonate a trusted authority.

Email Phishing
The attacker sends legitimate-looking electronic messages designed to trick the recipient into providing personal information through a fake website, where the data is collected for malicious use.

HTTPS Phishing
An HTTPS phishing attack involves sending an email with a link to a fake website designed to trick the victim into obtaining confidential information.

Pharming
A malicious code installed on the victim's computer redirects them to a fake website designed to collect their login credentials.

Pop-up Phishing
It uses pop-up windows that warn about security issues, tricking the victim into downloading malware or calling a fake technical support number.

Evil Twin Phishing
A hacker sets up a fake Wi-Fi network that appears to be legitimate, to capture confidential information from users who connect.

Whaling
It is an attack targeting senior executives, aiming to access company’s sensitive information.

Clone Phishing
A hacker creates an identical copy of a previous message, including a malicious link, to trick the recipient.

Deceptive Phishing
It uses technology to imitate legitimate companies, tricking targets into clicking on malicious links to divulge information.

Angler Phishing
Anglers use fake social media posts to trick users into providing information or downloading malware.

Smishing
Smishing is phishing via text messages or SMS.

Website Spoofing
A fake website that appears to be legitimate is created to steal login information.

Domain Spoofing
A hacker impersonates a company's domain to trick victims into providing confidential information.

Image Phishing
It uses malicious image files to steal information or infect computers.

Search Engine Phishing
A hacker uses fake ads to trick victims into entering confidential information on fake websites.

[1] https://www.fortinet.com/br/resources/cyberglossary/types-of-phishing-attacks#:~:text=Exemplo%20de%20phishing%20HTTPS,rede%20do%20grupo%20Scarlet%20Widow.

MALWARE

Malware, a combination of the words "malicious" and "software", refers to any computer program designed to cause damage, exploit, or compromise systems, networks, or devices. Cybercriminals use malware for a variety of purposes, including data theft, financial extortion, and service disruption.

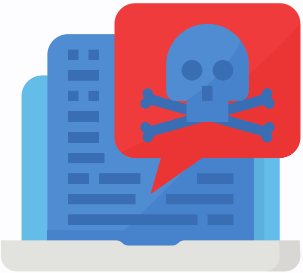
TYPES OF MALWARE

There are several categories of malware, each with distinct methods and objectives:

- **Virus:** A virus attaches itself to legitimate files and spreads when those files are executed. It can damage or corrupt data and systems.
- **Worms**: Unlike viruses, worms replicate automatically and spread across networks, without the need for user interaction. They can cause significant damage by consuming system resources.
- **Trojans:** These programs disguise themselves as legitimate software, but once installed, they can steal data, install other malware, or create backdoors for remote access.
- **Ransomware:** This type of malware encrypts user data and demands a ransom for recovery. It is one of the most profitable forms of malware for cybercriminals.
- **Spyware:** Designed to monitor user activity and collect personal information without consent, spyware can log keystrokes typed and capture sensitive data.
- **Adware:** While not always malicious, adware displays unwanted advertisements and can compromise user privacy by collecting browsing data.
- **Botnets:** Networks of infected devices that can be remotely controlled by cybercriminals to carry out large-scale attacks, such as denial-of-service (DDoS) attacks.

IMPACT OF MALWARE

Malware poses a significant threat to individuals and organizations, resulting in financial loss, identity theft, and reputational damage. Malware protection involves using antivirus software, cybersecurity practices, regular software updates, and awareness of phishing and other social engineering techniques. In short, malware is a powerful tool in the hands of cybercriminals, and its diversity and complexity require constant vigilance and proactive security measures.



RANSOMWARE

Ransomware is a type of malicious software designed to block access to computer systems or data, usually through encryption, until the victim pays a ransom to obtain the decryption key or another way to restore access. This type of malware can infect computers in a variety of ways, such as through malicious links in emails, infected file downloads, or by exploiting vulnerabilities in outdated operating systems. Once ransomware infects a system, it encrypts the user's files or completely blocks access to the computer, displaying a message asking for a ransom payment, usually in cryptocurrencies such as Bitcoin, in exchange for the key to decrypt the files or restore access to the system. Ransomware is one of the most lucrative forms of malware for cybercriminals and can cause significant harm to individuals and organizations by compromising sensitive data and disrupting business operations. [1]

CASE STUDY

In May 2017, there was a global WannaCry ransomware attack, affecting Microsoft Windows computers. It encrypted users' files and demanded a payment in Bitcoins to release them.

If it weren't for the use of outdated systems and the lack of awareness about the importance of software updates, the damage caused by this attack could have been avoided.

The cybercriminals who carried out the attack exploited a vulnerability in the Microsoft Windows operating system using an exploit* that was allegedly developed by the United States National Security Agency, known as EternalBlue. This exploit was made public by the hacker group known as Shadow Brokers prior to the WannaCry incident.

Microsoft had released a security patch to protect its users' systems against this exploit nearly two months before the WannaCry ransomware attack began. However, many people and organizations do not regularly update their operating systems, which has left them vulnerable to attacks.

Those who did not apply the Microsoft Windows update prior to the attack did not benefit from the patch, thus leaving this vulnerability exploited by EternalBlue open to be attacked.

Use of infected USB flash drive

Data blocking

Request for cash ransom

*An exploit is a technique, code, or program designed to take advantage of a specific vulnerability in a software, operating system, application, or device. The purpose of an exploit is typically to allow an attacker to compromise or gain control over the target system.

[1] https://www.kaspersky.com.br/resource-center/threats/ransomware-wannacry

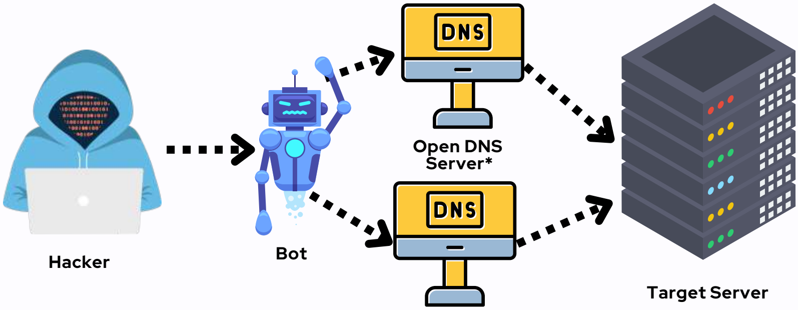
DENIAL OF SERVICE (DOS)

A denial-of-service attack, known as a DoS (Denial of Service), is a deliberate attempt to make a service, resource, or system unavailable to its intended users. This type of attack can be carried out in a number of ways, but typically involves overloading the target with an excessive volume of network traffic, requests, or connections, so that the system cannot process all legitimate requests.

In short, a denial-of-service attack aims to disrupt or reduce the availability of legitimate online services, typically by overloading the target server's resources with malicious traffic.

COMMON PRACTICES

- **Packet Flood Attacks:** Sending a large volume of network packets to overload the server's capacity. It is important to highlight that “packet” in cybersecurity can refer to different units of data or sets of information that are transmitted, processed, or used in specific contexts within the area of information security and computer networks.
- **Connection Flood Attacks:** Opening multiple connections to the server, exhausting processing resources.
- **Reflection/Amplification Attacks:** Sending requests to servers that respond with a much larger amount of data than requested, amplifying the impact of the attack.



*An open DNS server, also known as a public DNS server, is a DNS server that is available for public use, usually without access restrictions. These servers are maintained by organizations or companies and offer domain name resolution services to anyone on the Internet, without the need for prior authentication or authorization.

DENIAL OF SERVICE (DOS)

CHARACTERISTICS

Resource Overload: The attacker sends a massive volume of requests to the target server, consuming all available resources (such as bandwidth, memory, CPU).

Vulnerability Exploitation: Some DoS attacks exploit specific vulnerabilities in the server's software or operating system to exhaust resources more effectively.

Distributed Attacks (DDoS): In this type of attack, multiple compromised computers (called “botnets”) are coordinated by the attacker to simultaneously send malicious traffic to the target, significantly increasing the impact of the attack.

OBJECTIVE

Service Unavailability: The main purpose is to make the service or system inaccessible to legitimate users. This can result in business interruptions, lost revenue, and reputational damage.

Resilience Test: Some DoS attacks are performed as tests to assess a system's ability to withstand traffic spikes or real attacks.

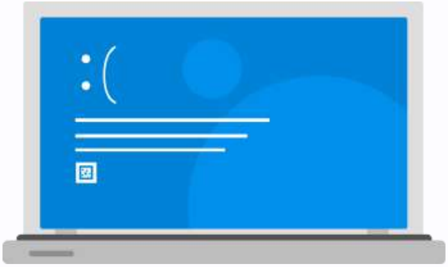
MITIGATION

Traffic Filtering: Use of firewalls and intrusion detection/prevention systems (IDS/IPS) to filter malicious traffic.

Load Balancing: Balanced distribution of traffic across multiple servers to mitigate the impact of traffic spikes.

Traffic Monitoring: Early identification of unusual traffic patterns that may indicate an ongoing attack.

Security Updates: Keep systems and software up to date to fix known vulnerabilities that could be exploited in DoS attacks.



DENIAL OF SERVICE (DOS)

DENIAL OF SERVICE (DOS) VS DISTRIBUTED DENIAL OF SERVICE (DDOS)

The difference between DoS (Denial of Service) and DDoS (Distributed Denial of Service) lies in the way these attacks are executed and the scale of impact they can have. See below:

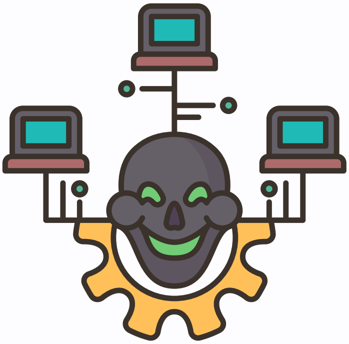
DoS (*Denial of Service*)

Description: A DoS attack involves sending an excessive volume of traffic or requests to a specific server, network, or service with the aim of overloading its resources and making it inaccessible to legitimate users.

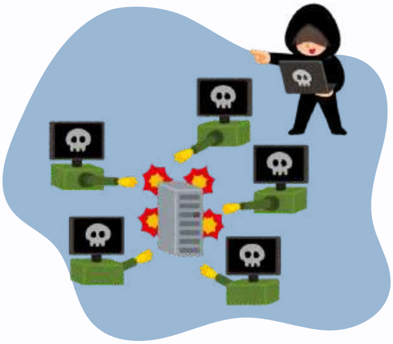
Execution: Typically, a single computer or device is used to generate the malicious traffic that overloads the target.

Example: Repeatedly sending HTTP requests to a web server until it can no longer respond to legitimate requests.

Impact: It can cause temporary service interruptions but is generally easier to detect and mitigate compared to DDoS attacks.



DDoS (Distributed Denial of Service)



Description: A DDoS attack is an evolution of DoS, where multiple devices (usually part of a botnet) are coordinated to send malicious traffic simultaneously to the target.

Execution: A botnet can consist of hundreds or thousands of compromised devices, geographically distributed, significantly increasing the amount of traffic directed to the target.

Example: Coordinating a botnet to flood an e-commerce website with requests, overloading its servers and making the website inaccessible.

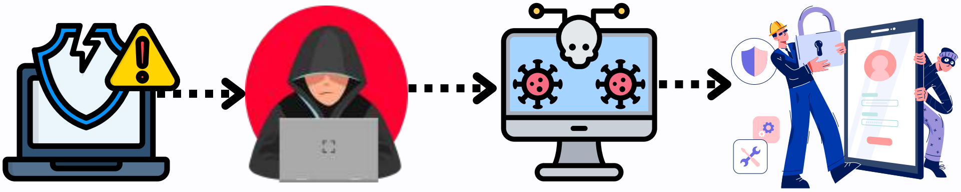
Impact: It can cause severe and prolonged service disruptions and is more difficult to mitigate due to its distributed nature and massive volume of traffic.

ZERO-DAY EXPLOITS

"Zero-day" is a broad term used to describe newly discovered security vulnerabilities that hackers can exploit to attack systems. It refers to the moment when developers become aware of a flaw, leaving them "zero days" to fix the problem before hackers can exploit it. A zero-day attack happens when hackers exploit this flaw before a patch is implemented.

The term can be written as "day 0". The words vulnerability, exploitation and attack are often associated with the concept of "zero-day" and help to understand its nuances:

- A **zero-day vulnerability** is a software flaw discovered by hackers before the developer identifies it, meaning there is no patch available yet. This increases the chance of an attack being successful.
- A **zero-day exploit** is a method used by hackers to exploit systems through a previously unknown vulnerability.
- A **zero-day attack** occurs when a zero-day exploit is used to cause damage or steal data from a system affected by this vulnerability.


Existence of a security flaw
Discovery by the hacker
Cybersecurity attack begins
Developers discover the attack and have zero days to fix it

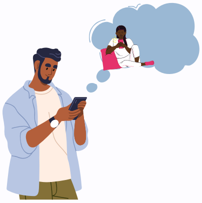
MAN-IN-THE-MIDDLE (MITM) ATTACKS

A Man-in-the-Middle (MITM) attack is a type of cyberattack in which an attacker intercepts and manipulates communication between two parties, such as an user and a website, without either party being aware of the attacker's presence. The goal of these attacks is usually to steal confidential information such as login credentials, banking details, and private communications.

MITM attack occurs in three main phases:

1. Interception: The attacker positions himself between the two communicating parties and intercepts the messages being sent.

2. Modification: The attacker can alter the content of intercepted messages before forwarding them to the original recipient.



3. Retransmission: The modified messages are then relayed to the target, who believes they are communicating with the legitimate party.

Some examples of techniques used in MITM attacks include:

- Traffic Routing: Connection traffic is redirected to pass through the attacker's device.
- Certificate attacks: A fake digital certificate is provided to establish a secure connection (HTTPS) with the target.
- Cookie theft: The attacker accesses and decodes the victim's cookies, obtaining information stored in them.
- SSL stripping attacks: The SSL/TLS* encryption layer of a secure connection is removed.

To protect yourself, it is recommended:

- Avoid using public Wi-Fi networks
- Keep your security software up to date
- Use a VPN to encrypt your traffic
- Install extensions such as HTTPS everywhere in your browser
- Verify the authenticity of websites before providing information

In short, MITM attacks are a significant threat to online security because they allow attackers to discreetly intercept and manipulate communications. Adopting adequate security measures is essential to protect yourself against this type of attack.

*SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are security protocols used to establish encrypted connections between a server and a client, such as a web browser. These protocols are essential to ensure the security of the transmission of sensitive data, such as personal and financial information, over the Internet.

CROSS-SITE SCRIPTING

Cross-Site Scripting (XSS) is a security vulnerability in web applications that allows an attacker to inject malicious scripts into trusted pages, aiming to execute these scripts in other users' browsers. This technique is often used to steal sensitive information such as session cookies, login credentials, and personal data.

Types of XSS Attacks

XSS attacks can be classified into three main categories:

1. **Stored (Persistent) XSS**: In this type, the malicious script is stored permanently on the server, such as in a database or in comment fields. When a user accesses the affected page, the script runs automatically, without the user needing to interact with a specific link.

2. **Reflected (Non-Persistent) XSS**: Malicious code is injected into a web page through unvalidated input, such as a form or URL. The script is reflected back to the user via the server, usually via a phishing link. This type of attack requires the victim to click on a malicious link for the script to execute.

3. **DOM-Based XSS**: This attack exploits the browser's Document Object Model (DOM), where the malicious script is executed directly on the client, without interacting with the server. The attacker manipulates the DOM to perform malicious actions, making detection more difficult.

Impacts and Consequences

XSS attacks can have severe consequences, including:

Data Theft: Attackers can access sensitive information stored in the victim's browser, such as cookies and session tokens.

Website Defacement: The attacker can alter the content of a web page, compromising the integrity of the website and damaging the company's reputation.

Phishing: Malicious scripts can be used to create fake forms that collect login credentials and other personal information from users.

Protective Measures

To mitigate the risks of XSS attacks, companies and developers should implement security practices such as:

- **Input Validation and Sanitization:** Ensure that all user input data is properly validated and sanitized before being processed or displayed.
- **Use of Content Security Policy (CSP):** Implement security policies that restrict which scripts can run on a web page.
- **User Education:** Inform users about the risks of clicking on unknown links and the importance of verifying the authenticity of the websites they visit.

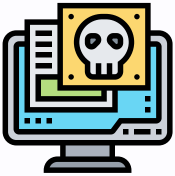
In short, Cross-Site Scripting is a significant threat to web application security, and preventing it requires a careful and proactive approach.

DNS SPOOFING

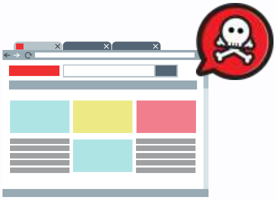
DNS spoofing, also known as DNS cache poisoning, is a type of cyberattack that involves corrupting a DNS resolver's cache to redirect traffic to a malicious website.*

The attack works as follows:

1. The attacker intercepts a DNS query between a client and a DNS server, typically through a man-in-the-middle (MITM) attack



2. The attacker sends a spoofed DNS response to the client with incorrect information, such as an IP address pointing to a malicious website.



3. If the client accepts the spoofed response, its DNS cache will be poisoned and subsequent requests will be directed to the attacker's site.

The consequences of DNS spoofing include:

- Redirect users to malicious websites for phishing, malware distribution, or other nefarious purposes
- Hijack domain names and redirect traffic to the attacker's servers
- Intercept network traffic and steal confidential information

To protect yourself, it is recommended:

- Implement DNSSEC* to authenticate DNS responses and ensure data integrity
- Use source port randomization and cryptographically secure random numbers
- Perform end-to-end validation using TLS and digital signatures, such as HTTPS
- Keep DNS software up to date and apply security patches promptly
- Configure firewalls to block unauthorized access to DNS servers

Understanding how DNS spoofing works and taking appropriate security measures is essential to protecting yourself against this type of cyberattack.

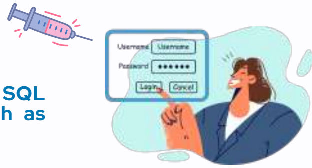
*Cache is a fast-access memory used to temporarily store data or instructions that are likely to be accessed again in the near future. It acts as an intermediary between the CPU and main memory, allowing the CPU to access data much faster than if it had to fetch it directly from main memory.

*DNSSEC (Domain Name System Security Extensions) is a set of specifications designed to strengthen the security of the Domain Name System (DNS), which is responsible for translating domain names into IP addresses. DNSSEC provides origin authentication, data integrity, and authenticated denial of existence for DNS information.

SQL INJECTION

SQL (Structured Query Language) Injection is a cybersecurity vulnerability that allows an attacker to interfere with the queries an application makes to a database. This type of attack is carried out by inserting malicious SQL commands into input fields, such as login forms or URLs, which are then executed by the application's database management system (DBMS).

How SQL Injection Works



1. **Malicious Code Insertion: The attacker inserts the SQL code into fields that normally accept user input, such as forms or URL parameters.**

2. **Executing Unwanted Queries: If the application does not properly validate or sanitize user input, the malicious code can be executed by the database. This could allow the attacker to access, modify, or delete sensitive data.**

3. **Data Exposure: The attacker can obtain confidential information such as customer data, login credentials, and financial information, resulting in data breaches.**

Consequences of SQL Injection

- **Data Breach:** Unauthorized access to sensitive information, which can lead to legal and financial consequences.
- **Damage to Reputation:** Exposing data can damage customer trust and company reputation.
- **Service Interruption:** In some cases, an attack may compromise application functionality, resulting in downtime.

SQL Injection Prevention

To protect applications against SQL Injection, several best practices should be implemented:

- **Input Validation and Sanitization:** Always validate and sanitize user input data to prevent malicious code execution.
- **Use of Prepared Queries:** Implement parameterized queries that separate data from SQL commands, reducing the possibility of injection.
- **Regular Updates:** Keep software and systems up to date to fix known vulnerabilities.
- **Web Application Firewalls:** Use firewalls that can detect and block SQL Injection attempts.
- **Continuous Monitoring:** Monitor security logs to identify suspicious activity that may indicate an attack.

SQL Injection is a significant threat that can severely impact businesses and organizations, making awareness and implementation of security measures essential for data protection.

PERSONAL DATA AND COMPLIANCE WITH LGPD

In an increasingly digital world, much of business operations and personal information is stored and transferred electronically. Unfortunately, this reality also brings with it a series of cyber risks that can compromise the data security and privacy. Cyberattacks related to data protection incidents can have devastating consequences for businesses, including financial losses, reputational damage, lawsuits, and fines.

In this context, compliance with the Brazilian General Data Protection Law (LGPD) plays a fundamental role in preventing and mitigating these incidents. The LGPD establishes a series of security, transparency, and accountability requirements that help companies implement appropriate technical and organizational measures to protect personal data, adopt policies and procedures to promptly respond to security incidents, carry out periodic risk and vulnerability assessments, train employees and third parties on good information security practices, and establish contingency and disaster recovery plans. By meeting LGPD requirements, companies can significantly reduce their exposure to cyberattacks and, if they do occur, have a solid structure in place to effectively detect, respond to, and mitigate damage.

Therefore, adopting a holistic approach to data protection, aligned with the LGPD, is essential for organizations to be prepared to face the cyber challenges of today's digital world.

Our team of experts is available to help companies with this adaptation.

OUR INFORMATION SECURITY SERVICES

- Prevention and action in cases of Security Incidents
- Vulnerability and risk analysis through data mapping
- Compliance with the Brazilian General Data Protection Law
- Drafting of contracts and amendments that ensure information security on-demand services related to IT legal risks

IN TECHNOLOGY, MEDIA, AND TELECOMMUNICATIONS (TMT)

- The members of the Technology, Media, and Telecommunications (TMT) Group are exceptionally qualified lawyers with command of several languages, exclusively dedicated to providing comprehensive assistance to national and international clients in the areas of Technology, Media, Telecommunications, Privacy, and Data Protection. The Group works together with lawyers from the Regulatory, Competition, Corporate, Tax, Labor, Compliance, International Trade, and Litigation/Arbitration/Mediation areas to resolve such matters.

Azevedo Sette
ADVOGADOS

COORDINATION

Ricardo Barretto Ferreira da Silva, Ingrid Bandeira Santos.
and Isabella da Penha Lopes Santana

REVIEW

Ingrid Bandeira Santos and Isabella da Penha Lopes Santana

PRODUCTION AND GRAPHIC DESIGN:

Tatiana H. Lau Cintra

SERIES - VOL. I - 1ST EDITION - BRAZIL, 2024

Azevedo Sette Advogados
www.azevedosette.com.br
faleconosco@azevedosette.com.br

This is a private communication from Azevedo Sette Advogados with the aim of informing its clients and lawyers about recent and relevant legal issues. This e-book is exclusively informative and does not consist of any type of legal advice or guidance, which must be provided personally and individually by lawyers. Azevedo Sette Advogados is not responsible for decisions made based on this material.

Brazil | Belo Horizonte | Brasília | Recife | Rio de Janeiro | São Paulo