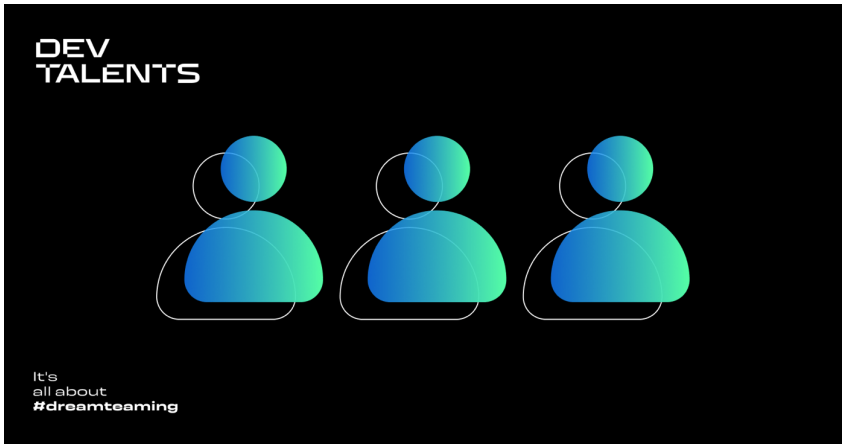
6 MINUTES READ

10 cyber security risks in software development and how to mitigate them

Olga Trąd | 02/10/2023



As cybercrime rates continue to rise, it is more important than ever for software development teams to take cyber security seriously. Unfortunately, many teams overlook the potential risks posed by their development process and are subsequently vulnerable to cyber attacks. In this blog post, we will explore the 10 most common cyber security risks in software development and how to mitigate them.

The importance of cyber security during software development

Every software development project is vulnerable to cyber attacks during its development, launch and maintenance stages. There are a number of cyber threats that can affect a software development process. These range from malicious code injection, cross-site scripting (XSS) attacks, and others. It is important for software developers to be aware of these threats and take the necessary steps to protect their software from cyber attacks.

Common security threats to software projects

I agree to receive commercial and marketing ... show more

SUBSCRIBE

Software projects are vulnerable to cyber security threats during the development, launch and maintenance phases. Hackers can exploit weaknesses in any of these stages, making it essential that software developers take cyber security seriously. There are many cyber security threats that must be taken into account during software development; here are 10 of the most common ones.

1. Data breaches

Data breaches occur when cyber criminals gain unauthorized access to sensitive data. This can include customer records, financial information and other confidential information. Ofted, data breaches are caused by cyber criminals exploiting weaknesses in software applications, such as weak passwords, outdated solutions, or a lack of encryption.

2. Insecure APIs

APIs are a common way for software developers to connect different systems; however, if they are not properly secured, cyber criminals can exploit them to access sensitive data or disrupt the system.

3. SQL injections

An SQL injection is a cyber attack in which malicious code is inserted into an application's database, allowing cyber criminals to gain access to sensitive data and disrupt operations.

4. Cross-site scripting (XSS)

XSS refers to cyber attacks in which cyber criminals inject malicious code into websites and web applications, typically through a form or URL parameter.

5. Malware

Malware is malicious software designed to disrupt systems and gain access to sensitive data. It can be spread via email, websites, downloads and other sources. One example of malware is the infamous WannaCry ransomware, which cyber criminals used to target businesses and government agencies.

6. Phishing attacks

Phishing attacks involve cyber criminals sending emails that appear to come from legitimate organizations in order to trick users into providing sensitive information or downloading malicious software.

7. Unpatched vulnerabilities

Unpatched vulnerabilities are security flaws that have not been patched and can be exploited by cyber criminals to gain access to systems and data. An example of such an attack was seen in the 2017 Equifax data breach, when cyber criminals gained access to millions of customers' personal information.

8. Poor password policies

Poor password policies can leave systems vulnerable to cyber attacks by allowing cyber criminals to easily guess passwords or gain access via brute force attacks. Brute force attacks involve malicious parties systematically trying every possible

TABLE OF CONTENTS

9. Insufficient logging

Logging is an important way of monitoring system activity and detecting cyber security threats; however, if insufficient logs are kept, cyber criminals may be able to carry out their attacks without being detected.

10. Unauthorized access

Unauthorized access occurs when cyber criminals gain access to systems and data without permission. This can happen when malicious parties exploit software vulnerabilities, gain access via stolen credentials or use brute force attacks.

Mitigating cyber security risks throughout the software development process

Now that we have explored the 10 most common cyber security threats, let us take a look at how developers can

mitigate them and ensure top cyber security for their software development projects.

1. Use secure coding practices

Secure coding practices can help to reduce the risk of cyber attacks by preventing cyber criminals from exploiting weaknesses in the code.

2. Implement multi-factor authentication

Multi-factor authentication adds an extra layer of security to systems by requiring users to provide additional credentials, such as a one-time PIN or biometric data, when logging in.

3. Monitor systems for cyber threats

Monitoring systems for cyber threats can help to detect cyber security incidents and respond to them quickly. This can include monitoring logs, patching vulnerable software and employing intrusion detection systems.

4. Encrypt sensitive data

Encrypting sensitive data helps to protect it from unauthorized access, as cyber criminals will be unable to view the data without the correct encryption key.

5. Train employees on cyber security best practices

Educating employees on cyber security best practices can help to reduce cyber security risks by ensuring that everyone is aware of them and knows what action to take in the event of a cyber attack.

6. Use security testing

Security testing helps to identify potential cyber security weaknesses early on in the software development lifecycle, allowing them to be addressed before they become a problem.

The impact of human behavior on software security

Human behavior can have a significant impact on cyber security. For example, employees who do not follow cyber security best practices or are unaware of cyber security threats may be more likely to click on malicious links, download malicious software or provide sensitive information to cyber criminals. They may also respond too slowly to a detected threat. It is therefore important for businesses to ensure that their staff are trained on cyber security best practices and risks.

Users can also be vulnerable to cyber attacks, since they may not be aware of cyber security risks or may interact with malicious links or websites. It is therefore important for users to also stay informed about cybersecurity threats. Developers and cyber security professionals can help users make more secure decisions by providing them with security advice and requirements, such as using strong passwords. Good UX design also helps to improve cyber security by making it easier for users to understand cyber security best practices and make safer choices.

Ensuring software development security

By following the above security best practices, software development teams can reduce cyber security risks and ensure their projects remain secure. Cyber security is an ongoing process that requires regular monitoring during all stages of the software development process, and engages everyone who interacts with the application. Secure software development should not be an afterthought, but rather built into the very foundations of any software project to ensure cyber criminals are unable to exploit weak points and access or steal sensitive data.

Software development teams are responsible for ensuring cyber security in their projects. By better understanding the threats and implementing cyber security best practices, software development teams can protect their projects more effectively.

Olga Trąd
Marketing Manager

Fascinated by the spirit of innovation that permeates the IT industry, Olga has never abandoned her roots as an IT content marketing specialist. She draws on years of experience in the technology sector to shed light on interesting trends, solutions and practices.

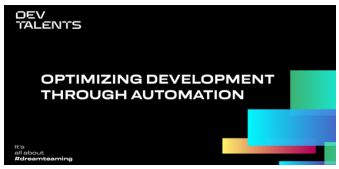
FIND ME ON SOCIAL MEDIA

6 MINUTES READ

#DREAMTEAMING DEVELOPER LIFE

Accelerating the growth of IT businesses with ChatGPT

Olga Trąd



7 MINUTES READ

#DREAMTEAMING DEVELOPER LIFE

Optimize your development team's performance with automation

Olga Trąd

6 MINUTES READ

#DREAMTEAMING MANAGEMENT

Managing remote development teams: strategies for achieving balance

Olga Trąd

6 MINUTES READ

#DREAMTEAMING MANAGEMENT

Eliminate the distance: strategies for creating positive remote team environments

Olga Trąd

Talk to our technology & business experts and to started today. The DEVTALENTS team is always ready to jump into a new project.

On average, we have a set of developer profiles ready within only 48 hours.

CONTACT US

DEVTALENTS LTD
USA: +1 888 514 1606
PL: +48 22 532 50 21
Email:
hello@devtalents.com

SERVICES

- Staff augmentation
- Ruby on Rails Developers
- Android Developers
- iOS Developers
- Flutter Developers

COMPANY

- About us
- Blog
- Get a quote
- Contact us

INDUSTRIES

- Healthcare
- Finance
- Legal
- Technology

Looking for specific talent? Build your team!

HIRE DEV TAI_ENTS

Privacy Policy