Last updated 29.10.2024

Data security check for OTTO Market service providers

Last updated 29.10.2024

Contents

Introduction

The security of sensitive customer data is of crucial importance in today's world. As a company trusted by over 11.5 million customers, it is our duty to justify this trust and protect the data entrusted to us in the best possible way. A key aspect of this is the security of the systems that process and store customer data. To ensure that you as a service provider meet these security standards, we have developed a 3-stage process for checking your data security. This document is intended to give you a brief overview of what you can expect at each stage.

Our aim is to carry out at least one data security audit per year at your company. The level of the audit essentially depends on the amount of customer data that passes through your system.

Level 1 - Description of data-secure software development

In this step, it is important that you describe in detail how you ensure in your software development cycle that secure software and applications are developed according to globally recognized standards, such as OWASP.
Please list the specific measures you take to fulfill security requirements and avoid security flaws. These include, but are not limited to:

1. Integration of security checks: Regular security checks and tests throughout the development process.
2. Development team training: training on secure programming practices and threat modeling.
3. Use of security tools such as Acunetix, AppScan, Burp or OWASP ZAP to identify vulnerabilities.
4. Documentation of the SSDLC: Provision of documentation of your secure software development cycle (SSDLC).
5. Regular audits and certifications: Conducting audits and obtaining relevant certifications to ensure compliance with safety standards.
6. Penetration tests: Conducting penetration tests and providing the corresponding results (also redacted or in excerpts, if necessary).

If available, please send us supporting documents that prove your actions. These can include the documents and results mentioned above.

Stage 2 - Questionnaire and auditing

If an audit is to be carried out at level 2, you will first receive a questionnaire with questions designed to check the technical and organizational measures.

The technical and organizational measures can be found in Appendix A of our Terms of Use. The measures for **confidentiality** (access control, access control, access control, separation control), **integrity** (transfer control, input control) and **availability** are checked.

Your details in the questionnaire will be checked by Otto's data security experts or by third parties commissioned by Otto. We will contact you if we have any queries. If the results of the questionnaire are critical, Otto will take appropriate measures depending on the severity.

Stage 3 - External review of software development

As the security of the processing systems is particularly important when processing a large amount of sensitive customer data, the third stage requires the results of tests / checks carried out by external bodies that are no more than one year old. These can be penetration tests, for example, whereby the OWASP Top 10 can be used as a basis.

Otto or a third party commissioned by Otto will check the documents sent. If we have any queries, we will contact you to obtain further information. If the results are critical, Otto reserves the right to take appropriate measures.

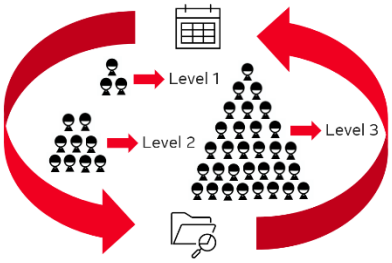
A precise definition of penetration testing, as well as the distinction from vulnerability scanning, can be found at the end of this document.

Possible measures in the event of non-compliance with safety standards

- Creation of an action plan that includes both steps already taken and future measures to resolve the vulnerability. This plan serves to document progress and ensure that all necessary steps are taken.
- OTTO sets a binding deadline for remedying the identified vulnerability(ies), within which you as the responsible party must take the necessary measures to resolve it.
- Inspection at the next higher level: If the safety standards are not met, an inspection is carried out at the next higher level of the process. Additional safety measures and checks are carried out here to ensure compliance with the standards.
- Partial restriction of the app: If security flaws are detected, the app can be restricted so that no further partners can be connected. This prevents potentially insecure connections to sensitive customer data from being established.

- Complete restriction of the app: In the event of serious security breaches, the app can be completely restricted so that no more data can be sent or received. This measure serves to protect customer data and prevent potential security risks.
- Informing service provider partners: If serious data security deficiencies are identified, the affected service provider partners are informed. This creates transparency and gives the partner the opportunity to take measures at an early stage.
- Exclusion from the Developer Program: In the event of serious or repeated violations of the security standards, we reserve the right to exclude the service provider from the Developer Program. As a result, the cooperation will be terminated and no further apps can be developed or offered.

When do the checks take place?

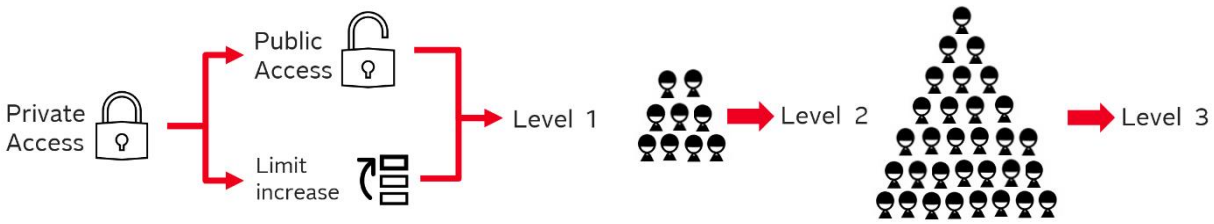


The inspections are carried out at regular intervals; you can expect an annual inspection.

In addition, checks are carried out as soon as the amount of customer data passing through your system makes this necessary.

The first check is carried out as soon as Public Access is requested or a limit increase for partner installations is requested in Private Access.

Subsequently, checks are carried out depending on the amount of customer data that passes through your system. Irrespective of the number of customer orders, a check can also be carried out in one of the three stages if we deem this necessary.



Definition of penetration test

A penetration test is an authorized simulated attack on a computer system, network or web application to identify, exploit and assess security gaps and vulnerabilities. The aim of a penetration test is to find out how an attacker could potentially gain access to systems, what data could be compromised and how far such an attack could go. This involves running through various attack scenarios that could be used by real hackers. The penetration test provides detailed information on the vulnerabilities found and gives recommendations on how these can be closed. It usually includes the following steps:

- Planning and preparation: Defining the objectives and scope of the test, including the systems to be tested and the test methods.
- Intelligence gathering: Gathering information to understand how the target operates and identify potential points of attack.
- Vulnerability analysis: Identification of potential vulnerabilities in the systems.

- Exploitation: Attempt to exploit the identified vulnerabilities to gain unauthorized access or perform other malicious activities.
- Reporting: Preparation of a detailed report that includes the vulnerabilities found, the attacks carried out and recommendations for remedying the vulnerabilities.

Differentiation from the vulnerability scan

An automated application-level vulnerability scan is a process in which specialized software is used to identify potential security vulnerabilities in an application. This type of scan focuses on reviewing the application itself, including the source code, configuration and interfaces, to uncover vulnerabilities that could be exploited by attackers.

The automated vulnerability scan at application level can use various techniques to identify potential vulnerabilities. These include scanning the source code for known vulnerabilities, testing the application for known attack patterns and checking the configuration settings for potential security issues.

Final clause

Compliance with security standards is crucial to justify the trust of our end customers and marketplace partners and to ensure the security of sensitive data. We therefore ask you to take this data security process seriously and to play an active role in securing customer data.