Last updated 13.03.2024

Data security check for OTTO Market service providers

Last updated 13.03.2024

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-level process for checking your data security. This document is intended to give you a brief overview of what you can expect at each level.

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

Level 1 - Vulnerability scan

In this step, it is mandatory for you to provide us with the results of a vulnerability scan from the **application** area that is no more than six months old upon request, as we expect the highest security standards here.

In addition to the scan results, we expect you to describe in detail what actions are being taken to address identified security deficiencies. Please explain the steps taken to address the identified findings and ensure that they are effectively removed. For example, Acunetix, AppScan, Burp or OWASP Zed Attack Proxy (ZAP) can provide corresponding reports.

It is important that all security flaws are removed before continuing with the connection of further partners. If no security flaws are found, you can of course continue with the next steps accordingly.

Level 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 (physical access control, logical 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 inquiries. If the results of the questionnaire are critical, Otto will take appropriate measures depending on the severity.

Level 3 - Penetration test

As the security of the processing systems is particularly important when processing a large amount of sensitive customer data, the results of a penetration test no more than one year old are requested in the third level. Here, for example, the OWASP Top 10 could be used as a basis.

Otto or a third party commissioned by Otto will review the results of the penetration test. If we have any questions, we will contact you for further information. If the results are critical, Otto reserves the right to take appropriate action.

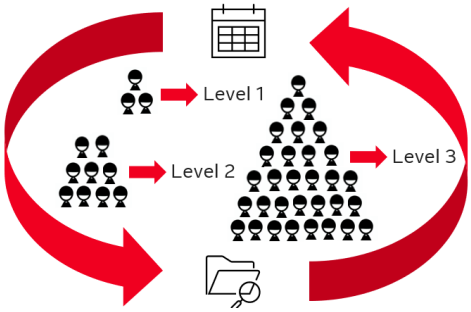
A precise definition of the penetration test, as well as the distinction from a vulnerability scan, can be found at the end of this document.

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

- Create an action plan that includes steps taken and future actions to address the vulnerability. This plan will be used to document progress and ensure that all necessary steps are taken.
- OTTO will set a binding deadline for the resolution of the identified vulnerability(ies), within which you, as the responsible party, must take the necessary action to resolve the vulnerabilities.
- Inspection at the next higher level: If safety standards are not met, an inspection will be carried out at the next higher level of the process. Additional security measures and checks are carried out to ensure compliance.
- Partial restriction of the application: If security flaws are found, the application can be restricted from connecting to other partners. This prevents potentially insecure connections to sensitive customer data.
- Complete application restriction: In the event of a serious security breach, the application can be completely locked down so that no data can be sent or received. This protects customer data and prevents potential security risks.
- Notify service provider partners: When serious data security breaches are identified, the affected service provider partners will be informed. This creates transparency and allows the partner to take early action.
- Exclusion from the developer Program: In the event of serious or repeated breaches of security standards, we reserve the right to exclude the service provider from the Developer Program.

When do the checks take place?

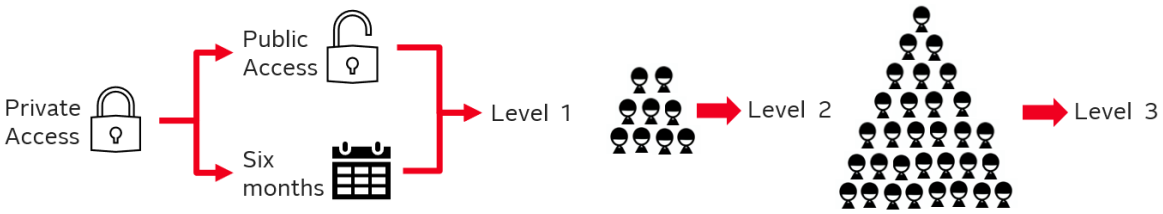
Audits are carried out on a regular basis; you can expect an annual audit.



Audits will also be carried out whenever the volume of customer data passing through your system makes it necessary.

The first audit will take place when you apply for Public Access or after six months in Private Access.

Subsequent checks will be based on the volume of customer data passing through your system. Regardless of the number of customer orders, a review may be performed at any of the three levels if we deem it necessary.



Definition Penetration test

A penetration test is an authorized simulated attack on a computer system, network or web application to identify, exploit and assess security weaknesses 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 makes recommendations on how to close them. It typically involves 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 to identify potential points of attack.
- Vulnerability analysis: Identifying potential vulnerabilities in the systems.
- Exploitation: Attempting to exploit the identified vulnerabilities to gain unauthorized access or perform other malicious activities.
- Reporting: Preparation of a detailed report detailing the vulnerabilities found, the attacks performed, and recommendations for remediation.

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

Adherence to security standards is critical to justifying the trust of our end customers and marketplace partners, and to ensuring 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.