Last updated 13.03.2024

Datensicherheits-überprüfung für OTTO Market Dienstleister

Last updated 13.03.2024

Inhalt

Einleitung

Die Sicherheit sensibler Kundendaten ist in der heutigen Zeit von entscheidender Bedeutung. Als Unternehmen, dem über 11,5 Millionen Kund*innen ihr Vertrauen schenken, ist es unsere Pflicht, dieses Vertrauen zu rechtfertigen und die uns anvertrauten Daten bestmöglich zu schützen. Ein wesentlicher Aspekt dabei ist die Sicherheit der Systeme, die Kundendaten verarbeiten und speichern. Um sicherzustellen, dass Sie als Dienstleister diese Sicherheitsstandards erfüllen, haben wir ein 3-stufiges Verfahren zur Überprüfung Ihrer Datensicherheit entwickelt. Dieses Dokument soll Ihnen einen kurzen Überblick darüber geben, was Sie in den einzelnen Stufen erwartet.

Unser Ziel ist es, mindestens eine Datensicherheitsüberprüfung pro Jahr bei Ihnen durchzuführen. Die Stufe der Prüfung hängt im Wesentlichen von der Anzahl der Kundendaten ab, die Ihr System durchlaufen.

Stufe 1 - Schwachstellenscan

In diesem Schritt ist es obligatorisch, dass Sie uns auf Aufforderung das Ergebnis eines maximal sechs Monate alten Schwachstellenscans aus dem Bereich **Applikation** vorlegen, da wir hier höchste Sicherheitsstandards erwarten.

Zusätzlich zu den Scan-Ergebnissen erwarten wir, dass Sie uns detailliert beschreiben, welche Maßnahmen zur Behebung festgestellter Sicherheitsmängel unternommen werden. Bitte erläutern Sie die Schritte, die eingeleitet wurden, um die identifizierten Findings zu adressieren und sicherzustellen, dass diese effektiv behoben werden. Exemplarisch können z.B. Acunetix, AppScan, Burp oder OWASP Zed Attack Proxy (ZAP) entsprechende Reports liefern.

Es ist wichtig, dass alle Sicherheitsmängel behoben werden, bevor mit der Anbindung weiterer Partner fortgefahren werden kann. Sollten keine Sicherheitsmängel festgestellt werden, können Sie natürlich entsprechend mit den nächsten Schritten weitermachen.

Stufe 2 – Fragebogen und Auditierung

Wenn eine Prüfung in der Stufe 2 erfolgen soll, erhalten Sie zunächst einen Fragebogen, dessen Fragen der Überprüfung der technischen und organisatorischen Maßnahmen dienen.

Die technischen und organisatorischen Maßnahmen finden Sie in Anlage A unserer Nutzungsbedingungen. Geprüft werden die Maßnahmen zur **Vertraulichkeit** (Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Trennungskontrolle), **Integrität** (Weitergabekontrolle, Eingabekontrolle) und **Verfügbarkeit**.

Ihre Angaben im Fragebogen werden durch Datensicherheitsexperten von Otto, bzw. durch von Otto beauftragte Dritte, geprüft. Bei Rückfragen nehmen wir Kontakt mit Ihnen auf. Sollten die Ergebnisse des Fragebogens kritisch sein, werden durch Otto je nach Schwere entsprechende Maßnahmen ergriffen.

Stufe 3 – Penetrationstest

Da bei der Verarbeitung einer großen Menge sensibler Kundendaten die Sicherheit der Verarbeitungs-systeme besonders wichtig ist, werden in der dritten Stufe die Ergebnisse eines maximal ein Jahr alten Penetrationstests eingefordert. Hier könnten z.B. die OWASP Top 10 als Grundlage herangezogen werden.

Otto oder ein von Otto beauftragter Dritter wird die Ergebnisse des Penetrationstests prüfen. Bei Rückfragen werden wir mit Ihnen Kontakt aufnehmen, um weitere Informationen zu erhalten. Sollten die Ergebnisse kritisch sein, behält sich Otto vor, entsprechende Maßnahmen zu ergreifen.

Eine genaue Definition des Penetrationstests, sowie die Abgrenzung zum Schwachstellenscan, finden Sie am Ende dieses Dokuments.

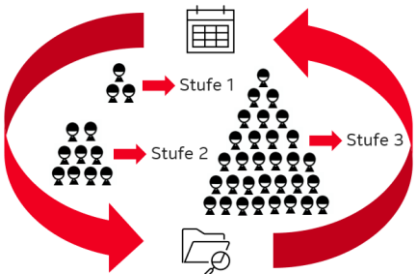
Mögliche Maßnahmen bei Nichteinhaltung der Sicherheitsstandards

- Erstellung eines Maßnahmenplans, der sowohl bereits unternommene Schritte als auch zukünftige Maßnahmen zur Lösung der Schwachstelle umfasst. Dieser Plan dient dazu, den Fortschritt zu dokumentieren und sicherzustellen, dass alle erforderlichen Schritte unternommen werden.
- OTTO setzt eine verbindliche Frist zur Behebung der identifizierten Schwachstelle(n), innerhalb derer Sie als Verantwortlicher die notwendigen Maßnahmen zur Lösung ergreifen müssen.
- Prüfung in der nächsthöheren Stufe: Falls die Sicherheitsstandards nicht erfüllt werden, erfolgt eine Überprüfung in der nächsthöheren Stufe des Verfahrens. Hier werden zusätzliche Sicherheitsmaßnahmen und Kontrollen durchgeführt, um die Einhaltung der Standards sicherzustellen.
- Teilweise Einschränkung der App: Bei festgestellten Sicherheitsmängeln kann die App so eingeschränkt werden, dass keine weiteren Partner aufgeschaltet werden können. Dadurch

wird verhindert, dass potenziell unsichere Verbindungen zu sensiblen Kundendaten hergestellt werden.

- Komplette Einschränkung der App: Im Falle schwerwiegender Sicherheitsverstöße kann die App komplett eingeschränkt werden, sodass keine Daten mehr gesendet oder empfangen werden können. Diese Maßnahme dient dem Schutz der Kundendaten und der Verhinderung von möglichen Sicherheitsrisiken.
- Information der Dienstleisterpartner: Sollten gravierende Datensicherheitsmängel festgestellt werden, werden die betroffenen Dienstleisterpartner darüber informiert. Dadurch wird Transparenz geschaffen und dem Partner die Möglichkeit gegeben, frühzeitig Maßnahmen zu ergreifen.
- Ausschluss vom Developer Program: Im Falle schwerwiegender oder wiederholter Verstöße gegen die Sicherheitsstandards behalten wir uns vor, den Dienstleister vom Developer Program auszuschließen. Dies hat zur Folge, dass die Zusammenarbeit beendet wird und keine weiteren Apps entwickelt oder angeboten werden können.

Wann erfolgen die Überprüfungen?



Die Überprüfungen erfolgen in regelmäßigen Abständen, Sie können sich auf eine jährliche Prüfung einstellen.

Außerdem erfolgen Prüfungen, sobald die Anzahl der Kundendaten, die Ihr System passieren dies erforderlich machen.

Die erste Überprüfung erfolgt, sobald der Public Access angefordert wird oder nach sechs Monaten im Private Access.

Im weiteren Verlauf erfolgen Überprüfungen in Abhängigkeit der Anzahl von Kundendaten, die Ihr System durchlaufen. Unabhängig von der Anzahl der Kundenbestellungen kann auch eine Prüfung in einer der drei Stufen erfolgen, wenn wir dies für notwendig erachten.

Definition Penetrationstest

Ein Penetrationstest ist ein autorisierter simulierter Angriff auf ein Computersystem, Netzwerk oder eine Webanwendung, um Sicherheitslücken und Schwachstellen zu identifizieren, auszunutzen und zu bewerten. Ziel eines Penetrationstests ist es, herauszufinden, wie ein Angreifer potenziell Zugriff auf Systeme erlangen könnte, welche Daten kompromittiert werden könnten und wie weit ein solcher Angriff reichen könnte. Dabei werden verschiedene Angriffsszenarien durchgespielt, die von echten Hackern genutzt werden könnten. Der Penetrationstest liefert detaillierte Informationen über gefundene Schwachstellen und gibt Empfehlungen, wie diese geschlossen werden können. Er beinhaltet in der Regel die folgenden Schritte:

- Planung und Vorbereitung: Festlegung der Ziele und des Umfangs des Tests, einschließlich der Systeme, die getestet werden sollen, und der Testmethoden.
- Informationsbeschaffung: Sammeln von Informationen, um zu verstehen, wie das Ziel funktioniert und potenzielle Angriffspunkte zu identifizieren.
- Schwachstellenanalyse: Identifizieren von potenziellen Schwachstellen in den Systemen.
- Ausnutzung: Versuch, die identifizierten Schwachstellen auszunutzen, um unautorisierten Zugriff zu erlangen oder andere bösartige Aktivitäten durchzuführen.
- Berichterstattung: Erstellung eines detaillierten Berichts, der die gefundenen Schwachstellen, die durchgeführten Angriffe und Empfehlungen zur Behebung der Schwachstellen umfasst.

Abgrenzung zum Schwachstellenscan

Ein automatisierter Schwachstellenscan auf Applikationsebene ist ein Prozess, bei dem eine spezielle Software verwendet wird, um potenzielle Sicherheitslücken in einer Anwendung zu identifizieren. Diese Art von Scan konzentriert sich auf die Überprüfung der Anwendung selbst, einschließlich des Quellcodes, der Konfiguration und der Schnittstellen, um Schwachstellen aufzudecken, die von Angreifern ausgenutzt werden könnten.

Der automatisierte Schwachstellenscan auf Applikationsebene kann verschiedene Techniken verwenden, um potenzielle Schwachstellen zu identifizieren. Dazu gehören das Durchsuchen des Quellcodes nach bekannten Sicherheitslücken, das Testen der Anwendung auf bekannte Angriffsmuster und das Überprüfen der Konfigurationseinstellungen auf mögliche Sicherheitsprobleme.

Schlussklausel

Die Einhaltung der Sicherheitsstandards ist von entscheidender Bedeutung, um das Vertrauen unserer Endkund*innen und Marktplatzpartnern zu rechtfertigen und die Sicherheit sensibler Daten zu gewährleisten. Wir bitten Sie daher, diesen Datensicherheitsprozess ernst zu nehmen und aktiv an der Sicherung der Kundendaten mitzuwirken.