Information Security

IONOS SE, Karlsruhe

Kunden-Pentest Anfrageformular

-

Pentesting Form for Customers

Version **1.4**

Einleitung

Generell erlaubt IONOS Penetrationstests von Diensten, Applikationen und Infrastruktur, die Ihnen als Kunde im Rahmen Ihres Vertrages zur Verfügung gestellt wird. Obwohl die IONOS regelmäßig eigene Tests durchführt, sind Sie als Kunde bei vielen Produkten selbst für die Sicherheit verantwortlich. Penetrationstest und das anschließende Beheben der gefundenen Schwachstellen können so die Sicherheit Ihres Angebotes verbessern.

In vielen Fällen teilen sich mehrere Kunden die Infrastruktur, so dass bei einem Penetrationstest Sorgfalt und Vorsicht geboten sind, damit der Test andere IONOS-Kunden und die IONOS Infrastruktur nicht beeinträchtigt. Daher sollten Penetrationstests vorher angemeldet und explizit genehmigt werden. Nicht genehmigte Tests sollten nicht durchgeführt werden. Zuwiderhandlungen gegen die folgenden Regeln können einen Verstoß gegen die IONOS AGB darstellen und zu einer Suspendierung oder Kündigung des Kundenverhältnisses führen.

IONOS lehnt jegliche Verantwortung für Schäden an Ihren Diensten, Applikationen und Infrastrukturen, die durch den Penetrationstest entstanden sind, ab. Erstellen und testen Sie daher Backups vor der Durchführung des Tests.

Welche Tests sind nicht erlaubt?

Folgendes soll aus technischen und rechtlichen Gründen nicht getestet werden:

- Dienste, Applikationen und Infrastruktur der IONOS Gruppe
- Dienste, Applikationen und Infrastruktur anderer Kunden
- Physische Hardware sowie die Einrichtungen der IONOS

Weiterhin sollten jegliche Aktivitäten unterbleiben, die andere Kunden oder die IONOS beeinträchtigen könnten. Dies sind unter anderem:

- Jegliche Angriffe über Netzwerk, die massiv Netzwerkverkehr verursachen, zum Beispiel Denial of Service (DoS) Angriffe
- Zugriff auf Daten die nicht Ihnen gehören
- Social Engineering oder Phishing Angriffe auf unsere Mitarbeiter

Welche Schritte müssen vor einem Test durchgeführt werden?

Vor jedem Penetrationstest sollte eine explizite Zustimmung der IONOS eingeholt werden. Der Antrag muss mindestens 5 Werktage vor dem eigentlichen Penetrationstest eingereicht werden, da er ansonsten nicht rechtzeitig bearbeitet werden kann. Er muss mindestens die folgenden Informationen enthalten und unter Angabe Ihrer Kunden- und Vertragsnummer an security@ionos.com geschickt werden.

1. Kontaktdaten des Auftraggebers. Die Erreichbarkeit muss während des Tests sichergestellt werden.
2. Kontaktdaten des durchführenden Pentesters. Die Erreichbarkeit muss während des Tests sichergestellt werden.
3. Grund für den Penetrationstest
4. Scope (z.B. Web-Application Test, Infrastruktur-Test) und eine kurze Beschreibung des Testes.
5. Genauer Zeitraum der Testes mit Angabe von Datum und Uhrzeit
6. Quell-IP-Adressen oder -Bereiche von denen der Test durchgeführt wird
7. IP-Adresse(n) des zu testenden Zieles

Nachdem der Antrag erfolgreich bei uns eingegangen ist, wird er bewertet und innerhalb von 5 Werktagen erhalten Sie eine Antwort. Wenn die Antwort durch IONOS nicht positiv ist, sollte der Penetrationstest nicht durchgeführt werden! Sollte sich bei Ihnen etwas kurzfristig ändern, stellen Sie bitte den Antrag erneut, der bisherige Antrag wird dadurch ungültig.

Melden von Schwachstellen

Sollten Sie während des Tests eine Schwachstelle in Applikationen, Diensten oder der Infrastruktur der IONOS entdecken, melden Sie diese bitte innerhalb von 24 Stunden an security@ionos.com. Wir werden danach Kontakt mit Ihnen aufnehmen und weitere Schritte besprechen.

Introduction

In general IONOS allows penetration testing of services, applications and infrastructure provided to you as a customer within the scope of your contract. Even though IONOS executes their own tests on a regular basis, you as a customer are responsible for the security of many products yourself. Penetration testing and the following resolving of found vulnerabilities can therefore improve the security of your offer.

In many cases several customers share the infrastructure so a penetration test requires care and attention to ensure that the test does not affect other customers and our own infrastructure. Therefore, penetration tests should be announced before execution and permitted. Unapproved tests should not be executed. Noncompliance with our terms and conditions and the following rules can lead to a suspension or dismissal of the customer relation.

IONOS declines any responsibility for damage to your services, applications and infrastructures caused by the penetration test. Therefore, create and test backups before running the test.

Which tests are not allowed?

The following must not be tested due to technical and legal grounds:

- Services, applications and infrastructure of IONOS group
- Services, applications and infrastructure of other customers
- Physical hardware as well as the facility of IONOS

Furthermore any activity that can compromise other customers or IONOS is prohibited. These include among others:

- Any attacks through the network that cause massive network traffic such as Denial of Service (DoS) attacks
- Access to data that does not belong to you
- Social Engineering or Phishing Attacks on our employees

Which steps do you have to take before a test?

Every penetration test should be permitted from IONOS. The request has to be submitted at least 5 workdays before the actual penetration test. It has to include at least the following information and should be submitted to security@ionos.com. Please provide your customer and contract number.

1. Contact data of the ordering party. Reachability has to be ensured during the test.
2. Contact data of the executing pentester. Reachability has to be ensured during the test.
3. Reason for the penetration test
4. Scope (e.g. web application test, infrastructure test) and a short description of the test
5. Exact time frame of the test with date and time
6. Source ID address or domain from which the test is executed
7. IP address of the target to be tested

Where to send the Request to?

After successfully submitting the request with us, it is rated and within 5 workdays you will receive an answer. Only with a positive feedback from IONOS the penetration test may be executed. If anything changes on short notice on your side please submit the request again. The previous request will be invalid.

Reporting of vulnerabilities

If you find any vulnerabilities in applications, services or infrastructure during the test please report them to security@ionos.com within 24 hours. We will contact you and discuss further steps.