Information Security

IONOS SE, Karlsruhe

Pentesting Form for Customers

Version **1.4**

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.