渗透测试流程

**渗透测试 – Windows Azure**

Windows Azure 非常重视平台的安全，已经实施了多项有助于提高平台安全的[技术和程序性措施](http://www.windowsazure.cn/zh-cn/support/trust-center/)。这些措施包括身份和访问管理、相互 SSL 身份验证、分层环境、监视、日志记录和报告。我们还进行定期渗透测试，以探测平台的弱点，并帮助我们改进安全控件。

我们深知，安全评估和测试也是客户应用程序开发和部署的重要部分。我们确立了一项策略，即让客户对托管在 Windows Azure 中的应用程序执行授权渗透测试。*因为此类测试可能无法与真实攻击区分，因此客户请务必在提前通知 世纪互联并获得批准后，再严格按照我们的条款和条件进行渗透测试。*

**渗透测试批准流程：**

1. *启动渗透测试的批准流程*

要获得渗透测试的批准，请填写“渗透测试批准表”，然后通过致电技术支持热线400 0890 365或者访问[https://support.windowsazure.cn/support/support-azure](https://na01.safelinks.protection.outlook.com/?url=https%3a%2f%2fsupport.windowsazure.cn%2fsupport%2fsupport-azure&data=01%7c01%7ckejiema%40064d.mgd.microsoft.com%7c32ec7789d3234a06b7d908d302a4eac5%7c72f988bf86f141af91ab2d7cd011db47%7c1&sdata=UJJdtdLRwRqRFqC4US1W7GZ9JIennqjl9U%2bEZUMDL%2fg%3d)来提交服务请求。成功提交后，将向您提供一个参考号，以用于与此测试申请相关的任何进一步通信。

1. *世纪互联进行批准*

提交批准表后，世纪互联将在五个工作日内响应申请。如果需要进一步信息，世纪互联将使用“渗透测试批准表”中提供的信息，通过电子邮件与您联系。您可以使用提交申请过程中提供的参考号跟踪申请状态。

1. *测试完成*

您只能进行获得世纪互联批准的测试，并且必须遵守批准电子邮件中规定的任何条件。如果您需要额外时间（或另定时间）来执行测试，必须提交新的批准表。只有获得 世纪互联对新日期的授权后，才能执行测试。

如果您认为自己发现了与 Windows Azure 服务相关的潜在安全缺陷或有对渗透测试或申请状态存有其他疑问，可通过http://www.windowsazure.cn/zh-cn/support/contact/与我们取得联系。

渗透测试批准表

|  |  |
| --- | --- |
| **姓名（主要联系人）** |  |
| **电子邮件地址** |  |
| **电话号码** |  |
| **Windows Azure 订阅 ID** |  |

1. 测试目的是什么？
2. 由谁执行渗透测试（内部团队还是第三方）？
3. 如果渗透测试由第三方执行，请提供以下详细信息：
   1. 第三方名称
   2. 联系人
   3. 电子邮件地址
   4. 电话号码
4. 您的渗透测试过程是否包括标准测试（如下文中所定义）？是/否

如果回答是，请提供这些测试的以下信息：

1. 测试的目标 DNS 名称
2. 标有时区的测试开始日期和时间 (+/- GMT)
3. 标有时区的测试结束日期和时间 (+/- GMT)
4. 您的渗透测试过程是否包括标准测试以外的测试（如下文中所定义）？是/否  
     
   如果您回答是，请列出所有此类测试：

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 测试的简短描述 | 列出您要测试的所有功能（例如 SQL Azure、Windows Azure 存储、Windows Azure 计算） | 测试的目标 DNS 名称 (\*.chinacloudapp.cn) | 从哪里启动测试？  （主机的 IP 地址） | 如果适用，请提供将使用的开源/商业工具的名称 | 标有时区的测试开始日期和时间 (+/- GMT) |  | 标有时区的 测试结束日期和时间 (+/- GMT) |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. 附加注释

**渗透测试条款和条件**

提交此表单即表示确认所提供信息的真实性和准确性，并同意以下条款和条件：

1. 您是上文中所指明 Windows Azure 订阅的所有者，且有权对该订阅执行渗透测试。
2. 您的测试不能针对任何其他订阅或任何其他 Windows Azure 客户。
3. 您不得进行任何禁止测试（参见下文）。
4. 您不得进行任何超过订阅的带宽配额的测试（如不确定，请询问客户支持）。
5. 您只能在世纪互联指定的时间和时段进行世纪互联授权电子邮件中批准的测试。您必须遵守世纪互联在授权电子邮件或任何后续通信中规定的有关这些测试的任何其他限制或条件。
6. 您的测试必须遵守此批准表中提供的信息，除非世纪互联另有规定。
7. 在测试过程中，如果您认为自己发现了与 Windows Azure 相关的潜在安全缺陷，可通过<http://www.windowsazure.cn/zh-cn/support/contact/> 与我们取得联系，在 24 小时内报告，且在至少 90 天内不得公开此信息。
8. 您对 Windows Azure 的使用（包括此测试）应继续遵守您购买 Windows Azure 时所签订协议的[条款和条件](http://www.windowsazure.cn/zh-cn/support/legal/)。
9. 如果因未能遵守本协议而导致对 Windows Azure 或其他 Windows Azure 客户造成损害，您必须承担全部责任。

**标准测试**

**以下标准测试可接受快捷审批：**

1. 为在您的端点上发现 [OWASP 前 10 大 Web 漏洞](http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf)而进行的测试
2. [在您的端点上进行的模糊测试](https://www.owasp.org/index.php/Fuzzing)

**禁止测试**

禁止执行任何类型的拒绝服务测试，或者任何其他旨在确定、演示或模拟任何类型拒绝服务 (DOS) 的存在的测试。

**隐私性**

我们将为您在此批准表中提供的信息保密，并仅用于帮助我们向您的渗透测试提供帮助，或者改进 Windows Azure 的安全。有关更多详细信息，请参阅我们的[隐私声明](http://www.windowsazure.cn/zh-cn/support/legal/privacy-statement/)。

Penetration Testing Process

**Penetration Testing – Windows Azure**

Windows Azure takes the security of our platform very seriously, and we have implemented a number of [technical and procedural measures](http://www.windowsazure.cn/zh-cn/support/trust-center/) to help with platform security. These include identity and access management, mutual SSL authentication, layered environment, monitoring, logging and reporting. We also conduct regular penetration testing to probe our platform for weaknesses and help us improve our security controls.

We understand that security assessment and testing is also an important part of our customers’ application development and deployment. We have established a policy for customers to carry out authorized penetration testing on their applications hosted in Windows Azure. *Because such testing can be indistinguishable from a real attack, it is critical that customers conduct penetration testing only after notifying and obtaining approval in advance from the Windows Azure team and only in accordance with our terms and conditions.*

**Penetration Test Approval Process:**

1. *Initiate Approval for Penetration Testing*

To obtain approval for penetration testing, please complete the ‘Penetration Testing Approval Form’, and then contact us via hotline(400 0890 365) or [https://support.windowsazure.cn/support/support-azure](https://na01.safelinks.protection.outlook.com/?url=https%3a%2f%2fsupport.windowsazure.cn%2fsupport%2fsupport-azure&data=01%7c01%7ckejiema%40064d.mgd.microsoft.com%7c32ec7789d3234a06b7d908d302a4eac5%7c72f988bf86f141af91ab2d7cd011db47%7c1&sdata=UJJdtdLRwRqRFqC4US1W7GZ9JIennqjl9U%2bEZUMDL%2fg%3d) . After successful submission, you will be provided with a reference number, which can be used for any further communication related to this request.

1. *Approval from Windows Azure Team*

Once the form is submitted, the Windows Azure team will respond to the request within five business days. In case any further information is required, the Windows Azure team will contact you by email using the information provided in the ‘Penetration Test Approval Form’. You can track the status of the request using the reference number provided during submission of the request.

1. *Test Completion*

You may only conduct those tests approved by the Windows Azure team and subject to any conditions specified in the approval email. In case you require additional time (or a different time) to carry out the testing, you must submit a new request for approval. The testing can only be carried out after authorization by the Windows Azure team for the new dates.

If you believe you have discovered a potential security flaw related to Windows Azure or or have other questions about penetration testing or the status of your request, you can reach us at <http://www.windowsazure.cn/zh-cn/support/contact/>.

Penetration Testing Approval Form

|  |  |
| --- | --- |
| **Name (Primary contact point)** |  |
| **Email address** |  |
| **Phone number** |  |
| **Windows Azure subscription ID** |  |

1. What is the purpose of your test?
2. Who is carrying out the penetration test (Internal Team or Third Party)?
3. If penetration test is going to be conducted by Third Party, please provide the following details:
   1. Name of third party
   2. Contact person
   3. Email address
   4. Phone Number
4. Does your penetration testing exercise include Standard Tests (defined below)? Yes / No

If you answered Yes, then provide the following information for these tests:

1. Target DNS name(s) for the testing
2. Test start date and time with time zone (+/- GMT)
3. Test end date and time with time zone (+/- GMT)
4. Does your penetration testing exercise include tests other than Standard Tests (defined below)? Yes / No  
     
   If you answered Yes, then list all such tests:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Brief description of test | List all features that you are targeting (e.g., SQL Azure, Windows Azure storage, Windows Azure Compute) | Target DNS names for testing (\*.chinacloudapp.cn) | From where will the test be launched?  (IP address of hosts) | If applicable, name of open source/ commercial tool that will be used | Test start date and time with time zone (+/- GMT) | Test End date and  time with time zone (+/- GMT) |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Additional comments

**Penetration Testing Terms & Conditions**

By submitting this form, you agree that the information you have provided is true and accurate and to the following terms and conditions:

1. You are the owner of the Windows Azure subscription specified above and authorized to conduct penetration testing against that subscription.
2. Your testing will not target any other subscription or any other customer of Windows Azure.
3. You will not conduct any Prohibited Tests (see below).
4. You will not conduct any tests that will exceed the bandwidth quota for your subscription (ask Customer Support if you are unsure).
5. You will conduct only those tests approved in the authorization email from the Windows Azure team for the time and duration the Windows Azure team specifies.  You will abide by any other restrictions or conditions the Windows Azure team specifies in the authorization email or any subsequent communication from the Windows Azure team regarding these tests.
6. Your testing will be in accordance with the information you provide in this form, except where the Windows Azure team specifies otherwise.
7. If during the course of your testing, you believe you have discovered a potential security flaw related to Windows Azure, you will report it to the Windows Azure team at <http://www.windowsazure.cn/zh-cn/support/contact> within 24 hours and will not disclose this information publicly or to any third party for at least 90 days.
8. Your use of Windows Azure, including this testing, will continue to be subject to the [terms and conditions](http://www.windowsazure.cn/zh-cn/support/legal/) of the agreement(s) under which you purchased Windows Azure.
9. You are responsible for any damage to Windows Azure or other Windows Azure customers that are caused by failure to abide by this agreement.

**Standard Tests**

**The following standard tests will be subject to expedited review:**

1. Tests on your endpoints to uncover [OWASP Top 10 web vulnerabilities](http://owasptop10.googlecode.com/files/OWASP%20Top%2010%20-%202010.pdf)
2. [Fuzz testing](https://www.owasp.org/index.php/Fuzzing) on your endpoints

**Prohibited Tests**

You are prohibited from carrying out any type of Denial Of Service tests, or any other tests that determine, demonstrate or simulate the existence of any type of Denial Of Service (DOS).

**Privacy**

The information you share with us in this form will be kept confidential and used only to assist us with respect to your penetration testing or improving the security of Windows Azure.  Please see our [Privacy Statement](http://www.windowsazure.cn/zh-cn/support/legal/privacy-statement/) for more details.