渗透测试流程

**渗透测试 – Microsoft Azure**

Microsoft 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](https://www.azure.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。

我们深知，安全评估和测试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 Microsoft 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。*

如果您的渗透测试过程符合下列条件之一，则无需申请渗透测试授权，我们同意您执行渗透测试，但您仍需遵循本文档中的渗透测试条款和条件：

1. 测试目的地址为您的Azure私网地址；

2. 测试目的地址为您的Azure公网地址，测试源地址为您的Azure公网/私网地址，且测试源和目的地址属于同一客户。

除以上情景外，您均需要申请渗透测试授权。

**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://www.azure.cn/support/contact/>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 Microsoft 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<https://www.azure.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** |  |
| **Microsoft 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. 提交渗透测试请求，需要完善以下内容：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 测试的简短描述 | 测试目标的 DNS 名称 (\*.chinacloudapp.cn) (没有DNS名称的，可以填写IP地址) | 从哪里启动测试？（测试源的 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 Microsoft 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 Microsoft Azure 客户。
3. 您不得有任何禁止的测试行为（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 Microsoft Azure 相关的潜在安全缺陷，可通过<https://www.azure.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 Microsoft Azure 的使用（包括此测试）应继续遵守您购买 Microsoft Azure 时所签订协议的[条款和条件](https://www.azure.cn/zh-cn/support/legal/)。

如果因未能遵守本协议而导致对 Microsoft Azure 或其他 Microsoft Azure 客户造成损害，您必须承担全部责任。

**禁止的测试行为**

1. 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。
2. 禁止进行流量型测试。
3. 禁止扫描或测试属于任何其他Microsoft Cloud客户的资产。
4. 禁止访问任何不完全属于您自己的数据。
5. 禁止对除了您的Azure虚拟机以外的任何资产执行网络密集型模糊测试。
6. 禁止故意访问任何其他客户的数据。
7. 禁止越权针对云基础设施执行POC漏洞验证程序。
8. 禁止试图对我们的员工进行网络钓鱼或其他社会工程攻击。

**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 Microsoft Azure 的安全。有关更多详细信息，请参阅我们的[隐私声明](https://www.azure.cn/zh-cn/support/legal/privacy-statement/)。