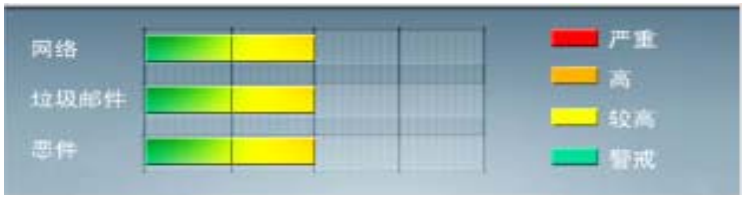
安全威胁每周警讯

2010/12/05～2010/12/11

本周威胁指数



TrendMicro 中国区网络安全监控中心

前十大病毒警讯

排名	病毒名称	威胁类型	风险等级	趋势	病毒行为描述
1	TROJ_DOWNAD.INF	木马	★★★	↑	DOWNAD 蠕虫关联木马
2	TROJ_IFRAME.CP	木马病毒	★★★	↑	GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序
3	WORM_DOWNAD.AD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
4	WORM_DOWNAD	蠕虫	★★★★	↓	该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒
5	Cryp_Xed-12	木马	★★★	→	疑似病毒
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	CRCK_KEYGEN	破解程序	★★	↓	非法破解程序
8	HTML_IFRAME.AZ	网页脚本	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
9	PAK_Generic.001	加壳程序	★★	↑	对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的
10	GRAY_Gen	间谍软件	★★	↑	间谍软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。

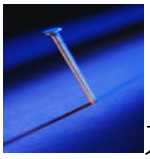
系统漏洞信息

MS10-089:Forefront Unified Access Gateway (UAG) 中的漏洞可能允许特权提升 (2316074)

受影响的软件:

Forefront Unified Access Gateway 2010

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-089.mspx



系统安全技巧

摘要: 虽然云计算的优点在不断彰显——包括可以增加企业效率和控制 IT 成本的按需服务，但是云安全却时常被认为是使得云方案无法被广泛接受的第一大障碍。下面就提供几点技巧以保障数据和网络安全。

虽然云计算的优点在不断彰显——包括可以增加企业效率和控制 IT 成本的按需服务，但是云安全却时常被认为是使得云方案无法被广泛接受的第一大障碍。

据业内专家透露，许多企业还踌躇于云环境中的数据完整性，恢复与隐私，规则服从性。

下面提供几点技巧以保障数据和网络安全。

评估你的目标

在决定要将 IT 服务迁移到云时，要了解你希望达到的商业目标是什么。比较典型的目标包括: 减少发布新应用的时间和精力；提高企业应对业务需要的能力;减少资金投入。

行利弊分析

在确定好商业目标后，还要确定向云转移的决定是否适合于企业目标。不妨考虑下列几个问题: 数据可能在哪些情况下受损，如果云服务失败，哪一部分流程会遭受损失。

予应有的关注

一旦企业选择云模式，就要选定所要部署的模式——公共云，私有云亦或是混合云——具体情况具体分析，最重要是适合企业自身需求。

明智地抉择

要选择在 IT 和安全服务领域都有实力的合作伙伴来通过云提供服务。验证其降低风险的能力是对供应 商安全考核的一部分。要选择一个可以将 IT，安全，网络服务以及强大的性能保障结合于一体的服务供应商。中立的第三方机构可以为选择此类供应商提供指导。 云服务联盟不仅为云服务的使用提供了很好的安全例证，还提供了许多合作对

象的清单。

保护数据

仔细考量供应商。据云安全联盟透露，对云安全最具威胁的就是数据流失和泄漏。因此，供应商是否能有效保护敏感数据时非常关键的。

评估供应商

要分析该公司传播那些与物理安全，逻辑安全，加密，更改管理和业务持续性以及灾难恢复等属于同类型控件的能力。同样，还要验证涉及有证明备份和灾难程序等处理的供应商。

考虑一种混合安全模式

将云中提供的服务与预置的服务混合起来。这样有助于减轻数据保护，隐私保护的压力。

注意服从性

如果无法实现服从性，那么对云和对安全的投资都不能达到我们的要求。另外，许多规则，如 PCI 数据安全标准，包括促进公司的安全姿态，与云供应商的沟通规则以及与供应商携手实现服从性。

云计算为企业带来了许多有形利益，如果仅因为对安全的顾虑就拒绝使用云，显然是不可取的行为。虽然安全方面的顾虑确实存在，但是我们也可以对症下药，积极部署风险管理，也就不用谈云色变。

来源： 网界网