SearchSecurity.com.cn

技术手册

漏洞管理指南

- ☆ 应用程序安全漏洞评估方法剖析
- ☆ 如何高效使用漏洞管理数据？
- ☆ 如何处理网络渗透测试结果？
- ☆ 如何确定你的Windows补丁级别？
- ☆ 五步评估你的安全状态

TechTarget
TT中国

漏洞管理指南

目录

应用程序安全漏洞评估方法剖析

安全管理人员对以下情景一定不会陌生：尽管企业要求安全管理人员保护企业业务，以防受到应用程序安全漏洞的威胁，但在企业部署的数百个甚至数千个应用程序中，很少有应用程序进行了充分的安全评估。

面对大量可能不安全的应用程序、有限的评估资源和难以承受的压力，在对企业的应用程序进行安全评估这一问题上，许多安全管理人员只能疲于应付。随着应用程序迅速成为最受恶意攻击者青睐的载体，攻击者试图利用应用程序中的漏洞破坏企业的日常业务活动，或者渗透企业的防御体系以窃取敏感数据。因此，安全管理人员应该确保对应用程序进行安全评估。

本文将对几种应用程序安全评估技术进行分析，并对应用程序评估的策略范例进行比较，以进一步阐明企业应用程序安全评估流程。

专业的应用程序安全评估方法

对于不熟悉应用程序安全性的人来说，下面的三种评估方法可能会令他们晕头转向。不过，每种方法都有其值得称道的地方，适用于不同的评估类型。

- **运行时漏洞评估（Runtime Vulnerability Assessment）**——运行时漏洞评估有三种方式：自动、手动和两者结合。一般来说，与手动评估相

比，自动评估的速度更快，评估的范围更广。但是，自动评估往往会漏掉不明显的漏洞，也不能发现业务逻辑缺陷。因此，大多数经验丰富的应用程序安全专家通常倾向于采用自动和手动相结合的方式。

- **源代码审查（Source-Code Review）**——利用源代码审查，评估人员可以发现应用程序中存在的各种漏洞，但该方法要求评估人员具有深厚的编程语言和安全功底，而且通常需要比运行时漏洞评估更长的时间。与运行时漏洞评估一样，源代码审查也有自动、手动和两者结合三种方式。这些方式各有利弊，类似于运行时漏洞评估的三种方式。
- **威胁建模技术（Threat-Modeling Technique）**——威胁建模技术主要是从设计的角度评估相关的、理论性的应用程序威胁。通常情况下，威胁建模先于源代码审查和运行时漏洞评估进行。

然而，选择适当的评估方法组合并不容易。许多企业都深受这一问题的困扰。下面我们将介绍几种方法，以帮助企业确定适当的应用程序安全评估流程：

1、**重点论法**：或许，最传统的方法是集中测试资源评估公开程度最高的应用程序，例如使用最为广泛的面向 Internet 的 Web 应用程序。一旦确定了公开程度最高的应用程序，评估人员就可以对其执行全面的自动和手动运行时漏洞评估。然

而，这种方法忽略了其他虽不显眼但却重要的应用程序，例如企业外部网应用程序、内部财务应用程序和关键的内部网站应用程序。

需要指出的是，尽管面向 Internet 的应用程序十分流行，但也往往容易受到外部攻击。而且，由内部威胁和客户端漏洞引起的风险也与日俱增。因此，忽略内部应用程序的安全性将会导致巨大的风险。此外，许多应用程序安全专家认为，单纯的黑盒测试的效果不如源代码审查与黑盒/灰盒评估相结合的方式。

我们已经看到，有些企业聘请了渗透测试团队，对企业的每个 Web 应用程序进行测试。可以想像的到，只有少数企业有实力采用这种方法。

2、**两点论法**：通常情况下，当认识到重点论法带来的风险以后，企业便会改弦更张，在较长的一段时间内将全面的测试计划扩展到更多的应用程序上。更为重要的是，对于那些尚未被立即测试的应用程序来说，在完成测试和漏洞修复之前，它们可能会受到攻击，而测试和漏洞修复往往需要一年甚至更长的时间。

3、**应用程序风险程度分级法**：一个可取的方法是根据多个因素对应用程序的风险程度进行分级，这些因素包括基于应用程序风险程度的各种评估技术。在开始介绍该方法之前，我们先来看一下每个应用程序的以下方面：

o 应用程序的目的：该应用程序要用来干什么？有多少人使用它？显然，一个电话簿应用程序的风险程度不会高于一个财务应用程序。

o 数据风险：该应用程序是否有机密性和完整性要求？该应用程序或运行该应用程序的服务器是否需要提供 99.999%的可用性？该应用程序是否受任何合规性法规（例如支付卡行业数据安全标准 PCI DSS、健康保险流通与责任法案 HIPAA 等）的影响？

o 架构与设计：该应用程序属于 Web 应用程序还是 Web 服务，是运行在客户端/服务器、大型机、中间层、台式机还是其他地方？该应用程序是面向 Internet 还是企业内网的？该应用程序是使用何种程序设计语言、在什么框架下开发的？该应用程序是否使用了任何已知的高风险组件（例如 Ajax 或 PHP）？该应用程序的规模大约有多大（以源代码的行数计）？

o 现有安全功能：该应用程序已经具有哪些安全功能？例如，该应用程序如何执行身份验证、授权、输入验证等？

采用这种方法，确立为上述各个因素赋以相应的风险值的准则至关重要。例如，“面向 Internet 的应用程序加 25 分”，“不共享数据和不与任何其他应用程序交互的应用程序减 5 分”，等等。最终的结果是，每个应用程序获得一个表示其风险程度的数值，你可以根据该数值对应用程序的风险程度进行分级。需要记住的是，

分析应用程序往往十分耗时，而且难以完全准确。因此，你应该尝试设定一个采集应用程序信息花费时间的上限，而不是强迫自己采集所有应用程序的所有信息。你的评分方法应该接受不完全准确的信息，并能够将这些应用程序的风险程度区分开来，即使你对这些应用程序的安全性有比较透彻的了解。不要过分迷信评分系统——如果安全专家认为一个应用程序的风险程度很高，而评分系统的结果与安全专家的意见不一致，则应以安全专家的意见为准。

对于高风险等级的应用程序，首先应该对其进行威胁建模，然后进行手动和自动运行时漏洞评估与源代码审查。

对于中度风险等级的应用程序，应该对其进行手动和自动运行时漏洞评估与源代码审查。对于低风险等级的应用程序，可能只需对其进行自动运行时漏洞评估。如果时间允许，还可以对其执行手动运行时漏洞评估。如果低风险等级应用程序的测试结果特别糟糕，则应该对该应用程序进行更加全面的测试。

4、**健康检查法**：一种替代常规风险程度分级法的方法是，采用手动和自动相结合的方式，对所有应用程序执行为期一天的短期运行时漏洞评估。在这种情况下，评估人员可以将自动扫描限制在较少的测试用例中，从而可以显著减少扫描时间（通常约为一个小时）。为此，需要减少每种攻击类型的测试用例的数目，例如

10 个跨站点脚本攻击、10 个 SQL 注入攻击等等，这一点非常重要。如果采用健康检查法，则需要对扫描结果进行审查和验证，甚至还可能需要花费额外的时间执行有限的手动测试。经验丰富的评估人员根据测试结果可以确定，究竟是优先对该应用程序进行额外的测试，还是将额外测试推迟到风险等级更高的应用程序评估完成之后进行。

5、**未经身份验证的健康检查法**：另一种健康检查方法是不需要提供身份验证凭据，在很短的时间内对所有应用程序执行为期 1 至 2 天的短期自动运行时漏洞评估。这种方法类似于脚本小子（script kiddies）和工具小子（bots）所使用的攻击方法，例如一直困扰 Web 应用程序的、臭名昭著的 ASP SQL 注入工具。当获得身份验证凭据极为困难或耗时时，可以考虑采用未经身份验证的健康检查法。但需要注意的是，通过身份验证的用户可能导致非常严重的风险，而未经身份验证的扫描将会漏掉所有针对这些漏洞的攻击。

那么，究竟采用什么方法最好呢？通过协调应用程序安全评估与业务风险评估，企业可以更好地安排时间和资金。多种方法相结合的方式是最合适的：立即确定风险等级最高的一小部分应用程序（例如公司网站的 Web 应用程序），并对其进行全面测试。与此同时，对应用程序风险程度进行分级，以确定应该对哪些应用程序执行进一步的测试。如果测试资源允许的话，在对应用程序风险程度分级的同时，

开始执行未经身份验证的健康检查评估。采用这样的评估流程，你可以获得对应用程序的全面分析和快速扫描的客观结果，从而准确了解应用程序的安全性。接下来的评估流程与常规的应用程序风险程度分级法类似：先测试风险等级最高的应用程序，再测试风险等级较低的应用程序。

当然，评估只是整个应用程序安全体系的一部分，接下来的重要步骤是漏洞修复。幸运的是，应用程序风险程度分级为确定漏洞修复的优先顺序奠定了基础：从风险等级最高的应用程序中风险最高的漏洞开始，依次解决各个风险等级的应用程序中存在的漏洞。此外，优秀的应用程序安全评估团队还能找出应用程序漏洞的根源，并在软件开发生命周期中提出修复建议，从而使应用程序从源头上更加安全。

需要强调的是，无论你采用何种应用程序安全评估方法，都比对不安全的企业应用程序引起的许多风险视而不见要好得多。

（作者：Rohit Sethi 和 Nish Bhalla　译者：王勇）

如何高效使用漏洞管理数据？

有很多机构都发现将自己的漏洞管理（VM）服务外包给别的公司有助于减少员工数量、日常开支、设备费和人事费用。但是在考虑外包漏洞管理服务能带来的诸多益处之前，机构应该谨记，期望值设定的高低在一定程度上决定了这个项目能否成功。外包公司清楚地知道，设定清晰直接的服务等级协议，完成合同上所有的指标可以避免项目开始后发现不清楚的地方，如升级导致的混乱问题和责任事故。然而最有可能被忽略的是，谁将控制数据访问和数据分享的途径。怎样才能把漏洞管理服务外包公司获取到的信息和服务供应商利用漏洞扫瞄器（如 Nessus）和网络入侵检测系统（如 Snort）收集到的信息结合起来，建立更全面的安全评估？我们一起看看下面的方法。

安全信息和事件管理以及规则遵从报表

所有的安全信息和事件管理解决方案都需要大量的数据，如日志文件和系统信息等等。对数据资源库、日志集中工具（如 Loglogic）和 COTS SIEM 产品（如 ArcSight、eSecurity/Novell）也是如此。没有这些数据就不可能对系统的安全现状进行评估。

无论安全信息和事件管理工具的使用者是外包公司还是终端客户，他们都需要从防火墙、防毒网关和网络入侵检测系统（IDS）等产品中获取日志信息和事件信

息。机构使用外包公司的漏洞管理数据的一种方法是，将漏洞评估获取的数据和从 IDS 获取的数据结合起来。这不仅为机构提供了数据，而且允许机构将特定的 IDS 警报与成功的攻击链接在一起。

获取的漏洞管理数据对机构来说有着重大的价值，特别是在审计的时候。很多 VM 工具都会建立它们管理的服务器和设备的数据清单。相应地，一些 VM 服务供应商也会使用客户提供的数据。漏洞管理工具也会实时捕捉主机或服务器的安全状况。举个例子，主机使用的是什么操作系统？系统目前运行了哪些服务？现有的补丁是什么水平？所有的这些信息都对 SIEM、配置报告以及管理工具起到至关重要的作用。实际上，很多审计员都会特别要求拟出一份关于设备网络状况和补丁情况的数据清单。当发生蠕虫病毒通过网络站点进行传播这类安全威胁时，在设备的网络状况和补丁状况都在掌握之中的情况下，一个具有报警功能的 SIEM 能够更好地利用已有数据应对潜在的危险。

“知识就是力量”这是安全信息和事件管理（SIEM）以及规则遵从报表行业的真实写照。

与 VM 服务外包公司合作

关于与 VM 服务外包公司合作，这里有如下建议：

- 要完全了解 VM 服务外包公司获取的数据情况。在签订合同之前，确保与外包公司达成一致，你拥有实时访问数据的权利，因为这些数据是通过扫瞄你的站点而得到的。
- 与外包公司确认他们所使用的产品以及信息分享的方式。通过 CSV 文件或者 XML 可以分享这些数据吗？你的 SIEM 或者法规遵从工具能够自动读取日志文件和警告信息吗？理想的情况是你能够将你的 SIEM 或者法规遵从工具与外包公司的 VM 工具直接链接，以实现实时数据共享。另一个引申而来的问题是与外包公司就计划如何将这些数据应用在服务改进中进行谈判。比如说，目前已经完成的某些任务可以如何优化以提高效率。如果对误报有一个记录，判断的标准就更精确些，管理员就不需要不断地检查同样的警告了。
- VM 收集到的一些数据，比如完成补丁所需的时间，可以成为关键性能指标（KPI），并可以体现出一些关键性能的改进情况。但最根本的问题是：如果外包公司不允许你访问这些本属于你自己的，而且很有价值的数据，那你就要仔细考虑是否要和他们合作了。

外包公司的漏洞管理工具获取的信息包含了你的设备状况和补丁状况等关键信息。即使你觉得你已经掌握了这些数据信息，依然要留心去比较那些信息，而不是直接就确定。所以当你和你的 VM 外包公司讨论系统正常运行时间和覆盖范围时，

不要忘记要求数据访问和使用的权限。因为这是你的数据信息——所以要确保你能够使用这些信息，从而使你的网络安全评估更加完善。

（作者：Diana Kelley 译者：Sean）

如何处理网络渗透测试结果？

你的第一个企业网络渗透测试现在完成了，恭喜你！而如今你将面临数目众多的漏洞信息，但是你不仅不知道怎样通过分析它们来辨别企业的脆弱之处，也不知道怎样使用这些信息对网络加强防护。

虽然采用网络渗透测试分析的做法可能会让你头晕，但这篇文章里我们还是要详细阐述如何对渗透测试的结果数据进行分析和处理。

在对网络渗透测试进行设计期间，需要设置许多界限来防止范围蔓延（scope creep），也就是哪些设备、服务以及网络需要测试，而哪些不用测试；这个范围依赖于测试的目标。一定要记录和保存这个计划，因为测试之后它就是你的测试框架，它能帮助你判断哪些测试结果应该分析，而哪些不用分析。

如果时间和要求允许，你可以把这个额外的数据写进报告的附录，作为测试范围外漏洞概述（需要更深入的调查）。

举个例子，如果你的测试范围是企业中所有的路由器和交换机，那么测试任务就是检查所有跟这些设备有联系的漏洞。而在扫描过程中，数据显示一台运行着 Windows 操作系统的机器其实是一台易受攻击的 FTP 服务器。虽然这个易受攻击的服务会带来一定风险，但是花费时间去评估这个任务范围之外的设备却会影响渗透测试分析的时间安排。出现这种情况可能是一个较小的特权访问管理问题，也可能是更严重的安全破坏，但不管怎样，简单地报告这个问题并存储相关信息就可以了。

无论如何，不要毁坏相关的测试结果，即使这些结果不属于目前需要交付的信息。

一旦你已经辨识出测试范围之内的那些漏洞测试结果，那么就要使用多种资源来验证它们的有效性。这是个重要的工作，因为不存在一种工具总是能够根据你的

测试范围提供准确的信息。这些资源一般应该包括像 Nmap 这样的工具所提供的网络测试结果。另外，还可以把数据跟 Nessus 之类的漏洞评估工具所提供的结果进行比较。

在最初的渗透测试结果分析中，其关键是去除那些可能跟特定设备相关、但跟平台无关的漏洞。Windows 的 SMB 漏洞利用程序就是一个很好的例子，虽然是针对 Windows 的漏洞利用程序，但是其运行平台实际上是一个运行 Samba 软件的 Linux 主机，它可以让几种非 Windows 的平台通过 TCP/IP 跟 Windows 系统相互联系。尽管新型的扫描器总是能更好的识别平台信息，但是由于专用安全设备，比如防火墙、IPS 以及负载平衡器等的使用，得到的实际平台结果往往并不准确。

从现在开始，把渗透测试结果数据跟所有的网络文档进行比较。今天，越来越多的渗透测试是在内部进行的白盒测试，用以验证网络设计是否反映了操作执行的情况，可以对数据的相关性进行深入剖析。从这个角度看，白盒测试一般而言会更正确一些，因为实际漏洞可能会跟网络结构图、IP 子网分配、服务列表以及其他的网络记录方面有联系。如果你正在运行一个内部测试并且可以访问这些信息的话，使用这些信息将帮助你避免浪费宝贵的的时间去做出针对关键漏洞的误报（false-positives）。

一旦你感觉测试结果已经减少到了能够处理的数量，那么就要使用标准把识别出来的风险进行分级。这个工作应该根据安全标准进行，这些标准是一般性的，但是也可以针对自己的环境进行细微的修改。这方面有许多深入的、免费的以及易于实现的标准框架。一个是开源安全测试方法手册（OSSTMM），另外一个是开放式软件保证成熟度模型（OpenSAMM）。虽然 OSSTMM 是直接面向安全测试的，但是两个标准都有很好的例子可以为你的企业建立一套标准体系。

有些渗透测试工具会提供有限范围内的相对的风险级别，即不考虑其他任何控制的实际漏洞的分级。这样做既有好处又有坏处——好处是因为它能够快速的查看高风险、能被远程利用的漏洞（这些漏洞可以让攻击者利用，进而完全控制终端设备）；但坏处是识别出的某种低风险漏洞有可能处于网络中受其他保护所控制的某台隐蔽的主机上，以至于这种漏洞才似乎更令人担心。

一旦你感觉测试结果已经减少到了能够处理的数量，那么就要使用标准把识别出来的风险进行分级。

最终，测试背后的动机将决定最终测试报告的形式。比如，测试报告可能描述了渗透测试的目标以及范围、分级别的渗透测试结果、带有修正建议的结论以及一个可选附录（为了更深入的调查或者描述测试范围之外的发现等）。请记住，真正

的危险等级是根据你自己定义的标准得来的，现成的高级、中级以及低级标准一般不会真实的反映出实际存在的风险。

渗透测试仍然是发现网络安全薄弱环节的重要方法，这需要花费大量的时间和努力，如果没有指定出如何使用测试结果的策略，那么进行测试是没有意义的。只有通过确认测试范围、验证结果、运用指标对它们的严重性进行分类、清楚简明地报告发现结果，才能真正反映出公司当前的网络安全风险状况。

（作者：David Meier　译者：Sean ）

如何确定你的 Windows 补丁级别？

对于 IT 管理员来说，给操作系统安装补丁是一件苦不堪言但又不可避免的事。不过，现在情况已大为好转，有许多方法和工具可以帮助 IT 管理员完成这一过程。首先，微软通过星期二补丁（微软通常会在每个月的第二个星期二发布安全补丁）简化了 Windows 补丁的部署和管理流程；其次，多数企业制定了补丁检查和部署策略；第三，自动化的补丁管理工具不断涌现。

那么，补丁安装是不是从此就万事大吉了呢？不，这当然不会一蹴而就。当一名新员工进入公司，在为其配备计算机之前，公司已经部署了最新的补丁，将会发生什么情况呢？当公司部署补丁时，如果漫游用户的便携式计算机未连接到公司网络，将会发生什么情况呢？当用户在自己的计算机上安装了新的软件而不知道该软件有重要的安全更新时，将会发生什么情况呢？

除了制定适当的补丁管理流程和使用自动化的补丁管理与部署工具之外，企业还需要一些方法来确定哪些计算机漏掉了补丁，以免未修复的漏洞导致这些计算机容易受攻击，并危及网络中的其他计算机。

确定漏掉的 Windows 操作系统补丁的方法主要有以下三种：

微软工具。微软为管理员提供了一些工具，可以确定漏掉的 Windows 补丁。

Microsoft Baseline Security Analyzer（MBSA）是微软免费提供的一个安全漏洞检测程序。对于 MBSA 来说，好消息是其检测范围不只局限于 Windows 操作系统，还可以用来确定微软其他应用程序（如 Microsoft Office、SQL Server 等）的安全问题和漏掉的补丁；坏消息是 MBSA 仍然是面向微软应用程序的，因此你仍然需要自行确定你的系统中是否安装了最新的 Firefox 或 Adobe Flash 更新。

通常情况下，其他厂商（如 GFI 和 Shavlik）开发的第三方补丁管理工具会提供扫描和确定系统漏掉的补丁的功能。

WSUS（Windows Server Update Services）是微软开发的一个自动化的补丁管理工具。Windows Server 2003 或 Windows Server 2008 的许可用户可以免费获得 WSUS。因为 WSUS 客户端可以自动连接到 WSUS 服务器并确定可用的补丁，所以 WSUS 能够确定系统漏掉的补丁。与 MBSA 一样，WSUS 也是一个以微软应用程序为中心的解决方案，不能确定和部署第三方应用程序漏掉的补丁。

第三方补丁管理工具。通常情况下，其他厂商（如 GFI 和 Shavlik）开发的第三方补丁管理工具会提供扫描和确定系统漏掉的补丁的功能。与微软的免费补丁管理工具不同的是，这些第三方补丁管理工具不但能够确定 Windows 操作系统上其

他应用程序（例如 Apple iTunes 或 Adobe Flash）漏掉的补丁和更新，而且能够扫描其他操作系统平台（例如 Linux 和 Mac OS X）并确定其漏掉的补丁。

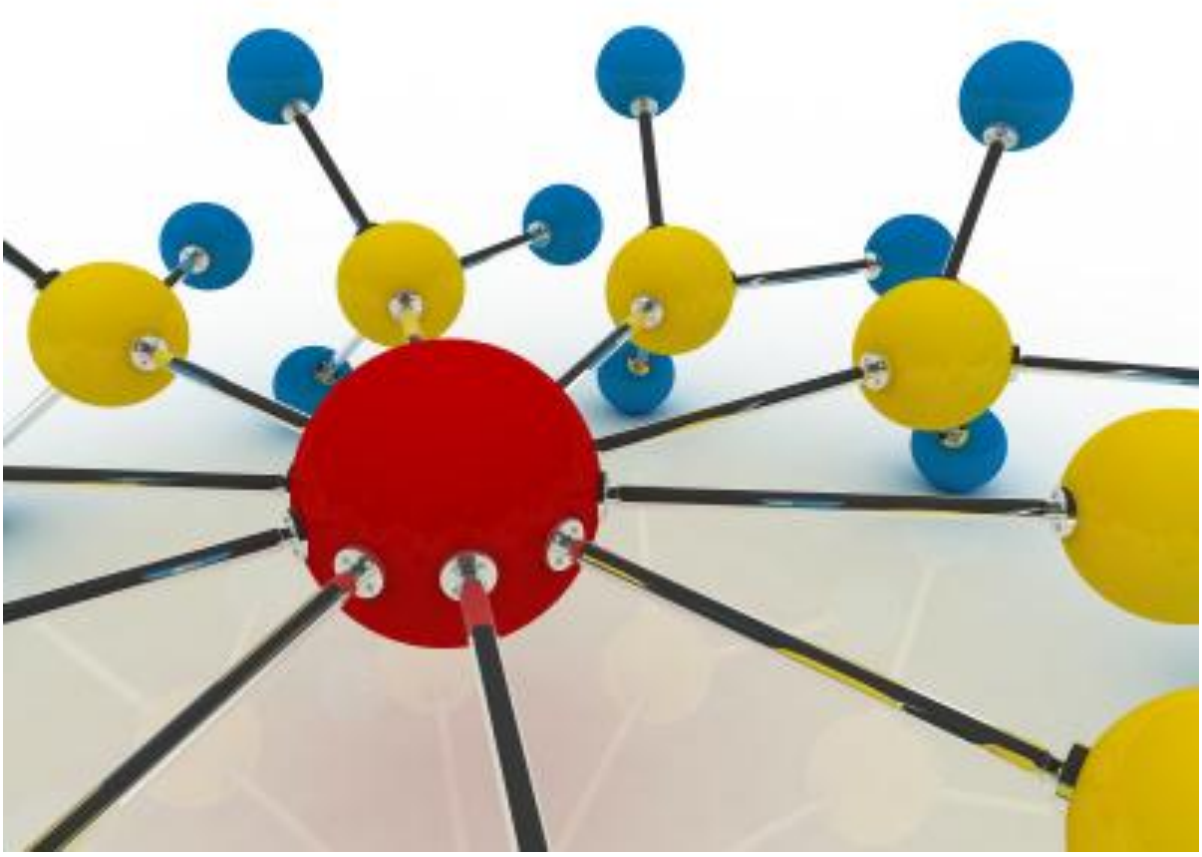
漏洞扫描器。漏洞扫描器（如 Nessus）也是一种可以用来确定漏掉的补丁的有效工具。

Nessus 不需要在目标系统上安装代理收集系统信息。通过扫描目标系统，Nessus 可以确定漏掉的安全补丁和系统配置的漏洞。Nessus 不依赖 Windows 注册表的信息，而是更深入地检查目标系统，从而发现系统实际存在的漏洞。另外，Nessus 还提供了针对各种合规性标准的扫描插件，以确保系统符合 SOX（萨班斯法案）或 PCI DSS（支付卡行业数据安全标准）的要求。

无论使用哪种解决方案来确定漏掉的补丁，你几乎都会遇到同一个问题，那就是需要跨越整个网络和目标系统的权限。如果系统的安全配置完全得当，则没有适当的授权，任何扫描器都不应该能分析整个网络中的每一台计算机。

不管采用哪种工具或方法，重要的是要将确定漏掉的补丁的定期扫描纳入到整个补丁管理流程中。忽视未安装补丁的系统不但会使这些计算机本身容易受到攻击或危害，而且可能会使其他的补丁管理工作前功尽弃。

（作者：Tony Bradley 译者：王勇）



五步评估你的安全状态

预算、时间以及人员限制要求公司有选择性地进行信息安全人力物力的投入。你如何确定哪些地方需要重点进行安全改进呢？具有成熟安全项目的企业可能有一套正式的风险管理过程，来协助完成这项工作。而另一方面，中型企业，他们的决定则更需要有策略性。

下面是评估安全状态的五个步骤，它们已经协助许多中型企业进行了评估工作：

1、**确定关键数据流**：对于企业来说，了解哪些数据是敏感数据并不容易。然而，解决这一挑战有助于你更好地理解企业的业务过程和优先事项。同时你也可以会见关键人物并听取他们的意见；他们日后也会支持你的安全改进工作。在与他们交谈时，要向他们了解数据从哪来，到哪去，哪个基础设施组件将会处理这些数据。此外，也要了解需要公司进行数据保护的所有规则遵从要求或者合同要求。

2、**了解用户的交互**：在上一个步骤中你确定的人群是怎样使用数据的？同时还要注意个人的访问权限，此外，弄清人们在公司内部，以及与合作伙伴和客户之间是如何分享数据的——脆弱的数据共享实践已经导致了许多数据泄漏事件。在这个阶段，还要评估存在哪些变化控制，以防止人们对基础设施以及其上的数据进行未授权的修改。

我们需要完成以下工作：哪些人只读取数据，哪些人需要有改变数据的权限？这将影响到执行访问控制的授权工作。

3、**检查网络周边**：当你对数据流和用户的交互有了清楚的了解之后，还需要研究网络的出口路径和入口路径。哪些地方抵抗攻击的能力最差？用来监测和阻止未授权访问的机制有哪些？如果一个外围组件（譬如说防火墙）未能阻止攻击，你的整个系统环境会不会门户大开呢？检查你的互联网连接和那些连向合作伙伴和客户的直接链接。在这个阶段的评估过程中，有线和无线网络都要检查。

4、**评估服务器和工作站**：在了解了你的网络周边的强弱点之后，请查看一下网络周边的内部系统。你需要查找可以被攻击者用来破解主机、盗窃数据的缺失补丁或者配置错误。从外部组件可以访问的服务器开始。然后再检查你的内部服务器。不要忘记评估你的台式电脑和笔记本电脑的安全状态，因为以客户端软件（比如浏览器和其插件）为目标的攻击很容易成功。

5、**查看应用程序**：最后，考虑一下第三方以及内部用户可访问的自定义应用程序中可能存在的漏洞。可以让攻击者破解应用程序的安全机制，从而进行未授权访问的漏洞有哪些？要特别注意基于网络的应用程序，近年来它们一直是攻击者喜欢的目标。解决应用程序级别问题并不简单，这也是我们不从这一步开始的原因。然而，重要的是要认识到与易受攻击的应用程序相关的风险，以便对自己的安全状态有一个完整的评估。

你不必在完成上面列出的所有的步骤之后才开始解决你发现的弱点。只要你确定了关键的风险，请尽可能好的解决它们，然后再继续评估。人们很容易在第一个阶段卡壳，因为他们试图用完美的方式解决所有的问题。可以考虑那些对当前而言足够好的状态，然后继续你的评估，以确定其他需要立即关注的关键地方。

业界有一句老话：安全是一个过程。你完成了所有的评估步骤并确定了适当的风险之后，请再次重复这个过程。重复的次数越多，你会感到你所遇到的风险越容易管理。

（作者：Lenny Zeltser 译者：Sean）