2010 年安全最佳实践汇总手册

2010年安全最佳实践汇总手册

2010年即将过去，在这一年中， IT安全各方面有哪些最佳实践值得大家去关注呢？本技术手册将为您总结2010年TT安全网站受欢迎的安全最佳实践，其中涉及网络安全、安全管理、身份认证与管理安全、系统安全、数据库安全和金融安全等方面。希望能够给安全朋友们提供一些帮助。

网络安全最佳实践

要可靠保障无线网络的安全，你必须了解你所面临的威胁。例如，PCI DSS要求每一个处理持卡人数据的组织必须对未授权的无线接入点(AP)所造成的威胁进行评估，包括那些没有WLAN的公司。

- 无线网络安全的最佳做法
- 保护企业FTP安全的最佳实践
- 应对微型botnet的最佳实践

安全管理最佳实践

合适的日志管理工具能够大幅减轻管理企业系统日志数据的负担。但是，除非组织为这个工具投入必要的时间和精力，否则再好的工具也会很快变成一个差劲的工具。

- 日志管理最佳实践：成功的六要诀
- 安全管理员职责分离的最佳做法
- 企业GRC项目管理基础最佳实践

身份认证与管理最佳实践

身份验证和访问管理（IAM）——这种用来管理用户信息和用户、网络以及应用程序之间关系的技术——最近引起了更多的关注，强大的多重身份认证手段已经成为企业 IAM 战略的核心部分之一。

- 用户供应最佳实践：访问权限重新认证
- 身份管理联盟最佳实践
- 基于风险的多重身份认证的最佳方案
- 密码加密方案：最佳做法和替代方案
- 投资管理网站用户账户设置的最佳实践

系统平台安全最佳实践

有些人声称，安全审计是测试 Windows 环境安全性的唯一方式。另外一些人则选择了漏洞扫描。还有部分人说，渗透测试才是最好的方法。更有甚者交替使用三种方法，这让人更加摸不着头脑。

- 微软 IIS 7 安全的最佳做法
- 为你的 windows 服务器找出最佳的安全测试方案

数据库安全最佳实践

数据库审计工具都有一些特殊的使用技巧，如果不花费时间合理地规划审计流程，使用这些工具可能会使得数据库运行性能遭受惨重打击。

- 数据库安全最佳实践：数据库审计工具调优

金融安全最佳实践

数据有很多不同的类型，其相应的敏感性程度也大不相同。金融机构内的安全团队应当如何去保护这些各不相同的数据类型呢？

- **金融服务领域数据分类的最佳实践**

无线网络安全的最佳做法

金融服务提供商受到为数众多的客户资料安全保障规则的制约。像 GLBA 法案(Gramm-Leach-Bliley Act)，涉及面广而且比较抽象，但它要求对所有类型的网络必须进行风险鉴定和评估，实现安全措施并对其进行监控，这其中就包括无线网。其他一些规定如著名的支付卡行业数据安全标准（PCI DSS），明确包含了在 WLAN 范围内必须执行的标准，例如检测异常操作，对无线传输的数据进行安全加密。虽然每种规则的具体情况不同，但金融服务机构通过采取以下的无线网安全最佳做法可以建立一个被全行业遵守的规则基础：

1.了解你的敌人

要可靠保障无线网络的安全，你必须了解你所面临的威胁。例如，PCI DSS 要求每一个处理持卡人数据的组织必须对未授权的无线接入点(AP)所造成的威胁进行评估，包括那些没有 WLAN 的公司。你需要从审核无线网络安全威胁着手，找出你业务中可能会遇到的威胁，并且评估敏感数据（比如个人财务信息，持卡人信息）所面临的风险。

2. 了解你自己

许多用于减少无线网络安全威胁的保障措施是否有成效，取决于是否准确理解了网络的拓扑结构(包括有线和无线)，和识别已验证设备的能力。为了制定 WLAN 安全审核和执行的标准，你必须维护那些已被认可的接入点和客户的清单、它们的用户及其地址，以及各自预期实施的安全措施。

3. 减少暴露

当 WLAN 的使用已被授权且数据流量通过一个敏感的网段时，一些规则如 PCI DSS 将会全力保证用户的安全。你可以通过对流量进行分割以减少暴露来降低风险。具体来说，就是使用防火墙对数据包进行检查，以防止数据包进入到不需相应权限即可访问的网段中，并实现时序同步的日志功能以记录那些被允许和被阻止的无线通信流量。作为一项规则，那些需要无线访问权限的网段需被看作是“隔离区”(DMZ)：默认和否认一切，只允许必要的服务和特殊目的的流量通过。

4. 堵住漏洞

使用传统的网络安全最佳做法，可以对所有暴露在无线网络中的基础设施（如接入点、控制器、DNS / DHCP 服务器）的安全性进行强化。例如，更改出厂默认值、设置强度很高的管理员密码、关闭不使用的服务、应用补丁和对系统进行渗透测试。在这一步中，你需要解决无线传输特有的漏洞问题，比如说你需要选择非默认的网络名称（SSID）以防止意外的入侵，并通过动态频率选择（dynamic frequency selection）来规避射频干扰。同时，你还可以采取措施，防止公众场合的接入点受到物理干扰（例如，移除电缆，重置为默认设置）。

5．确保传输安全

目前的接入点都支持 WPA2 (AES-CCMP)空中（over-the-air）加密，你需要尽可能多地使用它。如果传统的客户端要求的是 WPA（TKIP/MIC）标注，请谨慎使用该密码，最好是在同其他用户隔离开的无线局域网（SSID）条件下使用。请避免 WEP 加密，因为更新的安全规定将不再允许使用这一冗长零碎的加密协议。此外，使用高层加密（例如，SSLv3/TLS，IPSec）可以有选择地对敏感应用程序流和交易进行保护，同时也请不要忘了对所包含的服务器和网关的安全性进行加强。

6．限制访问

无线网打开了一个外人可以入侵的窗口，要想避免出现这种情况除非你能对其进行控制。选择并实施一个强有力的 WLAN 身份验证措施，最好选择有相互身份验证的 WPA2 企业标准 (802.1X)。如果你所在的组织缺乏这方面的技能、基础设施或对 802.1X 的客户端支持，你还可以使用 WPA2 个人标准(PSK)，但请至少使用含有 13 个字符长度并定期更改的随机密码。永远不要依靠 MAC 地址过滤器作为你唯一的访问控制措施。如果你的 WLAN 提供 guest 级的互联网访问权限，请限制它所能访问的内容，并对那部分网络通信做日志，从而减少对公司业务造成的风险。

7.无线监测

虽然许多规则强烈建议采用全天候分布式无线入侵检测或防御系统（WIDS/WIPS），但也允许在那些处理受控数据的站点上进行周期性的扫描。前者效率更高，效果也更加明显，特别适用于大规模的无线局域网。无论选择哪种方式，你都需要知道你监测的对象不仅仅是无线接入点欺诈，还包括未经授权的客户、配置错误的设备、意义不明确的安全策略、安全侦查、攻击通信流量，以及彼此相连或连到外部 WLAN 的异常客户端。

8. 做好准备

监测只是某种手段，你需要安装一个 WLAN 事件响应程序。例如，你如何暂时屏蔽掉异常的 AP？您如何找它，并从物理上移除它？你需要审查所有的扫描结果、无线入侵检测或入侵防御系统的警报和流量日志，从而及时评估潜在的威胁。实际上，利用自动化的工具（如无线入侵检测或入侵防御系统）对网络连接进行跟踪和隔离，可以实时地制止入侵。请确保监测工具能够收集充足数据，使得事件响应和取证调查更加精确。

9．保护终端

一台被盗的销售点终端或一台被黑了的笔记本电脑可以轻易获得授权并使用加密的连接，由此侵入具有严密保护措施的无线网络。这时，你可以采用远程访问安全的最佳做法，使得无线终端相互隔绝，阻止丢失和被盗的移动设备对无线网络进行未授权的访问。如果您的组织实施了网络访问控制（NAC），那么你可以对无线连接设备的完整性进行检查，并使用主机入侵检测或防御手段阻止终端的异常行为（如，同时对有线网络和无线网络进行连接）。

10．评估和改进

永远不要认为安全措施会像预期那样，你的安全审计人员就不会这么认为。你需要对无线连接的网络和设备进行渗透测试，它会有意触发 WIDS/WIPS 警报，捕获通无线信流量并对其进行分析。你可以尝试着从不同的位置去连接未经授权的设备和用户，记录下会发生的情况，然后通过对已发现的漏洞打上补丁来提高安全标准。你需要定时或不定时进行安全评估，以找到并修复新发现的漏洞，比如你可以通过对接入点、控制器或客户端打上安全补丁，阻止新型的黑客攻击。

综上所述，如果金融企业肯花时间评估无线安全威胁、管理访问权限、保障传输安全、对无线数据进行强有力的安全加密以及采取其他一些重要措施，其自身的安全性甚至可以超过审计人员的预期。

原文出处：http://www.searchsecurity.com.cn/showcontent_31795.htm

（作者：Lisa Phifer　译者：Sean　来源：TechTarget 中国）

保护企业 FTP 安全的最佳实践

虽然各种威胁在持续发展演变，但是文件传输协议（通常称为 FTP）基本上还是跟几年前一样，而且还在大范围的使用。

FTP 主要用来传输大文件，它就是为了这个目的设计的。FTP 是一种客户端服务器（主从模式）协议，它使用控制和数据两条通道进行文件传输。控制通道用来进行身份认证，并给服务器发送命令。该协议本身不支持加密，因此，在控制通道中发送的所有流量都是直接发送的，或者说是未加密的，这是该协议的弱点之一。在企业中，FTP 服务通常被用来处理那些不敏感的内容，而且跟其他敏感信息系统都是完全隔离的。人们还得保证 FTP 服务能够及时更新。配置错误的以及结构不合理的 FTP 服务可能会成为企业中重要的安全漏洞。

企业确保关键 FTP 安全的最佳做法是什么？FTP 安全状况达到可以传输敏感数据的地步了吗，或者说有什么好的方法可以让 FTP 更安全？如果 FTP 还不够安全，不足以用来传输敏感数据，那么有哪些协议可以替代它呢？我们会在本文中回答这些问题。

FTP 无处不在，这一点不可否认。就像其他广泛使用的技术一样，FTP 也开始成为攻击者易于攻击的目标。这么多年来，攻击者已经有了许多使用 FTP 以及利用 FTP 漏洞的经验。有关 FTP 服务安全性的讨论很激烈，一般来说，人们没有就哪种方法能最好地保护 FTP 安全达成共识。主要是由于商业需要，才让这项服务继续存在，而没有使用其他更加安全的替代产品。对我来说，任何使用或者考虑使用 FTP 的企业都应该先问自己以下三个问题：

a. 我们真的需要 FTP 吗？
b. 我们怎样才能安全地设置 FTP（我将会解释这个自相矛盾的情况）？
c. 有没有既安全又容易使用的 FTP 替代产品？

第一问题很有趣。从技术上讲，答案是否定的。其实市面上有许多更加安全的其他技术，我们将在后面讨论。然而，实际的答案却是肯定的，因为 FTP 应用非常广泛，而且具有跨平台的支持性，大多数企业都被迫选择支持 FTP。

我花了相当多的时间对过滤设备（即防火墙）上的 FTP 连接进行故障排除，了解到 FTP 的控制和数据通道设计不是很适合在数据包穿越多个不同的网络设备环境中使用。给你们举个例子，初始化一个网络代理后面的公司网络以及负载均衡环境中服务器之间的 FTP 会话，并不是那么简单的故障排除工作。

正如我先前提到的，FTP 是一个客户端服务器协议，使用单独的控制和数据通道进行文件传输。控制通道用来进行身份认证，并给服务器发送命令。这种身份认证机制比较脆弱，因为认证信息没有经过加密就直接发送到服务器，使得这种网络传输很容易被窃听。在一般的 FTP 实施过程中，一些典型的安全漏洞让这个问题更加复杂化。

尽管 FTP 存在安全弊端，但是许多企业还是选择它进行大容量的数据传输。大多数工作站、应用程序，甚至网络过滤设备都内置了对 FTP 的支持。其他产品可能会更加安全，但是它们还是无法与 FTP 的便利性和低成本相抗衡。

让我们暂且假设 FTP 是唯一的选择。那么，我们可以来仔细研究几种能够让这项服务达到一定安全性的方法。我先从网络设计阶段开始，我们可以把 FTP 服务限制在专用虚拟局域网网段上。这一般需要从你的交换机、路由器或者防火墙设备中分出一个单独的专用网段来管理 FTP 服务。这种做法有多方面的目的。不仅能使你专门使用防火墙的一部分来防护这个网段，并进行渐进政策（控制源 IP）控制和简化故障排除（主动/被动连接）；而且会给你提供一个阻塞点（choke point），从而监视和使用网络安全设备，比如 IDS 或者 IPS。在这种情况下，阻塞点方法可以非常方便的进行监测和预防，你能够监视利用 FTP 服务（比如 IDS）相关漏洞而发起的攻击，或者主动拦截利用 IPS 对 FTP 服务的攻击等。

下一步，我们需要侧重于让管理 FTP 的服务器本身变得更为强大（尽管我在上文中提到首先要进行网络设计，但是我不建议在所有的安全强化步骤完成之后才对服务器进行处理）。我建议大家不仅仅要考虑应用最新补丁，按照因特网安全中心（CIS）的标准来设置服务器，还要考虑更多的东西。当受到攻击的时候，FTP 服务往往会引起严重的附加损失。这是因为，在许多情况下，FTP 服务是具有高优先级的过程（比如，作为根用户），如果被攻击者成功利用的话，攻击者会得到系统级的权限。

在服务器上隔离 FTP 服务，可以很大程度的防止这种漏洞利用攻击。这与基于网络的隔离有所不同，这种隔离是通过处理服务的硬件实现的。FTP 隔离可以通过在虚拟环境（开源 Xen 系统管理程序）中运行 FTP 服务或者改变根目录（chroot）来实现。在改变根

目录这种方法中，管理员能够在处理过程中改变磁盘根目录，这基本上限制了超出自身限制范围的操作以及访问文件系统敏感区域的能力。改变根目录可以用几种方法实现；有些例子用“/etc/ftpchroot”为特定用户确定一个 chroot 环境，有些则使用“ftp-chroot”登录类。这两种方法都建议 FTP 后台程序在 ls 支持下重新编译，所以没有特殊的依赖关系。

最后，目前有一种易于安全维护的 FTP 替代品，叫做 Secure Shell（SSH）。与 FTP 不一样，SSH 以加密的形式发送所有内容。SSH 使用加密的传输服务，并且把一个文件传输代理放在最高层，避免了 FTP 服务普遍的安全缺陷和复杂性。为了简单起见，我认为 SCP（主要是文件传输）、SFTP（运行在 SSH 上面的、全新的文件传输协议）和以 SSH 为通道的 FTP 会话，每种服务都使用了 SSH，它们都可以作为 FTP 可以接受的、更加安全的替代品。在这个分类中比较奇怪的是 FTPS（SSL 上的 FTP）。说实话，我认为 FTPS 作为 FTP 替代品不可行，因为它与防火墙不兼容。使用更加安全的协议需要进行服务隔离，并且要采取适当的服务器安全强化步骤。

FTP 另外一个有趣的替代品可能就是数字内容传输服务了，它能够提供安全的文件传输，又能简化管理。它往往是基于云的服务，其中包括文件跟踪、传输通知、流程集成工具以及可编写脚本的 API 等功能。虽然这些服务原本是为了数字内容的传输而设计的，但我想它们也可以为企业提供好的文件传输服务。

FTP 是一个敏感的话题。有些用户喜欢它的便利性，但是总的来讲，网络和安全团队并没有被这一点所迷惑。人们能够指出 FTP 的多项缺点，并且指出可以替代它的解决方法。有许多方法可以与 FTP 共存，但如果你的企业更适合使用像 SSH 这样更加安全的产品，我强烈建议您用它取代 FTP。

原文出处：http://www.searchsecurity.com.cn/showcontent_39198.htm

（作者：Anand Sastry　译者：Sean 来源：TechTarget 中国）

应对微型 botnet 的最佳实践

最近出现一些有关于大型 botnet 的事件，比如那些用来破坏 Twitter 和 Facebook 网站的 botnet，已经是众所周知的新闻了。虽然那些大型的安全事件很容易引起人们的注意，但那些规模较小的、更加隐蔽的 botnet 攻击才是对于企业来说更大的威胁，这一点已被人们所证实。

随着企业的安全防护机制日渐增强，攻击者会去寻找系统的弱点，然后开始使用规模较小的、不太引人注意的 botnet，从而避开企业的安全防卫体系。在这篇技巧文章中，我们将分析为什么这些所谓的微型 botnet 能够成功地进行攻击、怎样识别它们，以及怎样阻止它们的破坏行为。

为什么微型 botnet 的攻击效果更好

大型的 botnet 经常被用来发起拒绝服务（DoS）攻击。为了能够让一个电子商务网站崩溃，或者阻止一个企业访问 Web，这些攻击需要一些资源——即 botnet 军队。就像在战争中派遣成千上万的士兵去打败敌人一样，攻击者会将很多计算机的资源集中起来去攻击一个服务器或网络。当攻击者想对一个企业发起 DoS 攻击时，他会给很多分散的 botnet 军队发送命令，让他们集中起来攻击受害者。因为这在目标环境中创建了多条连接，所以会引起几乎所有主机和周边保护系统的注意（以及资源），致使受害者完全没有任何办法，甚至整个系统都会崩溃。

与大型 botnet 利用大量资源去冲击网络发起拒绝服务攻击所不同的是，微型 botnet 被检测到的可能性很小。因为它们只需使用较少的计算机，发送较少的数据包，所以它们在避开防火墙的 botnet 监测以及入侵检测系统方面更有优势。为了进一步避开监测，控制 botnet 的人还可以通过对自己的微型 botnet 进行设置使得杀毒软件不能工作（虽然软件看起来还在正常工作）、长期潜伏在机器上、或者不定期的呼叫攻击者以获取新命令。没有能够监测的识别标志、没有不正常行为的模式，这使得哪怕是最先进的、基于行为的入侵防护系统都很难注意到微型 botnet。

为什么微型 botnet 能够成功

为了进入企业、绕过防火墙和 IPSes，攻击者们经常以用户为目标。

使用社会工程学对目标用户进行攻击是渗透到一个企业最简单的方法之一。它能够相对容易地找到企业和员工的信息，然后把这些信息融入到一个构思巧妙的钓鱼 email 里，并以恶意软件为邮件的附件。探测和踩点分析（footprinting）网络的弱点也是微型 botnet 攻击者常用的方法，但这比发送简单的 email 需要更长的时间。一旦一台机器被攻破，攻击者要么可以给受害者的发送恶意软件命令，让它们继续攻破其他的主机，进一步的扩展 botnet，从而在受害者的网络中提取到目标数据；要么干脆把 botnet 卖给别人，转而去寻找下一个受害者。

更糟的是，一旦他们攻破了一个网络，微型 botnet 还可以潜伏一段时间，等待进一步的命令或者特定的“触发”事件。大型 botnet 需要更好的命令和控制，这样做可能导致响应不正常或者被发现，与此不同的是，小型 botnet 更加精确，最适合发起定向的攻击，特别对特定数据进行偷窃时。

微型 botnet 能够比传统 botnet 更有效地搜寻出数据。微型 botnet 经常将多种方法混合来使用，从而获得敏感数据。它们更加谨慎，在探测网络时一次只发送几个包，能利用受操纵的帐户搜寻商业秘密，并且能通过删除关键的软件文件使得杀毒软件失效。一个微型 botnet 在跟正常的网络流量一起穿过网络时，会试图发起这些攻击，而且还会尝试其他的混合攻击。

帮助找到并组止微型 botnet 的最佳办法

很明显，人的因素是一个重要的环节，而且很明显 botnet 可以避开传统的防护系统并渗透到企业环境中去。为了保护自己不受到微型 botnet 的攻击，企业必须开始分配更多的资源来检测它们，而不是只把重心放在防御上。就像前面描述的一样，botnet 经常能够轻易的潜入企业环境，而传统的防御系统却总是不起作用。不是说防御就没有必要了，而是说监测已经进入企业的 botnet 是最应该做的，哪怕是一次鼠标的点击也不应该忽视。如果你认为防火墙、IDS 或者恶意软件防御软件足以应付外界的攻击，那么这种心态会导致你误认为自己的工作环境是安全的。企业必须做得更多，才能了解自己的网络中到底发生了什么。

了解和理解网络的活动可以更早的识别出攻击，从而能够更好的对攻击作出回击。然而，这超出了资产管理的范围，而且还需要对主机上运行的全部程序、主机放置在什么地

方、它们使用什么端口等等信息有所了解。它包括对环境的映射、保持客户端软件升级到最新配置的详细资料等。

在微型 botnet 开始显现的时候，不管这一动作多么的微小，都需要你注意网络流量中异常的增长、意外开放的端口，以及帐户权限突然提升等情况。如果你正在使用一个模式扫描器（pattern scanner），那么请提高灵敏级别，花点额外的时间确定那是不是一个错误的确认。对日志进行分析是一个好的网络安全习惯，这样你可以了解网络中到底发生了什么事情。如果想对大部分的日志进行自动化分析，你可以看看由 LogLogic Inc.、ArcSight Inc 公司或者 Tenable Network Security Inc 公司提供的产品。

最后，一定要重视培训和教育用户。用户必须懂得怎样识别和报告不正常的网络活动，以避免成为社会工程攻击的受害者。为了引起用户的注意，培训过程必须安排得有趣，还应该检查用户是否真正懂得了课程所学内容。为了找到以及阻止微型 botnet 的攻击，企业必须把更好的培训和上面提到的安全措施结合起来，列入到企业的安全策略中去。

原文出处：http://www.searchsecurity.com.cn/showcontent_29601.htm

（作者：Marcos Christodonte II　译者：Sean　来源：TechTarget 中国）

日志管理最佳实践：成功的六要诀

合适的日志管理工具能够大幅减轻管理企业系统日志数据的负担。但是，除非组织为这个工具投入必要的时间和精力，否则再好的工具也会很快变成一个差劲的工具。Diana Kelley 为大家提供了 6 个确保成功的日志管理最佳实践。

门外汉用上了工具依然是门外汉

如果你不准备投入时间和精力在恰当地安装、管理日志管理工具上，那么就不要把钱浪费在日志管理系统上面。日志管理系统必须进行合理的配置，以正确解析您网络中的事件和日志，这样出来的报表才具有商业和技术价值。另一个“愚蠢”的错误是不去浏览和审查告警控制台，因而错过了关键的安全事件。因此，不要犯只重视日志管理技术而不重视系统使用的错误。

通过预定义需求来精简 RFP（请求提案）

创建 RFP（请求提案，需求方案说明书）是一个费时的过程。而一些需求一旦被定义出来，就能在随后的 RFP 中复用。这在制定日志管理的需求时很常见，因为日志管理的基本需求（例如日志文件的格式，写入日志文件的数据，等等）都是一样的，可以预先定义出来。使用预定义需求的另一个好处是这确保了在精简 RFP 周期的同时保持需求的一致性。

确定你有所需的信息

为了能够写出有效的关联规则，日志管理系统必须有足够的上下文数据进行分析。例如，为了确定某个特定的流量或者行为来自哪里，就需要知道源 IP 地址信息，这意味着日志管理系统必须先记录下 IP 地址信息，这样引擎才能够将其解析出来。又例如，如果要写一条日志分析规则对目标设备或者应用发生了某种行为进行告警，相关的日志数据必须先记录下那些行为才行。

不要局限于静态分析

大部分组织需要做的最后一件事是将那些没有整体分析模型的数据填写到另一张大表中，然后利用这张大表来进行事件分析。根据预期或者可接受行为的基线设定的告警不仅要通过分析大表中单条记录的特征来产生，还要通过分析一组记录集的特征来产生。不妨设想一下关键数据库的登录记录。一般会将两次登录失败的行为设定为触发告警的基线，但是如果那个数据库系统的密码策略从使用简单的字典单词变为使用 8 位以上非字典单词字符串，那么登录失败次数的基线可能要增大，因为用户要适应新的策略。具有智能感知能力的日志管理系统应该可以进行调节，以监测发展趋势，并为管理员提供反馈。管理员可以决定使用该趋势信息临时地改变告警阀值。

使用日志数据描述正在或者已经发生的事情

“日志是检查故障的极佳信息源”。因为大部分情况下用户判断导致故障原因的所有所需信息都能够从日志文件中找到。在危机期间，管理人员经常不得不进入被动模式，往往只能通过直觉、猜测、将不可再分的无关信息拼凑到一起等方式来判断正在或者已经发生的事情。而日志是真实发生事件的记录，日志管理系统允许管理人员针对故障信息实时地撰写和产生报表，从而真实地告诉响应小组网络中发生了什么。

使用范畴可以超越安全本身

日志管理系统是一个绝佳的安全设备信息收集和分析工具，不仅可以用这些信息实现安全感知，而且可以利用这些信息实现其他目标。例如，可以将这些信息用于分析（你的）十大业务关系的客户体验。许多 WEB 应用分析系统无法提供展示真实客户体验的细粒度视图。而设计良好的应用系统日志可以记录这些客户体验，日志管理系统可以通过这些日志来分析客户体验，从而将日志管理系统的运用领域扩展到安全分析之外。

原文出处：http://www.searchsecurity.com.cn/showcontent_38824.htm

（作者：Diana Kelley　译者：叶蓬　来源：TechTarget 中国）

安全管理员职责分离的最佳做法

问：对于以下几种服务器，你建议应该给予安全管理员什么类型的访问权限呢？

- **Windows 2000 和 2003 服务器**
- **UNIX 服务器**
- **Linux 服务器**
- **域控制器**

答：很遗憾，除了域控制器外，你没有说明在你的 Windows、UNIX 和 Linux 服务器上运行了什么服务，所以我无法给你任何具体的建议。但是，对安全管理员分配权限有些约定俗成的习惯，以避免其他人滥用他们的特权权限。

职责分离（SoD），有时被称为职责划分，是在多人之间划分任务和特定安全程序所需权限的概念。它作为一个内部控制，通过限制人员对关键系统的权力与影响，从而降低因个人意外或恶意的行为而造成的潜在破坏。它还确保人们不会面对责任冲突的问题，如是以自己还是上司的名义汇报。我们的目标是避免某个用户在一个位置上可进行和隐瞒非法行为。因此，如果你的管理员可以删除、编辑或复制数据（不被人发现），那么你就需要去查查他们职责和任务的分离情况。

理想的情况是，任何遭受潜在滥用的任务都需要被划分为独立的步骤，并将每一个步骤分配给不同的人去完成。责任必须要落实到个人，以这样一种方式才能建立系统内的相互均衡，并把未经授权的访问或欺诈行为降到最低。分解一项进程来实现 SoD，需要确保各个步骤的完成，只有当每一步都进行了，进程才能被完成，并且确保没有人能自己完成所有的进程。因此，批准一项行动的人、执行行动的人、监督行动的人必须完全分开。通过分离授权、执行和监督角色，只有出现这几个人相互勾结的情况，才能成功地实施欺诈行为。

这种分离应该存在于你的公司的报告结构以及工作职责中。例如，安全管理员不应该向直接负责服务器日常管理工作的经理汇报。这可以确保他们有能力去维护安全控制，而不被那些受一部分进程控制的个人所影响。在你的 IT 基础设施中，发展、运作及安全性

测试的分离同样非常重要。确保安全管理员没有负责其他的任务（如规划或备份），以避免可能导致的职责冲突。

最后，执行最小权限原则，即用户被授予所需执行任务时最少的权力。一位安全管理员可能需要分析服务器的记录文件，所以他将需要读取权限，但没有必要授予他写入权限。最小特权的原则适用于上至高级管理层的整个公司。在体系中，一个人被授予的权利应与其所负责的任务相称，与他们在公司中的资历无关。

原文出处：http://www.searchsecurity.com.cn/showcontent_37822.htm

（作者：Michael Cobb　译者：Sean　来源：TechTarget 中国）

企业 GRC 项目管理基础最佳实践

管理 GRC（监管，风险和法规遵从）的软件正伴随着优秀的功能和特性而逐渐成熟。更加令人欣慰的是通过紧密联系通常分开的这三方面，公司在组织架构和战略上的进步；带来的好处包括降低面临的风险，更低的审计费用，更好的总体法规遵从以及更具依据的决策。

和多数大型企业范围的项目一样，实施一个企业 GRC 项目需要协调不同的，甚至有时相对立的各个目标、预期和资源。不过，还是有些最佳实践能够证明这些努力是成功的。

最佳实践 1：变成一个 GRC 销售人员

记住一个广泛的 GRC 项目的成功需要领导层的支持，以及业务流程主管的参与，重要的是要做好遇到困难和阻碍的准备。

大多数需要被说服参与到 GRC 项目的人对他们现有的流程都很满意。多数情况下，他们对何种问题会影响他们的流程以及如何避免类似情况十分清楚。所以，向他们介绍 GRC 的好处的时候，要从现有的流程说起，并指出将低效的任务自动化、剔除或者整合的机会。进行一些重组可能是有好处的，但是只要有可能，还是先尽力改进现有的工作方式。

GRC 的优势对不同的部门和业务单元是不同的。法律和遵从专业人士可能会从单一的法规和政策文档存放地点得到最多的好处，而运营风险人士会着眼风险评估的标准化。为每个参与者想出卖点无疑会花掉很多的气力，而且还要考虑说服那些可能会有疑虑的人。

最佳实践 2：记住项目管理的根本

没有统一的目标展望以及合理的期望的话，项目很容易会偏离方向、损失动力或者无法发挥出其潜力。经常会听说有项目作为一个快速项目启动，却在一年之后被放弃，因为公司想要一个健壮的、全功能的系统来实现更复杂的 GRC 项目。

记住项目管理的基本要点。设立并跟踪目标、路标以及可交付的成果是势在必行的；得到管理层和业务流程管理者的支持还不够。这些相关方面会要求了解他们能从 GRC 项目中能得到什么，什么时候能得到。如果不能展示达到目标的进程以及在过程中逐步实现价值，你得到的任何支持者都会迅速失去兴趣。

阶段性目标通常以 2-3 个月的间隔为起始，并扩展到 3 年左右的较长的周期。它们不一定必须很复杂，但是一定是很明确的。例如，很多公司会跟踪 GRC 项目覆盖的业务流程数量或者业务用户参与的程度，来演示它支持了多少的业务。

还有，使用分阶段的方式并包括概念原型。覆盖广泛并在全公司同步启动的 GRC 项目更不容易成功，因为它会受到巨大的投资、协调和不确定性的阻碍。成功的实施几乎都是从一到两个关键领域开始，在最初的几个演示成功之后再逐步推广到其它领域。

像对待所有需要大量的时间和金钱投入的项目一样，要在项目上线运行之后保证它会持续成功。随着业务的增长，监管环境的变化，以及 GRC 项目面对新的组织架构的变化，需要制定计划来迎接变化。

最佳实践 3：将 GRC 整合到文化中

通过向主要的相关人员推销 GRC 的业务核心价值，并具备严密的项目计划将保证进程的推进，但是真正成功的 GRC 只有在它已经深入到企业文化中的时候才能达成。

经常性的沟通是关键。一个典型的 GRC 项目会包括你的直接团队、管理层支持者、一个跨部门委员会、业务流程管理者以及大量的一般用户。所有这些团队必须知道和他们相关的信息，以保证实施的动力，显示已经取得的成果，并鼓励持续的参与。

然而，单靠沟通还不能推动参与者。重要的是要找到办法来鼓励并使得 GRC 进入标准流程。关键点是要找到办法来使这些变化能够对业务的其他方面也提供帮助。例如，跟踪风险事件及其成因，可以帮助业务流程管理者避免可能造成客户投诉、产品召回、隐私泄露甚至监管部门介入之类结果的系统方面的问题。

要保持开放性和灵活性。和任何的承诺一样，变化和失误会威胁到项目的方向。所以鼓励员工去发现问题、提出疑虑、并在出现问题时保持诚实就非常重要了。建立灵活的计划可以帮助你在出现意外的情况下也能达到阶段目标，而达到阶段目标则总能保证你得到持续的支持及参与。

原文出处：http://www.searchsecurity.com.cn/showcontent_31829.htm

（作者：Chris McClean　　译者：李博文　来源：TechTarget 中国）

用户供应最佳实践：访问权限重新认证

企业自身的供应系统（provisioning system）在加入并运转后，就开始在多个主要商业应用中进行用户账户的添加、修改和删除。这一工作流程需要创建运作良好的访问参数，并使得各项工作都能按计划进行。但是，实际情况真是这样的吗？企业如何知道自己所使用的访问规则就一定是对的呢？经理如何确信自己对员工的访问授权得当，而没有给予员工远大于他们工作需要的访问权限呢？

供应系统只是按照它事先的配置去工作，如果规则有误，供应系统就会错误地设置账户。 核实供应系统是否按照政策去运行，唯一正确的方法是对它的功能进行审计：“重新认证（Recertification）”就是极佳的审计过程。

何谓重新认证呢？重新认证是指以下过程：收集用户的访问权限信息，做对比性分析，确认该访问权限是否有效，是否有必要。审计功能与企业的供应系统一同使用，从而构成一个反馈回路（feedback loop），以确保供应系统对每项访问权限的授权都是得当的。这个过程定义起来很容易，可是实施起来却很麻烦。因此，企业必须遵循一系列预先确定的步骤，来合理的执行重新认证过程。

重新认证过程的第一步是，获取对所有账户的访问权，收集被供应系统的访问信息。在供应部署的最初阶段，这项工作是由审计者和安全人员进行的。他们要么亲自提取账户的信息，制成类似于电子表格格式的信息来做对比，要么请求授予在业务系统上的管理员权限，对已授权账户的信息进行审查。然后，在供应部署更为成熟的阶段中，大多数企业利用重新认证系统从业务系统上周期性地自动提取文件信息，来进行分析。当企业准备自动地提取访问信息时，会受到以下几个因素影响。

- 有多少系统是被供应的（provisioned）：庞大的系统数目会使个人对账户信息的访问变得困难。
- 参与到系统审计任务中的安全人员数量。
- 属企业独有部分的比重有多大：空间上分散的系统，不同业务类型的管理结构，针对不同管理类型的各种授权过程，这些都会影响到信息提取过程的快慢。企业独有的部分比重越小，信息提取速度越快。
- 由供应系统定期管理的账户数目。

下一步，需要对收集到的访问信息进行标准化处理并做比较。例如，针对主机 ACF2 权限的隐藏名，比如 ASYSRDPRGC1USER11，会导致外部审计者或安全人员无法了解供应系统到底赋予了用户何种权限。每个系统的访问权限都要转化为一套共同的访问规则，要同供应系统保持一致（如，基于角色或业务功能访问），这样就能进行一对一的比较。这一过程可以让人工去完成，使用带有转换公式（translation formulas）的电子表格，并进行高亮显示。但是，如果这一过程涉及较多的系统和账户，那么人工操作所耗的时间和难度就会增大。

这一步骤较为复杂，可以借助商用的企业访问管理工具（如，Aveksa 公司的 Access Certification、Oracle 公司的 Oracle Identity Analytics、Novell 公司的 Access Governance Suite 等）来进行这项工作。这些系统都具有应用程序连接器，能够自动提取账户信息，除此之外还配备了知识引擎（knowledge engines），从而将应用程序的权限转化为和供应系统一样的规则。账户信息被标准化处理之后，这些工具的知识引擎就能进行对比性分析了。这一步骤的最终结果是对以下两种情况做出确认和报告：“致命”的访问权限组合、由于供应系统疏忽而导致的不合理授权。

另一种情况，职能经理可能将系统账户和权限授权给某个终端用户。如果是这种情况，在账户的访问权限信息被整理和标准化之后，应该有通知职能经理下述内容：他们需要为职员核实一些应用程序账户。可以通过电子邮件或利用类似于微软 Exchange Messaging 服务的任务通知系统来进行通知。然后，职能经理可以利用某种应用程序来对职员的访问权限进行审核和更新。如果有必要的话，审核和更新工作应该在职员的访问权限被核准之前进行。虽然这种通知界面部署在内部，但企业在这一步骤中所使用的访问管理工具也提供了通讯接口，用来通知经理，或提供经理在审核时所需的网络应用程序。

最后，如果在上述的重新认证过程中发现了无效的访问权限，该信息必须反馈到供应系统，从而对错误账户进行改正或删除。同时，对创建这些无效账户的访问规则要进行识别和修改，确保不再发生类似的不当配置。在最初的供应实施中，该项操作可以由人来完成。不过，企业在最后肯定希望建立这样一种工作流程，即账户信息可以从核实工具中自动输入到供应系统中，而这些核实工具是用来确保反馈回路能达到最优化的。

供应系统是管理终端用户账户生命周期的强大工具。如果供应系统遵循的规则不健全、或者存在漏洞，那么它们创建的访问规则就会违背企业的政策，或者导致法规遵从的问题。实施重新认证过程属于初期供应系统部署的一部分，是为数不多的用户供应最佳实践之一。对终端用户访问负责的审计人员、安全人员和管理人员而言，他们可以利用该过

程来确保工作流程和供应系统内部所配置规则的正确性。另外，通过预先对该过程进行定义，新的系统就可以连接到供应系统上，新的工作流程也可以明确，而重新认证过程也可以被改正，从而确保供应系统在最开始就是正确的，而不是等到有人访问了他没有权限的信息而发生了安全事件之后。

原文出处：http://www.searchsecurity.com.cn/showcontent_43128.htm

（作者：Randall Gamby　译者：Sean　来源：TechTarget 中国）

身份管理联盟最佳实践

人不是生活在真空之中，公司也不应该这样。为了在当今的市场上取得成功，金融公司不得不重新思考他们的商业运作模式。对传统实体金融公司而言，他们已经意识到利用所有的人事、系统和服务资源为公司内部的信息服务这种策略已经过时，游戏规则已经开始改变了。为了维持高效率、低成本的商业运作，他们不得不开始寻找第三方合作伙伴来扮演那些不再增加价值的角色，比如效益管理、人力资源、信息中心、旅游服务、保险和股票估价。

虽然商业领袖们很容易明白这些关系的价值，比如支付给专家更低的工资，但是实现起来却比较困难。PCI DSS 和 HIPAA 等都明确规定将严惩入侵以及传输含有敏感信息、金融信息和个人信息的数据。另外，美国具体处理违约通知条例表明，企业应为个人信息以及金融信息泄露负责，即使这是由第三方的安全缺陷造成的。出于这些风险考虑，许多金融公司选择将信息保存在公司内部以保证其安全性，但是允许他们的合作伙伴来管理这些数据。这就导致身份管理联盟技术的兴起，OASIS 的安全声明标记语言（SAML）就是其中的一种。然而，就像 90 年代的公钥基础设施（PKI）的发展一样，采用“信任通道”的安全策略来管理企业与其合作伙伴的合作仍然滞后于商业发展的需要。

身份管理联盟

身份管理联盟发展滞后是有一些原因的。其中最主要的原因是金融公司与其合作伙伴之间缺乏如何进行“信任通道”的合同规范。没有适当的合同规范，公司就没有办法确定采用第三方之后给他们带来的风险，如果第三方违反条例后他们的责任会在多大程度上得到缓解。

另一个主要问题是，在身份管理联盟中，一个身份管理服务供应商要向多家合作伙伴提供信息身份管理服务。而运作这么多的身份管理要经过很多版本的多项条约，管理的复杂性不言而喻，所以很少有公司愿意成为身份管理服务供应商。

而信任关系信息传输过程中的主要技术也是造成管理复杂性的一部分原因。数据联合技术的采用使得“安全声明”的传输得以完成。数据联合技术包括：安全声明标记语言和自由联盟（Liberty Alliance，一个致力于解决数字身份问题的业界联盟）的身份认证联

盟框架（ID-FF），这两者都是切实可行的解决方案。现在已有三个版本的安全声明标记语言被金融产业采用，它们分别是：V1.0、V1.1 和 V2.0；还有两个版本的 ID-FF 被采用：V1.1 和 V1.2。虽然它们都是可行的，但是互相之间却不兼容。这就需要公司支持多种技术，甚至所有的技术。

最后，很难保证第三方能通过正确的授权进行系统查看和管理金融公司的信息。

身份认证联盟的关键考虑因素

怎么才能使身份认证管理的效率提高呢？可以根据以下这些步骤：

- 了解商业内容 ——在公司寻找合作伙伴之前必须了解外包公司的职能，并将其分类，战略性的运作必须排除在外包考虑之外。
- 了解工作流程——一个寻找外部合作伙伴的公司，必须了解其合作伙伴进入和离开公司业务的关键点。公司还必须知道数据是会继续在自己的限制范围之内还是会被合作伙伴带走。要反映新的商业运作流程，就必须对现有的工序和程序进行适当修改。
- 确定信息敏感度——公司必须清楚各个职能中包含的信息种类，其中是否包含敏感信息、金融信息或者个人信息。公司还需要清楚有无与这些信息相关的法律法规。公司必须与可能的合作伙伴共同决定接触这些信息的人员是否需要其他的背景，在被授权接触这些信息之前是否需要其他的确认。最后，公司必须决定这些信息有没有价值，如果出现信息丢失或者泄露时，有没有必要采取补救措施。
- 确定准入合作方的资源要求——一旦公司知道每个职能包含怎样的信息，就必须制定合作方进行职能管理的权限：身份管理联盟技术的行政身份，管理联盟关系的管理身份，使用联盟服务的应用服务和项目的系统准入以及使用联盟技术的终端用户的权限。
- 定义安全声明，确保信息安全——在得知了信息敏感性和访问需求后，金融公司就有能力定义合同义务、安全控制和通信需要，以确保合作伙伴的授权用户可以安全地就与业务功能有关的信息进行交流。这些都应传达给合作伙伴公司征求同意。
- 确定安全声明协议需要沟通渠道的支持——在这一点上，公司应该与它的合作伙伴确定合适的协议——安全声明标记语言、自由身份认证联合框架，或两者都有——并且各个版本都将要予以支持。如有可能，该协议的最新版本应该是

用来提供给请求者尽可能多的信息量，他们将在与金融公司的信息交互发挥作用。

这一点会很有争论。金融公司理所当然想支持一个最小的协议以减少他们的支持成本，而合作伙伴想支持他们所使用的标准。另外还存在合作伙伴不具备任何联合能力的风险。虽然不是最佳选择，但其他方法可能需要授权，如同步登陆/密码信息，但这应该被视为一种短期减损控制。在任何情况下，只要是同意的就应该纳入到合同中和未来的迁移，即从用户名/密码到安全声明标记语言在未来的两年应该与将会蒙受的损失和转换的时间表一起归档。

- 定义审计水平和报告要求——金融公司与它的合作伙伴共同确定审计和报告的水平是十分必要的，这可以确保合同条款和条件的规定。
- 定义如何管理沟通渠道——如果金融组织不希望提供身份服务，它必须把这一责任推给合伙人或寻求国际知名公司，如平安身份认证公司，它为公司及其合作伙伴提供第三方联合经营服务。利用第三方企业的明显优势是它可以提供联系到一家公司的所有合作伙伴，并且在必要的时候进行协议转换，而该公司不用承担正在进行的联系和管理费用。缺点是，公司必须为使用该合作伙伴的服务做额外的预算。
- 制定计划——在达成一项合作伙伴如何接触金融公司以及它会履行什么职能的协议后，该公司应建立一个执行计划，包括时间表、所需资源、结构变化、流程定义、筹资模式和商业抗辩理由。这些在执行之前都应该经过专门的渠道正式批准。

在理解了与第三方合作如何有利于公司，以及理解了围绕使用他们的服务而制定的周密计划之后，金融公司可以降低为他们的股东、客户和合作伙伴提供优化服务的风险。虽然通讯部分只在一个方面起作用，但如果没有它，你的系统将继续在真空中工作，而其他金融行业将把你的公司远远抛在后面。

原文出处：http://www.searchsecurity.com.cn/showcontent_40725.htm

（作者：Randall Gamby　译者：Sean　来源：TechTarget 中国）

基于风险的多重身份认证的最佳方案

身份验证和访问管理（IAM）——这种用来管理用户信息和用户、网络以及应用程序之间关系的技术——最近引起了更多的关注，强大的多重身份认证手段已经成为企业 IAM 战略的核心部分之一。

多重身份认证经常是开启 IAM 旅程的第一个端口。众所周知，仅仅依赖密码进行保密存在很大的风险，所以定期更换密码是大家很容易想到的解决方案。而多重身份认证则排在企业现已采用的 IAM 组件列表的首位。

尽管公司高管们对这种多重身份认证手段的概念感到满意，但是对于安全和风险专家来说，让高管们提供必要的资源支持才是真正的困难所在。Forrester 研究公司最近调查了很多已采用了多重身份认证的公司，以了解这种方案的最佳执行方式。在这次调查中，出现了以下四个优秀的方案：

1．了解用户是如何工作的

最佳安全方案是用户实际已经采纳的方案——让用户接受安全方案的关键是使这些方案尽可能不对用户的正常工作造成影响。安全方案不应该仅仅是 IT 系统上的一个事后才体会到其重要性的部件；相反，强大的安全认证措施必须尽可能地融入到员工的日常生活中去。

各大公司应该正确评估安全认证方案对其用户产生的实际效果。深入了解用户如何工作并对特定用户每天的工作进行准确的描述，是确保员工工作效率的关键所在。良好的沟通是用户最终是否适应的关键——包括提醒他们实现采取正确的改进措施——而这与所选择的技术无关。

和其他大规模的技术项目一样，不完整的研究、不充分的测试以及薄弱的授权会把多重身份验证的实现变为昂贵的负担。通常，这些都是技术方面的问题，但发生在人事方面的问题也同样麻烦。例如，安全机构有时会将 IT 员工与特定用户混淆。虽然以安全的名义在 IT 部门及高层用户组织中进行一次试点工作是比较容易的，但它会导致时间和金钱等方面的资源严重估计不足。

2．确定合作方的需求并预先采取行动

在商业活动中，多重认证可以看成是一种没有 ROI 的不可复原成本——这是一个当安全项目朝着与 IT 无关的方面倾斜时全球 CISO 们都会面临的问题。安全专家需要查看客户公司的每一个角落，从而提出可以表明客户需求的 MFA，并了解客户正在试图解决的业务问题。很明显，这不仅涉及到应该运用何种技术的问题，而且涉及到多重身份认证项目如何在内部开展。由于行业的纵向差异，确保遵从法规可能是一个更强大的营销方式，但这样会让项目面临一直延期到最后截止日期的风险。因此，试着将用户数据与项目结合并加以保护是一种非常有竞争力的方案。

许多 IT 人员对待任何事物都有这样一种倾向：看它是不是可以解决安全方面问题的技术手段——这样做可以在处理人和程序之间的关系时，解决不确定性问题。然而，让 CEO 们对这种方法有一个清楚的认识，或者叫他们尝试着去理解 MFA 解决方案的精妙之处，常常会让他们的目光变得呆滞。当你试图将一个 MFA 的解决方案出售给高级主管时，不要把它当做一个技术方案；恰恰相反，你更应该把它当做可以保护公司数据的商业方案。

3．提前预判，减轻技术上会遇到的挑战

在 Forrester 所调查过的所有人中，即使他是拥有丰富经验的 IT 安全专业人员，在处理多重身份认证的问题时几乎都会遇到一些意想不到的技术问题。他们对此的建议是什么呢？有如下几条建议：使用现有的技术解决它们；对现有系统进行详细的分析；不要低估项目所需的时间和资源；越早进行测试越好。测试是顺利解决问题的关键，并且次数越多越好——这样做的原因更多是为了避免匆忙就启动项目。不仅如此，测试将揭露意想不到的系统问题，包括需要更换过时的技术，如传统的物理访问系统或远程访问软件。

很轻松的就让现有部署了的技术通过评估，或者是认为一旦 MFA 投入使用，现有的技术仍然可以继续使用，那么这将对系统的使用造成不良的影响，例如项目的推迟不可预知，以及没能预计到与将来的技术不可兼容。不要成为忽视测试的牺牲品！

4．制定策略，在正确的时机得到支持

尽早开始内部的销售过程，并且尽快得到高层的支持。后者通常说起来容易做起来难，但幸运的是，近年来安全问题终于获得了应有的 C 级重视。密码作为连接 IT 资源的唯一手段，它的使用存在着巨大又显而易见的安全弱点——应该把它在历时多年、拥有多

个项目的 IAM 计划中置于优先地位。公司一旦引进，不要因为无法交付、或在回扣上做出过多的承诺而损害了自身信誉。

在这里，可用性是一个值得重点关注的问题，而它在赢取用户的支持上也显得非常重要，否则在项目交付后，你很有可能会耗费大量时间与那些对技术不感兴趣的客户进行交涉。对于大规模的首次展示，在起步阶段你应该着手获取来自公司上下所有重要员工（团队负责人、总监、顾问等）的支持。当然，其中肯定会存在批评和抵触情绪——因此首先应进行大量的研究，为核心用户选择合适的技术，并征求他们的改进建议。

这在将来会显示其自身价值的。

原文出处：http://www.searchsecurity.com.cn/showcontent_30725.htm

（作者：Bill Nagel　译者：Sean　来源：TechTarget 中国）

密码加密方案：最佳做法和替代方案

问：编写代码来加密密码的最佳做法是什么？您能提供一些示例代码吗？

答：这是个很有趣的问题：首先，我想问的是，为什么你要实施一个密码加密程序，而不是让操作系统或应用程序管理这些信息。

如果你问的是编写能管理加密代码的应用程序，在这方面，我们一般不把密码放在代码中，而是使用证书（如 Kerberos），或信任关系信息（如联邦 SAML 声明），因为如果黑客有足够的时间和精力的话，他最终还是可以破解加密密码的。

虽这么说，但加密的最佳做法还是取决于你用什么语言来编写。我想到两个网站（在 Google 上搜寻“加密密码”会显示许多网站的样本代码）：一个是加密 HTML，它有许多工具，而不仅仅是网页；另一个是 JavaScript 工具包，允许你放密码，并为你生成 Java 代码。

原文出处：http://www.searchsecurity.com.cn/showcontent_36499.htm

（作者：Randall Gamby　译者：曾芸芸　来源：TechTarget 中国）

投资管理网站用户账户设置的最佳实践

问：某家知名的投资管理公司的网站能够让其客户访问账户信息并提出变更请求（销售、购买等等）。访问这家网站之前，用户必须输入用户名、账户号码、社会安全号码和唯一的“用户定义”（是由用户创建的而不是由公司提供的）的密码。我认为使用社会安全号码的要求很不好。在这方面有什么类似“设置用户账户的最佳实践”的专门文献可供参考？

答：我很认可你的观点。使用社会安全号码作为用户标识从来都不值得推荐，但网站采集这一信息可能是出于交易验证过程步骤的正当需求。我希望这家公司能好好权衡这种信息需求和相应的使用风险各自的利弊，作出明智的决策。

针对你的问题，电子边界基金（EFF）有一本很好的在线服务提供商(OSPs)的白皮书，它“提供了用户和因特网间的链接，提供带宽、电子邮件、Web 和其它的因特网服务。”提供因特网应用服务的公司都能够从中收获到有效信息。

原文出处：http://www.searchsecurity.com.cn/showcontent_32489.htm

（作者：Randall Gamby　　译者：　唐波　来源：TechTarget 中国）

微软 IIS 7 安全的最佳做法

多年来，微软的互联网信息服务（IIS）Web 服务器给许多企业带来了大量的安全问题，包括十二年前臭名昭著的 Code Red 蠕虫病毒。IIS 的一个重要安全隐患是它会默认安装和启用很多功能，比如脚本和虚拟目录等，但这其中的许多功能又被证实是很容易被利用，从而导致重大安全事故。

几年前发布的 IIS 6 采用了一种“默认锁定”的方法，即不安装某些功能，或者安装以后将其默认禁用，而最新版本 IIS 7 则采取了更多措施。Windows Server 2008 甚至没有默认安装 IIS 7，而在安装的时候，IIS 7 网络服务器经过配置后只提供具有匿名身份验证和本地管理的静态内容，虽然生成的只是最简单的网络服务器，但却把受到安全攻击的几率降至最小。

做到这一点是可能的，因为 IIS 7 已被完全模块化。让我们简单的研究一下 IIS 7 更加安全的原因，以及它的安全性是如何实现的。通常而言，管理员可以从 40 多个单独的功能模块中做出选择，实现完全自定义的安装。通过只安装某个网站所需要的功能，管理员可以大大减小潜在的攻击面，并且节省资源。

然而，请注意这只适用于清洁安装（clean install）。如果你在运行老版本的 IIS，你又要升级你的 Windows 操作系统，所有的元数据库和 IIS 状态信息都会被收集并保存。结果，许多不必要的 Web 服务器功能会在升级时被安装到系统中。因此，企业在升级之后最好重新查看应用程序对 IIS 功能的依赖性，并卸载不需要的 IIS 模块。

更少的组件意味着更少的设置管理，以及更少的问题修补，因为人们只需要维护那些正在使用的模块附属内容。这样可以减少停机时间并提高可靠性。此外，标签混乱的 IIS 管理控制台已经被更加直观的 GUI 工具所取代，这让安全设置的可视化更加简单，理解起来也更加容易。比如，如果支持基本身份验证的组件没有安装在你的系统中，该组件的配置设置就不会出现，以免混淆视听。

那么，安全运行 IIS 可能需要哪些组件呢？下面列出的九个组件中，运行静态网页以及其他功能的网站都需要前六个；而需要加密服务器与客户端之间数据的人则需要第七和

第八项；当你拥有一个 Web farm，并且想要 farm 中每个 Web 服务器都使用相同的配置文件和加密密钥时，你将需要第九项共享配置：

1、验证组件，其中包括集成 Windows 验证、客户端证书验证以及基于 ASP.NET 格式的验证，这些验证可以让你在应用层上管理客户端注册和验证，而不是依靠 Windows 账户。

2、URL 验证，它很好地与 ASP.NET 会员和角色管理整合，然后根据用户名和角色来授权或者拒绝应用程序中的 URL，防止没有授权的用户去访问受限制的内容。

3、IPv4 地址和域名规则（Domain Name Rules）提供了基于 IP 地址和域名的内容访问管理。新属性“allowUnlisted”可以更容易的阻止人们访问所有的 IP 地址，除非列表中允许。

4、CGI 和 ISAPI 约束，它们允许你用 CGI 文件方式（.exe）和 ISAPI 扩展方式（.dll）启用或禁用动态内容。

5、请求过滤器，它结合了 UrlScan 工具中限制 HTTP 请求类型的功能，IIS 7 将会拒绝这些包含可疑数据的请求。像 Apache 的 mod_rewrite 属性一样，它可以用正则表达式来阻止攻击或者基于动词、文件扩展名、大小、命名空间和时序的修改请求。

6、日志，它现在可以提供有关应用程序池、进程、网站、应用程序域和运行请求的实时状态信息，并且能够在整个请求与应答过程中跟踪某个请求。

7、服务器证书

8、安全套接层

9、共享配置

其他增强 IIS 7 安全性的功能还包括：Web 服务器专用的新型内置用户帐户和组帐户。该功能启用了一个系统之间通用的安全标识符（SID），从而简化了访问控制列表管理，以及应用程序池保护机制（sandboxing）。同时，应用程序管理员可以配置哪些设置，服务器管理员都能完全控制，同时让他们直接在应用程序上做出配置的改变，无需使用管理权限去访问服务器。

IIS 7 与以前的产品相比非常不同，这对用户来说是一件好事。它的设计与创建遵循了经典的安全原则，它为使用 Windows 系统的企业提供了一个比过去更加安全的、更容易配置和管理的 Web 服务器。从安全的角度看，它可能还做得不够，还不能动摇 Linux 和 Apache 工作站的地位，但是微软的确已经缩小了与它们的差距。管理员可能还需要一段时间来适应新的模块化方式以及管理工具和任务。尽管管理员都熟悉 Windows 操作系统和框架，但仍需要培训和进行系统测试。

原文出处：http://www.searchsecurity.com.cn/showcontent_41915.htm

（作者：Michael Cobb　　译者：Sean　来源：TechTarget 中国）

为你的 windows 服务器找出最佳的安全测试方案

你一定了解自己需要测试 Windows 环境的安全性，但你知道应该如何着手吗？

有些人声称，安全审计是测试 Windows 环境安全性的唯一方式。另外一些人则选择了漏洞扫描。还有部分人说，渗透测试才是最好的方法。更有甚者交替使用三种方法，这让人更加摸不着头脑。

尽管安全测试方法没有对错之分，但你选择的安全测试类型将在很大程度上决定测试的结果，并最终影响到 Windows 服务器的安全性。而在选择安全测试方式时，重要的是要纵观全局，同时问自己以及安全部门的同事这样一个问题，“我们真正想要达到的目的是什么？”

如果你只是一名安全审计员，一份能够提供短期利益的系统安全性审查可能就足够了。但另一方面，如果你想确保长期安全，还需要设法将安全测试整合到整体业务风险管理过程中去。

换句话说，你是想简单地坚持基本的规则遵从呢，还是想真正深入地研究、发现你的系统是如何应对威胁的？只有你自己能回答这些问题。

不同的测试方法产生不同的测试结果

总的来说，安全审计是站在技术和操作的高度对系统的安全性进行评估；漏洞扫描在技术方面更加深入；而渗透测试，则高度集中于某一安全问题，通常不会提供关于系统安全性的全部信息。

三种测试类型的区别如图 1 所示。

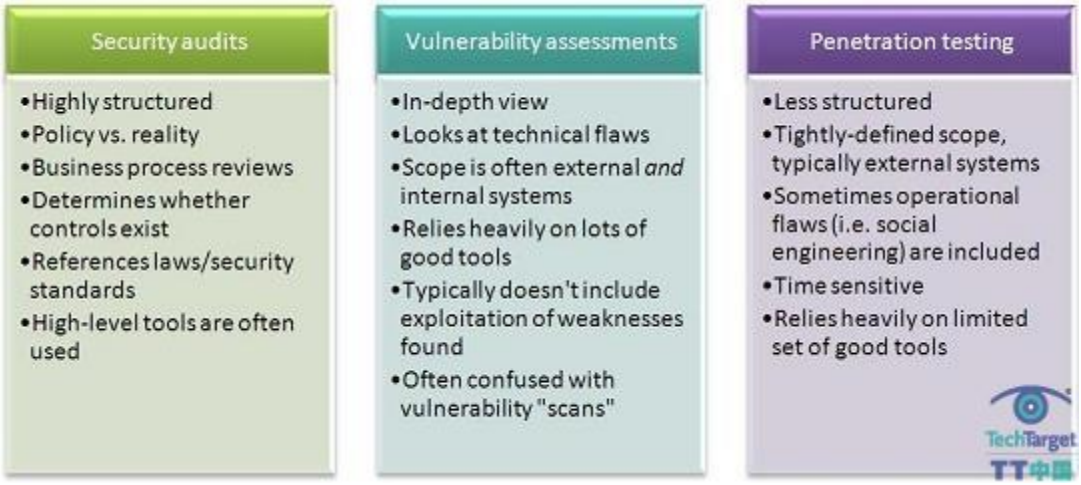

图 1：不同类型的安全测试比较

综合上述三种方法的优点并将其运用于安全测试中，虽然这样做没什么错，但道德黑客测试可以提供最有价值的测试信息，从各方面来看它也是最佳的安全测试方法。

道德黑客测试是系统安全测试的一种方式，即以恶意的心态，利用优秀的黑客工具对系统进行攻击、查找系统漏洞。这样，在真正恶意的黑客攻击系统之前你就能弥补漏洞。通过结合漏洞扫描与渗透测试，道德黑客测试不仅能让你发现重要的系统漏洞，还能让你了解这些漏洞对系统所造成的影响。

至于 Windows 安全，道德黑客测试可以提取出可能曾被忽略的技术和操作问题，如图 2 所示。

图 2：使用道德黑客测试找出 Windows 服务器中最薄弱的环节

坚持不懈地进行定期的道德黑客测试，你肯定能找到影响 Windows 服务器安全性的关键问题。

原文出处：http://www.searchsv.com.cn/showcontent_37950.htm

（作者：Kevin Beaver　译者：Dan　来源：TechTarget 中国）

数据库安全最佳实践：数据库审计工具调优

数据库管理员受命于创建审计记录以符合安全审计和合规审计的要求，但如果他们仅仅去阅读那些叙述如何进行数据库审计的标准操作手册的话，恐怕会很失望。数据库审计工具都有一些特殊的使用技巧，如果不花费时间合理地规划审计流程，使用这些工具可能会使得数据库运行性能遭受惨重打击。由于进行审计而导致数据库运行性能下降超过 50%的例子并不少见。这也就意味着，看起来简单的审计工作可能最终会导致数据库变慢、表空间占满、收集过量事件，以及给自己造成维护和报表生成方面的诸多麻烦。

相反，在开展审计工作的时候，首先应该建立一个测试数据库，并进行一些基本的性能测试：先关闭审计选项，建立性能基线，然后将其与在不同审计方式、配置和过滤选项下的审计方案测试后所获得的性能指标进行逐个比较。这样做不仅有助于理解每个审计选项对性能的影响，也可以帮助识别资源瓶颈。相信我，这些信息是你在对生产用数据库服务器进行配置之前就必须清楚的。即使是你正准备将数据库日志发送给 SIEM 或者日志管理系统的时候，创建并维护审计追踪策略仍然是必不可少的工作，别指望那些系统会去帮你优化审计设置。

以下是一些用于审计工具优化的数据库安全最佳实践：

审计方式：所有的数据库系统都提供了不止一种收集审计数据的方法，因此你可以简单地通过性能对比来比较不同的审计方式。对于 IBM DB2 数据库而言，审计有时候会是一个巨大的挑战，但是如果你仅仅审计特定用户的行为（事件），DB2 事件监控器的性能可能会表现的好一些。对于 Oracle 数据库而言，细粒度的审计机制以及一些审计选项提供了很好的伸缩性，但由于它会产生大量审计数据，同样存在潜在地数据库性能下降的风险。

审计选项：试着使用不同的审计选项组合，并进行测试。对于 Oralce 和 DB2 数据库，可以比较一下用数据库表存储审计数据和使用操作系统文件系统存储审计数据两种方案。前一种方案有助于进行数据检索，而后一种方案性能更优，并且不会占满表空间。

资源和管理：通过资源分配优化有助于审计数据的存储，尤其是打算将审计数据存储到数据库的时候，因为此时数据表很容易被写爆。应该创建一些用于归档审计数据和缩减

事件存放库表容量的脚本。对于 SQL Trace 而言，如果将事件流存储在不同的文件中，并放到指定的驱动器下，性能将会提升。审计进程也会占用不少的内存。DB2 的审计缓存大小对于性能会产生很大的负面影响，因此要增加对其所占内存的分配。针对 Sybase 公司的 ASE 数据库，为了在审计队列不断增加的时候保持处理和响应性能，需要分配大量的内存。为了提升写磁盘的效率，大部分数据库支持数据块优化，可以对只写（write-only）进行优化，并设置块大小的选项，使其大小为审计数据表行大小的整数倍。

过滤：过滤差不多是最重要的优化步骤了。请与您的安全与合规团队进行沟通，找出他们真正想要获取哪些审计信息，而不是仅仅对他们想要的信息知道个大概。从收集到的数据流中过滤出一到两种事件类型可以极大地降低存储和运算的负担。对于像 SQL Server 的 Trace 这样的工具而言，在收集数据的时候很好用，但是过滤数据就不是很方便。然而，在大多数情况下，所有的数据库都提供对用户事件、管理员事件、元数据操作事件和系统级事件的过滤功能。例如，对于 DB2 而言，如果进行细致的过滤，性能负担降低 80%不足为奇。所以，请花时间了解你到底需要什么数据，然后将你不需要的数据统统过滤掉。

在经过性能验证和比较之前，别轻易下结论说哪种审计方法一定就是好的。花些时间掌握那些审计选项，这样可以大大地减轻你审计工作的负担。

原文出处：http://www.searchsecurity.com.cn/showcontent_43172.htm

(作者：Adrian Lane　译者：Benny Ye　来源：TechTarget 中国)

金融服务领域数据分类的最佳实践

大多数信息安全从业人员都会同意这样的观点，即数据的重要性是各不相同的。换句话说，某些数据与其他数据相比更为敏感，更应该受到严格的保护。数据有很多不同的类型，其相应的敏感性程度也大不相同。金融机构内的安全团队应当如何去保护这些各不相同的数据类型呢？这就是数据分类（data classification）所涉及的领域，即每种数据类型都有自己特定的“标签”，而这些标签与基本的规则关联紧密，比如访问控制、加密、业务流程和数据处理等规则。

许多数据分类的最佳实践和计划都源自经典的安全和风险管理框架，例如 ISO 27001 和 COBIT。在很多情况下，ISO 27001 被用来开发与 Gramm-Leach-Bliley Act （GLBA，金融服务现代化法案）相吻合的控制。该标准的 A.7.2.1 节规定了数据分类指导方针应该如何进行创建和维护。FFIEC（美国联邦机构检查委员会）在颁布的信息安全 IT 考试手册中特别声明了数据分类的必要性。手册将数据分类与“保护设定文件（protection profiles）”相联系，描述了应该采取何种措施去保护特定的数据类型不受曝光和丢失的危害。

既然数据分类如此重要，金融机构应该如何进行这项过程呢？下面是一些在数据分类的最佳实践中，所有机构都应该遵循的关键步骤。

1、规定哪些数据是重要的，知道这些数据如何储存和转移。对金融机构而言，这一步　骤主要由以下方面的财务数据构成：客户（银行账户和个人信息）、公司财务记录（收入信息、销售数据）、与金融系统有关的知识产权，以及与认证和访问控制信息有关的数据。然后，与个体业务单元合作，评估应用结构和网络图，进而确定在何处存储数据，如何存储，以及数据在环境中如何移动。要确信已经将所有的合伙人和互联网都考虑到了。

2、规定数据分类类别和标签。这一步骤应该与业务单位共同开展，把重点放在金融或其它具有敏感性的数据类型上。首先，依据数据的保密性和危急层次对分类类别进行定义。举个例子，针对保密性进行的分类可以包括：公开（任何人都可以访问）、受限访问（只有特定的群体可以访问）、保密（受规则和法律授权的控制）。金融服务团队建议，应该将这些标签与危险程度结合起来：

a. 低：数据曝光和不正确使用不会造成财产损失和法律责任。

b. 中：数据曝光会造成有限程度的法律责任、客户信任的丧失和财产损失。

c. 高：数据曝光会导致重大的法律责任、客户信任的丧失和财产损失。

d. 很高：数据曝光和误用能带来灾难性的罚款、法律责任、客户信任的丧失和财产损失。

3、规定可接受性使用。数据的可接受性使用应该将内部和外部的规则遵从要求作为基础（包括各州颁布的数据泄露法），还要考虑谁会使用这些数据以及如何使用。在大多数情况下，数据的创建者会被指定为“所有者”，而创建数据的个人或者团体应该具有对数据的使用权限。例如，客户的银行数据只能有客户本人（数据“所有者”）和交易处理员工才能使用。

4、升级政策要反映出数据分类。确定了政策中已包含数据分类类型和规则遵从的影响，金融机构就可以将数据分类类型与安全意识、事件响应以及其他的危机处理方案措施结合起来。

5、建立一个维护过程。一个标准的数据生命周期包括以下阶段：创建、存储、使用、修改、保留和存档，以及清除。在每一个阶段里，数据的分类和安全都要通过常规的过程来处理。

虽然数据的分类是一项很复杂的过程，但有一些工具可以提供帮助。几家供应商提供了一些具有电子发现功能并结合了存储系统的产品，（如，EMC 公司的 Kazeon 系列产品和 StoredIQ 公司的智能信息平台），它们都能支持大型企业的数据分类工作。

尽管对数据进行分类和追踪不是一件容易的事情，但这些工作是金融服务机构进行数据保护的核心部分。许多规则遵从规定以及安全最佳实践框架都要求必须具备一定程度的数据分类，而且需要将安全工作的努力集中在更为敏感的数据类型上，从而有利于实现操作效果和效率的最优化。根据以最敏感客户和内部数据为基础创建的“保护设定文件”来看，金融机构可以更好的规划和制定自己的预防、检测和响应措施。

原文出处：http://www.searchsecurity.com.cn/showcontent_42253.htm

（作者：Dave Shackleford　译者：Sean　来源：TechTarget 中国）