IT 安全最佳实践集

IT 安全最佳实践集

“最佳实践”来自英文 Best Practice。维基百科对最佳实践的定义是一个管理学概念，认为存在某种技术、方法、过程、活动或机制可以使生产或者管理实践的结果达到最优，并减少出错的可能性。学习应用 IT 企业安全的最佳实践，其实就是借鉴别人成功的经验，让自己在保护企业安全方面少走弯路。在本手册中，将集合 IT 业内关于企业安全的最佳实践，并不断更新，以期在企业安全防护方面提供帮助。

网络安全最佳实践

网络安全最佳实践将包括网络安全的各个方面，从网络架构到具体的安全事件，目前本部分将涉及采用 IPS 的最佳实践、网络扫描和报告的最佳实践以及管理 DNS 的最佳实践。

- 防火墙规则管理最佳实践
- 采用 IPS 的最佳实践
- 网络扫描和报告的最佳实践
- 管理 DNS 的最佳实践
- 保护远程访问五个最佳实践
- 酒店网络最佳安全实践

应用安全最佳实践

应用安全最佳实践将包括如何最好地进行 IT 应用的防护，例如应用层防火墙选择与配置的最佳实践以及保护网络邮件数据安全的最佳实践等。

- 应用层防火墙选择与配置的最佳实践
- 网络邮件安全：保护数据的最佳实践
- 企业博客开发的最佳实践
- 应用软件开发最佳实践

系统安全最佳实践

系统安全最佳实践将介绍保护 Windows、linux 等系统安全的最佳方式，例如在系统上对加密密钥进行管理的一些最佳实践。

- 加密密钥管理的一些最佳实践

身份识别管理最佳实践

移动计算和远程访问越来越多，再加上无线网络的飞速增长，以及对应用程序访问需求增长，网络被未授权访问的几率显著增加，身份管理带来的问题越来越严重。本部分将集合进行身份识别管理的最佳实践。

- 企业实施单点登录的最佳实践
- 安全密码分配的最佳实践

安全管理最佳实践

在 IT 安全业界有一种说法，叫作三份技术，七分管理。IT 安全管理的重要性由此可见一斑。本部分的安全管理最佳实践将帮助您获得安全管理的最优成绩。

- 法规遵从的最佳实践

- 合并过程中制定法规的最佳实践
- 信息安全团队新成员选拔最佳实践
- 信息安全管理的炒作：揭穿最佳实践的谎言

防火墙规则管理最佳实践

有多少网络管理员想过如果他们对公司防火墙规则设置所作的变化会在网络防御上打开缺口呢？

现在网络的复杂性使对整个边界、应用和用户的纵览的维护变得很难。IT 人员经常有变更、新应用会添加，用户来来去去或者角色发生变化。这些变化都要要求对防火墙规则作出变更，许可证也会很快变得混乱。在本文中，我们将讨论成功变更防火墙规则的方法和技术。

首先，我认为管理防火墙规则的最佳方式是使用这三条关键指导方针：

- 保持规则库的简单
- 记录每一条规则
- 采用变更控制策略

保持规则库简单

防火墙使用手册经常难以理解，但要切记的关键点是过滤器指定了特定值的行为，例如阻止端口 80，但是规则采用了条件语言，如果 port=80，那就拒绝。配制防火墙的方式应该来源于在企业的安全策略中建立的业务规则。如果你以支持这些指令为目标而采用了防火墙配制，这些规则和过滤器就应该自我解释。

把过滤器和规则规则结合起来的最好方式是建立基本的 "拒绝"过滤器，然后设置独立的过滤器或者规则来处理特殊情况。例如，阻止所有端口，允许 80 端口。这种防火墙规则管理方式不能必然地规避互相重叠的规则，但是通过总是把"允许"规则放在"拒绝"过滤器前面，整体的规则设置就安全多了。

记录和变更控制策略

通过对每一条规则的评论和详细的记录，在做出变更的时候就很容易理解每一条规则背后的含义。还有一点很重要，只在遵循变更控制程序下作变更，正式协调的方法可以保住变更经

过测试，并在产生了非故意结果（例如，不安全的配置）发生后可以翻转。还要确保规则或者策略都有有意义的名字，文件名中要包含创建实践和管理员名字首字母。

有些管理员认为依靠单一的防火墙技术并不安心，淡然没有一个防火墙可以把多有的事情出色的完成。很多时候，多个防火墙需要处理网络上的多个入口，保护各种不同的业务应用。但是在网络上设置的防火墙越多，让他们在整个网络上协调一致工作就越难。

在这种情况下最好的策略是确定每一个防火墙在网络流量中的目都有明确的标和位置。例如，如果有一个防火墙是为了保护数据库，那么它的规则和过滤器就只需要关注控制流入流出数据库的流量，而不关注网络上的其他设备。这样规则设置就简单的多，从而管理也很容易。

可以自动管理防火墙规则的产品

目前已经有了自动进行防火墙管理的技术，这样在企业中维护防火墙设置的一致性和协调性就很简单了。例如只使用了四科防火墙的望楼哦可以使用 CiscoWorks Management Center for PIX 来管理多个 PIX Firewall 设备的配置，而 McAfee 的 Firewall Enterprise Control Center 提供了一个中央界面来简化多个 McAfee Firewall 工具的管理。

Juniper 的 Network and Security Manager (NSM)防火墙管理工具中我喜欢的一个功能是在每个 Junipei 防火墙上创建"开始"和"结束"规则的能力，而本地的管理员不能删除或者仅用这些规则。为了在复杂的环境中配置连贯的规则，可以尝试使用 Firewall Builder，这是一个中立场上的应用，可以配置和管理防火墙规则。使用 Firewall Builder 可以从它的 GUI 中的相同策略中为所支持的目标防火墙平台产生配置文件。

（原文此处还提到两款国外流行的防火墙管理工具，分别是 Algosec Inc.和 RedSeal Systems Inc.的产品，有兴趣的读者可以参照英文原文。）

不管使用哪个产品，切记对防火墙策略的不断改变会影响它们的性能。调整还包含了策划以及与网络上的其他方面协调变化的成本和时间。最后，我建议定期对防火墙规则进行审计，来确定"已经采用的"配置没有和"设计的"配置分离。在服务和系统从网络上移出的时候会产生孤立和不使用的规则，或者其他的变化也会导致规则的废弃。

（作者：Michael Cobb　　译者：Tina Guo　来源：TechTarget 中国）

采用 IPS 的最佳实践

问：我想要采用 IPS。我应该遵守哪些顶级的最佳实践呢？

答：采用入侵防御系统是个很棘手的问题。这些设备正在迅速成为很多公司安全架构的主要部分。第一次采用会是很恐怖的经历。你不仅是在网络路径中创建潜在的瓶颈和失败点，也是在增加设备，而这个设备可以有意地中断网络流量。这就足够任何网络工程师头疼的了。

下是在企业中配置 IPS 的最佳实践：

- 在“监控”模式下运行 IPS，直到系统已经适当地调整过了。这样的配置行为更像是入侵检测系统，识别潜在问题，但是不阻止网络流量。
- 把“阻止”模式规则的数量限制在最小量，做些细微的调整，减少假阳性阻止德可能性。
- 考虑使用不能打开（fail-open）的设备，限制网络上设备故障的影响。在 IPS 的失误事件中，这就会允许所有的流量继续而不受中断，虽然配置的安全性降低了，但是可以保持网络的状态和运行，而这无疑是网络架构团队会赞赏的。。

（作者：Mike Chapple 译者：Tina Guo 来源：TechTarget 中国）

网络扫描和报告的最佳实践

随着网络应用程序攻击现象越来越普遍，对网址漏洞检查工具的需求正日益增加。手动获取网址并检测常规攻击的时代已经一去不复返了。而自动测试工具得出的报告可以用于检查管理，开发者可以用来指导安全漏洞的修复。

网络扫描已经成为测试路径的一部分，用于捕捉软件开发生命周期中的其它漏洞。并且自从网络安全已经成为支付卡行业数据安全标准（Payment Card Industry Data Security Standard ，PCI DSS）等行业要求的一部分，漏洞扫描不再是毫无实用之处，现在成为一种默认的指令。

本文将讨论使用扫描工具和报告扫描结果的最佳方法，包括扫描的要素、扫描的内容，以及扫描结果的说明。

一个成功的扫描程序应当包含三个要素：定义扫描的范围和目的，选择合适的扫描工具并得出一份可读可用的报告。即使这个网址充满漏洞，你最不想要的是一份几百页无法理解的报告，没有人能读懂或领会。扫描报告的正确表述极为重要，这样开发者就可以在网址进入系统暴露在毫无防御措施的环境中之前采取正确的行动。

网址扫描的必要性

首先，定义扫描的范围和目的。是否应该遵从政府规划或诸如外设组件互连标准（PCI）之类的行业指导，还是确定特殊问题的起因？是否应该对事件或攻击做出回应，还是作为软件开发生命周期的一部分，企业要例行公事地在生存周期内加固站点？

如果扫描是为了遵从法规，那么它的功能仅仅集中在调整要求上。比如，PCI6.5 版要求测试开放网应用程序安全项目(OWASP)列出的十大漏洞。这是一个非常卓越的起始点，它几乎涵盖了网络黑客攻击的绝大部分。

但是，如果测试是公司软件开发生命周期的一个常规部分，运行主要扫描程序不失为一个好主意。理想状态下，企业的扫描要围绕 IT 安全策略。一些策略可能会采用用于高风险交易网址的双因素鉴定技术或 OWASP 没有列出但应该测试的密码策略。

切记：虽然法规遵从受到审计员和调整者的欢迎，但是安全远不止需要核对漏洞列表。

选择一个网址扫描工具

接下来，选择合适的工具。最理想的选择是这样一种工具：易于使用和启动、与网络相兼容、不会降低网络性能（配置较差的扫描工具就会降低网络性能）以及得出可用的报告。扫描工具应该同时能够模拟真正的攻击情景，而不仅仅扫描开发者自己所想象出来的攻击情景。

毕竟，当今网络黑客越来越复杂，从蛮力攻击登录界面到跨站脚本攻击(XSS)，现今已经发展为异步 JavaScript 和 XML（Ajax）攻击与 Web2.0 技术。

市场上一些比较好的工具有：WatchFire Corp 公司的 AppScan，Hewlett-Packard Co.’s SPI Dynamics group 的 WebInspect 7.0，Acunetix Ltd.公司的 Web Vulnerability Scanner Enterprise，以及 Cenzic Inc 公司的 Hailstorm Enterprise Application Risk Controller (ARC)。每一种工具拥有不同的优点和弱点。一些在检测 JavaScript 中的漏洞方面比较突出，一些在防止 SQL 和 XSS 插入攻击方面比较突出，而另一些在 Ajax exploits 方面比较突出。

由于大多数使用 Ajax 和 Web 2.0 的网址都是由多种编程语言编写而成的。如果费用在预算之中的话，使用两种扫描工具并比较其结果不失为一个好方法。除了商业扫描工具，也有一些免费的扫描工具，比如 Nikto、N-Stalker Web Application Scanner 和 Burp Suite。这些工具也可以和商业工具结合使用。比起颇受争议的商业工具而言，尽管没有商业产品的所有功能，但它们更为实用，而且不仅仅只有测试功能。

扫描测试应当在软件测试阶段进行，即开发之后，生产之前。这样在正式应用之前就有时间来鉴定和解决安全漏洞。测试应当在隔离的网段上进行，来阻止扫描工具“攻击”网址以外某个公司的网络。

当然，扫描工具应当在独立环境下运行——不与压力测试、性能测试或者其它测试同时运行，同时不能在高峰时段运行，可以在午夜或者是周末进行。测试者应当可以扫描到未经认可的工作站和服务器，并且通过合适的改变控制程序来记录其在 IT 部门的运行情况。如果一个扫描工具减慢了网速，那么至少网络团队人员会知道原因，并且不会对一个假想的攻击产生恐惧。

此外，不能单单依赖扫描工具。被发现的漏洞都应改经过首动测试。这就意味着测试者应该试图使用基于漏洞的搜索进入网址，但这个漏洞与存储在扫描工具中的版本不同。像 Metasploit 之类的工具箱提供了测试者可以使用的存储搜索。

当新的功能添加到网页上时，仅仅需要重新设定扫描指令。如果你正在配置一个新的带有新代码的网络应用程序，应当对其进行扫描。但是如果市场需要改变标志或网页的颜色，或是在主页中重新安排图形，则无须扫描。这些改变几乎不会将新的漏洞带入网址。

网络扫描报告所包含的内容

最后，在测试过所有网址，并发现漏洞之后，测试者需要得出一份可读的报告。扫描工具得出了报告，但是测试者应当考虑将其翻译为用户习惯的模式。当使用一种以上扫描工具时，不同的扫描工具会产生不同的报告格式；或者使用手动测试的自动扫描时，根本没有报告，因此，得出一份格式统一的单一报告的唯一方法是采用一种用户习惯的模式。

报告应当以执行指令总结开头，该总结包括，没能检测到的五个最为严重的漏洞的表格。并且应当将这些漏洞按严重等级降序排列，同时指定一个风险水平，比如高、中或低。这些等级可以为程序开发者提供行动计划，决定优先修补哪个漏洞，如果风险很低，程序开发者就可以决定先暂不处理，待下一次发布时再进行修补。

另一种实现报告具有可读性的方法是采用一系列彩色图标来代表风险等级。在高风险漏洞旁边的红色骷髅图可以引起人们的注意，即使是那些缺乏技术知识的经理也会留意到。

执行指令总结之后，应当有序地列出所有的漏洞，并附有简单介绍，可能带来的威胁，以及摘录小部分令人厌恶的编码。尽量保持所有漏洞描述在一页纸上。如果开发者需要考虑更多的数据或编码，可以在另一份报告中提供。

网络扫描程序成功的关键在于一处扫描到下一处扫描的连贯性。确保扫描范围、扫描工具和报告与你的行业和 IT 需求一致。改变参数带来的不连贯的后果，会使开发者忙于修补漏洞。此外，这对您的网络安全有害而无益。

（作者：Joel Dubin　译者：李娜娜 来源：TechTarget 中国）

管理 DNS 的最佳实践

问：我们已知的管理 DNS 的最佳实践，有哪些是可以信任的呢？更具体地说，在普通的企业风险排行中，DNS 安全应该处于什么位置？

答：如果 Dan Kaminsky 关于如何破解 DNS 的研究显示了什么内容的话，那就是企业正处于暴露的状态中。但是安全专家需要理解减轻这种风险的做法很少。第一种做法是确保公司的 DNS 服务器采取了资源端口的随机选择。这样并不能完全解决 Kaminsky DNS 攻击，但是它使得大幅减轻这种风险变得更困难（成本更高）。

这也就是说 DNS 服务器必须要打补丁，或者公司应该更新到更强大的服务器架构。其中的一个可能是 DNSSEC，这是没用联邦政府所采用的，但是它相当复杂。

另外重要的是确保所有的上游 ISP 需要协同工作。即使公司的系统是良好的，处理这些危险的名称服务器（name server）的损失也是巨大的。

DNS 安全责任取决于安全团队的操作责任。现在很多安全团队都是影响的受者而不是施与者，这也就是说他们需要和公司的网络团队和作，他们可以实际采用一些修复措施。

（作者：Mike Rothman 译者：Tina Guo 来源：TechTarget 中国）

保护远程访问五个最佳实践

管理对远程访问的保护是一项艰难的工作。因为远程系统可能直接和内网连接，而不是通过企业防火墙，他们对网络环境产生了越来越多的风险。病毒和间谍软件防护，以及普通 VPN 网络策略对于保护这些系统——和他们所连接的网络——的安全是不够的。以下是保护远程访问的五个最佳实践。

1. 软件控制策略

创建一条策略，说明必须和远程访问必须存在的准确的安全软件控制。例如，你可能需要阐明杀毒软件、反间谍软件和桌面防火墙必须安装，并以特定的方式配置最新的特征，以及厂商所都能接受的特征。最佳实践是把策略和连接设置或者终端用户相似的操作指南一起发布。通常灵容忍策略对端点安全来说是最好的。终端用户应该在连接到网络之前满足指导方针。没有杀毒软件、反间谍软件和桌面防火墙？那就不允许远程访问。这条策略还应该说明那些端口和服务可以在系统上显示。

2. 端点安全管理

选择在 VPN 或者远程访问解决方案中提供全面端点安全管理和策略执行的厂商。最好授权所有的远程用户使用企业支持的 VPN 客户端。这是获得真正的策略遵从并确保端点安全状态的唯一方法。你选择的远程访问解决方案应该有能力拒绝连接到布满足策略遵从检查的端点系统。理想的是，这个解决方案应该告诉终端用户那些项目不符合法规，这样他们可以在连接前调整这种状况。这样做可以减少咨询台的呼叫量。

3. 执行企业策略遵从

通知终端用户当连接到企业网络的时候，企业安全策略就会扩展到他们的远程桌面。例如，当连接到企业网络的时候不要使用文件共享和其他不能接受的应用。

4. 报告特征

终端用户的遵从报告非常重要。上面提到的大部分解决方案都提供了报告功能，让管理员了解最快了解连接端点的状态。根据你所管理的用户数量，最好设置闹钟，在明显不符合法规的计算机试图连接的时候给管理严发送邮件。在有些情况下管理员的介入是受到保证的——特别是当存在其他访问网络的方法的时候。

5. 定期检查策略和报告

每几个月，检查一下策略和报告，来识别访问违反的倾向和样式。确保策略和技术控制可以解决远程访问安全需求很重要。如果你发现了访问违反方面的倾向，就要相应地增加或者修改策略。

(作者：George Wrenn 译者：Tina Guo 来源：TechTarget 中国)

酒店网络最佳安全实践

在过去的岁月里，我曾读到过许多有关安全漏洞上的消息，有许多是发生在全球各地的酒店和度假胜地里的名流和商业旅行者身上的。我已看到一些研究和评估正试图估算这种酒店行业的安全形势。许多报告趋向于把这个行业看成是信息安全方面做得最差的行业。但是，该到了让我们每个人都行动起来对这个行业进行关注的时候了。

为了更好地理解酒店行业的安全问题，我们需要认真考虑两个不同的部分：把处理付款，存储客人的个人信息以及组织日常服务作为每天的生意的一部分，另一部分是通过英特网的连通性提供给客人的舒心服务。

典型的酒店网络是由许多不同的私有的系统所组成的，以此来为每位客人提供服务和追踪消费状况。这些系统还提供贯穿酒店或度假胜地的不同部门或领域的连续性的服务。目的是为客人在不同区域里的需求提供一种简单，自然的身份认证和响应流程服务。对客人的身份认证和个人偏爱的响应速度越快，酒店所提供的服务就越人性化；我们都能够对那些认识我们的酒店印象深刻。对这些系统，酒店或度假胜地都有职责进行保护。

国际化的服务酒店为他们的客人提供最贴心的服务，就好象为他们提供了一个室内的温水游泳池：对客人是可用的，但应该遵守某些规则来安全地去享受。但是如果某人自愿通过没有设置安全套接层协议层（SSL）的酒店网络服务来登录他的公司网络邮箱，那么酒店和度假胜地是没有义务承担这一责任风险的。作为客人，我们有义务在使用过程中保护好我们自己的资产和数据。酒店并没有技术人员、救生员或是警察，它仅仅是为我们提供贴心的服务，取决于我们来运用常识使用它们。

如果我们带着一个笔记本电脑入住酒店，我们应该保证它联网前的安全。如果我们在酒店里使用公司的业务电脑，我们需要保证使用之后要清理彻底。这能够包括不要忘记磁盘和闪存驱动以及清理掉留在浏览器上的私人数据。如果我们用无线连接，我们需要保证我们的敏感信息交流上使用了有效的加密技术。酒店提供的服务就如同我们家里的网络服务；通常情况下，这种服务提供的安全系数已被设置为最低级别并且通常需要你自己来添加安全控制来保护你的数据。这取决于我们自己每个人来更新补丁、清除病毒、设置防火墙、防止入侵、保护信息交流并且停止那些可能在我们设备上为外界提供文件访问和服务项的服务。

没有理由或原因来依赖服务提供商来保护我们。这样做会导致在将来发生很多的问题，并且反过来影响我们的工作或是家庭。

现在如果一个酒店经营网络使用和客人相同的网络会导致一些问题。那不仅违反了在信息安全中的普遍最佳实践并且还将违反 PCI 法规和潜在地影响在公众企业遵从 Sarbanes-Oxley。在许多的酒店产业中，客人的英特网服务仅仅在客人的网上可用，并且是完全与酒店经营系统隔离开来的。不幸的是，如今无法确信这种隔离的存在。对这一行业来说这是个通过采用产业标签提供保证——放弃还是证明这两个系统的隔离存在的巨大时机。

简单来说，如果酒店的客人网络或者那个"游泳池"是没有保护服务的完全开放式的，但你又需要使用，那么你就要保证你用自己所有力量来保护你自己。请不要把常识遗忘在家里！

（作者：Rick Lawhorn　　译者：Tang Bo　来源：TechTarget 中国）

应用层防火墙选择与配置的最佳实践

应用层防火墙已经成为那些对法规遵从感兴趣的人们谈论的热点话题。支付卡行业数据安全标准（PCI DSS）原来只推荐应用层防火墙作为最佳实践。该标准将要求公司要么安装这种防火墙，要么进行代码检查。

今天，虽然多数机构多少拥有一些边界防火墙，可以保护网络不受恶意的因特网信息流的攻击，但是这些种类的防火墙并不能保护企业，使其免于受到穿越应用程序的威胁。

据反恶意软件经销商 Sophos plc 和 Symantec Corp.的报告称，最近，应用层防火墙已经出现，它是一种防御 Web 应用攻击的工具。Web 应用程序攻击是一种最常见的入侵类型。传统的网络防火墙不能检测到应用攻击，原因是它们在合法应用程序的开放端口上才能起作用。虽然网络防火墙检查端口和 packet headers，但是，它们并不能核查应用程序和应用程序数据，它们可以在通过开放防火墙端口时，不知不觉地隐藏恶意活动。由于大多数 Web 信息流通过端口 80 或者端口 443，而关闭这些端口是不现实的。

PCI DSS 也已经开始关注应用层防火墙。名声不太好的 Section 6.6 涵盖了 Web 应用程序安全，号召公司对其应用程序进行代码核查，或者使用应用层防火墙，来保护用于处理信用卡的代码。

不幸的是，PCI DSS Section 6.6 将应用程序安全解释为一种非此即彼的命题，但是它远比这个要复杂得多。应用安全不仅仅是关于代码核查或者防火墙；在一些情况下，它可以意味着两者兼而有之。网络安全是关于关闭端口和关闭不必要的服务，应用程序安全与此不同，它是有关保护编码和设计的。

正如任何安全工具或者做法，应用层防火墙应当仅仅被看作是较大规模安全程序的一部分，并不是单一的防御 Web 应用攻击的一种方式。它应当是多层防御的一种。多层防御包括应用漏洞、渗透测试以及个软件开发生命周期中的安全漏洞的代码核查。

选择并配置应用层防火墙

在考虑应用层防火墙时，每个企业应该注意四个因素。我们来分别看一下这些因素，以及现在市场上的一些应用层防火墙。

首先，它真的是应用层防火墙吗？或者仅仅是一种深度信息包检测器？该区别很重要。为了与 PCI 一致，它必须是一个真正的应用层防火墙，而不是一个冒名顶替的工具。

一个真正的应用层防火墙可以检测应用程序的信息流，以防诸如 SQL 注入或者跨站脚本攻击（XSS）之类的恶意代码。当然，这就要求深度信息包检测，但是深度信息包检测仅仅查找信息流中诸如恶意软件和间谍软件之类的攻击，而无法检测到通过应用程序发送的恶意代码。

传统的网络防火墙仅仅可以检测 packet headers，与之不同的是，深度信息包检测可以检测信息包内部及其内容。这虽然绝对可以增强防火墙的能力，但并不能算作一种防止攻击的防御，它仍然有一些局限性。

另一种常见的误解是将应用层防火墙与网络安全网关和内容过滤产品混为一谈。不要因为安装了一个应用层防火墙，就关闭你的 Blue Coat、Vontu 或者 Vericept 系统。这两种产品进行不同的工作。内容过滤产品可以阻止不合适的网站，或者基于 Web 的电子邮件，这些都可能包含恶意软件。但是同样地，它们不能捕获网络应用攻击，有时这仅仅是网站内容的一部分。虽然这两种产品都可以使用 URL 过滤，但是，应用层防火墙可以在 URL 中查找恶意代码：比如 XSS 攻击中使用的 JavaScript；而内容过滤器仅仅在网络地址本身中查找。

尽管如此，网络安全网关、内容过滤产品和应用层防火墙已经慢慢地融合为统一的工具。该发展是自然而然的，因为许多威胁也已经结合起来并且现在需要多层防御。比如，虽然该内容过滤器可能会也可能不会阻止恶意站点，但是应用层防火墙会阻止它所携带的恶意代码。

在最低程度上，应用层防火墙应该防止注入攻击，比如 SQL 注入和 XSS、会话劫持、扫描和检索、cookie 篡改、以及路径遍历（path traversal）企图。应用层防火墙可以核查尖峰或者不规则信息流模式，进而阻止拒绝服务(DoS)攻击，也可以能够处理标准的 HTTP 和 SSL 信息流。

第二，应用层防火墙是否允许通过访问控制的精细保护？访问控制是流程稽核的一大部分。不仅仅是 PCI，SOX 和 HIPAA 都要求全部核查哪些人访问了企业的系统，以及他们都访问了什么。应用层防火墙可以扮演监测这个访问的角色。

在应用层防火墙中搜索的第二个特征是其与身份和访问管理系统的结合能力。这使得防火墙调整到允许员工访问特定的 Web 应用程序，但是不允许公司其他任何人访问。一些员工可能需要访问基于 Web 的电子邮件或 WebEx，来进行其工作。如果防火墙与公司的诸如 Active Directory 或者 LDAP 之类的目录服务结合起来的话，这是可以调整的。访问应用程序可以添加到员工的配置里。

应用层防火墙本身，与其相对的网络防火墙一样，也应该有角色访问，仅允许授权的管理员访问，进行维护和更新。

应用层防火墙的第三个关键的问题是其与公司网络的兼容性。应用层防火墙是另一种可能会拖延网络的设备。如果没有合理配置的话，或者与公司的构架不兼容时，它会导致运行问题。它是否会拖延你的网络，减缓访问者登录你的网址；或者由于它在你的网络上是无形的，它是否就是透明的？

一般说来，应用层防火墙与网络防火墙同时运行，通常是在它们后面的网络内部。入局通信量首先通过网络防火墙，然后再通过应用层防火墙。在考虑完全安装一个产品之前，经常核查防火墙的吞吐量，并且在你的运行环境中对其进行彻底的负载测试。在配置产品之前，任何速度变慢、瓶颈、或者性能问题都应当解决。

最后，就像网络防火墙一样，应用层防火墙应当有能力将信息流记入日志。除了是一种安全最佳方式以外，追踪事件也时很必要的，在一些情况下，法规遵 conh 可能需要这

个功能。记录日志是否有能力追踪事件并对不合适的访问出具报告？PCI 在网络监测方面的要求是非常严格的。这是应用层防火墙功能的核心部分。

应用层防火墙的主要市场来自 Barracuda、Palo Alto Networks、F5 Networks、Breach Security 和 Imperva。其它提供应用层防火墙的厂商还有 Juniper、Fortify 和 SonicWall。

Barracuda Web Site Firewall 宣称自己适用于 Sections 6.5 和 PCI6.6。Section 6.5 要求 Web 应用满足开放 Web 软件安全计划（OWASP）的编码导则。Barracuda Web Site Firewall 代理所有网络信息流，防御通常熟知的 Web 攻击、会话劫持企图和来自所有在线形式的验证输入，以及最为常见的 XSS 攻击。

Palo Alto Networks PA-4000 系列的产品宣称自己是一种以应用程序为中心的防火墙。它可以与策略编辑器协调使用，而策略协调器可以在特定的应用程序中添加一个基于漏洞的防火墙规则。Palo Alto Networks PA-4000 系列产品还拥有 App-IDTM，这是可以实时进行应用程序信息流分析的信息流分类技术。

应用层防火墙，与其它新的安全技术一样，正越来越流行，并被引入到现有的安全产品中。此外，随着应用程序安全越来越重要，它们也越来越受到人们的欢迎。但是应当仔细检查产品，确保正确使用，以保护您的公司免于受到应用攻击。

（作者：Joel Dubin　译者：李娜娜 来源：TechTarget 中国）

网络邮件安全：保护数据的最佳实践

越来越多的企业转向基于网络的电子邮件系统，为用户提供独立平台，进而不论从公共的工作站还是从移动设备都可以进入其电子邮件帐户。然而，由于共享公共的计算设备、用户认证问题以及日益增多的攻击，比如 cookie 窃取和跨站脚本攻击，使得网络邮件给企业带来了极大的安全挑战。

目前的网络邮件结构是由多个保护层组成的，通常包括一个高性能的拥有安全准入技术和加密能力的代理服务器、智能分析工具、以及攻击检测与拦截功能的搭配。这些特点可以独立地与网络邮件系统相结合，或者作为一个综合的网络邮件安全包一起发送。

尽管用户教育是每项安全策略的基础，但尤其重要的是拥有网络邮件用户执行每条规则的技术。通过组合工具可以传送策略，这些工具包括关键信息流咽喉要地的内容过滤器，该过滤器可以阻止恶意软件、间谍软件和垃圾邮件。由于大多数网络钓鱼攻击可以通过如下路径实现：电子邮件、使用网络扫描器和入侵监测系统扫描受感染代码或跨网络的恶意链接，膜通常可以阻止在其到达用户之前阻止这些基于电子邮件的供给。

网络邮件允许信息流通过标准的 HTTP 和 HTTPS 连接，而不是 SMTP，使得网络邮件成为僵尸网络成熟的目标，僵尸网络使用已被攻陷的主机，来加强垃圾邮件或受到病毒感染信息的屏障，然而，合理安置代理器，就可以对信息加码，同时确定并分析网络邮件通信量，减少缓冲器溢流和拒绝服务攻击的机会。

如果无法控制终端，网络邮件系统经理必须担当起确保公开 HTTP 和 HTTPS 的进程时间，或者用户一旦退出登陆网络邮件的应用程序时，就得结束进程。电子邮件证书不是本地缓冲的，这一点也很重要。执行这些控件，进而阻止下一个启动浏览器的人使用后端按钮或历史列表，防止其查看上一个用户的网络邮件页面。

启动带有加密登录和进程功能的网络邮件服务，企业就可以加强其基于浏览器的访问。然而，现在，一些电子邮件客户提供了这样一种能力：通过普通界面进入网络邮件。一定要确定你的网络邮件应用程序有能力对登录和 SMTP 所驱动的进程进行加密，这些都已经由非浏览器界面启动了。

有了网络邮件，攻击者通常使用浏览器脚本来盗窃 cookies、劫持进程、并获得用户的证书。尽管具有代表性的是该由用户来申请安全设备，但是罪犯会使用偷窃来的证书，经常性地验证安全的网站，这样做可以确保好的补丁方法减少罪犯验证的机会。

浏览器的漏洞修补不当，以及越来越多地使用 Javascript、Asynchronous JavaScript、XML (Ajax)、以及其它先进代码，带来了复杂的自动攻击：比如跨站脚本攻击，一个使用恶意链接来盗取信息的黑客策略；以及跨站点请求伪造，一种使用某个用户的身份威胁 Web 服务器的攻击。新种类的威胁已经迫使企业转向了先进的安全工具，比如 Web 应用程序防火墙。该工具使用大量的方法来阻止恶意代码穿过合法的网络通道。WAF 可以在应用层检测所有进入和流出的信息流，检查数据包的有效载荷，并提供比传统的包过滤式防火墙更强大的内容过滤能力。

当然，还没有这样的尚方宝剑，可以通过浏览器界面来保护基于网络的电子邮件访问。然而，通过将一些简单的安全方法结合到现有基础结构中，以及为用户提供关于可能存在的威胁和漏洞方面的信息，企业就能以一种可以处理普通风险的方式来配置网络邮件。

（作者：Sandra Kay Miller 译者：李娜娜 来源：TechTarget 中国）

企业博客开发的最佳实践

问：当创建企业博客的时候应该采用哪些安全最佳实践？

答：这是安全和市场方面的问题。好消息是我也曾在专业的市场部门工作过，可以解决这两个方面。首先，也是最重要的，博客中式最新和最有趣的内容。需要有人负责，并确保至少每周都有几次新内容的更新。这通常是企业市场部的工作。

从安全的角度来说，要考虑三种不同的情况。第一种涉及到博客中泄漏的企业敏感信息。虽然可能是无意的，但是在内容发布前采用检查周期或者批准程序是很好的方法。考虑到博客不能几周在会议上检查一次，以及提供及时相关信息的需要，这就很具有挑战性。

第二种情况涉及到员工发布的不合适信息。这通常发生在个人博客上，但是员工的行为反映了企业是否在工作时间。这就需要为员工设定行为准则，至少，应该在员工个人博客上生命，这些观点只代表个人意见。可以弥补这种不足的最佳实践是在企业博客和个人博客上都详细说明博客的可接受实用策略（AUP）。至于邮件和 Web AUP，在问题出现前管理期望值非常重要。

最后，关注读者的评论。博客的属性是公开的，而且需要热情的回应者不断地匿名回帖。不可避免， 有人会发表不利于公司的言词，你就需要谨慎对待了。

（作者：Mike Rothman 译者：Tina Guo 来源：TechTarget 中国）

应用软件开发最佳实践

问：从安全的角度，你如何看待 Web 应用程序开发中的帐号注销超时设置、缓存以及其他最佳实践的准则？

答：Web 应用程序必须通过建立会话来记录用户的请求，帐号的注销功能是活跃会话管理的一个重要方面。你的应用程序应该为用户提供一种方法途径，例如在每个页面上提供一个退出按钮或是链接，以便让用户退出帐号。另外，在一定时间内没有登录的用户应该被锁定起来，直到再次登录。

这一时间长度应该根据你的用户与 Web 应用的交互方式以及数据的敏感程序来确定。例如，一些银行网站把超时时间定为 10 分钟，其中一个考虑的因素就是它们的用户所访问的都是非常敏感的数据。另外，由于"记住我(Remember Me)"这一选项能使超时设置失效，因此你的程序还应该禁用自动登录以及常连接(keep-alive)功能。

不幸的是，你对应用内容的客户端缓存的控制能力是非常有限的。如果不希望浏览器缓存你的内容，那么你可以通过设置响应报文里的缓存控制指令来影响客户端的缓存操作。如果你不希望浏览器缓存你的网页，把响应头里的 cache-control 设为 no-store 就可以了。这一设置指示浏览器不要存储对它的任何响应或请求。不过，no-cache 和 no-store 是在 HTTP 1.1 里定义的，因此无法被 HTTP 1.0 缓存支持。此外，对于像 PDF 文档和 Excel 表格这样的非 HTML 内容，即使上面这些标签已经被设置了也往往会被缓存。另一点需要引起重视的是，一些浏览器可以存储用户填写的表单数据，这常常不安全。如果你的任何一个 Web 窗口采集敏感信息，那一定加上 AUTOCOMPLETE=FALSE 这一属性来警告浏览器不要保存数据。我之所以用"警告"这个词，是因为这一属性并不在 HTML 规范之内的。如果用户所用的是共享的 PC 机，而且你认为你的程序处于高危险中，那就需要要求用户清空浏览器的缓存和历史记录。

同样重要的是如果用户退出或会话超时，要清空服务端的会话状态，销毁服务器上的会话，还要把浏览器里的会话 cookie 覆盖掉，这是因为浏览器只有在它的线程实际终止了 cookie 之后才会把会话 cookie 删除掉。这样才能确保用户超时或退出后无法发起会话重放式攻击(session replay attack)。此外，URL 里会话 ID 也不应该出现，因为可能会被肩窥

者(shoulder surfer)看到、被浏览器缓存、还会被记录到其它网站的来路链接(referrer)里。理想的情况下，用户的整个会话，包括会话标识符，都应该用 SSL 加密保护，这样才能避免会话 ID 被网络窃听截取。会话 ID 应该是一长串随机生成的复杂数字，而且应该在进行重要处理前，或使用了一定次数或时间后废除并重新生成，特别是改用 SSL 后更应如此。最后，一定要把应用会话管理的目标和实现机制记录下来，放到你的安全策略里。

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

加密密钥管理的一些最佳实践

传输中的数据”密钥管理系统在加密数据“休息”的时候不起作用有两个原因。

第一个原因是传输中的数据加密没有密钥存储的概念。一旦你从一个密钥转移到另一个密钥，旧的密钥就不再需要了。然而，在加密存储的数据时，密钥是正常变化的。旧的密钥必须要保留，否则使用旧的密钥加密的数据就无法读了。第二个原因是如果这个密钥丢失就无法重新建立连接。如果由于损坏或者丢失密钥造成一个虚拟专用网中断，你要做的事情就是重新建立这个连接。然而，如果你丢失了或者损坏了你用来存储一段数据的密钥，那么，那个数据就永远丢失了。这就是好的密钥管理系统必须要跟踪在什么地方使用了什么密钥以及必须要保证没有任何人访问过这些密钥的原因。

目前用来存储加密数据的密钥系统主要有两种类型：单密钥和多密钥系统。单密钥系统使用某种类型的密钥加密数据，简单地拥有这个密钥对于解密数据就全够用了。如果一个黑客获得了那个密钥，他或者她就能够阅读你的加密的数据。这是所有密钥系统中最简单的。

因此，与单密钥系统有关的第一件事情就是创建一个密钥记录，记录系统中使用的密钥以及什么时候使用了这些密钥。这个记录包括当前的密钥和以前创建的目前仍在用来存储数据的磁带的密钥。如果发现一个密钥存在被攻破的可能性，你要立即改变这个密钥并且在密钥记录中登记。

你对单密钥系统做的第二件事情是在存储密钥记录的周围放上你自己的流程。你要尽一切努力保证没有一个单个的人能够访问这个密钥记录。例如，存储密钥记录与你的磁带分开，保证至少必须有两个人在另一个记录中登录才能访问这个密钥记录。

多密钥系统是完全不同的。这些系统使用一套密钥加密数据，使用另一套密钥对管理员进行身份识别。管理员从来不会真正看到用来加密数据的密钥。他们只能看到他们的用

户名和密钥。即使一个管理员能够偷走用来存储加密密钥的数据库，他或者她也不能用这些偷来的密钥阅读你的备份磁带，除非他或者她拥有授权使用这些密钥的系统。

授权系统使用这些密钥的方式每个厂商都不一样。但是，一种方法是使用一种密钥法定人数的概念。这就是要授权一个新的系统，必须要多个人输入用户名和密钥，有时候还需要插入一个物理的密钥卡。完成这个工作之后，这个加密密钥就可以在那个系统上使用了。这种做法可以防止一个恶意的员工窃取你的磁带和加密密钥并且利用这些数据。。

(作者：W. Curtis Preston　来源：TechTarget 中国)

企业实施单点登录的最佳实践

问：我希望在我们银行中配置单点登录（SSO）。这样的配置存在哪些常见的障碍？在企业中、Web 上或者处理系统中配置 SSO 的最佳实践是什么？

答：SSO 开发的最重要的部分是策划。实施 SSO 有很多种选择，这取决于你公司的规模和配置 SSO 的范围。银行还需要考虑法规，例如萨班斯法案（SOX）和 FFIEC。

由于 SSO 开发可能横跨多个不同的系统和平台，你先应该决定哪些系统需要注册。这样的选择应该基于你的员工使用最多的系统，例如邮件或者企业内网，看它是否需要登录。其次，决定适合企业的 IT 结构和基础架构的产品类型。

最大的障碍是计划那些系统因该包括到安装中，以及如何同时把它们和 SSO 技术同步。SSO 只是可以快速完成的简单开发。应该慎重策划，并在企业用户的不同小组中分布实施。

另外重要的一点是确保 SSO 系统和企业现有的 IT 架构向吻合。SSO 可以以硬件或者软件的方式实施。在这种情况下，都是对成员应用的网关认证。换句话说，用户认证到 SSO 网关，然后它就转向，并代表用户进行认证。SSO 系统是应用登录信任状的主数据存储。

软件 SSO 系统由模块组成，通常位于专门的服务器上。这些模块要求一些配置和调整，而在把它们和自己的应用相连接的时候还需要额外的开发努力。这类的产品包括 IBM 的 Tivoli Access Manager、Citrix Password Manager 和 Entrust GetAccess。由于对专门硬件和配置的要求，这些系统通常是用于大型企业。

对于硬件 SSO，要求较少配置的一个产品是 Imprivata 的 OneSign Single Sign On。这种工具在员工应用的简单注册中存在基于 Web 的 front end。Imprivata 是服务于中型

企业以及没有员工或者广泛的软件配置专业技术的企业的。还有，因为它自己的服务器设备齐全，小型公司就不需要在专门的 SSO 上投资了，就像软件 SSO 模块所要求的。

对于 Web Sso 产品，Microsoft Passport Network 允许用户在多个网站访问上只注册一次。在这种情况下，Passport 的作用就相当于在线 SSO 网关。

因为 SSO 可能成为认证失败的单独的一点，SSO 系统的所有的部分都需要在企业内部保护。如果恶意用户获得了 SSO 登录信任状，系统上所有注册的应用都会有风险。

因为 SSO 一个访问的集中点，它可以被用于严密地监控用户访问。萨班斯法案（SOX）等法规要求这样严密的观察。另外，因为 SSO 安装很复杂，他们需要存储大量的认证。这也是审计员和法规执行人员需要查看的资料。

（作者：Joel Dubin 译者：Tina Guo 来源：TechTarget 中国）

安全密码分配的最佳实践

问：我们公司最近发生了一起数据泄露，必须要为很多用户创建新的用户 ID 和密码。在邮件固有的不安全性的条件先，把新 ID 通知用户的最安全的方法是什么？

答：在数据泄露后创建新的用户名不能保证泄露不再发生，而且需要大量的时间和精力；还会产生多种漏洞，例如从旧帐户活动向新帐户导数据。在所有的系统和应用中应该有用户名的标准。我推荐使用员工认证信息，例如姓和名，或者 HP 给每位员工的 ID 号。这对终止程序也会产生简化的效果。

在用户名和密码被窃之后的恰当的回应和安全的分配策略应该是首先禁用可能受到威胁的所有帐户，并以严格的复杂要求重设密码。下一步，使用团队的取证技术来确定（一定要做的）企业的安全控制是如何发生漏洞的。然后把这些发现呈交给管理层，并提交计划来修正这些控制或者采用新的安全控制，减少以后发生的风险。

变更和增加密码的复杂度可以显著降低帐户被黑的可能性，但是只是在已经确定了原来的攻击是如何发生的，并做出了恰当的回应的情况下。

（作者：David Griffeth 译者：Tina Guo 来源：TechTarget 中国）

法规遵从的最佳实践

各种类型和规模的企业面临着来自各方面的规则遵守要求，不论是来自诸如健康保险携带和责任法案（HIPAA）、国家隐私法之类的规则，还是支付卡行业数据安全标准（PCI DSS）。

应对不同的要求，防止其发展为大量的规则的最有效的方法就是建立一个具备持续进程和机制的框架。然后可以调整单个程序，满足特定的规则要求。这里有五种最佳方式，可以帮助企业完成多项规则遵守的目标。

建立信息分类和分级程序。所有规则要求的核心都是信息。对诸如 HIPAA、PCI、和金融服务业现代化法（Gramm-Leach-Bliley）之类的规则所控制的信息需要加以保护，防止泄露和未授权的访问。为了成功地保护信息，企业必须知道信息的存储位置，信息为什么敏感，以及哪些人可以访问。信息分类决定了数据集和分配拥有权。分级确定了并证明了信息为何敏感，以及必须如何处理。这使企业可以确定处理数据的程序（比如，加密），确定了访问控制的进程和机制，并且建立确定需要审计验证规则的信息的范围。

建立风险管理程序。许多规则要求企业正式地进行风险评估和管理，保护的信息和系统。当企业变革时（比如，合并或收购），这一程序需要在高水平和小规模上（比如，当安装新的软件或系统时）应用。拥有基于认证模型的风险评估和管理框架，比如，卡内基？梅隆大学的 OCTAVE 模型，可以帮助组织满足来自多项规则中的要求，并且证明加固（或者减弱）控制是合适的。

开发稳定的身份和访问管理程序。每项规则（和审计人员）要求企业证明它们拥有强大的程序，可以控制哪些人可以访问受保护的信息和系统。虽然这很大程度上似乎是一个技术问题，但是从根本上讲，这是一个进程要求。这些规则趋向于强调对提出访问请求适

当人员的要求以及所有的请求和批准都需要有查帐索引的要求。虽然，身份和访问管理技术有助于这些活动，但是它们取决于你来开发合适的工作流程，并且选择合适的参与者。

开发日志检查程序和机制。所有的规则要求组织保存并监测日志。合理的完成保存和监测工作，日志记录允许公司追踪并证实哪些用户曾经访问过哪些信息，并且提供证据证明这些信息经过了维护，进程依照档案进行，并且适当地采取特定的保护措施（比如，防火墙和杀毒软件）。不幸的是，企业构建并且维持稳定的日志记录方案时面临许多挑战。不同的日志产品，格式不同，同时存储在不同的系统中，此外，还可能包括过少或过多的信息。企业需要分析他们的日志记录需求，对抗复杂的问题，评估事件和市场上的日志管理产品。对多个平台和产品日志格式的最佳理解可以将分布在不同位置的日志结合在一起，而且可以提供强大的分析工具。

存档管理程序。所有的规则要求完全对管理进程进行存档。然而，虽然许多组织认为这个要求是规则遵守包袱，但这项工作的确有意义。企业负担不起由于只有管理员们知道如何完成关键的管理功能而带来的风险状态。这没有任何捷径；关键是对工作存档，然后进行改进。在存档的时候，存在改进所有的程序的诱惑。这是愚蠢的行为。如果你想要实现遵守规则的目的，那么就需要存档，存档，再存档。

（作者：Richard E. Mackey　译者：Tina Guo 来源：TechTarget 中国）

合并过程中制定法规的最佳实践

即使是在最佳的环境中，对于所涉及的双方而言，并购也是痛苦的。对于合并企业而言，它们可能是合乎逻辑的，但是对于 IT 员工而言，试图将两个不相干的系统结合在一起就可以是一场噩梦。特别是对于那些专门负责任何法规制定问题的 IT 安全小组。

如果组合两个 IT 安全的基础设施看起来是项艰巨的任务的话，可想而知，将两家公司不同阶段的制定法规程序合在一起是一项多么艰难的任务。让我们感到欣慰的是，它可能并不像所看起来的那么坏。将法规制定结合起来的两个关键的决定性因素是合作伙伴所从事的行业，以及他们所必需面对的合并特殊法规所规定的具体细节。创建一个统一标准的遵守团队，包括两家公司从事制定法规的员工，这是减缓进程的一种有效方式。

行业内部

通常情况下，一个组织的法规要求是由其所从事的行业决定的。金融公司要求能够满足《萨班斯-奥克斯莱法案》（SOX）和《格雷姆-里奇-比利雷法案》（GLBA）的规定。那些从事健康中心和医疗领域的公司必须得满足《健康保险便利及责任法案》（HIPAA）的标准，发行或者使用信用卡的公司必须满足《支付卡行业数据安全标准》。

显而易见，暂且不谈合并的企业，即使是单个企业也经常会有重叠的现象发生。发行信用卡的银行必须要满足《萨班斯-奥克斯莱法案》（SOX）、《格雷姆-里奇-比利雷法案》（GLBA）和支付卡行业（PCI）数据安全标准的规定。大型的卫生保健公司，如果是公开交易或者是金融组织的一部分，除了需要满足通常的 HIPPAA 要求以外，可能要求满足《萨班斯-奥克斯莱法案》（SOX）标准。

法规的具体问题

关于上面所提到的每一种普遍适用的法规，最关键的问题是考虑访问管理、信息安全策略、客户数据的保护、以及监测与测试。

SOX 的第 404 条是关于影响 IT 安全的规定。这一条要求控制那些可以访问敏感客户和金融数据的 IT 系统。虽然它对于如何实施这些控制是模糊的名单是它基本上查找涵盖访问控制管理、加密、防火墙和恶意保护的文件。此外，适当的位置必须有一个可靠的信息安全策略，以概述这些条款的实施要求。

从合并的角度而言，SOX 审计员和管理者会寻找关于访问管理控制方面的报告。然而，在审计员到达之前，安全专业人士需要询问一些关键问题，以确保两家公司在同一级别的环境中：两家公司使用什么类型的访问管理系统呢？他们是否都使用 Active Directory，还是其中一个使用 LDPA，而另一个使用别的协议？现在，两家公司帐目审计的情况如何？

虽然，GLBA（Gramm-Leach-Bliley 法案）与 SOX 的规定类似，但是它更侧重于保护客户的数据，而非访问控制管理。GLBA 要求对机密数据加密；访问系统时，使用强密码；限制员工访问客户的数据，以及为客户记录的物理安全。在合并的情况下，有了 SOX，安全小组可以对比每家公司的加密方法、客户数据处理程序、以及全面坚持其各自的信息安全策略。策略和程序需要调整为两家公司都适用的共同标准。此外，有了 SOX，所有这些都需要为管理者提供文件证明。

HIPAA 规定了医疗行业公司对患者信息的保护。这里的重点是，与 GLBA 一样，HIPAA 是在保护客户的——在这种情况下，是在保护患者的——信息。在并购中，两家公司不得不对其控制客户信息的记录进行比较，然后为管理者提交一份共同的文件。

SOX、GLB 和 HIPAA 都是由法律支持的政府法规。另一方面，PCI 是由五家最大的信用卡公司组成的联盟支持的行业标准：Visa、 MasterCard、Discover、American Express 和 JCB。PCI 是一项综合的标准，有 12 条要求，囊括了客户数据的保护、加密、网络安全和防火墙、访问管理控制、信息安全策略、以及网络安全的监测和测试。它涵盖了多个领域，这些领域的安全方式各有不同，这就使合并公司成了件令人头疼的事情。

所有有关的数据和访问

即使所有的法规都是针对相同的基本项目——访问控制、客户数据的保护、以及网络安全的监测——确保遵守每一项这些特殊要求。与规定类似的法规并不意味着该法规可以转化为另一条法规。

为了使整个过程更加容易，新收购的公司必须为合并后的组织任命一个人负责法规制定的平衡点。这个人应当来自两个并购伙伴之一，并且能够直接与两家公司制定法规的员工合作，进而实现法规制定的和谐。

（作者：Joel Dubin　译者：李娜娜 来源：TechTarget 中国）

信息安全团队新成员选拔最佳实践

问：我是一名安全经理，最近想要扩充我的安全团队。公司的管理层希望我从内部服务台商提升一些员工。我们很多 IT 专家都有多年的经验，但是不是在安全方面。我应该在候选人身上寻找那些特定的素质或者经验呢？

答：在雇用信息安全专家的时候因该考虑两件重要的事情：能够以安全人员的身分考虑并在精神上能够灵活快速的适应新思想。

我说的像安全人员那样思考意思不是“像黑客一样思考”。尽管在某些特定环境中黑客技巧很有用，但是安全代表的更多。像安全人员一样思考意味着把自己放在各种用户的地位上，并考虑他们的需求是什么。他们如何使用软件？还有他们会怎么有意无意地误用软件？那么这就是寻找解决识别问题的解决方案的事情了。

新员工能够站在业务人员、或者程序员、或者其它任何类型的终端用户的角度思考也非常重要。但是最重要的是，他或者她必须立交，在现实中，安全是在完美的安全性和可用性之间寻找可以接受的妥协。
为了完成这种妥协，现在的团队成员应该能够快速吸收新观点和技术，这样他或者她就可以帮助用户作出明智的风险决定。所以在现实中，我提到的这两个特征其实是同一个。

依我看来，智力比多年的经验重要的多。如果有了正确的心态，那么他或她就可以学习工作中要求的特定的技术或者规则。和这种人工作要比打破墨守成规的人的想法容易的多。

（作者：David Mortman　译者：李娜娜 来源：TechTarget 中国）

信息安全管理的炒作：揭穿最佳实践的谎言

信息安全行业的人对炒作不会陌生。在"最佳实践"的宣传上，尤其如此。这个说法似乎本身就自相矛盾：要定义一个最佳实践，必须先调查足够多的组织，看他们在做些什么，如果足够多的人都在这么做的话，它就被称为最佳实践。但是如果大家都这么做的话，它不就只不过是一般实践了吗？

事实上，最佳实践是每个企业应该要做的， 但实际上，几乎没有能真正做到。就算侥幸有哪家公司在实行最佳实践的做法，他们也大多数只做到了嘴上说的一部分。这不是图谋不轨或是无能为力的问题，而是一个纯粹的商业现实问题。换句话来说：采取最佳安全实践得到的好处对企业来说并不值得。

案例分析：最佳实践（和各种应遵循的法规）说，员工应该每 30-90 天更改自己的密码，公司应该推行强密码规则--每个密码应该包括大小写字母，数字，符号/特殊字符而且最少要 8 个字符。由于上述规定，这是一个越来越多的公司都已经采取了的最佳实践。然而，相比之下只有很少的公司能完全按照这一最佳实践做。用 LDAP 或 Active Directory 架构实现这个可能并不难，但如果要在通过 NIS 进行验证的 UNIX 服务器上实现这个就需要第三方软件了。许多主机环境中也都有类似问题。

再让我们看看端到端加密。理论上来说这是个很了不起的想法。如果所有数据在网络中传输时都是加密过的，那想要窃取就难多了。但是，加密并不是万灵丹。有些人总能够随时攻击应用程序或者存储设施来窃取数据，所以检查这些数据的载体也是很重要的。即便如此，如果端到端加密是个好办法的话，为什么很少有公司这么做呢？为什么尽管域名仅限于存有组织最关键数据的 Web 应用，还是有一些组织采取这种最佳实践呢？这涉及到商业现实，那就是部署端到端加密所需的费用与数据加密提供给组织的感知价值有一种不合适的紧密关系。结果就是，虽然部署从浏览器到 Web 浏览器或负载均衡器的 SSL/TLS 比较便宜，但是加密会延伸到应用程序栈，每一个层次（应用程序服务器、认证服务器、数据库）都要增加一层新的复杂性和花费。

应用服务器和数据库连接尤其如此。再结合它给被动审计造成的不便，部署端到端加密所需的软件、硬件总花费突然就变得有点难以估算了。因此，这种技术可能只是在需要极高安全

性的公司才会部署，或者还有那些吃过教训的公司，比如哈特兰支付系统公司(Heartland Payment Systems)，这些公司知道这种加密在防止数据泄露时多么有价值。

最佳实践往往都是些好的想法，只不过它们往往与周围的商业现实联系不大。因此，无论我们这里安全专家怎么在房顶上大声疾呼这些安全措施是必要的，它们也得不到实施，除非这些最佳实践与商业实践有能够更加一致。

由于有了相关法规来强制实施安全控制，实施某些技术已经变得容易多了。我保证，如果支付卡行业数据安全标准（PCI DSS）的下一个版本会要求端到端加密的话，那么马上将有几千家公司会想办法去实现它，而且厂商还会在这上面进行更多投资研发，以满足他们的这种需要。同时这也要求信息安全专业人员必须认识到，对许多企业来说，并不是每个行业的最佳实践都是正确的（有些甚至是不现实的）。下次再看到有人提供了一系列最佳实践的话，一定要取其精华，去其糟粕。

（作者：David Mortman　译者：Sean 来源：TechTarget 中国）