

中小型企业数据安全的十大威胁

本文摘自 WatchGuard® LiveSecurity® 团队中的信息系统安全认证专业人员 (CISSP) Scott Pinzon 撰写的白皮书《中小型企业数据安全的十大威胁 (及对策)》。本摘要中列出了这十大威胁及相应的一种应对措施。如要详细了解我们如何选出这些威胁、我们处理何种类型的网络, 以及各种威胁对应的至少两种应对措施, 请免费下载此白皮书的完整版副本, 地址是 www.watchguard.com/whitepapers。

如今对于一般企业而言, 很难以事实为依据准确确定真正的网络安全威胁。

自 1999 年以来, WatchGuard LiveSecurity 团队每天都在监控新出现的网络安全威胁, 尤其关注会影响中小型企业 (SMEs) 的各种问题。我们一发现会给中小型企业带来负面影响的问题, 就会通过群发电子邮件来警告我们的服务订购者。由于我们的服务订购者都是时间有限、超负荷工作的 IT 专业人员, 因此我们仅在确信极有可能会发生攻击时才会发出警告。我们的服务着重考虑了企业的实际情况和实用性, 这在业内几乎是独一无二的。而且通过数以万计的服务订购者的反馈、上门服务、焦点组访谈、以及“一边喝啤酒一边讨论网络安全”式的闲谈, 服务得到持续改进。

最终结果是, 根据我们的中小型企业安全分析师的经验, 本白皮书中将列出十大最常见的数据泄密威胁。此外, 我们还列出了各种实用技巧以及如何防御各种威胁。

威胁 10: 内部攻击

Verizon 的入侵反应小组在 4 年内调查了 500 次入侵, 他们认为 18% 的安全缺口来自有恶意的内部人士。在这 18% 之中, 大约有一半来自 IT 人员¹。

贯彻双重控制原则。实施双重控制即表示对于每一种关键资源, 您都有可以仰仗的退路。例如, 您可能会让一名技术人员主要负责配置您的网站和简单邮件传送服务协议 (SMTP) 服务器。不过至少还应有另一个人知道或能获得这些服务器的登录凭证。

威胁 9: 缺少意外应急方案

以“敏捷”和“快速反应”为荣的企业, 为了达到所需的速度, 常常会抛弃标准化操作、成熟的流程及意外应急方案计划。很多中小型企业发现, 在没有业务连续性方案、灾难恢复方案、入侵响应策略、*可用于恢复*的最新备份系统或异地存储的情况下, 一点点数据损坏或漏洞都可能变成一场灾难。

针对缺少规划方案的应对措施

毫无疑问, 如果您有预算, 应该雇一名专家来帮助您开发可靠的信息保障方法。如果您没有足够的资金, 可以使用其他人已完成的杰作并配合自己的企业需要加以修改。SANS (系统管理, 网络和安全) 机构的安全策略项目提供免费模板和其它多种资源, 可帮助您编写自己的策略。要了解更多信息, 请访问 <http://www.sans.org/resources/policies/>。

威胁 8: 配置不当导致泄密

没有经验或资金不足的中小型企业, 在安装路由器、交换机等网络设备时, 通常不会聘请熟知如何确保这些设备安全性的人员。在此情况下, 非专业的网络安装人员只要见到能够成功发送和接收数据流量就非常高兴了。他不会更改厂商的默认用户名和密码等登录凭证。

针对配置选择不当的应对措施

执行一次自动漏洞审查扫描。如果您承担不起雇用顾问的费用, 您或许能承担一次自动网络扫描的费用。市面上有很多很多各种价格的“漏洞管理”产品, 应在日常网络维护工作之中定期使用此类产品。

¹ 见 http://www.infosec.today.com/Articles/2008_Data_Breach_Investigations_Report.htm 上的总结。要获取本报告的 PDF 版本, 请访问 <http://www.verizonbusiness.com/resources/security/databreachreport.pdf>。

威胁 7：鲁莽使用酒店网络和资讯服务站

众所周知，酒店网络里各种病毒、蠕虫、间谍软件和恶意软件泛滥，并且通常没有什么安全措施。而在公众资讯服务站，攻击者很方便即可留下一个键盘记录程序，然后只需等待有人上钩即可。没有安装最新个人防火墙软件、防病毒软件及防间谍软件的笔记本电脑，很容易在路途中遭遇泄密。除非用户严格让笔记本电脑经过网关防火墙且从受信区域内部进行连接，否则传统防御方式可能会不起作用。

针对鲁莽使用酒店网络的应对措施

设定并执行一条政策，强制要求员工不得关闭防御系统。根据一项受 Fiberlink 通信公司委托而展开的调查，四分之一的移动计算机用户承认会更改或禁用其笔记本电脑上的安全设置。您的策略应确保员工在未与您联系并获得您的许可的情况下，绝对不能关闭防御系统。很多流行的防病毒解决方案可以配置为无法关闭，即使用户具有本地管理员权限也是如此；请查看您当前所使用解决方案中的此类功能。

威胁 6：鲁莽使用 Wi-Fi 热点

公共无线热点具备所有与酒店网络一样的风险——再加上以下这些。攻击者通常会提供一个无担保的无线接入点，以传播自己为“免费公共 Wi-Fi”。然后他们等待极欲连接的移动计算机用户进行连接。在启用数据包嗅探器后，攻击者可看到这名员工输入的任何东西，包括登录信息。这种攻击尤其险恶，因为攻击者只是从空气中截取数据，在受害者计算机上几乎没有泄密的痕迹。

针对鲁莽使用 Wi-Fi 的应对措施

教导用户始终选择加密连接让他们通过虚拟专用网（VPN）进行连接。如此操作可加密数据流，即使偷听者采用无线侦听，他们收到的也只是无用数据。

威胁 5：丢失便携设备内的数据

每年都有大量敏感数据因员工意外将智能电话遗落在出租车内、将 USB 随身碟遗落在酒店房间或将笔记本电脑遗落在通勤火车上等情况而泄漏。当数据存储于小型设备中时，管理员明智的做法是停止考虑“如果设备丢失该怎么做……”，转为考虑“当设备丢失时该怎么做……”。

针对丢失便携设备内的数据的应对措施

集中管理移动设备。考虑投资于可集中管理移动设备的服务器和软件。RIM 公司的 Blackberry 企业级服务器可帮助您确保传输都是经过加密的；而且如果有员工通知您手机丢失，您可远程删除丢失的 Blackberry 智能手机上的数据。此类措施可最大程度地减少因设备丢失带来的负面影响。

威胁 4：Web 服务器泄密

如今最常见的僵尸网络攻击是针对网站的；而大多数网站的致命缺陷是编写质量不佳的自定义应用程序代码。攻击者通过一次自动化 SQL 注入攻击，就可攻陷数十万计的服务器，导致各合法网站执行恶意软件，在不知不觉中扩展僵尸操控者的帝国。

针对 web 服务器泄密的应对措施

审查网络应用程序代码。如果（举例而言）网页表单中有一个供访问者提交电话号码的字段，则 web 应用程序应摒弃多余的字符。如果 web 应用程序不知道该如何处理某些数据或命令，应予以拒绝，而不是进行处理。采用您负担得起的最佳代码审查解决方案（无论是一个专家团队还是一种自动化工具），重点是确认代码是否能够正确执行输入验证。

威胁 3：员工擅自浏览网络

2006 年华盛顿大学的一项研究发现，传播间谍软件最多的站点依次为：

1. 名人粉丝网站（比如提供 Paris Hilton 和 Britney Spears 最新蠢行之类的网站）；
2. 休闲游戏网站（在这里您可以与陌生人下棋）；
3. 色情网站（排在惊人的第三位）。

MySpace 和 Facebook 等社交网站中的垃圾邮件、木马和间谍软件泛滥，已居各类网站之最。员工如果浏览与业务无关的网站，最终会把僵尸网络客户端、木马、间谍软件、键盘记录程序、垃圾邮件程序等各种恶意软件带入公司网络。

针对擅自浏览网络的应对措施

实施网页内容过滤。使用 WatchGuard 的 WebBlocker 之类的网页过滤软件。网页过滤解决方案维护多种类别的拦截网址的数据库（每日更新）。类别越多，就表示细微差别越多。此类工具有助于以技术实现可接受使用策略。

威胁 2：恶意 HTML 电子邮件

目前最常见的电子邮件攻击形式，是通过 HTML 电子邮件链接内含陷阱的恶意站点。一次错误点击就可能引发推动式（drive-by）下载。其危害与威胁 3“擅自浏览网络”相同；不过这次攻击者是使用电子邮件来诱使受害者访问恶意网站。

针对恶意 HTML 电子邮件的应对措施

实施对外 web 代理。可对区域网（LAN）进行设置，将所有 HTTP 请求和应答都重定向到 Web 代理服务器上，该服务器将提供一个中转点，监控所有 Web 流量是否恰当。Web 代理不会捕获流入的恶意电子邮件，不过如果网络用户点击恶意 HTML 电子邮件中的链接，Web 代理就会捕获此时生成的 HTTP 请求。只要用户的 HTTP 请求没有进入攻击者的陷阱网站，用户就不会受到危害。

威胁 1：针对已知漏洞的自动入侵

Verizon 的《2008 数据失窃调查报告》中，汇编了从 4 年多的时间内发生的 500 多次数据失窃中获取的证据。Verizon 的风险小组发现，73% 的数据失窃是从外部来源处发生的。粗心大意的中小型企业如果在 Windows 补丁公布当月不进行安装，就会受到危害。不过网络中除微软的产品外还包括其它产品。因此应将定期打补丁的工作扩展为针对网络上的所有应用和操作系统组件进行。

针对自动入侵的应对措施

投资于补丁管理。补丁管理软件可帮助您扫描网络、确认缺少的补丁和软件更新、以及从中央控制台分发补丁，可极大程度地确保整个网络时刻保持最新。

构建费用低廉的测试网络。即使知名公司也可能会有疏忽。因此，在将补丁部署到整个网络之前，我们建议先将其安装到一个测试系统上，查看该补丁的运行。如果您目前没有测试网络，那么下一次您更换旧台式机和服务器时，可将其留下来，专门用于构建测试网络。

结论

以上我们所建议的各项应对措施，可大大提升您规避风险及保护网络的能力。不过这只是一个勤奋的 IT 管理员可以实施的例子之一，还有多种措施可用于提升网络安全性。如要获取更多增强网络、避免发生各种常见问题的实用建议，请从 [WatchGuard 网站](#) 免费下载完整版的《中小型企业十大安全威胁（及对策）》白皮书。

WatchGuard® 提供的扩展威胁管理（XTM）网关安全设备，可防御本文中列出的十种威胁中的九种。（很遗憾，我们的设备不能阻止您的员工丢失便携设备。）我们可帮助您保护无线网络的安全、检查请求访问网络的客户端的完整性、过滤垃圾邮件、代理 web 服务、尽可能减少内部威胁、创建 VPN 虚拟专用网连接等。

如欲详细了解 WatchGuard 安全解决方案及其对僵尸网络和其它网络威胁的防御措施，请访问 www.watchguard.com 或与经销商联系。