威胁评估与防御战略

威胁评估与防御战略

在过去几年中，恶意软件在五个领域发生了重大变化：僵尸网络、流氓安全软件、普通间谍软件、定向恶意软件领域、以及对手机和智能手机的攻击。反过来说，攻击者能够在这些领域实施攻击（发现新的漏洞并获取相关权限）正说明这些领域存在着相关的缺陷。在信息安全领域中几乎没有亘古不变的真理，但来自恶意软件的威胁会不停地进化却是安全界的永恒话题。

安全威胁现状评估

网络的日新月异在给我们带来众多资源的同时也给我们的安全问题带来了各种各样的威胁。如今，各种黑客攻击技术层出不穷，网络战的硝烟愈演愈烈；一直处于抽象状态的虚拟化威胁也开始崭露头角……

- 虚拟环境的安全威胁已由理论变为现实
- 网络战是企业的真正威胁吗？
- 恶意软件：不断进化的威胁
- USB会威胁到内置移动设备的安全吗？
- 信息安全威胁评估之物理安全威胁

威胁防御战略

安全威胁在每个行业都有所不同。但是，无论你在金融服务、制造业、教育、政府部门还是健康医疗行业工作，某些有效的防御战略总能够帮助你阻止安全威胁使你的业务陷入瘫痪。

- 2010 年安全威胁预测及防御战略

- 了解社会工程黑客攻击策略和威胁
- 应对不同行业安全威胁的最佳做法
- 网络安全：如何避免物理安全威胁
- 企业UTM安全：最好的威胁管理解决方案？

防御新型安全威胁

如今，许多公司热衷于新型的网络设备和媒介：使工作人员能在掌上电脑（PDAs）或者智能手机这类的无线手持设备上处理商业数据，或通过 Twitter 等社交网站来发布重要信息。在理想的情况下，所有的这些设备都是值得信赖的，并且不受恶意软件的干扰。可现实的情况是，许多设备都处于无人管理也没有安全保障的状态。企业如何才能在这些问题泛滥前，将潜在的威胁遏制在萌芽状态呢？

- 保护企业网络 防御新型移动应用程序下载的威胁
- 智能手机移动设备面临的安全威胁及应对策略
- 企业如何制定Twitter策略　防止来自社交网络的威胁

虚拟环境的安全威胁已由理论变为现实

从虚拟机中逃逸，一直以来被看作类似于一种黑色操作。你不断的能听到研究人员们研究一些恶意软件样本的传言，而这些恶意软件可以从虚拟客户机逃逸到主机里。与此同时，其他研究人员也在研究一些允许攻击者从虚拟机中逃逸的漏洞。

这些有形的攻击威胁到了虚拟化项目的神圣性，而虚拟化在许多公司里相当流行，因为在服务器整合和功耗方面，它们具有很大的优势。但漏洞利用工具的数量也正在日益高涨，每一个月都会增加不少。

在 2009 年 7 月下旬的美国黑帽大会上，一些研究机构对虚拟机的这一漏洞提出了最为清楚的阐释。Immunity 是一家安全评估和渗透测试的公司，它向外界提供了一个被称为 Cloudburst 的工具软件的详细信息，该工具由高级安全研究员 Kostya Kortchinsky 开发。Cloudburst 目前能提供给装有 Immunity 的 CANVAS 测试工具的用户使用，它利用的是 VMware Workstation 6.5.1 和更早期版本的显示功能 bug，而这一 bug 同样出现在 VMware Player、服务器、Fusion、ESXi 和 ESX［见 CVE 2009-1244，以得到确切版本编号］。

Kortchinsky 在 Cloudburst 的开发中有一些创新的思维，他选择利用的是虚拟机和一些设备的依赖关系（如视频适配器、软盘控制器、IDE 控制器、键盘控制器和网络适配器），从而获得对主机的访问。在黑帽大会上，他向外界做了一次报告，解释了他如何利用 VMware 模拟视频设备的漏洞来进行攻击，他还演示了如何利用主机泄漏到客户机的内存，以及如何从客户机向主机内存中的任何位置写入任意数据。

“视频适配器处理最复杂的数据，”他说到。 “它有一个特别巨大的共享内存。”

Kortchinsky 说，相同的代码模拟每个 VMware 产品上的设备。 “如果有一个漏洞存在，那么每一个 VMware 的产品上都存在该漏洞，而且通过 I / O 端口或内存映射 I / O 端口可以从客户机上对其进行访问”。 Immunity 表示，Cloudburst 具有可以破坏

（corrupt）内存的能力，这允许它以隧道方式在客户机帧缓冲区（frame buffer）之上建立起与主机的 MOSDEF 连接，从而与主机进行通信。MOSDEF 是 CANVAS 工具集里的漏洞利用工具，它由 Immunity 公司创始人 Dave Aitel 开发。

在今年 4 月 10 日，VMware 已经修补了这些版本的漏洞。4 天之后，Cloudburst 发布，并被加入到 CANVAS 工具集中。而正是这一点使得 Cloudburst 与众不同，它不再是一个漏洞验证性触发代码（proof of concept），这和大多数虚拟机恶意软件不同。

文章写到这里，该安全问题技术部分的内容已经结束了，但作为一个具有购买权力和负责决策的安全经理来说，它对于你意味着什么呢？在两年前经济还没有衰退的时候，这一问题给我们的启示会更多，你会争辩说企业的支出应更多的考虑安全因素，而不是经济因素。因为安全问题可能会影响企业的 IT 环境，而这种影响是可以切身感受到的。

虚拟化的威胁一直是抽象的，理论多于实践。当然，目前还存在着一些不易察觉的、虚拟的 rootkit 技术（如 Blue Pill），但这要求黑客具有对技术的理解天赋，而把一些非常复杂的东西作为攻击的工具对黑客来说似乎是不可行的。专家同时警告说，虚拟环境里有形的威胁已经出现，但对于这些理论性的东西，你仍然不可能制定企业自身战略并购买相应的虚拟化产品。你很可能需要做的就是，跟上虚拟化的趋势，因为它能带来很大的好处，让用户垂涎欲滴。而它的安全性问题将来也会随之来临。

不过，是在未来。

针对虚拟机的攻击已从理论慢慢的变成现实。目前，已经出现了关于虚拟机逃逸的五个 CVE 警报，在 Kortchinsky、iDefense 公司的 Greg McManus 以及 Core Security 公司研究小组工作的基础上，研究人员和其他的攻击者会继续对这一问题进行分析、研究，因此以后出现更多安全漏洞几乎是必然的事情。

专家说，网络不应该依赖传统的安全措施，因为它们不能抵御每个虚拟机的威胁。到目前为止，大多数组织都在反应有关虚拟环境的安全问题，以及不断涌现的新攻击、漏洞

利用程序和漏洞验证性触发代码（proof of concept）。虚拟机的安全正处于风口浪尖的境地。

两年前，安全专家、现任思科云和虚拟化解决方案的总监 Chris Hoff 曾说过：“虚拟化的安全威胁和漏洞晦涩难懂，而企业管理层对这些安全问题表现消极，他们认为在部署虚拟化技术的时候，安全问题不是考虑的重点。所以，即使尝试通过建立商业案例来考虑针对安全虚拟化环境的投资，这些努力也起不到多大的作用。”

随着 Cloudburst 被看作最近一次针对虚拟机的攻击，在这一背景下，Hoff 以及其他致力于虚拟环境安全的专家的预言似乎得到了验证。

所以，也是在两年前，Hoff 写了一篇关于某虚拟机漏洞的文章。在当时，攻击者利用该漏洞可以在 VMware 客户端操作系统上运行任意代码。在那篇文章中，他的最后一句话是：“这将是针对虚拟机的第一次攻击，以后还会出现更多，这是可以肯定的... 在你必须去重新配置或为你的全球虚拟数据中心（server farms）打补丁之前...你可以开始用这样的例子与管理层讨论进行冷静、理性的讨论...“

未来已经来临。

（作者：Michael S. Mimoso 译者：Sean 来源：TechTarget中国）

网络战是企业的真正威胁吗？

7 月初，出现了不少关于“大规模网络攻击”的报道，这些新闻说有来自朝鲜，目标是韩国和美国的一些重要网站。据报道，这些攻击是由分布在全球各地的“数万台”受感染的计算机发起的，它们被用来发动分布式拒绝服务（DDoS）攻击。被感染的系统本来要自毁（大概还想与全世界同归于尽）。

大多数安全爱好者都不解，为什么这么一次规模不大，动机不复杂，造成的破坏也不大的僵尸网络攻击会上华尔街日报的头版呢。一些面向大众的政府网络变得很慢或者有几天无法访问，但是并没有经济损失或者严重的服务中断的报告。

所有的这些炒作都是为了什么？网络战真的是企业信息安全专业人士应该关注的内容吗？

上个月发起这次攻击的僵尸网络还算是不太过分的，但是网络战（或网络事故）的潜在危害是巨大的--不是因为敌人有多么高超，而是因为我们自己的基础设施很薄弱，维护也不到位。在美国，关键的基础设施对 IT 的依赖已经超出了大多数人的认识。摩天大楼的加热，制冷和准入系统都可以通过互联网控制。医院通过 VoIP 电话联系心脏移植。这些只是两个例子，但是还有许多其它例子能说明一起有预谋，有针对性的攻击真的能造成大规模的混乱，甚至造成生命损失。
网络战只不过是一个更宏大的问题的小部分：我们需要设计出一个稳定的，全球性的 IT 基础设施。莽撞无知的青少年肆无忌惮地对互联网造成过无数次严重的破坏。例如 1986 年，Morris 蠕虫造成了比这回炒作的 DDoS 攻击还严重的破坏，它感染了数千台重要的 Unix 服务器。我们最大的问题不在于有人图谋不轨，而在于 Morris 蠕虫都过去了 2 3 年了， 我们的网络基础架构还是和积木塔一样。

即使是纯粹偶然的网络中断，也对关键的基础设施造成了重大损害。早在 2002 年，贝斯以色列女执事医疗中心的网络遭到洪泛攻击，陷入瘫痪，起因仅仅是一个偶然的生成树一路(spanning tree loop)。突然之间，医生和实验室技术人员无法在网络上查看病历和实验室结果，或是填写处方。最终，急诊室只好关门，病人转送到其他医院。

如果有人真的试图通过因特网破坏某些关键系统的话，会发生什么呢？

在去年的 SourceBoston 安全会议上，安全研究人员 Dan Geer 调查了用 2001 年的 Nimda 病毒可以造成些什么破坏 。2001 年，就在 9 月 11 日之后几天，Nimda 通过五种媒介传染到整个网络，第一天就感染了几十万台计算机。还有一种名叫 E911 的老病毒，它会让被感染的系统不断通过调制解调器拨打 911。Geer 评论说，如果病毒作者在代码里加进那个功能的话，美国人“9 月 19 号早上起来发现全国所有的紧急服务全部失效了，它被一次性全部关闭，就像电灯开关一样。那天可正是整个美国还惊魂未定的时候。

如何抵御网络攻击和网络事故

预知网络中的下一个危机很难，但是这里有一些最佳实践能让企业安全团队避免成为受害者。

1. **防患于未然。**把你们组织的信息流绘制出来。了解哪些系统/服务具需要关键的网络功能。很多情况下，没有网络后公司根本无法运作。我们没有纸笔或是员工培训来人工处理我们的信息。制定网络中断后的短期（即 1 小时）、中期（即 24 小时）和长期（即多天）后备计划。如果有可能的话，对其进行验证。要现实一点，看到会有哪些限制，规划可行的东西。
   鉴于目前的经济不景气，许多企业可能都没有资源投入到灾害规划上。但正如我的母亲所说，只求尽力而为。
2. **维护系统。** 对所有设备例行打补丁，包括服务器，工作站和网络设备。还一定要包括第三方应用程序。还要定期审计。集中收集日志。即使你没有时间做灾难恢复，那也至少要维护好你的系统。不要成为黑客眼中好。
3. **共享信息。** 这听起来似乎有悖常理，但我们大家都是唇齿相依的。如果在某个行业里的每个人都发现了相同的探测或是异常活动，那就可以让我们确定攻击的前导，从而避免重大的灾难。分享关于有效和无效的防御技术的信息也可以帮助我们更有效地作出反应。
4. **做一个好邻居。** 不要忽略非关键系统。即使角落里的那台 Windows 上“没什么重要的东西“，你也肯定不希望有感染它并利用它来攻击其它主机。
5. **要大惊小怪。**那些对一起又一起网络攻击的报道造成了不必要的恐慌。害得大家现在觉得，一个并不复杂的僵尸网络就可以造成全球性的恐惧，甚至还可能影响国际关系，这实际又是对那些攻击者的鼓励。我们都有自己的安全问题，网络战肯定是其中之一。但是，如果我们都能保持冷静，攻击者就又少了一个发起网络攻击的理由。

对“网络战”威胁的宣传已经太言过其实，但我们有理由担心：我们的国家基础设施是一个烂摊子。事故造成了和“网络战”或其他恶意袭击一样大的损害。“战争”不是问题所在，管理不善、混乱和恐惧，才是真正的威胁。

(作者：Sherri Davidoff　译者：Sean 来源：TechTarget中国)

恶意软件：不断进化的威胁

恶意的软件，也就是我们通常所说的恶意软件（malware）是一种动态种类的威胁。这种技术可以被用于破坏数据、中断服务、窃取信息，并进化到可以适应安全实践和对策的变化。例如，杀毒软件的应对措施可以通过在病毒的二进制代码中搜索样式可以检测到很多病毒和蠕虫，但是不能在其他程序中搜索。这些样式本质上都是数字指纹，是用于识别威胁软件的。在回应中，病毒撰写者开发了秘密行动技术来给恶意代码戴上面具。（如下图）

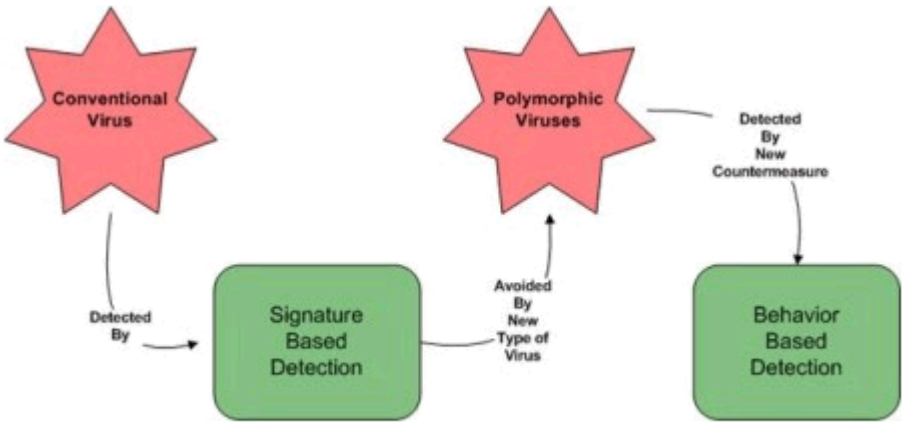

图1 恶意软件和应对措施在较量中的变化

今天的病毒比以前的病毒更加复杂了，而之前的恶意软件还可以引起 IT 用户的注意。他们还只是信息资产目前所面对的多种恶意软件之一。其他形式的恶意软件包括

- 蠕虫——利用操作系统、网络服务和应用中的漏洞来扩散并产生破坏。
- 击键记录器——捕获击键动作，并传送给攻击者
- 视频采集系统——复制电脑屏幕上显示的内容，并传送给攻击者
- Rootkits—隐藏自己和其他恶意软件的本来面目
- 特洛伊木马——看起来合法，但是实际包含击键记录器和间谍软件等恶意软件

所开发的用于检测病毒的应对措施通常也可以检测到其他形式的恶意软件。在客户短设备上配置杀毒程序，并在网络流量进入网络的时候进行扫描都是应对恶意软件的恰当的措施。另

外，锁定客户设备——例如，禁用大部分用户安装软件或者更新 Windows 注册表的权限——可以防止恶意软件的安装，而这些恶意软件可以设法逃避检测。

另一种有效的，但是很容易被忽略的应对措施是安全意识培训。现在，大家都知道不能打开你不了解的人发送来的邮件附件。不太普及的技巧有避免使用可能含有恶意软件的网站，例如对等文件共享网站，不要下载浏览器插件，他们可能是木马。技术上的应对对于保护信息资产非常重要，而让用户了解恶意软件开发人员和网络攻击者所使用的变化多端的诡计和技术是对技术方面的应对措施的有效补充。

（作者：Dan Sullivan　译者：Tina Guo 来源：TechTarget中国）

USB会威胁到内置移动设备的安全吗？

问：使用 USB 会威胁到内置设备的安全性吗？特别是当这些设备是通过 USB 和电脑主机连接的时候，通过使用在电脑主机上运行的应用，这些设备会被入侵吗？

答：确实可以。看一下 USB 设备是如何连接到电脑的，你就明白为什么了。通用串行总线（Universal Serial Bus），也就是通常所说的 USB，它是用于把设备连接到电脑主机上的串行总线标准。一条总线就是在电脑之间或者电脑组件只见个传送数据的一个子系统。最为一个串行总线，USB 一次发送一位的数据。它的创建是为了改善越来越多的想连接到电脑上的即插即用功能。

在刚使用个人电脑的时候，连接新设备是麻烦的事情。那时必须要设置传输器、增加额外的总线或者并口，安装设备驱动并重启，可能是多次。现在有了 USB 这种单一的标准界面接口，这些日子就过去了。USB 设备可以在不需重启电脑或者关闭设备的情况下连接或者断开。当然，它就被广泛地用于连接接口，根据 2008 年的 USB 使用者论坛（USB Implementers Forum）称，目前全球有 20 亿有线 USB 设备。但是，USB 只是连接到电脑主机的接口设备标准。它并不提供任何安全功能来过滤通过连接的数据。在这一方面，这和以太网或者打印机电缆相同；任何通过 USB 连接连到电脑的设备都可以被在电脑上运行的应用访问。所以，假如，如果电脑被恶意软件感染了，这些恶意软件就可以访问通过 USB 线连接到电脑的便携式硬盘上的数据。危险也可以发生在相反的情况，带有自动运行的应用（包括恶意软件）的 U3 USB 设备连接到一台电脑，然后就可以防火电脑主机上的数据或者记录电脑键盘上的所有字符。

为了减轻这种风险，你可以禁用电脑上的所有 USB 端口，但是这不太现实，因为这些端口可能被键盘或者鼠标等设备所使用。如果企业运行的是 Windows 的网络，就可以通过使用 Active Directory 控制 USB 设备。不需要使用 USN 设备的个人和团队，就可以通过 Active Directory 组策略，禁止访问 ubstor.pnf 和 ubstor.inf 文件。在 Windows Vista 中，管理员可以允许用户只安装在同意列表上的设备，或者禁止可移动或者使用可移动媒体读写访问设备。还有一些第三方程序可以提供 USB 设备的访问控制范围。

可喜地是我们看到的 USB 还只是把设备连接到电脑的方法，而不是控制设备行为的方式。为了保护 USB 设备，你可能需要一些安全措施，当然，这些措施可以被涵盖的策略支持，并可以清楚地和 USB 设备的恰当使用交流。

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

信息安全威胁评估之物理安全威胁

电子防御，特别是边界防御，可以在攻击者获得 IT 资源的物理访问的情况下被颠覆 。如果攻击者可以接近办公室，他就可以：

- 安装硬件按键记录器来捕获按键， 包括用户名和密码
- 假装成包裹发动服务的司机，并获得备份磁带和磁盘。
- 让办公室员工使用社会工程，学习安全程序、办公策略和办公室中的高级管理人员和经济的名字。
- 使用欺诈设备防火安全防护不够好的无线网络

这些手段的任何一种都不能攻击系统或者造成泄漏，但是他们可以像想要访问的攻击者提供这些安全谜题的提示。物理访问控制，监视和安全意识培训都是对这种类型攻击的应对措施。

从越来越复杂的恶意软件到社会工程，再到物理安全，有很多方法让受害者收到信息安全攻击。面对大量的应对措施，当问题出现时，应该如何选择呢？请看下一节：应对措施成本和收益的平衡。

(作者：Dan Sullivan 译者：Tina Guo 来源：TechTarget中国)

2010年安全威胁预测及防御战略

在过去几年中，恶意软件在五个领域发生了重大变化：僵尸网络、流氓安全软件、普通间谍软件、定向恶意软件领域、以及对手机和智能手机的攻击。反过来说，攻击者能够在这些领域实施攻击（发现新的漏洞并获取相关权限）正说明这些领域存在着相关的缺陷。最近几年中，恶意软件找到了更好的办法使自己安全地潜伏在新侵入的宿主机中，并使得恶意软件与攻击者间能够更顺利的进行通信，进而窃取受害者的各种重要资料。

绝大多数安全攻击正变得越来越有威胁，有些攻击技术还可能在2010年进行重大的改进。比如说，仅仅是以当前恶意软件所控制的僵尸网络来衡量，明年的情况将会变得更糟。由于恶意代码变得更易于使用，攻击者可能已经有能力将恶意代码装备成自己可以完全控制的应用程序、改进的攻击工具包、以及升级版的侵入工具，从而实施零日攻击和可定制的攻击。安全的前景似乎很悲观，企业安全专家也会发现这些问题难以排出。然而，明年也会出现更新的工具和手段来保护企业的网络和数据。

预测：2010年的安全威胁及防御策略

在信息安全领域中几乎没有亘古不变的真理，但“恶意软件（及来自它的威胁）会不停的进步”却是不变的神话。为了对抗不断更新的恶意软件和僵尸网络，企业可以将多种优秀预防策略结合起来，如对员工安全意识的培训、制定安全策略、采用安全程序，以及两种新兴技术：“白名单制度”和“基于云计算的反恶意软件技术”。接下来，我们将大致介绍这两种技术：

1.随着很多企业已对白名单制度就“功能性”及“如何使用才能更有效的保障企业的安全环境”等方面进行评估，这一技术将会在企业领域中不断发展。白名单制度将会对那些运行在系统中的可执行文件进行定义，其他所有未出现在这张可接受行为名单中的可执行文件都会被强制终止运行。

在过去两年中，白名单制度发生了重大改进。最初，该技术产品是一个相当复杂的系统，它要求企业对每一个可执行文件都进行定义。现在，基于白名单开发的产品已经携带有初始安全模板，用户可根据自己的需求添加新的安全步骤，并能对全部过程进行管理。企业将会逐渐意识到仅仅依赖杀毒软件的防护是不可靠的，一套全新的防御方案才是解决

问题的关键。2010 年中，更多的企业将会启用并建立自己的白名单和黑名单制度，以取代他们当前的反恶意软件策略，再制定策略以明确对那些在两个名单中都不存在的可执行文件应该采取什么措施。

2. 基于云计算的反恶意软件策略将会用在企业中，以解决白名单制度中的未知软件问题。基于云计算的反恶意软件策略可以将被测程序与中心数据库进行比对，从而判定其到底是不是恶意软件。由于签名技术是针对软件供应商及其用户的需求而开发出来的，因此中心数据库中将会保留更多的数字签名，其更新速度将比传统反病毒签名更快。然而，实时监测需要对连入数据库进行网络认证，并对执行过程进行优化。中心数据库的地址还将被用来对恶意文件的传播进行跟踪，同时又需保障用户的隐私。与 PC 领域类似的防御策略也将在智能手机领域继续发展并逐渐成熟。

另一个值得关注的易被攻击的领域是手机和无线设备。针对智能手机的攻击和恶意软件主要是利用手机中的蓝牙功能和 IP 连接中的问题。但到目前为止，它们还未表现出太强的攻击性。手机和智能手机平台上的攻击以后将会继续成为头条新闻，但由于这些设备的复杂性和多样性，跨平台的广泛攻击还不太可能。不过，这些领域的攻击技术也在不断更新，比如说最近的 iPhone SSH 默认密码蠕虫，以及最近 Android 平台上出现的可盗窃银行登录信息的恶意软件。这些威胁已经超出了低风险等级的范畴。

随着越来越多的商业活动在手机平台上进行，这些设备将会更频繁的受到攻击，尤其是那些任何人均可进行开发和修改的开源程序。尽管反恶意软件程序可以像保护个人电脑一样保护智能手机，但这需要用户对应用程序的传播采取更强的安全控制手段，例如只允许已做了标记的应用程序才能运行，或在对程序进行标记时设置更多的限制。

在 2010 年中，软件检测和防御领域中的一些共同缺陷并不会有太大的改善。用户和企业将会开始加快更新他们操作系统的速度以减弱安全威胁。老旧操作系统上的威胁依旧存在，虽然新系统已经为这些漏洞打上了补丁，但攻击者必然会发现新的方法对新系统进行攻击。在新的一年中，来自恶意软件和其他安全领域的威胁依然会不断恶化，因为犯罪分子已经看中了这其中所关联的巨大经济利益。

企业的信息安全专家们不仅需要通过利用当前的资源、技术和上文中提到的安全策略来减少潜在安全威胁，还要紧密跟踪这些威胁在未来一年中的发展动向。这是因为，即使攻击者在上述各领域中进行细微的改进，企业的安全防御也会遭受巨大的威胁。

(作者：Nick Lewis　译者：Sean 来源：TechTarget中国)

了解社会工程黑客攻击策略和威胁

你已经安装了两个防火墙，一个入侵防御系统（IPS）并配置了杀毒软件，因此对企业整个的网络安全状况感觉良好。服务器打过补丁了、信息数据包也处理过了，而且当网络流量出现异常的时候你会收到警报，并当场杀毒。耶！生活太美好了。那么问题出在哪儿呢？

黑客很聪明，而且在从毫不怀疑的员工身上获取信息的时候通常都很狡猾。你的服务台、IT 员工和普通的用户关心的是对需要帮助的人伸出援手并安抚他们。不管你的员工付出了多大的代价，它们都不能想防火墙处理数据包一样处理电话。实际上，大部分人都想在看似无辜的人需要帮助的时候伸出援助之手。

社会工程是黑客可以取得更多成绩的策略，这样必识别或者绕过防火墙和 IPS 用的时间要少很多。幸运还是不幸都依赖于你问的人是谁，安全管理员不可能屏蔽每个人的电话或者询问进入公司的每个人的 ID。你的员工，特别是那些非结构化的员工应过滤恶意请求，阻止它们通过大门和电话线进入。他们可以做这些昂工作吗？让他们做好准备的最好方式是对他们进行他们上下班时间可能遇到的社会工程黑客攻击策略的培训。

很简单，社会工程攻击包括采用明智的方式回答问题，然后使用这些问题还获取限制区域或者信息的访问。它可以是黑客假扮成服务台的技术人员询问用户的密码，或者假扮成其他人例如网络管理员、难过的用户或者需要访问通讯设备的电工、需要进入机房的消防人员、看门人或者其他可信人员。这些类型的人想要访问电脑或者机房的难度有多大呢？你向那些不期而遇的电工询问 ID 的次数有多少呢？如果你在布线室发现了一位“电工”，你会问他问题吗？如果你和大部分人一样，你就会认为一切正常，并继续做你的工作。这种行为试验模式正是黑客预计的行为。

除了员工培训，这些类型的攻击最好可以通过制定社会工程防御策略来阻止。这些策略要禁止在电话和邮件中泄露敏感信息，禁止通过大门，并要求访问者佩戴标志。我还高度推荐你读一下 Kevin Mitnick 关于社会工程的书，叫作《欺骗的艺术》（The Art of Deception）。通过查看安全的人为因素，你就可以防御对公司顶级机密的非授权访问。

（作者：Vernon Haberstetzer 译者：Tina Guo 来源：TechTarget中国）

应对不同行业安全威胁的最佳做法

网络安全威胁在每个行业都有所不同。但是，无论你在金融服务、制造业、教育、政府部门还是健康医疗行业工作，某些最佳安全做法都能够帮助你阻止安全威胁使你的业务陷入瘫痪。SearchNetworking.com 最近与读者进行了讨论，发现了他们最担心的安全问题。我们编辑了行业和安全专家和作者 Michael Gregg 对人们普遍担心的问题的一些答复。正如 Michael 在他的新书《Hack the Stack》(堆栈攻击)中的做法一样，他提供了一步一步的解决方案帮助锁定网络的安全，无论你在什么商业领域。

行业：政府部门/军事部门

威胁：无线安全

IT 计划经理 Philip Propes 说，在我的工作中，主要的威胁时是适当的设置和无线网络的安全。随着移动数据系统目前在本地和国家执法部门的广泛应用，各种类型的数据正在通过无线网络传输。

本地执法部门一般都被强制性要求采用增强的信息共享做法。由于仓促提供这些服务，机构通常由于受到时间和资金的限制没有保护这些数据。简言之，信息是以“仅仅可以使用”的方式共享的，而保护数据安全的原则通常被忽略或者降低到了最低的限度。

我们为本地、州和联邦政府执法机构提供网络和安全支持服务。我们看到许多部署不当的、大敞四开的无线网络。

Michael 答复：你提出了一些很好的问题。这里缺少的是总体的控制。

这里需要应用的某些类型的结构是克服这些问题。我建议采取下面五个步骤的方法：

1.评估。查看这个机构的资源并且确定它们的价值(金钱价值或者非金钱价值)。分析这些可能的威胁并且计算这些威胁实现之后可能产生的后果。最后，检查这些威胁的影响。这个第一个步骤的想法是确定这个机构拥有的这些东西有什么价值，应该采取什么措施保护这些资产。

2.政策。拥有了对于具体资产和信息的价值的理解，这个机构现在就可以开始制定政策，规定如何处理这些资产。在你的政策中，要详细说明必须使用什么控制措施保护重要的资产。例如，政策也许会规定你使用加密措施。拥有某些政策指南之后，这个机构就可以采取下一步措施了。

3.实施。遵守和实施在你的政策中规定的事情。最好是在你的政策中规定所有的无线接入点必须使用 WPA。但是，除非强制执行这些政策，否则这个政策是没有用的。

4.培训。需要对雇员进行培训以保证他们理解新的政策。雇员需要进行很好的安全培训。虽然某些人也许会认为事情到此就结束了，但是，实际上还有一个步骤。

5.审计/遵守法规。如果用户不遵守，全球最佳的政策也是没有用的。审计是对安全控制方法进行系统的评估以观察这些安全方法与已经建立起来的一套规则是不是一致。

我认为，这对你的问题是一个广泛的答案。但是，这里的问题是结构性的问题，需要高级官员的支持。

行业：教育

威胁：聪明的学生黑客

语法学校网络管理员 Neil Cross 说：在学校中工作，我们每天面临的现实是学生有能力比信息技术通讯技术支持人员和教师更快地吸收最先进的新技术。要跟上黑客迷的安全威胁的步伐是非常困难的。在允许和鼓励学生自由的学习的同时保证网络的安全是一项巨大的挑战。

Michael 答：与儿童在一起工作是有益的，但是，这也是一个挑战。这类问题的答案是工作人员不断地面临一个熟悉技术又不怕突破障碍的学生用户群的挑战。这里的网络管理员面临一种严峻的环境，因为学生不像成人那样担心法律责任(如失去工作等)。管理员还需要应付有限的预算问题以及没有高级计算机技能的员工的问题。

我这里最佳的答案是使用最低权限的原则。这个概念是雇员或者用户只有在他们需要完成分配给他们的任务的时候才有权访问应用程序或者使用资源。如果这个学校是微软的环境，管理员可以使用组策略锁定系统，这样，只能执行一些获得批准的必要活动。如果

有必要的话，组策略能够把 PC 锁定到它不能关闭的一个点。组策略提供许多设置选项，可以根据具体用户的需求和计算机使用的领域使用这些设置选项。

对于使用多种操作系统环境的学校来说，或设使用 Novell 环境的学校来说，防止计算机系统被修改或者防止使用非授权软件的工具也是有价值的。DeepFreeze 就是这种工具软件的一个例子。DeepFreeze 能够阻止用户对操作系统和应用程序进行永久性的修改。诸如 Anti-Executable 等其它程序提供了额外的保护功能，帮助限制这种程序的运行和安装。

另一个必须采取的步骤是教育和反应。学校应该采取措施反对学生黑客。突破学校的计算机系统是一种犯罪行为，并且要按照犯罪行为进行处理。许多学校正在通过重新评估学生的计算机道德十诫来解决这个问题，并且教育学生计算机犯罪可能遭受的处罚。随着更多的学校向学生提供笔记本电脑，安全教育将变得更加重要。其它能够帮助教师和管理员完成这个任务的资源还包括如下网站 CyberCitizenship.org 和 Education World(教育世界)。

行业：金融/保险

威胁：决定在什么地方划线

技术解决方案经理 Mark Woods 说，据我观察，任何行业排在第一位的威胁是过分热心的内部数据安全团队。这些人不知道风险与确保安全的计算方法。如果按照他们的方法，他们会把全部硬盘数据全都檫掉以保证环境尽可能地安全。但是，这会给业务造成损失。他们以为自己最了解政策和设置，没有考虑广域网延迟或者实施的任何解决方案的弹性。

Michael 答：

这类问题有趣的事情是在一些人似乎在有关“多大程度的安全是足够的和你如何找到平衡”的争论中站在反对派的一边。

要直接解决这个问题，我认为对每一个人都有帮助的事情是让机构进行一次正式的风险评估。这里是需要完成的项目列表。

首先是从目录开始并且编辑一个机构资产列表。如果你不知道这个机构有什么资产，你就没有办法保证这个机构的安全。

一旦完成这个列表，这家公司应该建立一个风险评估小组。这个小组应该检查所有现有的风险并且对可能影响这个机构的各种危险进行分类。这个小组应该检查飓风等自然灾害、恐怖袭击等人为的威胁以及设备故障等技术威胁。

下一步，这个风险小组可以开始考察这些应急事件的每一个事件的成本和发生事件的可能性。这可以使风险小组把高风险和高影响的担心放在列表的前面。这些计算可以通过质量或者数量的方式进行量化。Cramm 和 RiskWatch 等功能可以帮助自动实现这个计算过程。

完成上述步骤之后，这个小组应该就什么是最大的风险以及应该采取什么合理的措施保证这些有价值的资产的安全达成一致的意见。总之，这个目标是平衡安全和可用性，在提供成功地完成任务所需要的访问信息的同时保证资源的安全。

行业：健康医疗

威胁：数据安全

Bill Woods 说，最终用户安全是我们的最大挑战。我们的大多数最终用户在开放的地方都有工作站。同事或者过路的人都能够提取数据或者入侵这个网络。这包括最新发生的黑客入侵我们最近在我们园区的许多层楼中建立的无线网络。

Michael 答：健康医疗行业明显的担心是数据安全。在这种情况下，最佳的起点是进行隐私影响分析。隐私影响分析的目的是查看通过商务流程处理的不同类型的个人信息。隐私影响分析应该确定在电子系统中收集、维护和发布个人信息的风险和影响。隐私影响分析还应该确保存在适当的隐私控制。应该检查现有的控制措施以验证拥有责任制度，每一次出现新的计划或者流程的时候都要建立遵守这个规定的制度。

隐私影响分析与三个项目有关：

1.技术。任何时候你增加新的系统或者进行改变，你都需要对这个技术进行评估。

2.流程。商务流程变化，即使你的公司可能拥有很好的改变政策，这种变化管理系统也许会忽略个人信息隐私。

3.人员。企业改变与他们做生意的雇员。商业合作伙伴、厂商或者服务提供商发生变化的任何时候，都需要重新检查这些变化对隐私的影响。这个问题在健康医疗行业是非常重要的，因为它们要遵守 HIPAA(健康保险可移植性和责任法案)法。HIPAA 法第 1177 款规定，如果这个犯法行为是以商业利益、获取个人收益或者恶意伤害为目的销售、转移或者使用个人可以识别的健康医疗信息，犯罪分子最多可被处罚 25 万美元罚金或者最多 10 年监禁，或者同时进行这两项处罚。这个处罚足以引起每一个人的注意。

行业：制造业/工程行业

威胁：内部人员的威胁

目前失业的前电信服务工人说：我们最严重的威胁是心怀不满的雇员。系统管理员拥有这个“王国的钥匙”。随着大量的裁员，有些人会离开，大多数是人的离开是违背他们的意愿的。这可能会引起灾难性的后果。

Michael 答：企业通常仅担心外部的攻击者。这种想法并不是没有道理的。研究表明，内部人员实际上是最大的威胁。

这是以一个“MOM”原则为基础的。MOM 的含义是：动机、机会和手段。内部人员拥有手段和机会实施内部攻击，而外部人员只有动机。还有一种说法，内部人员拥有实施攻击所需要的三件事情中的两件。解雇或者裁减员工队伍等事件将增强这种威胁。这确实是一个问题。

要解决这个问题，企业需要有一个良好的控制措施。这就意味着当雇员被雇用时，他们要签署一个可接受的使用政策协议。这样他们就知道哪些事情是允许做的，哪些事情是不允许做的。工作轮换或者强制休假等控制措施可用来增强安全。此外，应该向员工提供最低限度的访问权限。有趣的是，市场研究公司 Gartner 曾经报告称，访问速度慢时大多数企业的一个大问题。最后，当雇员离开公司时，包括密钥、徽章和物理访问在内的所有的访问条件都应该终止。仅仅使用一些控制手段就能够极大地提高这个机构的安全。

最后，我想说，这确实是一个有趣的竞赛。阅读比赛参加者的文章能够使人们更清楚地了解一件事：我们面临共同的挑战。这些发现强调了沟通的必要。与同一个行业和领域

的人谈一谈是找到你的机构能够使用的最佳方法的一个好途径。你可以在每年召开的信息安全决策会议、RSA 意义以及其它许多网络和安全会议上遇到这些人。感谢所有参加这次竞赛的人员，祝你们保持安全!

(作者：Michael Gregg 译者：东缘 来源：TechTarget中国)

网络安全：如何避免物理安全威胁

在那儿...墙上的小插孔连接着世界，从互联网到你公司的薪水系统。只要网线插入这个插座，他们就开始工作！谁开始工作？你可能会问。让我们从那个神秘的，在一个还不错的，安静的会议或是培训室找到一个网络插孔的人开始来看这个问题。这么做的真正的问题是什么，你怎么对付他们呢？在这里，你将学习怎样提高网络安全性以消除物理安全威胁。

私人设施相较于公共设施一直拥有更高的安全性，因为它们更容易达到物理上的安全。公共场所——如医院，大学和图书馆——的安全保护可能是一项挑战，因为很难在物理上做到安全。不管公共或私人的场所，网络插座频繁使用的地方总是会有某种程度的安全风险。教室，座谈室和会议室都是通常不会锁门以及任何好奇的人都能进入一探究竟的问题区域。

让我们用实例来说明这些风险。假设黑客用笔记本电脑连上你所在大楼的网络插孔。大多数网络插孔是频繁使用，也就是说它们可以连接到网络设备功能区域上。假如你运行的是 DHCP 服务器，——它会为每一个连接到网络的设备分配一个 IP 地址——同样也会为黑客的笔记本电脑分配一个。如果没有使用 DHCP，黑客可以很容易地使用嗅探器为他的笔记本电脑找到一个未使用的 IP 地址。一旦连接上网络，几个简单的命令就可以定位你的关键服务器，然后列举出用户帐户，服务就开始了。于是几分钟内，密码可能就泄露了，一两个服务器就可能被攻击了，游戏也就此结束；黑客已经赢了。摆在你面前的是一个真正的混乱情况。

幸运的是，总有办法避免物理安全威胁并阻止黑客——甚至能阻止供应商和承包商之类找到网络插孔来连接到你的网络。第一件你可以做的事是禁用会议室和教室的网络插孔，直到需要时才启用。另一个最佳实践是在任何可能的时候都把房间锁起来。第三个防御的办法是让你的网络交换机只允许特定 MAC 地址的网卡连接到网络。每一个网卡都有一个独一无二的 MAC 地址，虽然这个地址可以通过欺骗软件改变。更严格的方案是，配置你的网络服务器，要求在每个用户登录前先认证计算机。请记住，如果你想防止未经授权的人使用已经连接到你的网络电脑，如教室的电脑，除了要求用户认证，你应该在用户端和

网络端都设置电脑开机锁和屏幕保护程序密码锁。欲了解更多有关证书的问题，请联系公钥基础设施（PKI）和数字证书系统的供应商。

大多数上述建议需要服务器和网络管理员的配合。如果你不向他们解释这些真实存在的安全风险，他们未必意识到这些改变能带来的价值。可用的网络插孔是黑客入侵的通道，一旦忽视，可能导致的重大安全事件。

（作者：Vernon Habersetzer　译者：Sean 来源：TechTarget中国）

企业UTM安全：最好的威胁管理解决方案？

如果你相信所看到的一切，那么企业统一威胁管理（UTM）产品和设备似乎就是信息安全的银弹。这些集所有功能于一身的设备号称能为任何企业的安全问题提供灵丹妙药，其功能包括网络边界防护，内容过滤，病毒防护等。但是，我从来没有遇到过会轻信资料的安全专家。实际上，UTM 确实能为中小型公司提供不错的网络安全防护，但是这在大企业中是行不通的。

什么是统一威胁管理（UTM）？

UTM 产品简单说来就是把几个安全产品整合在一个设备里。从性能的角度来看，这是完全合理的。我们都知道，许多专门的服务器，如那些用来运行安全软件的服务器，大部分时间都处于闲置状态。在一台服务器上运行多个服务可以有效利用，能充分利用性能。

UTM 产品的基础就是网络防火墙。UTM 的其它组件则视你所选择的厂商和型号而异。它们的共同点有：

- 垃圾邮件防护
- 内容过滤
- 防病毒/反间谍软件保护
- 入侵防御

UTM 厂商非常喜欢用花哨的图表向你“证明”部署 UTM 产品取代单独的组件可以省下大量时间和资金。然而根据我的经验，除了省下网卡配置这类基本设置的一点时间，部署 UTM 产品并不会让你在配置和使用上少花多少精力。从另一方面来说，它确实节省了开销，因为从一个设备里获得了多种安全服务--只需要购买一次--这让你的钱花得更值。

部署 UTM 带来的风险

在我看来，部署 UTM 产品时主要有两种风险：容错性不够和供应商差异不大。容错是一个非常重要的问题，因为 UTM 设备的一个硬件或软件错误就能让所有安全服务同时宕掉。根据你的网络配置，这要么导致整个公司网络断线（等着凌晨 3 点被电话吵醒吧！）

要么导致所有安全设施停机，这也不是什么好事。各个服务运行于独立的硬件平台，不用担心各种服务之间相互连累的这种畅快感是没法在使用 UTM 的过程中享受到的。

在我看来，供应商的夸大其辞，是 UTM 产品的最大消极因素。想想最先想到 UTM 的和最先生产它的厂商。这家公司该如何归类？如果你说：“防火墙厂商”，那么你将买到的就是该公司开发的防火墙，附带了厂商捆绑的其它安全一些功能，这样他们就可以把它冠上 UTM 的名号了。同样，内容过滤厂商提供的 UTM 产品能有出色的内容过滤功能，同时还很可能附上一个很一般的防火墙。这真的就是你想要的？

我喜欢用“最佳组合”的办法来组建安全基础设施：找最好的防火墙，最好的 IPS ，最好的内容过滤器（等等……）再把它们和好的安全信息与事件管理（SIEM)产品组合起来。这是 UTM 所不可能实现的。

UTM 所扮演的角色

说到这里，可能已经害得你想和你的 UTM 一起跳崖自尽了，先别急，让我们再看看它积极的一面。我能想到至少在两种情形下 UTM 产品能在网络安全中发挥重要作用。

首先，对中小型企业来说，UTM 可能是正确选择。把所有这些功能集中到一块所带来的经济性和易用性有可能比各个部件都选用最好的更值得考虑。如果是这样的话，那就一定要选用 UTM。

第二，如果由于预算或其他方面的限制导致无法购买单独的垃圾邮件防护、内容过滤、恶意软件防护或 IPS，那么购买 UTM 就是一个非常好的方法，它可以让你只要较先前增加一点点预算就获得在其它情况下无法买到的诸多功能。这种情况下，要记住新增的这些功能只不过是“免费赠品”，不要在决定购买时太把它当一回事。首先找最好的防火墙，然后再看看其它的，比如看免费附赠的 IPS 功能是不是适合你的环境。

总的来说，统一威胁管理产品还是有点被炒作过度了。它确实能通过在一个硬件平台上提供多种安全服务达到充分利用硬件性能的目的，但是安全人员不太可能从中看到明显的时间节省，并且还会发现自己被束缚在了不理想的供应商上。也就是说，如果预算不允许采取其它的替代途径，UTM 就很可能是出路所在。

(作者：Mike Chapple 译者：Sean 来源：TechTarget中国)

保护企业网络 防御新型移动应用程序下载的威胁

挫败移动设备应用程序的威胁

互联网安全中心（CIS）已经建立了安全配置标准，它是一系列经过协商的关于移动设备（比如 iPhone 等移动设备以及它们所支持的多种第三方应用软件）的最佳实践安全配置标准。

在基础层面，CIS 建议企业在移动应用程序安全以及用户怎样使用这些应用程序跟网络交换数据的政策方面要“实际而且谨慎”。举个例子，Apple 公司让用户可以很简单的配置 iPhone 从而访问公司的电子邮件以及其他的后端系统，比如 CRM 和 ERP 等，但这样做会带来一个问题：如果没有合适的控制，那么公司的敏感数据就有可能泄漏。然而，实施 CIS 标准将会减少这种数据泄漏的情况。比如设置密码标准，可以对数据丢失提供强有力的保护，这个标准包括“需要的密码”、“自动锁定时间”以及“访问密码识别失败清除数据”等特点和功能。

另一种潜在的威胁载体是 Wi-Fi 网络或者全球定位系统（GPS）。许多设备通过这两种方式传输数据。CIS 标准能解释并且指导用户如何设置移动设备，以便在不需要的时候把这些服务关闭。

然而，现实情况却是今天的无线设备可以非常方便的传送数据。举例来说，有许多第三方应用程序支持从台式机或者笔记本电脑到移动设备的文件无线传输，这导致那些想通过网络偷窃文件的人不再需要插入 U 盘就能获得敏感数据。

为了减少通过网络应用程序对移动设备远程攻击的危险，像 iPhone 这样的设备可以设置成禁止所有收发以及接受功能的模式---即所谓的“飞机模式”。当设置成这种模式之后，GPS 功能就会关闭，而且所有的无线信号（Wi-Fi、蓝牙以及手机信号）都会被屏蔽。

应该鼓励用户对员工自己的设备进行设置，防止这些设备自动连接到任何可用的 Wi-Fi 网络。虽然这种设置可能会妨碍设备对企业应用程序的访问（如电子邮件或者浏览

器），因为这两个应用程序是通过手机信号连接的，但却可以保证这些设备不会为攻击者敞开大门。

有些深入研究移动领域的企业使用第三方产品来保护移动设备的安全。最新发布的 iPhone 固件版本支持思科公司的 VPN 功能，还支持 Microsoft Exchange 功能。然而，IT 厂家需要更多的选择，利用现存的安全设施来预防那些未经认证的、具有潜在危险的、会接触到公司网络的移动应用程序。比如，Trust Digital 公司的企业移动管理（EMM）软件支持 iPhone，它可以通过一个集中的管理平台进行 IT 管理以及保护 iPhone 的安全。

“虽然有 3-5%的用户总是会受到攻击，但是如今 IT 职业人员在保护移动设备不受日益增加的第三方应用程序破坏方面比以前有了更多的选择。”Gold 说。

（作者：Sandra Kay Miller 译者：Sean 来源：TechTarget中国）

智能手机移动设备面临的安全威胁及应对策略

如今，许多公司的 IT 部门需要做这样一项工作：使工作人员能在掌上电脑（PDAs）或者智能手机这类的无线手持设备上处理商业数据。在理想的情况下，所有的这些设备都是值得信赖的，并且不受恶意软件的干扰。可现实的情况是，许多设备都处于无人管理也没有安全保障的状态，这就成为手机恶意软件感染的理想目标。企业如何才能在这些问题泛滥前，将潜在的风险遏制在萌芽状态呢？

智能手机和掌上电脑的安全威胁日益增加

和 Win32 平台上的情况相比，手机恶意软件的数量仍然很少。迄今为止，已被发现的、专门针对移动操作系统的病毒、蠕虫和特洛伊木马不到 500 例。大多数只造成相对较小的损害，诸如：文件丢失、硬件重置或产生额外的话费。

不幸的是，长期制约恶意攻击的门槛正渐渐消失。首先，移动设备的使用人数正飞快增长。其次，新型热门商用消费级终端设备（如苹果公司的 iPhone 和 HTC 公司的 Android G1）的市场可能最终会发展成一个利润丰厚的市场，吸引到大量恶意软件开发者。

此外，现代智能手机已不再受制于狭窄的无线覆盖范围、单一化的操作系统或兆级别的存储容量。近乎无处不在的 3G 及 Wi-Fi 简化了恶意软件的无线传播，而数 G 字节的存储容量使得更多的敏感数据会被窃取。随着用户越来越多地通过移动设备使用电子邮件和上网冲浪这些应用（这也是传统恶意软件的传播媒介），这使得恶意软件的传播变得更加可行。而短信服务（SMS）和多媒体信息服务（MMS）也成为传播恶意软件的新方式。

最后消失的一道门槛可能是：那种容易让攻击者妥协的单一的移动开发环境。在过去，各种不同规格、封闭的开发环境常常使恶意软件无从下手。而塞班软件公司 Symbian Software Ltd. Series 60 系统则因开发环境友好，成为被攻击次数最多的移动平台。如

今，Android 和 Linux 正建立起开放的系统开发平台。那些存在于 MacOS 和 Win32 环境中的恶意软件，也有可能入侵 iPhone 和 Windows 的移动开发平台。

智能手机和 PDA 安全软件

幸运的是，随着移动设备变得更加强大，移动操作系统的安全模式以及第三方的安全程序也得到了发展。移动智能手机和 PDAs 的管理者可以安装上这些现成的防御软件来检测和阻止移动恶意软件的安装和执行。

首先，可以通过检查所有移动设备的可执行文件和安装文件的数字签名。这些数字签名包括塞班（Symbian）或微软 Mobile2Market 签署的认证程序，以及 Research In Motion 公司针对黑莓的控制 APIs。通过使用像黑莓企业服务器或 Sybase 公司的 Afaria iAnywhere 这一类的移动设备管理工具来管理安装文件，可以帮助用户防范移动恶意软件的自动安装。另外，可以创建移动软件白名单和黑名单，教会用户如何避免运行未签名代码，并明白这样做的原因。

下一步，利用移动操作系统的访问控制，阻止恶意软件篡改文件和调用敏感功能。例如，塞班 9 的权限管理政策可以限制程序访问系统和/或用户的文件及网络接口，而数据锁定可以把数据划分到私人文件夹里，并对不受信任的程序不可见。配置这些访问控制策略有利于阻止间谍软件窃取数据，防止特洛伊木马留下后门。

最后，不同于笔记本电脑的是，移动手持设备没有在出厂时安装防火墙、杀毒软件或垃圾邮件过滤器。可以考虑通过安装常驻于系统的移动安全程序设备来填补这些空缺。例如，适用于一般的移动操作系统的防病毒和 SMS 垃圾邮件的程序（这些移动操作系统厂商包括 AirScanner、F-Secure、McAfee、赛门铁克、SMobile 系统、趋势科技和 Sophos 等公司）。这些程序精于处理移动设备的威胁，如检测移动操作系统的特洛伊木马、过滤短信，阻止恶意软件入侵企业服务器。

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

企业如何制定Twitter策略　防止来自社交网络的威胁

在短短三年时间里，Twitter 已经成为数百万人的“互联网短信服务（SMS）”。许多人也发现这种方式非常有利于生产和交流，但最近针对此服务的攻击，以及来自一些用户声明已显示 Twitter 和其他的此类社交网站存在着潜在的危险。而 Twitter 的这些安全威胁对于企业将会影响更甚。它们不仅需要面对生产效率降低和相关隐私泄露的问题，甚至有许多直接的安全威胁。

不幸的是，诸如 Twitter 此类微博客网站的成功依赖的是人类的本性，特别是利用人类愿意分享和接触我们所信任的人的这些天性。这和许多基于社会工程学的攻击具有相同点。

大多数人都知道不要点击陌生人发给你电子邮件中的链接和附件，然而，由于 Twitter 是一个友好的、以组为基础的服务，许多人会毫不犹豫地打开一个 Twitter 消息中的简写链接，甚至完全不知道这个链接会将他们带向何处。

这种自然而然的信任使 Twitter 特别吸引那些恶意用户，他们可以使用这些服务来发动攻击，其中最常用的攻击方式就是利用网络诈骗来安装恶意软件，例如一种 Koobface 恶意软件的变种，当被感染的用户登录 Twitter 时，会接收到该病毒发送的假消息或是一个 Twitter 留言，内容大多是一个恶意网站链接，该网站提示您下载并更新您的 Adobe Flash 播放器，但实际上下载的是一些恶意软件。Twitter 消息中简写网址的服务还增加了其他的攻击方式，如在 DNS 查找服务器上添加恶意网址和域名之间的转换。

创建企业的 Twitter 策略

Twitter 的部分吸引力在于它的方便和容易交互，但代价的往往是安全性的缺失。企业管理者必须知道“免费在线服务不一定能够提供符合系统需要的安全标准”，我们还要知道 Twitter 没有服务水平协议来应对你所面临的问题。说到这你可能觉得我们需要将 Twitter 的使用全面禁止，但是这可能不切实际，即使你所在的行业是银行或医学也不行。当然，并不是你的每一位员工都需要访问 Twitter，有时市场营销或人力资源部门的员工可能需要使用他们，甚至在英国的政府部门，也已经被要求使用更多的微博客工具。

降低使用 Twitter 时存在风险的关键，就是通过技术或培训来形成一个有效而敏感地策略保障。而确保这种方法的成功最好的办法是让你的员工同意接受此策略，并且必须严格的执行。一般来说当雇员理解了那些与公司整体的 Twitter 政策有关的规定和限制时，他们是不太可能试图绕过这些的，他们也不会再有借口说不知道什么可以在 Twitter 上说或做。为了保证政策执行应该部署 Web 监控工具，例如 Websense 公司的 Web Security Gateway 或 McAfee 公司的 Secure Web Gateway，以确保有违反纪律的事件发生时可被检测到，以便可以采取相应的处分措施。

由于存在许多基于社会工程学的攻击，而这些攻击方式也在不断发生巧妙变化，因此提醒那些经常登陆社交网络站点的工作人员安全风险的存在就显得非常重要。例如什么类型的内容和要求，应被视为可疑，还要加强诸如不能点击社交网络的横幅广告此类的指示，因为横幅广告常被用来传播恶意软件。对于其他新兴的攻击媒介，例如虚假的更新通知，也要提高警觉，也可以实施新的限制以防止他们。当然，强大并定期更改密码是非常必须的，并且 Twitter 密码应和用于访问内部网络和服务的密码不同。

很明显，那些可以应对基于 Twitter 攻击的防御技术包括了传统的反恶意软件扫描功能，可以用来检测甚至是防止感染。公司的 Twitter 策略也应该决定防火墙规则控制什么人可以在什么时候访问。信息被允许进入公司网络之前，考虑使用网络访问控制（NAC）进行审批。还应该通过链接检查或网站过滤清除那些已知的恶意网页。我还建议使用 OpenDNS，因为它有免费的内容过滤服务，以此可以来阻止网络用户访问不良内容以及钓鱼网站。如果你的组织使用的是 Firefox，Twitter 的网址缩短服务提供了一个 Firefox 插件，它使用户能够看到那些简写网址链接的全貌，包括网站的页面标题。

企业面临的挑战是防止那些来自社交网络的攻击，同时又不会失去通过使用社交网络所带来的潜在利益。

任何组织，如果不能列出具体政策，或在 Twitter 上不能按照该政策来要求员工安全而警觉的使用基础设施和资源，就会让组织面临更多的以 Twitter 作为媒介的攻击。如果企业不制定安全策略，而是让他们的员工自由的使用 Twitter，这毫无疑问会使他们的系统和数据存在安全隐患。

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