

使用Internet 如何给企业网络带来风险

引言

商业企业越来越依赖 Internet，并将 Internet 作为日常运作的重要组成部分。Internet 提供了快捷的信息获取渠道和与外界 24x7 的不间断联络。尽管 Internet 具有不可抗拒的优势，但是它也同时将企业置于一些安全威胁之中。随着使用率的增加，对 Web 的简单使用也会使公司承受来自互联网更高的风险威胁。

不当的使用

如果企业无法对员工的 Internet 使用进行过滤或者监控，那么可能会影响员工工作效率，甚至使公司声誉和网络安全等承受一定的风险。员工可能为了个人或者商务上的原因，浪费过多的时间在网络上冲浪。很多人还会访问在线商城、P2P 和社交网络站点——甚至是一些在线的年龄限制或者成人站点。所有这些访问将可能浪费工作时间并且将公司网络暴露于 Internet 的威胁当中。

举个例子，成人网站向来都因为携带大量的恶意软件而臭名昭著。这类型的网站都很简单并且不用很高花费便能访问，内容又相当吸引访客，而且，即使用户怀疑他们的系统因为浏览这些网站而被感染时，也会由于忌讳而保持沉默。这些特性使得成人网站非常适合用于传播恶意软件。

在线购物网站传播 Internet 威胁的程度跟成人网站同样值得注意。这类型的网站上往往遍布着大量猖獗的间谍软件。它们一般无形地把用户链接到第三方站点上去选择它们的产品。因此，就算主页是可靠的，用户也很难知道他们何时在“干净”的网站，何时又在未知的第三方网站上。

在 PricewaterhouseCoopers 代表英国商业企业管理改革部（BERR）进行的年度信息安全破坏调查中发现，过去的一年里，高达 1/6 的企业出现员工不当使用信息系统的情况。报告中指出，36%的员工使用过多的时间在互联网上冲浪，另外 41%的员工浏览了不恰当的网站。尽管不是非常普遍，但是也有员工访问了非法的内容。

包括可疑或风险在内的大部分不当的使用行为，可归因于员工对公司设备的漠不关心。

他们认为这是公司，而不是他们自己的计算机，使不使用安全措施关系不大。同样的，许多用户认为安全工作是 IT 部门的职责，所以冒险行为也不会产生任何负面影响。

外部威胁的传播手段

即使员工正常地使用网络资源，Internet 也是安全威胁的主要来源，包括间谍软件、特洛伊木马、僵尸程序、后门软件和 Rootkits 等。很多情况下，要感染用户只需要让他简单地访问一下那个站点即可。这种传播的方式被称为“偷渡式下载”，顾名思义是在用户正常的访问时通过后台进行下载——用户对此毫不知情，也不需要用户配合。

NETGEAR ProSecure™ 的研究指出，79%的安全威胁来自于被入侵的合法网站。黑客攻击了这些合法网站后在上面植入安全威胁软件。这种情况一般是黑客利用了一些 Web 的漏洞对尚未打上漏洞补丁的网站进行攻击。所以，任何网站都有可能被攻击。仅 2008 年的第一季度，全球 500 强企业、政府部门、学校的几千个网站都受到了攻击并植入恶意代码，甚至连知名的安全厂家，如赛门铁克、趋势科技、CA 等公司网站也受波及。

黑客也会采用合法网站来作为“社会工程学”攻击策略的诱饵，来诱导用户点击内嵌的连接或者是 Email 附件。2008 年 12 月，知名的公共社交网站 Facebook 就被利用来进行类似的攻击。用户收到了一个标题为“You look funny in this new video”的邮件。这个邮件让用户使用内嵌的连接去观看视频。这连接将用户引导到不属于 Facebook 的视频网站，还通知用户必须更新 Flash 播放器。通过升级的连接，蠕虫病毒就会安装到用户的系统上。蠕虫中包括了间谍软件并打开了系统的后门，再将用户的私人信息通过后门发送出去。这后门也为将来黑客在系统上安装其它代码做了准备。

剩下的 21%威胁来源于用户自身不注意地访问了不良网站。这些网站看起来是合法的，特别对于没有戒心的用户。许多这类网站在搜索引擎上做市场推广和广告，增加访问量。

通过在合法网站上植入安全威胁，黑客得到内置的监听器。通过建立他们自己的不良网站，他们得到对威胁更多的控制权。这两种情况下，仅仅通过限制网站内容来保护公司网络免受威胁明显是不够的。

保护您的商业网络

黑客通过入侵脆弱的用户系统来到达他们的真正目标——公司网络。因此，许多安全威胁都是通过用户的系统进入到公司网络的，而且畅通无阻地繁殖。一旦入侵成功，这些安全威胁将消耗大量网络带宽、窃取敏感公司资料 and 用户数据、破坏文件系统，或者入侵公司其它设备来发送垃圾邮件和其它邮件安全威胁。

因此，防御来自 **Internet** 安全威胁的第一道防线需要建立并且执行一套 **Internet** 访问策略。这个策略必须包括允许访问哪种网站而不允许访问哪种网站，同时规定允许访问的时间。但是，大多数的企业允许用户使用公司的设备来进行私人的 **Web** 活动，也允许用户随便将企业网络带入风险中。所以策略必须规定允许员工花费在私人 **Web** 活动上的时间，也包括允许他们访问的站点。

为执行使用策略，绝对有必要在公司安装强力的安全网关来对 **URL**、内容过滤和双向流量进行检测。安全平台的 **URL** 和内容过滤功能可以阻止禁止的 **URL** 和不良的内容。当员工访问被禁止或包含不良内容的站点时，网络的传输会被中止，而且会有一份报告发送给 **IT** 部门。

我们要记住重要的一点，过滤只能防御风险中的一小部分。为了更全面的保护，安全平台必须拥有实时、双向的流量检测功能，以主动防御未被指定的网站上的恶意软件。这为防御被黑客入侵的合法网站或不良网站增加了一道关键的防线。流量检测功能监控着员工对 **URL** 访问时的双向流量。若有员工不小心进入被感染的网站，只要流量一通过安全平台马上就会被中止。

总结

任何连接到 **Internet** 的企业都因为他们日常的访问而面临着 **Web** 安全威胁。如果公司缺乏全面的网关安全，风险指数将大大提升。建立和执行使用许可策略的同时，采用实时双向流量检测的主动防御方案将大大降低风险。

NETGEAR® ProSecure™ STM 内容安全网关解决方案

NETGEAR® ProSecure™ 采用特有的技术，通过爆发扩散的速度和广泛程度来检测并阻止爆发。通过这种方式，可以在垃圾邮件和恶意软件爆发产生的极短时间内检测出来，并且实时地阻止所有相关的信息。

ProSecure™ STM 平台采用了专利的串流扫描技术，能够在数据流进入网络的时候马上进行扫描。NETGEAR STM 使用单一的平台即可实现对垃圾邮件、恶意软件、安全破坏或不必要的应用程序进行扫描，通过串流扫描技术，能够实时地扫描大量的数据。这使得局域网中的用户可以接收到安全的 Email 和 Web 内容但却没有任何延时。

ProSecure™ STM 平台使用主动防御系统来避免漏洞从发现到修复之间的时间差。NETGEAR 的解决方案中采用“法医式鉴定方法”来识别进出网络数据流中的可疑的特征，并抵制这些特征直到它们能够更精确匹配。