网络安全防御全面封阻六种主要网络威胁 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/0/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c99_478.htm 如果你认真核对这份安全一览表，就很有希望让数据窃贼把目光转移到比较容易下手的对象。数据窃贼并不总是像电影《黑客帝国》里面那样躲在阴暗房间里不停地敲键盘的黑帽子黑客：考试.大提示有些数据中心的员工爱惹事生非，而且技术方面有本事欺骗“ 领导 ”，他们常常也负有责任。 那么你该怎样来对付呢？无论你仅仅负责自己的一台计算机，还是要管理一批成百上千台PC，PC都容易受到各种各样的威胁，其中包括： P2P客户程序 不安全的无线网络 网络钓鱼 间谍软件 病毒 不安全的在家办公环境 社会工程 本文教你如何阻止这些威胁。 对P2P文件共享说不 作为与其他媒体爱好者共享音乐和视频文件的一种简便方式，像Gnutella、BitTorrent、Kazaa和LimeWire这些对等文件传输客户程序几乎像病毒一样流行。可遗憾的是，它们还能够与周围街区、全国乃至全世界的陌生人共享敏感的公司和个人数据。 最近针对银行和联邦政府使用P2P文件共享情况的几项调查显示，当初为共享媒体编写的这类程序访问机密和秘密信息有多么容易。达特茅斯大学的塔克商学院曾对美国前三十家银行使用P2P文件共享的情况作了一项调查，结果发现，P2P文件共享搜索歌曲里面的歌词或者视频文件名，居然发现了各种类型的匹配信息，包括公司名称、地址及更多的信息。 安全公司Tiversa开展的一项调查发现，使用P2P客户程序LimeWire仅仅搜索了两三个小时，发现的机密文档就超过了200个。 为什么P2P文件共享会带来如此之大的

潜在危险呢？视客户程序而定，P2P文件共享通常按文件类型进行，而不是按文件夹进行。因而，P2P搜索之后，与机密信息放在同一文件夹里面的音乐或者视频文件就会把整个文件夹里面的内容暴露在面前。 更糟糕的是，有些P2P客户程序让人们便于共享整个驱动器，而不是单单共享指定文件夹。如今，P2P客户程序无处不在，包括孩子的PC或者其他家用PC，甚至还出现在公司PC上。 为了阻止P2P文件共享给工作环境带来的威胁，公司应当进行安全配置，阻止P2P客户程序。如果你在远程办公，请对工作文件夹进行文件加密，并且确保绝对不会安装P2P客户程序来监控工作文件夹。还要随时关注P2P方面的动态。 保护不安全的无线网络 无线网络很容易组建——特别是不安全的无线网络。你的办公室可能建有一个无线网络，采用WPA或者WPA2加密和Radius验证服务器加以保护；如果你在家或者在公共场所办公，但用的是不安全的无线网络，就有可能暴露敏感信息。那么，外头有哪几种威胁呢？ 如果餐馆或者其他零售店使用不安全的无线网络供销售点系统使用，那么泊在停车场的“ 无线窃听者 ”（wardriver）就能获得商业信用卡上的信用卡号码，然后伺机出售；或者使用它们擅自疯狂购物。 免费的无线热点大量出现在餐馆和咖啡馆。如果笔记本电脑上的网络共享没有被防火墙阻止，其他上网者就可以边吃东西，边偷偷窃取你的数据。 家庭无线网络具有双重的不安全性：它们可能是不安全的（缺乏WPA或者WPA2加密），还可能使用标准的服务集标识符（SSID）或者工作组名称；这样一来，入侵者轻而易举就能进入网络，访问系统上的任何共享文件夹。 这个问题是多方面的，而解决方案也是如此。你很难确定零售商的

销售点系统是否安全，但任何公共热点本身就是不安全的。WindowsVista的防火墙可以自动阻止访问公共网络（如无线热点）上的共享资源。不过，WindowsXPSP2的防火墙要求你选择“无例外打开”（noexceptions）设置，才能在你使用公共网络时保护共享资源。 如果你的电子邮件客户程序不提供安全登录机制，就不要在公共热点使用该客户程序。而是应当为电子邮件、文件传输、远程桌面及其他应用建立一条安全连接，办法就是与你的主计算机之间建立起安全的HTTP（HTTPS）或者虚拟专用网（VPN）连接，或者使用GoToMyPC之类的安全远程访问服务。 凡是在家办公的都应当建立安全无线网络。如果贵公司的远程办公人员缺乏网络技能，就帮助他们对网络进行配置以确保安全。如果你的人员比较熟悉支持特定的路由器，不妨列一份推荐路由器清单。 如果你或者你的员工使用VPN连接，不妨考虑推荐或者要求使用能够支持多路VPN连接的路由器。有了这种路由器，多路VPN连接就可以同时从家里拉出来。记住：VPN连接拥有端到端安全性，哪怕是在公共网络上。 阻止网络钓鱼和社会工程 网络钓鱼是指利用貌似官方的电子邮件警告用户信用卡、银行账户或者PayPal账户可能会有严重后果，以此诱骗用户，把他们引到旨在窃取身份的虚假网站。如今这种伎俩大行其道，但防范手段也从来没有现在这么多。 微软的最新款浏览器InternetExplorer7以及竞争对手Mozilla的最新款Firefox2.0都包含反网络钓鱼功能，可以把URL与已知的网络钓鱼网站进行对照，并且提供了把可疑网络钓鱼者标出来的报告工具。如果你在运行版本比较老的IE或者Firefox，是时候升级到最新版本了。 为了进一步提高安全性，应当

向PhishTank（http://www.phishtank.com/）和PIRTSquad（http://www.castlecops.com/pirt）等反网络钓鱼网站等网络报告可疑网站；PIRTSquad还会试图关闭网络钓鱼网站。 不过，你不需要高科技就能能够帮助阻止网络钓鱼行为——只要用一点常识就能取得奇效。不要点击银行或者其他机构提供的链接；人工登录，不要自动登录。如果你对某个电子邮件或者网站上的任何链接有所疑虑，就记住这个办法：把鼠标移到链接上方，就能发现链接的真实目的地。 网络钓鱼只是运用最古老的黑客技术：社会工程的一种最新手段而已。为了阻止黑客冒充来自“ 求助台 ”或者“ 网络提供商 ”，要核实能够访问敏感信息的人员的身份，比如打电话给对方员工的上司，或者提出答案已事先确定的质问。 如果你只能提供密码给某人，以便对方能为你解决问题，就要确保之后马上改掉。SecurityFocus网站（http://www.securityfocus.com/）是一个不错的资源，它提供了对付网络钓鱼、社会工程及其他威胁的一些对策。 使用操作系统的自带工具 微软WindowsXPServicePack2和Vista都提供诸多工具，可以用来帮助检测及阻止入侵者。正如前文所述，两者都拥有易于使用的防火墙，可以在“ 无例外打开 ”模式下设置而成，以便在公共场所使用；同时可以访问比较安全的网络上的共享资源。两者（商业版）还都支持加密文件系统（EFS），从而为敏感文件提供了基于用户的安全。 不过，WindowsVista包括了另外几项阻止入侵的功能。它包括WindowsDefender反间谍软件工具（可供WindowsXP下载）；InternetExplorer7（可供WindowsXP下载）及新的电子邮件客户程序WindowsMail拥有反网络钓鱼功能；新增添了浏览器附件管理器；通过父母

控制（ParentalControls）来报告网站及活动；新的内部设计采用了地址空间分配随机化，这样就可以改变系统功能使用的地址空间，从而有助于防止攻击得逞；另外在企业版和最终版中，BitLocker全磁盘加密可以阻止笔记本电脑或者台式电脑（或驱动器）失窃引起的数据被偷。 查漏补缺 虽然WindowsVista对堵住WindowsXP中的安全漏洞大有帮助，但你可以采取措施，进一步提高系统的安全性。确保一旦WindowsUpdate或者微软安全公告上出现新的安全更新程序，就要及时安装。 你可以在TechNet安全中心看到Windows方面的最新安全标题新闻。定期使用及更新反病毒和反间谍软件工具包，这有助于防止遭到基于软件的攻击。 