网络安全中容易被假象迷惑的误区思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_644344.htm 许多人对于自己的数据和网络目前有一种虚假的安全感.在边界安装了防火墙、在桌面上安装了防病毒和防间谍软件工具、使用加密技术发送和保存数据.此外,微软及各大安全公司不断增强安全工具和补丁程序……似乎可以松口气了,但果真如此吗? 以下是有关安全的七大误解,不妨看看你的数据是否有你想象中的那么安全. 误解一、加密确保了数据得到保护 对数据进行加密是保护数据的一个重要环节,但不是绝无差错.Jon Orbeton是开发ZoneAlarm防火墙软件的Zone Labs的高级安全研究员,他支持加密技术,不过警告说:如今黑客采用嗅探器可是越来越完善,能够截获SSL和SSL交易信号,窃取经过加密的数据.虽然加密有助于保护遭到窃取的数据被人读取,但加密标准却存在着几个漏洞.黑客只要拥有适当工具,就能够钻这些漏洞的空子.Orbeton说:“ 黑客在想方设法避开安全机制. ”误解二、防火墙会让系统固若金汤 SteveThornburg是开发半导体联网解决方案的Mindspeed科技公司的工程师,他说:“ 许多人说:我们装有防火墙.但防火墙功能再好,经过它们的IP数据痕迹照样能够被读取. ”黑客只要跟踪内含系统网络地址的IP痕迹,就能了解服务器及与它们相连的计算机的详细信息,然后利用这些信息钻网络漏洞的空子. 如此看来,仅有防火墙和加密显然不够.网络管理员不仅要确保自己运行的软件版本最新、最安全,还要时时关注操作系统的漏洞报告,时时密切关注网络,寻找可疑活动的迹象.此外,他们还要对使用网络的最终用户给出明确的指

导,劝他们不要安装没有经过测试的新软件,打开电子邮件的可执行附件,访问文件共享站点、运行对等软件,配置自己的远程访问程序和不安全的无线接入点,等等. Thornburg说,问题在于,愿意投入财力和人力来保持安全的公司寥寥无几.他说:“ 它们知道这么做不会受欢迎,因为这会降低工作效率.成本是主要的问题,因为这些公司都关注成本底线. ”误解三、黑客不理睬老的软件 一些人认为,如果运行老的系统,就不会成为黑客的攻击目标,因为黑客只盯住使用较为广泛的软件,而这些软件的版本要比我们自己正在用的来得新. 事实并非如此,Johannes Ullrich说.他是安全分析和预警服务机构SANS因特网风暴中心的首席技术官,这家机构负责发布有关安全漏洞和错误的警告.他提醒,对黑客来说,最近没有更新或者没有打上补丁的Web服务器是一个常见的攻击点.“ 许多旧版本的Apache和IIS(因特网信息服务器)会遭到缓冲器溢出攻击. ”如果存储空间处理不了太多信息,就会出现溢出,从而会发生缓冲器溢出问题.额外信息总会溢出到某个地方,这样黑客就可以利用系统的漏洞,让额外信息进入本不该进入的地方.虽然微软和Apache.org在几年前都发布了解决缓冲器溢出问题的补丁,但还有许多旧系统没打上补丁. 误解四、Mac机很安全 许多人还认为,自己的Mac系统跟老系统一样,也不容易遭到黑客的攻击.但是,许多Mac机运行微软Office等Windows程序,或者与 Windows机器联网.这样一来,Mac机同样难免遇到Windows用户面临的漏洞.正如安全专家Cigital公司的CTO Gary McGraw所说:出现针对Win32和OS X的跨平台病毒“ 只是迟早的事 ”. Mac OS X环境也容易受到攻击,即便不是在运行Windows软件.赛门铁克公司最近发布的一份报告发现,2004年查明Mac OS X存在37种漏

洞.该公司警告,这类漏洞可能会日渐成为黑客的目标,特别是因为Mac系统开始日渐流行.譬如在2004年10月,黑客编写了名为 Opener的一款脚本病毒.该脚本可以让Mac OS X防火墙失效、获取个人信息和口令、开后门以便可以远程控制Mac机,此外还可能会删除数据. 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com