思科认证辅导:内网安全体系思科认证 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__E6_80_9D_E7_A7_91_E8_AE_A4_E8_c101_644361.htm 在经历了外网安全建设后，企业普遍面临“ 内忧 ”胜于“ 外患 ”的局面，换言之，企业不仅需要坚固的边界安全，更需要稳定的内网安全。 最近，国内某大型造船厂发生了一起有惊无险的网络安全事件。由于该造船厂的计算机系统内储存有大量的重要设计数据，某一天，系统突然报警，显示某个电脑终端正在非法拷贝这些重要文件数据，而网管人员通过内网审计系统的跟踪，立刻锁定了拷贝文件的电脑和登陆系统的用户名，从而在重要文件还没被外传之前，及时制止了该非法行为，避免了无谓的经济损失。 事实上，类似的内网安全事件在很多企业都有发生，但由于内网安全的完善程度不同，并非每个企业都能避免损失发生。有调查显示，超过85%的安全威胁 来自企业内部，其中16%来自企业内部未经授权的非法访 问，40%来自电子文件的泄露，由此可见，内网安全问题已是企业网络安全建设的重头戏。 为了确保网络安全，防火墙、杀毒软件、IPS等产品早已成为企业用户的普遍部署，但是，这些主要针对外网的安全防护在面对内网安全威胁时，往往形同虚设，因为“ 内忧 ”胜于“ 外患 ”，企业不仅需要坚固的边界安全，更需要稳定的内网安全。 那么，目前企业CIO们对于内网安全的认识是否到位，他们在内网安全部署方面处于何种程度，还存在哪些有待完善之处，内网安全在产品技术上又存在哪些发展趋势。 过半企业重视内网安全 网络安全威胁层出不穷，网络安全问题无处不在，但是，事情总有

轻重缓急之分，哪个领域的安全问题是企业用户当前首需解决的呢?调查反馈显示，“ 内网安全 ”以54.9%的比例占据第一位置，其次，25.7%的用户选择外网安全，10.6%的用户选择了终端安全，8.8%的用户选择了Web安全。 显然，企业网络安全建设行进之今，过半用户已经将“ 内网安全 ”设定为首需解决的问题。同时，这也表明用户对于内网安全重要性的认识已经达到相当程度。 北京互联通网络科技有限公司产品项目部顾问黄毅就明确表示，内网的安全管理，很多时候比外网安全管理更加重要，因为企业的机密信息泄漏、业务系统被如侵等，往往就是透过内部的非授权访问和木马泛滥导致的，所以，保障内网安全势在必行。 作为内网安全建设领域的专家，北京鼎普科技股份有限公司战略市场部经理万俊告诉记者，一直以来，企业安全防御的理念更多局限在常规的网管级别 (防火墙等)、网络边界(漏洞扫描、安全审计、防病毒、IDS)等方面，主要的安全设施大多集中于机房、网络入口处。应该说，在这些安全设备的严密监控下，来自网络外部的安全威胁得到显着缓解。然而，随着企业信息化的不断深入，来自网络内部的安全威胁开始逐步凸显出来，网络的内部安全问题大于外部问题渐渐成为业界共识。 对此，我们可以从企业用户当前对于安全细节问题的关注度得到印证。在“ 哪些安全细节问题是贵公司当前比较重视的 ”这一问题中，83.2%的用户选择 了病毒查杀，69.0%的用户选择了数据库安全，46.9%的用户选择了网络设备安全，31.9%的用户选择了补丁升级管理，31.0%的用户选择了网站 运维安全，27.4%的用户选择了身份认证，22.1%的用户选择了信息加密。可以看出，不论是常见的病毒查杀，还是身份认证或信

息加密，用户对此都持有 相当的关注。“ 提高意识 管理到位 ”是首要 为什么需要管理内网安全，我们从企业员工的日常小事即可明白。如今，很多员工在上班闲暇时，偶尔聊聊QQ或MSN，要不上开心网玩“ 偷菜 ”或观看在 线电影，要不干脆打开BT电驴等下载软件下载大容量文件。这些在大小企业中普遍存在的现象不仅影响了员工的工作效率，而且还会占用企业网络流量，从而影响 其他正常业务的开展。 事实当然不仅如此，根据本次调查反馈，70.8%的企业存在“ 员工随便登陆MSN、QQ、BT等内容 ”，37.2%的企业存在“ 经常有人改动 IP地址从而造成冲突 ”，62.8%的企业存在“ 经常出现某台电脑没有打补丁或补丁不全 ”，31.0%的企业存在“ 经常受到非法入侵 ”，48.7%的企业存在“ 不能完全限制内网的设备与重要信息的保管 ”。 可以看出，近七成左右的企业存在“ 员工随便登陆MSN、QQ、BT等内容 ”和“ 经常出现某台电脑没有打补丁或补丁不全 ”的现象，另外三项困扰也有近五成企业有所遭遇。 另外，根据调查反馈，目前企业网络主要遭遇的安全威胁中，76.1%的用户选择木马病毒，14.2%的用户选择蠕虫，8.8%的用户选择电子邮件攻击，0.9%的用户选择网络钓鱼/欺骗。可见，木马泛滥的确到了人人喊打的地步。 需要指出的是，木马病毒除了可以跟随Web应用从外网进入内网之外，还有一个重要的传播渠道，即通过移动U盘直接在内网终端上蔓延开来。对此，在诸多安全厂商的内网安全产品中，都或多或少存在防止移动终端传播病毒的功能。比如鼎普科技的安全U盘系统，它是通过智能判断和权限访问控制技术，使数据信息在U盘上实现存取控制，同时也具备对U盘进行身份认证、敏感信息外带时防止非授权访问和

病毒窃取等功能。目前，金融、电信等行业用户大多应用了类似系统以杜绝终端隐患。 抛开行业特殊性，抛开单一内网安全产品或功能，目前企业用户针对网络安全的部署现状如何呢。根据调查反馈，96.5%的用户选择了杀毒软 件，78.8%的用户选择了防火墙，24.8%的用户选择了VPN(安全传输)，20.4%的用户选择了身份认证系统，27.4%的用户选择了内网安全管 理，8.8%的用户选择了IDS/IPS。 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