网络安全三分技术加上七分管理 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_251169.htm 企业该如何在有限的资金条件下，达到投入与安全的平衡？ 目前很多网络安全技术还处于探索阶段，如果人云亦云地简单购买安全产品，那么，这个所谓的“ IT黑洞 ”永远无法填满。 安全管理是填补“ IT黑洞 ”最经济有效的方式。 防病毒：要求病毒代码每周至少升级2~3次； 漏洞扫描：要求定期对网络扫描，发现系统的漏洞，指导打补丁； 网络入侵检测系统：随着网络结构和应用的变化调整重点预警区，不但要求网管员了解预警产品的功能及响应，还必须正确配置交换机监听端口。 一、领导高度重视 对网络安全而言，领导重视更重要。网络安全管理是一个动态的系统工程，关系到： 安全项目规划、用需求分析、网络技术应用、安全策略制定、人员职责分工、安全等级评定、网络用户管理、安全审计评价、人员安全培训、安全规章制度建立。这些是对网络管理者提出的要求，仅靠技术人员的工作职能无法完成。 二、随需求确定安全管理策略 随着网络拓扑结构、网络应用以及网络安全技术的不断发展，安全策略的制订和实施是一个动态的延续过程。当然可以请有经验的安全专家或购买服务商的专业服务。 但是一个单位的网络安全服务建设不可能仅依靠公司提供的安全服务，因为商业行为与企业安全有本质差别，不是所有的网络都需要所有的安全技术，何况有些安全技术本身并不成熟，只有采取适当防护，重点突出的策略，才能有的放矢，不会盲目跟风。 不同的网络有不同的安全需求： 内部局域网和互

联网接入有不同的要求；涉密计算机的管理与非涉密计算机的管理不同；不需实时在线的小型数据系统并不需要昂贵的NAS产品，活动硬盘即可；应该遵照国家和本部门有关信息安全的技术标准和管理规范，针对本部门专项应用，对数据管理和系统流程的各个环节进行安全评估，确定使用的安全技术，设定安全应用等级，明确人员职责，制定安全分步实施方案，达到安全和应用的科学平衡。 就现阶段而言，网络安全最大的威胁不是来自外部，而是内部人员对网络安全知识的缺乏。人是信息安全目标实现的主体，网络安全需要全体人员共同努力，避免出现“ 木桶效应 ”。 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