<<网管从业宝典>>

图书基本信息

书名：<<网管从业宝典>>

13位ISBN编号：9787562445326

10位ISBN编号：756244532X

出版时间：2008-6

出版时间：刘晓辉 重庆大学出版社 (2008-06出版)

作者：刘晓辉 编

页数：312

<<网管从业宝典>>

内容概要

系统分析了网管在日常工作中将遇到的各方面的网络安全问题。
从局域网安全策略、无线局域网安全策略、黑客攻击预防、服务器安全配置、漏洞补防、文件安全、数据备份与恢复等方面进行系统全面的介绍。
并通过资深网管多年的从业经验，介绍如何才能有效地将突发网络安全问题降到最低。
适合广大学生、网络爱好者及网络从业人员阅读学习。

<<网管从业宝典>>

书籍目录

章节摘录

插图：第1章 网络安全概述1.1　网络安全定义从本质上看，网络安全就是网络上的信息安全。
而对“信息安全”有多种理解。
种种偏差主要来自于从不同的角度来对待信息安全，因此出现了“计算机安全”、“网络安全”、“信息内容安全”之类的提法，也出“机密性”、“真实性”、“完整性”、“可用性”和“不可否认性”等描述方式。
1.1.1　国内对信息安全的定义信息安全保密内容分为：实体安全、运行安全、数据安全和管理安全四个方面。
我国计算机信息系统安全专用产品分类原则给出的定义是：“涉及实体安全、运行安全和信息安全三个方面。
”我国相关立法给出的定义是：“保障计算机及其相关的和配套的设备、设施（网络）的安全，运行环境的安全，保障信息安全，保障计算机功能的正常发挥，以维护计算机信息系统的安全。
”这里面涉及了物理安全、运行安全与信息安全三个层面。
国家信息安全重点实验室给出的定义是：“信息安全涉及信息的机密性、完整性、可用性、可控性。
综合起来说，就是要保障电子信息的有效性。
”1.1.2　国外对信息安全的定义英国BS7799信息安全管理标准给出的定义是：“信息安全是使信息避免一系列威胁，保障商务的连续性，最大限度地减少商务的损失，最大限度地获取投资和商务的回报，涉及的是机密性、完整性、可用性。
”美国国家安全局给出的定义是：“因为术语‘信息安全’一直仅表示信息的机密性，在国防部用‘信息保障’来描述信息安全。
它包含5种安全服务：机密性、完整性、可用性、真实性和不可抵赖性。
”国际标准化委员会给出的定义是：“为数据处理系统而采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭到破坏、更改、显露。
”这里面既包含了层面的概念，其中计算机硬件可以看作是物理层面，软件可以看作是运行层面，再就是数据层面；又包含了属性的概念，其中破坏涉及的是可用性，更改涉及的是完整性，显露涉及的是机密性。
纵观从不同的角度对信息安全的不同描述，可以看出两种描述风格。
一种是从信息安全所涉及层面的角度进行描述，大体上涉及了实体（物理）安全、运行安全和数据（信息）安全；一种是从信息安全所涉及的安全属性的角度进行描述，大体上涉及了机密性、完整性和可用性。
从上述定义中总结，信息安全的含义就是就是最大限度地减少数据和资源被攻击的可能性。
1.2　网络安全现状对许多网络用户而言，知道面临着一定的威胁。
但这种威胁来自哪里、究竟有什么后果，并不十分清楚。
一般来说，对普通的网络用户来说，面临的安全问题主要有以下几个方面。
1.2.1　病毒问题这是广大用户最了解的一个安全问题。
计算机病毒程序很容易制造巨大的破坏，其危害已被人们所认识。
从前的单机病毒就已经让人们谈毒色变了，通过网络传播的病毒无论是在传播速度、破坏性和传播范围等方面都是单机病毒所不能比拟的。
目前全球已发现将近10万余种病毒，并且还在以每天10余种的速度增长。
有资料显示，病毒威胁所造成的损失占网络经济损失的76%，仅“爱虫”病毒发作在全球所造成的损失，就达96亿美元。
谈到病毒问题还包括特洛伊木马（Trojan Horse）和蠕虫（Worms）问题。
这两种程序不是严格的病毒，但不仅和病毒的危害性相当，而且一般也会伴随着病毒一起向用户发起攻击。
特洛伊程序一般是由编程人员编制的，它提供了用户所不希望的功能，这些额外的功能往往把预谋的功能隐藏在公开的功能中，掩盖其真实企图。

蠕虫则是一个或一组程序，它可以从一台机器向另一台机器传播。
与病毒不同的是，它不需要修改宿主程序就能传播。
另外，病毒的生命周期正在无限制的延长。
计算机病毒的产生过程可分为：程序设计一传播一潜伏一触发一运行一实行攻击。
从2006年主要计算机病毒发作频率和变种速度看，病毒的生命周期延长的趋势十分明显，这主要是由于病毒载体的增多造成的。
无线上网技术、蓝牙、手机短信服务、IM聊天、电子邮件木马捆绑、BLOG中隐藏的跨站攻击代码、免费音频和视频中的病毒嵌入等都会寄存病毒代码，而变种和交叉感染的存在，都使得病毒从生成开始到完全根除结束的时间大大延长。
1.2.2　非法访问和破坏黑客攻击已有十几年的历史。
黑客技术对于许多人来说已经不再高深莫测，黑客技术逐渐被越来越多的人掌握和发展，目前，世界上有20多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用以及系统的一些漏洞，因而系统、站点遭受攻击的可能性就变大了。
尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，是网络安全的主要威胁。
黑客活动几乎覆盖了所有操作系统，包括UNIX、Windows NT、VMS及MVS等。
黑客攻击比病毒破坏更具目的性，因而也更具危害性。
Yahoo!、Amazon等国际著名网站“被黑事件”早已不是新闻。
1.2.3　管理漏洞网络系统的严格管理是企业、机构和用户免受攻击的重要措施。
事实上，很多企业、机构和用户的网站或系统都疏于这方面的管理。
据1T界企业团体ITAA的调查显示，美国90%的IT企业对黑客攻击准备不足。
目前，美国75%～85%的网站都抵挡不住黑客的攻击，约有75%的企业网上信息失窃，其中25%的企业损失在25万美元以上。
此外，管理的缺陷还可能出现系统内部人员泄露机密或外部人员通过非法手段截获而导致机密信息的泄漏，从而为一些不法分子制造了可乘之机。
1.2.4　网络的缺陷及漏洞因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的TCP／IP缺乏相应的安全机制，而且因特网最初的设计考虑的是该网不会因局部故障而影响信息的传输，基本没有考虑安全问题，因此它在安全可靠、服务质量、带宽和方便性等方面存在问题。
此外，随着软件系统规模的不断增大，系统中的安全漏或“后门”也不可避免的存在，比如人们常用的操作系统，无论是Windows还是UNIX几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、应用软件等都被发现存在安全隐患。
可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。
1.3　网络安全防御体系通俗地说，网络信息安全与保密主要是指保护网络信息系统，使其没有危险、不受威胁和不出事故。
从技术角度来说，网络信息安全与保密的目标主要表现在系统的保密性、完整性、可靠性、可用性、不可抵赖性和可控性等方面。
1.3.1　可靠性可靠性是网络信息系统能够在规定条件下和规定时间内完成规定功能的特性。
可靠性是系统安全的最基本要求之一，是所有网络信息系统的建设和运行目标。
网络信息系统的可靠性测试主要有三种：抗毁性、生存性和有效性。
第一，抗毁性是指系统在人为破坏下的可靠性。
比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。
增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。
第二，生存性是在随机破坏下系统的可靠性。
生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。
这里，随机性破坏是指系统部件因为自然老化等造成的自然失效。
第三，有效性是一种基于业务性能的可靠性。

有效性主要反映在网络信息系统部件失效情况下，满足业务性能要求的程度。
例如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。
可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性和环境可靠性等方面。
第一，硬件可靠性最为直观和常见。
第二，软件可靠性是指在规定的时间内，程序成功运行的概率。
第三，人员可靠性是指人员成功地完成工作或任务的概率。
人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。
人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。
因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。
第四，环境可靠性是指在规定的环境内，保证网络成功运行的概率。
这里的环境主要是指自然环境和电磁环境。
1.3.2　可用性可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。
可用性是网络信息系统面向用户的安全性能。
网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。
可用性一般用系统正常使用时间和整个工作时间之比来度量。
可用性还应该满足以下要求：身份识别与确认、访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问。
包括自主访问控制和强制访问控制）、业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞）、路由选择控制（选择那些稳定可靠的子网，中继线或链路等）、审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时采取相应的措施。
审计跟踪的信息主要包括事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。
1.3.3　保密性保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。
保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。
常用的保密技术包括：防侦听（使对手监听有用的信息）、防辐射（防止有用信息以各种途径辐射出去）、信息加密（在密钥的控制下，用加密算法对信息进行加密处理。
即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息）、物理保密（利用各种物理方法，如限制、隔离、掩蔽和控制等措施，保护信息不被泄露）等。

编辑推荐

版权说明