



网络信息安全与防范策略研究

Research on network information security and prevention strategy

佟敏¹, 张传博¹, 刘乃豪²/TONG Min¹, ZHANG Chuanbo¹, LIU Naihao²

1. 吉林吉大通信设计院股份有限公司 长春 130012;

2. 吉林大学通信工程学院 长春 130012

1. Jilin Jlu Communication Design Institute Co., Ltd., Changchun 130012, China;

2. College of Communication Engineering, Jilin University, Changchun 130012, China

摘要:随着网络的高速发展和普及,网络安全问题逐渐得到重视。首先介绍了影响网络信息安全的主要原因和常见的网络安全问题,基于此,提出了保护网络信息安全的措施。

关键词:网络信息安全;防范策略;网络技术

Abstract: With the rapid development and popularization of Internet, the issues of network security have been paid attention. Firstly, the main reasons that impact the network information security and the common network security problems were introduced, based on this, the measures how to protect the network information security were put forward.

Key words: network information security, prevention strategy, network technology

1 引言

随着 Internet 技术的迅速发展和网络的大规模普及,人们已逐步进入互联网时代。网络已经无所不在地影响着社会的经济、政治、文化、军事和社会生活的方方面面。在互联网建设初期,网络运营商和使用者更关注网络的方便性和可用性,并未注意到网络安全的重要性。近年来,在全球范围内,针对重要的信息资源和基础网络设施的入侵行为数量在持续上升,这对国家信息安全、经济发展、社会稳定造成了极大的影响和威胁。网络安全已经成为了当今世界共同关注的焦点问题。网络安全是为了防范计算机网络硬件、软件、数据被偶然或蓄意地破坏、篡改、窃听、假冒、泄露、非法访问以及保护网络系统持续、有效工作的综合。

2 网络信息安全

2.1 影响网络信息安全的主要原因

(1) 应用软件的漏洞

网络应用软件由软件工程师编写,虽然软件在商用之前经过多方面的测试,但是仍然不可避免地存在缺陷和漏洞,这些缺陷和漏洞成为黑客攻击的主要目标,黑客攻击事件屡见不鲜,造成的损失巨大,这都是因为网络安全措施不完善而导致的。部分软件开发人员为了自我方便而在开发时设置“后门”,一旦被不法之徒利用,后果将十分严重。

(2) 黑客攻击

黑客是目前网络信息安全最大的威胁,黑客掌握一定的网络技术,从黑客活动产生的影响来衡量,黑客可以分为破坏性和非破坏性两类。破坏性黑客一般是出于经济目的或其他社会性目的而攻



击网络、入侵他人电脑、盗取重要资料和信息、致使网络瘫痪等,有比较严重的破坏性。非破坏性黑客一般出于好奇、恶作剧、彰显其网络技术能力等原因,以不正当的手段入侵网络,一般会扰乱系统的正常运行,但不会造成严重破坏。

(3)计算机病毒

计算机病毒首次大规模爆发出现于20世纪90年代,主要攻击目标为计算机终端,并引起了世界范围内的恐慌。计算机病毒隐蔽性高、蔓延范围广、破坏力强,这之后出现的计算机病毒如“爱虫(I Love You)”“红色代码(Code Red)”“冲击波(Blaster)”“巨无霸(Sobig)”等皆造成了百亿美元的损失。当计算机终端感染病毒后,会出现运行缓慢、工作效率降低等问题,严重者会导致数据被盗、文件丢失,甚至会造成计算机硬件的损坏。

(4)网络管理漏洞

从网络安全管理角度看,管理问题是网络安全问题的首要问题。目前,大多数网络攻击能够得逞是因为网络管理人员管理策略不严格、管理意识松懈。许多安全管理漏洞只要增强安全意识就可以避免,因此,网络安全技术是保证网络安全的基本条件,而最有效的网络安全保障措施则是网络安全管理。

2.2 常见的网络安全问题

由于社会信息化的高速发展,互联网已经融入每个人的生活,网络形式多种多样,各种终端设备分布广泛,网络交易日趋频繁,这使得网络更容易受到来自黑客、病毒、木马和恶意软件的攻击。

(1)信息窃取

在未被授权的情况下,使用非法手段将信息透露给第三方以牟取利益,严重破坏了系统的保密性。目前,网络交易十分频繁,信息窃取往往会对个人、企业和社会造成巨大的损失。常见的信息窃取手段主要有病毒、木马、软件后门、钓鱼网站、网络监听、物理入侵等。

(2)DoS 攻击

DoS(Denial of Service,拒绝服务)攻击是指故意利用协议缺陷或直接通过野蛮手段耗尽被攻击目标的处理能力、带宽资源等,致使目标计算机或网络无法提供正常的服务或资源访问,使被攻击系统停止响应甚至崩溃,造成网络瘫痪。

(3)网络滥用

合法用户逾越权限滥用网络,造成不必要的网络安全威胁,主要包括外连/内连某些非法网站、网络终端滥用、业务滥用等。

(4)垃圾邮件

邮件地址具有公开性和可广播性,一些不法分子利用邮件地址的这些特性,强行将电子邮件发到他人邮箱进行社会活动,如商业诈骗、邪教传播等。

(5)间谍软件

间谍软件与病毒类似,都具有潜伏性,不同的是:间谍软件的主要目的不是为了破坏网络系统,而是为了盗取系统资料或个人信息,造成的损失也十分巨大。

(6)计算机信息网络犯罪

计算机网络犯罪通常采取非法手段入侵网络系统,实施贪污、诈骗、盗窃和金融犯罪等活动。网络是一个开放和共享的平台,它在为社会发展带来便利的同时,也降低了互联网技术学习的门槛,这也为计算机网络犯罪提供了一定的条件。

3 网络信息安全措施

3.1 数字加密与数字签名

(1)数字加密技术

数字加密技术是网络安全的核心技术之一,也是目前应对网络安全较为有效的措施之一,数据通过适当的加密管理机制可以有效地提高网络的安全性。目前,数字加密技术主要分为数据传输加密、数据存储加密、数据完整性鉴别以及密钥管理技术4种。在具体的网络安全应用中,通常采用的加密形式主要有对称密匙和公开密匙,具体采用何种加密算法要视具体应用环境和系统而定。

(2)数字签名技术

数字签名技术又被称为公钥数字签名或者电子签章,是一种类似于写在纸上的、普通的物理签名,但是使用了公钥加密技术,可用于鉴别数字信息。数字签名通常成套存在,定义两种互补的运算,一个用于签名,另一个用于验证。数字签名是非对称密钥加密技术与数字摘要技术的应用。

3.2 访问控制

对网络资源的访问进行授权管理,使整个计算机系统能够在合法的范围内使用。利用用户身份及

其所归属的某项定义组来限制用户对某些信息项的访问,或限制其对某些控制功能的使用。

3.3 防火墙技术

防火墙技术由来已久,目前防火墙一般是指由软件和硬件设备组合而成的专有安全设备。防火墙在内网和外网、专网和公网之间设置屏蔽,属于隔离控制技术,能够阻挡来自外部的网络入侵。

防火墙包括网络防火墙和计算机防火墙两种。网络防火墙是指在外部网络和内部网络之间设置的防火墙,这种防火墙主要通过静态或动态数据分组过滤,检测进入信息的协议、目的地址、端口(网络层)及被传输的信息形式(应用层)等,滤除不符合规定的外来信息。网络防火墙也对用户网络向外部网络发出的信息进行检测。

3.4 网络入侵检测技术与网络入侵检测系统

(1) 网络入侵检测技术

入侵检测是指通过对行为、安全日志、审计数据以及其他网络上可以获得的信息进行操作,检测到对系统闯入或闯入的企图。入侵检测是检测和响应计算机误用的学科,其作用包括威慑、检测、响应、损失情况评估、攻击预测和起诉支持。

(2) 网络入侵检测系统

入侵检测系统(IIntrusion Detection System,IDS)是对计算机网络系统的非授权检测,包括系统外部入侵检测和内部非授权行为检测,是一种用于检测计算机网络中违反安全策略行为的技术。现有入侵检测系统的检测速度远小于网络的传输速度,入侵检测系统基本都采用旁路加载,一般只能进行检测和记录,虽然也可被设置成主动防御,但是存在误报的可能性。

3.5 隔离技术

在需要保护的内网和公共网络的外网之间的安全解决方案中,存在着两种隔离方式:物理隔离和逻辑隔离。

(1) 物理隔离

物理隔离将内网与外网在物理层面进行阻断,不进行任何直接或间接的连接,可确保内网免受外网的非法网络攻击。同时,物理隔离也为安全等级较高的计算机、信息系统及其他终端划定了明确的安全边界,使得网络可管、可控。目前,物理隔离技术已成为网络安全保密体系中不可缺少的重

要手段。

(2) 逻辑隔离

逻辑隔离主要通过各种逻辑隔离器实现,被隔离的两个网络在物理层面仍然是连接的,但因为有逻辑隔离器的存在,两个网络之间不存在数据通道,在两个逻辑隔离区域之间不能直接进行数据交换。逻辑隔离器使用的技术手段包括协议转换、数据格式转换和数据流控制等。

4 结束语

计算机网络的安全性越来越受到重视,网络环境的复杂性、多变性以及信息系统的脆弱性决定了计算机网络不能只依靠防火墙,而应涉及管理和应用技术等多方面。总体来看,有效的网络安全管理可以极大地提高网络安全系数,网络安全绝不只是技术问题。计算机网络技术的发展日新月异,网络安全防范策略也将不断提升。

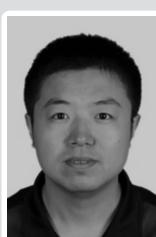
参考文献:

- [1] 葛秀慧.计算机网络安全管理[M].北京:清华大学出版社, 2003.
- [2] 张琳, 黄仙姣.浅谈网络安全技术[J].电脑知识与技术:学术交流, 2006(4):101-102.
- [3] 周小华.计算机网络安全技术与解决方案[M].杭州:浙江大学出版社, 2008.

作者简介



佟敏(1976-),女,吉林吉大通信设计院股份有限公司高级通信工程师,主要研究方向为光纤与光通信和网络安全。



张传博(1987-),男,吉林吉大通信设计院股份有限公司助理工程师,主要研究方向为光纤与光通信和网络安全。

刘乃豪,吉林大学通信工程学院在读研究生,主要研究方向为光纤与光通信。