文章编号:1004 - 5694(2001)增- 0150 - 03

建立动态实时统一的计算机网络安全系统

张德媛,张德明
(重庆邮电学院,重庆 400065)

摘 要:当今计算机网络发展神速,而网络的安全性却得不到保障,面对这种窘迫的局面,我们不得不慎重考虑建立一个动态、实时、统一的计算机网络安全系统,指出了系统安全隐患的来源,提供了计算机网络安全系统的内容。

关键词:计算机网络;安全系统;实时
中图分类号:TP393.08 文献标识码:B

Establish a Dynamic and Real-time Safety System of Computer Network

ZHANG De-yuan, ZHANG De-ming
(*Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: Today computer network is developing at an amazing speed whereas its safety is hard to be guarded. In order to cope with such a predicament, the authors hope to establish a dynamic and real-time safety system of computer network by pointing out some potential problems and providing the main features of the network safety system.

Key words: computer network; safety system; real time

随着计算机与网络通信技术的发展,越来越多的企业活动建立在计算机网络信息系统基础上。而 Internet 在世界范围内的迅速普及,使企业内部网络联入 Internet 的要求越来越迫切。Internet 的电子商务、网上银行等商务和经济活动的增多对网络系统安全提出了更高的要求,解决这些问题的难度也越来越大。来自企业内部和外部的非法访问和恶意入侵事件时有发生,并呈不断上升的趋势。这不仅影响了计算机网络系统的实际应用,还极大地动摇了用户的信心,而且越来越多的企业在建设自己网络系统的同时,不得不考虑网络的安全问题。

1 网络安全隐患

为了解决网络系统的安全问题,必须首先了解安全问题的来源,即:威胁来自何处? 计算机网络信息系统的安全问题主要来源于以下几个方面。

(1) 非法侵入。包括来自企业内部和外部的非法入侵,导致数据的丢失和泄密、系统资源的非法占有等;其手段五花八门,既有传统的密码窃取、强力侵入,又有"特洛伊木马"、路由攻击、身份截取等。

(2) 计算机病毒。导致系统的性能下降甚至崩溃,系统数据的丢失等;尽管计算机病毒已有十余年的历史,但它并不因为病毒防治手段的加强而销声匿迹,反而应用各种新的计算机技术而愈演愈烈,去年 4 月 26 日 CIH 病毒的攻击,国内有 3 千台计算机被破坏。

(3) 拒绝服务攻击 非法占用系统资源,导致系统服务停止甚至崩溃;从技术角度来说,1988 年轰动一时的"蠕虫"程序就是拒绝服务攻击的一个典

· 作者简介:张德媛(1953—),女,四川万源人,重庆邮电学院图书馆馆员,从事计算机应用方面的研究。

型；常见的拒绝服务攻击还包括电子邮件炸弹、PING 炸弹、UDP 炸弹等。

(4) 计算机网络系统安全威胁的另一个重要来源是人们通常将网络系统作为一项纯粹的技术或工程来实施，缺乏统一的安全管理策略和专门的网络安全管理人员。网络信息系统的安全环境是非常复杂并且不断变化的，但相当多的系统管理员只将精力集中于帐户的维护、系统日志审查和网络规范的设计及调整上面，很少有人去研究网络安全状态的发展变化、网络入侵手段、系统安全防范措施、安全策略，甚至更少有时间去监控网络的实际活动状态、入侵迹象或系统的错误使用等，这就导致了网络系统实际的安全状态和预期标准之间相差很远。

最终用户只期望方便、快捷、高效地使用网络，最大限度地获取有效的信息资源，很少考虑实际存在的风险和低效率。他们侧重于类似 Netscape Navigator、Internet、Explorer、Word 等应用软件的操作上面，很少接受密码保管、密码设置、信息保密、人为破坏系统和篡改敏感数据等有关安全常识的培训。

从本质上来说，计算机网络系统的安全隐患都是利用了网络系统本身存在的安全弱点，而系统在使用、管理过程中的误用和漏洞更加剧了问题的严重性。

2 建立实时动态统一的网络安全系统

2.1 计算机网络安全系统的内容

国际标准化组织(ISO)将计算机安全定义如下：为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然或恶意的原因遭到破坏、更改和泄露。计算机安全的内容应包括两方面：物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全包括信息完整性、保密性和可用性。保密性指高级别信息仅在授权情况下流向低级别的客体；完整性指信息不会被非授权修改，信息保持一致性等；可用性指合法用户的正常请求能及时、正确、安全地得到服务或回应。网络系统的安全涉及平台的各个方面，按照网络 OSI 的 7 层模型，网络安全体现在信息系统的以下几个层次。

(1) 物理层。物理层信息安全主要包括防止物理通路的损坏，通过物理通路窃听，对物理通路的攻击(干扰)等。

(2) 链路层。链路层的网络安全需要保证通过网络链路传送的数据不被窃听，主要采用划分 VLAN、加密通信等手段。

(3)网络层。网络层的安全需要保证网络只给授权的客户提供授权的服务，保证网络路由正确，避免被拦截或窃听。

(4)操作系统。操作系统安全指保证客户资料安全和操作系统访问控制的安全，同时能够对该操作系统上的应用进行审计。

(5)应用平台。应用平台指建立在网络系统之上的应用软件服务，如数据库服务器、电子邮件服务器、Web 服务器等，由于应用平台的系统非常复杂，通常采用多种技术(如 SSL 等)来增强应用平台的安全性。

(6)应用系统。应用系统完成网络系统的最终目的是为用户服务，应用系统的安全与系统设计和实现关系密切。应用系统通过应用平台提供的安全服务来保证基本安全，如通信内容安全、通信双方的认证、审计等。

2.2 网络安全系统的评估分析

网络安全系统的现实情况是：系统管理人员部署了一些安全措施，如防火墙、身份认证等，因此人们就存在一种相对安全的错觉：认为已经控制了系统的安全风险。实际上这只能解决某些理论上的安全问题，没有对安全需求的描述，没有对系统入侵的研究，没有对当前系统安全风险的评估和分析，也没有对实施效果的分析，随着时间的推移，网络信息系统的安全状态会显著下降。这种变化一般是由工作环境和包括企业正常活动在内的大量变化的网络事件造成的。因此，计算机网络信息系统的安全绝对不是一个静态、封闭的过程。

基于这种认识得出的基本结论是：真正的网络安全体系应当是构建在采用动态、实时、统一的可适应安全管理模型基础之上，将被动防守的安全策略和手段转变为对自身网络信息系统的自动探测，通过探测、监控和响应强制实施群体安全策略。其核心目的是：永远在损失之前发现系统安全隐患。

从更为精细的角度看，建立计算机网络安全系统应该包括以下几个方面。

(1) 安全风险评估和分析。依据安全策略的要求，定期检测主机和网络的安全状态，并可以按照用户设定，自动分析系统安全风险设置，并提供相应的分析报告以支持安全决策。

(2) 系统实时监控和响应技术。系统实时监控和分析。对网络活动、事件和状态进行实时监听和审计，并对入侵迹象、误操作和其他可疑动作进行实时分析和控制；从技术的角度来说，安全风险的量度标准包括实际风险、基准风险和残留风险等；从系统的角度来说，还包括安全意识等级、安全响应等级等。

安全系统响应。根据监控、漏洞探测、风险评估得到的分析报告，为用户提供快速检测非法入侵行为并提供反击手段。实时响应动作可以是简单的安全警告、数据记录，也可以是动态设置，网络甚至切断连接；事后的响应针对系统在监控和探测过程中发现的弱点，采取相应的对策，如配置防火墙、对关键数据的传输加密、修改安全参数设置、修补各种安全相关程序等。

(3) 操作系统的安全。包括操作系统主机和备份异地存放，操作系统备份，应急盘的制作和备份。

(4) 网络及通信服务的安全。采取网络备份，用内部专用网实现数据的传输，另外，防火墙技术虽然存在局限性，但对于系统内部网络来讲，仍不失为一种网络安全措施。

(5) 应用系统及数据库系统的安全。采用独特的随机密钥算法对数据库用户口令自动加密；充分利用数据库基于角色、分布权限的安全管理机制；限制口令掌握范围；采用先进的数据库安全技术，如动态链表结构、共享内存机制、多进程机制；本地和异地数据库多种线索协调机制等。

(6) 数据备份和恢复技术。对一个运行系统来说，应用系统数据是核心，它的安全尤为重要。采用磁带备份，磁带异地存放；磁盘阵列；异地双机远程数据备份等技术，是网络数据安全的重要手段。

(7) 计算机病毒防治技术。加强对外来软件和磁介质的管理，在没有进行计算机病毒检查之前，严禁上机应用操作；严禁在业务用机上做与业务无关的作业；建立自己的网络系统，使计算机应用系统运行在封闭的环境中，杜绝病毒的进入；根据病毒发作的规律建立病毒预告防范体系等。

(8) 身份认证技术：① 双重认证：即采用两种形式的证明方法，来保证用户的身份认证；② 数字证书：这是一种检验用户身份的电子文件，这种证书可以授权购买，提供更强的访问控制，并具有很高的安全性和可靠性；③ 其他还有智能卡和安全电子交易(SET)等身份认证技术。

(9) 信息的加、解密技术。加密是一种最基本的安全机制，它能防止信息被非法获取，加密机制是在网络环境中对抗被动攻击的行之有效的安全机制，也是建立动态、实时网络安全系统的重要部分。

(10) 网络的存取控制技术。应用网络提供的一些功能诸如远程登录、文件传送等工作，给入侵者提供了闯入的可能。为此，一方面可以用路由器控制外界对此路由器作为网关的局域网诸如 rlogin、telnet、ftp 等网络服务的信息流量，对一些非法访问进行控制。另一方面，对已闯关者，利用 UNIX 帐号管理功能，对注册口令次数严加控制，终端加锁，禁止 FTP 匿名传送，禁止使用 TFTP 等。

3　结束语

计算机网络信息系统的安全决不是一个静态、封闭的过程。真正的网络安全体系应当构建在采用动态、实时、统一的可适应安全管理模型基础之上，将被动防守的安全策略和手段转变为对自身网络信息系统的自动探测，通过探测、监控和响应强制实施群体安全策略。其核心目的是：永远在损失之前发现系统安全隐患。

参　考　文　献

[1] 熊桂喜，王小虎等译. 计算机网络[M]. 北京：清华大学出版社，1998.

[2] 雷震甲，马玉祥. 计算机网络[M]. 西安：西安电子科技大学出版社，1995.

[3] 张彩莱. 网络安全与身份验证[J]. 网络安全技术与应用，2001，(4)：25-29