万维贸易有限公司企业网络规划建设

刁慧茹
（内蒙古师范大学青年政治学院，内蒙古 呼和浩特 010051）

摘 要：当今社会科技水平高速发展，经济一体化、信息化、网络化已成为社会发展的方向。企业信息化建设正在逐步发展。目前，一些组织已经建立了自己的WEB服务器和门户，企业电子邮件服务系统，并推出了全面的查询、生产业务系统和EDI。大量关键数据信息存储在网络上，集中到一台服务器上。虽然它可以为用户提供方便、高效、快速、共享的条件，但由于大量用户的访问，它给网络系统带来了很多问题，网络系统的安全性尤为突出。面对系统中存在的各种安全问题和潜在威胁，需要建立一个安全可管理的安全防御系统，采用保护、检测、响应、恢复等有效的安全措施，使计算机网络系统能够安全、高效、可靠、稳定地运行。通过对企业网络安全系统的设计与实现，提高了企业网络安全系统的安全性和可靠性。同时，随着网络技术的不断发展，对网络系统的安全性提出了更高的要求。

关键词：域；网络安全；安全方案

1 企业网络安全规划与设计

1.1 明确网络系统安全策略

网络安全政策是保证企业网络安全的指导性文件。安全策略的目的是确定组织如何保护自己。一般而言，网络安全策略包括总体安全策略和具体的安全管理实现规则。总体安全战略用于构建企业网络安全框架和战略指导方针，包括分析安全需求、分析安全威胁、确定安全目标、确定安全覆盖、分配部门职责、人力资源、识别违规行为和适当的制裁措施。整体安全政策只是明确公司安全政策的整体理念，无法实施。只有在总体安全政策框架下为具体应用制定具体的安全管理实施方案，才能实现安全技术机制和管理策略。

1.2 建立网络安全模型

模型的建立可以简化复杂问题，更好地解决与安全策略相关的问题。网络安全模型的建立主要参考PPDR模型。PPDR模型是美国互联网安全系统提出的一种自适应网络安全模型。PPDR模型就是4个英文单词的头字符：Policy（策略）、Protection（防护）、Detection（检测）、Response（响应），这四个部分构成了一个动态的信息安全循环。PPDR模型的基本思想是，在统一的安全策略的控制和指导下，系统的安全应该受到各种安全技术（如防火墙、操作系统认证、加密等）的保护和控制。检测工具（如漏洞评估、入侵检测等）监控和评估系统的安全状态，通过适当的响应机制将系统调整到相对

“最安全”和“最低风险”状态。

1.3 设计原则

(1)系统、综合、整体性原则。

运用系统工程的观点和方法分析网络安全及具体措施。安全措施主要包括:行政法律手段、各种管理制度和专业措施。更好的安全措施通常是多种方法结合的结果。包括个人、设备、软件、数据等的计算机网络。这些环节在网络中的地位和影响只能从整个系统整体的角度来看待和分析,以获得有效可行的措施。

(2)需求、风险、代价平衡原则。

对于任何网络来说,绝对的安全性都是难以实现的,也不是必须的。对网络进行实际研究,结合定性和定量分析,分析网络的威胁和可能的风险,制定规范和措施,确定系统的安全策略。

(3)实用性原则。

随着技术水平的不断提高,计算机信息设备、服务器设备、网络设备的技术性能逐渐提高,价格逐渐下降。在网络设计中,我们力求掌握“足够”和“实用”的原则。网络系统采用成熟可靠的技术和设备,取得经济、实用、有效的效果。

(4)安全性原则。

从总体目标来看,设计中心的安全考虑主要是主机(包括服务器)和网络资源的安全,考虑到用户需要的安全保护功能。

1.4 系统安全方案设计

首先,划分网络层次结构。根据网络的流量模式和终端用户的分组方式,将网络分为三层:接入层、汇聚层和核心层。接入层直接连接用户,管理终端用户的网络接入,采用成本合理的设备。访问端口的数量是有保证的,可以很容易地扩展。汇聚层是多个访问层的汇聚点,需要访问性能更好的网络设备,以保证大数据传输。它主要用于访问层通信的集中处理数据,并将数据发送到核心层;核心层是网络的主干,负责数据的快速转发。

其次,在网络拓扑结构中采用了混合星型拓扑和总线拓扑的混合。接入层采用星形结构,有利于网络规模的扩大。考虑到未来可能提供的 Wi-Fi 信号和终端查询服务,在实际施工中可以在各部门配置相应的交换机;在汇聚层,每一个汇聚交换机都采用总线结构,便于逻辑结构的划分。对于核心层路由器,可以隔离广播域,减少网络风暴的形成。设计由三个路由器组成,其中两个分别连接到汇聚层,剩下的一个是互联网网络连接。考虑一个安全需求,在内部网络和外部 Internet 之间设置防火墙。这三个路由器中的每一个都相互连接以实现冗余连接。

2 办公域网络安全的实施

2.1 办公域网络安全系统总体描述

为了公司的网络和用户的安全,每个服务器和工作站都安装了杀毒软件。尽管如此,公司内部仍有网络病毒爆发,因为杀毒软件可以抵御一些病毒,但它不能拦截攻击操作系统和应用软件安全漏洞的新型蠕虫(如 SQLSlammer)。由于管理问题,一些客户端杀毒软件无法正常升级,对客户端和网络造成严重威胁。通过部署杀毒网关,杀毒墙安装在核心交换机和公司第三层交换机之间。一方面,可以适当减少网关需要过滤的数据量。另一方面,过滤网关系统本身也可以免受外界的干扰、恶性攻击。同时,服务器和工作站需要安装反病毒网关客户端。客户端的作用是保护杀毒软件无法清除的网络病毒。一旦反病毒网关的客户端因用户误操作或系统问题出现故障,反病毒网关将强制用户按照策略使用网络功能,直到客户端重新安装,起到自动管理的作用。

2.2 办公域网络的实施

根据 PPDR 模型,访问域是统一安全的。下面的测试验证了 PPDR 模型的合理性,以及通过部署反病毒网关来保护内部网访问域。在网络建设的稳定可靠方面,核心骨干节点在设计和实现过程中采用冗余连接,使用交换机隔离碰撞域和路由器隔离广播域。网络可扩展类型在接入层采用星形结构,通过交换机连接。传入的互联设备,在传输带宽上租赁高速 ADSL 租用线路,隔离广播域和冲突域,通过减少广播包间接增加有效带宽,采用分层结构保证核心层关注网络数据传输,提高数据转发速度。在安全监控管理方面,采用 VPN 技术和 VLAN 划分,增加备份数据服务器,在内部网络和外部网络之间增加防火墙,增加 UPS 对服务器正常关闭的保障,增加网络管理节点进行监控,监控网络状态或使用 VPN 远程访问。

对于企业内部网络,将企业内部三个层次的网络结构进行划分:在接入层,在汇聚层接入公司各行政部门的网络,如财务部、人事部、销售部等。在核心层连接服务器层和聚合层,以确保网络上各种应用程序对服务器组和聚合层的快速访问。为了在特定的网络实现中提供更好的安全性和减少不必要的网络流量,同一级别的每个节点都应该由 VLAN 隔离,整个网络应该由 VLAN 划分。注意路由器配置中的接口配置和动态。路由协议配置和 SNMP 协议配置。为了保证企业内部网络安全的安全,应该关闭冗余的服务和端口,避免多个应用程序之间相互影响,定期备份数据、进出口管控信息,直接禁止内部网络。

3 结束语

本文结合企业网络的特点,将企业网络划分为多个安全领域,通过安全领域的安全需求确定每个安全领域的安全策略,并提出一套安全解决方案。利用当今先进的安全设备,主动被动地防御企业网络。通过安装防病毒墙,结合缺少 PPDR 模型和防病毒软件,全面捍卫了办公领域。随着时间的推移,许多网络安全设备需要更新和升级,未来的杀毒软件将无法有效地处理越来越多的恶意程序。来自互联网的主要威胁是从计算机病毒转向恶意程序和木马。在这种情况下,所使用的特征库识别方法显然已经通过。因此,未来网络安全发展的方向应该是“云安全”。在云安全应用之后,病毒的识别和杀毒不再仅仅依赖于本地硬盘上的病毒数据库,而是依赖于庞大的网络服务来实时收集、分析和处理。整个互联网是一个巨大的“杀毒软件”。参与者越多,每个参与者就越安全,整个互联网就会更安全。

参考文献

[1]耿永彬,邢亮,唐国强.“互联网+”时代企业网络安全的思考[J].通讯世界,2017(01):58-59.

[2]回金强.企业网络规划建设应用研究[D].大连海事大学,2013.

[3]李涛,等.信息系统容灾抗毁原理与应用[M].北京:人民邮电出版社.2007.

作者简介:刁慧茹,内蒙古师范大学青年政治学院信息工程系 17 级计算机应用技术。