

新媒体网站安全技术架构与安全体系建立研究

谷 默

(山东广播电视台新媒体中心, 山东济南 250014)

摘 要: 随着网络技术的不断发展, 网站信息系统安全已成为日益关注的问题。对于新媒体网站而言, 同样面临着漏洞、病毒以及木马等因素的威胁, 给网站的安全运营造成了很大困难。本文根据笔者多年的理论学习与实践经验, 就新媒体网站安全技术架构与安全体系建立问题, 从其自身角度进行了深入探讨。

关键词: 新媒体网站; 安全技术架构; 安全体系

中图分类号: TP309 **文献标识码:** A **文章编号:** 1003-9767 (2013) 01-0015-02

1. 引言

新媒体网站的信息安全问题涉及到终端系统、网络体系以及服务应用管理制度等多个方面, 如何从体系与整体的角度来考虑对信息以及信息系统的保障, 是现阶段我们急需解决的问题。尤其对于新媒体网站而言, 受到其软硬件环境复杂、应用类别多等因素的限制, 给安全技术架构与安全体系建立等工作造成了很大困难。因此, 如何从体系的高度来探讨新媒体网站整体性安全技术的构架, 为工程的安全保障提供整体性的解决方案与技术路线, 对确保新媒体网站信息与信息系统的安全发挥着非常重要的作用。

1.1 新媒体网站安全技术架构

安全问题是新媒体网站运营的核心问题, 为确保网站的安全运营, 不仅应加强安全管理与信息安全法规建设, 还应采取一系列的网站安全技术来确保新媒体网站的安全运营。因此, 可以通过构建具有高度可信的信任系统与行为监控系统来确保新媒体网站整体信息安全解决方案与技术的实现, 从而有效避免网站所遭受的安全威胁。在具体的操作过程中, 可通过以下两种网络信息安全技术的构建来确保网站的安全运营。

1.1.1 防火墙技术的构建

防火墙是指处于 LAN 和 Internet 之间, 由软硬件设备共同组成的一种安全防范系统。该系统能有效控制内外部网络之间的信息交流, 通过提供接入控制与审查跟踪来形成一种有效的访问控制机制。就现有的防火墙技术而言, 主要包括数据包过滤和代理服务技术两大类。

在进行安装防火墙时, 网络安全管理人员需要对防火墙进行设置来确保拒绝或接受某种类型数据的传输。因防火墙能对进出的数据信息进行有选择性的过滤, 所以能有效避免对其进行的有意或无意的攻击, 从而确保了新媒体网站的安全。

将代理服务器与过滤防火墙结合起来使用是一种有效解决新媒体网络安全的方法。通过运行代理服务器的程序, 来实现网络提出的服务请求, 通过对进出数据的筛选, 能有效确保新媒体网站的信息安全。对于防火墙技术的构建而言, 同时也存在着以下两种局限性: (1) 只能防止经由防火墙的攻击, 不能避免网络内部用户对新媒体网站的攻击, 同时还不能有效防止数据驱动式的攻击。(2) 不能保证数据的秘密性, 并且不能对数据进行鉴别, 不能完全避免网站不受病毒的攻击, 同时对经病毒感染的软件及文件起不到良好的防护作用, 只能确保内部网络不受主动入侵与攻击。

1.1.2 数据加密技术的构建

加密技术是网站的一种最基本的信息安全防护措施, 在现有的条件下通常将该技术分为对称加密与不对称加密两大类。对于这两种加密技术而言, 对称加密技术具有加密速度快、效率高的特点, 被广泛用于新媒体网站信息加密处理工作。但该种加密技术的缺点是密钥的传输易被截获, 难以实现大量信息的安全管理。对于非对称加密技术而言, 能有效避免对称加密技术因密钥数量过大而导致的密钥泄露与管理工作困难等, 具有良好的保密性。但该种加密技术的缺点是算法复杂、加密速度慢, 在现阶段的新媒体网站信息安全处理过程中通常以两种技术相结合的形式使用。

1.1.3 网络安全域划分

在新媒体网站数据层面, 通过网络安全与划分, 能将数据库隐藏在安全区域, 并且同时采用安全加固技术对其进行安全配置, 对其访问权限进行严格限定, 能最大限度地保护新媒体网站数据库的安全。值得一提的是, 为了确保网站数据库信息的安全, 对于重要的数据, 应增加数字签名与验证、签名回执等来确保数据的安全。对于一些关键数据还应采取增加交叉认证, 并定期对数据进行备份, 以有效确保新媒体网站的信息安全。

1.2 新媒体网站安全体系建立

新媒体网站的安全管理不是一成不变的, 它是一个动态变化的过程。随着网络安全攻击与防范技术的不断发展, 新媒体网站也应不断调整网站安全策略, 通过建立起完善的安全管理机制来实现安全技术与管理工作的有机结合。在具体的操作过程中, 应做到以下几个方面:

1.2.1 加强新媒体网站安全制度的建立

建立新媒体网站安全体系, 首先应制定出一套切实可行的网站安全制度, 明确技术管理规范。为了应对新媒体网站安全的脆弱性, 除了应在网络安全设计上增加安全服务功能与加强保密措施外, 还应将工作重心放在加强新媒体网站的安全管理, 具体工作内容包括以下几个方面: (1) 严禁涉密、涉密网机器的混用, 对于非涉密机器而言, 不允许运行涉密信息; (2) 严格按照安全域与安全登记的划分, 制定相应的安全保密制度; (3) 对于不同的安全域与安全带等级之间, 必须使用相应的安全交换系统才能实现交流; (4) 只有在确保新媒体网站入网设备都安全的情况下才能确保整个网络的安全。

1.2.2 明确新媒体网站安全管理人员的职责

在该项工作的开展过程中, 应坚持人人负责、层层负责的原则, 完善由第一负责人负责的网站安全管理体系。同时, 应注重安全体系建设的实施, 在安全使用过程中取得相关部门的配合, 引导整个部门

电子设备电磁兼容设计研究

刘丽平

(南京机电职业技术学院, 江苏南京 210037)

摘要: 本文在分析电子设备电磁干扰源的基础上, 从PCB设计、屏蔽设计滤波设计以及接地设计等方面探讨了电子设备电磁兼容设计的方法。

关键词: 电子设备; 电磁兼容; 设计

中图分类号: TP31 文献标识码: A 文章编号: 1003-9767 (2013) 01-0016-02

1. 前言

近年来, 随着电子技术发展进程的不断推进, 电子设备已广泛应用于人们社会生活的各个领域, 成为推动社会经济发展的重要动力。然而, 电子设备制造技术在快速发展的同时, 电子系统的精密度、复杂度亦越来越高, 使用的频谱越来越宽。在工作运行时, 一电子系统可能需要几副甚至十几副工作在不同波段的天线来接收或发射电子信号, 其周围空间产生的电磁场电平非常强大, 进而导致系统内相互电磁干扰问题日益突出, 整个系统将无法正常工作。因此, 电子设备的电磁兼容设计已成为电子设备设计工作者探讨的重要课题。

本文笔者结合工作实践, 在分析电子设备电磁干扰源的基础上, 探讨了电子设备电磁兼容设计的方法。

2. 电子设备电磁干扰源的分析

电子设备电磁干扰源可以分为内部干扰和外部干扰, 两种干扰形

式都是影响电子设备正常运行的主要因素。

2.1 内部干扰

内部干扰主要指电子设备内部各元器件之间在相互作用影响下产生的干扰现象, 主要包括如下几种干扰形式:

电子设备工作电源在各线路上分布的电容以及绝缘电阻等元器件发生漏电现象而引发的干扰。

大量的无线电信号通过电源、传输导线以及地线时因阻抗发生互相耦合现象, 或导线之间的互感现象等等, 都容易造成电子设备的电磁干扰。

设备或系统内部的某些元器件因工作运行时间过长而导致发热现象, 对元器件本身或其他元器件的稳定造成的干扰影响。

电子设备内部高电压和大功率组件产生额电、磁场因发生耦合现象而对其他部件造成的干扰。

不断提升系统的安全等级。对于网站安全管理人员而言, 除应具有扎实的专业理论基础外, 还应具有丰富的实践工作经验, 熟悉网站的网络结构, 并根据网站自身特点制定相应的安全技术策略。同时, 还应确保网站安全管理工作的明确分工, 由安全操作人员来负责安全系统的具体实施; 信息编辑人员负责信息的采集、编辑与审核, 以确保信息的完整性、一致性与准确性。同时, 还应成立一个网站安全管理专家小组, 对于一些网站重大安全问题提出有针对性地应对决策。

1.2.3 建立应急响应机制

在新媒体网站安全管理工作过程中, 除了应加强安全制度建立、替身安全管理人员职责外, 还应从安全管理人员培养、安全管理制度制定等方面加强制定网络安全管理制度方面加强应急响应机制的建立, 以确保新媒体网站的安全运营。

1.2.4 建立网站信息安全检查监督与激励机制

在该项工作的开展过程中, 应根据相关已确立的标准、法规与制度, 定期开展信息安全检查工作, 将网站信息安全保障工作落到实处。同时, 还应建立起相应的责任通报制度, 对检查过程中安全问题与安全隐患, 应明确责任人, 并限期整改。此外, 还应建立起相应的激励机制, 从网站信息安全管理人才引进、培养等方面加强人员结构优化工作的开展, 以形成相应的人才梯队, 同时重点加强系统运行人员技能的培养, 不断提升他们的自我操作能力与应急能力。

1.2.5 做好新媒体网站信息安全培训工作

新媒体网站的安全运行与维护需要有一支具有较高政治素质与职业道德水准的技术队伍做支撑。为此, 应建立一套完善的技术培训体系, 使之更贴近于实际业务与技术前沿, 提升操作人员的理论与实践操作水平, 真正实现新媒体网站的全方位安全防范。

1.2.6 加强分布式多层次网站安全体系结构的构建

新媒体网站安全运营状况表明, 网站安全结构体系单靠防火墙、木马病毒防护软件等不能有效解决网站安全问题, 为此应加强对于传统安全体系结构的改进与新型安全体系的构建, 以有效提升网站的安全性与抗攻击能力。

2. 结语

综上所述, 随着网络技术的不断发展, 网站安全问题将会变得更加突出。对于新媒体网站安全技术架构与安全体系建立而言, 是一个复杂而又系统的工程, 安全问题还有赖于对相关课题的进一步研究与学习。在今后的工作过程中, 应充分利用现代化网络安全技术, 对网络安全构建技术不断完善与创新, 并充分利用相关法律法规与政策, 以促使新媒体网站的安全稳定运营。

参考文献:

- [1] 张伟, 袁敏, 夏勇. 视听新媒体分发网络安全控制架构研究 [J]. 世界广播电视, 2010, (10): 144-147.
- [2] 孙丽娜. “坚而后论工拙”理念与新媒体网站设计关系初探 [J]. 美术教育研究, 2011, (5): 137-138, 140.