计算机网络安全与防护手段分析

沈虹

哈尔滨铁道职业技术学院　黑龙江　哈尔滨　150000

[摘　要]随着计算机技术的快速发展，以及互联网的广泛应用，当前社会发展已经步入网络化阶段。在信息化发展模式下，计算机网络的安全已经成为社会稳定发展的重要保障。本文从当前互联网发展状况出发，探索计算机网络安全的重要性与防护手段，以供讨论与参考。

[关键词]计算机；网络安全；防护手段

【DOI】10.12252/j.issn.2096-6261.2020.02.035

引言

在信息技术和互联网快速发展的今天，网络技术已经成为一种重要的计算机应用模式。人们在充分利用互联网高效便捷的特性时，也面临着许多的安全问题。网络安全问题既影响到了人们在信息化时代的日常生活，也影响到了金融业、证券业、电子政务、电子商务等诸多经济生产行业和社会运转体系。要想保障整个网络系统的安全运行和有效运行，最重要的是提高网络的安全性、完整性和可用性。因此，提高互联网时代下的数据隐私性，保障网络空间安全，提高网络防护手段，已经成为社会保障领域的重要议题。

1 网络安全相关概念辨析

1.1网络安全的定义

网络安全指的是正常情况下，互联网运转系统不会因为意外或者人为的因素而遭到破坏，大众的网络数据不会受到更改和泄漏，同时系统能够在不间断的情况下持续、稳定工作。从学术上而言，所有有关互联网应用以及数据信息的保密、完整性、可用性、真实性和可控制性等方面的技术和知识，都属于网络安全的范畴。

对于网络安全的管理和防护而言，有关部门需要从技术层面和内部管理层面进行多方位的治理。技术层面着重于防止外来的非法网络入侵，而在管理层面，重点需要关注于企业内的人工干预，避免内部人为因素的发生。

1.2网络安全的特征

网络安全的主要特征分为以下几类：

（1）保密性。在互联网运转的过程中，需要保证数据传输的高保密性，避免用户信息以及隐私数据的泄漏。

（2）完整性。数据在进行储存以及传播的过程中不会受到人为因素的影响而发生破坏、丢失或改变，即数据在未授权的情况下需要保持完整。

（3）可用性。保证可以被许可的实体进行访问和利用所需的功能，也就是说，外部用户在必要时能够获得所需的数据。在网络中，如果服务申请被拒绝，该设备后续的网络访问都会被认定为侵入。

（4）可控性。指在网络安全的管理过程中，信息主体需要确保其对网络数据有绝对的控制力。

（5）可审查性。指在出现安全风险或面临内容审查时，需要根据需求提供相关的资料与应对依据。

2 网络安全所面临的主要风险

2.1互联网系统漏洞

系统漏洞是指程序或操作系统的设计出现问题，或是在编写过程中出现错误，导致被不法分子或计算机黑客所利用。通过这类安全漏洞，不法分子会在计算机中植入木马、病毒等，从而对计算机进行入侵，进而夺取控制权以及关键的数据信息，最终摧毁计算机的运行系统[1]。

系统缺陷会对网络的各个方面产生巨大的冲击，其中包含了自身的服务体系以及相关的具体应用软件。同时，系统漏洞发生的原因是多种多样的，这也导致了漏洞的类型复杂繁多。不同类别和运转机制的计算机系统，其安全性问题也各有不同。除此之外，各种软、硬件设备、同一设备的不同类型、设备组成的不同体系、同一设备的不同配置情况下，都会产生相应的安全问题[2]。

2.2网络环境的不安全性

因特网是一个面向全球的网络，任何人或单位都能轻易地在其中传送及取得资讯，因特网的开放性、共享性、国际性等特性，即使得其能够风靡世界，给人们带来良好的使用体验，同时又对其安全性构成了严峻的考验。互联网环境主要存在下列不安全因素：

（1）开放性。由于技术上的完全开放性，导致网络在运行过程中会面临各种威胁，包括对物理传输线的破坏、对网络通信系统的破坏、对计算机软件和硬件的漏洞袭击等。

（2）国际性。网络的国际性特征使网络受到的威胁不再局限于当地的网民，同时也有其他国家的黑客，因此，网络的安全正受到全球化的威胁。例如美国对我国西北工业大学的数据库袭击，就是典型的国际性网络威胁事件。

（3）自由性。大部分的网络环境不会对使用者进行技术上的限制，使用者可以随意发表及获得各种资讯和观点。

2.3防火墙的局限性

为了提高网络环境的安全性，互联网防护部门一般会采用防火墙的形式来降低网络风险。防火墙的工作原理就是将互联网一分为二，成为内部网络和外部网络，外部网络的内容需要经过防火墙的审查机制，才能够向内传输。同时，内部网络的用户也不能随意地进行外部访问。通过这种模式，能够依靠数据筛查以及过滤，有效降低网络安全风险。然而，防火墙仅仅是网络防护系统的一部分，其仍然存在一些缺点：

（1）对有用的网络业务进行限定。防火墙的设计目的在于过滤信息，然而有的时候也会出现误判的情况，即用户需求的网络业务无法有效运行。

（2）对内部使用者的袭击不能进行保护。防火墙主要用于隔绝内部网络与外部网络的交流，因此无法针对内部网络

自身发起的攻击进行有效应对。

（3）不能抵御除防火墙之外的其他方式的入侵。除了外部网络的数据交换入侵之外，还有例如U盘病毒，邮件病毒等，这类入侵方式往往不在防火墙的防护范围之内。

（4）无法对被病毒传染的软件或档案进行彻底的保护。防火墙的防护作用只能生效于入侵开始之前，面对已经发生的侵入行为，无法再进行应对。

（5）不能防御以数据为基础的袭击。若是有害数据假借正常的访问形式进行入侵，那么防火墙降温法进行有效防御。

（6）无法对新的网络安全性问题进行防御。受到数据库更新的限制，面对最新的入侵方式，防火墙往往无法立刻做出反馈。

2.4网络病毒的威胁

在当前的互联网时代，网络病毒正成为最大的威胁。一方面，由于病毒本身的自我修复能力极高，且传播极快，一旦发生感染，会导致机器的运转受到极大的阻碍，严重的话甚至会造成系统故障以及成硬件故障。另一方面，由于互联网上大量的数据和信息交流，使得不同用户计算机之间的联系变得更加复杂，更加难以防范。

2.5黑客攻击

近几年，网络黑客利用计算机系统、网络协议、数据库等软硬件存在的漏洞和不足，利用后门程序、DDOS攻击、邮件链接木马等对数据进行窃取，或是对硬件进行破坏。

2.6管理和防护制度不健全

管理安全的隐患在于责任不明、管理制度不完善，同时管理条例缺少可操作性。在发生网络攻击或其他信息安全问题的时候，安全防护系统不能实时监测、汇报、预警和应对。而在意外事件后，又不能为警方的后续行动和侦破提供线索，总而言之，当前的防护体系缺乏有效的控制力。

3 防护技术

3.1漏洞扫描

漏洞扫描是一种以漏洞的数据分析库为基础，对特定计算机安全弱点进行扫描或探测，从而找出可能出现风险的漏洞。一旦检测出漏洞，必须立即进行修补，否则计算机很可能被入侵者进行遥控，造成难以想象的结果。通过防火墙和入侵检测系统的结合，可以使防护体系更加可靠。在被入侵之前，网络防护和管理部门可以通过进行扫描来修正错误的网络配置[3]。

3.2入侵检测

IDS是一种用于探测网络侵入的系统。能够对网络行为、安全日志和电脑中一些重要节点的数据进行分析，从而检测网络中有无风险行为和受到袭击的情况，并提供相应的警示。作为一套成功的IDS，不仅可以让管理员随时掌握系统中的程序、文件和硬件的变化情况，而且可以为网络安全政策的制定提供指导。一旦网络环境受到攻击，入侵检测系统就会立即作出反应，切断网络连接，记录事件并发出警报，从而有效地帮助网络防护工作的进行。

3.3病毒防护

在网络时代，人们的生活和工作都与互联网紧密相关。电脑病毒对计算机应用的危害是无法估计的，从而也会对人类的正常生产和生活产生极为恶劣的影响。所以，在网络安全保障体系中中，电脑病毒的预防也是一个非常关键的环节。

计算机病毒防护体系包括病毒预防、病毒检测和病毒杀灭三大类。其防护原理主要是利用病毒数据库对可能的入侵访问进行筛查、检测和判定，随后根据相应的处置方式进行预警以及反馈，从而防止病毒侵入或对其进行攻击。

3.4数据加密

数据加密能够对数据传输的过程、所传输数据的完整性以及用户的身份进行保护。数据加密可以通过伪装的形式，来改变原有数据的格式、内容形式等特征，从而避免外部用户的访问。数据加密的主要形式分为公钥加密和私匙加密两种。

（1）私匙加密。指用于对消息进行保密的密匙就是用于对消息进行解密的密匙。私匙加密可以使信息的加密程度更加深入，但是不能提供验证，因为任何人都可以通过私匙进行信息的处理和传输。该加密方式具有快速、便捷，以及软硬件兼用的特点。

（2）公匙加密。相较于私匙加密的信息处理方式，公匙加密应用得较晚，与私匙加密的模式不同，公匙加密的密匙数量从一个增加到了两个，即加密和解密的过程都需要不同的密匙。由于加密和解密的过程是分开的，但是其计算体系的密集的，因此会导致计算流程变得更加复杂，加密和解密的速度也会慢很多。

如果在实际进行数据加密的过程在，能够将两种加密形式进行组合运用，就可以极大地提高加密效果。

3.5安全管理

在计算机网络的安全方面，除了采取以上技术手段，还应该加强网络的安全管理，制定针对计算机信息系统的标准化管理体系。通过不断地技术攻关来加强防护手段，增强用户和管理人员的安全防范意识，提高工作人员的安全素养，建立全面有效、易于操作的网络安全综合管理系统。

4 结束语

计算机网络的安全性问题是一个比较复杂的系统性工程，我们需要明确的是，没有完全的网络安全，只能通过采取尽可能完善的防护体系，来避免安全风险事故的发生。高素质的技术人员是整个系统安全性的技术保障，而严密的管理体系又是整个防护系统的运转保障，因此需要制订出一套科学的技术计划和系统的运行机制，以进一步提升整个安全防护系统的工作效果。

参考文献

[1]刘静.计算机网络安全防护技术研究[J].计算机光盘软件与应用，2012（22）：2.

[2]蒋东晖.计算机网络安全防护[J].科技创新导报，2009（1）：1.

[3]杨光，孙洋，王磊，等.计算机及网络的管理与安全防护[J].内蒙古林业调查设计，2013（2）：3.