# 浅谈网络信息安全问题的分析与防范

来源：网络 作者：春暖花香 更新时间：2024-07-17

*第一篇：浅谈网络信息安全问题的分析与防范浅谈网络信息安全问题的分析与防范【论文关键词】网络安全 信息安全 安全防范【论文摘要】随着互联网的广泛应用，网络信息安全问题越来越受到人们的关注。本文分析了目前网络信息安全领域存在的多种安全问题，提...*

**第一篇：浅谈网络信息安全问题的分析与防范**

浅谈网络信息安全问题的分析与防范

【论文关键词】网络安全 信息安全 安全防范

【论文摘要】随着互联网的广泛应用，网络信息安全问题越来越受到人们的关注。本文分析了目前网络信息安全领域存在的多种安全问题，提出了实现网络信息安全的防范措施。

1引言

随着Internet的迅猛发展，网络上各种新业务也不断兴起，比如电子商务、网上银行、数字货币、网上证券等，使得工作、生活变得非常方便，但病毒侵虐、网络犯罪、黑客攻击等现象时有发生，严重危及我们正常工作、生活。据国际权威机构统计，全球每年因网络安全问题带来的损失高达数百亿美元。因此网络信息安全问题的分析与防范显得非常重要。

2网络信息安全概述

网络信息安全就是网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改或泄漏，系统连续可靠正常地运行，网络服务不中断。网络信息安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。

3网络信息安全存在的戚胁

目前网络信息安全面临的威胁主要来自于以下几个方面：

3．1 TCP／IP协议存在安全漏洞

目前英特网上广泛使用的网络协议是TCP／IP协议，而TCP／IP协议恰恰存在安全漏洞。如IP层协议就有许多安全缺陷。IP地址可以软件设置，这就造成了地址假冒和地址欺骗两类安全隐患；IP协议支持源路由方式，即源点可以指定信息包传送到目的节点的中间路由，这就提供了源路由攻击的条件。再如应用层协议Telnet、FTP、SMTP等协议缺乏认证和保密措施，这就为否认、拒绝等欺瞒行为打开了方便之门。

3．2网络滥用

合法的用户滥用网络，引入不必要的安全威胁，包括用户私拉乱接网线、局域网内部私自架设代理服务器。近年来被广泛关注的P2P传输问题并不是一个典型的信息安全问题，但由于这些传输流量常常严重干扰单位的正常通信流量而且也存在着一些泄漏单位信息的风险。

3．3信息泄漏和丢失

由于存储设备、介质丢失而引起信息丢失，造成信息泄漏，特别是在计算机日益普及的今天，这些现象越发突出。比如由于工作人员的疏忽大意，忘记将存储有重要信息的笔记本电脑、存储介质、文件携带或删除，造成他人能够获得该重要文件，导致信息泄露和丢失。

3．4破坏数据完整性和真实性

以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应：假冒合法用户身份，干扰用户的正常使用。

3．5利用网络传播病毒

通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

4网络信息安全的主要防范措施

4．1信息加密技术

信息加密技术是利用数学或物理手段，对电子信息在传输过程中和存储体内进行保护，以防止泄露的技术。数据加密过程就是通过加密系统把原始的数字信息(明文)，按照加密算法变换成与明文完全不同的数字信息(密文)的过程。数据加密技术主要分为数据传输加密和数据存储加密。数据传输加密技术主要是对传输中的数据流进行加密，常用的有链路加密、节点加密和端到端加密三种方式。链路加密对用户来说比较容易，使用的密钥较少，而端到端加密比较灵活，对用户可见。在对链路加密中各节点安全状况不放心的情况下也可使用端到端加密方式。

4．2数字签名技术

所谓“数字签名”就是通过某种密码运算生成一系列符号及代码组成电子密码进行签名，来代替书写签名或印章，对于这种电子式的签名还可进行技术验证，其验证的准确度是一般手工签名和图章的验证所无法比拟的。“数字签名’可以确保传输电子文件的完整性、真实性和不可抵赖性4．3防火墙技术

“防火墙”是位于两个(或多个)网络问，实施网络之间访问控制的一组组件集合。防火墙的主要作用是提供行之有效的网络安全机制，其本身也是网络安全策略的有机组成部分。它能根据用户设定的安全策略控制和监测网络之间的信息流，且具有较强的抗攻击能力。防火墙的技术已经经历了三个阶段，即包过滤技术、代理技术和状态监视技术。现在大多数防火墙多采用以上几种技术的结合，以期达到最佳性能。

4．4加强病毒防范

为了能有效地预防病毒并清除病毒，必须建立起有效的病毒防范体系，这包括漏洞检测、病毒预防、病毒查杀、病毒隔离等措施，要建立病毒预警机制，以提高对病毒的反应速度，并有效加强对病毒的处理能力。4．4．1病毒预防。要从制度上堵塞漏洞，建立一套行之有效的制度。不要随意使用外来光盘、移动硬盘、u盘等存储设备。

4．4．2病毒查杀。主要是对病毒实时检测，清除已知的病毒。要对病毒库及时更新，保证病毒库是最新的。这样才可能查杀最新的病毒。

4．4．3病毒隔离。主要是对不能杀掉的病毒进行隔离，以防病毒再次传播和扩散。

4．5定期扫描系统和软件漏洞

坚持不定期地对重要计算机信息系统进行检查，发现其中可被黑客利用的漏洞。漏洞扫描的结果实际上就是系统安全性能的一个评估，它指出了哪些攻击是可能的。然后针对这些系统和软件漏洞，及时打上相关补丁。

4．6加强安全管理队伍的建设

在计算机网络系统中，绝对的安全是不存在的。俗话说：“三分技术，七分管理”，要不断地加强计算机信息网络的安全规范化管理力度，强化人员管理。制定健全的安全管理体制是计算机网络安全的重要保证，只有通过网络管理人员与使用人员的共同努力，运用一切可以使用的工具和技术，尽可能地把不安全的因素降到最低。

5结柬语

在网络信息化时代，网络信息安全已越来越受重视了。虽然现在用于网络安全防护的产品有很多，但是安全事故仍不断出现，对社会造成了严重的危害。根本原因是网络自身的安全隐患无法根除，这就使得黑客进行入侵有机可乘。尽管如此，只要我们综合运用各种网络安全技术并进行规范化管理，就能为我们的网络上的各种应用保驾护航。

**第二篇：信息安全问题分析与讨论**

信息安全问题分析与讨论(三等奖)来源：广东省东莞市光明中学 作者：严

灿洪 [日期：2024-10-15] [字体：大 中 小] 【适合年级】高一年级 【设计思想】

根据普通高中信息技术新课标指导思想，以建构主义学习理论和教学理论为理论基础，为学生营造较宽松自由的课堂，突出学生学习主体作用及教师的主导作用，通过教学活动培养学生的信息素养，提高学生的团队意识。【教材分析】

广东省编信息技术（必修）《信息技术基础》教材第六章第1节，内容是对信息安全各方面作一个总体介绍，引导学生主动了解更多的信息技术及安全方面的知识和更多的信息道德及相关法律法规知识，树立信息安全意识和自觉遵守信息道德规范意识，并通过活动，提高学生在各方面的水平。【教学目标】 【知识目标】

1、全面介绍信息安全方面的一些知识，引导学生自主了解在日常信息活动中存在的安全问题，使同学们在以后的信息活动过程中能注意这些方面的问题。

2、初步了解信息道德规范及相关法律法规知识。【能力目标】

1、通过讨合作活动，培养学生团队意识。

2、通过网络交流活动，培养学生利用网络主动学习新知识和研究问题能力。【情感目标】

1、提高学生与他人交流合作意识。

2、培养学生主动树立信息安全意识和自觉遵守信息道德规范意识。

【教学课时】1课时（40分钟）【学生分析】

学生通过前面几章的学习，对信息技术各方面的问题和对计算机的操作都有了比较深刻的了解，在此基础上，教师可以围绕在信息活动过程中存在的安全问题，搜集相关资料，精选案例资源。【学习内容】

根据教材的教学内容，以及结合本节课的实际情况，确定本节课的学习内容。

1、教材中关于信息安全问题的五个案例分析，并从中提及相关信息道德和法律问题；

2、讨论并完成表6－1 信息安全相关案例分析表；

3、根据第四章信息发布所学内容，学生自己完成发布分析表；

4、学生总结信息安全问题；

5、在线课堂练习，巩固本节所学知识；

6、网络论坛交流活动，讨论日常生活中所遇到信息安全及相关信息道德问题。【教学重点】

了解更多的信息技术及安全方面的知识和更多的信息道德及相关法律法规知识，树立信息安全意识和自觉遵守信息道德规范意识，并通过活动，提高学生在各方面的水平。【教学难点】

如何有效的开展活动问题。【教学策略】

突出学生为学习主体，教师主导。以Wquestion、任务驱动为主要教学方法，引导学生讨论合作、交流学习的教学策略。【教学媒体】

1、多媒体网络电脑室（与Internet相连，带音响设备）；

2、多媒体网络教学软件系统；

3、web服务器（支持ASP）；

4、信息技术教学网（平台）；

5、FTP服务器软件及客户端软件； 【教学准备】 教师准备】

1、准备详细的教案；

2、“在线课堂”网络教学课件与powerpoint课件；

3、架好FTP服务器软件及ASP支持的网络论坛。【学生准备】 预习课本第六章书。【教学过程】 【教学流程图】

【教学特色】

1、Wquestion教学法，“在线课堂”提供大量素材及课堂练习。

2、以学生为学习主体，通过案例分析，讨论合作完成相关分析表，培养学生团体意识；

3、通过网络交流活动，培养学生利用网络主动学习新知识和研究问题能力。【教学后记】

高中信息技术新课标指出：学生是学习和发展的主体，要给学生营造良好的信息环境，关注全体学生，注重交流与合作，以提高学生的信息素养、综合能力与创新精神为目标的课程理念。围绕新课标，回顾这节课的教学，我有以下几点深刻体会：

1、营造较宽松自由的课堂，有助于学生积极参与课堂活动；

2、选择合适的课堂教学策略，有助于激发学生的学习热情；

3、利用网络技术，提高教学质量；

4、围绕主题任务学习，有助于促进协作学习和提高班级凝聚力。

**第三篇：浅析网络信息安全问题与对策**

浅析网络信息安全问题与对策

12010115 高先余

摘 要：随着计算机技术的飞速发展，信息网络已经成为社会发展的重要保证。信息网络涉及到国家的政府、军事、文教等诸多领域，存储、传输和处理的许多信息是政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要的信息。其中有很多是敏感信息，甚至是国家机密，所以难免会吸引来自世界各地的各种人为攻击（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）。通常利用计算机犯罪很难留下犯罪证据，这也大大刺激了计算机高技术犯罪案件的发生。计算机犯罪率的迅速增加，使各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。本文结合实际情况，分析网络安全问题并提出相应对策。关键词：计算机；网络安全；网络威胁。

一、前言

随着计算机技术的迅速发展，在计算机上完成的工作已由基于单机的文件处理、自动化办公，发展到今天的企业内部网、企业外部网和国际互联网的世界范围内的信息共享和业务处理，也就是我们常说的局域网、城域网和广域网。计算机网络的应用领域已从传统的小型业务系统逐渐向大型业务系统扩展。计算机网络在为人们提供便利、带来效益的同时，也使人类面临着信息安全的巨大挑战。

组织和单位的计算机网络是黑客攻击的主要目标。如果黑客组织能攻破组织及单位的计算机网络防御系统，他就有访问成千上万计算机的可能性。据统计，近年来因网络安全事故造成的损失每年高达上千亿美元。计算机系统的脆弱性已为各国政府与机构所认识。

二、计算机通信网络安全概述

所谓计算机通信网络安全，是指根据计算机通信网络特性，通过相应的安全技术和措施，对计算机通信网络的硬件、操作系统、应用软件和数据等加以保护，防止遭到破坏或窃取，其实质就是要保护计算机通讯系统和通信网络中的各种信息资源免受各种类型的威胁、干扰和破坏。计算机通信网络的安全是指挥、控制信息安全的重要保证。根据国家计算机网络应急技术处理协调中心的权威统计，通过分布式密网捕获的新的漏洞攻击恶意代码数量平均每天112次，每天捕获最多的次数高达4369 次。因此，随着网络一体化和互联互通，我们必须加强计算机通信网络安全防范意思，提高防范手段。

三、影响计算机通信网络安全的因素分析

计算机通信网络的安全涉及到多种学科，包括计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等十数种，这些技术各司其职，保

护网络系统的硬件、软件以及系统中的数据免遭各种因素的破坏、更改、泄露，保证系统连续可靠正常运行。

3.1影响计算机通信网络安全的客观因素。

3.1.1网络资源的共享性。计算机网络最主要的一个功能就是“资源共享”。无论你是在天涯海角，还是远在天边，只要有网络，就能找到你所需要的信息。所以，资源共享的确为我们提供了很大的便利，但这为系统安全的攻击者利用共享的资源进行破坏也提供了机会。

3.1.2网络操作系统的漏洞。操作系统漏洞是指计算机操作系统本身所存在的问题或技术缺陷。由于网络协议实现的复杂性，决定了操作系统必然存在各种的缺陷和漏洞。

3.1.3网络系统设计的缺陷。网络设计是指拓扑结构的设计和各种网络设备的选择等。网络设备、网络协议、网络操作系统等都会直接带来安全隐患。

3.1.4网络的开放性。网上的任何一个用户很方便访问互联网上的信息资源，从而很容易获取到一个企业、单位以及个人的信息。

3.1.5恶意攻击。恶意攻击就是人们常见的黑客攻击及网络病毒．是最难防范的网络安全威胁。随着电脑教育的大众化，这类攻击也越来越多，影响越来越大。无论是DOS 攻击还是DDOS 攻击，简单的看，都只是一种破坏网络服务的黑客方式，虽然具体的实现方式千变万化，但都有一个共同点，就是其根本目的是使受害主机或网络无法及时接收并处理外界请求，或无法及时回应外界请求。

3.2影响计算机网络通信安全的主观因素。

主要是计算机系统网络管理人员缺乏安全观念和必备技术，如安全意识、防范意识等。

四、计算机网络的安全策略

4.1物理安全策略。

物理安全策略目的是保护计算机系统、网络服务器、打印机等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击；验证用户的身份和使用权限、防止用户越权操作；确保计算机系统有一个良好的电磁兼容工作环境；建立完备的安全管理制度，防止非法进入计算机控制室和各种偷窃、破坏活动的发生。物理安全策略还包括加强网络的安全管理，制定有关规章制度，对于确保网络的安全、可靠地运行，将起到十分有效的作用。网络安全管理策略包括：确定安全管理等级和安全管理范围；制订有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

4.2常用的网络安全技术。

由于网络所带来的诸多不安全因素，使得网络使用者必须采取相应的网络安全技术来堵塞安全漏洞和提供安全的通信服务。如今，快速发展的网络安全技术能从不同角度来保证网络信息不受侵犯，网络安全的基本技术主要包括网络加密技术、防火墙技术、操作系统安全内核技术、身份验证技术、网络防病毒技术。

4.2.1 网络加密技术。网络加密技术是网络安全最有效的技术之一。一个加密网络，不但可以防止非授权用户的搭线窃听和入网，而且也是对付恶意软件的有效方法之一。网络信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。信息加密过程是由形形色色的加密算法来具体实施的，它以很小的代价提供很牢靠的安全保护。在多数情况下，信息加密是保证信息机密性的唯一方法。

4.2.2 防火墙技术。防火墙技术是设置在被保护网络和外界之间的一道屏障，是通过计算机硬件和软件的组合来建立起一个安全网关，从而保护内部网络免受非法用户的入侵，它可以通过鉴别、限制，更改跨越防火墙的数据流，来实何保证通信网络的安全对今后计算机通信网络的发展尤为重要。现对网络的安全保护。防火墙的组成可以表示为：防火墙= 过滤器+ 安全策略+ 网关，它是一种非常有效的网络安全技术。在Internet 上，通过它来隔离风险区域与安全区域的连接，但不防碍人们对风险区域的访问。防火墙可以监控进出网络的通信数据，从而完成仅让安全、核准的信息进入，同时又抵制对企业构成威胁的数据进入的任务。

4.2.3 操作系统安全内核技术。操作系统安全内核技术除了在传统网络安全技术上着手，人们开始在操作系统的层次上考虑网络安全性，尝试把系统内核中可能引起安全性问题的部分从内核中剔除出去，从而使系统更安全。操作系统平台的安全措施包括：采用安全性较高的操作系统；对操作系统的安全配置；利用安全扫描系统检查操作系统的漏洞等。

4.2.4身份验证技术身份验证技术。身份验证技术身份验证技术是用户向系统出示自己身份证明的过程。身份认证是系统查核用户身份证明的过程。这两个过程是判明和确认通信双方真实身份的两个重要环节，人们常把这两项工作统称为身份验证。它的安全机制在于首先对发出请求的用户进行身份验证，确认其是否为合法的用户，如是合法用户，再审核该用户是否有权对他所请求的服务或主机进行访问，以此来防止一些非法入侵人员的侵入。

4.2.5 网络防病毒技术。在网络环境下，计算机病毒具有不可估量的威胁性和破坏力。CIH 病毒及爱虫病毒就足以证明如果不重视计算机网络防病毒，那可能给社会造成灾难性的后果，因此计算机病毒的防范也是网络安全技术中重要的一环。网络防病毒技术的具体实现方法包括对网络服务器中的文件进行频繁地扫描和监测，工作站上采用防病毒芯片和对网络目录及文件设置访问权限等。防病毒必须从网络整体考虑，从方便管理人员的能，在夜间对全网的客户机进行扫描，检查病毒情况；利用在线报警功能，网络上每一台机器出现故障、病毒侵入时，网络管理人员都能及时知道，从而从管理中心处予以解决。

五、结束语

随着信息技术的飞速发展，影响通信网络安全的各种因素也会不断强化，因此计算机网络的安全问题也越来越受到人们的重视，以上我们简要的分析了计算机网络存在的几种安全隐患，并探讨了计算机网络的几种安全防范措施。

总的来说，网络安全不仅仅是技术问题，同时也是一个安全管理问题。我们必须综合考虑安全因素，制定合理的目标、技术方案和相关的配套法规等。世界上不存在绝对安全的网络系统，随着计算机网络技术的进一步发展，网络安全防护技术也必然随着网络应用的发展而不断发展。

六、参考文献

【1】 陶阳.计算机与网络安全 重庆：重庆大学出版社

【2】 田园.网络安全教程 北京：人民邮电出版社

【3】冯登国.《计算机通信网络安全》，清华大学出版社

【4】陈斌.《计算机网络安全与防御》，信息技术与网络服务

【6】赵树升等.《信息安全原理与实现》，清华大学出版社

**第四篇：浅析计算机网络安全问题与防范策略**

浅析计算机网络安全与防范措施

关键词： 计算机网络 安全 防范技术

摘要：随着计算机科学技术和网络技术的高速发展，使得计算机系统功能与网络体系变得日渐复杂与强大。但是计算机网络技术的飞速发展，在给人们工作和生活提供方便的同时，也对人们构成日益严重的网络网络安全威胁。数据窃取、黑客侵袭、病毒感染、内部泄密等网络攻击问题无时无刻在困扰着用户的正常使用。因此，如何提高计算机网络的防范能力，增强网络的安全措施，已成为当前急需解决的问题。

一、计算机网络安全的基本概念。

计算机网络安全是指“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、软件数据不因偶然和恶意的原因而遭到破坏、更改、泄漏，使系统能连续、可靠、正常运行、网络服务不中断，或因破坏后还能迅速恢复正常使用的安全过程。计算机网络安全包括两个方面，即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。逻辑安全包括信息的可靠性、保密性、真实性、完整性及可用性。本质上，网络安全就是网络中信息的安全。

二、计算机网络安全面临的威胁

目前，随着网络应用的深入以及技术频繁升级，非法访问、恶意攻击等安全威胁也不断出新。各种潜在的不安全因素使网络每天都面临着信息安全方面的威胁。主要面现为：

１.系统漏洞威胁

网络系统本身存在的安全问题主要来自系统漏洞带来的威胁，且是不可估量的。系统漏洞是指应用软件或操作系统软件在逻辑设计上无意中造成的缺陷或错误，形成一个不被注意的通道。许多时候，在运行系统或程序这些漏洞被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个电脑，窃取电脑中的重要资料和信息，甚至破坏系统。在不同种类的软、硬件设备，同种设备的不同版本之间，由不同设备构成的不同系统之间，以及同种系统在不同的设置条件下，都会存在各自不同的安全漏洞问题。

２.“黑客”的攻击

当前黑客是影响网络安全的最主要因素之一，因为它对网络构成威胁，造成破坏。黑客是指：计算机网络行家中，热衷于神秘而深奥的操作系统之类的程序，又爱移花接木、拼凑或修改程序而随意攻击的人。黑客攻击，是指黑客利用系统漏洞和非常规手段，进行非授权的访问行为和非法运行系统或非法操作数据。黑客攻击手段可分为非破坏性攻击和破坏性攻击两类。非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹；破坏性攻击是以侵入他人电脑系统、盗窃系统保密信息、破坏目标系统的数据为目的。

３.计算机病毒的攻击

计算机病毒是指编制或在计算机程序中插入的破坏计算机功能或毁坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。由于计算机病毒具有隐蔽性、传染性、潜伏性、破坏性、可触发性、针对性、衍生性的特点。一旦计算机感染上病毒后，轻者会使计算机速度变慢，系统性能下降；重者能破坏系统的正常运行甚至还可以损失硬件，毁掉系统内部数据，格式化磁盘和分区，甚至导致整个网络瘫痪。

４.网络设备故障问题。

网络中的设备包括计算机、网络通信设备、存储设备、传输设备、防雷系统、抗电磁干扰系统、网络环境都是网络安全的重要保障，每个环节设备出现问题，都会造成网络故障。所以定期和不定期检测设备、使用先进的网络设备和产品是网络安全不可忽视的问题。

５.管理制度的问题

网络系统的正常运行离不开管理人员的管理。由于对管理措施不当，会造成设备的损坏，保密信息的人为泄露等，因而这些失误人为的因素是主要的。如果管理不严格，网络安全意识不强，设置的口令过于简单，重要机密数据不加密，数据备份不及时，用户级别权限划分不明确或根本无级别限制，就容易导致病毒、黑客和非法受限用户入侵网络系统，让数据泄露、修改、删除，甚至使系统崩溃。或者将自己的口令随意告诉别人或者无意中透露给他人等都会对网络安全带来威胁。或是，有条件接触计算机信息网络系统的工作人员为了获取一定的利益故意泄露保密系统的文件和资料和对网络安全进行破坏的行为。

三、计算机网络安全的防范技术

尽管计算机网络信息安全受到威胁，但是采取恰当的防护措施也能有效的保护网络信息的安全。

１.入侵防范技术

入侵检测技术只能对网络系统的运行状态进行监视，检测发现各种攻击企图、攻击行为或攻击结果，无法有效的保护网络被攻击破坏。入侵防范软件重在预防，能够对应用层渗透，对缓冲区溢出、木马、后门、SQL注入、XSS进行识别拦截。入侵防范技术的定义是哪些行为是正当的，哪些行为是可疑的，这样一旦企图作出超乎预期行为范围的举动，入侵防范技术会先发制人地削除不当的系统行为，一些高度结构化的入侵预防系统还能提供预先设定的规则，主动地加强桌面系统和服务器的安全，防止受到特征扫描的技术所无法实现的网络攻击的破坏。

２.病毒防范技术

在网络环境下，病毒传播的速度非常快，计算机病毒不断升级，极大威胁到网络的安全。现在我们普遍使用防病毒软件进行病毒的防范，常用的防病毒软件包括单机防病毒软件和网络防病毒软件两大类。单机病毒可以采取传统的防治病毒技术，以及采用功能较强的反病毒软件，基本上可保障计算机系统不受病毒侵害。在结构形式多样，有局域网、内网和外网、公网和涉密网这样的网络中，必须有面向独立网络全方位的防病毒产品才能保证网络系统良好运行。比如计算机网络系统上安装网络病毒防治服务器，在内部网络服务器上安装网络病毒防治软件。对于网络防病毒软件注重网络防病毒，病毒防范重点应在因特网的接入口，以及外网下的服务器和各独立内网中心服务器等。

３.防火墙技术

防火墙技术是实现网络安全最基本、最经济、最有效的安全措施之一。防火墙是网络安全的重要屏障，是指在网络安全边界控制中，用来阴止从处网想进入给定网络的非法访问对象的安全设备。防火墙是软硬件的安全组合体，一边与内部网相连另一边与因特网相连，可根据安全策略需要的各种控制规，阻止未经受、授权的来自因特网或对因特网的访问，或阻止某些通过访问对象连接的地址或传输的数据包，并以安全管理提供详细的系统活动的记录。比如，为保证网络中计算机的正常运行，可选用网络级防火墙来防止非法入侵，此类防火墙有分组过滤器和授权服务器，前者可检查所有流入本网的信息并拒绝不符合实现制定好的一套准则的数据，后者可检查用户的登录是否合法，这样最大限度地阻止网络中的黑客来访问自己的网络，防止他们随意更改、移动甚至删除网络上的重要信息。

４.数据加密技术

要保证数据信息及在网络传输中的保密信息不提供给非授权用户进行更改、窃取、删除等，应该对数据信息实行加密技术，即使数据被人截获，没有密钥加密数据也不能还原为原数据，网络数据的安全从而得到保证。数据加密技术是一种限制对网络上传输数据的访问权的技术主要是通过对网络中传输的信息进行加密钥匙及加密函数转换，变成无意义的密文，只有在指定的用户或网络下，接收方方可将此密文经过解密函数、解密钥匙还原成明文却原数据。加密的基本功能包括：防止不速之客查看机密的数据文件、防止机密数据被泄露或篡

改、防止特权用户(如系统管理员)查看私人数据文件、使入侵者不能轻易地查找一个系统的文件。数据加密可在网络OSI七层协议的多层上实现、所以从加密技术应用的逻辑位置看，有三种方式：链路加密、节点加密、端对端加密。

5.漏洞扫描技术

漏洞扫描技术是利用网络系统或者其他网络设备进行网络安全检测，以查找出安全隐患和系统漏洞，并采取相应防范措施，从而降低系统的安全风险而发展起来的一种安全技术。利用漏洞扫描技术，可以对局域网、WEB站点、主机操作系统、系统服务以及防火墙系统的漏洞进行扫描，可以检查出正在运行的网络系统中存在的不安全网络服务，在操作系统上存在的可能会导致遭受缓冲区溢出攻击或者拒绝服务攻击的安全漏洞，还可以检查出主机系统中是否被安装了窃听程序，防火墙系统是否存在安全漏洞和配置错误。漏洞扫描的结果实际就是对系统安全性能的评估，定时运行漏洞扫描技术，是保证网络安全不可缺少的手段。

6.其他应对策略

建立健全网络安全管理制度。只要有网络存在，就不可避免有网络安全问题的发生，为了把网络安全问题降到最低，就要建立健全网络安全管理制度，强化网络管理人员和使用人员的安全防范意识，严格操作程序，运用最先进的工具和技术，尽可能把不安全的因素降到最低。此外，还要不断加强网络安全技术建设，加强计算机信息网络的安全规范化管理，才能使计算机网络的安全性得到保障，最大限度保障广大网络用户的利益。最后，作为信息安全的重要内容——数据备份，数据备份与数据恢复是保护数据的最后手段，也是防止主动型信息攻击的最后一道防线。

四、结语

总之，由于随着计算机网络技术的迅速发展和进步，网络经常受到严重的安全攻击与潜在威胁，采取强有力的安全防范，对于保障网络的安全性将变得十分重要。因此，我们加强防范意识，建立严密的安全防范体系，采用先进的技术和产品，构造全方位的防范策略机制；同时，也要树立安全意识，建立健全网络安全管理制度，确保网络系统能在理想状态下运行。

参考文献：刘学辉.计算机网络安全的威胁因素肪防范技术.中国科技信息.2024(9)

张森.浅谈网络安全面临的威胁因素.科技园向导.2024(34)

宋华平.计算机网络安全与防范[J].机电信息.2024(12).孙会儒.浅谈计算机网络安全问题及应对策略.电脑知识与技术.2024(22)

**第五篇：网络与信息系统安全防范应急预案**

网络与信息安全事件应急预案

为保证我公司信息系统安全，加强和完善网络与信息安全应急管理措施，层层落实责任，有效预防、及时控制和最大限度地消除信息安全突发事件的危害和影响，确保信息系统和网络的通畅运行，结合实际，特制定本应急预案。

一、总则

（一）工作目标

保障信息的合法性、完整性、准确性，保障网络、计算机、相关配套设备设施及系统运行环境的安全，其中重点维护铁路局办公网络信息系统、多元投资集团办公网络信息系统的信息安全。

（二）编制依据

根据《中华人民共和国计算机信息系统安全保护条例》、《互联网信息服务管理办法》、《计算机网络信息安全保密制度》《涉密存储介质保密管理规定》、计算机网络保密要求“五条禁令，十个不得”等相关法规、规定、文件精神，制定本预案。

（三）基本原则

1、预防为主。根据《计算机信息安全管理规定》的要求，建立、健全计算机信息安全管理制度，有效预防网络与信息安全事故的发生。

2、分级负责。按照“谁主管谁负责，谁运营谁负责”的原则，建立和完善安全责任制。各部门应积极支持和协助应急处置工作。

3、果断处置。一旦发生网络与信息安全事故，应迅速反应，及时启动应急处置预案，尽最大力量减少损失，尽快恢复网络与系统运行。

（四）适用范围

本预案适用于公司所属各单位，公司各部门。

二、组织体系

成立网络与信息安全领导组，为我公司网络与信息安全应急处置的组织协调机构。

1．网络与信息安全应急领导组组长由主管领导担任，成员由各部门负责人及相关人员组成。负责网络与信息安全应急响应工作的整体规划、组织协调和决策指挥。

2．网络与信息安全应急领导组下设办公室。由部门主任担任检查组长。

职责：

（1）负责和处理应急领导小组的日常工作，检查督促应急领导组决定事项的落实。（2）负责网络与信息安全应急预案的管理，指导督促重要信息系统应急预案的修订和完善，检查落实预案执行情况。

（3）指导全公司应对网络与信息安全突发公共事件的预案演习、宣传培训、督促应急保障体系建设。

三、预防预警

1.信息监测与报告。

（1）按照“早发现、早报告、早处置”的原则，加强对公司属各单位、各部门有关信息的收集、分析判断和持续监测。当发生网络与信息安全突发公共事件时，按规定及时向应急领导小组报告，初次报告最迟不得超过1小时，重大和特别重大的网络与信息安全突发公共事件实行态势进程报告和日报告制度。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施等。

（2）建立网络与信息安全报告制度。发现下列情况时应及时向应急领导小组报告： 利用网络从事违法犯罪活动的情况；

网络或信息系统通信和资源使用异常，网络和信息系统瘫痪，应用服务中断或数据篡改，丢失等情况；

网络恐怖活动的嫌疑情况和预警信息； 其他影响网络与信息安全的信息。2.预警处理与发布。（1）对于可能发生或已经发生的网络与信息安全突发公共事件，立即采取措施控制事态，并向应急领导小组汇报情况。

（2）应急领导小组接到报告后，应迅速召开应急领导小组会议，研究确定网络与信息安全突发公共事件的等级，根据具体情况启动相应的应急预案，并向相关部门进行汇报。

四、应急预案

（一）网站、网页出现非法言论时的应急预案

1、网站、网页由负责网站维护的管理员随时监控信息内容。

2、发现在网上出现非法信息时，网站管理员立即向信息安全领导小组通报情况，并作好记录。清理非法信息，采取必要的安全防范措施，将网站、网页重新投入使用；情况紧急的，应先及时采取删除等处理措施，再按程序报告。

3、网站管理员应妥善保存有关记录、日志或审计记录，将有关情况向安全领导小组汇报，并及时追查非法信息来源。

4、事态严重的，立即向上级领导报告。

（二）黑客攻击或软件系统遭破坏性攻击时的应急预案

1、重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日的备份，并将它们保存于安全处。

2、当管理员通过入侵监测系统发现有黑客正在进行攻击时，应立即向局信息安全领导小组日常应急办公室报告。软件遭破坏性攻击（包括严重病毒）时要将系统停止运行。

3、管理员首先要将被攻击（或病毒感染）的服务器等设备从网络中隔离出来，保护现场，并同时向信息安全领导小组报告情况。

4、日常应急办公室负责恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。

5、事态严重的，立即向上级领导报告。

（三）数据库发生故障时的应急预案

1、主要数据库系统应定时进行数据库备份。

2、一旦数据库崩溃，管理员应立即进行数据及系统修复，修复困难的，可向县信息产业中心汇报情况，以取得相应的技术支持。

3、在此情况下无法修复的，应向信息安全领导组报告，在征得许可的情况下，可立即向软硬件提供商请求支援。

4、在取得相应技术支援也无法修复的，应立即向上级领导报告，在征得许可、并可在业务操作弥补的情况下，由信息安全岗人员利用最近备份的数据进行恢复。

（四）设备安全发生故障时的应急预案

1、小型机、服务器等关键设备损坏后，管理员应立即向上级领导报告。

2、安全岗负责人员立即查明原因。

3、如果能够自行恢复，应立即用备件替换受损部件。

4、如属不能自行恢复的，立即与设备提供商联系，请求派维护人员前来维修。

5、如果设备一时不能修复，应向上级领导汇报，并告知各部门，暂缓上传上报数据，直到故障排除设备恢复正常使用。

（五）内部局域网故障中断时的应急预案

1、办公室平时应准备好网络备用设备，存放在指定的位置。

2、局域网中断后，网络安全岗负责人员应立即判断故障节点，查明故障原因，并向日上级领导汇报。

3、如属线路故障，应重新安装线路。

4、如属路由器、交换机等网络设备故障，应立即从指定位置将备用设备取出接上，并调试通畅。

5、如属路由器、交换机配置文件破坏，应迅速按照要求重新配置，并调测通畅。

6、如有必要，应向上级领导汇报。

（六）广域网外部线路中断时的应急预案

1、广域网线路中断后，管理员应向上级领导报告。

2、管理员应迅速判断故障节点，查明故障原因。

3、如属可即时恢复范围，由网络管理员立即予以恢复。

4、如属电信运营商管辖范围，应立即与电信运营商的维护部门联系，要求尽快修复。

5、如果恢复时间预计超过两小时, 应立即向上级领导汇报。经领导同意后，应通知各部门暂缓上传上报数据。

（七）外部电中断后的应急预案

1、外部电中断后，值班室应立即向管理员汇报情况。

2、如因局内线路故障，由行政部通知维修人员迅速恢复。

3、如果是局外部的原因，由行政部立即与供电局联系，请供电局迅速恢复供电；如果供电局告知需长时间停电，提前做好存档工作。

（八）机房发生火灾时的应急预案

1、一旦机房发生火灾，应遵循下列原则：首先保证人员安全；其次保证关键设备、数据安全；三是保证一般设备安全。

2、人员灭火和疏散的程序是：应首先切断所有电源，同时通过119电话报警。并从最近的位置取出灭火器进行灭火，其他人员按照预先确定的路线，迅速从机房中有序撤出。

五、应急响应

1.先期处置。

（1）当发生网络与信息安全突发公共事件时，值班人员应做好先期应急处置工作，立即采取措施控制事态，同时向行政部报告。

（2）行政部在接到网络与信息安全突发公共事件发生或可能发生的信息后，加强与有关方面的联系，并做好启动本预案的各项准备工作。

2.应急指挥。

预案启动后，要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。3.应急支援。

预案启动后，立即成立应急响应先遣小组，督促、指导和协调处置工作。根据事态的发展和处置工作需要，及时增派专员小组，调动必需的物资、设备，支援应急工作。

4.信息处理。

（1）应对事件进行动态监测、评估，将事件的性质、危害程度和损失情况及处置工作等情况，及时汇报领导，不得隐瞒、缓报、谎报。

（2）要明确信息采集、编辑、分析、审核、签发的责任人，做好信息分析、报告和发布工作。

5.应急结束。

网络与信息安全突发公共事件经应急处置后，由事发部门向上级领导提出应急结束的建议，经批准后实施。

五、后期处置 1.善后处理。

在应急处置工作结束后，要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。

2.调查评估。

在应急处置工作结束后，行政部应立即组织有关人员和专员组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及财产损失情况，总结经验教训，写出调查评估报告，并根据问责制的有关规定，对有关责任人员作出处理。

六、保障措施 1.数据保障。

重要信息系统均应建立备份系统和相关工作机制，保证重要数据在受到破坏后，可紧急恢复。

2.应急队伍保障。

按照一专多能的要求建立网络信息安全应急保障队伍。3.经费保障。

落实网络与信息系统突发公共事件应急处置资金。

七、监督管理 1.宣传教育。

要充分利用各种传播媒介及有效的形式，加强网络与信息安全突发公共事件应急和处置的有关法律法规和政策的宣传，开展预防、预警、自救、互救和减灾等知识的宣讲活动，普及应急救援的基本知识，提高公众防范意识和应急处置能力。

要加强对网络与信息安全等方面的知识培训，提高防范意识及技能，指定专人负责安全技术工作。并将网络与信息安全突发公共事件的应急管理、工作流程等列为培训内容，增强应急处置工作的组织能力。

2.责任与奖惩。网络与信息系统的管理部门要认真贯彻落实预案的各项要求与任务，建立监督检查和奖惩机制。

本DOCX文档由 www.zciku.com/中词库网 生成，海量范文文档任你选，，为你的工作锦上添花,祝你一臂之力！