

# 关于新时期计算机网络安全分析

刘海龙

(河北省涿源县政务服务中心 河北 涿源 074300)

**[摘要]**近年来,随着计算机管理模式的到来,使计算机的管理、数据统计和其他信息应用紧密相连。同时也改变了我们的生活方式,减轻了我们的工作量。然而,黑客也开始出现,这对计算机安全是一个的威胁。一些公司也面临着数据丢失的风险,许多计算机门户已经被损坏不能保证正常工作。针对这一现象,需要与大型企业及相关实体进行安全分析,了解网络安全不同维度特征,分析并找到有效的风险防范措施,确保计算机网络安全。

**[关键词]**计算机;网络安全;思考

**[DOI]** 10.12252/j.issn.2096-627X.2021.04.1732

## 一、计算机网络安全概述

所谓计算机网络安全,包括硬件、软件和维护技术工具。同时,防止外部干扰的能力也是一个必要的条件。一般来说,确保网络信息安全是减少信息系统损失的有效措施。我国已经进入了信息时代,计算机网络技术得到了飞速的发展,网络信息安全也应进一步提高。

(一)计算机网络安全随着信息和通信技术使用日益增多,计算机网络安全问题也日益与人们的日常生活联系在一起,特别是互联网的快速发展。利用互联网是一种非常方便的电子商务手段,如网上购物和网上银行,这些都与计算机网络技术密切相关。随着信息通信技术的发展,网络安全问题和网络犯罪越来越普遍,给人们的生活带来了很大的负面影响。这些问题都预示着在网络信息安全防范上要更加的严谨。在计算机技术的应用中,网络安全问题大多是由于用户缺乏安全意识造成的。第一,他们的网络安全意识相对较低,这使得犯罪分子有机可乘。第二,人们有自我追求的意识,他们只关心自己行为的安全。不了解他人网络的安全性,这实际上给了罪犯交易的机会。目前,随着计算机技术的迅速发展,黑客技术的发展也更加迅速,一些黑客面临着巨大的利益,窃取个人或商业信息。因此,在今后的计算机网络安全管理中应采取预防措施。

(二)计算机网络安全策略概述科学实施计算机网络安全战略是保证网络安全的重要措施。为网络安全提供不同的策略。针对计算机网络中存在的各种安全问题,采取适当的策略来发挥积极作用。该策略的主要目的是保证网络资源的安全和防止异常访问。一般将安全策略与其他策略相结合,不仅包括计算机网络后台的一般安全,设备的物理安全也是网络安全策略的重要组成部分。

(三)计算机网络安全特性随着科学技术的快速发展,计算机技术发生了巨大的变化。计算机网络安全具有系统性、复杂性和多样性的特点。互联网是一个开放的系统,它对网络安全的系统化至关重要。为了使计算机适应复杂的网络环境,有必要改进网络安全技术。在网络提供便捷服务的同时,各种形式或内容的网络安全问题也应多样化,满足各种安全问题。

## 二、网络安全的重要性

计算机网络安全的存在关系到每个用户的切身利益。与计算机网络安全相关的风险需要我们充分重视。首先,随着普通用户对网络的使用和依赖程度的不断提高,普通用户在计算机使用中的网络安全已经变得尤为重要。其次,计算机网络安全威胁着企业的发展。第三,计算机网络安全风险的存在影响着计算机的发展和进步。它是计算机进步的标志,是计算机网络安全发展的核心。

## 三、计算机应用中存在的网络不安全因素

首先,计算机网络环境。在网络环境中,影响整个系统的主要问题往往是最重要的。如果运行设备外部的问题没有解决,可能会导致一些安全问题和其他恶意操作,从而给设备带来损坏。其次,计算机设备安全。路由器、服务器、交换机等设备在计算机运行过程中的信息流和网络通信中起着非常重要

的作用。许多硬件的正常运行直接影响到计算机网络的工作状态。计算机网络的建立必须坚持科学的原则,确保整个网络的安全,采取有效措施优化整个网络,适应计算机网络安全。对影响设备正常运行的环境必须严格控制,并进行日常维护。最后,计算机软件的安全性。许多与网络安全相关的问题都是由此引起。每个软件都有它的弱点。随着科学技术的发展和进步,如果不及时修复,就会受到病毒的攻击。应用程序本身对计算机内部信息资源有不同的调用权。在蓄意攻击的情况下,数据将丢失。

## 四、计算机应用中的网络安全措施

(一)计算机网络安全管理系统的改进加强IT安全管理的控制能力是解决安全管理中存在问题的有效途径。作为计算机网络安全运行管理的一部分,有必要建立规范的企业管理制度,对企业和个人的行为进行控制,以减少安全事故的发生。此外,应根据不同主题制定不同的应急预案;一旦发生网络安全事故,应尽快解决问题,减少损失,尽快恢复正常运行。管理制度是工作的基础和关键。设备运行标准和规则是保证计算机网络安全的重要条件。这就是为什么网络的使用和运行必须基于管理。

(二)通过防火墙更新病毒数据库防火墙是保证计算机应用网络安全的有效手段。它可以检测,过滤木马等。防火墙使计算机有可能将用户与其他不安全的网络隔离,并保护他们免受其他网络的干扰。

(三)信息加密密码在计算机网络安全中有着广泛的应用。在计算机的使用中,数据加密可以用来保护计算机安全,防止黑客的随机攻击。主要通过数学、电子、通信和信息学的合作,利用密码来提高计算机网络安全。为了保证计算机网络安全运行,计算机操作员必须输入和管理密码。同时,为了将计算机访问控制技术应用于计算机用户,用户必须输入相应的密码和控制文件权限来验证自己的身份,同时限制其他未经授权的入侵行为。

(四)提高公众安全意识造成计算机网络安全相关事故的部分原因是用户缺乏安全意识。因此,有必要提高计算机用户的安全意识和隐私意识。因此,有必要创建一个计算机和web应用程序相结合的计算机环境。随着科学技术的发展,网络安全形势不容乐观。

(五)加强硬件和软件管理计算机网络安全用户应定期维护和完善设备,通过访问权限进行有效的战略监控和更加多样化的认证方式。使用计算机的人也必须养成良好的习惯,定期更新软件系统,减少软件漏洞。

为了保证网络的正常运行,有必要建立一个计算机保护系统,确保和提高网络安全管理。避免无保护的网站,不断改善管理和更好地保护网络安全。

## 参考文献

- [1] 闫奕. 浅析大数据时代下计算机网络信息安全问题[J]. 数码世界, 2020, (7): 82.
- [2] 王桂梅. 基于大数据时代下计算机网络安全思路及对策[J]. 电子世界, 2020, (12): 97-98.