基于网络信息安全技术管理的计算机应用

李志新
津燃华润一分公司　天津　300060

摘　要：自我国进入现代化信息时代以来，互联网在人们生活的方方面面都有着广泛的应用，人们也已经习惯了互联网带来的便利。在人们享受这网络时代带来的方便的同时，也要警惕网络信息的安全问题。健康的网络可以为人们的生活和工作带来很大的便利，而不安全的网络环境又潜藏着对人们信息泄露的隐患，为人们的生活带来危害，因此怎样在使用计算机的时候，保证网络信息的安全性，已经成为人们关注的重点问题。

关键词：网络信息安全；计算机应用；技术管理；有效途径

引言

随着计算机技术的快速发展和互联网的广泛应用，网络信息安全问题越来越受到人们的关注。网络信息安全技术管理是确保信息安全性、保密性和完整性的重要手段，在计算机应用中具有重要意义。论文将探讨基于网络信息安全技术管理的计算机应用，以期提高人们的安全意识和保障信息安全，同时希望给从业者带来一些建议和参考。

1 常见的计算机网络信息安全问题

计算机网络信息安全是当前计算机信息技术发展的重要组成部分，也是社会各界关注的焦点问题之一。随着计算机网络信息技术的快速发展，网络信息安全问题也日益突出，给企业和个人的利益带来了极大的威胁。下文将介绍常见的计算机网络信息安全问题及其产生的原因和防范措施。

1.1 黑客攻击

黑客攻击是计算机网络信息安全面临的最大威胁之一。黑客通过各种手段入侵计算机网络系统，获取未授权的数据、破坏系统或服务、植入恶意软件等，对企业和个人的利益造成了极大的损害[1]。黑客攻击的主要方式有：1）暴力破解攻击。暴力破解攻击是一种常见的黑客攻击方式，指黑客通过尝试各种密码、账号等组合，强行破解系统或服务的登录口令，从而获取未授权的数据或权限。2）零日漏洞攻击。零日漏洞攻击是指黑客利用系统或应用程序中未公开的漏洞，在漏洞被公开前进行攻击，获取未授权的数据或权限。

1.2 病毒感染

病毒感染是另一种常见的计算机网络信息安全问题。计算机病毒是一种恶意软件，通过复制自身代码来传播，并在传播过程中不断复制自身，对计算机系统造成极大的危害。病毒感染的主要方式有：1）网络下载感染。网络下载感染是指用户从互联网上下载带有病毒的软件或文件，导致计算机系统被病毒感染。2）邮件附件感染。邮件附件感染是指通过电子邮件附件传播病毒，诱导用户打开恶意附件或下载病毒文件。3）USB设备感染。USB设备感染是指通过使用染有病毒的USB设备，将病毒传播到连接的计算机系统中。

1.3 数据泄露

数据泄露是指未经授权的数据泄露或丢失，包括内部人员泄露、外部人员泄露以及数据丢失等情况。数据泄露的主要方式有：1）内部人员泄露。内部人员泄露是指企业内部员工未经授权将敏感数据泄露给外部人员或发布到公共网络上。这种泄露方式通常因为企业缺乏必要的数据保护措施和意识所致。2）外部人员泄露及破坏：外部人员如黑客、特洛伊木马等利用漏洞或病毒入侵企业系统，窃取或破坏敏感数据；或者企业内部员工疏忽大意，将敏感数据泄露给外部人员。这种泄露方式可能对企业的声誉和经营带来严重损失[2]。3）数据丢失。数据丢失是指由于系统故障、灾害等不可抗力因素导致数据丢失或损坏的情况发生，这种泄露方式可能是由于企业没有做好数据备份和恢复工作所致。

2 网络信息安全技术管理的重要性

网络信息安全技术管理在现代社会中的重要性不容忽视。随着信息技术的迅猛发展，网络已经深入到各个领域，人们对网络依赖的程度也在不断加深。然而，与此同时，网络安全问题也日益凸显。网络信息安全技术管理的重要性主要体现在以下几个方面：

2.1 保障个人信息安全

网络信息安全技术管理可以有效地保护个人信息安全。在网络时代，人们的许多个人信息都存储在网络中，如姓名、地址、电话号码、密码等。如果这些信息没有得到充分的保护，就可能被黑客盗取，甚至被不法

分子利用，给个人带来严重的经济损失和精神损失。

2.2 维护国家安全和社会稳定

网络信息安全技术管理对于维护国家安全和社会稳定也具有至关重要的作用。网络是信息传递的主要渠道之一，如果网络信息安全得不到保障，就可能给敌对势力可乘之机，利用网络进行各种攻击、破坏社会稳定。

2.3 保护企业和机构的经济利益

网络信息安全技术管理还可以有效地保护企业和机构的经济利益。企业和机构在网络中存储了许多重要数据和机密信息，如果这些信息被黑客盗取或遭到破坏，就会给企业和机构带来严重的经济损失。此外，网络安全问题还可能影响企业的声誉，甚至引发法律责任。

2.4 促进信息化建设的安全发展

网络信息安全技术管理有助于促进信息化建设的安全发展[3]。随着信息技术的不断发展，网络安全问题越来越成为信息化建设的瓶颈。只有通过加强网络信息安全技术管理，才能保证信息化建设的安全性和稳定性，推动信息化建设的可持续发展。

2.5 增强国际间信息合作和交流的安全性

网络信息安全技术管理还有助于增强国际间信息合作和交流的安全性。在全球化的背景下，各国之间的信息交流和合作越来越频繁。然而，网络攻击和网络犯罪是全球性的威胁，只有通过国际合作和交流，才能有效地应对这些威胁，保障国际间信息合作和交流的安全性。

3 基于网络信息安全技术管理的计算机应用策略

随着信息技术的快速发展，计算机网络已经成为企业和个人日常生活中必不可少的组成部分。然而，与此同时，网络信息安全问题也日益突出，给企业和个人的利益带来了极大的威胁。基于网络信息安全技术管理的计算机应用策略是解决这一问题的重要手段之一。下文将从以下几个方面阐述基于网络信息安全技术管理的计算机应用策略。

3.1 加强网络安全意识和培训

加强网络安全意识和培训是保障网络安全的第一道防线，也是解决网络安全问题的根本。企业和个人应该加强网络安全意识培训，提高员工的安全意识和安全防范能力。具体措施包括：1）定期开展网络安全意识培训。企业和个人应该定期开展网络安全意识培训，提高员工对网络安全的重视程度和意识水平。培训内容可以包括网络安全的基本知识、常见的网络攻击手段和防范措施、密码安全等。2）可以把每个月固定的一天作为网络信息安全的宣传日，通过对相关的网络信息安全的法律法规的宣传，还有一些网络信息安全的实例的宣传，提高民众的网络信息安全的防范意识，也促使网络信息安全环境朝着健康的方面发展，为广大民众提供和谐的、安全的网络信息环境。3）开展网络安全知识竞赛。企业和个人可以开展网络安全知识竞赛，通过比赛的形式让员工更加深入地了解网络安全知识和技能，同时也可以增强员工的团队协作能力和凝聚力。

3.2 建立完善的网络安全体系

建立完善的网络安全体系是保障网络安全的重要措施之一。具体措施包括：制定严格的网络安全管理制度、建立网络安全审计机制、实施网络安全监控和预警机制等。1）制定严格的网络安全管理制度。制定严格的网络安全管理制度是保障网络安全的基础，包括安全策略、安全漏洞管理制度、安全事件处理制度等。2）建立网络安全审计机制。建立网络安全审计机制可以及时发现和解决网络中存在的安全问题，包括日志审计、入侵检测等。

3.3 合理配置安全设备和软件

全设备和软件的配置是保障网络安全的重要措施之一。具体措施包括：1）合理配置防火墙、入侵检测系统等安全设备和软件，及时更新系统和软件补丁，禁止使用弱密码等不安全的配置。2）合理配置安全设备和软件。安全设备和软件的配置是保障网络安全的基础，应该根据网络拓扑结构和业务需求来选择合适的安全设备和软件，并进行合理的配置。例如，防火墙应该禁止不必要的端口和协议，入侵检测系统应该配置相应的规则和检测引擎等。3）及时更新系统和软件补丁[4]。及时更新系统和软件补丁是保障网络安全的重要措施之一，可以修补系统或应用程序中存在的漏洞和缺陷，从而提高系统的安全性。4）禁止使用弱密码等不安全的配置。弱密码等不安全的配置是网络攻击者攻击的重要目标之一，因此应该禁止使用弱密码等不安全的配置，并定期更换密码。

3.4 使用安全软件和使用安全通道

使用安全软件和使用安全通道是保障网络安全的常用措施之一。具体措施包括：1）使用加密软件来加密重要数据和文件。加密是一种保护数据不被窃取的重要手段之一。使用加密软件可以对重要数据和文件进行加密，从而保护数据不被非法访问和使用。例如，BitLocker可以对Windows系统中的数据进行加密，Symantec Endpoint Encryption则可以对整个硬盘进行加密。2）使用VPN来连接远程办公和访问公共网络时可以保证数据的安全传输。VPN是一种可以在公共网络上建立加密通道的技术，通过这种技术可以使远程办公或访

问公共网络时数据传输的安全性得到保障。例如，Cisco ASA、Juniper Networks、Microsoft Azure等都提供VPN服务。3）使用安全浏览器可以防止浏览器被攻击和窃取数据。安全浏览器可以保护用户的隐私和数据的安全性。例如，Google Chrome、Mozilla Firefox等都具有内置的安全浏览器功能，可以防止恶意软件的入侵和窃取数据的行为。

3.5 加强重要数据的备份和恢复

加强重要数据的备份和恢复是保障网络安全的重要措施之一，即使在加强安全防范的情况下仍然可能会出现数据丢失或损坏的情况因此备份重要数据和及时恢复可以保证业务正常运行和避免损失具体措施包括：1）备份重要数据。备份重要数据可以采用定期备份和实时备份两种方式，定期备份是指定期将重要数据备份到本地或云端存储设备中，实时备份是指将重要数据备份到云端存储设备中。实现实时备份备份数据可以实现数据的快速恢复和容灾能力2）及时恢复。当数据丢失或损坏时应该及时恢复。数据的恢复可以采用手动恢复或自动恢复两种方式，手动恢复是指通过手动方式将备份数据恢复到原始位置，自动恢复是指通过设置自动恢复策略将备份数据自动恢复到原始位置。

3.6 加强供应链安全管理

加强供应链安全管理是保障网络安全的重要措施之一，可以避免由于供应链环节中的问题而导致的网络安全性降低。具体措施包括：1）建立供应链安全管理制度。建立供应链安全管理制度可以规范供应链环节中的安全管理行为，包括供应商选择、合同管理、物流管理等。2）对供应链环节进行全面安全审计。对供应链环节进行全面安全审计可以及时发现和解决供应链中存在的安全问题，包括供应商风险、物流风险等[5]。3）与供应商签订安全协议。与供应商签订安全协议可以明确供应链环节中的安全责任和要求，从而规范供应商的行为。例如，可以在合同中加入安全条款，要求供应商保证其提供的服务和产品符合安全标准。

3.7 加强网络安全监测和应急响应

1）运用安全监控技术。为了更有效地检测网络安全漏洞和攻击行为，需要运用多种安全监控技术。例如，可以部署入侵检测系统（IDS），它可以实时监控网络流量并检测异常行为。另外，安全事件管理工具可以用于收集、分析、存储和报告网络安全事件，以便更好地了解网络安全状况并做出相应的响应。2）建立安全事件应急响应计划。在网络安全事件发生之前，应该建立安全事件应急响应计划，明确响应流程、责任人和响应时间。同时，应该定期进行应急响应演练，以提高应对网络安全事件的能力。3）加强安全漏洞管理。安全漏洞管理是网络安全监测和应急响应的重要环节。对于已发现的安全漏洞，应立即采取措施进行修复，同时加强对漏洞的监测和预警。可以采用安全漏洞扫描工具，定期对系统和应用程序进行扫描，以便及时发现并修复安全漏洞。

结语

在目前的计算机应用过程中，需要有效保障计算机网络系统运行的安全性，而网络信息安全技术管理是这一目标实现的基础与前提。因此，作为计算机用户及管理人员，应当对计算机网络信息安全问题加强重视及认识，意识到网络信息安全技术管理的价值及意义，并且需要对各种网络信息安全管理技术加强掌握及应用，以满足网络安全的实际需求及要求，使网络信息的安全性得到保证，同时保证计算机网络系统的稳定安全运行，满足计算机应用的需求及要求。

参考文献

[1]陈少军.基于网络信息安全技术管理的计算机应用探讨[J].信息记录材料，2021，22（06）：68-70.

[2]申桐.基于网络信息安全技术管理的计算机应用[J].数字技术与应用，2021，39（05）：178-180.

[3]吴海威.基于网络信息安全技术管理的计算机应用分析[J].无线互联科技，2021，18（07）：31-32.

[4]方周泉.基于网络信息安全技术管理的计算机应用[J].科技风，2021（08）：86-87.

[5]孙海霞.基于网络信息安全技术管理的计算机应用初探[J].科技创新导报，2018，v.15；No.437（05）：143-144.