加强网络安全管理，保障计算机信息安全

郭丰收
中原运维海外工程有限公司　上海　200233

摘　要：文中全方位分析了当前网络信息安全计算机信息安全的状况，并给出对应的管理模式与实践对策。首先，文中归纳了网络信息安全计算机网络信息安全面临的主要挑战风险性。接着，论述了加强信息安全管理工作的各种对策，包含提升网络信息安全组织架构、健全管理制度、技术革新及应用等，阐述了网络安全知识和人才培养的必要性。除此之外，文中还详细阐述了建立信息保护管理体系、执行数据库加密和个人隐私保护综合性制度等保障计算机信息安全的重要对策。

关键词：加强；网络安全管理；保障；计算机；信息安全

引言

在信息科技飞速发展的今天，网络信息安全计算机数据安全问题日益突显，变成维护国家、公司稳定性和私人信息的关键所在。伴随着技术的进步，黑客攻击方式不断完善，给信息管理系统增添了严峻的考验。因而，加强信息安全管理方法，保证电子计算机网络信息安全至关重要。下面我们就讨论现阶段网络信息安全面临的主要威胁，剖析目前安全管理的不足，并给出高效的战略规划和对策，以提升网络安全保护水平，确保信息网络资源的安全运行。

一、网络安全与计算机信息安全的现状

1.网络安全现状概述

伴随着互联网的兴起与发展，网络信息安全日益凸显，现阶段，黑客攻击方式多元化，网络黑客、病毒感染、木马病毒等恶意程序五花八门，对网络信息安全构成巨大威胁。此外，由于5G的兴起，随着物联网、大数据等新技术的广泛运用，黑客攻击面不断发展，网络空间的复杂性不断增长，促使网络安全形势更加严峻。在网络信息安全现状下，各种各样黑客攻击屡屡发生，给公司、政府与本人增添了比较严重损失。钓鱼攻击、勒索病毒、DDoS攻击等攻击手段司空见惯，给网络用户的信息安全带来很多风险性。除此之外，互联网数据泄露、电信诈骗、网络盗窃等诸多问题也屡见不鲜，促使网络信息安全日益成为社会关注的重点。

2.计算机信息安全现状分析

计算机网络信息安全遭遇多方面考验。最先，黑客入侵方式日益严重，安全漏洞的应用造成重要数据泄漏。次之，网络病毒、木马病毒、勒索软件等各类恶意软件严重危害网络信息安全。与此同时，社交网络和电子商务的高速发展增加了客户个人隐私泄露风险。信息系统多元性扩大也使经营管理和维护比较困难，增加了安全隐患。因而，企业和机构应增加对网络信息安全的研发投入，采纳先进技术和策略。这包括部署智能化的安全检查系统软件、实施双因素认证以及加强数据信息管理和策略执行。

二、加强网络安全管理的策略与实践

1.网络安全管理体系建设

（1）网络安全组织架构的优化

在建立互联网安全风险管理时，需要优化网络信息安全组织架构，确立各个安全管理机构的职责和管理权限，确保网络安全管理方法的顺利进行。首先，要建立和完善网络安全防护组织，包括互联网安全领导小组、网络信息安全负责部门和信息安全技术支持团队等。进一步明确各个部门职责和协作机制。次之，要构建网络安全专家精英团队，提供优质的技术支持和具体指导，快速响应网络安全问题，积极应对网络安全隐患。

（2）网络安全管理流程的完善

在加强信息安全管理工作的战略规划和实践中，首先，建立一个完备的网络安全防护步骤，可以确保网络信息安全措施全面推行，提升网络安全防护的效率和稳定性。次之，通过确立网络安全防护的工作流程和明确职责分工，可以有效地规范网络安全防护活动，避免重复管理和信息交叉的问题。除此之外，完美的网络安全

防护步骤还能帮助机构及时发现和解决网络安全问题，提升应急处置的效率和精确性，降低网络信息安全损害。

2.网络安全技术创新与应用

（1）先进网络安全技术的研发

由于黑客攻击方式的不断升级和演化，传统信息安全技术已经无法满足现阶段错综复杂的安全需要。因而，开发设计前沿的信息安全技术已经成为当前网络安全防护的重要问题之一。首先，科研人员已经积极推进基于大数据的威胁检测、虚拟技术的安全隔离等新型安全防护技术，为应对传统式网络防火墙、入侵检测技术等网络安全产品的局限。这类技术结合实际取得了一定的成效，并逐步得到广泛应用。次之，对于新起的网络环境，如WiFi网络和物联网，也需要采用更为先进的安全策略和技术来应对特有的安全挑战和威胁，以保障这些日益普及的技术平台的安全性和用户的数据隐私。

（2）网络安全技术在实践中的应用

企业能够利用先进的信息安全技术，如网络防火墙、杀毒软件和入侵检测技术，有效预防黑客攻击和恶意软件威胁。次之，建立安全性密钥管理体制，限定职工访问限制，强化对核心数据及系统的维护，避免内部员工或外部网络黑客不法侵害和盗取。除此之外，计算机设备的网络安全问题应定期检测和恢复，以保证互联网产品的安全和稳定，从源头上提升网络安全防御水平。

3.网络安全教育与培训

（1）提升公众网络安全意识

政府机构应加大对网络信息安全的宣传力度，通过一些媒体渠道向社会传递互联网安全防范措施，提高公众对网络安全的了解。次之，学校及企业需要加强信息安全文化教育，塑造学生与员工的信息安全意识，普及网络安全文化教育，让她们识别避开网络安全风险。除此之外，社会组织和网络安全专业工作人员也可以通过各项活动和专题讲座向社会普及文化网络安全教育，引导大家提升信息安全意识。要提高公众信息安全意识，还需要加强监督和管理，政府机构可以形成互联网资产评估机构。

（2）网络安全专业人才培养

高等院校网络安全专业设置为培养网络安全人才的前提，不断优化课程体系，引入国内外先进的教育资源与技术，塑造学生具有扎实的理论基础和实践技能。次之，要加强与企业的合作，进行实习培训，使学生在日常工作中学习实践与运用信息安全技术，提升实践技能。除此之外，提升教师队伍建设，引进国内外优秀专家及老师，构建跨领域互动平台，推动老师与学生学术交流合作，不断提升网络信息安全人才培养模式。

三、保障计算机信息安全的措施与方法

1.信息安全防护体系建设

（1）信息安全防护策略的制定

要建立和完善信息安全管理体系，确立网络安全管理的职责分工和程序。要全面评估各种安全风险，从内部人员、外界攻击、安全漏洞等方面进行，为制定具体的安全防护对策提供参考。在制定具体对策时，各种各样的方式方法，包含电脑防火墙、入侵检测技术、数据库加密等。应根据实际情况熟练掌握，以多层面、多层次的方法维护计算机网络安全。除此之外，还要逐步完善和优化信息安全管理体系，不断完善的信息安全监测和应急安全防护创新机制，及时发现和响应机制。

（2）信息安全防护技术的实施

技术性信息保护的实施是保障电子计算机网络信息安全的重要环节。第一，企业可以创建网络防火墙、入侵检测技术。（IDS）及其入侵检测系统（IPS）完成对网络通讯的监控和过滤，及时发现和阻拦隐性的网络安全风险等手段。第二，加强对计算机设备和app的被动安全和更新，及时修复已经知道的系统漏洞，避免网络黑客利用系统漏洞侵略系统软件。除此之外，网络安全技术的实行还包含提升身份验证体验，选用多因素认证、感应卡等新技术，确保用户真实身份真实有效，避免未经授权的页面访问系统软件。除此之外，加密算法都是信息保护的关键所在方式，运用加密技术对隐私数据进行加密，确保数据在传输存储过程中的安全。根据对各种各样信息保护科技的综合运用，可以有效提高计算机软件安全性，确保系统和数据的安全性和完整性。

2.数据安全与隐私保护

（1）数据加密技术的应用

选用适宜的加密技术进行数据加密，可有效地防止数据泄漏和伪造，确保数据的商业秘密性和完整性，进而有效地防止数据泄漏和伪造。常见的加密技术主要包括对称加密算法和对称加密。对称加密算法就是指发布者和接受者使用相同的密匙开展加密和解密。该加密方法简单有效，适用于对数据传输速率要求高的情景。DES是一种常见的对称加密算法、AES等。可是，对称加密算法安全性极度依赖于密匙的维护，密匙的传输和监督是非常重要的。应用公钥和私钥对对称加密开展加

密和解密，公钥能够对外公布，公钥由接收者存放，用以破译接收到的加密数据。在电子签名、安全可靠传送等场景下，RSA和DSA等非对称加密算法得到广泛应用。虽然对称加密安全性较高，但是由于计算复杂，常与对称加密算法配合使用，从而达到安全和高效率平衡。hash算法除对称加密算法和对称加密外，还可以用于数据库安全验证和电子签名。在信息保护服务体系中，加密技术的使用不但可以确保网络信息安全，而且还能提高整个计算机网络安全性。

（2）隐私保护政策的制定与执行

为保证计算机软件的安全性，制定和实施个人隐私保护现行政策尤为重要。首先，个人隐私保护现行政策应该以相关法律法规为基础，确立个人信息收集、存放、使用及传送具体要求，确立企业维护个人信息安全承诺。第二，公司要高度重视内部人员的个人隐私意识教育，加强员工对个人隐私保护现行政策的认识和重视，才能做到真正重视用户的隐私。除此之外，公司还应当不断完善个人隐私保护体制，如建立专门个人隐私保护精英团队或分派特殊部门制定和实施隐私协议，以保证隐私协议的全面推行。企业还应经常评定和审计个人隐私保护现行政策，及时发现和改正需要注意的问题，逐步完善个人隐私保护管理体系，确保用户数据库的安全。

3.信息系统安全加固

（1）系统漏洞的及时发现与修复

在确保电子计算机网络信息安全的过程当中，及时发现和修补安全漏洞至关重要。首先，企业及机构应当建立定期进行的漏洞扫描系统和检查体制，以确保系统的全方位定期检查评定，并及早发现潜在性的漏洞。次之，针对已经知道的漏洞，应及时采取措施进行处理，安全风险能通过升级补丁和更新系统版本来减少。与此同时，安全团队必须及时跟踪和监控系统漏洞，以保证漏洞补丁工作中得到充分执行。

（2）安全加固技术的应用与实践

结合实际安全加固技术的发展与实践主要包含：首先，要建立和完善漏洞管理体制，及早发现系统漏洞，制定合理的修复计划。通过定期扫描漏洞和更新补丁，能够降低系统软件黑客攻击风险。次之，要高度重视系统的安全软件配置管理，包含核查和改进电脑操作系统、应用软件和互联网设备的安全配备。根据限定操作权限、开启网络防火墙、传输加密信息等对策，提升系统安全性，避免未经授权的浏览和数据泄露。

结论

伴随着信息内容技术的不断发展，网络信息安全计算机信息安全的威胁日益提升，已成为社会关注的重点。文中给出了加强信息安全管理方法的思路与实践，及其确保电子计算机信息安全的措施，根据分析当前网络信息安全计算机信息安全的现况，建立和完善互联网安全风险管理，推动网络信息安全技术创新与应用，加强信息安全教育培训，可以有效提高网络信息安全整体保护水平。与此同时，创建信息保护系统软件，并执行数据信息安全与隐私保障措施，以提升信息内容的总体安全性。

参考文献

[1]王秀玲.探究计算机信息管理中的网络安全对策[J].中国新通信，2023，25（16）：117-119.

[2]邱义.大数据时代的计算机网络安全防护研究[J].通信电源技术，2023，40（14）：223-225.

[3]陆卓遥.大数据背景下计算机网络安全问题与对策[J].网络安全技术与应用，2023（5）：62-63.

[4]时进.高校网络安全防护中的计算机信息管理技术应用分析[J].网络安全技术与应用，2022（8）：88-90.

[5]曾容.计算机网络办公自动化及安全策略研究[J].科技资讯，2022，20（18）：30-32.

[6]何宝海.网络安全管理技术研究[J].科技创新与应用，2022，12（30）：177-180.

[7]杨坤平，李卫峰.基于人工智能的高校计算机网络信息安全研究[J].长江信息通信，2022，35（9）：137-139.

[8]姚浩立，徐振宇，李从初，等.大数据环境下信息网络安全防范措施研究[J].通讯世界，2023，30（8）：61-63.

[9]赵霞.网络安全技术在计算机安全管理中的应用分析[J].通讯世界，2023，30（2）：49-51.

[10]毕然.信息工程建设中计算机网络安全问题及对策探究[J].成才之路，2021（1）：48-49.