新时期网络信息安全应对策略

陈 傲

西交利物浦大学智能工程学院 江苏苏州

【摘要】在大数据环境下，网络信息和服务应用犹如一把双刃剑。随着它的快速成长，为全国乃至各行业的客户带来巨大而良好的经济成长机会。但与此同时，也面临着日益复杂、庞大、严峻的网络信息安全风险，影响到网络的应用，阻碍信息时代的进步。因此，有必要对新时期的网络信息安全问题进行分析，制定有关的安全应对对策，从而发挥出新时代网络的价值。

【关键词】大数据；网络信息安全；危机应对与策略

【收稿日期】2022 年 11 月 6 日 【出刊日期】2022 年 12 月 21 日 【DOI】10.12208/j.aics.20220074

New era network information security coping strategy

Ao Chen

Xi'an Jiaotong-liverpool University

【**Abstract**】In the environment of big data, network information and service application is like a double-edged sword. With its rapid growth, for the whole country and all industries of customers to bring huge and good economic growth opportunities. However, at the same time, it also faces the increasingly complex, huge and severe network information security risks, which affect the application of the network and hinder the progress of the information age. Therefore, it is necessary to analyze the network information security problems in the new era and formulate relevant security countermeasures, so as to give play to the value of the network in the new era.

【**Keywords**】Big data; Network information security; Crisis response and strategy

引言

网络信息数据库是人们在生产和生活中用于查询一些重要数据的信息库，其中包含当前各种社会生产、生活、经营和管理中的一些重要网络数据。在互联网大数据的影响下，网络信息涉及的数据量显著提高，与此同时，互联网传播的速度也在迅速加快。人们经常会充分利用海量的网络信息来促进日常的生产作业和学习。在生活和等待的过程中，不可避免地会面临个人信息被盗泄露、黑客恶意入侵系统等一连串问题。由此，网络信息数据的安全保障也受到更多的关注。

1 研究背景

1.1 社会层面

网络应用越来越社会化。随着社会基础设施系统的数字化程度不断提高，可能会出现严重的问题，如网络控制权高度分散造成的信息安全管理问题，其中包含社会生命线网络和计算机核心控制系统，其中包含规模较大的政府网站，国防和通信系统设施、电力控制网络系统、商业和金融系统基础设施，极有可能面临恶意网络入侵攻击，最终造成信息系统故障、摧毁、瘫痪，社会秩序势必面临非常严重的风险。数据调查显示，国家各个领域的反计算机网络犯罪和惩治网络文化侵权行为，无论是在数量上、手段上、性质上、规模上，都可能达到了相当骇人听闻的程度[1]。

1.2 个人层面

一手机携带和存储了大量的用户信息，涉及个人身份信息、教育健康、娱乐消费、银行网络支付业务等。因此，个人生活中的手机信息存储安全也面临着严峻的考验，面临一定程度的风险。一是信

作者简介：陈傲（1998-）男，汉，山东滨州，硕士，研究方向：应用信息学。

息泄露，个人信息在未经书面授权的情况下被恶意窃取、滥用、复制、恶意传播；二是信息污染，个人信息未经用户授权被用户恶意篡改。

2 新时期下网络安全影响因素

鉴于网络具有很强的开放性和共享性，这给群众带来了方便。例如，用户在搜索相关信息资源时，能够快速检索到自己想要的内容。但是，某些黑客可能会借助此功能在下载的文件中植入病毒和特洛伊木马。很多文件资源在上传到网络平台之前没有通过安全检测，就会被用户直接下载，隐藏的木马病毒等窃取用户信息，进一步降低了网络平台的安全系数。网络传输形成的蠕虫种类繁多，同时漏洞管理工作本身也提高了很大程度的研究难度。病毒的存在会破坏整个计算机系统，严重时会造成所有文件损坏，系统瘫痪，无法运行。如果用户防范意识低下，或者系统安全级别低，就很容易受到一些不安全因素的困扰[2]。

有些软件存在安全隐患，无法面对不法分子的攻击。有些软件存在很多漏洞，给黑客留下可乘之机，从而致使软件信息和用户信息泄露。软件设计者没有考虑安全问题，从而致使设计不严谨，软件缺乏自我保护功能。在网络平台上，一些平台的管理员缺乏职业道德，会泄露用户信息、窃取机密文件，这在某种极大的角度上看来提高了网络平台的危险性。一些本地软硬件防护等级不高，防护系统不完善，面对病毒等文件时缺乏抵抗能力。另外，很多用户安全意识不强，综合素质不高，在开展相关工作时不够严谨。

3 网络信息安全的应对策略

3.1 访问控制策略

通过采用访问控制能够对网络用户的网络分类和网络访问级别进行有效控制。用户系统将结合特定的网络层级要求，对服务器、终端、数据、存储网络等几大资源节点的所有网络层访问行为进行有效控制。网络系统管理员应定期详细检查系统中是否存在一些未经授权的访问行为，特别是经常查看具备合法访问权限或更高访问网站权限的用户判断他们的在线活动是否合法。为保证一些外部黑客不能借助远程访问部分系统 Guest 账户来控制用户的计算机，计算机系统管理员应定期访问计算机系统默认配置中的部分系统 Guest 账户禁止远程访问[3]。另外，为有效防止计算机被病毒非法入侵，系统 Administrator 账户的管理员应定期更改系统账户名称，同时进行强制性设置，进一步增强对安全账户密码的保护功能和验证系统用户密码，对加固电脑系统网络信息安全工作无疑起到了非常有效和很好的管护作用。采取使用访问控制的安全策略，为网络系统的运行带来了保障，其中包含系统的机密性、完整性、可用性和稳定性能够进一步增强，并提供十分强力的保障，为了系统安全提供最有效的技术支持。

3.2 防火墙策略

防火墙系统主要由两部分组成：网络硬件设备系统和防火墙网络安全管理软件。在虚拟局域网中，在外部和内部互联网设备系统之间逐步形成一道防火墙，加载防火墙管理软件进行物理安全保护或隔离障碍。计算机内部的所有网络设备、通信网络命令程序和传输网络分组系统等硬件借助防火墙，保证用户的主机能够免受网络的影响，达到阻止非法用户入侵和保护主机的双重目的。防火墙本身已经起到了很好的网络自我保护作用。如果非法局域网的用户试图对网络进行恶意入侵和攻击，至少要通过防火墙设置的四道网络安全技术防线，才能入侵局域网的目标计算机。通常，专业的网络管理员会结合实际的网络安全工作情况和不同领域的需要，对防火墙系统功能进行适当的配置，具体的参数设置可能完全不同，保护功能的当然有一些区别。高级别的安全防护功能系统一般会自动予以一些安全监控服务，比如视频流等远程监控、实时流媒体监控功能等。防火墙系统能够对一些可疑的、陌生的用户与通信端口的用户数据进行系统检测。有效过滤和拦截，目标计算机还能够拒绝接收任何来自可疑和陌生用户的通信端口信息访问请求，从而避免病毒恶意运行。

3.3 数据加密策略

数据加密技术是指应用于网络数据防护的策略，是一种主动、安全的网络数据防御技术策略。其特点是能够采用多种数字密码方法对计算机信息系统中的信息数据进行加密，同时做到各种信息数据的加密存储和信息传输，更有效地保护用户网络数据信息和安全性能。依据安全技术和加密验证方法的分类，主要是指数据信息实时传输的加密、存

储和传输过程的加密以及信息数据完整性的识别和加密认证等。数据安全传输保护及端口加密技术主要包括数据端口的安全加密保护功能，可从单端口安全加密发展为多端口加密，其加密功能十分突出，它能够有效、安全地对网络上数据线路传输中存在的各种数据流信息进行加密[4]。密文安全存储方法和数据加密技术是目前另一种用于数据安全存储和加密管理的重要技术。密文安全存储方式一般是指算法转换、附加密码、加密存储模块转换等设计方法进行技术实现；用户访问数据权限控制管理系统的原理是借助算法，严格审查任何合法的用户资格和权限数据。借助审查权限级别，对数据进行严格的分级存储和操作限制，防止了一些重要数据信息被非法用户轻易窃取。同时，系统还能够自动限制任何数据使用者超越权限私自选用数据。数据完整性认证与验证技术专门用于对系统所有用户数据内容的真实、完整性以及系统进行认证，验证所有接入网用户实际输入的所有用户身份、密码、密码识别信息等相关信息内容的完整性，验证网络输入的真实性和安全特性验证客户网络的数据信息内容。用户系统实际预订数据的价值数据内容和网络安全参数值是否与所有真实数据一致，验证可信账户支持对数据源进行实时、安全的数据访问。

3.4 安全扫描策略

安全扫描检测是指对一台计算机系统或所有有关的网络设备系统进行一连串安全及相关数据的扫描检测，最终找出与当前网络中其他主机同时存在的网络端口，全面提供的网络服务，解决某些重要的系统信息、不正确的设备配置、已知系统的重大安全漏洞等。网络维护管理人员要积极选用网络安全漏洞扫描分析技术，及时自动调整优化计算机操作系统设备和实时更新网络应用，严防外部黑客恶意借助自身系统漏洞入侵

3.5 备份与恢复策略

数据信息的实时安全自动备份存储技术和自动安全容灾技术保护系统，是保障用户计算机信息存储安全和保密的重要工具，也是最终的保障。出于网络信息的安全性，促进达成的一种关键防护方法是客户网络系统在遭受外部恶意入侵和攻击后，合理且正确的、有效的被动入侵安全防御和保护技术。实时、定期备份存储网络数据信息文件，定期备份存储也是时刻保证数据安全的一种方式，是一种良好的维护操作习惯，而计算机网络也可能充满了各种未知的安全或入侵威胁，即使开始有效防范各种网络入侵威胁，并设置了有所关联的安全防护技术措施来防止黑客入侵以及恶意的攻击和入侵，但入侵行为是不可避免的，因此定期、有效地及时备份和保护计算机系统和数据文件等资源不可或缺。如果计算机系统突然受到黑客病毒的攻击，系统数据可能会被病毒意外破坏。并且当系统出现异常严重的故障时，系统容灾处理机制也应该得以快速、及时地做出响应，数据丢失会被迅速、及时地补救，尽可能效减少系统损耗[5]。

结语

网络信息应用安全建设是一项庞大、复杂、严谨的信息系统工程。近年来随着计算机技术的飞速发展和进步，以及新型网络工具的使用越来越广泛，面对当前对网络信息应用安全的入侵，为了防范环境中的各种网络威胁，应该仍着重于维护计算机网络信息应用安全中遇到的诸多实际问题，进一步增强和开展长期持续的主动探索、思考和对策研究，积极防范和应对当今网络领域的各种新威胁。一种新的安全态势，防止各种可能的外部入侵活动和对网络的破坏性攻击，确保网络信息的安全。

参考文献

[1] 石柱三. 新时代移动互联网信息安全与应对策略研究[J]. 科学与信息化, 2021, 000(015):61,63.

[2] 普布卓玛. 浅析新时期计算机网络信息安全问题及对策[J]. 信息周刊, 2019(29):1.

[3] 于彤, 杨红军. 新时期计算机网络系统信息安全的有效防范策略[J]. 无线互联科技, 2013(11):107-107.

[4] 李凯轩, 刘艳. 谈网络时代的信息安全问题以及应对策略[J]. 2021(2013-9):46-48.

[5] 刘传相. 物联网时代网络与信息安全风险及应对策略[J]. 重庆通信业, 2013(3):3.