计算机网络安全技术的影响因素与防范措施

王婷婷
北部战区海军　山东青岛　266071

摘　要：基于对计算机网络安全技术的影响因素与防范措施的研究，为了防止个人信息泄露以及因为操作不当带来的安全漏洞隐患，导致用户个人信息隐私泄露风险的产生。在这一背景下，研究计算机网络安全技术的影响因素，发现内部系统因素影响、外部环境因素影响、实际操作不规范因素影响等问题。因此，结合计算机网络安全技术的防范措施，对计算机网络安全技术进行优化，提出信息技术加密、身份信息安全认证技术、防火墙安全系统等策略。

关键词：计算机网络安全；影响因素；防范措施

Influencing factors and preventive measures of computer network security technology

Tingting wang
Northern Theater Navy, Qingdao, Shandong, 266071

Abstract: Based on the study of influencing factors and preventive measures of computer network security technology, in order to prevent personal information leakage and the emergence of security vulnerabilities due to improper operations, which can lead to the risk of personal information privacy breaches for users, research is conducted. In this context, the influencing factors of computer network security technology are examined, revealing issues related to internal system factors, external environmental factors, and non-compliant operational practices. Consequently, in conjunction with preventive measures of computer network security technology, optimizations are made to enhance the field. Strategies such as information technology encryption, secure authentication of identity information, and firewall security systems are proposed to bolster computer network security technology.

Keywords: computer network security; influencing factors; preventive measures

引言：

现阶段信息技术的飞速发展，人们的日常生活已经与计算机网络技术密不可分。通过网络技术开展的一系列活动中，存在一定的安全性问题以及安全隐患未得到有效的解决。需要人们在应用一段时间后，对个人信息进行及时更新与调整，同时对于密码的设置上，通过不同形式逐步增加网络黑客破解密码的难度。进而保障不法分子无法寻找漏洞，无法危害网络使用者的合法权益

一、计算机网络安全技术的影响因素

1.内部系统因素影响

但随着计算机网络信息技术的不断革新与发展，为进一步满足我同用户群体的切实需求而开发出的计算机应用系统类型，其数量上也在不断的扩增。大部分计算机应用系统已处于较完善阶段。同时在实际操作中仍然存在一定的，因操作不当产生的自身系统安全计方面缺陷，即是系统自身存在影响计算机网络信息安全的内部因素。同时，部分计算机的用户在实际使用本台计算机时，需要意识到操作系统自身存在一定的安全隐患问题，不存在完美的安全操作系统。因此，对于现阶段计算机操作系统与软件的安全性能，其描述上存在一定的夸大其词，或是对于安全问题多少存在一定程度上的，相对性指标作为依据[1]。

2.外部环境因素影响

如今，科技技术发达，计算机已经拥有较为先进的硬件设备以及软件设施配置，在计算机实际的运行过程中，容易产生因受到外部环境因素的影响，造成不同程

度的网络信息安全风险问题。同时，造成外部环境影响网络信息安全风险因素，主要是指受到网络黑客的信息化攻击。综上而论，网络非法分子通常会利用各种信息化手段并采集索要攻击的计算机目标信息，对其进行计算机远程系统数据的利用，并通过运用上述数据反复的对打击目标计算机进行多层次，多维度，多角度的扫描，从而找出所攻击计算机目标自身存在的网络安全漏洞，并瞄准这一网络信息漏洞，网络黑客逐步的破坏本台计算机所在的网络环境，进而造成人为因素影响计算机网络信息风险的发生。

3.实际操作不规范因素影响

计算机在系统实际操作的过程中，需要通过实施的更新在自身的软件、系统设备配置、不断的扫描自身系统漏洞并加以修复，进而在一定程度上保障计算机系统在实际运行过程中的安全性。大部分用户在使用计算机的过程中，鲜少有更新系统、更新软件的良好习惯、部分安全防护软件与用户的计算机系统配置难以融合且不适配等问题。均在一定程度上造成用户信息泄露、系统存在漏洞风险、容易遭受网络黑客的攻击。在计算机WEB服务器运行的过程中，部分系统对于主机用户在实际的操作行为不会设置相应的限制，并在一定程度上会造成网络黑客的入侵、盗取该系统、此IP地址的用户信息等现象的发生。同时在计算机实际操作的过程中，计算机系统自身存在一定的漏洞风险，当计算机系统未能得到及时的更新以及完善漏洞补丁等遗留问题入侵当前系统。与此同时，在计算机运行的过程中，其网点配置存在一定的不科学、不合理现象，进而在一定程度上会造用户成网络信息风险、信息安全泄露等相关问题。并且如果当前网络系统整体处于网络波动状态时，较为容易增加黑客入侵系统的风险几率。

二、计算机网络安全技术的防范措施

1.信息技术加密

部分计算机拥有主动型防护技术，如针对用户信息加密，就属于该技术领域。该项技术可以运用加密计算的方法，将文件转换成为密文，不允许非法用户读取密文数据。同时，在网络计算机安全管理中，通过运用该项，技术对用户信息加密在一定程度上可以保证数据的完整性与数据信息的安全性。可以通过采用不同算法进行不同的用户信息加密，如：对称加密、非对称加密两种加密技术实际运用在对当前系统用户信息加密手段中。

如在对用户信息加密中，采用对称加密技术，通常是指可以通过解密匿名中推算出加密密钥，用过利用解密计算重新获得原文进是对称加密技术。如在对当前用户信息数据进行加密时，我们通常运用DES值，既对称加密技术的核心算法；通过运用这以数据加密的密标准，在一定程度上可以有效的防范，部分未经过用户授权下产生的用户数据泄密情况发生。针对des的算法中，其中包含了data key mode三个入口参数[2]。针对上述三个入口参数逐一进行较为系统化的分析，首先，Data参数可以理解为被加密（被解密）的数据；其次，KEY代表密钥；最后，Mode可理解为数据工作模式。其实际的算法可以理解为如：Mode在被加密的工作模式下，用户通过KEY对Data参数进行数据加密，进而就生成了Data密码；而解密数据的还原输出结果正好与之相反。且网络信息通信的两端，实际是的运行过程中，是通过采用相同的KEY参数对该用户的数据核心进行加密处理，进而以保障用户数据的安全。

针对非对称加密技术分析，该项技术的，匿名则是作为当前技术的密钥，并在整体的加密体系中可以将密钥分为公开密钥、私密密钥两种。任意一把密钥均可向他人公开或选择不向他人公开；而私有密钥只有保护用户的权限。常规的非对称加密技术所运用的算法是基于RSA与PKI算法相结合。非对称加密技术支持远程登记，这一点与对称加密技术是具有一定差异性的，同时非对称加密技术还可以并执行对密钥数据的备、恢复机制。这一点上，与对称加密技术同样具有一定的差异性，同时可以提供证书管理功能，保障用户信息安全防护。

2.身份信息安全认证技术

在实际的计算机系统运行的过程中，采用如：身份认证技术、短信密码、动态口令、生物识别技术，全面实现当代用户网络信息安全。

身份认证技术是计算机网络信息安全防护中必须采用的基本防护技术。针对现阶段对身份认证技术通常采用双因素认证的方法进行，我们经常见到的有以下三种双因素认证的身份认证技术如：USB+KEY+静态密码技术；设置二层静态密码；设置动态口令与静态密码相结合的方式，并在一定程度上有效强化用户身份认证系统的安全性、稳定性、实用性[3]。

针对身份认证技术中的静态密码分析，静态密码的界定含义为指当前系统用户自行设置由数字、字母、符号经过不同顺序陈列而形成的具有一定私密性的密码组合数列，这一密码组合具备一定的复杂性，进而逐步的增加了网络黑客破译该用户密码的难度。其次是短信密

码，通过发送信息到用户指定手机中，并要求用户在有限的时间内完成正确的密码输入，此密码仅可以使用一次，同时具有时效性，保证计算机网络安全。第三点是动态口令。通过用户持有动态口令，由动态密码，终端系统可以产生60秒一次的口令，具有时效性的密码口令可以保障用户信息的安全。最后是生物识别；这子那个技术是指通过运用现代化科技信息技术，实际的测量计算机用户生理特征，并对此进行身份验证。在采集的过程中，可以运用人脸采集、人脸识别、虹膜识别、声音识别、指纹识别等科学技术手段相结合。该技术同时还需配合传感器，进而实际的读取该计算机用户的生理信息特征。并在传输的过程中由数据库分析比对，读取用户信息，预留信息的匹配程度，当匹配程度一致或达到一定高50°通过该项认证。

3.防火墙安全系统

大部分的计算机系统中均会拥有并设置防火墙，防火墙。该项技术主要控制内部网络以及外部网络之间的连接安全性，同时可以根据企业设置安全防护策略，对内部局域网进行有效的网络信息保护，进而防止因外部网网络病毒入侵到内部网络中产生安全性问题。同时，防火墙技术其主要包含软件以及硬件两部分，通过两个部分对进出内部网络的数据进行检测，进而防止受到外部网络入侵，恶意代码入侵，从而保护当前内部网络的数据安全性。防火墙技术均具有安全警报部署，转移网络地址的功能。同时，防火墙技术还可以实时的对该网络使用情况进行有效的监控，并对网络安全进行防护，从而在一定程度上强化内部网络安全的性能。

三、总结

切实的提升当前计算机网络安全意识，同时要求用户在实际操作计算机的过程中，通过设置隐私保护程序，前面提升当前系统对用户信息的保护程度。为防止部分用户信息的泄露，同时还应当关闭网络共享信息的设置，有效避免网络黑客利用共享信息，从而盗取用户信息造成的网络信息安全泄露问题的产生。

参考文献：

[1]贺云龙，陆星润.计算机网络安全技术的影响因素与防范措施[J].科技视界，2023（01）：60-64.

[2]姚玉开，赵杰，陈洋.浅析计算机网络安全技术的影响因素与防范措施[J].中国设备工程，2022（01）：235-236.

[3]刘丽娜.计算机网络安全技术的影响因素分析与防范措施[J].电子技术与软件工程，2021（17）：257-258.