关于信息化时代计算机网络安全问题的探讨

李 游
深圳市气象局，广东 深圳 518040

[摘要]在信息技术飞速发展的今天，我们正面临着一个新的时代，在这个新的社会环境中，计算机网络为人类的工作、生活带来了极大的方便，它突破了空间对人们传播信息的束缚，使人们的工作和生活发生了巨大的变化。随着计算机网络的应用领域不断扩大，人们发现它会被某些因素所影响，从而影响到数据的传输安全。因此，必须加大对网络安全技术的使用力度，监控其运行状况，及时发现和排除安全隐患，为广大群众在网络上进行数据传输等工作创造一个安全的环境。
[关键词]信息化；计算机网络；安全问题
DOI：10.33142/sca.v6i8.9832 中图分类号：TP393 文献标识码：A

Discussion on Computer Network Security in the Information Age

LI You
Meteorological Bureau of Shenzhen Municipality, Shenzhen, Guangdong, 518040, China

Abstract: In today's rapidly developing information technology, we are facing a new era. In this new social environment, computer networks have brought great convenience to human work and life. They have broken through the constraints of space on people's dissemination of information, causing tremendous changes in people's work and life. With the continuous expansion of the application field of computer networks, people have found that they can be influenced by certain factors, thereby affecting the security of data transmission. Therefore, it is necessary to increase the use of network security technology, monitor its operation status, timely identify and eliminate security risks, and create a secure environment for the general public to carry out data transmission and other work on the network.
Keywords: informatization; computer network; security problem

1 计算机网络安全维护的重要性

1.1 保护用户信息安全

随着信息技术的快速发展，计算机网络得到了广泛的普及与应用，这为人们的生产生活提供了极大的便利，但是计算机网络还面临着巨大的信息安全威胁，诸如非法访问、黑客攻击、系统漏洞等问题时刻困扰着人们的信息安全，一旦信息遭到泄露、篡改，必将会给人们的生产生活带来极大的不便。如果网络平台无法保证用户的信息安全，必然会造成大量的用户流失，网络数据的流通与共享就无从谈起。因此，互联网企业必须加强网络安全维护工作，确保用户的信息不会出现泄漏、篡改等问题，在提升网络服务质量的同时，为广大用户提供更好的网络使用体验，只有这样，互联网平台才能与用户建立信任，才能推动计算机网络的健康良性发展。

1.2 提升网络数据的准确性

做好网络信息安全维护工作，能够有效提升数据信息的准确性。互联网每时每刻都在传输大量的数据资料，如果数据传输过程中出现安全漏洞，可能导致整个数据系统出现错误，严重者使得整个网络出现瘫痪，给企业、用户造成巨大的损失。因此，网络从业者必须对网络信息安全给予高度重视，采用数据加密、防火墙、杀毒软件等，全面提升计算机网络的安全水平，降低信息被泄露、被盗窃、被篡改的可能，从根本上降低数据安全事故的发生概率。互联网具有较强的开放性特征，每个网络用户都可以在互联网上分享、查阅、下载网络信息，创造信息的数据财富，在此过程中，互联网平台应该建立强大的安全防御系统，来抵御网络病毒、网络黑客的攻击，保证网络数据的精准性、可靠性。

2 大数据背景下计算机网络安全问题

2.1 信息数据泄露

目前来看，信息泄露的途径主要有以下三条：一是平台信息泄露风险。随着互联网的普及和信息技术的发展，网络信息系统所应用的领域和范围不断增加。个人和企业需要在各种平台上进行注册，比如购物、通讯、就医、学习等。在实名制注册条件下，很多平台并没有对用户信息采取有效的保护措施，甚至有些平台在利益诱惑下将用户的个人信息作为数据资源出卖给第三方，造成严重信息泄露事件。二是云数据泄漏风险。目前有很多公司为了吸引用户，利用云技术为用户提供可以储存大量个人信息的云空间，但是云技术目前还很不成熟，容易受到黑客攻击，造成信息泄露。而且，由于对云数据的监管还存在一定的空白，云数据的泄露还存在责任主体不清的问题，这也导致用户信息安全难以得到保障。三是网络钓鱼风险。近些年，一些不法分子运用计算机技术制造虚假社交购物平台

或网站，通过广告、抽奖等形式向用户推送链接。一些用户网络安全意识淡薄或在利益的诱惑下，一旦点击链接，病毒很可能就会侵入计算机系统，盗取用户的个人隐私，获取非法收益。

2.2 病毒黑客入侵

病毒入侵是计算机网络安全面临的最常见的问题。计算机病毒具有隐蔽性，存在于不同的网络载体之中，例如隐藏在下载安装包、邮件、二维码、链接甚至是图片中，让人防不胜防。计算机一旦被病毒感染，首先可能会导致运行速度下降。随着病毒的蔓延和对网络的侵蚀，进而会导致系统故障甚至是瘫痪。在此期间，计算机中一些重要文件很可能被盗取或丢失，甚至还有可能损坏计算机的硬件设备，导致用户经济利益受损的同时面临严重的网络安全威胁。黑客的出现使得计算机网络安全面临更加严峻的挑战。黑客攻击主要借助用户网络漏洞对网络信息进行窃取，主要攻击对象包括政府网站、金融机构、国家重点高校网站等。黑客入侵主要会采取两种方式：一种是直接攻击网络系统，窃取数据信息；另一种是间接攻击，即在不直接影响计算机网络系统正常运转的情况下，通过其他途径获取数据信息。因为黑客的存在，计算机网络信息安全会遭受严重威胁，可能会给国家、企业和个人造成巨大的损失。

2.3 操作系统漏洞

操作系统漏洞主要是由两个方面的原因引起的。一是人为给系统开后门。后门实质上是一种网络病毒，会给用户电脑带来安全隐患。后门往往是系统开发者人为设定的，目的是绕过安全性控制而获取对程序或系统访问权。开后门的最初目的是程序员在软件的开发阶段可以通过后门修改和完善程序设计中的缺陷。但是，如果这些后门在发布软件之前没有删除，很可能被具有一定专业能力的人或黑客识破并当成漏洞进行攻击，带来网络安全风险。二是程序编写过程中出现错误。计算机人员在编写系统程序时，可能会出现程序代码错误而没有及时发现的情况，造成计算机网络系统出现漏洞，给黑客等不法分子以可乘之机。另外，计算机和操作系统之间存在兼容性问题也会造成网络安全问题。通常，计算机操作系统在使用一段时间后会进行自动更新，当更新完成后可能会导致操作系统和硬件设备不兼容的情况，使计算机操作系统无法正常运行，系统里所存储的信息和数据面临丢失或者损坏的风险。

3 计算机网络安全问题的防范策略

3.1 充分利用防火墙技术

防火墙能够有效阻止网络黑客的攻击以及电脑病毒的传播，在维护计算机网络安全方面发挥着不可忽视的职能作用。防火墙主要是利用拓扑结构来保障计算机安全的一项技术，在企业网络、个人电脑中得到了广泛的普及与应用。从技术层次分析，防火墙是通过设置访问权限，来维护计算机网络安全，在连接网络的时候，防火墙发现不正常的数据请求，及时阻止数据访问行为，从而避免计算机网络遭到非法入侵，防止数据信息遭到盗窃、篡改。防火墙通常将信息分为内外两个部分，将内部网络和外部网络有效隔离开来，通常来说内部管理安全程度比较高，能够达到更好的安全防护效果。防火墙技术能够定期对计算机内部存储进行筛选审查，从而找出藏匿在文件中的网络病毒，并将其隔离开来，避免网络病毒破坏计算机系统、非法窃取网络数据。因此在以后的计算机网络使用过程中，网络用户应该充分意识到防火墙技术的重要性，及时安装防火墙，并使用防火墙对计算机设备进行病毒查杀，充分保证计算机网络的安全性。

3.2 通过加密技术抵御黑客入侵

3.2.1 对称加密技术

对称加密技术种类较多。其中，3DES 技术就是一种常见的类型。3DES 技术在对网络信息进行加密的过程中需要使用 3 个密钥，能进一步提升加密的效果，使加密的步骤更加复杂，保障信息的安全性。这种加密技术如果用现在的计算机破解技术破解，大概需要百年时间，为计算机网络中的信息安全提供了强有力的保障。然而，由于这种加密技术相对比较复杂，用户在破解的过程中也需要花费较多的精力。例如：用户在获取相应的信息后，需要拥有 3 把钥匙才能完成解密工作，如果用户在解密时不小心丢失了一把钥匙，出于安全防护的设置，其他两把钥匙也会自动关闭，这在一定程度上给用户的解密带来了难度。为了解决这一问题，人们正在积极研发一种名为 AES 的加密技术，这种加密技术所用的加密运算方式更简单，其安全性和 3DES 加密技术不相上下，能进一步简化用户的解密流程，从而提高信息的传输质量和传输效率。

3.2.2 非对称加密技术

非对称加密技术中最常见的是 RSA 公开密钥加密技术。目前，RSA 加密技术在签署公开密钥密码的产品中得到了十分广泛的应用，能进一步保证信息数据的安全性。此外，非对称加密技术中还有 ECC 技术，人们称之为椭圆曲线密码，它比 RSA 技术拥有更大的优势：(1)ECC 技术能更好地帮助计算机网络抵御外界入侵；(2)ECC 技术的计算量更少，公钥处理的效率也更高；(3)ECC 技术在运行的过程中不需要使用过多的内存，能在各类微型计算机和联网装置中发挥更大的作用，能凭借小带宽的优势在无线通信中发挥更有效的作用。

3.3 身份认证技术

在计算机网络不断发展的背景下，人们进行身份信息的认证时主要是通过特征数据来实现的，因此通过有效的认证技术能够进一步强化计算机网络中的安全保护能力，避免黑客对个人信息进行窃取或篡改。目前，计算机网络中最常见的认证技术主要包括 3 种，分别是动态密码、静

态密码和短信密码。例如：用户根据需求自行设置了独立的静态密码，在登录相应的操作系统时需要输入正确的静态密码。静态密码长期处于不变动的状态，加上部分用户会在自己的系统中记录静态密码以防忘记，一旦黑客入侵就容易导致静态密码泄露，在一定程度上增加了身份认证的风险。在此基础上，人们开发出了动态密码和短信密码，能配合静态密码实现更加高效的身份认证，使未被授权的用户不能登入相应的操作系统，进一步增强了计算机网络的安全性。

3.4 完善的网络安全管理系统

企业需要制订详细的应急计划，以用来迅速应对用户网络、系统和应用可能受到的破坏。当某个系统或设备发生故障时，企业应优先对其运行环境进行检查，以确定具体的影响，并在规定的时间内对故障进行维修和恢复。

网络系统的安全离不开制度的约束，只有健全的安全管理制度，才能确保其运行状况的正常。企业必须根据国家安全管理制度来处理和维护网络系统、系统监视、设备维护和故障排除。

3.5 控制用户和权限，防范黑客攻击

从系统用户的特性出发，系统也可以通过设置相应的访问权限来控制用户对某些数据的访问，以提高数据的安全性。网络系统也拥有以用户身份为前提的控制权限，在具有正确的系统配置和合理的访问许可权配置条件下，文件有权利拒绝超出权限访问的合法用户。

同时，为了加强信息的有效利用，企业可以引用身份认证产品和技术。身份认证技术是指能够识别信息发送者和接收者真实身份的技术，是保障网络信息安全的第一道门。身份认证技术主要识别和验证用户身份的可靠性，授权访问以确保安全，并拒绝非法访客。在网络中，为了防止信息的丢失和泄露，网络可操作性和可管理性的重要性日益凸显，访问控制也是必然趋势。

专业的操作人员能把优质软件系统和硬件设备的作用发挥到极致，因此，专业人才培养是网络信息安全建设的首要措施。企业应尽可能地为网络管理人员安排定期专业培训或者举办技能大赛等，还可以为技能优秀者提供进入网络信息建设较为优秀的企业的学习、进修机会，增强其网络安全意识的同时提升专业能力。除此之外，企业也有必要建立和完善相应的制度，并成立一支处理网络信息安全问题的专业团队。同时，企业必须根据不同用户的需求设计个性化权限，尤其是信息系统的管理员和密码的设置，都需要特殊的设置和定期更改，以创建安全的企业网络信息。

3.6 提高平台的安全管理性能

为了保证数据的安全，本文提出了一种基于入侵检测技术的方法。该技术可以有效地解决网络安全问题，并将数据监测情形有效地结合起来。入侵检测技术是利用网络通信技术、人工智能技术以及其他监测手段进行网络防范的一种新技术。统计分析法是利用统计学的基本原理，对一般工况下的运动模式进行全面的分析，从而判断系统的运行状态有无异常；签名分析技术主要是利用已知的安全漏洞，利用模板匹配技术，找出签名中存在的攻击模式问题。此外，它还可以和其他的网络安全软件相结合，增强系统的防御能力，使系统的内部信息更加完善。

4 结论

影响网络安全问题的因素很多，要彻底消除这些因素几乎是不可能的，所以企业必须提前做好预防工作。为了构建一个安全可靠的网络系统，管理措施应最大限度地与安全技术相结合。首先，杀毒软件和防火墙技术可以结合起来；其次，及时备份和恢复数据；最后，加强对管理人员的专业能力培训，让他们继续学习和研究最新的网络安全技术，使他们有能力通过观察网络的运行状态发现潜在问题，并及时消除风险，调整网络安全防范策略。同时，开发一个合理有效的网络安全风险管理系统对于网络安全系统的持续更新和完善也非常重要，企业应该从可能造成网络安全威胁的软件和硬件方面，以最大限度地减少损失，实现网络信息系统安全稳定发展的目标。

[参考文献]

[1]张晓磊.信息化时代下计算机网络安全问题及建议[J].信息记录材料,2022,23(8):32-34.
[2]庞凯中.信息化时代下计算机网络安全问题的探讨[J].网络安全技术与应用,2022(6):155-157.
[3]赵铁牛.企业信息化与计算机网络安全问题研究[J].大众标准化,2021(18):61-63.
[4]赵玉萍.信息化时代下计算机网络安全问题的探讨[J].数字技术与应用,2019,37(10):194-195.
[5]翟丽.信息化时代计算机网络安全防护技术探索[J].产业与科技论坛,2018,17(12):85-86.

作者简介：李游（1983.7—），毕业院校：深圳大学，所学专业：电子与通信工程，当前就职单位：深圳市气象局，职务：负责网络安全业务管理，职称级别：高级工程师。