大数据时代计算机网络信息安全及防护策略

栾晓朋

（赛西认证有限责任公司）

摘要：计算机网络领域的迅速发展，为各行业均带来了新的经济增长点，成为社会进步与发展的重要领域。在技术支持与创新的背景下，计算机网络技术与大数据分析技术广泛应用于各行业，且实时产生大规模数据，在支持决策、助力企业可持续发展方面发挥着重要的作用；但是，计算机网络的应用也存在信息泄露、非法篡改等安全隐患。在大数据时代加强计算机网络信息安全隐患排查，保证计算机网络运行安全性、稳定性，深受企业关注。鉴于此，本文从数据加密、防火墙搭建、健全管理体系、用户权限管理四个方面，以大数据时代为背景，重点探究计算机网络信息安全防护的策略，希望能为行业从业者提供参考。

关键词：大数据时代；计算机网络；信息安全；防护策略

互联网平台的搭建与正常运行，在社会生产、生活中均发挥着重要的作用，便捷信息传递、数据存储与分析等，深受社会关注。互联网运行过程中产生的大量数据、信息，成为人们获取、判断的重要内容。对大体积数据的分析、处理与应用直接影响决策效率、工作水平等。在大数据时代背景下，加强对数据分析、处理与应用的重视度，积极应用大数据分析技术于各行各业势在必行。保证信息完整、真实、安全，是大数据时代计算机网络运行与发展至关重要的问题。本文则对此进行重点分析，研究在大数据支持下，计算机网络信息安全防护策略，希望能为企事业单位、个人用户安全用网、发挥数据支持作用提供经验支持。

一、运用运算法则，网络数据加密

大数据时代，各行业在内部治理、经济发展的过程中，实时产生大量数据、信息，虽然企业开展决策、管理等各项工作开展，能以大规模的数据为依据，从众多数据中抓取可支持企业经营、治理的关键信息，但也面临着信息泄露以及由此引起的安全风险。因此，加强数据管理、安全保护尤其重要。积极运用运算法则，将产生的数据、信息等进行加密，并将其转化为一种加密符号，只有掌握密钥的人才能通过解密，将加密符号转化为原来的资料，取用资料[1]。

无论是信息传递，还是信息产生、存储与管理，对数据进行加密处理都尤其重要。技术人员需要根据数据产生的方式、重要程度，设置相应的加密等级，利用相同密钥对数据信息进行加密、解密算法，依据相应的加密标准，进行全面的网络数据加密，如，数据加密标准、高级加密标准等，尽可能在最大程度上保证计算机网络数据安全。例如，在网络信息传递时，双方需要采取相同的密钥，保证双方能依托计算机网络，信息发送者将原来的信息转化为加密符号，接收信息方则使用密钥，将加密符号转换为原来的信息、文件等，避免在信息传递过程中发生信息泄露等问题，提升信息传递的安全性。在数据产生、存储、管理以及使用的全过程，网络数据加密能保证计算机运行过程所有数据的安全性，避免信息泄露给用户带来危害[2]。除此之外，哈希算法、数字签名等也是常见的加密方法，前者能将文件、资料转化为固定长度的哈希值，从而验证资料的正确性；后者则能加密资料、文件，并在此基础上，加上数位签章，保证资料的真实性，避免信息泄露。

计算机网络数据加密是大数据时代保证信息安全性、完整性、准确性的重要举措，充分发挥各种运算法则在计算机网络数据安全保护中的作用，避免数据泄露给用户带来较大危害、安全隐患。

二、搭建防火墙，避免恶意入侵

大数据时代，数据收集、分析、处理与应用尤其重要。数据存储、传递各环节，都要在最大程度上避免外部恶意入侵与内部恶意泄露，保护计算机网络运行稳定、数据安全，充分发挥计算机网络在各行业的作用。网络攻击、人员的不合规操作都是引起计算机网络安全风险的主要原因。在大数据时代，保护数据安全对计算机网络的稳定运行尤其关键。防火墙能对内、对外保护数据安全，约束人员的操作行为，规避外部恶意入侵引发的网络、信息安全风险。防火墙作为一种新型的计算机网络防护系统，不仅能动态监测、控制互联网数据，还能精准识别存在安全隐患的数据，并对其进行拦截，避免内部信息泄露、外部不良数据入侵[3]。要搭建有效的防火墙，并充分发挥防火墙在数据、网络安全保护方面的作用。

企业在搭建防火墙时，应对计算机网络运行特点、防火墙运行状态等进行深度分析与动态监测，及时发现、分析防火墙的安全隐患、不良因素，如，防火墙故障等，并针对存在的不良因素进行处理、控制，设计相应的安全防护系统，精准排除计算机网络故障。大数据、云计算、人工智能等现代技术在防火墙搭建中的应用，还能辅助技术人员根据网络运行参数，从众多数据中抓取异常参数，并以此为依据，预测网络运行问题，采取相应的安全防护措施，避免病毒、恶意软件、非法入侵等网

络攻击。尤其是随着信息技术的不断进步，计算机网络防火墙也应不断更新，动态改进、升级网络防火墙，提高防火墙安全防护功能，适应新的网络环境，提升计算机网络运行的安全性、稳定性。以隐藏 IP 防火墙为例，该防火墙能将正确的网络 IP 地址隐藏起来，转移为集中网络服务器。若外部恶意入侵，能直接转移、隐藏正确的服务器地址。

为了在最大程度上提升计算机网络与数据的安全性，防火墙的的搭建应以多层级化为方向，构建多层次防火墙系统，保护网络稳定运行，更好地增强计算机网络的安全性能。多层次防火墙、反向代理防火墙等构成的深层次防御体系，避免计算机网络被恶意入侵。

三、健全管理体系，组建安全队伍

适应大数据时代背景下的网络环境，保证计算机网络安全、稳定、高效运行，建立健全以安全运行为中心的计算机网络安全管理体系尤其重要，并招聘、培养专业的计算机网络人才，建设专业化技术人员队伍。

一方面，根据计算机网络运行的实际情况，制定科学、合理的网络安全管理制度，并推进管理制度全面落实到网络运行全过程。同时，制定安全防护管理制度，根据计算机网络运行的常见问题，制定应急处理方案，确保能在发生网络安全问题的第一时间，采取相应措施，有效分析、解决问题，避免各种故障引发的网络安全隐患与问题[4]。在制定管理制度之时，还应配合落实权责分配制度，将计算机网络安全防护管理职责细化到具体的员工个人，保证每一位员工明确自身在计算机网络运行过程中扮演的角色、承担的责任，不仅便于后期追责，还能约束、规范员工的不良网络操作行为，尽可能在最大程度上降低主观因素对计算机网络安全、稳定运行的不良影响。例如，将安全防御管理纳入计算机网络安全管理体系，完善相关管理制度，针对计算机网络运行常见的外部恶意入侵、内部数据泄露等安全问题以及已经采取的安全防护措施——搭建防火墙、安装杀毒软件等，不断完善管理制度，将主客观等各种可能引起计算机网络安全风险的因素进行严格控制，以完善的管理制度与管理体系，推进计算机网络安全管理工作有序开展，保证网络安全、稳定运行。

另一方面，人力资源在各领域都扮演着重要的角色，在计算机网络运行过程中，操作人员、技术人员的工作态度、认知、行为等都将直接反映在计算机网络运行全过程，负责各项工作员工的行为是引发网络安全问题的主观因素。因此，随着管理制度、体系的日益完善，负责计算机网络运行安全防护的专业化技术人才的引进与培养至关重要。为了保障用户的信息安全、网络安全，技术人员要以用户的用网需求和特点，优化计算机网络设计。相关单位则要加强员工网络安全意识培养，加大网络安全教育力度，逐步增强员工的网络安全意识，促使其自觉约束、规范个人用网行为，尽可能避免因个人因素引起的网络安全隐患与风险。随着信息技术在各行业的广泛应用，计算机网络用户的体积日益庞大，用户的用网行为直接影响网络运行状态。若用户在具备网络安全意识的同时，还能掌握专业的计算机操作知识与技能，则能有意识且专业化地避免网络安全问题，降低个人因素对计算机网络操作、互联网运行的不良影响[5]。国家、政府、社会以及企事业单位都要加大网络安全宣传、教育工作，采取多种多样的方式，培养具备网络安全意识、安全用网行为、计算机专业知识与技能的复合型人才，为大数据时代培养、储备专业化人力资源，推进大数据时代走进企业生产、社会建设、民众生活。

四、加强网络监控，管理用户权限

从用户的角度而言，用户使用计算机，在互联网平台上搜索资料、发送信息等行为都存在一定的信息泄露风险，进而引发各种数据、网络安全问题。虽然国家以多种方式加强网络安全教育，面向多个群体，采取不同方式，向网络用户输入网络安全、数据安全知识与自我防护技能，但是由于用户的主观性较强，用户的个人用网行为很有可能导致个人信息泄露、单位资料被入侵或窃取。针对上述情况，采取专业手段，加强网络监控，设置用户用网权限，能在一定程度上降低用户个人行为对计算机网络安全运行的不良影响。

将监控网络入侵作为重要内容，在计算机网络运行全过程，运用监控技术，监控计算机网络，识别隐患，排除风险，避免计算机网络受到不法分子、病毒软件入侵。监控技术的运用能全过程监控用户数据、信息，保证计算机运行全过程都能接受监督与控制。当计算机运行出现安全漏洞等问题时，技术人员可以采取监控技术对此进行及时处理，保证计算机运行状态平稳。网络安全审计是一种常用的网络监控技术，能自动上传、实时记录计算机运行过程中的各种操作、产生的参数等，将其存储至电子数据库，确保后续能作为不良事件追溯的主要依据[6]。具体而言，在计算机系统内安装安全审计系统，确保与计算机连接的各个设备都具有网络安全审计、数据安全审计的功能，计算机网络后台系统能自动获取各设备运行状态、参数，操作及其负责人等信息，后续可以此为依据判断负责人是否存在违规行为或计算机网络运行是否存在安全隐患等。

例如，在对会议记录数据库采取监控技术时，审计系统能自动、全面获取会话日志、访问日志、操作日志、会议日志等电子信息，全面整合各种信息，从中提取关键信息，审核、判断负责人以及参与人员的工作人员是否违规。在网络安全事件发生之时，审计系统能帮助纠察人员以最快的速度定位引发问题的个人、行为等，并在分析、明确问题原因的基础上，采取相应措施，对计

（下转第 22 页）

（上接第 7 页）
算机网络运行各环节存在的问题进行及时处理、解决。以审计系统为例的监控技术能动态监测、全面管控计算机网络运行状态以及各种电子数据，在第一时间发现、分析、解决问题，从而有效避免网络运行安全、数据安全问题的出现，降低主观因素对计算机网络运行的不良影响。

在大数据时代背景下，监控技术的大力运用以及用户权限监督与管理，能有效约束人员用网行为，尤其以权限方式，避免计算机网络知识与技能水平较低人员在实际操作中出现的不良行为，有效规避计算机网络安全风险。在计算机以及相关设备中安装审计系统，实现对网络运行过程中实时产生数据的自动化、动态化监督与控制，收集、分析、处理与应用数据，从大数据中抓取关键信息，在助力计算机网络安全运行方面发挥着重要的作用。对运用计算机网络各行业的发展都发挥着关键作用。加强网络监控、用户权限管理，对计算机网络适应大数据环境、数据安全防护至关重要。

五、结语：

精准识别引发计算机网络安全问题的主客观因素，进行数据加密、搭建防火墙、健全管理体系、加强网络监控是保证计算机网络信息安全、运行稳定的重要举措。在大数据时代背景下，推进计算机网络安全、高效运行以及持续发展，深受各行业重点关注。尤其随着互联网技术的不断发展，社会生产生活对计算机网络技术的依赖性提升，网络信息安全的防护与保证对用户、行业发展都至关重要。大数据分析技术的广泛应用，从数据收集、分析、处理、应用的角度入手，辅助技术人员及时发现网络运行风险，并对其加以控制，推进信息技术全行业以及相关领域整体、健康发展。因此，各行业要在大数据时代背景下，抓住机遇，迎接挑战，加强计算机网络数据监测、分析以及信息安全防护，提升计算机网络运行的安全性、稳定性与高效性。

参考文献：

[1]安玲.大数据时代计算机网络信息安全及防护策略分析[J].产业创新研究,2024,(10):61-63.

[2]姜辉.大数据时代计算机网络信息安全问题分析[J].居业,2024,(05):201-203.

[3]韩伟.大数据时代医院计算机网络信息安全应用研究[J].网络安全和信息化,2024,(03):156-158.

[4]张晶.大数据时代网络信息安全控制探究[J].山西电子技术,2024,(01):119-122.

[5]陆叶.大数据时代计算机网络信息安全问题的解决路径[J].百科知识,2023,(33):42-43.

[6]刘占凤.大数据时代如何加强计算机网络信息安全管理[J].网络安全技术与应用,2023,(07):162-164.