大数据视域的计算机网络信息安全防护研究

姜荣正
（广东科技学院，广东 东莞 523083）

摘要：随着时代发展，我们进入到网络时代，网络在给人们的生活带来诸多便利的同时，也存在一些安全方面的隐患，这就需要我们对网络安全防御提起充分重视。如何实现更好地维护网络环境的稳定、安全、有序，需要人们将更多方式、理念投入到网络安全防御工作中。大数据技术作为当前最高端科技的代表之一，在诸多领域都显露出了其优越性和有效性，将大数据应用到网络安全防御中逐渐成为我国创建网络安全环境的重要内容。本文将针对大数据技术应用到计算机网络安全防御中的应用进行分析，并提出一些策略，仅供参考。

关键词：大数据；计算机；网络安全；防护研究

大数据时代背景下，人们的生活模式发生了根本性变化，可以说，网络已成为人们日常生活中的一部分。近年来，影响网络安全的案例时有发生，造成了难以计数的经济损失。对此，如何提升网络系统的安全性成为每个人应该重点考虑的问题。本文就大数据背景下计算机网络安全问题进行分析，编制网络安全防护网。

一、大数据背景下进行计算机网络信息安全防护研究的意义

网络安全风险评估关键技术其实可以理解为一种预测技术，由于网络环境处在不断变化的过程中，防御系统只能对已经入侵和潜在的危险因素进行处理，难以确保网络环境的安全性。风险评估关键技术能够在一定程度上预测未来可能发生的网络安全问题，这样可以对其进行提前防御，所以，减少安全隐患相比于被动防御、查杀网络病毒更具现实意义。

在网络安全风险评估中，历史数据可以作为网络安全风险评估关键技术数据库的基础，通过优化风险评估关键技术，能够更加准确地检测出特殊情况下的木马类型、攻击次数等风险内容。在大数据时代来临之前，这些数据只能依靠研究员进行评估、整理，效率非常低下，通过将大数据应用到网络安全风险评估关键技术中，能对网络风险信息进行更加科学的判断和分析。简单来说，网络风险评估关键技术与大数据相结合，能够有效地帮助人们分析风险数据的走向和规律，这对维护网络安全有非常重要的现实意义。

二、大数据背景下计算机网络安全问题

（一）网络安全立法不严

目前来看，我国在网络安全管理方面的法律还不完善，从一定程度上影响了网络安全系统的建设，这种情况下也不利于安全的网络环境的营造。近年来，随着信息技术的不断发展，一些大型网络平台相继出现，给用户提供了便捷的沟通与工作渠道，在此过程中也极大地改善了网络用户之间的关系，为行业信息化发展奠定了基础。但从管理这一层面来看，一些危害用户隐私的案件时有发生，从一定程度来看，这一现象的出现与网络安全立法不严有一定关系，这种情况下也能使一些不法分子逍遥法外，不利于维护网络安全。

（二）病毒及黑客攻击

病毒及黑客攻击是影响计算机网络安全的核心要素，这两者的攻击性极强，且具有一定感染性，如不及时处理容易造成网络瘫痪，同时也会导致信息丢失，从一定程度上增大了信息感染风险。从运行机制来看，如病毒侵入计算机能够破坏程序中的代码，这种情况下也容易使某个程序乱码，不能继续工作。当然，计算机病毒也有良性与恶性之分，前者对计算机造成的危害比较小，可通过软件修复使计算机正常运行。而后者对计算机伤害比较大，且病毒自我复制速度比较快，在短时间内就能使整个计算机系统瘫痪。黑客攻击指的是未经过访问许可利用非法渠道进行访问，且在计算机内植入木马程序、病毒等，以此导入网络信息，对整个行业发展也有很大影响。

（三）网络风险监管不力

目前来看，计算机网络在发展过程中还存在很多问题，特别是网络的虚拟化特征，这种情况下如不注重网络安全管理则会导致关键数据丢失，于企业发展有不利影响。此外，还有一部分用户在浏览网页过程中没有将浏览记录清除干净，这种情况下黑客趁虚而入，跟随用户的访问记录寻找有效信息，导致信息泄露。如相关人员不注重网络风险管理，会造成难以预计的损失。

三、大数据背景下计算机网络安全问题解决对策

（一）健全法律法规，撑起网络安全防护伞

大数据背景下，相关部门要将计算机安全管理列为重点工作，完善相关法律法规，撑起网络安全防护伞，以此保障用户的上网安全。调查数据显示，计算机信息盗取案件时有发生，且年增长率为 1.22%，需引起相关部门的重视。对此，执法部门要做好立法工作，完善计算机网络安全管理的相关法律法规，严厉打击黑客攻击问题，避免用户关键信息丢失。此外，相关部门也要宣传计算机网络安全管理的重要性，向用户普及安全上网的常识，做到正确上网，降低安全风险。

（二）优化网络安全风险数据库

若想让网络安全风险评估关键技术有所发展，需要建立更加科学、有效的网络风险数据库。一般来说，网络风险数据库中存储的信息能够为网络风险评估提供重要的评测基础，若是未能建

立完善的网络安全风险数据库，评测结果将在很大程度上丧失实际意义。在进行网络安全风险评估时，以往的评估数据也会产生一定作用。但是，很少有人会对这部分数据提起重视，未能建立一个正规的数据库来存储、分析和整理相应的数据内容，这样进行的网络风险评估将存在较大的失真性。因此，风险评测人员要进行数据库优化时，可以采用 B/S 三层模式建立。这个数据库可以从浏览器、应用服务器、网页服务器以及数据服务器四个方面进行数据收集，这样可在最大程度上实现数据共享，确保网络安全风险评估数据库具有较强的可拓展性，也能在很大程度上增加数据库内容的灵活性。

当网络安全风险评估数据库中的其中一个服务器出现问题时，另外的数据库可以暂时接管相应数据，确保整个风险评估系统运行。比如，当客户端的服务器出现问题时，风险安全评估数据可暂时由应用数据库接管，确保其能正常处理和统计数据。此外，为增强网络风险安全评估数据的稳定性，可为其设置专门的防火墙，对一些机密数据进行适当加密，从而全面增强网络风险安全数据库的安全性。进行网络安全风险评估数据库优化时，可选择 MySQL，它在使用时更具简便性，管理起来也较为方面，可靠性和安全性可在很大程度上得到保证。

网络安全风险评估关键技术研究的第一步便是优化其数据库，这是之后工作开展的基础。结合数据对网络安全未来的发展状况进行分析时大数据时代的重要方向。通过对各类数据进行整理、统计和研究，并对这些历史数据进行较为合理的分析，能够更好地提升网络安全风险评估关键技术的发展速度。

（三）强化技术保障，为网络系统搭建安全防护网

1. 升级防火墙技术

防火墙具有一定的防御功能，其在数据库外层，且具有一定的信息识别功能，能够比较准确地判断信息来源，在此基础上为信息库套上安全防护网。可以说，防火墙能够为网络安全工作提供屏障。从本质来看，计算机网络安全的防护要从根源入手，抵御木马及病毒攻击，在此基础上提升网络系统的安全性。在此过程，防火墙技术为关键技术，其能准确判断信息来源，秉持“及时发现及时处理”的方针，将病毒隔离出去，同时也能避免非法访问。与此同时，相关部门还要定期升级防火墙技术，为网络系统搭建安全防护网。

2. 完善认证技术

大数据背景下，加强网络安全认证也为重点工作，其根据用户 IP 地址将用户分类，在此基础上进行访问权限的划分，能够保障网络系统的安全性。信息化背景下，相关部门要进一步要求认证技术。例如，该部门可以引入数字认证技术，在企业内部搭建 KPI 体系，用户根据相应的指令完成身份认证，同时用户还可设置自定义密码，系统根据用户密码设置情况准确评定密码的等级，进一步提升系统的安全性。此外，相关部门也可引入新型的认证技术，如设置动态电子口令，也可引入指纹和虹膜认证方式，丰富认证渠道，从根本上降低数据丢失风险，有效保障用户登录安全。

3. 优化代理服务技术

代理服务器对于有效避免不法黑客的攻击、网站浏览的加速缓冲等起了很大的作用。大数据背景下，相关部门要进一步优化代理服务技术，通过这种方式抵御黑客入侵，有效避免其他干扰因素的影响。在此过程中，还可引入防毒程序，准确识别病毒来源并自动查杀病毒，提高整个系统的安全性。

4. 强化加密技术

大数据背景下，相关部门要对重要数据库进行加密。客观来看，对数据库进行加密是提高其安全性最为有效的一种方法。目前来看，多个企业对数据库各个分系统进行加密处理，特别是对数据的访问，通过加密限制部分用户入内，提升整个系统的安全性。通过这种方式也能隔离部分用户，保障整个网络系统的安全性。为了进一步提升网络安全，相关部门还可以对数据库设置灵活的密码，实时更新密码，保证整个系统的安全。在数据密码设置过程中，相关人员可以设置两种类型的密码，这种密码能够有效防护数据库内容。

（四）加大监管力度，从根源降低安全风险

网络安全管理是一项重点工作，在新的时代背景下，相关部门可依托大数据技术之力进行网络安全管理。在此过程中，大数据供应商可结合用户的实际需求为其推送个性化的服务，在此基础上还要进一步优化安全管理标准，提升服务质量。客观来讲，用户端的安全管理也是网络安全管理的重要内容，在管理过程中，大数据供应商可及时更新各个应用程序，并对其进行安全升级，必要时请求用户安装对应的安全防护系统，以此来应对可能出现的网络安全入侵问题，保障用户数据信息操作安全性，提高用户数据安全管理质量。此外，相关部门还要加强内部网络管理，减少公网地址领域的消耗。在此过程中，也可对不同模块的用户进行安全检查，实时监控用户的各项操作，避免用户进行非法操作对大数据整体安全造成影响。

四、结语

网络安全是大数据背景下各个行业均面临的重要课题。在新的时代背景下，各个行业均要将网络安全管理放到核心位置，分析当前影响网络安全的因素，通过健全法律法规，撑起网络安全防护伞；强化技术保障（升级防火墙技术、完善认证技术、优化代理服务技术、强化加密技术），为网络系统搭建安全防护网；加大监管力度，从根源降低安全风险，全面提升网络系统的安全性，为用户创造更加安全的上网环境。

参考文献：

[1] 李新新 . 大数据技术在网络入侵检测的应用 [J]. 信息技术与信息化，2021，4（05）：235-237.

[2] 李鹏举 . 简析大数据背景下信息通信网络安全管理策略 [J]. 数字技术与应用，2021，39（05）：184-186.

[3] 陈君芳 . 计算机网络安全技术在网络安全维护中的应用 [J]. 电脑编程技巧与维护，2021，4（05）：165-166.