文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

网络安全分析中的大数据技术应用研究

林大龙
广东石油化工学院
DOI:10.12238/acair.v3i1.11910

[摘　要] 本文旨在讨论如何利用大数据分析技术来提升网络安全的防御能力和效益。采取了诸如数据融合、技术融合及跨平台融合的策略,以综合各种源自于不同的安全数据,并与其他的网络安全工具相结合,以此消除信息的隔阂,从而增强安全分析的精确度和广度。在数据分析技术被运用到网络安全中时,它能有效地增加其保护效力和成效,同时也能加强协作战斗力,进而提升整个网络安全系统的防卫等级。数据分析技术对于网络安全有着巨大的潜力,建立基于此种技术的大型网络安全平台能够更大幅度的提升网络安全防范的力量和级别,这无疑是对确保网络安全的重要贡献。
[关键词] 大数据分析技术；网络安全；数据融合；技术融合；跨平台融合
中图分类号：C35　**文献标识码**：A

Research on big data technology in network security analysis

Dalong Lin
East Institute of Petrochemical Engineering

[Abstract] This paper aims to discuss how to use big data analysis technology to improve the defense capability and benefits of network security. Strategies such as data fusion, technology fusion and cross-platform fusion are adopted to integrate various security data, and combine with other network security tools, so as to eliminate the information gap, so as to enhance the accuracy and breadth of security analysis. When data analysis technology is applied to network security, it can effectively increase its protection effectiveness and effectiveness, and at the same time can strengthen the collaboration combat effectiveness, and thus improve the defense level of the entire network security system. Data analysis technology has great potential for network security. The establishment of a large network security platform based on this technology can significantly improve the strength and level of network security prevention, which is undoubtedly an important contribution to ensuring network security.
[Key words] big data analysis technology; network security; data fusion; technology fusion; cross-platform fusion

引言

伴随着互联网技术飞速进步,网络安全挑战愈发明显。对于网络侵害与风险,现有的防御策略已不再适用。然而,大数据分析方法的发展为我们提供了一个全新的视角来处理这个问题。借助大量安全的数据融合、研究及探索,可以更精确地识别出可能存在的危险和攻击模式,并迅速实施预防和反应行动。

1 大数据背景下网络安全的现状

尽管我国大数据及互联网发展已经取得了进步,但仍有许多挑战需要克服。例如,基础设施相对脆弱,科技水平较低,缺乏足够的人才储备,以及创新力有限等问题。这些都表明在网络防护和管理的领域还有待提升。在大数据时代,虽然网络安全形势仍然非常严重,仅依靠单一手段来预防是无法完全消除所有潜在风险的。因此,要始终保持警觉,利用大数据技术,以确保个人的权益不受侵害,降低网络安全隐患的发生率。

1.1多样化的安全隐患

现今互联网上有丰富的多元化服务和用途。当我们在工作中使用它的时候,能够更有效地管理数据并提高效率。当需要休闲娱乐时,各种类型的游戏和数字图书能让我们安心下来,并在其中寻找一份宁静。然而,这个工具也是一把双刃剑。虽然它为我们带来了舒适和快乐,但也伴随着许多网络风险进入我们的生活。例如,在浏览网页时,常常会遇到一些负面内容、违法资料或色情影片等等,这些低劣的站点一直在损害着我们的身体和心理健康。另外,由于其复杂的病毒传播方式,即使是电子设备也不能幸免于难,个人信息被暴露,财务状况面临危险。例如,

常见的恶意软件如木马、脚本文件、捆绑式攻击、破坏型程序等等。

1.2社会网络安全意识淡薄

近些年里,我国持续关注到网络信息的保密性和公众对其认识度的提升问题上,并在整个社区中大力推广关于安全的理念教育工作。然而仅仅停留在理解层面上的知识并没有实际意义所在,因为普通大众对于计算机技术的掌握程度有限且缺乏足够的警惕心,以至于当面临着复杂的安全挑战的时候仍然束手无策。众所周知大部分的企业都会开发出属于自己的软件或应用程序来满足其需求,但是很多组织和个人却没有意识到他们可能存在的风险漏洞而未采取任何防范措施,这其中因管理的失误导致的麻烦更是屡见不鲜。另外一方面而言,绝大多数人普遍低估了自己在网上活动中的风险暴露度及潜在影响力,总觉得这些事情离他们的生活很远而不加注意。实际上并非如想象的那样简单：每个人都有他独特的个人信息记录,并且正是这个原因使得某些犯罪者能够利用它们的价值去出售给其他人获取利益,从最基本的数据外流至严重的财务受损等各种情况均有可能发生。所以增强网上安全感知能力,并对更多有关网站安危的相关信息有所认知是非常必要的自我防护手段之一[1]。

2 大数据分析技术应用研究

2.1数据采集

对于网络安全的评估,需要全面掌握网络状况并辨识潜在的风险。为此,需从多渠道收集数据,例如通过防火墙来跟踪网络流向的具体细节,以帮助侦测可疑的行为,利用入侵检测系统发出关于潜在攻击活动的即时警示。此外,可以透过观察网络流量的数据来理解整个系统的运作模式,同时也可以参考系统日志来洞察软件及硬件的使用情况。这种多元化的方式为我们提供丰富且精确的信息,从而提升分析效果。然而,因为原始资料有可能来自于各种装置或系统,其形式和品质可能会有所出入。所以,在开始研究前,有必要先把这些资料整理好,例如修正掉那些遗漏或者异于寻常的数据,并且要把各式各样的资料都转成适合作分析的形式。这项工作可以通过使用数据清理工具和算法自动执行,这样不仅能减轻人力负担而且还能提高工作的效率。

2.2数据检索

对于网络安全的评估而言,需要应对大量的资料,而这些资料有可能来自各种设备和体系,因此它们具备了多样的特性且十分复杂。为此,研究人员需能迅速地从海量数据中找到那些涉及网络安全问题或者存在异常的行为的数据,从而进一步展开深度的研究。这种搜索过程可通过基本的关键词查找、复合查找或是高阶的查询语言来完成。此外,也有一些大数据分析平台引入了利用机器学习技术进行智能化的搜索方式,它能够依据数据的特点和分析的需求,主动挑选出重要的内容。为提升搜寻速度及精确度,有必要对搜寻方法加以优化。此包含改善查询语法、调整索引结构、降低数据重复率等等。与此同时,还应考虑到数据的时间敏感性和扩充能力,以此适应于各类环境中的分析要求。

2.3数据处理

在互联网安全的研究与评估过程中,常常面临着海量信息的挑战。为了有效地应对这一情况,需要运用大数据技术的优势来从中筛选并提炼关键的信息,以用于威胁发现、异样行为辨识等工作。所以,数据处理成为了网络安全分析过程中的核心步骤之一。在这其中,常见的工具如数据挖掘、机器学习及深度学习等等都能够通过它们强大的功能从庞大的数据集中抽取出重要的特性与信息,进一步完成分组、归纳、异常探测等任务。而机器学习的使用能借助已有的样本建立模式,以此去区分新输入的数据或者预估其结果,这有助于揭示潜在的安全风险。至于深度学习,它更擅长解决那些复杂且非线的难题,从而提升了分析的效果和速度[2]。

3 构建大数据分析应用安全策略

3.1加强数据保护与安全建设

保证数据在传递与储存过程中保持其保密性和完整性,以防遭到非正当手段的窃取或者修改。例如,很多银行及金融企业会利用SSL/TLS加密技术保障顾客信息的网络传送,并且运用如AES之类的加密方式去保护关键的信息资料的储存加密。建立严谨的数据访问许可制度和认证流程,只允许有资格的人员可以接触相关的数据。例如,实施多种形式的身份确认方法,配合上密码规则和权限管控,限制用户对于数据的使用。当出现安全问题或是数据丢失时,要快速地恢复这些数据。定期地把数据复制下来,存放在安全的且可靠的地方。例如,在医学大量数据研究里,会对病人的名字、身份证号码等私密信息做匿名化处理。详细纪录所有的用户关于数据的使用情况和动作,以便追踪,及时察觉并解决任何异样的情况。

3.2提升大数据网络安全感知能力

3.2.1异常行为检测

借助大数据分析工具,能够实时的监控网络使用量与客户活动等信息的数据异样状况,并迅速识别出可能存在的攻击迹象。建立常规操作模式后,可以对脱离标准流程的网络流量及客户活动发出警报,从而成功预防像DDoS攻击或数据泄漏等的安全威胁。例如,某些系统采用机器学习方法来研究网络流量,以掌握标准的网络使用方式,一旦察觉到任何非同寻常的行为,就会自动启动预警机制,立即向安全小组发送提醒以便采取行动。此种异常行为侦测技术能大幅度提升网络安全的积极反应速度和即时性,降低遭受攻击的可能性[3]。

3.2.2威胁情报分析

大量网络安全的情报资料被搜集与解析后,可揭示可能的风险源头及攻击策略,从而实现预先警报并在实施预防行动前做出反应。从黑客社区到深层互联网等资源都是获得此类信息的有效路径。借助这种情报资料的解读,能找寻到新型的安全漏洞使用方法和攻击技巧,进而优化防护方案。例如,某些安全小组运用了自然语言处理的技术来研究黑客社区中的对话内容,

从中提炼出了有关漏洞应用和攻击策略的核心知识,这对于防卫工作而言具有极大的指导意义。

3.3提升大数据网络安全融合能力

3.3.1数据融合

利用大数据技术,可以把从各种渠道获取到的各类安全的信息融合起来,建立出一个一致性的安全信息集合。这样能有效提升对安全情况的解析精确度与完整性,由于各式各样的信息源能够供给不一样的角度及讯息,融合它们就能更为深入地理解网络安防环境。例如,互联网记录可揭示有关网络使用量及其活动的行为,而系统监测资料则展示了系统的运作形态及其效能表现,而威胁情报则提供了已知的危险因素及进攻手法的相关信息。当所有这些信息被合并在一起时,便能得到更加详尽的安全图像,从而帮助安全小组更精准地判定安全态势并制定适当的应变措施[4]。

3.3.2技术融合

通过融合大数据分析和其他网络安全的策略,能建立出一种协作式的防御机制,从而增强保护能力。例如,可以把大数据分析同入侵检测系统或防火墙等安防工具结合起来,利用它们所产生的信息来做进一步的数据分析,以更加精确的方式确定是否有任何潜在的安全威胁,并且立即做出相应的反应来预防这类事件的发生。这样一来,这项技术的集成能够提升安防系统的智能性和自动操作性能,降低人力的需求量,进而增加其有效性和精准度。

3.3.3跨平台融合

借助大数据技术,能够完成对各种平台的安保信息的融合与解析,消除各系统间的信息隔阂。这样能有效提升总体的安全防御能力,由于各类操作系统及软件可能会暴露出各自独特的安全缺陷和威胁,把所有这些资料综合起来研究就能更为深入理解整套体系的安全状态。

3.4构建基于大数据分析技术的网络安全平台

3.4.1数据采集和整合

利用大数据分析技术建立的互联网安全体系能够获取自多个渠道的信息保护信息,如网络流转数据、系统记录、软件使用情况等等。这种信息的搜集可以在企业内外的网络环境下,各类操作系统及软件上,并能从各个安全的设备里获得。借助数据收集与融合,这个平台有能力把那些零散的数据汇集成单一的数据储存系统,从而为后期的数据大解析提供了充足的基础资料。

3.4.2大数据分析

这个平台借助领先的数据挖掘科技来深究收集到信息。它包含了异样行为侦测功能,也就是通过持续监控互联网流量、使用者活动等资料,找寻与常规模式相悖的活动方式,也涵盖了危险情报解析部分,就是透过研究大量网络安全的信息数据,去辨识可能的风险源头及攻击策略。另外还有连接分析的部分,应用大数据技术把从各处得来的安全信息联结起来做分析,以揭露攻击者的行事风格及其目的。这种分析能帮助系统找到隐藏的安全隐患,并且给予指导建议[5]。

3.4.3实时监控和预警

此系统具备即时安全的监测能力,能迅速识别出异样的行为与潜在危险,并且发出警报。借助这种持续性的监视方式,它能在初始阶段就察觉到网络侵害或者反常的活动,然后利用警示机制立即向安全小组传递信息,以便他们能够快速应对。这有助于提升网络防御的积极性和敏捷度,从而降低遭受袭击的可能性。

3.4.4可视化展示

此系统提供了视觉化的安全信息解析成果呈现,帮助领导层迅速掌握现有的安全环境并制定适当的对策。借助数据可视化科技,系统能把繁杂的安全信息解析效果转化为清晰明了的形式,使领导人能够迅捷地把握网络安全的现状,进而作出精确的决定及调适安全措施。这样有助于提升网络安全管理的效力和精准度,保障企业的网络安全无虞。

4 结语

利用大数据分析技术于网络安全的运用有着关键性的价值,采用如数据融合、技术融合和跨平台融合等方式能增强对安全研究的高精度与全局视角,帮助安全团队更有效地察觉可能的风险和攻击行动,从而保障互联网的安全稳定。建立依赖大数据分析技术的大型网络安全体系则进一步提升了多层次保护手段,包括收集和整理数据、实施大数据分析、持续监测和警报以及视觉化的呈现方式,这有助于迅速捕捉到异样动作、给出即时警告,同时向管理人员展现出清晰明朗的网络安全状况,以此来维护网络安全。

[参考文献]

[1]鞠禹,程茗飞,张树贵,等.高斯混合模型和大数据技术在网络安全异常行为识别中的应用[J].网络安全技术与应用,2023(7):32-36.

[2]李媛,鲁春燕.大数据技术在网络安全分析中的应用[J].网络安全技术与应用,2023(4):71-73.

[3]崔彦君.网络安全中的大数据技术应用[J].集成电路应用,2023,40(4):288-290.

[4]刘玲.大数据技术在高校网络安全中的应用探究[J].软件,2023,44(3):144-146.

[5]孟卫娜.大数据技术在网络安全分析中的应用[J].科技与创新,2023(3):159-161.

作者简介：

林大龙(2001--),男,汉族,广东省茂名市化州市人,本科在读,研究方向：网络安全。