大数据环境下网络安全态势感知研究

鹿佳岩
赛尔网络有限公司浙江分公司　浙江　杭州　310000

摘　要：随着信息技术的快速发展，大数据在现代生活中扮演着越来越重要的角色。在此背景下，网络安全问题日益突出，必须加强对网络的管理，以保证网络在大数据环境中得到充分应用。本文针对安全运维人员而言，怎样从海量的安全事件以及日志之中寻找最具价值与亟待处理的安全问题，并对安全态势进行感知，以确保网络的安全状态，成为其必须解决的问题。

关键词：大数据环境；网络安全

引言

大数据时代的到来，使得人们借助网络技术可以进一步提高自身的工作以及学习效率，不断提高生活质量。但对于网络环境来讲，其本身具备着高度的开放性，这也使得大数据时代背景下人们的个人私密信息也非常容易泄露，进而衍生出一系列网络诈骗以及网络暴力等相应违法犯罪行为，此类行为的出现可以对人们的生活以及工作造成巨大的困扰和影响，甚至引发财产或者精神损伤。基于此，有必要对大数据时代下的网络如何做好安全防范措施进行深入研究。

1 大数据概述

大数据的出现，改变了人们获取信息、资源的方式，从以前的网络、服务器到现在的计算机等。大数据具有容量大、种类多、速度快、真实性高、价值大的特性，因此被大量运用在信息产业中。但随着大数据的不断覆盖，数据泄露事件可能会达到100%，因此我们需要在源头上保证数据的安全，企业要在数据创建之初就对客户及自身数据进行安全保障。随着大数据时代的到来，信息的获取变得更为容易，网络犯罪的成本也更为低廉，因此防范信息安全已是迫在眉睫。大数据的价值主要体现在对企业、个人的便利性上。服务型企业可以通过大数据对客户进行精准营销；中小微型企业可以通过大数据的支撑进行服务转型；而传统企业可以通过大数据分析进行企业转型；对于大型企业来说，可以通过大数据高性能分析来解决企业问题，为公司节约数额不菲的成本；而对于个人来说，大数据可以为我们的交通、旅游、数据浏览等提供便利。

2 大数据环境下网络安全现状

2.1 缺乏计算机网络安全意识

互联网信息网络化带来的影响是多方面、多角度以及多层次的。互联网上的信息非常丰富、五花八门，带给我们很多便利，丰富了我们的业余生活，降低了获取知识的成本，降低了提升工作能力的成本，提高了工作的效率，同时可以快速建立良好的人脉关系。但是人们在享受便利的同时，却忽略了网络安全问题，而现代网络系统为了让人们提升网络安全意识，设置了很多安全措施，例如物理措施、访问控制、数据加密、数据镜像、备份和审计等，但是对于中国目前的网络使用者来说，他们依然对网络安全不重视，甚至为了满足自身的好奇心去破坏保护措施，因此严重影响了网络安全。

2.2 缺乏计算机安全网络保护的专业技术

近年来，中国网络黑客的攻击手段越来越强、越来越复杂，他们利用网络漏洞来对人们的经济安全等造成了严重的破坏，使人们的损失严重。另一方面，应用计算机和网络技术，保护己方计算机网络系统对抗敌方网络攻击的措施和行动的目的是防止敌方利用、削弱和破坏己方网络系统，确保己方网络系统正常运行。但是，中国目前缺乏计算机安全网络保护的专业技术，这就导致很多的安全问题没有办法及时得到解决。

2.3 安全管理体系不够完善

对于企业而言，完善的网络安全管理体系是应对网络安全最基本的制度保障。但是就目前情况来看，大多数企业还是依靠最基本的防火墙、杀毒软件等来对计算机的网络安全进行保障，没有建立起相应的网络安全管理系统。或者是建立起了一定网络安全管理系统，但是没有与之相对应的责任体系，管理水平跟不上，出现了严重的权责混乱的情况，计算机网络安全也无法得到保障。完善的网络安全管理体系是可以为各项工作提供指导的，比如最基本的可以要求定期开展针对企业员工进行网格安全相关方面知识的培训，邀请专业人员开展讲座，普及网络安全常识和最新技术，提高相关人员的网络安全防范意识[5]。另外，虽然我国目前也有相关的法律

法规来对网络安全行为进行规范，但是针对个人信息安全方面的法律法规还是相对欠缺的，也是不完善的，针对网络安全防护工作发挥的作用还是很有限。

2.4 网络安全意识淡薄

近年来，国家不断强调网络信息安全的重要性，也在全社会宣传网络安全。但光了解并不能起到什么实质性的作用，由于人们对网络的操作不熟练，对网络安全的不重视，导致在遇到网络安全难题时仍无法下手。众所周知，许多公司大都研制属于自己公司的系统，但大多数公司和企业对网络隐患并不设防，由管理疏忽引发的问题数不胜数。其次，大多数普通人对互联网的了解不够，对网络安全隐患产生的影响并不关心，认为与自己十分遥远，从而并不重视。其实不然，每个人的信息都是独一无二的，也正是因为如此，一些不法分子对公民的信息进行非法售卖，轻则信息泄露，重则损失财产。因此，提高网络安全意识、了解更多的网络安全信息，是保护我们自己的重要举措。

3 大数据环境下网络安全优化

3.1 规范网络安全管理机制

大数据时代，人们的信息资源获取方式得到了彻底的改变，数据的潜在价值也得到了高度的体现。这些海量的数据储存在互联网上，就需要一个健全、完善的数据管理机制，以此来对团体和个人的网络行为进行约束、对违法行为进行惩处、对不法分子进行震慑，以达到从源头上对危害网络安全的行为进行管控的目的。从大的层面来看，国家相关部门已经制定出了法律法规，通过采取强制性的手段来对违反网络安全管理条例的个人与机构实施进行严厉的惩处。

3.2 重视数据管理

应用计算机网络，以交互数据信息为核心。计算机网络的普及应用，为人们传输信息获取数据带来了便捷体验。同时，随着数据处理任务量的增多，若在某一环节出现错误，便会导致系统内的所有信息都有可能陷入危险境况，诱发严重的网络安全问题。所以，在网络虚拟空间，应注重控制计算机安全问题，在每一环节都要加强数据管理及数据控制。具体来说，首先要强化数据采集管理工作，为了全面保障网络数据库系统正常使用，就应加强数据采集环节的防范工作，充分了解原始数据特性及原始代码，使用分类控制手段防范数据风险，并重视管理数据传输时的数据问题。

3.3 加强计算机网络安全防范意识

大数据网络时代，提高网络安全不仅要靠技术，还需要我们从自身意识着手，警惕危险、提高网络安全防范意识。从小处着手，个人在使用网络技术时，要注重个人信息的保护，不要将个人信息到处传播，对于一些不良网站或是不可信网站不要进行点击，不给不法分子任何可乘之机；然后是企业及各单位对员工、学生等人群进行网络安全防范意识的宣传，并向大家演示各种可以泄露个人信息或者被窃取信息的方式，以实例来提醒大家，我们的个人信息会在哪些地方被盗取。然后是政府可以加大对网络安全的宣传力度，用各种案例来警醒我们若是被盗取了个人信息会导致些什么样的后果，我们将承受什么样的损失，以此来加大我们对网络安全防范的意识，认识到网络安全防护的重要性。

3.4 加强网络安全人员的专业技能培训

通过更好地为网络安全的相关人才进行专业技能培训，可以加强人才队伍的建设。目前我国经济安全事故中存在很多由计算机网络安全带来的负面影响，计算机网络安全事故的发生原因和后果是多方面的。比如：恶意软件、木马病毒等网络攻击活动的不断出现，使得国家无法及时掌控网络安全状况并进行有效干预，这就需要政府加强网络安全专业人才队伍的建设。虽然从当前来说这种培训工作并不十分到位，但是针对一些网络安全事故频发的情况，有必要提高相关人员法律意识和政策意识，注重网络安全技术人员之间的沟通、交流以及协作能力，从而提高网络安全人员对突发情况下网络信息安全的防护能力和快速响应能力。

4 网络安全态势感知相关技术

4.1 证据理论支持的网络安全态势评估

大数据环境中，许多因素都不同程度的影响网络安全状态，网络安全态势评估将引入不同类型网络设备的二元数据，包括许多有害程序的信息数据以及漏洞信息数据等，这些数据将导致网络安全态势评估精准度减弱。大数据环境无法对不同类型证据源开展正确的检验以及识别，而业务应用、软件以及网络节点等证据源不同，用以检测的传感器可靠性也有一定的差异，可信度并不完全相同。此外，网络安全态势评估工作中，不同专家的可信度也有显著差异，所供应的证据信息之间可能产生高度的信息矛盾。为了尽量减少可信度不足的证据源影响网络安全态势的评估结果，处理证据信息之间冲突的问题。基于此，相关工作人员可选择根据对证据源予以预处理和修正组合规则这两种改进方式，提出以改进证据理论为基础的网络安全拟态评估算法，用以评价网络安全态势量化评估，基础思想是构建网络安全态势评估指标。然后构建引入不确定性变量的信度分配函数BPA，同时应用牛顿法改善专家信度，并利用基于一致

性度量方式改善证据源距离的计算方式，明确各个证据的可信度，最后利用线性加权的方式改变原始证据源，明确证据源的综合权重，并对证据MASS函数予以修正，根据新的证据模型应用基于局部冲突分配改善证据合成同时处理指标证据之间存在的局部冲突，同时融合计算机网络安全综合态势。

4.2 态势预测

态势预测将一定的科学依据作为基础，对比与分析历史和现状，以有效推断未来事物发展的状况及其不确定性，或是结合目前信息数据，应用科学理论与合理的方式对未来阶段网络可能形成的安全隐患予以预估。结合不同的预估状况运用不同的预估方式，例如常见有定性预估法、时间序列法以及因果关系预测法等，其中定性预测法主要是结合人的逻辑判断，主观分析历史与目前的经验，结合经验预估系统未来的发展走向以及状态。针对不完善的历史数据，建议运用主观方式予以预估。时间序列分析方式通常是针对历史资料开展时间改变，在预估系统未来某一段时间的表现之后，结合系统时间变化关系明确预估信息数据，在讨论数据因果关系的同时寻找原因因素，构建因果关系的模型，并结合模型实际状况明确结果的变化方向。

结束语

大数据的开发与应用为我国的经济发展和社会进步提供了较高的技术支持，在大数据时代下，个人和企业要规范的使用网络系统，加大网络安全的监管力度，提高个人和网络安全问题意识，推进网络安全防范软件的开发和有效利用，完善计算机网络安全管理制度，提高专业网络安全管理人员的技术水平和管理水平是维护大数据下网络安全的最好的方法。在网络环境多变的情况下，网络安全人员要时刻关注计算机网络的安全，保证网络稳定安全的运作。

参考文献

[1]李大玮，刘鹏，王璐.基于大数据的网络安全态势感知系统在网络安全管理中的应用[J].中国新通信，2022（02）：137-138.

[2]李程雄.网络安全态势感知系统关键技术研究[J].电子技术与软件工程，2021（23）：231-233.

[3]周娟.基于大数据的网络安全态势感知关键技术研究[J].电脑知识与技术，2021（31）：51-52.