大数据时代如何加强计算机网络信息安全管理

许应强
云南省工业和信息化厅　云南省　昆明市　650031

摘　要：随着科学技术的快速发展，大数据的应用范围越来越广泛，在大数据的时代背景下，计算机行业在为用户提供便捷高效的数据服务的同时，应重视计算机网络信息安全，避免用户的重要数据信息在传输过程中被破坏或泄露，对用户造成严重的经济损失。本文基于此，简要概述了大数据技术，结合大数据时代计算机网络信息安全的主要影响因素，探讨了在大数据时代背景下加强计算机网络信息安全管理的具体措施。

关键词：大数据；计算机；网络信息安全

引言

大数据时代，很多的信息信息开始在网络上散播。一般来说，当客户浏览互联网技术以获得需要信息时，她们借助计算机的数据传输作用来共享和互换信息网络资源。消费者浏览和数据传输里的信息安全隐患也引发了社会各界人士高度关注。在大数据时代，一些电子计算机网络黑客和病毒感染运用计算机网络的系统漏洞侵入计算机软件，积极或被动攻击特定对象，盗取、毁坏和泄漏信息数据信息，威协互联网信息安全性。通过加强计算机网络信息安全管理，对影响信息安全的因素进行分析，并寻求相应的解决措施，从而有效提升计算机网络安全防护水平。

1 大数据背景下计算机网络安全概念

伴随着用户的数量提升，计算机网络形成了大量的数据信息。这种很多的信息不但数量大，并且基本数据类型多种多样。电脑的普及化为人们的日常生产活动增添了质的改变。大家能够更加省时省力地获得各种各样信息网络资源，通过网络检索寻找自己基本上所需要的各种各样信息。在大数据持续引进的大环境下，计算机网络技术性对各行业的发展趋势起到关键性的功效，各个领域工作效率不断提升，巨大地区方便了广大人民群众最低生活保障。但是，在互联网时代，各种各样信息与知识技能的爆发式增长导致了很严重的就业就业问题，互联网时代的计算机网络信息安全现状令人担忧。为了能计算机网络的安全性，各个公司都是在不断完善自己的信息系统软件。从上述这几个方面能够得知，现在很多企业主对计算机网络安全性全是等候知道的，在计算机网络运行时都还没创建安全管理措施和优化对应的规章制度。为了方便预防网络黑客的黑客攻击，相关部门与企业设立了计算机网络安全管理体系，使本单位的计算机管理能力得到持续，前沿的计算机技术性可以立足于生产制造与生活，与此同时推动中国社会社会经济全方位发展[1]

2 计算机网络信息安全防护的必要性分析

（1）计算机网络信息安全可以保护计算机系统内部的重要数据，是计算机网络管理方法最为重要的工作中。在计算机网络中，管理人员能够防止一些外界病毒和计算机自身携带病毒侵入，维护计算机的内部关键信息，避免网络黑客运用计算机病毒盗取关键数据库文件。要避免黑客攻击，企业主需要具备保护与管理方法计算机网络信息安全水平，不可以降低个人信息的泄漏。

（2）加大计算机网络信息安全防护力度，避免计算机病毒的形成。现在大部分计算机都装上电脑杀毒软件，但是一些用户难以考虑到的网页页面和软件很有可能带有病毒。使用的时候把病毒带到计算机，下一次打开才知道病毒的出现。对于此事，提升计算机网络信息安全工作，搞好计算机网络信息安全防范工作，降低各种各样信息病毒的出现，让更多的网友安心网上。

（3）保护系统的安全。终端设备储存的信息量非常大，因此需要更高安全系数。终端设备的所有数据信息也是通过数据传输的。因为传送的信息包括了很多的机器设备硬件配置信息，假如不提升对互联网信息保护的，非常容易被犯罪分子传送的信息发放给终端设备。[2]

3 大数据时代计算机网络信息安全存在的问题

3.1 病毒入侵

危害计算机平稳运作的原因很多，主要的原因是病毒侵入。互联网技术用户在经过计算机网络开展互动交流和电子邮箱派发的过程当中，不可避免也会受到病毒的侵入。但病毒具备快速传播快、杀伤力强、隐秘性高的特性，许多用户的病毒也具有毁灭性。它不但可以借助电脑硬盘散播病毒，也可以在传送全过程中加入很多被丢掉文件，让被侵入的软件再次迟缓运作，进而毁坏

高效的系统文件。病毒或信息在电脑硬盘、光碟、硬盘等媒介上传递的全过程。它伴随着传输数据而散播，不但受到破坏互联网技术纪律，导致数据泄漏，并且在计算机系统内储存了海量数据。

3.2 误操作

在大数据环境下，不但数据库的数量及种类在不断增长，并且不同种类的数据信息也在不断地结合，这不但影响了用户工作效率和生活习惯，也帮用户互动增添了一定的难题。伴随着计算机操控的日益繁杂，人为因素对互联网信息安全威协愈来愈突显。在利用大数据技术实现数据处理方法与传播的过程当中，相当一部分职工的水平落后于信息安全规定，不能对统计数据进行合理的数据加密保护和。人为失误不但直接关系网络信息安全，也帮犯罪分子带来了机会。犯罪分子能通过各种各样方式方法，运用一些互联网病毒和恶意代码侵入计算机，盗取用户的信息资料和，威协用户的信息安全性，危害用户利益。互联网时代，计算机技术性更新换代快，相关负责人具有很高的计算机实际操作水准、专业技术人员和网络安全意识。互联网信息安全人员仅有了解并掌握各种各样计算机实际操作技术以及作用，才能达到各种各样互联网信息安全性。

3.3 网络崩溃，突遭黑客侵袭

现阶段来说，黑客攻击早已成为一种习惯。对于一些公司，在他看来已有的网络信息安全对策早已可以防止大规模的黑客攻击，从而减少对黑客的高效防治。这也为黑客的突击带来了室内空间，各种各样预防措施没法合理融合，不能满足网络安全的要求。自互联网技术数据应用发展趋势至今，大数据的监测和维护技术性持续改革创新和改进，但依然必须及管理技术相结合，以防护系统实效性。在设定预防措施时，依据黑客攻击的方式设定防护墙。黑客大多数盗取数据。如果他没法盗取数据，便会故意攻击系统软件，造成内部结构运用崩溃。因而，为了避免很多数据遗失，一定要注意在黑客侵入时获取信息，有效控制关键数据，将数据遗失带来的损失降至最低。一般来说，黑客会找寻系统软件里最欠缺区域进行攻击，扩张攻击面，让系统软件瞬间崩溃。这时必须相关应用管理者开展实战模拟，找到全面的薄弱点，有目的性的开展结构加固，确保信息安全性。[3]

3.4 解密攻击

为了能让互联网数据的信息传输更安全，相关负责人往往会在传输前对它进行数据加密，以保证网络服务器和手机客户端间的信息安全性传输。但对于有利益的信息，一些黑客会因权益引诱开展破译和攻击，立即毁坏计算机软件，使互联网信息的传输越来越不安全的。与此同时专业技术人员对数据开展数据加密，但很多计算机黑客的专业能力越来越强大。即便她们层层加码，也非常容易被黑客团队破译，盗取经济发展的利益数据信息。在破译攻击环节中，计算机软件自身存在一定的风险性，明显的时候会造成计算机软件奔溃，会严重影响客户的正常启动，也会给行业企业产生难以预测损失。

4 大数据时代加强计算机网络信息安全具体策略

4.1 采用新技术，加强数据信息监控

在科技进步快速发展的环节中，环境因素对互联网信息攻击更为隐敝，攻击的方法和方式更为多样化。这类传统式网络的信息保障措施无法积极应对。因而，积极主动选用新技术应用与创新的保障措施。从总体上，互联网便是灵活运用大数据技术性中强悍的优化算法和构架方式方法。在简单化数据信息的前提下，保证数据原始的信息不遗失、使用价值不损伤、数据传输高效率不降低，借助有关方式方法完成不一样数据间的互动。以诊疗信息数据储存为例子，为确保关键数据信息的安全性，关键执行三级管理，即搭建大数据云储存空间，将这些诊疗信息储存在本地服务器上，与云储存空间同步，多种形式数据加密数据，选用前沿的加密算法，将重要数据和数据加密信息分开储存。最终，创建数据信息的多路备份数据体制。这种关键数据信息的传输也设立了对应的流程管理。最先运用有关方式方法监管数据信息的传输全过程，随后创建统一的数据信息处理程序与处理分析平台，对每一个数据网络资源执行统一管理。在数据浏览阶段，可设置数据信息的健值对浏览客户进行排行，不同级别客户有着不同类型的访问限制和不同类型的健值。除此之外，对浏览客户进行全面的验证，避免非法侵入，对其浏览账户设置跟踪体制，一旦出现数据信息安全隐患，可以通过跟踪体制追责相关负责人义务。[4]

4.2 设置安全权限以及进行加密管理

在计算机网络信息安全性期内，相关工作员能够灵活运用核心技术对计算机系统实现监管。为防止客户比较敏感信息泄漏，相关工作人员提升计算机网络信息的密钥管理，立即避免非法访问，有效控制数据网络信息。但是，伴随着互联网技术发展，在计算机网络信息安全防护环节中，计算机网络信息密钥管理具有一定的局限，不可充分运用其性能和使用价值，不可从源头上完全阻拦违法侵略者。

一般来说，当计算机在系统无线路由器中间运作和转换时，都是会应用公钥来完成对计算机网络信息深度

维护。在互联网时代，为保证计算机网络信息安全性，相关工作员应依据计算机网络发展趋势具体开展数据加密，提升密匙验证和计算机网络信息实效性管理方法。另一方面，相关工作员运用密码算法构建网络管理平台，密匙使用价值的，计算机网络信息安全水准。换句话说，设定安全性管理权限和双因素认证有利于确保计算机网络信息的安全性。合理的安全性管理权限和加密算法能使计算机系统优化运作，维护商业秘密信息不会被网络黑客盗取。

4.3 提高网络安全管理

网络安全防护观念和网络安全的维护保养需要由个人或企业计算机客户互相配合。普通用户使用计算机传送信息以前，务必深入分析计算机的状况和自学能力，并运用到计算机中。运用云计算技术数据处理技术，企业理应不断完善网络安全防护规章制度，提升内部结构网络信息安全和互联网账号管理。密码设置复杂性能够降低数据泄露风险，因此可以在企业系统内对相关账户开展密码设置对策，按时互换登陆密码。针对隐秘数据信息，企业和政府都需要有安全性防范意识，创建安全性防御机制，保证比较敏感信息万无一失。企业和政府使用计算机时，必须进行全面核酸检测和删掉。因而，建议把外置硬盘与手机app防护，不必相互连接储存核心数据的电脑。最好是按时认证数据与信息安全性，立即清除一些风险性，确保企业比较敏感信息的安全性。除此之外，网络应用设施设备基本建设也非常重要。定期维护维护保养硬件配置和网络线，立即化解风险，避开互联网安全威协。

4.4 完善相关网络管理制度，提升管理水平

数据的收集和键入取决于网络信息安全，因此为了保障网络信息安全，务必提升互联网技术的监管与应用。但在现在的互联网管理制度下，有偏重于创作，并没有根据部分难题改革。为了更好发展趋势企业，在互联网时代应用计算机网络时一定要考虑管理方案，依据数据库的特性和数据统计分析方向摆脱文件格式管理方法。计算机智能管理系统的根本目的是保障信息和信息的安全性。与此同时，数据库的管理与储存务必一致。与此同时，职工需有正确使用观念和网络信息安全观念。在数据信息验证层面，包括对特定人开放访问限制，限定对于整个互联网信息平台系统的访问次数，数字证书技术性能够有效预防数据信息信息的泄漏。

建立和完善的远程教育系统必须国家和企业深度合作。在互联网平台上，国家必须从宏观角度对网络信息安全开展监管，为我国企业给予相关安全防范措施，让企业带来更多盈利。企业也要高度重视内部结构数据库管理，带来更多的福利，为社会做贡献，基本建设国家的国际地位。现阶段，网络信息安全还和国际冲突相关。国家和企业都需要完善内部的网络管控制度，利用更加先进的计算机防控技术，保证网络系统平稳运行。同时，还要使用网络监测技术，对有问题的环节需要及时处理，从源头避免隐患发生，为网络安全提供保障。[5]

结束语：大数据时代背景下，数据作为信息的载体，能够发挥各种各样的作用。但是必须以网络技术为承接对象。为了充分的保护数据安全，需要对网络技术提供一定的安全防护。信息使用单位要根据信息使用环境设置保护措施，降低计算机网络使用安全风险。另外，不仅是对数据安全进行维护，还要对计算机进行一个日常的病毒防护，防止网络被黑客入侵造成数据丢失，可以安装一些杀毒软件为系统提供更加全面的安全保障。

参考文献：

[1]韦超英．大数据环境下计算机网络信息安全的对策研究[J]．电脑知识与技术，2020(33):62-63.

[2]李雯瑞．大数据环境下计算机网络信息安全防护措施研究[J]．信阳农林学院学报，2020(3):109-112.

[3]韦超英，凌志梅，李海强．大数据环境下计算机网络信息安全的对策研究[J]．网络安全技术与应用，2021(9):70-71.

[4]李辉．大数据环境下计算机网络信息安全的对策研究[J]．信息记录材料，2021(5):44-46.

[5]宋曼．大数据环境下计算机网络信息安全的对策研究[J]．计算机产品与流通，2021(3):64-65.