大数据背景下计算机网络信息安全及防范策略研究

马锦贤
中国电信股份有限公司新疆分公司，新疆 乌鲁木齐 830000

[摘要]第四次工业革命是信息的革命，信息化在当代发展已经相当成熟，如今，人们更加愿意在互联网上进行信息的互换与交流，我们可以在任何地方看到信息化的影子。提升网络安全意识、熟悉简单的网络安全技术已经成了目前对付网络安全问题一定要达到的标准。本篇依据为什么要防范计算机信息安全、现阶段存在的一些问题并提供解决的方法作为引导。补全计算机互联网的安全性。

[关键词]大数据背景；计算机网络信息系统；安全防范策略
DOI：10.33142/sca.v5i8.8159 中图分类号：TP311.13 文献标识码：A

Research on Computer Network Information Security and Prevention Strategies in the Context of Big Data

MA Jinxian
Xinjiang Branch of China Telecom Co., Ltd., Urumqi, Xinjiang, 830000, China

Abstract: The fourth industrial revolution is the revolution of information. Information technology has become quite mature in contemporary development. Nowadays, people are more willing to exchange and exchange information on the Internet, and we can see the shadow of information technology anywhere. Improving network security awareness and becoming familiar with simple network security technologies have become the standards that must be met to deal with network security issues. This article is based on why it is necessary to prevent computer information security, some existing problems at this stage, and provides solutions as guidance, which is conducive to the security of the computer Internet.

Keywords: big data background; computer network information system; security prevention strategy

引言

现代互联网高速发展，信息的传播不再是以前的单一模式而是以多种形式传播，在这种情况之下，信息的获取变得不再困难，信息的安全性遭受到前所未有的挑战。针对计算机互联网信息系统安全问题提出标准的管理标准，确保信息在传播中是安全的，创建一个信息传播安全的互联网，体现出社会主义核心价值观，推动互联网朝着更安全方向发展。

1 为什么需要在大数据背景下强调信息的安全性

明确对计算机互联网进行信息保护的必要性和它拥有的现实意义，之后才可以在平常的工作中不会犯错并经过一段时间的学习之后自我进行创新。计算机技术是在不断发展的，想要在自动化和数字化领域中有所建树就不能够脱离学习，只有不断的学习计算机新技术才能够达到更高的境界。就现阶段计算机互联网信息系统安全技术的情况来说，必须特别注意技术是否安全是否可控，可以保证在大规模数据进行传输时不会失去控制，比如在数据传输过程中发生数据被窃取的情况，又或者是数据发生缺失的情况，以上这些都是继续处理的互联网信息安全的问题。提升计算机网络信息系统安全的整体水平，对于其他行业的发展也有一定的好处。[1]

把提高计算机信息系统安全系统放在首位，并制定相关的措施来帮助处理现阶段互联网环境存在的一些问题。因为现阶段的互联网环境不断发展，这就导致了计算机信息系统安全防范技术也必须进行自我提升，来适应现阶段的互联网环境。与此同时信息的传播也不再单一，这就催生了影响计算机信息系统安全发展的问题。以及在这些安全问题上，IT 人员如何对当前的技术进行检验，需要掌握相关技术，并对当前形势进行批判性分析，积极采取应对措施，以便更好地管理 IT 系统的安全，建立稳定的环境，安全信息的传播保持了在互联网上传播更健康信息的过程，以便所有行业都能更好地发展。

2 当前阶段影响计算机安全的因素

2.1 自然灾害影响因素

尽管目前计算机发展得很迅速，给予人们在平常的工作以及学习能够更加方便地完成任务，美中不足的是计算机网络安全信息并没有像想象中那么发展无阻，还是有一些因素会阻碍发展，进而影响信息的安全性。在这些影响发展的因素之中，自然灾害无疑是无法忽略的一个，由于计算机在实际运行中是需要硬件设备的。只有硬件设备是完整的才可以确保信息的传播速度，但是硬件大多数由金属做成，假如真的出现了某些自然灾害，这些设备的完整性极其容易受到威胁，严重的甚至会影响到计算机网络信息的安全。[2]比如某个在山脚下的区域突然受到泥石流的冲击那么相关的设备就会受到影响，就算泥石流造成的破坏不是很严重那也会损坏一些硬件设备，假如这时候再遭

受到其他自然灾害的侵害，硬件设备很有可能彻底瘫痪，这将最终导致信息的传播受到影响。

2.2 技术影响因素

除了上面谈到的自然灾害之外，计算机网络技术的高低也会对信息的安全产生影响。我们都知道计算机网络对信息是不作限制的，这种特性使得信息可以即时在互联网中进行上传以及分享。不同行业可以实时地进行数据之间的共享以及传输，这对于本行业来说利大于弊。但信息的开放性是一把双刃剑，既有好处也有坏处，坏处就算有一些心怀不轨的人会以信息的开放性作为突破口从而攻击计算机网络，这将导致各种网络信息安全问题产生，传统的计算机网络一般是用 TCP 来进行信息的防护，在目前看来这种方法已经落后了，且效果不好，信息在互联网上进行互换和交流的时候极容易受到攻击，这也侧面说明了为什么信息在互联网上进行交流和传输时是不安全的。

2.3 信息使用者造成的影响因素

想要提升计算机网络信息的保密性，就不能任由信息使用者随意进行操作，但是目前的状况并不是很乐观，计算机使用者对于计算机的理解不同，技能水平也有所区分，这就会导致不同的人在操作时会采取不同的操作，如果不对用户进行一些约束，计算机网络信息的安全就很难得到保证。计算机使用者在实际在互联网上进行信息的交流和传播时一定要注意自身的操作问题，要时刻注意不让信息泄露，这也有助于提高信息的保密性。

2.4 病毒

我们可以看到，在新时代计算机网络在不断发展，与此同时计算机病毒发展得也相当快。病毒对于计算机网络的破坏性是相当大的且病毒具有不断增殖难以消灭的特点。有一些特别的病毒卧底在计算机中在很长一段时间内很难被用户发现。所以有关部门必须针对常见的一些病毒开发一套行之有效的杀毒软件，让这些杀毒软件检测出并处理掉病毒，这些措施有利于保证信息在传输中的保密性。

3 当前大数据下需要注意的问题

3.1 网络带来了大量的资源

资源在互联网上可以相互分享是一把双刃剑，不仅能够让人们的生活更加方便也容易被一些心怀不轨的人利用从而破坏互联网信息共享模式，攻击将导致互联网瘫痪从而人们没有办法再继续进行资源共享。

3.2 网络上的资源基本没有限制

任何人都可以在互联网上找到一些不方便公之于众的信息，如果这些信息被心怀歹意的人通过互联网大肆传播极有可能对他人造成不可逆转的影响。

3.3 设计出来的系统越来越难使用

现阶段有部分系统涉及到的功能较多，系统的开发者设计出来的系统操作难度较大，故而一些能力不够的操作者没有办法完全驾驭，这就会导致后期出现许多安全管理层次的问题，难以掌控的问题层出不穷。

3.4 没有重视网络资源的管理

互联网上的资源范围的增长，但是针对网络资源利用的边界难题并开展对应的管理，第一没有办法确保互联网上的资源就是完全安全的，第二这些资源极其容易被盗版从而造成版权之争，这也会对当前社会产生不必要的影响。[3]

3.5 没有办法对网络资源散布途径进行追查

当前我国几乎每家每户都有手机和个人电脑，信息可以当前社会肆意传播且不受控制，部分互联网资源是需要被管理的，互联网信息传播途径众多，这些资源的保密性没有办法得到保证，一些保护措施实施起来也比较困难，没有办法在源头控制传播。

3.6 过于集中的网络信息资源容易遭到不利的攻击行为

一般来说，当网络信息资源不集中时，它们产生的价值较低，同时存在感极低；但是，当嵌入更多分散的信息时，显示值的影响和意义也会发生显著变化，此时很容易受到恶意攻击和其他人的传播。

3.7 当前关于网络的法律还不够完善

当前社会网络发展迅速连带着计算机在我国发展得相当不错，但是当前存在部分心怀歹意的人窃取互联网上的资源来取得利益，而当前法律法规在互联网这一块还不是很完善没有办法对这些不法分子进行惩罚，导致互联网上面的资源极其容易被窃取从而损害这些资源所有者的利益。关于中国用于计算机网络安全的保护技术和操作系统，存在一些技术限制和障碍问题。面对计算机网络信息技术的快速发展，其配备的安全防范系统无法适应当前的技术发展，再加上计算机用户缺乏相关技术知识，很容易对计算机网络信息体系造成安全风险。

4 建立系统的计算机网络信息安全防范

当前计算机网络信息是需要抗住黑客的攻击、能让互联网上的信息安全进行传输、可以被控制等有效的保护系统。具体的措施可以通过和防火墙、杀毒软件、系统文件检测软件联合来创建系统性的防护墙，这些举措可以有效减少计算机网络信息系统被黑客攻击的次数，也降低了黑客攻击计算机网络信息系统的成功率，导致黑客不想再进行下一次攻击。

4.1 安全服务器的建立

安全服务器是整个互联网的核心且必不可少的设备，它大致服务于电子信息行业。并且当前中国当前使用安全服务器大部分是中国境内安全服务器设备，它们所具有的功能和能力都可以很好地满足中国境内计算机信息安全的需求。利用这些服务器可以保证信息在互联网上进行传输和交流的时候不会被窃取且不会发生其他的安全性问题。

4.2 建立完整的预警系统的防护功能

预警系统的详细功能就是对互联网上获取的信息所蕴含的意义开展智能化的解析来看这些信息是否拥有对用户潜在的威胁或是将来一段时间会对计算机网络进行攻击等，并且提前作好防御的准备来防止计算机网络信息

系统被黑客攻击而陷入瘫痪状态。

4.3 合理利用网络防火墙是保证计算机网络安全的必要手段

互联网防火墙的基本定义是根据被防护网络和其他网络进行交流时把可能对用户网络造成伤害的隐患排除在外的一道自我保护壁垒。在防火墙进行工作的时候，防火墙会对所有进行交换的数据进行检测如果检测结果有可能是用户网络造成伤害那么就直接把这些数据排除在外，这个措施可以有效保障用户网络里面的数据不会被不法分子窃取并被恶意传播。有一些防火墙比较特殊，它们的大致作用是作为其他网络和网络安全域之间的进出口效果的防火墙，管理人员能够使用系统化的安全措施来管控互联网交流用的信息，有效地抵抗黑客发起的攻击。[4]除了保护信息安全，网络防火墙还可以检查、操控和监管内部和外部网络活动过程，增强使用者网络信息数据的保护，大大推动了计算机网络信息系统的保密性。

4.4 使用病毒检测软件来针对计算机病毒第一时间报警处理，依据可被识别和不可识别的病毒开展清除行动。

杀毒软件在病毒处理系统的使用可以在网络系统和网络合同的安全层面和操作系统的层面上开展病毒识别和清扫的管控，建立属于用户自己的病毒管理体系。该病毒管理体系的运行原理是已知的互联网病毒和正常的程序是不一样的，互联网病毒可以被病毒管理体系识别出来，不仅如此，病毒管理体系还可以对已经发现的病毒进行解析，从代码的角度来解析病毒可以有助于防止病毒的传播。

5 敲定真实有效的计算机网络信息系统安全的保护措施

5.1 人才是根本，应该在大学里面积极开设网络安全专业

到目前为止，中国国内已经有很多企业专门进行信息传输的研究、技术开发以及病毒拦截的研究，这些企业已经成为了我国信息安全防护产业的顶梁柱。但是如果想要提升我国计算机信息防护水平，就必须从基础上进行学习。当前我国高校已经在积极开设网络安全专业，让学生可以在高校中系统化地掌握网络安全知识，有助于学生增强网络安全方面知识的熟悉程度，并在以后积极投身于网络安全系统的建设，从而增强我国网络信息防范的综合水平。

5.2 不忽视日常计算机信息系统存在的问题并积极进行自我查漏

用户在平常操作计算机的时候一定要注意对当前系统已经存在的漏洞进行修补，防止受到黑客无端的攻击。用户还要把重心放在计算机信息系统的安全上面，从互联网上下载可以检测计算机中是否存在缺陷并自动处理的软件，这极大地提升了计算机对于互联网病毒的抗性。但是最基本的病毒防范手段还是需要用户自己要有相应的病毒查杀技术。及时看出病毒侵入时软件发出的警报信息，在病毒侵入的时候立即启动杀毒软件对计算机内部的病毒进行处理，使得存在于计算机内部的数据不会遭到窃取。

5.3 把生物识别技术和数据签名技术融合在一起开展双重身份识别认证

科学是在不断发展着的，科学在不断发展着的同时也带动着网络信息安全技术的发展，从而产生了许多更有效的安全技术。目前使用人的身体本来就有的生物特点来开展识别的技术方法已经在部分重要的安全防范行业中率先亮相了。前面提到的生物识别技术的关键是利用每个人的指纹是不同的、手掌也是不相同的、字迹上的区别、脸部方面的区别等人体完全不同的特点来实现身份检验的流程，生物识别和以往的识别技术相比有着巨大的优势。数字签名的含义就是指当需要验证身份的人员发送验证请求时，指挥部将给验证者发送一串不可伪造的数字，验证者将数字提交即可完成身份的验证。这一类方法将有效的提高计算机网络信息的安全性。

5.4 浏览控制以及信息加密技术融合在一起，坚决把控浏览权限

访问管控技术的使用十分的普遍，不管是不是计算机系统都很有可能会需要访问管控技术。一般情况是系统监管人员经过对想要访问的用户开展管理，确保了访问者对服务器、目录、文件等互联网资源的访问是安全的。不仅能够高效组织不合法的主体窃取需要保密的互联网资源；还可以有助于组织合法访问者对被保密的互联网资源进行非授权的浏览；这是计算机网络系统信息安全的核心预防措施。信息加密技术的使用是一种通过数学或物理手段等有效保护一系列电子信息免受盗窃或泄露的技术手段。在现阶段，信息加密技术已成为国际社会各国特别关注的话题，技术手段的升级正在迅速发展。

6 结语

我国计算机发展得相当快，但是在发展之下也有一些信息安全类问题产生。比如网络攻击层出不穷，这些攻击行为不仅会对我国信息发展造成影响还会阻碍互联网朝着健康的方向发展。只有不断努力提升计算机网络安全的水平，增强对应科技的研发，确保我国各行各业的经济都可以飞速发展，对于保持国家的安全、安稳起到了正面向上的作用。

[参考文献]

[1]代玉石.浅谈计算机网络下的信息安全及防护[J].信息系统工程,2022(9):79-82.
[2]罗潇.新环境下计算机网络信息安全及其防火墙技术应用研究[J].信息与电脑(理论版),2022,34(8):215-217.
[3]佘春燕.大数据背景下计算机网络信息安全防护手段研究[J].软件,2022,43(3):65-67.
[4]杨佳兰.基于大数据环境下的计算机网络信息安全与防护策略研究[J].南方农机,2021,52(23):132-134.

作者简介：马锦贤（1980.5-），毕业于新疆大学，通信工程专业，研究方向：网络信息安全。