

大数据时代计算机网络信息安全问题探讨

唐 玮

(苏州高新区教育发展中心, 江苏 苏州 215000)

摘 要: 信息数量的加大,在促进大数据技术发展、切实满足人们生活需求的同时,由于计算机网络规模的大幅度加大,带来了诸多的信息安全问题。本文主要对大数据时代计算机网络信息安全相关问题进行了简要的探讨。

关键词: 大数据时代; 计算机网络; 信息安全问题; 思考与对策

Discussion on computer network information security in the era of big data

TANG Wei

(Education Development Center of Suzhou High-tech Zone, Suzhou Jiangsu 215000, China)

【Abstract】 The increase of information quantity, while promoting the development of big data technology and effectively meeting people's needs for life, has brought many problems of information security due to the large scale of computer network. This paper mainly discusses the problems related to computer network information security in the era of big data.

【Key words】 big data era; computer network; information security; thinking and countermeasures

0 引言

近年来,科学技术得到了巨大的飞跃,计算机逐渐克服了地理限制,可以将不同地方的机构通过计算机联系在一起。通过公用的传输网络对一些交易信息进行传输,但是这些交易信息通常是比较敏感的。通过一些方法,就可以对一个机构的私有网络进行访问,并且私有网络也经常由于各种原因,与外界网络联系在一起,这些因素都会导致计算机网络的运行环境变的复杂,信息传播更加普及,从一定程度上降低了计算机网络的可控性和稳定性。

1 大数据时代背景

大数据时代,显而易见,就是有数量非常庞大的数据信息,从传统的单一化朝着多元化的方向不断发展。大数据时代下,数据更新周期变短,并且自身的成本也在逐渐降低。大数据时代一个非常典型的特征,就是有海量的数据信息。其次,也包括各种各样的数据类型。在当前发展阶段,计算机网络的发展十分迅速,大数据也被广泛应用,各行各业都开始使用大数据,包括各种各样的企业、学校、政府相关部门等等。但是随着大数据的广泛应用,也带来了一定的计算机网络安全问题。因此,创设一个好的网络环境,是社会发展的要求,可以从一定程度上提高数据的安全性,保障信息的隐秘性。

2 大数据时代信息安全问题

2.1 信息安全管理体制不完善

当前,人们在进行工作和生活的过程中,会频繁使用到计算机网络,很多事情都必须通过网络才能顺利的进行。特别是进行网上购物时,要把自己的各方面信息在 APP 或者是网站上进行详细的记录,这就有可能导致用户信息被泄露。如果信息安全管理体制不完善,那么网站很有可能被一些黑客非法入侵,那么用户信息就会被窃取,人们的财产安全得不到保障,也会从一定程度上影响到国内经济的发展。因此,设立一个科学合理的大数据信息安全管理体制是非常必要的。但当前此方面仍然有许多需要完善的地方,信息安全管理体制达不到标准化的要求,相关的安全法律法规也有待优化和完善。

2.2 黑客入侵

相关人员在对计算机网络安全故障进行排查的过程中,发现黑客入侵是一个主要原因。黑客入侵主要分为 2 种。第一,黑客进行主动性攻击。就是黑客在对数据信息进行破坏的过程中,是有一定针对性的,导致大量的数据信息丢失,带来巨大的损失。第二,黑客进行被动性攻击。在入侵的过程中,对一些数据信息进行一定程度的破解,或者是截获数据信息,但是计算机网络仍然可以进行正常的运转,此过程具有被动性。不论是哪一种形式的黑客

入侵,都会对数据信息带来较大的影响,导致数据信息丢失,为计算机网络的后续运行带来较大的影响,埋下隐患。在严重的情况下,可能会导致计算机网络出现瘫痪。

2.3 垃圾信息和信息窃取

在日常的生活中,经常会收到一些垃圾信息。垃圾信息的传播方式非常多,包括邮件传播、软件传播等等。垃圾信息的广泛传播,会对大量的数据信息进行扩散。信息被窃取,主要是由于计算机网络被一些非法软件入侵,但是这些非法软件和计算机病毒存在一定的差异性,非法软件不会对计算机系统造成一定的影响,但是会对其中的数据信息进行一定程度的窃取,严重影响到了用户信息的安全性,也会给计算机安全带来一定的危害。垃圾信息和信息窃取,也是急需解决的计算机网络信息安全问题。

2.4 病毒、木马入侵

对计算机病毒进行充分观察之后,会发现计算机病毒都会有很长一段潜伏过程。计算机只要连接上网络,就给病毒提供了一定的入侵机会。当计算机被病毒入侵之后,会带来巨大的危害。当前,计算机病毒的种类十分繁多,为了从一定程度上提高计算机的防御能力,必须要对计算机病毒进行查杀。一般来说,可以在计算机上安装一些病毒查杀软件,从而对计算机病毒入侵问题进行解决。对于木马入侵问题,木马的本质,就是一种人为制作的计算机病毒,会给计算机带来巨大的危害。

2.5 系统漏洞

计算机在不断发展的过程中,会对用户习惯和实际需求进行充分的研究和调查,并以此为基础,对计算机进行不断的升级,切实满足广大用户的需要。但是系统在不断升级和修补的过程中,同样会有系统漏洞的存在,计算机网络在使用的过程中,有可能会受到攻击,从而导致相关的数据信息缺失。同时,计算机面对的是不同的群体,用户之间的使用习惯由于各方面的原因存在一定的差异,因而从一定程度上提高了系统发生漏洞的几率,导致计算机的安全受到威胁,安全等级减小,并且对网络安全防护技术的研发造成了一定的阻碍。

3 网络信息安全问题的思考与对策

3.1 完善信息安全管理体制

在大数据时代,信息安全是必须要重视的一个问题。尤其是经过“斯诺登”事件,应该把信息安全上升到国家层面,引起高度重视。但是国内在此方

面仍然有所不足,面对信息安全管理体制不完善的问题,必须要采取积极措施对这一问题加以改善。可以借鉴国外的一些经验,改善信息安全制度不完善的局面,同时也可以优化中国的安全法律法规。其次,相关工作人员在对大数据信息进行安全管理的过程中,敏感数据保护是至关重要的一个部分。除此之外,大数据运行环境涵盖诸多方面的内容,包括网络环境、主机的运行状态、实际的计算资源等等,必须要具有充足的安全防护手段,才可以对大数据应用进行比较有效的安全管理。在进行安全防护的过程中,必须要重视两大核心。一方面是数据信息的隐私保护,另一方面是对计算机环境的安全防护。不断优化和完善大数据的信息安全管理体制,可以为数据安全防护提供坚实的基础。

3.2 完善黑客防范机制,提高防范意识

在对防范机制进行设计时,必须要设立科学合理的黑客防范机制,并以大数据时代下数据的各方面特点为基础,对黑客防范机制进行不断的优化,还可以设立一个数据资源应用模型,不断优化和完善黑客攻击技术应用程序。以黑客攻击防范的相关要求为依据,对一些黑客攻击软件进行充分的研究和分析,确定研发要素,并将具体的信息进行准确的登记,为计算机网络信息安全防护提供依据。其次,还应该提高黑客攻击防范意识。在黑客进行窃取行为时,进行快速的识别,并且利用一些安全防护措施,例如防火墙技术等等,从一定程度上减小计算机网络被攻击的概率。除此之外,要不断提高数据认证技术的使用力度,对计算机网络的数据访问次数进行一定程度的控制,提高信息流通渠道的安全性,有效防止黑客入侵,对计算机网络安全运行进行有效的保护。

3.3 提高数据保存和流通保护力度

在计算机网络中,数据信息经常需要保存和流通,为了防止信息被窃取,必须要提高数据保存和流通过程中的保护力度。对于数据保存,可以运用一些先进的数据保存方式,例如文件加密技术,对一些重要的文件进行加密保护。不仅可以达到数据保密性的要求,还可以从很大程度上避免数据被窃取、破坏。对于数据流通来说,可以采用数据签名技术。在数据进行流通传递的过程中,可以提供一定的加密服务,从很大程度上提升安全性。数据签名技术主要包括2种方式。第一,线路加密。在线路进行传输的过程中,运用多种多样的加密密钥,对需要进行保护的数据信息进行保护。第二,端对端加密。

此种数据签名技术在应用的过程中,会用到一些加密软件。通过加密软件,把需要进行发送的文件进行实时加密。文件当中所包含的数据信息是一些明文,要对其进行一定的转换,变换成密文之后,才可进行传输。当接收者收到文件之后,再通过密钥,对加密文件当中的密文进行充分的解读,获取相应的明文。

3.4 完善“双防”技术

“双防”技术,一般来说主要包括防病毒技术以及防火墙技术。对防病毒技术进行研究的过程中,主要是对杀毒软件进行研究,也可以在服务器和用户之间编辑一个科学合理的程序代码,可以对病毒入侵进行一定的避免,或者是对病毒进行删除。不断提高杀毒软件的有效性,可以大幅度改善网络安全问题。其次,防火墙技术经过多年的发展,已经变得比较成熟。对于防火墙技术来说,就是在用户和服务器之间,设立一道屏障,保障用户在使用计算机网络的过程中数据信息的安全性。防火墙技术在不断进行完善,可以进行监察、通知等各项功能,并且也能够为用户提供一定的建议,用户在遇到非法数据时,防火墙技术可以帮助用户对这些数据进行拒绝。“双防”技术的应用,从很大程度上提高了网络操作的安全性。

3.5 及时安装漏洞补丁程序,完善漏洞扫描技术

在计算机软件硬件设计过程中,如果设计不当,那么就会形成计算机漏洞,也是计算机受到攻击的一个弱点。通过对计算机漏洞进行充分的调查和研究之后发现,任何一台计算机,都会存在或多或少的漏洞,一些网络黑客,正是利用计算机系统存在的漏洞,对其进行攻击,进而带来损失。因此,必须要对

计算机漏洞进行深刻研究,研发出对应的漏洞修复补丁程序,广大用户必须要对这些漏洞补丁程序进行及时安装,保障计算机网络的安全性。其次,还应该采取科学合理的方法和措施不断优化和完善计算机网络漏洞扫描技术。该技术主要是对计算机网络进行充分排查,对其弱点和盲点进行一定的查询,并且还可以对一些入侵行为的相关信息采集,为后续安全防护工作奠定坚实基础。漏洞扫描技术的应用,可以从一定程度上提高网络安全技术的实效性,降低入侵行为导致的损失。

4 结束语

在计算机网络中,存在着大量的数据信息。这些数据信息和用户的利益密切相关。如果想从一定程度上提高信息的安全可靠性,就必须完善信息安全管理体系,提高黑客攻击防范意识,并且要及时安装漏洞补丁程序,防止数据信息丢失,保证计算机网络的安全性。

参考文献

- [1] 薛佳桦. 试论基于大数据环境下的计算机信息安全技术[J]. 电子制作, 2018(12): 53-55, 46.
- [2] 高午. 大数据背景下计算机网络信息安全风险及防护措施分析[J]. 电脑知识与技术, 2018, 14(7): 29-30, 36.
- [3] 刘志杰. 浅谈大数据时代下计算机网络信息安全现状及对策[J]. 电脑知识与技术, 2017, 13(21): 10-11.
- [4] 兰天静. 基于“大数据”分析计算机网络信息安全[J]. 电脑迷, 2017(3): 14-15.
- [5] 吴恩生, 王桂梅. 大数据时代计算机信息处理技术分析[J]. 江苏科技信息, 2015(12): 63-65.
- [6] 王磊. 关于计算机网络信息安全及防护策略探究[J]. 电脑知识与技术, 2014, 10(19): 4414-4416.

(上接第 253 页)

言 C# 作为编程语言, 设计了简洁易操作的发送电子邮件功能界面, 并详细说明了关键代码的运用。在程序调试过程中, 出现了错误“不允许使用邮箱名称。服务器响应为: authentication is required.”, 可以通过改变验证方式, 将提供的验证指定为用户名和密码方式, 即可排除此错误。最终测试, 本文设计的电子邮件系统能够正常地发送邮件, 且操作方便。

参考文献

- [1] 孙践知, 张迎新, 肖媛媛. C# 程序设计[M]. 北京: 清华大学出版

社, 2010.

- [2] 陈广. C# 程序设计基础教程与实训[M]. 2 版. 北京: 北京大学出版社, 2013.
- [3] 刘宴兵, 李春. 使用 SMTP 实现邮件发送设计[J]. 计算机工程与应用, 2002, 38(8): 142-144.
- [4] 孙琴琴, 钟琪. 基于 Java 的电子邮件系统的简单设计与实现[J]. 无线互联科技, 2018(17): 53-54.
- [5] 谢秋理. 电子邮件系统的设计与实现[J]. 信息与电脑, 2015(14): 58-59.
- [6] 陈国顺, 付卫华. .Net Framework 类库概述[J]. 现代情报, 2003(12): 58-59.