第 2 卷◆第 6 期◆版本 1.0◆2019 年 6 月
文章类型：论文|刊号（ISSN）：2630-4686

基于大数据时代下的计算机网络安全探究

王健豫
黑龙江省政务大数据中心
DOI:10.32629/er.v2i6.1867

[摘　要] 时代的进步、科技的发展使得我们的生产力获得了极大的解放,但与此同时也带来了一定的安全隐患,尤其是在大数据时代之下的计算机网络安全问题,更是需要我们每一个人都去关注的重要问题。本文重点探讨了目前所存在的计算机网络安全问题,并且提出了相应的防范措施,建议聘请专业团队及时检查、普及安全常识更换密码、下载购买网络防火墙软件、发现安全漏洞及时修复、政府出台网络安全法律。
[关键词] 计算机；安全；病毒；网络

信息时代已经悄然来临,甚至影响着我们身边的每一个人,对于信息时代的来临,我们最直观的感受就是计算机和互联网的普及,现如今,计算机网络安全问题已经危及了我们的每一个人,不仅使我们面对着更加不安全的网络环境,同时也会对我们自身的信息造成一定的线路。无论是现如今的网络病毒还是系统漏洞,都是计算机网络安全的一个表现,但同时也是大数据时代之下,我们所不可避免的一项问题。因此,现阶段为必须积极去探索如何利用科学手段来规避计算机网络安全问题,使得网络空间变得更加可靠,有保障。

1 大数据时代下的计算机网络安全问题分析

网络的普及使得我们的工作效率越来越高,也方便了我们的日常生活需求,但是在大数据的时代背景之下,我们也不能够忽视计算机网络安全问题,尤其是可能会对我们自身信息造成泄漏,甚至是对系统造成致命危机的问题。

一般来说,我们所常见的计算机网络安全问题就是木马病毒,对于不法分子来说,网络病毒的传播更加简单,追责也比较复杂。同时病毒就具有可复制的特点,当一个病毒已经进入到我们的计算机系统以后,那么就会以快速的繁殖速度进行再次复制及快速的占据我们整个系统,并且导致计算机网络的瘫痪,如果该计算机是以局域网的形式连接至多个电脑的话,那么甚至会导致本区内的大部分电脑均瘫痪。

另外,还有一种比较常见的网络安全威胁就是人为的黑客攻击,由于一些不法分子掌握了先进的计算机技术,可能会迫于利益诱惑,对于大型公司或集团的数据进行供给,造成集团内所有网络系统的瘫痪,并窃取相关的数据,这不仅会危及公司的运营和发展,同时也会造成公司内部员工信息,客户信息和项目信息的大规模泄露。

2 计算机网络安全防范措施

2.1 聘请专业团队及时检查

对于大型的企业和集团来说,他们才是最容易受到计算机网络病毒攻击的群体,同时,这部分企业一旦受到了计算机网络安全方面的威胁,那么不仅会造成信息泄露,还有可能蒙受经济损失。严重的会走向破产之路,因此我们说,对于大型的公司,企业和集团来说,应当及时的聘请专业的计算机网络安全防护团队,做到实时检查、维护。首先,企业方面应当加强对这方面人才的招聘力度,在对外展开招聘的时候,不能够仅仅招聘管理人才,更需要围绕计算机网络安全防护职位来提出相应的招聘要求,需要保证聘用的人才具有专业的学历和资质证书,同时也需要具备相应的工作经验。另外再组建完成一只专业的团队以后,也需要对团队的工作做出相应的要求——不仅需要做到定时定期的进行本公司内局域网的安全防护检查,还需要围绕公司实际的需求和网络特征来搭建一个更加安全的网络平台,为公司内部的局域网络安全设置密钥。针对一些规模较小、人力资源成本预算较少的公司,同样可以采取第三方外包的方式,由三方的专业计算机网络安全团队来为本公司的网络状况进行定期的检查。

2.2 普及安全常识更换密码

目前虽然计算机网络安全问题频发,但是究其原因,也不总是因为黑客攻击和病毒入侵,更重要的还是因为计算机网络的使用者自身缺乏安全的常识,并没有对病毒、木马以及黑客攻击有一个正确的认知。举例来说,有部分使用者在使用计算机网络的时候经常会浏览一些涉及淫秽暴力方面内容的网页,而这些网页当中经常有非常有可能含有一些隐性的病毒,对计算机进行攻击,甚至潜伏在计算机系统当中,一旦输入一些支付密码时就会对其中的资金进行窃取。因此,主流媒体应当积极地发挥社会职责,尽可能地在公众场所宣讲一些计算机网络安全的常识。包括,但不局限于鼓励人们经常性的更换登录密码和帐号信息,并且宣传一些常见的网络病毒方式,如电子邮件传播病毒、QQ群微信群图片下载传播病毒等等。当然,在这方面,目前国内知名的浏览系统都已经能够做到防患于未然,比如针对一些不安全的界面,百度和搜狐系统都已经能够在页面当中做出相应的提示,当使用者点开这一界面的时候,首先会出现浏览器自带的提示信息。这对于使用者来说是一次警示,与此同时,无论是QQ还是支付宝,目前都推出了密码的要求及要求,登录密码——即不能够少于多少字符,不能够带有重复性的字符等等。

2.3 下载购买网络防火墙软件

想要真正的从根源上防范计算机网络安全问题,那么,

首先需要对计算机设备设置一个强有力的网络防火墙,在这方面鼓励大家下载一些知名的防火墙软件,例如腾讯、百度、360等企业均研发了技术过关的查毒软件。

实际上,目前常见的一些病毒都可以通过防火墙进行防范,减少对计算机使用者的威胁。但是我们需要注意的是,下载防火墙软件来防范计算机网络安全问题的发生,并不是亡羊补牢之举,而是需要防患于未然,不能够在发生和发现病毒现象以后再进行下载,而是需要在登录网络之前或者说在购买计算机设备支出,就首先将这些防火墙和杀毒软件下载好。举例来说,目前知名的360安全卫士软件就可以对计算机当中所存在的木马病毒进行查杀,并可以在关机之时自动的进行漏洞的修复,这样一来就可以保证使用者的网络信息安全。

2.4 发现安全漏洞及时修复

针对企业和公司来说,他们需要在局域网内连接各个计算机设备,并形成总的网络系统,因此风险系数更大,这是因为在该系统之内的任何一台计算机设备遭受病毒攻击以后,都会对整个系统产生负面影响,因此需要建立相应的风险预警机制。笔者建议在机制当中,首先应当确立各个计算机设备的具体职能,一旦发生跨职能请求的时候,就需要进行预警,将这个警示信息及时的上传至计算机网络安全的专业维护团队以及公司领导人的设备当中。举例来说,如果本应是销售部门使用的计算机网络设备,突然发出了进入财务部门系统的请求时。那么,计算机网络管理者和财务部门、销售部门以及企业主要领导人的电子邮箱当中都会及时的收到一份预警邮件。同时,为了避免邮件查看的不及时情况发生,还会有电话的形式及时的通知网络专管员。

另外,计算机网络安全的维护团队,不仅需要对计算机网络设备进行及时的检查,已做到未雨绸缪,同时在面对一些已经检查出的安全漏洞和可能存在的安全隐患时,要保证具有宁错不放的原则,对这些隐患进行逐一的排查,并及时的修复漏洞。在这方面,笔者建议可以综合使用防火墙技术,不仅要设置专门的定期检查系统,还要形成一道安全防护墙,使得计算机网络设备在受到外界病毒的攻击时,能够具有一定的防护能力,减少漏洞出现的可能。

2.5 政府出台网络安全法律

这网络出现之日起,网络安全问题就是我们日益关注的一个重要问题,无论是哪行哪业,还是任何一个国家,都必然面临着网络安全所带来的威胁,尤其是对于国家机密信息来说。一旦这些信息造成泄漏,那么很有可能对国家安全造成巨大的威胁。这方面,我国政府则需要积极地发挥作用和职能,出台与网络安全相关的法律法规。

一方面需要对现有法规做出完善,目前我国政府已经出台了《中华人民共和国网络安全法》,通过法律制度为计算机网络发展与运行提高安全保证,规范网络行为。在法律条文当中,更需要明确相关责任部门的具体权责,赋予网络警察更多的权利,从而使得网络安全的案件尽可能的减少,促使行业的健康发展。

另一方面,有关网络管理有关部门,要根据当前计算网络运行状况,制定动态的、科学的安全管理制度对网络实现更合理的约束。与此同时,有关机构还要对计算机网络运行中出现的安全问题和可能出现的问题进行充分考虑,并且采取有效的措施,及时解决,为用户提供一个安全的网络环境。

3 结束语

总而言之,我们在积极地利用计算机网络从事日常的生产,生活工作之外,还需要辩证地去看待这一项科技的进步,需要意识到其中可能带来的安全隐患和威胁。与此同时,作为计算机网络的受益者和使用者的我们,更需要强调自身信息安全的保护,要树立起这方面的意识,不能够给犯罪分子以可乘之机,也需要积极地去维护计算机网络安全。唯有如此,才能够真正的使得计算机网络世界变得更加安全可靠,才能够使得我们每一名计算机网络的使用者都能够在其中受益,而不是过多的担心自我信息的泄露。

[参考文献]

[1]何元飞,李俐.大数据时代下的计算机网络安全[J].电子技术与软件工程,2019(11):202.

[2]赵丽华.大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用,2019(06):49-50.

[3]刘雷,董超.大数据时代背景下计算机网络安全防范应用与运行[J].网络安全技术与应用,2019(06):51-53.