

关于信息网络安全监测预警机制的研究

景妍华 罗菁菁

国网宁夏电力有限公司中卫供电公司 宁夏 中卫 755000

【摘要】随着经济的飞速发展，科学技术也在不断进步。现如今，我国已经全面进入信息化时代。在一定程度上改变了社会群众的生活、生产方式。然而，信息网络在为人们提供便利的同时，其中存在的安全问题也日益突出。为了营造安全、可靠的网络环境，需要进一步优化和完善信息网络安全预警机制。因此，本文结合信息网络安全监测预警机制的重点监测对象进行分析，深入研究信息网络安全预警机制的核心内容。希望能够为专业人士提供参考借鉴，为提高网络安全奠定良好基础。

【关键词】信息网络；安全；监测预警；网络病毒

引言

在科学技术不断推动下，网络环境建设越来越复杂，其中存在的安全问题日益突出，各类信息网络安全事件频繁发生，受到社会各界的广泛关注。为了维护网络安全，营造健康的网络环境，现阶段，研究一种完善的信息网络安全监测预警机制尤为重要。而想要实现这一目标，需要集中社会多方资源和力量，提高网络监测水平，通过实施监督信息网络动态，及时发现网络环境中存在的隐患问题^[1]，从而针对性采取措施解决。

1 信息网络安全监测预警机制的重点监测对象

现阶段，我国已经全面进入信息化时代，信息网络建设规模逐渐扩大，为社会群众生活、生产奠定良好基础。然而，随着网络环境的日益复杂，其中存在的安全隐患也逐渐突出，完善和健全信息网络安全监测预警机制，已经成为促进网络持续发展的当务之急。而信息网络监测的重要内容可以从以下几个方面分析：

1.1 网络漏洞

网络漏洞通常有两种形式，一种为设备漏洞，另一种为信息系统漏洞。近年来，我国网络建设水平不断提升，信息安全漏洞也随之增多，严重降低了信息资源的安全性，增加了网络安全事件的发生几率，无法充分满足人们的生活、生产需求。因此，在构建信息网络安全监测预警机制时，需要充分考虑和分析网络中存在的安全漏洞，并针对性采取措施修复和处理。

1.2 网络病毒

网络病毒是网络环境中常见的安全隐患，一旦计算机受病毒侵害，不仅会降低系统运行效率，还会使信息数据可靠性降低。甚至会导致重要文件丢失引发网络崩溃。例如：档案型病毒、开机磁区病毒等不仅严重威胁网络秩序，还会对人民利益、国家安全造成一定威胁^[2]。在信息网络安全监测预警机制完善过程中，需要重点针对网络病毒展开研究。

1.3 网络攻击

网络攻击有公开性攻击和隐蔽性攻击两种形式，前者具体体现在信息盗取、网页篡改等方面。后者主要是在网络系统中植入后门或在广告中进行挂马。近年来，信息网络受黑客攻击、恶意破坏等安全事件频繁发生，并且手段

千奇百样，为网络环境带来了巨大安全隐患。

1.4 网络恶意程序

近年来，互联网技术广泛普及，手机、IPad等电子设备应运而生，在为人们提供便利的同时，也增加了信息网络安全事件发生概率。以智能手机为例进行分析，垃圾信息、诱导付费等诸多恶意程序大量产生，为人们的信息安全和财产安全带来巨大威胁。

1.5 钓鱼网站

所谓“钓鱼”，是指意图引诱他人达到某一目标的一种行为。在网络环境中，不法分子通过构建不法电子商务网站，伪装成银行引导用户提供银行账号或密码，给人们的信息、财产安全带来巨大隐患。针对钓鱼网站，可以通过查杀软件有效解决。

2 信息网络监测预警机制构成平台

构建信息网络监测预警机制，需要由多个平台共同协作、相互配合才能完成。其构成平台可以从以下几个方面分析：第一，通报合作平台。为保证网络信息安全监测工作能够扩大覆盖范围。需要结合信息网络中存在的安全问题落实通报合作工作。如此，在通报合作平台监督下，如果发现网络环境中存在隐患问题，会及时上报给公安部门，有效提高监测力度。第二，报送平台。运营单位需要将每天网络系统运行的实际情况真实上报，实时了解网络系统运行状态。该平台不仅能够提高运营单位的信息网络安全监测水平，还能够为营造良好的网络环境奠定良好基础^[3]。第三，报警服务平台。公安部门在分析网络安全事件过程中，不仅要处理好安全问题，还要结合安全事件具体情况掌握问题解决方法，保证在处理各类网络安全问题时能够从容应对。第四，登记保护平台。公安部门在处理登记保护工作时，如果发现其中存在安全隐患，需要渗入分析，提炼其中的信息数据，并做好检查、监督、管理、侦破等一系列工作。

3 信息网络安全预警机制的核心内容

3.1 以社会热点为核心

近年来，计算机技术广泛普及，为信息传播奠定了良好基础，促进信息传播范围更加广泛，传播形式更加多元，为人们获取信息提供了便捷性。与此同时，网络环境的日

益复杂,也使得信息资源大量增加,各种信息资源鱼龙混杂,信息内容真假难辨。例如:某一时间内突然发生一件社会问题,会在瞬间被各种媒体报道和转载。另外,信息时代下,社会群众也不再是单一的信息接受者,也是信息传播者,而在信息传播过程中,越来越多的媒体言论和群众群众主观意愿添加在信息内容中,导致原本的网络信息在传播中被肆意曲解。除此之外,部分媒体在信息报道中没有调查事件真相,导致舆论导向发生偏移,严重甚至会遭到网民恶性攻击。因此,在信息网络安全预警机制构建过程中,需要时刻关注社会热点,全方位监测人民意愿集散地,坚持以引导群众向正确舆论导向发展。

3.2 充分应用新兴技术

在科学技术不断进步下,大数据技术、物联网技术等新兴技术应运而生。为构建信息网络安全监测预警机制奠定了良好基础。例如:云计算技术能够集中大量信息数据,并且可以实现实时共享的目标。是不法分子恶意攻击的重要目标之一,一旦受到攻击,网络系统会产生巨大安全隐患,并且在一定程度上为问题处理增加了难度和挑战^[4]。而物联网技术就有个性化、私有化特征,不仅能够覆盖网络资源,还能够兼容各种应用,如果收到不法分子恶意破坏,将会降低网络安全性。由此可见,强化网络系统监督管理力度,是维护网络环境安全的必要手段。

【参考文献】

- [1] 赵文文,刘鹏.信息网络安全监测预警机制分析与研究[J].信息通信,2018,190(10):155-156.
- [2] 王星宇.智能化计算机安全监控信息网络技术研究[J].电脑迷,2018,97(06):77.
- [3] 宋升松.智能化计算机安全监控信息网络技术研究[J].数码世界,2018(08):199-200.
- [4] 周振林.关于计算机网络信息安全的研究[J].中国战略新兴产业,2018,164(32):94-95.

3.3 重视监督节假日信息

当前,每逢节假日,各种媒体会相继报道“预防**病毒”、“**病毒受害事件”等内容,而这些病毒,也统称为节日病毒。具体来说,节假日网络浏览量大幅度增加,各种挂马网页、病毒侵入等现象频繁发生。尤其针对国庆、新年等时间较长的假期,外地务工的群众通常会通过网络购票方式返乡或旅游。而与此同时,该时间段信息网络安全监管力度也会相应降低,为不法分子提供了可乘之机,其通过钓鱼网站或购票软件,窃取他人信息或财产,为广大群众的信息安全和财产安全带来极大威胁。因此,针对节假日病毒,相关部门应提高监管力度,强化安全防范工作,并加大宣传力度,通过公告、平台等方式为社会群众传递安全提示,全面提高社会群众防范意识。

4 结束语

综上所述,现如今,互联网技术发展迅速,科技水平不断提升,网络环境日益复杂,在信息传播速度快、传播范围广的新时代环境下,如何保证信息网络安全,成为社会群众广泛关注的问题之一。因此,构建信息网络监测预警机制尤为重要,只有保证全方位监督、全过程监测,才能够提高网络系统安全水平,从而维护群众和国家的利益。