

计算机信息管理技术在网络安全中的应用探究

唐艳华

(哈尔滨医科大学附属第二医院, 黑龙江 哈尔滨 150086)

摘要: 在科学技术支持下, 21世纪被人们称为知识经济世纪, 互联网、大数据的出现很大程度上推动了经济发展。结合实际进行分析, 我国在发展中对计算机信息管理技术有较大需求和要求, 这意味着传统的计算机信息管理手段已难以满足网络社会发展需求, 其主要因素在于以往的信息管理技术有较大问题, 其不稳定性对网络技术发展产生不良影响。从这一角度进行分析, 为了确保社会各个行业顺利发展, 需要深入研究计算机信息管理技术, 应用有效的计算机信息管理技术, 确保我国的网络系统安全。

关键词: 计算机信息管理技术; 网络安全; 应用; 研究

一、网络信息安全的重要内涵与内容

随着科学技术的不断发展, 为进一步满足生产以及生活需求, 网络信息安全成为重要保护屏障, 同时其也是计算机信息管理中的关键组成部分, 需要相关单位在发展中用敏锐眼光看待网络信息安全问题。实际上, 网络信息管理涵盖了一些较为基础的运行信息, 例如 IP 地址、域名等, 这些内容能够支持用户信息区别以及认识服务, 同时其在运行过程中也能够确保网络安全, 避免不良信息入侵到网络中, 且能够结合用户需求, 为其提供大量信息、资源等, 切实发挥其引导价值。不仅如此, 多数情况下网络信息安全具备生命周期性, 例如其中涵盖了需求分析、风险把控、安全目标、对策等, 从而能够构成一个相对完整的生命周期。而在现实中网络安全问题愈加突出, 一些网络黑客技术水平也在不断提高, 相应地为了确保网络安全, 有关单位在发展中需要将安全体系、策略等适当调控, 确保整个网络信息安全系统都随时处于一个动态过程中, 不断进步、不断完善、不断更新。

二、计算机信息管理技术问题

(一) 访问控制安全难以保障

结合实际进行分析, 目前多数病毒传播的载体为网络、移动硬盘等, 借助这些媒介计算机病毒可侵入并控制电脑账户。从这一角度进行分析, 若科技水平相对较高, 且其能够有效控制外界信息对本地信息的访问与控制, 即可有效预防网络病毒入侵。在国内, 很多地区信息管理整体水平已初具检测能力, 其可以确保网络中站点安全性和稳定性, 不过很多部门难以实现屏蔽一切风险网点的目标, 具体来讲, 一些工作人员在实际工作过程中仅能使用提示的方法让使用者了解网点有问题和风险, 一些用户在使用过程中忽视了系统提示, 在使用过程中出现病毒入侵的情况, 这在很大程度上影响了网络信息安全, 甚至出现信息泄露情况; 一些用户在使用网络的过程中, 因自身防范意识较差, 时常出现外来访问与入侵的情况。为了避免出现类似情况, 相关单位技术人员则需具备一定方位权限有效把控风险, 不过反观不良信息也可借助这些访问权限威胁网络安全。

(二) 技术人员监管能力有限

相对来讲, 目前在网络安全领域影响相对严重的情况在于黑客、病毒的恶意入侵。随着科学技术、互联网技术飞速发展, 生活以及生产中出现的网络病毒类型、数量等不断增多, 且一些黑客技术能力也在不断创新, 为了在最大程度上避免出现安全类问题, 则需要相关部门适当加大网络监管和监督路阻, 并能够结合实际需求做好网络异常情况处理, 针对不同问题制定有效解决方案。不过在实际运行过程中, 其会受到不同因素影响以及限制, 总体来看目前国内现有的监测水平有限, 相关监测能力并未达标,

同时很多单位的网络监管以及监测能力相对较差, 并未从多方面入手开展网络管理监管等。这些因素的共同制约使得技术部门、企业等单位难以及时发现网络安全中存在的问题和隐患, 以至于出现病毒入侵时得不到及时处理, 这在很大程度上影响了企业、个人发展, 产生不同程度的损失。

(三) 整体应变能力较差

时下, 互联网技术、信息化平台等成为生活以及生产的有力推手, 而为了进一步提升经济效益, 互联网也在不断发展以及更新, 且为了最大化其利用价值, 网络信息的管理技术有必要与时俱进一同变化。不过结合部分企业和单位实际情况进行分析, 一些单位在发展中并未有效迎合互联网技术变化, 同时也并未发展相应技术, 使管理能力与实际需求不足。同时, 近年来国内即便有投入大量资源研发信息管理加密技术, 但起步晚、经验少, 所以遇到了很多坎坷与挫折, 并没有能够为保障网络安全提供支持。

(四) 加密能力与实际不符

目前多数单位为了确保网络信息安全, 都会在计算机中设置加密技术, 从网络安全维护角度进行分析, 加密技术最为直接且有效, 在使用过程中主要是技术人员借助加密函数、密钥等, 将信息变为没有意义、难以理解的文字, 而接受者则需要解密文件之后将其变为能够理解且可以使用的明文。在这一技术的支持下, 信息安全得以保障, 这也有效防止了黑客、病毒的入侵, 目前科学技术愈加发达, 相当多的案例也充分印证了现存的传统加密方式已经难以确保数据安全, 不过一些单位在发展中并未意识到这一点, 使得网络安全出现不同程度的问题。

三、在网络安全中应用计算机网络管理技术的重要性

首先, 目前网络信息系统时常会出现不良信息入侵、黑客攻击的情况, 这些问题在很大程度上对群众的生产以及生活产生大量不良影响。为了改善这一现状, 做到更好地应对安全问题, 更多的企业、单位等开始在计算机信息系统安全管理过程中使用管理技术, 其在运行过程中可以将计算机技术、网络实践紧密结合, 借助全新技术手段, 通过落实科学数据分析的方式进一步提升网络安全性能, 确保计算机网络信息系统的健康发展。其次, 当下计算机网络安全技术水平能够切实反映互联网技术发展整体现状, 计算机网络管理技术是一种在计算机网络系统进行更新后, 将网络信息安全也实施同步更新的安全管理技术。在这一全新技术支持下, 其可进一步解决网络系统中存在的安全隐患, 切实提升整体管理效果。

四、计算机信息管理技术在网络安全中的应用方法

(一) 提升安全防范意识

经过多年发展, 计算机网络可为社会提供全新的信息交流平

台,而为了充分发挥计算机信息管理技术的应用价值,相关单位、企业在发展中需树立网络安全控制理念。人员在使用计算网络平台时,应意识到网络资源、信息化平台的双面性,这样可以进一步建立客户自身的网络信息资源管理安全保障体系,为了进一步实现这一目标,主要的方式为用户进行网络存储的登录密码,实现网络资源管理的系统性、科学性发展;除此之外,企业和单位在发展过程中,需结合实际更新网络安全管理平台中的安全管理系统,这样能够进一步开展网络安全管理技术研究工作,例如借助计算机加密程序进行设定,从而将计算机网络平台密码结构升级为高级密码,借助这一方式优化计算机网络平台在计算机安全处理中的作用,切实提高网络资源应用的安全性。

(二) 建立并逐步完善安全管理制度

为了改善当前网络安全管理现状,企业在发展中需结合内部实际情况,制定并通过实践完善安全管理制度,通过这样的方式确保计算机信息管理技术能够获得长足发展动力。首先,人员管理体系。在平时工作以及发展过程中,企业应积极完善人才管理制度、体系,为了提升管理效果重视人才引进,让综合能力优秀、具备创新意识人才就职相关岗位;落实人员培训制度,侧重人员后期培训以及管理,提升其整体能力以及素养;应根据具体情况建立网络管理体系,成立专门小组,定期检查网络硬件、网络软件,更新软硬件,保障安全性,让计算机的信息管理拥有良好环境和条件。其次,企业需将管理制度落实在具体的系统实现中,实现管理自动化,借助这样的方式可进一步提升管理效果,并适当降低工作人员难度。

(三) 进一步落实系统操作安全管理

从计算机信息管理角度进行分析,操作系统为关键组成部分。受限于不同因素影响,目前很多群众电脑中都存在一些系统漏洞,这在很大程度上影响着计算机整体安全性。为了切实改善这一情况,企业在发展中需结合实际,建立并落实必要的安全防范体系、系统,这样能够确保网络安全性以及可靠性。例如,单位在发展中可设立安防系统,其能够在工作有效筛选网络信息,并在第一时间发现相关问题、系统漏洞时,借助与之对应的方法修复问题,在最大程度上避免出现病毒入侵的情况;建立必要的人侵监测系统,做到分析安全隐患,切实提升网络信息安全管理效果。

(四) 完善计算机安全保护系统

首先,完善内部系统。为了实现这一目标,则需要借助计算机中的大数据系统,建立并完善内部运行程序,并适当优化不同领域中数据系统之间所建立的网络数据资源管理库,如计算机网络和程序中应用计算机大数据的信息数据建立虚拟信息链,信息链在计算机网络数据资源运行中,逐步建立新的数据资源保护链,借助这样的方式可以确保网络资源应用、管理系统的完整性,从而对资源信息等有效管理。其次,外部保护系统。例如,提高计算机网络运行中网页的控制,网页系统记录的定期自动处理,避免用户使用的数据资源丢失,实现计算机安全管理的保护系统的完善,确保网络安全保护系统的保护作用性增强。

(五) 搭建智能化的线上应对措施

此种方式主要是将算法基础、机器学习等应对措施整合成全新合力,并借助大数据系统对数据资源进行分析,以此来确保信息资源查找的实效性,随后借助线上应对方式,构建全新的设计流程图。在此之后,通过安全云后台、日志上传服务分析,进一步明确数据资源的结构。不仅如此,这一全新系统将数据信息进行整合,结合这些内容积极构建紧急措施,寻找最为有效的解决

方案,从而实现在线处理的目标,进一步提升信息处理效率。

(六) 运用大数据技术积极搭建安全性的云服务平台

这一目标实现,可从以下几点入手。企业、单位在发展中,技术人员在打造良好网络安全环境这一过程中,需结合实际视网络安全局域网安全问题,并在发展过程中积极搭建安全云服务平台,通过引入信息化手段实现对网络安全系统的全方位监测。如果在网络问题分析中存在异常,则需及时采取措施,并及时制定全新方案。之后,则可实现对网络信息安全的监控以及有效处理,之后将相应的网络信息进行整合,以此来体现网络安全分析的使用价值。综合来讲,在搭建平台的过程中,可围绕网络使用整体性能,进行监测感知系统和决策系统的明确,这样能够进一步提升整体工作效率;云平台的运行,时刻进行安全事故的相关数据记录,若后续出现问题时则会对安全事故进行有效处理,这样进一步提升了管理效果,适当减轻工作人员压力。

(七) 有效把控安全风险

基于互联网时代,企业、单位为了确保网络信息安全,并提升安全信息分析工作实效,则需要建立一个相对科学、统一的安全防范系统,做到有效把控安全类风险,切实改善网络安全管理现状。结合实际情况来看,为了提升经济效益,目前很多企业、单位等在发展过程中积极利用安全监测系统来提升自身的安全防范指数,其主要原因在于安全监测系统有良好的使用性能,其在公共网络体系以及连接中得到了有效普及以及推广。在实际应用过程中,此项技术的主要工作原理在于将大量的处理信息分为内外两个管理系统,其中内部管理系统的安全要求较高,其重要部分的数据都可以被纳入内部管理系统中。同样的,若立足全新层次进行分析,防范系统的不断完善以及升级,也会不可避免地造成网络病毒、黑客水平升级,使得网络安全存在大量隐患。为进一步提升安全检查有效性,安全人员需要不断尝试以及实践,这意味着网络病毒查杀是长期任务。基于此,相关的技术人员应立足实际,不断学习相关领域的知识以及有效方法,通过这一方式方可及时应对病毒排查工作。而为了既定目标的实现,相关部门在发展过程中也要针对自身情况进行探索,围绕计算机信息安全选择、设立与之匹配的安全防范系统,切实确保信息安全。

五、结语

在当前时代背景下,网络技术最为直接的特征在于其交互性、便捷性的特征。随着科学技术的不断发展,网络技术逐渐覆盖到社会各个领域,为群众生活、生产带来极大便利,不过不能忽视的是,网络安全自身也涵盖了相当多复杂的内容,若在监管中出现工作纰漏,则容易出现相应的技术、安全问题,甚至会泄漏信息、造成网络瘫痪。为了避免出现类似情况,现阶段研究领域逐渐将视野投放至计算机信息管理和各项管理手段以及安全防控措施,将其运用信息管理有助于保障网络安全,利于提升网络监管整体效果。

参考文献:

- [1] 王捷,王峰.计算机信息管理技术在维护网络安全中的应用策略探究[J].电脑知识与技术,2020,16(04):15-16.
- [2] 杨丽丽.网络安全中计算机信息管理技术的应用[J].黑龙江科学,2019,10(04):54-55.
- [3] 邵力.计算机信息管理技术在维护网络安全中的应用策略探析[J].计算机产品与流通,2018(05):15.