政法单位计算机网络安全防护技术策略

梁 丰
（辽宁公安司法管理干部学院，辽宁 沈阳 110161）

摘要：随着信息技术的出现和发展，社会迎来飞速发展，它与人们的生活、生产方式结合得越来越紧密。在此情形下，政法单位也要跟上互联网的步伐，为了更好地促进网络工作的健康、有序、顺利地开展，将先进的计算机网络安全防护技术逐渐推广和引进到工作中去。但是，在日常的网络工作中，政法单位计算机信息网络的安全性，却常常受到来自不同形式信息的严重威胁，这给政法单位健康和经济发展带来了很大的挑战。对此，本文对政法单位计算机网络安全防护技术策略展开探索，以期为相关研究者提供一定的参考与借鉴。

关键词：政法单位；计算机网络；安全防护技术；策略

互联网在日常工作中得到了越来越多的应用，随着政法单位改革的推进，网络信息技术的应用也越来越多，数字化建设是一种不可避免的趋势，它可以帮助提高工作效率和质量。但值得关注的是，在促进计算机网络技术应用的过程中，也要考虑到可能出现的安全问题，如果出现数据泄漏、网络入侵等情况，势必会对信息安全造成威胁，并造成一定的经济损失。因此，政法单位应加强对网络安全的关注，并对其进行有效的安全保护，减少不良因素的影响，增强网络工作的安全和可靠度，才能够真正为政法单位改革与发展而赋能。

一、政法单位计算机网络安全防护的重要性

（一）有利于保证政法单位正常运行

在信息技术飞速发展的今天，政法单位要想更好地进行网络工作，需要计算机通信网络作为支撑，而网络信息量的储备也与计算机信息网络有着密切的关系。如果计算机内部网络受到黑客的入侵，那么它所面对的不仅是网络数据被破坏，甚至是数据的损失，还会严重地影响到政法单位相关工作正常组织和运行，导致整个网络信息系统的瘫痪。若使计算机网络安全性受到重大损害，不但会让政法单位工作人员不能按时完成工作，而且还会让使用者的个人资料安全性受到威胁。为了保持政法单位网络工作正常运转，需要加强对网络基础信息的安全保护力度，政法单位内部便是充分利用这些网络基础设施信息系统开展业务工作的。

（二）有利于保证政法单位信息安全

承担着重要的公共事业和社会治理功能。政法单位所掌握的私人数据都属于国家机密，这也决定了工作人员所开展各项工作具有高度机密性，并且对保障我国经济社会信息安全起着关键性作用。因此，要想保障政法单位信息安全性，需要做好计算机网络安全防护工作。毕竟，政法单位对个人资料保密还具有一定的限制性，在面临着海量的用户信息丢失和信息泄漏的情况下，计算机网络安全体系怎样可以迅速地进行数据处理，将可能受到的技术损失减少到最低，这都是由专职计算机行业网络安全相关技术人员来完成的。总之，专职计算机行业网络安全相关技术人员，是充分发挥利用互联网信息技术在加强政法单位基本管理作用的重要前提。

二、计算机网络安全防护技术分析

（一）防火墙技术

当前，在计算机网络安全防护中，防火墙属于较为常用的防护技术。防火墙技术主要通过其本身对外部网络和内部网络的隔离功能来进行安全防护。通过搭建防火墙，实现内外网连接的网络关卡，通过这个关卡，可以实现对各类外网数据进行有效监控与约束，从而避免黑客与病毒的侵入，从而使内网信息资源得到全面保障，从而增强计算机网络工作稳定度，并很好地反映防火墙对用户的保护功能。当前，防火墙技术逐步朝着多元化方向发展。比如，利用人工智能激活防火墙技术的动态学习功能，针对网络中的动态威胁加以捕捉，在此基础上，通过自动化技术实现防火墙的自动化设置，并对各类威胁进行全面拦截。在分布式技术的运用方面，可以将多个物理防火墙进行协作，从而构成具有强大处理能力和可控能力的逻辑防火墙，从而能够高效地处理计算机网络潜在的安全隐患，从而极大地提升防火墙的工作效率。

（二）入侵检测技术

入侵检测技术是指通过对外界数据进行分析，并对其中潜在不安全的因素进行分析，然后向用户提供分析和评价结果。据此，可以对计算机不安全因素进行预警，预防可能存在的计算机病毒对网络所带来的危害。另外，与防火墙技术相似，入侵检测技术也将会向智能化、分布式等方向发展。与此同时，入侵检测技术也必将向高速网络、标准化领域等方向发展。在高速网络方面，由于百兆、千兆乃至万兆等多种网络的应用与普及，要求入侵检测技术能够更好地与高速网络环境相匹配，从而更好地获得更多的入侵数据，从而更好地保护计算机信息安全。然而，目前入侵检测技术在进行数据安全采集与分析的过程中往往耗时过长，当网络速度进一步提高时，该防护技术将面临瓶颈。为此，对高速网进行入侵检测成为该领域今后研究的重点。此外，已有的入侵检测技术在协作方面存在着严重的缺陷，严重制约其工作性能。要想提高协作的效率，需要建立具有协作机制的入侵检测技术，并与其他防护技术相结合，实现对计算机网络有效的安全保护。

（三）防病毒技术

目前，计算机网络呈高速发展，不但病毒种类日益多样化，而且其防控工作也日益困难。如今，随着社会步入信息化时代，信息技术被广泛运用到各个领域，这也意味着政法单位相关工作均会涉及信息技术的使用，这为不法分子入侵政法单位的信息系统创设了便利，如他们会设计恶意程序攻击政法单位的信息系统创，造成信息系统的瘫痪，或者窃取重要的国家机密。如果国家不加强对这种行为的控制，会造成这种犯罪手段的进一步发展，最后，这种更加高级信息入侵技术不但会给政法单位正常工作带来极大的危害。而且这也增加了病毒蔓延的难度。因此，相关部门的当务之急，是加强对防病毒技术的研究和推广。

三、政法单位计算机网络安全防护技术策略

（一）提升计算机软件与硬件性能

由于计算机网络具有较强的开放特性，政法单位在应用计算机网络技术时，要做好安全防护工作，首先要做的是持续提高计算机软硬件的安全性。在这一流程中，政法大单位必须充分认识自身工

作需要，并据此购置满足要求的硬件设施，同时要紧跟时代步伐，对硬件设备进行更新升级，使计算机的安全性和稳定性等得到最大限度的保障。另外，在选购硬件设备的时候，也要考虑硬件之间的匹配是否合理，也就是说，要选用具有类似功能的硬件进行装配。倘若某一类型硬件设备具有很高的安全性，则计算机网络仍不能达到预想的安全防护状态。因此，政法单位工作人员在安装计算机软件的时候，要防止下载、安装非正规软件，一定要通过官方网站或者正规渠道对软件进行下载。另外，各部门工作人员还需在计算机中安装相应的杀毒软件，并且在安装防火墙，最大限度地保障计算机网络的安全水平。最后，政法单位进行软件安装时还要考虑到，该软件与计算机已有的硬件设备性能是否相符，若自身所安装的硬件设备配置较低，但所要安装的软件配置却比较高，那样的话，这个所安装软件便不能充分将自身功能充分发挥出来，甚至可能会导致计算机网络系统不能正常工作。

（二）加强信息数据保密性

伴随着信息技术的飞速发展，我国在计算机网络技术上取得了巨大的成绩，其快速发展与广泛应用给我们的生活、工作带来了很多方便，同时也带来很多的安全问题。在云技术使用过程中，技术人员需要努力提升相关资料审核工作的安全与实用性，增强数据信息的机密性，防止网络系统遭到恶意攻击。对此，相关技术人员在使用 InternetProtocolSrcurily 技术、安全审计等技术，对计算机网络访问、接入系统进行持续完善，还需要对传送到云计算中的有关信息进行加密，保证其不会被黑客盗取，从而提高云计算中数据的可靠性和安全性。云计算中密码学能够从不同角度对政法单位重要、机密信息进行保密。工作人员使用加密技术进行资料、信息、数据等加密时，要达到防止这些被盗用的目的，可以使用公钥算法、公钥加密技术公开密钥密码，其他工作人员需要通过密码，才能访问系统或获得相关信息，达到安全防护目的。在云计算环境下，工作人员想要共享信息数据的时候，还可以通过云计算等技术，将公钥作为密钥共享的加密方式，从而避免工作人员与其他人共享数据时，被他人恶意盗用的风险。由此，使计算机网络安全防护工作得到有效强化，并且政法单位工作人员的计算机使用合法权益得以保障。

（三）合理安装物理隔离网闸

在计算机网络中设置物理隔离网闸是保证网络安全的重要手段。物理隔离网闸是一种以硬件为基础，将不同的安全级别或领域隔离开来的一种安全装置，它可以有效地阻止外部的恶意攻击，也可以有效地抑制非法接入。首先，可以有效地抑制网络攻击的蔓延。随着网络安全威胁不断发展，当局部网络遭到攻击时，攻击者会把它的攻击范围扩展到其他的网络领域。政法单位通过在重要网络节点上设置物理隔离网闸，将被入侵网络隔离开来，阻止网络中病毒等蔓延，并对可能存在的网络威胁进行控制。其次，可以对网络流量进行。通过对网络门的设置，实现了对不同安全级别、用户身份或服务要求的数据流的划分与控制。这样既可以防止可能的攻击，又可以使网络的性能得到最大程度的改善，从而保证重要服务的正常运转。此外，物理隔离网闸还能对不同级别、类型网络保护，如，将高度机密、敏感信息或系统，把它们配置在独立的区域内，把它们同其他区域隔离开来。如此一来，即使某一区域受到威胁，其他区域安全性仍然能够得到保障。在实际应用中，为了保证隔离的有效性，可以采取空气隔离和电磁隔离等方法。最后，物理隔离网闸的部署还应与网络设计及拓扑结合起来，确保其在整个网络安全架构中发挥最大效益。

（四）科学使用防火墙技术

防火墙技术是一项十分重要的防护技术，所能起到的防护作用也是十分重要的。防火墙像是一道巨大的屏障，可以使计算机网络安全性得到最大限度的保障。采用防火墙技术，既能阻止黑客对网络屏障造成的危害，又能控制“出入”通道的通信流程，显得尤为重要。在网络边界方面，这种技术可以建立起完备网络通信监视系统，并通过数据包过滤等手段对内部和外部进行隔离管理，防止黑客攻击和入侵。另外，政法单位还需要建立完善、规范、全面的网络安全管理平台，保证有关工作的平稳运行，同时也要制定科学有效的策略来逐渐提高工作人员的使用效率。在实现网络信息安全管理的过程中，运用防火墙技术，可以对网络信息平台进行全面的分析和研究，从而掌握不同的网络系统和内部部件的特性，使网络信息的安全性得到最大程度的提升。当技术人员使用防火墙技术进行网络信息的维修时，能够通过各部门的协作和支援，最大限度地维持网络信息的安全性，保证政法单位工作人员正常使用计算机网络，最大限度地提高信息、数据等传输过程中的稳定性和安全性。

（五）提高网络管理员综合能力

政法单位的计算机网络安全管理工作主要由专职网络管理员来完成，而网络管理员的综合素质又会对网络安全管理的成效产生很大的影响，所以，要加强网络管理员的综合素质，保证网络的安全。首先，政法单位要根据自己在电脑网络安全管理方面的具体需求，针对性地对网络管理员进行日常训练，从而使政法单位信息安全管理水平持续提高。与此同时，政法单位可以定期联合网信办、公安局、一些成熟的信息科技企业等对网络管理员进行技术能力的培训，使其能够跟上时代的步伐，防止老的技术跟不上新病毒的步伐。其次，政法单位应建立完善的网络管理者的培训和评估体系，提高他们参加培训的热情，保证他们能全面地了解各类先进的信息技术，切实增强网络安全防范意识，从而保障政法单位计算机网络信息安全。最后，政法单位还可以结合自己的发展状况，与一些高校进行合作与交流，从中选拔出高素质、高素质的网络管理人员，以此来对政法单位计算机网络信息安全管理队伍进行补充，从而解决缺少网络管理人才的问题。

四、总结

总而言之，网络安全关乎国家安全，在信息技术飞速发展的今天，政法单位更应该充分重视网络安全问题，强化网络安全意识，提高网络安全防御技术，规范网络安全管理，对此，可以尝试从以下策略着手：提升计算机软件与硬件性能、加强信息数据保密性、合理安装物理隔离网闸、科学使用防火墙技术、提高网络管理员综合能力，这样可以确保政法单位网络系统安全稳定运行，从而能让政法单位的管理和服务得到保障。

参考文献：

[1] 黄凯 . 行政政法单位网络安全建设对策分析 [J]. 行政事业资产与财务，2021（8）：104-106.

[2] 李伟 . 新时期提高政法单位网络安全的对策 [J]. 数字技术与应用，2021（8）：185-187.

[3] 王保义，张少敏 . 电力企业信息网络系统的综合安全策略 [J]. 华北电力技术，2003（4）：19-22.

[4] 赵跃 . 机关政法单位中计算机网络安全与管理的探讨 [J]. 科技创新导报，2019（20）：77-78.

[5] 胡波 . 政法单位计算机网络安全防护技术分析 [J]. 信息与电脑，2018（17）：175-177.