消防计算机网络安全中的问题及策略

张博

（海南政法职业学院　海南省海口　571100）

摘要：本文基于计算机网络技术在消防领域中应用重要性和现状，从合理使用防火墙技术；强化网络安全，提高保障能力开展有关的培训工作；合理运用计算机漏洞扫描修复技术；确保局域网安全；确保广域网安全提出解决消防计算机网络安全问题的主要措施，以供参考。

关键词：计算机网络安全；问题；措施；消防救援队伍

引言：

目前，在信息化的指引下，消防系统发生了巨大的变化，其计算机网络技术在消防领域中也得以充分利用。计算机网络技术多项功能都得到了发展，其中包括远程控制系统、火警接收系统、辅助决策系统、GPS 定位系统等。通过消防计算机网络技术，不仅有效提升了灭火救援效率也提高了消防工作的质量。同时，利用计算机网络技术，可以有效地完成办公任务的自动化，减少了人员工作强度。

1、计算机网络技术在消防领域中应用重要性和现状

1.1 计算机网络技术在消防领域中应用重要性

在运用计算机网络技术的过程中，其具有许多显著的特点，包括信息多元性、档案保密性等。同时，因完整性特点致使计算机的数据未经许可不得被随意更改，可以说运用计算机网络技术在火灾管理中，可以有效地促进火灾信息的透明性，强化监督管理成效。

1.2 计算机网络技术在消防领域中的应用现状

计算机网络技术在火灾中的运用，可以起到积极作用。整个火灾系统都为计算机技术支撑。其中包括火灾报警处理与调度、网络资料的维护、电脑辅助决策的专家辅助系统等。火灾报警是通过光纤与当地消防大队的程控交换机连接，随后从交换机中提取有关的号码，并根据实际基础所在地自动生成相应的数据文件，这样再接到该报警电话后可快速得到处理，有效提高了受理效率，并且也会消防救援队伍争取了救援时间。可以说在计算机网络技术的帮助下，消防救援能力的整体都得到了提高，并且随着网络技术的进一步发展，在消防领域当中的应用得到有效的改善与升级，这些技术不仅可满足日常的消防工作，也可在后续发展中持续推动我国消防领域信息化建设水平。然而，这些计算机网络技术在发挥其正面效应的同时，也有其对应的缺陷。总体来说，计算机网络技术在火灾救援工作中的实际应用，需要消防人员提高对网络技术以及网络安全防范意识的掌握，确保注重计算机网络的安全操作，并及时更新防火墙以及杀毒软件的功能，但由于部分人员在这方面处理能力较弱，自身的网络安全意识不足致使消防计算机网络存在一定的安全问题，严重影响了该技术在消防领域的实际使用价值。

2、消防计算机网络的安全问题

计算机网络的安全性是确保各种资料不被篡改、泄露，针对消防计算机网络安全问题进行分析，其主要的风险因素为：

一是自然损坏。在地震、火灾、洪水等自然灾害面前，计算机外部受到破坏或因计算机使用时间较长，线路、设备出现损伤或老化，这些情况都会对网络计算机安全造成影响。

二是人为损坏。该情况因计算机运行状况良好，但由于运营商的某些操作，导致数据的丢失、篡改、系统瘫痪等问题。该问题也分为两种特定的情况，第一是由于操作者的无意识，或者操作人员安全意识不强、技术有待提高等主观问题导致的计算机网络风险。第二是因为运营商的恶意攻击，导致网络崩溃。如黑客的任意攻击，竞争者的蓄意压制，将会对计算机网络安全造成极大的危害。

三是病毒入侵。计算机病毒容易侵入计算机控制运行系统，使其无法正常运行。

四是由于开放的网络资源，造成信息数据较多，在为当地消防救援队伍提供便捷的同时，也产生了巨大的安全隐患，若不加以防范，则会被不良人员窃取到有关的数据信息，产生较为严重的后果[1]。

3、加强消防计算机网络安全措施

3.1 合理使用防火墙技术

目前，为加强消防计算机网络安全性，应合理运用防火墙技术。防火墙技术从字面上来说，即为隔离网络安全风险的防御手段，其是由计算机软硬件组成的一种防御体系。确保网络、资料在安全区域不被盗用、篡改，防火墙技术可以确保电脑内部的网络与互联网的隔离，只有在外部的信息足够安全的情况下，才能让数据进入到系统中，从而确保计算机网络内部安全。

（1）防火墙技术特点

防火墙的最大特征为具有防护和隔离功能。在信息的传递中，防火墙将会对所有的信息进行严格的控制，当出现不合格的信息时，防火墙会阻止信息的传输。防火墙不但对外部的数据进行严密的监控，同时，对一些不健康的站点进行恶意攻击，也能及时阻止这些限制，确保计算机网络安全。防火墙不但具有监视和限制信息的作用，而且能够记录所有的存取，当出现隐患问题时，可根据信息数据的不同，产生不同的诊断与处理。在类似的情况下，防火墙会发出警告，提示网络安全受损。尽管防火墙对网络的安全起到了一定的保障作用，但是它本身也存在着很多问题。为此当地消防救援队伍应按照实际需求合理使用该防护技术。如，虽然防火墙可以阻止恶意的入侵，但无法将其彻底消灭，针对新兴漏洞信息防火墙还无法做出有效的预防[2]。

（2）防火墙技术在网络安全的具体应用

由于信息数据安全性较差，很容易被不法人员利用，造成资料泄露、丢失。而防火墙系统会将特定的文档进行加密，并以特定的密码进行解密，使得在传输时，有效提升信息传输的安全性确保所传输的信息与数据不会发生任何问题。同时，针对信息数据在传输时，该技术也可确保所传输通道得以安全，并通过防火墙技术将双方进行授权验证，在得到授权证后建立有效的身份识别信息，并完成安全传输通道的开启状态，以防止未经过授权的终端记录到此过程中，以确保计算机网络得以安全。在有效的监控信息数据时，防火墙技术可编写特定的保护功能以及相关规则，完善网络之间的安全屏障，针对内部网络以及互联网内部所产生的信息进行监控，在监控后针对不合格的信息进行限制，有效确保了计算机网络安全环境，并针对某些会造成威胁的信息数据进行了检测，以全方位、全

过程确保计算机所输入的信息数据为有效性、安全性[3]。

3.2 强化网络安全，提高保障能力开展有关的培训工作

目前，为了有效地提高当地消防救援队伍网络信息安全工作，提高消防救援人员对网络安全和信息保密的认识，防止各种违法行为。当地可积极组织一场关于“互联网安全”的专题讲座。讲座中可邀请专业教师分享自己的教学经验，对计算机网络基础知识、网络设备操作及网络安全检查等方面内容进行了培训，并对网络安全的概念及重要性、安全预防对策等方面进行了详细的讲解。在此过程中，消防救援人员还就日常工作中使用电脑网络的信息安全问题进行了探讨和交流。通过这次活动，广大消防救援人员对网络安全工作的重要性有了进一步的认识，对基本的网络安全知识有了一定的了解，提升了自身的网络安全防范意识，为今后的消防安全工作奠定了良好的基础。

最后，当地消防救援队伍还应持续做好有关网络安全的工作，定期检查各大队和各大基层大队的计算机。同时，通过层层签订责任书，以各级机关、各部门的领导为单位，强化消防救援人员信息安全意识，让安全意识深入人心，为其使用计算机网络技术奠定扎实可靠的基础，为消防救援队伍网络安全保驾护航[4]。

3.3 合理运用计算机漏洞扫描修复技术

由于计算机网络技术是依靠计算机主体加以运行，再加上网络信息环境具有开放性以及便捷性等特点，导致计算机系统很容易出现诸多漏洞，针对这种情况，应合理运用计算机漏洞扫描修复技术，帮助消防救援队伍所使用的电脑系统完成全方位的扫描，在扫描过程中，可以有效查找计算机内部是否存在病毒或安全漏洞，在分析查找完毕后，可自动化地通过修复处理解决计算机内部漏洞，以避免不法分子通过漏洞获取到当地消防救援队伍的内部机密信息[5]。

3.4 确保局域网安全

现今消防救援队伍局域网大部分采用以太网，两个结点间的通讯资料，不但可以由两个结点同时收到。在相同的以太网中，任意一个节点都可以对其进行拦截。所以，黑客可以访问任何一个以太网的结点来监听，这样就能捕捉到以太网上产生的数据包，并对其进行解封分析，从而盗取到重要的信息，其属于局域网重大的安全隐患问题。目前，有一些方法可以解决局域网安全问题：

（1）网络区段

网络区段被视为一种基本的控制手段，同时也是保障网络安全的一种有效手段。其目标是把非法使用者与敏感网络资源隔离开来，以避免被窃听。

（2）将共用集线器替换为交换型集线器一

局域网中央交换器完成区段后，依然会有以太网监听的风险。这是由于终端用户经常通过分支集线器而非中央交换机访问，而最常用的分支集线器则是共用集线器。因此，在与主机进行数据通信时，同一中心内的其他用户仍然可以监听到两个计算机间的数据分组（即单点播分组）。并且会产生较为严重的安全隐患：当用户通过TELNET 连接到一台计算机时，因为 TELNET 程序没有密码，所以用户输入的所有重要信息（包括用户名、密码等）都会以明文方式传送，从而使黑客有机可乘。为此，当将共用的集线器改为交换型集线器，使得单播包只在两个结点间进行传输，以避免被窃听。当然，交换中心仅能对单一点进行控制，而不能对广播和多点数据进行控制。但因广播和多点播报中，所包含的重要信息要比单一的数据包要少得多所以该方法措施也会产生实质作用。

（3）VLAN 的划分

VLAN 技术包括三大类：基于交换端口的 VLAN、基于节点 MAC 地址的 VLAN 以及基于应用协议的 VLAN。在某个集中的网络环境下，一般会把中央的主机系统都集中到 VLAN 内，在 VLAN 内没有任何使用者结点，以此更好地保护敏感的主机资源。在分布式网络中，可以根据组织或部门的设定来进行 VLAN 的分区。每个部门的服务器和用户节点都具有独立的 VLAN，互不干扰。VLAN 的内部连接可通过交换机来实现保护效果，VLAN 技术的连接是通过路由来实现与 VLA.N 的贯通效果。当前大部分交换机都支持两种国际标准 RIP 和 OSPF，该标准可确保交换器可以让系统管理员把所有或特定端口数据包映射到特定端口内，并将其输送到与此时端口相连的入侵监视装置或协议分析装置中，以达到防范安全风险的效果。

3.5 确保广域网安全

在广域网中，大部分都是使用公共网络进行数据传送，因此，通过广域网进行信息的拦截与使用，其概率远远高于局域网。在缺乏完善的监控系统时，通过在互联网上免费下载的“包检测”软件，可以轻松地拦截和破解通讯数据。为了确保消息的传送和接收，除发件人和接收者之外，任何人都无法知悉（隐私）；在传送期间不受干扰（真实）；发送者可以确定接受者并非伪造（非伪装）；发送者无法否认其自身的传输（不可否认），一般来说广域网一般使用下列安全措施：

（1）VPN 技术

VPN (Virtual Network, VPN）的关键技术为利用隧道技术，将消防救援队伍专用网络中的数据进行加密，然后通过虚拟的公共网络隧道进行传输，以防止敏感数据被窃取。VPN 可以在互联网、 IP、帧中继或 ATM 网络上建立。消防救援队伍在公共网络中设置 VPN，即通过专用网络建立内部网在安全性、先进性、可靠性和可管理性方面，其建设周期、投入资金和维持成本都大幅下降。

（2）身份认证技术

若用户在局域网上拨号，则会因使用公用电话网络进行资料传送产生安全风险问题，为此应加以进行管理。其常用的身份识别技术可通过验证拨号验证对方身份，并将完整的登录日志记录下。比较常见的为 Cisco 公司的 TACACS+和 RADIUS 的行业标准。

结束语：

综上所述，计算机网络的使用范围日益扩大，网络的安全问题在社会持续发展中，也日益引起了人们的重视。我国在计算机安全领域已有了一些成就，在消防救援队伍使用计算机网络技术时，可有效提高消防工作效率。但也会因为网络信息的开放性产生不小的安全隐患，导致信息数据受到攻击，因此，在实际解决消防计算机网络技术存在的问题时，应通过防火墙、局域网加密等技术措施，减少计算机所受到的危险攻击，既能保证计算机使用安全，还可持续提高消防救援队伍计算机网络技术应用能力。

参考文献：

[1]李健，李小虎，焦志勇. 浅析计算机信息管理技术在维护网络安全中的应用[J]. 中国新通信，2020,22(20):63-64.

[2]周琦. 影响计算机网络安全的因素及防范措施[J]. 中国科技纵横,2020(19):58-59.

[3]刘赫. 大数据时代的计算机网络安全及防范措施分析[J]. 中国宽带,2020(11):29-31.

[4]李志江. 高校网络安全中计算机信息技术的有效运用[J]. 科教导刊,2020(36):18-19.

[5]解皓. 计算机应用中的网络安全防范研究[J]. 信息记录材料,2020(12):220-221.

作者简介：张博，出生年 1983，男，汉族，吉林长春，海南政法职业学院 公安司法系，副教授，硕士，研究方向：计算机应用、声响鉴定、消防工程技术等。