企业局域网网络安全防范措施浅述

李明清
（上汽通用五菱汽车股份有限公司 青岛分公司，山东 青岛 266000）

摘 要 在计算机网络技术飞速发展的时代背景下，企业在局域网网络安全方面的投入逐年增加。企业局域网能够提高员工工作的通畅性和高效性，但是同时也会存在一定的安全风险。安全防范的质量对于企业的不同工作都会产生影响，企业首先需要跟随行业发展的潮流及时更新计算机的软件和硬件，而后则需要不断提高工作人员的安全意识，保证使用企业局域网网络时不存在会增加安全隐患的操作。基于此，本文深入研究了企业局域网网络安全防范措施，并针对存在的问题提出了有效的防范策略，希望对提高企业局域网的安全性提供帮助。

关键词 企业局域网 网络安全 互联网络攻击 防火墙
中图分类号：TP393.1；TP393.08 **文献标识码**：A **文章编号**：1007-0745(2022)03-0022-03

企业局域网网络能够为员工提供漫游、信息通信等多种功能，借助无线信道能够提高员工的工作效率，与其他网络相比具有明显的灵活性和便捷性。但是企业局域网网络的安全性在近几年也受到了较大的威胁，无线电波的使用导致入侵者可以在外部进行物理连接，并且对其内部的网络进行恶意攻击，因此深入研究和总结企业局域网网络安全防范措施具有十分重要的意义。

1 企业局域网网络所面临的安全威胁

计算机网络技术影响着群众的学习、生活和工作中的方方面面，因为计算机可以为人们提供丰富的资料信息，所以工作中信息收集和整理环节的效率将可以大幅度提升。但是网络的广泛适应在一定程度上也增加了其脆弱性，广泛的治疗共享和分布导致网络更容易受到外界的攻击。企业局域网不仅能够通过接入方式连接到网络，而且也可以成为独立的体系，借助计算机网络技术实现信息资料的接收和发布。作为独立体系的企业局域网可以通过接口界面软件 CGI 与其他软件实现连接。

企业的局域网具有适应十分方便和便利的优点，但是存在入侵者可以比较轻易地攻克的问题。无线信号对墙壁和门窗都具有覆盖能力，但是覆盖范围的精确度比较低，在接受信号的过程中接受范围和设备都没有定向，因此很容易出现目标外泄和各种各样的安全问题。使用企业局域网的最初目的是保证企业资料的机密性和真实性，但是随着网络开放性的不断扩大，网络存在的安全隐患也在不断扩大。隐患产生的原因可能是人为因素、意外失误或者软件漏洞，从而使发生非法访问和恶意攻击等事件的概率显著提升。[1]

1.1 硬件方面

现如今，部分企业存在设备相对落后的问题，在计算机服务器较为落后的情况下，软件安装和运行系统的使用都会遇到更大的阻碍。其中无线设备和防火墙对于企业局域网网络的安全性影响都很大，落后的防火墙很难起到防范内部网络遭受入侵的目的，企业工作人员在使用无线网时也需要承担较大的安全隐患。

1.2 软件方面

软件和操作系统都需要工作人员对其进行调试和编写，其设计和结构主要受到使用者和制造者的影响，因此无法避免的存在一定的漏洞和缺陷。而入侵者则可以通过软件和操作系统的漏洞进行攻击，遭受恶意程序破坏的计算机一般也很难正常工作。网络系统同样需要人为给予的程序支持，才能够顺利地完成提供网络服务和实现网络协议的功能。人为因素也会导致网络使用过程中出现各种很难预测的漏洞。

1.3 人为方面

技术人员和使用者都会对企业局域网网络安全性造成一定的影响。企业局域网可以让工作人员方便地进行信息共享，工作人员对于计算机的依赖程度呈现出了不断提高的趋势，所以网络的安全隐患也逐渐增大。

1.4 互联网络攻击类型

互联网络攻击可以分为两种类型，其中一种是包括了口令攻击、协议攻击、溢出攻击、IP 地址攻击和路由攻击五种的静态数据攻击，而另一种则是包括了主动攻击和被动攻击的动态数据攻击。口令攻击是指通过穷举口令或者寻找相关文件的方式确定正确的口

令，而后顺利进行非法的系统侵入。协议攻击的基础是操作系统通信协议中存在的漏洞，入侵者借助漏洞可以得到系统管理员的权限。IP 地址攻击则需要入侵者伪装内部系统源 IP，达到冒充他人和窃取资料的目的。动态数据攻击中的主动攻击是指攻击者通过监听信息流，或者收集信息流长度等资料，进行科学的流量分析。被动攻击则是指攻击者会对数据流进行删除、修改或者复制等操作，达到破坏数据流的目的。[2]

2 企业局域网网络应当具备的功能

为了能够十分有效地规避来自外界的安全威胁和攻击，必须要有针对性地采取网络信息保护策略，确保企业局域网网络受到的外界威胁能够得到有效控制，完善的网络安全系统应当具备身份识别、存取权限控制和数字签名等功能。首先身份识别是网络安全系统十分重要的功能之一，能够十分可靠地确定出通信双方的真实身份。然后存取权限控制则可以十分有效地防止非法用户进入系统以及进行非法操作。数字签名功能的基础是公钥加密算法，信息接收方可以相信信息来源的唯一性。数字签名可以起到判断信息完整性、审计追踪和密钥管理的效果。

优秀的企业是非常注重网络安全管理的，网络安全的管理可以涉及很多的方面，包括企业内部重要的信息和企业私密的资料，这对于网络重要系统的部分硬件保护是势在必行的，有了网络安全的保护，就可以在很大的程度上保护企业的数据不会遭到破坏和泄露。企业的很多安全都是需要在管理和技术这两个层面上进行探究的。

2.1 安全管理层面

对于企业的安全管理，最重要的还是人本思想，创建一个网络安全管理的系统，让每人的责任具体化，不仅如此，还需要做到的是增加对涉及的网络的使用情况管控，同时加大对技术人员的培训学习时长，这样可以在一定的程度上增加安全意识，能在技术和意识方面保障企业网络的安全性。

2.2 技术应用层面

涉及到有关企业的网络安全和其他的网络还是有很多不一样的地方，最初的防火墙技术、网络分辨技术和侵入保护技术都需要强化，这样可以使得企业的数据安全得到保障。

1. 对于企业网络的防火墙设置，是能够和企业内部的很多的系统相连接的，可以使用权限设置和密码设置，作为一个保护的屏障，可以起到保护企业内部网络的作用，不让外界潜在威胁进入企业内部，与此同时，网络防火墙也可以起到一定的保护作用，不让内部的资料对外界传输。

2. 在分类的时候，企业的隔离有很多种，使用这些隔离，可以在一定的程度上识别危险信号，防止危险信号的攻击，将有危险的信号隔离开来，从而让工作人员能在比较安全的环境里进行操作。

3. 而对于以上两种方式都不能有效避免危险信号的情况，企业就需要设置另外的防止系统，以随时监测外界的动态，做好保护的工作，通过这些操作，可以在一定的程度上保护企业的局域网。

3 企业局域网网络安全的防范策略

3.1 落实备份工作

在网络安全隐患种类不断增加的情况下，备份工作在企业的运营过程中是十分重要的，因为有效落实备份工作可以保证企业的数据不会因为外界攻击而丧失。如果出现了企业局域网网络受到他人恶意入侵或者数据资料被他人篡改的情况，工作人员可以借助之前的备份对数据进行修正和完善，尽可能降低网络安全隐患对企业项目的影响。完全备份、差异备份以及文件备份都是比较常见的备份形式。如果工作人员采取完全备份的方式，将会花费较多的时间成本，但是完全备份在工作过程具有十分重要的地位。企业在运营过程中需要定期地进行全部备份工作，确保项目的完整性和安全性可以得到最大化的保障。差异备份的含义是工作人员在完成了完全备份之后，需要对资料中可能发生的变化进行及时的备份。最后，文件备份在实际工作中的概率相对而言比较低，企业应当对数据备份工作给予高度的重视，确保重要的数据不会出现被恶意篡改或删除等等。[3]

3.2 设置和安装防火墙

设置和安装防火墙十分有利于实现精细化的企业网络管理工作，通过有效限制网络之间的访问可以大幅度提高网络信息安全性。防火墙可以为企业局域网网络形成保护屏障，内网和外网之间形成的隔离可以保证网络的安全性。除此以外，防火墙还可以保证信息数据传输过程的安全性，计算机之间传输的信息都需要经过防火墙的检测。网络分割管理也是防火墙的重要作用之一，使用者在访问过程中会受到来自防火墙的全程检测，只有符合规则的数据才可以得到访问的机会。

3.3 重视内部监测工作

内部检测工作主要包括了硬件设施检测以及网络管理、网络控制两个方面，首先工作人员需要对硬件

设备进行定期的严格检查，对路由器、交换机、主机和防火墙等一系列设备进行全面的检查和监督，确保硬件设备存在的问题可以得到及时地发现和处理。工作人员还需要对硬件设备出现的问题进行备案，以此不断提高监管工作的科学性和有效性，企业重要数据的备份工作也可以在硬件设备的支持下第一时间完成，再者工作人员还需要积极落实网络管理和控制工作。[4]

3.4 安装杀毒软件

杀毒软件可以十分有效地保障软件安全，以及提高操作系统对于网络病毒的防御能力。杀毒软件能够在第一时间发现病毒并进行清除，确保恶意软件和木马程序不会对设备造成严重影响。现如今，杀毒软件已经成为了计算机安全防御中十分重要的组成部分，能够起到主动防御、软件监控和病毒查杀等十分关键的功能。

3.5 及时修复系统漏洞，预防交叉感染

系统漏洞和补丁都会严重降低企业局域网网络的安全性，部分危险性较高的漏洞会导致计算机无法有效防御病毒的侵害，所以系统补丁的更新和修补工作必须要严格落实。工作人员需要对系统漏洞的修复工作给予高度的重视，尽最大的努力减少系统漏洞，尽可能减少企业局域网网络和计算机可以存在的安全隐患。

企业局域网网络具有相对封闭的特征，所以严格管理外界设备的措施可以十分有效地保障局域网网络的安全。U 盘是企业工作人员最常使用的信息储存载体之一，U 盘方便快捷的使用方式在一定程度上提高了企业整体的工作效率，但另一方面也增加了病毒交叉感染的概率。所以为了能够保护企业资料和企业局域网网络的安全性，必须要重视和落实 U 盘的管理工作，保证员工使用的 U 盘不携带可传染的病毒，员工也可以在 U 盘使用前后进行病毒查杀操作。[5]

3.6 落实 IP 地址保护工作

IP 攻击是十分常见的网络恶意攻击方式之一，黑客可以结合用户的上网痕迹进行 IP 跟踪，一旦黑客得到了具体的 IP 地址，就会对选定的目标进行各种各样的攻击。为了能够有效保护企业局域网网络的 IP 地址，工作人员可以使用代理服务器隐藏真实的服务器地址。黑客通过 IP 跟踪只能够掌握代理服务器的 IP，而无法对企业的服务器进行恶意攻击。企业在日常运营过程中也同样需要高度重视 IP 地址的保护工作，尽可能降低信息泄露的可能性。IP 地址保护工作需要工作人员足够耐心和细心，使用代理服务器对于保护企业局域网网络是十分有效的。

4 结语

总的来说，企业的局域网建设是非常重要的，也是非常复杂的，是一个有规则的大系统，会和很多的工作相联系，这就要求我们在具体的工作中，要对安全引起足够重视，可以采用一些合理的方式方法，这样就可以在一定的程度上保障局域网的合理安全，可以让局域网发挥更大的作用，为企业的发展提供更多的帮助，提高企业的效益。企业局域网网络的安全防范措施还需严格落实备份工作、加强内部监管、防止交叉感染和及时修复漏洞等等，企业和工作人员在日常工作过程中都需要严格实施有效的防范措施，尽可能降低企业局域网网络遭受恶意攻击的概率 [6]。

局域网的使用需要将无线信号作为一种媒介，并在此基础上支持漫游、移动通信和网络通信，其移动性、灵活性、可伸缩性和方便性更加明显。其在使用中的优势主要体现在对无线电波的使用上，但在使用中，局域网也会产生一定的安全问题，即入侵者不需要进入内部物理位置进行物理连接，只需要攻击内部网络。为了加强网络设计功能的安全管理，改进网络安全防范措施，还必须大力加强网络安全管理规范的建立，因为许多不安全因素都反映在组织管理和人员管理等方面，这是企业局域网安全管理必须考虑的基本问题。

参考文献：

[1] 盖广昕 . 浅谈企业局域网网络安全防范 [J]. 山东工业技术 ,2016(04):143.
[2] 吴磊 . 企业级局域网内的网络管理监控及信息安全防范 [J]. 通讯世界 ,2015(19):36-37.
[3] 秦一方 . 浅谈大中型企业局域网络信息安全与防范 [J]. 网络安全技术与应用 ,2015(09):47,49.
[4] 马代军 . 企业级无线局域网的网络安全防范措施 [J]. 电子制作 ,2014(12):140-141.
[5] 葛玉峰 . 国有企业局域网络攻击与安全防范措施 [J]. 计算机光盘软件与应用 ,2014,17(10):188,190.
[6] 吴凌智 . 企业级局域网内的网络管理监控及信息安全防范 [J]. 计算机光盘软件与应用 ,2014,17(07):177-178.