企业信息化建设中的网络安全问题浅析

高 敏*
国能大渡河瀑布沟发电有限公司 甘肃 白银 625304

摘 要：随着信息时代的来临，信息技术在各行各业都取得了广泛的应用，促进社会经济迅速发展的同时，也为企业工作提供了极大的便利，提高了企业的管理手段。现代企业利用信息技术进行资源管理，在强化管理的同时，也加速了现代化进程，而随着信息化建设的大阔步前进，网络安全问题也随之而来，我国已经越来越重视网络安全，提出网络安全就是国家安全，将其提到了前所未有的高度。目前，企业在应用信息技术的过程中还存在一些弊端，基于此，本文浅析了企业信息化建设过程中的网络安全问题和面临的困难，并提出相应加强网络安全建设的观点。

关键词：企业；信息化建设；网络安全；管理
DOI：https://doi.org/10.37155/2717-5170-0305-31

引言

在步入信息化时代的过程中，网络安全问题也随之而来，滞后的网络安全管理和先进的信息化建设，使得企业本身的信息化系统存在潜在的危险，一旦遭受到网络动荡或者人为的干扰和破坏，企业将会面临巨大的损失[1]。所以在享受信息化建设带来利益的同时，必须严把安全关，做好在信息化建设中的网络安全管理工作，尽量杜绝安全问题的发生。

1 现代信息化建设中的网络安全现状

我国的网络安全防护技术还处在发展的过程中，网络安全管理方面起步较晚，网络攻击屡禁不止，整个互联网的大环境对于企业安全管理极为不利，信息网络环境的安全性是否能够得到保障，关乎企业是否能够持续健康发展，若企业内部没有完善的网络安全保障体系，一旦出现安全问题，企业将面临着信息泄露、管控瘫痪等问题，影响正常运转，造成巨大的财产、信誉损失。

相比较黑客、红客等专业组织团体，大部分企业网络安全管理团队人员配备都不是很充分[2]。目前在世界范围内有名的黑客团体不胜枚举，他们通常是有组织的开展网络攻击活动，通过各种社工手段筛选攻击目标，找准目标之后分工合作，投入技术力量攻击专一的目标，他们信息共享、技术共享，这使得攻击效率会比较高。除了这些组织团体，在互联网上还散落着很多独立的网络攻击技术爱好者，数量也是非常庞大的，这些人手中掌握着大量0day漏洞，在互联网这个空旷的原野上，他们的目标是所有暴露在网络中的漏洞、系统等等，黑客的跃跃欲试，或者技术爱好者的简单尝试，对于企业网络安全来说都是一次次不容小觑的冲击。

要想让信息技术能够更加安全可靠地为企业服务，就需要企业掌握最新的信息技术，了解互联网漏洞、提高防御手段，这要求企业的管理人员必须提高自身的综合素质，不断更新知识和专业技术人才储备，使信息技术管理更加专业化、系统化。

2 企业信息化建设中面临的网络安全问题与措施

2.1 网络架构趋于凌乱

大部分企业的网络架构是在一开始的时候统一建设部署的，前期规划和后期信息化建设契合度不高，更甚至有些网络架构都没有考虑整个网络扩展性。在企业信息化建设的进程中，新兴管理系统层出不穷、智能化项目大量开发应用，而在此过程中，为了信息化建设项目的快速投入使用，基础架构问题往往是最容易被忽视的，通常都是随意取点连接，这就使得企业网络结构随着信息化进程逐渐趋于混乱。

*通讯作者：高敏，1992.10，汉，女，甘肃会宁，国能大渡河瀑布沟发电有限公司，信息系统专责，助理工程师，本科，研究方向：网络与信息化管理。

企业网络基础架构要合理规划、统一管理，提前规划短期和长期信息化建设的需求，预留网络接入点，具有前瞻性的管理企业网络基础架构，在信息化项目快速落地进程中，更要关注网络规划，避免凌乱的网络架构给企业管理带来的隐患，有了基础规划才能结合自身企业的特征，采取有效的安全防护对策，降低信息安全问题的发生率。

2.2 防护体系不完善

由于缺乏专业的技术人才进行网络安全防护体系建设，大多数企业的防护体系并不健全，而边界防护也一直都没有被重视，很多企业边界防护不够严谨，只是配备了一个简单的防火墙，甚至防火墙的策略配置都只是使用了一下简单的默认配置，并没有真正用好[3]。此外还存在一些隐蔽性很强的数据通道，这些通道很可能会成为黑客攻击的路径，盗取企业的数据，对于企业本身的网络安全造成极大的干扰。

现如今网络安全防护已经在形成一套成熟的体系，包括边界防护、使用点对点专线、网络分区、加密传输等。传统的单一防火墙已经无法很有效的抵御外部入侵，所以强化防护体系便是重中之重。在防火墙的基础上可以搭配服务器防火墙、行为管理设备等，构建一套完整的防护体系，利用多种认证技术控制网络访问，增加审计跟踪技术，保障企业的信息数据资源安全，这些防护手段都是非常有必要的。

2.3 非法入侵花样繁多

受到恶意攻击和非法侵入，严重阻碍用户正常使用网络，对于正常的商务活动造成破坏，这也是企业工作者最为头痛的网络安全问题之一。在传统利用系统漏洞和软件漏洞进行入侵攻击的可能性越来越小的前提下，网络钓鱼攻击已经逐渐成为黑客们趋之若鹜的攻击手段。网络钓鱼迅速泛滥，其对企业网络威胁已经逐渐超过其他攻击手段。同时，黑客攻击和非法入侵对于企业造成的危害相当大，利用暴力手段破解密码阻止用户正常使用、大流量包攻击堵塞企业网络、恶意植入木马病毒等层出不穷，这些花样繁多的入侵都会给企业造成很多无法挽回的损失。

网络信息技术的普及程度越来越高，当前防护体系能够过滤很大一部分钓鱼邮件和病毒木马，所以在企业安全管理中，要用好已有的防护体系，提高企业的安全管理指数。然而一些经过伪装的钓鱼邮件仍然会穿过层层防护到达内网员工电脑里，这些邮件往往都具有针对性、内容非常诱人，诱使员工点击邮件中的一些链接，而链接的背后便是各种病毒和木马[4]。当员工点击之后，便为攻击者提供了一个畅通无阻的后门。所以企业应该增强网络安全培训，提高员工的网络安全意识，用职工的安全意识编织一张有效的防护网，形成一面可靠的安全屏障。另外，办公电脑配备有效的杀毒软件和防火墙也可以提高企业安全防护能力，强化网络信息安全。

2.4 上网准入还不完善

目前大多数企业对于上网准入还很陌生，办公区域中为了方便而开放的wifi和网线接口没有经过任何隔离就可以接入企业内网，对于这种企业网络，非法入侵人员可以不费吹灰之力就进入企业内网中，存在极大的安全隐患。

在企业的安全网络管理工作中，接入点的管理也是非常重要的，而这也是非常容易被忽略的一点，开放的wifi和网线接口只要连接一台感染病毒木马的电脑，便可以毫无阻拦的进入企业网络，木马便能很快感染内网，所以上网准入是网络连接的第一道防线[5-6]。企业可以使用行为管理器等硬件设备或软件配置上网准入，在设备接入内网时，对设备信息进行记录、并进行安全扫描，只有符合安全管理要求的电脑经过账户密码认证才可以接入内网，这将会大大提高内网安全度。

2.5 安全管理未被重视

近年来，我国计算机和网络技术取得了突飞猛进的发展，信息技术在各个领域都得到了广泛应用，同时随着在各个领域的使用，信息技术变得越来越完善，而网络安全管理技术却进步稍缓，没有受到人们的重视，部分企业的网络安全管理技术人员配备非常薄弱，甚至没有配置专业安全管理人员，这给企业网络安全管理带来巨大的压力和挑战。

企业的管理归根到底是人的管理，网络安全管理最重要的也是人的管理。因此，企业在信息化建设的过程中，首先要加强人才储备和培养，让专业的人员从事网络安全管理工作，同时也要培养全体员工的网络安全意识，使员工认识到网络安全管理工作的重要性。

3 结束语

综上所述，现代企业想要真正利用信息化技术带来优势，推动企业获得长足稳定的发展，就必须重视网络安全管理工作，采取有效的管理手段，提升管理认识，真正杜绝网络安全问题的发生。

参考文献：

[1]曹宏亮.企业信息化建设中网络安全管理问题的思考[J].信息与电脑:理论版,2019(17):218-219,222.

[2]吕计英.浅谈企业信息化建设中网络安全管理问题[J].数字通信世界,2019(5):256.

[3]张能.企业信息化建设中的网络安全管理问题[J].计算机与网络,2019(8):56-57.

[4]崔尧. 企业信息化建设中的网络安全管理问题[J]. 电子技术与软件工程 ,2018(16):198.

[5]崔凯. 对企业信息化建设中网络安全管理问题的思考[J]. 电子测试 ,2018(12):122-123.

[6]谢志明 . 关于企业信息化建设中网络安全管理问题的思考[J]. 科学与信息化 ,2019(13):92.