浅谈企业信息系统数据安全管理与应用

沈豪杰
德和科技集团股份有限公司 浙江嘉兴 314000

摘　要：随着信息时代的到来，计算机网络已经成为社会活动的重要媒介，它不仅使企业的日常运营更加方便，而且成为提高经济水平的必要手段。对于企业的发展来说，网络信息安全建设具有重要意义。随着大数据等技术的发展，加强企业网络信息安全维护势在必行。然而，在企业信息系统运用范围日益广泛的过程中，数据丢失、信息泄露等安全问题也变得愈加严峻。由此可见，如何对企业信息系统数据安全技术的影响因素形成正确认知也成为当下迫切需要关注的内容。

关键词：企业管理；信息系统；数据安全；管理应用

引言

随着计算机在各个领域的普及和网络用户群体的不断扩大，一旦用户在使用计算机时出现问题，就容易造成极大的危害，给企业造成的损失是不可估量的，保证企业信息系统的数据安全非常重要。在我国，计算机的使用已经基本实现普及，在这个过程中，企业信息系统数据安全问题也日渐明显，这对我国网络安全工作来说，是个巨大的挑战。在此过程中，不仅要提升企业信息系统数据安全的防护意识，还需定期扫描系统，及时发现并修复系统漏洞，以保障企业信息系统数据的安全性。

1 企业信息系统数据安全问题

1.1 安全漏洞

软硬件技术问题主要体现在网络硬件安全隐患、软件缺陷和漏洞、病毒和恶意程序等方面。其中，路由器是硬件层面安全隐患的代表。如果路由器的安全性能较低，可能会带来一些安全问题。在生产经营过程中，企业不可避免地会涉及到操作系统和应用软件。软件或系统中的缺陷和漏洞将成为恶意攻击者关注的焦点。恶意攻击方基于该通道窃取机密数据和信息，将会给企业带来严重的经济损失。病毒和恶意程序具有传播速度快、影响范围广的特点，大多通过各种渠道入侵到内部网络中，严重者可能造成网络的瘫痪。部分企业安全防护更新速度较慢，难以对各类病毒起到保护作用，是病毒和恶意程序蔓延的重要因素。

1.2 管理不严

（1）缺乏整体规划。企业没有根据自身需要制定长期的信息安全管理计划。公司领导参与信息安全规划有限或受专业能力限制，无法有效提出指导和发展方向。安全目标不明确、管理职责不明确、重要信息资产失控等问题将导致企业信息安全危机。（2）缺乏安全管理制度。在国家层面，因信息安全属于较新领域，政府已发布的信息安全法律法规并不完善，处罚力度与管制范围不能满足当前企业安全要求。在企业层面，多数企业尚未制定适宜本企业的信息安全管理制度，导致企业对信息安全管控薄弱，容易出现不安全事件。

1.3 操作失误

目前，计算机系统的操作难度大大降低。一些员工只能通过简单的培训掌握相应的操作技能，导致操作人员缺乏警惕性，操作失误频发。同时，一些员工的安全意识不强，在工作期间使用不正当手段对企业内的信息系统进行访问，造成系统安全漏洞，也会影响到企业网络信息的安全。

2 企业信息系统数据安全管理与应用

2.1 注重设备设施更新

随着网络信息技术的飞速发展，新型硬件设备和软件系统层出不穷。传统的安全管理软硬件已经难以满足新形势下企业安全管理的需要。因此，有必要及时更换与网络安全相关的软硬件设备，以提高应对复杂网络攻击的水平。比如强化网络安全防护设计，对网络架构、安全运维设备等进行升级加固设计，部署安全防护设备提升安全性能。注重网络安全攻防演练，制定网络安全攻防演练详细方案，在真实的网络环境下高强度地发起网络攻击，对各系统安全防护功能进行测试，及时发现自身存在的安全漏洞和风险点并及时进行完善。

2.2 健全企业网络信息管理机制

在相关法律法规的基础上完善服务提供商的行为管理机制，防止服务提供商在利益诱惑下使用不当手段威胁用户数据安全。按照相关法律法规保证服务商能够自觉遵守自身的义务，使服务商尊重企业自身的知情权、并在企业的数据信息受到不正常攻击时发出通知，确保企业能够收

到示警。确保企业自身的知情权能够受到保护。

2.3 应用信息安全管理技术

为了保证计算机网络的安全稳定，我们可以通过不断增加技术的应用来解决这个问题，即将各种网络安全防护技术应用到计算机网络中，确保计算机网络的秩序和行为能够得到规范，同时也大大减少了各种因素的影响。计算机网络中常用的技术主要包括防火墙技术、加密技术、数字签名技术和身份认证技术。防火墙技术是最具代表性、应用最广泛的网络安全技术，由应用级网关和网络级防火墙组成。防火墙技术的不同部分具有的作用和功能各不相同。例如，为了保证网络中计算机进行数据传输时不被干扰，检查并记录传输数据的功能则由应用级网关来完成。如果是利用地址数据端口实现对网络进行控制，网络级防火墙是首选，能够有效防止、阻断各类网络安全问题。

2.4 运用代理服务器

数据安全问题主要是由于各种不安全信息和病毒进入网络系统造成的。因此，在应用企业信息系统的数据安全技术时，还应重点降低企业信息系统的数据接收压力。在这方面，可以安装代理服务器，以便在从计算机网络系统接收信息的过程中发挥缓冲作用。代理服务器可以有效减少公网IP地址的数量，减轻公网信息处理的压力，避免公网系统“超负荷”破坏带来的安全问题。代理服务器还可以实时监控网络运行，可以有效地管理不同级别的用户信息，实现用户信息管理的分散和细化，进一步保证用户信息的安全。代理服务器也存在一定缺陷，那就是在网络监管过程中无法做到获取全部用户的数据信息，但由于其在数据安全问题管理的过程中主要扮演分担压力的角色，在相关工作当中已经能起到充足的作用。

2.5 提升人员责任意识和技能水平

部分企业员工网络信息安全意识薄弱，影响了企业安全防护的效果。要注重加强网络安全管理员和用户的风险防范意识。一方面，企业要落实责任管理制度，明确个人对信息安全的责任，提高相关人员的积极性和责任感，最大限度地避免人为失误造成的安全漏洞。加强信息安全实时监控，及时纠正问题。另一方面，对于已经上岗的工作人员定期开展专业培训，通过专家授课等方式提升工作人员的网络安全防护水平。增强企业内员工的安全意识，使其自觉警惕可疑链接、不明来源软件等等。除此之外，网络安全管理人员需要加大管理力度，坚决贯彻企业内部控制管理条例，将不安全因素控制在摇篮里。定期对企业内员工进行抽查，检查其在信息安全方面的文化修养与实操能力，从根本上保证企业内信息的安全。

2.6 构建网络安全监测预警与应急处置管理机制

根据国家计算机病毒应急中心的病毒预测，做好病毒预警工作，加强网络安全信息的收集、分析和通报，通过各单位网络管理员OA网络公告，及时发布严重的计算机病毒疫情，并在OA网络的软件下载栏提供严重的计算机病毒处理工具和措施。建立网络安全风险评估和应急工作机制，制定网络安全事件应急预案，网络安全事件应急预案按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施，并定期组织演练。

结束语

综上所述，现阶段网络信息安全技术非常丰富，企业应结合自身实际需要，合理应用安全管理技术，解决企业网络信息安全问题。从实际出发，制定健全企业信息安全管理机制，规范单位内人员的具体行为，防止因人员操作失误为企业带来经济损失。同时，加强对现有安全技术的创新，应用新技术构建云安全管理体系，解决黑客攻击问题。

参考文献：

[1] 赵若冰. 局域网环境下计算机网络安全防护技术应用分析[J].电子世界，2018（17）：177-178.

[2] 徐晨莉，李国贞.局域网环境背景下的计算机网络安全技术应用研究[J].网络安全技术与应用，2014（4）：72.