计算机安全技术在企业信息管理中的应用刍议

杭州拱墅华数科技有限公司 李志强
航天科工广信智能技术有限公司 王俊飞

摘要：在竞争日益加剧的市场环境下，企业必须与时俱进，采用信息技术进行管理，改进运作方式，提升运作效率和品质。当前，信息技术的广泛运用为企业带来了机遇和挑战，如何更好地运用信息技术并使其在经营过程中发挥关键作用，对企业而言具有重大意义。本文主要探讨计算机安全技术在企业信息管理中的应用，并提出相应的措施，旨在优化信息管理效果，以供参考。

关键词：计算机安全技术；信息管理；应用措施
DOI：10.12433/zgkjtz.20233444

随着信息技术的不断发展，企业在日常管理工作中利用信息技术，有利于优化管理效果，提高管理工作的便利性，节省人力资源。对企业进行适当的信息管理，可以为决策制定提供参考，增强企业之间的信息沟通，促进企业可持续发展。

一、计算机安全技术概述

（一）计算机安全技术

技术人员可以根据计算机软硬件和重要计算数据，利用计算机安全技术落实针对性的防护管理方案，保密处理重要的机密数据，及时检测网络病毒，修补计算机系统出现的漏洞，确保信息的安全性。

使用计算机安全技术目的是保障信息安全使用，维护整体网络环境的稳定性。计算机数据数量较多，因此在信息收集阶段很容易出现数据丢失等情况，还会影响最终计算结果的精准性，造成严重损失。从这一点就可以看出，计算机安全技术发挥着重要的作用，技术水平会直接影响信息安全，因此需要注重信息安全，完善信息安全保证体系，充分发挥计算机安全技术优势，为社会经济可持续发展奠定基础。

（二）计算机安全问题

1.计算机病毒

计算机网络病毒，是指以计算机自身存在的漏洞为基础，通过各种方法生成的、隐蔽的、难以检测的信息，计算机网络病毒会直接影响信息安全，甚至引发整个系统瘫痪。计算机技术经过不断完善后，会逐渐增多计算机网络病毒的数量，例如，用户的软件下载和网络链接点击等行为都可能引入计算机病毒，侵入到计算机后台之后将会自动化操作，增加计算机CPU的运行负担，引发重要数据丢失等问题，严重侵犯用户的权利，导致网络用户蒙受较大损失。计算机病毒具有隐蔽性特征，入侵手段多样，会增加病毒防护的难度，因此需要不断升级防毒软件，更好地防范不断变化的计算机病毒。

2.黑客攻击

随着互联网的发展，电脑的应用日益普及，一些信息系统的安全性问题也日益凸显。有些犯罪分子通过电脑技术，侵入信息系统，盗取关键资料，并获得巨额利益。也有人利用互联网，骗取账号和口令，从而获得不义之财。一旦被侵入，不仅会导致资料泄露，还会损害网络用户的权益。当前，网络诈骗行为屡禁不止，不法分子通过各种各样的手段获得用户信任，盗取用户账号和密码后，会达到不法目标，损害用户的财产和权益，阻碍企业发展，影响网络环境健康发展。

3.计算机发展不成熟

现在的计算机在实际应用过程中还存在很多缺点，分散在各处，很难被发现，需要不断寻找。目前，我国计算机安全防护系统普遍存在着防御能力低下的问题，不利于保证计算机信息的安全性。除了对电脑进行维护、对电脑进行病毒定位外，相关技术人员还要不断增加自身计算机安全知识，顺应计算机发展趋势，保障计算机信息的安全性。

4.不可抗因素

在遭遇洪水、地震等自然灾害时，不仅系统稳定性难以保证，还会威胁系统的安全。不可抗力造成的后果是无法避免的，但事后可以弥补，当出现无法抵抗的情形时，需及时保护和监控计算机。当然，随着信息技术的不断进步，信息技术也面临着新的挑战。

（三）计算机安全技术的意义

1.提高企业经营管理水平

利用计算机信息技术，可以帮助企业高层管理者优化企业运营模式，也可以通过网络向用户提供各种资讯，供用户挑选，提升综合素养，从而为企业发展创造有利条件。此外，在企业内部还设置了一个电力检测设备，监控整体的运营情况，确保更好地运用计算机信息技术，提高企业的运营与管理水平。

2.推动信息技术发展

随着人们对计算机的应用日益重视，计算机信息技术的应用也日益普遍，应用要求也日益提高。当前，科技对企业的制造与经营具有重要意义，可以帮助企业提高产品的使用质量，促进企业发展。

二、企业管理中信息安全的现状

（一）终端设备审核

目前，很多企业都把重点放在了对用户数据安全上，却忽视了终端设备管理。因为不够重视用户的访问权限和操作权限没，导致用户的信息管理效果不佳，系统的安全性未能得到良好的保障。电脑、手机和平板电脑等设备的随意访问和操作，可能会因为操作人员的疏忽而造成信息泄露、数据外流。同时，由于用户的终端本身可能带有一些其他的病毒程序，当用户访问的时候，病毒可能进入到用户的计算机中，威胁用户的信息安全。所以对终端设备进行审核，有利于提高信息的安全性。

（二）网络安全问题

目前，许多中小企业缺少内部网络，影响整个网络安全。公共网络通常对用户的接入没有任何的约束，但容易威胁到企业的数据安全。网络攻击的强度直接关系到网络系统的整体安全性，仅依靠公共网络很危险，每个企业都要建立独立的内部网络，控制终端访问，减少随机访问，确保只有内部人员才可以正常访问终端设备，保障设备的安全性和可靠性，降低隐患问题的发生率。

（三）数据保护问题

在企业日常经营过程中，数据管理发挥着不可代替的作用，一方面，可以及时存储重要信息；另一方面，可以为规划管理工作奠定数据基础。在企业规划未来方向时，要确保数据的真实和可靠性，降低经营费用，辅助制定科学的工作决策，保障企业的综合发展效益。如果无法保证数据的准确性，就会导致企业作出偏离或失误的决定，出现资产损失，造成经营失败。因此，企业要对数据予以足够重视，增强数据保护和管理的意识。

（四）系统维护和管理问题

在进行信息管理时，企业要持续关注运行系统，并对其进行有效的维护和管理，主动防范漏洞或黑客攻击等情况，如果出现问题，及时进行修补，将危害降到最低。当前，许多企业都忽略了对系统的维护，为了降低费用，经常把企业信息交给系统制造商，从而威胁企业的信息安全。因此，在对网络进行系统的维护和管理过程中，需要招聘有经验的IT运营人才，成立专门的IT运营部门，维护信息安全。

三、计算机安全技术在企业信息管理中的应用

（一）在局域网中的应用

局域网是一种可以在某一区域进行信息传递的网络，具有传递信息方便、建设容易、保密性等特点，目前在企业的信息管理中得到了普遍运用。与公共网络相比，局域网的用户数量较小，可以对接入设备进行有效控制和监测，找到正在使用该设备的人员，当发生信息泄漏等问题时，可以快速找到问题根源，及时解决问题，避免引发较大的损失。在企业局域网中引入计算机安全技术，有利于增强信息管理的安全性，确保进入局域网终端设备的可靠性，减少信息外溢的情况的出现，有效保护核心信息。

（二）数据加密技术

数字加密是一种有效的信息保护手段，通过数字加密技术，可以实现对数字密码的安全性验证。计算机加密技术既能对内部消息进行加密处理，又能对用户的接入进行控制，确保用户信息安全。同时，还可以利用非对称件加密技术，进一步提高信息的保密性，合理增加信息解密难度，不给不法分子留下可乘之机，提高信息安全防护水平。

（三）入侵检测技术

入侵检测技术可以分析网络中的信息，降低黑客

入侵行为的发生率，提高信息的安全性和可靠性。例如，在信息收集阶段，需要核对收集的信息和安全日志资料，如果二者内容一致，可以继续开展后续工作，审核资料信息，找到威胁计算机信息安全的数据。信息分析主要是整理用户需要的信息，可以全面检测整体计算机环境的安全性，如果检测到危险因素，可以发挥网络安全系统的作用，并在此基础上，针对不同类型的网络攻击采取不同的防御措施，避免发生黑客入侵问题。

（四）防病毒技术

计算机系统由于自身特点，在应用中面临严重威胁。在计算机网络上，由于信息技术和大数据技术的发展，导致病毒越来越多、种类越来越复杂，加大了对电脑安全防范工作的难度。当前，对互联网的应用越来越广泛，信息化越来越普遍，在日常生活中，通过互联网完成智能化服务，导致对用户信息存储的安全性挑战越来越大。一些不法分子借助电脑技术，开展了一些违法犯罪的活动，例如，盗取用户账户、密码以及相关的个人资料等，影响了企业的信息管理，增加了财产损失，而防病毒技术可以高效拦截侵入电脑的病毒，减少由于病毒问题导致的信息混乱和丢失等情况。

（五）验证技术

验证技术也被称作计算机网络ID校检验技术，是指通过一种或多种参数校验建立统一的系统连接机制，目标是防范黑客攻击，使用户更方便地使用计算机。在用户进入系统查询和调取信息时，需要检查ID，筛选人工和机械的操作，降低病毒等入侵系统的可能性，保障信息安全。目前，验证技术在企业信息管理、网络平台等方面得到了大量使用，对提升信息的安全性和保密性具有重要作用，可以保护信息安全，维护用户和企业的权益，因此应对其加大研究力度。

（六）身份认证技术

在云计算环境下，身份鉴别是确保用户安全的重要手段。基于计算机安全存储，通过验证身份信息确保存储过程和用户访问权限的安全，保证计算机中的信息和数据不被泄露或随意篡改。例如，设定电脑的注册密码，密码由数字和字母组成，只有输入正确密码，使用者才能打开计算机，完成登录，再进行下一步操作。此外，基于云计算的个人识别技术也在各类APP中被大量运用。随着科学技术的进步，出现了多种身份认证技术，例如，指纹识别、人脸识别等，降低了密码泄露的风险。大数据时代，信息的重要性不言而言。如果未进行身份验证，不仅会威胁个人信息和企业信息的安全，还会增加黑客攻击的风险。

（七）网络数据库加密

网络数据库加密技术是计算机使用的一种安全防护手段，主要应用于金融企业等。这类企业设计大量的私密信息和数据，且各企业之间存在激烈的竞争，必须确保数据库的安全，防止外部入侵数据库。此外，还要提高信息传输过程中的安全性，最大程度上满足企业的数据安全需求，提高市场竞争力。

（八）防火墙技术

当前，网络环境较复杂，落实计算机网络安全防护的过程中开始广泛利用防火墙技术。通过开展安全筛选工作，可以避免发生非法入侵的行为，隔离不安全和无法识别的信息，保护用户计算机系统。需要注意的是，黑客入侵技术也在不断发展，必须加快计算机防火墙技术的更新换代，以更好地发挥安全防护作用。

四、结语

在当前的互联网环境中，运用现代化的科技手段对企业进行科学、系统化的管理，是企业快速发展的必由之路。通过对企业信息的合理分析，可以提升企业的管理和管理能力，推动企业乃至整个行业发展。企业在信息管理中，要充分发挥计算机安全技术的优势，在实际工作中不断加大研究力度，切实保障企业信息安全。

参考文献：

[1]齐雪.浅谈计算机信息管理技术在网络安全中的应用[J].中国新通信,2023,25(01):91-93.
[2]刘博舒.计算机安全技术在企业信息管理中的应用[J].现代工业经济和信息化,2022,12(11):93-95.
[3]柳少华.计算机信息管理技术在网络安全中的实施与应用[J].造纸装备及材料,2022,51(08):126-128.
[4]贾康炜.计算机信息管理技术在网络安全中的应用分析[J].现代工业经济和信息化,2022,12(06):106-107+169.
[5]董辰,陈玲,李桂英,等.计算机信息管理技术在维护网络安全中的应用[J].数字技术与应用,2022,40(06):228-230.
[6]郭勇.计算机信息管理技术在维护网络安全中的运用[J].网络安全技术与应用,2022(03):174-175.
[7]高慧.计算机信息管理技术在网络安全中的应用[J].信息与电脑(理论版),2022,34(05):119-121.
[8]杨鸿章,王波.探讨计算机信息管理技术在网络安全中的应用[J].网络安全技术与应用,2021(11):167-169.

作者简介：李志强（1975），男，江西省上饶市广丰区人，研究生，毕业于浙江工商大学，中级网络工程师，主要研究方向为计算机信息技术。