企业网络安全的重要性及防护策略

任江红
新疆昆仑工程咨询管理集团有限公司　新疆　乌鲁木齐　832000

摘　要：在互联网高速发展的今天，企业信息化能显著提高员工工作效率和工作质量，增强企业的核心竞争力。然而，网络安全问题也随之而来，成为企业亟待解决的重要问题。随着网络攻击方式和手段的多样化，企业网络安全不断面临各种安全威胁和挑战。因此，企业必须重视网络安全问题，适时采取防范和控制措施，提高网络安全防御能力，有效防范网络安全风险。加强员工安全意识教育、完善安全管理制度和规范、采用先进的网络防御技术工具和系统，都是企业有效应对网络安全问题的关键。只有重视网络安全、加强相关建设，才能有效保障企业的业务安全、数据安全、用户隐私以及企业的声誉和信誉。

关键词：信息化时代；企业网络安全；重要性

引言：在信息化时代，企业网络安全面临越来越多的威胁和挑战。随着技术的不断发展，网络攻击的方式和手段越来越复杂多样，企业在面对网络安全问题时更需要保持警惕和应对能力。企业的网络安全不仅关乎企业的核心业务，还涉及到企业信誉和用户隐私等敏感问题。因此，企业必须重视网络安全，采取一系列措施来保护企业网络及相关数据信息的安全性。不仅需要提高员工的安全意识，加强安全培训，还需要制定完善的安全管理制度和规定，积极采取安全措施，加强安全防御体系建设，及时处理和应对网络安全事件。只有加强企业网络安全建设，才能保障企业经营的稳定和顺利进行，更好地满足用户和市场的需求。

1 信息化时代企业网络安全的重要性

随着时代的变迁和信息技术的快速发展，企业面对的威胁也日益增加。网络安全问题已经成为当前企业所面临的一个重要挑战。网络安全不单单是针对网络系统的攻击，更是针对企业自身关键信息资料、知识产权、品牌形象、财务、生产等核心数据的安全防护。如果企业在网络安全方面不加强防范，势必会导致信息泄露、系统瘫痪、财产损失等问题的出现，严重影响企业的发展和生存。首先，企业网络安全的重要性在于保护企业重要信息。当下企业的重要信息既有储存在本地数据库中的数据文件，也有储存在网络上的视频、音频、文档等文件。存在本地的数据文件大多是企业生产经营数据，如果被黑客恶意攻击或泄露，将对企业造成无法承受的损失。而网络传输的多媒体文件是企业在广告宣传等方面重要的资料，一旦被窃取，将导致企业信誉受损。所以企业在保护重要信息资料时应适当采用加密技术等手段，切不可通过未经核实的网络渠道泄露企业重要资料。其次，企业网络安全的重要性在于保护企业品牌形象。在当今市场竞争激烈的环境下，企业的品牌形象被认为是最重要的竞争力之一。一旦品牌形象受到损害，将直接影响企业的商业信誉以及市场竞争力。而网络攻击则正是最容易损害企业品牌形象的因素，针对企业品牌形象的网络攻击有很多类型，如诋毁、抄袭、网络谣言等。因此，企业在网络营销时，应注意在网站、社交媒体上对品牌形象的保护[1]。最后，企业网络安全的重要性在于实现生产运营的稳定性。对于企业来说，生产和运营是其创造价值的主要手段，任何因网络安全问题导致的生产系统瘫痪都将给企业带来致命打击。例如黑客攻击、病毒入侵、网络故障等，不仅会使企业无法正常生产和运营，还会影响企业产品质量和客户满意度。因此企业要做好备份、灾难恢复等必要措施，确保生产系统的稳定运行。企业网络安全对于信息化时代的企业来说已经成为其生存和发展的一个重要因素。企业必须认识到网络安全问题的严重性，采取有效措施进行防范和规避，以保障企业的正常运营和发展。

2 信息化时代企业网络安全存在的问题

在信息化时代，企业网络安全正日益受到重视，但是企业网络安全问题仍然存在许多隐患。企业网络安全面临的问题不仅来自外部威胁，而且也来自内部的管理人员和技术人员等。以下是企业网络安全存在的主要问题。

2.1 企业网络安全技术体系不完善。目前许多企业的网络安全技术体系不完善，无法满足企业安全需要。企业的网络安全设备不足，很多企业的重要系统也缺乏多层次、多机房和备用设施的技术支持，难以满足长期稳定运行和复杂业务变革的需求。此外，企业应用的一些安全技术如防病毒软件、安全监控设备等也存在漏洞，

需要进一步完善相关安全技术体系。

2.2 企业网络安全人才短缺。与当今网络安全技术的复杂性和快速发展速度相比，当前企业缺乏网络安全人才和相关资源，无法满足企业安全管理的需求。 相反，大多数黑客和网络攻击者都是在网络安全技术方面具有一定知识背景的专业人员，因此企业迫切需要增强网络技术安全人才招聘、培训、引进和留住人才方面的投入。

2.3 企业员工网络安全意识不强。在企业网络安全方面，员工是既是安全威胁又是安全防御的重要环节。然而，当前在某些企业中，员工的网络安全意识并不高，不注意保密，使用简单的密码和公司公共电脑等，这使企业受到了更多的安全威胁。

2.4 企业网络安全合规管理存在问题。在企业网络环保中，合规方面的问题仍然很严重，如密码管理、准入控制、身份认证等方面的问题。此外，也有部分企业忽略了安全事件的记录、跟踪和处置等重要工作[2]。

3 信息化时代企业网络安全管理的防护策略

随着互联网和信息技术的飞速发展，企业网络安全问题日益凸显。企业在日常运营中越来越依赖数字技术、互联网和移动应用程序，这也使得它们面临着越来越多的网络安全威胁。关于网络安全的问题，企业需要始终保持其安全性，特别是保护其企业数据，以防止如此多的潜在威胁。因此，制定和实施适当的网络安全策略已经变得至关重要。下面就介绍几种有效的防护策略。

3.1 企业应制定安全策略和紧急应变预案

针对网络安全问题，企业应制定相应的安全策略和紧急应变预案。这些文件标准化和规范化了企业的网络防御策略，保护企业业务免受各种威胁。下面是两种重要的文件。（1）安全策略。安全策略是企业确定信息安全目标和标准并制定适当安全安保措施的文件。这些文件应准确记录安全目标、操作规程、评估标准以及实施控制的细节等，以确保网络安全上的稳定和预测性。安全策略的开发必须围绕承担的风险、业务需求和管理目标，针对企业所面临的不同威胁，制定相应的安全策略。其中，包括身份验证、访问控制、数据加密、威胁管理、复杂性管理、合规性和工业标准、事件响应和备份和可恢复等方面内容。安全策略制定过程中要确保所有工作人员明确了自身的职责，同时，要使用合法和标准的工具和方法，以确保产生的结果符合企业要求。（2）紧急应变预案。紧急应变预案也是企业网络安全管理中非常重要的文件。这个计划描述了紧急响应小组在面对突发事件时所需的流程和原则。这个计划会根据具体情况和事件类型来确定该如何应对。紧急应变预案应考虑针对不同类型的事件，采取不同级别的响应[3]。例如，对于数据泄漏事件，应当立即形成一个单独的团队来迅速调查、评估和解决问题。针对网络攻击事件，企业应立即启动应急响应方案，以隔离受影响区域，并进行修复和恢复操作。如果企业出现业务中断，应根据紧急部署、支援外部团队、切换到备用基础架构、进行数据恢复等操作来保障业务正常运行。

3.2 企业应采取合适的安全防御措施

企业在面对网络安全威胁时必须采取一系列的安全防御措施。以下是常用的几种安全防御措施。（1）网络访问控制：企业可以利用防火墙技术、虚拟专用网络（VPN）技术以及远程访问、无线局域网络（WLAN）等多种方式来控制网络访问。网络访问控制有助于保护重要数据和系统远离恶意的入侵者。（2）加密技术：加密技术是保护数据的重要手段。企业应该通过数据加密技术、安全套接字协议（SSL）以及传输层安全协议（TLS）等技术，保护敏感数据的隐私与完整性。（3）网络监控：企业应该使用网络安全监控和报警系统，对网络进行24小时全天候监控。这可以及早发现可能的安全问题，并有助于提供快速响应。同时，系统管理员应该对网络设备程序进行定期更新，以确保最大程度上防范潜在的安全威胁。（4）应用安全：对于现代应用程序，企业应确保有相关的安全软件和配置管理，强制使用最佳安全实践并限制用户权限。企业也可以通过测试、代码审查和其他安全审查技术来增强应用程序的传输安全性[4]。企业需要采取适当的安全防御措施以减少安全威胁和数据丢失风险。管理员应该将安全防御技术部署到企业的整个IT环境中，以确保网络安全和数据安全。此外，企业应该定期检查和评估已有的安全防御技术和方案，随着技术威胁和企业变化进行调整和改进。这种持续不断的反馈过程是确保企业网络安全和数据安全的关键所在。

3.3 企业应提高员工安全意识

员工安全意识是企业网络安全管理中不可或缺的一部分。以下是企业提高员工安全意识的一些有效方法：（1）教育和培训：企业应开展相关的网络安全培训和教育。培训内容应包括密码管理、数据备份、数据管理以及安全意识等方面。这样有助于提高员工对网络安全和数据安全的重视程度。（2）减少疏忽：员工经常会因疏忽给企业带来潜在的安全问题，如：弱密码、未锁定电脑、未切换账户等。企业应该向员工提供在日常操作中的安全提示，以减少疏忽。例如，企业可以提醒员工不随意泄露私有信息，不将密码与其他人分享，以及文档

打印后及时清理。（3）安全规则：企业应实施统一的安全规则，明晰员工在网络使用方面的限制和禁止事项。例如：禁止员工使用未经批准的应用程序或工具，禁止打开未知的邮件和链接，禁止使用违规移动存储设备存取和传输企业数据等。（4）信息保密：员工应时刻意识到保护企业保密信息的重要性。企业可以通过信息分类和权限设置，保障重要的计算机和数据设备被有意或无意的访问导致信息泄露的风险减到最小[5]。（5）实施责任制：企业需要明确的责任制，确保所有员工都有对网络安全的责任意识。同样重要的是，要根据实际安全情况和操作错误制定相应的惩罚措施。企业应该重视员工的安全意识培训和教育，明确员工的网络安全责任，确保员工按照企业的安全政策和规定进行工作，减少安全漏洞的发生和最大程度上保障网络及数据安全。

3.4 企业应对安全事件进行及时的监测、记录和分析

企业应对安全事件进行及时的监测、记录和分析以及建立事件响应机制。以下是企业要做好安全事件监测、记录和分析方面的一些建议:（1）监测安全事件：企业应在系统中使用安全日志管理，以提供准确的可追溯性和完整可验证性的数据记录。对于网络和系统报警，企业应建立实时监控机制，以便立即发现，及时报警，迅速处置才行。（2）记录安全事件：企业应建立完善的安全事件记录流程，并在记录流程中包含事件详情，时间，地点，相关人员和设备等信息。（3）分析安全事件：企业应对事件记录进行分析，确定事件的原因和影响，以便在将来加强相关的安全防范措施。（4）建立事件响应机制：企业应当先建立初步的安全事件响应预案和组织事件响应团队。在事件发生之后尽快进行调查，确定导致事件的原因，并在保持安全控制的情况下努力恢复良好状态，避免企业遭受二次攻击和损失的进一步扩大。（5）实时更新和完善安全策略：企业应根据事件结果及时更新和完善企业的安全策略，为今后的安全管理奠定基础。企业应建立完善的安全事件管理机制，确保监测、记录和分析安全事件，并建立相应的响应和处理策略[6]。这些措施将帮助企业防止安全漏洞和网络攻击，及时消除安全隐患，或者在未产生大的损失情况下，把企业对更坏的局势转化为具体有助于缓解风险带来的小胜利。

结束语

随着信息技术的迅速发展，企业网络已成为日常工作和运营的关键支撑。随之而来的是，网络安全问题也日益突出。企业网络的安全问题不仅会给组织的核心业务造成巨大的影响，还可能导致公司在外部市场上的声誉受到损害。网络安全问题涉及数据泄露、业务干扰、网络攻击等多种形式。为了确保企业的数据和软件安全，企业必须重视网络安全威胁，积极采取安全措施，强化安全意识，提高防御能力，制定完善的安全管理制度和规定。同时，企业应该做到员工持续性的安全培训，及时加强和更新防御系统和技术，对安全事件进行监测和处理。企业网络安全关乎企业未来的发展，是企业经营稳定的重要保障，也是企业确保安全经营和用户信息安全的重要前提。

参考文献

[1]唐文平.网络安全技术在企业信息化领域的发展研究[J].电脑知识与技术,2021,17(14):26-27.

[2]王爱鹏.数字化企业应对信息安全挑战[J].中国仪器仪表,2020(06):28-31.

[3]王海.现代企业信息网络安全优化研究与应用[J].硅谷，2020，(23):88+65.

[4]雷涛.中小企业的信息网络安全与防护[J].华南理工大学，2020.

[5]马涛.试谈大数据时代的计算机网络安全及防范措施[J].网络安全技术与应用，2020(12):11-12.

[6]郑英杰.企业信息化安全问题及其网络管理优化方案浅谈[J].山东工业技术，2019(05)：165.