聚知刊出版
JZK publishing

人力资源数据泄露的计算机防御策略探析

赵晓伟

中南财经政法大学，湖北省武汉市，430073；

摘要：为探讨人力资源数据泄露的风险及其防御策略，本研究通过分析内部威胁、外部攻击和技术漏洞等主要风险来源，深入剖析了数据泄露的具体表现和潜在影响，并综合提出了企业在防御人力资源数据泄露方面的策略。研究认为完善的访问控制、先进的网络安全技术、持续的安全意识培训以及有效的风险评估与改进机制，均能防止数据泄露。企业应综合运用多种防御策略，建立全面的安全管理体系，以有效抵御多样化的安全威胁。

关键词：人力资源数据泄露；计算机防御策略；风险分析

DOI：10.69979/3029-2700.24.3.009

引言

在信息化时代，人力资源管理系统中包含了大量敏感的个人和财务信息，数据的安全性已成为企业管理中的关键问题。随着数字化转型的加速推进，数据泄露事件的频发不仅对企业的正常运营构成威胁，还对员工的隐私和权益产生了深远影响。为此本文将深入探讨人力资源数据泄露的多种风险因素，并提出一系列针对性的防御策略，以期为企业构建更加稳固的信息安全屏障提供理论支持和实践指导。

1 人力资源数据泄露的风险及影响

1.1 内部威胁

内部威胁是人力资源数据泄露的主要风险之一。具备数据访问权限的员工可能出于个人利益、报复心理或疏忽大意导致敏感信息泄露。HR 部门员工由于工作需要通常拥有较高的系统权限，若滥用权限或未遵守数据保护规定，可能造成大规模数据泄露。离职员工的访问权限未及时撤销也是潜在的安全隐患，他们可能利用仍然有效的凭证非法访问或窃取数据。内部人员熟悉公司的 IT 基础设施和安全措施，更容易绕过安全控制。随着远程办公和 BYOD（自带设备办公）政策的普及，员工在个人设备上处理敏感数据的情况增多，增加了数据外流的风险。

内部威胁往往难以及时发现，通常会在造成重大损失后才被察觉。泄露的数据可能包括员工个人信息、薪资数据、绩效评估、人事决策等核心信息，不仅严重损害公司声誉和员工信任，还可能引发法律纠纷、监管处罚和巨额赔偿。内部数据泄露还会导致商业机密外流，影响公司的市场竞争力。此外，内部威胁可能与外部攻击相结合，内部人员有意或无意地协助外部攻击者，大大增加了防御难度和潜在损失。

1.2 外部攻击

因 HR 系统包含大量有价值的个人和财务信息，黑客和网络犯罪分子经常将其作为攻击目标，常见攻击手段包括网络钓鱼、恶意软件、暴力破解、SQL 注入和社会工程学等。攻击者会通过发送精心设计的钓鱼邮件，诱导员工点击恶意链接或附件，从而窃取登录凭证或植入恶意软件。一旦成功入侵，攻击者会在系统中植入后门程序，获取长期的数据访问权限。弱口令和多因素认证的缺失使得暴力破解攻击成为可能。社会工程学攻击则利用人性弱点，通过伪装、欺骗等手段获取敏感信息或系统访问权限。高级持续性威胁（APT）攻击具有长期性和隐蔽性，可能在系统中潜伏多时，持续窃取数据。

大规模数据泄露事件频发，造成的经济损失和声誉损害往往是灾难性的。被盗的 HR 数据可能会在暗网上出售，用于身份盗窃、金融诈骗等犯罪活动，给受害者带来长期困扰。外部攻击还会导致系统瘫痪或数据加密勒索，严重影响企业正常运营。成功的外部攻击还会暴露公司的安全漏洞和合规问题，引发监管调查和处罚。

1.3 技术漏洞

技术漏洞是人力资源数据泄露的重要风险来源，涉及软件系统、网络基础设施和安全配置等多个方面。过时的 HR 管理系统存在已知的安全漏洞，若未及时更新修复，极易被攻击者利用。软件开发过程中的编码错误会导致 SQL 注入、跨站脚本（XSS）等安全漏洞，使攻击者能够非法访问或操纵数据库。不安全的数据传输和存储方式，如使用明文传输敏感信息或采用弱加密算法，增加了数据被窃取和篡改的风险。访问控制机制不当，如权限设置过于宽松或缺乏最小权限原则，导致越权访

问和数据泄露。不完善的身份认证机制，如单因素认证或会话管理缺陷，为攻击者提供了可乘之机。日志记录和监控系统的不足使得异常行为难以及时发现和溯源。云服务的不当配置，如错误的访问权限设置或公开的存储桶，导致数据意外暴露在互联网上。移动设备和远程访问带来的新型安全挑战，如设备丢失、不安全的 Wi-Fi 连接等，增加了数据泄露的风险。网络架构设计不当，如缺乏有效的网络分段，会导致攻击者突破外围防御后可以自由访问内部资源。

2 人力资源数据泄露的计算机防御策略

2.1 防范内部威胁的策略

实施严格的访问控制应基于最小权限原则为员工分配数据访问权限，确保员工只能访问履行职责所需的最小数据集。通过身份和访问管理（IAM）系统的集中化用户身份验证与授权管理，结合多因素认证技术，提高认证安全性。同时，需要定期对权限设置进行审核和更新，确保及时撤销离职员工的系统访问权限，以防潜在的数据泄露风险。

数据的分类和标记、对敏感数据的加密存储与传输，是保护关键信息的另一重要环节。数据泄露防护（DLP）系统能有效监控和阻止敏感数据的未授权传输，从而减少企业面临的安全威胁。全面的日志记录与审计机制的建立，允许追踪所有数据访问和操作活动，通过用户和实体行为分析（UEBA）技术可以有效检测并应对异常数据访问模式。

在数据传输过程中，使用加密技术防止信息被窃取。通过终端安全管理措施限制员工在非官方设备上存储和处理敏感数据，降低因个人设备引起的安全隐患。为强化员工的责任意识，公司还需制定严格的数据保护政策，规定在处理敏感信息时的具体责任与义务，且通过持续的安全意识培训，提升员工对数据保护的认识与重视。建立内部举报机制促使员工积极参与安全保障，通过报告可疑行为，协助企业及早发现和处理安全事件。进行职责分离避免单一员工掌握过多的权限，从而降低内部人员对安全威胁的影响，同时进行定期的内部安全审计和渗透测试以评估现有安全措施的有效性，协助企业不断调整和优化安全策略。

2.2 抵御外部攻击的策略

在构建有效的网络安全防护系统中，企业必须实施一系列先进的技术措施。在网络边界部署新一代防火墙与入侵防御系统（IPS），阻止已知攻击模式和过滤恶意流量。通过网络分段技术，将关键的人力资源系统与其他网络区域隔离，可降低攻击者的横向移动能力，从而加强网络的整体安全性。Web 应用防火墙（WAF）有利于保护人力资源门户网站免受如 SQL 注入和跨站脚本（XSS）等常见的网络攻击。安全邮件网关和反垃圾邮件解决方案则可以有效地过滤钓鱼邮件和恶意附件，减少因电子邮件传递带来的威胁。为加强用户账户的安全性，企业也应强制实施强密码策略和定期更换密码，结合多因素认证增强账户保护。实施高级威胁防护（ATP）解决方案，利用机器学习与行为分析技术，识别并阻止复杂的攻击行为。通过加密措施以实现数据传输和存储的安全保护，同时使用虚拟专用网络（VPN）保证远程访问的安全性。在终端设备上，采用终端检测与响应（EDR）系统进行实时监控并响应潜在威胁，提升端点安全。

建立安全运营中心（SOC），为企业提供持续的网络活动监控与实时安全事件响应能力。实施漏洞管理程序，包括定期漏洞扫描与及时修复，以确保技术环境适应持续变化的威胁景观。还需定期进行安全意识培训，帮助员工识别并防范钓鱼攻击及其他社会工程学威胁。进行网络访问控制（NAC）策略以限制未经授权的设备接入，通过沙箱技术在隔离环境中分析可疑文件和链接，阻止恶意软件的侵入。在模拟的攻击环境中，利用渗透测试和红队评估识别并弥补安全漏洞，进一步加固企业的网络防御体系。

2.3 修补技术漏洞的策略

建立全面的漏洞管理流程，包括定期的漏洞扫描、风险评估、修复优先级排序和修复验证。使用自动化的漏洞扫描工具，定期对 HR 系统、数据库和相关基础设施进行全面扫描吗，针对已知高危漏洞，进行及时应用安全补丁和更新，对于无法立即修复的漏洞，采取临时的缓解措施，如网络隔离或访问限制等。定期审核和优化系统配置包括禁用非必要服务和端口及移除默认或弱密码，以保证系统安全性；实施安全开发生命周期（SDLC）确保软件开发过程中安全措施的整合，同时使用静态与动态应用程序安全测试（SAST 和 DAST）工具识别和修复应用程序中的安全缺陷。加强数据库安全，如实施最小权限原则、数据加密及审计日志的启用，以防止数据被非法访问。企业还应定期评估和更新加密算法和安全协议，确保符合最新的安全标准。建立身份验证机制如多因素认证和单点登录（SSO），提高访问控制的安全层级。实施网络架构的优化和深度防御策略，

如 DMZ 的使用和网络分段，进一步提升安全防护能力。采用容器化和微服务架构提升系统的隔离性，增强系统的可维护性。通过持续监控和日志分析以确保安全事件能够被及时识别和处理。建立定期的安全配置审核和供应商管理流程，保证所有系统和设备以及第三方软件和服务均遵循最佳安全实践，通过虚拟补丁技术使企业在正式补丁发布前有效缓解高危漏洞的风险。

3 防御策略实施与持续改进

3.1 防御策略实施步骤

实施防御策略需要系统性的方法和分阶段的执行计划。组织需要成立专门的项目团队，包括 IT 安全专家、人力资源管理人员和高级管理层代表，以全面评估当前安全状况，识别关键资产和潜在威胁。基于评估结果，制定详细的实施计划，明确各项措施的优先级、时间表和资源需求。实施计划应包括技术措施和管理措施的配套实施。

在技术层面，从网络架构优化开始，实施网络分段和访问控制。部署新一代防火墙、入侵检测系统和 Web 应用防火墙，加强网络边界防护。升级身份认证系统，实施多因素认证和单点登录。部署数据泄露防护系统和加密解决方案，保护敏感数据。实施终端安全管理，包括终端检测和响应系统的部署。建立集中化的日志管理和安全信息事件管理（SIEM）系统，提高威胁检测和响应能力。

在管理层面，制定和更新相关政策和流程，如数据分类政策、访问控制策略和事件响应计划。开展全员安全意识培训，确保员工理解和遵守新的安全措施。建立安全运营中心，负责日常的安全监控和事件处理。实施变更管理流程，确保新系统和更新的安全部署不会影响业务连续性。建立供应商管理流程，评估和管理第三方风险。在实施过程中，采用阶段性方法，先在小范围内试点，然后逐步推广。每个阶段结束后进行效果评估和必要的调整，同时建立定期的安全审计机制，验证各项措施的有效性。制定应急响应预案并定期演练，提高组织应对安全事件的能力。建立度量指标体系，持续监控和评估安全防御体系的效果。

3.2 风险评估与持续改进

企业在构建有效的安全管理体系中，必须实施全面而持续的风险评估与改进机制，涵盖技术、人员和流程三大关键方面。定期进行全面风险评估，至少年度一次，并在重大变化后立即进行额外评估，确保及时识别与响应新的安全挑战。技术评估涉及持续的漏洞扫描、定期的渗透测试及安全配置审查，利用自动化工具以确保技术措施的有效性与时效性。

人员安全评估聚焦于内部威胁的分析，审视员工的安全意识与安全政策的遵守情况，从而从人员角度降低风险。流程评估则确保安全政策、事件响应流程及业务连续性计划的适当性与执行力，使这些流程能够在安全事件发生时提供必要的支持。基于评估结果，企业应识别安全控制的差距，制定包含短期至长期目标的详尽改进计划，优先解决高风险问题，同时考虑安全需求与业务需求的平衡。

利用安全信息和事件管理系统（SIEM）对安全数据进行收集和分析有助于识别新兴威胁和攻击模式。同时，通过与行业伙伴和安全组织共享威胁情报，可以加强对新兴安全挑战的理解和准备。随着云计算、物联网和人工智能等新技术的广泛应用，定期评估这些技术的安全影响并调整防御策略，确保技术部署的安全性。定期审查和更新安全政策和程序以适应当前的安全需求和威胁环境，同时实施安全成熟度模型以评估和指导组织的长期安全策略。

结论

人力资源数据的泄露防御策略必须基于对内部威胁、外部攻击和技术漏洞的深刻理解，并结合具体的防御措施加以实施。从构建完善的网络安全架构到优化访问控制机制，每一项策略都应围绕着数据保护的核心目标展开。未来应注重动态风险评估与持续改进，以应对不断变化的安全威胁环境，保障信息安全的长远稳定。

参考文献

[1]罗雅过.基于 Web 的高校人力资源管理系统的安全体系研究[J].陕西教育（高教版）,2012(9):104-104.
[2]马腾.基于信息融合的企业网络安全威胁态势智能感知方法[J].计算机应用文摘,2024,40(13):96-98.
[3]吕敬兰.数据加密技术在计算机网络信息安全中的应用[J].科技创新与应用,2024,14(18):185-188.
[4]迟晓临,杨毅.数字化信息技术在人力资源管理系统中的创新应用[J].集成电路应用,2023,40(10):386-387.

作者简介：赵晓伟（2000.1.3-），男，汉，吉林，本科，研究方向：管理科学与工程。