2024年数据泄露调查报告 (DBIR) 阅读笔记

引言

2024年数据泄露调查报告 (DBIR) 是该系列的第17版，旨在深入分析网络安全事件的各个方面，包括参与者、策略以及攻击目标。报告通过全球多方合作和Verizon威胁研究咨询中心 (VTRAC) 团队的努力得以完成。今年的报告分析了30,458起安全事件，其中10,626起确认发生数据泄露，这一数据创下新高，受害者分布在94个国家。

发现摘要

报告识别出网络安全领域的几个关键趋势。零日漏洞的利用，如影响MOVEit的漏洞，依然普遍存在，同时也有更多常规但有效的攻击方式，如勒索软件和拒绝服务 (DoS) 攻击。人类因素依旧在网络安全中扮演重要角色，如保护不当的密码导致了安全复杂性的增加。

结果与分析

VERIS 行动者

数据泄露的行动者主要分为外部、内部和合作伙伴。外部行动者是大多数泄露事件的主要责任方，他们采用各种策略来获取系统的未经授权访问。内部行动者，通常出于经济动机，有时会与外部行动者合谋，从而在数据泄露中扮演重要角色。

VERIS 行动

恶意行动者的行动包括黑客攻击、恶意软件、社会工程、滥用、物理行为和错误。拒绝服务 (DoS) 攻击在事件行动种类中排名第一，占记录事件的59%。勒索软件与敲诈相结合构成了相当大比例的事件。报告强调了错误和电子邮件作为泄露向量的增长，粗心大意和欺骗（通常导致商业电子邮件泄露或BEC）变得更加常见。

VERIS 资产

这些行动的主要目标是服务器、用户设备和网络设备。这些资产的泄露往往导致重大数据泄露，数据被外泄或系统被破坏。保护和监控这些资产对于防止泄露至关重要。

VERIS 属性

泄露主要影响机密性、完整性和可用性。通过暴露敏感数据导致机密性丧失是最常见的结果，其次是通过未授权数据更改导致的完整性丧失和通过拒绝服务 (DoS) 攻击导致的可用性丧失。

事件分类模式

报告将事件分类为几种模式：

1. **系统入侵**：利用漏洞获取系统的未经授权访问。
2. **社会工程**：包括钓鱼、欺骗和其他诱骗个人泄露敏感信息或执行破坏安全的操作的策略。
3. **基本的网络应用攻击**：攻击网络应用以窃取数据或破坏服务。
4. **杂项错误**：导致安全事件的人为错误。
5. **拒绝服务 (DoS)**：破坏系统或服务可用性的攻击。
6. **遗失和被盗资产**：包含敏感数据的设备的物理盗窃或丢失。
7. **权限滥用**：滥用合法访问权限以破坏数据或系统。

行业分析

报告对各行业的数据泄露进行了深入分析：

- **住宿和食品服务业**：由于金融交易和客户数据量大，频繁成为攻击目标。
- **教育服务**：易受到攻击，利用安全措施不完善的弱点。
- **金融和保险**：由于处理敏感金融数据，高价值目标。
- **医疗保健**：由于患者数据的敏感性而处于风险中。
- **信息行业**：经常被攻击，因其持有宝贵的数据和知识产权。
- **制造业**：易受工业间谍活动和操作中断的影响。
- **专业、科学和技术服务**：因宝贵的知识产权和客户数据而成为目标。
- **公共行政**：面临来自内部和外部行为者的威胁，动机通常为间谍活动或经济利益。
- **零售业**：由于金融数据和客户信息而成为攻击目标。

地区分析

报告还包括地区分析，突出事件和泄露的地理分布。不同地区面临的威胁格局各不相同，受监管环境、网络安全成熟度和流行的网络犯罪活动类型影响。

结论

2024年DBIR突显了网络安全格局的动态性。虽然某些威胁保持不变，但新的和创新的攻击不断涌现。组织必须保持警惕，适应网络犯罪分子不断演变的策略。报告强调了综合性安全策略的重要性，结合强大的技术防御与全面的安全政策和用户教育。

详细观察

内部行动者的动机和方法

员工窃取数据的主要动机是经济利益，通过直接的金融犯罪或利用被窃数据在新工作中获益。间谍活动是另一个动机，员工可能将数据带到竞争对手处或用来开办自己的企业。尽管内部和外部行为者合谋的事件有所减少，内部威胁仍然显著。个人数据、内部数据和银行信息是内部行为者最常见的目标。

商业电子邮件泄露 (BEC)

BEC依然是主要威胁，涉及欺骗的事件占了大量的经济动机攻击。在BEC事件中，交易中位数约为5万美元。尽管对网络钓鱼的意识和报告增加，但用户点击恶意链接的速度仍然令人担忧，这凸显了持续安全意识培训的必要性。

勒索软件和敲诈

勒索软件仍然是普遍的威胁，通常伴随着敲诈要求。尽管勒索软件事件的总体发生率有所下降，但勒索软件与敲诈的结合仍然是一个重大问题。攻击者利用漏洞并使用社会工程方法渗透系统，强调了强大的漏洞管理和事件响应计划的必要性。

拒绝服务 (DoS) 攻击

DoS攻击仍然是最常见的事件类型，破坏服务的可用性，造成重大运营和财务影响。组织需要实施有效的DoS缓解策略以防止这些破坏。

安全措施和最佳实践

报告建议采用若干安全控制措施来减轻风险，包括管理访问、确保配置安全以及实施强有力的账户管理流程。这些措施对于防止未经授权访问和保护敏感数据至关重要。

未来展望

报告总结呼吁网络安全社区将重点从单个漏洞转移到解决软件缺陷类别的反复出现上。这个战略方法旨在提高技术开发的整体安全性，使系统更能抵御已知和新兴的威胁。

最终思考

2024年DBIR为不断演变的网络安全格局提供了宝贵的见解。通过了解网络犯罪分子的策略和动机，组织可以更好地准备和防御数据泄露。不断改进安全实践，结合意识和教育，是在当今数字世界中减轻风险、保护敏感信息的关键。