好莱坞艳照门

工程伦理分析报告

**姓 名**： 周林犷

**班 级**： 工程伦理14班

**学 号**： 2112333047

**学 院：** 网络空间安全学院

**授课教师**： 张登辉

2024年6月27日

好莱坞艳照门

|  |  |
| --- | --- |
| 研究生姓名：周林犷 | 学号：2112333047 |
| 所在专业：计算机技术 | 研究生所在学院：网络空间安全学院 |
| 递交课程老师姓名:张登辉 | 评分（百分制）： |
| 课程名称：工程伦理 | 评分教师签名： |

目录

[1 事件经过 1](#_Toc130453607)

[2 事故产生的原由 1](#_Toc130453608)

[3 伦理剖析 2](#_Toc130453609)

[4 教训与总结 2](#_Toc130453610)

[5 相关防患的创新思路 3](#_Toc130453611)

[6 参考文献 3](#_Toc130453612)

# 

# 1 事件经过

**1.1背景**

近年来，随着数字化转型的深入推进和新兴技术的不断涌现，云服务将渗透到更多的行业和领域，为人们的生产生活提供更加便捷、高效、智能的服务。

云计算服务也面临诸多挑战，如云计算技术基础平台安全性、云上数据的安全管理、云计算服务安全专业人才匮乏等安全风险问题，导致云平台数据安全事件层出不穷

**1.2 事故情况**

2014年9月1日，有境外媒体报道，多位好莱坞女星的私密照在社交网站Reddit上疯传。新闻报道之后，相关照片、视频的传播迅速漫延至国内，刚开始大部分人对照片的真实性提出了质疑，但随着越来越多女星的艳照被曝出，怀疑逐渐消失，人们意思到这是一次隐私数据的泄露，经过调查发现这些照片大多来自于苹果公司的icloud云服务系统。

**1.3 事故处理**

在事件发生后Reddit公司第一时间关闭了相关的子聊天板块以避免内容被进一步传播。

苹果公司第一时间对其云服务展开调查并发表声明表示并非是安全漏洞而是黑客的蓄意攻击从而导致用户隐私数据的泄露。苹果之后对其云服务安全进行了升级，扩大了iCloud端到端加密的范围。

美国FBI展开了近一个月的调查，最终成功将相关黑客和泄露者抓获。

# 2 事故产生的原由

**2.1 云服务安全的定义和原理**

云安全是专门保护云计算系统的网络安全学科。这包括在基于在线的基础架构、应用程序和平台上保持数据的私密和安全。保护这些系统需要云提供商和使用它们的客户的努力，无论是个人、中小型企业还是大企业使用。

云提供商通过始终在线的互联网连接将服务托管在其服务器上。由于他们的业务依赖于客户的信任，因此使用云安全方法来确保客户数据的私密和安全存储。但是，云安全也部分掌握在客户手中。理解这两个方面对于健康的云安全解决方案至关重要。

**2.2 事故原因**

调查发现，当时一名黑客在Github上载了一个iCloud的暴力破解工具，绕过“Find My iPhone”的安全系统，经过暴力破解工具上万次无脑尝试成功破解，之后，黑客就凭借着这个破解工具，攻破了一百多位女星的iCloud账户，从中窃取了200多张好莱坞知名女星的不雅照，在之后这些不雅照在一个“名人艳照分享”的小圈子里面流出，再之后有人将这些照片进行交易和出售，由于流通范围越来越大最终这些照片在Reddit网站上被完全公开。

# 3 伦理剖析

**3.1 伦理与法律问题**

伦理问题：苹果公司在隐私泄露后第一时间发表声明声称并非安全漏洞而是蓄意攻击来以次撇清关系，但在之后苹果iCloud仍然出现了小规模的隐私泄露，这使得苹果公司不得不扩大了iCloud端到端加密的范围。这也间接证明了苹果的iCloud服务确实存在安全漏洞，但苹果公司这种不主动承担责任的表现致用户对公司的信任度和满意度下降。

法律监管：根据《网络安全法》，公司企业因有责任保护用户的数据安全，iCloud作为艳照泄露的源头，苹果公司应承担起相关的法律责任。

**3.2 工程师和公司的伦理责任**

在云服务安全中，工程师和公司承担着不容忽视的伦理责任。

公司应确保用户数据的保密性、完整性和可用性，透明化数据收集、存储和使用过程。向用户清晰说明数据的用途，不滥用用户数据，不将数据出售给第三方或用于未经授权的目的，在涉及用户隐私的决策中，优先考虑用户的利益和权利。

云服务工程师应该开发和维护安全的系统，确保设计和实现符合最佳安全实践，在发现潜在安全漏洞时，及时报告并采取措施修复，对公司和用户保持透明，明确沟通安全措施和潜在风险，在涉及用户数据和隐私的决策过程中，积极参与并提供技术建议，确保决策的伦理性。

# 4 教训与总结

**4.1教训总结**

对于云服务提供商来说，做好数据安全至关重要，一旦服务器由于黑客入侵导致用户数据泄露，其结果都是灾难性的，这将造成成千上万的用户信息泄露。如果是由于服务提供商的问题导致，企业有面临集团诉讼甚至破产的可能。

对于云服务用户来说，应具备一定的网络安全知识从而能够避免一些黑客的钓鱼陷阱。

**4.2 反思与改进**

云服务提供商应做到对用户的数据安全负责，而不是撇清关系降低用户的信任度，定期进行安全审计和漏洞评估，及时修补安全漏洞。

用户应该提高数据的保护意识，在使用云服务时应尽量避免使用私密数据，妥善管理云服务帐号密码，小心使用公共场所的网络，避免下载下载危险程序。

在法律监管方面应制定和完善全面的数据保护法律，确保平台对用户数据的收集、存储、处理和分享进行严格规范，设立专门的云安全监管机构，负责监督云服务提供商的合规性和安全性，明确云服务提供商和用户在数据安全方面的法律责任，对违规行为进行严厉处罚。

# 5 事故相关防患的创新思路

**5.1 对于开发者**

思路：通利用AI和ML算法分析海量数据，过学习用户的正常行为模式，检测异常活动，及时发现和阻止内部威胁和恶意行为。扩大端到端加密范围，确保数据在传输和存储过程中始终加密，只有授权用户才能解密和访问数据

关键技术：用户行为分析、数据加密、机器学习

**5.2 对于使用者**

思路：在将数据上传到云端之前，在本地进行加密处理，确保即使数据泄露，攻击者也无法读取。使用行为分析工具监控账户活动，检测异常行为，如突然的大量数据下载或非正常时间的登录，使用一些云访问的安全工具监控和控制云应用的使用，保护数据安全，防止数据泄露。

关键技术：使用云安全工具、使用行为分析工具、本地数据加密

# 参考文献

[1]腾讯云.(2023).云安全 https://cloud.tencent.com/developer/techpedia/1562

[2]人民网.(2014). 好莱坞女星艳照门引爆 金山毒霸截获相关病毒. http://it.people.com.cn/big5/n/2014/0901/c1009-25582128.html

[3]网易新闻.(2022).苹果决定了，要彻底封杀“艳照门”！. <https://m.163.com/dy/article_v2/HOLA0TCO0550PLRZ.html>

[4]知乎.(2014). 好莱坞 iCloud 艳照门给我们什么警示？. <https://www.zhihu.com/question/25080182/answer/30031413?utm_psn=1789602167419719681>

[5]中国人大网.(2016)中华人民共和国网络安全法. <http://www.npc.gov.cn/zgrdw/npc/xinwen/2016-11/07/content_2001605.htm>

[6] cioctocdo.(2022).【美国数据隐私法】数据隐私法：2022年你需要知道的. https://www.cpo.work/data-privacy-laws-what-you-need-know-2022