Equifax数据泄露事件深度分析报告

angel010 / 2018-02-18 23:03:23 / 浏览数 9151 技术文章 技术文章 顶(1) 踩(0)

背景

Equifax是美国最大的征信机构之一。2017年9月，Equifax被暴泄露超过1.45亿的美国公民个人隐私信息，这是美国历史上最大规模和影响的数据安全事件。更多关于该数据

摘要

在Equifax承认数据泄露之后，Elizabeth Warren议员办公室就对该事件的起因、影响和响应进行了调查。

1. Equifax的预防和解决数据安全问题的方案存在缺陷。

数据泄露的原因是因为Equifax公司使用的网络安全方案没有足够的能力来保护消费者的数据。该公司没有选择最合适的网络安全方案并且没有遵循防止和缓解数据泄露影响Struts中存在漏洞，可以用来入侵系统，然后邮件通知职员来修复该漏洞，但是最终没有确认该补丁。之后的扫描只评估了Equifax公司系统的一部分，也没有找出Apache Struts漏洞是否修复。

2. Equifax 忽视了大量关于隐私数据威胁的警告。

其实Equifax意识到了系统的脆弱性和风险。Equifax收到了国家安全部发来的关于黑客用来入侵该公司系统的漏洞的告警消息。在这次大规模数据泄露前，Equifax还遭遇过

3. Equifax没有以一种及时、有效的方式向客户、投资者和管理者通告数据泄露事件

数据泄露事件发送在2017年5月13日，Equifax在7月29日就发现了一些线索。但是直到公司确认数据泄露后40天才向客户、投资者和管理者通告数据泄露事件。因为Equifa

4.Equifax利用了联邦合同的漏洞，没能适当地保护敏感的IRS（美国国内税务局）纳税人数据

在公布了数据泄露事件后，Equifax和IRS就被关于即将签署的720万美元的合同的新闻所淹没。Senator Warren的调查发现Equifax公司利用合同的漏洞迫使IRS签署了合同，该合最终在IRS得知Equifax的安全能力可能危及纳税人数据时被及时取消了。

5.Equifax在数据泄露后提供给消费者的帮助和信息是不够的

Equifax公司40天后才公布数据泄露事件，也就是说用了40天时间来准备如何应对公众的质询；即使延迟了40天时间，也没有进行适当的回应。因此，可以得出结论Equifax

6.联邦立法可以预防未来的数据泄露和对此类事件的响应

Equifax和其他的征信机构在没有授权的情况下手机了消费者的数据，而消费者无法阻止数据被该企业收集和拥有，而企业更加关注的是自己的利润和增长，而不是如何保护2）授权联邦交易委员会确立基本的标准来确保征信机构能够对消费者数据进行合理保护。

发现

在Equifax承认数据泄露之后，Elizabeth Warren议员办公室就对该事件的起因、影响和响应进行了调查。

A. Equifax的预防和解决数据安全问题的方案存在缺陷

1. Equifax公司使用的网络安全方案没有足够的能力来保护消费者的数据安全

调查发现数据泄露的原因是因为Equifax公司使用的网络安全方案没有足够的能力来保护消费者的数据。网络信心安全的优先级比较高，CEO Richard Smith说在网络信息安全的预算约占3%，而同期对股东的分红大约是6%。

Senator Warren咨询的网络安全专家说像Equifax这样拥有隐私数据的公司应该有多层的网络安全方案。Equifax应该：

（1）经常更新安全工具来预防黑客入侵系统；

（2）应该有限制黑客在入侵系统内进行相关活动的措施；

（3）在系统入侵后能限制对敏感数据的访问；

（4）监控和记录所有非授权访问的程序，能够尽快地停住入侵
调查同时发现了Equifax公司网络安全方案的弱项：

补丁管理程序。对于软件和应用中的许多漏洞，Equifax只使用了软件补丁来秀股漏洞，并限制对易受感染系统的访问。同时发现，无数的软件漏洞修复的时间长达几个月，Struts漏洞，Equifax并没有有效地使用简单、低成本的补丁来保护消费者数据。比如，使用邮件通知职员修复该补丁，但并不是所有职员都收到了该邮件。之后的扫描只评Struts漏洞是否修复。

对终端和邮件安全的无力的监控。黑客常会利用系统中某个消费者的安全漏洞来黑进系统，比如通过邮件的鱼叉式攻击。为了检测系统中的攻击，必须能够监控笔记本和其

敏感信息泄露。除了没有严格的终端和邮件安全措施，Equifax还没有采取有效的措施来确保敏感信息安全。比如，当银行晚上关门后，不会把现金留在柜台，而是会锁在保
Struts漏洞获取Equifax系统的权限后，就发现了一个客户信息库。

网络分段脆弱。Equifax没有预防黑客从不安全的直面互联网的系统跳转到含有更加有价值的数据的后台系统的安全措施。企业的网络分段措施没能采取适当的措施来阻止攻

不适当的证书授权。Equifax系统中的每个消费者都有一些适当的权限。在一个严格的安全标准下，Equifax会限制消费者对重要数据系统的访问，这让公司免受内部攻击。但

日志记录。Equifax没有采用健壮的日志记录技术，该技术可以将黑客从系统中驱除，并且可以限制数据泄露的大小和范围。日志不能预防系统入侵或数据泄露事件，但是在

2. Equifax 忽视了大量关于隐私数据威胁的警告

Equifax在数据泄露事件前就收到很多关于系统的潜在风险和脆弱性的警告。Equifax收到了国家安全部发来的关于黑客用来入侵该公司系统的漏洞的告警消息。在这次大规模

B. Equifax没有以一种及时、有效的方式向客户、投资者和管理者通告数据泄露事件

Equifax在2017年3月8日就意识到可能导致数据泄露的漏洞，而数据泄露事件发生在2017年5月13日，Equifax在7月29日就发现了一些线索。但是直到公司确认数据泄露后

C. Equifax利用了联邦合同的漏洞，没能适当地保护敏感的IRS（美国国内税务局）纳税人数据

近年来，Equifax与IRS签署了很多商业采购合同。调查发现，Equifax利用联邦采购法的漏洞来获取补充合同，将纳税人数据置于威胁中。在公布了数据泄露事件后，Equifa
Warren的调查发现Equifax公司利用合同的漏洞迫使IRS签署了合同，该合最终在IRS得知Equifax的安全能力可能危及纳税人数据时被及时取消了。

截止目前，尚未发现此次数据泄露事件中有任何IRS数据泄露。

D. Equifax在数据泄露后提供给消费者的帮助和信息是不够的

2017年9月7日，Equifax公布了数据泄露事件，CEO写到：……我们目前最关注的是对所有消费者数据的保护，无论是否受到本词数据泄露事件的影响。Equifax公司40天后

在没有成功预防数据泄露之后，Equifax又没有成功地对该事件进行响应，也没有对数百万处于风险中的美国公民的数据提供合理的保护（帮助）。即使延迟了40天时间，也

1. 没有成功采纳或遵循有效的应急响应方案

针对Senator Warren提出的问题，Equifax确认公司内部有许多解决网络安全突发事件的方案和规范指南，包括Security Incident Handling Procedure Guide,
Security Incident Response Team Plan, Security and Safety Crisis Action Team Plan。但是调查人员在这些应急方案中也发现了一些问题。

Security incident procedures的日期是2014年10月，也就是说有3年时间没有更新和修订了。Crisis management
plan好像没有太重视保护Equifax收集数据的个人，反而更加关注物理安全威胁和股东的利益。Equifax Security Incident Handling Policy &
Procedures中的unauthorized access incident
handling并不含有通知消费者关于他们个人数据的可能的访问。这些步骤散落在危机响应手册的不同章节，而且没有细节。最尴尬的是Equifax并没有按照内部的要求（规范

2. Call center的问题

从一开始，Equifax的call
center就有许多问题。有消费者等待了1个小时才接通人工客服，而消费者在等待的这1个小时接受了该公司其他产品的广告。接通人工客服后，人工客服并不能向消费者提

3. EquifaxSecurity2017.com的问题

Equifax搭建了一个网站（EquifaxSecurity2017.com）来指导消费者确定他们的数据有没有泄露，还可以在网站上了解公司提供的针对此次数据泄露事件进行保护的安全产
monitoring项目。

EquifaxSecurity2017.com网站的设计和网址都存在安全问题，攻击者可以利用很轻易地利用钓鱼网站或其他方式手机消费者信息，比如www.securityequifax2017.com就

4. 要求消费者放弃仲裁

在数据泄露初期，Equifax要求所有消费者注册一个为期一年的免费信用监控项目，该项目是Equifax所有的另一款产品。在注册该项服务时，消费者首先要签署一份声明，声

5. Equifax将此次数据泄露事件当作一次赚钱的机会

在数据泄露事件发生后，Equifax并没有想着如何去帮助客户，反而把这当作一次盈利的机会，利用自己之前的错误来盈利。在数据泄露事件公布后，Equifax让消费者冻结
their
credit），也就是停止向第三方提供消费者信用文件，这是一种常用的防止身份盗取的方法。刚开始的时候，Equifax向消费者收费30.95美元。直到消费者对此强烈反应后，
lock后才考虑重新评估这些费用。

对消费者来说，Equifax的免费服务结束后，风险是仍然存在的；如果消费者想要在免费服务结束后继续保护自己，就必须要注册新的产品服务。FTC的数据显示，社会安全

Equifax前CEO Richard Smith
8月份说，公司发现数据泄露后，诈骗分子认为这是一个极大的机会。Equifax向企业和政府出售产品来帮助他们应对和从数据泄露中进行恢复，同时也出售信用监控产品来
银行委员会听证会上，统计数字显示有750万消费者注册了免费的信用监控服务。如果其中有1万消费者1年后购买付费监控服务，以17美元每月的费用计算，Equifax因为数

E. 联邦立法可以预防未来的数据泄露和对此类事件的响应

Equifax和其他的征信机构在没有授权的情况下手机了消费者的数据，而消费者无法阻止数据被该企业收集和拥有。在调查中，Equifax向Senator Warren确认说公司并不会向用户提供删除个人信息的服务。但是调查发现，Equifax又不能提供强有力的安全措施来保护用户的数据，又不愿意或者不能完全解决系统中的安

企业有责任保护个人信息。但是从Equifax的数据泄露和对数据泄露事件的响应说明了联邦立法的必要性，立法可以给管理者和消费者一个工具来确保征信机构等将消费者的

针对征信机构严重信息安全泄露事件的罚款机制

联邦政府现在不能对征信机构进行罚款，当这些机构不能保护个人信息，将消费者安全和经济安全至于风险当中。事实上，FTC已经要求立法了，因为罚款立法可以帮助确保

建立严格的网络信息安全标准，并授权联邦交易委员会更新和监控这些标准

目前没有一个机构有适当的权限来建立基本的信息安全需求，并监控企业是否执行了这些标准。联邦交易委员会也说需要一些额外的工具。Equifax没有对属于数百万美国公

FTC应当有监管授权来监控征信机构，确保这些机构遵循相应的标准。如果没有授权，FTC应当能够要求机构更新他们的安全程序。如果Equifax这样的机构发生入侵事件，且

报告原文：https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf

上一篇：Linux下shellcode的编写 下一篇：入门学习linux内核提权

1. 0 条回复
   - 动动手指，沙发就是你的了！