从数据泄露和品牌信任事件中汲取网络安全教训

简译版

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	Cybersecurity lessons learned from data breaches and brand trust matters		
原文作者	宾度·桑达雷桑（Bindu Sundaresan）	**原文发布日期**	2020年9月28日
作者简介	宾度·桑达雷桑是AT&T网络安全总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/09/28/cybersecurity-lessons-learned-data-breaches-brand-trust-matters/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公有方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 • 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 • 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 • 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。		

从数据泄露和品牌信任事件中汲取网络安全教训

宾度·桑达雷桑

2020 年 9 月 28 日

企业品牌是宝贵的资产，也是很重要的攻击向量。攻击者经常利用公众对企业品牌的信任，冒充企业或其产品进行网络钓鱼。如今，企业需要与众多数字平台（网络、社交媒体、移动应用等）交互，这些交互对企业的业务至关重要，导致上述问题更加棘手。

企业应该意识到，保护公众对他们的数字信任不仅是合规性检查的一部分，更对其业务成败攸关。

新冠疫情期间，越来越多的用户开始从远程或非传统位置访问企业数据。因此，企业应特别注意防范网络攻击和数据泄露。疫情助长了网络犯罪——我们发现，随着数字化转型计划的加速，以及越来越多的员工在没有适当防火墙和备份保护的情况下在家工作，黑客攻击活动大大增加。

数据泄露的影响不再局限于 IT 部门。勒索软件、网络钓鱼和数据泄露的频率和复杂程度持续增长，不断破坏着企业的品牌声誉和经济活力。攻击者利用此次疫情危机，对各行业的企业发动攻击，并攻破其系统。

在处理网络安全问题时，良好的监管至关重要。强大的网络安全能够向客户表明，企业正努力采取措施避免黑客入侵，保护其数据的安全。

疫情并未改变网络安全的根本。新“常态”会是什么样的？疫情给企业和整个社会带来了翻天覆地的变化，但完善的网络安全实践（有些已经存在了数十年）仍然是企业保护自己的最佳方法。

1. 数据监管

数据监管是指，企业在整个数据生命周期中保护高质量数据的能力。这包括数据完整性、安全性、可用性和一致性。数据监管策略需要涵盖相关的人员、流程和技术，以便恰当处理数据，包括：

- 为负责管理数据资产的人员划定责任

- 为相关人员分配数据管理和保护职责
- 规定哪些人员，可以在什么情况下，使用什么方法，对哪些数据采取何种行动。
- 确定数据保护措施
- 提供完整性控制措施，保证数据的质量和准确性。

2. 补丁管理和漏洞管理：硬币的两个面

企业可以通过漏洞管理处理威胁。攻击者试图利用发现的漏洞来感染工作站或服务器。威胁管理是一个被动的过程，必须建立在威胁已经被发现的基础之上；而漏洞管理则是主动的，其目的是在漏洞被利用之前将其修复。

漏洞管理不仅仅是修复漏洞。正式的漏洞管理不仅涉及修复和重新配置不安全设置，它是一种纪律严明的实践，IT 部门需持有这样的观念“新的漏洞每天都会出现，需要不断地加以识别和修复”。

3. 遭受攻击是迟早的事：假设自己已被攻击

如果企业基于这一点进行运营和防御，就能够更好地检测攻击并防止数据泄露。

事件响应计划的重要性

企业应将数据泄露视为“何时会发生”而非“是否会发生”，并为此做好准备。一旦发生重大事件，企业根本没有时间来制定事件响应计划。前期投入时间和精力来制定事件响应计划，定会为后期带来极大的便利。

当重要资产面临威胁时，企业进行响应的时间会非常有限。在这种情况下，事件响应计划能够提供帮助，更快地指导企业成功地进行遏制和恢复。响应时间越短，事件造成的损害就会越小。因此，成功的关键在于提前制定事件响应计划。

4. 公司规模和安全成熟度没有相关性

企业的规模如何，其安全团队能够访问多少资源，与其安全性都没有什么关系。作为防御者，我们通常认为：“只要有足够的资金或人力，就能解决问题”。我们需要改变这种观念了。重点不是企业投入了多少资金，而是是否将资金用在了恰当的地方。企业的安全团队能否抵御攻击，还是说只能坐以待毙？无论企业处于“实现安全成熟度”的哪一步，风险评估

都是很重要的，能够帮助企业确定何时、对哪些资源进行最大程度地改进。

对于更成熟的企业来说，风险评估过程将不再侧重于发现主要漏洞，更多地在于寻找持续改进安全性的机会。对不成熟的计划进行评估，能够发现计划与业务目标不符，流程或体系结构效率低下等问题，并确定能够在哪些方面增强保护措施。

5. 好钢用在刀刃上

企业的预算有限，人员有限，时间有限。安全专家在尝试启动新计划或完成日常任务时，都面临这些限制——这可能是他们面临的最棘手的问题。这些问题会影响所有企业，无论其行业、规模或位置如何，即使是准备最充分的公司也无法幸免。没有任何一家公司拥有无限的资金或时间。此外，企业还缺乏网络安全专家。

企业应如何应对这些限制呢？答案是对资源排优先级和改善运营。企业应了解哪些流程可以精简，并确定最严重的风险，以便在这些限制之下保护其系统。

6. 定期培训

安全不能只靠 IT 一个部门来完成。因此，企业应付出时间和精力创建安全文化。此外，企业应定期举行网络安全意识培训（至少每季度一次），就安全问题与员工进行持续的对话。想要一劳永逸是不可能的。

人的记忆力很短，因此在涉及对企业如此重要的安全问题时，企业应重视定期培训。应从高级管理层开始，自上而下创建网络安全意识。安全意识培训不应局限于数据监管、威胁检测和事件响应部门，而应在所有部门中进行。此外，企业还要注意，安全意识培训不仅仅是制定枯燥的规则。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）
http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com