

简译版

数据隐私不仅仅是指机密性

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	Data Privacy Must Evolve Beyond Confidentiality		
原文作者	Sue Poremba	原文发布日期	2018 年 12 月 7 日
作者简介	Sue Poremba 从 2011 年开始撰写文章，其专长是网络安全和技术领域。 https://securityintelligence.com/author/sue-poremba/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/data-privacy-must-evolve-beyond-confidentiality/		
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	<ul style="list-style-type: none"> 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共方式，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。 		

数据隐私不仅仅是指机密性

Sue Poremba

2018 年 12 月 7 日

如今，大多数安全系统在构建时都考虑到了数据的机密性，这一点非常重要。但是，机密性只是数据隐私的一个方面。正如安全专家布鲁斯 施奈尔（Bruce Schneier）在 2018 年 SpiceWorld 大会上所说的那样，现在是时候重新理解数据隐私并制定数据隐私策略了。

考虑到数据使用的方式，我们需要将更多的精力放在保护数据的完整性和可用性上。

了解“CIA 数据安全三要素”

越来越多的安全专家开始关注“CIA 三要素”：机密性（confidentiality）、完整性（integrity）和可用性（availability）。对于数据安全来说，这三点最为重要。

根据 Infosec Institute 的说法，机密性（目前仍然是数据隐私的重点）是指通过结构化的分类指南，来规范个人和第三方机构对私人数据的访问权限。

完整性是指“确保信息从源头传输到目的地的过程中不被篡改（即活动的数据），还包括存储的信息也不被篡改（即静止的数据）。”可用性则是指“确保机构的数据服务是可用的”。

威胁到可用性的典型案例是 DoS 和勒索软件攻击，这两种攻击都会阻止用户访问文件或网站。威胁到完整性的典型案例是，威胁源操纵用户账户并篡改其中的信息，例如更改银行账户——这样一来，即使用户的信息没有被盗，也已经不再准确。

施奈尔在 SpiceWorld 大会上说，物联网（IoT）以前所未有的方式将人和机器互联起来，这对数据的完整性和可用性带来了很大的威胁，远超过机密性面临的威胁。

“此类威胁影响到受害者的生命和财产安全，可能会造成更加严重的后果。”他说，“比如，虽然我很担心黑客会侵入医院网络并窃取我的就诊记录，但我更担心他们会篡改我的血型。”

转变对数据隐私的理解

在过去的几年中，最严重的安全事件都围绕着数据机密性问题。网络犯罪分子能够窃取

信用卡信息、姓名、出生日期、社保号，甚至诸如指纹等生物识别信息——这些信息都保存在政府工作人员的安全审查文件中。

考虑到目前的网络环境，当消费者的数据机密性受到损害时，他们会感到不安也就不足为奇了。诸如《通用数据保护条例》（GDPR）和美国加州《消费者隐私法案》（CCPA）等隐私法规，旨在保护信息的机密性，同时将信息的控制权移交给其合法的所有者——消费者。

GDPR 还规定，即使发生安全事件，公司也要保证数据的可用性。施奈尔指出，数据隐私不仅涉及消费者数据（关于消费者个人身份的信息），还涉及汽车、家用恒温器、无人机、智慧城市、医疗设备、关键基础设施和军用系统等（即任何能够联网并生成数据的设备）产生的数据。

“我们开始看到针对关键系统的 DDoS 攻击，以及针对联网汽车的勒索软件攻击。”施奈尔说。

我们必须认识到，针对 CIA 三要素中每个要素的攻击会带来什么影响。医院用来处理患者信息的电子表格系统崩溃会导致患者数据丢失，但患者使用的联网起搏器崩溃则可能会危及患者的生命，显然这两者（均指可用性）之间存在着根本性的区别——因此我们应该为安全策略确定相应的优先级。如果数据的完整性和可用性更加重要，我们可以设计安全系统来应对潜在的漏洞和攻击向量。

通过备份和审计来保护数据完整性

如果文件难以访问，那么它们就会更加难以处理。因此，保护数据的完整性涉及机密性的多个方面。数据完整性的一个关键方面是：确保信息是准确的、未被篡改的。在保护数据完整性方面，备份至关重要。在发生疑似网络安全事件之后，可以将现有文件与之前备份的文件进行对比，以确定文件是否遭到了篡改。

对数据进行定期审计，也有助于各机构了解数据是否发生了变化。当信息应该保持不变时，是否发生了变化？是否出现了规律性的变化？是否出现了不寻常的变化？

各机构对数据越了解，就能更好地保护其完整性。此外，接触数据的人越少越好。访问或编辑数据的员工太多，会增加某人犯错且未能被及时发现的可能性。

数据可用性极其重要

数据可用性旨在确保发生攻击事件后可以快速访问相关信息。同样，我们可以通过可靠的备份或数据丢失恢复系统，来确保数据的可用性。

各机构需要考虑其数据的可用性是否存在风险。例如，是否存在勒索软件攻击风险？是否存在 DDoS 攻击风险？基础设施是否过于老旧，无法防御自然灾害或黑客攻击？

数据备份有助于应对数据可用性风险。在不同地区设立数据中心、采用可以在几分钟内恢复网站可访问性的云服务、开展降低勒索软件攻击风险的工具和意识培训，都有助于降低数据丢失风险。

由于网络世界的互联性日益增强，机密性已经不再是数据隐私的唯一方面。保护好数据的机密性、完整性和可用性，不仅对隐私保护至关重要，甚至可能导致生与死的差别。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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>