简译版

平衡数据安全性和可用性的三种方法

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	3 tips for balancing data security and usability		
原文作者	杰森·多布斯（Jason Dobbs）	**原文发布日期**	2021年7月8日
作者简介	杰森·多布斯是PKWARE公司的首席技术官。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/07/08/data-security-practices/		
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		
摘要	企业应如何在数据安全性和可用性之间找到适当的平衡呢？本文介绍了三种方法：（1）利用员工参与安全的意愿；（2）赋予员工一些安全权力；（3）确保用户知道他们正在参与安全实践。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

平衡数据安全性和可用性的三种方法

杰森·多布斯

2021 年 7 月 8 日

在网络安全方面，企业面临着诸多挑战。许多企业最关心的挑战是：在数据的可用性和安全性之间取得适当的平衡。

现实情况是，对于大多数员工来说，安全不是最要紧的——他们只想随时随地访问所需的数据，并完成工作。然而，大多数安全措施都会降低数据的可用性。

举例来说，访问控制列表会阻止用户访问信息，甚至阻止他们了解数据是否存在。加密会干扰实时协同和搜索，而企业对此无能为力。搜索是通过索引信息来运作的，无法重复进行，因为这会违背保护数据的目的。此外，依靠员工来管理密钥就像要求员工为每个网站设置不同的口令一样，是不会有什么建树的。

那么，企业应如何在数据安全性和可用性之间找到适当的平衡呢？下述三种方法可以帮助企业应对该挑战。

1. **利用员工参与安全的意愿。**好消息是，大多数员工都希望参与公司的安全计划——前提是这不会影响他们完成工作的能力。这能够确保员工在数据安全实践方面达成共识。安全培训计划有助于员工了解公司的安全策略，以便做出更好、更明智的决策。此外，使公司的安全策略透明化，有助于员工了解他们是否遵守安全策略或法规，也有助于员工在改善可用性等方面提供反馈意见。

2. **赋予员工一些安全权力。**企业需要在“让员工就数据保护做出决策”与“实现自动化的保护”之间找到微妙的平衡。例如，如果员工需要通过电子邮件向企业外部发送敏感文件，则该数据安全流程应完全实现自动化，以确保应用适当的保护措施。员工可能会认为，他们了解哪些规则适用于哪些数据，但是最终还是会犯错误。在这方面，企业不应冒险，以避免敏感信息被泄露。

但是，在将标签和分类应用于包含敏感信息的文档时，可以给予员工更多的自由。企业可以采用自动化技术来保护最敏感的数据，而用户可以选择将分类标签应用于不太敏感的信息（如果他们认为有必要）。

3. 确保用户知道他们正在参与安全实践。关键是要提高员工对数据安全实践的认识。这与“赋予员工一些安全权力”相呼应——如果要给员工选择，应确保选择的数量有限，然后根据他们的选择实施恰当的安全措施。例如，使用提供可视化指标（有关应用保护和文档分类）的工具，能够提醒员工关注数据安全实践，使他们更积极地思考哪种策略最合适。此外，这也能够提醒他们采用正确的安全实践。

上述三种方法不仅可以帮助企业遵守数据安全实践，还可以确保员工接受培训、获得授权并了解公司安全实践。此外，对于加密等领域，企业应使用工具，来确保所有员工都遵守企业加密策略，并且不会导致企业无法访问自己的数据。

企业还应为员工管理密钥，并使用能够提供灵活性和安全性的工具（员工成功、安全地导航数据需要这样的工具）。最后，企业应对安全实践及其对这些实践的期望保持透明，这有助于员工成为安全管家，同时还可以减轻企业面临的风险。

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