

简译版

## 防止数据泄露的四种方法

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	Four ways to prevent data breaches		
原文作者	汤姆·莫瓦特 (Tom Mowatt)	原文发布日期	2020 年 3 月 27 日
作者简介	汤姆·莫瓦特是西雅图 Tools4ever 公司的董事总经理。		
原文发布单位	Help Net Security		
原文出处	<a href="https://www.helpnetsecurity.com/2020/03/27/prevent-data-breaches/">https://www.helpnetsecurity.com/2020/03/27/prevent-data-breaches/</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

# 防止数据泄露的四种方法

汤姆·莫瓦特

2020 年 3 月 27 日

数据泄露没有大小之分，更是逃避不了的问题。几乎每种类型的组织机构（包括您的公司）都存储了重要的个人身份信息（PII）。不管企业规模大小、是何行业，只要存储着 PII，就会成为攻击者的目标，而成功进行网络钓鱼攻击只需一名员工把虚假邮件误认为合法邮件那么简单。这就意味着所有人都有风险。

统计数据显示，数据泄露事件正在逐步增加，并可能给企业带来毁灭性的、长期的财务和声誉影响。波耐蒙研究所（Ponemon Institute）发布的《2019 年数据泄露成本报告》估计，美国发生一次数据泄露的平均总成本将近 400 万美元。报告称，每条丢失的数据记录的平均价格约为 150 美元。

造成数据泄露原因有很多，因此不存在一种放之四海而皆准的解决方案。需要多方面的努力才能保障安全。企业可以通过以下四种方法（外加一种）来加强其数据安全屏障，防止数据泄露。

## 1. 加强员工安全培训

对所有新员工进行数据安全培训，并要求所有员工在每年年初参加复习课程，让他们了解最新的安全指导方针并牢记于心。

虽然这类培训很枯燥，但只需要几分钟员工就能掌握基本的细节。例如，员工应：

- 将所有设备（如台式机、笔记本电脑、平板电脑、手机）都视为能够访问企业系统的设备
- 永远不要把密码记在别人容易找到的地方
- 对于未经证实身份的人要求提供密码或其他敏感信息（在下面的最后一条中有更多相关内容）的电子邮件或电话，要格外小心

在培训中加入一些最新的数据泄露统计信息，以帮助传达威胁的严重性和普遍性以及可能造成的财务影响。

## 2. 模拟网络钓鱼攻击

许多安全问题都是人为错误造成的，比如点击恶意电子邮件中的链接。

鱼叉式网络钓鱼攻击（即针对性强与定制化的网络钓鱼攻击）由于针对特定的人员，往往会导致更多的数据泄露。这些信息可能涉及某个部门或常规工作，可能与目标收件箱中任意一天的其他相关信息相似。

利用免费或付费的网络钓鱼模拟器，自己发送一些电子邮件来测试员工检测网络钓鱼邮件的能力。当有员工点击其中某一封邮件时，模拟器就会发出告警与报告。

采用模拟网络钓鱼的方式来培训和教育员工，以识别最新的网络钓鱼伎俩，使他们变得更加安全。记住提醒员工，如果他们不是完全肯定收到的电子邮件是合法的，那么就要仔细检查。如果员工从他们认识的或能联系到的发送者那里收到一些看起来有点不正常或不寻常的东西，那应该由 IT 团队来处理这些邮件。

## 3. 评估帐户

您的 IT 团队多久才会评估一次现有帐户？毫无疑问，这可能是一个复杂的过程，但是评估企业账户可在保障安全的情况下，减少工作量。

企业中是否存在前员工仍然可以访问的孤立帐户？当不同的用户在企业中的位置发生变化时，是否有确定和更新他们应该能够访问哪些内容的审查过程？

一年中评估帐户的最佳时间可能是对上一年的帐户进行更新时。如果 IT 团队一直没有时间来评估帐户，可以让他们把评估帐户加入到其他流程中，或者将其作为一个大项目安排在工作量较少的月份。

## 4. 检查用户帐户的生命周期流程

当员工离职或外部顾问不再提供服务时，停用帐户的标准流程是什么？这些类型的离开（无论是否涉及直接的安全问题）是造成系统中孤立帐户问题的最重要因素。

手动管理或自动停用帐户非常重要。审查并优化企业的停用流程，以确定它们在快速限制帐户方面的速度和全面性。

快速响应非常重要，您可以放心的将帐户交给审查流程，因为它可以对您的帐户进行全

面审查。

## 旁注：考虑实施安全的 SSO 解决方案

对于大多数系统和应用程序，单一入口点可以使所有员工的工作更轻松。用户只需要记住一组凭据，管理员就可以在不受更多限制的情况下保护资源，同时又不会加大访问的难度。通过将入口点限制在一个位置，可以防止潜在的数据泄露。可配置的安全设置（例如日期和时间限制）使管理员可以控制其环境，即使系统和应用程序已扩展到云中也是如此。

包含某些敏感信息的应用程序和系统可以设置为除特定物理位置之外的任何位置都无法访问，以帮助企业预防风险，而安全门户可以维护用户活动的日志，包括何时以何种方式访问信息。

数据是企业拥有的最有价值的资源之一。保护它的方案不一定是复杂的或昂贵的，但必须是正确的。现在，开始实施其中一些或所有方法来加强企业的数据安全实践。

## 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 endpoint 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,截止到 2019 年 9 月 30 日,安天的威胁检测引擎为全球超过六十万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>