简译版

# 长期远程办公的数据丢失防护策略

**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 loss prevention strategies for long-term remote teams | | |
| **原文作者** | 艾萨克·科恩（Isaac Kohen） | **原文发布日期** | 2021 年 2 月 5 日 |
| **作者简介** | 艾萨克·科恩是 Teramind 研发副总裁。 | | |
| **原文发布单位** | Help Net Security | | |
| **原文出处** | https://www.helpnetsecurity.com/2021/02/05/data-loss-prevention-remote-teams/ | | |
| **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。<br>• 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。<br>• 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。<br>• 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。 | | |

# 远程办公的数据丢失防护策略

艾萨克·科恩

2021 年 2 月 5 日

在疫情肆虐的情况下，许多高管开始意识到与网络安全相关的风险和机遇。2019 年，Optiv Security 就网络安全优先事项进行了调查，发现 96%的首席信息安全官（CISO）开始采取“更具战略性的网络安全方法”，许多 CISO 甚至愿意放慢业务发展以应对与网络安全相关的风险。

在数据泄露成本持续增长的情况下，这是一个好消息。不幸的是，疫情给他们的工作带来了更大的困难，他们不得不在全新的环境中处理这些优先事项。

对很多公司来说，分布式混合型劳动力已经成为一种新常态，这极大地扩展了他们的威胁范围，使其在保护数据和 IT 基础架构方面面临更大的挑战。在这种环境下，他们需要加强防御能力，以做好应对威胁的准备。

## 了解内部人员威胁

在考虑网络安全威胁时，我们通常会想到网络犯罪分子或国家支持的黑客。这是因为，当此类攻击事件发生时，会在全球范围内登上新闻头条。

但是，对于大多数公司而言，外部攻击者并非最严重的风险。公司员工通常会带来更为严重的威胁，幸运的是，这种威胁更易于管理。

IBM 预计，在公司的数据泄露事件中，人为错误占了将近四分之一。此外，员工通常会因不良口令安全、意外数据共享、技术使用不当、网络钓鱼诈骗等原因，无意中泄露公司的数据。

还有一些员工会恶意行事——他们为了获取利润、报酬或只是为了好玩，故意窃取公司数据。敏感数据的市场非常火爆，一些网络安全专家预测，随着攻击者利用远程办公趋势来渗透公司，将会出现“内部人员即服务”（insiders-as-a-service）之类的攻击方法。

## 最佳防御实践

虽说内部人员严重威胁着公司的数据安全，但此类威胁是最容易控制的。通过采用最佳

防御实践，公司可以大大降低数据泄露的风险。

### 1. 部署员工监控软件

特别是在保护远程办公的员工时，功能强大的监控软件可以提供关键的可见性和防御能力。具体而言，员工监控措施可以：

- 分析员工行为模式，以便在威胁出现之前予以识别。
- 限制员工对敏感数据的访问
- 防止数据渗漏
- 协助数字取证，帮助公司进行调查和分析。

多年来，公司已投入大量资金来保护现场 IT 基础架构。在长期混合办公的大趋势下，希望保持网络安全的公司应将非现场投资作为优先考虑事项。

### 2. 创建并执行数据管理策略

有很多公司的员工使用个人设备进行办公。将近 60%的公司允许个人设备访问其网络和数据，这种做法使公司的数据面临风险。

公司发布的数据和网络访问技术，是一种更好、更全面的数据管理方法。通过此类监控服务，公司可以监督员工如何使用公司发行的设备，从而确保以最佳的方式保护敏感数据。

### 3. 保护账户

可能有超过三分之一的员工从未更新过其账户口令。在过去的几年中，数十亿的登录凭证被窃取。由此可见，这是一个严重的漏洞，但是可以通过简单的方法予以解决。

公司应敦促员工定期更新账户口令（比如在电脑屏幕上跳出更新口令的提示），这样可帮助员工阻止攻击者，以简单而有意义的方式降低风险。

同时，员工应启用可用的安全功能（例如双因子身份鉴别）。这样一来，即使攻击者有正确的登录凭证也无法访问公司数据。

### 4. 对全体员工进行安全培训

大多数员工都希望参与数据安全解决方案。公司应对全体员工进行安全培训，帮助他们有效管理数据、识别网络钓鱼诈骗并保护账户；即，将全体员工都变成防御资产，而非安全

漏洞。

## 结论

即使在疫情干扰许多公司的运营架构之前，他们也面临着广泛且成本高昂的网络安全威胁。

自 2015 年以来，数据泄露事件逐年增加，数十亿条记录被窃取，给各公司带来了数百万美元的损失。在监管审查日益严格的大环境下，公司应将网络安全作为优先考虑事项。

远程办公人员的增加给公司带来了更大的内部人员风险，因此公司必须采取行动。有效的网络安全策略将为企业奠定坚实的基础。

# 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