简译版

如何在混合办公模式下保持安全

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	Five tips on how to stay (cyber)secure in a hybrid work world		
原文作者	拉金·莱德（Larkin Ryder）	**原文发布日期**	2022 年 1 月 6 日
作者简介	拉金·莱德是 Slack 产品安全总监。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2022/01/06/hybrid-work-security/		
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	在过去的 18 个月中，攻击者正是利用混合办公的不确定性对企业及其员工发动了多起攻击。企业可以采取下述措施来防御攻击，在不牺牲安全性的情况下获得混合办公的优势：（1）了解企业风险；（2）减少对电子邮件的依赖；（3）使用企业级工具为员工赋能；(4)增强身份和设备管理控制；（5）转变安全观念。		
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。		

如何在混合办公模式下保持安全

拉金·莱德

2022 年 1 月 6 日

从“减少通勤时间”到“更好地平衡工作与生活”，保持灵活办公是员工目前的首要任务。

对于企业而言，这意味着混合办公模式将继续存在。这种模式不仅有助于在人才严重短缺的情况下吸引人才，还有助于提高员工参与度、创建更完善的团队，以及提高企业生产力。

然而，在采取这种新型办公模式时，企业很容易忽视它带来的诸多挑战。其中一个挑战就是维护网络安全。

在过去的 18 个月中，攻击者正是利用混合办公的不确定性对企业及其员工发动了多起攻击。企业可以采取下述措施来防御攻击，在不牺牲安全性的情况下获得混合办公的优势。

1. 了解企业风险

疫情期间，员工居家办公的情况大幅增加，他们使用自己的设备来访问公司网络。攻击者正是利用了这一点来实施诈骗，从新冠检测诈骗到二维码诈骗的各类诈骗增加了 70%。要想防御此类攻击，企业必须了解其安全风险，不断识别新的威胁和漏洞，并不断改进检测和防御措施。

此外，企业还要了解“弱安全性”对他们的影响，并就这一主题开展员工培训。“弱安全性”不仅会影响企业的业务，还会伤害员工的感情，导致他们幸福感降低和焦虑。如今，安全不仅包括保护企业的的技术和资产，还包括保护企业的员工。

企业在开展员工培训时，要让员工知道，他们遇到安全问题时会获得帮助和支持。

2. 减少对电子邮件的依赖

电子邮件是重要的攻击向量，攻击者最常用的方法是“电子邮件欺骗”。在这种攻击中，攻击者会伪装为其他人（通常是公司高管）发送电子邮件。

在内外部通信中，改变电子邮件习惯和减少对电子邮件的依赖是减少此类攻击最有效的

方法。此外，企业不应仅仅使用电子邮件，而是采用基于渠道的通信应用类工具。这样不仅能使通信更加安全，还有助于与团队成员协同。

3. 使用企业级工具为员工赋能

IT 团队必须满足员工的需求，否则员工会自己寻找解决方案，这会增加敏感信息泄露的风险。此外，一旦采用了所谓的“影子 IT”，就很难摆脱。简而言之，员工自行寻找解决方案（例如，使用消费级通信应用）会产生不必要的安全风险。在办公协同中，加密是最基本的要求。企业级应用程序可以提供诸如企业密钥管理、审计日志等功能，能够进一步为 IT 团队赋能，以确保数据和员工的安全。

此外，企业级协同工具拥有专门的安全和合规伙伴生态系统，这意味着它们可以轻松连接到安全设备（例如 Okta 或 Splunk）。

4. 增强身份和设备管理控制

现在，越来越多的员工开始使用个人 Wi-Fi 和个人设备办公，企业是时候建立新的安全基线了。在混合办公环境中，保护企业信息要从身份控制开始。企业可以采用会话持续时间指标、双因子身份验证和域声明等措施，以确保只有合适的人员（无论他们在哪里办公）才能访问企业信息。

此外，会话管理工具、默认浏览器控件、额外的身份验证层，以及阻止越狱或 root 设备的能力，也有助于确保只有经过批准的人员和设备才能访问企业网络。

5. 转变安全观念

自 2020 年初以来，企业的办公环境和安全问题都发生了巨大的变化。随着员工转向远程办公，威胁也发生了变化，IT 团队面临着严峻的挑战。

如今看来，远程办公的情况将会继续存在。与此同时，武器化人工智能等新威胁开始出现。为了帮助 IT 团队保护企业的安全，企业必须转变其安全观念。

企业应为居家办公的员工提供保护措施，让他们获得与在办公室中相同级别的保护。此外，企业还应倾听远程和混合办公员工的需求，并为其提供企业级办公工具（包括办公套件和协同工具），这样员工就不必求助于非企业级或未经批准的平台了。

最后，企业应对其技术堆栈采取“安全第一”的方法。举例来说，企业应减少使用老旧工具，这些工具会为攻击者提供可利用的漏洞。此外，企业应建立企业级工具生态系统，以增强其安全性。这样一来，IT 团队和员工就可以随处办公，在安全的情况下专注于真正重要的工作。

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