疫情期间远程办公的安全问题

简译版

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	Remote Work Security: Handling Setbacks in the Time of COVID-19		
原文作者	迈克·埃尔根（Mike Elgan）	**原文发布日期**	2021 年 10 月 29 日
作者简介	迈克·埃尔根是一位专栏作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/remote-work-security-solving-changes-covid-19/		
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	远程办公安全需求和混合办公安全需求将伴随企业很长时间。因此，企业需要重新考虑其网络安全措施。现在，企业需要采取更全面的安全方法（例如零信任模型），并使用工具来了解连接到企业网络的所有内容。企业还需要更全面的云安全解决方案、更好的员工网络安全培训，并给远程办公的员工提供更好的安全建议和管理。总的来说，企业需要开发一套全新的居家办公最佳实践。		
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。		

疫情期间远程办公的安全问题

迈克·埃尔根

2021 年 10 月 29 日

大多数安全专家、IT 工作者和领导者都知道，新冠疫情导致企业的业务和数字安全性下降。很重要的一个原因是，疫情迫使企业迅速转向远程办公，而有多个因素会降低远程办公的安全性。

我们先来说一下远程办公的情况。众所周知，新冠疫情的爆发带来了一场突然的、计划外的大规模远程办公迁移。这导致员工无法再在防火墙内物理安全的位置办公，也无法再使用经批准的设备办公，他们开始转向居家办公。“远程办公扩展了企业的攻击面”这一说法早已存在，但是其带来的后果现在才变得清晰起来，这种办公模式带来了许多安全挑战。

未经审查的工具

转向远程办公需要新工具，但是企业没有那么多时间来审查新工具的安全性。因此，平均而言，应用程序和服务的安全性大不如前。Forrester Consulting 对 1300 名安全领导者进行了调查，其中近四分之三（74%）表示，最近的网络攻击源于疫情期间部署的技术中存在的漏洞。

更多影子 IT

企业让员工在家里办公，实际上是让员工使用自己的设备办公。许多员工的办公设备不受保护，从而威胁到企业的网络安全。员工通过家庭网络连接办公设备，而这些网络还为智能恒温器、联网玩具、家庭娱乐系统、游戏机和许多其他家庭物联网（IoT）设备提供服务。这些设备可能缺乏物理安全性，并且往往很少或从不进行更新。

缺乏可见性

更糟糕的是，企业缺乏对远程办公员工家庭网络的可见性。这反过来又对企业网络安全造成了障碍。

云服务的使用增加

安全公司 Zscaler 发现了另一个严重的问题——大型公司通常有数百台云服务器暴露在公共互联网上。“暴露”是指只要能够找到相关服务，任何人都可以连接到这些服务器。而许多企业并不知道这一点。Forrester 指出，80%的安全和业务领导者表示，由于远程办公存在安全问题以及将关键功能迁移到云中，他们面临着更大的风险。

广泛分布的连接

远程办公的特征是全球化、移动和分布的劳动力，这些特征使得检测威胁变得更加困难。举例来说，来自东欧的登录可能是一个勒索软件组织在探查企业的防御；也可能是企业销售经理异地登录。在检测异常行为上，“位置”已经是一个较弱的信标。

利用疫情相关的信息

Proofpoint 的《人为因素报告》指出，攻击者利用人们对疫情的焦虑和恐惧，使用与疫情相关的内容执行社会工程网络钓鱼攻击。企业需要记住，在远程办公的安全性上，很重要的一点是消除人为错误。

以远程办公人员为攻击目标

根据 Forrester 的报告，大约 67%的企业网络攻击针对的是远程办公的员工。

在线交易增加

随着越来越多的人开始在网上购物，攻击者开始更多地瞄准在线零售商及其客户。

远程办公安全需求和混合办公安全需求将伴随企业很长时间。因此，企业需要重新考虑其网络安全措施。现在，企业需要采取更全面的安全方法（例如零信任模型），并使用工具来了解连接到企业网络的所有内容。企业还需要更全面的云安全解决方案、更好的员工网络安全培训，并给远程办公的员工提供更好的安全建议和管理。总的来说，企业需要开发一套全新的居家办公最佳实践。

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