

简译版

远程办公带来的网络安全问题

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	The cybersecurity implications of working remotely		
原文作者	米尔科·佐尔茨 (Mirko Zorz)	原文发布日期	2020年3月20日
作者简介	米尔科·佐尔茨是 Help Net Security 网站的总编辑。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2020/03/20/cybersecurity-working-remotely/		
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.antivy.cn 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> 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。 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。 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。 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。 		

远程办公带来的网络安全问题

米尔科·佐尔茨

2020 年 3 月 20 日

我们与以色列 Panorays 公司的首席技术官（CTO）德米·本-阿里（Demi Ben-Ari）进行了交流，讨论了在虚拟环境推动下远程办公带来的网络安全风险。

COVID-19 冠状病毒在全球的传播对全球工作场所产生了显著影响，许多企业都鼓励员工在家远程办公。这一转变对网络安全有何影响？

突然有大量员工远程办公，可能会给企业带来重大变化，并带来诸多网络安全方面的问题。

其中一个问题是缺乏身份认证和授权。由于人们无法面对面的看到对方，因此越来越需要使用双因子身份认证、监控访问控制并创建强密码。网络钓鱼和恶意软件等攻击也有增加的风险，尤其是员工现在可能会收到数量空前的电子邮件和在线请求。

此外，远程办公会显著的扩大企业的攻击面。这是因为使用自己设备办公的员工会引入不同平台和操作系统，而这些员工设备的安全性及其不同系统的安全性和可靠性都无法得到保证。随着越来越多的设备被使用，其中一些设备会很可能会出现安全漏洞。

最后，同样的安全注意事项也适用于企业的供应链。这可能非常具有挑战性，因为通常规模较小的供应商缺乏实施必要的安全措施所需的专业知识和安全人员，导致安全措施不足。黑客已经意识到了这一点，开始瞄准第三方供应商进行渗透攻击。

人为失误的隐藏风险是什么？

毫无疑问，如果缺乏有效的沟通，企业更容易出现人为失误。当您没有坐在同事旁边时，发生配置错误的几率会大大增加，从而暴露出安全漏洞。恶意行为者就可以利用这些网络漏洞攻击企业。

远程办公导致 IT 部门必须改变常用的系统配置设置，这样才能保证远程办公的可能，使得员工可以从外部访问内网。这就涉及网络和 VPN 的配置、新设备的加入、新端口的开

放等。这样新加的设置显然增加了攻击面，当然在实施这些变更时，导致了更多人为失误的可能。

事实上，人们无法面对面工作加剧了这种情况：因为确认一个人的身份更困难，出错的概率更大。

移动办公的巨大增长对合规性有何潜在影响？

因员工以及其办公设备的物理地址的分散，导致企业集中控制和统一配置非常困难，这样企业就面临着更大的风险。从根本上说，企业已经失去了在物理保护区的安全性。其结果是，企业因不能满足一些网络安全条例的规定而暴露在更大的风险中。

另一个合规性问题与变化有关。例如，一个企业获得了 SOC2 认证，但是那些远程办公的人员可能没有办法保持这些控制措施。重大且突然的变化会导致违规行为，比如大量的远程办公导致原来的合规可能不再适用。

企业应如何有效地评估新供应商，消除安全差距，并持续监控他们的网络态势？

作为第三方安全战略的一部分，企业应采取以下步骤：

1. **梳理与所有供应商的关系，厘清不同供应商的作用。**例如，一些供应商可能保存或处理相关的敏感数据，而其他供应商可以升级维护生产环境设备的软件代码。
2. **给供应商划分重要等级。**从商业运营的角度，给不同的供应商划分不同的等级，主要评估对方对公司运营的影响程度。比如有的供应商处理所有员工的财务信息（显然重要性就高）；有的供应商会则为公司的宣传海报进行图形设计（显然重要性就不如前者高）。
3. **对供应商增强可见性和控制措施。**这可以通过使用解决方案全面彻底评估供应商来实现，扫描其可能存在的攻击面以及对其进行安全访谈，以确保其为远程办公做好了准备。
4. **持续监控供应商的安全态势。**根据对不同供应商的不同评估结果，动态调整控制方案。这些方案包括限制供应商访问公司资源、完全切断访问途径等。这些都是基于企业对众多供应商的可见性和控制措施的基础上实施的。

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，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”等几十个高级网络威胁行为体（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络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，“您们也是国家队，虽然您们是民营企业”。

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>