简译版

疫情期间筑牢网络安全“藩篱”

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	Advocating Security Fundamentals During and After COVID-19		
原文作者	玛丽·奥布莱恩（Mary O'Brien）	**原文发布日期**	2020年5月29日
作者简介	玛丽·奥布莱恩是IBM Security总经理。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/posts/advocating-security-fundamentals-during-and-after-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		
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。 • 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。		

疫情期间筑牢网络安全“藩篱”

玛丽·奥布莱恩

2020 年 5 月 29 日

新冠疫情几乎立刻改变了世界的运作方式，带来了新的安全威胁和挑战。企业努力寻找前进的方向，希望变得更加强大。要实现这一点，关键在于盘点企业的安全现状以及安全目标。

远程工作

与许多其他企业一样，我们的员工也转向了远程工作——目前将近 95%的 IBM 员工都在远程工作。随着这一新现象的出现，需要提高员工对全球疫情下分散员工队伍相关安全风险的认识。

举例来说，自 2 月以来，视频会议、远程访问工具和虚拟专用网等促进远程工作的工具，其使用增加了 84%。同时，自 3 月 11 日新冠肺炎被宣布为全球疫情以来，IBM X-Force 发现与新冠肺炎相关的垃圾邮件增长了 6,000%以上。

当我们在这些未知领域中探索时，我们还应记住，困难的局势往往会激发出我们最大的潜力。尽管疫情给 IT 和安全团队带来了新的挑战，但各行业的企业都在利用 IT 工具来确保客户的安全和高效——从为世界各地的学生提供远程授课，到保护大型银行交易，乃至阻止对关键医院系统的勒索软件攻击等。

关注基本安全措施

问题的核心是 推动将安全渗入到业务的各个环节和流程。无论我们在哪里或如何工作，企业都要继续关注基本安全措施，实现灵活可靠的安全方法。

目前，IBM 通过以下三种方式为自己和客户提供安全保护：保护远程员工、检测并响应不断加剧的威胁 ,以及虚拟扩展安全团队以增加专业知识。有多种方法可以满足这些需求，包括：

- 利用云，解决全球远程员工使用的设备和网络的容量和数量增加问题。

- 挖掘数据以识别潜在漏洞，了解疫情期间出现的网络安全威胁的性质。
- 依靠具有丰富经验、装备精良的专家和业界领袖来抗击威胁，然后将这些最佳实践分享给其他利益相关者。

引领创新

有了基本安全措施，企业还可以借此机会来发展网络弹性策略。例如，随着混合多重云和自带设备等技术在疫情中驱动远程工作环境，零信任（在疫情之前就开始受欢迎）等解决方案再次被重视起来。零信任是一种灵活的安全框架，可在 IT 边界内提供更大的安全性，并依靠安全工具之间共享情境来保护用户、数据和资源之间的连接。

创新也要在安全框架之中进行。在我们为未来做准备时，这一点更加重要。

记住你的目的

即使我们的工作方式和工作地点可能已经改变，但我们的工作理由没有改变。在 IBM，我们的使命是：保护客户的安全。面对这一挑战，我们拥有可确保客户业务连续性和 IT 弹性的工具，以及改善未来的力量。

为了保护未来的安全，各行业的领导人应继续采取有效的基本安全措施，并利用创新和跳出传统思维模式来加速积极的变革。

通过这种平衡的企业安全方法，我们在远程工作时能够实现更好的安全性。

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