计算机世界/2020 年/8 月/17 日/第 008 版
产品潮流汇

# 后疫情期安全方面将出现的 10 种变化

ESG 高级首席分析师　Jon　Oltsik　编译　Charles

首席信息安全官应预见到对分散的安全规模、情报和自助服务日益增长的需求。

早在三月份,我从几位首席信息安全官那里听说了新冠病毒是怎样破坏了他们网络安全计划以及怎样打乱了他们工作安排。几周后,我联系了一些首席信息安全官朋友,了解到他们在疫情第二阶段的最新情况。

虽然没有人知道新冠病毒的影响何时会结束,但大家真的认识了什么是新常态。以下是我预计的 10 种变化(顺序不分先后):

1.在家工作(WFH)成为默认模式。这是一个显而易见的假设,但我们可以用数据来佐证:据 ESG 的研究,79%的 IT 高管表示,在疫情逐渐消退后,他们的部门在 WFH 策略方面会更加灵活。而且,WFH 看起来效果也不错:78%的知识型员工表示,在家工作的效率更高了,或者至少工作效率没有变化。在提高工作效率和节约办公空间方面,WFH 是赢家,导致了安全投资和工作安排等方面的很多变化。

2.安全周界现在彻底消失了。近 20 年前,当我开始从事安全工作时,一群金融服务公司成立了一家名为 Jericho 论坛的组织,它提出了去周界化的概念。虽然大多数安全专家都同意这一概念,但扩展安全措施仍然是个难题,因此网络周界仍然存在,并且随着时间的推移缓慢变化。新冠病毒可能是安全周界的最后一颗“ 棺材钉 ”。为了支持更分散的 IT 基础设施,安全控制措施将大规模地转移到端点——用户、设备、应用程序、数据,等等。好消息是,基于云的管理平面使这种架构比过去更易于扩展和操作。新周界在哪里?用户和设备(即身份)以及数据。

3.迁移到云。新冠病毒加速了云工作负载的迁移,因为与本地服务器、网络和存储设备相比,更容易管理云基础设施。为了跟上这一趋势,首席信息安全官必须加强其部门云安全人员聘用、培训和技能发展等方面的工作。现在很明显,公有云是网络安全控制、整合 SD-WAN 和安全服务事实上的基础设施。安全分析也是如此,其数据和分析引擎正在快速迁移到云端。最后,安全管理平台也同样朝着云方向发展。首席信息安全官需要新技能来迁移数据和工具,以及管理云订阅。

4.攻击面管理(ASM)的主流化。随着用户和资产变得更加分散和远程化,首席信息安全官需要更好的方法来收集、处理和分析用于网络风险管理的数据。这应该会很快发生,因为大多数企业并不清楚与网络的所有连接,很多方面会经常有所发现,例如,以前未知的设备、错误配置的服务器、默认密码、合作伙伴连接,等等。ASM 将不再那么神秘,而逐渐成为企业的必需。BitSight、Bugcrowd、CyCognito、Randori 等供应商将受益于这种转变。

5.加强策略管理。由于所有一切都变得分散,首席信息安全官需要与业务经理合作,以确定谁可以从哪里干什么,并真正使用细粒度和动态规则集来收紧他们的安全策略。一旦确定了策略,他们还需要首席信息官的帮助,构建用于策略执行和监控的基础设施。安全技术在这方面有着巨大的机会——构建直观、灵活、可扩展策略管理引擎的供应商将收益颇丰。

6.身份管理需进行彻底改革。分散的安全控制和策略管理必须以现代身份管理基础设施为基础——而不是我们在过去 20 年里拼凑起来的越来越多的各种补丁。为了简化这种迁移,身份管理也会很快迁移到云上。这对于 JumpCloud、Okta 和 Ping 等公司来说是个好消息,但我认为亚马逊、谷歌、VMware 这样的云服务提供商,当然少不了微软,也会在这方面大显身手。

7.大规模网络威胁情报。新冠病毒是网络黑社会的全球机遇,引发了新一波的诈骗和攻击浪潮。为了应对这种趋势,企业必须以前所未有的规模寻找、分析和处理威胁。这将为高端市场的威

胁情报平台和调查工具(例如,Anomali、King&Union、Palo Alto Networks、RecordedFuture、ThreatConnect 和 ThreatQuotient) 带 来增长机遇。小型企业可能会更深入地研究来自思 科、FireEye、IBM 和 Secureworks 等公司的威胁情报服务。

8.下一代人工智能和机器学习。安全部门在资产、连接、动向和威胁等方面都需要同时了解更多的信息。业务管理部门对永久性 WFH 结构的推动使得这成为了绝对的必然,而世界上没有一个安全部门能够在没有帮助的情况下跟上新现实的发展。我们目前正在迈向人工智能/机器学习,我们应该赶紧加速了。这其中蕴含着非常多的机会,而我认为像 Devo、谷歌(Chronicle)、IBM、微软、SAS 和 Splunk 这样的公司将会大展身手。

9.开始认真进行安全培训。WFH 和冠状病毒相关的骗局意味着不应再像以前那样简单地进行“ 复选框 ”式的安全意识培训了。展望未来,我认为大多数员工在安全方面都应具备一定的能力,并根据他们的表现发奖金或者采取惩罚措施。业务管理人员还要负责对员工的教育,在其部门因无知而导致出现安全泄露事件时要受到惩罚。在供应方面,供应商应该为知识型员工设计更全面的课程,以补充基本的合规培训。

10.加强安全部门和 IT 运营部门的合作。配置安全端点、云工作负载或者网络基础设施要求安全部门“ 置身其中 ”,而不是“ 袖手旁观 ”。此外,安全策略的执行和监控需要各方的协调。过去,安全部门和 IT 运营部门有不同的目标、指标和薪酬结构。考虑到以前的所有工作,企业会根据共同的项目而不是各自不同的目标来评估这些部门。这对于 ExtraHop、Netscout、ServiceNow 和 Tanium 等在这两个领域都有技术和经验的供应商来说,这应该是个好消息。如果安全供应商想跟上,他们就必须增强他们的 IT 运营能力。

Jon Oltsik 是 ESG 公司网络安全服务的创始人。