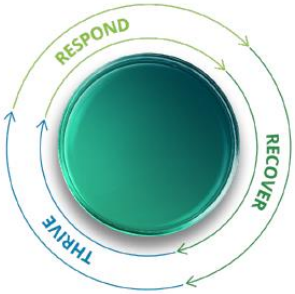
Deloitte.



全球网络COVID-19高管每周安全简报

本周报重点介绍德勤网络威胁情报中心（CTI）所识别的一些最新网络安全威胁和趋势，并提供近期有关管理网络安全风险的建议，帮助企业高管在全球COVID-19疫情背景下积极响应、稳健恢复、全面反弹。

管理远程办公带来的网络安全风险

随着越来越多的企业在疫情期间转向远程办公，企业员工使用个人设备而非企业核准的设备来访问企业网络和系统。将这些设备添加到公司网络后，增加了更多的网络安全攻击面，使得网络攻击者有更多的途径对企业进行访问和攻击，并对企业最关键资产、数据和运营环境进行渗透。**以下是本周重点介绍的一些在远程办公场景下的针对全球化企业的网络安全威胁。**

虚拟通信/团队协作应用程序的网络安全风险

在COVID-19期间，全球数以百万计的企业员工需要开展日常工作，并且企业内部、企业之间需要借助虚拟通信软件进行沟通，从而推动了虚拟通讯平台工具（例如Zoom，Microsoft Teams和Slack）的爆发式应用和推广。

我们观察到的网络安全威胁： 视频会议应用程序已经是在家里工作和学习的常态化应用，如果没有适当的安全控制，攻击者可能可以访问和参加任何会议。 此外，基于云的通信平台可能允许网络罪犯访问敏感信息，例如会议详情和对话信息。

我们建议的首要行动：
1. 确保在Zoom上的讨论不涉及高度敏感信息。 如果是高度敏感信息的讨论，请使用替代平台。
2. 在采用Zoom的个人会议应采用密码访问以确保安全，或者可以采用用户组、账号级别的安全措施。
3. 一旦会议开始，“锁定会议”以防止其他人参加。
4. 针对疫情期间需要快速部署的IT项目，IT和安全专家需要共同参与；在采用新技术时，需要重点考虑将安全控制集成到常规的IT管控措施中。

影响范围： *所有行业*
区域： *全球*

在COVID-19爆发之前，全球**27%**的用户在普通工作日是远程办公。

截至2020年3月31日
超过
60%
的用户是远程办公。

针对员工的网络钓鱼活动增加

COVID-19的经济影响刺激了一系列政府补贴，在此背景之下，员工会收到相关外部机构及其雇主的许多电子邮件，避免它们伪装成补贴的邮件进行攻击，开展防网络钓鱼的活动显得十分重要。

我们观察到的网络安全威胁： 在北美和欧洲，收到伪装成政府发放新型冠状病毒救济金的邮件接收者打开了使用宏的恶意文档的电子邮件附件。该附件自动安装了主要用于获取银行信息的恶意软件。 我们预计，随着类似更多救济金计划的出台，这种网络钓鱼威胁在很多地区国家将非常普遍。

我们建议的首要行动：
1. 提高可能会收到恶意钓鱼邮件的员工的安全意识，让其了解他们自己组织发送邮件的具体内容（如格式、时间等）。
2. 加强威胁检测和响应，主动鉴别恶意活动。
3. 确保您的企业制定了危机应对计划，并已通知员工来避免错误信息的传播。

影响范围： *政府、公共部门、银行* ***区域：*** *北美、欧洲*

在 2020 年3月13日至26日，有
超过
+400K
与COVID-19相关的垃圾邮件事件发生。

远程办公时激增使用的个人设备

在家工作的员工使用个人设备会大大增加网络攻击者访问企业内部基础设施的风险。数据和知识产权可以在这些内部基础设施中被访问。 个人设备可能没有安装最新的安全补丁程序和工具，甚至没有VPN连接来确保更安全地与业务环境进行网络连接。

我们观察到的网络安全威胁： 有垃圾邮件活动利用假冒的“Corona Antivirus”诱饵散布恶意软件。 黑客使用虚假的以新型冠状病毒（COVID-19）为主题的网站发布了“Corona Antivirus”广告，该虚假声明声称可以保护用户免受COVID-19感染； 但是，实际上该应用程序致使用户设备感染了恶意软件。

我们建议的首要行动：
1. 确保IT团队制定并实施企业自带设备（BYOD）的公司安全策略和准则，并要求在员工设备上安装公司安全软件之后才能使用此类设备进行网络连接。
2. 审查并建立用于远程访问、用户执行和行为分析（UEBA）、文件完整性监视的公司防火墙规则来为远程员工有效部署。
3. 限制未经批准的个人设备访问公司网络，并仅允许个人设备根据关键业务运营需求访问公司云服务。

影响范围： *所有行业*
区域： *全球*

在没有IT经验的情况下，美国、英国和德国有30%的公司每天都会有超过
1,000+
不安全的个人设备
连接到企业网络。

稳健恢复及全面反弹：随着COVID-19在全球范围内的形势日益严重，各企业在为“下一个常态”做准备时将以不同的速度反弹。

有关每个突出显示的主题的见解，请访问下面的文章链接。

业务连续性与经济环境
工作和经济环境将继续加剧企业内部威胁的数量。 管理层应考虑企业准备如何实施基于风险的内部威胁监测程序。

定期向管理层汇报
安全和IT管理人员应定期向企业高级管理层汇报，并确保对管理层的期望及其能接受的真实风险水平有清晰的了解。 早期的潜在攻击造成的威胁仍然存在于企业环境中，并将带来持续升高的风险。

客户需求恢复
随着市场从COVID-19疫情中恢复，消费者安全、隐私和法规方面的审查可能会受加州消费者隐私法案（CCPA）、欧洲通用数据保护法规（GDPR）、南美的各种隐私法规、中国的个人信息和重要数据监管要求而增加。 这正在改善全球市场中企业和行业的网络态势。

数字化能力
企业应考虑在不断扩大的数字化能力的同时，平衡日益新增的网络风险。 新兴技术通常会给那些希望暴露企业数字生态系统弱点的网络犯罪分子提供了一个诱人的机会。 缺乏精密安排的网络安全规划，新产品和服务将面临更大的财务、品牌和监管风险，这可能会减缓企业的发展及其市场渗入。

托管安全服务
许多国家仍然没有弹性的网络安全基础设施、高效而敏捷的研究机构，以及准备就绪的应急计划。 投入更多的技术、资源和人员来加强网络安全状况是必要的。 在社会差距的重要性在全球获得理解的背景下，我们也可以帮助培训企业员工，以保护企业免受网络威胁。 通过培训、意识和教育来改变行为是任何新过程成功的关键。 并且通过寻找增加员工人数的方法，企业可以考虑使用托管安全服务来运行现有的安全程序，或者采用一个开箱即用的解决方案，从而使其可以更快地恢复，这样对整个企业的压力会更小。

在COVID-19疫情期间我们将在您身边帮助您

相关德勤文章：

- **The heart of resilient leadership: Responding to COVID-19 (2020年3月)**
- **Manage rapid employee return and ramp up future state (2020年3月)**
- **Design digitally enabled flexible work arrangements (2020年3月)**
- **Cyber management critical for remote workforces (2020年4月)**

德勤网络安全服务：帮助企业更好地解决复杂的网络问题，从容应对未来的挑战。 面向企业、人员和全球有更智能，更快捷，更互联的特点。 作为网络安全咨询领域公认的领导者，德勤可以更好地帮助企业将网络安全战略和投资与业务重点保持一致，提高网络威胁意识和可视性，并增强企业在面对网络安全事件时的应对能力。 凭借专业洞察力、技术创新能力以及优秀的企业网络安全解决方案，德勤网络安全团队在这个安全无界的时代，帮助企业畅行无限。

德勤中国网络安全服务合伙人


薛梓源
德勤中国网络风险服务领导合伙人
+86 10 85207315
tonxue@deloitte.com.cn


江玮
东区
+86 21 23127088
davidjiang@deloitte.com.cn


何晓明
北区
+86 10 85125312
the@deloitte.com.cn


郭儀雅
南区香港
+852 28526304
evakwok@deloitte.com.hk


冯晔
东区
+86 21 61411575
stefeng@deloitte.com.cn


石沛恩
东区
+86 21 33138366
nathanshih@deloitte.com.cn


肖腾飞
北区
+86 10 85125858
frankxiao@deloitte.com.cn


Pihkanen, Miro
南区香港
+852 28526778
miropihkanen@deloitte.com.hk


Kukreja, Puneet
东区
+86 21 33138338
puneetkukreja@deloitte.com.cn


张震
东区
+86 21 61411505
zhzhang@deloitte.com.cn


何微
南区大陆
+86 755 33538697
vhe@deloitte.com.cn


馬國鈞
南区香港
+85228521086
lukema@deloitte.com.hk

欲了解更多联系信息，请访问 Deloitte.com/covid 或 Deloitte.com/cyber