Deloitte.

德勤

COVID-19疫情爆发加大内部威胁

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

2020 年 5月 总第六期

内部威胁参与者正在利用漏洞

COVID-19疫情引发了大规模的劳动力转移。如前几周所述，无数员工、承包商和第三方前所未有地过度到远程办公，使得许多组织未做好准备监测或发现由于以下原因而可能导致的内部威胁：未经授权的远程访问、个人设备的滥用、对云基础设施的日益依赖、薄弱的密码和身份验证策略、不安全的网络和打印设备以及公司资产的滥用。 同样关键的是，COVID-19造成的动荡正为恶意内部人员提供肥沃的土壤。由于内部人员处于独特的位置，可以规避外围网络监控并暴露组织的安全漏洞，因此这些事件可能尤其具有破坏性。事实上，内部威胁的平均成本在过去两年中猛增了30%以上，达到每年1,145万美元。 本周，我们着重指出日益增加的恶意内部威胁风险。

92% 内部威胁案件发生之前，会发生负面的工作事件，例如解雇、降职或与主管发生争议

59% 自愿或非自愿离开组织的员工表示，他们随身携带敏感数据

威胁者收买内部员工访问个人用户数据——*影响范围：全部 | 区域：全球*

2020年5月4日，新闻媒体Vice报道说，一名身份不明的威胁者贿赂了Roblox员工，访问了流行的在线视频游戏的后台客户支持界面。该访问使威胁者可以查看超过1亿用户的个人信息，并可能更改密码并禁用双因素认证的帐户身份验证。威胁者首先向内部人员付款，内部人员为威胁者查找用户数据，然后对客户分别进行网络钓鱼。目前已通过LinkedIn的个人资料识别出了有嫌疑的员工。

被解雇的员工干扰了医疗用品的交付——*影响范围：全部 | 区域：全球*

2020年4月16日，美国司法部指控一家医疗器械包装公司的一名前雇员对其前雇主的运输系统进行计算机入侵，从而破坏了向医疗保健提供者的个人防护设备（PPE）的交付。在受雇期间，被告具有访问公司运输系统的管理员权限。入侵发生在被告解雇后，距离他收到最后一笔薪水仅三天。 据称，被告使用的是他在被雇佣期间创建的虚假帐户，被告编辑了115,580条记录、删除了2,371条记录后停用了该虚假用户帐户。

注意：内部威胁的类型

内部人员是指具有内部知识或访问权限、可能给组织带来危害的人。内部人员威胁可能会对组织的任何方面产生负面影响，包括员工或公共安全、声誉、运营、财务、国家安全和业务连续性。

信息盗窃/泄露
通过内部人员访问来窃取、利用或发布信息

物理安全威胁
通过内部人员访问来窃取重要物品或违反安全策略

间谍
通过内部人员访问获取敏感信息，影响国家或公司的安全和公共安全

恐怖主义
通过内部人员访问实施或促进暴力行为，作为政治破坏或者胁迫的一种手段

行为风险
被视为对客户不利或可能损害市场诚信的行为，例如，违反行为准则

供应商风险
承担与外部实体订立合同所涉及的风险

贿赂/腐败
内部人员接受金钱、商品或其他形式的补偿，从而改变其行为以使贿赂者受益

安全妥协
通过内部人员访问来促进和凌驾安全措施，例如权限提升，恶意软件攻击等

内幕交易
通过内部人员访问获取内部信息或影响市场汇率的交易

职场暴力
使用暴力或暴力威胁影响他人并影响组织员工的健康和安全

破坏
故意破坏设备或IT以造成特定伤害，例如，插入恶意代码，关闭服务等

违反政策
承担内部人员违反组织安全性和可接受使用政策的风险

共谋
与其他内部或外部方的秘密合作或欺骗性协议，以进行欺诈或损害组织

强迫
使用武力或威胁说服某人做某事的做法

其他
捕获不断变化的威胁场景，包括先前示例中未涵盖的新型威胁

预计在COVID-19期间最为流行

这些威胁可以通过以下方式实现：

恶意
故意**滥用职权，并使经济或个人利益**遭受损害

忽视
缺乏**对安全责任的**认识和理解

自满
*采取**宽松的**安全措施，与组织期望**相反***

复原与发展| 确保“下一个常态”的内部威胁管理

尽管大多数内部威胁是由疏忽行为引起的，但是COVID-19引起的动荡为内部威胁利用者提供了绝佳的机会，可以滥用其帐户权限或者技术知识泄露敏感数据、进行欺诈或破坏业务运营。根据观察到的活动和公开披露的信息，德勤CTI确信恶意内部威胁正在上升。

以下是一些应对威胁的方法：

确定高风险内部人员。通常，大多数恶意内部人员是高风险人员，他们一般：最近被终止或休假、有违反IT政策的历史、请求了不当访问权限、或不满的人。但是，在疫情期间，组织应该意识到COVID-19的影响可能给以前可能没有考虑过此类活动的员工带来压力，绝望甚至机会主义的情况。请注意，内部人员可以不仅是使用其经验证的访问权限来实施恶意行为的员工，还可以是合同工或供应商。重要的是要从企业的各个部门（例如HR、举报人专线、网络、欺诈等）中识别出潜在的风险指标并整合，以主动发现可能会遇到内部威胁的潜在员工。

保持领先. 内部人员的方法、策略和掩盖其足迹的尝试将不断进化，这意味着内部威胁方案及其分析的预警也应不断进化。这可以通过反馈机制来实现，该机制包括对正在进行的和历史案例以及调查的分析。

信任但要验证. 维护计算机、移动设备和可移动介质清单的准确性，并进行例行和随机审核以跟踪资产。

访问控制. 遵循最小特权原则，根据员工的角色和职责为他们提供所需的、最小系统访问权限。

寻找异常. 根据FBI的内部威胁计划，对内部威胁的检测应使用基于行为的技术。考虑使用能够监视用户活动并标记异常行为的用户行为分析（UBA）工具。

监控内部威胁指标. 组织可能会发现员工因为担心在COVID-19期间失去工作而感到不安全感和压力，并可能尝试通过主动采取恶意措施来“保护自己”。通过实施移动和云安全解决方案，例如云访问安全代理（CASB）（一种在云中访问资源时可帮助实施安全策略的工具），组织可以开始识别确定潜在风险指标和远程员工表现出的高风险行为。这可用于识别内部威胁，并了解薄弱或缺失的环节。

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
电话：+86 10 8520 7315
电子邮件：tonxue@deloitte.com.cn


江玮
东区
电话：+86 21 2312 7088
电子邮件：davidjiang@deloitte.com.cn


何晓明
北区
电话：+86 10 8512 5312
电子邮件：the@deloitte.com.cn


郭仪雅
南区香港
电话：+852 2852 6304
电子邮件：evakwok@deloitte.com.hk


冯晔
东区
电话：+86 21 6141 1575
电子邮件：stefeng@deloitte.com.cn


石沛恩
东区
电话：86 21 3313 8366
电子邮件：nathanshih@deloitte.com.cn


肖腾飞
北区
电话：+86 10 8512 5858
电子邮件：frankxiao@deloitte.com.cn


Pihkanen, Miro
南区香港
电话：+852 2852 6778
电子邮件：miropihkanen@deloitte.com.hk


Kukreja, Puneet
东区
电话：+86 21 3313 8338
电子邮件：puneetkukreja@deloitte.com.cn


张震
东区
电话：+86 21 6141 1505
电子邮件：zhzhang@deloitte.com.cn


何微
南区大陆
电话：+86 755 3353 8697
电子邮件：vhe@deloitte.com.cn


马国均
南区香港
电话：+852 2852 1086
电子邮件：lukema@deloitte.com.hk

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