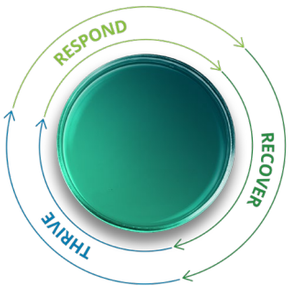
Deloitte.



COVID-19疫情爆发加大供应链网络安全威胁

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 总第五期

在COVID-19背景下日益严重的网络威胁可能威胁到供应链安全

40%
制造商

接受调查的企业表示，在过去12个月中，他们的运营受到了网络安全事件的影响*

制造业始终是**最受关注的行业之一**

重大网络安全风险

在2017年至2018年期间，网络安全事件增加了

- 3.5倍的勒索软件
- 2.5倍的欺骗攻击
- 0.7倍的鱼叉式钓鱼攻击

33万美元
以物联网为重点的网络安全事件造成的平均财务影响

750万美元
2018年数据泄露造成的平均财务影响

87% 未授权的访问

86% 运营中断

85% 知识产权盗窃

在过去的60天里，与COVID-19相关的供应链攻击有所增加，包括对知名组织（例如UPS）发起的针对性攻击。

明确安全要求及网络风险管理实施程序，以评估第三方（甚至第四方）服务，帮助组织降低对其供应链进行攻击的风险。

在供应链环节，众多供应商通过电子邮件进行通信。

2020年4月上旬，美国联邦调查局（FBI）发表声明，指出与COVID-19疫情相关的企业电子邮件入侵（BEC）预计会增加。恶意攻击者利用这些业务关系，通过电子邮件入侵攻击的方式来诱骗一个或多个供应商向其汇款。根据美国联邦调查局（FBI）的数据，2019年BEC攻击给组织造成的损失约为17.7亿美元。

与海外实体开展业务的公司更容易受到BEC攻击，因为其员工可能无法识别国外供应商表现出的异常商业行为。

供应链中的网络安全漏洞正在增加

在全球性疫情防控的背景下，更好地了解供应链是如何变化的，可以帮助零售商和其他企业在这个艰难时期过后获得安全、适应并向前发展的能力。在2019年，40%制造商的运营受到网络安全事件的影响。由于供应链已经面临实体关闭、社交距离而导致的运营活动减少以及为了生产个人防护设备造成的运营改革等风险，因此网络安全事件造成的中断可能会产生更加严重的影响。
本周我们重点介绍针对供应链要素的不断上升的威胁（在4月22日至4月28日的详细威胁报告中已识别）。

网络钓鱼活动影响知名物流公司

影响范围：所有行业|区域：全球

2020年4月，德勤CTI观察到两次网络钓鱼活动和一种恶意软件，均使用COVID-19作为诱饵。这些COVID-19网络钓鱼活动冒充诸如联邦快递，DHL和UPS之类的知名物流公司，并使用恶意附件攻击美国医疗服务提供商。

商业电子邮件入侵（BEC）导致欺诈性的资金转移

影响范围：所有行业|区域：全球

2020年4月15日，德勤CTI观察到多次使用COVID-19为主题进行商业电子邮件入侵攻击企业的垃圾邮件事件。在这些攻击过程中，攻击者使用了COVID-19相关主题的电子邮件，例如工资单，电汇或法律关注的社会工程主题，要求其目标进行欺诈性的资金转移。

根本原因| 在COVID-19爆发期间降低运营技术（OT）环境中的风险

随着全球范围内许多领先的制造企业在竞相生产关键的COVID-19防疫物资，例如个人防护设备和呼吸机，甚至是新疫苗。这些制造企业也可能成为网络攻击者盗窃或勒索的目标，攻击者试图利用漏洞获得被攻击者宝贵的知识产权。在运营环境中潜在的损坏可能会极大地影响收入，并可能导致企业倒闭。在延伸的供应链中管理风险非常具有挑战性，对于大型公司，无论是将某些内容嵌入供应商的子组件中，还是软件产品，可能需要考虑成千上万个不同的第三、第四和第五方。随着更多的连接组件、通信和存储数据风险的增加，攻击面也在扩大。这次COVID-19引起的不确定性向我们表明，我们并不如我们预期的那样做到了万事俱备。在IT和OT生态圈之间，许多领域存在人员、流程和技术方面的重叠。下面重点介绍制造企业在融合IT和OT时应注意的主要网络问题。

OT系统特性*	网络问题
IT与OT融合的复杂性	• OT通常由工程师，自动化及运营（团队和人员）管理而非IT。 • 难以让某一个团队独立承担所有OT系统和基础安全的职责。 • 在缺乏详细评估的情况下，企业通常不会执行传统的应用安全控制，例如补丁或漏洞扫描。 • 对工业流程、技术资产、网络架构、风险和安全性方法的深入了解通常至关重要，因此需要跨IT和OT的整合团队一起协作。
更新悖论	• 无法使用单一方法来修补或更新系统。 当检测到漏洞时，可能会使响应变得困难，因而经常需要采用深度防御方法。
传统系统的局限性	• 许多OT系统的生命周期很长（超过10年），并且原系统不是为构建外部连接建造的。 随着边缘计算，云平台的增加以及其他智能工厂技术的应用，互联互通不再仅仅是可选项。
基础设施不稳定	• 较旧的设备通常使用专有的通信协议，如果网络上的数据通信增加，则很容易导致这些协议中断。 • 现有的网络和相关体系结构并非为处理需采用这些新技术的数据流而设计。 • 只有有限的审查流程可以识别或发现已经购买和部署的新技术相关的安全风险，这同时增加了攻击风险，从而影响新技术和同一网络上其他原有技术的使用。
运营局限性	• 实时性能通常至关重要。 引入其他安全控制措施可能会导致延迟。 • 进行网络变更或其他变更可能需要宕机或停机， 因维护而导致的宕机时间应严格限制在最低限度内。 • 由于产品本身属性或合同限制或设备使用年限等因素，通常无法进行软件更新。 • 建立和明确跨职能（IT和OT）的责任至关重要。 考虑到各个小组本职工作和擅长能力，使用跨职能团队应对网络安全风险至关重要。

*来源: 智能工厂的网络安全

稳健恢复和全面反弹| 确保“下一个常态”的供应链安全–聚焦智能工厂

在COVID-19中，制造业组织改进流程和协议的同时，他们应该投资于企业（IT和OT）的整体网络管理计划，以识别、保护和响应网络攻击，并从网络攻击中恢复。
具体来说，在开始建立有效的网络安全计划时，应考虑以下四个步骤：

对开发的新技术进行网络安全成熟度评估。

智能工厂中的每个新应用在试验或生产阶段中，都会面临新的威胁。评估应包括OT环境，业务网络和更深层次的制造业网络安全风险，例如IP保护、控制系统、连接的产品，以及与工业生态系统密切相关的第三方风险。

建立正式的网络安全治理架构，考虑OT环境下应对COVID-19的转型。

对于围绕业务的治理架构来说，允许IT和OT团队在适用的领域协作对管理业务非常重要。制造业安全团队应与现场密切合作，以考虑风险和适当的缓释策略。

根据COVID-19情况下的风险概况和需求确定行动的优先级。

以网络安全成熟度评估的结果作为输入，设计战略和路线图，并针对与组织的风险承受能力和管理能力相对应的风险，与高级管理层及董事会（在适当情况下）进行沟通汇报。

建立与COVID-19相关的安全技术转型。

由于许多智能工厂用例仍处于计划和早期阶段，因此现在需要考虑项目与网络安全风险程序的一致性。在项目的前期设计或开展阶段融入适当的安全控制要求。需要考虑的重要控制措施包括使用安全的网络分段模型、部署被动监控解决方案、安全的远程访问、可移动媒体设备的控制、改进的特权访问管理以及执行一致的备份流程。

在COVID-19疫情期间我们将在您身边帮助您

相关德勤参考资料：

- Responding to COVID-19 with business resilience, trust, and security
- COVID-19 Government Response Portal
- Privacy and Data Protection in the Age of COVID-19
- GDPR: How to make your business more resilient against data protection breaches in light of the COVID-19 crisis?

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
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


何薇
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