企业如何应对供应链带来的网络安全风险

2024年6月14日

EY 安永

Building a better working world

企业如何应对供应链带来的网络安全风险

2024-6-14

在数字化浪潮下，供应链的安全防线正受到前所未有的考验，成为网络攻击的重点目标。网络攻击不仅可能导致巨大的经济损失，还可能对企业的声誉造成不可逆转的损害。本文将探讨全球范围内供应链面临的网络攻击威胁现状、供应链成为攻击重灾区现象的成因，以及如何构建有效的供应链安全计划和策略。

一、供应链侧网络攻击成为业务持续经营的巨大隐患

近年来，一些影响深远的供应链攻击已经证明了其对全球组织的破坏力。如NotPetya勒索软件，它通过感染供应链中的一个环节—某会计软件进行传播，导致一家全球物流公司超过50,000个端点感染[1]。全球范围内的企业面临的NotPetya勒索软件攻击并造成的损失预计超过100亿美元[2]。

此外，近期一家美国领先健康保险服务提供商的信息科技子公司的医疗支付交换平台系统遭到勒索软件攻击,为集团造成了8.72亿美元的损失。该攻击扰乱了美国医疗系统，造成了全美范围内医疗服务和保险理赔业务的严重中断。

	NotPetya勒索软件攻击	美国某健康保险服务提供商遭受勒索软件攻击
威胁类型	勒索软件，以加密文件要求支付赎金。	
受攻击的供应链环节	通过某会计软件的更新程序传播，影响使用该软件的组织和企业。	针对其子公司医疗支付交换平台系统，影响了医疗服务提供者和相关保险公司。
缺陷	会计软件的更新机制缺乏足够的安全验证，易受攻击者劫持。	子公司的信息系统安全措施不足，未能有效防御外部攻击。
后果影响	经广泛传播影响全球多个国家的组织,造成严重的数据和经济损失；对关键基础设施造成破坏。	影响了美国的医疗系统和保险理赔处理,造成了8.72亿美元经济损失和业务中断；泄露了大量敏感数据。

表1 供应链网络攻击案例对比解析

由于供应链中不同组织之间的相互连接和依赖，这种攻击能够迅速从一个单一的点扩散到整个网络，影响到全球范围内的公司。包括勒索软件在内的各类网络攻击给业务的持续经营造成了严重的干扰，并会对声誉产生重大影响。网络攻击通常会导致生产和发货的延迟、库存问题及由于供应链的相互联系而波及多个行业的运营中断。其后的持续影响还包括财务损失、交付失败和延误所造成的声誉损害。

根据Centrify的一项研究[3]，在安全漏洞或事件发生后，65%的客户对组织失去信任。世界经济论坛[4]还指出，中断可能导致工业生产在1-2年内下降4%-5%。供应链安全事件的影响可能会对声誉和信任造成毁灭性的影响；该事件的影响可能会影响全球的客户、利益相关者和其他公司。

除了损害公司的形象外，事故还可能产生法律监管后果。一些公司因没有采取适当的治理措施（如数据保护和安全等）而面临罚款、处罚和清算。

---

[1] Ransomware: The key lesson Maersk learned from battling the NotPetya attack https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/#google_vignette

[2] The Untold Story of NotPetya, the Most Devastating Cyberattack in History https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[3] Analyzing Company Reputation After a Data Breach https://www.varonis.com/blog/company-reputation-after-a-data-breach

[4] Why are supply chains facing disruptions, and how long will they last? https://www.weforum.org/agenda/2022/07/supply-chain-disruptions/

二、为何供应链成为网络攻击的重灾区?

供应链的全球互联性和复杂性使其成为网络攻击的首要目标。导致供应链易受攻击的关键原因有:

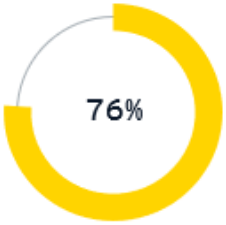
1. **网络威胁复杂多样:** 复杂的供应链场景为攻击者提供了许多可供利用的载体，从而导致多种多样的网络攻击持续发生，包括内部威胁、恶意软件和勒索软件、敏感数据暴露、固件攻击、实物盗窃和入侵、未经授权访问物联网设备、供应链中介的违规行为、社会工程等。

2. **安全漏洞隐蔽分散:** 在现代供应链中，发现和弥补安全漏洞对企业而言是一项极大的挑战。供应链涉及众多环节和多方参与者，企业对于识别上下游合作伙伴的安全漏洞往往存在滞后性，这使得攻击者能够长期接触漏洞并获得巨大的经济回报。

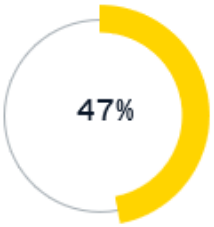
3. **供应商管理意识与资源不足:** 许多企业缺乏足够的供应商管理意识和资源来有效地识别和控制供应链安全风险，特别是对于中小企业来说，由于缺乏有效的安全支持能力，无法应对供应链上下游带来的安全挑战。根据2022年世界经济论坛[5]发布的《全球网络安全展望》，39%的组织已受到第三方网络事件的影响。这项调查显示，许多组织并未充分评估其供应链中的第三方，并且可能未被告知他们参与事件的情况。

4. **运营技术（OT）安全默认缺失:** 随着工业4.0的到来，运营技术（OT）在供应链中的使用正随着IT和OT资产的互联融合而快速增长。然而，根据欧洲网络安全局（ENISA）[6]在2022年进行的一项调查，76%的组织缺乏OT供应链网络安全的专门角色和责任；仅47%的组织为OT供应链网络安全分配了专属预算。其中，制造业往往比其他行业更容易受到针对性攻击。根据IBM网络安全专家2022年的一份报告[7]，制造业占所有OT攻击的58%。因为在制造业中大量使用的OT设备在默认情况下大多没有安全保护。

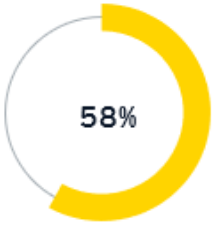
5. **风险评估执行积极度低:** ENISA的调查数据揭示了一个令人担忧的事实，即只有37%的组织积极地对其供应链进行风险评估。供应链领域缺乏风险评估的情况也解释了供应链攻击成功案例持续增加的原因。



76%的组织在OT供应链网络安全方面缺乏专门的角色和责任。



47%的组织为OT供应链网络安全分配了单独预算。



在所有针对操作技术（OT）的攻击中，制造业占了58%。

37%的组织积极开展供应链风险评估。

图1 供应链安全相关的多项调查关键数据概览

[5] Global Cybersecurity Outlook 2022 https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[6] Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[7] IBM X-Force Threat Intelligence Index 2023 https://www.ibm.com/reports/threat-intelligence

三、如何构建供应链安全计划和策略?

安永《2023全球网络安全领导力洞察研究》显示，尽管供应链带来的风险广泛存在，网络安全发展中企业更专注于财务风险，而网络安全成熟型企业（38%）高度关注供应链风险的可能性几乎是网络安全发展中企业（20%）的两倍；在安永2021年全球信息安全调查中，67%的CISO（首席信息安全官）不相信其供应链可以有效抵御网络威胁或从网络威胁中恢复过来。那么，供应链安全到底是什么?供应链安全是指企业供应链中涉及的所有流程、资产和基础设施免受威胁的保护和风险管理。由于网络攻击的高度危险性，应在整个供应链的基础设施中建立安全。构建供应链安全计划和策略需要一个全面的视角，涵盖人员、流程和技术三个方面。

人员

人员是供应链安全中最关键但也可能是最薄弱的环节。构建供应链安全计划中人员方面的策略可以包括:

- **强制性培训计划:** 为内部员工和外部供应商合作伙伴提供定期的安全意识培训，以增强其安全知识，并了解其如何影响供应链。培训内容应包括敏感信息保护意识、遵守安全协议、权限管理、OT技术和社会工程等。
- **桌面演练:** 设计切合实际的桌面演练，以促进事件响应的协作，确保所有人员都为潜在的事件做好准备。
- **内部认证:** 制定内部认证计划，确保员工具备执行安全相关任务的资格和能力。

流程

供应链的运作在很大程度上依赖于明确定义的流程。因此，稳健的管理流程将有助于减轻一部分供应链安全风险。流程方面需要重点关注的要素包括:

- **治理和合规:** 供应链安全倡议的第一步是调整政策、标准，以及数据保护制度。通过参考一些重要的网络安全实践和标准，将标准化安全控制纳入供应链，并实施法律要求的隐私与合规控制，有效增强其整体安全态势。
- **第三方管理:** 对供应商和合作伙伴进行风险评估、分级和持续监控，签署服务级别协议，建立第三方风险数据库；为供应商建立一个安全的沟通渠道，确保在发现新的漏洞时及时通知所有各方。
- **事件响应运行手册:** 制定详细的事件响应运行手册，包括恢复点目标（RPO）和恢复时间目标（RTO）。
- **网络资产生命周期管理:** 对网络资产进行全生命周期管理，确保从采购到停用的每个阶段都符合企业的安全标准。

技术

技术是保护供应链免受网络攻击事件影响的工具。构建供应链安全计划中技术方面的策略包括:

- **安全控制塔:** 开发和实施供应链控制塔，利用实时数据提供关键的网络安全指标。
- **供应链架构重新设计:** 采用"安全设计"概念，重新检查和优化设计其企业资源规划（ERP）以及数据架构和基础设施。
- **供应链DevSecOps:** 实施DevSecOps，通过持续集成和部署最新的OT、物联网设备和软件更新，并实施监控和自动化，将安全整合到软件开发、运营的每个阶段。
- **数据保护:** 通过数据安全治理、数据加密和数据防泄漏技术保护敏感数据。
- **安全性测试:** 对OT和IoT设备进行安全性测试，包括代码审查、静态/动态应用程序安全测试等，确保没有后门和关键漏洞。
- **身份访问管理（IAM）:** 利用单点登录（SSO）和多因素身份验证（MFA）等IAM技术在整个组织中集成安全性，实施基于角色的身份和访问管理解决方案来保护资源。

四、安永支持企业做好供应链安全建设工作

安永为企业提供一系列服务来帮助构建和维护其供应链安全。这些服务包括但不限于：

供应链安全体系转型咨询

- **建立或加强供应链安全计划和策略：**提供适当的治理、流程和风险框架，包括管理和监督、政策和标准、第三方清单、风险管理方法和模型等。
- **定义供应链安全管理要求：**定义基本的信息安全要求，以支持所有产品和服务的采购和供应，如产品的制造或装配、业务流程采购、软件和硬件的组件、知识流程采购和云计算服务等。
- **设计供应链安全管理流程：**围绕供应商关系生命周期，为供应商关系规划、供应商选择、供应商关系协议、供应商关系管理、供应商关系终结的全过程提供可落地的标准流程。

供应链安全风险评估：

帮助企业了解供应链的结构，识别供应链中可能存在的安全风险（如恶意篡改、假冒伪劣、供应中断、信息泄露等）；确定风险的可能性和影响程度，对风险进行分类和优先级排序；根据风险评估的结果，制定风险处置计划。

供应链安全联合运营

- **供应商安全评估执行：**使用企业特定安全要求与框架，开展现场/远程调研和审查供应商安全能力,识别基于业务场景的实际安全风险，制定风险控制措施，确保其符合企业的安全标准。
- **安全培训：**为供应商提供安全培训，提高其供应链安全意识与能力，加强供应商对于公司服务的安全重视程度。
- **持续监督：**建立监督机制，持续评估供应商的安全表现，指导供应商优化提升自身安全管理水平。

技术实施和支持：

提供专业的技术支持，推荐适合企业需求的安全技术工具和解决方案，制定相关策略并协助实施，赋能企业掌握完整功能，有效预防、监控、缓解企业供应链安全风险。

此外，安永还可以通过政策和标准制定、事件响应计划制定、合规性评估等专项咨询服务助力企业优化供应链安全管控，建立一个更加安全和有韧性的供应链，以抵御不断演变的网络威胁。

结语

安全措施的实施对于发现、保护和应对因网络问题导致的供应链中断至关重要。供应链中可能发生的网络攻击的受害者不仅会遭受财务损失，还会遭受严重的声誉损害，从而削弱供应链合作伙伴、客户和利益相关者之间的信任。

为了建立一个有韧性的供应链，企业必须制定一个包括人员、流程和技术方面的供应链安全计划。一个有韧性的供应链能够抵御各种挑战，有助于公司实现长期业务目标，在充满挑战的业务环境中为持续增长、盈利能力和成功做好定位。然而，实施安全保护不是一次性的努力，它需要持续评估、主动改进和长效治理。

如需了解更多信息，欢迎联系我们：

高轶峰
大中华区网络安全与隐私保护咨询服务
主管合伙人
安永（中国）企业咨询有限公司
kelvin.gao@cn.ey.com

张楠弛
风险管理与决策创新咨询服务合伙人
安永（中国）企业咨询有限公司
nancy-nc.zhang@cn.ey.com

司昌伟
风险管理与决策创新咨询服务高级经理
安永（中国）企业咨询有限公司
dylan.si@cn.ey.com

张羽
风险管理与决策创新咨询服务高级顾问
安永（中国）企业咨询有限公司
skyler.zhang1@cn.ey.com

安永 | 建设更美好的商业世界

安永的宗旨是建设更美好的商业世界。我们致力帮助客户、员工及社会各界创造长期价值，同时在资本市场建立信任。

安永坚持创新与技术投入，通过一体化的高质量服务，帮助客户把握市场脉搏和机遇，加速升级转型。

在审计、咨询、战略、税务与交易的专业服务领域，安永团队对当前最复杂迫切的挑战，提出更好的问题，从而发掘创新的解决方案。

APAC no. 03020050
ED None.

ey.com/china

关注安永微信公众号
扫描二维码，获取最新资讯。