简译版

采取四项措施减轻供应链和价值链网络攻击

非官方中文译文·安天技术公益翻译组 译注

文档信息			
原文名称	4 things you can do to minimize cyberattacks on supply and value chains		
原文作者	丹尼斯·麦克德莫特（Dennis McDermott）	**原文发布日期**	2021 年 4 月 8 日
作者简介	丹尼斯·麦克德莫特是 OpenText 身份和访问管理部门高级产品营销经理。		
原文发布单位	Help Net Security		
原文出处	https://www.helpnetsecurity.com/2021/04/08/minimize-supply-chain-cyberattacks/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
摘要	如果供应链或价值链中的第三方遭遇数据泄露，企业该如何保护自己不受影响呢？除了采取基本安全措施（例如，对第三方用户实施最低权限原则，初次使用时重置管理口令）外，企业还可以本文所述四种措施减轻与第三方访问相关的风险。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

采取四项措施减轻供应链和价值链网络攻击

丹尼斯·麦克德莫特

2021 年 4 月 8 日

供应链攻击的目标是大多数企业安全计划中最薄弱的方面：第三方访问。

SolarWinds 攻击事件是一种经典的供应链攻击，它会感染下游企业，遍历受害者的客户、供应商和其他第三方，从而未经授权地访问其本地和云系统。

此次攻击事件可谓“前无古人”。它通过提权、伪造访问令牌以及其他未被发现的更改，将核心安全产品转变为恶意软件交付系统，该系统提供了至少 9 个月的访问权限，使攻击者能够未经授权地访问敏感数据。

最大限度地减少供应链网络攻击

如果供应链或价值链中的第三方遭遇数据泄露，企业该如何保护自己不受影响呢？除了采取基本安全措施（例如，对第三方用户实施最低权限原则，初次使用时重置管理口令[避免“username:admin，password:admin”组合]）外，企业还可以采取下述四种措施减轻与第三方访问相关的风险。

1. 为连接到企业的所有事物（人员、系统和设备）提供身份

通过这一措施，企业可以建立所有第三方实体及允许其访问的系统和数据之清单——这是第三方风险管理的基本组成部分。之后，企业可以使用诸如基于角色或属性的访问控制、自动化的身份生命周期管理、基于策略的身份验证和授权、多因子身份鉴别（MFA）等技术创建控制措施，以减轻未授权或不恰当访问的风险。

2. 利用身份代理技术验证凭证并增加身份鉴别要求

美国国土安全部（DHS）网络安全和基础设施安全局（CISA）指出，SolarWinds Orion 攻击事件利用了伪造的 SAML 令牌，能够在未经检测的情况下，未经授权地访问企业资源。

企业可以使用高级云身份代理，针对本地或远程数据存储区，分析和验证令牌属性（例如，用户凭证、设备声誉、不可能的位置情况等），从而识别和拒绝伪造的令牌。根据验证结果，企业可以拒绝请求、原样传递请求，或者创建更复杂的令牌，以调用强大或多因子身

份鉴别来增强可靠性。

3. 第三方身份的访问管理

访问管理能够衡量企业身份创建和管理程序的有效性。访问认证过程是身份管理计划的关键，要求批准者、发起者和其他认证者验证并证明用户具有正确的访问权限。如果验证者发现错误的访问授权，则说明存在供应链攻击。

例如，每个月或每个季度对高风险应用程序进行认证，可以避免数月的未授权访问。认为“访问证书是发现攻击的关键或基础”可能想的太简单了；但是，这可以作为身份管理策略的一部分，是一种低风险、高回报的阻止攻击的方法。

4. 集中管理所有的第三方访问

集中管理第三方身份是有可能的，而且势在必行。大多数企业直接在业务应用程序线（孤岛）中管理第三方用户，这使他们面临极大的风险。例如，许多第三方用户可以访问企业内的多个云和本地系统。但是，管理业务线应用程序访问权限的人员（或系统）通常不具备可见性，不知道该用户是否也能访问其他数百个系统。

除非在配置访问权限之前已知用户的账户和访问权限，否则企业无法采用适当的策略来应对用户带来的风险。缺乏这种可见性会导致高风险的情况，例如，对“特权”用户的身份验证不力，以及无法在企业范围内查看每个用户的访问权限。

集中管理第三方用户的身份，实现访问管理的自动化，可以广泛、深入地了解每个用户所面临的风险，从而正确地应用和执行策略。企业也可以通过适当的解决方案，实现第三方用户生命周期的自动化，以实时响应事件，自动更改或撤消用户访问权限。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全企业、IT 企业选择安天作为检测能力合作伙伴，目前，安天的威胁检测引擎为全球超过八十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

安天是中国应急响应体系中重要的企业节点，在“红色代码”、“口令蠕虫”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体（如 APT 组织）及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

安天实验室更多信息请访问： http://www.antiy.com（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： http://www.antiy.cn

安天移动安全公司（AVL TEAM）更多信息请访问： http://www.avlsec.com