数字化环境下的供应链网络威胁

文 / 赵毅

当前经济环境下，互联网技术的发展和广泛应用使传统商业模式产生颠覆性变革，在营销拓展、生产制造、运营服务、资源整合等方面开启了全新的经营模式。企业数字化转型过程中，数据是企业的燃料，同时客户数据对黑产和竞争对手具有极高吸引力，因此除了要应用好数据，还要对其进行保护。

从数据流转过程看，一方面，数据在企业内部运作时，信息系统、企业员工都可以接触到敏感数据；另一方面，数据也在外部流转，更多供应商和合作伙伴也可以接触到敏感数据。当有人利用外部伙伴或供应商窃取数据时，就会发生供应链攻击，这种第三方威胁改变了数字化转型前传统企业模式的攻击面。由于数据在外部第三方合作伙伴或供应商应用过程中企业无法对其进行控制，因此第三方是数字化转型企业生态系统中最薄弱的环节。

由第三方供应商引起的数据泄露事件并非少数，2013 年零售巨头塔吉特 Target 因第三方 HVAC 供应商导致上亿用户信息泄漏，预计损失成本为 2.92 亿美元；2014 年美国最大的家庭装饰品与建材零售商家得宝 HomeDepot 因黑客利用第三方供应商网络入侵导致数据泄露，预计损失成本为 1.98 亿美元；2017 年 7 月，Verizon 公司 1400 多万用户个人资料因第三方供应商 NICE Systems 云服务器安全配置不当遭到外泄。Ponemon Institute 研究报告表明，56% 的企业数据泄露事件由其供应商造成。

监管部门对敏感数据或隐私的保护越来越关心，欧盟提出《一般数据保护法案》GDPR，适用于从欧洲收集个人信息的所有公司，罚款最高到全球总收入的 4%。例如谷歌因 GDPR 合规问题被开出 27.3 亿美元罚单。在我国，《中华人民共和国网络安全法》自 2017 年 6 月 1 日起已经实施，提出了个人信息保护的要求，并且《个人信息保护条例》也正在制定当中。在《国家网络安全空间战略》中也提出“加强供应链安全管理”

供应链网络威胁范围

企业无法知晓诸多合作伙伴 / 供应商在使用数据时对其敏感数据及隐私的保护状况，第三方风险正处在失控状态。Gartner 预测 2018 年企业重要的数字合作伙伴最高将达 143 个（2017 年是 78 个），Ponemon Institute 2017 年研究报告中显示，能够接触敏感信息的第三方平均数量比去年增加了 25%（从 378 个增加到 471 个）。这种情况下，更需要注意对 DMP 服务商、数字广告投放服务商、广告跟踪服务商、渠道商、分销商、代理商、公有云、行业云提供商、独立软件开发商 ISV、物流公司、客服公司、健康医疗机构、法律咨询机构等第三方进行管理。

措施建议

专家指出，如果一家公司对所有供应

商的安全和隐私策略进行评估，其数据泄露的可能性可以从 66% 下降到 46%。这种评估需要覆盖所有供应商，虽然其中较好的供应商可能已经具备了详细的网络安全防御措施，但是较小的供应商组织并没有相同级别的网络安全控制措施，甚至连安全负责人和基本的安全意识都没有。

第一，企业和供应商之间应达成协议，在 SLA 中包含安全要求，明确数据所有权和安全责任，要求供应商履行他们对安全的承诺。并要求这些第三方供应商对他们的伙伴（第四方）也实施类似的控制。

第二，应要求供应商进行自评估，并反馈他们的评估结果。要求供应商同意开展审计工作，可以采用调查问卷的形式进行，这种自评估是静态且主观性的方式，利用对外部威胁情报数据的分析结果可以进行验证和作为客观性的补充。

第三，要进行深入的供应商现场安全评估。企业可以结合供应商接触敏感数据的程度判断重要性，同时结合对外部大数据分析的结果来初步判断安全性，综合重要性和安全性来选择对供应商的管理策略。例如对重要性高且安全性较差的供应商进行深入的现场安全调查，并在现场进行安全测试，对内部安全策略和流程进行评估，了解从数据采集、存储、传输到最后销毁全生命周期，了解数据流转和受保护过程。这些对供应商的调查工作一般会由企业负责数字化的业务部门（如电子商务）、合规部门、采购部门、安全部门联合开展。

第四，建立供应商安全持续监测和安全评价。Gartner 在 2016 年定义了一项新兴技术 Security Rating Service（SRS），基于事实数据进行独立、定量、持续的安全评价服务。国际上有几家提供安全评级的组织，例如：BitSight Technologies、SecurityScorecard、Riskrecon；国内也看到像“安全值”这样的新兴服务。基于问卷的评估是很重要的，但不够充分，因为它们是静态和主观的。定期现场评估测试费用更加昂贵，并且不够及时。为了主动降低风险，需要借助这样的自动化工具，持续的监测和评估，并完成供应商的安全评分。第三方 / 供应商风险管理是 Security Rating Service 很重要的应用场景，实现企业与供应商一起持续地了解相关的风险。

第五，建立完整的供应商信息安全风险管理流程。OCEG 是一个提供企业治理、风险与合规 GRC 解决方案的非赢利组织，2017 年发布了一份研究成果《对于管理第三方信息安全的步骤与方法分析》，资料显示“2015 年，网络攻击为企业带来超过 4000 亿美元的经济损失，其中超过 2/3 的攻击是通过处理企业或客户数据的第三方合作伙伴实现的，因此有效控制企业供应商风险对于存在外部扩展业务的企业至关

重要。完成上述风险管理工作就需要验证、修复和监控第三方控制的有效性，这需要使用复杂且基于任务设计的技术支撑。定义了该流程的关键步骤，并对第三方安全管理的发展做出了一些预测”。一共分 7 个步骤指导企业在签约、续约前，第三方关系发生变化或到达考核期应触发企业的第三方息安全风险管理流程。这 7 个步骤是：

1. 分析第三方带来的风险分析和供应商分类，识别第三方服务类型和重要性，基于风险层次来定义对第三方进行尽职调查的频率、方式，包括远程验证、现场验证，对于低风险的供应商可以接受问卷的回复而无需进行尽职调查；

2. 确定供应商风险范围，根据每个第三方触及的数据、系统、提供的服务（例如：敏感数据处理、软件开发、云服务、基础设施等）映射到需要的控制措施，评估每种关系的固有风险和服务的关键性；

3. 收集证据，获取问卷调查结果和相关文件作为评估第三方控制有效性的证据，结合客观事实的“公开数据”（例如威胁情报数据），可以对低风险的第三方结果进行自动审核以减少工作负担；

4. 评估风险，通过文件分析、技术验证、现场评估手段确认供应商所需的安全控制措施到位，评估控制策略和运行效果；

5. 修复，标记无效控制识别安全问题，并跟踪必要的安全问题整改的情况，完成整改之后进行复查（例如：发现数据访问权限过大，任何角色都可以访问数据库，供应商需要主动将工作计划和整改进度进行反馈。）；

6. 报告，报告残余风险和补救措施，以便让董事会、管理层等相关利益方都可以了解（一般涉及到 IT 风险管理部门、供应商管理部门、和供应商合作的业务部门、合规部门）；

7. 监控，对供应商进行 SLA、安全事件、安全漏洞和安全状况变化的监控，在重新分类和更新评估结果时进行风险提醒。通过对威胁情报和外部数据的分析，可以从外部视角观察到供应商的互联网资产、安全事件和脆弱性三类信息，包括域名、主机、IP 网络、云服务网络、僵尸网络、DDOS 攻击、恶意代码、垃圾邮件、黑名单、安全漏洞、开放端口、安全配置缺失等信息。

目前金融、教育、医疗、快消品、生产制造行业客户数据的敏感性都非常高，同时其在数字化转型过程中必然要和大量的第三方进行合作，风险不容忽视。有效管理需要一种新的方法，使企业在其数字生态系统中了解风险，定制控制措施。第三方的安全意识、能力、资源都相对较弱，需要共同修复和减轻这些风险。

作者单位：北京谷安天下科技有限公司