小型组织的网络安全

CISO 检查清单：保护与第三方的连接

在考虑网络安全的同时选择供应商

您每次评估潜在供应商时，检查以下问题：

- □ 他们具备哪些为类似贵组织的客户服务的经验？
- □ 它们是否已记录符合已知网络安全标准的情况（例如 NIST 框架或者 ISO 27001）？它们是否能提供 SOC2 报告？
- □ 它们履行服务需要访问您的哪些数据和/或资产，以及它们是否将要求任何明显不必要的访问权限？
- □ 它们怎样计划保护它们拥有的贵组织的资产和数据？
- □ 它们如何管理自身的第三方网络风险，它们是否能够提供有关其供应链安全性的信息？
- □ 发生影响贵组织的事件时，它们有哪些灾难恢复和业务连续性计划？
- □ 它们将如何让贵组织了解通信趋势、威胁，以及其组织内部变更等方面的最新情况？

通过第三方发现风险

履行第三方网络风险评估，包括以下步骤：

- □ 创建并持续更新所有供应商关系列表以及每个供应商关系中暴露的资产和数据。
- □ 审核各供应商或第三方已经访问的数据，确保各访问级别遵守“最少权限”原则 。
- □ 基于泄露其系统将会对贵组织产生的影响评估您的供应商和第三方关系（低、中、高）。
- □ 从风险最高的供应商开始，评估各供应商的网络安全能力以及遵守相关标准的情况。
- □ 为常规安全评估制订一个计划，谨记您可能偶尔希望对具有最高风险和/或对客户数据拥有最大访问权限的供应商作现场评估。

管理第三方安全

- □ 开展全面的尽职调查。在征求建议书，与供应商签订的合同、业务连续性、事故响应和服务级别协议中明确网络安全预期。约定出现网络事件时的责任和义务。
- □ 向您与其进行交易或分享数据的金融组织和其他实体询问网络安全实践，谨记您的供应商和第三方还应遵循贵组织必须符合的任何网络安全规定。
- □ 使用确定和约定的措施监测您的供应商遵守网络安全标准的情况。
- □ 与您的处理敏感数据的供应商核实，其是否为您在该供应商处开立的账户提供双因素验证、加密或其他安全措施。

- □ 确保您安装的所有第三方软件和硬件拥有安全握手协议，从而使启动程序通过认证码得到加密，如果不能识别代码将不予以执行。
- □ 如果您遇到假冒或不符合规格的供应商产品，可协商一个解决方案或者退出策略。
- □ 逐年评估供应商合同并确保它们持续符合您的战略方向和监管数据安全规定。合同终止后，包括将收回您资产或数据以及核实供应商已经将该资产或数据全部删除的规定，并撤销访问您系统或服务器的任何权限。

分享信息

- □ 确保您具有明确的沟通渠道和联系人，以便与贵组织的供应商和对手方沟通关于安全的问题。
- □ 核实您具备能够确保与内部或外部利益相关者（包括金融领域内外的实体和公共机构）及时分享可靠、可操作的网络安全信息的程序。
- □ 通过成为金融服务信息共享分析中心（FS-ISAC）这样的信息分享组织的一部分以及寻求其他威胁信息来源，追踪关于其他组织与其第三方在威胁、漏洞、事故和响应方面的经历。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org