数据安全法解读系列（四）
应对勒索软件的攻守之道

（来源：安永微信公众号，2021-07-21）

一、勒索软件威胁新态势

（一）勒索软件对金融机构的数据安全构成巨大威胁

勒索软件是一种利用强加密等技术手段阻止用户正常访问设备或数据并以此为条件威胁用户索要高额赎金的恶意软件。勒索软件的攻击对象覆盖个人用户和企业用户，其中高价值的大型政企机构是主要的攻击目标。勒索软件可通过多种渠道传播，如电子邮件、远程桌面协议漏洞、网站木马、移动存储介质或针对性攻击等。

勒索软件历经三十余年的发展，已呈现出变种繁多、传染性和破坏性极强、难以追踪和查杀等特征，并逐渐形成产业化的攻击链条，提供从勒索软件开发到赎金收取的全套服务。

自 2018 年下半年起，勒索软件呈飞速增长的态势。

2019 年，国家计算机网络应急技术处理协调中心(CNCERT)捕获勒索病毒 73.1 万余个，较 2018 年增长超过 4 倍。

2020 年，CNCERT 捕获勒索软件 78.1 万余个，较 2019 年同比增长 6.8%。

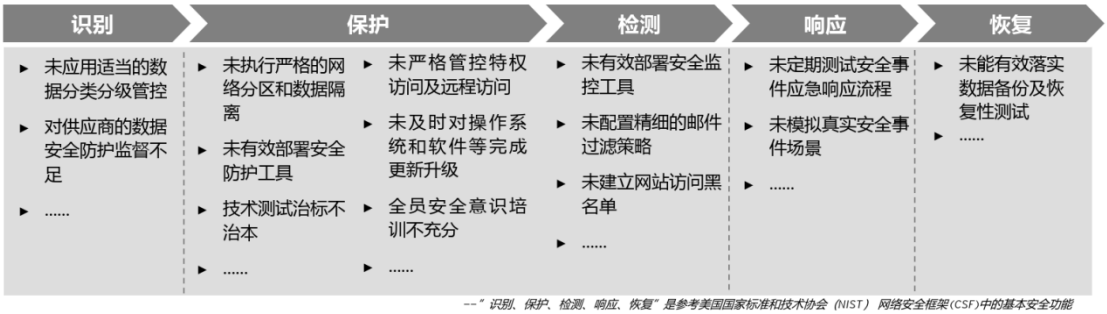
—— 数据来源于 CNCERT

随着金融行业数字化进程的不断推进，金融机构所面临的信息科技风险日益突出，其中数据安全风险尤甚。因为金融行业的数据具有多元复杂、高价值、高敏感等特性，面对愈发严峻的勒索软件攻击局势，金融机构的特殊性也使其成为勒索软件的重点攻击对象。

- 某北美银行于 2020 年遭遇勒索软件 Maze 攻击，被窃取和泄露上千万张信用卡信息
- 某南美国家银行于 2020 年遭遇勒索软件 Revil 攻击，被迫关闭所有分支机构
- 某国际保险公司于 2021 年遭遇勒索软件 CryptoLocker 攻击，支付 4000 万美元赎金
- 某巨头保险集团于 2021 年遭遇勒索软件 Avaddon 攻击，被窃取 TB 级别的敏感数据

—— 数据来源于公开信息

（二）金融机构常见的防守薄弱环节



--"识别、保护、检测、响应、恢复"是参考美国国家标准和技术协会（NIST）网络安全框架(CSF)中的基本安全功能

二、应对勒索软件的攻守之道

（一）金融机构应如何应对勒索软件来袭

1.识别

加强数据资产精细化管控

金融机构的数据资产通常包含勒索攻击所瞄准的高价值敏感数据，如何识别这些敏感数据并集中资源加强数据保护是金融机构防范勒索软件攻击的首要之务。因此，金融机构应梳理自身数据资产，落实数据分级分类的安全要求，对已明确的敏感数据范围采取加密传输、存储等保护措施，以防范明文数据被恶意加密而遭受勒索。

重视供应商安全能力审核

金融机构许多重要业务的运营依赖于外包服务，部分供应商可处理和存储金融机构的重要敏感数据。金融机构应在与供应商合作前评估供应商是否落实较为完备的安全策略及其安全控制的有效性，降低因供应商遭遇勒索软件攻击而引起的供应链安全风险。金融机构还应与供应商就安全事件报告机制和服务连续性机制等在合同或服务水平协议中正式约定，以保障自身和客户的利益。

2.保护和检测

强化网络和数据隔离

中大型金融机构的网络环境通常较为复杂，若未依据安全要求对网络区域进行清晰的边界划分和隔离，那么当遭遇勒索软件攻击时，

金融机构将缺乏足够的缓冲处理时间，攻击将极易在网络中横向扩散。此外，金融机构处理的数据庞杂，若未依据数据重要程度对数据进行数据库级别或文件级别的隔离控制，在遭遇勒索软件攻击时，大批量数据将极易被一并加密或泄露。因此，金融机构应对网络环境有效分区及物理隔离，对高价值及敏感数据的存储实行逻辑或物理隔离，提高勒索软件攻击的扩散门槛，以防被攻击范围过广而造成事件升级。

提升漏洞、补丁管理有效性

IT 环境中所存在的安全漏洞是攻击者常利用的重点突破口，因此在定期执行的全网漏洞扫描和渗透测试中，能否及时发现、评估、分析、修复、跟踪整改漏洞，当是安全运维的重要任务。同时，为改进技术测试的“治标不治本”的现状，企业应结合技术和管理视角，对测试结果进行根因分析，力求从根源出发解决漏洞表象下的“通病”。此外，金融机构还应持续关注、主动跟进相关设备厂商及服务机构所发布的漏洞、补丁更新信息，建立内部专家小组综合分析更新的适用性，对高危漏洞和重要更新及时下载和安装，避免存在高危的、公开的安全漏洞被攻击者轻易利用，而成为勒索软件肆意进攻的爪牙。

全面增强员工信息安全意识

在安全意识不足的内部员工不经意间的行为，如轻信并点击钓鱼邮件中的链接、由于好奇开启欺诈网站、由于识别不足下载、运行了恶意软件等，勒索软件便可通过这样的快速通道进入组织内部。在面临如此的“内外夹攻”挑战时，企业应积极开展针对勒索软件等多种攻击手段的安全教育、培训及模拟演练，有效提升内部员工的安全意识，形成安全文化氛围，这也是一项较低投入成本、较高成效的重要措施。

部署新一代安全技术架构和产品

面对勒索软件的强势攻击，金融机构应搭建符合自身业务体量和安全要求的新一代安全技术架构，精准分析、精细部署并精确配置各类安全产品，通过在网络中各个节点、环节中，对异常操作、威胁性行为及安全事件进行实时监测、报警、拦截和阻断，为企业建立网络的“马奇诺防线”，提升纵深防御的安全技术能力，最大限度地抵御来自外部的攻击。金融机构应基于其安全架构设计和成本效益分析的结果，在品类繁多、功能侧重点不同的安全产品中，有效选择并部署最贴合实际需求的安全产品组合，改善产品应用泛滥但配置粗放的现状。

限制特权访问和远程访问控制

特权账户的访问权限和凭证若被勒索软件利用，其攻击将以权限范围为载体，从个别感染主机迅速蔓延至网络中其他设备，攻击者可恶意加密的数据范围将会进一步扩大。基于此，金融机构应加强特权账户的身份、权限及访问管理，确保用户基于最小权限原则按需访问数据和资源，并考虑通过使用特权账户管理工具对特权账户集中化管理，考虑登录采用多因素身份认证方式，并对特权会话操作执行监控审计等。随着后疫情时代的到来，远程工作逐渐成为新常态，不安全的远程访问方式如远程桌面协议（RDP）将允许攻击者通过暴露在互联网上的端口入侵到远程服务器。为保障远程访问的安全，金融机构应禁用不必要的远程桌面连接，并考虑使用虚拟专用网络（VPN）完成远程连接。

3.响应

强化安全事件的响应和处置能力

若以上的事前防御措施均失效，金融机构将直接面临攻击者的勒索要挟。金融机构应建立针对包括勒索软件攻击在内的各类型、不同场景的安全事件的应急流程和操作手册，在安全事件响应和处置的危急时刻指导企业管理层、执行层的各部门、各岗位及相关方恰当、迅速地响应，通过隔离被感染的机器（关机、拔掉物理网线或禁用无线网卡等）、分析勒索病毒特征、排查并确定被感染范围、执行溯源分析、安全加固等行为，分秒必争地减小受影响的网络范围和数据量，遏制威胁的蔓延。除去流程的建立外，企业应定期开展安全事件应急响应的模拟行动，在“实战”中提升应急响应能力，持续改进沟通协调机制。

4.恢复

巩固数据备份和恢复性测试

支付赎金不是企业被勒索后的最佳选择，也不是唯一的选择。作为应对加密型勒索攻击的补偿性措施，重要数据的有效备份是面对勒索软件攻击时恢复业务运行的可靠基础和保障。金融机构应基于业务需求，对重要系统及数据定期考虑执行在线、离线双重备份，确保网络遭受攻击时可利用离线备份数据恢复业务；同时，对已备份数据执行定期恢复性测试，保障备份数据的可用性。

（二）安永助力赋能

为助力企业抵御勒索软件攻击，全面提升安全事件响应能力，降低遭受攻击的风险、影响及损失，安永将为客户提供以下服务：

新一代安全技术架构

通过规划、设计新一代的安全技术架构，以改变数据孤岛现状，协助企业完成**安全领域的数字化转型**。

红蓝对抗-攻防演练

通过设计及构建多维度对抗场景，实网开展“红蓝对抗”，全面评估企业网络安全防御体系的有效性；针对演练结果完成**根因分析**，并根据企业的实际情况提出**针对性的、可落地的**改进建议。

War gaming

以**新颖的培训模式**模拟实战演习，提高高级管理层的网络及数据安全意识。

安全培养机制

针对企业不同工作角色所需的具体知识和能力需求，制定详细的培训和宣贯计划，筑建全面安全能力高墙。

原文链接：https://mp.weixin.qq.com/s/IPsH9qW29BR5gE9PF4QIcQ ，转载请注明。