小型组织的网络安全

事故响应检查清单

准备

- □ 基于在贵组织的网络风险评估中发现的最紧迫的风险制订响应和业务连续性计划，与贵组织的高级领导人和其他相关人员合作。
- □ 制定与贵组织的最高优先级网络风险相关的事故类型的威胁情景。注重培养响应该等情景的能力。
- □ 识别、记录和在组织内部提供一份事故响应联系人名单。
- □ 识别和记录相关本地和联邦执法机构和官员的联系信息。
- □ 制定指明哪些事故必须报告、必须何时报告和向谁报告的规定。
- □ 基于相关因素（例如事故的功能和信息影响力以及事故发生后可能的恢复能力）制订列明员工如何迅速响应事故以及应采取什么行动的书面指南。
- □ 事故发生后，通知所有员工联系您的技术团队——最常见的情况是将联系 IT 人员和/或 CISO/CIO/其他有可比性的经理。
- □ 部署监督员工行动和识别内部威胁和事故的解决方案。
- □ 纳入业务持续性计划，以协调贵组织在业务紧急情况下如何与供应商和主要客户合作，包括您如何开展人工或替代性业务运营活动（如需要）。
- □ 纳入针对系统紧急关停和重启的书面程序。
- □ 制订并测试检索和恢复备份数据的方法；定期测试备份数据以验证其合法性。
- □ 针对在替代性设施/场地开展业务运营制作已确定的协议和程序。
- □ 具备面向所有客户的清晰的传播渠道。
- □ 制订并测试检索和恢复备份数据的方法; 定期测试备份数据以验证其合法性。
- □ 针对在替代性设施/场地开展业务运营制作已确定的协议和程序 。
- □ 具备面向所有客户的清晰的传播渠道。

练习

- □ 与所有级别的员工或代表（包括贵组织的高管、人力资源/通讯人员和法务与合规团队成员）组织小型的桌面练习。
- □ 发现且最好参加行业范围内的与贵组织相关的桌面练习。
- □ 制订程序以确保从练习中学到的内容被纳入贵公司的网络安全战略中并在其中进行陈述。

响应

- □ 实施事故响应计划措施，使对业务运营的影响最小化。
- □ 明确受到影响/损害的系统并评估损害。
- □ 通过移除（分割）受到影响的资产减少损害。
- □ 在团队怀疑发生事故时尽快记录所有信息。在分割/隔离受到影响的已明确资产的同时尝试保存事故的证据，从受影响的资产中收集系统配置、网络和入侵侦测日志。
- □ 通知适当的内部各方、第三方供应商和机构，并在必要的情况下请求协助。
- □ 按照法律、法规和机构内部指引发出客户通知并启动协助活动。
- □ 利用威胁分享平台（如 FS-ISAC 或者 MISP）就该威胁通知行业。
- □ 记录在事故期间采取的所有措施，供以后审核。

恢复

- □ 在可行的情况下将复原的资产恢复到定期的“恢复点”并使用备份数据将系统恢复到最近已知的“良好”状态。
- □ 从恢复的资产中创建已更新的“清洁”备份并确保关键资产的所有备份在物理和环境均安全的地点存储。
- □ 测试并验证受到影响的系统已全面恢复。 确认受到影响的系统运行正常。

审核

- □ 在事故发生后开展“所学教训”讨论——与高级职员、受信任的顾问和计算机支持供应商会面，以审核可能的薄弱环节或建议执行新措施。
- □ 如果可行，指明可能导致事故的薄弱环节（不管是软件、硬件、业务运营还是员工行为）并制订缓解计划。
- □ 确认受到影响的系统运行正常。
- □ 制定监督计划，检测与已识别问题相关的类似事故或其他事故。
- □ 通过 FS-ISAC 等威胁分享平台分享所学教训和该事故相关信息。
- □ 将所学的教训融入贵组织的事故响应方案中。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org