小型组织的网络安全

勒索软件检查清单

勒索软件准备

- □ **您制定勒索软件预防和保护计划时，定期评估以下方面：**
  - 贵组织是否具备定期安排的备份？
  - 是否有任何非必要设备连接至贵组织的网络？
  - 贵组织是否了解支付赎金所涉及的监管和法律风险？
  - 贵组织是否定期更新其软件系统？ 是否为自动更新？
  - 贵组织是否具有处理勒索软件攻击和数据丢失的计划？
  - 您的系统是否具有网络保险保单？ 如果是，该计划是如何给勒索软件攻击保险的？

实时保护

- □ **购买实时适应新威胁情报的反恶意软件保护系统 。**
- □ **评估连接到存储敏感或重要信息的网络的所有设备的安全性。**
  - □ 将所有非必要系统连接到单独的网络。
  - □ 考虑远程工作设置的安全性。确保安全工具离线工作，监测所有网络流量。
- □ **围绕钓鱼攻击和强密码保护必要性，推动员工教育 。**
- □ **如果可行，考虑在整个组织内实施多因素验证。**
- □ **使所有软件和系统定期更新。**
  - □ 更改设置以便在可能时进行自动更新。
- □ **制定一项关于如何处理勒索软件攻击和有价值数据丢失的事故响应和危机管理计划。**
  - □ 准备一项发生勒索软件攻击时的外部通讯计划。

数据备份

- □ **购买安全、定期更新的备份系统，保护您的数据。**
  - □ 如果使用 USB 或硬盘备份，在备份完成后将该等设备与联网的计算机物理断开。
  - □ 如果使用云存储，为服务器配备高级别加密和多因素验证。
- □ **创建总账的只读版本，应对最糟糕灾难的恢复。**
- □ **开发执行自动数据恢复和纠正的系统。**
- □ **制定评估恢复关键数据和业务服务将花多长时间的情景。**

监管环境

- ☐ **评估您的操作环境中有关勒索软件的相关监管和法律指南。**
  - ☐ 考虑国家特定指南。
  - ☐ 考虑金融领域特定指南。
  - ☐ 考虑国际法律和监管要求。
  - ☐ 制定一项定期评估不断变更的指南的计划。
- ☐ 评估支付赎金涉及的风险。
- ☐ 与当地执法部门保持联络。
- ☐ 建立在发生攻击时快速进行信息分享的连接。
- ☐ 评估勒索软件网络保险保单的优点和缺点。