小型组织的网络安全

CISO 检查清单:保护您的组织

制定一项基于风险的信息安全计划

- ☐ 明确并列出贵企业存储和使用的所有信息类型(例如客户名称和电子邮件)。
- ☐ 询问并记录有关各信息类型的答案:
  - 如果该信息被公开，会发生什么?
  - 如果该信息有误，我的企业会发生什么?
  - 如果我/我的客户无法查看该信息，我的企业会发生什么?
- ☐ 记录什么技术与您识别的信息相联系。这可能包括硬件 (例如计算机) 和软件应用程序 (例如浏览器电子邮件)。
  - 在适用时，包括贵企业以外的技术 (例如“云”) 和您已经拥有的防火墙等任何保护技术。
  - 包括在家工作时可能使用的技术。
  - 包括牌子、型号、序列号和其他识别码。
  - 追踪各产品的位置。对于软件而言，识别装载该软件的机器。
- ☐ 定期查看您的国家 CERT、FS-ISAC、您的本地 InfraGard 分部，以及金融行业可能面临的威胁和薄弱环节的其他相关内容，并估计您将受影响的可能性。
- ☐ 每月至少开展一次薄弱环节扫描或分析。
- ☐ 为贵组织制定网络安全政策，包括“在家工作”方案。
- ☐ 对所有员工进行该政策细节的相关培训，并让他们签署文件，认可他们在遵守该政策，持续维护贵组织的网络安全中所发挥的作用。
- ☐ 制定保护计划，应对内部威胁，包括企业风险评估和访问控制管理。

预防恶意损害

- ☐ 激活您的防火墙，设置访问控制列表 (ACL)。使用白名单设置限制访问。
- ☐ 在所有计算机和笔记本电脑中使用防病毒软件和反间谍软件。
  - ☐ 确保安全工具可以在“在家工作”环境中有效运行。
- ☐ 应用制造商和供应商提供的最新软件更新。在有新版本时“自动更新”。
- ☐ 将安装新程序的权利限于具有管理员权限的 IT 员工。
- ☐ 维护和监督保护/检测硬件或软件生成的活动日志。使用密码保护和加密技术保护日志。
- ☐ 确保所有主机时钟同步。
- ☐ 控制对 SD 卡和 USB 硬盘等可移动媒体的访问。鼓励员工通过电子邮件或云存储传输文件。告知员工使用外部来源 USB 或将自己的 USB 交给他人的风险。
- ☐ 在您的电子邮件服务中设置电子邮件安全和垃圾邮件过滤器。
- ☐ 使用加密和其他可用工具保护贵组织面向公众的网站的所有页面。
- ☐ 考虑聘用渗透测试服务，评估贵组织资产和系统的安全性。

培训员工

- ☐ 计划在所有新员工入职时以及定期为已有员工 (每年至少一次) 开展强制性网络安全培训。要求员工:
  - 在所有专业设备和账号上使用强密码，并鼓励他们在个人设备上也如此，并使用密码管理器。
  - 使所有设备上的所有操作系统、软件和应用程序为最新版本，包括家用 IT 基础设施，
  - 所有账号使用双因素认证，
  - 保护账户资料和访问卡的安全，在无人照看时，为设备上锁。
  - 禁止通过未加密的电子邮件或其他开放通信方式，分享账户资料和其他敏感数据，
  - 避免立即打开未经请求主动发送的或可疑电子邮件的附件或点击其中的链接。
  - 提供个人信息之前，验证外观可疑电子邮件或弹出框的真实性，并密切关注该电子邮件，以及
  - 向贵组织的技术人员和/或更高管理层报告任何潜在的内部或外部安全事件、威胁或错误处理的数据或设备。
- ☐ 计划并通过模拟定期测试员工意识，包括通过虚假账户发送钓鱼邮件。评估任何员工出错情况，并利用这些错误作为学习和改善的机会。

保护您的数据

- ☐ 对您的重要数据 (例如文件、电子邮件、日历) 定期备份，测试该等数据是否可被存储。考虑备份至云。
- ☐ 确保包含您备份的设备不会通过物理连接或本地网络永久连接至持有原始版本资料的设备。
- ☐ 安装浪涌保护器，使用发电机，并确保您的所有计算机和关键网络设备插入不间断供电系统。
- ☐ 使用移动设备管理 (MDM) 解决方案。

保护您设备的安全

- ☐ 打开移动设备的 PIN 或密码保护器。配置设备，以便在设备丢失或失窃时可以追踪、远程删除其中的内容或远程锁定。
- ☐ 在可行时，使用“自动更新”选项使设备 (以及安装的所有应用程序) 保持最新版本 。
- ☐ 发送敏感数据时，请勿连接至公用 Wi-Fi 热点——使用运营商的蜂窝基站 (包括用手机当猫和无线显示转换器) 或使用 VPN 连接网络。
- ☐ 更换制造商不再提供最新替代版本支持的设备。
- ☐ 设置丢失或失窃设备的上报程序。

使用密码

- ☐ 确保所有计算机均使用需要密码启动的加密产品 。打开移动设备的密码或 PIN 保护。
- ☐ 使用强密码，避免可预测出的密码 (比如 passw0rd) 和个人识别符 (例如家庭和宠物名字)。指示所有员工也如此 。
- ☐ 在可行时，使用双因素验证 (2FA)。
- ☐ 在将所有设备 (包括网络和 IoT 设备) 分发给员工之前，更改该等设备的制造商发布的默认密码。

- ☐ 确保员工可以轻松地重新设置自己的密码 。您也可能希望要求员工定期更改他们的密码 (例如，每季度、每半年或每年一次)
- ☐ 考虑使用密码管理器 。如果您不使用密码管理器，确保 (提供您所有其他密码的访问权限的) “主”密码为强密码。

控制许可

- ☐ 确保所有工作人员每次访问您的系统时均拥有经过认证的、唯一可识别的账户。
- ☐ 仅将管理权限交给可信的 IT 员工和关键工作人员，并撤销标准用户工作站的管理员权限。
- ☐ 仅向员工提供其工作所需的具体数据系统的访问权限，确保他们未经许可无法安装任何软件。
- ☐ 在贵组织的计算机上为每位员工创建用户账号。
- ☐ 明确远程工作的员工和管理员的清晰访问选项。

保护您的 WI-FI

- ☐ 确保您工作地点的 Wi-Fi 安全，并使用 WPA2 加密。路由器一开始经常为加密关闭状态，所以请确保打开。密码保护路由器的访问权限，所以确保该密码已更新，不再为预设默认密码 。关闭任何 “远程管理” 功能。
- ☐ 仅允许具有某些媒体访问控制地址的设备访问您的 Wi-Fi 网络。如果客户需要 Wi-Fi，设置单独的公共**网络**。
- ☐ 启用登录您的网络设备的动态主机配置协议 (DHCP)，以便于轻松跟踪已加入您的网络的所有设备。
- ☐ 在您设置路由器之后以管理员身份退出登录。
- ☐ 确保您的路由器的软件为最新版本。向生产商注册您的路由器，并签约获得更新。

避免网络钓鱼攻击

- ☐ 确保员工不通过服务器或使用拥有管理员权限的账户浏览网络或检查电子邮件。
- ☐ 设置网络和电子邮件过滤器。考虑阻止员工访问通常与网络安全威胁相关的网站。
- ☐ 教会员工查找明显的钓鱼迹象，例如拼写或语法错误，或可辨认的标识的低品质版本。发件人的电子邮件地址是否看起来合法?
- ☐ 扫描恶意软件，如果怀疑发生攻击，尽快更改密码。如果员工成为钓鱼攻击的受害人，请勿惩罚员工 (惩罚会降低员工将来汇报的积极性)。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org