小型组织的网络安全

CISO 检查清单：保护您的客户

告知客户和员工个人层面的数据保护

□ **为员工和客户提供其需遵循的以下个人指南，更好地保护他们的数据：**

- 在所有个人和专业设备上使用强密码并考虑使用密码管理器。
- 使所有计算机和移动设备上的操作系统和其他软件和应用程序保持为最新版本。
- 安装阻止、侦测和删除恶意程序的反病毒、反恶意软件和反勒索软件。
- 使用防火墙计划阻止未经授权访问您的计算机的行为。
- 仅使用声誉良好的公司提供的安全产品。阅读计算机和消费者刊物上的评论，考虑咨询您计算机或操作系统的生产商的意见。
- 谨慎处理敏感信息。不要通过未加密的电子邮件发送银行账户密码或者其他敏感财务账户数据。
- 进行涉及敏感个人信息的银行或其他通信活动时，要留心在何地以及如何连接互联网。
- 不要立即打开电子邮件附件或点击未主动要求的链接或可疑的电子邮件。停下。思考。点击。
- 如果有人意外地在网上或通过电话联系您或者要求您提供个人信息，请持怀疑态度。即使与已知晓的地址通信，尽量通过电子邮件分享最低程度的信息。
- 记住，金融机构不会通过电子邮件或电话要求您提供他们已经拥有的与您有关的信息。
- 假定您从未开户的银行要求您提供信息的情况是一个骗局。
- 在提供个人信息之前核实可疑电子邮件或弹出窗口的合法性。密切注意该电子邮件地址。

管理账户

□ **要求客户使用强用户 ID 和密码登录您的服务。建议他们不要使用与其他账户相同的密码 。**

□ **使用即时验证、实时验证、尝试存款验证、身份验证和/或与钱包不相关的问题验证真实客户的身份或减少欺诈的机会。**

□ **客户登录您的服务时提供（或最好是要求）使用双因素验证。**

□ **定期检查用户账户的欺诈迹象。**

保护数据

□ **考虑贵组织要执行服务必须收集哪些客户数据，并警惕收集超过该范围的任何客户数据。**

□ **制订并发布数据保留政策。处理不再需要的客户数据。**

□ **加密传输中或者静态的客户数据。**

□ **制订数据安全政策，以明确哪些数据传输方法得到批准与受到限制，并明确处理客户数据时所有员工可以接受什么 。确保这些政策有书面记录，已向所有员工传达、实施，并定期得到审核和更新。**

保护公共网络应用程序安全

- □ 对贵组织面向公众的网络应用程序执行 HTTPS 并将所有 HTTP 流量重新导向 HTTPS。
- □ 使用您网站上的内容安全政策。
- □ 启动您网站上的公钥固定。
- □ 确保您面向公众的网络应用程序决不使用 cookie 存储高度敏感或关键的客户信息（例如密码），且针对 cookie 的到期日比较保守（宜早不宜迟）。
- □ 考虑对存储于您使用的 cookie 中的信息进行加密。
- □ 考虑聘用渗透测试服务至少每年一次评估您的面向公众的网络应用程序。

培训员工

- □ **向您的员工讲授责任和策略，将可能暴露客户数据的人为错误减少到最低程度。这意味着建议他们：**
  - 将客户数据的访问权限和传输对象限定在履行其工作职能必要的范围之内，
  - 通过使用强密码、启用双因素验证、保持软件更新以及不点击可疑链接在处理客户数据的所有设备和账户上保持可靠的安全实践，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、威胁或客户数据错误处理事件。
- □ **确保您的员工理解并已签署文件，遵守贵组织的数据保护和安全政策。**

通知客户

- □ **在处理客户数据泄露时形成对贵组织的监管环境的意识，以确保您在真正发生事故时已准备好实现合规。**
- □ **在贵组织知晓未经授权访问敏感客户信息的事故时，立即进行调查，以确定信息曾经或将被滥用的可能性。按照通知的最佳实践尽快通知受影响的客户并提供：**
  - 事故和遭到泄露的信息的总体说明；
  - 进一步提供信息和帮助的电话号码；
  - 在此后 12 至 24 个月“保持警惕”的提醒；
  - 立即报告疑似身份被盗事件的建议；
  - 金融机构为保护信息免遭进一步未经授权访问或使用的措施的总体说明；
  - 信用报告机构的联系信息；以及
  - 贵组织必须遵守的法规规定的任何其他信息。

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE

CarnegieEndowment.org