未来工厂 - 场景 #260

客户所见：未来工厂应该重视网络安全管理

七月 08, 2023 03:15 下午 - rick

状态:	Define:需求分析	**开始日期:**	七月 08, 2023
优先级:	普通	**计划完成日期:**	
指派给:		**% 完成:**	20%
类别:		**预期时间:**	0.00 小时
目标版本:	未来工厂参访		
关联联系人:			

描述

我的本机电脑曾被人黑如，客户的自动化设备被入侵锁定勒索，数字系统被黑，未来工厂应该重视网络安全建设与管理

常见的网络威胁：

- 恶意软件

  “ 恶意软件 ”一词是指恶意软件的变体，例如蠕虫、病毒、木马和间谍软件，它们提供未经授权的访问或对计算机造成破坏。

- 勒索软件

  勒索软件是恶意软件的一种类型，它会锁定文件、数据或系统，并威胁要删除或销毁数据（或将私人或敏感数据公开），除非向发起攻击的网络犯罪分子支付赎金

- 网络钓鱼/社会工程

  网络钓鱼是社会工程的一种形式，它诱使用户提供自己的 PII 或敏感信息。

- 内部威胁

  现任或前任员工、业务合作伙伴、承包商或过去曾访问过系统或网络的任何人，如果滥用其访问权限，那么都可以被视为内部威胁。

- 分布式拒绝服务 (DDoS) 攻击

  DDoS 攻击试图通过让服务器、网站或网络的流量过载（通常来自多个协调系统），致使其崩溃。

- 高级持续性威胁 (APT)

  在 APT
  中，单个或一群入侵者会渗透到系统中，并在很长一段时间内未被察觉。入侵者保持网络和系统完好无损，以便监视业务活动，窃取敏感数据，同时避免企业启动防御对策

- 中间人攻击

  中间人是一种窃听攻击，即网络犯罪分子拦截和转发双方之间的消息以窃取数据。例如，在不安全的 Wi-Fi
  网络上，攻击者可以拦截在访客设备和网络之间传递的数据。

source

历史记录

#1 - 七月 08, 2023 04:07 下午 - rick

- 标签 从 security 变更为 security, danfoss

- 主题 从 未来工厂应该重视网络安全管理 变更为 客户所见：未来工厂应该重视网络安全管理