Security posture and strategy assessment for the Operational Technology (OT) environment (Agricultural, Food & Beverage Industry)

Task: Evaluate current OT cybersecurity posture and assess the risks and events that may happen as the result of a successful cybersecurity incident carried out by external or internal adversaries.

Solution: A comprehensive penetration testing focused on the industrial network, simulating multiple scenarios for potential adversaries with various levels of access to the infrastructure.

Key fact: During the penetration testing UDV Technologies' experts managed to obtain full access to the Customer's critical industrial control systems, thus establishing control over the OT environment. The Customer was immediately provided with the list of discovered vulnerabilities and was able to remediate them before the project finished, thus significantly improving the cybersecurity posture for the OT infrastructure.

Outcomes:

- Based on the pentest results UDV Technologies proposed several immediate steps to secure the critical infrastructure segments.
- A cybersecurity strategy was developed as the ultimate result of the provided service, containing the detailed action plan required for reaching and maintaining the target cybersecurity posture.
- Customer's management department gained a strong understanding of the possible negative business impact related to cybersecurity shortcomings allowing them to switch from a patchwork security approach to the strategic planning and consistent actions.

CUSTOMER PROFILE

A large agricultural holding incorporating companies producing a multitude of foods.

- **Distributed IT and OT infrastructure of a unique architecture.**
- **Highly automated production lines using a variety of industrial control systems.**
- **Unplanned facility downtime or product quality reduction are business critical and will lead to severe financial and reputational impact.**

Starting point

The holding consists of multiple companies each relying on several business-critical technological systems, making uninterruptible operation a top business priority. The Customer has run several pentests on the corporate IT infrastructure, however industrial networks require a different approach. In OT vulnerability scanning can be performed during either planned system downtime or using lab environment. However, preparing a relevant lab infrastructure for multiple systems proved to be very time and effort consuming, therefore the actual pentest could only be carried out during maintenance windows or even live operation taking maximum precaution against impacting the main system functions. A separate project challenge was posed by the geographical dispersity of the infrastructure leading to difficulties in communications between the Customer's cybersecurity team members.

After assessing the current situation UDV Technologies' experts proposed the following plan:

1 Perform the OT environment pentest simulating external (Internet-based) adversary actions accounting for the infrastructure characteristics and avoiding interruption in system operation.
2 Perform the OT environment pentest simulating internal (from inside the corporate network) adversary.
3 Evaluate current cybersecurity posture of the Customer's ICS network.
4 Develop a detailed action plan covering the steps necessary for establishing sufficient cybersecurity posture for the critical assets.

Project steps

In controlled attempts to obtain unauthorized access to OT network segments of the Customer's infrastructure, UDV Technologies' experts followed gray box and black box approaches. The experts discovered several exploitable unauthorized access scenarios that could allow potential adversaries to disrupt operations of the deployed OT assets. If happened, these incidents would be crippling this food and beverage producing business. Successful penetration scenarios included:

- Obtain unauthorized access to a print dispatching service and upload modified label templates. Possible outcomes: about $5K fine per each case when the food with the wrong label is discovered in the retail.
- Obtain the full control over industrial control systems via arbitrary code execution (incl. guest account usage) to block legitimate system access and completely inhibit production line operation. The impact estimate depends on the resulting facility downtime.
- Disrupt certain climate conditions in the livestock buildings by impacting HVAC system operation resulting in livestock death. Possible impact starts from $100k.

Conclusions

After completing the project UDV Technologies' experts have demonstrated adversary potential:

- Obtaining unauthorized access to the ISC equipment
- Producing the impact resulting in significant financial losses and facility downtime

The overall cybersecurity posture of the OT infrastructure has been significantly improved during the project by implementing immediate remediation steps for the most critical vulnerabilities.

Nevertheless, the Customer will continue focusing their effort on implementing sufficient cybersecurity measures for the critical assets according to the cybersecurity strategy developed by UDV Technologies' experts in collaboration with the Customer's security team.

Future plans

Currently UDV Technologies continues to work with the Customer supporting multiple business initiatives in the field of cybersecurity. Several scientific projects have been started with focus on securing the industry-specific technological systems and networks.

INTERESTED IN ASSESSING YOUR IT/OT INFRASTRUCTURE?

Contact UDV Technologies today for a scoping call and a quote on our services!
ASPIN COMMERCIAL, Trade Center First, 106 Sheikh Zayed Rd, DIFC, Dubai, 118467, Dubai
+971 52 416 6738
commercial@udvtech.com