**3. Do you conduct quarterly anti-phishing, smishing, and vishing campaigns?**

**No:** They face operational challenges that lower the frequency of anti-phishing campaigns. Resource and time constraints impact the ability to conduct these campaigns quarterly, though they are recognized as crucial for cybersecurity.

**4. Does everyone in your organization understand the risk associated with cybersecurity?**

**No:** Universal awareness is lacking at Avanza, and reporting procedures may lack clarity. The organization recognizes the variability in employee backgrounds and the complexity of cybersecurity topics, contributing to inconsistent awareness levels.

**5. Are all vendor default accounts changed or disabled?**

**No:** Changes to vendor default accounts are inconsistently applied across systems at Avanza. Decentralized IT management and oversight contribute to disparities in security practices.

**7. Is all unnecessary functionality removed or disabled?**

**No:** They face challenges in removing all non-essential functionality due to operational requirements and system interdependencies. Balancing security with operational needs is a complex task.

**9. Are all screen idle times set for 15 minutes and require reauthentication to unlock?**

**No:** Uniform implementation of screen idle times is challenging at Avanza. Device variations and user needs contribute to difficulties in standardizing this security measure.

**10. Do you provide end-users a tool to save all passwords?**

**No:** They do not uniformly provide tools for password management to end-users. The organization acknowledges the diversity of user preferences and the complexity of implementing a unified system, contributing to this limitation.

**13. Do you harden all endpoints and remove unnecessary functionalities?**

**No:** Complete hardening of all endpoints is challenging for Avanza. This is due to the diverse requirements of job functionalities, varying applications, and potential limitations in removing non-essential components without impacting job performance.

**14. Do you have next-generation anti-malware protection on all endpoints with a threat intelligence-based platform?**

**No:** Implementation challenges arise for They due to compatibility issues with existing systems. The organization acknowledges the importance of advanced protection but faces difficulties in ensuring uniform deployment across all endpoints.

**18. Do all endpoints have next-generation anti-malware applications?**

**No:** Limited implementation on all endpoints is due to compatibility issues faced by Avanza. Despite recognizing the importance of advanced malware protection, achieving widespread deployment is hindered by compatibility challenges with existing systems.

**19. Are all logs stored for at least 2 years?**

**No:** The duration of log storage at Avanza may vary. Achieving uniform storage for a minimum of two years poses challenges, considering factors such as resource constraints, evolving compliance requirements, or the nature of the logged information.

**20. Are all devices generating logs?**

**No:** Logging capabilities across devices may not be uniform at Avanza. The organization faces challenges in ensuring that all devices consistently generate logs, with non-uniformity arising from differences in device types,

**21. Are all logs reviewed daily by inside and/or outside sources?**

**No:** Daily log reviews present a challenging task for them. Achieving daily analysis is difficult due to factors such as resource constraints, the volume of generated logs, or the need for specialized expertise in log analysis.

**26. Do you require multifactor authentication (MFA) for all connections outside of the network?**

**No:** Implementing multifactor authentication (MFA) for all external connections is challenging for They.

**32. Is your demilitarized zone (DMZ) secured?**

**No:** Securing the demilitarized zone (DMZ) is a significant challenge for Avanza. The complexity of maintaining security in these intermediate areas between the internal network and the external internet is a reason for this difficulty.

**33. Has it been ensured that there are no data, databases, or stored accounts on the DMZ?**

**No:** Ensuring that the DMZ is free of data, databases, or stored accounts is challenging for Avanza. This might be due to the complexities involved in managing and segregating network traffic and data storage in these zones.

**44. Does it include performing routine dark web reconnaissance to learn what exists on the dark web about your brand and enterprise structures?**

**No**: They do not regularly monitor the dark web for information about their brand. This is mainly because dark web monitoring requires specialized tools and expertise, which can be challenging to maintain in-house.

**61. Do you require data classification throughout the network?**

**No:** The company strives for data classification throughout their network, but implementing a universal system is challenging. The complexity arises from the diverse nature of data and the need for detailed categorization to ensure appropriate handling and security measures for different data types.

**65. Are software engineering techniques or other methods defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in all software?**

**No:** They face challenges in achieving universal adoption of prevention techniques by software development personnel. While techniques are defined, ensuring consistent implementation across all software remains challenging due to various factors, including resource constraints and evolving technologies.