TVRA Report

Threats Vulnerability Risk Assessment Report on Agricore

Prepared For:

Marc Hayes

Seneca Polytechnic

Prepared By:

Ornan Roberts

Syed Mujahid Hamid Ali

Ramachandra Muralidhara

Yannish Kumar Ballachandher Sreedevi

December 11, 2023

Table of Contents

Executive Summary

The report comprehensively outlines the key findings on the threats, vulnerabilities and risks associated within the infrastructure of the Agricore. The TVRA assessment was conducted on the technical infrastructure of the ecommerce business where risks associated within the threats were analyzed.The scope of the report covers analyzing the threats and vulnerabilities within the infrastructure. Through the usage of the NIST framework the assessment was conducted. The NIST 800-30 revision 1 was used as reference for identifying the threats, threat sources and vulnerabilities. The assessment is conducted on the company domain www.agricore-spr.com. The summary table below shows the numbers of risks identified for each level of risk based on the assessment conducted.

Very High	High	Moderate	Low	Very Low
0	2	4	4	0

Risk Assessment

Risk assessment serves as a foundational step for identifying, evaluating, and managing potential risks and vulnerabilities present within the business. Through understanding these risks, we can take proactive measures to mitigate or minimize the risk. There are various business processes that play an integral role in business operations and can pose different risks. The assessment allows us to systematically identify, evaluate, and prioritize potential risks and vulnerabilities that could compromise the integrity of our ecommerce business. The assessment of infrastructure is crucial for safeguarding customer information, ensuring the secure processing of transactions, and maintaining the availability of our website.

Methodology

The methodology employed by Agricore is a systematic process designed to identify, evaluate, and manage potential risks and vulnerabilities within our operations. Based on the frameworks of NIST SP 800-30 Rev. 1, our methodology was designed to examine the business and technical requirements of our ecommerce business. We employed a risk matrix which was an integral component of our risk assessment methodology. Through the matrix, we systematically categorized and identified risks into different levels, which provided a structured way to prioritize and decide the compensatory controls. The following is the risk matrix acquired from NIST framework and was utilized to perform the risk assessment. To understand the risk matrix, and determine the risk, we define the risk by the combination of the level of impact and the likelehood.

Risk = Likelihood x Level of Impact

Likelihood - Chances or the probability the event will occur

Level of Impact - Extend of impact of the event

Likelihood	Level of Impact					
		Very Low	**Low**	**Moderate**	**High**	**Very High**
	Very High	Very Low	Low	Moderate	High	Very High
	High	Very Low	Low	Moderate	High	Very High
	Moderate	Very Low	Low	Moderate	Moderate	High
	Low	Very Low	Low	Low	Low	Moderate
	Very Low	Very Low	Very Low	Very Low	Low	Low

TVRA Chart

Based on the matrix, the TVRA assessment was performed. The chart below shows the critical risk findings based on the assessment.

Threat Event	Threat Source	Capability	Intent	Targeting	Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
Perform pervasive network reconnaissance/scanning.	Outsider	low	high	very low	Predicted	low	-Lack of regular network vulnerability assessments. -Absence of real-time network monitoring and detection mechanisms.	moderate	moderate	low	low	low
Craft phishing attacks.	Outsider	high	moderate	very low	Possible	low	-Insufficient employee training on recognizing phishing attempts. -Lack of advanced email filtering and threat intelligence integration.	very low	high	low	high	low
Exploit recently discovered vulnerabilities.	Outsider	moderate	low	very low	Predicted	moderate	-Delayed patch management and update procedures. -Inadequate prioritization of vulnerabilities based on criticality.	high	high	moderate	high	moderate
Compromise mission-critical information.	Outsider	moderate	low	very low	Possible	low	-Weak access controls and insufficient user privilege management. -Lack of encryption for sensitive data at rest and in transit.	high	very high	moderate	very high	high
Conduct attacks using unauthorized ports, protocols and services.	Outsider	low	high	very low	Predicted	high	-Poorly configured firewalls with overly permissive rules. -Absence of network access controls and segmentation.	moderate	moderate	moderate	moderate	moderate
Conduct brute force login attempts/password guessing attacks	Outsider	very low	low	very low	Predicted	high	-Weak password policies and lack of complexity requirements. -Inadequate account lockout mechanisms and monitoring for multiple failed login attempts.	moderate	high	high	low	low
Obtain unauthorized access.	Outsider	moderate	high	very low	Possible	low	-Insecure authentication mechanisms and practices. -Poorly managed user access reviews and audits.	high	very high	moderate	high	moderate
Incorrect privilege settings	Outsider	low	low	very low	Possible	low	-Lack of regular access reviews and role validation. -Absence of least privilege principles in user roles and permissions.	moderate	moderate	low	moderate	low
Conduct Distributed Denial of Service (DDoS) attacks.	Outsider	moderate	moderate	very low	Possible	moderate	-Lack of DDoS mitigation solutions and traffic filtering. -Insufficient redundancy and failover capabilities in critical services.	high	very high	high	high	high
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Outsider	moderate	low	very low	Possible	moderate	-Insecure mobile device configurations and lack of MDM solutions. -Absence of strict security policies and enforcement on mobile devices.	moderate	moderate	moderate	high	moderate

Controls

Control	Description

Access Management Control	Limit the access to sensitive data and files to only those individuals who require it based on their roles and responsibilities.
Log Management Control	Collecting all the logs for activity and anomalies. The control focuses on the importance of collecting and analyzing log data to monitor for suspicious activities.
Web Browser Protection	The control delves into the protection of the web server and web based resources. SSL Encryption was added to secure the website. A web application firewall (WAF) in the network infrastructure to protect against web attacks.
Malware Defense Control	This control protects the endpoint from executing any malicious file. The control is disabling the feature of autorun and autoplay for removable devices.
Network Segmentation Control	Implement VLANs and network segmentation. This control is focused on establishing and maintaining network boundaries.
Data Recovery Control	This control is for deploying a backup plan incase of disaster. It ensures that backups are conducted at scheduled intervals.
Software Assets Inventory Control	This control would allow management and tracking of software assets within the organization. Inventories created for all assets for administrative uses.

Generate and use certificate from trusted CA (like LetsEncrypt or Verisign)	Secure communication by obtaining and using SSL/TLS certificates from trusted CAs like Let's Encrypt or Verisign.

Conclusion

The risk assessment conducted on the Agricore infrastructure has shed light on critical threats and vulnerabilities that must be addressed to ensure the confidentiality, integrity, and availability of the system. Using the NIST framework, we conducted the assessment to understand the risk landscape and implement measures to mitigate identified risks. We discovered critical findings in the system which we discussed and expanded on the controls. The TVRA chart outlines the findings that pose risk to the system. Mitigation controls were discussed for the controls to improve the security of the infrastructure.