Cybersecurity Assessment Report

Cyber Security Assessment on Agricore Infrastructure

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

This assessment report is performed on the entirety of Agricore e-commerce infrastructure, designed to meet business and technical requirements, and demonstrates a commendable foundation. The report emphasized the critical balance between operational efficiency and robust security measures. While essential services and applications are in place, this report serves as an examination uncovered underlying weaknesses that could pose risks to the system's security. To address these threats, our report provides a set of practical recommendations and mitigation controls that were implemented and could be added on top to enhance the security posture of Agricore.

Threats

Based on the infrastructure developed for the Agricore ecommerce business, most of the business and technical requirements were met. The essential services that serve as paramount for the infrastructure were implemented. The business applications were also added to an extent where the operations could be carried out seamlessly. The Agricore e-commerce infrastructure demonstrated a robust foundation for the operations of the online agricultural marketplace. However, there are some underlying weaknesses in the system that could pose some risk. These findings were found based on rigorous examination and assessment of the Agricore e-commerce infrastructure.

Active Directory:

- ○ Credential harvesting and brute force attacks against user accounts and group policies. Hackers may attempt to steal user credentials or gain unauthorized access through repeated login attempts. Kerberos attacks are common in AD, where adversaries can impersonate that user without needing to know the user's password. Protecting the confidentiality of TGTs is crucial.

DHCP Attacks:

- ○ DHCP spoofing attacks which consist of rogue DHCP servers on the network to distribute false IP addresses can assign incorrect IP addresses to devices, leading to network issues and potential security risks. This is a common threat for e-commerce businesses. Though an IDS was added in the infrastructure, there could be chances of such attacks.

MySQL Database:

- Databases are exposed to Denial of Service (DoS) attacks that can make resources and databases unavailable, denying users access to data or applications. Improperly sanitized user inputs can lead to SQL injection attacks, allowing attackers to manipulate database queries. The SQL injection is a major threat which we mitigated through WAF.

File Transfer and Sharing:

- Unauthorized access to sensitive files during data transfer is susceptible in businesses. Sensitive data being transferred via FTP can be intercepted or accessed by unauthorized parties. However, we have implemented secure standards to protect file sharing between employees.

Web Browser:

- Man-in-the-middle (MITM) attacks on web content are commonly conducted for ecommerce businesses. These can be used to compromise the integrity of web content or eavesdrop on communication between users and the web server. Having applied controls such as SSL, there still could be a chance of attacks as such.

IDS (Snort):

- The intrusion detection systems can tell false positives/negatives leading to either blocking legitimate traffic or allowing malicious traffic. This could lead to Inaccurate threat detection which can result in either blocking legitimate traffic or allowing malicious traffic to pass through. There could be a possibility for remote users who are trying to access resources remotely.

Backup services:

- Inadequate redundancy in backup storage may pose a risk. Our backup strategy serves by performing the backup of endpoints and stores on single server. This could be enhanced by adding more backup locations to have high availability in case of data breach.

Recommendations

To mitigate these threats, it's essential to implement security best practices and standards that are widely used in the industry. While implementing the infrastructure we ensured that security is the utmost point for the business. The following are recommendations and mitigation controls which were applied and could be added on top of the current implementation to make the system more robust and secure.

DNS:

- Implement DNSSEC. DNSSEC adds a layer of security to the DNS by digitally signing data to ensure its authenticity. This helps prevent DNS spoofing and cache poisoning attacks.
- Monitor DNS traffic. Use DNS monitoring tools to detect and respond to any unusual DNS activity, such as a high volume of failed DNS queries or unauthorized changes to DNS records.

DHCP Attacks:

- Enable DHCP snooping on network switches to mitigate rogue DHCP server attacks. This feature allows the switch to differentiate between untrusted DHCP messages and only forward trusted messages. DHCP snooping filters out DHCP messages arriving on untrusted ports.
- Configure the DHCP server to allocate IP addresses from a specific range and set a limit on the number of addresses that can be assigned to prevent exhaustion or misuse
.

Active Directory:

- Implement multi-factor authentication (MFA). Enable MFA to add an extra layer of security, requiring users to provide two or more forms of verification before gaining access to the network. This additional layer significantly enhances the security of user accounts and sensitive systems.

MySQL Database:

- To protect the database system against attacks, WAF was implemented into the network which will protect the web traffic flow. This firewall offers security for web based traffic which we were able to add into our system. To enhance the security we can further create policies which limit maximum connections, disabling persistent connections, and closing opened connections that are not in use. Also Implement strict access controls, audit trails, and change management processes to prevent and detect unauthorized modifications to the database.

File Sharing:

- To enhance the file sharing system and processes we can consider using SFTP (SSH File Transfer Protocol) or FTPS (FTP over SSL) instead of traditional FTP to encrypt data in transit and enhance the security of file transfers. Access control policies are also a measure which could restrict access to the FTP server to authorized users only.

Web Browser Protection:

- As mentioned we utilized web application firewalls (WAF) to protect web applications from a variety of attacks, including cross-site scripting (XSS) and SQL injection, by filtering and monitoring HTTP traffic between a web application and the Internet. Similarly we also implemented SSL/TLS to encrypt web traffic and ensure the integrity and confidentiality of data being transmitted between clients and the web server. Since we used self-signed certificates, we could further enhance the SSL encryption by signing through trusted certificate authority.

IDS (Snort):

- The IDS rules can be more fine-tuned and adjusted to reduce false positives and negatives without compromising security, ensuring that the system effectively detects and responds to potential threats. Conducting a review of security alerts is also good security practice. Regularly review and analyze security alerts generated by the IDS/IPS to identify and respond to potential security incidents in a timely manner.

Backup services:

- Deploying a secondary backup server is recommended to offer redundancy. Multiple backup servers can offer a high availability of services in case of breach or data recovery. Regularly test the integrity of backups by performing restoration tests to ensure that critical data can be successfully recovered in the event of data loss or a security incident.

Conclusion

In the comprehensive examination of the Agricore e-commerce infrastructure, where our approach was to build a robust foundation for the online agricultural marketplace. Our team implemented essential services and business applications that showcased a commitment to operational seamlessness. To fortify the security posture of Agricore, our recommendations and controls that we added focused on established security best practices and industry standards. As discussed, some of the threats remain in some infrastructure which includes vulnerabilities in certain services. Services such as active directory to potential DHCP attacks, MySQL database risks, file sharing concerns, and web browser vulnerabilities. All these highlight the multifaceted nature of cybersecurity challenges in an e-commerce environment. However, the controls and recommendations are designed not only to address the identified threats but also to improve the overall security posture. Some of the controls were implemented in the infrastructure and we further assessed what else could be added to improve. This included Multi-Factor Authentication (MFA) to enhance user account security, while DHCP snooping and DNS monitoring are advocated to counteract potential network vulnerabilities. In summary, the recommendations and cybersecurity trends are crucial to maintain a resilient and secure online platform