Cybersecurity Risk Assessment for ACME Software Company

Prepared by: Yengkong Sayaovong

Course: Introduction to Cyber Attacks

Date: 8/30/24

Introduction

This report presents an analysis of the cybersecurity risks facing ACME Software Company, a small, fully virtual organization. The assessment covers confidentiality, integrity, and availability (CIA) concerns for three critical departments: Product Development (PD), Software Sales (SS), and Business Operations (BO). The analysis focuses on the potential risks posed by unauthorized access, malicious changes, and denial of service attacks across these departments.

Risk Analysis by Department and Threat

1. Confidentiality of Product Development (C, PD)

Risk Identified: Unauthorized disclosure of sensitive information, such as source code, documentation, and development tools.
Assessment: High risk due to the critical nature of intellectual property and the tools used in product development. Breaches in confidentiality could result in competitive disadvantages or intellectual property theft, leading to financial losses or reputational damage.
Recommendation: Strengthen access control measures, implement data encryption, and establish monitoring for unauthorized access attempts.

2. Integrity of Product Development (I, PD)

Risk Identified: Unauthorized modification of source code, documentation, and other development resources.
Assessment: Medium to high risk. Tampering with product development assets could lead to compromised software products and, ultimately, loss of customer trust. Integrity must be protected to ensure that the software remains functional and secure.
Recommendation: Implement version control systems with strict access permissions, use checksums or hashing techniques, and regularly audit code repositories for unauthorized changes.

3. Denial of Service to Product Development (D, PD)

Risk Identified: Blocking access to development tools, systems, and data, leading to delays in product creation.
Assessment: Medium risk. While such attacks could halt development activities, they are likely to cause operational delays rather than long-term damage. However, repeated attacks could affect productivity and project deadlines.
Recommendation: Deploy robust DDoS protection mechanisms and ensure that development environments have redundancy and failover capabilities.

4. Confidentiality of Software Sales (C, SS)

Risk Identified: Unauthorized access to sensitive sales information, including customer data and hosting configurations.
Assessment: High risk, as a breach of confidentiality could expose customer data, leading to

potential legal issues, regulatory fines, and loss of consumer trust.
Recommendation: Encrypt all customer and transactional data, ensure PCI DSS compliance, and implement multi-factor authentication for all systems accessing sales data.

5. Integrity of Software Sales (I, SS)

Risk Identified: Unauthorized changes to sales-related data, such as product configurations and customer information.
Assessment: High risk, as compromised sales data could result in faulty transactions, inaccurate customer information, and corrupted product configurations, leading to business disruptions.
Recommendation: Utilize data integrity checks and encryption, and ensure that sales data systems are frequently audited for integrity.

6. Denial of Service to Software Sales (D, SS)

Risk Identified: Malicious attacks that prevent access to sales platforms and customer data.
Assessment: High risk. A denial of service attack could shut down the company's ability to process transactions, directly impacting revenue and customer satisfaction.
Recommendation: Implement DDoS protection, maintain regular backups of the sales platform, and develop a business continuity plan to ensure minimal disruption.

7. Confidentiality of Business Operations (C, BO)

Risk Identified: Unauthorized disclosure of internal data, such as employee records, payroll information, and financial data.
Assessment: High risk, as exposure of business operations data could lead to financial losses, identity theft, and other severe legal ramifications.
Recommendation: Encrypt all sensitive data, use role-based access controls, and ensure regular reviews of access privileges.

8. Integrity of Business Operations (I, BO)

Risk Identified: Unauthorized modification of critical business information, such as payroll or financial data.
Assessment: Medium to high risk. Any modification of sensitive business data could result in financial mismanagement, employee dissatisfaction, or regulatory non-compliance.
Recommendation: Enforce strict data integrity policies, audit financial systems regularly, and ensure that all changes to operational data are logged and monitored.

9. Denial of Service to Business Operations (D, BO)

Risk Identified: Disruption of access to key operational systems, including payroll, contracts, and financials.
Assessment: Medium risk. While a denial of service attack could temporarily halt business operations, the overall impact may be limited to short-term disruptions if proper backups and recovery processes are in place.
Recommendation: Implement business continuity planning, ensure critical business systems have redundant access paths, and regularly test backup and recovery processes.

Conclusion

ACME Software Company faces several cybersecurity risks across its Product Development, Software Sales, and Business Operations departments. The most critical risks are associated with the confidentiality of sensitive data, particularly in the Software Sales and Business Operations departments, where customer and financial data are handled. ACME should prioritize implementing strong access controls, encryption, and regular auditing across all departments to mitigate these risks. Additionally, developing a comprehensive incident response plan and improving overall cyber awareness within the company will further strengthen its security posture.

Recommendations Summary

1. Access Control: Implement strict access permissions, multi-factor authentication, and role-based access control.
2. Data Encryption: Ensure that sensitive data in all departments is encrypted both in transit and at rest.
3. DDoS Protection: Deploy protection against denial-of-service attacks and ensure business continuity plans are in place.
4. Regular Audits: Conduct regular security and data integrity audits across all systems.
5. Incident Response Planning: Develop and test an incident response plan that covers potential breaches in confidentiality, integrity, and availability.

References

Coursera. (n.d.). Stages of Incident Response. Retrieved from https://www.coursera.org/learn/stages-of-incident-response/home/info