Threat Modeling a Business Process Using STRIDE

Jeytha Sahana Venkatesh Babu

Pace University

Introduction to Cybersecurity Fall 2024 72308 - CYB 611- 72308 - 202470

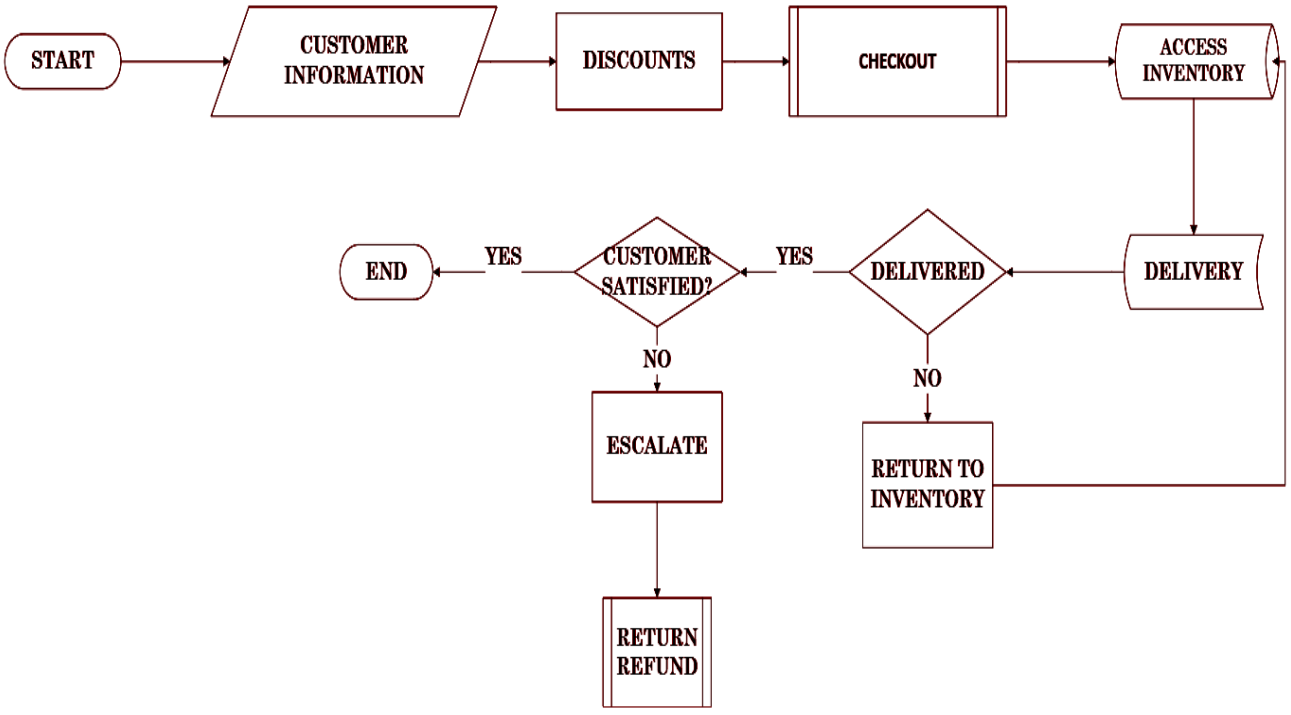
Todd M. Hammond

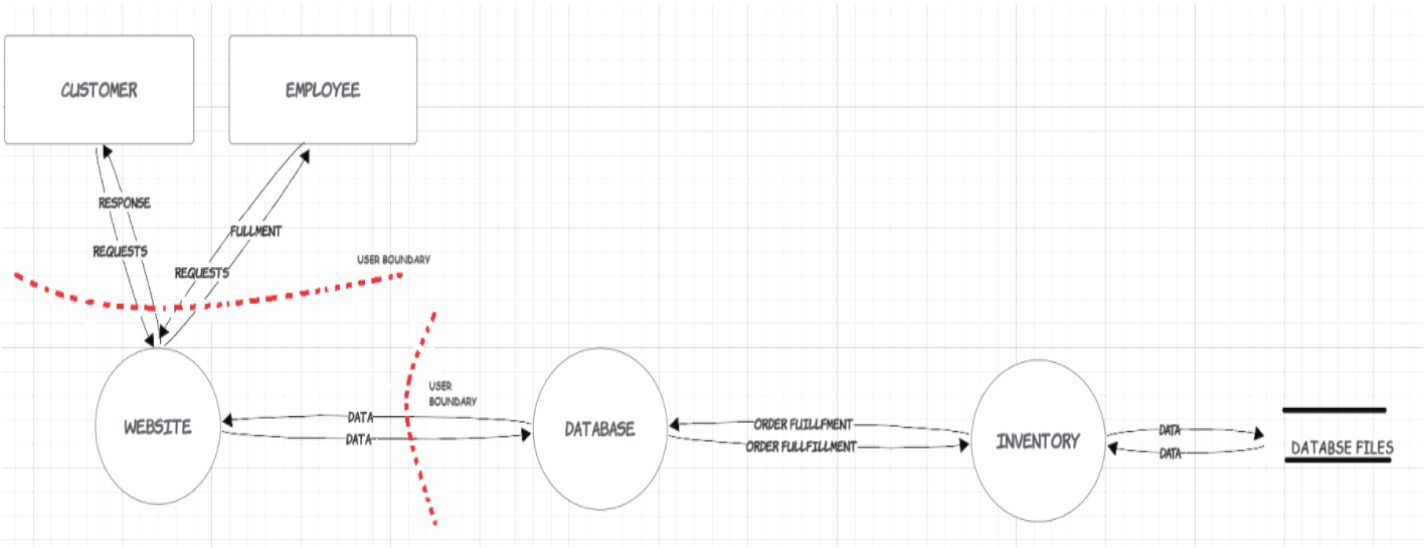
October 28, 2024

Threat Modeling a Business Process Using STRIDE

Introduction

The company chosen for the STRIDE analysis is an e-commerce t-shirt company whose entire database is based online and their sales entirely depend on online traffic. The company is currently making its foothold in the industry and is fast growing in terms of revenue and has quickly secured a spot among one of the top-selling fast fashion clothing brands. Since the entire business runs on an online platform, there is a crucial need to maintain the security and integrity of the company. The company has multiple business processes involved in ensuring its success, this paper will focus on and analyse one such process - Order Processing and Fulfilment(*Order Fulfillment Process: Definition and 7 Key Steps*, 2024). The process begins with retaining customer information in the company database followed by a secure payment gateway, and delivery logistics, and finally ends with ensuring customer satisfaction(Lisa Schwarz, 2020).





Threat Table

Trust Boundary	**STRIDE Category**	**Threat Identified**	**Weakness/Vulnerability**	**Mitigation Control**
Checkout page ↔ Customer details	Information Disclosure	Customer details exposed	Unencrypted data transmission, excessive access	Utilising end-to-end encryption, RBAC, Least privilege principle, Masking data
Checkout Page ↔ Payment Gateway	Spoofing	Attacker disguises to claim payment details	Secure payment gateways use authentication methods	(PCI DSS) compliance and implementing secure electronic transactions
Order Processing System ↔ Database	Tampering	The attacker tampers with order details and makes changes	Lack of encryption, absence of access control, database corruption	Constant monitoring of logs, RBAC, and Least privilege principle.
	Denial Of Service	The attacker prevents the processing of	Lack of security controls in server and database.	Monitor threats in real-time and limit network

		the order		traffic
Order Processing System ↔ Warehouse System	Information Disclosure	Customer details exposed	Unencrypted data transmission, excessive access	Utilising end-to-end encryption, RBAC, Zero Trust principle
Order Management System ↔ Delivery	Spoofing	Impersonate delivery partner	Identify verification failure	User authentication systems, PCI DSS Compliance
	Elevation of Privilege	Leak customer addresses and delivery details	Lack of secure access controls	Masking data, RBAC, Least privilege principle
	Denial of Service (DoS)	Prevents delivery of products	Lack of security controls in server and database.	Monitor threats in real-time and limit network traffic
Customer Service Portal ↔ Customer Support	Customer fraud/ Repudiation	Customer denies receiving the product, raises fake complaints	Failure to document proper delivery and item information	Proper documentation, auditing, and customer query logs maintained

Conclusion

From the above, we can infer that each step along the process seems to come with its own type of risk and vulnerabilities that could pose risks especially in handling sensitive customer data and ensuring seamless order fulfilment. Risks discussed range from something as simple as tampering with data to as risky as denial of service that could adversely affect business operations and the reputation of the company, to ensure such circumstances are avoided, the analysis also provides mitigation control suggestions that include but are not limited to

methods such as zero trust, least privilege, role-based access controls, regular motoring and logging access as well as secure encryption and masking on private customer data(Allen-Addy, 2023). Ensuring these procedures are implemented and complied with could prevent any drastic loss or risk to the growth of the company to the best of its capacity.

References

Allen-Addy, C. (2023, September 29). *Threat Modeling Methodology: STRIDE*. Www.iriusrisk.com. https://www.iriusrisk.com/resources-blog/threat-modeling-methodology-stride

Conducting a STRIDE-based threat analysis Secure Connected Places Playbook Cyber security resources for local authorities. (n.d.). https://assets.publishing.service.gov.uk/media/65e732717bc3290adab8c234/Conducting_a_STRIDE-based_threat_analysis_2.0.pdf

Conklin, L. (2022). *Threat Modeling Process | OWASP*. Owasp.org. https://owasp.org/www-community/Threat_Modeling_Process

Lisa Schwarz. (2020, August 20). *The heart of your business: Order fulfillment*. Oracle NetSuite. https://www.netsuite.com/portal/resource/articles/erp/order-fulfillment.shtml

Order Fulfillment Process: Definition and 7 Key Steps. (2024). Indeed Career Guide. https://www.indeed.com/career-advice/career-development/order-fulfillment-process

WebFX. (2023, October 4). *How to Conduct a Supply Chain Risk Assessment at Scale | TrueCommerce*. TrueCommerce. https://www.truecommerce.com/blog/supply-chain-risk-assessment/