Chapter 20
Understanding Cybersecurity Threats in E-Commerce

Ruchi Rai
Shri Ram Group of Colleges, Muzaffarnagar, India

Ankur Rohilla
https://orcid.org/0009-0006-4322-2246
Shri Ram Group of Colleges, Muzaffarnagar, India

Abhishek Rai
S.D. College of Engineering and Technology, Muzaffarnagar, India

ABSTRACT

In the dynamic realm of e-commerce, the pervasive and evolving landscape of cybersecurity threats presents formidable challenges to businesses and consumers alike. This chapter provides a succinct overview of the key themes explored in the comprehensive discussion on cybersecurity threats within the e-commerce domain. The chapter begins by delineating the spectrum of cybersecurity threats confronting e-commerce platforms, ranging from sophisticated malware and ransomware attacks to deceptive phishing tactics and disruptive distributed denial of service (DDoS) assaults. By illuminating the diverse array of threats, the chapter underscores the imperative for e-commerce stakeholders to remain vigilant and proactive in safeguarding their digital assets and customer data. Furthermore, the chapter delves into the underlying vulnerabilities inherent in e-commerce infrastructures, emphasizing the critical importance of fortifying payment gateways, securing web applications, and implementing robust authentication mechanisms to mitigate potential risks.

DOI: 10.4018/979-8-3693-6557-1.ch020

1. INTRODUCTION

E-commerce has evolved from simple online storefronts to complex ecosystems that integrate various technologies such as cloud computing, mobile applications, and artificial intelligence. This evolution has expanded the attack surface for cybercriminals, who exploit vulnerabilities in these technologies to conduct malicious activities.

2. TYPES OF CYBERSECURITY THREATS

2.1 Phishing Attacks

Phishing attacks are the most prevalent and insidious cybersecurity threats in the e-commerce domain. These attacks involve cybercriminals masquerading as legitimate entities to deceive individuals into divulging (Ramanathan, V., & Wechsler, H, 2012) important information, such as login ids and passwords, credit card numbers, and personal details. The sophistication and variety of phishing techniques have increased over the years.

Mechanisms of Phishing Attacks

1. **Email Phishing:** Attackers send emails that appear to be from reputable sources, such as banks, online retailers, or trusted organizations. These emails often contain urgent messages prompting recipients to click on malicious links or download infected attachments. For example, a phishing email might claim that there is an issue with a user's account and require immediate verification to avoid suspension.
2. **Spear Phishing:** Unlike generic phishing attempts, spear phishing targets specific individuals or organizations. Attackers conduct thorough research to craft personalized messages that increase the likelihood of the recipient falling for the scam. These tailored attacks can be highly convincing, as they often reference specific details relevant to the target.
3. **Smishing and Vishing:** Phishing extends beyond emails to SMS (smishing) and voice calls (vishing). In smishing, attackers send text messages that contain malicious links or prompt recipients to share sensitive information. Vishing involves fraudulent phone calls where attackers pose as legitimate representatives (Gupta, B. B., Joshi, R. C., & Misra, M, 2009) of organizations to extract personal information.