Technical Report: E-commerce Server Infrastructure Security and Administration at mbazars

Samson Tesfamichael
Server Administrator, mbazars

December 2, 2025

Abstract

This report details the cybersecurity framework and defensive measures implemented at the server infrastructure level for the active e-commerce platform mbazars.com. It covers critical server administration responsibilities including system hardening, network security configurations, monitoring protocols, and data recovery procedures designed to protect sensitive data and ensure business continuity for a commercial online marketplace.

Contents

0.1 Introduction 2
0.2 Problem Statement 2
0.3 System Architecture and Infrastructure 2
0.4 Implemented Administrative Security Measures 2
0.4.1 Server Hardening and Configuration Management 2
0.4.2 Network Security and Access Control 2
0.4.3 Monitoring, Logging, and Auditing 2
0.4.4 Backup and Disaster Recovery 3
0.5 Outcomes and Lessons Learned 3
0.6 References 3

0.1 Introduction

The integrity and availability of an e-commerce platform are directly dependent on the security of its underlying server infrastructure. This report outlines the operational security (OpSec) measures and administrative protocols utilized to maintain a secure, resilient, and compliant server environment for mbazars.

0.2 Problem Statement

As the server administrator for mbazars, the primary challenge is mitigating persistent threats such as brute-force attacks, unauthorized access attempts, DoS/DDoS attacks, and data exfiltration while maintaining 99.9% uptime. Robust administrative controls and continuous monitoring are essential to protect both the company's assets and customer trust.

0.3 System Architecture and Infrastructure

The mbazars infrastructure utilizes a segmented architecture hosted on [e.g., AWS, Azure, Private Data Center].

- **Environment:** [e.g., Linux CentOS/Ubuntu OS across all servers]
- **Infrastructure Components:** Web Servers (e.g., Nginx/Apache), Application Servers, Database Servers (PostgreSQL/MySQL), and Load Balancers.
- **Segregation:** Production, Staging, and Development environments are strictly segregated using VLANs and dedicated firewall rules.

0.4 Implemented Administrative Security Measures

The core of the server administration role involves implementing multi-layered security controls:

0.4.1 Server Hardening and Configuration Management

- **Minimization:** Disabled all non-essential services and daemons on production servers.
- **SSH Security:** Enforced key-based SSH authentication only (passwords disabled), restricted root login, and modified default SSH ports.
- **Patch Management:** Implemented a routine monthly patching cycle for all operating systems and core software packages to address known vulnerabilities (CVEs).

0.4.2 Network Security and Access Control

- **Firewalls (IPtables/Security Groups):** Configured stateful firewall rules to only allow necessary traffic (e.g., 80, 443, specific admin VPN IPs).
- **VPN Access:** All administrative access is strictly enforced via a secure, audited VPN connection with multi-factor authentication (MFA).
- **Principle of Least Privilege:** Configured user accounts with minimal necessary permissions required for their specific role.

0.4.3 Monitoring, Logging, and Auditing

- **Centralized Logging:** Utilized a centralized logging system (e.g., ELK stack) to aggregate logs from all servers for analysis and auditing.

- **Intrusion Detection:** Implemented host-based intrusion detection systems (HIDS) to alert on file integrity changes and suspicious process activity.
- **Vulnerability Scanning:** Coordinated regular infrastructure vulnerability scans to proactively identify and remediate security gaps.

0.4.4 Backup and Disaster Recovery

- **Automated Backups:** Established daily, weekly, and monthly automated backups of the entire database and critical configuration files.
- **Redundancy:** Backups are stored off-site in an encrypted format.
- **Restoration Drills:** Conducted periodic restoration tests to ensure data integrity and validate the disaster recovery plan (DRP) in alignment with business continuity objectives.

0.5 Outcomes and Lessons Learned

The disciplined application of these server administration best practices has ensured consistent platform stability and protected sensitive PII/PCI data, resulting in zero major security incidents to date for mbazars. The primary lesson learned is that robust cybersecurity relies fundamentally on secure infrastructure management and proactive monitoring.

0.6 References

- National Institute of Standards and Technology (NIST). "Guide to Enterprise Server Security." csrc.nist.gov
- CIS (Center for Internet Security). "CIS Benchmarks for Operating Systems." www.cisecurity.org
- PCI Security Standards Council. "PCI DSS Quick Reference Guide." www.pcisecuritystandards.org
- AWS Documentation. "Security Best Practices for Your EC2 Instance." docs.aws.amazon.com