Cybersecurity Threat Report

Generated: 2025-07-28 13:55:28
Business Context: i run a online clothing business

Summary of Findings

Based on the information from your system logs, here's a summary of the suspicious activities detected:

1. **Suspicious User-Agent Activity**:
- Several IP addresses (192.168.0.6, 192.168.0.7, 192.168.1.2, 192.168.1.3, 192.168.1.4, 192.168.2.2, 192.168.3.1, 192.168.3.2, 192.168.3.5) have been flagged for using suspicious user-agents. This means that the way these users are accessing your website is unusual and could indicate automated tools or bots trying to find vulnerabilities.
- These activities targeted various sensitive paths like '/admin', '/login.php', '/wp-admin', '/admin/config', '/.env', '/private', and '/config.php'.

2. **Path Traversal Attempt**:
- The IP address 192.168.0.8 attempted a path traversal attack. This is when someone tries to access restricted areas of your server by manipulating the URL path. The specific attempt was to access a sensitive file ('/../../../etc/passwd').

3. **SQL Injection Attempts**:
- Two IP addresses (192.168.0.9 and 192.168.3.3) attempted SQL injection attacks. This is a technique used to manipulate your database through your website's search functionality. The goal is often to extract sensitive information or compromise the database.

Risk Assessment:
- **Suspicious User-Agent Activity**: Low to Medium Risk. While these could be benign, the volume and targeting of sensitive paths suggest caution.
- **Path Traversal Attempt**: High Risk. This is a direct attempt to access sensitive server files.
- **SQL Injection Attempts**: High Risk. These are serious attempts to compromise your database.

Next Steps:
1. **Block IPs**: Consider blocking the IP addresses involved in high-risk activities (192.168.0.8, 192.168.0.9, 192.168.3.3) to prevent further attempts.
2. **Monitor Activity**: Keep an eye on the IPs involved in suspicious user-agent activities. If they persist, consider blocking them as well.
3. **Secure Your Website**: Ensure your website software is up-to-date and consider using a web application firewall (WAF) to protect against these types of attacks.
4. **Consult IT Support**: If you have access to IT support, discuss these findings with them to ensure your systems are secure.

Rest assured, while these activities are concerning, taking the above steps can help protect your business from potential threats.

Type	IP	Reason	Path
web_attack	192.168.0.6	Suspicious User-Agent	/admin
web_attack	192.168.0.7	Suspicious User-Agent	/login.php
web_attack	192.168.0.8	Path Traversal	/../../../etc/passwd
web_attack	192.168.0.9	SQL Injection	/search.php?q=test' OR '1'='1
web_attack	192.168.1.2	Suspicious User-Agent	/wp-admin