Min Lwin (Cybersecurity)

Recommendation and Improvement plan for Network Security for Jackson Corporation

Network Component	Findings	Recommendations (Solution to improve network security)
Firewalls	Currently, a singular firewall exists that indiscriminately filters both external traffic from the internet and internal traffic from within the organization. This setup poses a potential risk as it does not allow for targeted security protocols based on the traffic source.	Implement Next-Generation Firewalls (NGFWs) to apply deep packet inspection and advanced threat intelligence. Use an Internal Firewall to separate internal traffic from external traffic. Enable IDS/IPS (Intrusion Detection/Prevention System) on firewalls for real-time threat monitoring
Web servers	The current web server of Jackson Corporation is located internally, within the organization's primary network. This setup means that the server, a crucial and sensitive asset, is exposed to the same potential risks as the rest of the internal network. In terms of security, a basic firewall is the only mechanism in place for protecting the web server. This singular firewall is tasked with filtering both incoming external traffic and internal traffic within the network, creating a potential vulnerability.	Move the web server to a Demilitarized Zone (DMZ) to separate it from the internal network. Use Web Application Firewall (WAF) to protect against web-based attacks like SQL injection and XSS. Enable TLS encryption to secure data transmission. Regularly update and patch the web server to fix vulnerabilities.
Network monitoring	Jackson Corporation's network infrastructure currently consists of wired and wireless networks. All devices, including employee workstations, servers, and other digital assets, are interconnected within this network, facilitating seamless data exchange and collaboration. There is no comprehensive system to centrally monitor, log, and analyze the security events happening across the entire network. While this interconnected setup allows for operational efficiency, it also opens potential vulnerabilities that could be exploited by internal or external threats. Currently, there is no comprehensive system in place. This limitation makes threat detection and incident response slower and less efficient, leaving the corporation at increased risk.	Deploy a SIEM solution (e.g., IBM QRadar, Splunk) to centrally monitor logs and detect threats. Implement Network Traffic Analysis (NTA) to monitor anomalies. Use Endpoint Detection and Response (EDR) to track suspicious activity on devices. Enable automated alerting for security incidents.

Breach detection	As it currently stands, Jackson Corporation primarily relies on a basic network monitoring system. This system monitors the traffic and the network's performance but lacks an advanced threat detection mechanism. The current network monitoring setup involves regular checks on the network's health, performance statistics, and traffic volume. However, it does not provide detailed analysis or real-time alerts about potential security threats, anomalies, or suspicious activities within the network. While this setup allows for maintaining basic network performance and identifying bandwidth, latency, or server downtime issues, it falls short in proactively identifying and mitigating potential security threats. As a result, the company might not be able to detect a cyber threat until after a breach has occurred. This reactive approach to network security puts the corporation's sensitive data and digital assets at significant risk.	Deploy Intrusion Detection & Prevention Systems (IDPS) for real-time threat detection. Use AI-based anomaly detection to identify unusual patterns in network traffic. Perform regular penetration testing to proactively find vulnerabilities. Enable log correlation in a SIEM to detect potential security breaches.
Remote work	As Jackson Corporation expands globally, its workforce becomes increasingly remote and mobile. Employees frequently travel or work from home, needing to access the corporation's internal resources from different parts of the world. Users are currently using shared resources using web-based tools. However, accessing these resources over public or unsecured networks poses significant security risks. The data exchanged could be intercepted and compromised by malicious entities. In this context, the absence of a secure remote access solution could potentially limit the productivity and efficiency of the corporation's mobile workforce, while also exposing the corporation's internal resources to unnecessary security risks.	Use a Secure VPN (SSL) for remote employees to securely access company resources. Implement Multi-Factor Authentication (MFA) to prevent unauthorized access. Deploy Zero Trust Network Access (ZTNA) to enforce strict authentication for each user. Use Endpoint Security Solutions to protect employee devices.
Software development	Jackson Corporation currently follows a traditional waterfall approach to software development. The coding process begins with clear-cut requirements that the development team translates into functional code. Developers code in isolation, focusing primarily on the software's functionality, with little consideration for potential	Adopt Secure Software Development Lifecycle (SDLC) principles. Implement Dev SecOps to integrate security into every stage of development. Use Static & Dynamic Application Security Testing (SAST/DAST) to detect vulnerabilities early.

	security vulnerabilities. Code reviews are not a regular practice and are typically only conducted on an ad hoc basis when a problem arises. The final product is then passed on to a separate team for testing before it's ready for deployment. The current process creates gaps in understanding and practicing secure coding principles. Without focusing on security from the outset and regular code reviews, vulnerabilities could be overlooked and make their way into the deployed software. This could potentially provide an avenue for cyber threats to compromise the application and the data it handles.	Conduct regular code reviews and security audits to identify weak points