# *Subject: Security Recommendations*

---

By: Danielle Daza

Good morning Philip,

As per your request to the team on suggesting security policies and protocols for the company, I have summarized some notes I have on the current state of the network into succinct tables for quick reference if you choose to use them in developing the security policies. The tables are by no means extensive as it serves to be more of a draft of recommendations to further build upon and plan if need be.

Below is a brief analysis of the major points of concern in regards to the current network topology.

| Observation | Key Threats | Vulnerabilities |
|---|---|---|
| Flat network with minimal segmentation | Lateral movement by attackers, unauthorized access | No ACLs or firewall rules, shared switching infrastructure, lack of VLAN segmentation for employee |
| Webserver in the internal network | Webserver compromise leading to internal breaches | No DMZ, direct access to internal database and file server |
| Lack of redundancy | Single point of failure, downtime risks | No backup firewall or switches, lack of failover systems |
| Lack of IPS/IDS and Monitoring | Undetected incidents of compromise, delayed incident response | No IPS/IDS, no SIEM or logging for security event detection |
| Database Security Concerns | Database breach, sensitive data theft | Database and webserver on same VLAN, no firewall restrictions |
| No Mention of Encryption | Data interception, payment fraud | No mention of TLS for transit, AES-128 for data at rest |

Below are the major IoCs observed that are specific to Premium House Lights' current network and recommended strategies for detection.

| Threat Category | Relevant IoCs | Detection Strategy |
|---|---|---|
| Web Application Attacks | - Unusual outbound traffic from the webserver<br>- Unauthorized file uploads or modifications | - Web server logs<br>- WAF alerts<br>- SQL database monitoring |
| Ransomware & Data Theft | - Files being encrypted in bulk<br>- Unauthorized exfiltration of large data volumes | - EDR logs<br>- SIEM alerts for unusual encryption activity |
| Credential Theft & Unauthorized Access | - Multiple failed login attempts (brute-force attempts) | - MFA logs<br>- User behaviour analytics |

| | | |
|---|---|---|
| | - Use of breached credentials | |
| DDoS/DoS Attacks on Website | - Large number of requests from a single IP<br>- High CPU/Memory consumption on webserver | - Cloud-based DDoS protection services<br>- Real-time traffic analysis (IDS) |

The following table contain industry-standards I would recommend referencing when developing the security policies.

| Publication/Framework | Use |
|---|---|
| NIST CSF v2 | Offers an extensive template of best cybersecurity practices for organizations to easily customize to organizational needs and relevant threats |
| MITRE ATT&CK Framework | A database for known tactics, techniques and procedures (TTPs) used in modern attacks to be aware of. With this knowledge, organizations can develop informed decisions on practical security standards and policies. |
| NIST Special Publication 800-52 Revision 5 of Security and Privacy Controls for Information Systems and Organizations | Provides a comprehensive catalog of security and privacy controls designed to protect information systems and organizations from the modern threat landscape. |
| PCI DSS | Mandatory for organizations processing credit card payments |

Below is an outline of a few recommendations in regards to the current network topology to remedy the observed vulnerabilities as well as my assessment each recommendations' priority – critical (0-3 months), high (3-6 months), and medium (6+ months). The prioritization is determined by the severity of the impact and likelihood of the relevant threats that the recommendation addresses. However, there are several other security measures that would be supplementary to what is provided below that would further fortify the overall security posture of the company. For brevity, I have only provided what would I feel would be required for a relatively competent security architecture.

| Task | Action | Priority |
|---|---|---|
| Implement network segmentation and DMZ | Move webserver to DMZ, apply strict firewall rules to restrict access between VLANs | **Critical** |
| Access Control Implementation | Enforce least privilege, firewall access control lists between VLANs | **Critical** |
| Deploy IDS/IPS and SIEM | Deploy IDS/IPS to monitor network traffic and implement SIEM for log analysis | **Critical** |
| Encrypt data in transit | Implement TLS 1.3 for web traffic | **Critical** |

| | | |
|---|---|---|
| Wi-fi security hardening | Upgrade to VPA3, implement RADIUS authentication, and isolate guest Wi-fi from employee network | **Critical** |
| Introduce redundancy (firewall, switches, backup systems) | Deploy redundant firewalls, switches and backup internet links | **High** |
| Encrypt data at rest | Ensure the use of AES-128 encryption for data at rest | **High** |
| Incident Response Plan | Develop and test incident response and disaster recovery plans | **High** |
| Zero-Trust Architecture (ZTA) Implementation | Adopt a ZTA by continuously verifying users and devices | Medium |
| Security awareness training | Implement cybersecurity training for employees to prevent potential phishing or insider threats | Medium |

I hope the information provided is of use when developing the necessary security policies. Thank you for your time in reviewing my notes and recommendations. Have a great day and see you at the office.

Best Regards,

Danielle Daza