Dear Manager,

I'm writing to talk about the security posture of Premium House Lights' network. We've conducted a thorough assessment of your current infrastructure and identified several areas where we can significantly improve our defenses against potential threats. Our analysis indicates that your current network configuration has vulnerabilities that could expose the company to data breaches, malware attacks and service disruptions.

Key Vulnerabilities:

The primary weaknesses in your current setup include:

- Over-Reliance on a single firewall: The single firewall represents a single point of failure. If it's compromised or fails, the entire network loses its primary protection.
- Lack of Network Segmentation (Flat Network within VLANs): Within the Production and Employee VLANs (Virtual Local Area Network), the lack of segmentation allows attackers to move laterally between devices with ease if they gain credentials to a single machine.
- Insecure Web Server Placement: The public-facing web server is located within the Production VLAN, which also holds sensitive servers like database and file server. This creates a direct path for attackers to target critical assets if they compromise the webserver.
- Absence of a DMZ (Demilitarized Zone): Currently there is no DMZ, which could provide an extra layer of security for the public-facing web server.
- Potential weaknesses in Wi-Fi security: Without robust encryption and authentication, the Wi-Fi network could be an easy entry point for attackers.

Proposed Security Enhancements:

To address these vulnerabilities and significantly enhance the security posture, we recommend the following:

1. Network Redundancy and Segmentation:
    - Implement Firewall Redundancy: Deploy a second firewall in a high-availability configuration to ensure continuous protection if one firewall fails.
    - Create a DMZ: Establish a DMZ to isolate public-facing servers like the webserver from the internal network.
    - Segmentation within VLANs: Implement role based access within each VLAN to limit communication between devices based on the principle of least privilege. This will help contain breaches and prevent lateral movement.
2. Enhance Security Controls
    - Intrusion Detection/Prevention Systems (IDS/IPS): Implement IDS/IPS to monitor network traffic for malicious activity and IP addresses in real time.
    - Strengthen Access Controls:
        - Enforce strong password policies and implement multi-factor authentication (MFA) for all users and devices.
        - Implement Role-Based access control to restrict user access based on job responsibilities.
    - Secure Wi-Fi network: Implement WPA2/WPA3 encryption and robust authentication for the employee wifi network. Separate the guest Wi-Fi network.
3. Proactive Security Measures:

- Regular Security Assessments: Conduct regular vulnerability scans and penetration testing to identify weaknesses proactively
- Path Management: Establish a formal patch management process to ensure timely updates for all systems
- Security Awareness Training: Provide regular training to employees on security best practices, including phishing awareness, password security and safe internet usage.
- Log monitoring: Implement a SIEM system to analyze security events and detect potential incidents.
- Code Verification: Implement a process for regularly scanning and reviewing the code of the website and web applications to identify and remediate vulnerabilities. This can be done through automatic vulnerability scanning services such as OWASP ZAP

4. Data Protection:
    - Data Encryption: Implement encryption for sensitive data at rest and in transit.
    - Data Backup: Regularly backup critical data, including offsite backups, to ensure business continuity in case of a disaster or ransomware attack.
    - Data Privacy Compliance: Ensure you comply with all relevant data privacy regulations, such as PIPEDA.
5. Server Hardening
    - Implement server hardening on existing and new servers. This includes removing any unnecessary services, closing unused ports and implementing strong password policies.

Implementation Timeline:

We propose a phased implementation approach:

- Phase 1 (Immediate - Next 3 Months): Focus on implementing firewall redundancy, establishing the DMZ, and strengthening Wi-FI security. Begin employee security awareness training. Initiate web application vulnerability scanning.
- Phase 2 (4-6 Months): Implement micro-segmentation within VLANs, deploy IDS/IPS, and enhance access controls (MFA, Role based access control). Begin server hardening process.
- Phase 3 (7-12 Months): Establish robust log monitoring and analysis through a SIEM, conduct regular security assessments and penetration testing, and implement a formal patch management process.

Next Steps:

We believe that implementing these recommendations will dramatically improve Premium House Lights' security posture. WHen you have a moment, let's schedule a meeting to discuss the proposals in more detail. Thank you for your time and commitment to strengthening your security.

Sincerely,

Scott Maclean
Security Analyst

References

- Cybersecurity & Infrastructure Security Agency. (n.d.). *Cybersecurity Best Practices*. https://www.cisa.gov/topics/cybersecurity-best-practices#:~:text=Using%20strong%20passwords%2C%20updating%20your,to%20both%20individuals%20and%20organizations.

- National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- National Institute of Standards and Technology. (2020, January 15). Small Business Cybersecurity Corner. *Small Business Information Security: The Fundamentals.* https://www.nist.gov/system/files/documents/2021/01/13/Getting-Started-NIST-Privacy-Framework-Guide.pdf

- Office of the Privacy Commissioner of Canada. (n.d.). *PIPEDA in brief*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/