Name: [Alexander Focsha]

Date: [07/09/2025]

Role: Junior Cybersecurity Analys

Vulnerability and Network Resilience Assessment for Acme AeroTech

1. Organizational Context

Purpose: Acme AeroTech is dedicated to the design and manufacturing of lightweight aerospace components, which necessitates stringent security measures to protect sensitive information and maintain operational integrity.

Critical Assets:

- **Sensitive Data:** This includes proprietary designs and specifications for aircraft components, as well as customer contractual information, particularly due to the recent government contract.
- **Operational Systems:** These comprise critical infrastructure like the web server, database server, and FTP server that facilitate business processes and data management.

Business Processes: The company's core activities include the design, manufacturing, and distribution of aerospace components, necessitating robust IT support and security measures.

Potential Threat Actors:

- **Cybercriminals:** Individuals and groups seeking to exploit sensitive data for financial gain.
- **Competitors:** Other aerospace manufacturers aiming to gain an advantage through intellectual property theft.
- **Insiders:** Employees with malicious intent who could compromise sensitive information.

---

2. Network Diagram Interpretation

Major Components:

- **Endpoints:** Personal Computers (PCs) utilized by Accounting, HR, and Engineering departments.
- **Servers:** The infrastructure includes a web server, database server, and FTP server that handle critical operations.
- **Network Devices:** Key devices consist of a router, firewall, and a main switch, which facilitate network traffic and security.
- **External Connections:** The network interfaces with the Internet, Wireless Access Points (AP), IP cameras, and smart printers.

---

3. Mapping Critical Assets

Sensitive Data Locations:

- **Web Server:** Hosts public-facing content but could inadvertently expose sensitive information.
- **Database Server:** Contains critical proprietary data, necessitating stringent security controls.
- **FTP Server:** May expose sensitive information to unauthorized access if not properly secured.

Access Paths: Remote access is facilitated through a VPN or a direct internet connection to the router, posing potential security risks if not properly managed.

---

4. Identifying Trust Boundaries

Trust Boundaries:

- **Internal vs. External:** The firewall serves as a primary barrier protecting the internal network from external threats.
- **User LAN vs. Server Segment:** It is crucial to separate user PCs from server resources to mitigate risks and enhance security.

Access Points:

- **Internet Access:** Managed through the router.
- **Wireless AP:** Provides internal resource access, which requires additional security measures.

---

5. Evaluating Security Controls

Current Controls:

- **Firewall:** Present but requires a detailed configuration review to enhance security.
- **Default Credentials:** A critical vulnerability exists on routers and servers, exposing the network to unauthorized access.
- **Segmentation:** Minimal segmentation is currently in place; all devices are on the same subnet without appropriate access controls.
- **Lack of Patch Management:** This increases vulnerability to known exploits, necessitating immediate action.

---

6. Identifying Likely Vulnerabilities

- **Default Credentials:** The use of factory settings on routers and servers significantly increases the risk of exploitation.
- **Flat Network Design:** The absence of segmentation permits unrestricted access to sensitive systems, heightening security risks.
- **Intermittent Outages:** The lack of redundancy in critical areas leads to service disruptions and operational challenges.
- **Outdated Infrastructure:** The absence of a patch management program results in outdated systems, making them vulnerable to attacks.

---

7. Documenting and Prioritizing Risks

Vulnerability	Impact Level	Likelihood	Mitigation Priority
Default Credentials	High	High	Immediate
Lack of Network Segmentation	High	Medium	High
Absence of Patch Management	Critical	High	Immediate
Single Points of Failure	High	Medium	High
Outdated Hardware/Software	Medium	Medium	Medium

Recommendations for Improved Network Design

1. **Change Default Credentials:** Immediately update all default credentials on network devices and servers to enhance security.
2. **Implement a Patch Management Program:** Establish a routine for regular updates of systems and applications to protect against vulnerabilities.
3. **Segment the Network:** Implement VLANs (Virtual Local Area Networks) to create distinct segments:
    - **VLAN 10:** Dedicated for the web server, database server, and FTP server, with an added load balancer and Intrusion Detection and Prevention System (IDPS) between these servers and the main switch.
    - **VLAN 20:** Designated for Accounting, HR, and Engineering PCs, complemented by a Security Information and Event Management (SIEM) system between VLAN 20 and the main switch for credential management and log collection.
    - **VLAN 30:** Allocated for wireless access points, IP cameras, printers, and other wireless devices (e.g., smartphones, laptops). An additional firewall should be placed between the main switch and VLAN 30 to enhance traffic control and security.
4. **Add Redundancy:** Introduce redundant network paths (e.g., dual routers, load balancers) to enhance availability and reliability.
5. **Enhance Firewall Rules:** Configure the firewall to permit only necessary traffic and block unauthorized access, ensuring a robust defense against external threats.
6. **Monitor and Log Activities by adding SIEM and IDPS systems:** Implement comprehensive logging and monitoring solutions to detect and respond to anomalies in real-time, enhancing situational awareness.

Conclusion

Acme AeroTech's network infrastructure requires immediate and comprehensive attention to address identified vulnerabilities and improve resilience. By executing the above recommendations, the company will bolster its security posture and operational reliability, ensuring compliance with government contract requirements and enhancing overall operational capabilities. These proactive measures are essential for safeguarding sensitive data and maintaining the integrity of critical business processes.