Case Study: UK Company Network Attack via Corporate Website

Background

A large UK company experienced a serious internal network attack that originated through their externally managed corporate website. The attackers exploited a vulnerability in the company's network service provider. This vulnerability was already known and could be purchased on the Dark Web as an exploit tool.

The attack demonstrates how third-party services and suppliers can introduce security risks, and how sophisticated attackers combine multiple stages to compromise an organisation's network.

Stages of the Attack

1. **Survey Stage**
   - The attackers examined the victim's network and services to identify weaknesses.
   - They discovered that the corporate website was hosted by a service provider whose systems contained a known vulnerability.
2. **Weaponisation**
   - The attackers created a specialised exploit delivery script targeting the vulnerability.
   - The script was added to the corporate website and designed to check the IP addresses of visitors against the company's internal IP range.
3. **Delivery Stage**
   - The malware was delivered to computers that accessed the website and could execute files in a particular directory.
   - More than 300 company computers were infected with remote access malware during this stage.
4. **Exploitation**

   Once installed, the malware collected network information and sent it to domains controlled by the attackers.
5. **Command and Control / Anti-Forensics**
   - The attackers installed additional tools to maintain access and consolidate their position in the network.
   - They identified high-value users and sensitive systems for potential further exploitation.
6. **Detection and Repair**
   - The breach was detected using network security monitoring.

- The organisation followed its incident response plan, using system and network logs and forensic examinations to investigate the attack.
- To remove the malware, infected computers were restored to a known uninfected state using backups.
- The company renegotiated its contract with the website provider to ensure similar security standards and reduce the risk of future attacks through the same route.

Impact of the Attack

1. **Operational Disruption**
   - Hundreds of computers were compromised, potentially affecting business operations.
   - Sensitive internal information was at risk of being stolen or misused.
2. **Security Awareness**
   - The attack highlighted vulnerabilities introduced by third-party providers.
   - It reinforced the importance of monitoring external systems and enforcing security standards across all partners.
3. **Financial and Reputational Risk**
   - Costs associated with investigation, system restoration, and contract renegotiation were significant.
   - If the attack had become public, it could have damaged the company's reputation and customer trust.

Lessons Learned

- **Third-Party Risk Management:** Organisations must assess the security standards of external service providers.
- **Incident Response Planning:** A clear response plan allows rapid investigation and containment of attacks.
- **Network Monitoring:** Continuous monitoring can detect suspicious activity before it escalates.
- **Backup and Recovery:** Regular backups are critical to restoring systems to a safe state after a breach.
- **Patch Management:** Known vulnerabilities should be patched promptly to prevent exploitation.

Conclusion

This attack shows how external vulnerabilities can compromise an entire organisation. Effective third-party management, strong monitoring, and an established incident response plan are essential to limit the impact of cyber attacks.