**Sirius Cybernetics Corp: Threat Analysis Study**

COMPANY NAME

STUDENT NAMES

RapidAscent

Capstone Paper

Customer: Sirius Cybernetics

DATE

**Abstract**

The Sirius Cybernetics Corporation is the leading U.S. manufacturer and supplier of androids, robots, automatic doors, digital watches, operating systems, and autonomic assistants. The company constructs a wide range of products using advanced robotics and software, including doors, lifts, toaster ovens, drink machines, and vacuum cleaners. Sirius Cybernetics currently has 342 employees, with most based at headquarters and some working remotely.

Recent audit findings revealed significant security issues: no VPN for secure remote access, use of admin credentials for file sharing, open RDP ports, lack of centralized logging and Data Loss Protection, no regular penetration testing, and no disaster recovery or incident response plans. Additionally, the company does not monitor for suspicious login activity or follow a documented security framework, relying on Windows Automatic Updates for patch management. An attack was identified, exploiting these vulnerabilities.

**Introduction**

The recent audit of Sirius Cybernetics was conducted to determine the company’s cybersecurity posture, identify vulnerabilities in its information and robotics systems, and investigate a possible intrusion. The goal was to develop methods to strengthen the company's defenses against internal and external threats, ensuring the security and integrity of their information and robotics systems.

This study aims to highlight critical areas for improvement and provide actionable recommendations for enhancing their overall security framework. In this study we also explain the methodology and tools used to examine network packet captures, user logs, and open-source intelligence, leading us to discover the source of the attack.

**Forensic Findings**

This should be the bulk of technical findings. Include technical depth, screenshots of evidence, etc.

Want to be high speed? Got STIX?

**The Threat Landscape**  
  
THREAT INTEL ANALYSIS. Diamond models? TTP Analysis, threat COA development.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tactic** | **TTP** | **Title** | **Purpose** | **Relevance** |
| Defense Evasion | T1562.001 | Impair Defenses: Disable or Modify Tools | Living Off the Land (LOTL) | Using existing tools and protocols like TELNET and FTP aligns with LOTL techniques to avoid detection |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Vulnerability Assessment and Security Recommendations**

**Identity and Access Management (IAM):** We suggest several IAM controls that Sirius Cybernetics can implement to protect again future attacks:

**Mitigations against other identified Vulnerabilities**

* Adopt a documented security framework.
* ???
* ???
* …

Implementing these solutions will significantly enhance Sirius Cybernetics' cybersecurity position. By conducting regular vulnerability assessments, the company will be able to identify and address security issues before they can be exploited. Identity and Access Management (IAM) controls, such as Multi-Factor Authentication (MFA), Role-Based Access Control (RBAC), and the elimination of insecure protocols, will harden access-based security, ensuring that only authorized users are able to access sensitive systems and data. By enforcing the least privilege principle, conducting periodic access reviews, and implementing account lockout and strong password policies the company will be able to limit the risk of unauthorized access.

Further, monitoring login attempts will enable the early detection of suspicious activities. Sirius Cybernetics can mitigate other identified vulnerabilities by choosing a trusted security framework, implementing centralized log management, closing RDP ports, using a VPN, and employing a dedicated patch management solution will provide enhancements to its security posture. Additionally, deploying a Data Loss Protection solution, developing disaster recovery and incident response plans, reconfiguring file share access, and scheduling regular penetration testing will ensure the company’s ongoing protection against potential threats.

**Log Management System**

We recommend implementing a centralized logging system to enhance the security and network visibility of Sirius Cybernetics. The company should ensure the following is implemented:

* Enable Logging for Key Systems and Applications: Ensure that logging is enabled across all critical systems and applications to capture comprehensive activity data.
* ????
* ????
* ????
* Provide Training and Awareness: Train employees on the importance of logging and how to use the centralized logging system effectively.

Properly implementing these measures will provide greater visibility into the company's information systems and network environment, enhance incident response capabilities, and support ongoing compliance efforts.

**Adopting a Security Framework**

By adopting a trusted and documented security framework, Sirius Cybernetics will be in a position to enhance its network security posture and protect its information systems. This will allow the company to minimize further attacks and more quickly recover from unprecedented events against its systems. Furthermore, Sirius Cybernetics could be positioned to regain the trust and confidence of its customers and stakeholders.

**Recommendation**: We recommend …….

**Summary**

……

**References**

Black Lotus Labs. (2023, December 13). Routers Roasting On An Open Firewall: The KV-Botnet Investigation. <https://blog.lumen.com/routers-roasting-on-an-open-firewall-the-kv-botnet-investigation/>