Simeon Hawkins
Artemis Inc.
Vulnerability Assessment
08/01/2024

Executive Summary

This report summarizes the results of a cybersecurity assessment conducted for Artemis, Inc. The purpose of the assessment was to identify security weaknesses and recommend ways to protect the company's digital assets and sensitive information. This summary presents the key findings in straightforward terms and outlines steps that Artemis, Inc. Should take to improve its security defenses.

Key Summary Findings

Remote Desktop Protocol (RDP) Exposed:

- **What We Found:** Some company computers are accessible from the internet using Remote Desktop Protocol, and they haven't been updated with the latest security patches.
- **Why it Matters:** Hackers could exploit this to gain unauthorized access to company systems.
- **Recommendation:** Immediately update all systems and restrict RDP access to authorized personnel only.

Web Application Vulnerability:

- **What We Found:** The company's web application has a flaw that could allow unauthorized users to access the database.
- **Why it Matters:** This could lead to data theft or manipulation.
- **Recommendation:** Implement stronger security checks in the web application to prevent unauthorized access.

Default Passwords on Network Devices:

- **What We Found:** Some network devices are still using default passwords, which are widely known and easily exploitable.
- **Why It Matters:** Hackers could gain control over these devices and disrupt network operations.
- **Recommendation:** Change all default passwords to strong, unique passwords immediately.

Outdated Software on Servers:

- **What We Found:** Certain servers are running outdated software that is vulnerable to attacks.
- **Why It Matters:** This could allow attackers to take control of these servers.
- **Recommendation:** Update all server software to the latest versions with security patches.

Sensitive Data Exposure:

- **What We Found:** Some sensitive company data is exposed and can be accessed without proper security measures.
- **Why It Matters:** Unauthorized access to this data could lead to data breaches and loss of customer trust.
- **Recommendation:** Implement strict access controls and encrypt sensitive data to protect it from unauthorized access.

Weak Access Controls in Applications:

- **What We Found:** Users can access parts of the application they should not be able to, due to insufficient access controls.
- **Why It Matters:** This could lead to unauthorized data access and misuse.
- **Recommendation:** Strengthen access control mechanisms to ensure users can only access data relevant to their roles.

Cloud Storage Misconfiguration:

- **What We Found:** Cloud storage services are misconfigured, potentially allowing unauthorized users to access sensitive data.
- **Why It Matters:** This could lead to data breaches and unauthorized data sharing.
- **Recommendation:** Correct the configuration settings to ensure that only authorized personnel have access to sensitive data in the cloud.

Email Server Vulnerability:

- **What We Found:** the company's email server has a vulnerability that could be exploited by attackers.
- **Why It Matters:** This could lead to unauthorized access to email communications and data breaches.
- **Recommendation:** Apply necessary security patches to secure the email server and protect communications.

Conclusion

Addressing these security issues is crucial for protecting Artemis, Inc. valuable data and maintaining the trust of customers and partners. By taking immediate action on the recommendations provided, Artemis, Inc. can significantly enhance its security posture and safeguard its digital assets against cyber threats. By following these steps, Artemis, Inc. can reduce its risk of cyber attacks and ensure the safety of its data and systems. It is essential to act swiftly and comprehensively to maintain strong security practices and protect the organization's reputation and assets.