A close up of a logo  Description automatically generated

CONFIDENTIALITY NOTE: The information contained in this report document is for the exclusive use of the client specified above and may contain confidential, privileged and non-disclosable information. If the recipient of this report is not the client or addressee, such recipient is strictly prohibited from reading, photocopying, distributing or otherwise using this report or its contents in any way.

Scan Date: 08/07/2025

Prepared for: TEL5

Prepared by: TEL5

07/08/2025

**Cyberattack Risk Assessment**

**Cyberattack Risk Assessment**

|  |  |
| --- | --- |
|  | **INTRODUCTION**  **CYBERATTACK RISK ASSESSMENT** |
| pic148 | A cyberattack risk assessment is a systematic examination of your organization's potential vulnerabilities to cyber-attacks and the likelihood of such attacks occurring. It involves identifying, analyzing, and prioritizing potential security threats, and evaluating the current security measures in place to mitigate those threats.  The goal of a cyberattack risk assessment is to identify areas of risk and recommend steps that can be taken to reduce the risk of a successful attack, thereby improving the overall security posture of your organization. |

|  |  |
| --- | --- |
| pic149 | **CYBERATTACK RISK ASSESSMENT** |

CONTENT

|  |  |
| --- | --- |
| [**EXECUTIVE SUMMARY**](#ExecutiveSummary) |  |
| [**FINDINGS**](#Findings) |  |
| [**DETAILED FINDINGS**](#DetailedFindings) |  |

[**SYSTEM CONFIGURATION**](#SystemConfiguration)

[**ENDPOINT PROTECTION**](#EndpointProtection)

[**ENCRYPTION**](#Encryption)

[**SENSITIVE DATA**](#SensitiveData)

[**EXTERNAL THREATS**](#ExternalThreats)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | pic150 | | **POTENTIAL DATA BREACH LIABILITY**  pic151  **$0** | | pic152  pic153   |  | | --- | | **OVERALL RISK SCORE** | | **100** | | | **Top Risk**   |  |  | | --- | --- | | **1** | **Potential compromised account credentials** | | **2** | **Able to crack passwords found in browser** | | **3** | **Verified lack of protection against malicious file download** | | **4** | **Bitlocker not enabled on Windows computer** | | |  | |  |  |  |  |  | | --- | --- | --- | --- | --- | |  |  |  |  |  | | EXECUTIVE SUMMARY |  |  |  |  | | |  |  |  | | --- | --- | --- | | pic154 |  |  | |  | SYSTEM  CONFIGURATION |  | |  | pic155 |  | |  |  | 1  Issues | |  | |  |  |  | | --- | --- | --- | | pic156 |  |  | |  | APPLICATIONS |  | |  | pic157 |  | |  |  | 0  Issues | |  | |  |  |  | | --- | --- | --- | | pic158 |  |  | |  | ENDPOINT  PROTECTION |  | |  | pic159 |  | |  |  | 1  Issues | | |  |  |  |  |  | | |  |  |  | | --- | --- | --- | | pic160 |  |  | |  | PATCHING |  | |  | pic161 |  | |  |  | 0  Issues | |  | |  |  |  | | --- | --- | --- | | pic162 |  |  | |  | ENCRYPTION |  | |  | pic163 |  | |  |  | 1  Issues | |  | |  |  |  | | --- | --- | --- | | pic164 |  |  | |  | SENSITIVE DATA |  | |  | pic165 |  | |  |  | 2  Issues | | |  |  |  |  |  | | |  |  |  | | --- | --- | --- | | pic166 |  |  | |  | NETWORK |  | |  | pic167 |  | |  |  | 0  Issues | |  | |  |  |  | | --- | --- | --- | | pic168 |  |  | |  | USER BEHAVIOR |  | |  | pic169 |  | |  |  | 0  Issues | |  | |  |  |  | | --- | --- | --- | | pic170 |  |  | |  | EXTERNAL  THREATS |  | |  | pic171 |  | |  |  | 1  Issues | | |  |  |  |  |  | | |  |  |  |  | | --- | --- | --- | --- | | ⚫ High Risk | ⚫ Medium Risk | ⚫ No Risk | ⚫ Not Assessed | |  |  |  |  | | **WHY IS THIS IMPORTANT?**  This "blue team" report summarizes our activities and findings for protecting your organization's information systems and networks. We use various tactics, techniques, and procedures (TTPs) to simulate an attack on the systems, assess the security posture, and identify potential weaknesses. This report documents the results, including the vulnerabilities discovered, and recommendations for improvement. The report is intended to serve as a reference for management to help guide their security efforts and prioritize resources. |  |  |  |  | |

Here is a summary list of the vulnerabilities and issues detected in each category. A more detailed description of each of these vulnerabilities can be found in the last section of this report.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | pic172 |  | **System Configuration** |  |
|  | **High Risk** |  | **1** | Enabled generic accounts |
|  | **1 Issues Found** |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | pic173 |  | **Endpoint Protection** |  |
|  | **High Risk** |  | **1** | Verified lack of protection against malicious file download |
|  | **1 Issues Found** |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | pic174 |  | **Encryption** |  |
|  | **High Risk** |  | **1** | Bitlocker not enabled on Windows computer |
|  | **1 Issues Found** |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | pic175 |  | **External Threats** |  |
|  | **High Risk** |  | **1** | Potential compromised account credentials |
|  | **1 Issues Found** |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | pic176 |  | **Sensitive Data** |  |
|  | **High Risk** |  | **1** | Sensitive data found |
|  | **2 Issues Found** |  | **2** | Able to crack passwords found in browser |

|  | Findings |  |
| --- | --- | --- |
|  |  |  |
| **1** | **Enabled generic accounts** |  |
|  | **Why is this important?**  Generic accounts are accounts that do not identify a unique individual. Examples of a generic account include the use of "guest", "user", or "manager" and indicate that multiple individuals may be using the account to access computing resources. These accounts are more difficult to track, manage access and reduce accountability. A best practice is to assure only named accounts, accounts that can be tied to a unique individual, are enabled for use. | **1 computer affected**  ∙ T5-ROY |
|  |  |  |

|  | Findings |  |
| --- | --- | --- |
|  |  |  |
| **1** | **Verified lack of protection against malicious file download** |  |
|  | **Why is this important?**  We tested system security by downloading a benign, anti-malware test file that should have been blocked by your firewall and/or endpoint protection. This is a security threat because it allows attackers to introduce malware into systems and networks that can compromise system security, introduce ransomware, steal sensitive information, modify or delete files, or use the system as a gateway to launch further attacks. To mitigate the risk of security breaches, organizations should implement effective security measures, including using up-to-date firewalls and antivirus software. | **1 computer affected**  ∙ LAPTOP-GEPIT4MJ |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **LACKING MALICIOUS FILE PROTECTION** |  | pic180 |
| pic179 |  | |  |  | | --- | --- | | |  | | --- | | **ENDPOINT PROTECTION** | | | pic181  **RISK** | | |  | | --- | |  | | **1 computer affected**  ∙ LAPTOP-GEPIT4MJ | |  | | | **Why is this important?**  We tested system security by downloading a benign, anti-malware test file that should have been blocked by your firewall and/or endpoint protection. This is a security threat because in the event someone clicked on a malicious link, malware or ransomware could be downloaded onto those systems, causing a data breach and compromising system security. | |

|  | Findings |  |
| --- | --- | --- |
|  |  |  |
| **1** | **Bitlocker not enabled on Windows computer** |  |
|  | **Why is this important?**  BitLocker is a built-in encryption feature in Windows that helps protect data on a computer's hard drive from unauthorized access. Not enabling BitLocker can become a security risk because if a computer is lost or stolen, an attacker could potentially access sensitive data on the hard drive. Enabling BitLocker helps protect sensitive data on the hard drive, reducing the risk of security incidents. | **3 computers affected**  ∙ LAPTOP-GEPIT4MJ  ∙ T5-ROY  ∙ TEL5-NETDETECTI |
|  |  |  |

|  | Findings |  |
| --- | --- | --- |
|  |  |  |
| **1** | **Able to crack passwords found in browser** |  |
|  | **Why is this important?**  The ability to crack passwords found in a browser can become a security risk as it can be used by an attacker to obtain passwords and gain access to sensitive accounts. Password cracking tools are readily available and easy to use. To minimize risk, users should avoid storing credentials in browsers. | **4 credentials affected**  ∙ victor@tel5.com.au  ∙ admin  ∙ victor  ∙ VictorZ |
|  |  |  |
|  |  |  |
| **2** | **Sensitive data found** |  |
|  | **Why is this important?**  Examples of sensitive data include information pertaining to credit card, driver's license, bank accounts, and other similar information. If a computer is lost or stolen, an attacker could potentially access sensitive data and use it for malicious purposes. Malware could also access and steal sensitive data, and unauthorized users could compromise the data. Sensitive data may be subject to legal and regulatory requirements, and failure to protect this data could result in legal and financial consequences. Strong access controls, encryption, and regular backups can help reduce the risk of security incidents. | **1 computer affected**  ∙ LAPTOP-GEPIT4MJ |
|  |  |  |

|  | Findings |  |
| --- | --- | --- |
|  |  |  |
| **1** | **Potential compromised account credentials** |  |
|  | **Why is this important?**  Compromised account credentials are user account details that have been found during a Dark Web scan. Attackers can use these credentials to access user accounts and perform malicious activities such as stealing data, modifying system settings, or launching further attacks. To mitigate this threat, passwords should be changed using strong, unique passwords, multi-factor authentication should be enabled, and suspicious account activity should be regularly monitored. | **5 credentials affected**  ∙ varun@tel5.com.au  pwd: Ade\*\*\*\*  ∙ nick@tel5.com.au  pwd: 003\*\*\*\*  ∙ 3 additional credentials |
|  |  |  |

|  |  |  |
| --- | --- | --- |
| **LEAKED CREDENTIALS** |  | pic186 |
| pic185 |  | |  |  | | --- | --- | | |  | | --- | | **EXTERNAL THREATS** | | | pic187  **RISK** | | |  | | --- | |  | | **5 credentials affected**  ∙ varun@tel5.com.au  pwd: Ade\*\*\*\*  ∙ nick@tel5.com.au  pwd: 003\*\*\*\*  ∙ 3 additional credentials | |  | | | **Why is this important?**  Compromised or "leaked" account credentials are user account details that have been found during a Dark Web scan. Attackers can acquire and use these credentials to access user accounts and perform malicious activities such as stealing data, modifying system settings, or launching further attacks. To mitigate this threat, passwords should be changed using strong, unique passwords, multi-factor authentication should be enabled, and suspicious account activity should be regularly monitored. | |