



CYBERATTACK RISK ASSESSMENT

Your IT Company Name Here

Prepared for:
Sam's Windows & Doors

16-Aug-2023

122 Atlantic Ave, Ormand, FL | 386-222-1212 | sales@ormandit.com | www.ormandit.com

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

INTRODUCTION

CYBERATTACK RISK ASSESSMENT

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.

CONTENT

EXECUTIVE SUMMARY	4
FINDINGS	5
DETAILED FINDINGS	7
SYSTEM CONFIGURATION	
ENDPOINT PROTECTION	
PATCHING	
ENCRYPTION	
SENSITIVE DATA	
EXTERNAL THREATS	

POTENTIAL DATA BREACH LIABILITY



\$1,165



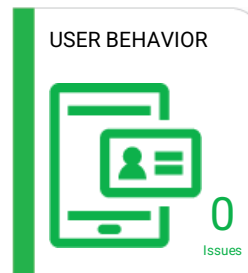
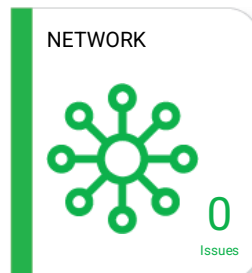
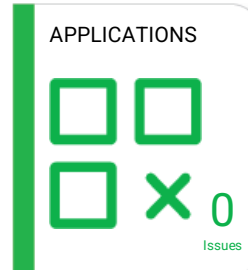
OVERALL
RISK SCORE

100

Top Risk

- 1 Potential compromised account credentials
- 2 Unsupported Operating Systems pose a threat
- 3 Able to crack passwords found in browser
- 4 Verified lack of protection against malicious file download

EXECUTIVE SUMMARY



● 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.

Prepared for: [Sam's Windows & Doors](#)
[www.ormandit.com](#) | 16-Aug-2023



FINDINGS

CYBERATTACK RISK ASSESSMENT

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.



Endpoint Protection

High Risk

- 1 Verified lack of protection against malicious file download

1 Issues Found



Encryption

High Risk

- 1 Bitlocker not enabled on Windows computer

1 Issues Found



External Threats

High Risk

- 1 Potential compromised account credentials

1 Issues Found



Patching

High Risk

- 1 Missing security patches

2 Issues Found

- 2 Recent failed patches

FINDINGS

CYBERATTACK RISK ASSESSMENT



Sensitive Data

High Risk

2 Issues Found

- 1 Sensitive data found
- 2 Able to crack passwords found in browser



System Configuration

High Risk

3 Issues Found

- 1 Unsupported Operating Systems pose a threat
- 2 Using a Student Edition or Limited-Edition Windows OS
- 3 Insecure Password Policy - Maximum password age greater than 90 days



Findings

1 Unsupported Operating Systems pose a threat

Why is this important?

Unsupported Operating Systems pose an inherent risk to the environment because they cannot be patched. Overall, unsupported operating systems can lead to decreased security, increased risk of compliance violations, technical limitations, and a lack of support, which can negatively impact IT operations and the reputation of the business.

2 computers affected

- SGODWIN-18
- MWINKER-18

2 Insecure Password Policy - Maximum password age greater than 90 days

Why is this important?

Setting the maximum password age greater than 90 days can reduce the effectiveness of passwords as a security measure. Limiting the age of passwords protects against breaches where old passwords are exposed.

1 computer affected

- SGODWIN-18

3 Using a Student Edition or Limited-Edition Windows OS

Why is this important?

Use of a student edition or limited edition of Windows OS may lead to lower security and performance. Pro and Enterprise versions of Windows include several built-in features such as BitLocker encryption, Remote Desktop, and Hyper-V virtualization. Most importantly encryption provides protection in the event of loss or theft. Consider upgrading to a Pro or Enterprise version or implementing alternative methods to provide encryption and other enterprise class features.

1 computer affected

- MJANESPC

UNSUPPORTED OPERATING SYSTEMS



SYSTEM CONFIGURATION

THE TOP 5 DANGERS OF Unsupported Operating Systems

The security issues from using an unsupported operating system can put your system and your business at risk. It is generally recommended to use supported software that receives regular updates and patches to help protect against these dangers.

1.

Security Vulnerabilities

Unsupported software is no longer being updated with security patches, leaving it vulnerable to new security threats and exploits. Attackers can exploit these vulnerabilities to gain unauthorized access to your system, steal sensitive information, or launch attacks against other targets.



2.

Compatibility Issues

Unsupported software may not be compatible with modern hardware or other software, leading to crashes, data corruption, or other issues. This can make it difficult or impossible to use the software effectively, or to exchange data with other systems.



3.

Compliance Violations

Using unsupported software can put you at risk of violating regulatory requirements or industry standards. For example, if you are using unsupported software to store or process sensitive data, you may be violating data protection laws or industry regulations.



4.

Business Disruption

If unsupported software experiences problems or becomes unusable, it can disrupt your business operations. This can result in lost productivity, missed deadlines, or other negative consequences.



5.

Lack of Support

If you encounter problems or have questions about unsupported software, you may not be able to get help from the manufacturer or other support channels. This can make it difficult to troubleshoot issues or get the assistance you need to use the software effectively.



2 computers affected

- SGODWIN-18
- MWINKER-18

Why is this important?

Unsupported operating systems may have known security vulnerabilities that have not been patched and will not receive security updates from the manufacturer, making them more susceptible to attacks. Overall, this can lead to decreased security, increased risk of compliance violations, technical limitations, and a lack of support, which can negatively impact the overall operation and reputation of the organization.



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

• MJANESPC

LACKING MALICIOUS FILE PROTECTION



ENDPOINT PROTECTION

RANSOMWARE is primary threat

Over 350,000

pieces of malware are detected every day. There are more than 970 million pieces of malware circulating the internet right now.

<https://dataprot.net/statistics/antivirus-statistics/>

Just 4.5 days

The average time between breach and ransomware detonation.

Secureworks – 2022 report



1 computer affected
• MJANESPC

Phishing is the most common form of cyber crime, with an estimated **3.4 billion spam emails** sent every day. The use of stolen credentials is the most common cause of data breaches. Google blocks around 100 million phishing emails daily.



According to CISCO's 2021 Cybersecurity Threat Trends report, about **90% OF DATA BREACHES OCCUR DUE TO PHISHING.**

PHISHING ATTACKS CONTINUE TO RISE



According to APWG, 2022 was another record-shattering year for phishing, with more than 4.7 million attacks

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.

Smaller organizations see a higher rate of malicious emails.

1-250 Employees:
1 in 323 emails are malicious

1001-1500 employees:
1 in 823 emails are malicious.



Findings

1 Missing security patches

Why is this important?

Security patches are released by vendors to address vulnerabilities and improve system security. By not installing these patches, organizations leave their systems exposed to known threats. To mitigate the risk of security breaches, organizations should implement effective patch management programs to identify, prioritize and install necessary patches, and establish policies and procedures to ensure prompt application of patches to prevent potential exploitation by attackers.

1 computer affected

- MWINKER-18

2 Recent failed patches

Why is this important?

Failed patches can leave systems in a partially patched state, which can be exploited by attackers to gain unauthorized access to systems, steal sensitive information, or launch further attacks. To mitigate the risk of security breaches, organizations should monitor patch installations closely, regularly test the effectiveness of patches, and quickly remediate failed patches. This can include backing up systems before applying patches, deploying patches to a small subset of systems before a broad rollout, and validating the success of patch installations.

2 computers affected

- MJANESPC
- SGODWIN-18

MISSING CRITICAL PATCHES



PATCHING



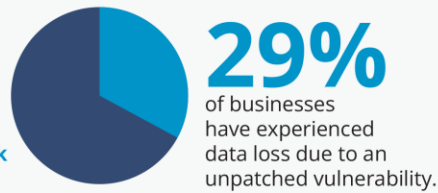
RISK

1 computer affected

• MWINKER-18

Why is this important?

Missing critical patches are a threat to organizations because unpatched software and operating systems can have known security vulnerabilities that can be exploited to gain access to sensitive information, disrupt operations, and cause damage to systems and data. By not keeping systems patched, organizations leave themselves open to these types of threats and increase their overall risk of a successful cyber-attack.



On average, it takes organizations **106 days** to patch a vulnerability.



The average cost of a data breach caused by an unpatched vulnerability is **\$3.86 million**

<https://abdalslam.com/patch-management-statistics>





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

- DESKTOP-O319KDN
- MWINKER-18
- MJANESPC



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.

103 credentials affected

- m_winker@samswin.com
- mhwinker@samswin.com
- nqrest6@intrepid7s.com
- MWINKERUS
- 99 additional credentials

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

- DESKTOP-O319KDN



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.

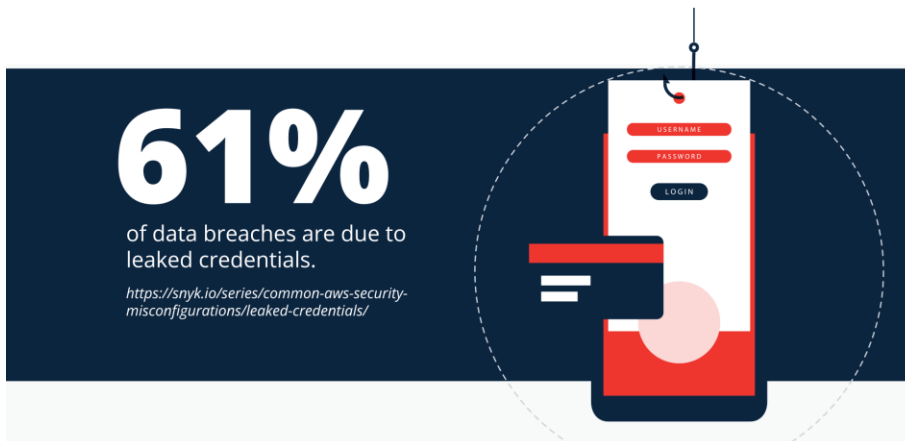
95 credentials affected

- tty@samswin.com
pwd: 94CP****
- 28101cfcsider-lsunic...
pwd: ecs1****
- 93 additional credentials

LEAKED CREDENTIALS



EXTERNAL THREATS



PASSWORD

24 billion usernames and passwords are available on the dark web – an increase of 65% in just two years, according to a new study from Digital Shadows.



RISK

95 credentials affected

- tty@samswin.com
pwd: 94CP*****
- 28101cfcside-lsunic...
pwd: ecs1*****
- 93 additional credentials

Digital Shadows found that 6.7 billion unique credentials exist –

an increase of approximately 1.7 billion or 34% in two years.



The top 5 most common passwords list in 2023

123456

123456789

1q2w3e

qwerty

password

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.