Carson City

Endpoint Security Assessment – Summary Report

April 2022

Submitted By:

Nathan Kramer – CEH
Senior Threat Management Consultant

Michael Nouguier – CISSP, PMP
Director, Cybersecurity Services

EideBailly®

CYBERSECURITY SOLUTIONS

Overview

Carson City contracted Eide Bailly to conduct an Endpoint Security Assessment to determine their exposure to a targeted attack. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against the organization. The goal of the Endpoint Security Assessment is to identify how an attacker could circumvent Carson City's endpoint defenses, workstation security configurations, and group policy settings in order to determine the impact of a cybersecurity incident.

Efforts were placed on identifying and exploiting security weaknesses that could allow an onsite attacker to gain unauthorized access to organizational data or escalate privileges. The assessment was conducted with the level of access that a standard employee would have. The assessment was conducted following industry best practices and standards, with all tests and actions being conducted under controlled conditions.

This report documents the Endpoint Security Assessment performed on a standard employee workstation issued by Carson City, conducted from April 25 to April 28, 2022.

Scope

The scope of this Endpoint Security Assessment was limited to the workstation and user account provided by Carson City.

Summary of Results

Based on the results of the Endpoint Security Assessment, **Eide Bailly identified five (5) high, five (5) medium, and one (1) low-risk finding**. The technical details of this assessment's results, including a full list of the findings and recommendations, have been obfuscated from this report for security purposes. A version of this report that includes those details was provided to Carson City's Technology team in April of 2022.

Recommendations:

1. Remediate the vulnerabilities identified in the city workstation and user account during the Endpoint Security Assessment to address the following high-risk findings: Undetected virus; security changes by users; disabled networks security controls; unquoted service paths; and unsecure ciphers.
2. Remediate the following medium and low risk findings noted on the Endpoint Security Assessment: enforce BitLocker; implement newer version of TLS; require signing on remote service; upgrade the remote Windows host; apply vendor recommended setting for remote host; implement best practice web browsing solution (noted in report).

Risk Rating Information

The findings are summarized within the body of the report and include the assignment of risk and CVSS score. The risk was determined based on our expertise of the defined risk with subjective consideration of the impact to the organization and is not based solely on CVSS.

Critical Risk - A vulnerability identified as "critical risk" should be viewed as an immediate priority for mitigation and remediation. These findings identify conditions in which exploits readily exist and/or are currently being exploited. If exploited will most likely result in the compromise and/or unauthorized access of a networked system, application, or information system. Significant security breaches and/or costly downtime may result if the vulnerability is not mitigated promptly.

High Risk - A vulnerability identified as "high risk" should be viewed as a top priority for mitigation and immediate attention. These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information. Significant security breaches or costly downtime may result if the vulnerability is not addressed within an appropriate time frame.

Medium Risk - A vulnerability identified as "medium risk" should be viewed as an essential priority for mitigation which should be addressed as soon as possible. These findings may identify conditions that, while they do not immediately or directly result in a compromise, do provide a capability or information that could result in a compromise or network disruption in combination with other vulnerabilities.

Low Risk - A vulnerability categorized as "low risk" identifies a condition that does not immediately or directly results in a compromise. However, it may provide information that could be used to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. While they can be prioritized for mitigation at a lower level, they are still of concern and may lead to more severe security threats.

About Eide Bailly

Eide Bailly advocates penetration testing for impact instead of penetration testing for coverage. Penetration testing for coverage has risen in popularity in recent years as a simplified assessment method used in situations where the goal is to meet regulatory needs. As a form of vulnerability scanning, penetration testing for coverage includes selective verification of discovered issues through exploitation, allowing service providers to conduct the work mainly through automated toolsets and maintain product consistency across multiple engagements.

Penetration testing for impact is a form of attack simulation under controlled conditions, which closely mimics the real-world, targeted attacks that organizations face on a day-to-day basis. Penetration testing for impact is a goal-based assessment, which creates more than a simple vulnerability inventory instead of providing the true business impact of a breach. An impact-based penetration test identifies areas for improvement that will result in the highest rate of return for the business.

Penetration testing for impact poses the challenge of requiring a high skill set to complete. As demonstrated in this report, Eide Bailly believes that it is uniquely qualified to deliver world-class results when conducting penetration tests for impact due to the level of expertise found within our team of security professionals.

Eide Bailly offers a product that cannot be matched in the market. However, we may not be the right fit for every job. Eide Bailly typically conducts consulting services with a low volume, high skill ratio to allow Eide Bailly staff to more closely mimic real-world situations, enabling customers to have increased access to industry-recognized expertise, all while keeping costs reasonable. High volume/fast turn-around engagements are often not a good fit for our services. Eide Bailly is focused on conducting high-quality, high-impact assessments and actively seeks out customers in need of services that other vendors cannot deliver.

If you would like to discuss your penetration testing needs, please contact us at khendrickson@eidebailly.com.