Rye Neck Union Free School District
Autonomous Penetration Test
May 14, 2024

SANOSSIAN, SARDIS & CO., LLP
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

SANOSSIAN, SARDIS & CO., LLP
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

700 WHITE PLAINS ROAD
SCARSDALE, NEW YORK 10583-5063
(914) 725-9800 • FAX (914) 725-9858
www.sscpa.co

GEORGE O. SANOSSIAN
* JACK N. SARDIS

* ALSO LICENSED IN NJ

May 14 2024

The Audit Committee
Board of Education
Rye Neck Union Free School District
310 Hornidge Road
Mamaroneck, New York 10543

Re: Penetration testing

Dear Members of the Committee and the Board,

This report is in response to your request to conduct a test of the security and potential vulnerability of the District's servers. We engaged Thrive, a global leader in cybersecurity, Cloud and digital transformation Managed Services. In prior systems tests we utilized Edge Technology Group LLC, which was acquired by Thrive in 2022. Thrive was tasked with performing a Penetration Test (Pentest) of the Districts Servers from January 29 to February 1.

A Pentest, or in this instance an Autonomous Penetration Test is an advanced cybersecurity technique that mimics an attacker, learning as it goes by pivoting through the subject environment, chaining together techniques and exploits based on what it finds.

Thrive performed three Pentests, the first two were internal Pentests initial Pentest was from January 29 to February 1 and then performed a follow up Pentest on April 1 to retest those items found to be in need of remediation during the the initial Pentest. A third external Pentest was conducted on February 2.

Procedures employed to complete the Pentest

The objective of these tests was to determine the susceptibility of the Districts servers to malicious attack by outside actors. Part of the District's regular security measures is to create, certain counter measures intended to thwart system attacks. Two different types of tests were utilized in the testing, an internal test and an external test. During an internal test a device is connected to the District's network environment and it attempts to gain access to other servers and hardware components attached to the system. An external test is a test conducted from a device outside the District environment, ie. via the internet.

Procedures employed to complete the Pentest, concluded

The initial internal Pentest was first performed from January 29 through Feb 1. The follow up, or second Pentest was conducted on April 1 to test the remediation of the weaknesses identified during the initial test. An external test of the environment was performed on April 2.

A successful attack can have devastating results, from the corruption of system databases, stealing District data, compromising individual's identities, to holding the system access hostage.

The District utilizes Edu Tek Ltd. (Edu-Tek) to assist in the maintenance and support of IT operations, and they were an invaluable resource throughout this process. The Edu Tek team was eager to contribute to the enhancement of the District's operations. Thrive worked with Edu-Tek to coordinate the Pentests.

Results of the tests

The details and results of tests are not included in this report as to not create a road map for a bad actor should they wish to illegally access the District's servers.

Internal test (initial test 1/29/24 – 2/2/24)

The severity of the weaknesses identified are placed in one of four categories ranging from critical to low. Critical weaknesses are weaknesses that could potentially lead to further compromise of additional systems or the acquisition of sensitive data. Low weaknesses are the equivalent of being able to see that something is available on a host (i.e. view that fileshares exist, view informational details about printer hardware, etc.). The other categories High and Medium which fill the ranges between critical and low.

The results of the initial test revealed that 19% of the weaknesses were of a Critical or High nature and of these weaknesses 94% were attacks on the previously mentioned countermeasures. Weaknesses identified as Low were 74% of the total weaknesses. Details of the results were communicated to the District but omitted from this report for security purposes.

Internal test (follow up test 4/1/24)

The results of the follow up Pentest on April 1 revealed that 81% of the weaknesses identified in the initial test were remediated and all of the Critical, High and Medium weaknesses identified thwarted by the system counter measures. The remaining weaknesses 81% were of the Low nature.

Results of the tests, concluded

External Test (4/2/24)

The external test yielded no instances of penetration of any level, this, according to Jason Lisnak of Thrive, who oversaw the test, results such as this are extremely rare. Similar tests performed on Hospitals and Hedge Fund clients of theirs often do not generate such positive results.

Conclusion

The results of the tests, as explained to us, show that the District's network environment is secure. Counter measures in place are operating as to be expected. Whereas, no environment can be completely secure, as evidenced by the hacks that take place against multibillion dollar companies and Government agencies, having the overwhelming majority of the attacks defined as critical actually duped by the counter measures inherent in the system, should be considered a success.

Remediation's put in place prior to the follow up Pentest eliminated 81% percent of the critical attacks identified in the initial Pentest, this is a testament to the staff overseeing the environment.

Closing

We appreciate the cooperation and assistance that we and the representatives from Thrive received from the District and its consultants. The operation's staff from Thrive specifically singled out Mary Lanza, Rye Neck Director of Technology and Communications and Steven Bavaro, Operations Manager at Edu-Tek, for their development of the District's network security as well as for their help and assistance in the timely and efficient completion of this project.

We are available to discuss the content of this report, or the District in general, at your convenience

Very truly yours,

Sanossian, Sardis & Co, LLP