Harlem
SCHOOL DISTRICT 122

MEMO TO: Harlem Board of Education
Josh Aurand, Assistant Superintendent of Business Operations
FROM: Aaron Guske, Director of Technology
DATE: July 7, 2021
RE: Cyber Risk Assessment Recommendation

Recommendation:

In our continued effort to protect the District's staff and student data and to comply with our cyber security insurance, we are recommending a cyber security risk assessment that includes the following (from Secure Halo proposal):

External Scanning and Testing (Phase 1)

During the assessment we will perform port scans, vulnerability scans and we also test the firewalls to ensure they are blocking the appropriate traffic. The testing team will apply a similar methodology for testing each scenario below which includes but is not limited to:

- Discovery using automated tools / scanners
- Discovery and verification of scanner & tool output using manual methods
- Identification of potential weaknesses and attack vectors
- Proof of concept exploitation of identified weaknesses as coordinated
- Privilege escalation, network pivoting, etc.

We will determine the exposure that the environment has to anonymous Internet attackers. During external testing, the Secure Halo team will use open source intelligence and/or information provided by the customer to perform scanning and enumeration from the outside. The test team will identify vulnerabilities that may be present in these external assets and attempt to exploit them to gain access to sensitive data or internal resources. Where exploitation may cause system instability in network systems, the test team will note the vulnerability and provide details for additional investigation.

As a part of the external testing an in-depth company profiling and threat modeling exercise is performed. One of the values provided by this testing is an understanding of what information can be gathered about your organization and, more importantly, what attackers can do with it. We will use

various tools and resources to collect public information about your organizations, coupled with custom threat modeling, to perform attacks and report on them.

Internal Vulnerability Scan and Testing (Phase 2)

This phase will determine the exposure that our environment has to a malicious insider who has gained network access to internal user networks or an external attacker who has gained access to internal networks through exploitation of externally accessible resources or social engineering. Once identified, any weaknesses and vulnerabilities will be analyzed for potential impact, and recommendations will be provided for mitigation efforts. The test team will attempt to verify that findings identified through manual and automated testing are legitimate, eliminating false positives as necessary, to deliver an accurate final report. If a finding cannot be verified without causing damage to the systems, the test team will note in the report that it could not be verified and may be a false positive.

During the internal and external testing, web applications may be discovered which require specialized skill and tools. When discovered, web application testing will commence looking for ways to leverage the web application to gain unauthorized access to the system and networks. Secure Halo will also perform system hardening checks to verify the hardening index and consistency of workstations, servers, and networking devices

Pricing

We have solicited proposals from three vendors and Secure Halo provided the lowest cost proposal without compromising any of our testing requirements. The proposed price for internal and external penetration testing is $12,000.00. This will be paid for with Technology Department funds.