Vendor Questions and MUSL Responses

Question 1. For the physical social engineering security assessment, what is MUSL's expectation for duration? This type of assessment, depending on the complexity, can range from 1-5 days. Can MUSL confirm expectations for this component of the assessment?

Response 1: MUSL expects the physical social engineering security assessment to be performed over two to three days.

Q2. For the web application assessment,

a. Can you provide a list of the applications along with the approximate number of pages where users can input or interact with the application (e.g., pages that are not static)?

R2a: The project will likely include ten (10) applications (a combination of external, internal and external/internal), with various roles tested for each web application. A list of applications will be provided to the selected vendor.

b. Do you require the web application testing to be completed with credentials or without? Can you provide the number of roles to be tested?

R2b: MUSL will require the testing to be completed with credentials.

c. Do you have test environments for these applications?

R2c: Yes, test environments are available for the applications.

Q3. For social engineering, does MUSL expect technology-based social engineering (e.g., phishing) or just physical social engineering?

R3: MUSL expects both technology-based social engineering and physical social engineering to be part of the project.

Q4. Regarding the internal/external network penetration test, will the selected vendor attempt to exploit identified vulnerabilities?

R4: If a vulnerability is identified, the selected vendor may attempt to exploit the vulnerability, so long as exploitation does not disrupt online services and/or cause damage to the internal and external networks.

Q5. Regarding the physical security assessment: If we do/do not gain access, is a physical security assessment with recommendations for improvement expected?

R5: A physical security assessment with recommendations for improvement is expected as part of this project.

Q6. Would you please provide the number of active external IP addresses to scope the external portion of the penetration test?

R6: We have two ranges in the scope of the project, with each having a /24. Both are only sparsely used.

Q7. Would you please provide a list of internal active IP addresses or network segments on the internal network?

R7: MUSL has 15 ranges in scope with each having a /24.

Q8. Regarding the web app penetration tests:

a. For internal application penetration tests, will remote access be provided for the 8 applications?

R8a: Yes.

b. Do all 12 applications require authenticated testing? If so, would you please complete the following questions for each application?

i. Please provide an overview of the application, including:

- A general overview of system/application functionality.
- Primary features of the application and which ones are being tested.
- What type of information is stored?
- How is data transmitted between systems?

R8b: Not all of the 12 applications require authenticated testing. MUSL anticipates that approximately ten (10) applications will require this type of testing. Specific information on the applications will be provided to the selected vendor, and will be included in the Statement of Work.

c. Who hosts the webserver(s)?

R8c: MUSL hosts the webserver(s) internally.

d. Who manages the systems in scope (your team or a partner)?

R8d: MUSL manages the systems that are included in this project.

e. What type of server and web server software is used?

R8e: MUSL uses IIS and NGINX. Additional information will be provided to the selected vendor.

f. Does the site use any backend databases? If so, what type(s)?

R8f: Yes. MUSL uses an SQL backend database.

g. What security controls are in place protecting the website (E.g - Web Application Firewall, etc.)?

R8: MUSL uses firewalls as a security control when protecting the website.

h. What code bases are utilized (i.e .NET, ASP, PHP, ColdFusion, etc.)?

R8h: MUSL uses Angular/C# and Classic ASP.

i. Are there any data connectors/API's to outside parties? If so, please provide a list.

R8i: No, there are no data connectors/APIs to outside parties.

j. Will the testing be in development, test, or production environment(s)?

R8j: Testing will be in the production environment.

k. How many unique functions exist across the site/application?

R8k: This information will be provided to the selected vendor.

l. How many forms are configured on the website?

R8l: This information will be provided to the selected vendor.

m. Please list each user role, including privilege, and purpose.

R8m: This information will be provided to the selected vendor.

Q9. Azure and Office 365 are listed. Is the expectation that configs are checked or are you letting us know these are in-scope for the overall test?

R9: Azure and Office 365 are in scope for penetration testing, and must be performed per Microsoft guidelines.

Q10. Can you clarify the timeline? If the kickoff is in October with work to be complete in January and February, that leaves very little time to write the report. If we have availability prior to January/February, can the testing start before then?

R10: MUSL expects initial web application and technology-based social engineering to take place once the kick-off meeting and Statement of Work have been completed.