REQUEST FOR PROPOSALS: Penetration Testing Services
Questions & Answers
02/01/2023

1. On Page 9 – Section I: Services to be Provided – For Social engineering, will all RIHousing employees be in-scope, or will we be provided a list of in-scope employees?
    - **All employees will be in scope.**

2. On Page 9 – Section III: Project Approach – Will the scope listed be for each individual test or will that be broken down in each of the 4 engagements?
    - **The scope provided for testing should be included on each individual test.**

3. On Page 9 – Section III: Project Approach – Are the 5 web applications internal or external and how many roles are in each application?
    - **The web applications are both internal and external. Additional details can be provided to the awardee during the follow-on scoping calls.**

4. On Page 9 – Section I: Services to be Provided – Does RI Housing envision more white or gray box testing (excluding black box since the SOW mention authenticated testing)? Will additional details (design documents, network maps, etc.) be provided to the awardee beyond what is provided in this document?
    - **This will depend on the methodology of the awardee, but we envision gray box testing. Additional details can be provided to the awardee during the follow-on scoping calls.**

5. General – Any time restriction on testing? Is testing confined to weekends or overnight?
    - **Hackers don't have time restrictions, so we do not place any on the vendor.**

- **Regarding Social Engineering:**
    - Will RIHousing provide the list of targets/users, including email and phone numbers, or will this information be obtained by the respondent via open-source intelligence?
        - **No, this information should be obtained via open-source intel.**
    - If provided, would you like all your users phished/vished, or a sampling?
        - **Sampling of 50 employees.**
    - What are the goals? i.e., Phish users for metrics (how many clicked or submitted credentials), for access:
        - **Simulate dropping off payload.**
    - Do you host your email services/servers?
        - **No**
    - Do you utilize multi-factor authentication for email/active directory accounts?
        - **Yes**

- **Regarding Wireless Security Testing:**
  - How many wireless networks are in place? (SSIDs)
    - **6**
  - How many Access Points are there?
    - **12**
  - Are the APs identically configured?
    - **Yes**
  - Is a guest wireless network used? If yes, does the guest network require authentication?
    - **Yes, Yes**
  - What type of encryption is used on wireless networks? (WPA2-Enterprise, TKIP, AES, WEP, etc.)
    - **WPA2-Enterprise**
  - Wireless Security Testing requires testers to be on site?
    - **Only on the physical site test for the last test of the 2-year agreement**.
  - What is the desired frequency of this testing?
    - **Only on the physical site test for the last test of the 2-year agreement**.
  - Would RIHousing be open to having the wireless security testing performed on-site for the physical penetration testing to occur once within the two-year time frame?
    - **Yes**

- Clarify the "physical" penetration test for the 1 location.
  - **Attempt to gain entry to our Providence office targeting physical weaknesses and gain unauthorized access to the network.**
- Are there any internal networks in scope outside the wireless access point(s)?
  - **Yes**

- ➢ **Web Application(s) Testing – For all five applications**
1. What environment will testing be performed against? **Only Production**
   a. **Production**
   b. Production Alternative
   c. Q/A or Test
   d. Development
   e. Other
2. Where is the application hosted? **Hybrid**
   a. **On-premises network**
   b. **Private Cloud**
   c. Public Cloud (AWS, Azure, Google)
3. What is the general type or purpose of the application? **N/A**
   - **Additional details can be provided to the awardee during the follow-on scoping calls.**
4. Please provide URL(s) for each application in the scope of testing:
   - **Additional details can be provided to the awardee during the follow-on scoping calls.**

5. Is there a login function? **A & B**
   a. **Yes**
   b. **Yes, with multi-factor authentication (MFA)**
   c. No
6. How many user roles are to be tested?
   - **Additional details can be provided to the awardee during the follow-on scoping calls.**
7. Does the application have any APIs that require testing?
   - **No**