เอกสารชี้แจงข้อสอบถาม

ประกวดราคาจ้างทดสอบเจาะระบบ (Penetration Testing) และประเมินความเสี่ยง

เพื่อหาช่องโหว่ (Vulnerability Assessment)

ด้วยวิธีประกวดราคาอิเล็กทรอนิกส์ (e-bidding)

ตามประกาศประกวดราคา และเอกสารประกวดราคา เลขที่ บสส.อ.016/2567 ลงวันที่ 19 กันยายน 2567 ได้กำหนดสอบถามรายละเอียดเพิ่มเติมเกี่ยวกับรายละเอียดและขอบเขตงาน ภายในวันที่ 24 กันยายน 2567 โดย บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด (บสส.) จะชี้แจงรายละเอียดดังกล่าวในวันที่ 25 กันยายน 2567 นั้น บสส. จึงขอชี้แจงข้อสอบถาม ดังนี้:-

1. ข้อสอบถาม ข้อ 4.2 ดำเนินการค้นหาช่องโหว่ ประเมินหาจุดอ่อน ประเมินความเสี่ยงและผลกระทบ (Vuinerability Assessment) เป็นการดำเนินการแบบ Credentials scan หรือ Non-Credentials scan

   คำชี้แจง ให้ดำเนินการแบบ Credentials Scan ครับ

2. ข้อสอบถาม ข้อ 4.2 ข้อย่อยที่ 1 (1)ระบบเครือข่าวสื่อสารภายใน บสส. จำนวนไม่น้อยกว่า 3 เครื่อง (2) ระบบคอมพิวเตอร์แม่ข่ายภายในห้องศูนย์ข้อมูล จำนวนไม่น้อยกว่า 86 เครื่อง (3)ระบบ Internet และระบบป้องกันและรักษาความปลอดภัยทางคอมพิวเตอร์ จำนวนไม่น้อยกว่า 10 เครื่อง มีโอกาสที่จำนวนเครื่องเป้าหมายในการทดสอบจะเพิ่มกว่าที่ระบุหรือไม่ หากเพิ่มขึ้นสามารถระบุจำนวนได้หรือไม่

   คำชี้แจง เท่ากับจำนวนที่กำหนดใน TOR ครับ

3. ข้อสอบถาม ข้อ 4.2, ข้อย่อยที่ 1) (1) ระบบเครือข่าวสื่อสารภายใน บสส. (2) ระบบคอมพิวเตอร์แม่ข่ายภายในห้องศูนย์ข้อมูล (3) ระบบ Internet และระบบป้องกันและรักษาความปลอดภัยทางคอมพิวเตอร์ อุปกรณ์ทั้ง 3 ส่วนนี้ติดตั้งในสถานที่เดียวกันหรือไม่ สามารถระบุสถานที่ตั้งของอุปกรณ์ได้หรือไม่

   คำชี้แจง ในส่วนของระบบป้องกันและรักษาความปลอดภัยทางคอมพิวเตอร์ จะมี 6 ตัวที่อยู่ต่างสถานที่กันครับ

4. ข้อสอบถาม ข้อ 4.2, ข้อย่อยที่ 3) ผู้รับจ้างต้องทำการทดสอบและวิเคราะห์ ด้วยตัวบุคคลเอง (Manual Test) และเครื่องมือทดสอบ อัตโนมัติ (Automatic Test Tool) เนื่องจากการทำ Vulnerability Assessment เป็นการใช้ซอฟต์แวร์ทั้ง Commercial และ Non-Commercial ในการตรวจสอบ จึงขอรบกวนขอคำอธิบายเพิ่มเติมเกี่ยวกับการทดสอบด้วย Manual Test ในหัวข้อนี้ หรือหมายถึงการวิเคราะห์ผลการสแกนจากเครื่องมือที่ใช้ดำเนินการด้วยบุคคล

คำชี้แจง ให้มีการทดสอบเจาะระบบด้วย Manual Test ด้วยตัวบุคคล ไม่ได้แค่ให้ใช้ Tools ในการทดสอบเจาะระบบอย่างเดียว

5. ข้อสอบถาม ข้อ 4.3 และ 4.4 ยืนยันเป็นการทดสอบจากภายนอกเท่านั้นหรือไม่ เนื่องจาก ข้อ 4.6 ข้อย่อยที่ 1 มีการกำหนดการทดสอบให้มี การค้นหาช่องทางการเข้าถึงระบบจากเครือข่ายภายนอกและภายใน (Network Scanning)

คำชี้แจง จากที่เคยดำเนินการมา สามารถเข้ามา Onsite เพื่อทำการเจาะระบบแบบ Gray box ได้ครับ หรือ จะดำเนินการผ่านการ Remote ก็สามารถดำเนินการได้เช่นเดียวกันครับ โดยในข้อ 4.6 มีกำหนดไว้ว่าให้มีการเข้ามาดำเนินการเจาะระบบแบบ Onsite ด้วย

6. ข้อสอบถาม ข้อ 4.5 ข้อย่อยที่ 1 การทดสอบเจาะระบบเครือข่ายไร้สาย (Wireless LAN) ตามข้อย่อยที่ 1) Coverage: ระยะการให้บริการของสัญญาณไร้สาย หมายถึงการหาระยะการให้บริการของสัญญาณไร้สายในพื้นที่ของ บริษัทบริหารสินทรัพย์สุขุมวิท จำกัด เลขที่ 123 อาคารซันทาวเวอร์ส เอ ชั้น 27-30 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ ใช่หรือไม่

คำชี้แจง เข้ามาทดสอบเจาะระบบเครือข่ายไร้สายเฉพาะใน บริษัท บริหารสินทรัพย์สุขุมวิท จำกัด เลขที่ 123 อาคารซันทาวเวอร์ส เอ ชั้น 27-30 ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร กรุงเทพฯ เท่านั้นครับ

7. ข้อสอบถาม ข้อ 4.15 ขอข้อมูลการจำลองอีเมลฟิชชิงเพิ่มเติม

- จำนวนครั้งในการทดสอบอีเมลฟิชชิง
- จำนวน Scenario ในการทดสอบต่อครั้ง
- จำนวนอีเมลที่รับการทดสอบต่อครั้ง

คำชี้แจง
- จำนวน Scenario ในการทดสอบ คือ 2 Scenario
- จำนวน Email ในการทดสอบประมาณ 700 Account
- จำนวนครั้งในการทดสอบ 1 ครั้ง

8. ข้อสอบถาม ข้อ 6. การส่งมอบงาน, รายละเอียดงวดที่ 1 และงวดที่ 2

- รายงานผลการตรวจสอบผลการปิดช่องโหว่หรือจุดอ่อน หมายถึงรายงานการดำเนินการ Vulnerability Assessment ข้อ 4.2 และรายงานการทดสอบเจาะระบบตามขอบเขตข้อ 4.3, 4.4, 4.5 ใช่หรือไม่
- รายงานผลการตรวจสอบผลการปิดช่องโหว่หรือจุดอ่อนเฉพาะระบบ CDRP (ระบบงานฐานข้อมูลโครงการคลินิกแก้หนี้) หมายถึงการจัดทำรายงานการทดสอบเจาะระบบดังกล่าวแยกเล่มใช้หรือไม่

คำชี้แจง ใช่ครับ

9. ข้อสอบถาม ข้อ 6. การส่งมอบงานงวดที่ 2 ข้อย่อยที่ 3 รายงานผลการดำเนินการตามที่กำหนดไว้ในข้อ 4.13 เป็นรายงานชิ้นเดียวกันกับ การส่งมอบงานงวดที่ 2 ข้อย่อยที่ 1 หรือไม่

คำชี้แจง ในข้อย่อยที่ 3 ในงวดที่ 2 จะมีระบุว่าถ้ามีการขอเพิ่มรายงานจากที่ประชุม จะต้องมีการทำเพิ่มครับ

10. ข้อสอบถาม ในหัวข้อ 4.15 ผู้รับจ้างจะต้องดำเนินการจำลองอีเมลฟิชชิงส่งให้บัญชีผู้ใช้งานระบบจดหมายอิเล็คทรอนิกส์ ของบสส. เพื่อวัดระดับความเสี่ยงขององค์กรต่อภัยคุกคามประเภทฟิชชิงและวัดความตระหนักของผู้ใช้งานการแยกแยะฟิชชิงอีเมลโดยมีการเก็บบันทึกผลการทดสอบและวิเคราะห์ข้อมูลพร้อมนำเสนอผลการทดสอบต่อที่ประชุมตามที่ บสส.กำหนดต้องดำเนินการจำลองอีเมลฟิชชิงส่งให้บัญชีผู้ใช้งานระบบจดหมายอิเล็คทรอนิกส์ ของบสส.

- ไม่ทราบว่าบัญชีผู้ใช้งาน จำนวนเท่าไรคะ
- ไม่ทราบว่าต้องการจำนวนกี่การจำลองอีเมลฟิชชิงคะ

คำชี้แจง
- จำนวน Scenario ในการทดสอบ คือ 2 Scenario
- จำนวน Email ในการทดสอบประมาณ 700 Account
- จำนวนครั้งในการทดสอบ 1 ครั้ง

****