ร่างขอบเขตงาน (Terms Of Reference : TOR)
โครงการตรวจสอบความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ กรมควบคุมโรค
การทดสอบการเจาะเข้าสู่ระบบและอุปกรณ์เครือข่าย (Pen Test)

๑) ความเป็นมา

ศูนย์สารสนเทศเป็นหน่วยงานหนึ่ง ที่มีบทบาทในการสนับสนุนให้การดำเนินกิจกรรมของกรมควบคุมโรคเป็นไปด้วยความมั่นคงปลอดภัย จากความเสี่ยงที่เกิดจากภัยคุกคามซึ่งมีหลายรูปแบบ ดังนั้น การประเมินด้านความปลอดภัยจึงเป็นการประเมินหาช่องโหว่ และทดสอบการเจาะระบบจากผู้โจมตีภายนอกระบบ เพื่อประเมินประสิทธิภาพของเทคโนโลยีในการรักษาความปลอดภัยที่มีอยู่ในองค์กร ว่าสามารถป้องกันภัยคุกคามในรูปแบบต่างๆได้ในระดับใด โดยจะต้องทราบถึงวิธีการที่ผู้โจมตีใช้ในการเจาะระบบ เพื่อที่จะได้แก้ไขช่องโหว่ก่อนที่ข้อมูลที่สำคัญจะได้รับความเสียหายหรือถูกนำออกจากองค์กรไปโดยไม่ได้รับอนุญาต จึงจำเป็นต้องมีการจัดหาผู้รับจ้างเพื่อดำเนินกิจกรรมจัดจ้างการตรวจสอบความมั่นคงปลอดภัยระบบเครือข่ายคอมพิวเตอร์ กรมควบคุมโรค

๒) วัตถุประสงค์

เพื่อให้ระบบขององค์กรมีความปลอดภัย และเพิ่มประสิทธิภาพของการรักษาความมั่นคงปลอดภัยให้สูงขึ้น

๓) ข้อกำหนดทั่วไป

๓.๑) คุณสมบัติของผู้เสนอราคา

๓.๑.๑) ผู้เสนอราคาต้องเป็นนิติบุคคลตามกฎหมายที่จดทะเบียนในประเทศไทย ซึ่งมีวัตถุประสงค์ในการประกอบธุรกิจเป็นผู้พัฒนา หรือติดตั้ง หรือผู้ผลิต หรือจำหน่าย และ/หรือเช่า/ให้เช่าซื้อ ด้านระบบคอมพิวเตอร์ และอุปกรณ์มาไม่น้อยกว่า ๓ ปี นับจนถึงวันยื่นเอกสารหลักฐานการเสนอราคา

๓.๑.๒) ผู้เสนอราคาต้องได้รับการแต่งตั้งจากเจ้าของผลิตภัณฑ์ หรือสาขาของบริษัทผู้ผลิตประจำประเทศไทย

๓.๑.๓) ผู้เสนอราคาต้องมี Call Center หรือ Hot Line เพื่อเป็นช่องทางรับแจ้งปัญหาต่างๆ ที่อาจเกิดขึ้นได้ (๕ วันทำการ (จันทร์-ศุกร์) วันละ ๘ ชั่วโมง)

๓.๒) การดำเนินการและการส่งมอบงาน

๓.๒.๑) ผู้รับจ้างต้องเข้าทำการทดสอบการเจาะเข้าสู่ระบบและอุปกรณ์เครือข่าย (Pen Test) จำนวนไม่น้อยกว่า ๒ ครั้ง โดยนับถัดจากวันที่ลงนามในสัญญา และจะต้องไม่เกินเดือนเมษายน ๒๕๖๑ (ไตรมาสที่ ๒)

๓.๒.๒) ผู้รับจ้างต้องส่งมอบรายงานการทำการทดสอบการเจาะเข้าสู่ระบบและอุปกรณ์เครือข่าย (Pen Test) จำนวน ๒ ชุด พร้อมไฟล์เอกสารอิเล็กทรอนิกส์แนบกับเล่มรายงาน

๔) ข้อกำหนดเฉพาะ

๔.๑) ทดสอบ VA (Vulnerability Assessment) เพื่อทำการทดสอบการเจาะเข้าสู่ระบบและอุปกรณ์เครือข่าย (Pen Test) ที่รองรับได้จำนวนอย่างน้อย ๘ ไอพี มีคุณสมบัติอย่างน้อยดังนี้

๔.๑.๑) รายงานผลการทดสอบข้อมูลของช่องโหว่ตามหัวข้อดังต่อไปนี้

๔.๑.๑.๑) ทำการทดสอบ SQL Injection
๔.๑.๑.๒) ทำการทดสอบ XSS Cross Site Scripting
๔.๑.๑.๓) ทำการทดสอบ Command Execution
๔.๑.๑.๔) ทำการทดสอบ ทำการโจมตีแบบ DoS
๔.๑.๑.๕) ทำการทดสอบ Web Errors
๔.๑.๑.๖) ทำการทดสอบ Automatic web crawling engine identifies known and unknown files on websites
๔.๑.๑.๗) ทำการทดสอบ Black Hat SEO Scanner
๔.๑.๑.๘) ทำการทดสอบ Google Hack DB
๔.๑.๑.๙) ทำการทดสอบการ Hack ด้วยช่องโหว่ LFI (Local File Inclusion)
๔.๑.๑.๑๐) ทำการทดสอบการ Hack ด้วยช่องโหว่ RFI (Remote File Inclusion)
๔.๑.๑.๑๑) ทำการทดสอบ ช่องโหว่ประเภท Cross-site Request Forgery (CSRF)
๔.๑.๑.๑๒) ทำการทดสอบ WordPress Scanner
๔.๑.๑.๑๓) ทำการทดสอบ Joomla Scanner
๔.๑.๑.๑๔) ทำการทดสอบ Drupal Scanner
๔.๑.๑.๑๕) ทำการทดสอบ Magento Scanner
๔.๑.๑.๑๖) ทำการทดสอบ Shopify Scanner
๔.๑.๑.๑๗) ทำการทดสอบ Umbraco Scanner
๔.๑.๑.๑๘) ทำการทดสอบ Advanced CMS vulnerability detection crawler

๔.๑.๒) รายงานประกอบไปด้วยข้อมูลต่อไปนี้อย่างน้อย

๔.๑.๒.๑) ความเป็นมา วัตถุประสงค์ และแผนการดำเนินการ
๔.๑.๒.๒) ไอพีที่ทำการสแกน
๔.๑.๒.๓) ประเภทโปรไฟล์ที่ใช้ในการสแกน
๔.๑.๒.๔) กราฟสรุปผลการสแกน
๔.๑.๒.๕) ช่องโหว่ที่มีปัญหา
๔.๑.๒.๖) ผลกระทบของช่องโหว่ที่มีปัญหา
๔.๑.๒.๗) วิธีการแก้ไขช่องโหว่ที่มีปัญหา
๔.๑.๒.๘) หลักฐานการเจาะช่องโหว่ที่มีปัญหา

๔.๑.๓) การส่งมอบรายงานผลการทดสอบในรูปแบบรายงานและไฟล์เอกสารอิเล็กทรอนิกส์

๕) วงเงินงบประมาณ

งบประมาณสำหรับโครงการนี้ วงเงินรวมทั้งสิ้น ๑๐๐,๐๐๐ บาท (หนึ่งแสนบาทถ้วน)

สาธิต สันติสุขสานะ

๖) การจ่ายเงิน

กรมควบคุมโรคจะจ่ายเงินเมื่อมีการส่งมอบรายงานผลการทดสอบครั้งสุดท้ายเป็นที่เรียบร้อยแล้ว ภายในปีงบประมาณ ๒๕๖๑

๗) การปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของกรมควบคุมโรค

๗.๑) ผู้รับจ้างต้องยินยอมปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และวิธีปฏิบัติที่เกี่ยวข้องของกรมควบคุมโรคอย่างเคร่งครัด

๗.๒) ผู้รับจ้างต้องตระหนักถึงการรักษาความปลอดภัยในข้อมูลและทรัพย์สิน รวมทั้งความปลอดภัยของบุคลากรของกรมควบคุมโรค ในช่วงเวลาที่ผู้รับจ้างทำงานให้กรมควบคุมโรคอย่างเคร่งครัด

๗.๓) ผู้รับจ้างต้องต้องปฏิบัติตามข้อตกลงในการไม่เปิดเผยความลับ (ถ้ามี) รวมทั้งเงื่อนไขอื่นหรือข้อกำหนดต่างๆ ที่เกี่ยวข้องกับการไม่เปิดเผยความลับของข้อมูลสำคัญของกรมควบคุมโรค

๗.๔) ผู้รับจ้างต้องยินยอมให้กรมควบคุมโรคตรวจสอบการทำงานได้โดยไม่มีเงื่อนไข ในช่วงเวลาที่ผู้รับจ้างทำงานให้กรมควบคุมโรค

๗.๕) ห้ามผู้รับจ้างนำอุปกรณ์ประมวลผลหรือสื่อบันทึกข้อมูลที่ไม่ใช่ของกรมควบคุมโรค มาต่อเชื่อมเข้ากับระบบเครือข่ายของกรมควบคุมโรคโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากกรมควบคุมโรคโดยเครื่องที่ได้รับอนุญาตต้องต่อเชื่อมในตำแหน่งที่ระบุไว้เท่านั้น

๗.๖) ข้อมูลและสื่อบันทึกข้อมูลที่จัดเก็บอยู่ในลำดับชั้นความลับขึ้นไป ห้ามนำออกไปใช้งานโดยไม่ได้รับอนุญาตจากกรมควบคุมโรคโดยเด็ดขาด

๗.๗) ห้ามเคลื่อนย้ายอุปกรณ์ของกรมควบคุมโรคโดยเด็ดขาดเว้นแต่ได้รับอนุญาต โดยการดำเนินการดังกล่าวกรมควบคุมโรคจะจัดให้มีเจ้าหน้าที่ ติดตาม ควบคุม ทุกครั้ง

๗.๘) การพัฒนาระบบงาน การติดตั้งและการทดสอบระบบผ่านระบบเครือข่ายของกรมควบคุมโรค ต้องได้รับอนุญาตจากกรมควบคุมโรคและต้องใช้งานพอร์ตสื่อสาร (Service Port) ที่กำหนดให้เท่านั้น

๗.๙) ไม่อนุญาตให้ผู้รับจ้างติดตั้ง หรือเช่าบริการระบบอินเตอร์เน็ต หรือต่อเชื่อมเครื่องคอมพิวเตอร์ที่นำมาใช้งานไปยังเครือข่ายภายนอกโดยเด็ดขาด เว้นแต่ได้รับอนุญาตอย่างเป็นทางการเท่านั้น

๗.๑๐) ซอฟต์แวร์ทุกประเภทที่นำมาใช้กับงานกับกรมควบคุมโรค ต้องได้รับสิทธิ์การใช้งานถูกต้องตามกฎหมายและต้องไม่มีโปรแกรมแอบแฝงหรือโปรแกรมมุ่งร้ายใดๆ ฝังตัวอยู่ และหากกรมควบคุมโรคตรวจพบว่ามีโปรแกรมลักษณะดังกล่าวและได้ก่อให้เกิดความเสียหายต่อระบบเครือข่ายของกรมควบคุมโรค ผู้รับจ้างต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นทั้งหมด

๗.๑๑) ห้ามนำบุคคลภายนอกที่ไม่มีรายชื่อตามเอกสารที่ได้แจ้งไว้ต่อกรมควบคุมโรคเข้าพื้นที่ควบคุมความปลอดภัยโดยเด็ดขาด

๗.๑๒) ผู้รับจ้างต้องปฏิบัติงานในพื้นที่ที่กรมควบคุมโรคกำหนดเท่านั้น หากต้องการปฏิบัติงานในพื้นที่อื่นที่นอกเหนือจากที่กำหนดไว้ต้องได้รับอนุญาตจากกรมควบคุมโรคก่อนทุกครั้ง