โครงการจัดทำระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ วิเคราะห์และตอบสนองแบบอัตโนมัติโดยกลไกอัจฉริยะ (AI and Machine Learning (ML))

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานปลัดกระทรวงมหาดไทย

วัตถุประสงค์

- สำนักปลัดกระทรวงมหาดไทยมีระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ ที่มีประสิทธิภาพ และมีความมั่นคงปลอดภัยเป็นไปตามมาตรฐานสากลและสามารถรับมือภัยคุกคามเทคโนโลยีสารสนเทศรูปแบบใหม่ที่ทันสมัยได้อย่างทันท่วงที
- เพื่อสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วน ต่อการดำเนินธุรกรรมต่าง ๆ ผ่านระบบงานสารสนเทศรวมถึงการให้บริการภาครัฐในรูปแบบระบบออนไลน์
- เพื่อปกป้องผลประโยชน์และความมั่นคงของชาติจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่
- เพื่อรองรับการดำเนินงานตามนโยบาย และกฎหมายที่เกี่ยวข้อง เช่น ตามพระราชบัญญัติการรักษาความปลอดภัยทางไซเบอร์ พ.ศ.๒๕๖๒ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

เป้าหมาย

มีระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ที่ทันสมัยสามารถวิเคราะห์ เฝ้าระวัง และแจ้งเตือนภัยคุกคาม และ/หรือเหตุการณ์ผิดปกติรูปแบบใหม่อันอาจก่อให้เกิดความเสียหายอย่างรุนแรงกับข้อมูลและระบบสารสนเทศของสำนักปลัดกระทรวงมหาดไทย โดยสามารถตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ทุกรูปแบบได้อย่างมีประสิทธิภาพ ช่วยให้เกิดความมั่นคงปลอดภัยที่ได้มาตรฐานสากลและสามารถรับมือภัยคุกคามเทคโนโลยีสารสนเทศรูปแบบใหม่ที่ทันสมัยได้อย่างทันท่วงที

ความจำเป็นที่จะต้องจัดทำโครงการ

ปัจจุบันการใช้ให้บริการสารสนเทศของสำนักปลัดกระทรวงมหาดไทย มีการป้องกันทางไซเบอร์เป็นส่วน ๆ ยังไม่มีระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพในการป้องกันภัยคุมคามที่ทันสมัยเพื่อให้บรรลุเป้าหมายและเกิดผลสัมฤทธิ์ตามภารกิจของกระทรวง จึงเห็นความสำคัญในการป้องกันภัยคุกคามทางไซเบอร์ จึงมีความประสงค์จัดทำโครงการจัดทำระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ เพื่อสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วน ต่อการดำเนินธุรกรรมต่าง ๆ ผ่านระบบงานสารสนเทศรวมถึงการให้บริการภาครัฐในรูปแบบระบบออนไลน์ เพื่อปกป้องผลประโยชน์และความมั่นคงของชาติจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ความจำเป็นที่จะต้องจัดทำโครงการ

กลุ่ม Maze Ransomware ปล่อยข้อมูลชุด 100% ซึ่งเป็นผลมาจากการโจมตีระบบของการไฟฟ้าส่วนภูมิภาคแล้วหลังจากถึงเส้นตายตามมาตรการใหม่ของกลุ่ม Maze

ตามมาตรการใหม่ของ Maze ซึ่งไอ-ซีเคียวได้เคยนำเสนอข่าวไปก่อนแล้วนั้น กลุ่ม Maze จะทำการปล่อยข้อมูลชุดแรกบางส่วนเพื่อยืนยันการโจมตีว่าได้เกิดขึนจริง หลังจากนั้นกลุ่ม Maze จะมีการให้เวลาเหยื่อเป็นเวลา 10 วันเพื่อให้ดำเนินการทำตามข้อตกลง (คำขู่กรรโชก) โดยหากเหยื่อไม่สามารถทำได้ภายในเวลา 10 วัน กลุ่ม Maze จะมีดำเนินการปล่อยข้อมูลทั้งหมดที่กลุ่มได้มาจากการปฏิบัติการนั้น

ในสถานการณ์ปัจจุบันนั้น เป็นที่แน่ชัดแล้วว่าทาง PEA ตัดสินใจที่จะไม่ปฏิบัติตามคำเรียกร้องของกลุ่ม Maze ซึ่งส่งผลให้เกิดการปล่อยข้อมูลชุดนี้ออกมา การตัดสินใจในครั้งนี้หากอยู่บนพื้นฐานของการมีข้อมูลที่เพียงพอและสามารถประเมินผลกระทบหากข้อมูลที่ถูกผู้โจมตียึดครองถูกปล่อยออกมาได้ก็อาจถือได้ว่าเป็นการตัดสินใจที่ถูกต้อง เพราะการยินยอมทำตามคำขู่กรรโชกในทางอ้อมก็ถือเป็นการสนับสนุนให้กลุ่ม Maze คงอยู่และปฏิบัติการต่อไปได้

ไฟล์ที่ถูกปล่อยออกมาในครั้งล่าสุดนี้มีจำนวน 18 ไฟล์ รวมจากที่ปล่อยออกมาแล้วจำนวน 3 ไฟล์เป็นจำนวนทั้งหมด 21 ไฟล์ มีการปรากฏของชื่อไฟล์ที่บ่งชี้ให้เห็นถึงความเกี่ยวข้องกับโครงการของทาง PEA อาทิ ELGBlockchanin.7z และ EnergyProject.7z รวมไปถึงไฟล์ที่อาจเกี่ยวข้องกับสถานการณ์ COVID-19 อย่าง CovidDocs.7z ด้วย

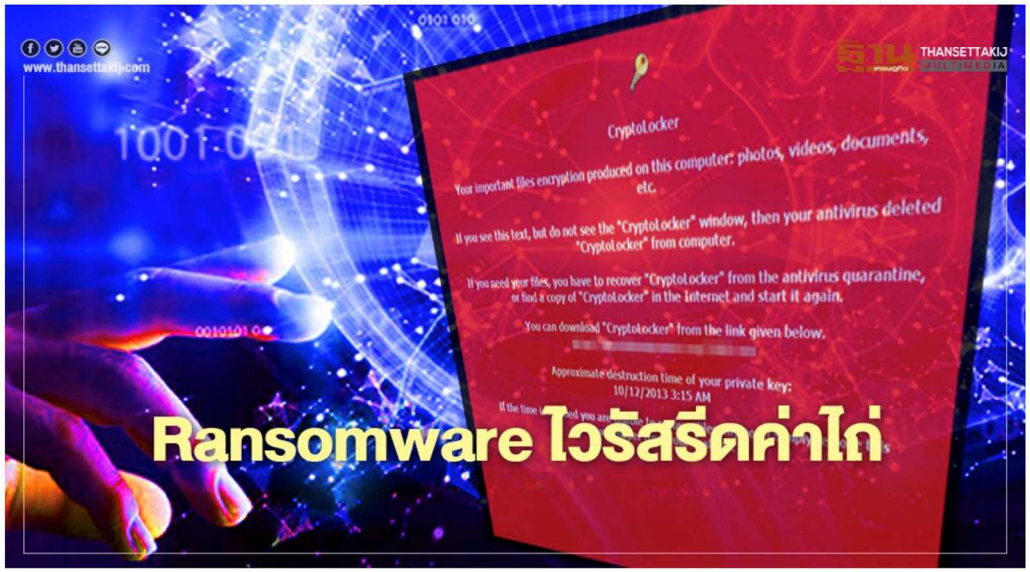
ข่าวที่เกี่ยวข้อง
กลุ่ม Maze Ransomware ประกาศกฎการจ่ายค่าไถ่ใหม่ พร้อมขู่ปล่อยข้อมูลหากไม่มีการพูดคุยกันหลังจาก 10 วัน
คาด "การไฟฟ้าส่วนภูมิภาค" อาจถูกปล่อยข้อมูลหากไม่ยอมจ่ายค่าไถ่เร็วๆ นี้

ทำความรู้จัก" Ransomware" มัลแวร์ตัวร้ายเจาะระบบโรงพยาบาลสระบุรี

09 Sep 2020 14:28 น.

182 Shares

อ่าน 3,216 ครั้ง



ความจำเป็นที่จะต้องจัดทำโครงการ

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

ระบบงานที่ขอความเห็นชอบ

ลำดับ	รายการ	จำนวน
1	ระบบคัดกรองและสำเนาข้อมูลจากระบบเครือข่าย (Network Packet Broker)	1 ระบบ
2	ระบบตรวจจับภัยคุกคามชั้นสูง	1 ระบบ
3	ระบบวิเคราะห์และตรวจจับการบุกรุก ในระบบเครือข่าย	1 ระบบ
4	ระบบบริหารจัดการและควบคุมสิทธิ์ในการเข้าใช้งาน	1 ระบบ
5	ระบบสำรองและคืนค่า Configuration ของอุปกรณ์เครือข่ายอัตโนมัติ	1 ระบบ
5	อุปกรณ์จัดเก็บข้อมูลคอมพิวเตอร์แบบรวมศูนย์ (Centralize log management)	1 ชุด
6	โทรทัศน์แอล อีดี(LED TV) แบบ Smart TV ระดับความละเอียดจอภาพ 3840 x 2160 พิกเซล ขนาด 55 นิ้ว	4 ชุด
7	เครื่องคอมพิวเตอร์ สำหรับงานประมวลผล แบบที่ 2 * (จอขนาดไม่น้อยกว่า 19 นิ้ว)	2 ชุด

- เป็นระบบงานที่ออกแบบเพื่อให้สามารถรองรับการตรวจจับการบุกรุกในระดับเครือข่ายในระยะที่ 1 โดยสามารถขยายการโครงสร้างการป้องกัน (Protection Framework) ไปยังเครื่องคอมพิวเตอร์ลูกข่ายในระยะถัดไปได้

งบประมาณ

งบประมาณรายจ่ายประจำปีงบประมาณ พ.ศ. 2565 จำนวน 154,200,800.- บาท

(หนึ่งร้อยห้าสิบสี่ล้านสองแสนเจ็ดแปดร้อยบาทถ้วน)

ผูกพันงบประมาณ ปี 2565 31,000,000 บาท

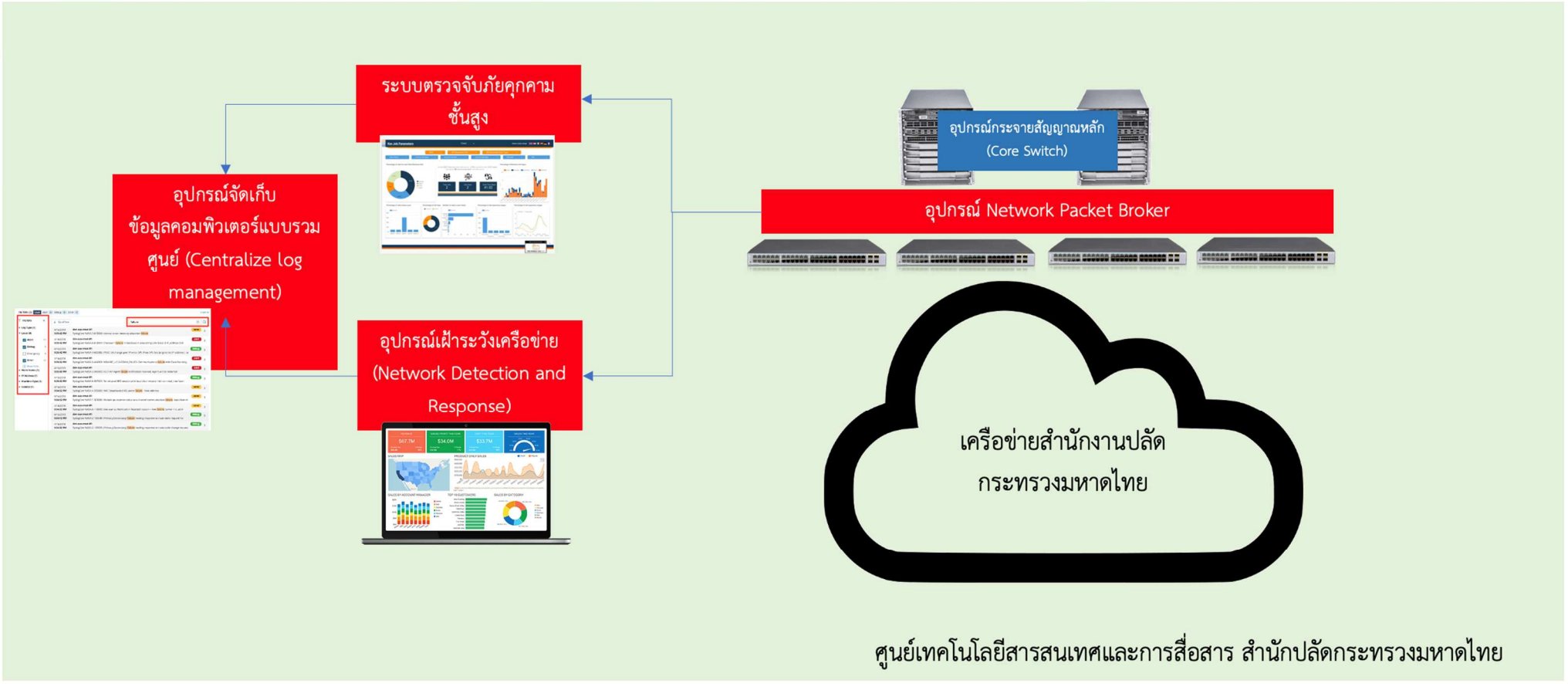
ผูกพันงบประมาณ ปี 2566 123,200,800 บาท

ลักษณะการขออนุมัติ	ระยะเวลาดำเนินการ
จัดซื้อ	14 เดือน

ประโยชน์ที่คาดว่าจะได้รับ

- ระบบสารสนเทศของสำนักปลัดกระทรวงมหาดไทยสามารถให้บริการปลอดภัยต่อภัยคุกคามต่าง ๆ โดยสำนักปลัดกระทรวงมหาดไทยสามารถรับมือภัยคุกคามเทคโนโลยีสารสนเทศรูปแบบใหม่ที่ทันสมัยได้อย่างทันท่วงที
- สร้างความเชื่อมั่นในการใช้งานเทคโนโลยีดิจิทัล ต่อประชาชน และหน่วยงานที่เกี่ยวข้อง

โครงการจัดทำระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์ วิเคราะห์และตอบสนองแบบอัตโนมัติโดยกลไกอัจฉริยะ (AI and Machine Learning (ML))



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักปลัดกระทรวงมหาดไทย

ค่าใช้จ่าย

ลำดับ	รายการ	จำนวนเงิน
1.	ครุภัณฑ์คอมพิวเตอร์ ซอฟต์แวร์ และเครื่องมือที่ใช้ในการพัฒนาระบบ	151,407,200 บาท
2.	ค่าใช้จ่ายบุคลากรดูแลระบบเฝ้าระวัง และป้องกันภัยคุกคามทางไซเบอร์	2,793,600 บาท
	รวมทั้งสิ้น	154,200,800 บาท