ETDA

ที่ ดศ (สพธอ) ๕๑๑/ว๒๖๙

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น ๒๐-๒๒ เลขที่ ๓๓/๔ ถนนพระราม ๙
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ ๑๐๓๑๐

๒๙ มีนาคม ๒๕๖๕

เรื่อง ขอเชิญเข้าร่วมโครงการ Government Monitoring System (GMS)

เรียน อธิการบดีมหาวิทยาลัยทักษิณ(สงขลา)

สิ่งที่ส่งมาด้วย ๑. เอกสารรายละเอียดและแผนการดำเนินงานโครงการฯ จำนวน ๑ ชุด
๒. แบบตอบรับโครงการฯ จำนวน ๑ ชุด

ด้วยสถานการณ์ด้านภัยคุกคามไซเบอร์ได้ขยายขอบเขตและสร้างความเสียหายให้แก่เศรษฐกิจและสังคมที่รุนแรงขึ้น จึงจำเป็นอย่างยิ่งที่จะต้องยกระดับการดูแลความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานสำคัญของรัฐอย่างเร่งด่วนและมีประสิทธิภาพ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพธอ. จึงได้ดำเนินโครงการระบบตรวจจับและวิเคราะห์การโจมตีผ่านเครือข่าย (Government Monitoring System หรือ GMS) (สิ่งที่ส่งมาด้วย ๑.)

ในการนี้ สพธอ. เห็นว่าโครงการดังกล่าว จะเป็นประโยชน์อย่างยิ่งต่อหน่วยงานของท่าน ในด้านการยกระดับมาตรการเฝ้าระวัง ติดตาม และป้องกันภัยคุกคามไซเบอร์ ตลอดจนการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์อย่างมีระบบและยั่งยืน สามารถรับมือกับภัยคุกคามไซเบอร์ ในรูปแบบการโจมตีแบบใหม่อยู่เสมอได้ จึงขอเรียนเชิญหน่วยงานของท่านเข้าร่วมโครงการดังกล่าว หรือหากหน่วยงานของท่านได้เข้าร่วมโครงการดังกล่าวอยู่แล้ว สพธอ. ขอเข้าปรับปรุงอุปกรณ์เดิมที่มีอยู่ โดยขอความร่วมมือหน่วยงานให้กรอกรายละเอียดแบบตอบรับ (สิ่งที่ส่งมาด้วย ๒.) และกรอกข้อมูลหน่วยงานเพิ่มเติมได้ที่ https://forms.gle/fQG52pv2wKuNEdf56

ทั้งนี้ การเข้าร่วมโครงการดังล่าวไม่เสียค่าใช้จ่ายใด ๆ ทั้งสิ้น หากหน่วยงานต้องการสอบถามข้อมูลเพิ่มเติมสามารถติดต่อได้ที่หมายเลขโทรศัพท์ ๐ ๒๑๒๓ ๑๒๑๒ หรือที่ไปรษณีย์อิเล็กทรอนิกส์ : gtm@etda.or.th

จึงเรียนมาเพื่อโปรดพิจารณาให้ความร่วมมือในโครงการนี้ด้วย จะขอบพระคุณยิ่ง

ขอแสดงความนับถือ

(นายมีธรรม ณ ระนอง)
รองผู้อำนวยการ ปฏิบัติการแทน
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์ระบบโครงสร้างพื้นฐานด้านสารสนเทศและความมั่นคงปลอดภัย
โทร. ๐ ๒๑๒๓ ๑๒๑๒
อีเมล: gtm@etda.or.th

แบบตอบรับ
โครงการ Government Monitoring System (GMS)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

หน่วยงาน .....

เว็บไซต์ .....

1. **กรณีที่หน่วยงานของท่านยังไม่เคยเข้าร่วมโครงการ GMS**

☐ สนใจเข้าร่วมโครงการ GMS

☐ ไม่สามารถเข้าร่วมโครงการ GMS ได้

เนื่องจาก

.....

.....

ข้อเสนอแนะ

.....

.....

2. **กรณีที่หน่วยงานของท่านเข้าร่วมโครงการ GMS อยู่แล้ว**

☐ อนุเคราะห์ให้ สพธอ. เข้าปรับปรุงอุปกรณ์ภายใต้โครงการ GMS

☐ ไม่สามารถให้ความอนุเคราะห์ สพธอ. ในการเข้าปรับปรุงอุปกรณ์ภายใต้โครงการ GMS

เนื่องจาก

.....

.....

ข้อเสนอแนะ

.....

.....

ผู้มีอำนาจลงนาม

.....

( )

ตำแหน่ง .....

วันที่.....

หมายเหตุ

๑. ขอสงวนสิทธิการพิจารณาการเข้าร่วมโครงการ Government Threat Monitoring (GTM) ให้กับหน่วยงานที่มีความพร้อมในการติดตั้งอุปกรณ์ก่อน ซึ่งหน่วยงานยังสามารถเข้าร่วมโครงการ Government Website Protection (GWP) ได้

๒. ในการเข้าปรับปรุงอุปกรณ์ครั้งนี้ สพธอ. สามารถเปลี่ยนแปลงอุปกรณ์ที่ติดตั้งอยู่เดิม และสามารถเรียกคืนอุปกรณ์เดิมภายใต้โครงการ GMS ได้

๓. ผู้มีอำนาจลงนาม คือ ผู้ที่มีสิทธิ์ในการตัดสินใจและอนุมัติการดำเนินการที่เกี่ยวข้องกับโครงการฯ ได้ เช่น ผู้จัดการฝ่าย, หัวหน้าฝ่าย, ผู้อำนวยการฝ่าย

๔. หากมีปัญหาหรือข้อสงสัยใดสามารถสอบถามข้อมูลเพิ่มเติมได้ที่หมายเลขโทรศัพท์ ๐-๒๑๒๓-๑๒๑๒ อีเมล : gtm@etda.or.th

เอกสารรายละเอียดและแผนการดำเนินงานโครงการ

Government Monitoring System (GMS)

โดย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

สารบัญ

ความเป็นมาของโครงการ GMS

ปัจจุบันนี้ มีการนำระบบเทคโนโลยีสารสนเทศมาใช้กับระบบงานหรือการให้บริการต่าง ๆ ที่สำคัญในหน่วยงานของรัฐอย่างแพร่หลาย ซึ่งภายในระบบนั้น ๆ ยังมีข้อมูลรายละเอียดที่สำคัญและเป็นความลับจัดเก็บอยู่ด้วย ซึ่งอาจมีความเสี่ยงที่ผู้ไม่ประสงค์ดีต้องการโจมตี โดยอาจก่อให้เกิดเหตุขัดข้องกับระบบ การเปลี่ยนแปลงข้อมูลในระบบงาน รวมไปจนถึงจารกรรมข้อมูลสำคัญของระบบหรือของผู้ใช้งาน ซึ่งอาจก่อให้เกิดความเสียหายที่รุนแรงและอาจประเมินเป็นมูลค่าตัวเงินไม่ได้ ทั้งนี้การป้องกันเหตุการณ์เหล่านี้จำเป็นจะต้องได้รับความร่วมมือจากทุกภาคส่วน ไม่ว่าจะเป็นเจ้าของระบบงานนั้น ๆ ไปจนถึงผู้ให้บริการอินเทอร์เน็ต ในการให้ความร่วมมือเพื่อป้องกันเหตุการณ์การโจมตีที่อาจจะเกิดขึ้นรวมถึงตรวจสอบเมื่อมีเหตุการณ์ภัยคุกคามเกิดขึ้น และด้วยในปัจจุบันนี้บุคลากรทางด้านเทคโนโลยีสารสนเทศนั้นมีอยู่อย่างจำกัดหรืออาจจะมีความรู้ ความเข้าใจทางด้านความมั่นคงปลอดภัยสารสนเทศไม่เท่าเทียมกัน จึงจำเป็นที่จะต้องมีหน่วยงานกลางเพื่อประสานงาน ให้ความรู้ และช่วยสร้างเสริมให้กับบุคคลกรด้านเทคโนโลยีสารสนเทศไปจนถึงการแนะนำภาพรวมระบบของหน่วยงานของรัฐต่าง ๆ ให้มีความมั่นคงปลอดภัยสารสนเทศที่เพิ่มมากขึ้น โดยอ้างอิงตามมาตรฐานสากลเพื่อที่จะสามารถรับมือกับภัยคุกคามได้อย่างเหมาะสม และสร้างความน่าเชื่อและปลอดภัยให้กับระบบสารสนเทศของหน่วยงานของรัฐให้ยั่งยืนต่อไป

โดย สพธอ. ได้จัดเตรียมโครงการสำหรับดูแลหน่วยงานของรัฐ ภายใต้ชื่อ "Government Monitoring System (GMS)" ประกอบด้วย 2 โครงการย่อย คือ โครงการ Government Threat Monitoring System (GTM) สำหรับเฝ้าระวังและวิเคราะห์ภัยคุกคาม และโครงการ Government Website Protection System (GWP) สำหรับป้องกันการโจมตีเว็บไซต์ของหน่วยงานของรัฐ โดยมีแนวทางในการให้ความช่วยเหลือหน่วยงานของรัฐในการรับมือปัญหาภัยคุกคามทางไซเบอร์ รวมถึงการป้องกันการโจมตีของเว็บไซต์ของหน่วยงานทั้งในลักษณะที่เป็นการโจมตีเว็บแอปพลิเคชัน (Web hacking) หรือเป็นการโจมตีในลักษณะทำให้สูญเสียสภาพความพร้อมใช้งาน (Distributed Denial of Service) ตลอดจนเครื่องมือในการตรวจจับภัยคุกคามและการโจมตีบนเครื่องลูกข่ายในลักษณะ Incident response ซึ่งจะช่วยยกระดับให้หน่วยงานมีขีดความสามารถในการเฝ้าระวัง รับมือและจัดการภัยคุกคามทางเทคโนโลยีสารสนเทศที่เกิดขึ้นได้อย่างเหมาะสม ทันท่วงที สร้างความน่าเชื่อถือให้กับระบบสารสนเทศของหน่วยงานภาครัฐ

วัตถุประสงค์ของโครงการ GMS

1. เพื่อให้หน่วยงานของรัฐมีเครื่องมือในการตรวจจับ และวิเคราะห์ภัยคุกคามทางไซเบอร์ รวมถึงยกระดับขีดความสามารถในการป้องกันการโจมตีให้กับระบบและเว็บไซต์ของหน่วยงานของรัฐ

2. เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานของรัฐอย่างมีระบบและยั่งยืน โดยมีการจัดเตรียมทีมงานเฝ้าระวังเหตุการโจมตีทางไซเบอร์ในลักษณะเป็นศูนย์ CSOC (Cybersecurity Operation Center) มีการติดตามเหตุการณ์ภัยคุกคามไซเบอร์จากทั่วโลก และภัยคุกคามที่เกิดกับหน่วยงานที่สำคัญในประเทศไทย รวมถึงมีการให้คำปรึกษาในการแก้ไขปัญหาเหตุภัยคุกคามและเรื่องต่าง ๆ ที่เกี่ยวข้องผ่านรูปแบบโทรศัพท์และอีเมล ตลอด 24 ชั่วโมง

3. เพื่อนำข้อมูลภัยคุกคามที่ตรวจพบมาวิเคราะห์ และนำมาซึ่งข้อมูลสถิติทางด้านความมั่นคงปลอดภัยไซเบอร์หน่วยงานของรัฐสำหรับการคาดการณ์สถานการณ์ ด้านความมั่นคงปลอดภัยไซเบอร์ และให้หน่วยงานของรัฐต่างๆ สามารถนำไปใช้เป็นข้อมูลเพื่อวางแผนบริหารจัดการระบบต่างๆ อย่างมีประสิทธิภาพ

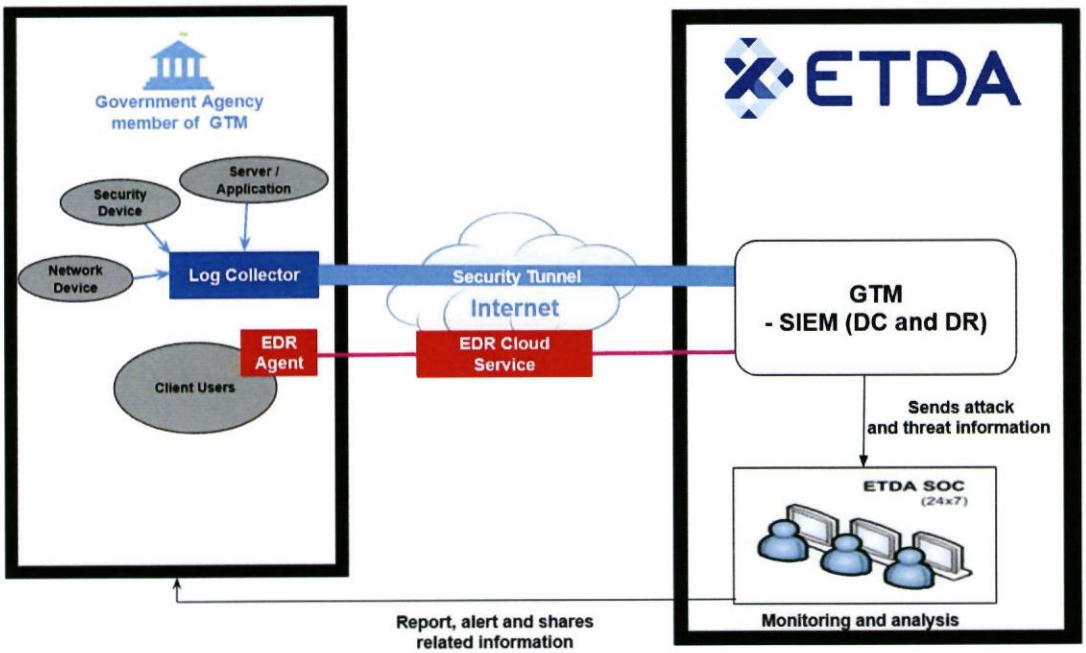
4. เพื่อให้หน่วยงานของรัฐมีความพร้อมในการรับมือกับภัยคุกคามไซเบอร์ ในรูปแบบการโจมตีแบบใหม่อยู่เสมอ รวมถึงมีระบบที่สามารถแจ้งเตือนและป้องกันการโจมตีทางไซเบอร์ได้

โครงการ GMS (Government Monitoring System)

โครงการ GMS เป็นโครงการที่จัดทำขึ้นเพื่อให้หน่วยงานของรัฐมีความพร้อมในเรื่องการรับมือและการตอบสนองต่อการโจมตีในโลกไซเบอร์ ประกอบด้วย 2 โครงการย่อย คือ โครงการ Government Threat Monitoring System (GTM) และโครงการ Government Website Protection System (GWP) โดยมีรายละเอียดดังนี้

1.) โครงการ Government Threat Monitoring System (GTM)

ดำเนินการนำข้อมูล Log จากระบบต่างๆ เช่น Firewall log IDS log หรือ Web log มาวิเคราะห์เพื่อหาความสัมพันธ์ของเหตุการณ์ (Log Correlation)



รูปที่ 1 แผนภาพแสดงการเชื่อมต่อระบบโครงการ GTM

โครงการ Government Threat Monitoring System (GTM) มีองค์ประกอบและคุณลักษณะเฉพาะที่ช่วยเฝ้าระวังการโจมตีทางไซเบอร์ มีการเก็บข้อมูล Log ของระบบต่าง ๆ มาใช้เพื่อวิเคราะห์ยังศูนย์กลาง (HQ) โดยมีการทำงานของแต่ละอุปกรณ์แยกกัน ดังนี้

1.1. อุปกรณ์ Log Collection Server สำหรับระบบตรวจจับและวิเคราะห์การโจมตีบนเครือข่ายสำหรับติดตั้งที่หน่วยงาน ควรติดตั้งอยู่ใน DMZ Zone สาเหตุเพื่อให้เกิดความสะดวกในการรับส่งข้อมูล Log จากเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายที่เปิดให้เข้าถึงได้จากภายนอก (Public Facing System/Server) ซึ่งทำให้ไม่จำเป็นต้องส่งข้อมูล Log ข้าม Security Zone ในขณะที่อีก Network Interface ของอุปกรณ์ Log Collector Server จะเชื่อมต่อเข้าสู่อุปกรณ์ Switch เพื่อส่งข้อมูลที่วิเคราะห์ได้ ผ่าน Secure Tunnel กลับไปยังส่วนกลาง เพื่อทำการบันทึกข้อมูลลงบน Storage ของศูนย์ปฏิบัติการ SOC ทั้งนี้ผู้เชี่ยวชาญจะทำการเฝ้าระวังภัยคุกคามทางด้านเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Security Operations Center (SOC) ซึ่งมีการทำงานตลอด 24 ชั่วโมง ตลอดระยะเวลาการให้บริการ

1.2. EDR (Endpoint Detection and Response) Agent เป็นระบบตรวจจับภัยคุกคามและการโจมตีบนเครื่องลูกข่ายในลักษณะ Incident response จะติดตั้งที่เครื่อง Client ภายในหน่วยงาน เพื่อวิเคราะห์พฤติกรรมที่น่าสงสัยจากเครื่องลูกข่าย แล้วส่งข้อมูลไปทำการวิเคราะห์ที่ระบบ Cloud หลังจากวิเคราะห์แล้วจะส่งข้อมูลไปศูนย์ปฏิบัติการ SOC เพื่อให้ผู้เชี่ยวชาญจะทำการเฝ้าระวังภัยคุกคามทางด้านเทคโนโลยีสารสนเทศผ่านศูนย์ปฏิบัติการ Security Operations Center (SOC) ซึ่งมีการทำงานตลอด 24 ชั่วโมง ตลอดระยะเวลาการให้บริการ

ตารางที่ 1 แสดงตัวอย่างเหตุการณ์ภัยคุกคามที่ตรวจสอบได้ตามโครงการ GTM

ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด	ชนิดของอุปกรณ์/ระบบที่นำมาใช้วิเคราะห์	ประเภทของ Log ที่ใช้วิเคราะห์
User Authentication Rules and Alerts			
Repeat Attack-Login Source	เกิดเหตุการณ์ที่กรอกรหัสผ่านไม่สำเร็จจาก IP Address เดียวกัน เกินจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด	• Operating System	• Authentication Logs
		• Authentication server	• Authentication Logs
		• Application Log*	• Authentication Logs
Repeat Attack-Login Target	เกิดเหตุการณ์ที่กรอกรหัสผ่านไม่สำเร็จโดยใช้ Username เดียวกัน เกินจำนวน/ครั้ง ภายในช่วงเวลาที่กำหนด	• Operating System	• Authentication Logs
		• Authentication server	• Authentication Logs
		• Application Log *	• Authentication Logs
Attacks Detected on the Network			
Repeat Attack-Firewall	เกิดเหตุการณ์ที่ connection ถูก Drop/Reject/Deny จาก IP Address เดียวกัน เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall	• Drop/Reject/Deny Logs
		• Router, Switch Layer 3 *	• Drop/Reject/Deny Logs
Repeat Attack-Network Intrusion Prevention System	เกิดเหตุการณ์การแจ้งเตือนจากระบบ IPS หรือ IDS ว่ามีการพยายามบุกรุกเข้าสู่เครือข่ายภายในเกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall, Router, Switch Layer 3 *	• Allow Logs
		• Network IDS/IPS	• Detected Intrusion Logs
Denial of Service Attempt	เกิดเหตุการณ์ที่มีปริมาณ Connection ที่ติดต่อเข้าสู่เครื่องแม่ข่ายจำนวนมากกว่าปกติ หรือเกิดเหตุการณ์การแจ้งเตือนจากระบบ DDoS	• Firewall, Router, Switch Layer 3 *	• Allow Logs
		• Network IDS/IPS	• Detected DoS/DDoS Logs

ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด	ชนิดของอุปกรณ์/ระบบที่นำมาใช้วิเคราะห์	ประเภทของ Log ที่ใช้วิเคราะห์
		• DDoS Protection System	• Detected DoS/DDoS Logs
		• Web Server	• Web Access Logs
Attacks and Infections Detected at the Host Level			
Repeat Attack-Host Intrusion Prevention System	เกิดเหตุการณ์การแจ้งเตือนจากระบบ Host IPS หรือ IDS ว่ามีเครื่องภายในเครือข่ายอาจจะเป็นผู้บุกรุก เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall, Router, Switch Layer 3 *	• Allow Logs • Drop/Reject/Deny Logs
		• Host IDS/IPS	• Detected Intrusion Logs
Virus or Spyware Detected	เกิดเหตุการณ์การแจ้งเตือนจากโปรแกรม Anti-Virus หรือ Anti-Spyware ว่ามีการแพร่กระจาย Malware ภายในเครือข่าย	• Antivirus Server	• Malware Detected Logs
		• Host IDS/IPS, Network IDS/IPS *	• Detected Intrusion Logs
Attacks from Unknown/Untrusted Sources			
Repeat Attack-Foreign	เกิดเหตุการณ์การพยายามบุกรุก เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall	• Drop/Reject/Deny Logs • Allow Logs
		• Router, Switch Layer 3 *	• Drop/Reject/Deny Logs
		• Host IDS/IPS, Network IDS/IPS	• Detected Intrusion Logs
Known Attacker Allowed in Network	เกิดเหตุการณ์การตรวจพบ packet ของเครือข่ายภายนอกที่มี Source IP address ที่ถูกขึ้นบัญชี (Black List)	• Firewall	• Allow Logs
		• Router, Switch Layer 3 *	• Allow Logs
		• Host IDS/IPS, Network IDS/IPS	• Detected Intrusion Logs
		• SIEM Threats Intelligence	• IP Black List DB

ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด	ชนิดของอุปกรณ์/ระบบที่นำมาใช้วิเคราะห์	ประเภทของ Log ที่ใช้วิเคราะห์
Traffic to Known Attacker	เกิดเหตุการณ์ตรวจพบ packet จากภายในเครือข่าย ไปยังเครือข่ายภายนอกที่มี Destination IP Address ที่ถูกขึ้นบัญชี (Black List) เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall	• Drop/Reject/Deny Logs • Allow Logs
		• Router, Switch Layer 3 *	• Drop/Reject/Deny Logs
		• Host IDS/IPS, Network IDS/IPS	• Detected Intrusion Logs
		• SIEM Threats Intelligence	• IP Black List DB
High Threat Targeting Vulnerable Asset	เกิดเหตุการณ์พยายามโจมตีเข้าสู่ระบบที่มีความเสี่ยงสูง จากการแจ้งเตือนของ Network IPS หรือ IDS เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Network IPS/IDS	• Intrusion Detected Logs
Repeat Attack-Multiple Detection Sources	เกิดเหตุการณ์มีการแจ้งเตือนจากหลายระบบ ว่ามีการพยายามบุกรุกจาก Source IP Address เดียวกัน เกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall	• Drop/Reject/Deny Logs • Allow Logs
		• Router, Switch Layer 3 *	• Drop/Reject/Deny Logs
		• Host IDS/IPS, Network IDS/IPS	• Detected Intrusion Logs
		• Antivirus Server	• Malware Detected Logs
		• Operating System	• Authentication Logs
		• Authentication Server	• Authentication Logs
		• Application Log *	• Authentication Logs
Possible Outbreak Excessive Connections	เกิดเหตุการณ์ที่เครื่องลูกข่ายมีการเชื่อมต่อกับเครื่องอื่นๆ มากกว่าเหตุการณ์ที่กำหนดไว้	• Firewall	• ALLOW Logs • DENY Logs
		• Network IPS/IDS	• Intrusion Detected Logs

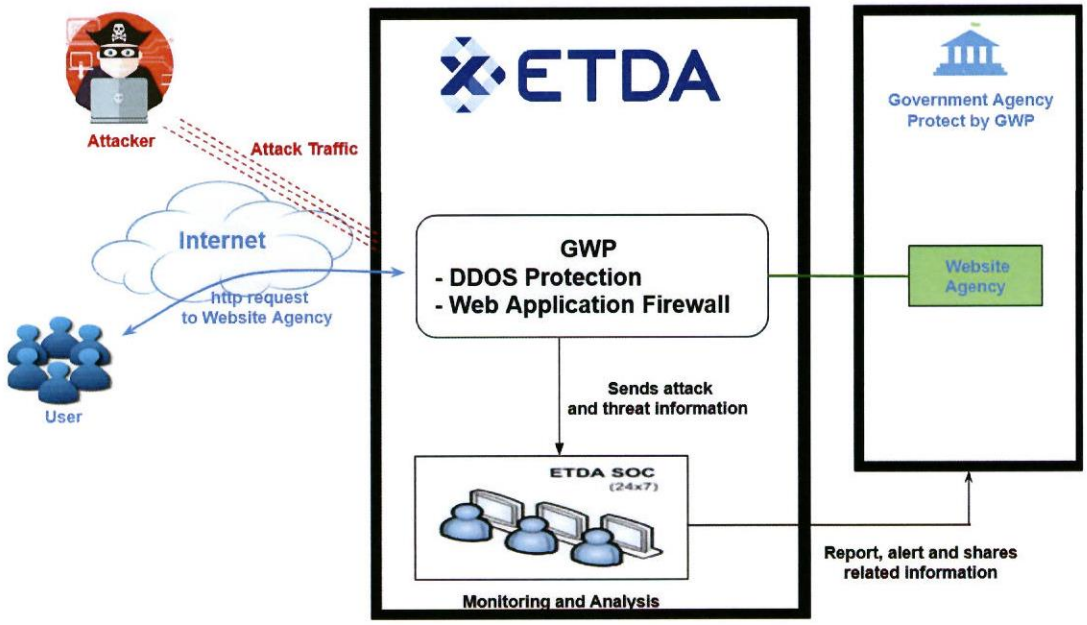
ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด	ชนิดของอุปกรณ์/ระบบที่นำมาใช้วิเคราะห์	ประเภทของ Log ที่ใช้วิเคราะห์
Possible Outbreak Multiple Infected Hosts Detected on the Same Subnet	เกิดเหตุการณ์การแจ้งเตือนว่ามีการแพร่กระจาย Malware ภายในเครือข่ายเกินจำนวน/ครั้งภายในช่วงเวลาที่กำหนด	• Firewall	• ALLOW Logs • Deny Logs
		• Antivirus	• Malware Detected Logs
Web Server (IIS, Apache) Attack			
Suspicious Post from Untrusted Source	เกิดเหตุการณ์ที่มีการอัพโหลด Executable code ขึ้นไปบน Web server	• Network IPS/IDS	• Intrusion Detected Logs
		• Web Server	• Web Access Logs
Attack-Web Application Firewall	เกิดเหตุการณ์การแจ้งเตือนจากระบบ WAF ว่ามีการพยายามบุกรุกเข้าสู่ Web Application	• Firewall, Router, Switch Layer 3 *	• Allow Logs
		• Web Application Firewall	• Detected Attack Log
		• Network IPS/IDS	• Intrusion Detected Logs
Availability Monitoring			
Monitored Log Source Stopped Sending Events	เกิดเหตุการณ์ที่อุปกรณ์ Log Source หยุดการส่ง Log เกินกว่าช่วงเวลาที่กำหนด	• SIEM	• "NO LOGS RECEIVED" Logs

หมายเหตุ

1. ตัวอย่าง Authentication server ได้แก่ LDAP Server, RADIUS Server, TACACS, Active Directory เป็นต้น
2. ชนิดอุปกรณ์/ระบบที่มีสัญลักษณ์ * หมายถึง ข้อมูลดังกล่าวใช้เป็นส่วนเสริมในการวิเคราะห์เหตุการณ์ภัยคุกคาม

2.) โครงการ Government Website Protection System (GWP)

สำหรับป้องกันการโจมตีเว็บไซต์ โดยมีการป้องกันการโจมตีเว็บไซต์ด้วยเทคนิคพื้นฐาน เช่น การโจมตีด้วยเทคนิค SQLi (SQL injection) หรือ XSS (Cross Site Scripting) เป็นต้น รวมถึงการป้องกันการโจมตีด้วยเทคนิคขั้นสูงอย่าง DDoS (Distributed Denial of Service)



รูปที่ 2 แผนภาพแสดงการเชื่อมต่อระบบโครงการ GWP

โครงการ Government Website Protection System (GWP) มีองค์ประกอบและคุณลักษณะเฉพาะในทางที่ช่วยเฝ้าระวังการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับเว็บไซต์ โดยมีการตรวจจับการโจมตีทางเว็บไซต์และการป้องกันการโจมตี พร้อมกับการแจ้งเตือนและส่งข้อมูลการโจมตีเพื่อมาวิเคราะห์ยังศูนย์กลาง (HQ) โดยมีการทำงานของแต่ละระบบแยกกัน ดังนี้

2.1. ระบบป้องกันการโจมตีเว็บไซต์และการโจมตีในลักษณะ DDoS มีคุณลักษณะเฉพาะในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับการโจมตีในลักษณะ DDoS มีขีดความสามารถในการป้องกันการโจมตีให้กับเว็บไซต์ของหน่วยงาน รวมถึงสามารถป้องกันการโจมตีแบบ DDoS ขนาดใหญ่ด้วย Cloud service ที่ให้บริการคัดกรองข้อมูลส่วนที่เป็นการโจมตีออก ก่อนที่จะส่งเฉพาะข้อมูลที่เป็นการใช้งานจริงไปยังระบบของหน่วยงาน

2.2. ระบบป้องกันการโจมตีเว็บไซต์ด้วย Web Application Firewall (WAF) มีคุณลักษณะเฉพาะในการตรวจจับและวิเคราะห์ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ มีขีดความสามารถในการป้องกันการโจมตีเว็บแอปพลิเคชัน ดังมีรายการตัวอย่างตามข้อมูลด้านล่าง รวมถึงในขั้นตอนการดำเนินงานจะมีการจัดทำรายงานการตรวจสอบช่องโหว่ของเว็บไซต์ที่เข้าร่วมโครงการ พร้อมข้อแนะนำในการแก้ไขให้และป้องกันเพื่อให้เกิดความมั่นคงปลอดภัยกับเว็บไซต์ของหน่วยงาน

ตารางที่ 2 แสดงตัวอย่างเหตุการณ์ภัยคุกคามที่ตรวจสอบได้ตามโครงการ GWP

ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด
Abuse of Functionality	ช่องโหว่ที่เกิดจากการใช้งาน Function ของระบบเว็บไซต์มีการทำงานผิดปกติ เช่น การใช้ในการหลบเลี่ยงการตรวจสอบการเข้าถึงสิทธิ์ของผู้ใช้ หรือการตรวจสอบการทำงานต่าง ๆ เป็นต้น
Injection	ช่องโหว่ที่เกิดจากการที่ระบบไม่มีการป้องกัน การตรวจค่าที่รับจากผู้ใช้ ก่อนนำไปประมวลผล ส่งผลให้ผู้ไม่ประสงค์ดีสามารถส่งคำสั่งอันตรายไปยังระบบเว็บไซต์ได้ เช่น การโจมตีในรูปแบบ SQL injection คือการที่ผู้ไม่ประสงค์ดีโจมตีผ่านช่องทางการติดต่อกับฐานข้อมูล ทำให้สามารถส่งคำสั่ง SQL อันตรายไปประมวลผลกับ Database ได้โดยตรง ส่งผลให้ผู้ไม่ประสงค์ดีมองเห็นข้อมูลภายใน Database และเข้าเปลี่ยนแปลงข้อมูลภายใน Database รวมถึงส่งคำสั่งในการควบคุมระบบปฏิบัติการ เช่น สั่งให้สร้างบัญชีผู้ใช้งานบนวินโดวส์ เป็นต้น
Brute Force Attack	เป็นวิธีการโจมตีด้วยการพยายามสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้นหรือเลือกใช้เพื่อให้ได้มายังซึ่งข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น บัญชีผู้ใช้งาน (username) รหัสผ่าน (password) สำหรับเข้าสู่ระบบ หรือในบางครั้งผู้โจมตีอาจใช้เพื่อสแกนหาไฟล์สำคัญของเว็บไซต์ ซึ่งการโจมตีในลักษณะนี้จะได้ผลกับการตั้งค่าที่คาดเดาง่ายหรือเป็นค่าตั้งต้นของระบบ เช่น การตั้งบัญชีผู้ใช้งานและรหัสผ่านที่ง่ายต่อการคาดเดา โดยแนวทางการป้องกันการโจมตีอาจทำได้โดยการใช้งานโมดูล Captcha บนเว็บไซต์ ซึ่งเป็นเทคนิคที่ช่วยยืนยันว่าการส่งข้อมูลเข้ามายังระบบดังกล่าวเป็นผู้ใช้งานที่เป็นมนุษย์จริง ไม่ใช่โปรแกรมคอมพิวเตอร์ หรือการใช้งานโปรแกรมประเภท Anti Bruth Force บนระบบปฏิบัติการ
Buffer Overflow	เป็นความผิดพลาดของโปรแกรมเมื่อข้อมูลที่โปรแกรมรับเข้าขนาดใหญ่เกินกว่าขนาดของ Buffer (พื้นที่ที่จองไว้สำหรับเก็บข้อมูลชั่วคราว) ที่จองเอาไว้ เมื่อข้อมูลถูกส่งเข้ามามากเกินกว่าที่จะรับได้ ข้อมูลส่วนที่เกิน จะล้น (Overflow) ออกไปนอกพื้นที่ที่กำหนดไว้ซึ่งอาจจะไปทับข้อมูลที่เป็นส่วนสำคัญของโปรแกรม เช่น ชุดคำสั่งของโปรแกรมใช้ในการทำงาน เป็นต้น ส่งผลให้ผู้ไม่ประสงค์ดีสามารถเรียกใช้คำสั่งอันตรายได้
Broken Authentication and Session Management	ช่องโหว่ที่เกิดจากระบบ ไม่มีการตรวจสอบการเข้าถึงหรือไม่มีการตรวจสอบ Session ของบัญชีผู้ใช้อย่างเหมาะสม ส่งผลให้ผู้ไม่ประสงค์ดีสามารถปลอมแปลงเป็นบัญชีผู้ใช้อื่น ๆ ได้ โดยการเปลี่ยนค่า keys, session tokens หรือโจมตีกระบวนการตรวจสอบบัญชีผู้ใช้ของระบบได้ เป็นต้น
Cross-Site Scripting (XSS)	ช่องโหว่ Cross Site Scripting หมายถึง ช่องโหว่ที่อนุญาตให้ผู้ไม่ประสงค์ดีโจมตีระบบในลักษณะที่มีการป้อนค่าสคริปต์อันตรายเข้าสู่ระบบ เพื่อให้เกิดการแสดงผลต่อผู้ใช้งานคนอื่นๆ ส่วนใหญ่ผู้ไม่ประสงค์ดีมักจะป้อนค่าสคริปต์อันตรายประเภท JavaScript, VBScript, ActiveX, HTML หรือ Flash ทำให้ภายหลังจากผู้ใช้งานเปิดหน้าแสดงผลดังกล่าวแล้ว จะเริ่มประมวลผลสคริปต์อันตรายที่ผู้ไม่ประสงค์ดีใส่ไว้ในทันที ส่งผลให้อาจถูกขโมยข้อมูลการล็อกอิน หรือสั่งโจมตีเครื่องคอมพิวเตอร์อื่นๆโดยผู้ใช้งานไม่รู้ตัว

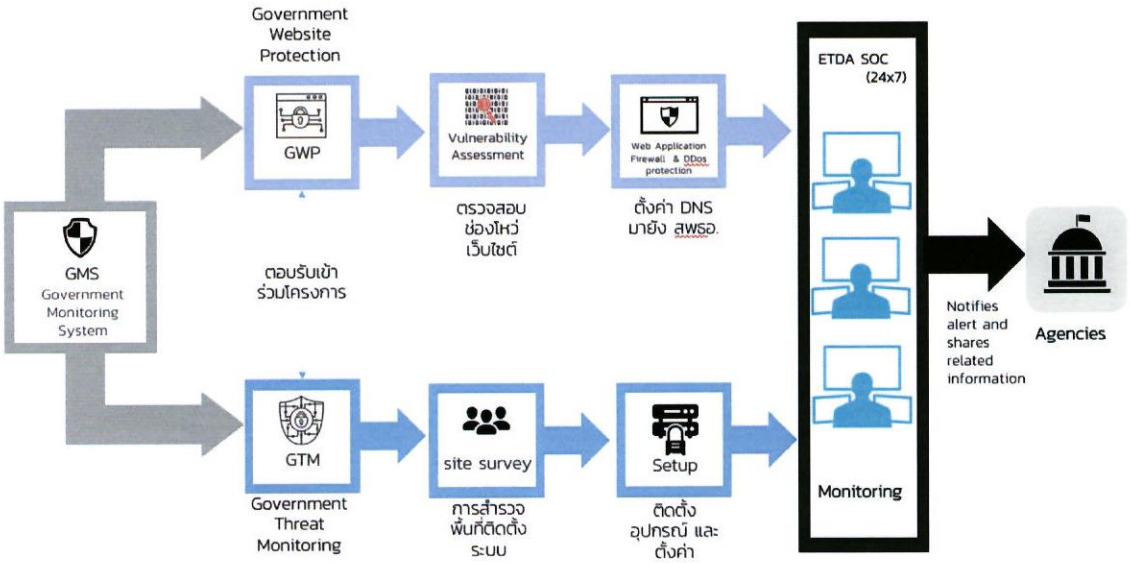
ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด
Cross-Site Request Forgery (CSRF)	CSRF หรือ Cross Site Request Forgery เป็นเทคนิคการโจมตีรูปแบบหนึ่งโดยมีจุดประสงค์ในการสั่งให้ผู้ใช้งานประมวลผลสคริปต์หรือสั่งรัน URL อันตราย เพื่อให้ผู้ใช้งานทำการส่งค่าในแบบฟอร์มที่เฉพาะเจาะจง เช่น แบบฟอร์มโพสต์ข้อมูลในเว็บบอร์ด แบบฟอร์มโอนเงินในเว็บไซต์ E-Banking โดยอาศัยการหลอกให้ผู้ใช้งานที่กำลังล็อกอินระบบเป้าหมายอยู่นั้น ทำการประมวลผลสคริปต์อันตรายหรือลิงก์ดังกล่าว ส่งผลให้ผู้ใช้งานสั่งประมวลผลฟังก์ชันการทำงานบางอย่างโดยไม่รู้ตัว
Detection Evasion	การโจมตีในลักษณะที่มีการหลบหลีกหรือซ่อนตัวจากระบบตรวจจับ จากรูปแบบต่าง ๆ (Attack signature)
Directory Indexing	ช่องโหว่ที่เกิดจากการตั้งค่า ระบบ เพื่อเปิดให้บุคคลทั่วไปสามารถเข้าถึงข้อมูลรายการไฟล์ทั้งหมดใน Directory หนึ่ง ๆ ได้ ส่วนใหญ่เป็นการตั้งค่าโดย Default ของเว็บเซิร์ฟเวอร์ ซึ่งการเปิดให้เข้าถึงข้อมูลดังกล่าวอาจมีความเสี่ยงต่อการที่ผู้ไม่ประสงค์ดีจะใช้เป็นช่องทางสำหรับรวบรวมข้อมูลต่าง ๆ สำหรับโจมตีระบบต่อไป
Malicious File Upload	การโจมตีที่ผู้ไม่ประสงค์ดีสามารถอัพโหลดไฟล์อันตรายขึ้นไปยังระบบเว็บไซต์ได้ โดยไฟล์ดังกล่าวสามารถส่งผลให้สามารถควบคุม หรือเข้าถึงข้อมูลสำคัญของเครื่องได้
Parameter Tampering	เว็บไซต์มีช่องที่ผู้ไม่ประสงค์ดีสามารถโจมตีผ่าน Parameter ด้วยวิธีการเปลี่ยนค่าที่ใช้รับ-ส่ง ไปกับ Parameter ระหว่าง Client – Server ส่งผลให้ผู้ไม่ประสงค์ดีอาจสามารถฝัง code อันตรายหรือ สามารถปรับเปลี่ยนการทำงานของโปรแกรมได้
Path Traversal	ช่องโหว่ที่ผู้ไม่ประสงค์ดีสามารถเข้าถึงไฟล์ใดๆ ในเครื่องแม่ข่ายได้ ซึ่งรวมถึงไฟล์ที่ไม่ได้อยู่ภายใต้ Root ไดเรกทอรีของเว็บไซต์
Sensitive Data Exposure	ช่องโหว่ที่มีการเปิดให้สามารถเข้าถึงข้อมูลที่สำคัญของระบบ เช่น ข้อมูลการตั้งค่าระบบหรือ ข้อมูลไฟล์ต่างๆ ที่อยู่บนเว็บไซต์ เป็นต้น
Denial of Service Attempt	เกิดเหตุการณ์ที่มีปริมาณ Connection ที่ติดต่อเข้าสู่เครื่องแม่ข่ายจำนวนมากกว่าปกติ หรือเกิดเหตุการณ์การแจ้งเตือนจากระบบ DDoS
Flood attack	การส่งข้อมูลไปยังระบบปลายทางพร้อมกันเป็นจำนวนมาก ส่งผลให้ประสิทธิภาพในการให้บริการของระบบลดลง จนกระทั่งระบบไม่สามารถให้บริการได้ตามปกติ โดยทั่วไปมักเป็นการโจมตีด้วยการส่งข้อมูลผ่านโพรโทคอล TCP, UDP และ ICMP ตัวอย่างเช่น TCP SYN flood ที่เป็นการส่งข้อมูลร้องขอการเชื่อมต่อ (SYN) ไปยังปลายทางเป็นจำนวนมาก โดยไม่ตอบกลับ (ACK) ไปยังปลายทางเพื่อสร้างการเชื่อมต่อให้ครบตามกระบวนการ TCP 3-way handshake
Fragmentation attack	การส่งข้อมูลที่ถูกแบ่งออกเป็นส่วนเล็ก ๆ (Fragment) ในลักษณะที่ผิดปกติไปยังระบบปลายทาง เช่น แต่ละ Fragment มีส่วนที่ทับซ้อนกัน หรือส่ง Fragment ของแพ็กเกจไปเพียงบางส่วน ส่งผลให้ประสิทธิภาพในการให้บริการของระบบลดลง หรือเกิดปัญหาระหว่างการประมวลผลข้อมูล จนกระทั่งระบบไม่สามารถให้บริการได้ตามปกติ ตัวอย่างเช่น Teardrop attack

ชนิดของเหตุการณ์ภัยคุกคาม	รายละเอียด
Malformed traffic attack	การส่งข้อมูลที่มีรูปแบบผิดไปจากมาตรฐานของโพรโทคอลที่กำหนดไว้ไปยังระบบปลายทาง ส่งผลให้เกิดปัญหาระหว่างการประมวลผลข้อมูล จนกระทั่งระบบไม่สามารถให้บริการได้ตามปกติ การโจมตีในลักษณะดังกล่าวมักเป็นการส่งข้อมูลผ่านโพรโทคอลในระดับ Application layer เช่น HTTP,DNS, SIP และ TLS/SSL

โดยเพื่อเป็นการเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับหน่วยงานของรัฐอย่างมีระบบและยั่งยืนทั้ง 2 โครงการที่ได้กล่าวไปนี้ ทาง สพธอ. ได้มีการจัดเตรียมบุคลากรไว้คอยเฝ้าระวังเหตุการณ์การโจมตีที่อาจเกิดขึ้นกับหน่วยงาน พร้อมทีมงานผู้เชี่ยวชาญในเรื่องการรักษาความมั่นคงปลอดภัย สำหรับช่วยในการให้คำปรึกษา และการแก้ไขปัญหาเหตุภัยคุกคาม เพื่อให้หน่วยงานมีความพร้อมและสามารถตอบสนองต่อเหตุภัยคุกคามอย่างเหมาะสม ในลักษณะบริหารจัดการจากศูนย์กลางและดำเนินงานในลักษณะ 24 x 7 ชั่วโมง

แผนการดำเนินงานโครงการ GMS โดยคร่าว

สพธอ. ได้กำหนดแผนการดำเนินงานโครงการทั้ง 2 ส่วนในภาพรวม ขั้นตอนการดำเนินงานของโครงการ GMS



รูปที่ 3 แผนภาพแสดงการเชื่อมต่อระบบโครงการ GTM

เพื่อให้เกิดความเข้าใจไปในทิศทางเดียวกัน โดยแบ่งเป็น 4 กิจกรรมหลัก (4 ระยะ) ซึ่งเป็นการดำเนินการในลักษณะของการวางแผน การติดตั้งและตั้งค่า รวมถึงการเฝ้าระวังการโจมตี โดยไม่คิดค่าใช้จ่ายกับหน่วยงานของรัฐที่เข้าร่วมโครงการ ตามรายละเอียดดังต่อไปนี้

1.) เชิญหน่วยงานเข้าร่วมโครงการ GMS

ขอบเขตของโครงการครอบคลุมการเฝ้าระวังภัยคุกคามและป้องกันการโจมตีเว็บไซต์ให้กับหน่วยงานของรัฐ และหน่วยงานที่เป็นโครงสร้างพื้นฐานที่มีความสำคัญ โดย สพธอ. ได้ดำเนินการพิจารณาคัดเลือกหน่วยงานที่มีความสำคัญในการเข้าร่วมโครงการ และเพื่อให้หน่วยงานเข้าใจวัตถุประสงค์และเป้าหมายที่ชัดเจนของโครงการ สพธอ. จึงจัดการประชุมและเชิญผู้แทน (ฝ่ายบริหารและฝ่ายเทคนิค) จากหน่วยงานที่ได้รับคัดเลือก เพื่อชี้แจงถึงรายละเอียดและแผนงานของการดำเนินโครงการ GMS

2.) เตรียมความพร้อมการติดตั้งและตั้งค่าระบบต่างๆ ที่เกี่ยวข้องในโครงการ

สพธอ. เริ่มเข้าหารือและประเมินการติดตั้งให้กับหน่วยงานที่ตอบรับเข้าร่วมโครงการ GMS โดยมีหัวข้อต่างๆ ด้านโครงสร้างระบบสารสนเทศและรายละเอียดด้านเทคนิคของหน่วยงาน เพื่อกำหนดขอบเขตการเฝ้าระวังและป้องกันภัยคุกคามของหน่วยงาน โดยมุ่งเน้นการวิเคราะห์ภัยคุกคามที่เกิดขึ้นจากภายนอกหน่วยงานและการรับมือการโจมตีในส่วนของระบบสารสนเทศของหน่วยงานที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง เช่น ระบบเว็บไซต์ของหน่วยงาน ซึ่งเป็นระบบที่ไม่ได้มีข้อมูลที่มีความสัมพันธ์โดยตรงหรือสามารถระบุถึงผู้ใช้งานของหน่วยงาน หรือสามารถระบุถึงกิจกรรมการใช้งานเครือข่ายอินเทอร์เน็ตของหน่วยงานได้ ทั้งนี้ สพธอ. จะดำเนินการภายใต้ขอบเขตที่มีการกำหนดร่วมกันเท่านั้น

3.) ติดตั้งและตั้งค่าการทำงานของระบบต่าง ๆ ที่เกี่ยวข้องในโครงการ

ดำเนินการนัดหมายกับผู้ที่ได้รับมอบหมายให้เป็นผู้ประสานงานของหน่วยงาน เพื่อเข้าติดตั้งอุปกรณ์ที่เกี่ยวข้องและตั้งค่าระบบ โดยรูปแบบการเชื่อมต่อจะมีการตกลงกันในระยะที่ 2 (เตรียมความพร้อมการติดตั้งและตั้งค่าระบบต่างๆ ที่เกี่ยวข้องในโครงการ) เพื่อให้แน่ใจว่าอุปกรณ์ที่ติดตั้งที่หน่วยงานจะทำงานภายใต้ขอบเขตที่ตกลงกัน รวมถึงนัดหมายกำหนดการในส่วนต่าง ๆ ที่เกี่ยวข้อง โดยมีรายละเอียดเบื้องต้นดังนี้

3.1. โครงการ Government Threat Monitoring System (GTM) จะดำเนินการติดตั้งอุปกรณ์วิเคราะห์ Log Collection Server และ EDR (Endpoint Detection and Response) ซึ่งการดำเนินการส่วนนี้ สพธอ. จะนำอุปกรณ์มาติดตั้งยังพื้นที่ของหน่วยงานที่จัดเตรียมไว้ให้ และทดสอบการเชื่อมต่อระหว่างอุปกรณ์วิเคราะห์ Log Collection Server ที่ติดตั้งที่หน่วยงาน กับส่วนกลาง (HQ) ที่ติดตั้งที่ สพธอ. จากนั้นจึงเริ่มตั้งค่าการเก็บข้อมูล Log เข้าสู่กระบวนการวิเคราะห์และเฝ้าระวังภัยคุกคามต่อไป

กิจกรรมที่จะดำเนินการที่หน่วยงานของรัฐ

ตารางที่ 3 แสดงกิจกรรมที่จะดำเนินการที่หน่วยงานของรัฐ

ลำดับ	กิจกรรม	ประเมินระยะเวลา
1	การสำรวจพื้นที่ติดตั้งระบบ • วัตถุประสงค์การดำเนินงาน - เพื่อทราบตำแหน่งติดตั้งอุปกรณ์และจุดเชื่อมต่อระบบเครือข่าย - เพื่อประเมินความพร้อมของพื้นที่ติดตั้งอุปกรณ์และวางแผนการปฏิบัติงานในวันติดตั้งอุปกรณ์ - เพื่อรับทราบขั้นตอน ระเบียบปฏิบัติของการเข้าปฏิบัติงานในพื้นที่ของหน่วยงาน • ความต้องการ - ผู้ประสานงานหรือผู้ควบคุมดูแลพื้นที่ติดตั้งอุปกรณ์ - ผู้ดูแลระบบเครือข่ายที่สามารถให้ข้อมูลการเชื่อมต่ออุปกรณ์ในปัจจุบัน	1 วัน
2	การติดตั้งอุปกรณ์และเชื่อมต่อสายสัญญาณ • วัตถุประสงค์การดำเนินงาน - เพื่อติดตั้งอุปกรณ์เข้าตู้ Rack เชื่อมต่อระบบไฟฟ้าและระบบเครือข่าย • รายการอุปกรณ์ที่จะติดตั้ง - Log Collector Server จำนวน 1 ชุด - EDR Agent จำนวน (ประเมินจากการสำรวจ) • ความต้องการ (บุคลากร) - ผู้ประสานงานหรือผู้ควบคุมดูแลพื้นที่ติดตั้งอุปกรณ์ - ผู้ดูแลระบบเครือข่าย	1 วัน

ลำดับ	กิจกรรม	ประเมินระยะเวลา
3	การตั้งค่า Configuration อุปกรณ์ให้ส่ง Log ไปที่ Log Collector • วัตถุประสงค์ - เพื่อปรับปรุงแก้ไข Configuration ของอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้ส่ง Traffic Log หรือ Access Log ของ Internet Facing System (DMZ) ไปยัง Log Collector Server • ความต้องการ - ผู้ดูแลระบบเครือข่ายที่ดูแลอุปกรณ์ Firewall, IPS, Web Server, Web Application Firewall หรือระบบอื่นๆ ที่เปิดให้เข้าถึงได้จากภายนอก - แก้ไข Configuration ของอุปกรณ์ให้ส่ง Log ไปยัง Log Collector Server	2 วัน
รวม		**4 วัน**

รายการอุปกรณ์/ระบบที่สนับสนุนการส่งข้อมูล Log ของโครงการ GTM ดังแสดงในภาคผนวก ก

รายการอุปกรณ์/ระบบที่สนับสนุนการติดตั้ง EDR (Endpoint Detection and Response) ของโครงการ GTM ดังแสดงในภาคผนวก ข

3.2. โครงการ Government Website Protection System (GWP) สามารถตั้งค่าการใช้งานแบบ Whitelist เพื่อใช้สำหรับการรับส่งข้อมูลร่วมกับระบบให้บริการเว็บไซต์ รวมถึงการตั้งค่า DNS record ให้เชื่อมต่อมายังระบบป้องกันที่ส่วนกลาง (HQ) ที่ติดตั้งที่ สพธอ. ซึ่งการดำเนินการในส่วนนี้ สพธอ. จะมีการนัดหมายกำหนดการเพื่อดำเนินการประเมินความเสี่ยงและตรวจสอบช่องโหว่ของเว็บไซต์ที่อยู่ภายใต้ขอบเขตของโครงการ GWP จากนั้นจึงเริ่มตั้งค่าการป้องกันที่เกี่ยวข้องต่อไป

3.2.1. กิจกรรมที่จะดำเนินการที่หน่วยงานของรัฐ

ตารางที่ 4 แสดงกิจกรรมที่จะดำเนินการที่หน่วยงานของรัฐ

ลำดับ	กิจกรรม	ประเมินระยะเวลา
1	การสแกนช่องโหว่ (Vulnerability Scanning) ให้กับระบบเว็บไซต์ • วัตถุประสงค์การดำเนินงาน - เพื่อให้ทราบถึงรายการช่องโหว่ของระบบเว็บไซต์ และจัดทำรายงานข้อแนะนำในการแก้ไขให้กับผู้ดูแลเว็บไซต์ - เพื่อนำข้อมูลช่องโหว่ที่พบ ไปปรับใช้หรือตั้งค่าเงื่อนไขในการป้องกัน (Rule) ให้กับอุปกรณ์ WAF • ความต้องการ - ผู้ประสานงานหรือผู้ควบคุมดูแลระบบเว็บไซต์ - ผู้ดูแลระบบตั้งค่า Firewall โดยอนุญาตให้ IP Address ของ สพธอ. สามารถดำเนินการได้ โดยที่ไม่มีการตรวจสอบการโจมตี	7 วัน

ลำดับ	กิจกรรม	ประเมินระยะเวลา
2	การตั้งค่า Firewall ในลักษณะ Whitelist เพื่อเชื่อมต่อระหว่างหน่วยงานกับ สพธอ. กรณีที่ระบบเว็บไซต์ของหน่วยงานมีระบบป้องกันการโจมตี • วัตถุประสงค์ - เพื่อปรับปรุงแก้ไข Configuration ของอุปกรณ์เครือข่ายของหน่วยงานให้เชื่อมต่อกับ สพธอ. ได้ • ความต้องการ - ผู้ดูแลระบบเครือข่ายที่ดูแลอุปกรณ์ Router หรือ Firewall	1 วัน
3	การอัปเดตหรือตั้งค่า DNS ในส่วนของเว็บไซต์ ไปที่ IP Address ของ สพธอ. • วัตถุประสงค์ - เพื่อให้มีการส่งข้อมูลที่มีการร้องขอในการเข้าถึงเว็บไซต์ ให้มีการส่งผ่านระบบป้องกันการโจมตีก่อน ส่งไปยังระบบเว็บไซต์ของหน่วยงาน • ความต้องการ - ผู้ดูแลระบบเครือข่ายที่ดูแลอุปกรณ์ DNS - แก้ไข Configuration ของ DNS Server ในส่วนของเว็บไซต์ให้มีการส่งค่า IP Address เป็นของ สพธอ. แทน	1 วัน
4	การตั้งค่า Firewall ในลักษณะ Whitelist เพื่อเชื่อมต่อระหว่างหน่วยงานกับ สพธอ. ให้สามารถเชื่อมต่อกันได้เท่านั้น • วัตถุประสงค์ - เพื่อจำกัดรูปแบบการเข้าใช้งาน ป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถเข้าใช้งานเว็บไซต์ผ่าน IP ของหน่วยงานเดิมได้จากเครือข่ายอินเทอร์เน็ต โดยการใช้งานของผู้ใช้งานจากอินเทอร์เน็ตจะผ่านเข้ามาทาง IP ของ สพธอ. เท่านั้น อย่างไรก็ตามการดำเนินการในส่วนนี้ ต้องเกิดขึ้นหลังจากการตั้งค่าในข้อที่ 3 เสร็จสิ้นแล้ว และระบบ DNS ทั่วโลก รับข้อมูลการตั้งค่าใหม่แล้ว เพื่อป้องกันผลกระทบต่อผู้ใช้งานโดยตรง • ความต้องการ - ผู้ดูแลระบบเครือข่ายที่ดูแลอุปกรณ์ Router หรือ Firewall	1 วัน
5	การตั้งค่าโหมดรับรู้ (Learning) ของอุปกรณ์ Web Application Firewall (WAF) จะทำการเปิดคุณสมบัติของตัวอุปกรณ์ Web Application Firewall (WAF) เพื่อเก็บข้อมูลต่างๆ ที่เข้าออกเว็บไซต์ของผู้เข้าร่วม โดยในระหว่างนี้อุปกรณ์จะยังไม่มีการบล็อคข้อมูลใด ๆ ทั้งสิ้น • วัตถุประสงค์ - เพื่อให้ระบบ WAF ทำฟังก์ชันที่เรียกว่า Learning ข้อมูลที่รับส่งผ่านเว็บไซต์ เพื่อสร้างเงื่อนไขที่เหมาะสมในการตรวจสอบ • ความต้องการ - ผู้ดูแลระบบเว็บไซต์	7 - 14 วัน

ลำดับ	กิจกรรม	ประเมินระยะเวลา
6	การนำผลลัพธ์ที่ได้จากการทำ Vulnerability Scanning มาทำการตรวจสอบและเป็นข้อมูลในการตั้งค่า Rule ของ WAF ให้มีความเหมาะสม • วัตถุประสงค์ - เพื่อทำให้ระบบมีความมั่นคงปลอดภัย และสามารถป้องกันการโจมตีช่องโหว่เดิมที่เว็บไซต์เคยมีอยู่ได้	7 วัน
รวม		**25 - 30 วัน**

การตั้งค่าเครือข่ายของอุปกรณ์ที่หน่วยงานในโครงการ GWP ดังแสดงในภาคผนวก ค.

4.) เริ่มกระบวนการวิเคราะห์เฝ้าระวังภัยคุกคามและการป้องกันการโจมตีเว็บไซต์

ดำเนินการวิเคราะห์เฝ้าระวังภัยคุกคามและการป้องกันการโจมตีเว็บไซต์ ตามขอบเขตที่มีการตกลงกัน เพื่อให้บรรลุตามจุดประสงค์ของโครงการ โดย สพธอ. ได้จัดเตรียมบุคลากรไว้คอยเฝ้าระวังเหตุการณ์การโจมตีที่อาจเกิดขึ้นกับหน่วยงาน พร้อมทีมงานผู้เชี่ยวชาญในเรื่องการรักษาความมั่นคงปลอดภัย สำหรับช่วยในการให้คำปรึกษา และการแก้ไขปัญหาเหตุภัยคุกคามเพื่อให้หน่วยงานมีความพร้อมและสามารถตอบสนองต่อเหตุภัยคุกคามอย่างเหมาะสม ในลักษณะบริหารจัดการจากศูนย์กลางและดำเนินงานในลักษณะ 24 x 7 ชั่วโมง

เงื่อนไขในการรักษาความลับของข้อมูลของหน่วยงาน

สพธอ. ตกลงจะเก็บรักษาข้อมูล Log และผลการวิเคราะห์ข้อมูลของแต่ละหน่วยงานที่ได้จากการดำเนินการในครั้งนี้ไว้เป็นความลับ และจะไม่เปิดเผยแก่บุคคลอื่น เว้นแต่จะได้รับความยินยอมเป็นหนังสือจากหน่วยงานที่เป็นเจ้าของข้อมูลนั้นก่อน หรือเป็นการเปิดเผยแก่พนักงานเจ้าหน้าที่ หรือเจ้าหน้าที่ของรัฐ หรือเจ้าหน้าที่ตามกฎหมายอื่น หรือเป็นการกระทำตามคำสั่งศาล หรือกรณีที่กฎหมายกำหนดไว้เป็นอย่างอื่น หรือเป็นการเปิดเผยข้อมูลในเชิงสถิติหรือในลักษณะที่ไม่ระบุชื่อหรืออ้างอิงไปถึงหน่วยงาน

ภาคผนวก ก.

รายการอุปกรณ์/ระบบที่สนับสนุนการส่งข้อมูล Log ของโครงการ GTM

กลุ่ม Network/Security Device ชนิด IPS/IDS, Web Application Firewall

ตารางที่ 1 กลุ่ม Network/Security Device ชนิด IPS/IDS, Web Application Firewall

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	AirMagnet Enterprise
2.	Arbor Networks Peakflow SP5
3.	Arbor Networks Peakflow X
4.	Astaro Security Gateway
5.	Barracuda Web Application Firewall
6.	Bee Ware Web Application Firewall
7.	Check Point IPSO
8.	Check Point Security Suite, IPS-1
9.	Cisco Adaptive Security Appliance
10.	Cisco ASA Security Services Module
11.	Cisco PIX Firewall
12.	Cisco Secure IDS or IPS
13.	CyberGuard Classic Firewall
14.	Cyberoam UTM
15.	Enterasys Dragon
16.	F5 Big-IP Application Security Manager
17.	FireEye Web Malware Protection System
18.	Fortinet FortiGate
19.	Hewlett-Packard TippingPoint Security Management System
20.	IBM ISS SiteProtector
21.	Imperva SecureSphere
22.	Juniper Networks Intrusion Detection and Prevention (IDP)
23.	Juniper Networks NetScreen Firewall
24.	Juniper Networks NetScreen ScreenOS
25.	Juniper Networks NetScreen-Security Manager
26.	McAfee Firewall Enterprise
27.	McAfee Network Security Platform
28.	Motorola AirDefense Enterprise Console

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
29.	NFR NIDS
30.	Nortel Alteon Switch Firewall
31.	Open Source SNORT
32.	Palo Alto Networks Enterprise Firewall
33.	Radware DefensePro
34.	SonicWALL Firewall
35.	Sourcefire Defense Center

กลุ่ม Network/Security Device ชนิด Router, Switch

ตารางที่ 2 กลุ่ม Network/Security Device ชนิด Router, Switch

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Alcatel-Lucent OmniSwitch
2.	Aruba Networks AirWave
3.	Aruba Networks Mobility Controller
4.	Brocade FastIron Switch
5.	Cisco Aggregation Services Router
6.	Cisco Aironet AP (Wireless Access Point)
7.	Cisco Switch
8.	Cisco Wireless Control System
9.	Cisco Wireless LAN Controller (2100 Series and 4400 Series)
10.	Dell PowerConnect 5324 Switch
11.	Enterasys Switch
12.	Hewlett-Packard ProCurve Switch
13.	Juniper Networks JUNOS
14.	Juniper Networks Wireless LAN Controller

กลุ่ม Network/Security Device ชนิด Network Access Control Server

ตารางที่ 3 กลุ่ม Network/Security Device ชนิด Network Access Control Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Aruba Networks ClearPass Policy Manager
2.	Cisco Network Admission Control
3.	ForeScout CounterACT
4.	Juniper Networks Unified Access Control
5.	McAfee Network Access Control
6.	Microsoft Network Access Protection

กลุ่ม Network/Security Device ชนิด VPN Server

ตารางที่ 4 กลุ่ม Network/Security Device ชนิด VPN Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Cisco Adaptive Security Appliance
2.	Cisco Aggregation Services Router
3.	F5 Firepass SSL VPN
4.	Juniper Networks SSL VPN
5.	Nortel Networks Contivity VPN Switch
6.	SonicWall E-Class SRA / Aventail SSL VPN

กลุ่ม Network/Security Device ชนิด Proxy Server

ตารางที่ 5 กลุ่ม Network/Security Device ชนิด Proxy Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Blue Coat ProxySG
2.	Cisco IronPort Web Security Appliance (WSA)
3.	McAfee Web Gateway
4.	Trend Micro InterScan Web Security
5.	Websense Web Security

กลุ่ม Network/Security Device ชนิด Mail gateway Server

ตารางที่ 6 กลุ่ม Network/Security Device ชนิด Mail gateway Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Cisco IronPort Email Security Appliance
2.	Fortinet FortiMail
3.	McAfee Email Gateway (formerly known as CipherTrust IronMail)
4.	Proofpoint Email Security
5.	SonicWALL Email Security
6.	Symantec Brightmail
7.	Trend Micro ScanMail

กลุ่ม Service Server ชนิด Operating System(Authentication Log)

ตารางที่ 7 กลุ่ม Service Server ชนิด Operating System(Authentication Log)

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	ActivIdentity 4TRESS AAA Server
2.	CentOS
3.	Debian GNU/Linux
4.	Hewlett-Packard UNIX
5.	IBM AIX
6.	IBM iSeries AS400
7.	Juniper Steel-Belted Radius
8.	Microsoft Windows
9.	Novell eDirectory
10.	Novell SuSE Linux Enterprise
11.	Red Hat Enterprise Linux
12.	RSA Auth Manager
13.	Sun ONE Directory Server
14.	Sun Solaris

กลุ่ม Service Server ชนิด Web Server

ตารางที่ 8 กลุ่ม Service Server ชนิด Web Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Apache Web Server
2.	IBM WebSphere
3.	Microsoft IIS

กลุ่ม Service Server ชนิด Database Server

ตารางที่ 9 กลุ่ม Service Server ชนิด Database Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	IBM DB2
2.	Microsoft SQL Server 2000
3.	Microsoft SQL Server 2005
4.	Microsoft SQL Server Trace
5.	Oracle DB
6.	Oracle Collector from Logs
7.	Sybase

กลุ่ม Service Server ชนิด DHCP Server

ตารางที่ 10 กลุ่ม Service Server ชนิด DHCP Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	ISC DHCP
2.	Microsoft DHCP
3.	Infoblox
4.	BlueCat

กลุ่ม Service Server ชนิด DNS Server

ตารางที่ 11 กลุ่ม Service Server ชนิด DNS Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Microsoft DNS
2.	BIND
3.	Infoblox
4.	BlueCat

กลุ่ม Service Server ชนิด Mail Server

ตารางที่ 12 กลุ่ม Service Server ชนิด Mail Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการ/หรือโปรแกรมให้บริการ
1.	Microsoft Exchange MT
2.	SendMail

กลุ่ม Service Server ชนิด Proxy Server

ตารางที่ 13 กลุ่ม Service Server ชนิด Proxy Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการ/หรือโปรแกรมให้บริการ
1.	Squid Web Proxy

กลุ่ม Service Server ชนิด Antivirus Server

ตารางที่ 14 กลุ่ม Service Server ชนิด Antivirus Server

ลำดับ	ชนิดของข้อมูล Log จากอุปกรณ์ ระบบปฏิบัติการหรือโปรแกรมให้บริการ
1.	Kaspersky Administration Kit
2.	McAfee VirusScan Enterprise
3.	Symantec Endpoint Protection

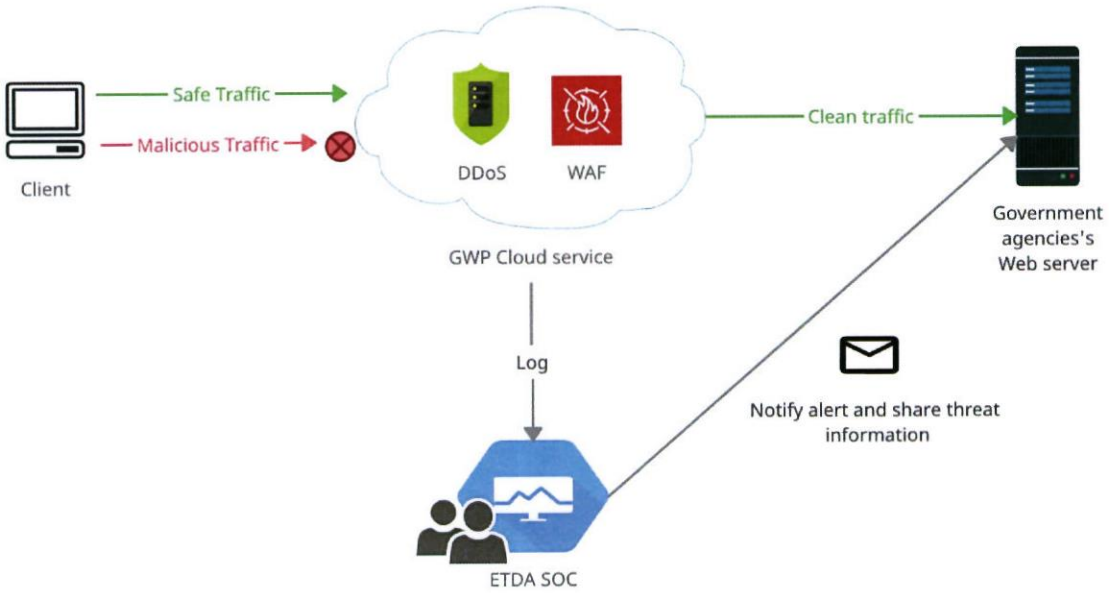
ภาคผนวก ข.

รายการอุปกรณ์/ระบบที่สนับสนุนการติดตั้ง EDR (Endpoint Detection and Response) ของโครงการ GTM

ตารางที่ 1 EDR Client operating system

Operating System
Windows Server 2019 (64-bit only)
Windows Server 2016 (64-bit only)
Windows Server 2012 (64-bit only)
Windows Server 2008 R2 Enterprise (64-bit only)
Windows Server 2008 R2 Standard (64-bit only)
Windows 10 Enterprise (32-bit and 64-bit)
Windows 8.1 Enterprise (32-bit and 64-bit)
Windows 8.0 (32-bit and 64-bit)
Windows 7 Enterprise (32-bit and 64-bit)
Windows 7 Professional (32-bit and 64-bit)

การตั้งค่าเครือข่ายของอุปกรณ์ในโครงการ GWP สำหรับหน่วยงานที่เข้าร่วม

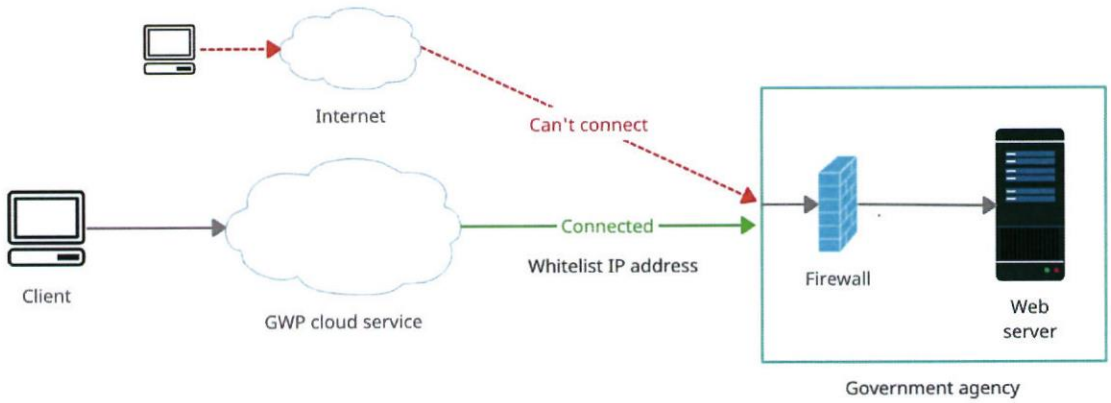


รูปที่ 1 แสดงแผนภาพการเชื่อมต่อระบบป้องกันแบบคลาวด์ (Cloud service)

จากรูปที่ 1 แสดงระบบป้องกันแบบคลาวด์ ซึ่งประกอบด้วยการป้องกันผ่านระบบ DDoS และ WAF ซึ่งเปรียบเสมือนการป้องกันด่านแรกที่คอยเฝ้าระวังการโจมตีทางไซเบอร์ที่เกี่ยวข้องกับเว็บไซต์ ด้วยการทำงานแบบคลาวด์จะช่วยเพิ่ม Performance และ Scalability ประกอบด้วยการทำงานในรูปแบบ Content Delivery Network (CDN) เพื่อลดภาระการใช้งานเครื่องให้บริการปลายทางของหน่วยงาน และการสำรองเนื้อหาหน้าเว็บไซต์ (Static Content) เพื่อให้บริการได้ ในกรณีที่เว็บไซต์ของหน่วยงานไม่สามารถให้บริการได้ โดยระบบมีการตรวจจับและป้องกันการโจมตีก่อนส่งข้อมูลไปยังเว็บไซต์ของหน่วยงาน พร้อมทั้งทีม ETDA SOC ที่ช่วยเฝ้าระวังและวิเคราะห์ข้อมูลเหตุการณ์การโจมตีที่เกิดขึ้น ณ ศูนย์กลาง (HQ) ของ สพธอ. และแจ้งเตือนไปยังหน่วยงานที่เกี่ยวข้อง

การตั้งค่าเครือข่ายของอุปกรณ์ของหน่วยงาน

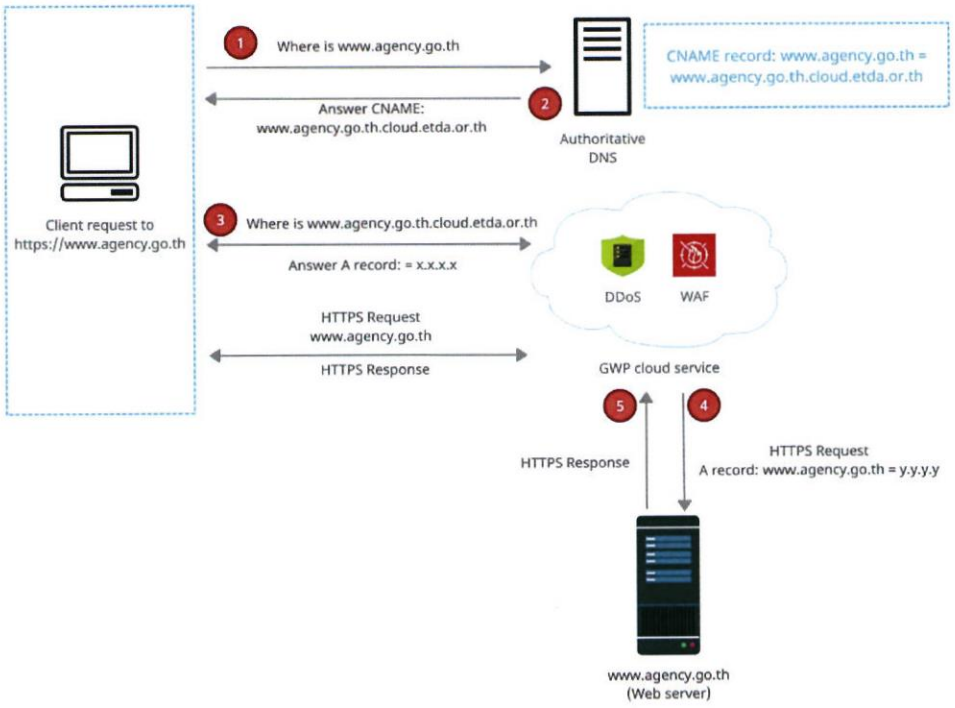
การเปิดใช้งานระบบป้องกันแบบคลาวด์ หน่วยงานต้องดำเนินการตั้งค่า DNS record เว็บไซต์ของหน่วยงานให้ชี้ CNAME ไปยังระบบป้องกัน ของ สพธอ. เพื่อให้ทำงานในลักษณะ Reverse Proxy โดยกระบวนการดังกล่าวจะต้องผ่านขั้นตอนยืนยันการเป็นเจ้าของโดเมนเนมของหน่วยงานด้วยการตรวจสอบค่า TXT record บน Authoritative DNS ตามที่ สพธอ. ได้จัดเตรียมไว้



รูปที่ 2 แสดงแผนภาพเครือข่ายที่มีการเชื่อมต่อระบบผ่าน Internet โดยการทำ Whitelist ให้กับ IP Address ของระบบป้องกันแบบคลาวด์ (Cloud service)

จากรูปที่ 2 เพื่อการเชื่อมต่อที่มั่นคงปลอดภัยทาง สพธอ. แนะนำให้หน่วยงานทำการตั้งค่าอุปกรณ์ป้องกันทางเครือข่าย เช่น Firewall, IPS และอื่นๆ โดยอนุญาตให้หมายเลข IP Address ระบบป้องกันแบบคลาวด์ ของ สพธอ. เท่านั้นที่สามารถเชื่อมต่อกับเว็บเซิร์ฟเวอร์ของหน่วยงานได้ (หรือเรียกว่าเป็นการทำ Whitelisting ให้เฉพาะ สพธอ.) เพื่อป้องกันไม่ให้ผู้ใช้หรือ IP Address อื่นๆ สามารถเข้าถึงเว็บเซิร์ฟเวอร์ได้โดยตรง (ไม่ได้ผ่านระบบป้องกันในโครงการ GWP)

ตัวอย่างการทำงานของระบบป้องกันแบบคลาวด์ (Cloud service) โดยสังเขป



รูปที่ 3 แผนภาพแสดงตัวอย่างขั้นตอนการทำงานในการค้นหาข้อมูล DNS ของโดเมนที่มีการใช้งานระบบป้องกันแบบคลาวด์ (Cloud service)

จากรูปที่ 3 สามารถอธิบายการทำงานเมื่อผู้ใช้มีการเข้าถึงเว็บไซต์ของหน่วยงาน www.agency.go.th ตามหมายเลขในรูปได้ดังนี้

1) เมื่อผู้ใช้งานเข้าถึงเว็บไซต์ www.agency.go.th จะมีขั้นตอน DNS query ไปยัง Authoritative DNS ของหน่วยงาน หรือที่ถูกตั้งค่าไว้เพื่อร้องขอข้อมูลที่อยู่ของเว็บไซต์ www.agency.go.th
2) Authoritative DNS จะตอบกลับด้วย CNAME record ที่ถูกระบุไว้ใน www.agency.go.th ดังตัวอย่างเช่น CNAME “www.agency.go.th” = “www.agency.go.th.cloud.etda.or.th” ซึ่งเป็นที่อยู่ CNAME ของระบบป้องกัน Cloud Service ของ สพธอ.
3) เมื่อได้รับ CNAME แล้วเครื่องผู้ใช้งานจะทำการ Request ต่อไปยังระบบป้องกันของ สพธอ. โดยจะเป็นการเชื่อมต่อเว็บไซต์ผ่านระบบป้องกันประกอบด้วย DDoS และ WAF ในลักษณะ Reverse Proxy เพื่อกรองข้อมูลส่วนที่ไม่เหมาะสมออกไป
4) ระบบป้องกันของ สพธอ. จะทำการ Request ต่อไปยังเว็บเซิร์ฟเวอร์ของเว็บไซต์ www.agency.go.th ผ่าน IP Address “y.y.y.y”
5) เว็บเซิร์ฟเวอร์ของหน่วยงานจะได้รับข้อมูลการ Request จากระบบป้องกัน ของ สพธอ. และส่งต่อข้อมูล Response กลับไปยังผู้ใช้ต่อไป