

ที่ สภามช ๐๘๐๐/๘๘๖

สลด. (eMail)

ส่ง : กสค.

รับที่ : ๕3231/66

10 มี.ค. 2566 เวลา 17.33 น.



ณ มีนาคม ๒๕๖๖

เรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ
ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบ
อย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอเรื่อง รายงานสรุป
ผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่
๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ มาเพื่อคณะรัฐมนตรีทราบ โดยเรื่องนี้เข้าข่ายที่จะต้องนำเสนอ
คณะรัฐมนตรีตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่อง และการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑)
รวมทั้ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของ
การรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐาน
การรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” ทั้งนี้ พลเอก ประวิตร วงษ์สุวรรณ
รองนายกรัฐมนตรี/ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้เห็นชอบให้นำเรื่องดังกล่าว
เสนอคณะรัฐมนตรีด้วยแล้ว

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี

ตามอ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำ
รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ
หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” นั้น
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงขอรายงานสรุปผลการดำเนินงานของการรักษา
ความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕
ให้คณะรัฐมนตรีเพื่อรับทราบ โดยมีสาระสำคัญประกอบด้วย ข้อมูลทั่วไป สรุปสถานการณ์ของภัยคุกคาม
ทางไซเบอร์ในประเทศไทย ผลการดำเนินการที่สำคัญ บทวิเคราะห์สถานการณ์ แนวโน้มเหตุการณ์ภัยคุกคาม
ทางไซเบอร์ เพื่อใช้เป็นข้อมูลสำหรับการพัฒนาแนวทางและมาตรการในการป้องกัน รับมือ เพื่อลดความเสี่ยง
ต่อการเกิดภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานซึ่งมีภารกิจหรือบริการที่ส่งผลกระทบต่อประชาชน
ต่อไป

๒. สารระสำคัญ ข้อเท็จจริงและข้อกฎหมาย

๒.๑ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์ และประมวลผล ข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือ หน่วยงานที่เกี่ยวข้อง ในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยได้นำเสนอ รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ในการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ แห่งชาติ ครั้งที่ ๑/๒๕๖๖ เมื่อวันที่พฤหัสบดีที่ ๕ มกราคม ๒๕๖๖ เวลา ๑๐.๐๐ น. ณ ห้องประชุม ชั้น ๒ มูลนิธิ อนุรักษ์ปารอยต่อ ๕ จังหวัด โดยที่ประชุมมีมติเห็นชอบให้รายงานคณะรัฐมนตรีเพื่อทราบ

๒.๒ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้จัดทำ รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในแต่วันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ในภารกิจเกี่ยวกับการป้องกัน รับมือ แก้ไขปัญหา และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ รวมทั้งสิ้น ๕๕๑ เหตุการณ์ รายละเอียดปรากฏ ตามสิ่งที่ส่งมาด้วย โดยสรุปสาระสำคัญ ได้ดังนี้

๒.๒.๑ สถิติเหตุการณ์ภัยคุกคามทางไซเบอร์ ที่ได้ดำเนินการและตรวจพบมากที่สุด แบ่งเป็นประเภทของภัยคุกคามทางไซเบอร์ ได้ดังนี้

๒.๒.๑.๑ ประเภท Hacked Website จำนวนรวม ๓๖๗ เหตุการณ์ แบ่งออกเป็น ประเภท Gambling (การพนันออนไลน์) จำนวน ๑๘๖ เหตุการณ์, Website Defacement จำนวน ๑๒๕ เหตุการณ์, Website Phishing จำนวน ๓๘ เหตุการณ์ และ Website Malware ๑๘ เหตุการณ์

๒.๒.๑.๒ ประเภทจุดอ่อนช่องโหว่ (Vulnerability) จำนวน ๖๓ เหตุการณ์

๒.๒.๑.๓ ประเภทข้อมูลรั่วไหล (Data Breach) จำนวน ๔๘ เหตุการณ์

๒.๒.๑.๔ ประเภท Ransomware จำนวน ๒๑ เหตุการณ์

๒.๒.๑.๕ ประเภท Emotet Malware จำนวน ๙ เหตุการณ์

๒.๒.๑.๖ ประเภท Command and Control Server จำนวน ๖ เหตุการณ์

๒.๒.๑.๗ ประเภทอื่น ๆ จำนวน ๓๗ เหตุการณ์

๒.๒.๒ สถิติการปฏิบัติงานในการสนับสนุนช่วยแก้ไขปัญหาและรับมือกับภัยคุกคาม ทางไซเบอร์ โดยสรุปได้ ดังนี้

๒.๒.๒.๑ แจ้งเตือนเหตุการณ์ ให้คำปรึกษา และแนะนำในการแก้ไขปัญหา จำนวน ๔๖๗ เหตุการณ์

๒.๒.๒.๒ การแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๔๓ รายงาน

๒.๒.๒.๓ การประเมินความเสี่ยง และทดสอบการเจาะระบบเพื่อหาจุดอ่อน ช่องโหว่ให้กับหน่วยงานของรัฐ จำนวน ๒๙ หน่วยงาน

๒.๒.๒.๔ การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ จำนวน ๑๒ ครั้ง

๒.๒.๒.๕ การเผยแพร่ข้อมูลภัยคุกคามและข่าวสารที่เป็นประโยชน์ต่อ สาธารณะ จำนวน ๓๒๒ รายงาน

๒.๒.๒.๖ ประสานงานเพื่อให้ระงับการเผยแพร่เว็บไซต์ปลอมหรือเลียนแบบ จำนวน ๔๓ หน่วยงาน

๒.๒.๓ ประเภทของหน่วยงานที่ถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ สรุปได้ดังนี้

๒.๒.๓.๑ ด้านการศึกษา จำนวน ๒๑๑ เหตุการณ์

๒.๒.๓.๒ หน่วยงานของรัฐที่ไม่ใช่ CII จำนวน ๑๓๕ เหตุการณ์

๒.๒.๓.๓ ด้านสาธารณสุข จำนวน ๖๗ เหตุการณ์

๒.๒.๓.๔ ผู้ประกอบการที่เป็นบริษัทเอกชน สัญชาติไทย จำนวน ๒๔ เหตุการณ์

๒.๒.๓.๕ ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์ จำนวน ๑๒ เหตุการณ์

๒.๒.๓.๖ ด้านพลังงานและสาธารณูปโภค จำนวน ๑๑ เหตุการณ์

๒.๒.๓.๗ ด้านการขนส่งและโลจิสติกส์ จำนวน ๑๐ เหตุการณ์

๒.๒.๓.๘ ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี จำนวน ๙ เหตุการณ์

๒.๒.๓.๙ เทคโนโลยีสารสนเทศและโทรคมนาคม จำนวน ๕ เหตุการณ์

๒.๒.๓.๑๐ ด้านบริการภาครัฐ จำนวน ๔ เหตุการณ์

๒.๒.๓.๑๑ ด้านการเงินการธนาคาร จำนวน ๔ เหตุการณ์

๒.๒.๓.๑๒ ผู้ประกอบการธุรกิจอีคอมเมิร์ซ จำนวน ๓ เหตุการณ์

๒.๒.๓.๑๓ ด้านอื่น ๆ จำนวน ๙ เหตุการณ์

๒.๒.๔ แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ จากเหตุการณ์ภัยคุกคามทางไซเบอร์ จำนวน ๕๕๑ เหตุการณ์ มีข้อมูลที่สำคัญสรุปได้ดังนี้

๒.๒.๔.๑ การโจมตีทางไซเบอร์ที่ถูกตรวจพบมากที่สุด ได้แก่ การโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) หน่วยงานราชการและหน่วยงานสำคัญซึ่งมีมากกว่าการโจมตีรูปแบบอื่น ๆ โดยคิดเป็น ๒ ใน ๓ ของการโจมตีทางไซเบอร์ที่ตรวจพบในประเทศไทย อันดับหนึ่ง ได้แก่ การโจมตีในลักษณะทำไปเพื่อการแฝงหน้าเว็บพบนอนไลน์ในเว็บไซต์ของหน่วยงาน เพื่อเพิ่มโอกาสและประสิทธิภาพการค้นหาผ่าน Search Engine ส่วนอันดับสอง ได้แก่ การโจมตีโดยเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ของหน่วยงาน เพื่อใช้เป็นพื้นที่ทดสอบความสามารถของแฮ็กเกอร์หรือเป็นผลลัพธ์จากการเคลื่อนไหวทางการเมืองของกลุ่มต่าง ๆ นอกจากนี้ ยังพบการโจมตีด้วยการแฮ็กเว็บไซต์แบบอื่น ๆ ที่น่าสนใจ เช่น การสร้างหน้าเว็บไซต์เพื่อหลอก Phishing อยู่บนเว็บไซต์หน่วยงานของรัฐ และการฝังมัลแวร์อันตรายบนหน้าเว็บไซต์หน่วยงานที่อาจหลอกให้ผู้เข้าถึงดาวน์โหลดไปติดตั้งได้ เป็นต้น

๒.๒.๔.๒ หน่วยงานที่พบการโจมตีทางไซเบอร์สูงสุด ได้แก่ หน่วยงานด้านการศึกษา และหน่วยงานด้านสาธารณสุข ซึ่งมีเว็บไซต์และระบบต่าง ๆ ให้บริการอยู่เป็นจำนวนมาก และใช้เว็บไซต์เป็นสื่อประชาสัมพันธ์หลัก การบริหารงานในส่วนที่เกี่ยวข้องกับระบบไอทีที่มีความเป็นเอกเทศทำให้การดูแลจากหน่วยงานส่วนกลางทำได้ยาก เมื่อมีการพัฒนาระบบที่ต้องดำเนินการเอง หรือว่าจ้างบุคคลจากภายนอกนั้น จะมีการปรับปรุงแค่เฉพาะเนื้อหาในเว็บไซต์เพียงอย่างเดียว จึงขาดการดูแลรักษาระบบและการตรวจสอบอย่างสม่ำเสมอ

๒.๒.๔.๓ สถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนและมีความสัมพันธ์กับความมั่นคงปลอดภัยทางไซเบอร์ โดยพบว่า อาชญากรรมทางไซเบอร์ในประเทศไทย ได้ใช้เทคนิคผสมผสานการ Phishing และ Social Engineering หลายรูปแบบเพื่อหลอกลวงเหยื่อ และนอกจากจะได้ไปซึ่งทรัพย์สินของเหยื่อแล้ว การกระทำดังกล่าว ทำให้เกิดผลกระทบต่อการรักษาความลับของข้อมูลส่วนตัว

รวมถึงความปลอดภัยในตัวระบบและอุปกรณ์ของเหยื่อเช่นเดียวกัน อาทิเช่น กรณีมีจิวซีพหลอกขอรหัสผ่าน ส่วนตัวของเหยื่อผ่านโทรศัพท์หรือผ่านแอปพลิเคชัน การปลอมแปลงเว็บไซต์หน่วยงานของรัฐโดยตั้งชื่อโดเมนให้คล้ายคลึง และมีเนื้อหาเลียนแบบเว็บไซต์จริง เพื่อหลอกเอาข้อมูลส่วนบุคคล หรือหลอกให้ดาวน์โหลดไฟล์ที่มีมัลแวร์บนหน้าเว็บไซต์ การส่งลิงก์ Phishing ที่แฝงโฆษณา หรือมีชื่อผู้ส่งเลียนแบบ Platform ธนาคาร เพื่อพาเหยื่อไปในหน้าเว็บไซต์ให้กรอกข้อมูลส่วนบุคคลหรือมีการดาวน์โหลดมัลแวร์ลงไปที่เครื่อง การจำหน่ายข้อมูลส่วนบุคคลที่ได้มาด้วยวิธีการต่างๆ ใน Dark web หรือ Communities ต่าง ๆ เป็นต้น

๒.๒.๔.๔ การโจมตีด้วย Ransomware ที่เกิดขึ้นกับหน่วยงานภาครัฐที่มีความสำคัญ และภาคเอกชนที่เป็นธุรกิจที่มีชื่อเสียง มีทุนจดทะเบียนสูง กระจายตัวในหลายประเภทอุตสาหกรรม โดยเมื่อเกิดเหตุ Ransomware ขึ้นแล้ว ความเสียหายที่เห็นชัดเจนของแต่ละหน่วยงาน คือการที่ไม่สามารถเข้าระบบเพื่อใช้งานข้อมูลที่สำคัญได้ และบางแห่งไม่สามารถใช้งานระบบสำรองได้ นอกจากนี้ ยังส่งผลกระทบต่อการบริหารจัดการและทำงานของระบบสารสนเทศในภาพรวมของหน่วยงาน ซึ่งหน่วยงานแต่ละหน่วยจะต้องใช้ระยะเวลาในการแก้ไขปัญหาจากการโจมตีด้วย Ransomware ที่ยาวนาน และอาจต้องพึ่งพาผู้เชี่ยวชาญจากบุคคลภายนอกอีกด้วย

๒.๒.๕ แนวทางการจัดการภัยคุกคามทางไซเบอร์ ในการดำเนินมาตรการที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ (incident handling) ได้มีการแนะนำให้กับหน่วยงานต่าง ๆ ดำเนินการให้มีความสอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ และเป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ โดยแบ่งขั้นตอนได้เป็น ๔ ขั้นตอนหลัก ดังนี้

- (๑) การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)
- (๒) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)
- (๓) การระงับภัยคุกคามทางไซเบอร์ การปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication and recovery)
- (๔) การดำเนินกิจกรรมภายหลังการระงับภัยคุกคามทางไซเบอร์ (post-incident activity)

๒.๒.๖ ข้อเสนอแนะในการแก้ไขปัญหาที่สำคัญจากแนวโน้มสถานการณ์ทางไซเบอร์ที่สำคัญในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ สรุปได้ดังนี้

๒.๒.๖.๑ การถูกโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) เป็นเรื่องที่คุณและผู้ดูแลระบบของหน่วยงานควรให้ความสนใจกับการปรับปรุงแพตช์ (PATCH) ของระบบปฏิบัติการ หรือระบบบริหารจัดการเว็บไซต์ (CMS) ให้เป็นปัจจุบัน ทบทวนการใช้งาน Themes หรือ Plug-in ต่าง ๆ ที่อาจมีช่องโหว่ การเปลี่ยนแปลงแก้ไขรหัสผ่านต่าง ๆ ทำให้ยากต่อการคาดเดา ตรวจสอบการนำเข้าไฟล์ต่าง ๆ สำหรับผู้ใช้งานเว็บไซต์ให้อนุญาตเฉพาะไฟล์ที่ต้องการเท่านั้น รวมไปถึงใช้วิธีการเข้ารหัสข้อมูลที่มีความสำคัญต่าง ๆ ด้วย

๒.๒.๖.๒ การดูแลเว็บไซต์และระบบที่เกี่ยวข้องของหน่วยงานต่าง ๆ โดยเฉพาะหน่วยงานที่มีความเป็นเอกเทศนั้น หน่วยงานส่วนกลางควรมีการกำหนดนโยบายเกี่ยวกับการดูแลและพัฒนาเว็บไซต์ ซึ่งหากจะดำเนินการเองหรือว่าจ้างบุคคลภายนอกแล้ว ควรให้มีการดูแลรักษาระบบ และตรวจสอบอย่างสม่ำเสมอ รวมไปถึงแนวทางการเขียนร่างขอบเขตของงาน (TOR) และการกำหนดคุณสมบัติเพื่อการจัดจ้างทำเว็บไซต์หรือพัฒนาระบบที่เกี่ยวข้องที่ต้องคำนึงถึงเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วย

๒.๒.๖.๓ ในเรื่องสถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนนั้น การสร้างความรู้ความเข้าใจ และการให้ความตระหนักรู้กับประชาชนเป็นสิ่งที่สำคัญมาก โดยเฉพาะการสร้างการรับรู้เกี่ยวกับรูปแบบและวิธีการที่เหล่ามิจฉาชีพใช้ในการหลอกลวง รวมไปถึงประชาชนจะต้องรับทราบถึงความเสี่ยงหรือผลกระทบจากการที่ตนเองตกเป็นเหยื่อหรือถูกหลอก ซึ่งนอกจากจะส่งผลทำให้สูญเสียทรัพย์สินแล้ว ยังเป็นผลสัมพันธไปถึงความมั่นคงปลอดภัยทางไซเบอร์ที่จะถูกแฮ็กเกอร์นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในการเข้าถึงระบบต่าง ๆ ได้

๒.๒.๖.๔ ในเรื่อง Ransomware หน่วยงานต่าง ๆ สามารถลดความเสี่ยงได้ โดยการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP) และปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยให้ความสำคัญกับการสำรองข้อมูล และตรวจสอบอย่างสม่ำเสมอ

๓. ประเด็นด้านกฎหมาย

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ”

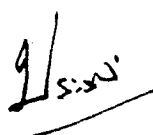
๔. ข้อเสนอส่วนราชการ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้วเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) จึงเห็นควรนำเสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ต่อที่ประชุมคณะรัฐมนตรีเพื่อรับทราบ

จึงเรียนมาเพื่อโปรดนำกราบเรียนนายกรัฐมนตรีเพื่อเสนอคณะรัฐมนตรีทราบต่อไป

ขอแสดงความนับถือ

พลเอก



(ประวตร วงษ์สุวรรณ)

รองนายกรัฐมนตรี

ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕

E-Mail : ncert@ncsa.or.th



QR code เอกสารแนบ