

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์

พ.ศ. ๒๕๖๖

โดยที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์กำหนดหลักเกณฑ์และวิธีการรายงาน เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๑๓ (๕) และมาตรา ๕๗ แห่งพระราชบัญญัติการรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ในประกาศนี้

“เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ” หมายความว่า เหตุภัยคุกคามทางไซเบอร์ ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคาม ทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ข้อ ๔ กรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงาน ของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบ ข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม เพื่อประเมิน ว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และเป็นภัยคุกคามระดับใด หากตรวจพบต้องดำเนินการ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของตน พร้อมทั้งแจ้งข้อมูลดังกล่าว ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติโดยเร็ว หลังจากการตรวจพบ หรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าว และในส่วนของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้แจ้งภัยคุกคามนั้นไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือ กำกับดูแลกำหนดไว้ด้วย ทั้งนี้ ให้แจ้งข้อมูลตามที่กำหนดในเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง ท้ายประกาศนี้

ทั้งนี้ การแจ้งข้อมูลตามวรรคหนึ่งให้เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัย ไซเบอร์แห่งชาติ มีหน้าที่และอำนาจในการกำหนดแนวทาง วิธีปฏิบัติและอื่น ๆ เพื่อประโยชน์ ในการปฏิบัติตามประกาศนี้

ข้อ ๕ กรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดังกล่าวจัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์นั้น ตามแบบที่กำหนดในเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ ทำयประกาศนี้ ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในระยะเวลา ๒๔ ชั่วโมง หลังจากการตรวจพบหรือเกิดภัยคุกคามทางไซเบอร์ดังกล่าวแล้ว พร้อมทั้งให้จัดส่งรายงานดังกล่าว ไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดด้วย

ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับนโยบายการรักษาความลับของหน่วยงานด้วย และต้องปรับปรุงข้อมูลในรายงานเหตุภัยคุกคามทางไซเบอร์และสถานะการตอบสนองภัยคุกคามทางไซเบอร์ ให้สอดคล้องกับข้อมูลอันเป็นปัจจุบันที่หน่วยงานได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือเหตุภัยคุกคาม รวมทั้งจัดส่งรายงานปิดเหตุการณ์ภัยคุกคามดังกล่าวด้วย

ให้นำความในวรรคหนึ่งและวรรคสอง มาใช้บังคับแก่หน่วยงานของรัฐ กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ โดยอนุโลม

ข้อ ๖ ให้หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตน ในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี ทำยประกาศนี้

ข้อ ๗ การแจ้ง การรายงาน และการรายงานสรุปตามประกาศนี้ จะทำเป็นหนังสือ หรือโดยวิธีการทางอิเล็กทรอนิกส์ก็ได้

ข้อ ๘ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เป็นผู้รักษาการตามประกาศนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ หรือประกาศนี้ไม่ได้กำหนดเรื่องใดไว้ ให้ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์เป็นผู้มีอำนาจตีความและวินิจฉัยชี้ขาด และคำวินิจฉัยของประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๐ มีนาคม พ.ศ. ๒๕๖๖

ชัยวุฒิ ธนาคมานุสรณ์

รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ประธานกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

เอกสารแนบท้ายประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
ว่าด้วยข้อมูลที่ต้องแจ้งและแบบการรายงานภัยคุกคามทางไซเบอร์

บทนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และภัยคุกคามทางไซเบอร์ในระดับวิกฤติ และให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำรายงานเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ นั้น

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานการดำเนินมาตรการตามที่กำหนดในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ จึงกำหนดให้หน่วยงานดังกล่าวจัดทำรายงานเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานตามรายการที่กำหนดไว้ในแนบท้ายนี้ ผ่านการส่งทางอีเมล โทรสาร หรือด้วยวิธีการทางอิเล็กทรอนิกส์อื่นใดที่มีความปลอดภัย เช่น การส่งรายงานที่เข้ารหัสด้วย PGP มาทางอีเมล (เป็นอย่างน้อย)

เนื่องด้วยการส่งรายงานของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ทันการณเป็นเรื่องที่สำคัญ^๑ ในกรณีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศยังไม่สามารถแจ้งข้อมูลตามแบบรายงานได้อย่างครบถ้วนภายในระยะเวลา ๒๔ ชั่วโมง ให้หน่วยงานดังกล่าวจัดส่งรายงานด้วยข้อมูลเท่าที่มี และเมื่อมีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในการดำเนินการรับมือ ให้แจ้งต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเป็นระยะ และรีบจัดทำและส่งรายงานที่สมบูรณ์ให้แก่สำนักงานโดยเร็ว ทั้งนี้ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศพิจารณาส่งข้อมูลสำคัญที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ และสอดคล้องกับนโยบายการรักษาความลับของหน่วยงาน

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศไม่สามารถดำเนินการจัดเตรียมข้อมูลในรายงานได้ด้วยเหตุผลบางประการ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศแจ้งหน่วยงานควบคุมหรือกำกับดูแลของตนและสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติให้ทราบโดยเร็ว

ทั้งนี้ เพื่อให้หน่วยงานของรัฐ มีแนวทางปฏิบัติที่ชัดเจนในการรายงานเหตุภัยคุกคามทางไซเบอร์กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของหน่วยงานของรัฐ จึงให้นำหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดังกล่าวข้างต้น มาบังคับใช้แก่หน่วยงานของรัฐโดยอนุโลม

^๑ การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างมีนัยสำคัญต้องรายงานภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

^๒ มาตรา ๗๓ กำหนดให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ไม่รายงานเหตุภัยคุกคามทางไซเบอร์ โดยไม่มีเหตุอันสมควร ต้องระวางโทษปรับไม่เกิน ๒๐๐,๐๐๐ บาท

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น																	
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง																	
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม																	
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)																	
๔. ความต่อเนื่องของเหตุภัยคุกคาม <input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม																	
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ^๓ ในระดับใด (มาตรา ๖๐) <input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิกฤต (ก) <input type="checkbox"/> วิกฤต (ข) <input type="checkbox"/> ยังไม่สามารถระบุได้																	
๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ) <table border="1"> <thead> <tr> <th>หมวดหมู่*</th> <th>คำอธิบาย</th> </tr> </thead> <tbody> <tr> <td>หมวดหมู่ที่ ๒</td> <td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td> </tr> <tr> <td>หมวดหมู่ที่ ๓</td> <td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td> </tr> <tr> <td>หมวดหมู่ที่ ๔</td> <td>การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)</td> </tr> <tr> <td>หมวดหมู่ที่ ๕</td> <td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๖</td> <td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td> </tr> <tr> <td>หมวดหมู่ที่ ๗</td> <td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td> </tr> <tr> <td>หมวดหมู่ที่ ๘</td> <td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td> </tr> </tbody> </table>		หมวดหมู่*	คำอธิบาย	หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)	หมวดหมู่ที่ ๔	การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)	หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
หมวดหมู่*	คำอธิบาย																
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)																
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)																
หมวดหมู่ที่ ๔	การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)																
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)																
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)																
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)																
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)																
* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)																	

^๓ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรตระบุ หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรตระบุ วันที่: เลือกวันที่ เวลา: โปรตระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรตระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรตระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรตระบุ ตำแหน่งงาน: โปรตระบุ ชื่อหน่วยงาน: โปรตระบุ อีเมล: โปรตระบุ โทรศัพท์ (ที่ทำงาน / มือถือ): โปรตระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม <input type="checkbox"/> เหตุภัยคุกคามใหม่ <input type="checkbox"/> การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน <input type="checkbox"/> ใช่ <input type="checkbox"/> ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ^๔ ในระดับใด (มาตรา ๖๐) <input type="checkbox"/> ไม่ร้ายแรง <input type="checkbox"/> ร้ายแรง <input type="checkbox"/> วิกฤต (ก) <input type="checkbox"/> วิกฤต (ข) <input type="checkbox"/> ยังไม่สามารถระบุได้

^๔ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์	
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ	
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ <input type="checkbox"/> ยังไม่ได้แจ้ง <input type="checkbox"/> แจ้งแล้ว _____	
ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)	
หมวดหมู่*	คำอธิบาย
<input type="checkbox"/> หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
<input type="checkbox"/> หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
<input type="checkbox"/> หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
<input type="checkbox"/> หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
<input type="checkbox"/> หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
<input type="checkbox"/> หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
<input type="checkbox"/> หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
<input type="checkbox"/> อื่น ๆ	โปรดระบุ
<p>* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)</p>	
ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ: สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง): โปรดระบุ ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : โปรดระบุ บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการเงิน): โปรดระบุ ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด มีผลกระทบต่อการใช้งาน (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ รายละเอียดอื่น ๆ: โปรดระบุ	

หมวด ค: ข้อมูลการรับมือภัยคุกคาม	
ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)	
<input type="checkbox"/> เพิ่งพบเหตุการณ์	<input type="checkbox"/> อยู่ในขั้นตอนการขอความช่วยเหลือ
<input type="checkbox"/> อยู่ในขั้นตอนการสอบสวน	<input type="checkbox"/> กำลังลุกลาม
<input type="checkbox"/> อยู่ในขั้นตอนการระงับภัย	<input type="checkbox"/> สามารถระงับภัยได้แล้ว
<input type="checkbox"/> รายงานปิดเหตุการณ์ภัยคุกคามแล้ว	<input type="checkbox"/> อื่น ๆ: โปรดระบุ
ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว	
<input type="checkbox"/> ยังไม่ได้ดำเนินการแก้ไขใด ๆ	<input type="checkbox"/> ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว
<input type="checkbox"/> ตรวจสอบข้อมูลจราจร (Log) แล้ว	<input type="checkbox"/> ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว
<input type="checkbox"/> กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว	
<input type="checkbox"/> รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ	
ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)	
โปรดระบุ	

ง๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้โจมตี: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

- ระบบล่ม รายการข้อมูลจรรยาทางคอมพิวเตอร์ที่ผิดปกติ
- บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
- การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
- ประสิทธิภาพของระบบต่ำลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
- การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
- การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
- การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
- การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
- การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
- การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
- รูปแบบการใช้งานที่ผิดปกติ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
- ความพยายามที่จะเขียนไฟล์ของระบบ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
- การแก้ไขหรือลบข้อมูลที่ผิดปกติ การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
- ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ การใช้งานหรือมีกิจกรรมที่เกิดขึ้นในเวลาที่ไม่ปกติ
- การแก้ไขหน้าเว็บ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
- การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
- การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
- สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)

โปรดระบุ

ง๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง๒. ข้อมูลการระงับ ปรามปราม และฟื้นฟู

ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ

ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์^๕

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) / เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์^๖

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

^๕ หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตราการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

^๖ ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒