แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานศาลรัฐธรรมนูญ

๑. หลักการและเหตุผล[1]

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานศาลรัฐธรรมนูญฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานศาลรัฐธรรมนูญด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในสำนักงานศาลรัฐธรรมนูญ โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้สำนักงานศาลรัฐธรรมนูญ การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้[2] รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย[3] เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของสำนักงานศาลรัฐธรรมนูญ

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของสำนักงานศาลรัฐธรรมนูญ รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

กลุ่มงานพัฒนามาตรฐานดิจิทัล สำนักเทคโนโลยีดิจิทัล มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer) ของสำนักงานศาลรัฐธรรมนูญ

๕. หน้าที่ในการดำเนินการตามแผน

สำนักเทคโนโลยีดิจิทัล มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กลุ่มงานพัฒนามาตรฐานดิจิทัล และกลุ่มงานนวัตกรรมพัฒนา

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานศาลรัฐธรรมนูญ

๖.๒ นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานศาลรัฐธรรมนูญ

---

[1] ส่วนนี้ ให้หน่วยงานของท่านอธิบายถึงเหตุผลความจำเป็นที่หน่วยงานของท่านต้องมีแผนรับมือฉบับนี้ ยกตัวอย่างเช่น เหตุผลความจำเป็นทางกฎหมาย (ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒) หรือเหตุผลความจำเป็นทางนโยบาย ระเบียบ หรือข้อบังคับ จากการที่หน่วยงานควบคุมหรือกำกับดูแลออกข้อกำหนดให้หน่วยงานภายใต้การควบคุมหรือกำกับดูแลต้องมีการจัดทำแผนรับมือฯ หรือผู้บริหารสูงสุดของหน่วยงานมีการออกนโยบายแนวปฏิบัติให้หน่วยงานจะต้องจัดทำแผนรับมือฯ เป็นต้น

[2] โดยปกติ องค์กรมักจะกำหนดขอบเขตของระบบสารสนเทศที่จะต้องรักษาความมั่นคงปลอดภัยไซเบอร์ไว้ในนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร หรือแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

[3] หน่วยงานอาจจัดทำแผนการติดต่อสื่อสารไว้เป็นส่วนหนึ่งของแผนรับมือฯ ฉบับนี้ หรือแยกออกไปเป็นอีกแผนหนึ่งก็ได้

๗. นิยาม[4]

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)[5]

สำนักงานศาลรัฐธรรมนูญ ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะ[6]แบบรวมศูนย์ประกอบด้วย

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล โทร. ๐๒-๑๔๑๗๗๐๑	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	ผู้อำนวยการกลุ่มงานพัฒนามาตรฐานดิจิทัล โทร. ๐๒-๑๔๑๗๖๑๒	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นักวิชาการคอมพิวเตอร์ กลุ่มงานพัฒนามาตรฐานดิจิทัล โทร. ๐๒-๑๔๑๗๗๘๐	เจ้าหน้าที่รับมือฯ (Incident lead)	ทำหน้าที่ช่วยเหลือหน่วยงานเจ้าของระบบงานหรือผู้ดูแลระบบงานให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	ผู้อำนวยการกลุ่มงาน/นักวิชาการคอมพิวเตอร์ กลุ่มงานนวัตกรรมพัฒนา โทร. ๐๒-๑๔๑๗๗๗๓	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

[4]นอกจากนิยามตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ แล้ว หน่วยงานควรกำหนดนิยามตามบริบทของหน่วยงาน เช่น กฎหมายอื่นที่เกี่ยวข้อง กฎ ระเบียบ ข้อบังคับ รวมถึงนโยบายและแนวปฏิบัติของหน่วยงานด้วย

[5]หน่วยงานอาจพิจารณาใช้วิธีการในการกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ตามแนวปฏิบัติอื่นได้ตามความเหมาะสมโดยในตัวอย่างนี้ เลือกที่จะใช้หลักการจัดโครงสร้างตาม NIST SP ๘๐๐-๖๑r๒ข้อ ๒.๔.๓ หน้าที่ ๑๖ศึกษาเพิ่มเติมได้ที่ https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.๘๐๐-๖๑r๒.pdf

[6]หน่วยงานอาจเลือกใช้โมเดลโครงสร้างทีมรับมือฯ แบบรวมศูนย์ (Centralize)แบบกระจาย (Distributed)แบบให้คำปรึกษา (Coordinating)หรือแบบอื่นๆ ตามบริบทของหน่วยงานที่อาจแตกต่างกัน ทั้งนี้ ท่านสามารถศึกษาเพิ่มเติมได้ที่NIST SP ๘๐๐-๖๑r๒ ข้อที่ ๒.๔ หน้าที่ ๑๓ https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.๘๐๐-๖๑r๒.pdf

๙. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังนี้

๙.๑ ขั้นการเตรียมการ เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) โดยดำเนินการตรวจสอบและปิดช่องโหว่จากข้อมูลที่คาดว่าเป็นช่องโหว่ที่ใช้ในการโจมตีทางไซเบอร์ ได้แก่

(๒.๑) มีการปรับค่าการทำงานของระบบ Next-Gen Firewall เพื่อควบคุมช่องทางการเข้าถึงจากระบบเครือข่ายภายนอก (Internet) โดยเปิดเฉพาะบริการที่จำเป็นสำหรับการให้บริการจากภายนอกเท่านั้น เช่น http, https และมีการกำหนดนโยบาย (Policy) ระบบ NG-FW ของสำนักงานฯ ให้มีการแยก Policy การรักษาความปลอดภัยในแต่ละระบบงาน (Application Server) ที่แตกต่างกันตามความจำเป็นและเหมาะสมในการรักษาความปลอดภัย เพื่อควบคุมความปลอดภัยให้รัดกุมขึ้น

(๒.๒) สำนักงานฯ มีการติดตั้งระบบรักษาความปลอดภัยจากการโจมตีทางเว็บไซต์หรือเว็บแอพพลิเคชั่นในรูปแบบต่างๆ (Web Application Firewall : WAF) รวมถึงการป้องกันการเข้าถึงเว็บไซต์ที่มีความเสี่ยงจากบุคลากรในสำนักงานฯ เพิ่มเติม เพื่อเพิ่มประสิทธิภาพการป้องกันภัยทางไซเบอร์ของสำนักงานฯ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT โดยสำนักงานฯ มีระบบการป้องกันด้วยระบบตรวจสอบความปลอดภัยด้วยการตรวจจับและหยุดยั้งการโจมตีแบบ (Intrusion Prevention System : IPS) เพื่อป้องกันการโจมตีที่อาจเกิดขึ้นในระบบเครือข่ายในรูปแบบการป้องกันระดับสูง (High Security)

๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

เป็นการดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and analysis) โดยสำนักงานฯ ได้ดำเนินการกำหนดแนวทาง เฝ้าระวังระบบเครือข่ายและตรวจสอบการทำงานของอุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall) และ อุปกรณ์ป้องกันการบุกรุกเครือข่าย (Firewall) ทุกวันและรายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) เกี่ยวกับผลการตรวจสอบ Log file และพฤติการณ์แวดล้อมในระบบทุกสัปดาห์ ทั้งนี้ เมื่อพบความผิดปกติหรือการจู่โจมที่เป็น Critical กลุ่มงานพัฒนามาตรฐานดิจิทัล ได้พิจารณาแนวทางป้องกัน ดังนี้

(๑) กรณีพบการโจมตีระบบสารสนเทศของสำนักงานฯ กลุ่มงานพัฒนามาตรฐานดิจิทัล ได้ประสานไปยังผู้ดูแลระบบที่เป็นเป้าหมายการโจมตี ให้เฝ้าระวังและตรวจสอบความผิดปกติของระบบสารสนเทศที่ดูแลอยู่ พร้อมแนะนำให้สำรองข้อมูลที่สำคัญป้องกันการสูญหายของข้อมูล

(๒) กรณีพบเป็นเครื่องของเจ้าหน้าที่ที่ติดไวรัสคอมพิวเตอร์ หรือมีพฤติกรรมเสี่ยงที่พยายามโจมตีเครื่องคอมพิวเตอร์อื่นภายนอกองค์กร กลุ่มงานพัฒนามาตรฐานดิจิทัลจะตัดเครื่องคอมพิวเตอร์ดังกล่าวออกจากระบบเครือข่ายและให้เจ้าหน้าที่สำนักเทคโนโลยีดิจิทัลดำเนินการลบไวรัสคอมพิวเตอร์หรือแก้ไขความเสี่ยงอื่นๆ ก่อนที่จะเชื่อมโยงเข้าสู่ระบบเครือข่ายอีกครั้ง

๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก

ทั้งนี้ ในด้านการสำรองข้อมูล สำนักงานศาลรัฐธรรมนูญได้ดำเนินการสำรองอย่างน้อย ๓ ชุด โดยมีการ Backup แบบ Offline และให้สำเนาข้อมูลอยู่ในอุปกรณ์จัดเก็บข้อมูล หรือ Cloud ที่แยกออกจากระบบงาน และไม่สามารถเข้าถึงได้จากระบบงานปกติ ดังนี้

(๖) สำนักงานฯ มีการทำการป้องการการสูญหายของข้อมูลและระบบสารสนเทศ โดยใช้เทคโนโลยีบนระบบคอมพิวเตอร์ประเภท HCI ในระดับที่หนึ่ง และ

(๗) มีการจัดทำระบบสำรองระดับที่สอง โดยใช้ระบบสำรองข้อมูลร่วมกับอุปกรณ์จัดเก็บข้อมูลภายนอก (External Storage) สำหรับสำรองข้อมูลและระบบงานสารสนเทศ (Backup / Archive File) จากภายในระบบ HCI ไปจัดเก็บใน External Storage เพื่อรองรับเหตุฉุกเฉินที่อาจเกิดขึ้นกับระบบ HCI หลัก ทั้งนี้ สำนักงานฯ ได้ดำเนินการสำรองข้อมูลและระบบงานที่อยู่ภายในระบบ HCI จากส่วนกลางไปไว้ที่อาคารโทรคมนาคมแห่งชาติ บางรัก (DR Site)

(๘) แนวทางในการทำระบบสำรองข้อมูลระดับที่สาม เพื่อแยกการจัดเก็บข้อมูลสำรองออกจากการจากเชื่อมต่อ (Offline backup) อยู่ระหว่างการวิเคราะห์และหารือในทางปฏิบัติ

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) โดยดำเนินการ ดังนี้

(๑) ด้านการจัดเก็บข้อมูลจราจร (Log)

สำนักงานฯ มีการจัดเก็บข้อมูลจราจร (Log) ในการใช้บริการเครือข่ายอินเตอร์เน็ตของสำนักงาน เพื่อการตรวจสอบ วิเคราะห์ความปลอดภัยและความเสี่ยงในการใช้งาน โดยตรวจสอบข้อมูลการเข้าถึงระบบงานจากระบบเครือข่ายอินเตอร์เน็ตและระบบเครือข่าย VPN อย่างสม่ำเสมอ จากอุปกรณ์รักษาความปลอดภัยเครือข่าย (Firewall) เพื่อป้องกันความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของหน่วยงาน

อย่างสม่ำเสมอ และไม่อนุญาตให้มีการเข้าถึงเครือข่ายจากทางไกล (Remote Desktop Protocol) ซึ่งเป็นนโยบายที่ผู้บริหารได้เคยให้ไว้เป็นแนวทางในการปฏิบัติ

(๒) ด้านการพิสูจน์ตัวตน (Authentication)

สำนักงานฯ ได้ดำเนินการจัดทำระบบการพิสูจน์ตัวตนแบบ ๒FA สำหรับผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายภายในสำนักงานฯ จากระบบเครือข่ายอินเตอร์เน็ตภายนอกด้วยวิธีการ VPN โดยผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายภายในสำนักงานฯ จำเป็นต้องยืนยันการเข้าถึง ๒ ระดับ ด้วยรหัสผ่านและการยืนยัน token ผ่าน Email เพื่อเป็นการยืนยันตัวตนแบบ Multi-Factor Authentication และตั้งรหัสผ่านให้ซับซ้อน คาดเดาได้ยาก

(๓) ด้านการกำหนดนโยบายความปลอดภัย

สำนักงานฯ มีการกำหนดนโยบายการปรับปรุงคุณสมบัติด้านการรักษาความปลอดภัยของระบบปฏิบัติการสำหรับให้บริการระบบงานสารสนเทศ (Application) ให้มีการปรับปรุงคุณสมบัติ (Patch) ตามข้อแนะนำของเจ้าของผลิตภัณฑ์ และทำการทดสอบผลกระทบก่อนการให้บริการระบบงานให้เป็นปัจจุบันอยู่เสมอ

(๔) ด้านระบบการป้องกันไวรัส

สำนักงานฯ มีระบบการป้องกันไวรัสคอมพิวเตอร์จากส่วนกลาง และมีนโยบายควบคุมการปรับปรุงคุณสมบัติการป้องกันไวรัสให้เป็นปัจจุบันอยู่เสมอ รวมถึงการตรวจสอบรายงานการตรวจจับและการทำงานของระบบจากระบบจัดทำรายงานส่วนกลางอยู่เสมอ โดยดำเนินการจัดหาอุปกรณ์และติดตั้งโปรแกรมป้องกันมัลแวร์ โดยใช้ Endpoint Detection and Response ยี่ห้อ Fortinet รุ่น FortiEDR เพื่อใช้งานเป็นระบบป้องกันภัยคุกคามจากภายนอก ผ่านระบบ Cloud

(๕) ด้านการควบคุมการเข้าถึงระบบจากนโยบาย Work from Home

(๕.๑) สำนักงานฯ มีการกำหนดให้เครื่องของผู้ดูแลระบบ (Admin) และเครื่องคอมพิวเตอร์แม่ข่ายมีการติดตั้งโปรแกรมป้องกันไวรัส ทั้งจากช่องทางการเข้าถึงเครือข่ายภายในผ่านระบบเครือข่ายอินเตอร์เน็ต หรือเข้าถึงด้วยระบบ VPN เพื่อรักษาความปลอดภัยและป้องกันปัญหาที่อาจจะเกิดจากเครื่องคอมฯ ของผู้ดูแลระบบมาสู่ระบบเครือข่ายภายใน

(๕.๒) การเข้าถึงเครือข่ายภายในผ่านการเชื่อมต่อด้วยช่องทาง VPN จะมีการกำหนดนโยบายการเข้าถึงที่อนุญาตให้เฉพาะรายบุคคลที่จำเป็นเฉพาะระบบงานที่เกี่ยวข้องเท่านั้น ไม่สามารถเชื่อมต่อจากระบบเครือข่ายอินเตอร์เน็ตได้โดยตรง และไม่สามารถเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายหรือระบบงานที่ตนไม่เกี่ยวข้องได้

(๖) ด้านการปรับคุณสมบัติการรักษาความปลอดภัย

สำนักงานฯ มีการติดตั้งระบบตรวจสอบพฤติกรรมการใช้งานของพนักงานเพื่อปรับแต่งระบบการรักษาความปลอดภัยให้เหมาะสมและมีประสิทธิภาพอยู่เสมอ โดยเพิ่ม Indicators of Compromise (IOCs) ลงในอุปกรณ์รักษาความมั่นคงปลอดภัยของระบบเพื่อเป็นการป้องกันการโจมตีอีกทาง

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber security Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๘
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๒)
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ ๙.๑ (๓)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๑)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๒) (๗)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๓)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๔)
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	ข้อที่ ๙.๓ (๕)
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔