ระบบรักษาความปลอดภัยด้านสารสนเทศ กรมทรัพยากรทางทะเลและชายฝั่ง

สารบัญ

ระบบความปลอดภัยกรมทรัพยากรทางทะเลและชายฝั่ง

๑. บทนำ

ปัจจุบันทุกหน่วยงานราชการ ได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานเพิ่มมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและการสร้างข้อมูลสารสนเทศและฐานข้อมูลต่างๆ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ นับวันจะมีจำนวนมากขึ้น ดังนั้น การจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้รวดเร็ว แม่นยำ ถูกต้องและมีประสิทธิภาพจึงนับเป็นสิ่งที่ต้องให้ความสำคัญเพิ่มมากขึ้นไปด้วย

กรมทรัพยากรทางทะเลและชายฝั่ง ถือเป็นหน่วยงานราชการที่มีฐานข้อมูล องค์ความรู้เฉพาะด้านและมีข้อมูลที่หลากหลาย จำเป็นต้องดำเนินการเก็บข้อมูลเป็นประจำอย่างต่อเนื่อง และได้นำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานเพิ่มมากขึ้น เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของทั้งหน่วยงานและเครือข่ายอนุรักษ์ที่เกี่ยวข้อง ดังนั้น การป้องกันระบบสารสนเทศจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จาก Hacker Malware Trojan และอื่นๆ จึงมีความจำเป็นอย่างยิ่งที่จะต้องมีบริหารจัดการที่ดี โดยการพัฒนาระบบรักษาความปลอดภัยให้มีประสิทธิภาพ รองรับการดำเนินงานในอนาคตได้อย่างเพียงพอ และสามารถป้องกันและรักษาระบบสารสนเทศของกรมให้มั่นคง ปลอดภัย และสามารถใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

๒. วัตถุประสงค์

๑. เพื่อดูแลรักษา เฝ้าระวัง และป้องกันการบุกรุกโจมตีที่อาจมีต่อระบบสารสนเทศของกรม ทั้งจากปัจจัยภายในและภายนอก และทั้งจากไวรัสคอมพิวเตอร์ Hacker Malware Trojan และอื่นๆ

๒. เพื่อลดความเสียหายที่จะอาจเกิดต่อระบบเทคโนโลยีสารสนเทศ ฐานข้อมูล และข้อมูลสารสนเทศอื่นๆ ของกรม และสามารถตรวจสอบ เฝ้าระวัง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๓. เพื่อการให้ใช้งานระบบเครือข่าย (Internet) ที่มีความปลอดภัย น่าเชื่อถือ

๓. ระบบรักษาความปลอดภัยของกรม**ทรัพยากรทางททะเลและชายฝั่ง**

เนื่องจากภารกิจของกรมทรัพยากรทางทะเลและชายฝั่งที่มีความหลากหลาย และมีการพัฒนาระบบเทคโนโลยีสารสนเทศเข้ามาช่วยอำนวยความสะดวกในการปฏิบัติงานเพิ่มมากขึ้น เมื่อมีระบบและมีการใช้งานที่เพิ่มมากขึ้น ความเสี่ยงในการถูกโจมตีก็จะมีเพิ่มมากขึ้นไปด้วย ซึ่งจำเป็นอย่างยิ่งที่กรมฯ จะต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา การลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบ การประเมินความเสี่ยงด้านสารสนเทศ และการกู้คืนระบบ อันจะส่งต่อความเชื่อมั่นในการใช้งานระบบเทคโนโลยีสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่ง ให้สามารถใช้ระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุดได้ตามวัตถุประสงค์

การรักษาความปลอดภัยด้านสารสนเทศของกรมทรัพยากรทางทะเลและชายฝั่ง มี ๔ ด้านหลัก ดังนี้

๓.๑ การรักษาความปลอดภัยจากไวรัสคอมพิวเตอร์ Hacker Malware Trojan (Attack)

๓.๒ การรักษาความปลอดภัยด้านฐานข้อมูล (Database)

๓.๓ การรักษาความปลอดภัยด้านระบบเครือข่าย (Network)

๓.๔ การรักษาความปลอดภัยด้านการยืนยันตัวบุคคล (Authen)

๔. มาตรการควบคุม เพื่อปกป้องระบบสารสนเทศ

๔.๑ วิเคราะห์สาเหตุวิธีหรือขั้นตอนของความเสี่ยงต่อระบบสารสนเทศ เพื่อวางแผนการป้องกันความเสี่ยงนั้น ๆ อย่างเป็นระบบ

๔.๒ ลำดับความสำคัญที่จะดำเนินการกับความเสี่ยงที่สำคัญๆ ก่อน หรือป้องกันในจุดที่จะก่อให้เกิดความเสียหายรุนแรง ตามลำดับก่อนหลัง

๔.๓ นำเสนอข้อมูลตัวชี้วัดต่างๆ ที่เกี่ยวข้อง เช่น มูลค่าความเสียหายหากถูกโจมตีจากจุดอ่อนต่างๆ ความสำคัญของระบบ หรือข้อมูลในองค์กร และข้อมูลอื่นๆ ที่สามารถประเมินได้ให้กับผู้บริหาร ฝ่ายไอที ผู้ตรวจสอบ และบุคคลต่างๆ ที่เกี่ยวกับความปลอดภัยเพื่อช่วยกันประเมินและปรับปรุงข้อมูลนั้นได้รวดเร็วขึ้น

๔.๔ ดำเนินการตรวจสอบอย่างต่อเนื่อง เพื่อทดสอบและตรวจสอบประสิทธิผลของมาตรการรักษาความปลอดภัยในปัจจุบัน

๕. มาตรการป้องกันระบบสารสนเทศ

การกำหนดมาตรการสำคัญสำหรับป้องกันระบบสารสนเทศที่มีประสิทธิภาพ มีดังนี้

๕.๑ จัดทำรายการจัดเก็บชื่ออุปกรณ์ที่ได้มีการเข้าถึงเครือข่ายภายในองค์กรทั้งที่ได้รับอนุญาต และอุปกรณ์แปลกปลอมอื่นๆ

๕.๒ จัดทำรายการชื่อโปรแกรมที่ได้มีการติดตั้งภายในองค์กร ทั้งที่ได้รับอนุญาต และไม่ได้รับอนุญาต

๕.๓ ปรับแต่งอุปกรณ์ และโปรแกรมต่างๆ ในองค์กรให้มีความมั่นคงปลอดภัย (Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, Servers, Firewall)

๕.๔ ตรวจสอบ วิเคราะห์ และแก้ไขช่องโหว่ต่างๆ ของระบบอย่างต่อเนื่อง

๕.๕ ป้องกันอุปกรณ์ และโปรแกรมต่างๆ จากโปรแกรมไม่ประสงค์ดี

๕.๖ ตรวจสอบ ป้องกัน และแก้ไขจุดอ่อนของโปรแกรมที่พัฒนาขึ้น หรือนำมาใช้งาน

๕.๗ ตรวจสอบ และป้องกันการใช้งานเครือข่ายไร้สายของอุปกรณ์ที่ไม่ได้รับอนุญาต

๕.๘ การสำรองข้อมูลที่สำคัญๆ และมีการซ้อมการกู้คืนระบบอย่างสม่ำเสมอ

๕.๙ จัดฝึกอบรมหรือทำความเข้าใจกับช่องโหว่ต่างๆ ที่มีอยู่ในองค์กร

๕.๑๐ ปรับแต่งอุปกรณ์เครือข่ายให้มีการใช้งานตามที่ได้กำหนดไว้ เช่น กฎของไฟร์วอลล์ การตั้งค่าเส้นทางอุปกรณ์ค้นหาเส้นทาง

๕.๑๑ จำกัด และควบคุมการใช้งานเครือข่ายและบริการต่างๆ อย่างเหมาะสม

๕.๑๒ ควบคุมผู้ใช้งานที่ได้สิทธิ์สูง เช่น สิทธิ์เป็นผู้ดูแลระบบ

๕.๑๓ ควบคุมการเชื่อมต่อของแต่ละวงเครือข่ายที่มีระดับความลับของข้อมูลแตกต่างกัน

๕.๑๔ ตรวจสอบ และวิเคราะห์ข้อมูลสำหรับการตรวจสอบ

๕.๑๕ ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความลับในลำดับชั้นต่างๆ ตามที่ได้รับอนุญาต

๕.๑๖ ควบคุม และตรวจสอบชื่อผู้ใช้งานในระบบต่างๆ

๕.๑๗ ควบคุม และตรวจสอบข้อมูลที่ผ่านเข้าออกระบบ

๕.๑๘ ควบคุม จัดการ และตอบสนอง ต่อเหตุการณ์ต่างๆ ทางคอมพิวเตอร์

๕.๑๙ ป้องกัน และควบคุมภัยคุมคามในรูปแบบอื่นๆ

๕.๒๐ ดำเนินการตรวจสอบ และซักซ้อมการทดสอบเจาะบุกรุกระบบ