มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์

มาตรการและวิธีปฏิบัติการรักษาความปลอดภัยเว็บไซต์ของกระทรวงมหาดไทย ดังนี้

1. มาตรการที่จังหวัดต้องดำเนินการในการดูแลเว็บไซต์

1.1 การป้องกันและรักษาความปลอดภัยของข้อมูลและเว็บไซต์ของจังหวัด ให้ผู้ดูแลเว็บไซต์กำหนดสิทธิการใช้งานเครื่องแม่ข่าย (Server) ระบบงาน Application Server และเครื่องแม่ข่าย(Server) ฐานข้อมูล Database Server ที่ติดตั้ง ณ จังหวัด ดังนี้

1.1.1 การใช้งานเว็บไซต์ ต้องกำหนดให้มีผู้รับผิดชอบดูแลระบบ (ADMIN)

1.1.2 ให้บริหารจัดการ ติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

1.1.3 การกำหนดค่าเริ่มต้นพื้นฐานของการใช้งานเว็บจะต้องเป็นการปฏิเสธทั้งหมด เปิดให้ใช้เฉพาะที่จำเป็นใช้งาน

1.1.4 ทุกเส้นทางเชื่อมต่ออินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาต จะต้องถูกบล็อก (Block) โดยระบบรักษาความปลอดภัยเครือข่ายของหน่วยงาน

1.1.5 ค่าการเปลี่ยนแปลงทั้งหมดในไฟร์วอลล์ เช่น ค่าพารามิเตอร์ การกำหนดค่าใช้บริการ และการเชื่อมต่อที่อนุญาต จะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง

1.1.6 การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

1.1.7 ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน

1.1.8 ระมัดระวังการดาวน์โหลด โปรแกรมใช้งานจากระบบอินเตอร์เน็ต (Internet) การดาวน์โหลด (Download) การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องตรวจสอบความถูกต้องปลอดภัยก่อนนำไปใช้งาน

1.1.9 การกำหนดค่าการให้บริการของเครื่องแม่ข่าย (Server) ที่ใช้งานเว็บไซต์จะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยข้อกำหนดนโยบายจะต้องถูกระบุให้กับเครื่องแม่ข่าย (Server) เป็นรายเครื่องที่ให้บริการจริง

1.1.10 จะต้องมีการสำรองข้อมูลและกำหนดค่าต่าง ๆ ของเครื่องแม่ข่าย (Server) คอมพิวเตอร์เป็นประจำทุกเดือน หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

1.1.11 การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่าย (Server) หรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องแม่ข่าย (Server) และอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากจังหวัด

1.1.12 ดูแล บำรุงรักษา เครื่องแม่ข่าย (Server) คอมพิวเตอร์ให้ใช้งานอย่างมีประสิทธิภาพ

1.1.13 ต้องทำการตรวจสอบการเข้าใช้งานเครื่องแม่ข่าย (Server) จากภายนอกว่ามีการใช้งานที่ผิดปกติหรือไม่เป็นประจำ

1.1.14 จัดเจ้าหน้าที่ตรวจสอบและเฝ้าระเว็บไซต์ของจังหวัดหากตรวจพบการบุกรุกหรือโจมตีให้ทำการระงับยับยังหรือปิดระบบในทันที่และทำการแก้ไขโดยด่วน

1.1.15 ให้มีการเปลี่ยนรหัสผ่านในการเข้าถึงระบบคอมพิวเตอร์โดยตั้งรหัสผ่านให้ยาก เช่น อักษรตัวใหญ่ผสมกับอักษรตัวเล็กและตัวเลขสลับกันไปโดยให้มีการเปลี่ยนอย่างน้อยทุก ๆ 2 เดือนหรือเร็วกว่านั้น

1.1.16 ให้เลือกใช้โปรแกรมในการพัฒนาเว็บไซต์ที่มีระบบป้องกันการบุกรุก/โจมตีและมีการ ปรับปรุง (Update) ให้เป็นปัจจุบันอย่างต่อเนื่อง

1.1.17 ให้จัดทำระบบสำรองข้อมูลเมื่อเกิดเหตุสุดวิสัยสามารถเปิดใช้งานได้ภายใน 3 - 5 ชั่วโมง

1.2 การเข้าถึงข้อมูลการและการดูแลเครื่องแม่ข่าย (Server)

1.2.1 จังหวัดที่ได้รับการติดตั้งระบบรักษาความปลอดภัยเครือข่ายสารสนเทศและการสื่อสารของกระทรวงมหาดไทยแล้วให้ดำเนินการนำเครื่องแม่ข่าย (Server) ไปติดตั้งภายในโซนรักษาความปลอดภัย (DMZ)

1.2.2 จังหวัดจะต้องกำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมเครื่องแม่ข่าย (Server)

1.2.3 ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากจังหวัด และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

1.2.4 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อจังหวัด และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำของระบบและผู้ใช้บริการอื่น ๆ

1.2.5 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (System Administrator)

1.2.6 มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการเครื่องแม่ข่าย (Server) ได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะเครื่องแม่ข่าย(Server) ข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องจำกัดเส้นทางการเข้าถึงเครื่องแม่ข่าย(Server) ที่มีการใช้งานร่วมกัน

(3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย(Server) เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

(4) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรม ประสงค์ร้าย (Malware) ด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

(7) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(8) กำหนดให้มีผู้รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

1.3 จังหวัดจะต้องกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องแม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

1.3.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องแม่ข่าย(Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากจังหวัด

1.3.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

1.3.3 วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากจังหวัด

1.3.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

1.3.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากจังหวัดก่อน

1.3.6 ห้องเครื่องแม่ข่าย(Server) จะมีระบบรักษาความปลอดภัย คือ มีระบบตรวจสอบการเข้าออกห้อง ต้องมีการตรวจสอบก่อนว่ามีสิทธิ์ในการเข้าห้องหรือไม่โดยมีประกาศเงื่อนไขการเข้าใช้ห้องติดไว้ที่หน้าห้องเครื่องแม่ข่ายให้ทุกคนทราบ

2. กระทรวงมหาดไทยจะดำเนินการติดตามประเมินผลการดูแลรักษาและเฝ้าระวังเว็บไซต์และเครื่องแม่ข่าย (Server) โดยจัดทำแบบสำรวจ สอบถาม ถึงวิธีการดูแลและเฝ้าระวัง

3. กระทรวงจะดำเนินการประเมินความเสี่ยงของเว็บไซต์จังหวัดที่มีความเสี่ยงต่อการโจมตีหรือปรับเปลี่ยนข้อมูลในเว็บไซต์พร้อมทั้งดำเนินการระงับยับยั้งเว็บไซต์ที่มีความเสียงเพื่อดำการแก้ไขให้ปลอดภัยต่อไป

4. วิธีดำเนินการของเจ้าหน้าที่ผู้ดูแลเว็บไซต์

4.1 ตรวจสอบเว็บไซต์ของหน่วยงานทุกวัน อย่างน้อยวันละ 3 ครั้ง โดยเฉพาะในช่วงวันหยุดราชการให้มีเจ้าหน้าที่ตรวจสอบเฝ้าระวัง หากตรวจพบการบุกรุกโจมตีให้ทำการแก้ไขในทันที

4.2 ตรวจสอบ ป้องกัน และแก้ไขจุดอ่อนของโปรแกรมที่พัฒนาขึ้น หรือนำมาใช้งาน (Application Software Security) หากตรวจพบให้ดำเนินการแก้ไขทันที

4.3 ป้องกันอุปกรณ์ และโปรแกรมต่าง ๆ จากโปรแกรมไม่ประสงค์ดี (Malware Defenses)

4.4 มีการกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์ ควบคุมผู้ใช้งานที่ได้สิทธิ์สูง เช่น สิทธิ์เป็นผู้ดูแลระบบ (Controlled Use of Administrative Privileges)

4.5 ทำการสำรองข้อมูลที่สำคัญ ๆ และมีการซ้อมการกู้คืนระบบอย่างสม่ำเสมอ (Data Recovery Capability) โดยต้องสามารถกู้คืนได้ทันทีที่ระบบถูกโจมตี

4.6 ตรวจสอบ วิเคราะห์ และแก้ไขช่องโหว่ต่างๆ ของระบบอย่างต่อเนื่อง (Continuous Vulnerability Assessment and Remediation)

4.7 ปรับแต่งอุปกรณ์เครือข่ายให้มีการใช้งานตามที่ได้กำหนดไว้ เช่น กฎของไฟร์วอลล์ การตั้งค่าเส้นทางอุปกรณ์ค้นหาเส้นทาง (Secure Configurations for Network Devices such as Firewalls, Routers, and Switches)

4.8 ควบคุม และตรวจสอบข้อมูลที่ผ่านเข้าออกระบบ (Data Loss Prevention)

4.9 จำกัด และควบคุมการใช้งาน การเข้าถึงเครื่องแม่ข่าย (Server) และบริการต่าง ๆ อย่างเหมาะสม

4.10 ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความลับในลำดับชั้นต่างๆ ตามที่ได้รับอนุญาต(Controlled Access Based on the Need to Know)

4.11 ให้ทำการเปลี่ยนรหัสผ่านของผู้ดูแลระบบทุก ๆ 2 เดือนหรือเร็วกว่านั้น โดยการตั้งรหัสผ่านให้มีความยาว อักขระพิเศษ ตัวอักษร และตัวเลข ผสมกัน

4.12 ให้เจ้าหน้าที่ติดตามและแจ้งเหตุภัยคุกคามการแจ้งเตือนภัยจากช่องโหว่ต่าง ๆ การตรวจสอบช่องโหว่และข้อแนะนำในการป้องกันและแก้ไขจากเว็บไซต์ของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
