บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มบริหารจัดการระบบเครือข่ายฯ โทร. ๔๐๔๐
ที่ กษ ๐๕๒๓.๔/ ๑๘๓ **วันที่** ๒๘ กุมภาพันธ์ ๒๕๖๗
เรื่อง แนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง พ.ศ. ๒๕๖๗

เรียน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง (นายถาวร ทันใจ)

๑. เรื่องเดิม

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศทส.) ได้จัดทำแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง เพื่อสร้างความตระหนักรู้ ให้แก่บุคลากรของหน่วยงาน และแนะนำวิธีป้องกัน แก้ปัญหา รับมือภัยอันตรายบนโลกออนไลน์ให้บุคลากรปฏิบัติได้อย่างถูกต้อง สามารถป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตีทางไซเบอร์ได้ และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง (นายวิชาญ อิงศรีสว่าง) เห็นชอบแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง พ.ศ. ๒๕๖๓ และมอบให้ ศทส. แจ้งแนวปฏิบัติดังกล่าวให้หน่วยงานภายใต้กรมประมงรับทราบตามเอกสารแนบ ๑

๒. ข้อรายงาน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ประชุมหารือพิจารณาแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง แล้วพบว่าในปัจจุบันเทคโนโลยีด้านคอมพิวเตอร์มีการปรับเปลี่ยนไปมีการนำอุปกรณ์เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) และอุปกรณ์ต่อพ่วงที่สามารถเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ได้โดยตรงในจำนวนที่สูงขึ้น และมีการเปลี่ยนแปลงของหน่วยงานภายนอกที่รับผิดชอบด้านไซเบอร์จึงได้จัดทำร่างแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง พ.ศ. ๒๕๖๗ ตามเอกสารแนบ ๒ เพื่อให้แนวปฏิบัติมีความทันสมัยสอดคล้องกับการใช้งานเทคโนโลยีสารสนเทศในปัจจุบัน

๓. เรื่องเสนอเพื่อพิจารณา

ในการนี้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พิจารณาเพื่อประโยชน์ของราชการจึงได้จัดทำร่างแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมงให้มีความทันสมัยสอดคล้องกับการใช้งานเทคโนโลยีสารสนเทศในปัจจุบัน ตามเอกสารแนบ ๒ และแจ้งเวียนให้หน่วยงานภายใต้กรมประมงทราบและปฏิบัติ

จึงเรียนมาเพื่อโปรดพิจารณาให้ความเห็นชอบแนวปฏิบัติฯ เพื่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะได้เผยแพร่ให้หน่วยงานทราบและปฏิบัติในส่วนที่เกี่ยวข้องต่อไป

(นายพลพิศิลป์ สุวรรณชัย)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(นายศุภกิตติ์ ใสกระจ่าง)
เลขานุการกรม
๒๘ ก.พ. ๒๕๖๗

เรียน ศทส.
/ ๑ มี.ค. ๒๕๖๗

(นายถาวร ทันใจ)
รองอธิบดีกรมประมง

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร คปท. โทร. ๐-๒๙๔๐-๕๖๐๒, ๔๐๔๐-๔๒

ที่ กษ ๐๕๒๓.๔ / ๘๙๒ **วันที่** ๑๑ สิงหาคม ๒๕๖๓ 17 ส.ค. 2563 10.49

เรื่อง ขอความเห็นชอบแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ของกรมประมง

เรียน ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง (นายวิชาญ อิงศรีสว่าง)

ด้วยปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนเพิ่มสูงขึ้นและทวีความรุนแรงขึ้นตามลำดับ การโจมตีมีความหลากหลาย มีรูปแบบที่ซับซ้อน มุ่งเน้นการโจมตีไปสู่ข้อมูลที่มีความสำคัญ ทำให้ส่งผลกระทบและสร้างความเสียหายทั้งต่อระดับหน่วยงานและระดับประเทศ ซึ่งรัฐบาลได้ให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก จึงได้มีการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อกำหนดแนวทางและมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรม ซึ่งหน่วยงานรัฐจะต้องมีการป้องกันรับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ

ในการนี้ เพื่อเตรียมพร้อมรับมือกับปัญหาภัยคุกคามดังกล่าว และเป็นการดำเนินการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงได้จัดทำแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสร้างความตระหนักรู้ (Awareness) ให้แก่บุคลากรของหน่วยงาน อีกทั้งแนะนำวิธีป้องกัน แก้ปัญหา รับมือภัยอันตรายบนโลกออนไลน์ให้บุคลากรปฏิบัติได้อย่างถูกต้อง สามารถป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตีทางไซเบอร์ได้ รายละเอียดตามเอกสารแนบพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณาให้ความเห็นชอบแนวปฏิบัติฯ เพื่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะได้เผยแพร่ให้หน่วยงานในสังกัดกรมประมงทราบและปฏิบัติในส่วนที่เกี่ยวข้องต่อไป

(นายศุภวัฒฑ์ โกมลมาลย์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

(นางศิริจันทร์ แย้มแสน)
เจ้าพนักงานธุรการชำนาญงาน
ปฏิบัติราชการแทนเลขานุการกรม
๑๑ ส.ค. ๒๕๖๓

(นางกมลลักษณ์ สร้างเอี่ยม)
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มบริหารจัดการระบบเครือข่าย
และความปลอดภัยเทคโนโลยีสารสนเทศ

(นายวิชาญ อิงศรีสว่าง)
รองอธิบดีกรมประมง
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงกรมประมง
๑๔ ส.ค. ๒๕๖๓

(นายศุภวัฒฑ์ โกมลมาลย์)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

แนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ ของกรมประมง ปีงบประมาณ พ.ศ. ๒๕๖๗

ปัจจุบันภัยคุกคามทางไซเบอร์มีจำนวนเพิ่มสูงขึ้นและทวีความรุนแรงขึ้นตามลำดับ การโจมตีมีความหลากหลาย มีรูปแบบที่ซับซ้อน มุ่งเน้นการโจมตีไปสู่ข้อมูลที่มีความสำคัญในลักษณะค่อยเป็นค่อยไปแต่ต่อเนื่อง ปัจจุบันภัยคุกคามทางไซเบอร์ที่พบมาก ได้แก่ ไวรัส มัลแวร์ขั้นสูง มัลแวร์เรียกค่าไถ่ (Ransomware) จนถึงการใช้ความรู้ทางคอมพิวเตอร์ขั้นสูงเพื่อเจาะระบบคอมพิวเตอร์ หรืออาศัยหลักจิตวิทยาเพื่อหลอกลวงผู้ใช้งานให้เปิดเผยข้อมูลสำคัญ เพื่อสร้างความเสียหายหรือรวบรวมข้อมูลที่ต้องการให้ได้มากที่สุด ส่งผลกระทบและสร้างความเสียหายทั้งต่อระดับหน่วยงานและระดับประเทศ ซึ่งรัฐบาลได้ให้ความสำคัญในการดำเนินงานเพื่อรับมือกับปัญหาภัยคุกคามดังกล่าวอย่างมาก จึงได้มีการประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ เพื่อกำหนดแนวทางและมาตรการต่าง ๆ ที่เกี่ยวข้องอย่างเป็นรูปธรรม ซึ่งหน่วยงานรัฐจะต้องมีการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงในด้านต่าง ๆ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมประมงจึงได้จัดทำแนวปฏิบัติเมื่อเกิดเหตุกระทบความมั่นคงปลอดภัยทางไซเบอร์ เพื่อสร้างความตระหนักรู้ (Awareness) ให้แก่บุคลากรของหน่วยงาน อีกทั้งแนะนำวิธีป้องกัน รับมือภัยอันตรายบนโลกออนไลน์ ให้สามารถปฏิบัติได้อย่างถูกต้อง ป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตีทางไซเบอร์ โดยประกอบด้วย ๕ แนวปฏิบัติ ดังนี้

๑. แนวปฏิบัติการรักษาความปลอดภัยจากอีเมลปลอมแปลง (Phishing Mail)

๒. แนวปฏิบัติการป้องกันการบุกรุกโจมตีเว็บไซต์

๓. แนวทางการปฏิบัติในการป้องกันภัยคุกคามจากไวรัสคอมพิวเตอร์และมัลแวร์ (Malware)

๔. แนวทางการปฏิบัติในการป้องกันภัยคุกคามอุปกรณ์เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) และอุปกรณ์ต่อพ่วงที่สามารถเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ได้โดยตรง

๕. แนวทางการปฏิบัติในการป้องกันภัยคุกคามโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศกรมประมง (Information Technology Infrastructure)

มีรายละเอียด ดังนี้

๑. แนวปฏิบัติการรักษาความปลอดภัยจากอีเมลปลอมแปลง (Phishing Mail)

๑.๑ ข้อสังเกตอีเมลที่เป็น Phishing Mail ดังนี้

(๑) อีเมลที่ส่งมาจากต้นทางอ้างว่าเป็นบริษัทที่ถูกต้องตามกฎหมาย มีลักษณะคล้ายหรือเหมือนสถาบันการเงินหรือหน่วยงานต่าง ๆ เพื่อหลอกให้ผู้ใช้งานกรอกข้อมูลหรือเปิดเผยข้อมูลสำคัญ เช่น เลขบัตรประจำตัวประชาชน วัน/เดือน/ปีเกิด ข้อมูลบัญชีธนาคาร หมายเลขบัตรเครดิต รหัสผ่านอีเมล รหัสผ่านบัญชีออนไลน์ รหัสผ่านการเข้าใช้งานระบบ

(๒) อีเมลผู้ส่ง (Email Address) มักใช้ชื่ออีเมลที่คล้ายหรือใกล้เคียงกับสถาบันการเงินหรือหน่วยงานนั้น ๆ

(๓) ลักษณะเนื้อหา ข้อความที่ใช้ในอีเมล จะใช้ข้อความให้รีบดำเนินการ เปลี่ยนแปลง หรืออัปเดตข้อมูลผู้ใช้งาน เพื่อความปลอดภัยของข้อมูลหรือบัญชี เป็นต้น และข้อความอาจมีการสะกดคำผิดหลักไวยากรณ์

(๔) มีการแนบลิงก์เชื่อมโยงหรือเว็บไซต์มาในอีเมล โดยลิงก์ดังกล่าวอาจเชื่อมไปยังเว็บไซต์ปลอม ถึงแม้

ขึ้นต้นด้วย https:// ก็ควรตรวจสอบ URL ว่าเป็นสถาบันการเงินหรือหน่วยงานนั้น ๆ จริง

(๕) ตรวจสอบว่ามีบัญชีการใช้งานของสถานบันการเงินหรือหน่วยงานต่าง ๆ หรือเว็บไซต์ที่อ้างถึงหรือไม่ บางกรณีท่านไม่มีบัญชีแต่ได้รับอีเมลจากหน่วยงานหรือบริษัทที่อ้างถึง

๑.๒ แนวปฏิบัติการรักษาความปลอดภัยการใช้งานอีเมล

๑) ผู้ใช้งาน (User)

(๑) ตั้งรหัสผ่านที่มีความปลอดภัยและคาดเดาได้ยาก ไม่ควรใช้รหัสที่สั้นจนเกินไป หรือใช้ข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนตัว อย่างเช่น วันเดือนปีเกิด การตั้งรหัสผ่านที่มีความปลอดภัยและคาดเดาได้ยากควรมีอักขระตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์ อย่างน้อย ๑๐ ตัว

(๒) เก็บรักษารหัสผ่าน (Password) อีเมลเป็นความลับ ไม่ควรเขียนใส่กระดาษติดไว้หน้าจอหรือบริเวณใกล้เคียง หรือตั้งค่าให้โปรแกรมบราวเซอร์ช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save password) หลังจากใช้งานระบบอีเมลเสร็จสิ้น ควร Logout ออกจากระบบทุกครั้ง

(๓) ไม่ตอบกลับอีเมลที่น่าสงสัย ไม่เปิดลิงก์ URL และไม่ดาวน์โหลดหรือติดตั้งโปรแกรมที่แนบมาในอีเมล ที่ส่งมาจากผู้ส่งที่ไม่รู้จัก ไม่ทราบแหล่งที่มาเพราะอาจทำให้อีเมลโดนแฮกหรือโดนขโมยข้อมูลสำคัญของผู้ใช้งานได้ อย่างเช่น มีอีเมลแจ้งว่า บัญชีอีเมลของคุณจะถูกระงับ ขอให้ผู้ใช้งานกรอกข้อมูลส่วนตัวและรหัสผ่านเพื่อยืนยัน หรืออัปเดตข้อมูล เพื่อความปลอดภัย เป็นต้น

(๔) ตรวจสอบไฟล์แนบและสแกนไวรัสก่อนเปิดไฟล์แนบทุกครั้งไม่เปิดไฟล์แนบที่เป็น Executable file หรือมีนามสกุลไฟล์เป็น .exe .com

(๕) ตรวจสอบ Mail Box ของตนเองเป็นประจำ และลบอีเมลที่ไม่สำคัญหรือไม่ต้องการออกจากระบบ

(๖) สำรองข้อมูลอีเมลที่สำคัญไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ของตนเองอย่างสม่ำเสมอ

(๗) ตรวจสอบชื่ออีเมลผู้ส่ง (Email Account) ว่าเป็นอีเมลที่ส่งมาจากผู้ส่งตัวจริงหรือไม่ เนื่องจากชื่อผู้ส่งอาจถูกแก้ไขโดยวิธี Spoof Mail (ปลอมแปลงชื่อผู้ส่งเมล์) หากพบว่าชื่อผู้ส่งไม่ตรงกัน ให้รีบแจ้งมาเจ้าหน้าที่ผู้ดูแลระบบ (Admin) เพื่อตรวจสอบแหล่งที่มาของอีเมลทันที

๒) ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ (อีเมล) กรมประมง (Admin)

(๑) ควรมีการติดตั้งระบบ Anti Spam mail เพื่อกลั่นกรองอีเมลที่ไม่พึงประสงค์ที่ถูกส่งมาจากที่ผู้ที่ไม่สามารถระบุตัวตนได้ว่าเป็นใคร (โดเมนที่ไม่ได้รับการยืนยันตัวตน) อีเมลก่อกวนที่มีการกระจายข้อความที่ไม่พึงประสงค์ อาจจะมีการฝังสคริปต์ (Script) ต่าง ๆ ไว้ในไฟล์เอกสารที่แนบมากับอีเมลนั้นด้วย ซึ่งเมื่อเปิดไฟล์นั้นหรือดาวน์โหลดลงมาที่เครื่องคอมพิวเตอร์ อาจจะทำให้เกิดความเสียหายได้

(๒) ควรมีการตั้งค่าแบลงค์ สแปม (Blank SPAM) คือ SPAM ที่มีจุดประสงค์หลักคือก่อกวนระบบอีเมลโดยการส่งอีเมลที่ไม่มีเนื้อหาทำให้เกิดการติดขัดในระบบ หรือทำให้ระบบทำงานช้าลง เนื่องจากมีเมลจำนวนมากที่ต้องจัดการโดยไม่จำเป็น

(๓) ควรมีการตั้งค่าฟิชชิ่งอีเมล (Phishing Email) ที่มีลักษณะหลอกสอบถามข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ควรเปิดเผยสู่สาธารณะด้วยวิธีการหลอกล่อต่าง ๆ ผ่านเนื้อหาในจดหมาย เช่น หลอกถามข้อมูล Password หรือสอบถามข้อมูลส่วนบุคคล ซึ่งหากผู้รับไม่รู้เท่าทันแล้วส่งข้อมูลกลับไปอาจเกิดความเสียหายแก่ผู้ที่ได้รับอีเมลฉบับนั้น ๆ ด้วย

(๔) ควรมีการตั้งค่าสแปมเวอร์ไทด์ ไซต์ (Spamvertised sites) คือ อีเมลที่มีเนื้อหาเกี่ยวกับการโฆษณาสินค้า ผลิตภัณฑ์หรือบริการ ซึ่งในบางครั้งมักจะมีการโฆษณาแอบแฝงและหลอกลวงด้วย

(๕) ควรมีการตั้งค่าอิมเมจ สแปม (Image SPAM) เป็นลักษณะของ Spamvertised sites ชนิดหนึ่งแต่ส่งข้อมูลมาในลักษณะของรูปภาพแทนที่จะเป็นข้อมูลตัวอักษรเพื่อให้ยากต่อการตรวจจับของระบบดักจับ Spam (Spam Filter)

(๖) ควรมีการตั้งค่าแบล็กสเก็ตเตอร์ (Backscatter SPAM) คืออีเมลที่มีการแนบไฟล์ที่มีการทำงานเป็นไวรัสหรืออีกทั้งยังมีเนื้อหาเชิญชวนให้ผู้ใช้งานทำการ run (รัน) ไฟล์ดังกล่าว เพื่อให้ไวรัสนั้น ๆ ทำงานซึ่งอาจสร้างความเสียหายแก่ข้อมูลหรือทรัพย์สิน

(๗) สร้างมาตรฐานในการสร้างรหัสผ่าน เช่น Minimum Password Length, Password Expiration, Require a number in the password, Require a symbol in the password

(๘) มาตราการป้องกันการ Random Login (Brute Force Policy) เพื่อป้องการการสุ่ม Password หรือ Dictation Attack จากผู้ไม่หวังดี

(๙) มาตรการความปลอดภัย Encryption ข้อมูลผ่านทาง SSL (Secure Socket Layer) และ TLS (Transport Layer Security) ซึ่งระบบทำการรองรับ

(๑๐) มาตรการป้องกันการเข้าถึง Cloud Server โดยใช้ Cloud Firewall Protection โดยมีการเปิดใช้งานเฉพาะส่วนการเข้าถึงเฉพาะการใช้บริการในส่วนของระบบจดหมายอิเล็กทรอนิกส์เท่านั้น

(๑๑) มาตรการป้องกันการ DOS Attack (distributed denial-of-service) เพื่อป้องการการโจมตีใน Protocol ต่าง ๆ ในระบบให้บริการ Email จากผู้ไม่หวังดี

(๑๒) การป้องกันและปิดกั้นผู้ใช้งานที่มีการติด Malware / Spammer

(๑๓) ระบบมีการตรวจจับการใช้งานและการส่งออกของจดหมายอิเล็กทรอนิกส์ หากมีการส่งออกที่เกินหรือผิดปกติระบบจะทำการกักจดหมายที่ทำการส่งไว้ และทำการแจ้งไปยังผู้ดูแลระบบเพื่อทำการตรวจสอบ

๑.๓ แนวปฏิบัติเมื่อเปิดใช้อีเมล Phishing Mail ดังนี้

๑) ผู้ใช้งาน (User)

กรณี คลิกลิงค์เว็บไซต์ หรือ เปิดไฟล์แนบจาก Phishing Mail ดำเนินการ ดังนี้

(๑) เมื่อผู้ใช้งานคลิกลิงค์เว็บไซต์ หรือเปิดไฟล์แนบ หรือติดตั้งโปรแกรมจากอีเมล แล้วพบว่าเครื่องคอมพิวเตอร์ได้ทำงานผิดปกติ ให้สังเกตว่า URL ของเว็บไซต์นั้นได้ตรงกับหน่วยงานหรือเว็บไซต์ที่แจ้งในอีเมลหรือไม่ ให้แจ้งมายังผู้ดูแลระบบ (Admin) ทันที

(๒) นำเครื่องคอมพิวเตอร์ที่ผิดปกติหรือสงสัยว่าติดไวรัส มัลแวร์ ออกจากระบบเครือข่ายและอินเทอร์เน็ตของหน่วยงาน เพื่อป้องกันการแพร่กระจายของไวรัสหรือมัลแวร์ไปยังเครื่องลูกข่ายอื่นในหน่วยงาน และทำการสแกนไวรัสเครื่องคอมพิวเตอร์นั้นเพื่อแก้ไขปัญหา

(๓) แจ้งให้ผู้ดูแลระบบ (Admin) ตรวจสอบความผิดปกติเครื่องคอมพิวเตอร์

กรณี กรอกข้อมูลสำคัญในเว็บไซต์ปลอมที่ส่งมาจาก Phishing Mail ดำเนินการ ดังนี้

(๑) เมื่อผู้ใช้งานกรอกข้อมูลส่วนบุคคลในเว็บไซต์ปลอม เช่น ข้อมูลชื่อ นามสกุล รหัสบัตรประชาชน วันเดือนปีเกิด รหัสเข้าใช้งาน (Username) รหัสผ่าน (Password) ผู้ใช้งานต้องรีบเปลี่ยนรหัสผ่านในทุกระบบที่ใช้รหัสผ่านเดียวกันทันที และไม่กลับมาใช้รหัสผ่านนั้นอีก

(๒) หากกรอกข้อมูลบัญชีธนาคาร ให้แจ้งเรื่องไปยังธนาคารที่ใช้บริการ และทำการปิดบัญชี หรืออายัดบัญชีนั้นทันที และเฝ้าระวังการใช้งานบัญชีอย่างต่อเนื่อง หากพบความเสียหายทางการเงินให้รวบรวมหลักฐานแจ้งตำรวจ และติดต่อธนาคาร เพื่อระงับบัญชีปลายทาง

(๓) แจ้ง Phishing Mail ให้ผู้ดูแลระบบ (Admin) ทราบ

๒) ผู้ดูแลระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย กรมประมง (Admin)

(๑) ปรับปรุงฐานข้อมูลบัญชี Spam Mail เครื่องคอมพิวเตอร์แม่ข่าย Mail Server ให้เป็นปัจจุบัน

(๒) เพิ่มบัญชี Phishing Mail เป็น Blacklist Mail ในระบบ Anti-Spam เพื่อป้องกันกันอีเมล์ Phishing นั้นเข้ามาในระบบบริการอีเมลของกรมประมงอีกครั้ง

(๓) ปิดกั้นเว็บไซต์ปลอม (Phishing URL) ในระบบ Firewall, Proxy เพื่อไม่ให้ผู้ใช้งานเรียกใช้เว็บไซต์ปลอมจากระบบเครือข่ายภายในกรมประมงได้

(๔) แจ้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) เพื่อปิดกั้น Phishing Mail และเว็บไซต์ปลอม (Phishing URL) ไม่ให้ผู้ใช้งานเรียกใช้เว็บไซต์ปลอมได้จากระบบเครือข่ายภายนอก และติดตามตรวจสอบ Phishing Mail นั้น

(๕) ส่งอีเมลหรือแจ้งเวียนหนังสือแจ้งเตือนภัย Phishing Mail และข้อแนะนำการป้องกันภัยให้ทุกหน่วยงานของกรมประมงทราบ เพื่อเฝ้าระวังและเตรียมพร้อมรับมือได้อย่างทันท่วงที

๒. แนวปฏิบัติการป้องกันการบุกรุกโจมตีเว็บไซต์

๒.๑ แนวปฏิบัติการป้องกันการบุกรุกโจมตีเว็บไซต์

๑) ผู้พัฒนา/ดูแลเว็บไซต์หน่วยงาน

(๑) เฝ้าระวังและตรวจสอบเว็บไซต์ของหน่วยงานทุกวัน โดยเฉพาะในช่วงวันหยุดราชการให้มีเจ้าหน้าที่ตรวจสอบเฝ้าระวัง หากตรวจพบการบุกรุกโจมตีให้ทำการแก้ไขในทันที

(๒) ดำเนินการตรวจสอบ ป้องกัน และแก้ไขจุดอ่อนของโปรแกรมที่พัฒนาขึ้นหรือนำมาใช้งาน หากตรวจพบให้ดำเนินการแก้ไขทันที

(๓) มีการกำหนดสิทธิ์การเข้าถึงระบบคอมพิวเตอร์ควบคุมผู้ใช้งานที่ได้สิทธิ์สูง เช่น สิทธิ์เป็นผู้ดูแลระบบ

(๔) ทำการสำรองข้อมูลเว็บไซต์และฐานข้อมูลอยู่เสมอ และทดสอบการกู้คืนค่าไฟล์ที่สำรองว่าสามารถใช้งานได้ปกติ

(๕) ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความสำคัญในลำดับชั้นต่าง ๆ ตามที่ได้รับอนุญาต

(๖) ให้ทำการเปลี่ยนรหัสผ่านของผู้ดูแลระบบทุก ๆ ๓ เดือน หรือเร็วกว่านั้น โดยการตั้งรหัสผ่านให้มีความยาว อักขระพิเศษ ตัวอักษร และตัวเลข ผสมกัน

(๗) ผู้พัฒนาควรพัฒนาเว็บไซต์ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับโปรแกรมประยุกต์บนเว็บไซต์ Web Application security Standard: WAS)

๒) ผู้ดูแลระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย กรมประมง (Admin)

(๑) ตรวจสอบการทำงานของ Firewall และกำหนดค่า Policy การเข้าถึงระบบเครือข่ายภายในกรมประมงเฉพาะที่ส่วนที่ให้บริการเพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้

(๒) อัปเดต Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน

(๓) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์และปรับปรุงฐานข้อมูลไวรัสให้ทันสมัยอยู่เสมอ

(๔) ตรวจสอบการทำงานของ IPS (Intrusion Prevention System) ป้องกันการบุกรุก และหยุดยั้งผู้บุกรุกที่พยายามเข้าสู่ระบบ และปรับปรุงค่า Configuration ให้สามารถป้องกันการบุกรุกในรูปแบบใหม่

(๕) ตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเทอร์เน็ตของกรมประมง เพื่อเฝ้าระวังภัยจากระบบเครือข่ายและอินเทอร์เน็ต

(๖) เครื่องคอมพิวเตอร์แม่ข่าย Web Server ควรมีการรองรับ SSL บนเว็บไซต์ของหน่วยงาน (Secure Sockets Layer)

(๗) ควรมีระบบรักษาความมั่นคงปลอดภัยของเว็บไซต์ตามมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard: WSS)

(๘) ควรมีการใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ของเครื่องบริการเว็บอย่างสม่ำเสมอ จะช่วยให้ผู้ดูแลเครื่องบริการเว็บในการค้นหาข้อบกพร่องของเว็บไซต์ในเบื้องต้น

(๙) ควรมีการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการใช้งานของผู้ใช้ (Log) เพื่อใช้ในการตรวจหาสาเหตุได้การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการเข้าใช้งานเว็บไซต์ (Log) กรณีเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุขัดข้องทางเทคนิคขึ้นระหว่างการให้บริการ ให้เป็นไปตามกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๑๐) การสำรองข้อมูลเว็บไซต์ โดยองค์ประกอบหลักในการสำรองข้อมูลบนเครื่องบริการเว็บมี ๒ องค์ประกอบ คือการสำรองข้อมูลและระบบปฏิบัติการบนเครื่องบริการเว็บ และการดูแลรักษาข้อมูลสำรองที่เชื่อถือได้ (Authoritative Copy) ของเว็บไซต์ โดยมีการป้องกันแยกต่างหากจากเครื่องบริการเว็บเพื่อให้เกิดความมั่นใจว่าจะสามารถกู้คืนเว็บไซต์ให้อยู่ในสภาพสมบูรณ์พร้อมใช้งานได้เหมือนเดิม

๒.๒ แนวปฏิบัติเมื่อเกิดเหตุการณ์

เมื่อพบเหตุการณ์ผิดปกติในเว็บไซต์หน่วยงาน เช่น ถูกเปลี่ยนแปลงแก้ไขข้อมูลในเว็บไซต์ หรือแก้ไขหน้าจอแสดงผลบนเว็บไซต์ หรือไม่สามารถเข้าใช้งานหน้าเว็บไซต์ได้

๑) ผู้พัฒนา/ดูแลเว็บไซต์

(๑) แจ้งผู้ดูแลระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย กรมประมง เพื่อนำเครื่องคอมพิวเตอร์แม่ข่าย Web Server ที่เกิดปัญหาออกจากระบบเครือข่ายโดยทันที

(๒) ดำเนินการตรวจสอบระบบที่ทำงานผิดปกติ อาทิเช่น ข้อมูลและขั้นตอนการทำงานต่าง ๆ ของระบบ ในกรณีที่สามารถเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายได้

(๓) ทำการสแกนเพื่อตรวจสอบมัลแวร์บนเครื่องคอมพิวเตอร์แม่ข่าย และแก้ไข/กำจัด

(๔) ตรวจสอบการทำงานของระบบสารสนเทศที่ติดตั้ง หลังดำเนินการกำจัดมัลแวร์เรียบร้อยแล้ว

(๕) หากระบบยังไม่สามารถใช้งานได้ ให้นำข้อมูลที่ได้สำรอง (Backup) ไว้มาใช้งาน

(๖) ติดตามการปรับปรุงซอฟต์แวร์ เช่น ระบบปฏิบัติการ โปรแกรมป้องกันไวรัสมัลแวร์ ซอฟต์แวร์ที่ใช้ในการพัฒนาเว็บไซต์ และควรปรับปรุงซอฟต์แวร์ให้ทันสมัยอยู่เสมอ

๒) ผู้ดูแลระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย กรมประมง (Admin)

โดยแนวทางการรับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์ จำแนกออกเป็น ๖ ประเภท ของรูปแบบการโจมตีดังต่อไปนี้

กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)

ภัยคุกคามจากการบุกรุกและควบคุมเว็บไซต์ (Intrusions) สามารถพบเห็นและยืนยันได้ง่ายที่สุด เนื่องจากการโจมตีนั้นมักจะต้องมีการสร้างร่องรอยหรือหลักฐานที่เห็นได้อย่างชัดเจน ตามแต่ละจุดประสงค์ของผู้ประสงค์ร้ายตัวอย่าง เช่น การสร้างหน้าเว็บไซต์หลอกลวง (Phishing) เพื่อหวังผลทางการเงินการเปลี่ยนแปลง

ข้อมูลต่าง ๆ บนเว็บไซต์ (Web Defacement) เพื่อหวังผลในการทำลายชื่อเสียงหรือแม้กระทั่งการเผยแพร่มัลแวร์บนเว็บไซต์ (Malware) เพื่อให้ผู้เข้าชมเว็บไซต์ติดมัลแวร์ เป็นต้น ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกบุกรุกและควบคุมนี้สามารถดำเนินการได้ในลักษณะเดียวกัน ดังนี้

(๑) ปิดการเชื่อมต่อของเว็บไซต์

(๒) สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น WebLog Source code Database

(๓) ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามาโดยในระหว่างที่ผู้ดูแลกำลังตรวจสอบช่องทางการโจมตี

(๔) ระหว่างการตรวจสอบจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง รวมไปถึงเพื่อให้หน่วยงานสามารถดำเนินภารกิจได้อย่างต่อเนื่อง โดยเว็บเพจดังกล่าวควรติดตั้งอยู่ในเครื่องบริการเว็บใหม่ เพื่อลดความเสี่ยงจากการที่เครื่องบริการเว็บเดิมถูกควบคุมและปรับเปลี่ยนการตั้งค่าต่าง ๆ เพื่อป้องกันไม่ให้มีผลกับข้อมูลต่าง ๆ ที่อยู่บนเครื่องเดิม

(๕) กู้คืนโปรแกรมที่เกี่ยวข้อง ข้อมูลเว็บ และฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์เป็นเวอร์ชั่นก่อนหน้าที่จะถูกโจมตี

(๖) ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชั่นก่อนหน้าที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment แก้ไขช่องโหว่ของเว็บไซต์ที่ทำให้ผู้ประสงค์ร้ายสามารถเจาะเพื่อเข้าควบคุมระบบได้

(๗) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ในหลายครั้งพบว่าผู้ประสงค์ร้ายสามารถบุกรุกและเข้าควบคุมเว็บไซต์ได้มาเป็นเวลานานแล้วแต่เพิ่งมาสร้างร่องรอยหรือเปลี่ยนแปลงข้อมูลในเวลาต่อมา ส่งผลให้การวิเคราะห์ข้อมูลการโจมตีและช่องโหว่ของเว็บไซต์ผ่านข้อมูล Log นั้นทำได้ยากขึ้น เนื่องจากในบางหน่วยงานมีเก็บข้อมูล Log ไว้เพียงชั่วขณะหนึ่ง ทำให้การวิเคราะห์ข้อมูลในช่องเวลาที่มีการโจมตีจริง ๆ นั้นไม่สามารถทำได้ อย่างไรก็ตามผู้ดูแลต้องทบทวนข้อมูล Log อย่างสม่ำเสมอเพื่อตรวจสอบดูการโจมตีที่เกิดขึ้น

กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service)

การโจมตีเว็บไซต์ในลักษณะ DoS นั้น กล่าวคือ การโจมตีเพื่อมุ่งเน้นให้เว็บไซต์ไม่สามารถให้บริการต่อได้ ซึ่งเป้าประสงค์สามารถเกิดได้จากหลายส่วน เช่น การลดความน่าเชื่อถือของหน่วยงาน การลดโอกาสในการทำธุรกิจ รวมถึงในปัจจุบันพบว่ามีเป้าประสงค์ในเชิงการเมืองการบริหารเข้ามาเกี่ยว ดังที่เห็นกลุ่มแฮกเกอร์ประกาศว่าจะโจมตีหน่วยงานราชการแบบไม่ให้เปิดบริการได้อีก ในปัจจุบันการโจมตีขยายตัวออกไปถึงการโจมตีที่เรียกว่าดีดอส หรือ DDoS (Distributed Denial of Service) เป็นลักษณะการโจมตีเป็นกลุ่มที่เกิดจากเครื่องคอมพิวเตอร์หลาย ๆ เครื่องโจมตีเป้าหมายในเวลาเดียวกัน ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกโจมตีในลักษณะ DDoS นั้น โดยมีแนวทางการดำเนินการ ดังนี้

(๑) ปิดการเชื่อมต่อของเว็บไซต์

(๒) สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น Web Log หรือ Firewall Log

(๓) ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา โดยปกติจะพบเห็นข้อมูลในลักษณะที่เกิดซ้ำ ๆ ในรูปแบบเดียวกัน เช่น มีการเรียกเว็บไซต์ด้วยยูอาร์แอลหนึ่งเป็นจำนวนมาก หรือมี

การส่งข้อมูลมายังบริการหนึ่งซ้ำ ๆ เป็นจำนวนมาก

(๔) ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าวและแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ต เพื่อหามาตรการที่รองรับในกรณีที่อุปกรณ์ป้องกันของหน่วยงานไม่สามารถรองรับปริมาณข้อมูลที่มากมายได้

(๕) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

การจัดการกับเหตุการณ์ภัยคุกคามในกรณีถูกโจมตีด้วยเทคนิค DoS หรือ DDoS นั้น สิ่งสำคัญคือผู้ดูแลต้องมีทักษะในการพิจารณาและคัดแยกไอพีแอดเดรสที่คาดว่าจะเป็นการโจมตีที่รวดเร็วและถูกต้อง เพื่อป้องกันข้อผิดพลาดจากการปิดกั้นการเชื่อมต่อ โดยอาจอาศัยการประมวลผลในลักษณะสถิติ และลักษณะการเข้าใช้งานที่ผิดปกติ รวมถึงยังจำเป็นต้องมีความร่วมมือกับผู้ให้บริการอินเทอร์เน็ตเพื่อให้การป้องกันการโจมตีทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

กรณีโดเมนถูกขโมย (Domain Hijack)

การขโมยโดเมน (Domain Hijack) เป็นหนึ่งในรูปแบบการโจมตีที่มีมานานแล้ว และดูเหมือนว่ายังคงเป็นรูปแบบการโจมตีที่พบอยู่เสมอ เหยื่อที่ถูกขโมยโดเมนสามารถเป็นได้ตั้งแต่บริษัทขนาดเล็กและไม่เว้นแม้แต่บริษัทขนาดใหญ่ที่ดำเนินธุรกิจด้านเทคโนโลยีสารสนเทศที่ยังพบว่าตกเป็นเหยื่อในหลายครั้ง โดยจุดประสงค์ของการขโมยข้อมูลนั้นส่วนใหญ่มุ่งประโยชน์ไปยังการหาผลประโยชน์ในหลายลักษณะ ตัวอย่างเช่น ขโมยโดเมนเนมเพื่อนำไปหาประโยชน์โดยการเรียกค่าไถ่จากเจ้าของโดเมนตัวจริง นำไปใช้สร้างสถานการณ์การหลอกลวงหน้า Phishing เป็นต้น ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกขโมยโดเมนนั้น สามารถดำเนินการได้แต่อย่างไรก็ตามจำเป็นต้องมีข้อมูลที่เพียงพอเพื่อให้การแก้ปัญหาทำได้อย่างมีประสิทธิภาพ โดยมีแนวทางการดำเนินการ ดังนี้

(๑) เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปี ที่ข้อมูลโดเมนเปลี่ยนหน้าจอของโดเมนที่ใช้งาน

(๒) ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน ในบางครั้งพบว่าผู้ดูแลถูกขโมยข้อมูลรหัสผ่านโดยการติดมัลแวร์ ทำให้ผู้ประสงค์ร้ายสามารถเข้าสู่เว็บไซต์บริหารจัดการโดเมนและทำการเปลี่ยนแปลงข้อมูลส่วนบุคคล

(๓) แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่เราใช้บริการ โดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย เช่น หลักฐานการโอนเงิน หลักฐานการตอบรับ เป็นต้น

(๔) เมื่อได้รับสิทธิในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน เช่น ข้อมูลอีเมลผู้จดทะเบียนโดเมน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน

(๕) บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ภายหลังจากถูกขโมยโดเมนแล้ว สิ่งที่ยากที่สุดสำหรับผู้ดูแลคือ การทำให้ผู้ให้บริการลงทะเบียนโดเมนเชื่อว่าโดเมนถูกขโมยจริง และยอมคืนสิทธิกลับคืนให้กับผู้ดูแลตัวจริง แต่อย่างไรก็ตามความสำคัญไม่น้อยไปกว่านั้นคือผู้ดูแลจำเป็นต้องทราบสาเหตุของการถูกขโมยโดเมนที่เกิดขึ้น เพื่อเป็นการป้องกันและรับมือสถานการณ์การโจมตีที่อาจเกิดซ้ำอีก

กรณีปัญหาเกิดจากช่องโหว่ของโปรแกรมหรือเฟรมเวิร์ค (Framework) ที่ล้าสมัย/เวอร์ชันเก่า ทำการลบข้อมูลบนเครื่องทั้งหมด (Format) เพื่อป้องกันโทรจันที่ซ่อนอยู่ในเครื่อง จากนั้นติดตั้งระบบปฏิบัติการและโปรแกรมที่เกี่ยวข้องใหม่ และแจ้งให้ผู้ดูแลเว็บไซต์อัปเดต Patch ที่สามารถปิดช่องโหว่ของโปรแกรมหรือเฟรมเวิร์ค (Framework) ได้ และนำเว็บไซต์ที่สำรองมากู้คืนข้อมูล (Recovery) มาติดตั้งใช้งานตามปกติ

กรณีปัญหาเกิดจากช่องโหว่ซอร์สโค้ด (Source code) ของเว็บไซต์ แจ้งสาเหตุของปัญหาให้ผู้ดูแลเว็บไซต์ทราบ และให้คำแนะนำ/วิธีการปรับปรุงซอร์สโค้ด (Source code) เพื่อปิดกั้นช่องโหว่จากนั้นให้ดำเนินการติดตั้งระบบปฏิบัติการ และโปรแกรมที่เกี่ยวข้องใหม่ และนำซอร์สโค้ด (Source code) เว็บไซต์ที่ปรับปรุงเรียบร้อยแล้วมาติดตั้งเพื่อเปิดใช้งานปกติ

กรณีตรวจสอบปัญหาแล้วไม่ทราบสาเหตุหรือไม่พบแหล่งที่มาของแฮกเกอร์ (Hacker) แจ้งให้ผู้ดูแลเว็บไซต์หน่วยงานพัฒนาเว็บไซต์ใหม่ เพื่อปิดกั้นช่องโหว่และดำเนินการติดตั้งระบบปฏิบัติการใหม่ พร้อมทั้งโปรแกรมที่เกี่ยวข้อง นำซอร์สโค้ด Source code เว็บไซต์ที่ปรับปรุงใหม่แล้วมาติดตั้งและเปิดใช้งานปกติ

๓. แนวทางการปฏิบัติในการป้องกันภัยคุกคามจากไวรัสคอมพิวเตอร์และมัลแวร์ (Malware)

๓.๑ แนวปฏิบัติเพื่อป้องกันภัยจากมัลแวร์ (Malware)

๑) ผู้ใช้งาน (User)

(๑) มีการติดตั้งโปรแกรม Antivirus ในเครื่องคอมพิวเตอร์ที่ใช้งาน ตรวจสอบการอัปเดตฐานข้อมูล Antivirus และสแกนข้อมูลจากอุปกรณ์จัดเก็บข้อมูลก่อนนำข้อมูลลงในเครื่องคอมพิวเตอร์

(๒) ติดตั้งโปรแกรมที่มีลิขสิทธิ์ถูกต้องและติดตั้งเท่าที่จำเป็น และอัปเดตระบบปฏิบัติการให้เป็นปัจจุบัน

(๓) ตรวจสอบช่องโหว่ที่มีความเสี่ยง ปิด Service ที่ไม่ได้ใช้งาน ตรวจสอบสิทธิ์การแชร์ข้อมูลร่วมกันผ่านระบบเครือข่ายของเครื่องคอมพิวเตอร์ส่วนบุคคล

(๔) หลีกเลี่ยงการใช้โปรแกรมอัปโหลดไฟล์ FTP หรืองดใช้ชั่วคราว

(๕) ใช้โปรแกรมเว็บบราวเซอร์ที่ทันสมัยและอัปเดตให้เป็นปัจจุบันอยู่เสมอ

(๖) เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม หรือการเข้าเว็บไซต์ที่มีความเสี่ยง เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์เผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์

(๗) ไม่คลิกลิงค์หรือเปิดไฟล์จากเว็บไซต์หรือจากอีเมล์ที่น่าสงสัย

(๘) ไม่ดาวน์โหลดและติดตั้งใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ เพราะอาจจะมีมัลแวร์ (Malware) แฝงมาด้วย

(๙) มีการสำรองข้อมูล (Backup) ที่ใช้งานอยู่เสมอและทดสอบการกู้คืนค่า (Recovery) ไฟล์ที่สำรองข้อมูลไว้ ว่าสามารถใช้งานได้

(๑๐) ติดตามข้อมูลข่าวสารเกี่ยวกับความปลอดภัยทางไซเบอร์ สถานการณ์การแพร่ระบาดของมัลแวร์ (Malware) และประกาศช่องโหว่ร้ายแรง (Critical Vulnerability) เป็นประจำ เพื่อเตรียมพร้อมรับมือและปิดกั้นช่องโหว่ร้ายแรงจากภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้นได้อย่างทันท่วงที

๒) ผู้ดูแลระบบ (Admin)

(๑) ตรวจสอบการทำงานของระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ (Firewall) ในส่วน Module การป้องกันไวรัสระบบเครือข่าย (Antivirus-Gateway) และตั้งค่าให้ระบบอัปเดตฐานข้อมูลไวรัสคอมพิวเตอร์ใหม่โดยอัตโนมัติ รวมทั้ง Update Category บัญชีเว็บไซต์ที่มีความเสี่ยง เช่น เว็บไซต์ลามก

เว็บไซต์การพนัน เพื่อป้องกันไม่ให้เครื่องลูกข่ายเข้าสู่เว็บไซต์ดังกล่าวได้

(๒) ตรวจสอบการทำงานของอุปกรณ์ป้องกันไวรัสคอมพิวเตอร์ในระบบอีเมล์ (Email Security) ว่าทำงานสถานะปกติ

(๓) ตรวจสอบและวิเคราะห์ Log File จากรายงานการพบภัยคุกคาม เพื่อวิเคราะห์สถานการณ์และเฝ้าระวัง เมื่อพบว่าเครื่องคอมพิวเตอร์ลูกข่ายมีลักษณะ การส่งข้อมูล (Transaction) ที่ผิดปกติหรือคาดว่าอาจติดมัลแวร์ (Malware) ให้แจ้งเจ้าของเครื่องคอมพิวเตอร์และเข้าดำเนินการแก้ไขโดยเร่งด่วน

(๔) ตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) เครื่องลูกข่ายให้ทันสมัย เพื่อปิดช่องโหว่ที่ร้ายแรง (Critical Vulnerability)

(๕) มีการจำกัดสิทธิ์และการยืนยันตัวตนในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กร เพื่อป้องกันการแอบเข้ามาใช้งานของผู้ที่ไม่ประสงค์ดี

๓.๒ แนวปฏิบัติเมื่อเกิดเหตุการณ์ติดมัลแวร์ (Malware)

๑) ผู้ใช้งาน (User)

(๑) ตรวจสอบช่องโหว่ที่มีความเสี่ยง ปิด Service ที่ไม่ได้ใช้งาน ตรวจสอบสิทธิ์การแชร์ข้อมูลร่วมกันผ่านระบบเครือข่ายของเครื่องคอมพิวเตอร์ส่วนบุคคล

(๒) ถอนการติดตั้งโปรแกรมอัปโหลดไฟล์ FTP ออกหรืองดใช้ชั่วคราว

(๓) หากผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ทำงานผิดปกติ นำเครื่องคอมพิวเตอร์ที่สงสัยว่าติดมัลแวร์ (Malware) ออกจากระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน เพื่อป้องกันการแพร่กระจายของมัลแวร์ (Malware) ไปยังระบบเครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ลูกข่ายเครื่องอื่น ๆ

(๔) ให้ผู้ใช้งานแจ้งมายังเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้เจ้าหน้าที่ได้ดำเนินการแก้ไขโดยเร่งด่วน

(๕) หากผู้ใช้งานได้ทำการสำรองข้อมูล (Backup) ไว้ ให้เตรียมข้อมูลที่ได้สำรองไว้ให้เจ้าหน้าที่ในกรณีที่จำเป็นต้องติดตั้งระบบปฏิบัติการใหม่

๒) ผู้ดูแลระบบ (Admin)

(๑) ตัดการเชื่อมต่อระบบเครือข่ายของเครื่องคอมพิวเตอร์แม่ข่ายที่ติดไวรัส มัลแวร์ เพื่อกักกันไวรัสมัลแวร์ ไม่ให้แพร่กระจาย

(๒) ตั้งค่าไฟร์วอลล์ (Firewall) ปิดพอร์ต ๑๓๕ ๑๓๙ ๔๔๕ ๓๓๘๙ และ ๘๐๐๙ เพื่อป้องกันผู้ไม่ประสงค์ดี

(๓) ประสานงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อแจ้งปัญหาและรับคำปรึกษาเบื้องต้น

(๔) ประสานงานผู้ดูแลระบบสารสนเทศของกรมประมงทั้งหมด (ที่ยังไม่ติดไวรัส มัลแวร์) ให้อุดช่องโหว่เครื่องคอมพิวเตอร์แม่ข่าย ตรวจสอบการสำรองข้อมูล เตรียมความพร้อมในการกู้คืนระบบ และเฝ้าระวังในช่วงการแพร่กระจาย

(๕) แจ้งเวียนคู่มือการปิดช่องโหว่ของเครื่องคอมพิวเตอร์ส่วนบุคคลให้แก่หน่วยงานกรมประมง เพื่อป้องกันการโจมตีของไวรัส มัลแวร์ในระบบเครือข่าย และลดช่องโหว่ที่อาจมาจากเครื่องคอมพิวเตอร์ลูกข่าย

(๖) กู้คืนข้อมูลที่สำรองไว้ ทำการติดตั้งระบบใหม่ พร้อมทั้งซ่อมแซมแอปพลิเคชันและฐานข้อมูล

(๗) ทำการอุดช่องโหว่ อัปเดต Patch Windows

(๘) ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) บนเครื่องคอมพิวเตอร์แม่ข่ายที่กู้คืนทั้งหมด และเครื่องคอมพิวเตอร์แม่ข่ายทั้งหมดที่ติดตั้งอยู่ในห้อง Data Center กรมประมง เพื่อป้องกันการเจาะระบบและโจมตีทางระบบเครือข่ายอีกในอนาคต

(๙) เปิดระบบสารสนเทศและแจ้งผู้ใช้งานทราบ

๔. แนวทางการปฏิบัติในการป้องกันภัยคุกคามอุปกรณ์เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) และอุปกรณ์ต่อพ่วงที่สามารถเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ได้โดยตรง

๔.๑ แนวปฏิบัติเพื่อป้องกันภัยคุกคามอุปกรณ์เทคโนโลยีอินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) และอุปกรณ์ต่อพ่วงที่สามารถเชื่อมต่อผ่านระบบเครือข่ายคอมพิวเตอร์ได้โดยตรง

๑) ผู้ใช้งาน (User)

(๑) แจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อขอหมายเลขไอพีแอดเดรส (IP Address) พร้อมทั้งวัตถุประสงค์ของการใช้งานอุปกรณ์ ก่อนติดตั้งอุปกรณ์ดังกล่าวเข้ากับระบบเครือข่ายของกรมประมง

(๒) ตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) หรือให้ทันสมัย เพื่อปิดช่องโหว่ที่ร้ายแรง (Critical Vulnerability)

(๓) มีการสำรองข้อมูล (Backup) ที่ใช้งานอยู่เสมอและทดสอบการกู้คืนค่า (Recovery) ไฟล์ที่สำรองข้อมูลไว้ ว่าสามารถใช้งานได้

(๔) ตรวจสอบการทำงานของอุปกรณ์อยู่เสมอ หากเกิดความผิดปกติให้แจ้งศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒) ผู้ดูแลระบบ (Admin)

(๑) พิจารณาความเหมาะสมตามวัตถุประสงค์ ความจำเป็นในการเชื่อมต่ออุปกรณ์กับระบบเครือข่ายกรมประมง ก่อนอนุญาตติดตั้งอุปกรณ์

(๒) พิจารณาการตั้งค่าของอุปกรณ์ให้เหมาะสม ปิดบริการที่อาจจะมีผลกระทบต่อเครือข่ายของกรมประมง เช่น บริการกำหนดค่าไอพีแอดเดรสอัตโนมัติ (DHCP Server) เป็นต้น

(๓) พิจารณาการให้สิทธิเข้าถึงเครือข่ายอินเทอร์เน็ตถ้ามีความจำเป็น

(๔) ตั้งค่าค่าไฟร์วอลล์ (Firewall) เปิดพอร์ตที่จำเป็นต่อการใช้งานเท่านั้น หากมีความจำเป็นต้องเปิดให้มีการเชื่อมต่อจากภายนอก เพื่อป้องกันผู้ไม่ประสงค์ดี

(๕) ตรวจสอบและวิเคราะห์ Log File จากรายงานการพบภัยคุกคาม เพื่อวิเคราะห์สถานการณ์และเฝ้าระวังเมื่อพบว่าอุปกรณ์มีลักษณะการส่งข้อมูล (Transaction) ที่ผิดปกติหรือคาดว่าอาจติดมัลแวร์ (Malware) ให้แจ้งเจ้าของเครื่องคอมพิวเตอร์และเข้าดำเนินการแก้ไขโดยเร่งด่วน

(๖) ตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) หรือให้ทันสมัย เพื่อปิดช่องโหว่ที่ร้ายแรง (Critical Vulnerability)

(๗) มีการจำกัดสิทธิ์และการยืนยันตัวตนในการเข้าใช้งานระบบเครือข่ายคอมพิวเตอร์ขององค์กรเพื่อป้องกันการแอบเข้ามาใช้งานของผู้ที่ไม่ประสงค์ดี (ถ้าอุปกรณ์รองรับ)

๔.๒ แนวปฏิบัติเมื่อเกิดเหตุการณ์

๑) ผู้ใช้งาน (User)

(๑) ปิดอุปกรณ์ หรือตัดการเชื่อมต่ออุปกรณ์ออกจากเครือข่ายกรมประมง

(๒) ติดต่อผู้ให้บริการ หรือผู้รับจ้างบำรุงรักษาอุปกรณ์

(๓) จัดทำบันทึกเหตุการณ์ความผิดปกติจัดส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อยประกอบด้วย

- วัน เวลา ที่พบความผิดปกติ
- รายละเอียดความผิดปกติ
- วิธีการแก้ไข (หากแก้ไขได้เอง)
- ลักษณะการใช้งาน
- ผู้ใช้งาน

๒) ผู้ดูแลระบบ (Admin)

(๑) ตัดการเชื่อมต่ออุปกรณ์จากระบบเครือข่ายกรมประมง (หากผู้ใช้งานไม่สามารถตัดการเชื่อมต่อได้เอง) เพื่อบรรเทาผลกระทบความเสียหาย

(๒) ตรวจสอบไฟร์วอลล์ (Firewall) หรืออุปกรณ์ป้องกันการโจมตีไซเบอร์อื่น ๆ เพื่อหาสาเหตุของเหตุการณ์

(๓) ประสานงานผู้ดูแล/ใช้งานอุปกรณ์ลักษณะเดียวกันให้เฝ้าระวัง

(๔) หากผลกระทบเป็นในวงกว้างต้องประสานงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อแจ้งปัญหาและรับคำปรึกษาเบื้องต้น

(๕) แจ้งเวียนคู่มือการแก้ไขปัญหาแก่ผู้ดูแล/ใช้งานอุปกรณ์ลักษณะเดียวกันเมื่อพบต้นเหตุของปัญหา

(๖) สนับสนุนกู้คืนข้อมูลที่สำรองไว้ ทำการติดตั้ง ตั้งค่าอุปกรณ์ให้มีความมั่นคงปลอดภัย

(๗) เชื่อมต่ออุปกรณ์ดังกล่าวเข้ากับเครือข่ายกรมประมง และเปิดใช้งาน

๕. แนวทางการปฏิบัติในการป้องกันภัยคุกคามโครงสร้างพื้นฐานที่สำคัญด้านเทคโนโลยีสารสนเทศกรมประมง (Information Technology Infrastructure)

๕.๑ แนวปฏิบัติเพื่อป้องกันภัยคุกคามโครงสร้างพื้นฐานที่สำคัญด้านเทคโนโลยีสารสนเทศกรมประมง (Information Technology Infrastructure)

๑) ผู้ดูแลระบบ (Admin)

(๑) จัดทำ ปรับปรุง รายการอุปกรณ์ที่เป็นโครงสร้างพื้นฐานที่สำคัญด้านเทคโนโลยีสารสนเทศกรมประมง (Information Technology Infrastructure) โดยหลักการสำคัญคือหากอุปกรณ์ดังกล่าวเสียหาย หรือหยุดให้บริการจะทำให้กระทบต่อผู้ใช้งานจำนวน ๑ หน่วยงาน (ระดับกองขึ้นไป)

(๒) ตรวจสอบการทำงานของอุปกรณ์ที่เป็นโครงสร้างพื้นฐานที่สำคัญด้านเทคโนโลยีสารสนเทศกรมประมง โดยเชื่อมต่ออุปกรณ์เข้ากับโปรแกรมตรวจสอบและเฝ้าระวังเครือข่าย (Network monitoring tools) เพื่อติดตามสถานะการทำงานเป็นประจำ และแจ้งเตือนอัตโนมัติเมื่ออุปกรณ์ดังกล่าวมีการทำงานผิดปกติ

(๓) จัดหาอุปกรณ์ที่เป็นโครงสร้างพื้นฐานที่สำคัญด้านเทคโนโลยีสารสนเทศกรมประมง จำนวนไม่น้อยกว่า

๒ ชิ้น เพื่อเพิ่มประสิทธิภาพการให้บริการและสามารถทำงานทดแทนกันได้อัตโนมัติเมื่อมีอุปกรณ์ชิ้นใดเสียหาย

(๔) ตรวจสอบและอัปเดตระบบปฏิบัติการ (Operating System) อุปกรณ์ให้ทันสมัย เพื่อปิดช่องโหว่ที่ร้ายแรง (Critical Vulnerability)

(๕) มีการสำรองข้อมูล (Backup) ที่ใช้งานอยู่เสมอและทดสอบการกู้คืนค่า (Recovery) ไฟล์ที่สำรองข้อมูลไว้ ว่าสามารถใช้งานได้

(๖) ตรวจสอบและวิเคราะห์ Log File จากรายงานการพบภัยคุกคาม เพื่อวิเคราะห์สถานการณ์และเฝ้าระวัง เมื่อพบว่าอุปกรณ์มีลักษณะการส่งข้อมูล (Transaction) ที่ผิดปกติหรือคาดว่าอาจโดนโจมตีด้านไซเบอร์และแจ้งผู้ให้บริการ หรือผู้รับจ้างบำรุงรักษา

(๗) มีการจำกัดสิทธิ์และการยืนยันตัวตนในการเข้าใช้งานอุปกรณ์ เพื่อป้องกันการแอบเข้ามาใช้งานของผู้ที่ไม่ประสงค์ดี

๕.๒ แนวปฏิบัติเมื่อเกิดเหตุการณ์

๑) ผู้ดูแลระบบ (Admin)

(๑) ปิดอุปกรณ์ หรือตัดการเชื่อมต่ออุปกรณ์ออกจากเครือข่ายกรมประมง และติดตั้งสลับอุปกรณ์ลักษณะเดียวกันทดแทน

(๒) ติดต่อผู้ให้บริการ หรือผู้รับจ้างบำรุงรักษาอุปกรณ์ หรือเจ้าของผลิตภัณฑ์

(๓) จัดทำบันทึกเหตุการณ์ความผิดปกติจัดส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างน้อยประกอบด้วย

- วัน เวลา ที่พบความผิดปกติ
- รายละเอียดความผิดปกติ
- วิธีการแก้ไข (หากแก้ไขได้เอง)
- ลักษณะการใช้งาน
- ผู้ใช้งาน

(๔) ตรวจสอบไฟร์วอลล์ (Firewall) หรืออุปกรณ์ป้องกันการโจมตีไซเบอร์อื่น ๆ เพื่อหาสาเหตุของเหตุการณ์

(๕) ตรวจสอบอุปกรณ์ลักษณะเดียวกันและให้เฝ้าระวัง

(๖) หากผลกระทบเป็นในวงกว้างต้องประสานงานศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อแจ้งปัญหาและรับคำปรึกษาเบื้องต้น

(๗) ดำเนินการแก้ไข ปรับปรุง ระบบปฏิบัติการ หรือซอฟต์แวร์ของอุปกรณ์ให้เป็นรุ่นล่าสุด

(๘) ดำเนินการแก้ไข ปรับปรุง การตั้งค่าอุปกรณ์ให้เป็นไปตามข้อปฏิบัติที่ดี หรือตามวิธีการแก้ไขปัญหาที่พบจากเจ้าของผลิตภัณฑ์

(๙) กู้คืนข้อมูลที่สำรองไว้ ทำการติดตั้ง ตั้งค่าอุปกรณ์ให้มีความมั่นคงปลอดภัย

(๑๐) เชื่อมต่ออุปกรณ์ดังกล่าวเข้ากับเครือข่ายกรมประมง และเปิดใช้งาน