ที่ นร ๐๕๐๕/ว(ล) ๘๖๔๒

สำนักเลขาธิการคณะรัฐมนตรี
ทำเนียบรัฐบาล กทม. ๑๐๓๐๐

๒๑ มีนาคม ๒๕๖๖

เรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕

เรียน รัฐมนตรีว่าการกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม

อ้างถึง หนังสือสำนักเลขาธิการคณะรัฐมนตรี ลับ ที่ นร ๐๕๐๕/ว(ล) ๒๐๑๕๙ ลงวันที่ ๑๖ สิงหาคม ๒๕๖๕

สิ่งที่ส่งมาด้วย สำเนาหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๘๐๐/๘๘๖ ลงวันที่ ๘ มีนาคม ๒๕๖๖

ตามที่ได้แจ้งมติคณะรัฐมนตรี (๑๖ สิงหาคม ๒๕๖๕) เกี่ยวกับรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงตุลาคม ๒๕๖๔ - มีนาคม ๒๕๖๕ มาเพื่อทราบ ความละเอียดแจ้งแล้ว นั้น

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้เสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ไปเพื่อคณะรัฐมนตรีทราบ ความละเอียดปรากฏตามสำเนาหนังสือที่ส่งมาด้วยนี้

คณะรัฐมนตรีได้มีมติเมื่อวันที่ ๒๑ มีนาคม ๒๕๖๖ รับทราบตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

จึงเรียนมาเพื่อโปรดทราบ

มอบ ผช.ปคร ดำเนินการ

(ศาสตราจารย์สิริฤกษ์ ทรงศิวิไล)
ปอว.
3 เมย. 2566

ขอแสดงความนับถือ

ปริยนงคราญ จงธรรมคุณ

(นางสาวปริยนงคราญ จงธรรมคุณ)
ผู้อำนวยการกองพัฒนายุทธศาสตร์และติดตามนโยบายพิเศษ ปฏิบัติราชการแทน
เลขาธิการคณะรัฐมนตรี

กองพัฒนายุทธศาสตร์และติดตามนโยบายพิเศษ
โทร. ๐ ๒๒๘๐ ๙๐๐๐ ต่อ ๑๗๐๓ (จิดานุช), ๑๕๒๒ (เฉลิมขวัญ)
โทรสาร ๐ ๒๒๘๐ ๑๔๔๖
www.soc.go.th
ไปรษณีย์อิเล็กทรอนิกส์ saraban@soc.go.th

มอบ ปอว. แจ้งหน่วยงานที่เกี่ยวข้อง

(นายดนุช ตันเทอดทิตย์)
เลขา รมว.อว.

๓๑ มี.ค. ๒๕๖๖

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ที่ สกมช ๐๘๐๐/๘๘๖

๘ มีนาคม ๒๕๖๖

เรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอเรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ มาเพื่อคณะรัฐมนตรีทราบ โดยเรื่องนี้เข้าข่ายที่จะต้องนำเสนอคณะรัฐมนตรีตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่อง และการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) รวมทั้ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” ทั้งนี้ พลเอก ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี/ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้เห็นชอบให้นำเรื่องดังกล่าวเสนอคณะรัฐมนตรีด้วยแล้ว

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

ตามอ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” นั้น คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงขอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ให้คณะรัฐมนตรีเพื่อรับทราบ โดยมีสาระสำคัญประกอบด้วย ข้อมูลทั่วไป สรุปสถานการณ์ของภัยคุกคามทางไซเบอร์ในประเทศไทย ผลการดำเนินการที่สำคัญ บทวิเคราะห์สถานการณ์ แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อใช้เป็นข้อมูลสำหรับการพัฒนาแนวทางและมาตรการในการป้องกัน รับมือ เพื่อลดความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานซึ่งมีภารกิจหรือบริการที่ส่งผลกระทบถึงประชาชนต่อไป

/๒. สาระสำคัญ...

๒. <u>สาระสำคัญ ข้อเท็จจริงและข้อกฎหมาย</u>

๒.๑ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้อง ในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยได้นำเสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ในการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๑/๒๕๖๖ เมื่อวันพฤหัสบดีที่ ๕ มกราคม ๒๕๖๖ เวลา ๑๐.๐๐ น. ณ ห้องประชุม ชั้น ๒ มูลนิธิอนุรักษ์ป่ารอยต่อ ๕ จังหวัด โดยที่ประชุมมีมติเห็นชอบให้รายงานคณะรัฐมนตรีเพื่อทราบ

๒.๒ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ในภารกิจเกี่ยวกับการป้องกัน รับมือ แก้ไขปัญหา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ รวมทั้งสิ้น ๕๕๑ เหตุการณ์ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย โดยสรุปสาระสำคัญ ได้ดังนี้

๒.๒.๑ สถิติเหตุการณ์ภัยคุกคามทางไซเบอร์ ที่ได้ดำเนินการและตรวจพบมากที่สุด แบ่งเป็นประเภทของภัยคุกคามทางไซเบอร์ ได้ดังนี้

๒.๒.๑.๑ ประเภท Hacked Website จำนวนรวม ๓๖๗ เหตุการณ์ แบ่งออกเป็นประเภท Gambling (การพนันออนไลน์) จำนวน ๑๘๖ เหตุการณ์, Website Defacement จำนวน ๑๒๕ เหตุการณ์, Website Phishing จำนวน ๓๘ เหตุการณ์ และ Website Malware ๑๘ เหตุการณ์

๒.๒.๑.๒ ประเภทจุดอ่อนช่องโหว่ (Vulnerability) จำนวน ๖๓ เหตุการณ์

๒.๒.๑.๓ ประเภทข้อมูลรั่วไหล (Data Breach) จำนวน ๔๘ เหตุการณ์

๒.๒.๑.๔ ประเภท Ransomware จำนวน ๒๑ เหตุการณ์

๒.๒.๑.๕ ประเภท Emotet Malware จำนวน ๙ เหตุการณ์

๒.๒.๑.๖ ประเภท Command and Control Server จำนวน ๖ เหตุการณ์

๒.๒.๑.๗ ประเภทอื่น ๆ จำนวน ๓๗ เหตุการณ์

๒.๒.๒ สถิติการปฏิบัติงานในการสนับสนุนช่วยแก้ไขปัญหาและรับมือกับภัยคุกคามทางไซเบอร์ โดยสรุปได้ ดังนี้

๒.๒.๒.๑ แจ้งเตือนเหตุการณ์ ให้คำปรึกษา และแนะนำในการแก้ไขปัญหา จำนวน ๔๖๗ เหตุการณ์

๒.๒.๒.๒ การแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๔๓ รายงาน

๒.๒.๒.๓ การประเมินความเสี่ยง และทดสอบการเจาะระบบเพื่อหาจุดอ่อนช่องโหว่ให้กับหน่วยงานของรัฐ จำนวน ๒๙ หน่วยงาน

๒.๒.๒.๔ การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ จำนวน ๑๒ ครั้ง

๒.๒.๒.๕ การเผยแพร่ข้อมูลภัยคุกคามและข่าวสารที่เป็นประโยชน์ต่อสาธารณะ จำนวน ๓๒๒ รายงาน

๒.๒.๒.๖ ประสานงานเพื่อให้ระงับการเผยแพร่เว็บไซต์ปลอมหรือเลียนแบบ จำนวน ๔๓ หน่วยงาน

/๒.๒.๓ ประเภท...

๒.๒.๓ ประเภทของหน่วยงานที่ถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ สรุปได้ดังนี้

๒.๒.๓.๑ ด้านการศึกษา จำนวน ๒๑๑ เหตุการณ์

๒.๒.๓.๒ หน่วยงานของรัฐที่ไม่ใช่ CII จำนวน ๑๓๕ เหตุการณ์

๒.๒.๓.๓ ด้านสาธารณสุข จำนวน ๖๗ เหตุการณ์

๒.๒.๓.๔ ผู้ประกอบการที่เป็นบริษัทเอกชน สัญชาติไทย จำนวน ๒๔ เหตุการณ์

๒.๒.๓.๕ ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์ จำนวน ๑๒ เหตุการณ์

๒.๒.๓.๖ ด้านพลังงานและสาธารณูปโภค จำนวน ๑๑ เหตุการณ์

๒.๒.๓.๗ ด้านการขนส่งและโลจิสติกส์ จำนวน ๑๐ เหตุการณ์

๒.๒.๓.๘ ผู้ผลิตซอฟต์แวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี จำนวน ๙ เหตุการณ์

๒.๒.๓.๙ เทคโนโลยีสารสนเทศและโทรคมนาคม จำนวน ๕ เหตุการณ์

๒.๒.๓.๑๐ ด้านบริการภาครัฐ จำนวน ๔ เหตุการณ์

๒.๒.๓.๑๑ ด้านการเงินการธนาคาร จำนวน ๔ เหตุการณ์

๒.๒.๓.๑๒ ผู้ประกอบการธุรกิจอีคอมเมิร์ซ จำนวน ๓ เหตุการณ์

๒.๒.๓.๑๓ ด้านอื่น ๆ จำนวน ๙ เหตุการณ์

๒.๒.๔ แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ จากเหตุการณ์ภัยคุกคามทางไซเบอร์ จำนวน ๕๕๑ เหตุการณ์ มีข้อมูลที่สำคัญสรุปได้ดังนี้

๒.๒.๔.๑ การโจมตีทางไซเบอร์ที่ถูกตรวจพบมากที่สุด ได้แก่ การโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) หน่วยราชการและหน่วยงานสำคัญซึ่งมีมากกว่าการโจมตีรูปแบบอื่น ๆ โดยคิดเป็น ๒ ใน ๓ ของการโจมตีทางไซเบอร์ที่ตรวจพบในประเทศไทย อันดับหนึ่ง ได้แก่ การโจมตีในลักษณะทำไปเพื่อการแฝงหน้าเว็บพนันออนไลน์ในเว็บไซต์ของหน่วยงาน เพื่อเพิ่มโอกาสและประสิทธิภาพการค้นหาผ่าน Search Engine ส่วนอันดับสอง ได้แก่ การโจมตีโดยเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ของหน่วยงาน เพื่อใช้เป็นพื้นที่ทดสอบความสามารถของแฮ็กเกอร์หรือเป็นผลลัพธ์จากการเคลื่อนไหวทางการเมืองของกลุ่มต่าง ๆ นอกจากนี้ ยังพบการโจมตีด้วยการแฮ็กเว็บไซต์แบบอื่น ๆ ที่น่าสนใจ เช่น การสร้างหน้าเว็บไซต์เพื่อหลอก Phishing อยู่บนเว็บไซต์หน่วยงานของรัฐ และการฝังมัลแวร์อันตรายบนหน้าเว็บไซต์หน่วยงานที่อาจหลอกให้ผู้เข้าถึงดาวน์โหลดไปติดตั้งได้ เป็นต้น

๒.๒.๔.๒ หน่วยงานที่พบการโจมตีทางไซเบอร์สูงสุด ได้แก่ หน่วยงานด้านการศึกษา และหน่วยงานด้านสาธารณสุข ซึ่งมีเว็บไซต์และระบบต่าง ๆ ให้บริการอยู่เป็นจำนวนมาก และใช้เว็บไซต์เป็นสื่อประชาสัมพันธ์หลัก การบริหารงานในส่วนที่เกี่ยวข้องกับระบบไอทีมีความเป็นเอกเทศทำให้การดูแลจากหน่วยงานส่วนกลางทำได้ยาก เมื่อมีการพัฒนาระบบที่ต้องดำเนินการเอง หรือว่าจ้างบุคคลจากภายนอกนั้น จะมีการปรับปรุงแค่เฉพาะเนื้อหาในเว็บไซต์เพียงอย่างเดียว จึงขาดการดูแลรักษาระบบและการตรวจสอบอย่างสม่ำเสมอ

๒.๒.๔.๓ สถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนและมีความสัมพันธ์กับความมั่นคงปลอดภัยทางไซเบอร์ โดยพบว่า อาชญากรทางไซเบอร์ในประเทศไทย ได้ใช้เทคนิคผสมผสานการ Phishing และ Social Engineering หลายรูปแบบเพื่อหลอกลวงเหยื่อ และนอกจากจะได้ไปซึ่งทรัพย์สินของเหยื่อแล้ว การกระทำดังกล่าว ทำให้เกิดผลกระทบต่อการรักษาความลับของข้อมูลส่วนตัว

/รวมถึงความ...

รวมถึงความปลอดภัยในตัวระบบและอุปกรณ์ของเหยื่อเช่นเดียวกัน อาทิเช่น กรณีมิจฉาชีพหลอกขอรหัสผ่านส่วนตัวของเหยื่อผ่านโทรศัพท์หรือผ่านแอปพลิเคชันไลน์ การปลอมแปลงเว็บไซต์หน่วยงานของรัฐโดยตั้งชื่อโดเมนให้คล้ายคลึง และมีเนื้อหาเลียนแบบเว็บไซต์จริง เพื่อหลอกเอาข้อมูลส่วนบุคคล หรือหลอกให้ดาวน์โหลดไฟล์ที่มีมัลแวร์บนหน้าเว็บไซต์ การส่งลิงก์ Phishing ที่แฝงโฆษณา หรือมีชื่อผู้ส่งเลียนแบบ Platform ธนาคาร เพื่อพาเหยื่อไปในหน้าเว็บไซต์ให้กรอกข้อมูลส่วนบุคคลหรือมีการดาวน์โหลดมัลแวร์ลงไปที่เครื่อง การจำหน่ายข้อมูลส่วนบุคคลที่ได้มาด้วยวิธีการต่างๆ ใน Dark web หรือ Communities ต่าง ๆ เป็นต้น

๒.๒.๔.๔ การโจมตีด้วย Ransomware ที่เกิดขึ้นกับหน่วยงานภาครัฐที่มีความสำคัญ และภาคเอกชนที่เป็นธุรกิจที่มีชื่อเสียง มีทุนจดทะเบียนสูง กระจายตัวในหลายประเภทอุตสาหกรรม โดยเมื่อเกิดเหตุ Ransomware ขึ้นแล้ว ความเสียหายที่เห็นชัดเจนของแต่ละหน่วยงาน คือการที่ไม่สามารถเข้าระบบเพื่อใช้งานข้อมูลที่สำคัญได้ และบางแห่งไม่สามารถใช้งานระบบสำรองได้ นอกจากนี้ ยังส่งผลกระทบต่อการบริหารจัดการและทำงานของระบบสารสนเทศในภายรวมของหน่วยงาน ซึ่งหน่วยงานแต่ละหน่วยจะต้องใช้ระยะเวลาในการแก้ไขปัญหาจากการโจมตีด้วย Ransomware ที่ยาวนาน และอาจต้องพึ่งพาผู้เชี่ยวชาญจากบุคคลฝ่ายนอกอีกด้วย

๒.๒.๕ แนวทางการจัดการภัยคุกคามทางไซเบอร์ ในการดำเนินมาตรการที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ (incident handling) ได้มีการแนะนำให้กับหน่วยงานต่าง ๆ ดำเนินการให้มีความสอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ และเป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ โดยแบ่งขั้นตอนได้เป็น ๔ ขั้นตอนหลัก ดังนี้

(๑) การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

(๒) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

(๓) การระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication and recovery)

(๔) การดำเนินกิจกรรมภายหลังการระงับภัยคุกคามทางไซเบอร์ (post-incident activity)

๒.๒.๖ ข้อแนะนำในการแก้ไขปัญหาที่สำคัญจากแนวโน้มสถานการณ์ทางไซเบอร์ที่สำคัญในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ สรุปได้ดังนี้

๒.๒.๖.๑ การถูกโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) เป็นเรื่องที่ผู้ดูแลระบบของหน่วยงานควรให้ความสนใจกับการปรับปรุงแพทช์ (PATCH) ของระบบปฏิบัติการ หรือระบบบริหารจัดการเว็บไซต์ (CMS) ให้เป็นปัจจุบัน ทบทวนการใช้งาน Themes หรือ Plug-in ต่าง ๆ ที่อาจมีช่องโหว่ การเปลี่ยนแปลงแก้ไขรหัสผ่านต่าง ๆ ทำให้ยากต่อการคาดเดา ตรวจสอบการนำเข้าไฟล์ต่าง ๆ สำหรับผู้ใช้งานเว็บไซต์ให้อนุญาตเฉพาะไฟล์ที่ต้องการเท่านั้น รวมไปถึงใช้วิธีการเข้ารหัสข้อมูลที่มีความสำคัญต่าง ๆ ด้วย

๒.๒.๖.๒ การดูแลเว็บไซต์และระบบที่เกี่ยวข้องของหน่วยงานต่าง ๆ โดยเฉพาะหน่วยงานที่มีความเป็นเอกเทศนั้น หน่วยงานส่วนกลางควรมีการกำหนดนโยบายเกี่ยวกับการดูแลและพัฒนาเว็บไซต์ ซึ่งหากจะดำเนินการเองหรือว่าจ้างบุคคลภายนอกแล้ว ควรให้มีการดูแลรักษาระบบและตรวจสอบอย่างสม่ำเสมอ รวมไปถึงแนวทางการเขียนร่างขอบเขตของงาน (TOR) และการกำหนดคุณสมบัติเพื่อการจัดจ้างทำเว็บไซต์หรือพัฒนาระบบที่เกี่ยวข้องที่ต้องคำนึงถึงเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วย

/๒.๒.๖.๓ ในเรื่อง...

๒.๒.๖.๓ ในเรื่องสถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนนั้น การสร้างความรู้ความเข้าใจ และการให้ความตระหนักรู้กับประชาชนเป็นสิ่งที่สำคัญมาก โดยเฉพาะการสร้างการรับรู้เกี่ยวกับรูปแบบและวิธีการที่เหล่ามิจฉาชีพใช้ในการหลอกลวง รวมไปถึงประชาชนจะต้องรับทราบถึงความเสียหายหรือผลกระทบจากการที่ตนเองตกเป็นเหยื่อหรือถูกหลอก ซึ่งนอกจากจะส่งผลทำให้สูญเสียทรัพย์สินแล้ว ยังเป็นผลสัมพันธ์ไปถึงความมั่นคงปลอดภัยทางไซเบอร์ที่จะถูกแฮ็กเกอร์นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในการเข้าถึงระบบต่าง ๆ ได้

๒.๒.๖.๔ ในเรื่อง Ransomware หน่วยงานต่าง ๆ สามารถลดความเสี่ยงได้โดยการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP) และปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ในการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยให้ความสำคัญกับการสำรองข้อมูล และตรวจสอบอย่างสม่ำเสมอ

๓. <u>ประเด็นด้านกฎหมาย</u>

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ”

๔. <u>ข้อเสนอส่วนราชการ</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้วเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) จึงเห็นควรนำเสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ต่อที่ประชุมคณะรัฐมนตรีเพื่อรับทราบ

จึงเรียนมาเพื่อโปรดนำกราบเรียนนายกรัฐมนตรีเพื่อเสนอคณะรัฐมนตรีทราบต่อไป

ขอแสดงความนับถือ

พลเอก

(ประวิตร วงษสุวรรณ)
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕
E-Mail : ncert@ncsa.or.th

QR code เอกสารแนบ

สำเนาถูกต้อง

(นางสาวเฉลิมขวัญ ทองจันทร์)
นักวิเคราะห์นโยบายและแผนชำนาญการพิเศษ
๑๑ มิ.ย. ๖๔

รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ห้วง ต.ค. 64 – ก.ย. 65

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)

สำนักงานคณะกรรมการการรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ

Email: ncert@ncsa.or.th
Website: http://www.ncsa.or.th

120 ชั้น 7 อาคารรัฐประศาสนภักดี (อาคารบี) ศูนย์ราชการเฉลิมพระเกียรติ
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

NCSA สกมช

บทนำ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ภายใต้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ได้จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วง 1 ตุลาคม 2564 ถึง 30 กันยายน 2565 ซึ่งเป็นไปตามมาตรา 9 (12) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อเสนอต่อคณะรัฐมนตรีทราบ โดยมีสาระสำคัญประกอบด้วย ข้อมูลทั่วไป สรุปสถานการณ์ภัยคุกคามทางไซเบอร์ในประเทศไทย ผลการดำเนินการที่สำคัญ บทวิเคราะห์สถานการณ์ แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ ดังรายละเอียดที่ปรากฏอยู่ในรายงานฉบับนี้

หวังเป็นอย่างยิ่งว่า ข้อมูลดังกล่าวจะเป็นประโยชน์ต่อการพัฒนาแนวทางและมาตรการในการป้องกันรับมือ เพื่อลดความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน ซึ่งมีภารกิจหรือบริการที่ส่งผลกระทบถึงประชาชนได้ต่อไป

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

กันยายน 2565

สารบัญ

บทที่ 1
เกี่ยวกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

1. การก่อตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดให้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ "Thailand National CERT" เรียกโดยย่อว่า ศปช. ขึ้น เป็นหน่วยงานภายในสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ได้มีประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การจัดตั้งหน้าที่และอำนาจของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ พ.ศ. 2564 เพื่อจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ เมื่อวันที่ 11 สิงหาคม 2564

2. อำนาจหน้าที่

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ได้กำหนดให้ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ มีหน้าที่และอำนาจรวมทั้งให้มีการดำเนินมาตรการในด้านต่าง ๆ ดังต่อไปนี้

1. การดำเนินมาตรการเชิงรุกเพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ให้เป็นไปตามหลักเกณฑ์ ดังนี้

1.1 ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานภายใต้การดูแลเพื่อเฝ้าระวังติดตามและเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

1.2 เป็นศูนย์กลางเครือข่ายข้อมูลและส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยอาจประสานงานหรือร่วมมือกับเครือข่ายหรือภาคี ทั้งในประเทศและต่างประเทศเพื่อรับ ส่งต่อ หรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

1.3 จัดทำข้อมูลทางสถิติด้านการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตลอดจนข้อมูลการแจ้งเตือนที่สำคัญและข้อมูลอื่น ๆ ที่เกี่ยวข้องเพื่อเผยแพร่ต่อสาธารณะ

1.4 วิเคราะห์และตรวจสอบข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ดำเนินการเพื่อป้องกันปัญหาที่อาจเกิดขึ้น รวมถึงการเผยแพร่ข้อมูลที่มีความจำเป็นเพื่อให้หน่วยงานภายใต้การดูแล

สามารถดำเนินมาตรการป้องกันหรือจัดการกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น การให้คำแนะนำแก่หน่วยงานดังกล่าวในการตรวจจับการบุกรุกและการวิเคราะห์ข้อมูล เป็นต้น

1.5 ให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น หรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานภายใต้การดูแล ดำเนินการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบงานที่มีความสำคัญอื่น ๆ ได้อย่างทันท่วงที

1.6 ติดตามความก้าวหน้าด้านเทคโนโลยีต่าง ๆ เพื่อจัดทำข้อเสนอแนะเกี่ยวกับการป้องกันภัยคุกคามทางไซเบอร์ หรือแนวปฏิบัติพื้นฐานในการป้องกันหรือเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

1.7 เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล หรือเมื่อได้รับการประสานงานในกรณีที่คาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้นกับหน่วยงานดังกล่าว ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ อาจพิจารณาดำเนินการ ดังนี้

(1) รวบรวมข้อมูล ติดตาม วิเคราะห์ และประมวลผลข้อมูลเพื่อทำวิจัยเชิงรุกเกี่ยวกับรูปแบบของการเกิดภัยคุกคามทางไซเบอร์ เพื่อประเมินผลกระทบและแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ

(2) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินมาตรการป้องกันตามแนวทางปฏิบัติที่ดี เพื่อเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

(3) ประเมินความเสี่ยงและช่องโหว่ที่อาจถูกใช้ในการก่อภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การจัดการช่องโหว่ การดำเนินมาตรการป้องกันหรือกระทำการอื่นใดเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

(4) ตรวจจับเหตุการณ์ที่อาจนำมาสู่การบุกรุก วิเคราะห์สิ่งบอกเหตุการณ์ หรือดำเนินการอื่นใดที่เกี่ยวข้อง เพื่อตรวจสอบโปรแกรมหรือค้นหาสิ่งที่ไม่พึงประสงค์ ซึ่งอาจเป็นอันตรายต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือระบบงานที่มีความสำคัญอื่น

2. ดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นให้เป็นไปตามหลักเกณฑ์ ดังนี้

2.1 เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ และประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที ตลอดจนให้การสนับสนุนข้อมูลต่าง ๆ ที่จำเป็นแก่หน่วยงานดังกล่าว เพื่อดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์ โดยจัดให้มีช่องทางในการรับ และแจ้งเหตุผ่านระบบอิเล็กทรอนิกส์ที่กำหนดขึ้นโดยเฉพาะหรือช่องทางอื่นใด ตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติกำหนด

2.2 พิจารณาความเหมาะสมในการกำหนดระดับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ตามที่ได้รับแจ้งจากหน่วยงานภายใต้การดูแล โดยอาจพิจารณากำหนดความเร่งด่วนตามที่ได้รับแจ้ง หรือกำหนดความเร่งด่วนขึ้นใหม่จากลักษณะหรือผลกระทบจากภัยคุกคามทางไซเบอร์ และให้คำแนะนำในการกำหนดแผนการรับมือและแก้ไขภัยคุกคามทางไซเบอร์ที่เหมาะสมเพื่อจำกัดขอบเขตความเสียหาย

2.3 ติดตามการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ ผลกระทบเกี่ยวกับภัยคุกคามทางไซเบอร์ และผลการตอบสนองและรับมือเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

3. การดำเนินมาตรการด้านการบริหารจัดการคุณภาพเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามหลักเกณฑ์ ดังนี้

3.1 ผลักดันและสนับสนุนให้เกิดการสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อนำไปสู่การดำเนินมาตรการในการป้องกันและการรักษาความมั่นคงปลอดภัยไซเบอร์

3.2 ยกระดับความรู้ความสามารถของหน่วยงานภายใต้การดูแล เพื่อเตรียมความพร้อมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และสามารถยกระดับการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศและระบบงานที่มีความสำคัญอื่น ๆ

3.3 เมื่อได้รับการร้องขอจากหน่วยงานภายใต้การดูแล ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ อาจพิจารณาดำเนินการ ดังนี้

(1) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการประเมินความเสี่ยงของการเกิดภัยคุกคามทางไซเบอร์ โดยใช้กระบวนการเรียนรู้ที่ได้รับจากการดำเนินมาตรการเชิงรุก เพื่อป้องกันและเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ และการดำเนินมาตรการเชิงรับเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เพื่อช่วยให้หน่วยงานดังกล่าว สามารถวางแผนการรับมือในกรณีที่ต้องเผชิญเหตุภัยคุกคามทางไซเบอร์

(2) ให้การช่วยเหลือ แนะนำ และสนับสนุนในการจัดทำแผนความต่อเนื่องของการดำเนินงานเพื่อรับมือในกรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ แผนการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และแผนฟื้นฟูภายหลังเกิดภัยคุกคามทางไซเบอร์

3. โครงสร้างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประกอบไปด้วย

สำนักประสานงาน ทำหน้าที่เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ และประสานงานกับหน่วยงานภายใต้การดูแล เพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที สำนักประสานงานประกอบไปด้วยหน่วยงาน ดังนี้

1. ฝ่ายประสานงานภาครัฐ เอกชน มีหน้าที่ปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานภายใต้การกำกับดูแล เพื่อเฝ้าระวัง ติดตาม และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ และให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น

2. ฝ่ายประสานความช่วยเหลือ มีหน้าที่เป็นศูนย์กลางในการรับและแจ้งเหตุเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในประเทศและต่างประเทศ และประสานงานกับหน่วยงานภายใต้การดูแลเพื่อตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์อย่างเหมาะสมและทันท่วงที

3. ฝ่ายประสานงานกิจการต่างประเทศ มีหน้าที่เป็นศูนย์กลางการส่งเสริมความร่วมมือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ โดยประสานงานหรือร่วมมือกับเครือข่ายหรือภาคีทั้งภาครัฐ เอกชน และองค์กรต่างประเทศต่าง ๆ

4. ฝ่ายบริหารจัดการข้อมูลภัยคุกคามทางไซเบอร์ มีหน้าที่เป็นศูนย์กลางเครือข่ายข้อมูลเพื่อรับ ส่งต่อ หรือแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ และเตรียมความพร้อมในการรับมือเมื่อได้รับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

5. งานสารบรรณและธุรการ มีหน้าที่ดำเนินการเกี่ยวกับงานบริหารทั่วไป งานสารบรรณ งานธุรการ งานรับ - ส่งเอกสารและพัสดุ งานประสานงานกับหน่วยงานภายในและภายนอก การปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง และปฏิบัติงานอื่น ๆ ตามที่สำนักมอบหมาย

สำนักปฏิบัติการ ทำหน้าที่ให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นและให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อนำไปสู่การจัดการช่องโหว่โดยจะทำการวิเคราะห์และตรวจสอบข่าวกรองที่เกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ในการสืบสวนสอบสวนเกี่ยวกับการกระทำความผิดและสามารถให้การช่วยเหลือ แนะนำ และสนับสนุนในการดำเนินงานของกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัลและสนับสนุนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นหรือดำเนินการฟื้นฟู เพื่อให้สามารถกลับมาดำเนินภารกิจหรือการให้บริการได้ต่อไป ภายหลังจากการระงับเหตุภัยคุกคามทางไซเบอร์นั้นได้เสร็จสิ้นลง สำนักปฏิบัติการประกอบไปด้วยหน่วยงานต่าง ๆ ดังนี้

1. ฝ่ายเฝ้าระวังความมั่นคงปลอดภัยทางไซเบอร์ มีหน้าที่ให้การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นหรือให้คำเตือนเกี่ยวกับช่องโหว่ที่อาจถูกใช้เป็นช่องทางในการก่อภัยคุกคามทางไซเบอร์ เพื่อให้หน่วยงานภายใต้การดูแลดำเนินการเพื่อให้มีการป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือระบบงานที่มีความสำคัญอื่น ๆ

2. ฝ่ายปฏิบัติการทางไซเบอร์ มีหน้าที่รวบรวมข้อมูล ติดตาม วิเคราะห์ และประมวลผลข้อมูลเพื่อทำวิจัยเชิงรุกเกี่ยวกับรูปแบบของการเกิดภัยคุกคามทางไซเบอร์ เพื่อประเมินผลกระทบและแนวโน้มของการเกิดภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ จัดทำข้อมูลทางสถิติด้านการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ตลอดจนข้อมูลการแจ้งเตือนที่สำคัญและข้อมูลอื่น ๆ ที่เกี่ยวข้อง เพื่อเผยแพร่ต่อสาธารณะ

3. ฝ่ายตอบสนองและรับมือภัยคุกคามทางไซเบอร์ มีหน้าที่ให้การช่วยเหลือ แนะนำ และสนับสนุนในการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เช่น การช่วยวิเคราะห์ต้นเหตุของภัยคุกคาม โปรไฟล์ของผู้โจมตี วิธีการระงับเหตุ การตอบโต้ ผู้บุกรุก และการกำจัดช่องโหว่ โดยอาจเข้าไปในสถานที่ที่เกิดเหตุการณ์หรือดำเนินการผ่านวิธีการทางอิเล็กทรอนิกส์

4. ฝ่ายสืบสวนและตรวจพิสูจน์หลักฐานทางไซเบอร์ มีหน้าที่สืบสวนหรือสอบสวนเกี่ยวกับการกระทำความผิดที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์และการเชื่อมโยงข้อมูลภัยคุกคามทางไซเบอร์

จากแหล่งข้อมูลต่าง ๆ ให้การช่วยเหลือ แนะนำและสนับสนุน ในการดำเนินกระบวนการทางนิติวิทยาศาสตร์ การตรวจพิสูจน์พยานหลักฐานทางดิจิทัล และปฏิบัติงานอื่น ๆ ตามที่สำนักมอบหมาย

5. งานสารบรรณและธุรการ มีหน้าที่ดำเนินการเกี่ยวกับงานบริหารทั่วไป งานสารบรรณ งานธุรการ งานรับ - ส่งเอกสารและพัสดุ งานประสานงานกับหน่วยงานภายในและภายนอก การปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้อง และปฏิบัติงานอื่น ๆ ตามที่สำนักมอบหมาย

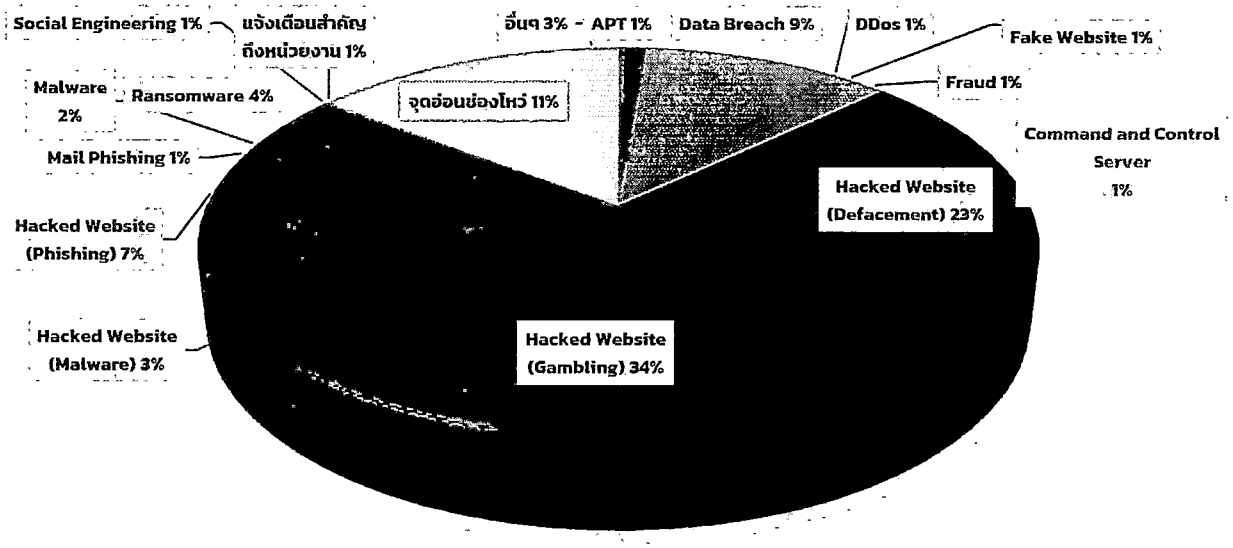
4. ทิศทาง วิสัยทัศน์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ หรือ National Computer Emergency Response Team (NCERT) มีพันธกิจทำงานร่วมกับ หน่วยงานควบคุมหรือกำกับดูแลศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หน่วยงานของรัฐ ตลอดจนหน่วยงานที่เกี่ยวข้อง เพื่อดำเนินการแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับแจ้งหรือตรวจพบ อีกทั้งให้ความสำคัญกับการพัฒนาบุคลากรเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในประเทศไทย และให้คำปรึกษาแก่หน่วยงานต่าง ๆ ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ (Critical Information Infrastructure) ในการป้องกันและแก้ไขปัญหาภัยคุกคามทางไซเบอร์ เพื่อรักษาความต่อเนื่องในการดำเนินภารกิจของหน่วยงานนั้น ๆ

บทที่ 2
สถิติและเหตุการณ์สำคัญที่เกิดขึ้นในประเทศไทย

1. สถิติภัยคุกคามทางไซเบอร์

ในห้วง ตุลาคม 2564 ถึง กันยายน 2565 สามารถแบ่งประเภทภัยคุกคามทางไซเบอร์ ที่ ศปช. ได้สนับสนุนการปฏิบัติในการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ รวมทั้งสิ้น 551 เหตุการณ์ ดังนี้



ภาพที่ 1: จำแนกการสนับสนุนการปฏิบัติของ ศปช. ตามประเภทภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคามทางไซเบอร์	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
Hacked Website - Gambling (186) ร้อยละ 34 - Website Defacement (125) ร้อยละ 23 - Website Phishing (38) ร้อยละ 7 - Website Malware (18) ร้อยละ 3	367	67
จุดอ่อนช่องโหว่ (Vulnerability)	63	11
ข้อมูลรั่วไหล (Data Breach)	48	9
Ransomware	21	4
Emotet Malware	9	2
Command and Control Server	6	1
อื่นๆ	37	6

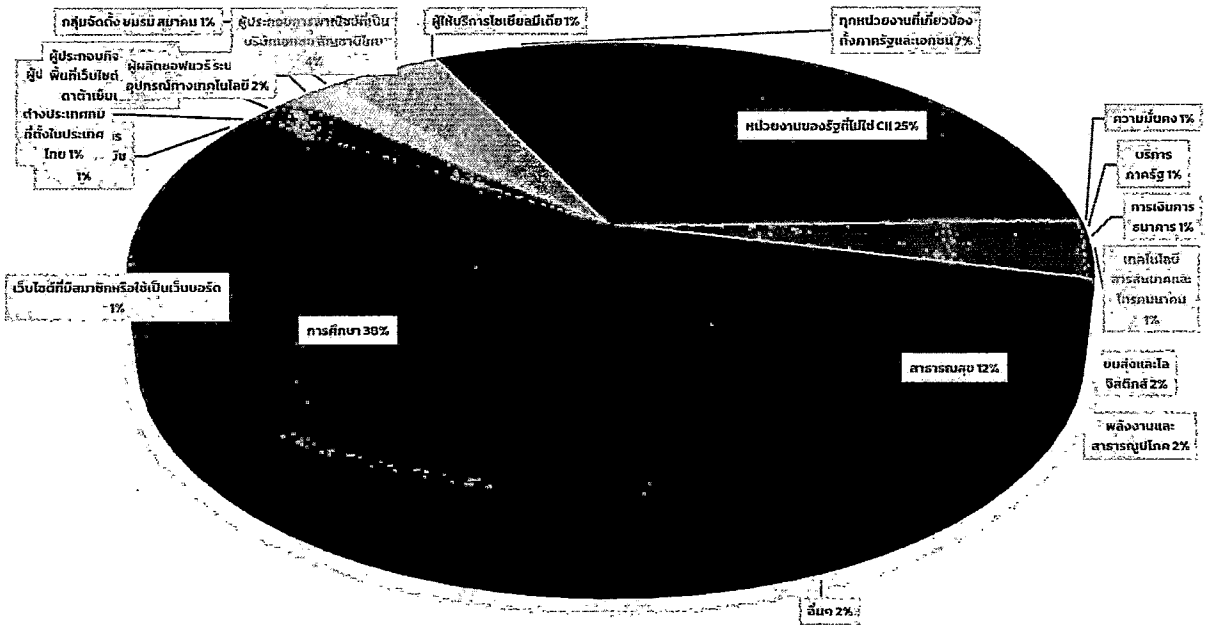
ตารางที่ 1: ตารางแสดงจำนวนประเภทภัยคุกคามทางไซเบอร์

จากการปฏิบัติ ประเภทภัยคุกคามทางไซเบอร์ที่ ศปช. ดำเนินการและตรวจพบมากที่สุด ได้แก่ Hacked Website 367 เหตุการณ์ แบ่งเป็นประเภท Gambling (การพนันออนไลน์) 186 เหตุการณ์ Website Defacement (เปลี่ยนแปลงหน้าเว็บไซต์) 125 เหตุการณ์ Website Phishing 38 เหตุการณ์ Website Malware 18 เหตุการณ์ จุดอ่อนช่องโหว่ (Vulnerability) 63 เหตุการณ์ ข้อมูลรั่วไหล (Data Breach) 48 เหตุการณ์ Ransomware 21 เหตุการณ์ Emotet Malware 9 เหตุการณ์ Command and Control Server 6 เหตุการณ์ และอื่น ๆ 37 เหตุการณ์ แบ่งเป็นหน่วยงานต่าง ๆ ได้ดังนี้

1. Hacked Website หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2 เหตุการณ์ หน่วยงานควบคุมและกำกับดูแล 2 เหตุการณ์ หน่วยงานรัฐ 332 เหตุการณ์ หน่วยงานเอกชน 27 เหตุการณ์ และแจ้งเตือนสำคัญถึงหน่วยงาน 4 เหตุการณ์

2. จุดอ่อนช่องโหว่ (Vulnerability) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2 เหตุการณ์ หน่วยงานควบคุมและกำกับดูแล 2 เหตุการณ์ หน่วยงานรัฐ 30 เหตุการณ์ หน่วยงานเอกชน 9 เหตุการณ์ และแจ้งเตือนสำคัญถึงหน่วยงาน 20 เหตุการณ์

3. ข้อมูลรั่วไหล (Data Breach) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2 เหตุการณ์ หน่วยงานควบคุมและกำกับดูแล 2 เหตุการณ์ หน่วยงานรัฐ 22 เหตุการณ์ หน่วยงานเอกชน 20 เหตุการณ์ และแจ้งเตือนสำคัญถึงหน่วยงาน 2 เหตุการณ์



ภาพที่ 2: สัดส่วนประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ

2. ประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ

ประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ	จำนวน (เหตุการณ์)	สัดส่วนร้อยละ (%)
การศึกษา	211	38
หน่วยงานของรัฐที่ไม่ใช่ CII	135	25
สาธารณสุข	67	12
แจ้งเตือนทุกหน่วยงานภายใต้ พ.ร.บ.ไซเบอร์ฯ	39	7
ผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชน สัญชาติไทย	24	4
ผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์	12	2
พลังงานและสาธารณูปโภค	11	2
ขนส่งและโลจิสติกส์	10	2
ผู้ผลิตซอฟแวร์ ระบบ หรืออุปกรณ์ทางเทคโนโลยี	9	2
เทคโนโลยีสารสนเทศและโทรคมนาคม	5	1
บริการภาครัฐ	4	1
การเงินการธนาคาร	4	1
ผู้ประกอบการธุรกิจอีคอมเมิร์ซ	3	1
อื่นๆ	9	2

ตารางที่ 2: ตารางแสดงจำนวนประเภทหน่วยงานที่ได้รับการสนับสนุน แบ่งตามภารกิจหรือบริการ

ประเภทหน่วยงานที่ถูกโจมตี แยกตามภารกิจหรือบริการที่ ศปช. ดำเนินการและตรวจพบมากที่สุด ได้แก่ การศึกษา หน่วยงานของรัฐที่ไม่ใช่ CII และสาธารณสุขตามลำดับ

3. การสนับสนุนการแก้ไขปัญหาเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์

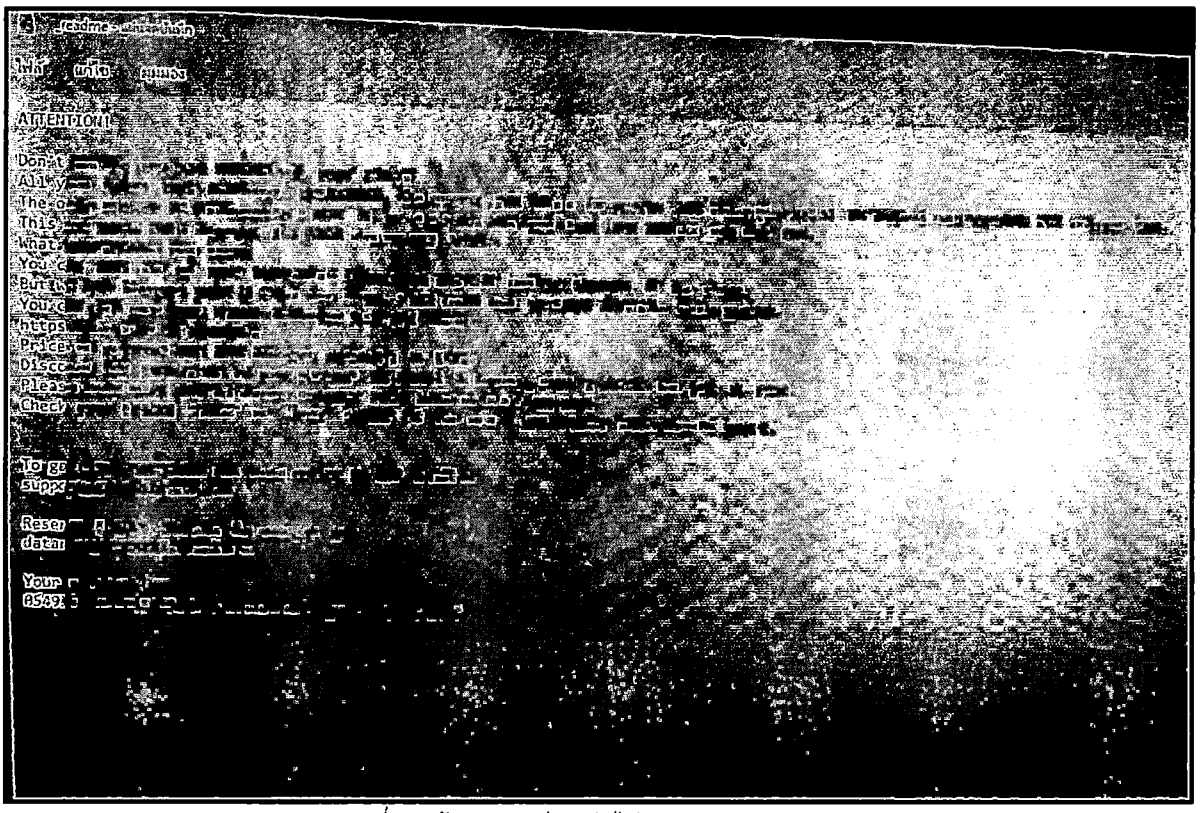
ในห้วงเดือน ตุลาคม 2564 ถึง กันยายน 2565 ศปช. ได้สนับสนุนการแก้ไขปัญหาเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น มีรายละเอียดตามภาพที่ 4

ภาพที่ 3: แสดงการปฏิบัติที่สำคัญของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

4. เหตุการณ์สำคัญด้านไซเบอร์ที่สำคัญในประเทศไทย

(1) หน่วยงานควบคุมหรือกำกับดูแล ด้านพลังงานและสาธารณูปโภคแห่งหนึ่ง ถูกโจมตีด้วย RANSOMWARE

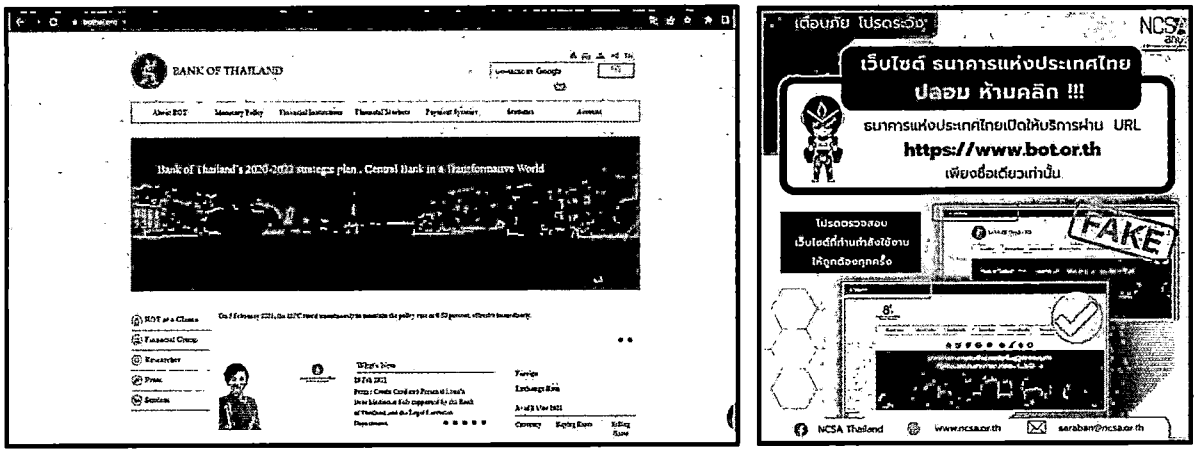
เมื่อวันที่ 5 กันยายน 2565 ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์จากหน่วยงานควบคุมหรือกำกับดูแลด้านพลังงานและสาธารณูปโภคแห่งหนึ่ง ถูกผู้ไม่ประสงค์ดีเข้าโจมตีด้วย RANSOMWARE ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการและเครื่องคอมพิวเตอร์ลูกข่ายอื่น ๆ โดยการกู้คืนไฟล์คือการซื้อเครื่องมือถอดรหัสและกุญแจที่ไม่ซ้ำกัน จากการตรวจสอบพบข้อมูลตัวอย่าง เช่น รูปภาพ ฐานข้อมูลเอกสารและอื่น ๆ ที่สำคัญ โดยผู้โจมตีได้แสดงไฟล์ตัวอย่างฐานข้อมูลของหน่วยงาน และมีข้อมูลตัวอย่างรวมทั้งสิ้น 25 ไฟล์



ภาพที่ 4: ข้อความเรียกค่าไถ่จาก RANSOMWARE

(2) ธนาคารแห่งประเทศไทย ถูกปลอมแปลงเว็บไซต์ให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริง

เมื่อวันที่ 7 กรกฎาคม 2565 ได้ตรวจพบการปลอมแปลงเว็บไซต์หน่วยงานของรัฐซึ่งเป็นของธนาคารแห่งประเทศไทย โดยภายในหน้าเว็บไซต์ที่มีการปลอมแปลงมีลักษณะคล้ายคลึงกับเว็บไซต์จริง พบว่าเมื่อทำการคลิกลิงก์ที่ ACCOUNT และเลือก REGISTER จะนำไปที่ URL : HXXPS://BOTHAI[.]ORG/ENGLISH/PAGES/REGISTER.ASPX/ ที่เป็นหน้าเว็บไซต์ให้สมัครบัญชีใหม่ โดยให้กรอกชื่อ สกุล USERNAME PASSWORD ที่อยู่ เบอร์โทรศัพท์ EMAIL ประเภทบัญชี รหัสบัญชี เป็นต้น ซึ่งผู้ไม่หวังดีได้สร้างเว็บไซต์ปลอมขึ้นมาเพื่อหลอกลวงแบบ PHISHING หากมีประชาชนหลงเชื่อกรอกข้อมูลส่วนบุคคลในเว็บไซต์นั้นแล้ว จะทำให้คนร้ายได้รับข้อมูลส่วนบุคคลดังกล่าวสามารถเข้าทำธุรกรรมในระบบแอปพลิเคชันธนาคารแทนเจ้าของบัญชีได้

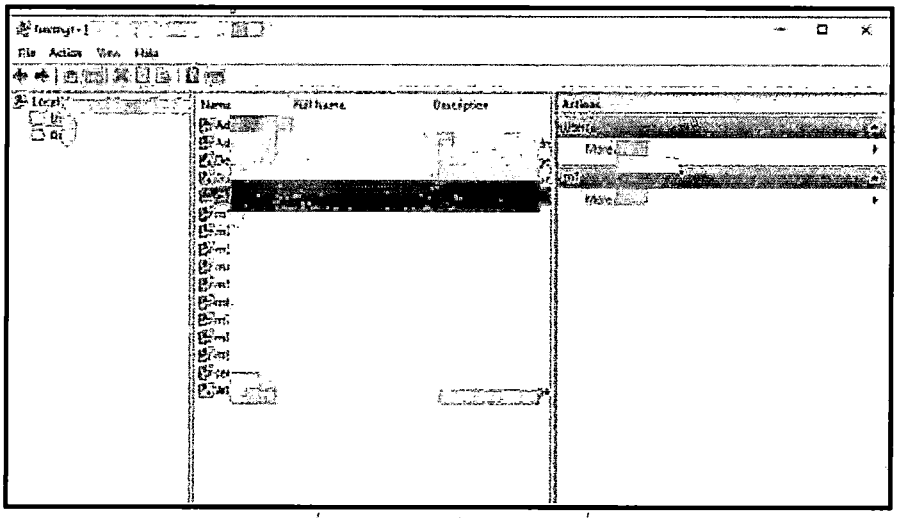


ภาพที่ 5: หน้าเว็บไซต์ที่มีการปลอมแปลง

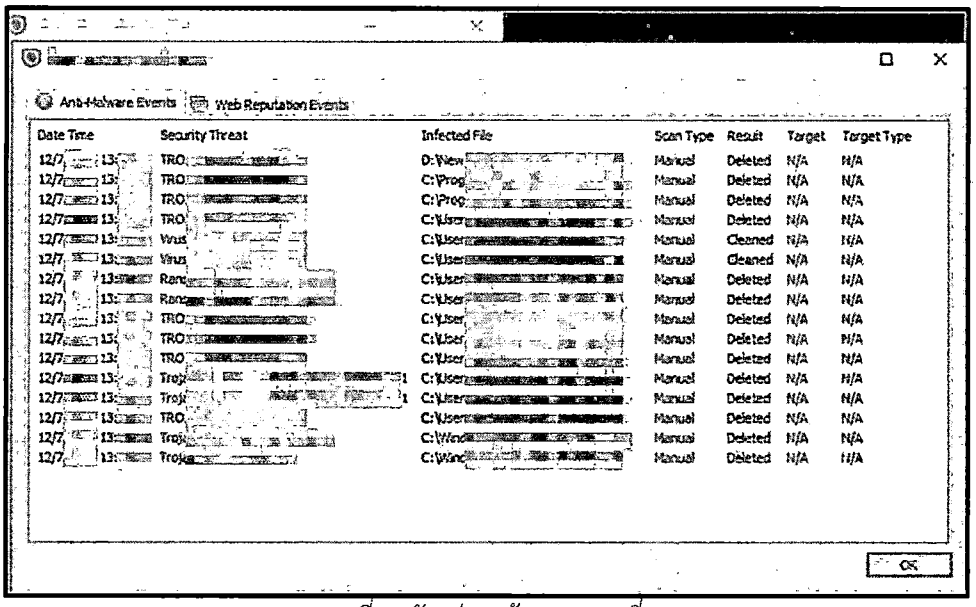
ภาพที่ 6: การแจ้งเตือนจาก สกมช.

(3) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านการขนส่งและโลจิสติกส์ ถูกบุกรุกระบบงานของฝ่ายเทคโนโลยีสารสนเทศ หรือระบบ (INTRUSION ATTEMPTS) โดยใช้เทคนิคฟิชชิ่ง (PHISHING TECHNIQUES) ประเภท COMPROMISED ACCOUNTS

เมื่อวันที่ 11 กรกฎาคม 2565 ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์จาก หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านการขนส่งและโลจิสติกส์ ถูกบุกรุกระบบงานของฝ่ายเทคโนโลยีสารสนเทศ หรือเจาะเข้าระบบ (INTRUSION ATTEMPTS) โดยใช้เทคนิคฟิชชิ่ง (PHISHING TECHNIQUES) ประเภท COMPROMISED ACCOUNTS เกิดจากการเดารหัสผ่าน (INITIAL PASSWORD) ทำให้เกิดผลกระทบต่อระบบงานภายในของหน่วยงาน จำนวน 7 ระบบงาน เครื่องคอมพิวเตอร์แม่ข่ายได้รับผลกระทบ จำนวน 11 เครื่อง



ภาพที่ 7: ตัวอย่างหน้าระบบงานที่ถูกบุกรุก



ภาพที่ 8: ตัวอย่างหน้าระบบงานที่ถูกบุกรุก

(4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านสาธารณสุขแห่งหนึ่ง ถูกโจมตีด้วย RANSOMWARE

เมื่อวันที่ 25 กรกฎาคม 2565 ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์จาก หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านสาธารณสุขแห่งหนึ่ง ถูกโจมตีด้วย RANSOMWARE โดยเจ้าหน้าที่ของหน่วยงานตรวจพบการโจมตีที่เครื่อง Client หน่วยงานได้จำกัดผลกระทบที่อาจเกิดขึ้น ด้วยการตัดการเชื่อมต่อของระบบจากภายนอก ตัดการเชื่อมต่อเครือข่ายที่เชื่อมต่อกับอินเทอร์เน็ต และระบบ VPN ผู้ดูแลระบบดำเนินการตรวจสอบความเสียหายต่อระบบต่าง ๆ และสำรวจไฟล์ข้อมูล พร้อมกับทำการติดตั้งโปรแกรมตรวจจับมัลแวร์ รวมถึงจัดทำแผนฟื้นฟูระบบและให้บริการ

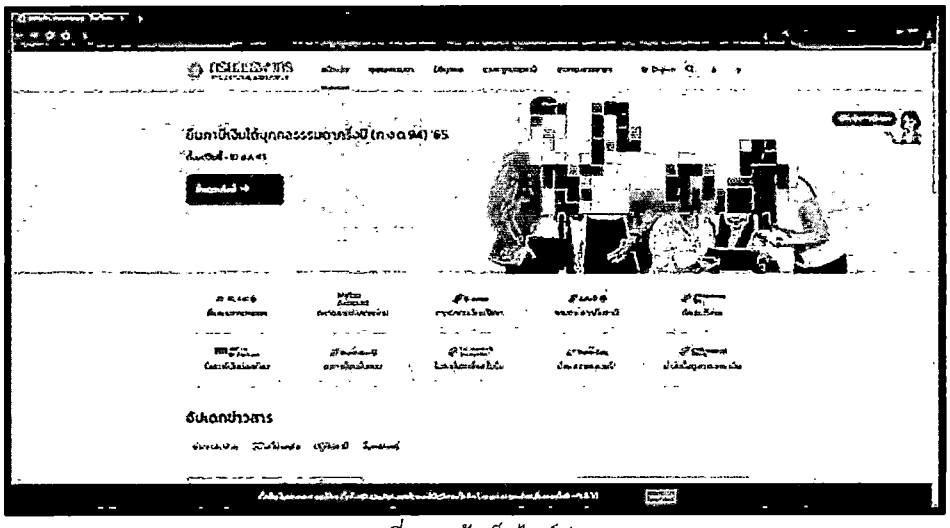
จากเหตุการณ์ดังกล่าว ศปช. ได้ให้คำแนะนำในการรับมือ ช่วยตรวจสอบ วิเคราะห์สถานการณ์ และประเมินผลกระทบ โดยให้เจ้าหน้าที่ของหน่วยงาน ปิดการใช้งานระบบ Active Directory ตรวจสอบ Logs File ตรวจสอบ Database Log เพิ่มระบบตรวจจับการบุกรุกเครือข่ายเพื่อเฝ้าระวังการถูกโจมตีซ้ำ

นอกจากนั้น ศปช. ได้ดำเนินการตอบสนองและรับมือต่อภัยคุกคามที่เกิดขึ้นประกอบกับแนวทางการแก้ไขปัญหาจนหน่วยงานสามารถนำระบบที่ถูกโจมตีกลับมาใช้งานได้ตามปกติ และหน่วยงานได้นำบทเรียนจากเหตุการณ์ดังกล่าว สร้างความตระหนักรู้ ถึงความสำคัญของความรู้ความเข้าใจด้าน Cyber Security ภายในองค์กร ทำให้องค์กรมีแนวทางการรับมือต่อภัยคุกคามทางไซเบอร์ที่เข้มแข็ง สามารถดำเนินงานตามภารกิจของหน่วยงานในการบริการประชาชนได้อย่างมั่นคงปลอดภัยต่อไป

(5) กรมสรรพากร

ศปช. ได้รับแจ้งเหตุภัยคุกคามทางไซเบอร์จากกรมสรรพากร ผ่านจดหมายอิเล็กทรอนิกส์ พบเว็บไซต์ที่มีการเลียนแบบเว็บไซต์กรมสรรพากร โดยภายในหน้าเว็บไซต์มีลักษณะคล้ายคลึงกับเว็บไซต์จริง และยังแนะนำให้ผู้ใช้งานดาวน์โหลดแอปพลิเคชันที่ใช้ชื่อว่า “คลิกเพื่อดาวน์โหลด” โดยแอปพลิเคชันดังกล่าวเป็น Android Remote Access Trojan (RAT) ซึ่งหากมีผู้หลงเชื่อทำการดาวน์โหลดแอปพลิเคชันและติดตั้งโปรแกรมที่เป็นอันตราย ลงในอุปกรณ์โทรศัพท์มือถือ Android ก็จะถูกขโมยข้อมูลที่มีความละเอียดอ่อน เช่น ยี่ห้อของอุปกรณ์ หมายเลข IMEI ชื่อ นามสกุล หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ ข้อมูลเกี่ยวกับแอปพลิเคชันที่เกี่ยวข้องกับธนาคารที่ใช้ในอุปกรณ์ของเหยื่อ รวมไปถึงบัญชีผู้ใช้งานที่เข้าถึงแอปพลิเคชันของธนาคาร รหัสผ่านสำหรับการเข้าถึงแอปพลิเคชันของธนาคาร ซึ่งเมื่อผู้ใช้งานทำธุรกรรมใด ๆ และมีการส่งรหัส OTP มายังผู้ใช้งาน โปรแกรมจะดักจับข้อมูล ทำให้คนร้ายสามารถเข้าทำธุรกรรมแทนเจ้าของเครื่องได้

จากเหตุการณ์ภัยคุกคามทางไซเบอร์ดังกล่าว ศปช. ได้ดำเนินการทำการรายงานไปยังเว็บไซต์ที่จดทะเบียนเว็บไซต์ปลอม เพื่อขอให้ปิดกั้นและระงับการให้บริการ Domain ดังกล่าว โดยในห้วงวันที่ 1 ตุลาคม 2564 ถึง 30 กันยายน 2565 ศปช. ได้ดำเนินการขอให้ปิดกั้นและระงับการให้บริการ เว็บไซต์ปลอมของกรมสรรพากร จำนวน 9 Domain



ภาพที่ 9: หน้าเว็บไซต์ปลอม

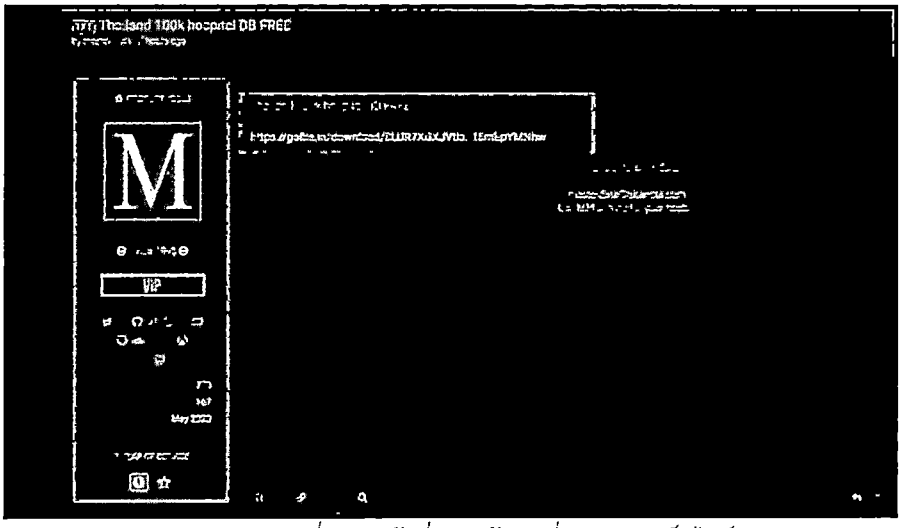
ภาพที่ 10: หน้าเว็บไซต์จริง

(6) หน่วยงานราชการแห่งหนึ่ง สังกัดกระทรวงสาธารณสุข

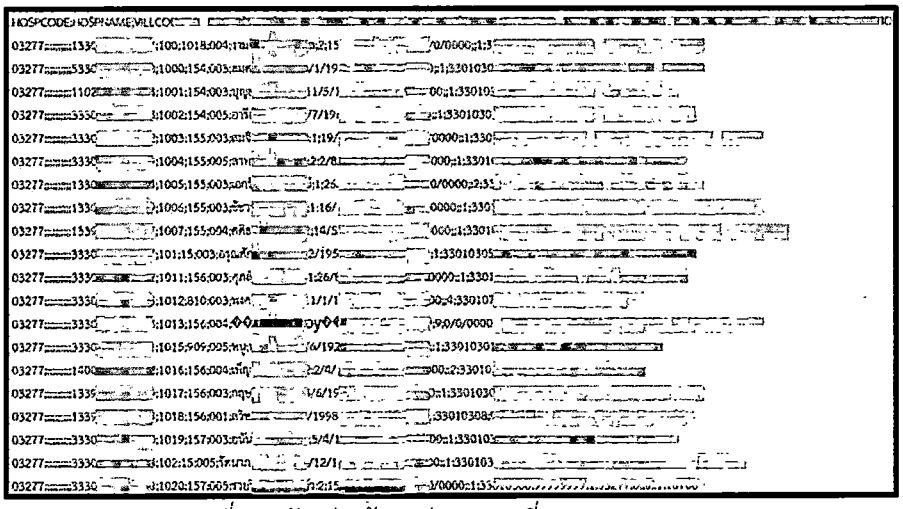
เมื่อวันที่ 7 ตุลาคม 2564 พบแหล่งข่าวเปิดบนอินเทอร์เน็ต มีการประกาศแจกฟรีข้อมูลของโรงพยาบาลในประเทศไทย จำนวน 100,000 Record บนเว็บไซต์ Raidforums จากผู้ใช้งานที่เรียกตัวเองว่า “master data” ซึ่งเชื่อมโยงกับเว็บไซต์ภายนอกในการดาวน์โหลดข้อมูลทั้งหมด เบื้องต้นตรวจสอบแล้วพบข้อมูล มีจำนวนประมาณ 108,000 records ประกอบไปด้วยข้อมูลส่วนบุคคล อาทิเช่น รหัสสถานพยาบาล ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขบัตรประชาชน เป็นต้น

จากเหตุการณ์ดังกล่าว ทาง ศปช. ได้ส่งหนังสือแจ้งเตือนเร่งด่วนไปยังสำนักงานปลัดกระทรวงสาธารณสุข ให้รับทราบถึงสถานการณ์ และดำเนินการจัดทำเอกสารแจ้งเตือนถึงหน่วยงานที่ได้รับผลกระทบต่อเหตุการณ์ดังกล่าว เพื่อแนะนำการแก้ไข และป้องกันเพื่อลดความเสี่ยงมิให้ถูกโจมตีซ้ำอีก

นอกจากนั้น ศปช. ได้ให้คำแนะนำกับเจ้าหน้าที่ของหน่วยงาน โดยแนะนำว่าสำหรับกรณีผู้ที่เป็นเจ้าของเว็บไซต์ควรจะต้องดำเนินการตรวจสอบว่าเว็บไซต์มีช่องโหว่ที่จุดใด และควรดำเนินการแก้ไข เพื่อไม่ให้ผู้ที่ไม่หวังดีใช้เป็นที่กระทำความผิดต่อไป โดยทั่วไปแล้วในเบื้องต้น ผู้ดูแลระบบควรจะเปลี่ยนรหัสผ่านของผู้ใช้ทั้งหมด ทำการลบลิงก์ที่ไม่ได้ใช้งานออกจากเว็บไซต์ กำหนดสิทธิ์ในการเข้าถึงเว็บไซต์ใหม่ทั้งหมด จากนั้นจึงดำเนินการทดสอบหาช่องโหว่ของเว็บไซต์เพื่อป้องกันการโจมตีต่อไป



ภาพที่ 11: หน้าที่แสดงข้อมูลที่ถูกขายบนเว็บไซต์



ภาพที่ 12: ตัวอย่างข้อมูลส่วนบุคคลที่ถูกประกาศขาย

(7) หน่วยงานของรัฐที่เป็นองค์กรอิสระแห่งหนึ่ง

เมื่อวันที่ 11 พฤศจิกายน 2564 มีผู้โจมตีเว็บไซต์ได้ทำการเปลี่ยนแปลงหน้าเว็บไซต์เป็นวิดีโอจากผู้ใช้ YouTube ที่ชื่อว่า “Death Grips” ชื่อเพลง Guillotine (It goes Yah) เข้าแทนที่พร้อมตั้งชื่อเว็บไซต์ (Website Title) เป็น Kangaroo Court

ศปช. จึงได้ดำเนินการประสานงานเร่งด่วนไปยังหน่วยงานที่เกิดเหตุภัยคุกคาม และได้ให้คำแนะนำในการดำเนินการเบื้องต้น โดยให้หน่วยงานนำ Web Server ออกจากเครือข่าย เพื่อรอการตรวจสอบ และได้ทำหน้า Website แบบ static ขึ้นใช้งานแทน

จากเหตุการณ์ดังกล่าว ทาง ศปช. ได้ให้คำแนะนำในการรับมือต่อเหตุการณ์ โดยให้เจ้าหน้าที่ของหน่วยงาน ดำเนินการถอดสายเชื่อมเครือข่ายออกจาก Web Server เพื่อตัดการเชื่อมต่อของผู้โจมตี และได้แนะนำให้หน่วยงาน แจ้งความดำเนินคดี เพื่อให้เจ้าหน้าที่ได้เข้าไปเก็บรวมรวบพยานหลักฐานที่เกี่ยวข้อง ในการนำมาสืบหาผู้กระทำผิด โดย ศปช. ได้รับการร้องขอให้เข้าร่วมตรวจสอบจนทำให้สามารถระบุหมายเลข IP ของผู้โจมตีได้ และนำไปสู่การจับกุมผู้ต้องหา

นอกจากนั้น ศปช. ได้ให้ความร่วมมือกับเจ้าหน้าที่ สอท. ในการสอบสวนเชิงเทคนิคที่ใช้ในการโจมตีเว็บไซต์ของหน่วยงานดังกล่าว โดย ศปช. ได้รับการร้องขอให้ทำการทดสอบความปลอดภัยระบบเว็บไซต์ก่อนที่จะเปิดให้บริการ การปฏิบัติในด้านกฎหมาย ศปช. สนับสนุนการวิเคราะห์และรวบรวมพยานหลักฐานส่งให้พนักงานสอบสวน บช.สอท. นำไปสู่การจับกุมตัวผู้ต้องหาในคดี การปฏิบัติในด้านเทคนิค หน่วยงานได้ดำเนินการจัดจ้างพัฒนาเว็บไซต์ขึ้นใหม่ และขอรับการสนับสนุนจาก สกมช. เพื่อให้ตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ต่อไป

ภาพที่ 13: หน้าที่ถูกเปลี่ยนแปลงเว็บไซต์

(8) หน่วยงานของรัฐที่เป็นองค์กรอิสระแห่งหนึ่ง

เมื่อวันที่ 18 พฤศจิกายน 2564 มีการตรวจพบว่าเว็บไซต์ของหน่วยงานของรัฐถูกโจมตีด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ทำให้หน้าเว็บไซต์เป็นการโฆษณาเว็บการพนันออนไลน์

จากเหตุการณ์ดังกล่าว ศปช. ได้มีหนังสือแจ้งเตือนเร่งด่วนไปยังหน่วยงานให้รับทราบสถานการณ์เพื่อดำเนินการตรวจสอบแก้ไขหน้าเว็บไซต์และระบบที่เกี่ยวข้องให้เป็นไปตามมาตรฐานและมีความมั่นคงปลอดภัย

ศปช. ได้สนับสนุนเจ้าหน้าที่ของหน่วยงาน โดยให้คำแนะนำในการรับมือกับการเหตุการณ์ Website Defacement ว่าควรติดต่อผู้ให้บริการเช่าพื้นที่ฝากเว็บไซต์เพื่อใช้งานระบบ และแก้ไข config เพื่อความปลอดภัย จากนั้นให้หน่วยงานแก้ไขรหัสผ่านที่เกี่ยวข้องทั้งหมด โดยให้เจ้าหน้าที่ของหน่วยงาน ตรวจสอบช่องโหว่ CMS platform theme และ plug-in ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็น version ล่าสุด และควรตรวจสอบและแก้ไข source code ให้มีความปลอดภัยก่อนถึงให้กลับมาใช้งานได้

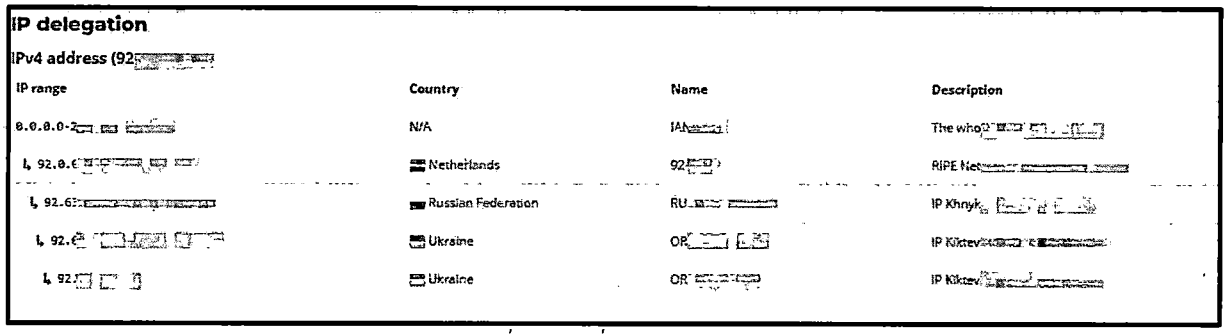
ภาพที่ 14: หน้าที่ถูกเปลี่ยนแปลงเว็บไซต์

(9) การโจมตีทางไซเบอร์ต่อระบบสำคัญระบบหนึ่ง สังกัดกระทรวงสาธารณสุข

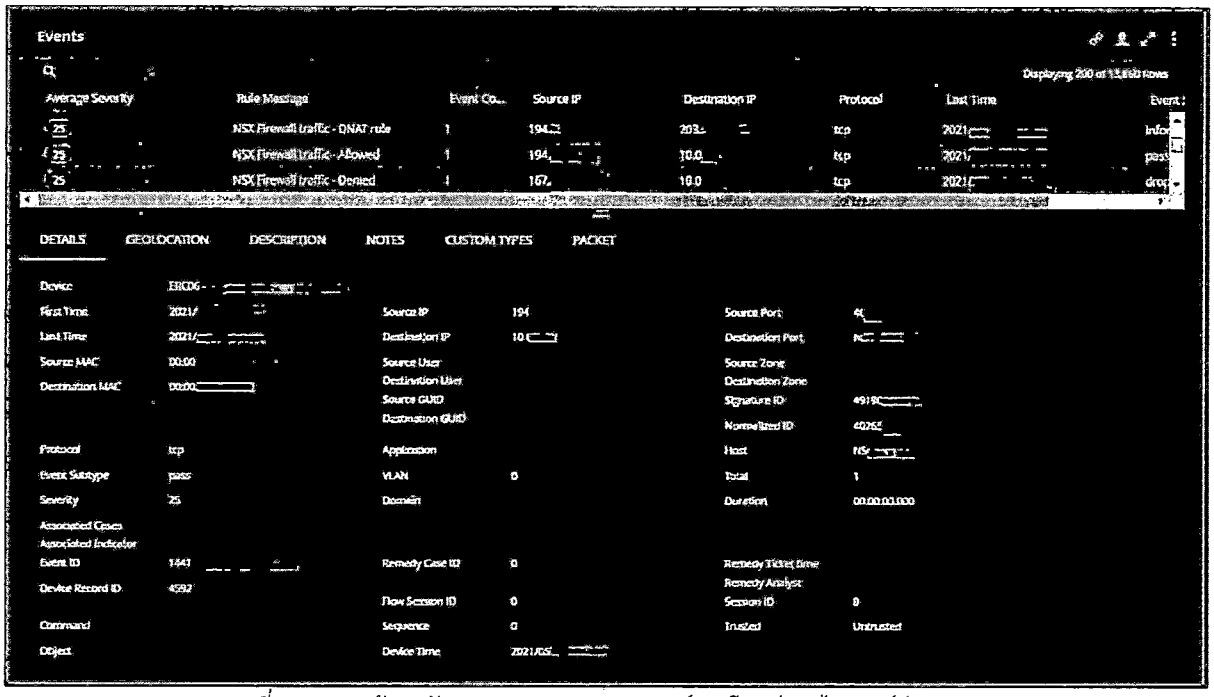
เมื่อวันที่ 26 มีนาคม 2565 ได้รับการประสานจากเจ้าหน้าที่ของกระทรวงสาธารณสุข เพื่อขอรับการสนับสนุนในการเฝ้าระวัง และตรวจสอบเหตุการณ์พบการโจมตีทางไซเบอร์ต่อระบบสำคัญระบบหนึ่ง ซึ่งพบว่ามี IP ที่น่าสงสัยจำนวน 2 IP ADDRESS ได้ทำการส่ง request เข้าไปที่ระบบฯ เป็นจำนวนมากจนผิดปกติ

เหตุการณ์ดังกล่าว ทาง ศปช. ได้ดำเนินการร่วมสนับสนุนในการเฝ้าระวัง และตรวจสอบเหตุการณ์ตรวจพบการโจมตีทางไซเบอร์ต่อระบบฯ โดยได้ประสานไปยังผู้ให้บริการอินเทอร์เน็ต เพื่อให้ระงับการโจมตีจากแหล่งที่มาของ IP ตามผู้ให้บริการแล้ว

จากการดำเนินการของ ศปช. ผู้ดูแลระบบแจ้งว่าระบบฯ กลับมาทำงานได้เป็นปกติ และในขั้นตอนสุดท้าย ศปช. ได้ติดตามตรวจสอบจากแหล่งข่าวรวมถึงเว็บไซต์ต่าง ๆ สรุปผลว่าปัจจุบันไม่พบว่ามีข้อมูลรั่วไหล



ภาพที่ 15: IP ที่น่าสงสัยในระบบฯ



ภาพที่ 16: ภาพเฝ้าระวัง และตรวจสอบเหตุการณ์การโจมตีทางไซเบอร์ต่อระบบฯ

(10) เฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์ จากกรณีความขัดแย้งระหว่างประเทศ

จากเหตุการณ์ความขัดแย้งระหว่าง ประเทศสหพันธรัฐรัสเซีย กับ ประเทศยูเครน ทำให้เกิดปฏิบัติการที่เรียกว่า “สงครามไฮบริด” ครั้งแรกของโลก ซึ่งมีการปฏิบัติการโจมตีทางทหาร และการโจมตีทางไซเบอร์ระหว่างประเทศคู่ขัดแย้งกันเอง และมีประเทศที่เป็นพันธมิตรรวมอยู่ด้วยนั้น ซึ่งการโจมตีทางไซเบอร์ที่สำคัญอีกเรื่องหนึ่งคือ การใช้แฮ็กเกอร์เข้ามาทำลายระบบไอทีและโครงสร้างพื้นฐานต่าง ๆ ทั้งการแฮ็กเว็บไซต์ การส่งมัลแวร์เข้าไปทำลายระบบของฝ่ายตรงข้าม ซึ่งเป็นที่ทราบกันดีว่าทั้งประเทศสหพันธรัฐรัสเซีย และประเทศยูเครน ต่างก็มีความเชี่ยวชาญในด้านการโจมตีทางไซเบอร์มาก โดย สกมช. จึงได้ติดตามสถานการณ์ความขัดแย้งดังกล่าว โดยพบว่ามีการโจมตีทางไซเบอร์ต่อหน่วยงานต่าง ๆ ภายในประเทศยูเครน ดังนี้

1. การโจมตีทางไซเบอร์ ในรูปแบบ DDoS (Distributed-Denial-of-Service) ต่อเว็บไซต์ของหน่วยงานสำคัญระดับประเทศ เช่น กระทรวงการต่างประเทศ กระทรวงสาธารณสุข และภาคธนาคาร

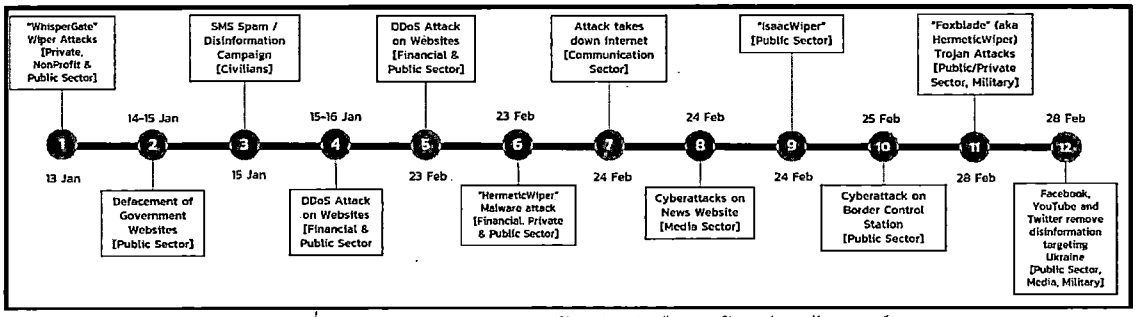
2. ตรวจพบมัลแวร์ชื่อ Hermetic Wiper ซึ่งมีลักษณะการทำงานที่เน้นการล้างข้อมูลของเป้าหมายบนระบบเครือข่ายภายในประเทศยูเครน ซึ่งมัลแวร์นี้จะสร้างความเสียหายให้กับ Master Boot Record (MBR) ทำให้คอมพิวเตอร์ที่ติดมัลแวร์ ไม่สามารถทำงานได้

3. ตรวจพบมัลแวร์ชื่อ Cyclops Blink แพร่กระจายโดยการปลอมแปลงเว็บไซต์หน่วยงานรัฐบาลของประเทศยูเครน ซึ่งในเว็บไซต์ปลอมนี้ทำการรณรงค์ในประเด็น “Support the President” เพื่อหลอกให้ผู้ใช้งานหลงเชื่อ ทำการคลิกลิงก์ที่เป็นอันตราย จากนั้นมัลแวร์จะถูกดาวน์โหลดไปยังเครื่องคอมพิวเตอร์ของผู้ใช้งาน เพื่อเก็บรวบรวมข้อมูลที่สำคัญ

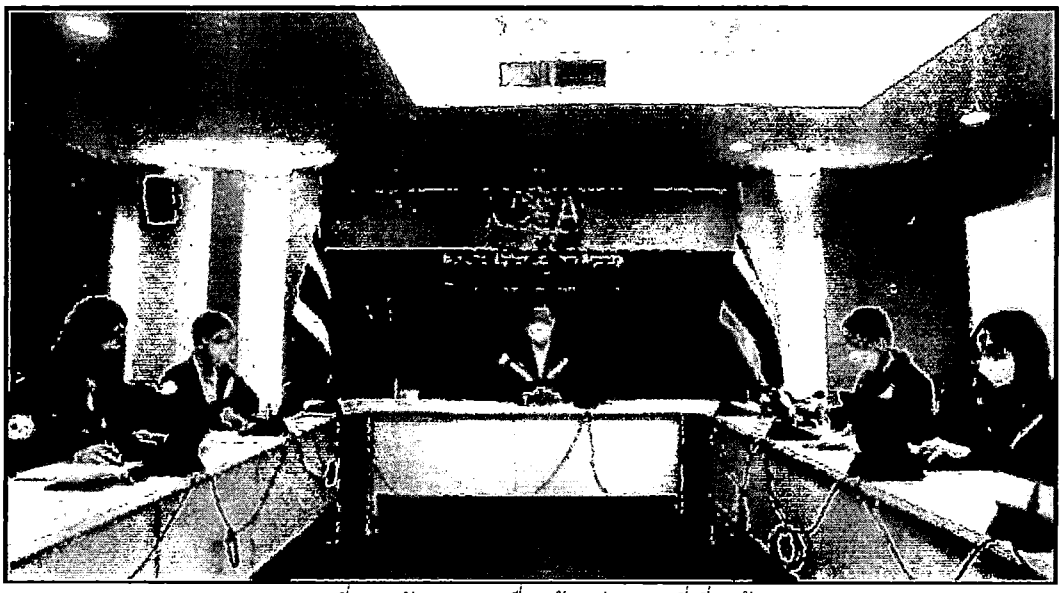
4. รัฐมนตรีกระทรวง Digital Transformation ของประเทศยูเครนได้ทวีตข้อความประกาศตั้งกองทัพไอที (IT Army) และรับอาสาสมัครชาวยูเครนที่มีความเชี่ยวชาญด้านไอที รวมถึงแฮ็กเกอร์ทั่วโลกเพื่อมาช่วยกันทำหน้าที่ดูแลและป้องกันระบบไอทีของประเทศยูเครน และยังรวมไปถึงการตั้งเป้าหมายเข้าไปโจมตีระบบไอทีของประเทศสหพันธรัฐรัสเซีย โดยมีอาสาสมัครเข้าร่วมเป็นจำนวนมาก

จากกรณีความขัดแย้งดังกล่าว เพื่อให้หน่วยงานควบคุมหรือกำกับดูแลระบบโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศของประเทศไทย ได้รับทราบสถานการณ์และผลกระทบที่อาจจะเกิดขึ้นต่อความมั่นคงปลอดภัยไซเบอร์ของระบบโครงสร้างพื้นฐานที่สำคัญทางสารสนเทศของประเทศไทย นั้น สกมช. ได้จัดประชุมเตรียมการป้องกันรับมือด้านความปลอดภัยทางไซเบอร์ ร่วมกับ หน่วยงานควบคุมหรือกำกับดูแล (REGULATOR) และ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ฯ (CERT) เพื่อประมวลสถานการณ์ และแนวทางป้องกันรับมือการโจมตีทางไซเบอร์ โดยมีหน่วยงานควบคุมหรือกำกับดูแล (REGULATOR) เข้าร่วม 19 หน่วยงาน ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ฯ (CERT) เข้าร่วม 5 ศูนย์ฯ รวมผู้แทนจากหน่วยงานทั้งสิ้น 82 ท่าน

หลังจาก ศปช. แจ้งเตือนหน่วยงานป้องกัน ติดตาม เฝ้าระวังสถานการณ์ภัยคุกคามทางไซเบอร์จากกรณีความขัดแย้งในต่างประเทศในครั้งนั้น ทำให้สำนักข่าวภายในประเทศไทยออกข่าวแจ้งเตือนไปยังหน่วยงาน และประชาชนให้ทราบอย่างทั่วถึง



ภาพที่ 17: Timeline แนวทางป้องกันรับมือการโจมตีทางไซเบอร์



ภาพที่ 18: จัดประชุมเพื่อแจ้งหน่วยงานที่เกี่ยวข้อง

ภาพที่ 19: สำนักข่าวภายในประเทศไทยออกข่าวแจ้งเตือนไปยังหน่วยงาน และประชาชนให้ทราบ

บทที่3
บทวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์

1. แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์

แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ ในห้วง ตุลาคม 2564 ถึง กันยายน 2565 จากกว่า 551 เหตุการณ์ มีข้อมูลที่น่าสนใจดังนี้

การโจมตีทางไซเบอร์ที่ถูกตรวจพบมากที่สุด ได้แก่ การโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website) หน่วยราชการและหน่วยงานสำคัญซึ่งมีมากกว่าการโจมตีรูปแบบอื่น ๆ โดยคิดเป็น 2 ใน 3 ของการโจมตีทางไซเบอร์ที่ตรวจพบในประเทศไทย อันดับหนึ่ง ได้แก่ การโจมตีในลักษณะทำไปเพื่อการแฝงหน้าเว็บพนันออนไลน์ในเว็บไซต์ของหน่วยงาน เพื่อเพิ่มโอกาสและประสิทธิภาพการค้นหาผ่าน Search Engine ส่วนอันดับสอง ได้แก่ การโจมตีโดยเปลี่ยนแปลงหน้าเว็บไซต์ (Website Defacement) ของหน่วยงาน เพื่อใช้เป็นพื้นที่ทดสอบความสามารถของแฮ็กเกอร์หรือเป็นผลลัพธ์จากการเคลื่อนไหวทางการเมืองของกลุ่มต่าง ๆ นอกจากนี้ ยังพบการโจมตีด้วยการแฮ็กเว็บไซต์แบบอื่น ๆ ที่น่าสนใจ เช่น การสร้างหน้าเว็บไซต์เพื่อหลอก Phishing อยู่บนเว็บไซต์หน่วยงานของรัฐ และการฝังมัลแวร์อันตรายบนหน้าเว็บไซต์หน่วยงานที่อาจหลอกให้ผู้เข้าถึงดาวน์โหลดไปติดตั้งได้ เป็นต้น ทั้งนี้ สาเหตุหลักที่หน่วยงานถูกโจมตีด้วยการแฮ็กเว็บไซต์ มาจากการที่หน่วยงานยังคงใช้ซอฟท์แวร์ที่มีช่องโหว่หรือล้าสมัย ทั้งที่เป็นระบบปฏิบัติการ รวมถึงซอฟท์แวร์ในการจัดทำหรือบริหารจัดการเว็บไซต์ ปัญหาการที่ผู้ดูแลระบบขาดความรู้ความเข้าใจในการตั้งค่าหรือการใช้งาน อีกทั้งไม่มีการเปลี่ยนแปลงรหัสผ่านที่ถูกตั้งไว้เป็นค่าเริ่มต้น หรือใช้รหัสผ่านที่คาดเดาง่าย

หน่วยงานที่พบการโจมตีทางไซเบอร์สูงสุด ได้แก่ หน่วยงานด้านการศึกษา และหน่วยงานด้านสาธารณสุข ซึ่งหน่วยงานทั้ง 2 ด้าน มีเว็บไซต์และระบบต่าง ๆ ให้บริการอยู่เป็นจำนวนมาก ซึ่งแต่ละหน่วยงานใช้เว็บไซต์เป็นสื่อประชาสัมพันธ์หลัก การบริหารงานในส่วนที่เกี่ยวข้องกับระบบไอทีมีความเป็นเอกเทศทำให้การดูแลจากหน่วยงานส่วนกลางทำได้ยาก เมื่อมีการพัฒนาระบบซึ่งดำเนินการเองหรือโดยว่าจ้างบุคคลจากภายนอกแล้วจะมีการปรับปรุงเฉพาะเนื้อหา จึงขาดการดูแลรักษาระบบและการตรวจสอบอย่างสม่ำเสมอ

สถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนและมีความสัมพันธ์กับความมั่นคงปลอดภัยทางไซเบอร์ โดยพบว่า อาชญากรทางไซเบอร์ในประเทศไทย ได้ใช้เทคนิคผสมผสานการ Phishing และ Social Engineering หลายรูปแบบเพื่อหลอกลวงเหยื่อ และนอกจากจะได้ไปซึ่งทรัพย์สินของเหยื่อแล้ว การกระทำดังกล่าว ทำให้เกิดผลกระทบต่อการรักษาความลับของข้อมูลส่วนตัว รวมถึงความปลอดภัยในตัวระบบและอุปกรณ์ของเหยื่อเช่นเดียวกัน อาทิเช่น กรณีมิจฉาชีพหลอกขอรหัสผ่านส่วนตัวของเหยื่อผ่านโทรศัพท์หรือผ่านแชทไลน์ การปลอมแปลงเว็บไซต์หน่วยงานของรัฐโดยตั้งชื่อโดเมนให้คล้ายคลึง และมีเนื้อหาเลียนแบบเว็บไซต์จริง เพื่อหลอกเอาข้อมูลส่วนบุคคล หรือหลอกให้ดาวน์โหลดไฟล์ที่มีมัลแวร์บนหน้าเว็บไซต์ การส่งลิงก์ Phishing ที่แฝงโฆษณาหรือมีชื่อผู้ส่งเลียนแบบ Platform หรือธนาคาร เพื่อพาเหยื่อไปในหน้า

เว็บไซต์ให้กรอกข้อมูลส่วนบุคคลหรือมีการดาวน์โหลดมัลแวร์ลงไปที่เครื่อง การจำหน่ายข้อมูลส่วนบุคคลที่ได้มาด้วยวิธีการต่างๆ ใน Dark web หรือ Communities ต่าง ๆ เป็นต้น

การโจมตีที่อาจสร้างความเสียหายให้กับหน่วยงานต่าง ๆ และอาจใช้เวลาในการแก้ไขมากที่สุด ได้แก่ Ransomware จากการรายงาน และการตรวจพบเหตุการณ์ Ransomware ที่เกิดขึ้นกับหน่วยงานภาครัฐ และเอกชนในประเทศ พบว่า เกิดการโจมตีด้วย Ransomware กับหน่วยงานรัฐที่มีความสำคัญ ส่วนภาคเอกชนมักเป็นธุรกิจที่มีชื่อเสียง มีทุนจดทะเบียนสูง กระจายตัวในหลายประเภทอุตสาหกรรม ซึ่งหากเป้าหมายหลักของผู้ไม่ประสงค์ดีอยู่ที่การเรียกร้องผลประโยชน์ที่อาจได้รับจากการโจมตี เป็นไปได้ว่าเป้าหมายของการโจมตีจะเน้นไปที่หน่วยงานที่มีความสำคัญหรือบริษัทที่มีขนาดใหญ่มากกว่าหน่วยงานหรือธุรกิจที่มีขนาดเล็ก โดยเมื่อเกิดเหตุ Ransomware ขึ้นแล้ว ความเสียหายที่เห็นชัดเจนของแต่ละหน่วยงาน คือ ปัญหาในการไม่สามารถเข้าใช้งานข้อมูลสำคัญได้ และบางแห่งไม่สามารถใช้งานระบบสำรองได้ นอกจากนี้ ยังส่งผลกระทบต่อการบริหารจัดการและทำงานของระบบสารสนเทศในภายรวมของหน่วยงาน ซึ่งหน่วยงานแต่ละแห่งต้องใช้ระยะเวลาในการแก้ไขปัญหากับการโจมตีด้วย Ransomware ยาวนาน และอาจต้องพึ่งพาบุคคลภายนอกผู้เชี่ยวชาญอีกด้วย

การโจมตีทางไซเบอร์ในรูปแบบ APT โดย ศปช. ได้รับการประสานข้อมูลจากหน่วยงานทั้งในและต่างประเทศเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบ APT ว่ามีการโจมตีเข้าไปในเครือข่ายหรือระบบของหน่วยงานรัฐที่มีความสำคัญของประเทศไทยมาเป็นระยะ ๆ ทั้งนี้ ได้มีการประสานงานไปยังหน่วยงานที่มีข้อมูลว่าถูกโจมตีแล้ว แต่ในชั้นนี้ยังไม่ได้รับรายงานความเชื่อมโยง หรือพบหลักฐานบ่งชี้ชัดว่าหน่วยงานได้ถูกโจมตีจริง

จากการวิเคราะห์สถิติเหตุการณ์ภัยคุกคามทางไซเบอร์ดังกล่าว พบว่าภัยคุกคามทางไซเบอร์โดยส่วนใหญ่มาจากจุดอ่อนช่องโหว่ โดยมีประเภทจุดอ่อนช่องโหว่ที่พบสูงสุด 5 อันดับ ได้แก่

1. SQL Injection คือ ช่องโหว่ด้านความปลอดภัยของ web application ทำให้แฮ็กเกอร์ สามารถแฮ็กข้อมูลโดยการแอบใส่คำสั่ง SQL ที่ความละเอียดอ่อนต่อฐานข้อมูล เช่น พาสเวิร์ด ข้อมูลบัตรเครดิต ข้อมูลส่วนบุคคล ทำให้สามารถแทรก อัปเดต แก้ไข ลบข้อมูล รวมถึงการกู้คืนฐานข้อมูล และในบางกรณีหากไม่เร่งแก้ไข แฮ็กเกอร์จะสามารถเข้าระบบเซิร์ฟเวอร์ และนำไปสู่การรั่วไหลของข้อมูล ในระยะยาวได้

2. Weak Password คือ การตั้งรหัสผ่านที่คาดเดาได้ง่าย ทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลได้อย่างง่ายดาย ดังนั้น ควรใช้รหัสผ่านที่แตกต่างกันในแต่ละบัญชี และไม่ซ้ำกับรหัสผ่านเดิมที่เคยใช้งานมาก่อน อีกทั้งควรตั้งรหัสผ่านที่มีอักขระพิเศษรวมถึงตัวอักษรพิมพ์เล็กและพิมพ์ใหญ่คละกัน วิธีนี้จะทำให้ผู้ไม่ประสงค์ดีคาดเดารหัสผ่านได้ยากยิ่งขึ้น

3. Vulnerable and Outdated Components คือ ช่องโหว่นี้เป็นช่องโหว่ยอดนิยมสำหรับองค์กรที่มีซอฟต์แวร์ที่ล้าสมัยและไม่กล้าอัปเดตซอฟต์แวร์ เพราะกลัวว่าซอฟต์แวร์ที่ใช้อยู่จะทำงานไม่ได้

4. Security Misconfiguration คือ การตั้งค่าผิด หรือลืมตั้งค่า ส่งผลให้มีช่องโหว่ที่ไม่ได้ตั้งใจหลุดออกไป เช่น Default Configuration หรือการใช้ค่า default ของซอฟต์แวร์โดยเฉพาะอย่างยิ่งฐานข้อมูลโดยไม่แก้ไข username และ password ก่อนใช้ (เช่น admin, admin หรือ password ว่างเปล่า) ส่งผลให้

ผู้ไม่ประสงค์ดีสามารถคาดเดารหัสผ่านจาก google ได้ทันที และสามารถเข้าถึงฐานข้อมูลได้ ซึ่งทำให้ส่งผลเสียอย่างร้ายแรง

5. Broken Access Control คือ การกำหนดสิทธิของผู้ใช้ (Permission) ที่สามารถเข้าระบบ Web application ได้ ซึ่งผลที่ตามมาก็คือ ผู้ที่ไม่มีสิทธิเข้าระบบ (Unauthorized User) จึงสามารถเข้าถึงข้อมูลได้ เช่น เข้ามาดูไฟล์ข้อมูลบัตรเครดิตลูกค้าที่เก็บอยู่ใน Web Server หรือ เข้าถึงไฟล์ข้อมูลในลักษณะ Directory Browsing โดยเห็นไฟล์ทั้งหมดที่อยู่ใน web Server เป็นปัญหาที่เกิดจากการกำหนด File Permission ไม่ดี อาจเกิด Path Traversal

2. แนวทางการจัดการภัยคุกคามทางไซเบอร์

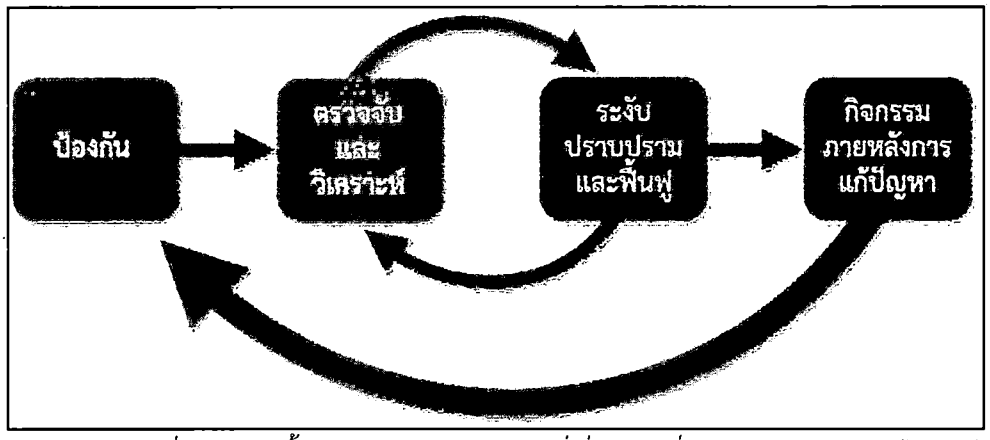
การดำเนินมาตรการที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ (incident handling) ซึ่ง ศปช. ได้มีการแนะนำให้กับหน่วยงานต่าง ๆ มีความสอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ และเป็นไปตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องรายละเอียดของลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 โดยแบ่งขั้นตอนได้เป็น 4 ขั้นตอนหลัก ดังนี้

(1) การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

(2) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

(3) การระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

(4) การดำเนินกิจกรรมภายหลังการระงับภัยคุกคามทางไซเบอร์ (post-incident activity)



ภาพที่ 20: แสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)

ขั้นตอนที่ 1: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม

การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ เป็นต้น

ขั้นตอนที่ 2: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอ เพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เช่น การจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม การวิเคราะห์ข้อมูลและประวัติการใช้งานเครือข่ายและระบบงาน การทำการศึกษาวิจัยและค้นหาความสัมพันธ์ของข้อมูล ในระบบกับสถานการณ์ต่าง ๆ เป็นต้น

ขั้นตอนที่ 3: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น เพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ตัวอย่างเช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การเก็บรวบรวมและจัดการหลักฐานต่าง ๆ การระบุแหล่งที่มาของการโจมตี การดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด เป็นต้น

ขั้นตอนที่ 4: การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) นั้น หน่วยงานควรกำหนดขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น

อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง (โดยการเก็บข้อมูลบางประเภทนั้น อาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าว อาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี)

เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นตามวรรคก่อนแล้ว หน่วยงานควรนำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

อนึ่ง ในการป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ ตามที่เสนอไว้ข้างต้น นั้น หน่วยงานควรจัดให้มีมาตรการที่สอดคล้องกับระดับของภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานนั้น ๆ โดยให้ใช้แนวทางการประเมินความเสี่ยงของหน่วยงานเป็นเกณฑ์ในการพิจารณา ประกอบกับความสำคัญของภารกิจหรือบริการที่อยู่ภายใต้ความรับผิดชอบของหน่วยงาน ความสำคัญของทรัพย์สินสำคัญทางสารสนเทศมาประกอบการพิจารณาด้วยก็ได้ นอกจากนี้ หน่วยงานอาจพิจารณากำหนดแนวทางการดำเนินมาตรการต่าง ๆ เพิ่มเติมหรือแตกต่างจากที่กำหนดไว้ เพื่อป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์ หรือจัดทำนโยบายที่เกี่ยวข้องร่วมกับหน่วยงานควบคุมหรือกำกับดูแลเพื่อให้มีแนวทางการดำเนินมาตรการที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับมาตรการต่าง ๆ ที่ได้เสนอข้างต้น

3.ข้อเสนอแนะ

การแก้ไขปัญหาที่สำคัญจากแนวโน้มสถานการณ์ทางไซเบอร์ที่สำคัญในรอบปี โดยเฉพาะ**การถูกโจมตีด้วยการแฮ็กเว็บไซต์ (Hacked Website)** เป็นเรื่องที่ผู้ดูแลระบบของหน่วยงานควรให้ความสนใจกับการปรับปรุงแพทช์ (PATCH) ของระบบปฏิบัติการ ระบบบริหารจัดการเว็บไซต์ (CMS) ให้เป็นปัจจุบัน ทบทวนการใช้งาน Themes หรือ Plug-in ต่าง ๆ ที่อาจมีช่องโหว่ การเปลี่ยนแปลงแก้ไขรหัสผ่านต่าง ๆ ทำให้ยากต่อการคาดเดา ตรวจสอบการนำเข้าไฟล์ต่างๆ สำหรับผู้ใช้งานเว็บไซต์ให้อนุญาตเฉพาะไฟล์ที่ต้องการเท่านั้น รวมไปถึงใช้วิธีการเข้ารหัสข้อมูลที่มีความสำคัญต่าง ๆ ด้วย สำหรับ **การดูแลเว็บไซต์และระบบที่เกี่ยวข้องของหน่วยงานต่าง ๆ** โดยเฉพาะหน่วยงานที่มีความเป็นเอกเทศนั้น หน่วยงานส่วนกลางควรมีการกำหนดนโยบายเกี่ยวกับการดูแลและพัฒนาเว็บไซต์ ซึ่งหากจะดำเนินการเองหรือว่าจ้างบุคคลภายนอกแล้ว ควรให้มีการดูแลรักษาระบบและตรวจสอบอย่างสม่ำเสมอ รวมไปถึงแนวทางการเขียนร่างขอบเขตของงาน (Tor) และการกำหนดคุณสมบัติ เพื่อการจัดจ้างทำเว็บไซต์หรือพัฒนาระบบที่เกี่ยวข้องที่ต้องคำนึงถึงเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ด้วย ทั้งนี้ หน่วยงานสามารถศึกษาและดำเนินการเพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยเพิ่มมากขึ้น ตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guildline) สามารถดูรายละเอียดเพิ่มเติมได้ที่ https://drive.ncsa.or.th/s/BE6BgHf5ik6sTmA **ในเรื่องสถานการณ์**

อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชนนั้น การสร้างความรู้ความเข้าใจ และการให้ความตระหนักรู้กับประชาชนเป็นสิ่งที่สำคัญมาก โดยเฉพาะการสร้างการรับรู้เกี่ยวกับรูปแบบและวิธีการที่เหล่ามิจฉาชีพใช้ในการหลอกลวง รวมไปถึงประชาชนจะต้องรับทราบถึงความเสียหายหรือผลกระทบจากการที่ตนเองตกเป็นเหยื่อหรือถูกหลอก ซึ่งนอกจากจะส่งผลให้เสียในเรื่องของทรัพย์สินแล้ว ยังเป็นผลสัมพันธ์ไปถึงความมั่นคงปลอดภัยทางไซเบอร์ที่จะถูกแฮ็กเกอร์นำข้อมูลส่วนบุคคลไปใช้ประโยชน์ในการเข้าถึงระบบต่าง ๆ ได้ **ในเรื่อง Ransomware** ที่อาจสร้างความเสียหายได้อย่างรุนแรงนั้น หน่วยงานต่าง ๆ สามารถลดความเสี่ยงได้โดยการจัดทำแผนดำเนินธุรกิจอย่างต่อเนื่อง (BCP) และปฏิบัติตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ฯ ในการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยให้ความสำคัญกับการสำรองข้อมูล และตรวจสอบอย่างสม่ำเสมอ ส่วนกรณีที่จะปฏิบัติตามแนวทาง **การรับมือและตรวจสอบการโจมตีในรูปแบบ APT** ยังเป็นเรื่องที่มีความละเอียดอ่อนซับซ้อน จำเป็นต้องพึ่งพาทรัพยากรสูง อีกทั้งต้องอาศัยความเข้าใจจากทุกฝ่าย และพึ่งพาความร่วมมือจากหน่วยงานนั้นเป็นสำคัญ จึงถือเป็นความท้าทายอย่างมากสำหรับการโจมตีในรูปแบบ APT ที่จะมีความสำคัญมากขึ้นในอนาคต

ภาคผนวก

คำจำกัดความคำศัพท์ทางด้านไซเบอร์

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
APT	เอพีที	APT ย่อมาจาก Advanced Persistent Threat คือ การที่ผู้โจมตีฝังตัวอยู่ในระบบของเหยื่อเป็นเวลานานเพื่อเฝ้าดูพฤติกรรมและดักรับข้อมูล	ETDA Thailand Facebook page
Data Breach	ดาต้าบรีช	การเจาะระบบและขโมยข้อมูลสำคัญออกไปขายหรือเผยแพร่ เช่น การนำข้อมูลส่วนบุคคลของลูกค้าไปขาย หรือการล้วงข้อมูลงานวิจัยเพื่อแข่งขันทางการค้า	ETDA Thailand Facebook page
Fake Website	เฟค เว็บไซต์	เป็นองค์ประกอบที่ฟิชชิง สร้างขึ้นเพื่อล่อลวงข้อมูลโดยการสร้างเว็บไซต์ที่มีความเหมือนเว็บไซต์จริงมากที่สุดเพื่อให้ผู้ใช้งานหลงกลเข้ามาในระบบ รอให้ผู้ใช้ใส่ข้อมูลส่วนตัวต่าง ๆ ทำให้ข้อมูลส่วนตัวที่ควรรักษาเป็นความลับ ถูกโจรกรรมข้อมูลไปได้ ซึ่งทำให้ผู้ใช้ได้รับผลกระทบเป็นอย่างมากเพราะข้อมูลอาจถูกนำไปใช้ในทางที่เสียหาย โดยที่เราไม่สามารถหยุดได้เลยเพราะข้อมูลเป็นข้อมูลจริงของผู้ใช้เอง ส่งผลเสียให้กับเหยื่อที่หลงกลเป็นอย่างมาก	www.mindphp.com[fake webpage] หมายเหตุ : เนื่องจากคำว่า Fake website มีข้อมูลจำกัดและไม่เพียงพอต่อการให้ความหมาย และมีคำที่คล้ายเคียงกันคือ Fake webpage ที่มีข้อมูลอธิบาย จึงทำการนำข้อมูลความหมายของ Fake webpage มาใช้เพื่ออธิบายความหมาย
Fraud	ฟรอด	คดีฉ้อโกง หมายถึง คดีอาญาที่ผู้กระทำผิดมีเจตนาแสวงหาประโยชน์โดยมิชอบเอาจากผู้ถูกหลอกลวง โดยหลอกลวงด้วย	www.etda.or.th / ETDA Thailand Facebook page หมายเหตุ : เนื่องจาก Fraud มีความหมายโดยทั่วไปด้วย

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		การแสดงข้อความอันเป็นเท็จหรือปกปิดข้อความจริงที่ควรบอก ซึ่งการหลอกลวงและปกปิดนั้น ผู้ถูกหลอกลวงต้องเสียทรัพย์สินให้แก่ผู้กระทำผิดหรือทำให้ผู้ถูกหลอกลวงหรือบุคคลที่สามทำ ถอน หรือทำลายเอกสารสิทธิ นอกจากนี้ ถ้าผู้เสียหายมีจำนวน 1 คนขึ้นไป เช่นนี้เป็นคดีฉ้อโกงประชาชน (Public fraud) ซึ่งเป็นความผิดอันยอมความไม่ได้ ภัยคุกคามประเภทฟรอด หรือการฉ้อโกงหลอกลวง สามารถแบ่งออกได้เป็น 2 ประเภท คือ Phishing (ฟิชชิง) คือการล่อหลอกเหยื่อเข้าหน้าเว็บไซต์ปลอม ซึ่งทำให้ดูคล้ายกับหน้าล็อกอินของเว็บไซต์จริง จุดประสงค์เพื่อขโมยพาสเวิร์ดและนำไปสู่การขโมยข้อมูลอื่น ๆ โดยเฉพาะในเรื่องธุรกรรมทางการเงิน Scam (สแคม) คือการแอบอ้างเพื่ออาศัยผลจากความเข้าใจผิด เช่น การสร้างหน้าเว็บไซต์ปลอมแอบอ้างว่าเป็นเว็บไซต์ของบริการที่มีชื่อเสียงหลอกให้ร่วมเล่นเกมเพื่อชิงรางวัล เพื่อขโมยข้อมูลส่วนบุคคล ซึ่งจะนำไปสู่การปลอมแปลงอื่น ๆ เพื่อผลประโยชน์ของผู้ไม่หวังดีต่อไป	จึงทำการค้นหาด้วยการใส่แหล่งอ้างอิงตามหลังเพื่อให้ได้ความหมายที่เกี่ยวข้องกับงานด้านไซเบอร์ยิ่งขึ้น เป็นคำว่า Fraud etda และได้พบข้อมูลที่เกี่ยวข้อง

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
Malware	มัลแวร์	โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมา เพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูลหรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้	www.etda.or.th
Misconfiguration	มิสคอนฟิกกูเรชั่น	การกำหนดค่าที่ไม่ถูกต้องหรือไม่เหมาะสมของระบบข้อมูลหรือส่วนประกอบของระบบ ที่อาจนำไปสู่ช่องโหว่หรือจุดอ่อนของระบบ	https://csrc.nist.gov หมายเหตุ : ภายในwww.digitalskill.org มีการให้ความหมายของคำว่า Security Misconfiguration คือช่องโหว่เกี่ยวกับการตั้งค่าความมั่นคงปลอดภัย โดยสามารถเกิดได้ทุกที่ในระบบที่มีการตั้งค่า สาเหตุหลักเกิดจากการตั้งค่าอย่างไม่มั่นคงปลอดภัย หรือใช้ค่าตั้งต้น ที่ไม่มั่นคงปลอดภัยมาตั้งแต่ต้นอยู่แล้ว เกือบทุกระบบสามารถเกิดการตั้งค่าที่ไม่มั่นคงปลอดภัยเกิดขึ้นได้ แต่เนื่องจากคำศัพท์หลักคือ Misconfiguration จึงยึดคำศัพท์หลักโดยการหาข้อมูลจากเว็บไซต์ https://csrc. nist.gov และทำการแปลความหมายจากเว็บไซต์ดังกล่าว
Penetration Test	เพนิเทรชันเทส	Penetration Test หรือPenTest เป็นวิธีการประเมินความเสี่ยงด้วยการทดสอบเจาะระบบเพื่อค้นหาจุดอ่อนในการเข้าถึงระบบ	www.uih.co.th

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		ต่าง ๆ โดยใช้ผู้เชี่ยวชาญ ช่วยให้สามารถประเมินความเสี่ยงของระบบเครือข่ายลูกค้าว่ามีความเสี่ยงตรงจุดใด ซึ่งจะเป็นการทดสอบเจาะระบบในเชิงลึก พร้อมแจ้งผลการทดสอบ และประเมินความเสี่ยงเพื่อเตรียมการป้องกันไว้ก่อน ซึ่งการตรวจหาช่องโหว่นี้เป็นหนึ่งในมาตรการป้องกันภัยคุกคามทางไซเบอร์ที่ เหมาะสำหรับองค์กรที่ต้องการรักษาความปลอดภัยเป็นพิเศษและจำเป็นต้องตรวจสอบระบบอย่างสม่ำเสมอ	
Ransomware	แรนซัมแวร์	มัลแวร์เรียกค่าไถ่ เป็นมัลแวร์ที่เข้ารหัสลับข้อมูลในเครื่องเหยื่อ ทำให้ไม่สามารถเข้าถึงข้อมูลได้ และเรียกค่าไถ่จากเหยื่อเพื่อแลกกับการถอดรหัสลับ	ETDA Thailand Facebook page
Social Engineering	โซเชียว อินเจอเนริ่ง	วิศวกรรมสังคม เป็นเทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล ซึ่งบางครั้งอาจไม่จำเป็นต้องใช้เทคโนโลยีเข้ามาเกี่ยวข้องเลย ผู้ที่ตกเป็นเหยื่อของ Social Engineering อาจจะตกเป็นเหยื่อโดยความตั้งใจหรือไม่ตั้งใจของผู้ไม่หวังดีก็ได้ กล่าวคือ ถ้าผู้ไม่หวังดีมีเป้าหมายเฉพาะเจาะจง เช่น ต้องการข้อมูลความลับขององค์กรใดองค์กรหนึ่ง เหยื่อใน	Social Engineering

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		ที่นี้ก็มักจะเป็นผู้ที่มิสิทธิในการเข้าถึงข้อมูลความลับขององค์กรนั้น แต่หากเป้าหมายของผู้ไม่หวังดีเป็นแบบที่ไม่ได้เจาะจงเหยื่อ เช่น ต้องการรหัสบัตรเครดิต หรือบัญชีผู้ใช้และรหัสผ่านของบริการต่าง ๆ ของใครก็ได้ เหยื่อของผู้ไม่หวังดีนี้จะเป็นใครก็ตามซึ่งหลงเชื่อการหลอกลวงนั้น	
Supply Chain Attack	ซัพพลายเชนแอทแทค	การจู่โจมไปที่ผู้พัฒนาซอฟต์แวร์โดยมีจุดประสงค์เพื่อสอดแทรกมัลแวร์ลงในแอปพลิเคชัน ซึ่งจะทำให้ลูกค้าผู้ใช้งานแอปพลิเคชันนั้นตกเป็นเหยื่อได้โดยไม่รู้ตัว เนื่องจากมัลแวร์จะแฝงตัวมาในรูปของแอปพลิเคชันที่องค์กรซื้อใช้งานอยู่แล้ว หรืออาจกระจายตัวออกมาในรูปของอัปเดตสำหรับแอปนั้น จึงมีโอกาสที่จะหลุดรอดจากการตรวจจับได้สูงกว่าปกติ และสามารถทำงานในเครือข่ายของเป้าหมายได้เสมือนเป็นแอปพลิเคชันดั้งเดิมที่องค์กรไว้วางใจ	https://news.microsoft.com/
Website Defacement	การปลอมแปลงหน้าเว็บไซต์	การลอบเจาะระบบเข้าไปเปลี่ยนหน้าเว็บไซต์ แสดงสัญลักษณ์ โอ้อวดความสามารถ หรือความเห็นทางการเมือง	ETDA Thailand Facebook page
Website Phishing	ฟิชชิง	การหลอกให้เข้าเว็บไซต์ปลอมเพื่อลวงเอาข้อมูลที่สำคัญ เช่น	ETDA Thailand Facebook page

ภาษาอังกฤษ	ภาษาไทย	ความหมาย / คำจำกัดความ	แหล่งอ้างอิง / แหล่งที่มา
		การปลอมเว็บไซต์ธนาคารและส่งอีเมลแจ้งลูกค้าธนาคารให้เข้ามากรอกข้อมูล username และ password ที่เว็บปลอม และข้อมูลที่กรอกจะส่งไปยังมิจฉาชีพ	
Vulnerability	จุดอ่อนช่องโหว่	ช่องโหว่หรือจุดบกพร่องด้านระบบความปลอดภัยของคอมพิวเตอร์ โดยเปิดโอกาสให้ระบบข้อมูลอัตโนมัติถูกเจาะในรูปแบบการทำงานทางด้านฮาร์ดแวร์ และซอฟท์แวร์ ซึ่งสามารถเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต ก่อให้เกิดความเสียหายหรือสามารถสร้างภัยคุกคามให้กับองค์กร	www.nsm.or.th

ประเภทหน่วยงานที่ได้รับการสนับสนุน

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน 9 เหตุการณ์

หน่วยงานควบคุมและกำกับดูแล จำนวน 17 เหตุการณ์

หน่วยงานภาครัฐ จำนวน 404 เหตุการณ์

หน่วยงานเอกชน/อื่นๆ จำนวน 79 เหตุการณ์

แจ้งเตือนเหตุการณ์สำคัญ จำนวน 40 เรื่อง

ลำดับที่	วันตรวจพบ	เรื่อง	ประเภทภัยคุกคามไซ
1	8 ตุลาคม 2564	Apache HTTP Server Exploited	อื่น ๆ
2	18 พฤศจิกายน 2564	แจ้งเตือนการโจมตีเว็บไซต์ของหน่วยงานราชการ	Hacked Website (Website Defacement)
3	30 พฤศจิกายน 2564	แจ้งเตือนกรณีพบกลุ่ม call center แอบอ้างเป็นธนาคารเพื่อหลอกลวง	อื่น ๆ
4	3 ธันวาคม 2564	แจ้งเตือนเพื่อเฝ้าระวัง และตรวจสอบช่องโหว่เพื่อป้องกันการถูกโจมตีโดยฝังหน้าเว็บไซต์การพนันออนไลน์	อื่น ๆ
5	12 ธันวาคม 2564	Apache Log4j Security Vulnerabilities	อื่น ๆ
6	17 ธันวาคม 2564	Apache Log4j2 Security Vulnerabilities	อื่น ๆ
7	30 มกราคม 2565	Win32 Elevation Vulnerability	จุดอ่อนช่องโหว่
8	14 กุมภาพันธ์ 2565	Hive Ransomware	Ransomware
9	24 กุมภาพันธ์ 2565	BVP47	อื่น ๆ
10	25 กุมภาพันธ์ 2565	แจ้งหน่วยงานป้องกัน ติดตาม เฝ้าระวังสถานการณ์ ภัยคุกคามทางไซเบอร์ จากกรณีความขัดแย้งในต่างประเทศ	อื่น ๆ
11	9 เมษายน 2565	Spring4Shell	จุดอ่อนช่องโหว่
12	18 เมษายน 2565	Windows CVE-2022-26809	จุดอ่อนช่องโหว่
13	29 เมษายน 2565	Emotet Malware	Malware
14	3 พฤษภาคม 2565	Windows 10	Ransomware
15	5 พฤษภาคม 2565	การแจ้งเตือนการโจมตีเหตุการณ์ภัยคุกคามทางไซเบอร์ต่อหน่วยงานองค์การมหาชนแห่งหนึ่ง	Mail Phishing
16	10 พฤษภาคม 2565	F5 CVE-2022-1388	จุดอ่อนช่องโหว่

ลำดับที่	วันตรวจพบ	เรื่อง	ประเภทภัยคุกคาม
17	11 พฤษภาคม 2565	CVE-2022-1040 – authentication bypass vulnerability	จุดอ่อนช่องโหว่
18	23 พฤษภาคม 2565	CVE-2022-22954 และ CVE-2022-22960	จุดอ่อนช่องโหว่
19	3 มิถุนายน 2565	CVE-2022-30190	จุดอ่อนช่องโหว่
20	3 มิถุนายน 2565	MySQL Server	Data Breach
21	8 มิถุนายน 2565	แจ้งเตือนเหตุการณ์ภัยคุกคามทางไซเบอร์	Hacked Website (Defacement)
22	16 มิถุนายน 2565	Phishing Email เพื่อติดตั้ง Emotet Trojan Epoch5	Malware
23	27 มิถุนายน 2565	การโจมตีจากกลุ่ม APT32 หรือ OceanLotus โดยมีการโจมตีในรูปแบบใหม่	จุดอ่อนช่องโหว่
24	8 กรกฎาคม 2565	การแจ้งเตือนแอปพลิเคชันที่เป็นอันตราย	Hacked Website (Phishing)
25	15 กรกฎาคม 2565	CVE-2022-22047	จุดอ่อนช่องโหว่
26	19 กรกฎาคม 2565	การแจ้งเตือนกรณี MongoDB database มีจุดอ่อนช่องโหว่	จุดอ่อนช่องโหว่
27	27 กรกฎาคม 2565	13 แอปพลิเคชัน สามารถดูดเงิน และล้วงข้อมูลต่างๆได้	Malware
28	2 สิงหาคม 2565	NIST อัปเดตคำแนะนำความปลอดภัยด้านการดูแลสุขภาพ	อื่น ๆ
29	10 สิงหาคม 2565	แจ้งเตือน Agenda Ransomware	Ransomware
30	11 สิงหาคม 2565	ช่องโหว่ร้ายแรงที่เราท์เตอร์ของ DRAYTEK	จุดอ่อนช่องโหว่
31	11 สิงหาคม 2565	RapperBot	จุดอ่อนช่องโหว่
32	18 สิงหาคม 2565	แจ้งเตือน SOVA malware	Malware
33	23 สิงหาคม 2565	CISA เพิ่มช่องโหว่ใหม่ 7 ช่องโหว่ในรายการช่องโหว่ที่ต้องเฝ้าระวัง	จุดอ่อนช่องโหว่
34	24 สิงหาคม 2565	การอัปเดตความปลอดภัย CVE-2022-31676	จุดอ่อนช่องโหว่
35	24 สิงหาคม 2565	การอัปเดตความปลอดภัย CVE-2022-0028	จุดอ่อนช่องโหว่
36	26 สิงหาคม 2565	พบ Cobalt Strike Command and Control Server	จุดอ่อนช่องโหว่
37	2 กันยายน 2565	กรณี Apple ออกอัปเดต iOS 12.5.6 สำหรับอุปกรณ์รุ่นเก่า	จุดอ่อนช่องโหว่

ลำดับที่	วันตรวจพบ	เรื่อง	ประเภทภัยคุกคาม
38	14 กันยายน 2565	CVE-2022-34718	จุดอ่อนช่องโหว่
39	15 กันยายน 2565	Iranian Islamic Revolutionary Guard Corps Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations	จุดอ่อนช่องโหว่
40	24 กันยายน2565	กรณี NSA และ CISA เผยแพร่คำแนะนำเพื่อช่วยรักษาความปลอดภัยของระบบควบคุมโครงสร้างพื้นฐานที่สำคัญของ OT/ICS	จุดอ่อนช่องโหว่

ตารางที่ 3: แจ้งเตือนเหตุการสำคัญ