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

กวค. 42
วันที่ 18 มี.ค. 67
เวลา 9.10

ที่ สกมช ๐๘๒๐/๑๑๒๘

สลค. (eMail)
ส่ง : กวค.
รับที่ : ธ3280/67
15 มี.ค. 2567 เวลา 18.10 น.

๑๕ มีนาคม ๒๕๖๗

เรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖

เรียน เลขาธิการคณะรัฐมนตรี

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖

ด้วยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ขอเสนอเรื่อง รายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖ มาเพื่อคณะรัฐมนตรีทราบ โดยเรื่องนี้เข้าข่ายที่จะต้องนำเสนอคณะรัฐมนตรีตามพระราชกฤษฎีกาว่าด้วยการเสนอเรื่อง และการประชุมคณะรัฐมนตรี พ.ศ. ๒๕๔๘ มาตรา ๔ (๑) รวมทั้ง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) ให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” ทั้งนี้ นายภูมิธรรม เวชยชัย รองนายกรัฐมนตรี ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้เห็นชอบให้นำเรื่องดังกล่าวเสนอคณะรัฐมนตรีด้วยแล้ว

ทั้งนี้ เรื่องดังกล่าวมีรายละเอียด ดังนี้

๑. <u>เหตุผลความจำเป็นที่ต้องเสนอคณะรัฐมนตรี</u>

ตามอ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) บัญญัติให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีหน้าที่และอำนาจ “จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่มีผลกระทบอย่างมีนัยสำคัญ หรือแนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้คณะรัฐมนตรีทราบ” นั้น คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จึงขอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖ ให้คณะรัฐมนตรีเพื่อรับทราบ โดยมีสาระสำคัญประกอบด้วย ข้อมูลทั่วไป สรุปสถานการณ์ของภัยคุกคามทางไซเบอร์ในประเทศไทย ผลการดำเนินการที่สำคัญ บทวิเคราะห์สถานการณ์ แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ เพื่อใช้เป็นข้อมูลสำหรับการพัฒนาแนวทางและมาตรการในการป้องกัน รับมือ เพื่อลดความเสี่ยงต่อการเกิดภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงานซึ่งมีภารกิจหรือบริการที่ส่งผลกระทบถึงประชาชนต่อไป

/๒. ความเร่งด่วน...

๒. <u>ความเร่งด่วนของเรื่อง</u>

ไม่มี

๓. <u>สาระสำคัญ ข้อเท็จจริงและข้อกฎหมาย</u>

๓.๑ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้ดำเนินการติดตามวิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึงการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้อง ในการปฏิบัติการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ โดยได้นำเสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖ ในการประชุมคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ครั้งที่ ๔/๒๕๖๖ ในวันอังคารที่ ๒๘ พฤศจิกายน ๒๕๖๖ เวลา ๑๓.๐๐ น. ณ ห้องประชุม ๓๐๑ ชั้น ๓ ตึกบัญชาการ ๑ ทำเนียบรัฐบาล โดยที่ประชุมมีมติเห็นชอบให้รายงานคณะรัฐมนตรีเพื่อทราบ

๓.๒ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้จัดทำรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖ ในภารกิจเกี่ยวกับการป้องกัน รับมือ แก้ไขปัญหา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ รวมทั้งสิ้น ๑,๘๐๘ เหตุการณ์ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย โดยสรุปสาระสำคัญ ได้ดังนี้

๓.๒.๑ สถิติเหตุการณ์ภัยคุกคามทางไซเบอร์ ที่ได้ดำเนินการและตรวจพบมากที่สุด แบ่งเป็นประเภทของภัยคุกคามทางไซเบอร์ ได้ดังนี้

๓.๒.๑.๑ ประเภท Hacked Website จำนวนรวม ๑,๐๕๖ เหตุการณ์ แบ่งออกเป็นประเภท Gambling (การพนันออนไลน์) จำนวน ๕๒๒ เหตุการณ์, Website Defacement จำนวน ๔๗๕ เหตุการณ์, Website Phishing จำนวน ๔๗ เหตุการณ์ และ Website Malware ๑๒ เหตุการณ์

๓.๒.๑.๒ ประเภทเว็บไซต์ปลอม (Fake Website) จำนวน ๓๑๐ เหตุการณ์

๓.๒.๑.๓ ประเภท Finance Scam (หลอกลวงการเงิน Online) จำนวน ๑๑๑ เหตุการณ์

๓.๒.๑.๔ ประเภทข้อมูลรั่วไหล (Data Lesk) จำนวน ๑๐๓ เหตุการณ์

๓.๒.๑.๕ ประเภทจุดอ่อนช่องโหว่ (Vulnerability) จำนวน ๘๔ เหตุการณ์

๓.๒.๑.๖ ประเภทการละเมิดข้อมูล (Data Breach) จำนวน ๕๐ เหตุการณ์

๓.๒.๑.๗ ประเภทการโจมตี Distributed denial of service (DDoS) จำนวน ๓๓ เหตุการณ์

๓.๒.๑.๘ ประเภทมัลแวร์เรียกค่าไถ่ (Ransomware) จำนวน ๓๐ เหตุการณ์

๓.๒.๑.๙ ประเภทอื่น ๆ จำนวน ๓๑ เหตุการณ์

๓.๒.๒ ประเภทของหน่วยงานที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ โดยแบ่งตามภารกิจหรือบริการของหน่วยงาน สรุปได้ดังนี้

๓.๒.๒.๑ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จำนวน ๒๐๒ เหตุการณ์

๓.๒.๒.๒ หน่วยงานควบคุมหรือกำกับดูแล จำนวน ๕๐ เหตุการณ์

๓.๒.๒.๓ หน่วยงานของรัฐ จำนวน ๑,๓๐๙ เหตุการณ์

๓.๒.๒.๔ หน่วยงานเอกชน จำนวน ๒๔๗ เหตุการณ์

/๓.๒.๓ ผลการ...

๓.๒.๓ ผลการปฏิบัติงานเพื่อสนับสนุนหน่วยงานในการช่วยแก้ไขปัญหาและรับมือกับภัยคุกคามทางไซเบอร์ โดยเป็นการปฏิบัติตามมาตรการเชิงรุก เชิงรับ และบริหารจัดการคุณภาพ โดยสรุปได้ ดังนี้

๓.๒.๓.๑ การแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๗๑ รายงาน

๓.๒.๓.๒ การเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์และข่าวสารที่เป็นประโยชน์ต่อสาธารณะ ๔๔๗ รายงาน

๓.๒.๓.๓ การทดสอบความปลอดภัยของระบบเครื่องแม่ข่ายและเว็บไซต์เพื่อหาจุดอ่อนช่องโหว่ จำนวน ๑๑๕ หน่วยงาน

๓.๒.๓.๔ การแจ้งเตือนเหตุการณ์และให้คำแนะนำในการแก้ไขปัญหา ๑,๘๐๘ หน่วยงาน

๓.๒.๓.๕ การตอบสนองและรับมือภัยคุกคามทางไซเบอร์ ๔๕ เหตุการณ์

๓.๒.๓.๖ การดำเนินการที่เกี่ยวข้องกับอาชญากรรมทางไซเบอร์ที่กระทบต่อหน่วยงานและประชาชน โดยการขอปิดกั้นการเข้าถึงหน้าเว็บไซต์ที่ปลอมแปลงเป็นหน่วยงานสำคัญ จำนวน ๔๒๖ เว็บไซต์

๓.๒.๓.๗ การสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน ๓๘ ครั้ง มีจำนวนผู้เข้าร่วมทั้งสิ้น ๕,๘๗๔ คน

๓.๒.๓.๘ การทำบันทึกความเข้าใจว่าด้วยความร่วมมือ ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ จำนวน ๕ หน่วยงาน

๓.๒.๔ แนวทางการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ เนื่องด้วยปัจจุบันการให้บริการหรือประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม มีความเสี่ยงจากภัยคุกคามทางไซเบอร์ อันอาจกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ จึงได้มีการจัดทำแนวทางการปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นแนวทางในการปฏิบัติภารกิจต่าง ๆ จำนวน ๒ แนวทาง ดังนี้

๓.๒.๔.๑ แนวทางการปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ให้กับกิจกรรมเฉพาะกิจระดับประเทศ

๓.๒.๔.๒ แนวทางการปฏิบัติเพื่อการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ให้กับหน่วยงานที่เกี่ยวข้องกับการเลือกตั้งระดับประเทศ

๓.๒.๕ แนวโน้มสถานการณ์ภัยคุกคามทางไซเบอร์ในปี พ.ศ. ๒๕๖๗ มีแนวโน้มว่าการโจมตีแบบ Hacked Website ยังคงเป็นภัยคุกคามที่มีโอกาสพบเป็นจำนวนมาก ซึ่งกลุ่มที่เป็นภัยคุกคามจะทำการฝังเนื้อหาเว็บไซต์การพนันออนไลน์ เปลี่ยนแปลงหน้าเว็บไซต์ เพื่อทำเว็บไซต์ฟิชชิ่ง และฝังมัลแวร์ สำหรับกรณีการโจมตีแบบ Fake Website ซึ่งผู้ไม่หวังดีจะทำการปลอมหน้าเว็บไซต์ให้มีความคล้ายกับเว็บไซต์จริง เพื่อหลอกให้ผู้ใช้งานดาวน์โหลดแอปพลิเคชันที่เป็น Android Remote Access Trojan (RAT) ซึ่งหากมีผู้หลงเชื่อทำการดาวน์โหลดแอปพลิเคชันและติดตั้งโปรแกรมที่เป็นอันตราย ดังกล่าว ลงในอุปกรณ์โทรศัพท์มือถือ Android ก็จะถูกขโมยข้อมูลที่มีความ Sensitive ออกไปได้ และรูปแบบการโจมตีประเภท Ransomware มีแนวโน้มสูงขึ้นเรื่อย ๆ และมีการเปลี่ยนแปลงรูปแบบการโจมตีเป็นรูปแบบบริการในลักษณะ Ransomware as a Service (RaaS) โดยนักพัฒนาจะปรับแต่ง Ransomware ตามความต้องการของผู้โจมตีที่จะนำไปใช้ เพื่อบล็อกผู้ใช้งานไม่ให้เข้าถึงระบบคอมพิวเตอร์ของตนเพื่อแลกกับค่าไถ่ และจะมีการสร้างคำขู่เพื่อเรียกค่าไถ่เกี่ยวกับการชำระเงินทางการเงินเพื่อแลกกับการถอดรหัส ส่วนใหญ่กลุ่มที่เป็นเป้าหมายจะเน้นที่องค์กรภาครัฐมากกว่าบุคคล ดังนั้น ผู้ดูแลระบบควรทำการสำรองข้อมูล (Backup) เป็นประจำและเพื่อป้องกัน

/ข้อมูลที่...

ข้อมูลที่ Backup ถูกเข้ารหัสไปด้วย ผู้ใช้งานควรสำรองข้อมูลลงบนอุปกรณ์สำหรับจัดเก็บข้อมูลภายนอกเครือข่าย (Cloud Storage, External Hard Drive, USB Flash Drive) อัปเดตซอฟต์แวร์ในเครื่องอย่างสม่ำเสมอ ซึ่งการอัปเดตระบบปฏิบัติการและซอฟต์แวร์จะช่วยป้องกันการโจมตีที่ต้องอาศัยช่องโหว่ของซอฟต์แวร์ได้ และควรติดตามข่าวสารช่องโหว่หรือภัยคุกคามต่าง ๆ รวมถึงศึกษาวิธีการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อของเหล่าผู้ไม่หวังดีและเพื่อความปลอดภัยของตัวผู้ใช้งานเอง

๔. <u>ประเด็นด้านกฎหมายและมติคณะรัฐมนตรีเกี่ยวข้อง</u>

คณะรัฐมนตรีมีมติ (๒๑ มีนาคม ๒๕๖๖) รับทราบรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๔ - ๓๐ กันยายน ๒๕๖๕ ได้แก่ (๑) สถิติเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยมีการโจมตีด้วยการแฮกเว็บไซต์มากที่สุดถึง ๓๖๗ เหตุการณ์ (๒) สถิติการปฏิบัติงานในการสนับสนุนช่วยแก้ไขปัญหาและรับมือกับภัยคุกคามทางไซเบอร์ เช่น แจ้งเตือนเหตุการณ์ให้คำปรึกษาและแนะนำในการแก้ไขปัญหา ๔๖๗ เหตุการณ์ (๓) ประเภทของหน่วยงานที่ถูกโจมตีด้วยภัยคุกคามทางไซเบอร์มากที่สุด ๕ อันดับแรก รวม ๔๔๙ เหตุการณ์ ได้แก่ หน่วยงานด้านการศึกษา ๒๑๑ เหตุการณ์ หน่วยงานของรัฐที่ไม่ใช่หน่วยงานโครงสร้างพื้นฐานสำหรับทางสารสนเทศ ๑๓๕ เหตุการณ์ หน่วยงานด้านสาธารณสุข ๖๗ เหตุการณ์ ผู้ประกอบการที่เป็นบริษัทเอกชนและสัญชาติไทย ๒๔ เหตุการณ์ และผู้ประกอบกิจการให้เช่าพื้นที่เว็บไซต์หรือที่เป็นดาต้าเซ็นเตอร์ ๑๒ เหตุการณ์ (๔) แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ เช่น การโจมตีด้วยการแฮกเว็บไซต์หน่วยงานราชการและหน่วยงานสำคัญเป็นรูปแบบที่ถูกตรวจพบมากที่สุด (๕) แนวทางการจัดการภัยคุกคามทางไซเบอร์ เช่น การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ และการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ และ (๖) ข้อเสนอแนะในการแก้ไขปัญหาที่สำคัญจากแนวโน้มสถานการณ์ทางไซเบอร์ เช่น การถูกโจมตีด้วยการแฮกเว็บไซต์ เป็นเรื่องที่ผู้ดูแลระบบของหน่วยงานควรให้ความสนใจกับการปรับปรุง Patch ของระบบปฏิบัติการหรือระบบบริหารจัดการเว็บไซต์ให้เป็นปัจจุบัน และสถานการณ์อาชญากรรมทางไซเบอร์ที่กระทบต่อประชาชน ควรสร้างความรู้ความเข้าใจและให้ความตระหนักรู้กับประชาชน โดยเฉพาะการสร้างการรับรู้เกี่ยวกับรูปแบบและวิธีการที่เหล่ามิจฉาชีพใช้ในการหลอกลวง ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเสนอ

๕. <u>ข้อเสนอส่วนราชการ</u>

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พิจารณาแล้วเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๙ (๑๒) จึงเห็นควรนำเสนอรายงานสรุปผลการดำเนินงานของการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีผลกระทบอย่างมีนัยสำคัญ ในห้วงวันที่ ๑ ตุลาคม ๒๕๖๕ - ๓๐ กันยายน ๒๕๖๖ ต่อที่ประชุมคณะรัฐมนตรีเพื่อรับทราบ

จึงเรียนมาเพื่อโปรดนำกราบเรียนนายกรัฐมนตรีเพื่อเสนอคณะรัฐมนตรีทราบต่อไป

ขอแสดงความนับถือ

(นายภูมิธรรม เวชยชัย)
รองนายกรัฐมนตรี
ประธานกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕
อีเมล thaicert@ncsa.or.th

QR code เอกสารแนบ