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

ด่วนที่สุด

ที่ สกมช ๐๘๑๐/๔๕๗

๕ มิถุนายน ๒๕๖๘

เรื่อง ขอให้หน่วยงานดำเนินการตามแนวปฏิบัติขั้นพื้นฐานสำหรับการป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย ๑. แนวทางการตอบสนอง ป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์
๒. แบบตอบรับการดำเนินการตามแนวทางการตอบสนอง ป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

ตามอ้างถึง ๑ มาตรา ๔๕ และ มาตรา ๒๒ (๖) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์” ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันสถาณการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ ภายในประเทศเพิ่มสูงขึ้นอย่างมีนัยสำคัญ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หรือ ThaiCERT ได้ดำเนินการเฝ้าระวัง ตรวจสอบ และได้ร่วมเผชิญเหตุตอบสนองรับมือกับภัยคุกคามที่เกิดขึ้นหลายเหตุการณ์ พบว่ามีการโจมตีหน่วยงานและอาจส่งผลกระทบต่อการให้บริการประชาชน ดังนี้

๑. การโจมตีแบบ DDoS ต่อหน่วยงานในประเทศไทยหลายแห่ง ส่งผลให้บริการหยุดชะงักชั่วคราว

๒. การโจมตีทางไซเบอร์ต่อหน่วยงานของรัฐโดยใช้บัญชีผู้ใช้งาน (Credential) ที่เคยรั่วไหลในการเข้าสู่ระบบ โดยผู้โจมตีได้รับข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตนจากแหล่งซื้อขาย เช่น Dark Web หรือ Breach Forum รวมถึงมีการแชร์ข้อมูลบัญชีผู้ใช้งาน (Credential) ที่ขโมยมาได้ในแพลตฟอร์มการสื่อสารผ่านระบบอิเล็กทรอนิกส์ต่าง ๆ โดยผู้โจมตีจะใช้ข้อมูลที่ได้มาในการเข้าถึงช่องทางเครือข่ายภายในของหน่วยงาน อย่างเช่น ระบบ VPN และใช้ข้อมูลเหล่านั้นเข้าสู่ระบบงานสำคัญต่าง ๆ จากนั้นก็ทำการขโมยข้อมูลของหน่วยงานออกไปและโจมตีเพื่อทำลายระบบต่าง ๆ ด้วย Ransomware เป็นต้น

๓. การโจมตีในรูปแบบเปลี่ยนแปลงหน้าเว็บ (Web Defacement) เพื่อสร้างความไม่น่าเชื่อถือให้แก่หน่วยงาน

๔. Data Breach เหตุการณ์ที่ข้อมูลสำคัญขององค์กร เช่น ข้อมูลลูกค้า ข้อมูลส่วนบุคคล หรือข้อมูลทางธุรกิจ ถูกเข้าถึง ดัดแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจเกิดจากการถูกแฮก การตั้งค่าระบบผิดพลาด หรือความประมาทของบุคลากร โดยเหตุการณ์นี้สามารถส่งผลกระทบรุนแรงต่อชื่อเสียง ความเชื่อมั่น และความเสียหายทางการเงินขององค์กร

/ในการนี้...

ในการนี้ เพื่อให้สามารถป้องกัน รับมือ และลดความซึ่งอาจส่งผลให้เกิดความเสียหายต่อระบบอย่างร้ายแรง และถูกขโมยข้อมูลสำคัญรวมถึงข้อมูลส่วนบุคคลของหน่วยงานและประชาชน สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้จัดทำแนวปฏิบัติขั้นพื้นฐานสำหรับตอบสนอง ป้องกันและรับมือสำหรับหน่วยงานระยะเร่งด่วน เพื่อมิให้สร้างผลกระทบต่อระบบสารสนเทศหรือประชาชนที่มาใช้บริการหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงขอให้หน่วยงานของท่านนำไปดำเนินการให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น และเมื่อได้รับหนังสือฉบับนี้ ขอความอนุเคราะห์ยืนยันการรับทราบหนังสือให้ สกมช. ทางอีเมล thaicert@ncsa.or.th ทันที และขอให้ผู้บริหารหน่วยลงนามยืนยันแจ้งผลการดำเนินการตามแบบตอบรับ (สิ่งที่ส่งมาด้วย) ให้ สกมช. ทราบทางอีเมล thaicert@ncsa.or.th อีกครั้ง ภายในวันที่ ๓๐ มิถุนายน ๒๕๖๘ ทั้งนี้ สกมช. จะได้รวบรวมรายงานผลให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยมี นายกรัฐมนตรี เป็นประธาน เพื่อรับทราบต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

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

TLP:CLEAR

การแจ้งเตือนกรณีเหตุการณ์การโจมตีหน่วยงานในประเทศไทย

ปัจจุบันสถาณการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานต่าง ๆ ภายในประเทศเพิ่มสูงขึ้นอย่างมีนัยสำคัญ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หรือ ThaiCERT ได้ดำเนินการเฝ้าระวัง ตรวจสอบ และได้ร่วมเผชิญเหตุตอบสนองรับมือกับภัยคุกคามที่เกิดขึ้นหลายเหตุการณ์ พบว่ามีการโจมตีหน่วยงานและอาจส่งผลกระทบต่อการให้บริการประชาชน ดังนี้

๑. การโจมตีแบบ DDoS ต่อหน่วยงานในประเทศไทยหลายแห่ง ส่งผลให้บริการหยุดชะงักชั่วคราว

๒. การโจมตีทางไซเบอร์ต่อหน่วยงานของรัฐโดยใช้บัญชีผู้ใช้งาน (Credential) ที่เคยรั่วไหลในการเข้าสู่ระบบ โดยผู้โจมตีได้รับข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตนจากแหล่งซื้อขาย เช่น Dark Web หรือ Breach Forum รวมถึงมีการแชร์ข้อมูลบัญชีผู้ใช้งาน (Credential) ที่ขโมยมาได้ในแพลตฟอร์มการสื่อสารผ่านระบบอิเล็กทรอนิกส์ต่าง ๆ โดยผู้โจมตีจะใช้ข้อมูลที่ได้มาในการเข้าถึงช่องทางเครือข่ายภายในของหน่วยงาน อย่างเช่น ระบบ VPN และใช้ข้อมูลเหล่านั้นเข้าสู่ระบบงานสำคัญต่าง ๆ จากนั้นก็ทำการขโมยข้อมูลของหน่วยงานออกไปและโจมตีเพื่อทำลายระบบต่าง ๆ ด้วย Ransomware เป็นต้น

Domain	จำนวนบัญชี
go.th	2,157,625
ac.th	1,504,870
or.th	406,082
co.th	2,295,370

๓. การโจมตีในรูปแบบเปลี่ยนแปลงหน้าเว็บ (Web Defacement) เพื่อสร้างความไม่น่าเชื่อถือให้แก่หน่วยงาน

๔. Data Breach เหตุการณ์ที่ข้อมูลสำคัญขององค์กร เช่น ข้อมูลลูกค้า ข้อมูลส่วนบุคคล หรือข้อมูลทางธุรกิจ ถูกเข้าถึง ดัดแปลง หรือเปิดเผยโดยไม่ได้รับอนุญาต ซึ่งอาจเกิดจากการถูกแฮก การตั้งค่าระบบผิดพลาด หรือความประมาทของบุคลากร โดยเหตุการณ์นี้สามารถส่งผลกระทบรุนแรงต่อชื่อเสียง ความเชื่อมั่น และความเสียหายทางการเงินขององค์กร

TLP:CLEAR

แนวทางการป้องกัน เฝ้าระวัง และรับมือภัยคุกคามทางไซเบอร์

๑. Distributed Denial of Service (DDoS)

๑.๑ แนวทางการป้องกัน

- ใช้บริการป้องกัน DDoS จากผู้ให้บริการ Cloud หรือ CDN เช่น Cloudflare, Akamai, AWS Shield
- วางระบบ Load Balancer เพื่อกระจายโหลดไปยังหลายเซิร์ฟเวอร์
- Rate Limiting และ Firewall Rules บน Web Application Firewall (WAF)

๑.๒ แนวทางการเฝ้าระวัง

- ติดตั้งระบบ Monitoring เพื่อตรวจสอบทราฟฟิกการใช้งานแบบ Real-time
- กำหนด Threshold การใช้งาน Bandwidth และ Connections เพื่อแจ้งเตือนเมื่อเกินค่าที่กำหนด
- ตรวจสอบ Logs การใช้งานจากอุปกรณ์จต่างๆ เช่น Firewall, Router และ Load Balancer อย่างสม่ำเสมอ

๑.๓ แนวทางการรับมือ

- จัดทำ Playbook การตอบสนองฉุกเฉิน (Incident Response Plan) สำหรับ DDoS
- แจ้งผู้ให้บริการระบบรับทราบ เพื่อบล็อกทราฟฟิกที่โจมตีหากจำเป็น

๒. Credential Leak

๒.๑ แนวทางการป้องกัน

- ใช้งาน Multi-Factor Authentication (MFA) สำหรับทุกบัญชีที่เข้าถึงระบบ
- บังคับใช้นโยบายรหัสผ่านที่เข้มงวด (เช่น มีความยาวขั้นต่ำ, complexity)

๒.๒ แนวทางการเฝ้าระวัง

- ตรวจสอบรหัสผ่านรั่วไหลในฐานข้อมูลสาธารณะ (เช่น HaveIBeenPwned) ด้วยเครื่องมืออัตโนมัติ
- ตรวจสอบการเข้าสู่ระบบนอกเวลาทำงานหรือจากอุปกรณ์หรือแหล่งที่ไม่ทราบที่มา3.3 แนวทางการรับมือ

๒.๓ แนวทางการรับมือ

- รีเซ็ตรหัสผ่านทันที เมื่อทราบถึงเหตุการณ์รั่วไหลจากบัญชีผู้ใช้ภายในหน่วยงาน
- แจ้งผู้ใช้และแนะนำการเปลี่ยนรหัสผ่าน

๓. Web Defacement

๓.๑ แนวทางการป้องกัน

- อัปเดต CMS/Framework และ Plugins เสมอ
- จำกัดสิทธิ์ของผู้ใช้งาน (Principle of Least Privilege) โดยเฉพาะบัญชี Admin
- ใช้ Web Application Firewall (WAF) เพื่อตรวจจับและป้องการโจมตี

๓.๒ แนวทางการเฝ้าระวัง

- ใช้ระบบ File Integrity Monitoring (FIM) เพื่อตรวจสอบการเปลี่ยนแปลงของไฟล์ในเว็บเซิร์ฟเวอร์
- ตั้งระบบตรวจจับการเปลี่ยนแปลงหน้าเว็บแบบอัตโนมัติ (เช่น เครื่องมือ Web page diff checker)

๓.๓ แนวทางการรับมือ

- ตรวจสอบช่องโหว่ที่ถูกใช้ และทำการอุดช่องโหว่ทันที
- เก็บหลักฐานการโจมตี (Logs, Snapshot) เพื่อใช้ในการวิเคราะห์และดำเนินคดี
- แจ้งผู้เกี่ยวข้อง เช่น ผู้ให้บริการ Hosting หรือ CERT

๔. Data Breach

๔.๑ แนวทางการป้องกัน

- การควบคุมสิทธิ์การเข้าถึงข้อมูล (Access Control) โดยใช้หลัก Least Privilege และ Role-Based Access Control (RBAC) จำกัดสิทธิ์ให้ผู้ใช้งานเข้าถึงเฉพาะข้อมูลที่จำเป็นเท่านั้น
- เข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะส่งผ่าน โดยใช้มาตรฐานการเข้ารหัสที่ยอมรับได้ เช่น AES-256, TLS 1.3
- ใช้นโยบายรหัสผ่านและ MFA บังคับใช้รหัสผ่านที่รัดกุมและใช้ Multi-Factor Authentication (MFA) สำหรับการเข้าถึงระบบที่สำคัญ

๔.๒ แนวทางการเฝ้าระวัง

- ใช้ระบบ SIEM (Security Information and Event Management) รวม log จากหลายแหล่งเพื่อตรวจสอบและแจ้งเตือนเหตุการณ์ผิดปกติ เช่น การเข้าถึงข้อมูลจำนวนมากผิดปกติ
- ติดตามพฤติกรรมของผู้ใช้งานใช้ เพื่อระบุพฤติกรรมผิดปกติที่อาจบ่งชี้ถึงการละเมิดข้อมูล

๔.๓ แนวทางการรับมือ

- จัดทำ Incident Response Plan สำหรับ Data Breach โดยเฉพาะ ระบุขั้นตอนการรับมือ การติดต่อภายใน/ภายนอก และการรายงานเหตุการณ์ตามกฎหมาย
- แจ้งเตือนผู้ได้รับผลกระทบ ดำเนินการตามข้อกำหนดด้านกฎหมาย เช่น NCSA, PDPA โดยแจ้งผู้ใช้งานหรือลูกค้าที่ได้รับผลกระทบโดยเร็ว
- ดำเนินการฟื้นฟูระบบและปรับปรุงมาตรการรักษาความปลอดภัย อัปเดตระบบ, รีเซ็ตรหัสผ่าน, แก้ไขช่องโหว่ และทบทวนมาตรการที่ใช้