

แจ้งเตือนหน่วยงานเพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์

วันที่แจ้งเตือน 1 ตุลาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เฝ้าระวังความเสี่ยงด้านภัยคุกคามไซเบอร์ และพบสัญญาณการเคลื่อนไหวสืบเนื่องจากสถานการณ์ความขัดแย้งด้านภูมิรัฐศาสตร์ (Geopolitical Conflict) โดยกลุ่มผู้ไม่หวังดีได้ประกาศเจตนามุ่งโจมตีหน่วยงานภาครัฐและเอกชนในประเทศไทย ผ่านช่องทางต่าง ๆ เช่น Telegram และโซเชียลมีเดีย ดังรายละเอียด

รูปแบบการโจมตี	คำแนะนำ
1. DDoS Attack การส่งทราฟฟิกจำนวนมากจากหลายแหล่งเข้าสู่ระบบพร้อมกัน จนทำให้เว็บไซต์ล่ม ระบบช้า บริการออนไลน์ไม่สามารถให้บริการได้ตามปกติ 2. Website Defacement การแก้ไขหน้าเว็บไซต์ แทรกข้อความหรือรูปภาพ เผยแพร่เนื้อหาไม่เหมาะสม ซึ่งอาจส่งผลต่อภาพลักษณ์และความน่าเชื่อถือขององค์กร 3. ภัยคุกคามอื่น ๆ ซึ่งอาจนำไปสู่การรั่วไหลของข้อมูลและการหยุดชะงักของบริการสำคัญ • การเข้าถึงระบบโดยไม่ได้รับอนุญาต • การขโมยข้อมูล • การแก้ไขหรือทำลายข้อมูล • Malware • Ransomware	1. ด้านเครือข่ายและระบบ • เพิ่มความสามารถในการรองรับทราฟฟิกจำนวนมาก • เฝ้าระวังและวิเคราะห์ Network Traffic อย่างต่อเนื่อง • ใช้มาตรการป้องกัน เช่น WAF, Anti-DDoS, IDS/IPS เป็นต้น • ตรวจสอบและอุดช่องโหว่อย่างสม่ำเสมอ 2. ด้านบัญชีผู้ใช้ (Identity Security) • ตรวจสอบบัญชีผู้ใช้และบัญชีผู้ดูแลระบบ • บังคับเปลี่ยนรหัสผ่านหากมีความเสี่ยง • ใช้รหัสผ่านที่ซับซ้อน • หลีกเลี่ยงการใช้รหัสผ่านซ้ำ • กำหนดการล็อกบัญชีเมื่อมีการใส่รหัสผิดหลายครั้ง • ทบทวนสิทธิ์การเข้าถึงระบบเป็นประจำ 3. จัดทำหรือปรับปรุง แผนตอบสนองเหตุการณ์ไซเบอร์ (Incident Response Plan) และ เตรียมช่องทางประสานงานภายในให้พร้อมใช้งาน
การยกระดับ: ThaiCERT แนะนำให้เปิดใช้ Multi-Factor Authentication (MFA) หรือระบบพิสูจน์ตัวตนบุคคลผ่านแอปพลิเคชัน ThaiID (ไทยดี) สำหรับ Administrator Account Privileged Account บัญชีที่เข้าถึงข้อมูลสำคัญบัญชีที่เข้าถึงระบบจากภายนอกองค์กรเพื่อป้องกันการนำ Credential ที่รั่วไหลไปใช้งานโดยมิชอบ ให้สอดคล้องกับมติคณะรัฐมนตรี เมื่อวันที่ 11 สิงหาคม 2569 เรื่อง แนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (MFA) เพื่อลดความเสี่ยงจากการรั่วไหลของข้อมูลยืนยันตัวตนหรือการนำบัญชีผู้ใช้งานไปใช้โดยไม่ได้รับอนุญาต (อ้างอิง2)	
แนวทางปฏิบัติเพิ่มเติมที่สามารถทำทันที: 1. Patch & Vulnerability Management ตรวจสอบช่องโหว่และปิดช่องโหว่ที่อาจถูกใช้โจมตี 2. Backup สำรองข้อมูลอย่างน้อย 3 ชุดมี Offline Backup แยก Backup ออกจากระบบหลัก 3. Remote Access Review ตรวจสอบ VPN, Remote Desktop Protocol (RDP) การเข้าถึงจากภายนอกองค์กร	4. Update Systems อัปเดต Operating System, Applications, Firmware ช่องโหว่ Zero-Day 5. ตรวจสอบอุปกรณ์ Work From Home โดยเฉพาะเครื่องของผู้ดูแลระบบ 6. ThaiCERT แนะนำให้สมัครใช้บริการ Thailand Cyber Threat Intelligence (TCTI) เพื่อรับข้อมูล Threat Intelligence และนำไปใช้กับ Firewall, IPS, EDR เพื่อเพิ่มประสิทธิภาพในการป้องกันและตรวจจับภัยคุกคาม

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 1 ต.ค. 2569
2. https://resolution.soc.go.th/?prep_id=416138