แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

การยกระดับมาตรการเฝ้าระวัง ป้องกัน และเตรียมความพร้อมรับมือภัยคุกคามทางไซเบอร์

วันที่แจ้งเตือน 9 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (“ThaiCERT สกมช.”) ได้ติดตามสถานการณ์ความขัดแย้งระหว่างประเทศที่มีความตึงเครียด ประกอบกับภัยคุกคามทางไซเบอร์ที่มีความรุนแรงและซับซ้อนมากขึ้น รวมถึงการนำเทคโนโลยีปัญญาประดิษฐ์ (AI) มาใช้สนับสนุนในการโจมตี เช่น การค้นหาช่องโหว่ การสร้างข้อความหลอกลวง การปลอมแปลงตัวตน และการโจมตีแบบอัตโนมัติ เป็นต้น ซึ่งอาจเพิ่มความเสี่ยงต่อระบบสารสนเทศและการให้บริการของผู้ประกอบธุรกิจ ทั้งนี้ เพื่อเตรียมพร้อมในการรับมือต่อภัยคุกคามทางไซเบอร์ ขอให้หน่วยงานพิจารณายกระดับมาตรการด้านความมั่นคงปลอดภัย ดังนี้

1) เพิ่มการเฝ้าระวังและเตรียมความพร้อม กำหนดผู้รับผิดชอบติดตามสถานการณ์และการแจ้งเตือนด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง โดยเฉพาะระบบสำคัญและระบบงานที่เชื่อมต่ออินเทอร์เน็ต รวมทั้งกำหนดผู้มีอำนาจตัดสินใจ ช่องทางประสานงาน และขั้นตอน Incident Escalation ให้พร้อมใช้งานเมื่อเกิดเหตุ

2) ตรวจสอบและลดความเสี่ยงของระบบที่เปิดให้เข้าถึงจากภายนอก โดยดำเนินการสำรวจระบบ internet-facing เช่น เว็บไซต์ อีเมล VPN อุปกรณ์เครือข่าย ระบบคลาวด์ และระบบบริหารจัดการ เป็นต้น และพิจารณาเร่งแก้ไขช่องโหว่ที่มีความรุนแรงสูง ช่องโหว่ที่มีการนำไปโจมตีจริง และ Zero-day รวมทั้งปิดพอร์ต บริการ หรือฟังก์ชันที่ไม่จำเป็น และจำกัดการเข้าถึง VPN และ Remote management เฉพาะผู้ที่จำเป็น ทั้งนี้ หากยังไม่สามารถแก้ไขช่องโหว่ได้ทันที ควรกำหนดมาตรการชั่วคราวเพื่อลดความเสี่ยง

3) เพิ่มความเข้มงวดด้านบัญชีผู้ใช้งานและสิทธิการใช้งาน ใช้นโยบายรหัสผ่านที่เหมาะสม เปิดใช้งาน MFA โดยเฉพาะบัญชีผู้ดูแลระบบและระบบสำคัญ ตรวจสอบ Credential ที่อาจรั่วไหล ทบทวนสิทธิบัญชีผู้ใช้งาน ปิดบัญชีที่ไม่ใช้งานหรือไม่ทราบผู้รับผิดชอบ และเฝ้าระวังพฤติกรรมเข้าสู่ระบบที่ผิดปกติ

4) สำรองข้อมูลและทดสอบการกู้คืนระบบ ดำเนินการสำรองข้อมูลสำคัญตามหลัก 3-2-1 พร้อมพิจารณาใช้ Offline หรือ Immutable Backup และทดสอบการกู้คืนอย่างสม่ำเสมอ โดยกำหนด RTO/RPO ให้สอดคล้องกับความสำคัญของระบบ รวมทั้งทบทวน Incident Response Plan, BCP และ DRP และฝึกซ้อมแผนดังกล่าวเพื่อให้สามารถปฏิบัติได้จริงเมื่อเกิดเหตุ

5) บริหารความเสี่ยงจากบุคลากร ผู้ให้บริการภายนอก และ AI ทบทวนสิทธิของผู้ให้บริการภายนอก และช่องทางแจ้งเหตุฉุกเฉิน รวมทั้งแจ้งเตือนบุคลากรให้ระมัดระวัง Phishing, Social Engineering, AI-Generate Phishing และ Deep Fake ตลอดจนหลีกเลี่ยงการนำข้อมูลสำคัญขององค์กรและข้อมูลส่วนบุคคล เข้าสู่บริการ AI ภายนอกที่ไม่ได้รับอนุญาต

6) เตรียมพร้อมการแจ้งเหตุและประสานการตอบสนอง หากตรวจพบพฤติกรรมหรือสงสัยว่าระบบถูกโจมตี ควรดำเนินการตาม Incident Response Plan โดยเร็ว ประเมินขอบเขตและผลกระทบ จำกัดความเสียหาย เก็บรักษาพยานหลักฐานทางดิจิทัล และประสาน ThaiCERT สกมช., TCM-CERT รวมถึงหน่วยงานกำกับดูแลที่เกี่ยวข้อง โดยไม่จำเป็นต้องรอให้ตรวจสอบเหตุการณ์เสร็จสมบูรณ์ก่อนแจ้งเหตุ

สำนักงาน ก.ล.ต. และ TCM-CERT ตระหนักถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและความต่อเนื่องในการดำเนินธุรกิจของหน่วยงานในภาคตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวเพื่อให้บริษัทพิจารณาตรวจสอบระบบที่เกี่ยวข้อง และดำเนินการมาตรการป้องกันและลดความเสี่ยงตามความเหมาะสม เพื่อป้องกันหรือลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 7 พฤศจิกายน 2569
2. รายงานสรุปสถานการณ์และแนวโน้มภัยคุกคามทางไซเบอร์ ประจำปี 2569 (ระหว่างเดือนตุลาคม 2568 - กันยายน 2569) https://dg.th/i6hke2bnxd