แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ให้เฝ้าระวังความเสี่ยงทางไซเบอร์ในช่วงเทศกาลหรือช่วงวันหยุดยาว

วันที่แจ้งเตือน 9 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ผู้ไม่หวังดีอาจใช้โอกาสการโจมตีเป้าหมาย ในช่วงเทศกาลหรือช่วงวันหยุดยาว ซึ่งเป็นจังหวะที่องค์กรต่าง ๆ อาจมีการผ่อนมาตรการการเฝ้าระวังและติดตามภัยคุกคาม รวมถึงความพร้อมในการตอบสนองและรับมือเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์

สำนักงานจึงขอแจ้งเตือนผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลทุกแห่ง เพื่อให้ความสำคัญต่อการยกระดับมาตรการเฝ้าระวังเหตุการณ์หรือสัญญาณที่อาจจะเป็นภัยคุกคามทางไซเบอร์ในช่วงเทศกาลหรือช่วงวันหยุดยาว เพื่อลดความเสี่ยงและผลกระทบต่อหน่วยงานท่านโดยควรพิจารณาดำเนินการอย่างน้อย ดังนี้

1. ทบทวน อัปเดต และ ซักซ้อมแผน Incident Response Plan (IRP)	เพื่อให้ครอบคลุมลักษณะเหตุการณ์ทางไซเบอร์ที่อาจเกิดขึ้น และ ตรวจสอบความพร้อมของทีมงานและยืนยันรายชื่อผู้ติดต่อฉุกเฉิน (รวมถึงผู้ให้บริการภายนอก) ให้เป็นปัจจุบัน
2. ตรวจสอบระบบสำรองข้อมูล (Data Backup)	อาจพิจารณาหลัก 3-2-1 Backup Rule และตรวจสอบให้แน่ใจว่ามีข้อมูลสำรองแบบ Offline หรือ Immutable และ ตรวจสอบ/ทดสอบความพร้อมในการกู้คืนข้อมูลสำรอง
3. ปิดช่องโหว่ระบบสำคัญ (Patch Management)	อัปเดตแพตช์ความปลอดภัยตามที่กำหนด (เช่น ระดับ Critical และ High เป็นต้น) โดยเฉพาะสำหรับระบบงานสำคัญ หรือ ระบบที่เชื่อมต่ออินเทอร์เน็ต (Internet Facing)
4. ยกระดับการเฝ้าระวังตลอด 24 ชั่วโมง	กำชับทีมเฝ้าระวังเหตุการณ์ทางไซเบอร์ของบริษัท หรือ Security Operations Center (SOC) ให้เฝ้าระวังพฤติกรรมผิดปกติในการเข้าถึงระบบ (Anomaly Detection)
5. สื่อสารพนักงานภายในองค์กร (Security Awareness)	สร้างความตระหนักรู้และซักซ้อมความเข้าใจแก่พนักงานก่อนช่วงวันหยุดยาว โดยเน้นย้ำ: **ระวัง Phishing**: ตรวจสอบอีเมลที่แนบลิงก์แปลกปลอม หรืออ้างว่ามาจากแผนก IT **การดูแลอุปกรณ์:** Lock Screen เสมอ และไม่ทิ้งคอมพิวเตอร์ของบริษัทไว้ในที่สาธารณะ **ช่องทางแจ้งเหตุ:** แจ้งเบอร์ติดต่อฉุกเฉิน หากพนักงานพบสิ่งผิดปกติให้รีบรายงานทีม IT ทันที

ในการนี้ สำนักงาน ขอแจ้ง URL ของเว็บไซต์ https://web-incident.sec.or.th/ ในการรายงาน cyber incident ให้บริษัทท่านทราบอีกครั้ง ทั้งนี้ สำหรับผู้ประกอบธุรกิจรายใดที่ยังไม่เคยลงทะเบียน สามารถดูรายละเอียดการลงทะเบียน และ การเข้าใช้งานได้ที่ https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-INCIDENTREPORT.aspx

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจจะเกิดต่อผู้ประกอบธุรกิจรวมถึงผู้ใช้บริการในภาคตลาดทุน จึงขอแจ้งให้บริษัทท่านเฝ้าระวังและเตรียมความพร้อมเพื่อตอบสนองต่อเหตุการณ์ เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นต่อระบบงานภายใน และข้อมูลลูกค้าของบริษัทท่านได้

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ