แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ
- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ
- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

# แจ้งเตือนให้หน่วยงานยกระดับความมั่นคงปลอดภัยทางไซเบอร์

**วันที่แจ้งเตือน 8 มีนาคม 2567**

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่เอกสารแจ้งเตือนกรณี มีการเผยแพร่ข้อมูลบัญชีผู้ใช้งาน (username) และรหัสผ่าน (password) จากหน่วยงานในประเทศไทยจำนวนมากสู่สาธารณะ ซึ่งอาจส่งผลให้ผู้ไม่หวังดีใช้ข้อมูลดังกล่าวเพื่อโจมตีระบบของหน่วยงาน เช่น เว็บไซต์ สื่อโซเชียลมีเดีย แพลตฟอร์มอื่น ๆ ของหน่วยงาน เป็นต้น

โดยปัจจุบัน สกมช. พบว่ากลุ่มผู้ไม่หวังดีเริ่มมีการเคลื่อนไหว โจมตีเว็บไซต์และระบบของหน่วยงานในประเทศไทยแล้ว จึงขอให้หน่วยงานต่าง ๆ ยกระดับการเฝ้าระวังความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างใกล้ชิด

ทั้งนี้ สกมช. ได้ออกคำแนะนำสำหรับหน่วยงาน เพื่อดำเนินการตรวจสอบระบบสารสนเทศของหน่วยงานให้มีความมั่นคงปลอดภัย เพื่อป้องกันตนเองจากภัยคุกคามทางไซเบอร์ โดยสามารถดำเนินการได้ทันที ดังนี้

1. ตรวจสอบ และปิดช่องโหว่ บนระบบงานที่คาดว่าเป็นช่องทางให้ผู้ไม่หวังดีใช้โจมตีมายังหน่วยงานได้
2. ตรวจสอบระบบการเข้าถึงเครือข่ายจากระยะไกล เช่น Remote Desktop Protocol : RDP, Virtual Private Network : VPN ว่ามีการเข้าถึงที่ผิดปกติหรือไม่ และหมั่นตรวจสอบสิทธิการเข้าถึงระบบอย่างสม่ำเสมอ
3. ตรวจสอบระบบของพนักงานที่ Work from home ใช้งาน โดยเฉพาะระบบที่ System Admin ใช้งาน
4. อัพเดตคอมพิวเตอร์ ระบบปฏิบัติการ อุปกรณ์ต่าง ๆ รวมถึง Applications ให้ทันสมัยอยู่เสมอโดยเฉพาะช่องโหว่ที่มีการแจ้งเตือนล่าสุด หรือช่องโหว่ประเภท Zero-day ต่าง ๆ เช่น log4j, SolarWinds Supply Chain, Exchange Server และ Win32 Elevation Vulnerability เป็นต้น
5. ติดตั้งโปรแกรมป้องกันมัลแวร์ และอัพเดตให้ทันสมัยอยู่เสมอ
6. พิจารณาสำรองข้อมูลอย่างน้อย 3 ชุด โดยควรBackup แบบ Offline และให้สำเนาข้อมูลอยู่ในอุปกรณ์จัดเก็บข้อมูล หรือ Cloud ที่แยกออกจากระบบงาน และไม่สามารถเข้าถึงได้จากระบบงานปกติ
7. พิจารณาเพิ่มการใช้การยืนยันตัวตนแบบ Multi-factor Authentication (MFA) และตั้งรหัสผ่านให้ซับซ้อนคาดเดาได้ยาก
8. หมั่นอัปเดตเพิ่มข้อมูลตัวชี้วัดการโจมตี (Indicators of Compromise (IOCs)) ลงในอุปกรณ์รักษาความมั่นคงปลอดภัยของหน่วยงานเพื่อเฝ้าระวัง และป้องกันการโจมตี

**ข้อมูลอ้างอิง**

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 7 มี.ค. 2567