

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

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



CISA แจ้งเตือนให้เสริมมาตรการรักษาความปลอดภัยระบบ Microsoft Intune ภายหลังพบหน่วยงานสำคัญถูกโจมตี

วันที่แจ้งเตือน 22 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Cybersecurity and Infrastructure Security Agency (CISA) ได้ออกแจ้งเตือนให้องค์กรธุรกิจเร่งเสริมมาตรการรักษาความปลอดภัยระบบ Microsoft Intune และระบบบริหารจัดการอุปกรณ์ปลายทาง (Endpoint Management Systems) ภายหลังจากเหตุการณ์การโจมตีทางไซเบอร์ต่อบริษัทขนาดใหญ่ด้านเทคโนโลยีทางการแพทย์ของสหรัฐฯ ทำให้กระทบต่อสภาพแวดล้อมระบบ Microsoft ขององค์กรอย่างมีนัยสำคัญ

รายงานดังกล่าวระบุว่า ผู้ไม่หวังดีสามารถเข้าถึงบัญชีผู้ดูแลระบบของ Microsoft Intune และควบคุมอุปกรณ์ภายในองค์กร โดยมีการสั่งลบข้อมูลระยะไกล (Remote Wipe) ผ่านระบบ ส่งผลให้อุปกรณ์จำนวนมากได้รับผลกระทบและเกิดการหยุดชะงักของการดำเนินงานอย่างมีนัยสำคัญ นอกจากนี้ ยังพบว่ามี การเข้าถึงและนำข้อมูลสำคัญขององค์กรออกจากระบบ (Data Exfiltration) สะท้อนให้เห็นถึงความเสี่ยงจากการถูกโจมตีโดยระบบบริหารจัดการอุปกรณ์ปลายทางที่มีสิทธิ์ระดับสูง

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบพิจารณาดำเนินการเสริมความมั่นคงปลอดภัยของระบบ Microsoft Intune และระบบบริหารจัดการอุปกรณ์ปลายทาง โดยการบริหารจัดการบัญชีผู้ใช้และกำหนดสิทธิ์การเข้าถึงระบบ พร้อมทั้งบังคับใช้การยืนยันตัวตน MFA สำหรับบัญชีที่มีสิทธิ์ระดับสูง รวมทั้งเฝ้าระวังและวิเคราะห์บันทึกเหตุการณ์ (Log Monitoring) อย่างต่อเนื่อง เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ผิดปกติได้อย่างทัน่วงที

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

- <https://www.bleepingcomputer.com/news/security/cisa-warns-businesses-to-secure-microsoft-intune-systems-after-stryker-breach>
- <https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization?>
- <https://techcommunity.microsoft.com/blog/intunecustomersuccess/best-practices-for-securing-microsoft-intune/4502117?>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ