วันที่ 22 เมษายน 2568

ผู้ใช้จำนวนมากถูกล็อกบัญชี หลัง Microsoft Entra เปิดใช้งานฟีเจอร์ความปลอดภัยใหม่

Executive Summary

การเปิดใช้งานฟีเจอร์ความปลอดภัยใหม่ของ Microsoft Entra ID ที่ชื่อว่า MACE Credential Revocation ได้ก่อให้เกิดปัญหาการล็อกบัญชีผู้ใช้เป็นวงกว้างในหลายองค์กร โดยฟีเจอร์ใหม่นี้มีจุดประสงค์เพื่อช่วยตรวจจับและจัดการกับบัญชีที่อาจมีข้อมูลรั่วไหล แต่กลับตรวจพบแบบ False Positive ทำให้บัญชีของผู้ใช้จำนวนมากถูกล็อก แม้จะใช้รหัสผ่านที่ไม่ซ้ำกับบริการอื่น และมีการเปิดใช้งาน Multi-Factor Authentication (MFA) โดยเหตุการณ์เริ่มต้นขึ้นเมื่อผู้ดูแลระบบจำนวนมากได้รับการแจ้งเตือนจาก Microsoft Entra ว่าพบบัญชีผู้ใช้ที่มีข้อมูลรั่วไหลใน Dark Web หรือแหล่งข้อมูลภายนอกอื่นๆ หลังจากนั้นระบบจึงทำการล็อกบัญชีเหล่านั้นโดยอัตโนมัติ

ณ ตอนนี้ทาง Microsoft ยังไม่ได้ออกแถลงการณ์ต่อสาธารณะอย่างเป็นทางการ แต่จากการพูดคุยกับฝ่ายสนับสนุน ได้รับการยืนยันว่าปัญหานี้เกิดจากการเปิดใช้งานแอปพลิเคชัน MACE Credential Revocation ซึ่งมีผลทำให้เกิดการตรวจสอบและล็อกบัญชีจำนวนมากโดยอัตโนมัติ โดยมักจะแสดงเป็น Error Code 53003 ที่เกี่ยวข้องกับ Conditional Access Policy

เหตุการณ์นี้สะท้อนให้เห็นถึงความเสี่ยงของระบบป้องกันบัญชีอัตโนมัติที่ไม่ได้มีการควบคุมแบบละเอียด และชี้ให้เห็นถึงความจำเป็นในทดสอบก่อนใช้งานจริง

คำแนะนำ (Recommendation)

- หากได้รับผลกระทบให้พิจารณาปิดการใช้งาน MACE Credential Revocation Application ชั่วคราว
- วิธีการแก้ไขเกี่ยวกับการล็อกบัญชีให้ติดต่อ Microsoft Support และเปิดเคสเพื่อขอเปลี่ยน Ticket จาก compromised account เป็น false lockout เพื่อเร่งการกู้คืนบัญชี
- แจ้งฝ่าย Helpdesk หรือ IT Support ให้เตรียมรับมือกับเคสการล็อกอินไม่ได้จากผู้ใช้

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/microsoft/widespread-microsoft-entra-lockouts-tied-to-new-security-feature-rollout/