64015172 เอกรินทร์ องอาจ

รายละเอียดข่าว : เว็บไซต์ธนาคารและหน่วยงานรัฐบาลของยูเครน ถูกโจมตีทางไซเบอร์

เว็บไซต์หน่วยงานของรัฐบาลยูเครน และธนาคาร ถูกโจมตีด้วย DDoS โดยยังไม่มีการยืนยันว่า ถูกโจมตีโดยฝ่ายใด

มิไคโล เฟโดรอฟ รัฐมนตรีว่าการกระทรวงการเปลี่ยนผ่านสู่ดิจิทัลของยูเครน เปิดเผยผ่านช่องทางเทเลแกรมว่า เว็บไซต์ของหน่วยงานรัฐบาลยูเครน ประสบปัญหาล่มใช้การไม่ได้ จากการถูกโจมตีแบบ Distributed Denial of Service หรือ DDoS

การโจมตีดังกล่าวไม่ได้มีแค่เว็บไซต์ของหน่วยงานรัฐบาลเท่านั้น แต่ยังมีการโจมตีทางไซเบอร์ไปยังเว็บไซต์ของธนาคารอีกด้วย โดยระบบเครือข่ายธนาคารของยูเครนบางแห่งไม่สามารถออนไลน์ได้ในช่วงเวลาประมาณ 4 โมงเย็นตามเวลาท้องถิ่นยูเครน ทั้งนี้ ยังไม่มีการเปิดเผยมูลค่าความเสียหายจากการถูกโจมตีไปจนถึงผู้ได้รับผลกระทบในครั้งนี้

ก่อนหน้านี้ หน่วยงานไซเบอร์ของยูเครน เคยออกมาประกาศเตือนแล้วว่า มีโอกาสที่เว็บไซต์ของหน่วยงานรัฐบาล หน่วยงานความมั่นคง และธนาคาร จะถูกโจมตีทางไซเบอร์โดยแฮกเกอร์ แล้วก็เกิดเหตุการณ์ดังกล่าวขึ้นจริง โดยตลอดช่วงสัปดาห์ก่อนที่จะมีประกาศ หน่วยงานด้านความมั่นคงทางไซเบอร์ของสหรัฐอเมริกา ก็มีการเปิดเผยว่า ประเทศรัสเซียอยู่เบื้องหลังการโจมตีทางอินเทอร์เน็ตหลายครั้งในยูเครน

หลังจากนั้น ยูเครนได้ออกรายงานสนับสนุนแนวคิดของสหรัฐอเมริกา โดยบอกว่า รัสเซียน่าจะอยู่เบื้องหลังการโจมตีทางอินเทอร์เน็ตของยูเครนเพื่อทำลายเว็บพอร์ทัลของกระทรวงกลาโหม และหวังทำให้ระบบการเงินของยูเครนต้องหยุดชะงัก ซึ่งรัสเซีย ออกมาปฏิเสธว่า ไม่ได้เกี่ยวข้องใดๆ กับการโจมตีหน่วยงานต่างๆ ของยูเครน

จนถึงเวลานี้ ยังไม่มีการยืนยันว่า การโจมตีด้วย DDoS เป็นฝีมือของแฮกเกอร์กลุ่มใด แต่สถานการณ์ดังกล่าว เกิดขึ้นท่ามกลางความขัดแย้งระหว่างรัสเซียและยูเครน

ทางด้านโฆษกของทำเนียบขาวกล่าวกับสำนักข่าวเอ็นบีซีว่า สหรัฐอเมริกา กำลังติดตามสถานการณ์เรื่องนี้อย่างใกล้ชิด.

สรุปช่องโหว่ของระบบ -> เทียบกับ OWASP 2021 ข้อต่างๆ

จากรายละเอียดข่าวเกี่ยวกับการโจมตีทางไซเบอร์ต่อเว็บไซต์ธนาคารและหน่วยงานรัฐบาลของยูเครน ประเมินว่าอาจมีปัญหาตาม OWASP Top 10 2021 ดังนี้

1. การควบคุมการเข้าถึงที่ไม่ปลอดภัย (Broken Access Control)
    - การโจมตีแบบ DDoS มุ่งเป้าไปที่การรบกวนบริการของเว็บไซต์
      เป็นไปได้ว่าระบบควบคุมการเข้าถึงมีช่องโหว่ ทำให้ผู้โจมตีมุ่งเป้าไปที่ระบบได้ง่าย
2. การออกแบบที่ไม่ปลอดภัย (Insecure Design)
    - การโจมตีแบบ DDoS มักใช้ช่องโหว่ในสถาปัตยกรรมระบบ
      เป็นไปได้ว่าระบบถูกออกแบบมาโดยไม่มีการคำนึงถึงความปลอดภัยเพียงพอ
3. การกำหนดค่าที่ผิดพลาด (Security Misconfiguration)
    - การโจมตีแบบ DDoS อาจเกิดจากการตั้งค่าระบบที่ไม่ปลอดภัย เช่น
      การเปิดใช้งานบริการที่ไม่จำเป็น
4. ส่วนประกอบที่มีช่องโหว่และล้าสมัย (Vulnerable and Outdated Components)
    - เป็นไปได้ว่าระบบใช้ซอฟต์แวร์หรือไลบรารีที่มีช่องโหว่
      ซึ่งผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่นั้น
5. ความล้มเหลวในการบันทึกและตรวจสอบความปลอดภัย (Security Logging and Monitoring Failures)
    - ข่าวไม่ได้ระบุถึงกลไกการบันทึกและตรวจสอบความปลอดภัย
      เป็นไปได้ว่าระบบไม่มีกลไกเหล่านี้ หรือกลไกเหล่านั้นไม่มีประสิทธิภาพเพียงพอ
6. การปลอมแปลงคำขอฝั่งเซิร์ฟเวอร์ (Server-Side Request Forgery)
    - ข่าวไม่ได้ระบุถึงการโจมตีแบบ SSRF
      แต่เป็นไปได้ว่าผู้โจมตีอาจใช้ช่องโหว่นี้เพื่อเข้าถึงข้อมูลหรือระบบภายใน