วันที่ 25 มิถุนายน 2569

Microsoft เร่งแผนเปลี่ยนผ่านสู่การเข้ารหัสแบบ Post-Quantum Cryptography ภายในปี 2029

Microsoft ประกาศเมื่อวันอังคารว่า บริษัทกำลังเร่งแผนด้านความปลอดภัยเพื่อรองรับยุคคอมพิวเตอร์ควอนตัม โดยระบุว่าความก้าวหน้าของเทคโนโลยีควอนตัมกำลังเกิดขึ้นเร็วกว่าที่คาดไว้ ทำให้จำเป็นต้องเปลี่ยนจากมาตรฐานการเข้ารหัสที่ใช้อยู่ในปัจจุบันไปใช้มาตรฐานใหม่ให้เร็วขึ้น

Mark Russinovich ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (CTO) ของ Microsoft Azure กล่าวว่า ความก้าวหน้าในการวิจัยและพัฒนาเทคโนโลยีควอนตัมทำให้กรอบเวลาของความเสี่ยงเปลี่ยนไป เราเชื่อว่าคอมพิวเตอร์ควอนตัมที่มีศักยภาพเพียงพอในการถอดรหัสข้อมูลจริงอาจเกิดขึ้นเร็วกว่าที่เคยคาดการณ์ไว้ และการเตรียมความพร้อมต้องใช้เวลามาก ดังนั้นองค์กรต่างๆ ควรเริ่มดำเนินการตั้งแต่ตอนนี้ ด้วยเหตุนี้ Microsoft จึงตัดสินใจเร่งแผนงานของ Microsoft Quantum Safe Program (QSP) โดยตั้งเป้าให้ผลิตภัณฑ์และบริการที่มีความสำคัญทั้งหมดเปลี่ยนไปใช้ Post-Quantum Cryptography (PQC) ภายในปี 2029 นอกจากนี้ บริษัทยังมีแผนบรรจุข้อกำหนดด้าน PQC เข้าเป็นส่วนหนึ่งของโครงการ Secure Future Initiative (SFI) อีกด้วย

แนวทางสำคัญที่ Microsoft จะผลักดัน ได้แก่

- ปรับปรุงระบบเข้ารหัสของเครือข่ายด้วยการนำ TLS 1.3 มาใช้งาน
- พัฒนาความสามารถด้าน Crypto-Agility สำหรับข้อมูลที่จัดเก็บ เพื่อให้สามารถเปลี่ยนอัลกอริทึมการเข้ารหัสในอนาคตได้โดยไม่ต้องออกแบบระบบใหม่ทั้งหมด
- เปลี่ยนไปใช้อัลกอริทึมแบบ Post-Quantum Cryptography (PQC) เพื่อปกป้องห่วงโซ่ความเชื่อถือ (Trust Chain) เช่น การลงลายมือชื่อดิจิทัล (Code Signing) การออกใบรับรองดิจิทัล (Certificate Issuance) การปกป้องกุญแจเข้ารหัส (Key Protection) และกระบวนการอัปเดตซอฟต์แวร์ (Update Pipelines)

Russinovich กล่าวเพิ่มเติมว่า การดำเนินงานนี้จะทำให้การเตรียมพร้อมด้าน Quantum-Safe กลายเป็นส่วนหนึ่งของกระบวนการด้านวิศวกรรมความปลอดภัยที่มีมาตรฐานเดียวกับงานด้านความปลอดภัยอื่นๆ โดยมีผู้รับผิดชอบที่ชัดเจน กำหนดเป้าหมายที่สามารถวัดผลได้ และมีการรายงานความคืบหน้าอย่างโปร่งใส การผสานความสามารถเหล่านี้เข้าไปในแพลตฟอร์มของเรา จะช่วยให้ลูกค้าสามารถเริ่มเปลี่ยนผ่านได้เร็วขึ้นและมีความมั่นใจมากยิ่งขึ้น

Microsoft ยังระบุว่า Crypto-Agility ถือเป็นหัวใจสำคัญของการย้ายไปสู่ยุค Post-Quantum Cryptography โดยองค์กรควรหลีกเลี่ยงการฝังอัลกอริทึมการเข้ารหัสไว้แบบตายตัวในระบบ จัดเก็บข้อมูลที่จำเป็นสำหรับการสร้างบริบทของการเข้ารหัสย้อนหลัง และออกแบบระบบให้สามารถเปลี่ยนอัลกอริทึมใหม่ได้เหมือนการอัปเดตซอฟต์แวร์ทั่วไป แทนที่จะต้องรื้อระบบทั้งหมดเมื่อเกิดเหตุฉุกเฉิน

บริษัทอธิบายเพิ่มเติมว่า Crypto-Agility จำเป็นต้องมีข้อมูลเมตาที่สามารถอธิบายรายละเอียดของการเข้ารหัสได้ด้วยตัวเอง หรือใช้รูปแบบข้อมูลที่มีการกำหนดเวอร์ชันของข้อความที่ถูกเข้ารหัสไว้ เพื่อให้ระบบสามารถอ่านข้อมูลที่เข้ารหัสด้วยมาตรฐานเดิมได้ ขณะเดียวกันก็สามารถเขียนข้อมูลใหม่ด้วยอัลกอริทึมที่ได้รับการอนุมัติล่าสุด ระบบที่ออกแบบมาอย่างเหมาะสมควรรองรับการอ่านข้อมูลที่เข้ารหัสด้วยรูปแบบเก่าในช่วงระยะเวลาการเปลี่ยนผ่าน แต่เมื่อสร้างข้อมูลใหม่ ควรใช้มาตรฐานล่าสุดที่ได้รับการรับรอง

ความเคลื่อนไหวครั้งนี้เกิดขึ้นเพียงไม่กี่วันหลังจากที่ประธานาธิบดี Donald Trump ของสหรัฐอเมริกา ลงนามในคำสั่งฝ่ายบริหาร กำหนดกรอบเวลาที่ชัดเจนให้หน่วยงานรัฐบาลกลางเร่งเปลี่ยนระบบและทรัพย์สินด้านไอทีที่มีความสำคัญสูง ไปใช้เทคโนโลยี Post-Quantum Cryptography

ก่อนหน้านี้ในเดือนมีนาคม Google ได้ประกาศโครงการใหม่ในเว็บเบราว์เซอร์ Chrome เพื่อให้ใบรับรอง HTTPS มีความปลอดภัยต่อความเสี่ยงจากคอมพิวเตอร์ควอนตัมในอนาคต พร้อมทั้งประกาศว่าจะย้ายโครงสร้างพื้นฐานของบริษัททั้งหมดไปสู่มาตรฐาน Quantum-Safe ภายในปี 2029 ขณะที่ Cloudflare ผู้ให้บริการโครงสร้างพื้นฐานด้านเว็บ ก็ได้ประกาศแผนเปลี่ยนผ่านไปสู่ Post-Quantum Cryptography ภายในปีเดียวกันเช่นกัน

ภัยคุกคามที่หลายฝ่ายกังวลมากขึ้น คือเทคนิคที่เรียกว่า "Harvest Now, Decrypt Later" ซึ่งหมายถึงการที่ผู้โจมตีเก็บรวบรวมข้อมูลที่ถูกเข้ารหัสไว้ตั้งแต่วันนี้ แม้ยังไม่สามารถถอดรหัสได้ในปัจจุบัน แต่หวังว่าจะนำข้อมูลเหล่านั้นกลับมาถอดรหัสในอนาคต เมื่อคอมพิวเตอร์ควอนตัมที่มีประสิทธิภาพสูงพร้อมใช้งาน

นอกจากนี้ ทีมนักวิจัยจาก Google ยังเปิดเผยว่า พวกเขาสามารถพัฒนาอัลกอริทึมควอนตัมสำหรับโจมตีระบบเข้ารหัสแบบ Elliptic Curve Cryptography (ECC) โดยเฉพาะ 256-bit Elliptic Curve Discrete Logarithm Problem (ECDLP-256) ให้ใช้จำนวน Qubits และขั้นตอนการประมวลผล (Gates) น้อยกว่าที่เคยเชื่อกันมาก

ขณะเดียวกัน นักวิจัยจาก Caltech และ Oratomic ก็ได้เผยแพร่งานวิจัยเกี่ยวกับเทคนิคการแก้ไขข้อผิดพลาด (Error Correction) รูปแบบใหม่ ซึ่งอาจทำให้อัลกอริทึม Shor's Algorithm สามารถนำมาใช้งานได้จริงด้วยคอมพิวเตอร์ควอนตัมที่มี Reconfigurable Qubits เพียงประมาณ 10,000 Qubits และอาจมีศักยภาพในการถอดรหัสมาตรฐาน RSA-2048 และ P-256 ได้ในอนาคต

ข้อมูลอ้างอิง

Jul 1, 2026, By Ravie Lakshmanan

- https://thehackernews.com/2026/07/microsoft-accelerates-post-quantum.html