สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คำแนะนำเรื่องแนวทางการปฏิบัติ
การเตรียมความพร้อมสำหรับยุคควอนตัม
Guidelines for Post–Quantum Readiness

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

คำนำ

ในอดีตคอมพิวเตอร์ควอนตัม (Quantum Computer) เคยเป็นเพียงทฤษฎีและการทดลองในห้องปฏิบัติการ แต่ปัจจุบัน หลายประเทศได้มีการพัฒนาเทคโนโลยีนี้อย่างจริงจังมากขึ้น และมีความเป็นไปได้ที่จะมีการนำมาใช้งานเชิงพาณิชย์ในอีกไม่กี่ปีข้างหน้า สิ่งที่จะเกิดขึ้นและเป็นสิ่งที่น่ากังวลคือ คอมพิวเตอร์ควอนตัมมีความสามารถในการถอดรหัสลับข้อมูลที่สูงกว่าคอมพิวเตอร์ในยุคปัจจุบันอย่างมาก ทำให้อัลกอริทึมการเข้ารหัสลับข้อมูลที่ใช้อยู่ในปัจจุบันมีความเสี่ยงในการถูกถอดรหัสลับสูงและอาจไม่สามารถใช้ปกป้องข้อมูลในเครือข่ายระบบคอมพิวเตอร์ได้อีกต่อไป

แนวทางการปฏิบัติที่นำเสนอในเอกสารฉบับนี้ เป็นความพยายามในการนำเอาเทคโนโลยีการสื่อสารและการเข้ารหัสลับที่มีความสามารถต้านทานการโจมตีโดยใช้การประมวลผลของคอมพิวเตอร์ควอนตัมเพื่อใช้ทดแทนหรือทำงานร่วมกันกับอัลกอริทึมการเข้ารหัสลับที่ใช้อยู่ในปัจจุบัน การมาถึงของคอมพิวเตอร์ควอนตัมมีแนวโน้มพร้อมใช้งานได้อย่างรวดเร็วจนคาดไม่ถึง แต่การเตรียมความพร้อมในการเปลี่ยนผ่านเทคโนโลยีการเข้ารหัสลับแบบเดิมไปสู่เทคโนโลยีการเข้ารหัสลับแบบใหม่ เป็นเรื่องที่ต้องใช้เวลา ซึ่งอาจไม่ทันต่อการเผชิญหน้ากับคอมพิวเตอร์ควอนตัมที่จะมาถึง โดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ร่วมกับ บริษัท ควอนตัม เทคโนโลยี ฟาวเดชั่น (ประเทศไทย) จำกัด ได้จัดทำ (ร่าง) คำแนะนำแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม (Guidelines for Post–Quantum Readiness) เพื่อเสนอเป็นข้อมูลให้ผู้ที่มีส่วนเกี่ยวข้องทุกภาคส่วนได้ร่วมพิจารณา และเตรียมความพร้อมในการรับมือกับความท้าทายที่จะเกิดขึ้นในอนาคตอันใกล้นี้ หวังเป็นอย่างยิ่งว่า ข้อมูลที่ได้นำเสนอนี้จะเป็นประโยชน์ต่อท่านและหน่วยงาน ไม่มากก็น้อย

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ธันวาคม ๒๕๖๖

กิตติกรรมประกาศ

“คำแนะนำเรื่องแนวทางการปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม (Guidelines for Post-Quantum Readiness)” ได้รับความอนุเคราะห์ข้อมูลและข้อเสนอแนะที่เป็นประโยชน์จากคณะผู้จัดทำ บริษัท ควอนตัม เทคโนโลยี ฟาวเดชั่น (ประเทศไทย) จำกัด ดังต่อไปนี้

ดร.จิรวัฒน์ ตั้งปณิธานนท์	ประธานกรรมการบริหาร
ดร.ภูมิพงศ์ ไชยวงศ์คต	ผู้ร่วมก่อตั้ง
ดร.ณัฐวุฒิ กองสุวรรณ	นักวิจัย
นางสาว สุณาทิพย์ เบญมาตย์	นักวิเคราะห์ธุรกิจ

ซึ่งได้ใช้ความรู้ ความสามารถ และประสบการณ์ของท่านในการจัดทำคำแนะนำฉบับนี้ อันจะเป็นประโยชน์กับผู้สนใจและหน่วยงานที่ปฏิบัติงานเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงขอขอบคุณทางทีมงาน หน่วยงานและบุคคลต่าง ๆ ที่มาร่วมประชุมพร้อมทั้งซักถามและให้คำแนะนำที่เป็นประโยชน์ต่อการจัดทำเอกสารฉบับนี้จนเสร็จสมบูรณ์มา ณ โอกาสนี้

ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สารบัญ

๑. เหตุผล **๑**

๒. ขอบเขต **๒**

๓. นิยาม **๒**

๔. ภัยคุกคามจากคอมพิวเตอร์ควอนตัม **๓**

๔.๑ ประเภทระบบรหัสลับที่โดนผลกระทบ ๔

๔.๒ การเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง (Harvest Now, Decrypt Later) ๕

๕. วิธีการรักษาความมั่นคงปลอดภัยในยุคควอนตัม **๗**

๕.๑ ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum cryptography) ๗

๕.๒ การกระจายกุญแจเชิงควอนตัม (Quantum key distribution) ๑๑

๕.๓ ระบบแบบผสม (Hybrid Solutions) ๑๒

๖. ระยะเวลาที่เกี่ยวข้องต่อการเตรียมความพร้อมและประเมินความเสี่ยง **๑๓**

๖.๑ ระยะเวลาในการเตรียมความพร้อม (Migration Time) ๑๓

๖.๒ ระยะเวลาที่ต้องเก็บรักษาข้อมูล (Security Shelf Life) ๑๔

๖.๓ ระยะเวลาก่อนเกิดภัยคุกคาม (Threat Timeline) ๑๕

๖.๔ โมเดล Mosca ๑๕

๗. การประเมินและติดตามระยะเวลาก่อนเกิดภัยคุกคาม **๑๖**

๗.๑ การคาดการณ์ระยะเวลาก่อนเกิดภัยคุกคามโดยผู้เชี่ยวชาญ ๑๗

๗.๒ ปัจจัยเร่งระยะเวลาก่อนเกิดภัยคุกคาม ๑๘

๗.๓ แนวทางการติดตามระยะเวลาก่อนเกิดภัยคุกคาม ๑๘

๘. แนวปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม **๑๘**

๘.๑ ขั้นตอนการเตรียมความพร้อม ๑๙

๘.๒ แนวทางการสื่อสารเพื่อสร้างความตระหนักรู้ภายในองค์กร ๒๐

๘.๓ แนวทางการจัดทำรายการสินทรัพย์ทางสารสนเทศ ๒๑

๙. ข้อมูลเพิ่มเติม **๒๓**

๑. เหตุผล

เศรษฐกิจและสังคมของประเทศไทยมีการพึ่งพาเทคโนโลยีสารสนเทศและการสื่อสารเพิ่มมากขึ้นอย่างต่อเนื่อง ทั้งในอุตสาหกรรมการเงิน การธนาคาร การคมนาคม การแพทย์ รวมถึงด้านการทหารและความมั่นคงของชาติ เป็นต้น ดังนั้น การยกระดับความปลอดภัยในการสื่อสาร การสร้างและเตรียมบุคลากรพร้อมทั้งโครงสร้างพื้นฐานเพื่อการสื่อสารที่ปลอดภัย รวมถึงการแก้ไขเพิ่มเติมกฎและระเบียบให้รองรับ ครอบคลุม และทันต่อการเปลี่ยนแปลงจึงเป็นสิ่งสำคัญอย่างยิ่ง

ในปัจจุบัน ระบบรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศมีองค์ประกอบหลัก คือ ระบบบรหัสลับแบบกุญแจสาธารณะ (Public Key Cryptography) ซึ่งถูกใช้งานอย่างแพร่หลาย โดยถูกใช้เป็นองค์ประกอบพื้นฐานในกระบวนการแลกเปลี่ยนข้อมูลให้มีความปลอดภัย เช่น การแลกเปลี่ยนกุญแจระบบรหัสลับ (Key Exchange) การลงลายมือชื่อดิจิทัล (Digital Signatures) และการยืนยันตัวตน (Authentication) ทั้งนี้ หากระบบรหัสลับแบบกุญแจสาธารณะถูกโจมตี ผู้ไม่ประสงค์ดีอาจปลอมแปลงเอกสารอิเล็กทรอนิกส์โดยใช้ลายมือชื่อดิจิทัลปลอมเพื่อการทำธุรกรรมโดยไม่ได้รับอนุญาตหรือแอบอ้างเป็นบุคคลอื่นได้ เป็นต้น

คอมพิวเตอร์ควอนตัมขนาดใหญ่ (Large-Scale Quantum Computers) หากถูกพัฒนาขึ้น จะมีความสามารถในการโจมตีระบบบรหัสลับแบบกุญแจสาธารณะ ซึ่งจากการประมาณการในรายงานโดย Gouzien ระบบบรหัสลับ RSA-2048 อาจสามารถถูกแยกตัวประกอบเพื่อถอดรหัสลับได้ภายใน 177 วันด้วยคอมพิวเตอร์ควอนตัมขนาด 13,436 คิวบิตและหน่วยความจำแบบ multimode[๑] ส่งผลให้ความมั่นคงปลอดภัยของระบบการสื่อสารในปัจจุบันลดลงไปอย่างมาก และมีความเสี่ยงที่จะส่งผลกระทบในวงกว้างทั้งทางด้านเศรษฐกิจ สังคม และความมั่นคงของราชอาณาจักรไทย

การพัฒนาคอมพิวเตอร์ควอนตัมขนาดใหญ่อาจใช้ระยะเวลาหลายปี แต่หลายหน่วยงานได้เริ่มศึกษาวิจัยและทุ่มเทการพัฒนาคอมพิวเตอร์ควอนตัมอย่างจริงจังและมีเครื่องต้นแบบที่สามารถใช้ได้ในงานที่ไม่ซับซ้อน ตัวอย่างเช่น บริษัท IBM ได้เปิดตัวชิปควอนตัม Osprey ขนาด 433 คิวบิตในเดือนพฤศจิกายน พ.ศ. 2565 และเปิดตัวชิปควอนตัม Condor ขนาด 1,121 คิวบิตและ Quantum System Two ในเดือนธันวาคม พ.ศ. 2566[๒] นอกจากนี้ในเดือนเดียวกัน กลุ่มนักวิจัยจากมหาวิทยาลัยฮาร์วาร์ดและหน่วยงานพันธมิตรได้ตีพิมพ์บทความวิชาการเกี่ยวกับความสำเร็จในการพัฒนาและทดลองคอมพิวเตอร์ควอนตัมขนาด 48 คิวบิตเชิงตรรกะ[๓] สำนักงานกลางเพื่อความมั่นคงปลอดภัยสารสนเทศเยอรมนี (The Federal Office for Information Security of

---

[๑] Gouzien É, Sangouard N. Factoring 2048-bit RSA integers in 177 days with 13 436 qubits and a multimode memory [J]. Physical review letters, 2021, 127(14): 140503.

[๒] https://www.nature.com/articles/d41586-023-03854-1

[๓] Bluvstein, D., Evered, S.J., Geim, A.A. et al. Logical quantum processor based on reconfigurable atom arrays. Nature (2023). https://doi.org/10.1038/s41586-023-06927-3

Germany : BSI) คาดการณ์ว่าในช่วงประมาณ พ.ศ. 2578 คอมพิวเตอร์ควอนตัมจะมีศักยภาพเพียงพอที่จะเป็นภัยคุกคามต่อระบบรหัสลับแบบกุญแจสาธารณะที่ใช้กันอยู่ในปัจจุบัน[๔]

ทั้งนี้การเปลี่ยนแปลงระบบสารสนเทศขององค์กรให้มีความพร้อมต่อภัยคุกคามจากคอมพิวเตอร์ควอนตัมอาจใช้ระยะเวลาที่ยาวนานเทียบเท่าหรือนานกว่าการพัฒนาคอมพิวเตอร์ควอนตัมขนาดใหญ่ ข้อมูลที่เป็นความลับขององค์กรซึ่งมีความจำเป็นต้องจัดเก็บไปเป็นระยะเวลานานอาจมีความเสี่ยงจากการถูกโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง (Harvest Now, Decrypt Later) ตั้งแต่วันนี้ ซึ่งผู้ไม่ประสงค์ดีเก็บรวบรวมข้อมูลสำคัญที่ถูกเข้ารหัสลับเอาไว้ช่วงเวลานี้ เพื่อนำไปถอดรหัสลับด้วยคอมพิวเตอร์ควอนตัมในอนาคต

ดังนั้นภาครัฐและเอกชน ควรเริ่มต้นศึกษา วางแผน และเตรียมความพร้อมต่อการรับมือภัยคุกคามจากคอมพิวเตอร์ควอนตัม โดยควรดำเนินการแบบองค์รวม ทั้งในระดับการวางนโยบายและกำหนดกลยุทธ์โดยผู้บริหารระดับสูง การบริหารจัดการโดยระดับผู้จัดการ จนไปถึงกระบวนการดำเนินงานโดยเจ้าหน้าที่ระดับปฏิบัติการขององค์กร

๒. ขอบเขต

คำแนะนำฉบับนี้ให้ใช้กับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีการประมวลผลข้อมูล (เช่น เก็บรวบรวม ใช้ แลกเปลี่ยน และเปิดเผยข้อมูล) ที่เป็นความลับผ่านระบบสารสนเทศ

๓. นิยาม

“กลศาสตร์ควอนตัม (Quantum Mechanics)” หมายความว่า ทฤษฎีทางฟิสิกส์ที่ใช้ในการอธิบายพฤติกรรมและคุณสมบัติของระบบที่มีขนาดเล็กในระดับอะตอม

“คอมพิวเตอร์ควอนตัม (Quantum Computer)” หมายความว่า คอมพิวเตอร์ที่ใช้ปรากฏการณ์ทางฟิสิกส์ของระบบที่มีขนาดเล็กในระดับอะตอมซึ่งสามารถอธิบายได้ด้วยทฤษฎีกลศาสตร์ควอนตัมในการคำนวณและประมวลผลทางคอมพิวเตอร์ โดยมีคุณสมบัติในการแก้ปัญหาทางคณิตศาสตร์บางประเภทที่คอมพิวเตอร์ธรรมดาไม่สามารถแก้ได้อย่างมีประสิทธิภาพ

“ระบบรหัสลับ (Cryptography)” หมายความว่า ศาสตร์ที่ศึกษาเกี่ยวกับการสร้างความมั่นคงปลอดภัยในการสื่อสาร (Secure communication) เพื่อปกป้องข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต

“การเข้ารหัสลับ (Encryption)” หมายความว่า การแปลงข้อความหรือข้อมูลที่สามารถอ่านได้ (Plaintext) ให้อยู่ในรูปแบบที่ถูกเข้ารหัสลับและไม่สามารถอ่านได้ (Ciphertext)

“การถอดรหัสลับ (Decryption)” หมายความว่า การแปลงข้อความหรือข้อมูลจากรูปแบบที่ถูกเข้ารหัสลับและไม่สามารถอ่านได้ (Ciphertext) ให้กลับไปอยู่ในรูปแบบเดิมที่สามารถอ่านได้ (Plaintext)

---

[๔] Quantum-safe cryptography - fundamentals, current developments and recommendations. Federal Office for Information Security, Germany, May 2022.

“ระบบบรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography)” หมายความว่า ระบบบรหัสลับที่ใช้กุญแจรหัสลับ (Secret Key) ดอกเดียวกันในการเข้ารหัสลับและถอดรหัสลับ

“ระบบบรหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Cryptography)” หรือ **“ระบบบรหัสลับกุญแจสาธารณะ (Public Key Cryptography)”** หมายความว่า ระบบบรหัสลับที่คู่กุญแจ (Key pair) ประกอบด้วย กุญแจสาธารณะ (Public Key) ใช้เข้ารหัสลับเพื่อรักษาความลับ หรือตรวจสอบความครบถ้วนแท้จริงของข้อมูล และ กุญแจส่วนตัว (Private Key) ใช้สำหรับถอดรหัสลับหรือลงลายมือชื่อดิจิทัลเพื่อรับรองความแท้จริงของข้อมูล โดยกุญแจส่วนตัวต้องจัดเก็บไว้เป็นความลับ ในขณะที่กุญแจสาธารณะสามารถส่งต่อและเปิดเผยให้กับผู้อื่นได้

“การลงลายมือชื่อดิจิทัล (Digital Signature)” หมายความว่า ลายมือชื่ออิเล็กทรอนิกส์ที่ได้จากกระบวนการเข้ารหัสลับด้วยระบบรหัสลับแบบกุญแจอสมมาตร โดยใช้กุญแจส่วนตัว (Private Key) ในการลงลายมือชื่อ และ ใช้กุญแจสาธารณะ (Public Key) ที่เป็นคู่กุญแจกัน ในการตรวจสอบลายมือชื่อ ทำให้สามารถยืนยันตัวเจ้าของลายมือชื่อ (Authenticity) และตรวจพบการเปลี่ยนแปลงของข้อความและลายมือชื่ออิเล็กทรอนิกส์ได้ (Data Integrity) รวมถึงการทำให้เจ้าของลายมือชื่อไม่สามารถปฏิเสธความรับผิดจากข้อความที่ตนเองลงลายมือชื่อได้ (Non-Repudiation)

“ฟังก์ชันแฮช (Hash Function)” หมายความว่า กระบวนการทางด้านคณิตศาสตร์ที่ใช้แปลงข้อมูลให้กลายเป็นข้อมูลย่อย (Digest) โดยข้อมูลย่อยจะมีขนาดคงที่ (Fixed Size) ไม่ว่าข้อมูลตั้งต้นจะมีขนาดเท่าใดก็ตาม

“ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum Cryptography: PQC)” หมายความว่า ระบบรหัสลับที่ใช้อัลกอริทึมที่ทนทานต่อการโจมตีจากคอมพิวเตอร์ควอนตัม (Quantum-Resistant Algorithm)

“การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD)” หมายความว่า กระบวนการทางควอนตัมสำหรับการสร้างและกระจายกุญแจรหัสลับ (Key Distribution) อย่างปลอดภัย

๔. ภัยคุกคามจากคอมพิวเตอร์ควอนตัม

คอมพิวเตอร์ควอนตัมอาศัยคุณสมบัติเชิงควอนตัมในการคำนวณและประมวลผลทางคอมพิวเตอร์ ทำให้มีคุณสมบัติในการแก้ปัญหาทางคณิตศาสตร์บางประเภท ที่คอมพิวเตอร์ในปัจจุบันยังไม่สามารถแก้ปัญหาได้อย่างมีประสิทธิภาพและต้องใช้เวลานานในการแก้ปัญหาดังกล่าว เช่น ปัญหาการแยกตัวประกอบของจำนวนเต็ม (Integer Factorization) การจำลองทางคณิตศาสตร์ (Simulation) และการคำนวณหาค่าเหมาะสมที่สุด (Optimization)

ความสามารถในประมวลผลของคอมพิวเตอร์ควอนตัมอาจถูกนำไปใช้เพื่อก่อให้เกิดประโยชน์ต่อเศรษฐกิจและสังคม เช่น การพัฒนาวัสดุหรือตัวยาชนิดใหม่ การวินิจฉัยโรค และ การเพิ่มประสิทธิภาพในห่วงโซ่อุปทาน

(Supply Chain Optimization) ทว่า ผู้ไม่ประสงค์ดีก็อาจนำคอมพิวเตอร์ควอนตัมไปใช้ในทางที่ผิด เช่น การโจมตีระบบของความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบันได้

ระบบรักษาความปลอดภัยในปัจจุบัน เช่น Transport Layer Security (TLS) มีองค์ประกอบพื้นฐานสำคัญ คือ อัลกอริทึมรหัสลับทั้งประเภทกุญแจอสมมาตร และ กุญแจสมมาตร ในการรักษาความปลอดภัยในการสื่อสารผ่านทางอินเทอร์เน็ต ซึ่งเป็นอัลกอริทึมที่คอมพิวเตอร์ทั่วไปในปัจจุบันถ้าไม่มีกุญแจที่ใช้ในการเข้ารหัสลับจะไม่สามารถถอดรหัสลับได้ในระยะเวลาอันสั้น ซึ่งซูเปอร์คอมพิวเตอร์ (Supercomputer) อาจต้องใช้เวลามากกว่าพันปีในการถอดรหัสลับอัลกอริทึมรหัสลับดังกล่าว ทว่า คอมพิวเตอร์ควอนตัมอาจจะใช้เวลาเพียงไม่กี่ชั่วโมงในการถอดรหัสลับอัลกอริทึมเดียวกันนี้

๔.๑ <u>ประเภทระบบรหัสลับที่โดนผลกระทบ</u>

๔.๑.๑ ระบบรหัสลับแบบกุญแจอสมมาตร (Asymmetric Key Cryptography)

คอมพิวเตอร์ควอนตัมขนาดใหญ่สามารถใช้ในการประมวลผลอัลกอริทึมประเภท Shor (Shor’s Algorithm) เพื่อการแก้ปัญหาทางคณิตศาสตร์ประเภทการแยกตัวประกอบเฉพาะ (Prime Factorization Problem) และ ลอการิทึมไม่ต่อเนื่อง (Discrete Logarithm Problem) ซึ่งสามารถนำไปใช้โจมตีระบบรหัสลับแบบกุญแจอสมมาตร เช่น อัลกอริทึมประเภท Rivest–Shamir–Adleman (RSA) Diffie–Hellman และ Elliptic-Curve Cryptography (ECC) ได้รวดเร็วมากกว่าคอมพิวเตอร์ทั่วไปแบบเอกซ์โพเนนเชียล (Exponential Speed-Up) ส่งผลให้โพรโทคอล หรืออัลกอริทึมสำหรับการสื่อสารและแลกเปลี่ยนข้อมูลซึ่งอาศัยระบบรหัสลับแบบกุญแจอสมมาตรเป็นองค์ประกอบ เช่น การลงลายมือชื่อดิจิทัล (Digital Signatures) และการแลกเปลี่ยนกุญแจ (Key Exchange) อาจไม่มีความปลอดภัยเพียงพออีกต่อไป

โพรโทคอลและอัลกอริทึมเหล่านี้มีความเสี่ยงจากการถูกโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง โดยผู้ไม่ประสงค์ดี (Threat Actor) อาจดำเนินการดักฟังระบบเครือข่ายการสื่อสารและจัดเก็บข้อมูลที่เป็นความลับ จากนั้นนำไปถอดรหัสลับในอนาคต ภายหลังจากที่คอมพิวเตอร์ควอนตัมขนาดใหญ่ได้ถูกพัฒนาขึ้นแล้ว นอกจากนี้ การลงลายมือชื่อดิจิทัลบนเอกสารอิเล็กทรอนิกส์ก็มีความเสี่ยงโดยผู้ไม่ประสงค์ดีอาจใช้คอมพิวเตอร์ควอนตัมเพื่อคำนวณหากุญแจส่วนตัว เพื่อใช้ในการลงลายมือชื่อบนเอกสารสำคัญและแอบอ้างเป็นบุคคลอื่น

๔.๑.๒ ระบบรหัสลับแบบกุญแจสมมาตร (Symmetric Key Cryptography)

ความปลอดภัยของระบบรหัสลับแบบกุญแจสมมาตรนั้น มีฐานปัญหาทางคณิตศาสตร์ที่แตกต่างจากระบบรหัสลับแบบกุญแจอสมมาตร ทำให้ไม่สามารถใช้อัลกอริทึมประเภท Shor ในการโจมตีด้วยความเร็วที่เพิ่มมากขึ้นแบบเอกซ์โพเนนเชียลได้ โดยอัลกอริทึมสำหรับการโจมตีระบบรหัสลับแบบกุญแจสมมาตรคืออัลกอริทึมประเภท Grover (Grover's Algorithm) ซึ่งมีความรวดเร็วมากกว่าอัลกอริทึมแบบดั้งเดิมแบบยกกำลังสอง (Quadratic Speed-Up) เท่านั้น ดังนั้น อัลกอริทึมสำหรับการสื่อสารและแลกเปลี่ยนข้อมูล

ซึ่งอาศัยระบบบรหัสลับแบบกุญแจสมมาตร เช่น Advanced Encryption Standard (AES) จึงได้รับผลกระทบจากการถูกโจมตีด้วยคอมพิวเตอร์ควอนตัมน้อยกว่าอัลกอริทึมที่ใช้ระบบบรหัสลับแบบกุญแจอสมมาตร

หากคอมพิวเตอร์ควอนตัมขนาดใหญ่ถูกพัฒนาขึ้น องค์กรอาจดำเนินการเพิ่มความยาวของกุญแจรหัสลับให้มากขึ้นเป็น ๒ เท่า เพื่อให้ระบบสารสนเทศมีระดับความปลอดภัยจากคอมพิวเตอร์ควอนตัมเทียบเท่ากับระบบเดิม ทั้งนี้ การเพิ่มความยาวของกุญแจนั้นอาจไม่สามารถดำเนินการได้โดยง่าย เนื่องจากข้อจำกัดในทั้งทางด้านซอฟต์แวร์และฮาร์ดแวร์ของแอปพลิเคชันที่มีการใช้งานขององค์กร โดยเฉพาะในระบบที่มีการใช้งานเป็นเวลายาวนานและในอุปกรณ์ขนาดเล็ก เช่น อุปกรณ์ IoTs (Internet of Things) อาจมีปริมาณหน่วยความจำไม่เพียงพอ ทำให้องค์กรอาจมีความจำเป็นต้องพิจารณาใช้ทางเลือกอื่น

ตารางที่ ๑ แสดงผลกระทบจากคอมพิวเตอร์ควอนตัมต่อระบบบรหัสลับแบบกุญแจอสมมาตรและสมมาตร

โพรโทคอลระบบการเข้ารหัส (Crypto Protocol)	กรณีการใช้งาน (Use Case)	ผลกระทบจากควอนตัม (Quantum Impact)	ระดับความเร่งด่วน (Urgency)
ระบบบรหัสลับแบบกุญแจอสมมาตร (เช่น RSA, DH, ECC)	การแลกเปลี่ยนกุญแจ	มีความเสี่ยงและผลกระทบสูงจากการโจมตีด้วย Shor's Algorithm	สูงสุด: มีความเสี่ยงจากการโจมตีแบบเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง
	การลงลายมือชื่อและการยืนยันตัวตน		สูง: มีความเสี่ยงเมื่อคอมพิวเตอร์ควอนตัมขนาดใหญ่พัฒนาขึ้น
ระบบบรหัสลับแบบกุญแจสมมาตร (เช่น AES)	การเข้ารหัสลับ	ปลอดภัยน้อยลงจากการโจมตีด้วย Groover's Algorithm	ปานกลาง: สามารถใช้วิธีเพิ่มความยาวกุญแจเพื่อรักษาระดับความปลอดภัยให้คงเดิม

ตารางที่ ๑ สรุปผลกระทบจากคอมพิวเตอร์ควอนตัมต่อระบบบรหัสลับแบบกุญแจอสมมาตรและสมมาตร[๕]

๔.๒ <u>การเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง (Harvest Now, Decrypt Later)</u>

ผู้ไม่ประสงค์ดี รวมถึง อาชญากรหรือผู้ก่อการร้ายข้ามชาติ อาจจะดำเนินการเก็บรวบรวมข้อมูลสำคัญขององค์กรหรือหน่วยงานของรัฐที่ถูกเข้ารหัสลับไว้ตั้งแต่ตอนนี้ และจัดเก็บไว้เพื่อรอวันที่คอมพิวเตอร์ควอนตัมถูกพัฒนาถึงจุดที่สามารถถอดรหัสลับข้อมูลเหล่านี้ได้ในอนาคต ดังนั้น ข้อมูลความลับที่มีความจำเป็นต้องจัดเก็บรักษาไว้เป็นระยะเวลานานมากกว่า ๑๐ ปี เช่น ข้อมูลทางการทหาร ความลับทางธุรกิจ และ ข้อมูลทางด้านสุขภาพ เป็นต้น อาจมีความเสี่ยง ณ วันนี้ ต่อการถูกโจมตีแบบ Harvest Now, Decrypt Later ตัวอย่างที่สำคัญและเกิดขึ้นจริงในประวัติศาสตร์คือ โครงการเวโนนา (Venona Project) ในช่วงสงครามเย็น ซึ่งรัฐบาล

[๕] "A Guide to a Quantum-Safe Organization: Transitioning from today's cybersecurity to a quantum-resilient environment", The Quantum Economic Development Consortium (QED-C), July 2022.

ประเทศสหรัฐอเมริกาดำเนินการเก็บเกี่ยวและจัดเก็บข้อมูลสื่อสารที่ถูกเข้ารหัสลับของสหภาพโซเวียตเพื่อการถอดรหัสลับในภายหลัง ระหว่างปี พ.ศ. ๒๔๘๖ ถึง พ.ศ. ๒๕๒๓ ทำให้สามารถดำเนินการจับกุมสายลับที่ปฏิบัติการจารกรรมในประเทศสหรัฐอเมริการได้

การโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง สามารถแสดงตัวอย่างได้ในรูปที่ ๑ โดยในการสื่อสารระหว่างสองบุคคลดังแสดงในขั้นตอนที่ (๑) ถึง (๒) มีผู้ไม่ประสงค์ดีดำเนินการโจมตีดังแสดงในขั้นตอนที่ (ก) ถึง (ง) ดังนี้

(๑) ทั้งสองบุคคลเริ่มต้นการสื่อสารโดยจัดตั้ง Session การสื่อสารที่ปลอดภัย (Secure Communication Session) โดยใช้อัลกอริทึมการแลกเปลี่ยนกุญแจ ซึ่งเป็นอัลกอริทึมระบบรหัสลับแบบกุญแจอสมมาตร ทำให้ทั้งสองบุคคลมีกุญแจเข้ารหัสลับแบบสมมาตรชุดเดียวกัน เช่น การใช้โพรโทคอล TLS เพื่อการแลกเปลี่ยนกุญแจและสร้างช่องทางการสื่อสารที่ปลอดภัยระหว่าง Client กับ Server

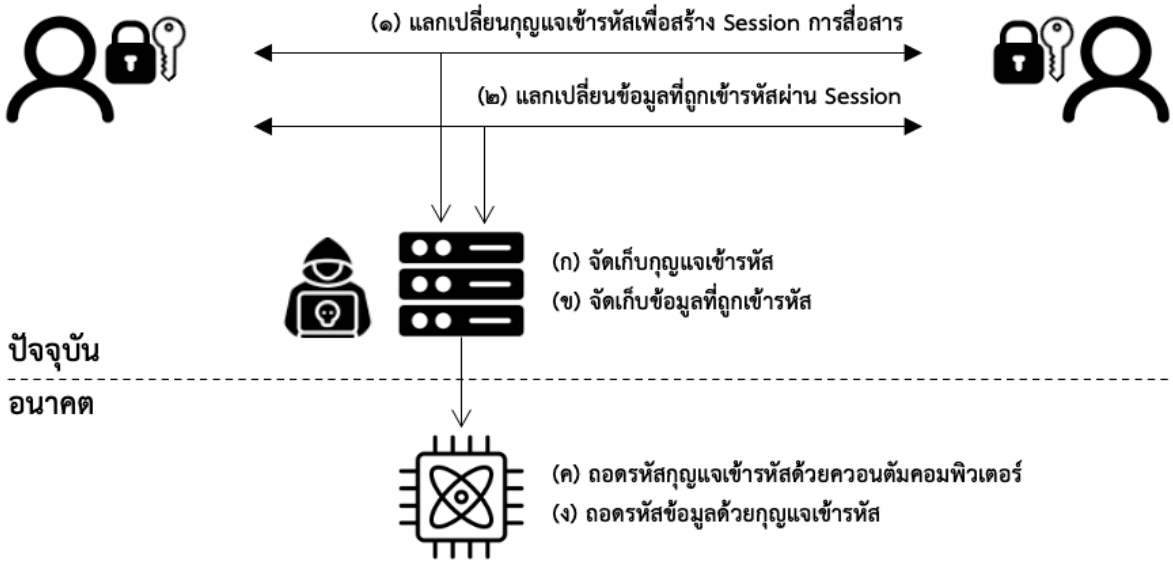
(๒) ทั้งสองบุคคลแลกเปลี่ยนข้อมูลสำหรับการสื่อสาร โดยใช้กุญแจเข้ารหัสลับแบบสมมาตรในขั้นตอนที่ (๑) เพื่อการเข้ารหัสลับข้อมูลการสื่อสารดังกล่าว

(ก) ผู้ไม่ประสงค์ดีดำเนินการจัดเก็บข้อมูลที่ใช้ในระหว่างกระบวนการแลกเปลี่ยนกุญแจเข้ารหัสลับในขั้นตอนที่ (๑) โดยผู้ไม่ประสงค์ดียังไม่สามารถโจมตีอัลกอริทึมแลกเปลี่ยนกุญแจได้ด้วยคอมพิวเตอร์ในยุคปัจจุบัน

(ข) ผู้ไม่ประสงค์ดีดำเนินการจัดเก็บข้อมูลที่ใช้ในการสื่อสารในขั้นตอนที่ (๒) โดยผู้ไม่ประสงค์ดียังไม่สามารถโจมตีอัลกอริทึมการเข้ารหัสลับอัลกอริทึมเข้ารหัสลับข้อมูลได้ด้วยคอมพิวเตอร์ในยุคปัจจุบัน

(ค) ผู้ไม่ประสงค์ดีรอให้คอมพิวเตอร์ควอนตัมขนาดใหญ่ถูกพัฒนาขึ้นในอนาคต เพื่อใช้ในการโจมตีอัลกอริทึมแลกเปลี่ยนกุญแจและคำนวณหากุญแจเข้ารหัสลับในขั้นตอนที่ (๑) โดยใช้ข้อมูลที่ถูกจัดเก็บไว้ในอดีตในขั้นตอน (ก)

(ง) ผู้ไม่ประสงค์ดีใช้กุญแจเข้ารหัสลับที่คำนวณได้จากคอมพิวเตอร์ควอนตัมในขั้นตอน (ค) เพื่อถอดรหัสลับข้อมูลที่ใช้สื่อสารในขั้นตอนที่ (๒)



รูปที่ ๑ การโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง ด้วยคอมพิวเตอร์ควอนตัม[๖]

๕. วิธีการรักษาความมั่นคงปลอดภัยในยุคควอนตัม

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของเทคโนโลยีสารสนเทศในยุคของคอมพิวเตอร์ควอนตัม สามารถดำเนินการได้หลากหลายวิธี ปัจจุบันวิธีการหลัก คือ การปรับเปลี่ยนระบบรหัสลับในปัจจุบันไปใช้ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum Cryptography: PQC) ซึ่งประกอบไปด้วยอัลกอริทึมที่ถูกพัฒนาให้มีความทนทานต่อการโจมตีจากคอมพิวเตอร์ควอนตัม อีกวิธีการสำคัญหนึ่งคือการใช้การกระจายกุญแจเชิงควอนตัม (Quantum Key Distribution: QKD)

๕.๑ <u>ระบบรหัสลับสำหรับยุคควอนตัม (Post-Quantum cryptography)</u>

ระบบรหัสลับสำหรับยุคควอนตัม คือ กลุ่มระบบรหัสลับที่ถูกออกแบบเพื่อมีความทนทานต่อการโจมตีจากคอมพิวเตอร์ควอนตัม ซึ่งถูกพัฒนามาจากปัญหาทางคณิตศาสตร์ที่ไม่สามารถแก้ได้ด้วยทั้งคอมพิวเตอร์ควอนตัมและคอมพิวเตอร์ทั่วไปอย่างมีประสิทธิภาพ โดยระบบรหัสลับแบบ PQC ถูกพัฒนาขึ้นมาเพื่อนำมาใช้ทดแทนที่ระบบรหัสลับดั้งเดิมที่มีความเสี่ยงจากการถูกโจมตีจากคอมพิวเตอร์ควอนตัม เช่น อัลกอริทึมประเภท RSA DH และ ECC

อัลกอริทึมประเภท PQC ถูกออกแบบให้สามารถใช้งานได้กับโครงสร้างพื้นฐานทางสารสนเทศและอินเทอร์เน็ตในปัจจุบัน อัลกอริทึมประเภท PQC อาจมีประสิทธิภาพในการประมวลผลใกล้เคียงหรือช้ากว่าอัลกอริทึมแบบดั้งเดิม โดยทั่วไปความยาวกุญแจรหัสลับของอัลกอริทึมประเภท PQC มักจะมีขนาดใหญ่กว่า

---

[๖] “Canadian National Quantum-Readiness: Best Practices and Guidelines Version 01”, Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), July 7, 2021.

กุญแจรหัสลับของอัลกอริทึมแบบดั้งเดิมมากจึงทำให้มีต้นทุนในการจัดเก็บและส่งข้อมูลผ่านระบบเครือข่ายที่สูงขึ้น

การปรับปรุงซอฟต์แวร์ของระบบสารสนเทศในองค์กรให้ไปใช้ PQC อาจไม่ใช่เรื่องง่ายในทางปฏิบัติ เนื่องจากว่าในหลาย ๆ องค์กรอาจมีการออกแบบให้ระบบรหัสลับมีความสัมพันธ์กับระบบสารสนเทศที่ซับซ้อน และการเปลี่ยนแปลงระบบรหัสลับอาจส่งผลกระทบกับองค์ประกอบอื่น ๆ ของระบบเป็นวงกว้าง นอกจากนี้ อุปกรณ์ฮาร์ดแวร์ขององค์กรอาจไม่มีหน่วยความจำและหน่วยประมวลผลที่เพียงพอต่อการทำงานของ PQC เช่น อุปกรณ์ประเภท IoTs ดังนั้น การปรับปรุงฮาร์ดแวร์จึงอาจเป็นสิ่งจำเป็นสำหรับองค์กร เพื่อให้ฮาร์ดแวร์มีหน่วยความจำและประสิทธิภาพการประมวลผลเพียงพอต่อการใช้งานอัลกอริทึมประเภท PQC

องค์กรควรพิจารณาปรับปรุงระบบสารสนเทศขององค์กรให้มีความยืดหยุ่นรองรับการปรับเปลี่ยนอัลกอริทึมระบบรหัสลับ โดยมีความสอดคล้องตามหลักการความคล่องตัวระบบรหัสลับ (Crypto Agility) ซึ่งหมายถึง การที่ระบบรักษาความปลอดภัยสามารถปรับเปลี่ยนอัลกอริทึมระบบรหัสลับให้มีความทันสมัยได้อย่างรวดเร็ว หลักการนี้มีความสำคัญอย่างยิ่งในการเตรียมตัวเข้าสู่ยุคควอนตัมในอนาคต การจะปฏิบัติตามหลักการนี้ไม่ใช่เพียงการออกแบบและพัฒนาให้ระบบและโพรโทคอลมีความคล่องตัว แต่จะต้องมีมาตรฐานอัลกอริทึม PQC ที่พัฒนาจากปัญหาที่ยากแบบต่าง ๆ เพื่อเป็นตัวเลือกที่หลากหลาย ตัวเลือกของอัลกอริทึมที่หลากหลายเหล่านี้ยังเป็นประโยชน์ต่อการใช้งานที่มีความต้องการด้านประสิทธิภาพและความมั่นคงปลอดภัยที่แตกต่างกัน ทั้งนี้ อัลกอริทึม PQC ยังไม่ได้อยู่ในสภาวะที่สมบูรณ์เต็มที่และยังจำเป็นที่จะต้องได้รับการพัฒนาต่อยอด ทดสอบ และผ่านบทพิสูจน์อีกมากมาย บางอัลกอริทึม PQC ในปัจจุบันอาจถูกค้นพบจุดอ่อนหรือช่องโหว่ที่ทำให้ไม่มีความมั่นคงปลอดภัยจากการศึกษาเพิ่มเติมในอนาคต เช่น SIKE ที่ได้รับการประเมินหลายปีโดย NIST จนกระทั่งเดือนสิงหาคม พ.ศ. ๒๕๖๕ จึงค้นพบว่ามีปัญหาด้านความมั่นคงปลอดภัย ดังนั้นอัลกอริทึมที่ใช้ในระบบควรที่จะสามารถถูกสับเปลี่ยนทดแทนได้อย่างคล่องตัวและรวดเร็ว

ถึงแม้ว่าอัลกอริทึม PQC จะถูกเริ่มพัฒนามาตั้งแต่หลายปีก่อนและได้รับการพัฒนาอย่างต่อเนื่องจนในปัจจุบันมีอัลกอริทึม PQC จำนวนหนึ่งที่ได้รับความสนใจจากผู้เชี่ยวชาญบางกลุ่มและบางองค์กร แต่อัลกอริทึม PQC เหล่านี้ยังคงอยู่ในช่วงการพัฒนาและยังไม่สมบูรณ์เต็มที่ ยังจำเป็นต้องมีการศึกษาเพิ่มเติมและการทดสอบอย่างเข้มงวดจึงจะเชื่อมั่นได้ว่ามีความมั่นคงปลอดภัยและเหมาะกับการใช้งานในสภาพแวดล้อมจริง

หลายองค์กรด้านมาตรฐานและองค์กรด้านความมั่นคงปลอดภัยทั่วโลกได้มีการศึกษา พัฒนา จัดประกวด และออกมาตรฐานและแนวปฏิบัติการใช้อัลกอริทึม PQC เอกสารฉบับนี้ได้รวบรวมสถานะและมุมมองขององค์กรเหล่านี้ต่ออัลกอริทึม PQC ต่าง ๆ ทั้งนี้ สกมช. ไม่ได้สนับสนุนหรือรับรองการใช้งานอัลกอริทึม PQC ใด ๆ ที่กล่าวถึงในเอกสารฉบับนี้มากกว่าอัลกอริทึม PQC อื่น ๆ ที่ไม่ได้กล่าวถึง เพียงแต่ได้นำเสนอเพื่อเป็นข้อมูลตั้งต้นให้ผู้สนใจสามารถไปศึกษาเพิ่มเติมได้ สกมช. มีจุดยืนที่เป็นกลางต่อการเลือกใช้อัลกอริทึม PQC

และแนะนำให้ผู้ใช้งานศึกษาคุณลักษณะ การใช้งาน และข้อจำกัดของแต่ละอัลกอริทึม PQC อย่างถี่ถ้วน เลือกใช้อัลกอริทึมที่สามารถตอบโจทย์ความต้องการได้และเหมาะสมต่อบริบท และควรทดสอบอัลกอริทึมให้รอบด้านก่อนนำไปใช้งานกับระบบในสภาพแวดล้อมจริง

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (The National Institute of Standards and Technology: NIST) กำลังพัฒนามาตรฐานสำหรับอัลกอริทึมประเภท PQC โดยเริ่มดำเนินการพัฒนามาตรฐานตั้งแต่ปี พ.ศ. ๒๕๕๙ โดยในปัจจุบันได้ดำเนินการคัดเลือกอัลกอริทึมมาแล้วทั้งหมด ๓ รอบ ซึ่งในแต่ละรอบนั้นทางหน่วยงาน NIST ได้ประเมินคุณสมบัติของแต่ละอัลกอริทึมที่สมัครเข้ารับการคัดเลือก (Candidate Algorithms) เพื่อเปรียบเทียบความปลอดภัยต่อการโจมตีจากทั้งคอมพิวเตอร์แบบดั้งเดิมและแบบควอนตัม รวมถึงการเปรียบเทียบด้านประสิทธิภาพการใช้งาน และปัจจัยอื่น ๆ โดยประกาศผลการคัดเลือกครั้งล่าสุดในวันที่ ๕ กรกฎาคม พ.ศ. ๒๕๖๕ และมีแผนในการออกมาตรฐานฉบับสมบูรณ์ในปี พ.ศ. ๒๕๖๗ อัลกอริทึมที่ได้รับการคัดเลือกในรอบที่ ๓ ประกอบด้วยอัลกอริทึมสำหรับการแลกเปลี่ยนกุญแจและการเข้ารหัสลับ คือ CRYSTALS-Kyber[๗] และอัลกอริทึมสำหรับการลงลายมือชื่อดิจิทัล ได้แก่ CRYSTALS-Dilithium[๘] FALCON[๙] และ SPHINCS+[๑๐] ซึ่งอัลกอริทึมเหล่านี้ถูกนำไปพัฒนาเป็นมาตรฐาน Federal Information Processing Standards (FIPS) สำหรับการใช้งานโดยหน่วยงานรัฐในประเทศสหรัฐอเมริกา ได้แก่ FIPS 203 (CRYSTALS-Kyber) FIPS 204 (CRYSTAL-Dilithium) และ FIPS 205 (SPHINCS+)[๑๑] ตามลำดับ อีกทั้งกำลังดำเนินการคัดเลือกอัลกอริทึมประเภท PQC เป็นรอบที่ ๔ โดยมีอัลกอริทึมเพิ่มเติม ได้แก่ (๑) BIKE (๒) Classic McEliece (๓) HQC และ (๔) SIKE (ทั้งนี้ล่าสุดมีการศึกษาพบว่า SIKE ไม่มีความมั่นคงปลอดภัย จึงไม่ควรนำไปใช้งาน)[๑๒]

BSI ได้แนะนำอัลกอริทึม PQC ที่ส่งสมัครเข้าประกวดในการคัดเลือกของ NIST แต่ให้น้ำหนักการพิจารณาด้านระดับความมั่นคงปลอดภัยมากกว่าด้านประสิทธิภาพในการทำงาน BSI ยังได้แนะนำการใช้ระบบรหัสแบบดั้งเดิมร่วมกับ PQC แต่ลายมือชื่อดิจิทัลที่พัฒนาจากแฮชสามารถใช้งานโดยลำพังได้ถ้ามีการพัฒนาและนำไปใช้ที่มั่นคงปลอดภัย ในรายงาน TR 02102-1 (2023.1)[๑๓] BSI ได้แนะนำ FrodoKEM

---

[๗] https://pq-crystals.org/kyber/index.shtml

[๘] https://pq-crystals.org/dilithium/index.shtml

[๙] https://falcon-sign.info/

[๑๐] https://sphincs.org/

[๑๑] https://csrc.nist.gov/news/2023/three-draft-fips-for-post-quantum-cryptography

[๑๒] https://csrc.nist.gov/projects/post-quantum-cryptography/round-4-submissions

[๑๓] https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf

และ Classic McEliece สำหรับการเข้ารหัสลับแบบกุญแจอสมมาตรและการแลกเปลี่ยนกุญแจรหัสลับ และแนะนำ XMSS และ LMS สำหรับการทำลายมือชื่อดิจิทัล

สำนักงานความมั่นคงปลอดภัยระบบสารสนเทศแห่งชาติฝรั่งเศส (French National Agency for the Security of Information Systems: ANSSI) แนะนำอัลกอริทึม PQC ที่เข้ารอบสุดท้ายของ NIST โดยใช้พารามิเตอร์ที่ให้ระดับความมั่นคงปลอดภัยสูงที่สุด นอกจากนี้ยังได้แนะนำการใช้ระบบรหัสแบบดั้งเดิมร่วมกับ PQC ในช่วงต้นของการย้ายระบบไปสู่ยุคควอนตัม

สมาคมวิจัยวิทยาการรหัสลับแห่งชาติจีน (Chinese Association for Cryptologic Research: CACR) สนับสนุนโดย การบริหารระบบรหัสลับแห่งชาติจีน (State Cryptography Administration of China) ได้เปิดรับสมัครการแข่งขันการออกแบบอัลกอริทึมระบบรหัสลับแห่งชาติในปี พ.ศ. ๒๕๖๑ และประกาศผลในปี พ.ศ. ๒๕๖๒ วัตถุประสงค์ในการประกวดครั้งนี้ไม่ได้มุ่งเน้นเพื่อเป็นการพัฒนามาตรฐานระบบรหัสลับ แต่เป็นการซักซ้อมภายในประเทศ มีอัลกอริทึมแบบกุญแจอสมมาตรส่งเข้าประกวด ๓๘ รายการซึ่งถูกออกแบบมาให้ทนทานต่อการโจมตีแบบควอนตัม และมี ๑๑ รายการที่ได้รับรางวัล โดยอัลกอริทึมที่ได้รับรางวัลชนะเลิศ ได้แก่ Aigis สำหรับการเข้ารหัสลับและลายมือชื่อดิจิทัล และ LAC สำหรับการเข้ารหัสลับ

ศูนย์วิจัยรหัสลับที่ทนทานต่อการโจมตีแบบควอนตัมแห่งประเทศเกาหลี (Korean Quantum Resistant Cryptography Research Center: KpqC Center) ได้จัดการแข่งขันรหัสลับที่ทนทานต่อการโจมตีแบบควอนตัม เพื่อเป็นการยกระดับเทคโนโลยีภายในประเทศด้านรหัสลับที่ทนทานต่อการโจมตีแบบควอนตัม เสริมสร้างศักยภาพการแข่งขัน และสร้างการพัฒนาเทคโนโลยีเชิงรุกโดยการร่วมมือระหว่างภาคอุตสาหกรรม วิชาการ รัฐบาล และสถาบันวิจัย และคัดเลือกอัลกอริทึมรหัสลับสำหรับใช้ภายในประเทศ เริ่มเปิดรับประกวดในช่วงเดือนพฤศจิกายน พ.ศ. ๒๕๖๔ เริ่มพิจารณารอบแรกเดือนธันวาคม พ.ศ. ๒๕๖๕ ซึ่งมีเข้าประกวด ๑๖ รายการ และ พิจารณารอบที่สองเดือนธันวาคม พ.ศ. ๒๕๖๖ คัดเลือกเหลือ ๔ รายการสำหรับลายเซ็นดิจิทัล และ ๔ รายการสำหรับการแลกเปลี่ยนกุญแจรหัสลับ[๑๔] ได้แก่ AIMer, HAETAE, MQ-Sign, NCC-Sign, NTRU+, PALOMA, REDOG, และ SMAUG + TiGER

องค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization: ISO) ได้เริ่มดำเนินการพัฒนามาตรฐานด้าน PQC โดยได้จัดตั้งกลุ่มทำงาน ISO/IEC SC 27/WG 2 SD8 ในปี พ.ศ. ๒๕๖๐ มีการดำเนินโครงการ ISO/IEC PWI 19541 และอยู่ระหว่างพัฒนามาตรฐาน ISO/IEC 18033-2:2006/WD Amd 2 โดยมีการพิจารณาเพิ่มอัลกอริทึม PQC ได้แก่ FrodoKEM, NTRU, Classic McEliece และ CRYSTAL-Kyber โดยกฎการโหวตหลักโดยสมาชิก คือ จำนวนอัลกอริทึมควรมีจำนวนน้อยที่สุด โดยให้น้ำหนักกับอัลกอริทึมที่มีลักษณะทางประสิทธิภาพที่แตกต่างกันมากหรือพัฒนาจากหลักการ

---

[๑๔] https://www.kpqc.or.kr/competition.html

เทคนิคที่แตกต่างกัน และการโหวตเลือกให้ ๑ คะแนนต่อ ๑ หน่วยงานมาตรฐานของชาติโดยไม่ขึ้นอยู่กับจำนวนผู้แทนเข้าร่วมของแต่ละสมาชิก ให้โหวตเลือกเพื่อประโยชน์ต่อหน่วยงานมาตรฐานของชาติ ปัจจุบันมีสมาชิกเข้าร่วม (Participating members: P) ๕๘ สมาชิก และสมาชิกสังเกตการณ์ (Observing members: O) ๓๕ สมาชิก

คณะทำงานเฉพาะกิจด้านวิศวกรรมอินเทอร์เน็ต Internet Engineering Task Force: IETF) ได้มีการจัดตั้งกลุ่มทำงาน Post-Quantum Use In Protocols (PQUIP) Working Group[๑๕] เพื่อรองรับวิวัฒนาการของ PQC โดยปรับปรุงโพรโตคอลและเอกสารของ IETF ให้เหมาะสมกับยุคควอนตัม

๕.๒ <u>การกระจายกุญแจเชิงควอนตัม (Quantum key distribution)</u>

การกระจายกุญแจเชิงควอนตัมเป็นกระบวนการที่อาศัยปรากฏการณ์เชิงควอนตัมเพื่อการแลกเปลี่ยนกุญแจรหัสลับ โดยทั่วไป QKD จะใช้ฮาร์ดแวร์เฉพาะทางเพื่อการส่งคิวบิตเชิงแสง (Photonic qubits) ผ่านทางใยแก้วนำแสงหรือทางอากาศ หากมีผู้ไม่ประสงค์ดีพยายามที่จะดักฟัง (Eavesdrop) ข้อมูลที่สื่อสารกัน การดักฟังนั้นจะส่งผลกระทบต่อคิวบิตเชิงแสงดังกล่าว ทำให้ผู้รับข้อมูลปลายทางสามารถใช้คุณสมบัติเชิงควอนตัมเพื่อตรวจสอบได้ว่ามีการดักฟังเกิดขึ้นหรือไม่ ดังนั้นผู้ที่สื่อสารสามารถมั่นใจได้ว่าข้อมูลที่สื่อสารไม่รั่วไหลไปยังผู้อื่น QKD เป็นกระบวนการที่เพิ่มความปลอดภัยในการแลกเปลี่ยนกุญแจรหัสลับสำหรับการใช้ในโพรโทคอลการสื่อสารอื่น ๆ ต่อไป

การแลกเปลี่ยนกุญแจด้วยกระบวนการประเภท QKD มีความปลอดภัยในทางทฤษฎี (Theoretically Secure) จากทั้งคอมพิวเตอร์แบบดั้งเดิมและคอมพิวเตอร์ควอนตัม ทั้งนี้ QKD นั้นมีข้อจำกัดในแง่ของการใช้งาน ทำให้ใช้ได้กับบางกรณีการใช้งานที่เฉพาะเจาะจงเท่านั้น ข้อจำกัดของเทคโนโลยี QKD ในปัจจุบันมีดังนี้

- QKD มีความเหมาะสมกับการใช้งานที่มีระยะทางสั้นไม่เกิน ๑๒๕ กิโลเมตรเท่านั้น[๑๖] โดยการส่งคิวบิตเชิงแสงผ่านใยแก้วนำแสงแบบจุดต่อจุด (Point-to-point) ทั้งนี้ เทคโนโลยี Quantum repeaters หรือการจัดส่งคิวบิตเชิงแสงผ่านทางดาวเทียม อาจถูกนำมาใช้เพื่อขยายระยะทางของ QKD ได้ในอนาคต

---

[๑๕] https://datatracker.ietf.org/wg/pquip/about/

[๑๖] “A Guide to a Quantum-Safe Organization: Transitioning from today’s cybersecurity to a quantum-resilient environment”, The Quantum Economic Development Consortium (QED-C), July 2022.

- QKD มีอัตราในการแลกเปลี่ยนกุญแจรหัสลับ (Key exchange rate) ที่ต่ำ เมื่อเทียบกับโพรโทคอลการแลกเปลี่ยนกุญแจแบบดั้งเดิม ทั้งนี้ ในปัจจุบัน QKD มีอัตราการแลกเปลี่ยนกุญแจที่มากกว่า 1 Mbps ซึ่งเพียงพอต่อการใช้งานสำหรับบางแอปพลิเคชันเท่านั้น
- QKD มีความจำเป็นต้องใช้ฮาร์ดแวร์เฉพาะทาง ซึ่งอาจมีต้นทุนสูง
- QKD สามารถนำไปใช้เพื่อการแลกเปลี่ยนกุญแจ แต่ไม่สามารถนำไปใช้ในการยืนยันตัวตน (Authentication) ได้ ทำให้ติดตั้งเครือข่าย QKD ต้องอาศัยการยืนยันตัวตนโดยบุคคล (Manual Authentication) หรือ อาศัยโพรโทคอลการยืนยันตัวตนแบบอื่นร่วมด้วย
- QKD มีความเสี่ยงต่อการโจมตีที่ช่องโหว่ด้านความปลอดภัยของอุปกรณ์ฮาร์ดแวร์ (Hardware Vulnerabilities) และการโจมตีประเภท Side-Channel ซึ่งอาศัยการวิเคราะห์ข้อมูลความร้อนหรือคลื่นแม่เหล็กไฟฟ้าจากอุปกรณ์ฮาร์ดแวร์ในการโจมตี เป็นต้น

นอกจากนี้หน่วยงานที่มีบทบาทสำคัญและเกี่ยวข้องในต่างประเทศมีมุมมองต่อ QKD ดังต่อไปนี้[๑๗-๑๘]

- ANSSI ได้ทำการศึกษาและวิเคราะห์ข้อดีข้อเสียของ PQC และ QKD และได้ข้อสรุปว่า PQC เป็นทางเลือกที่ง่ายและต้นทุนต่ำกว่าในการนำไปใช้งานจริงและไม่ติดข้อจำกัดต่าง ๆ ของ QKD ดังนั้น จึงควรที่จะมุ่งเน้นการพัฒนา PQC เพื่อเตรียมตัวเข้าสู่ยุคควอนตัม
- สำนักงานความมั่นคงแห่งชาติเห็นข้อจำกัดของ QKD และยังไม่สนับสนุนการใช้ QKD ในระบบความมั่นคงของชาติจนกว่าข้อจำกัดดังกล่าวจะได้รับการแก้ไข
- ศูนย์ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Centre: NCSC) สหราชอาณาจักรยังไม่สนับสนุนการใช้ QKD ในแอปพลิเคชันของรัฐและทหาร

ข้อจำกัดทางด้านเทคโนโลยีในปัจจุบันดังกล่าว ทำให้ QKD อาจยังไม่เหมาะสมต่อการใช้งานทั่วไป อาจเหมาะสมเพียงแอปพลิเคชันบางประเภทเท่านั้น

๕.๓ <u>ระบบแบบผสม (Hybrid Solutions)</u>

การพัฒนาระบบสารสนเทศให้มีความทนทานจากการโจมตีโดยคอมพิวเตอร์ควอนตัมนั้นสามารถดำเนินการได้หลากหลายวิธี โดยเทคโนโลยีที่แตกต่างกันสามารถนำมาใช้ร่วมกันเพื่อส่งเสริมและชดเชยข้อจำกัด

---

[๑๗] Quantum-safe cryptography – fundamentals, current developments and recommendations. Federal Office for Information Security (BSI), May of 2022.

[๑๘] Preparing for Quantum-Safe Cryptography (version 2.0). NCSC, the UK, Nov. 2020. https://www.ncsc.gov.uk/whitepaper/preparing-for-quantum-safe-cryptography.

ของกันและกัน ดังนั้นจึงควรนำเทคโนโลยีเหล่านี้มาใช้งานร่วมกันอย่างเหมาะสมเพื่อให้การย้ายระบบรหัสลับเป็นไปได้อย่างราบรื่น ใช้งานได้ดี และมีประสิทธิภาพ

ในการจัดทำระบบสารสนเทศแบบผสมระหว่างระบบรหัสลับแบบดั้งเดิมและ PQC องค์กรควรประเมินความต้องการภายในองค์กรตนเองเพื่อที่จะได้วางแผนการออกแบบระบบเพื่อลดความเสี่ยงต่าง ๆ ให้มีความเหมาะสมกับสินทรัพย์ทางสารสนเทศและแอปพลิเคชันขององค์กร ANSSI BSI และ IETF ได้ให้ความเห็นว่าวิธีการแบบผสมที่คุ้มค่าที่สุดคือการผสมระบบรหัสลับแบบดั้งเดิมและ PQC ด้วยกัน ซึ่งทาง IETF เพิ่งออก RFC 9370 สำหรับ IKEv2 โดยใช้การแลกเปลี่ยนกุญแจรหัสลับผสมทั้งแบบดั้งเดิมและแบบที่ทนทานต่อการโจมตีด้วยควอนตัมเพื่อใช้ในการสร้างกุญแจรหัสลับสุดท้าย[๑๙-๒๐]

๖. ระยะเวลาที่เกี่ยวข้องต่อการเตรียมความพร้อมและประเมินความเสี่ยง

แต่ละองค์กรมีความเสี่ยง หรือ Risk Profiles ในแง่มุมต่าง ๆ ที่แตกต่างกัน ดังนั้นแต่ละองค์กรอาจต้องเตรียมความพร้อมรับมือกับภัยคุกคามทางควอนตัมด้วยวิธีที่แตกต่างกันไป ทั้งนี้ ศาสตราจารย์ Michele Mosca จากมหาวิทยาลัยวอเตอร์ลู (University of Waterloo) ซึ่งเป็นผู้เชี่ยวชาญทางด้านระบบรหัสลับแบบควอนตัม ได้พัฒนากรอบการทำงานสำหรับการเริ่มต้นประเมินความเสี่ยงขององค์กร เรียกว่า โมเดล Mosca (Mosca Model) ซึ่งประกอบไปด้วย ๓ ตัวแปรสำคัญ ได้แก่ ระยะเวลาในการเตรียมความพร้อม (Migration Time) ระยะเวลาที่ต้องเก็บรักษาข้อมูล (Security Shelf Life) และ ระยะเวลาก่อนเกิดภัยคุกคาม (Threat Timeline)[๒๑]

๖.๑ <u>ระยะเวลาในการเตรียมความพร้อม (Migration Time)</u>

ตัวแปรแรกที่ต้องพิจารณา คือ **ระยะเวลาในการเตรียมความพร้อม (Migration Time)** เป็นระยะเวลาที่องค์กรต้องใช้เพื่อเปลี่ยนแปลงระบบขององค์กรให้มีความปลอดภัยต่อภัยคุกคามจากคอมพิวเตอร์ควอนตัม ทั้งนี้ ระยะเวลาในการเตรียมความพร้อมสำหรับแต่ละองค์กรจะมีความแตกต่างกัน ขึ้นกับปริมาณและความหลากหลายของข้อมูลและแอปพลิเคชันขององค์กร โดยผู้เชี่ยวชาญทางด้านเทคโนโลยีควอนตัมคาดการณ์ว่าองค์กรหนึ่ง ๆ อาจต้องใช้ระยะเวลานานมากกว่า ๑๐ ปี ในการเปลี่ยนระบบขององค์กรทั้งหมด

---

[๑๙] ANSSI views on the Post-Quantum Cryptography transition. Released on March 2022. https://www.ssi.gouv.fr/uploads/2022/01/anssi-technical_position_papers-post_quantum_cryptography_transition.pdf

[๒๐] Quantum-safe cryptography - fundamentals, current developments and recommendations. Federal Office for Information Security, Germany, May 2022.

[๒๑] M. Mosca, “Cybersecurity in an era with quantum computers: will we be ready?”, IEEE Security & Privacy, 16(5), 38-41.

ให้มีความปลอดภัยต่อการโจมตีจากคอมพิวเตอร์ควอนตัม ดังนั้น องค์กรจึงไม่ควรประเมินระยะเวลาในการเตรียมความพร้อมน้อยเกินไป อีกทั้งควรตระหนักถึงความซับซ้อนในการเปลี่ยนแปลงระบบขององค์กร ดังนี้

- โพรโตคอลประเภท PQC เป็นเทคโนโลยีใหม่ที่ต้องดำเนินการทดสอบการใช้งานในสถานการณ์จริง โดยต้องทดสอบการใช้งานอย่างถี่ถ้วน เพื่อให้มั่นใจว่าระบบต่าง ๆ ภายในองค์กรสามารถทำงานร่วมกันได้
- โพรโตคอลประเภท PQC มีขนาดของกุญแจที่ใหญ่กว่า และมีประสิทธิภาพในการทำงานที่ต่ำกว่าโพรโตคอลการเข้ารหัสลับที่ใช้ในปัจจุบัน ทำให้การใช้งานโพรโตคอลประเภท PQC อาจมีผลกระทบต่อประสิทธิภาพการทำงานของระบบเครือข่ายและฮาร์ดแวร์ โดยเฉพาะอุปกรณ์ประเภท IoTs ซึ่งมีข้อจำกัดด้านความจุในการจัดเก็บข้อมูลและการประมวลผลข้อมูล
- ระบบโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure: PKI) เป็นโครงสร้างพื้นฐานของระบบอินเทอร์เน็ตในปัจจุบัน ซึ่งมีความสัมพันธ์อย่างแน่นแฟ้นกับระบบเทคโนโลยีสารสนเทศต่าง ๆ ดังนั้น การเปลี่ยนแปลงระบบ PKI ให้มีความปลอดภัยจากคอมพิวเตอร์ควอนตัมจึงเป็นสิ่งที่จำเป็นและมีความสำคัญต่อการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ปัจจุบันหน่วยงานที่มีบทบาทสำคัญและเกี่ยวข้องในหลายประเทศได้ออกรายงานหรือแนวปฏิบัติเกี่ยวกับการเตรียมพร้อมการย้ายระบบสารสนเทศเข้าสู่ยุคควอนตัม ทว่า มีเพียง Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) โดย สำนักงานความมั่นคงแห่งชาติ (National Security Agency: NSA) สหรัฐอเมริกา ได้ระบุเส้นเวลาที่ชัดเจนในการอัปเดตระบบความมั่นคงของชาติให้พร้อมกับยุคควอนตัมภายในปี พ.ศ. ๒๕๗๖

๖.๒ <u>ระยะเวลาที่ต้องเก็บรักษาข้อมูล (Security Shelf Life)</u>

ตัวแปรที่สองที่องค์กรต้องพิจารณา คือ **ระยะเวลาที่ต้องเก็บรักษาข้อมูล (Security Shelf Life)** ของข้อมูลสำคัญภายในองค์กร กล่าวคือ ระยะเวลาที่ข้อมูลต้องถูกจัดเก็บไว้โดยมีความมั่นคงความปลอดภัย โดยอายุการเก็บรักษาข้อมูลจะมีระยะเวลาที่แตกต่างกัน ขึ้นกับประเภทแอปพลิเคชันที่ใช้งาน ประเภทขององค์กร และประเภทของอุตสาหกรรมของข้อมูลนั้น ๆ ซึ่งตัวอย่างข้อมูลที่จำเป็นต้องรักษาความปลอดภัยไว้เป็นเวลานาน ได้แก่ ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลทางด้านสุขภาพ เป็นต้น

ระบบการเข้ารหัสลับในปัจจุบันซึ่งขึ้นอยู่กับระบบโครงสร้างพื้นฐานกุญแจสาธารณะ มีความเสี่ยงต่อการโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง ทำให้ข้อมูลที่เป็นความลับและมีความจำเป็นต้องจัดเก็บมากกว่า ๑๐ ปี มีความเสี่ยงต่อการถูกโจมตีประเภทนี้ ดังนั้น องค์กรจึงควรให้ความสำคัญกับการจัดเก็บข้อมูลให้ปลอดภัยจากคอมพิวเตอร์ควอนตัม โดยเฉพาะหน่วยงานของรัฐ สถาบันทางการเงิน และสถาบันทางการแพทย์ เป็นต้น ซึ่งจัดเก็บข้อมูลความลับระดับชาติ และข้อมูลส่วนบุคคลที่มีความอ่อนไหว

อุปกรณ์ฮาร์ดแวร์ เช่น อุปกรณ์ IoTs และรถยนต์ไฟฟ้า อาจมีอายุการใช้งานนานและใช้การยืนยันตัวตนผ่านสัญญาณสื่อสารแบบไร้สายเพื่อการอัปเดตระบบ อาจถูกใช้งานต่อเนื่องภายหลังการพัฒนาคอมพิวเตอร์ควอนตัมที่มีความสามารถในการถอดระบบรหัสลับแบบดั้งเดิม ดังนั้น อุปกรณ์ฮาร์ดแวร์เหล่านี้มีความเสี่ยงจากการถูกโจมตีระบบยืนยันตัวตนด้วยคอมพิวเตอร์ควอนตัม ทำให้ผู้ไม่ประสงค์ดีสามารถอัปเดตระบบด้วยซอฟต์แวร์ที่เป็นอันตราย (Malicious software updates) นอกจากนี้ ระบบโครงสร้างพื้นฐานสาธารณะ เช่น ระบบโครงข่ายสำหรับส่งไฟฟ้าอัจฉริยะ (Smart grid) เป็นอีกตัวอย่างหนึ่งซึ่งใช้งานอุปกรณ์ประเภท IoTs ซึ่งมีอายุการใช้ยาวนานและอาจส่งผลกระทบอย่างกว้างขวางหากถูกโจมตี

๖.๓ <u>ระยะเวลาก่อนเกิดภัยคุกคาม (Threat Timeline)</u>

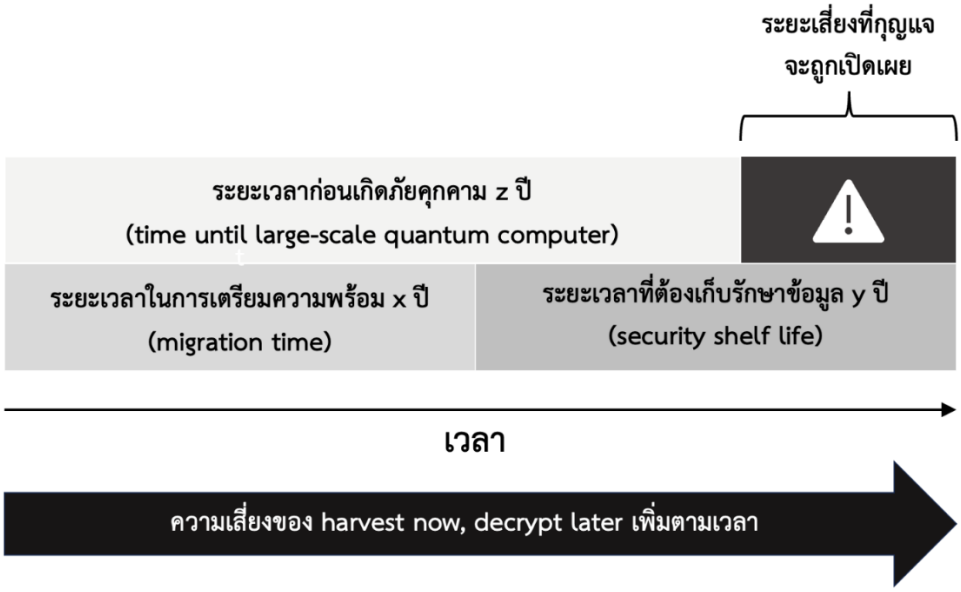
ตัวแปรที่สามที่องค์กรต้องพิจารณา คือ **ระยะเวลาก่อนเกิดภัยคุกคาม (Threat Timeline)** เป็นระยะเวลาที่ต้องใช้ในการพัฒนาคอมพิวเตอร์ควอนตัมขนาดใหญ่ที่สามารถใช้โจมตีระบบรหัสลับที่ใช้ในปัจจุบันได้

๖.๔ <u>โมเดล Mosca</u>

กำหนดให้ตัวแปร x y และ z แสดงถึงมีตัวแปรทั้ง ๓ ปัจจัย ดังต่อไปนี้

- **ตัวแปร x** คือ ระยะเวลาในการเตรียมความพร้อม (Migration Time) เป็นจำนวนปี
- **ตัวแปร y** คือ ระยะเวลาที่ต้องเก็บรักษาข้อมูล (Security Shelf Life) เป็นจำนวนปี
- **ตัวแปร z** คือ ระยะเวลาก่อนเกิดภัยคุกคาม (Threat Timeline) เป็นจำนวนปี

ในระหว่างระยะเวลา x ปีที่หน่วยงานต้องใช้ในการเตรียมความพร้อมเพื่อเปลี่ยนระบบรหัสลับให้มีความทนทานต่อการโจมตีแบบควอนตัม ข้อมูลที่สร้างขึ้นในระหว่าง x ปีนี้ (ปีที่ ๐ ไปจนถึงปีที่ x) มีความเสี่ยงที่จะถูกโจมตีแบบเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง โดยข้อมูลสุดท้ายที่ถูกสร้างขึ้นก่อนการเตรียมความพร้อมเสร็จสิ้น อาจถูกผู้ไม่ประสงค์ดีเก็บเกี่ยวไว้ (Harvest) และมีความเสี่ยงในการถูกถอดรหัสลับระยะเวลา y ปีนับจากขณะที่หน่วยงานเตรียมความพร้อมเสร็จสิ้น ดังนั้น ผลรวมของตัวแปรทั้งสอง (x + y) คือ ค่าประมาณระยะเวลาที่องค์กรต้องใช้เพื่อให้ข้อมูลสำคัญมีความปลอดภัยจากคอมพิวเตอร์ควอนตัม ถ้าผลรวมดังกล่าวมีค่ามากกว่าระยะเวลาในการพัฒนาคอมพิวเตอร์ควอนตัมขนาดใหญ่ซึ่งใช้เวลา z ปี กล่าวคือ (x + y) - z > 0 แสดงว่าข้อมูลนั้นมีความเสี่ยงจากการถูกโจมตี ดังแสดงในรูปที่ ๒



รูปที่ ๒ ระยะเวลาที่เกี่ยวข้องต่อการเตรียมความพร้อมและประเมินความเสี่ยงของภัยคุกคามจากคอมพิวเตอร์ควอนตัมต่อองค์กร[๒๒]

ยกตัวอย่างเช่น หน่วยงานหนึ่งต้องใช้เวลาเตรียมความพร้อม ๕ ปี (x = 5) และข้อมูลของหน่วยงานต้องจัดเก็บไว้ ๑๐ ปี (y = 10) โดยหน่วยงานเริ่มต้นการเตรียมความพร้อม ณ วันที่ ๑ มกราคม พ.ศ. ๒๕๖๗ ระบบหน่วยงานและข้อมูลของหน่วยงานจะมีความปลอดภัยจากการโจมตีคอมพิวเตอร์ควอนตัมนับจากวันนี้ ๑ มกราคม พ.ศ. ๒๕๗๒ เป็นต้นไป ทว่า ข้อมูลที่ถูกสร้างขึ้น ณ วันที่ ๓๑ ธันวาคม พ.ศ. ๒๕๗๑ ซึ่งยังไม่มีความปลอดภัยจากการโจมตีด้วยคอมพิวเตอร์ควอนตัม อาจถูกผู้ไม่ประสงค์ดีจัดเก็บไว้ โดยข้อมูลดังกล่าว ต้องถูกจัดเก็บรักษาไว้เป็นเวลา ๑๐ ปี ถึงวันที่ ๓๑ ธันวาคม พ.ศ. ๒๕๘๑ (x + y = 15) ดังนั้น ถ้าคอมพิวเตอร์ควอนตัมขนาดใหญ่ถูกพัฒนาสำเร็จในวันที่ ๑ มกราคม พ.ศ. ๒๕๗๗ (z = 10) จะมีระยะเวลาที่ข้อมูลดังกล่าวอาจถูกถอดรหัสลับเป็น ๑๕ – ๑๐ = ๕ ปี

๗. การประเมินและติดตามระยะเวลาก่อนเกิดภัยคุกคาม

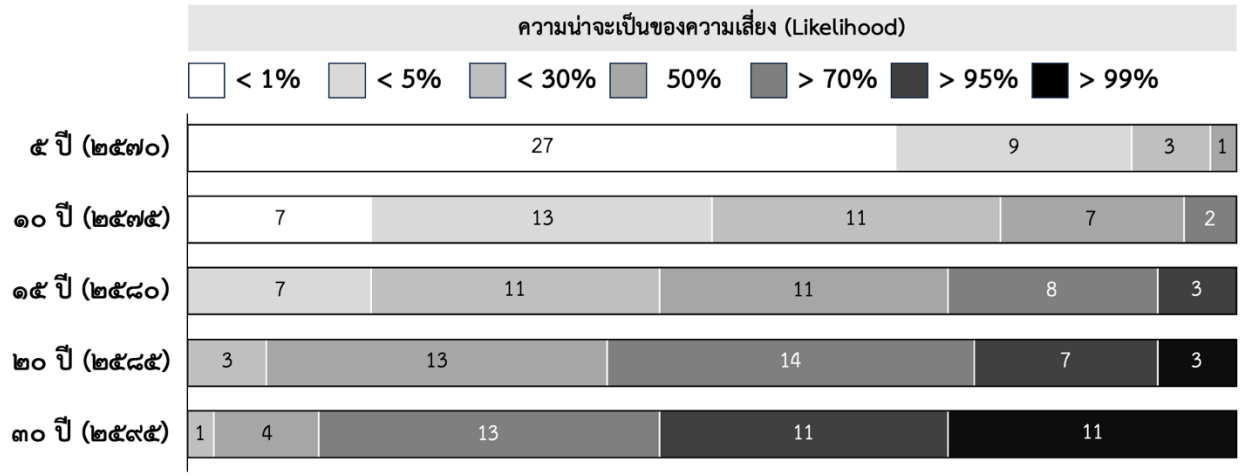
การประเมินระยะเวลาก่อนเกิดภัยคุกคาม (ตัวแปร z) มีความสำคัญอย่างยิ่งการประเมินความเสี่ยงของภัยคุกคามจากคอมพิวเตอร์ควอนตัม รวมถึงการวางแผนเพื่อเตรียมความพร้อมขององค์กร หัวข้อนี้จึงแสดงผลการประเมินระยะเวลาก่อนเกิดภัยคุกคามจากผลการศึกษาที่ดำเนินการสำรวจความคิดเห็น

[๒๒] “A Guide to a Quantum-Safe Organization: Transitioning from today’s cybersecurity to a quantum-resilient environment”, The Quantum Economic Development Consortium (QED-C), July 2022.

จากผู้เชี่ยวชาญด้านควอนตัม อีกทั้ง ให้รายละเอียดปัจจัยที่อาจเร่งระยะเวลาดังกล่าว และแนวทางในการติดตามความก้าวหน้าในการพัฒนาคอมพิวเตอร์ควอนตัม เพื่อการประเมินระยะเวลาใหม่อย่างต่อเนื่อง

๗.๑ การคาดการณ์ระยะเวลาก่อนเกิดภัยคุกคามโดยผู้เชี่ยวชาญ

บริษัท evolutionQ ได้จัดทำรายงานเส้นเวลาภัยคุกคามควอนตัม (Quantum Threat Timeline Report 2022)[๒๓] ได้สอบถามการคาดการณ์จากผู้เชี่ยวชาญด้านเทคโนโลยีควอนตัมทั้งหมด ๔๐ คน ถึงโอกาสที่คอมพิวเตอร์ควอนตัมที่สามารถถอดรหัสลับ RSA-2048 ได้ภายในเวลา ๒๔ ชั่วโมงด้วยอัลกอริทึม Shor จะถูกพัฒนาขึ้นภายในระยะเวลา ๕ ถึง ๓๐ ปี ดังแสดงใน รูปที่ ๓ ผู้เชี่ยวชาญมีความเห็นตรงกันว่าคอมพิวเตอร์ควอนตัมจะกลายเป็นภัยคุกคามสำคัญในระยะเวลาที่ไม่นาน โดยผู้เชี่ยวชาญ ๒๐ จาก ๔๐ คน เชื่อว่าคอมพิวเตอร์ควอนตัมมีโอกาสน้อยกว่าร้อยละ ๕ ที่จะเป็นภัยคุกคามภายในเวลา ๑๐ ปี ในขณะที่ผู้เชี่ยวชาญ ๙ คน เชื่อว่ามีโอกาสมากกว่าร้อยละ ๕๐ ที่จะเป็นภัยคุกคามภายในเวลา ๑๐ ปี



รูปที่ ๓ โอกาสที่คอมพิวเตอร์ควอนตัมจะกลายเป็นภัยคุกคามต่อระบบรหัสลับแบบกุญแจอสมมาตร ภายในปี ๒๕๗๐ ถึง ๒๕๙๕ จากผลสำรวจการคาดการณ์โดยผู้เชี่ยวชาญด้านเทคโนโลยีควอนตัม ๔๐ คน

โปรโตคอลระบบรหัสลับที่แตกต่างกันก็อาจจะถูกถอดรหัสลับได้ภายในระยะเวลาที่แตกต่างกัน ตัวอย่างเช่น ที่ระดับความปลอดภัยเทียบเท่ากัน อัลกอริทึมประเภท ECC อาจมีเสี่ยงต่อการถูกถอดรหัสลับมากกว่าอัลกอริทึมประเภท Rivest-Shamir-Adleman (RSA)[๒๔]

---

[๒๓] https://www.evolutionq.com/publications/quantum-threat-timeline-2022

[๒๔] Roetteler, Martin, et al. "Quantum resource estimates for computing elliptic curve discrete logarithms." Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Springer International Publishing, 2017.

๗.๒ <u>ปัจจัยเร่งระยะเวลาก่อนเกิดภัยคุกคาม</u>

ระยะเวลาที่จะเกิดภัยคุกคามจากคอมพิวเตอร์ควอนตัม (ตัวแปร z) อาจเกิดขึ้นรวดเร็วมากกว่าที่ผู้เชี่ยวชาญได้คาดการณ์ไว้ โดยอาจมีปัจจัยที่สามารถเร่งระยะเวลาได้ ดังนี้

- การพัฒนาขีดความสามารถของคอมพิวเตอร์ควอนตัมโดยการเพิ่มจำนวนคิวบิต (Qubits) ที่สามารถใช้งานได้ และ ลดอัตราการเกิดข้อผิดพลาด (Error rates) จากการคำนวณ
- การพัฒนาคอมพิวเตอร์ควอนตัมแบบเฉพาะทาง (Purpose-Built Quantum Computers) ที่ถูกออกแบบมาสำหรับใช้ในการประมวลอัลกอริทึมหนึ่ง ๆ โดยเฉพาะ ซึ่งอาจสามารถพัฒนาได้รวดเร็วกว่าคอมพิวเตอร์ควอนตัมแบบทั่วไป (General-Purpose Quantum Computers)
- การพัฒนาอัลกอริทึมประเภทอัลกอริทึม Shor (Shor's Algorithm) หรืออัลกอริทึมเชิงควอนตัมอื่น ๆ ให้สามารถทำงานได้อย่างมีประสิทธิภาพมากขึ้น กล่าวคือ สามารถใช้จำนวนคิวบิตที่น้อยลงได้ในการประมวลผล

๗.๓ <u>แนวทางการติดตามระยะเวลาก่อนเกิดภัยคุกคาม</u>

เพื่อการประเมินระยะเวลาก่อนเกิดภัยคุกคาม (ตัวแปร z) เจ้าหน้าที่ขององค์กรจำเป็นต้องติดตามความก้าวหน้าในการพัฒนาคอมพิวเตอร์ควอนตัมและควรดำเนินการอย่างต่อเนื่อง ทว่าการติดตามนั้นอาจไม่ใช่เรื่องง่าย เพราะนักพัฒนาคอมพิวเตอร์ควอนตัมมักรายงานผลความก้าวหน้าในการพัฒนาโดยใช้หน่วยวัดที่แตกต่างกัน เช่น จำนวนคิวบิตเชิงกายภาพ (Physical Qubits) จำนวนคิวบิตเชิงตรรกะ (Logical Qubits) ปริมาตรควอนตัม (Quantum Volume) ฯลฯ ซึ่งทำให้เกิดความยากลำบากในการเปรียบเทียบผลความก้าวหน้าต่าง ๆ ดังนั้น เจ้าหน้าที่ขององค์กรที่รับผิดชอบการติดตามความก้าวหน้าการพัฒนาคอมพิวเตอร์ควอนตัมต้องตีความผลลัพธ์ของข้อมูลเหล่านี้อย่างระมัดระวังและรอบคอบเพื่อให้เข้าใจความก้าวหน้าได้อย่างถูกต้องและเป็นประโยชน์ในการบริหารจัดการโครงการและการวางแผนในอนาคตที่เกี่ยวข้องกับเทคโนโลยีควอนตัม

หนึ่งในตัวชี้วัดที่สำคัญคือ "คิวบิตเชิงตรรกะ" ซึ่งถูกพิจารณาว่าเป็นหน่วยพื้นฐานที่ใช้ในการเขียนและอ่านข้อมูลของคอมพิวเตอร์ควอนตัม โดยคิวบิตเชิงตรรกะประกอบไปด้วยคิวบิตเชิงกายภาพหลายตัวที่มีการทำงานร่วมกันให้เป็นคิวบิตเดียวกันซึ่งมีอัตราความผิดพลาดที่ต่ำกว่า เจ้าหน้าที่ขององค์กรสามารถใช้จำนวนคิวบิตเชิงตรรกะเป็นมาตรวัดในการประเมินความก้าวหน้าในการพัฒนาคอมพิวเตอร์ควอนตัม

๘. แนวปฏิบัติการเตรียมความพร้อมสำหรับยุคควอนตัม

การคาดการณ์ระยะเวลาและทรัพยากรที่ต้องใช้เพื่อเตรียมความพร้อมสำหรับยุคควอนตัมอาจเป็นเรื่องยาก ทั้งนี้ องค์กรสามารถศึกษาตัวอย่างการเปลี่ยนแปลงโพรโทคอลระบบรหัสลับของระบบสารสนเทศในอดีต เพื่อใช้เป็นกรอบระยะเวลาและงบประมาณอ้างอิงเบื้องต้น

กรณีศึกษาหนึ่งในอดีต คือ การเปลี่ยนมาตรฐานของโพรโทคอลกุญแจระบบรหัสลับแบบกุญแจสมมาตร โดยในอดีตอัลกอริทึมประเภท Data Encryption Standard (DES) เคยได้รับการรับรองว่าเป็นมาตรฐาน

ในปี พ.ศ. ๒๕๑๙ ทว่าต่อมา DES ถูกโจมตีและถูกถอดรหัสลับได้ในช่วงทศวรรษ ๒๕๓๐ จึงถูกยกเลิกการรับรองว่าเป็นมาตราฐานเมื่อปี พ.ศ. ๒๕๔๘ และถูกแทนที่ด้วยอัลกอริทึมประเภท Triple Data Encryption Standard (3DES) จากนั้น ในปี พ.ศ. ๒๕๔๔ หน่วยงาน NIST ได้แนะนำอัลกอริทึมประเภท Advanced Encryption Standard (AES) เป็นมาตรฐานแทน โดยการศึกษาจากบริษัท Boston Consulting Group (BCG) พบว่าบางองค์กรใช้เวลานานมากถึง ๒๐ ปี ในการเปลี่ยนอัลกอริทึมระบบรหัสลับจากประเภท DES และ 3DES มาเป็น AES

ทั้งนี้ ผู้เชี่ยวชาญได้ประมาณการณ์เวลาที่องค์กรต้องใช้ในการเปลี่ยนแปลงระบบรหัสลับให้เป็น PQC ในกรอบระยะเวลาที่ใกล้เคียงกันกับข้างต้น คือประมาณ **๕ – ๒๐ ปี** ดังนั้น องค์กรควรจะเริ่มต้นการเปลี่ยนแปลงระบบสารสนเทศให้มีความปลอดภัยต่อการโจมตีจากคอมพิวเตอร์ควอนตัมแต่เนิ่น ๆ

๘.๑ ขั้นตอนการเตรียมความพร้อม

โดยมีแนวปฏิบัติการเตรียมความพร้อมมีขั้นตอนการดำเนินงานโดยสังเขป ดังนี้

๑. จัดทำแผนงาน : กำหนดบุคลากรที่มีความรู้ความสามารถให้ดำเนินการพัฒนาแผนงาน (Roadmap) เพื่อการเตรียมความพร้อมขององค์กรต่อภัยคุกคามจากคอมพิวเตอร์ควอนตัม โดยบุคลากรที่เหมาะสมต่อการพัฒนาแผนงานไม่จำเป็นต้องมีความเชี่ยวชาญด้านเทคโนโลยีควอนตัม ทั้งนี้ การเริ่มต้นจัดทำแผนงานแต่เนิ่น ๆ จะช่วยทำให้กระบวนการเปลี่ยนแปลงเทคโนโลยีมีความราบรื่น อีกทั้งทำให้องค์กรสามารถประเมินค่าใช้จ่ายที่ต้องใช้ในการลงทุน

๒. เสริมสร้างความตระหนักรู้ : ดำเนินการศึกษาเทคโนโลยีที่เกี่ยวข้อง รวมถึงเสริมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามจากคอมพิวเตอร์ควอนตัมให้แก่บุคลากรในแผนกต่าง ๆ ขององค์กร เช่น การให้ความรู้ความเข้าใจแก่แผนกฝ่ายจัดซื้อจัดจ้าง เพื่อให้เจ้าหน้าที่ที่เกี่ยวข้องเลือกใช้ซอฟต์แวร์หรือฮาร์ดแวร์ที่มีข้อกำหนดด้านความปลอดภัยต่อการโจมตีโดยคอมพิวเตอร์ควอนตัม

๓. กำหนดหน้าที่ความรับผิดชอบ : มอบหมายความรับผิดชอบให้กับเจ้าหน้าที่ในแต่ละส่วนงานที่เกี่ยวข้องกับการเตรียมความพร้อม ทั้งนี้ แม้ว่าองค์กรจะไม่ได้พัฒนาระบบซอฟต์แวร์ของตนเอง บุคลากรขององค์กรควรมีความรู้ความเข้าใจเกี่ยวกับเทคโนโลยีระบบรหัสลับที่องค์กรของตนเลือกใช้

๔. จัดทำรายการสินทรัพย์ทางสารสนเทศ : จัดทำรายการสินทรัพย์ทางสารสนเทศ (IT asset inventory) ที่มีความเกี่ยวข้องกับระบบรหัสลับ โดยตรวจสอบและจัดทำรายการสำหรับสินทรัพย์ที่เป็นทั้งซอฟต์แวร์และฮาร์ดแวร์ เพื่อทำความเข้าใจว่าองค์กรมีการใช้เทคโนโลยีระบบรหัสลับอย่างไร เช่น ศึกษาว่ากุญแจเข้ารหัสลับถูกสร้าง จัดเก็บ และ ใช้งานอย่างไรบ้างในปัจจุบัน

๕. ประเมินความเหมาะสมของเทคโนโลยีตัวเลือก : ประเมินความเหมาะสม ประสิทธิภาพ รวมถึงข้อดีและข้อเสีย ในการประยุกต์ใช้เทคโนโลยีประเภท PQC หรือ QKD กับระบบสารสนเทศภายในองค์กร

ตามความเหมาะสมกับองค์ประกอบของระบบที่แตกต่างกัน ทั้งนี้ องค์กรอาจเตรียมประยุกต์ใช้ระบบความปลอดภัยแบบผสม (Hybrid Security Approach) ซึ่งอาจผสมผสานทั้งระบบรหัสลับแบบดั้งเดิมและ PQC

๖. ทำการทดลองและทดสอบ : แม้ว่า ในปัจจุบันมาตรฐานเกี่ยวกับ PQC และ QKD ยังอยู่ในระหว่างการพัฒนา องค์กรสามารถเริ่มต้นดำเนินการทดลองและทดสอบระบบและเทคโนโลยีที่เกี่ยวข้องได้เลย เพื่อเตรียมความพร้อมสำหรับการเปลี่ยนแปลงระบบสารสนเทศในอนาคต ทั้งนี้ การดำเนินการทดลองและทดสอบดังกล่าว จะช่วยเสริมสร้างความรู้ความเข้าใจให้องค์กรเกี่ยวกับเทคโนโลยีที่ควรนำมาประยุกต์ใช้และปัญหาที่อาจเกิดขึ้นจากการปรับเปลี่ยนระบบรหัสลับในระบบสารสนเทศขององค์กร

๗. ติดตามความก้าวหน้าอย่างต่อเนื่อง : ติดตามความก้าวหน้าขององค์กรในการเตรียมความพร้อมอย่างต่อเนื่อง พร้อมทั้งดำเนินการประเมินความเสี่ยงและระยะเวลาก่อนเกิดภัยคุกคามใหม่เป็นระยะ

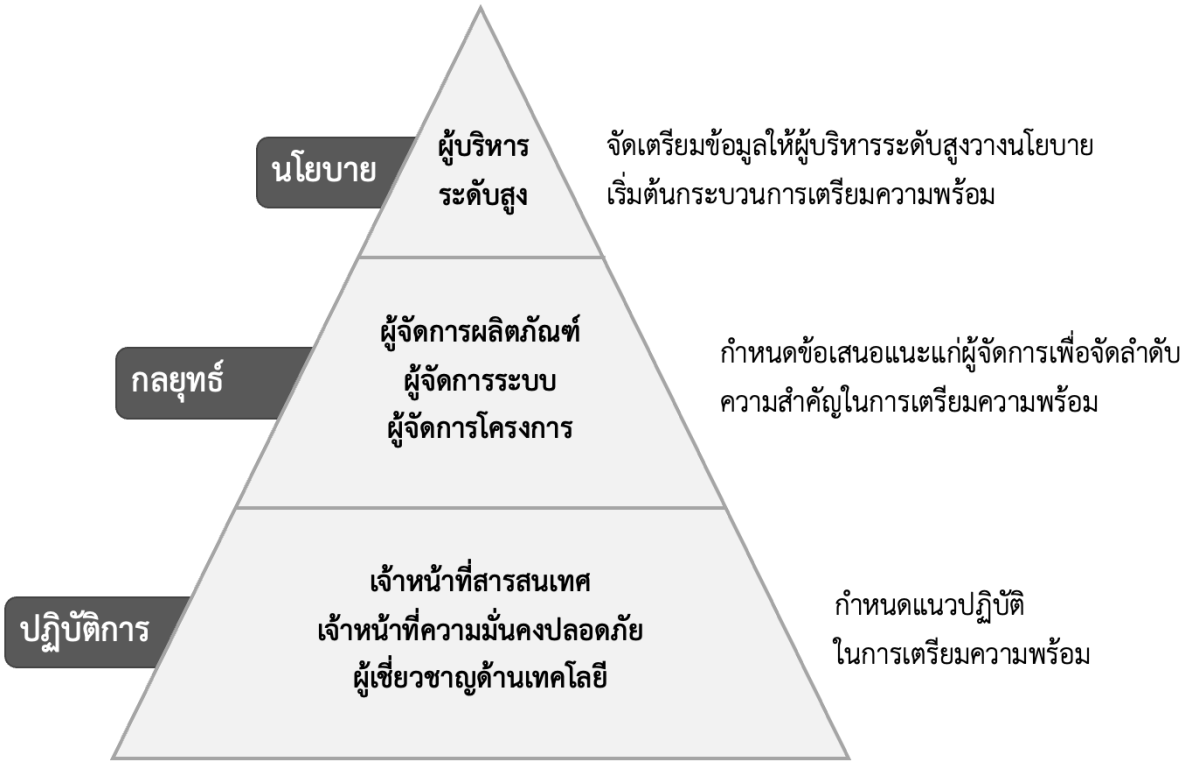
๘.๒ <u>แนวทางการสื่อสารเพื่อสร้างความตระหนักรู้ภายในองค์กร</u>

การเตรียมองค์กรให้มีความพร้อมต่อภัยคุกคามจากคอมพิวเตอร์ควอนตัมต้องอาศัยความร่วมมือจากเจ้าหน้าที่ในทุกระดับภายในองค์กร ตั้งแต่ ผู้บริหารระดับสูง ผู้จัดการ จนไปถึงเจ้าหน้าที่ระดับปฏิบัติการ เนื่องจากว่าการเปลี่ยนแปลงระบบรหัสลับภายในองค์กรอาจส่งผลกระทบต่อการทำงานของระบบสารสนเทศทั้งหมดภายในองค์กร ดังนั้น เจ้าหน้าที่ที่ได้รับมอบหมายให้ผู้นำเตรียมความพร้อมและเปลี่ยนแปลงระบบขององค์กร ควรดำเนินการสื่อสารและสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามจากคอมพิวเตอร์ควอนตัมให้กับเจ้าหน้าที่ในองค์กรทุกภาคส่วน

การสื่อสารและสร้างความตระหนักรู้มีแนวทางโดยสังเขป สามารถสรุปในรูปที่ ๔ ดังนี้

- **ผู้บริหารระดับสูง :** ควรจัดเตรียมข้อมูลที่เกี่ยวข้องกับการกำหนดนโยบายขององค์กร เพื่อให้ผู้บริหารระดับสูงมีความรู้ความเข้าใจถึงภัยคุกคามจากคอมพิวเตอร์ควอนตัมที่อาจเกิดขึ้นในอนาคต และสามารถตัดสินใจเพื่อวางนโยบายเกี่ยวกับการพัฒนาและปรับเปลี่ยนระบบสารสนเทศสนเทศขององค์กร ทั้งในด้านการจัดสรรทรัพยากรบุคคล งบประมาณการลงทุนการจัดซื้อจัดจ้างซอฟต์แวร์และฮาร์ดแวร์ขององค์กร เป็นต้น
- **เจ้าหน้าที่ระดับผู้จัดการ** : ควรจัดเตรียมข้อมูลเชิงกลยุทธ์รวมถึงกำหนดข้อเสนอแนะการเตรียมความพร้อมให้แก่เจ้าหน้าที่ระดับผู้จัดการ ให้มีความรู้ความเข้าใจถึงภัยคุกคามจากคอมพิวเตอร์ควอนตัม ทำให้สามารถจัดระดับความสำคัญในการเตรียมความพร้อม บริหารจัดการระบบงาน รวมถึงนำนโยบายของผู้บริหารระดับสูงมาปฏิบัติใช้ได้อย่างมีประสิทธิภาพ
- **เจ้าหน้าที่ระดับปฏิบัติการ** : ควรจัดเตรียมแนวปฏิบัติเชิงเทคนิคให้แก่เจ้าหน้าที่ระดับปฏิบัติการที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้สามารถดำเนินการเปลี่ยนแปลงซอฟต์แวร์และฮาร์ดแวร์ขององค์กรให้ทันสมัย

มีความปลอดภัยต่อการโจมตีจากทั้งคอมพิวเตอร์ในปัจจุบันและคอมพิวเตอร์ควอนตัมในอนาคต



รูปที่ ๔ เตรียมความพร้อมสำหรับยุคควอนตัม[๒๕]

๘.๓ <u>แนวทางการจัดทำรายการสินทรัพย์ทางสารสนเทศ</u>

การจัดทำรายการสินทรัพย์ทางสารสนเทศ (IT Assets Inventory) ในขั้นตอนที่ ๔ หัวข้อ ๘.๑ อาจถือได้ว่าเป็นขั้นตอนที่มีความซับซ้อนและมีความสำคัญที่สุดในการการเตรียมความพร้อมขององค์กร

ทั้งนี้ การจัดทำรายการสินทรัพย์ทางสารสนเทศเพื่อการเตรียมความพร้อมต่อการโจมตีจากคอมพิวเตอร์ควอนตัมจะทำให้เกิดผลพลอยได้ คือ อาจช่วยทำให้ระบบสารสนเทศขององค์กรมีความปลอดภัยทางไซเบอร์มากยิ่งขึ้นต่อการโจมตีโดยคอมพิวเตอร์ธรรมดาในปัจจุบัน เนื่องจากว่า การจัดทำรายการดังกล่าวจะช่วยให้องค์กรสามารถระบุจุดอ่อนหรือช่องโหว่ในระบบรักษาความปลอดภัยในปัจจุบันและทำให้สามารถดำเนินการปรับปรุงระบบได้อย่างมีประสิทธิภาพ

---

[๒๕] “Canadian National Quantum-Readiness: Best Practices and Guidelines Version 01”, Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR), July 7, 2021.

การจัดทำรายการสินทรัพย์ทางสารสนเทศ จะช่วยให้องค์กรสามารถจัดระดับความสำคัญเพื่อการเตรียมความพร้อม โดยมีองค์ประกอบสำคัญ ได้แก่ รายการข้อมูล (Data Inventory) และ รายการสินทรัพย์ระบบรหัสลับ (Crypto Assets Inventory)

๘.๓.๑ การจัดทำรายการข้อมูล (Data Inventory)

องค์กรควรจัดทำรายการข้อมูล (Data Inventory) ที่มีการใช้งานภายในองค์กร เพื่อให้ทราบถึงประเภท ระดับความสำคัญ และระยะเวลาที่ต้องเก็บรักษาข้อมูลต่าง ๆ รวมถึงสามารถเตรียมปรับปรุงซอฟต์แวร์เกี่ยวกับการเข้าถึงข้อมูลดังกล่าวได้ โดยมีปัจจัยที่ต้องระบุและพิจารณาดังนี้

- ระบุว่าข้อมูลประเภทใดในองค์กรที่มีความสำคัญและต้องจัดเก็บให้เป็นความลับ
- ระบุข้อมูลที่ต้องเก็บรักษาให้เป็นความลับเป็นระยะเวลานาน เช่น มากกว่า ๑๐ ปี
- ระบุสถานที่ ระบบ หรือ อุปกรณ์ ที่ใช้จัดเก็บข้อมูลขององค์กร
- ระบุกระบวนการหรือระบบที่ใช้ในการโอนย้ายข้อมูล
- ระบุวิธีการบริหารจัดการการเข้าถึงข้อมูล และ วิธีป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

๘.๓.๒ การจัดทำรายการสินทรัพย์ระบบรหัสลับ (Crypto Assets Inventory)

องค์กรควรจัดทำรายการสินทรัพย์ระบบรหัสลับคือ รายการของระบบอัลกอริทึมและโพรโทรคอลที่เกี่ยวกับระบบรหัสลับทั้งหมดที่มีการใช้งานภายในองค์กร เพื่อให้ทราบว่าระบบใดบ้างที่มีความเสี่ยงจากการถูกโจมตีด้วยคอมพิวเตอร์ควอนตัม เช่น รายการโพรโทคอลแลกเปลี่ยนกุญแจที่องค์กรใช้ในปัจจุบัน ซึ่งมีความเสี่ยงต่อการโจมตีประเภทเก็บเกี่ยวข้อมูลเพื่อถอดรหัสลับในภายหลัง โดยมีปัจจัยที่ต้องระบุและพิจารณาดังนี้

- ระบุกระบวนการเข้ารหัสลับและวิธีการรักษาความปลอดภัยของกุญแจเข้ารหัสลับ
- ระบุประเภทของอัลกอริทึมระบบรหัสลับและขนาดของกุญแจที่ใช้ในใบรับรองอิเล็กทรอนิกส์ (Digital certificates) แอปพลิเคชัน โพรโทคอลการสื่อสาร และระบบเครือข่าย
- ระบุซอฟต์แวร์ขององค์กรที่มีอัลกอริทึมระบบรหัสลับเป็นองค์ประกอบสำคัญ รวมถึงระบุข้อจำกัดของซอฟต์แวร์ในการเปลี่ยนไปใช้ระบบรหัสลับประเภทอื่น
- ระบุกระบวนการและขั้นตอนที่จำเป็นในการเปลี่ยนแปลงซอฟต์แวร์ขององค์กรไปใช้อัลกอริทึมระบบรหัสลับประเภทใหม่

ทั้งนี้ องค์กรอาจใช้ซอฟต์แวร์อัตโนมัติ เช่น ซอฟต์แวร์ประเภท “Crypto Healthcheck” เพื่อดำเนินการสแกนระบบสารสนเทศทั้งหมดขององค์กรเพื่อจัดทำรายการสินทรัพย์ระบบรหัสลับ จากนั้นตรวจหาจุดอ่อนหรือช่องโหว่ในระบบรักษาความปลอดภัย เป็นต้น

๙. ข้อมูลเพิ่มเติม

หน่วยงานสามารถติดตามข่าวสารล่าสุดจากสำนักงานผ่าน Line Openchat ตาม QR Code นี้

****

บรรณานุกรม

Felbinger J. (2022). *A guide to a quantum-safe organization: transitioning from today's cybersecurity to a quantum-resilient environment*. The Quantum Economic Development Consortium (QED-C). https://quantumconsortium.org/quantum-safe-guide/

Canadian National Quantum-Readiness: Best Practices And Guidelines Version 01. Quantum-Readiness Working Group (QRWG) of the Canadian Forum for Digital Infrastructure Resilience (CFDIR) (2021). https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/CFDIR-Prati-Tech-Quant-EN.pdf/$file/CFDIR-Prati-Tech-Quant-EN.pdf

Dilithium. CRYSTALS. (2023). https://pq-crystals.org/dilithium/index.shtml

KYBER. CRYSTALS. (2023). https://pq-crystals.org/kyber/index.shtml

Falcon. FALCON. (2023). https://falcon-sign.info/

SPHINCS^{+}. SPHINCS. (2023). https://falcon-sign.info/https://sphincs.org/

FIPS 203 (Initial Public Draft) Module-Lattice-Based Key-Encapsulation Mechanism Standard. NIST [Internet]. 2023 August. [cited 2023 September 12]; Available from: https://csrc.nist.gov/pubs/fips/203/ipd

FIPS 204 (Initial Public Draft) Module-Lattice-Based Digital Signature Standard. CRYSTALS [Internet]. 2023 August. [cited 2023 September 12]; Available from: https://pq-crystals.org/dilithium/index.shtml

FIPS 205 (Initial Public Draft) Stateless Hash-Based Digital Signature Standard. NIST [Internet]. 2023 August. [cited 2023 September 12]; Available from: https://falcon-sign.info/https://sphincs.org/

Horvath M, Lowans B, Fritsch J. *Preparing for the quantum World with crypto- agility*. Gartner Inc. (2022). https://www.gartner.com/en/documents/4019118

Mosca M. *Cybersecurity in a era with quantum computers: will we be ready?*. IEEE Security & Privacy. (2018). https://ieeexplore.ieee.org/document/8490169

Quantum Threat Timeline Report, 2022. evolutionQ. (2023). https://www.evolutionq.com/publications/quantum-threat-timeline-2022