การเข้ารหัสเชิงควอนตัม แนวทางการรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต

ในยุคสมัยที่ความก้าวหน้าทางเทคโนโลยีส่งผลให้มีการเผยแพร่ข้อมูลอยู่แทบจะตลอดเวลา วิธีที่ปลอดภัยในการส่งผ่านข้อมูลสำคัญจึงเป็นที่ต้องการอย่างมาก โดยทาง Cisco มีการคาดการณ์ว่า การรับส่งข้อมูลผ่านโทรศัพท์มือถือจะเพิ่มสูงขึ้นกว่าเจ็ดเท่าในระหว่างปีพ.ศ. 2559 ถึงพ.ศ. 2564 ซึ่งผู้ที่ทำงานด้านไอทีทั้งหลายต่างก็ตระหนักถึงความท้าทายนี้ เห็นได้จากผลการวิจัยล่าสุดของโตชิบาที่แสดงให้เห็นว่า 52% ของธุรกิจในยุโรปมองว่าความปลอดภัยของข้อมูลเป็น 1 ใน 3 การลงทุนที่สำคัญอันดับต้นๆ ในปีนี้ แต่ถึงกระนั้น บรรดาธุรกิจต่างๆ ก็ยังไม่ค่อยรู้จักหรือตระหนักถึงเทรนด์และนวัตกรรมด้านการรักษาความปลอดภัยบนโลกไซเบอร์เท่าไร และนี่คือจุดที่การเข้ารหัสเชิงควอนตัม หรือ Quantum Cryptography เข้ามาตอบโจทย์ ด้วยการใช้หลักการของควอนตัมฟิสิกส์ เทคโนโลยีนี้จะช่วยพาเราเข้าสู่ยุคสมัยของการติดต่อสื่อสารที่มีความปลอดภัยอย่างแท้จริง แต่การเข้ารหัสเชิงควอนตัมคืออะไร สามารถช่วยแก้ปัญหาอะไรได้บ้าง และสามารถเข้ามาเสริมความปลอดภัยให้กับธุรกิจในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในปัจจุบันและอนาคตอย่างไรบ้าง

การเข้ารหัสเชิงควอนตัมทำงานอย่างไร

“พูดง่ายๆ การเข้ารหัสเชิงควอนตัมเป็นวิธีที่ปลอดภัยสำหรับการสร้างและแจกจ่ายกุญแจเข้ารหัสระหว่างสองฝ่ายบนเครือข่ายออปติคัล” ดร. แอนดรูว์ ชีลด์ส ผู้ช่วยกรรมการผู้จัดการ ห้องปฏิบัติการวิจัยของโตชิบาในเคมบริดจ์ กล่าว “ด้วยคุณสมบัติที่คาดเดาสถานะไม่ได้ของอนุภาคอย่าง อิเล็คตรอน หรือ โฟตอน วิทยาการเข้ารหัสเชิงควอนตัมจึงสามารถนำมาใช้สุ่มตัวเลขสำหรับการใช้งานเข้ารหัสต่างๆ นอกจากนี้ การส่งกระแสข้อมูลของโฟตอนเดี่ยวแบบเข้ารหัสผ่านเครือข่ายการสื่อสารแบบออปติคัล ก็จะทำให้สามารถส่งต่อกุญแจดิจิทัลเพื่อไขรหัสและตรวจสอบข้อมูลได้”

เพราะเหตุใดการเข้ารหัสเชิงควอนตัมจึงเป็นที่ต้องการในปัจจุบัน และอนาคต

ทุกวันนี้การเข้ารหัสกุญแจสาธารณะถือเป็นส่วนสำคัญของการรักษาความปลอดภัยของข้อมูล แต่วิธีการนี้กำลังพบเจออุปสรรคจากกลยุทธ์การโจมตีรูปแบบใหม่ ๆ รวมถึงวิวัฒนาการของคอมพิวเตอร์ควอนตัมที่สุดท้ายแล้วจะทำให้เทคโนโลยีการเข้ารหัสส่วนใหญ่ในปัจจุบันไม่ปลอดภัยอีกต่อไป ความท้าทายที่เกิดขึ้นในปัจจุบันนี้ และความกังวลในอนาคตเกี่ยวกับความปลอดภัยของข้อมูลเป็นสิ่งที่ขับเคลื่อนให้เกิดการนำบริการและวิธีการเข้ารหัสควอนตัมที่เชื่อถือได้มาใช้งาน เพื่อการรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพยิ่งขึ้น

และนั่นส่งผลให้มีการคาดการณ์ว่ามูลค่าตลาดของวิทยาการเข้ารหัสเชิงควอนตัมทั่วโลกจะเติบโตจาก 285.7 ล้านเหรียญดอลล่าร์สหรัฐฯในปี 2017 ขึ้นไปสู่ 943.7 ล้านเหรียญในปี 2022 หรือคิดเป็นอัตราการเติบโตเฉลี่ย 27% ต่อปี อย่างไรก็ตาม การเข้ารหัสเชิงควอนตัมก็ยังไม่เป็นที่รู้จักหรือมีการใช้งานอย่างแพร่หลายในสายงานที่เกี่ยวข้อง ซึ่งแน่นอนว่าจุดนี้ไม่ได้ทำให้คุณค่าหรือความจำเป็นของมันลดลงแต่อย่างใด โดยเฉพาะเมื่อเรากำลังก้าวเข้าสู่ยุคควอนตัม

แต่คำถามคือ อีกนานเท่าไรเราจึงจะได้ใช้การเข้ารหัสเชิงควอนตัม และต้องมีการดำเนินการอย่างไรบ้างเพื่อไปถึงจุดนั้น

เมื่อไรวิทยาการนี้จะเข้าสู่กระแสหลัก

แม้ว่าจะยังไม่ได้มีวางจำหน่ายทั่วไป แต่ตอนนี้นักวิทยาศาสตร์ก็สามารถนำเทคโนโลยีการเข้ารหัสเชิงควอนตัมมาปรับใช้เพื่อแสดงให้เห็นถึงคุณประโยชน์ของมันได้แล้ว โดยเมื่อเร็ว ๆ นี้ ห้องปฏิบัติการวิจัยของโตชิบาในเคมบริดจ์ได้ตีพิมพ์เอกสารทางวิชาการที่บรรยายถึงความสำเร็จในการใช้เกณฑ์วิธีที่เรียกว่า Twin-Field QKD ในการขยายพิสัยการแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัม (Quantum Key Distribution: QKD) ได้มากกว่า 500 กิโลเมตรผ่านเส้นใยโทรคมนาคมมาตรฐาน

“มันเป็นการเปิดโอกาสให้เกิดการติดต่อสื่อสารอย่างปลอดภัยข้ามเมืองใหญ่อย่างระหว่างลอนดอน ปารีส ดับลิน แมนเชสเตอร์ หรืออัมสเตอร์ดัมได้ นอกจากนี้ยังมีโครงการความร่วมมือใหญ่ ๆ อีกมากมาย เช่น โครงการ Innovate UK EQUIP และโปรแกรม Horizon 2020 ของคณะกรรมาธิการสหภาพยุโรปที่กำลังพัฒนาเทคโนโลยีซึ่งจะทำให้การแจกจ่ายกุญแจเข้ารหัสเชิงควอนตัมกลายเป็นเครื่องมือที่องค์กรธุรกิจสามารถเข้าถึงและใช้ประโยชน์จากมันได้” ดร. ชีลด์ส กล่าวเสริม

นอกเหนือจากความต้องการด้านความปลอดภัยในการส่งต่อข้อมูลระหว่างจุด A ไปยังจุด B ของผู้ที่ทำงานในสายไอทีแล้ว การเปลี่ยนแปลงตัวบทกฎหมายเพื่อบังคับให้ข้อมูลส่วนบุคคลถูกจัดเก็บอย่างปลอดภัยก็เป็นเรื่องสำคัญเช่นกัน ซึ่งข้อกำหนดการป้องกันข้อมูลทั่วไป (General Data Protection Regulation: GDPR) เป็นตัวอย่างที่ดีในกรณีนี้ โดยเฉพาะอย่างยิ่งในเวลานี้ที่ภัยคุกคามในโลกไซเบอร์มีความหลากหลายและเพิ่มมากขึ้นเรื่อย ๆ อีกทั้งการดูแลความปลอดภัยของข้อมูลก็เป็นเรื่องยุ่งยาก จึงจำเป็นอย่างยิ่งที่จะต้องมีมาตรการใหม่ในการป้องกันการรั่วไหลของข้อมูล ซึ่ง QKD ถือเป็นเครื่องมือสำคัญในการช่วยให้มั่นใจได้ว่าข้อมูลของเราจะได้รับการป้องกันและดูแลรักษาอย่างปลอดภัย

แผนการในอนาคต
การเข้ารหัสเชิงควอนตัมเป็นเทคโนโลยีที่มีศักยภาพสูงที่จะเข้ามาเป็นหัวใจหลักของการปกป้องดูแลโครงสร้างพื้นฐานในการติดต่อสื่อสารจากการถูกโจมตีทางไซเบอร์ และยังช่วยให้ธุรกิจนำหน้าไปอีกขั้นในการดูแลข้อมูลการ

ดำเนินงานที่สำคัญ การเข้ารหัสเชิงควอนตัมนั้นต่างจากวิธีการรักษาความปลอดภัยแบบอื่นที่มีอยู่ในตอนนี้ตรงที่มันสามารถรักษาความปลอดภัยได้จากการโจมตีทุกรูปแบบทางคณิตศาสตร์และคอมพิวเตอร์ รวมทั้งจากความสามารถในการคำนวณตัวเลขของคอมพิวเตอร์ควอนตัมได้อีกด้วย

แต่ก่อนที่การเข้ารหัสเชิงควอนตัมจะสามารถนำมาใช้ในเชิงพาณิชย์ เกณฑ์วิธี QKD จะต้องถูกทำให้มีมาตรฐานเสียก่อน ต้องทำให้เทคโนโลยีต่าง ๆ สามารถทำงานร่วมกันได้ และจะต้องมีการพัฒนาตลาดส่วนประกอบ รวมไปถึงกรรมวิธีและเทคโนโลยีให้เติบโตยิ่งขึ้น เพื่อช่วยลดค่าใช้จ่ายในการสร้างและนำมาใช้งาน ซึ่งจะทำให้การใช้งานบนโลกออนไลน์ของเราทุกคนมีความปลอดภัยยิ่งขึ้นในอนาคต