แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ 2019 จบ

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

และสุดท้าย แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศในมุมของประเทศไทยจากงาน Cyber Defense Initiative Conference (CDIC) 2018 ช่วงปลายปีที่ผ่านมา โดย อ.ปริญญา หอมเอนก ประธาน และผู้ก่อตั้ง ACIS ระบุว่า ประเด็นสำคัญในปัจจุบัน คือ การทำ Digital Transformation หรือหมายถึงการผสานรวมเทคโนโลยีดิจิทัลเข้ากับทุกส่วนของธุรกิจ ซึ่งจะก่อให้เกิดการเปลี่ยนแปลงพื้นฐาน ทั้งในด้านการดำเนินธุรกิจ และการส่งมอบมูลค่า และบริการให้แก่ลูกค้า นั้นจริงๆ แล้วไม่ใช่เพียงแค่เรื่องที่ต้องดำเนินการในด้านเทคโนโลยีเท่านั้น แต่เป็นเรื่องทางรูปแบบ และกระบวนการดำเนินธุรกิจโดยตรง ต้องมีการหารือวางแผน และกำหนดแนวทางการดำเนินงานร่วมกันทุกฝ่าย ซึ่งเทคโนโลยีจะมีหน้าที่คอยสนับสนุนให้การดำเนินงานดังกล่าวมีประสิทธิภาพสูงสุด ดังนั้น การที่องค์การจะทำเรื่อง Digital Transformation ให้ประสบความสำเร็จจะต้องเริ่มที่นโยบายจากคณะผู้บริหาร และอาศัยความร่วมมือจากทุกๆ คนในองค์การ

โดย อ.ปริญญา หอมเอนก ได้สรุปแนวโน้มภัยคุกคามในปี 2019 ดังนี้

- การโจมตีแบบ State-sponsored Attack หรือการโจมตีทางไซเบอร์ที่มีหน่วยงานภาครัฐของประเทศคอยให้การสนับสนุนปฏิบัติการนั้นจะมีแนวโน้มเพิ่มขึ้น ซึ่งไม่ได้มีวัตถุประสงค์เพื่อสร้างความเสียหาย แต่ใช้เพื่อสร้างความพร้อมในการรับมือ และโจมตีตอบโต้ระหว่างประเทศเมื่อเกิดสถานการณ์
- GDPR และกฎหมายคุ้มครองข้อมูลส่วนบุคคลจะถูกบังคับใช้ และมีบทบาทมากขึ้นอย่างต่อเนื่อง อาจจะได้เห็นหลายๆ ประเทศเริ่มบังคับใช้กฎหมายดังกล่าวอย่างจริงจังในปี 2019
- หลายองค์การจะให้ความสำคัญกับการทำ Incident Management หรือการบริหารจัดการเมื่อเผชิญเหตุการณ์ โดยจะสามารถวางแผนการดำเนินการได้เหมาะสมสอดคล้องต่อการปรับตัวขององค์การภายใต้แนวคิด Cyber Resilience คือ ความสามารถในการรองรับความเปลี่ยนแปลง และทนต่อการถูกโจมตีทางไซเบอร์ขององค์การ
- Data Breach หรือการถูกละเมิดสิทธิ์ในข้อมูลจะเกิดมากขึ้นจากการใช้บริการบนระบบ Cloud เนื่องจากไม่มีมาตรการควบคุมที่เหมาะสม และรัดกุมจากผู้ให้บริการ
- การโจมตีที่มาจาก email ในรูปแบบเดิมๆ ยังคงเป็นการโจมตีที่เกิดขึ้นอย่างต่อเนื่อง และมีจำนวนมากที่สุด
- การพิสูจน์หรือยืนยันตัวตนแบบปัจจัยเดียวจะลดน้อยลง เปลี่ยนไปเป็นแบบสองปัจจัย หรือแบบหลายปัจจัยมากขึ้น

- อุปกรณ์ internet of thing จะตกเป็นเป้าหมายของการโจมตีมากขึ้น
- ปัญญาประดิษฐ์ หรือ AI (Artificial Intelligence) จะช่วยสนับสนุนให้สามารถรับมือต่อภัยคุกคามได้อย่างมีประสิทธิภาพยิ่งขึ้น แต่ในขณะเดียวกัน ผู้ไม่ประสงค์ดีก็สามารถนำ AI มาใช้เพื่อช่วยให้การโจมตีประสบผลสำเร็จได้มากยิ่งขึ้นเช่นกัน
- เรื่องอื้อฉาว การกลั่นแกล้ง การเปิดเผยข้อมูล การละเมิดสิทธิ์ และการฟ้องร้อง จะเกิดมากขึ้นซึ่งเป็นเหตุมาจากการใช้สื่อออนไลน์บน Social media โดยจะค่อนข้างรุนแรงส่งผลกระทบเป็นวงกว้าง
- องค์การจะไม่ได้ทำแค่ Digital Transformation แต่จะดำเนินการเรื่อง Cybersecurity Transformation ควบคู่ไปด้วย

นอกจากนี้ ในงานสัมมนาดังกล่าวได้มีการนำเสนอความก้าวหน้าในการจัดทำแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดย พลโทเจิดวุธ คราประยูร รองผู้บัญชาการสถาบันวิชาการป้องกันประเทศ กองบัญชาการกองทัพไทย แผนดังกล่าวเป็นแผนยุทธศาสตร์ระยะ 20 ปี ซึ่งกำลังจัดทำโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม โดยจะใช้หลักของ Comprehensive Security หรือความมั่นคงปลอดภัยต้องครอบคลุมทุกมิติ ไม่ว่าจะเป็นด้านสังคม เทคโนโลยี สภาพแวดล้อม เศรษฐกิจ การเมือง และการทหาร รวมไปถึงมีการประเมินช่องโหว่ และภัยคุกคามเป็นหัวใจสำคัญ รวมถึง พ.ต.อ.ญาณพล ยั่งยืน กรรมการผู้ทรงคุณวุฒิด้านการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศและการสื่อสาร ได้ออกมาพูดถึงร่าง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ ของไทยแสดงให้เห็นถึงการเตรียมความพร้อมของประเทศไทยเพื่อรับมือกับภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ

โดยสรุปแล้ว จากรายงานสำคัญเกี่ยวกับแนวโน้มภัยคุกคามทางด้านเทคโนโลยีสารสนเทศ และจากบทสรุปจากงานสัมมนาด้านความปลอดภัยไซเบอร์ของไทยจะเห็นได้ว่า ความเสี่ยงที่องค์การต้องรับมือต่อจากนี้จะประกอบไปด้วย

- การใช้งาน Cloud ที่ต้องให้ความสำคัญกับรายละเอียดด้านการรักษาความมั่นคงปลอดภัยของผู้ให้บริการ

- การปรับกระบวนการขององค์การเพื่อรองรับการเปลี่ยนแปลง ในเชิงนโยบาย ข้อกำหนด วิธีปฏิบัติที่ต้องละเอียดรอบคอบรัดกุมเพราะความเสี่ยงจะเกิดจากตัวบุคคล ที่จะสร้างความเสียหายต่อตนเองและองค์การ การเฝ้าติดตามพฤติกรรมเสี่ยง และการให้ความรู้สร้างความเข้าใจ
- การปรับปรุงกระบวนการยืนความถูกต้อง ยืนยันตัวตนให้เหมาะสม ใช้ข้อมูลยืนยันแบบหลายปัจจัย
- การปรับตัวเตรียมพร้อมรองรับกฎหมายที่เกี่ยวข้องทั้งในและระหว่างประเทศ
- การวางแผนในการใช้งานเทคโนโลยีใหม่ๆ เพื่อนำมาสนับสนุนการบริหารจัดการภายในองค์การ รวมถึงเสริมสร้างประสิทธิภาพในการทำธุรกิจ และระหว่างคู่ค้าพันธมิตร อาทิ เทคโนโลยี AI อุปกรณ์ IoT เป็นต้น
- การเตรียมความพร้อมรองรับสถานการณ์ไม่พึงประสงค์ มีการกำหนดกระบวนการ ขั้นตอน แผนงาน ผู้รับผิดชอบ กลไก และเทคโนโลยีที่ใช้เพื่อทำการสำรอง กู้คืนข้อมูล และระบบที่มีความรัดกุมเหมาะสมกับสถานการณ์

เหล่านี้ คือประเด็นที่องค์การควรให้ความสำคัญ และตระหนักถึงความเสียหายที่อาจเกิดขึ้นจากการโจมตีไซเบอร์ ซึ่งไม่รู้ว่าเมื่อไหร่องค์การของเราจะตกเป็นเป้าหมายของการโจมตีที่เกิดขึ้นอย่างรวดเร็วเพียงระยะไม่กี่วินาที แต่สร้างความเสียหายที่อาจรุนแรงส่งผลต่อการดำเนินงานของทั้งองค์การ ซึ่งนี่อาจจะเพิ่งเริ่มต้น เนื่องจากยังอยู่ในยุคที่ทุกองค์การเริ่มทำ Digital Transformation และเมื่อไหร่ที่ Digital ได้ Transformation เสร็จแล้ว ทุกส่วนในกระบวนการทางธุรกิจขององค์การอาจจะต้องพึ่งพาการทำงานของเทคโนโลยีไปโดยปริยาย การเชื่อมต่อเกิดขึ้นกับทุกส่วนงาน ซึ่งก็อาจหมายถึงเป้าหมายการโจมตีถูกทำให้กว้างขึ้น และทำได้ง่ายขึ้น ดังนั้นการรักษาความมั่นคงปลอดภัยหรือแม้แต่การเปลี่ยนผ่านที่เหมาะสมอาจจะเป็นสิ่งที่องค์การต้องเลือกปฏิบัติอย่างหลีกเลี่ยงไม่ได้ในโลกของธุรกิจที่ต้องเชื่อมต่อ หลายองค์การอาจจะคิดเล่นๆ ว่า ในยุคสมัยแบบนี้ ถ้าสามารถถอดเอาหัวใจสำคัญของธุรกิจไปวางไว้ในที่ที่ปลอดภัยได้เหมือนไมยราพหรือทศกัณฑ์ได้ก็คงดี TPA news

ข้อมูลอ้างอิง

- Top 10 Cybersecurity Risks For 2019, United States Cyber Security Magazine
- 2019 Cyber Security Risk Report, Aon
- Risk in Focus 2019 report, European Confederation of Institutes of Internal Auditing's (ECIIA)
- Cyber Defense Initiative Conference (CDIC) 2018, www.techtalkthai.com