# แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ 2019

วิชย์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

### ■ รหัสผ่านปัจจัยเดียว

ในปี 2019 ด้วยเทคโนโลยีการยืนยันหรือระบุตัวตนที่มีการพัฒนาต่อเนื่อง อาจจะหมดยุคของการใช้รหัสผ่านเพียงอย่างเดียวในการยืนยันตัวตน การใช้รหัสผ่านเพียงปัจจัยเดียวคือความเสี่ยงด้านความปลอดภัยที่องค์การควรให้ความสำคัญ เนื่องจากมันจะช่วยให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูลได้ง่าย ดังนั้น องค์การจะต้องให้ความสำคัญกับการใช้งานรหัสผ่าน ซึ่งข้อแนะนำคือการใช้การยืนยันตัวตนหรือรับรองความถูกต้องแบบหลายปัจจัยจะเป็นวิธีที่ดีที่สุดในการดำเนินการ โดยปัจจุบันมีหลายทางเลือกให้ใช้งาน อาทิ เสียง ลายนิ้วมือ การจดจำลักษณะทางกายภาพของใบหน้า เป็นต้น

### ■ ภัยคุกคามจากภายใน

องค์การต่างๆ จะยังคงเผชิญกับภัยคุกคามจากภายในเนื่องจากการละเมิดความปลอดภัยทางไซเบอร์ที่สำคัญ นั้นส่วนใหญ่เกิดจากผู้ใช้งานในองค์การ รวมถึงบุคลากรที่เคยร่วมงานกับองค์การก็ถือเป็นภัยคุกคามที่สำคัญต่อความปลอดภัยทางไซเบอร์ การแก้ปัญหานี้คือการที่ต้องให้ความรู้แก่บุคลากร การตรวจสอบกิจกรรมสุ่มเสี่ยงต่างๆ ซึ่งอาจจะดำเนินการโดยใช้ระบบแบบอัตโนมัติ และการออกมาตรการควบคุมที่มีความรัดกุม

### ■ การสำรอง และกู้คืนข้อมูล

ความเสี่ยงของการสูญหายของข้อมูลในขั้นตอนการสำรองข้อมูล และกู้คืนข้อมูลนั้น องค์การส่วนใหญ่ไม่ค่อยได้ให้ความสำคัญหรือมีตรวจสอบที่จริงจังมากเท่าใดนัก ยิ่งกว่านั้นยังไม่มีการควบคุมผู้ที่เข้าถึงข้อมูล ทำให้องค์การเสี่ยงต่อการถูกโจมตีด้วยผู้ไม่ประสงค์ดี เพื่อลดความเสี่ยงนี้องค์การต้องกลับมาให้ความสำคัญกับกระบวนการการสำรอง และกู้คืนข้อมูลอย่างจริงจัง ร่วมด้วยการให้ความรู้สร้างความเข้าใจ และตระหนักแก่บุคลากรที่เกี่ยวข้อง

จากการประเมินของ United States Cyber security Magazine ข้างต้น สามารถสรุปได้ว่าในปี 2019 ภัยคุกคาม ในมุมมองของ United States Cyber security Magazine ที่อ้างอิงจากรายงานของ CISCO นั้น จะเน้นไปที่ว่า องค์การส่วนใหญ่มีการใช้

บริการระบบ Cloud จำเป็นต้องวิเคราะห์ และประเมินความเสี่ยงจากการใช้บริการดังกล่าว รวมถึงให้ความสำคัญกับระบบรักษาความปลอดภัยไซเบอร์ และความรับผิดชอบของผู้ให้บริการ นอกจากนี้จะเป็นเรื่องของการที่ต้องมีการออกมาตรการหรือกลไกในการควบคุมการใช้งานอุปกรณ์พกพา อุปกรณ์ Internet of thing กลไกการเข้าถึงด้วยการยืนยันตัวตนแบบหลายปัจจัย การติดตามกิจกรรมที่สุ่มเสี่ยงของบุคลากรในองค์การ และการให้ความสำคัญต่อกระบวนการสำรอง และกู้คืนข้อมูล เพราะสิ่งเหล่านี้จะนำไปสู่ความเสี่ยงทางไซเบอร์ที่จะส่งผลเสียต่อองค์การ

รายงานฉบับต่อมาเป็นการประเมินของ Aon องค์การที่ปรึกษาชั้นนำระดับโลกที่มีความเชี่ยวชาญในการวิเคราะห์และประเมินความเสี่ยงให้กับองค์การต่างๆ โดย Aon ได้ทำการวิเคราะห์และสรุปเป็นรายงาน “-2019 Cyber Security Risk Report” ซึ่งมีประเด็นความเสี่ยง 8 เรื่องดังนี้

## 1. เทคโนโลยี

เทคโนโลยีที่พัฒนาขึ้นในปัจจุบันได้เปลี่ยนแปลงวิธีการที่องค์การใช้ดำเนินธุรกิจ เกิดการใช้เทคโนโลยีในวงกว้างและกว้างขึ้นเรื่อยๆ นำมาซึ่งความเสี่ยง และจุดอ่อน ทุกองค์การในทุกๆ อุตสาหกรรมกำลังเผชิญกับการพัฒนารูปแบบบริการและธุรกิจใหม่ๆ อย่างไรก็ตามโอกาสเหล่านี้นำมาซึ่งความเสี่ยงที่แตกต่างกันอย่างรุนแรงซึ่งองค์การจะต้องคาดการณ์ และจัดการเมื่อดำเนินการตามกระบวนการเปลี่ยนแปลงดิจิทัลที่เกิดขึ้นต่อไป

## 2. ห่วงโซ่อุปทาน

ความเสี่ยงที่เกิดจากห่วงโซ่อุปทานที่มีอยู่สองประการ ประการที่หนึ่งคือการขยายตัวอย่างรวดเร็วของข้อมูลการดำเนินงานที่เชื่อมโยงระหว่างคู่ค้า ผู้ให้บริการ ลูกค้า อาจถูกเปิดเผยผ่านการใช้งานผ่านอุปกรณ์พกพาด้วยเทคโนโลยีต่างๆ ที่เกี่ยวข้อง หากไม่ได้มีมาตรการควบคุมที่รัดกุม และเหมาะสม ประการที่สองคือการที่องค์การต่างๆ ให้ความไว้วางใจต่อบุคคลที่สามหรือแม้กระทั่งบุคคลที่สี่ที่เป็นผู้ขาย และผู้ให้บริการมากขึ้น ซึ่งแนวโน้มทั้งสองจะนำมาซึ่งการเปิดช่องโหว่ในห่วงโซ่อุปทาน องค์การจำเป็นต้องบริหารความเสี่ยงอย่างเหมาะสมเพื่อที่จะรักษาไว้ซึ่งการดำเนินธุรกิจที่เชื่อถือได้และมีศักยภาพ

## 3. IoT

อุปกรณ์ IoT หรือ internet of thing ในที่ทำงานอาจจะสร้างให้เกิดความเสี่ยงขึ้น องค์การหลายแห่งยังไม่ได้มีการจัดการอย่างปลอดภัย แม้กระทั่งการใช้อุปกรณ์ IoT กับสินค้าคงคลังก็อาจส่งผลให้เกิดช่องโหว่ได้ อย่างไรก็ตามจำนวนการใช้งานอุปกรณ์ IoT ขององค์การต่างๆ ก็มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องเพราะสามารถนำมา

ใช้เพิ่มประสิทธิภาพในการบริหารจัดการได้อย่างมีประสิทธิภาพ ดังนั้น องค์การควรมีกำหนดกระบวนการตรวจสอบความปลอดภัยในการใช้งาน และขั้นตอนปฏิบัติที่เหมาะสม โดยต้องดำเนินการอย่างต่อเนื่องเพื่อลดช่องโหว่ที่อาจเกิดขึ้นจากการใช้งานอุปกรณ์ IoT

## 4. การดำเนินธุรกิจ

การเชื่อมต่อกับ internet นั้น ช่วยปรับปรุงประสิทธิภาพของส่วนงานปฏิบัติการได้เป็นอย่างมาก แต่ทว่าการเชื่อมต่อ internet ที่เพิ่มมากขึ้นก็อาจนำไปสู่ช่องโหว่ด้านความปลอดภัยใหม่ๆ ขอบเขตการโจมตีทางไซเบอร์ก็จะขยายขนาดอย่างต่อเนื่อง โดยเมื่อเกิดการเชื่อมต่อเพิ่มขึ้นทำให้ผู้ไม่ประสงค์ดีสามารถเลือกโจมตีได้หลากหลายทั่วทั้งเครือข่ายขององค์การ นอกจากนี้กระบวนการสำรองข้อมูลที่ไม่มีประสิทธิภาพก็อาจสร้างผลกระทบจากการโจมตีทางไซเบอร์ได้เช่นกัน องค์การจึงต้องมีความตระหนัก และเตรียมพร้อมสำหรับผลกระทบจากการเชื่อมต่อที่เพิ่มขึ้นนี้

## 5. บุคลากร

บุคลากรยังคงเป็นหนึ่งในสาเหตุที่พบมากที่สุดของการละเมิดสิทธิ์การเข้าถึงข้อมูล และความปลอดภัยไซเบอร์ขององค์การ ถึงแม้องค์การจะมีการสร้างความตระหนักถึงภัยคุกคาม แต่บุคลากรบางส่วนก็ยังมีพฤติกรรมเสี่ยงต่อความมั่นคงปลอดภัยซึ่งส่งผลกระทบต่อทั้งองค์การ จึงเป็นสิ่งจำเป็นสำหรับองค์การที่จะกำหนดวิธีการที่ครอบคลุมเพื่อลดความเสี่ยงจากการใช้ข้อมูลภายในรวมถึงการกำกับดูแลข้อมูลที่เข้มแข็ง รวมถึงนโยบายในการการสื่อสารประชาสัมพันธ์องค์การ สินค้า และบริการผ่านทางโลกไซเบอร์ และการป้องกันข้อมูลสำคัญ

อ่านต่อฉบับหน้า