ฟอร์ซพอยต์ เผย การคาดการณ์ความปลอดภัยบนไซเบอร์ประจำปี 2562 การสื่อสารร่วมกันได้อย่างวางใจ คือหัวใจของการขับเคลื่อนนวัตกรรมและการเติบโต ให้องค์กรธุรกิจ และรัฐบาล

ผู้เชี่ยวชาญด้านไซเบอร์ และทีมวิจัย เตือนภัยถึงความเสี่ยงในระบบโครงสร้างพื้นฐานสำคัญและแหล่งข้อมูลของชาติ รวมถึงภัยคุกคามการระบุตัวตนทางชีวภาพ และความเสี่ยงจากการเชื่อมั่น AI ในระบบรักษาความปลอดภัยบนไซเบอร์มากเกินไป

ฟอร์ซพอยต์ Forcepoint ผู้นำระดับโลกด้านการรักษาความปลอดภัยบนไซเบอร์ เผยผลรายงานเกี่ยวกับการคาดการณ์ความปลอดภัยบนไซเบอร์ของฟอร์ซพอยต์ ประจำปี 2562 (2019 Forcepoint Cybersecurity Predictions Report) ซึ่งผู้เชี่ยวชาญด้านการรักษาความปลอดภัย นักวิจัยที่มีความรอบรู้เกี่ยวกับพฤติกรรมการใช้งาน และนักวิทยาศาสตร์ข้อมูล ต่างชี้แนะแนวทางการรับมือให้กับองค์กรที่อาจต้องเผชิญกับภัยคุกคามซึ่งมีความซับซ้อนในอีกไม่กี่เดือนข้างหน้า

รายงานดังกล่าว ได้สำรวจใน 7 ประเด็นที่จะมีความเสี่ยงเพิ่มขึ้นในปี 2562 โดยผู้เชี่ยวชาญของฟอร์ซพอยต์ได้เจาะลึกถึงเทคโนโลยีที่เป็นแนวโน้ม รวมถึงปัจจัยที่ขับเคลื่อนอยู่เบื้องหลังการโจมตีบนไซเบอร์ เพื่อที่ผู้นำองค์กรธุรกิจและหน่วยงานภาครัฐฯ รวมถึงทีมงานด้านการรักษาความปลอดภัยขององค์กรเหล่านี้ จะได้เตรียมพร้อมในการเผชิญหน้ากับคลื่นลูกใหม่ของภัยคุกคาม ทั้งนี้องค์กรธุรกิจและภาครัฐบาล ต่างกำลังเผชิญกับโลกแห่งการควบรวมระบบงานหลายส่วนเข้าด้วยกัน (hyper-converged world) ซึ่งนอกจากจะทำให้ระบบงานต่างๆ ที่เชื่อมต่อกับข้อมูลสำคัญและสินทรัพย์ทางปัญญาตกอยู่ในความเสี่ยงแล้ว ยังรวมถึงความเสี่ยงในเรื่องความปลอดภัยทางกายภาพด้วยเช่นกัน โดยรายงานได้สำรวจประเด็นเหล่านี้ พร้อมกับให้ข้อสรุปว่าเมื่อใดก็ตามที่ผู้คนสามารถประสานความร่วมมือกันได้อย่างวางใจ รวมถึงสามารถใช้ข้อมูลผ่านเทคโนโลยีได้อย่างอิสระและสร้างสรรค์ เมื่อนั่นองค์กรธุรกิจก็จะสามารถคิดค้นนวัตกรรมที่สร้างคุณค่าได้อย่างมั่นใจ

“ทั้งอุตสาหกรรมด้านการรักษาความปลอดภัยบนไซเบอร์ และผู้โจมตี จะพยายามมากยิ่งขึ้น ในการดำเนินการโต้ตอบ หลบหลีกและป้องกันช่องโหว่ที่เกิดขึ้นอย่างไม่จบไม่สิ้น นับเป็นเกมแมวไล่จับหนูอย่างแท้จริง” นายแบรนดอน

แทน หัวหน้าทีมที่ปรึกษาด้านความปลอดภัย ประจำภาคพื้นเอเชียตะวันออกเฉียงใต้ ฟอร์ซพอยต์ กล่าว “เราต้องหนีจากเกมนี้ให้ได้ ซึ่งการวิจัยเกี่ยวกับการคาดการณ์เหล่านี้ นับเป็นการบังคับให้เราก้าวถอยหลังและมองผืนป่าทั้งหมดที่อยู่ท่ามกลางต้นไม้นับหลายล้านต้นในแบบภาพรวม ทั้งนี้มืออาชีพด้านการรักษาความปลอดภัยบนไซเบอร์และผู้นำธุรกิจ จำเป็นต้องปรับตัวให้เข้ากับการเปลี่ยนแปลงเพื่อรับมือกับความเสี่ยงที่มองเห็น เพื่อสร้างสิ่งดีๆ พร้อมทั้งหยุดเรื่องที่ไม่ดี”

การต่อกรกับการปฏิรูปทางดิจิทัล และความเชื่อมั่น
ผลรายงาน การคาดการณ์ความปลอดภัยบนไซเบอร์ของฟอร์ซพอยต์ประจำปี 2562 ได้สำรวจผลกระทบต่อธุรกิจที่เชื่อมั่นและให้ความไว้วางใจในผู้ให้บริการคลาวด์ รวมถึงผลกระทบจากความเชื่อมั่นของผู้ใช้ปลายทางเรื่องการรักษาความปลอดภัยของข้อมูลส่วนตัวด้วยการใช้เทคโนโลยียืนยันตัวบุคคล (biometrics) และผลกระทบที่เกิดจากความไว้วางใจต่อกันเป็นทอดๆ ในห่วงโซ่ของการให้บริการที่เกี่ยวข้อง

ในการสำรวจลูกค้าของฟอร์ซพอยต์นั้น 94 เปอร์เซ็นต์ระบุว่าการรักษาความปลอดภัยเป็นประเด็นสำคัญที่สุดในการย้ายไปสู่ระบบคลาวด์ โดย 58 เปอร์เซ็นต์ กำลังมองหาผู้ให้บริการที่สามารถเชื่อถือและไว้วางใจได้จริงและเป็นผู้ที่มีชื่อเสียงด้านการรักษาความปลอดภัย โดย 31 เปอร์เซ็นต์ กำลังจำกัดปริมาณข้อมูลที่จะนำไปไว้บนคลาวด์เนื่องจากยังกังวลเรื่องความปลอดภัยอยู่

“วิธีการหนึ่งที่จะเพิ่มความเชื่อมั่นและควบคุมเรื่องความปลอดภัยได้ ก็คือการสร้างแบบจำลองพฤติกรรมผู้ใช้ หรือที่พิเศษไปกว่านั้น ก็คือการตรวจสอบอัตลักษณ์ทางดิจิทัลของผู้ใช้ เพื่อให้เข้าใจถึงเหตุและผลที่อยู่เบื้องหลังกิจกรรมต่างๆ” นายแบรนดอน กล่าว “การเข้าใจถึงรูปแบบการใช้งานผ่านเครือข่ายหรือในการใช้แอปพลิเคชัน สามารถระบุความผิดปกติทางพฤติกรรม ซึ่งจะช่วยให้มีข้อมูลในการตอบโต้เพื่อรับมือกับความเสี่ยงได้

การคาดการณ์จากฟอร์ซพอยต์ใน 7 ประเด็น ที่สุ่มเสี่ยงในปี 2562
ประเด็นที่น่าจับตามองในรายงานปีนี้ มีดังต่อไปนี้
• การขับเคลื่อนไปสู่เอดจ์ หรือปลายทางเครือข่าย
ผู้บริโภคต่างเหนื่อยใจกับช่องโหว่และการละเมิดข้อมูลส่วนตัวที่ถูกนำไปใช้ในทางที่ผิด เรื่องนี้นำไปสู่ผลก็คือองค์กรต้องเสนอวิธีการใหม่ที่ช่วยปกป้องความเป็นส่วนตัวในบริการที่นำเสนอ โดยเอดจ์ คอมพิวติ้ง จะช่วยให้ผู้บริโภคควบคุมข้อมูลส่วนตัวได้มากยิ่งขึ้น ด้วยการเก็บข้อมูลไว้ในสมาร์ทโฟน หรือแลปท็อป ซึ่งโซลูชันในปัจจุบันจะต้องทำให้ผู้บริโภคเชื่อมั่นได้ว่าข้อมูลจะไม่รั่วไหลไปบนคลาวด์ จึงนับว่าจะประสบความสำเร็จ

• เส้นทางการปะทะกันของสงครามเย็นบนไซเบอร์
การจารกรรมข้อมูล มักจะนำไปสู่ความตื่นตัวและทำให้ประเทศชาติมีการนำเทคโนโลยีใหม่มาใช้ แต่เนื่องจากโอกาสในการเข้าถึงข้อมูลอย่างชอบธรรมค่อยๆ ลดลง ด้วยเหตุผลในเรื่องของการปกป้องทางการค้า จึงทำให้ผู้ที่อยู่อีกฟากได้รับประโยชน์จากเรื่องนี้อย่างแท้จริง ด้วยการนำเทคโนโลยีมาใช้ในทางที่ไม่เหมาะสม ฉะนั้นองค์กรจะเก็บรักษา

ทรัพย์สินทางปัญญาให้พ้นมือของแฮกเกอร์ที่ฉวยโอกาสจากเรื่องนี้ได้อย่างไร?

• ฤดูที่หนาวเหน็บของปัญญาประดิษฐ์

ถ้าปัญญาประดิษฐ์ หรือ AI กำลังสร้างการรับรู้ด้วยตัวเองขึ้นมาใหม่ ปัญญาประดิษฐ์ในเรื่องการรักษาความปลอดภัยไซเบอร์จะทำได้จริงหรือไม่? ผู้โจมตีจะหาประโยชน์อย่างไรจากการชะลอการระดมทุนของ AI? การที่เราเชื่อมั่นในขั้นตอนวิธีการ (algorithms) และการวิเคราะห์เพื่อนำร่องยานยนต์ได้อย่างสำเร็จ เพื่อให้มุมมองเชิงลึกที่นำไปสู่การตัดสินใจด้านการดูแลสุขภาพ และเพื่อแจ้งเตือนมืออาชีพด้านการรักษาความปลอดภัยถึงความเป็นไปได้ที่จะเกิดเหตุการณ์ที่ทำให้ข้อมูลสูญหาย เรื่องเหล่านี้ให้ความเชื่อมั่นได้มากน้อยแค่ไหน? ผู้จำหน่ายจะอ้างถึงประสิทธิภาพของ AI ที่ขัดกับข้อเท็จจริงเรื่องการโจมตีบนไซเบอร์ด้วยวิธีการซับซ้อนได้อย่างไร?

• ภาพสะท้อนการปลอมแปลง

การโจมตีแบบฟิชชิ่งยังคงดำเนินต่อไปอย่างไม่ลดละ กลเม็ดของแฮกเกอร์ เช่น “การเปลี่ยนซิม” ทำลายประสิทธิภาพในการยืนยันตัวตนผู้ใช้งาน 2 ขั้นตอน หรือ 2FA (two-factor authentication) เช่นการส่งข้อความยืนยันกลับมาที่ผู้ใช้งาน ซึ่งการยืนยันด้วยไบโอเมทริกซ์ หรืออัตลักษณ์เฉพาะของผู้ใช้ จะช่วยเสริมความปลอดภัยได้อีกชั้น ด้วยการยืนยันด้วยข้อมูลที่มีความเฉพาะตัวยิ่งขึ้นสำหรับผู้ใช้แต่ละราย แต่ช่องโหว่ใหม่ๆ ที่พบในซอฟต์แวร์ระบบจดจำใบหน้า ทำให้ผู้เชี่ยวชาญหันมาเชื่อใจในการยืนยันด้วยลักษณะทางพฤติกรรม

ดาวน์โหลดรายงานฉบับเต็ม เพื่อดูรายละเอียดทั้งหมดเกี่ยวกับธีมการคาดการณ์ทั้ง 7 ประเด็นของฟอร์ซพอยต์ รวมถึงผลกระทบจากการคาดการณ์ในปี 2562

ข้อมูลเกี่ยวกับรายงานการคาดการณ์ความปลอดภัยบนไซเบอร์ของฟอร์ซพอยต์ ประจำปี 2562

• 2019 Forcepoint Cybersecurity Predictions Report
• Summary blog มีรายละเอียดเกี่ยวกับการคาดการณ์ทั้งหมด
• Scorecard ของการคาดการณ์ความปลอดภัยบนไซเบอร์ในปี 2561