ข่าว+ภาพอินโฟกราฟฟิก –> ซิสโก้รายงานผลสำรวจไซเบอร์ซีเคียวริตี้ประจำปี 2560 ชี้ วิธีการโจมตีแบบเก่าเริ่มกลับมาอีกครั้ง

ซิสโก้รายงานผลสำรวจไซเบอร์ซีเคียวริตี้ประจำปี 2560 ผู้บริหารเปิดเผยต้นทุนที่แท้จริงของการคุกคามความปลอดภัย และมาตรการแก้ไข

รายงานฉบับปีที่ 10 นี้ชี้ วิธีการโจมตีแบบเก่าเริ่มกลับมาอีกครั้ง
ซิสโก้ลด “ระยะเวลาตรวจจับ” เหลือ 6 ชั่วโมง

กรุงเทพฯ, 15 กุมภาพันธ์ 2560 – รายงานไซเบอร์ซีเคียวริตี้ (Annual Cybersecurity Report – ACR) ประจำปี 2560 ของซิสโก้ (NASDAQ: CSCO) ระบุว่า กว่าหนึ่งในสามขององค์กรที่ประสบปัญหาการละเมิดระบบรักษาความปลอดภัยในปี 2559 รายงานถึงการสูญเสียลูกค้า โอกาส และรายได้มากกว่า 20 เปอร์เซ็นต์ และหลังจากที่ถูกโจมตี 90 เปอร์เซ็นต์ขององค์กรเหล่านี้กำลังปรับปรุงเทคโนโลยีและกระบวนการป้องกันภัยคุกคาม โดยเป็นการดำเนินการของฝ่ายไอทีและฝ่ายรักษาความปลอดภัย (38 เปอร์เซ็นต์), เพิ่มการฝึกอบรมเพื่อสร้างจิตสำนึกเรื่องความปลอดภัยสำหรับพนักงาน (38 เปอร์เซ็นต์) และปรับใช้เทคนิคป้องกันความเสี่ยง (37 เปอร์เซ็นต์) รายงานฉบับนี้สำรวจความคิดเห็นของประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัย (Chief Security Officer – CSO) และผู้บริหารฝ่ายปฏิบัติการด้านการรักษาความปลอดภัย เกือบ 3,000 คน จาก 13 ประเทศ ภายใต้การศึกษาเรื่องความสามารถด้านการรักษาความปลอดภัย (Security Capabilities Benchmark Study) ซึ่งเป็นส่วนหนึ่งของรายงานไซเบอร์ซีเคียวริตี้ของซิสโก้

รายงานฉบับปีที่ 10 นี้เน้นย้ำถึงความท้าทายและโอกาสสำหรับทีมงานรักษาความปลอดภัยในการรับมือกับพัฒนาการที่ไม่หยุดยั้งของอาชญากรรมทางไซเบอร์และวิธีการโจมตีที่เปลี่ยนไป ผู้บริหาร CSO ระบุว่าข้อจำกัดด้านงบประมาณ ความเข้ากันไม่ได้ของระบบต่างๆ และการขาดแคลนบุคลากรที่มีความเชี่ยวชาญ ถือเป็นอุปสรรคสำคัญที่สุดในการปรับปรุงขีดความสามารถด้านการรักษาความปลอดภัย นอกจากนี้ ผู้บริหารยังเปิดเผยว่าฝ่ายรักษาความปลอดภัยได้เพิ่มสภาพแวดล้อมที่ซับซ้อนมากยิ่งขึ้น โดย 65 เปอร์เซ็นต์ขององค์กรใช้ผลิตภัณฑ์ด้านการรักษาความปลอดภัยมากกว่า 50 ผลิตภัณฑ์ ซึ่งอาจก่อให้เกิดช่องว่างเพิ่มมากขึ้นในด้านประสิทธิภาพการรักษาความปลอดภัย ข้อมูลจากรายงาน ACR ชี้ให้เห็นว่า อาชญากรหันกลับมาใช้วิธีการโจมตีแบบ “เก่า” เช่น แอดแวร์ และอีเมลสแปม

ในระดับที่เทียบเท่ากับเมื่อปี 2553 โดยอีเมลสแปมคิดเป็นสัดส่วนเกือบสองในสาม (65 เปอร์เซ็นต์) ของอีเมลทั้งหมด และ 8-10 เปอร์เซ็นต์ถูกระบุว่าเป็นอีเมลอันตราย จำนวนอีเมลสแปมทั่วโลกกำลังเพิ่มขึ้นอย่างต่อเนื่อง และโดยมากแล้วถูกแพร่กระจายโดยบ็อตเน็ต (Botnet) ขนาดใหญ่ที่เติบโตอย่างไม่หยุดยั้ง

การตรวจวัดประสิทธิภาพของมาตรการรักษาความปลอดภัยท่ามกลางการโจมตีเหล่านี้นับว่าเป็นเรื่องสำคัญอย่างยิ่ง ซิสโก้ได้ตรวจสอบติดตามความคืบหน้าในการลด “ระยะเวลาการตรวจจับ” (Time to Detection – TTD) ซึ่งหมายถึงช่วงเวลาระหว่างการโจมตีและการตรวจพบภัยคุกคาม ระยะเวลาการตรวจจับที่เร็วกว่าจะช่วยจำกัดพื้นที่ปฏิบัติการของผู้โจมตี และลดความเสียหายที่เกิดจากการบุกรุก ซิสโก้สามารถลดระยะเวลาการตรวจจับจากค่าเฉลี่ย 14 ชั่วโมงในช่วงต้นปี 2559 ให้เหลือเพียง 6 ชั่วโมงในช่วงครึ่งหลังของปีเดียวกัน ตัวเลขนี้อ้างอิงข้อมูลการตรวจวัดด้านความปลอดภัยที่เก็บรวบรวมจากผลิตภัณฑ์ด้านการรักษาความปลอดภัยของซิสโก้ที่ติดตั้งและใช้งานในองค์กรต่างๆ ทั่วโลก

ต้นทุนทางธุรกิจของภัยคุกคามทางไซเบอร์: สูญเสียลูกค้า สูญเสียรายได้

รายงาน ACR ประจำปี 2560 เปิดเผยถึงผลกระทบด้านการเงินจากโจมตีที่เกิดขึ้นกับธุรกิจ ตั้งแต่องค์กรขนาดใหญ่ไปจนถึงธุรกิจขนาดกลางและขนาดย่อม โดยมากกว่า 50 เปอร์เซ็นต์ขององค์กรถูกเฝ้ามองและตรวจสอบหลังจากที่เกิดปัญหาการละเมิดระบบรักษาความปลอดภัย ขณะที่ส่วนปฏิบัติการและระบบการเงินได้รับผลกระทบมากที่สุดตามมาด้วยชื่อเสียงของแบรนด์และการรักษาฐานลูกค้า สำหรับองค์กรที่ถูกโจมตี ความเสียหายที่เกิดขึ้นมีมูลค่าสูงมากเลยทีเดียว:

- 22 เปอร์เซ็นต์ขององค์กรที่ถูกโจมตีต้องสูญเสียลูกค้า โดย 40 เปอร์เซ็นต์สูญเสียลูกค้ามากกว่า 20 เปอร์เซ็นต์ของฐานลูกค้าทั้งหมดที่มีอยู่
- 29 เปอร์เซ็นต์สูญเสียรายได้ โดย 38 เปอร์เซ็นต์ขององค์กรเหล่านั้นสูญเสียรายได้ไปกว่า 20 เปอร์เซ็นต์
- 23 เปอร์เซ็นต์ขององค์กรที่ถูกโจมตีสูญเสียโอกาสทางธุรกิจ โดย 42 เปอร์เซ็นต์สูญเสียมากกว่า 20 เปอร์เซ็นต์ของโอกาสที่พึงจะได้รับ

การปฏิบัติการของแฮคเกอร์ และโมเดล “ธุรกิจ” แบบใหม่

ในปี 2559 การเจาะระบบดำเนินการในรูปแบบของ “องค์กร” เพิ่มมากขึ้น การเปลี่ยนแปลงที่เกิดขึ้นอย่างไม่หยุดยั้งในด้านเทคโนโลยี โดยเฉพาะอย่างยิ่งการปรับเปลี่ยนสู่ระบบดิจิตอล ก่อให้เกิดโอกาสสำหรับอาชญากรไซเบอร์ แม้ว่าคนร้ายยังคงใช้เทคนิคแบบเดิมๆ อย่างต่อเนื่อง แต่ขณะเดียวกันก็ใช้แนวทางใหม่ๆ ที่ใช้กับโครงสร้าง “ระดับกลาง” (Middle Management)

- วิธีการโจมตีแบบใหม่ๆ มีการแบ่งลำดับชั้น: แคมเปญโฆษณาที่แฝงภัยคุกคามใช้นายหน้า (หรือ “ทางผ่าน”) ที่ทำหน้าที่เหมือนผู้บริหารระดับกลาง เพื่อซ่อนเร้นกิจกรรมอันตราย จากนั้นคนร้ายก็ดำเนินการได้รวดเร็วยิ่งขึ้น โดยยังคงสามารถรักษาพื้นที่ปฏิบัติการ และเล็ดลอดการตรวจจับได้อย่างแนบเนียน
- โอกาสและความเสี่ยงของระบบคลาวด์: 27 เปอร์เซ็นต์ของคลาวด์แอพพลิเคชั่นของบริษัทอื่นที่พนักงานนำเข้ามาใช้ในองค์กรโดยมีจุดมุ่งหมายเพื่อขยายโอกาสใหม่ๆ ทางด้านธุรกิจและเพิ่มประสิทธิภาพ ถูกจัดประเภทว่ามีความ

เสี่ยงสูงและก่อให้เกิดข้อกังวลใจอย่างมากในเรื่องความปลอดภัย

• แอดแวร์แบบเดิมๆ: ซอฟต์แวร์ที่ดาวน์โหลดโฆษณาโดยไม่ได้รับอนุญาตจากผู้ใช้ ยังคงใช้การได้ดี โดยก่อให้เกิดผลกระทบ 75 เปอร์เซ็นต์ขององค์กรที่ได้รับการสำรวจ

• ข่าวดีก็คือ การใช้ชุดเครื่องมือขนาดใหญ่สำหรับการเจาะระบบ เช่น Angler, Nuclear และ Neutrino มีแนวโน้มลดลง เพราะมีการกวาดล้างผู้ผลิตชุดเครื่องมือดังกล่าวในปี 2559 อย่างไรก็ตาม พบว่ามีผู้เล่นรายย่อยเริ่มเข้ามาแทนที่

การปกป้องธุรกิจ และตื่นตัวอยู่เสมอ

รายงาน ACR ประจำปี 2560 ระบุว่า มีเพียง 56 เปอร์เซ็นต์ของการแจ้งเตือนด้านความปลอดภัยเท่านั้นที่ได้รับการตรวจสอบ และไม่ถึงครึ่งหนึ่งของการแจ้งเตือนที่ถูกต้องได้รับการแก้ไข แม้ว่าฝ่ายที่ทำหน้าที่ป้องกันจะมั่นใจในเครื่องมือที่มีอยู่ แต่ก็ต้องรับมือกับปัญหาท้าทายในเรื่องบุคลากรและความยุ่งยากซับซ้อน จนก่อให้เกิดช่องว่างและเปิดโอกาสให้ฝ่ายโจมตีมีข้อได้เปรียบเหนือกว่า ซิสโก้แนะนำขั้นตอนต่อไปนี้เพื่อป้องกัน ตรวจจับ และหลีกเลี่ยงภัยคุกคาม และลดความเสี่ยงโดย:

• กำหนดให้การรักษาความปลอดภัยเป็นภารกิจสำคัญทางด้านธุรกิจ: ผู้บริหารจะต้องเข้ามาดูแลและสนับสนุนงานด้านการรักษาความปลอดภัย พร้อมทั้งจัดสรรเงินทุนให้กับงานในส่วนนี้ โดยถือเป็นภารกิจสำคัญ

• ตรวจสอบวินัยในการดำเนินงาน: ตรวจสอบแนวทางการรักษาความปลอดภัย ติดตั้งแพตช์เพื่อแก้ไขช่องโหว่ และควบคุมจุดเชื่อมต่อกับระบบเครือข่าย แอพพลิเคชั่น ฟังก์ชั่น และข้อมูล

• ทดสอบประสิทธิภาพในการรักษาความปลอดภัย: กำหนดดัชนีชี้วัดที่ชัดเจน ใช้ดัชนีดังกล่าวเพื่อตรวจสอบและปรับปรุงแนวทางการรักษาความปลอดภัย

• ปรับใช้แนวทางป้องกันแบบครบวงจร: กำหนดเกณฑ์การประเมิน โดยให้ความสำคัญกับการผนวกรวมส่วนต่างๆ และระบบงานอัตโนมัติ เพื่อปรับปรุงความสามารถในการตรวจสอบดูแลอย่างทั่วถึง เพิ่มความคล่องตัวในการทำงานร่วมกันของระบบต่างๆ และลดระยะเวลาที่ใช้ในการตรวจจับและสกัดกั้นภัยคุกคาม ซึ่งจะช่วยให้ทีมงานฝ่ายรักษาความปลอดภัยมีเวลามากขึ้นในการตรวจสอบและแก้ไขปัญหาภัยคุกคามที่แท้จริง

รายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ – 10 ปีของการรวบรวมข้อมูลและการกลั่นกรองข้อมูลเชิงลึก

สถานการณ์ไซเบอร์ซีเคียวริตี้ได้เปลี่ยนแปลงไปอย่างมากนับตั้งแต่ที่ซิสโก้จัดทำรายงานด้านความปลอดภัยฉบับแรกเมื่อปี 2550 แม้ว่าเทคโนโลยีจะทำให้การโจมตีมีอานุภาพทำลายล้างมากขึ้น และทำให้ระบบป้องกันมีความก้าวหน้ามากกว่าเดิม แต่รากฐานของระบบรักษาความปลอดภัยยังคงมีความสำคัญมาโดยตลอด

• เมื่อปี 2550 รายงาน ACR ระบุว่าแอพพลิเคชั่นบนเว็บและแอพพลิเคชั่นด้านธุรกิจเป็นเป้าหมายหลักสำหรับการโจมตี โดยมักจะอาศัยใช้วิธีการโจมตีแบบ Social Engineering หรือช่องโหว่ที่เกิดจากผู้ใช้ ส่วนในปี 2560 แฮคเกอร์มุ่งโจมตีแอพพลิเคชั่นบนระบบคลาวด์ และอีเมลสแปมมีการขยายตัวเพิ่มมากขึ้น

• เมื่อ 10 ปีที่แล้ว การโจมตีด้วยมัลแวร์มีแนวโน้มเพิ่มสูงขึ้น โดยกลุ่มอาชญากรแสวงหากำไรจากการโจมตีดัง

กล่าว ในระบบเศรษฐกิจในปัจจุบัน คนร้ายดำเนินธุรกิจเกี่ยวกับอาชญากรรมทางไซเบอร์ โดยนำเสนอทางเลือกที่มีอุปสรรคน้อยกว่าให้แก่ลูกค้าเป้าหมาย ทุกวันนี้คนร้ายอาจเป็นใครก็ได้ และพบเห็นได้ทุกที่ ไม่จำเป็นต้องมีความเชี่ยวชาญด้านระบบรักษาความปลอดภัย และสามารถซื้อชุดเครื่องมือ “สำเร็จรูป” สำหรับการโจมตี

• รายงานฉบับปี 2550 ระบุถึงการแจ้งเตือนของ Cisco IntelliShield Security จำนวน 4,773 รายการ ซึ่งใกล้เคียงกับระดับที่ตรวจพบโดยระบบฐานข้อมูลช่องโหว่แห่งชาติ (National Vulnerability Database) และรายงานฉบับปี 2560 สำหรับรอบระยะเวลาเดียวกัน การแจ้งเตือนเกี่ยวกับช่องโหว่ที่ผู้ขายเปิดเผยมีจำนวนเพิ่มขึ้น 33 เปอร์เซ็นต์ เป็น 6,380 รายการ เราเชื่อว่าการเพิ่มขึ้นนี้เป็นผลมาจากการตระหนักรู้เรื่องความปลอดภัยที่เพิ่มมากขึ้น พื้นผิวการโจมตีที่กว้างขวางมากขึ้น และการดำเนินการอย่างจริงจังของคนร้าย

• เมื่อปี 2550 ซิสโก้แนะนำให้องค์กรต่างๆ ใช้แนวทางป้องกันแบบรอบด้านสำหรับการรักษาความปลอดภัย โดยผนวกรวมเครื่องมือ กระบวนการ และนโยบายเข้าด้วยกัน และให้ความรู้แก่ทุกฝ่ายที่เกี่ยวข้องเพื่อปกป้องสภาพแวดล้อมของตนเอง องค์กรธุรกิจไว้วางใจให้ผู้นำเสนอเทคโนโลยีที่ช่วยแก้ไขปัญหาอย่างครบวงจร แต่โดยมากแล้วมักจะไม่เป็นผล เพราะผู้ขายมักจะแนะนำโซลูชั่นที่แก้ปัญหาเฉพาะจุด และในปี 2560 ผู้บริหารฝ่ายรักษาความปลอดภัยต้องรับมือกับปัญหาความยุ่งยากซับซ้อนของสภาพแวดล้อมที่มีอยู่ ซิสโก้พยายามแก้ไขปัญหานี้ด้วยการนำเสนอแนวทางเชิงสถาปัตยกรรมสำหรับการรักษาความปลอดภัย เพื่อให้ลูกค้าสามารถใช้ประโยชน์อย่างเต็มที่จากระบบรักษาความปลอดภัยที่มีอยู่ ควบคู่ไปกับการขยายขีดความสามารถ และลดความยุ่งยากซับซ้อน

คำกล่าวสนับสนุน

“ในปี 2560 ไซเบอร์คือธุรกิจ และธุรกิจคือไซเบอร์ ที่จำเป็นต้องมีการสื่อสารหลากหลายรูปแบบ และก่อให้เกิดผลที่หลากหลาย และประสิทธิภาพด้านความปลอดภัยจึงต้องมีอย่างต่อเนื่อง ดังนั้นจึงต้องมีการปรับปรุงอย่างต่อเนื่อง และจะต้องมีการตรวจสอบประเมินเกี่ยวกับประสิทธิภาพ ค่าใช้จ่าย และการบริหารความเสี่ยง รายงานไซเบอร์ซีเคียวริตี้ประจำปี 2560 ชี้ให้เห็นถึงคำตอบสำหรับปัญหาของเราในเรื่องงบประมาณ บุคลากร นวัตกรรม และสถาปัตยกรรม”

– นาย จอห์น เอ็น. สจ๊วต รองประธานอาวุโสและประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัยและความน่าเชื่อถือของซิสโก้

“รายงานไซเบอร์ซีเคียวริตี้ประจำปี 2560 ระบุถึงดัชนีชี้วัดที่สำคัญ นั่นคือ ‘ระยะเวลาการตรวจจับ’ ซึ่งหมายถึงเวลาที่ใช้ในการตรวจพบและยับยั้งกิจกรรมอันตรายที่เกิดขึ้น โดยเราสามารถลดระยะเวลาดังกล่าวให้เหลือเพียง 6 ชั่วโมงเท่านั้น นอกจากนี้ยังมีดัชนีชี้วัดตัวใหม่ นั่นคือ ‘ระยะเวลาการพัฒนา’ ซึ่งเป็นการตรวจสอบว่าคนร้ายสามารถปรับเปลี่ยนการโจมตีเพื่อปกปิดตัวตนได้รวดเร็วเพียงใด ด้วยการใช้แนวทางการตรวจสอบเหล่านี้และแนวทางอื่นๆ ตามที่ระบุไว้ในรายงาน รวมถึงการทำงานร่วมกับองค์กรต่างๆ เพื่อสร้างระบบงานอัตโนมัติและผนวกรวมระบบป้องกันภัยคุกคาม เราจะสามารถช่วยให้ลูกค้าลดความเสี่ยงด้านการเงินและการดำเนินงานและขยายธุรกิจให้เติบโตอย่างยั่งยืน”

– นาย เดวิด ยูเลวิทช์ รองประธาน/ผู้จัดการทั่วไปฝ่ายธุรกิจการรักษาความปลอดภัยของซิสโก้

เกี่ยวกับรายงาน
รายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ ซึ่งจัดทำขึ้นเป็นปีที่ 10 สำรวจตรวจสอบข้อมูลข่าวกรองล่าสุดเกี่ยวกับภัยคุกคามที่รวบรวมโดยผู้เชี่ยวชาญด้านการรักษาความปลอดภัยของซิสโก้ โดยนำเสนอข้อมูลเชิงลึกด้านอุตสาหกรรมที่เปิดเผยถึงแนวโน้มการรักษาความปลอดภัยของลูกค้า นอกจากนี้รายงานฉบับปี 2560 ยังเน้นย้ำประเด็นสำคัญจากผลการศึกษาดัชนีชี้วัดความสามารถด้านการรักษาความปลอดภัย (Security Capabilities Benchmark Study – SCBS) ของซิสโก้ ฉบับที่ 3 ซึ่งมุ่งตรวจสอบการรับรู้ของบุคลากรฝ่ายรักษาความปลอดภัยในเรื่องที่เกี่ยวกับสถานะด้านความปลอดภัยขององค์กร และยังมีการกล่าวถึงแนวโน้มทางภูมิศาสตร์การเมือง พัฒนาการของข้อมูลทั่วโลก และความสำคัญของไซเบอร์ซีเคียวริตี้ในที่ประชุมของคณะกรรมการบริหาร

For a complete copy of the 2017 Cisco Annual Security Research report, and to read more about Cisco's recommendations as to how businesses can mitigate against risk, click here.

หากต้องการสำเนาฉบับสมบูรณ์ของรายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560 และอ่านข้อมูลเพิ่มเติมเกี่ยวกับคำแนะนำของซิสโก้สำหรับองค์กรธุรกิจในการป้องกันความเสี่ยง คลิกที่นี่

ทรัพยากรสนับสนุน
วิดีโอของซิสโก้ เดวิด ยูเลวิทช์, จอห์น เอ็น. สจ๊วต: รายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560
รายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560
บล็อกของซิสโก้: ก้าวล้ำนำหน้าภัยคุกคามที่พัฒนาอย่างต่อเนื่อง – เผยแพร่รายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560
อินโฟกราฟิกในรายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560
ภาพกราฟิกในรายงานไซเบอร์ซีเคียวริตี้ของซิสโก้ประจำปี 2560
ติดตามซิสโก้บน Twitter @CiscoSecurity
ถูกใจซิสโก้ ซีเคียวริตี้ บน Facebook

###