ซิสโก้เผยรายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 คาดการณ์การโจมตีรูปแบบใหม่ “Destruction of Servicec (DeOS)”

ซิสโก้เผยรายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 คาดการณ์การโจมตีรูปแบบใหม่ “Destruction of Servicec (DeOS)” มีการขยายตัวและส่งผลกระทบของภัยคุกคามเพิ่มขึ้น

อุตสาหกรรมหลักต้องปรับปรุงการรักษาความปลอดภัย ขณะที่เทคโนโลยีสารสนเทศและเทคโนโลยีส่วนปฏิบัติการถูกรวมเข้าด้วยกัน

กรุงเทพฯ, 26 กรกฎาคม 2560 – ซิสโก้ (NASDAQ: CISCO) เผยแพร่รายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 (2017 Midyear Cybersecurity Report – MCR) ซึ่งระบุถึงพัฒนาการที่รวดเร็วของภัยคุกคามและการโจมตีหลากหลายรูปแบบที่เพิ่มมากขึ้น ทั้งยังคาดการณ์เกี่ยวกับการโจมตีแบบ “Destruction of Service” (DeOS) ที่มุ่งเป้าไปที่การทำลายระบบเพื่อไม่ให้ผู้ถูกโจมตีสามารถกู้คืนระบบหรือกู้คืนข้อมูลได้ นอกจากนี้ การเกิดขึ้นของ Internet of Things (IoT) ส่งผลให้อุตสาหกรรมหลักๆ ดำเนินงานผ่านระบบออนไลน์เพิ่มมากขึ้น ขณะเดียวกันก็ทำให้ช่องทางการโจมตีและผลกระทบจากภัยคุกคามเพิ่มขึ้นตามไปด้วย

การโจมตีทางไซเบอร์ที่เกิดขึ้นเมื่อไม่นานมานี้ เช่น กรณีของ WannaCry และ Nyetya แสดงให้เห็นถึงการแพร่กระจายอย่างรวดเร็วและผลกระทบในวงกว้างของการโจมตี ซึ่งอาจดูเหมือนมัลแวร์เรียกค่าไถ่ทั่วไป แต่ที่จริงแล้วมีอานุภาพทำลายล้างเพิ่มขึ้นอย่างมาก กรณีดังกล่าวบ่งบอกถึงการโจมตีรูปแบบใหม่ที่ซิสโก้เรียกว่า Destruction of Service (DeOS) ซึ่งอาจสร้างความเสียหายอย่างรุนแรงจนทำให้องค์กรธุรกิจไม่สามารถกู้คืนระบบที่ใช้ในการดำเนินงานได้เลย

Internet of Things ขยายโอกาสใหม่ๆ ให้แก่อาชญากรไซเบอร์อย่างต่อเนื่อง ทั้งยังมีจุดอ่อนด้านความปลอดภัย ซึ่งจะส่งผลให้การโจมตีทางไซเบอร์มีความรุนแรงเพิ่มมากขึ้น การใช้บ็อตเน็ต IoT ที่เกิดขึ้นเมื่อไม่นานมานี้เผยให้เห็นว่า คนร้ายอาจกำลังวางรากฐานสำหรับการโจมตีทางไซเบอร์ที่ส่งผลกระทบรุนแรงเป็นวงกว้างจนอาจทำให้เครือข่ายอินเทอร์เน็ตหยุดชะงัก

การประเมินประสิทธิภาพของระบบรักษาความปลอดภัยเพื่อรับมือกับการโจมตีเหล่านี้ถือเป็นเรื่องจำเป็นอย่างยิ่ง โดยซิสโก้ได้ทำการตรวจสอบติดตามความคืบหน้าในการลดระยะเวลาที่ใช้ในการตรวจจับภัยคุกคามหลังจากที่ถูก

โจมตี หรือ “Time to Detection” (TTD) ทั้งนี้ องค์กรต่างๆ จำเป็นที่จะต้องตรวจจับภัยคุกคามให้ได้เร็วที่สุด เพื่อจำกัดพื้นที่ปฏิบัติการของการโจมตี และลดความเสียหายที่เกิดขึ้นจากการบุกรุกเครือข่ายขององค์กร ตั้งแต่เดือนพฤศจิกายน 2558 เป็นต้นมา ซิสโก้สามารถลด TTD โดยเฉลี่ยจาก 39 ชั่วโมงให้เหลือเพียง 3.5 ชั่วโมงในช่วงระยะเวลาตั้งแต่พฤศจิกายน 2559 ถึงพฤษภาคม 2560 ตัวเลขนี้อ้างอิงข้อมูลที่เก็บรวบรวมจากผลิตภัณฑ์ด้านการรักษาความปลอดภัยของซิสโก้ที่ติดตั้งไว้ภายในองค์กรต่างๆ ทั่วโลก

สถานการณ์ภัยคุกคาม: เทคนิคที่ได้รับความนิยมเพิ่มขึ้นและลดลง
คณะนักวิจัยด้านความปลอดภัยของซิสโก้ได้เฝ้าดูพัฒนาการของมัลแวร์ในช่วงครึ่งแรกของปี 2560 และพบว่ามีการเปลี่ยนแปลงในแง่ของเทคนิคการแพร่กระจาย การหลีกเลี่ยง และการบุกรุก กล่าวอย่างเฉพาะเจาะจงก็คือ ซิสโก้พบว่ามีแนวโน้มเพิ่มมากขึ้นที่ผู้โจมตีจะหลอกล่อให้เหยื่อคลิกที่ลิงค์หรือเปิดไฟล์เพื่อเรียกใช้งานมัลแวร์ นอกจากนี้ยังมีการพัฒนามัลแวร์แบบไม่มีไฟล์ที่ฝังตัวอยู่ในหน่วยความจำ และยากแก่การตรวจจับหรือตรวจสอบ เพราะมัลแวร์จะถูกลบออกเมื่อมีการรีสตาร์ทอุปกรณ์ ยิ่งไปกว่านั้น คนร้ายพึ่งพาโครงสร้างพื้นฐานที่ไม่ระบุตัวตนและไม่มีการรวมศูนย์ เช่น บริการพร็อกซี่ Tor เพื่อซ่อนเร้นกิจกรรมสั่งการและควบคุม

ซิสโก้พบว่าการใช้ชุดเครื่องมือเจาะระบบมีแนวโน้มลดลง ขณะที่วิธีการโจมตีแบบเดิมๆ เริ่มถูกนำกลับมาใช้:

• อีเมลสแปมมีจำนวนเพิ่มขึ้นอย่างมาก เนื่องจากคนร้ายหันไปใช้วิธีการแบบเดิมๆ ที่ได้รับการพิสูจน์แล้วว่าใช้งานได้จริงอย่างเช่นอีเมล เพื่อแพร่กระจายมัลแวร์และสร้างรายได้อย่างเป็นรูปธรรม นักวิจัยด้านภัยคุกคามของซิสโก้คาดการณ์ว่าจำนวนอีเมลสแปมที่มีไฟล์แนบที่เป็นอันตรายจะยังคงเพิ่มขึ้นอย่างต่อเนื่อง ขณะที่สถานการณ์ของชุดเครื่องมือเจาะระบบมีการเปลี่ยนแปลงอย่างต่อเนื่องเช่นกัน

• สปายแวร์และแอดแวร์ ซึ่งบุคลากรฝ่ายรักษาความปลอดภัยมักจะมองว่าสร้างความรำคาญมากกว่าที่จะก่อให้เกิดอันตราย เป็นรูปแบบของมัลแวร์ที่จะคงอยู่และก่อให้เกิดความเสี่ยงต่อองค์กร ซิสโก้ได้ดำเนินการศึกษาวิจัย โดยสุ่มตัวอย่างบริษัท 300 แห่งในช่วงระยะเวลา 4 เดือน และพบว่า 20 เปอร์เซ็นต์ของกลุ่มตัวอย่างมีการติดเชื้อสปายแวร์ 3 สายพันธุ์หลัก ทั้งนี้ ในสภาพแวดล้อมขององค์กร สปายแวร์สามารถขโมยข้อมูลของผู้ใช้และข้อมูลของบริษัท ลดทอนสถานะความปลอดภัยของอุปกรณ์ และเพิ่มโอกาสในการติดมัลแวร์

• พัฒนาการของมัลแวร์เรียกค่าไถ่ เช่น การเติบโตของบริการ Ransomware-as-a-Service เพิ่มความสะดวกให้แก่คนร้ายในการดำเนินการโจมตี ไม่ว่าคนร้ายจะมีความชำนาญมากน้อยเพียงใดก็ตาม มัลแวร์เรียกค่าไถ่ก่อให้เกิดข่าวคราวมากมายตามสื่อต่างๆ และมีการรายงานว่ามัลแวร์ประเภทนี้สร้างรายได้มากกว่า 1 พันล้านดอลลาร์ให้แก่คนร้ายในช่วงปี 2559 อย่างไรก็ตาม แนวโน้มดังกล่าวอาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนสำหรับบางองค์กรที่ต้องเผชิญกับภัยคุกคามที่ร้ายแรงกว่า แต่ไม่ได้ปรากฏเป็นข่าวคราวมากนัก นั่นคือ อีเมลเชิงหลอกลวงทางธุรกิจ หรือ Business Email Compromise (BEC) ซึ่งเป็นการโจมตีแบบวิศวกรรมสังคม (Social Engineering) โดยมีการส่งอีเมลเพื่อล่อหลอกให้องค์กรโอนเงินให้แก่คนร้าย การโจมตีวิธีนี้สร้างผลตอบแทนให้แก่คนร้ายอย่างเป็นกอบ

เป็นกำ โดยในช่วงเดือนตุลาคม 2556 ถึงธันวาคม 2559 มีการโจรกรรมเงินมากถึง 5.3 พันล้านดอลลาร์ผ่านการโจมตีแบบ BEC ตามข้อมูลจากศูนย์ร้องเรียนอาชญากรรมทางอินเทอร์เน็ต

อุตสาหกรรมต่างๆ เผชิญปัญหาความท้าทายร่วมกัน
ปัจจุบัน กลุ่มอาชญากรพัฒนาการโจมตีให้มีความซับซ้อนและรุนแรงเพิ่มขึ้นอย่างต่อเนื่อง องค์กรธุรกิจในอุตสาหกรรมต่างๆ จึงต้องรับมือกับความท้าทายในการปรับปรุงระบบรักษาความปลอดภัยขั้นพื้นฐานเพื่อก้าวให้ทันกับสถานการณ์ที่เปลี่ยนไป ขณะที่เทคโนโลยีสารสนเทศ (Information Technology – IT) และเทคโนโลยีส่วนปฏิบัติการ (Operational Technology – OT) ผสานรวมเข้าด้วยกันบน Internet of Things องค์กรต่างๆ ก็ประสบปัญหาเรื่องความซับซ้อนของระบบและความสามารถในการตรวจสอบ ในการศึกษาเกี่ยวกับความสามารถด้านการรักษาความปลอดภัย (Security Capabilities Benchmark Study) ซิสโก้ได้สำรวจความคิดเห็นของผู้บริหารฝ่ายรักษาความปลอดภัยเกือบ 3,000 คนใน 13 ประเทศ และพบว่าในทุกกลุ่มอุตสาหกรรม ทีมงานด้านการรักษาความปลอดภัยต้องรับมือกับการโจมตีที่มีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง ส่งผลให้หลายๆ องค์กรจำเป็นต้องใช้แนวทางการรักษาความปลอดภัยในลักษณะตั้งรับมากขึ้น

• มีองค์กรเพียง 2 ใน 3 ที่ดำเนินการตรวจสอบการแจ้งเตือนเรื่องความปลอดภัย และในบางอุตสาหกรรม (เช่น การแพทย์ และคมนาคมขนส่ง) ตัวเลขนี้อยู่ที่ระดับเกือบ 50 เปอร์เซ็นต์
• แม้กระทั่งในอุตสาหกรรมที่มีการตอบสนองรวดเร็วที่สุด (เช่น การเงิน และการแพทย์) องค์กรธุรกิจก็สามารถป้องกันการโจมตีที่รู้จักได้ไม่ถึง 50 เปอร์เซ็นต์
• กรณีการเจาะระบบก่อให้เกิดแรงกระตุ้นในระดับหนึ่ง กล่าวคือ ในอุตสาหกรรมส่วนใหญ่ เมื่อเกิดปัญหาการเจาะระบบขึ้น ก็จะมีการปรับปรุงระบบรักษาความปลอดภัยบางส่วนในองค์กรต่างๆ อย่างน้อย 90 เปอร์เซ็นต์ และในบางอุตสาหกรรม (เช่น คมนาคมขนส่ง) มีการตอบสนองที่รวดเร็วน้อยกว่า โดยอยู่ที่ 80 เปอร์เซ็นต์โดยประมาณ

ประเด็นสำคัญสำหรับแต่ละกลุ่มอุตสาหกรรมมีดังนี้:

• ภาครัฐ – ในบรรดาภัยคุกคามที่มีการตรวจสอบ 32 เปอร์เซ็นต์ถูกระบุว่าเป็นภัยคุกคามจริง แต่มีเพียง 47 เปอร์เซ็นต์ของภัยคุกคามจริงเท่านั้นที่ได้รับการแก้ไขในท้ายที่สุด
• ค้าปลีก – องค์กรธุรกิจ 2 ใน 3 สูญเสียรายได้เนื่องจากการโจมตีในช่วงปีที่ผ่านมา โดยราว 1 ใน 4 สูญเสียลูกค้าหรือโอกาสทางธุรกิจ
• การผลิต – 40 เปอร์เซ็นต์ของบุคลากรฝ่ายรักษาความปลอดภัยในอุตสาหกรรมการผลิตระบุว่า ตนเองไม่มีกลยุทธ์การรักษาความปลอดภัยที่เป็นทางการ หรือไม่ได้ปฏิบัติตามนโยบายการรักษาความปลอดภัยสารสนเทศตามมาตรฐาน เช่น ISO 27001 หรือ NIST 800-53
• สาธารณูปโภค – บุคลากรฝ่ายรักษาความปลอดภัยระบุว่า การโจมตีแบบเจาะจงเป้าหมาย (42 เปอร์เซ็นต์) และภัยคุกคามขั้นสูงแบบต่อเนื่อง (Advanced Persistent Threat หรือ APT) (40 เปอร์เซ็นต์) เป็นความเสี่ยงด้าน

ความปลอดภัยที่ร้ายแรงที่สุดสำหรับองค์กร

• การแพทย์ – 37 เปอร์เซ็นต์ของสถานพยาบาลระบุว่า การโจมตีแบบเจาะจงเป้าหมายก่อให้เกิดความเสี่ยงในระดับที่สูงต่อองค์กร

คำแนะนำจากซิสโก้สำหรับองค์กรต่างๆ

เพื่อรับมือกับผู้โจมตีที่ใช้เทคโนโลยีก้าวล้ำเพิ่มมากขึ้น องค์กรต่างๆ จำเป็นที่จะต้องปรับใช้แนวทางเชิงรุกเพื่อป้องกันการโจมตี โดยกลุ่มธุรกิจการรักษาความปลอดภัยของซิสโก้มีคำแนะนำดังนี้:

• การดูแลโครงสร้างพื้นฐานและแอพพลิเคชั่นให้ทันสมัย เพื่อป้องกันไม่ให้คนร้ายใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนที่มีอยู่

• ลดความยุ่งยากซับซ้อนด้วยระบบรักษาความปลอดภัยแบบครบวงจร จำกัดการลงทุนในผลิตภัณฑ์ที่ทำงานแยกออกจากกัน

• เปิดโอกาสให้ผู้บริหารเข้ามามีส่วนร่วมแต่เนิ่นๆ เพื่อให้เข้าใจเกี่ยวกับความเสี่ยง ผลตอบแทน และข้อจำกัดด้านงบประมาณอย่างรอบด้าน

• กำหนดดัชนีชี้วัดที่ชัดเจน และใช้ดัชนีดังกล่าวเพื่อตรวจสอบและปรับปรุงแนวทางการรักษาความปลอดภัย

• ตรวจสอบการฝึกอบรมด้านความปลอดภัยสำหรับพนักงาน โดยเปรียบเทียบระหว่างการฝึกอบรมตามหน้าที่การทำงาน กับการฝึกอบรมทั่วไปที่ใช้กับทุกคน

• สร้างสมดุลระหว่างมาตรการรักษาความปลอดภัยกับการตอบสนองที่ฉับไว อย่าใช้วิธี “ตั้งค่าครั้งเดียวและใช้งานได้ตลอด” สำหรับการควบคุมหรือกระบวนการด้านการรักษาความปลอดภัย

สำหรับรายงาน MCR ประจำปี 2560 มีการเชิญกลุ่มพันธมิตรด้านเทคโนโลยีการรักษาความปลอดภัย 10 รายให้เข้าร่วมแบ่งปันข้อมูล เพื่อหาข้อสรุปร่วมกันเกี่ยวกับสถานการณ์ภัยคุกคาม พันธมิตรที่ร่วมจัดทำรายงานฉบับนี้ได้แก่ Anomali, Flashpoint, Lumeta, Qualys, Radware, Rapid7, RSA, SAINT Corporation, ThreatConnect และ TrapX เครือข่ายพันธมิตรด้านเทคโนโลยีการรักษาความปลอดภัยของซิสโก้ถือเป็นองค์ประกอบสำคัญในวิสัยทัศน์ของซิสโก้สำหรับการนำเสนอระบบรักษาความปลอดภัยที่เรียบง่าย เปิดกว้าง และทำงานแบบอัตโนมัติให้แก่ลูกค้า

คำกล่าวสนับสนุน

“การโจมตีที่เกิดขึ้นล่าสุด เช่น กรณีของมัลแวร์ WannaCry และ Nyetya แสดงให้เห็นว่ากลุ่มคนร้ายมีความคิดสร้างสรรค์เพิ่มมากขึ้นในแง่ของการออกแบบวิธีการโจมตี ขณะที่องค์กรส่วนใหญ่ดำเนินการอย่างจริงจังเพื่อปรับปรุงระบบรักษาความปลอดภัยหลังจากที่เกิดปัญหา ธุรกิจในกลุ่มอุตสาหกรรมต่างๆ ยังคงต้องแข่งขันและรับมือกับผู้โจมตีอย่างต่อเนื่อง ประสิทธิภาพในการรักษาความปลอดภัยเริ่มต้นด้วยการปิดช่องว่างที่มีอยู่และทำให้การรักษาความปลอดภัยกลายเป็นภารกิจสำคัญของธุรกิจ”

นายสตีฟ มาร์ติโน รองประธานและประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัยสารสนเทศของซิสโก้

“ความยุ่งยากซับซ้อนยังคงเป็นอุปสรรคที่ขัดขวางความพยายามของหลายๆ องค์กรในการรักษาความปลอดภัย เห็นได้ชัดว่าการลงทุนในผลิตภัณฑ์แบบติดตั้งเฉพาะจุดที่ไม่สามารถผนวกรวมเข้าด้วยกันตลอดหลายปีที่ผ่านมา เปิดโอกาสให้คนร้ายสามารถค้นพบจุดอ่อนที่ถูกมองข้ามหรือช่องโหว่ในการรักษาความปลอดภัยได้อย่างง่ายดาย เพื่อลดระยะเวลาที่ใช้ในการตรวจจับและจำกัดผลกระทบของการโจมตี แวดวงอุตสาหกรรมจำเป็นที่จะต้องปรับใช้แนวทางเชิงสถาปัตยกรรมแบบครบวงจร ซึ่งจะช่วยเพิ่มขีดความสามารถในการตรวจสอบและจัดการอย่างทั่วถึง และช่วยให้ทีมงานฝ่ายรักษาความปลอดภัยสามารถแก้ไขปัญหาช่องว่างและจุดอ่อนได้อย่างมีประสิทธิภาพ”
นายเดวิด ยูเลวิทช์ รองประธานอาวุโสและผู้จัดการทั่วไป กลุ่มธุรกิจการรักษาความปลอดภัยของซิสโก้

เกี่ยวกับรายงาน
รายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 ของซิสโก้ตรวจสอบวิเคราะห์ข้อมูลภัยคุกคามล่าสุดที่เก็บรวบรวมโดยหน่วยงาน Cisco Collective Security Intelligence รายงานฉบับนี้นำเสนอข้อมูลเชิงลึกเกี่ยวกับอุตสาหกรรมและแนวโน้มทางด้านไซเบอร์ซีเคียวริตี้ในช่วงครึ่งแรกของปี พร้อมด้วยคำแนะนำที่ใช้งานได้จริงสำหรับการปรับปรุงมาตรการรักษาความปลอดภัย รายงานนี้อ้างอิงข้อมูลรายวันที่ได้รับจากระบบตรวจวัดระยะไกลที่ติดตั้งไว้อย่างกว้างขวางกว่า 4 หมื่นล้านจุด นักวิจัยของซิสโก้ใช้ประโยชน์จากข้อมูลข่าวกรองที่ได้รับเพื่อกำหนดแนวทางป้องกันแบบเรียลไทม์สำหรับผลิตภัณฑ์และบริการของเรา ซึ่งจะถูกจัดส่งในทันทีให้แก่ลูกค้าของซิสโก้ในทุกที่ทั่วโลก

ทรัพยากรสนับสนุน
วิดีโอการสนทนากับผู้บริหารกลุ่มธุรกิจการรักษาความปลอดภัยของซิสโก้ สตีฟ มาร์ติโน: รายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560
รายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 ของซิสโก้
บล็อกของซิสโก้: รายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 ของซิสโก้ชี้ ภัยคุกคามก่อให้เกิดผลกระทบเพิ่มมากขึ้น
กราฟิกในรายงานไซเบอร์ซีเคียวริตี้ประจำกลางปี 2560 ของซิสโก้
ติดตามซิสโก้บน Twitter @CiscoSecurity
ถูกใจ Cisco Security บน Facebook

เกี่ยวกับ ซิสโก้
ซิสโก้ (NASDAQ: CSCO) เป็นผู้นำระดับโลกด้านเทคโนโลยีที่ทำงานกับอินเทอร์เน็ตตั้งแต่ปี ค.ศ. 1984 บุคลากรของเรา ผลิตภัณฑ์ และ พันธมิตรช่วยเหลือสังคมเชื่อมต่อโอกาสทางดิจิตอลอย่างปลอดภัย ดูข่าวและข้อมูลเพิ่มเติมเกี่ยวกับซิสโก้ได้ที่ newsroom.cisco.com และติดตามข่าวสารของซิสโก้บนทวิตเตอร์ที่ @Cisco
###

document is Cisco Public Information.

ประชาสัมพันธ์ข่าวโดย:

วราวอง จงรักษ์

โทรศัพท์: 02-971-3711

อีเมล์: warawong@pc-a.co.th