ซิสโก้เผยรายงานความปลอดภัยกลางปี 2558

ซิสโก้เผยรายงานความปลอดภัยกลางปี 2558
ระบุ “มีความจำเป็นเร่งด่วน” สำหรับองค์กรต่างๆ ในการ “ลดเวลาตรวจจับภัยคุกคาม”

14 ตุลาคม 2558 – แม้ว่าระบบรักษาความปลอดภัยไซเบอร์จะมีความก้าวล้ำอย่างมาก แต่มีกลุ่มอาชญากรใหม่ๆ ที่ใช้เทคโนโลยีขั้นสูงเพิ่มขึ้นอย่างต่อเนื่องในช่วงหลายปีที่ผ่านมา โดยมีการพัฒนาแนวทางการโจมตีโดยอาศัยมัลแวร์และวิธีการเจาะระบบใหม่ๆ อย่างไม่หยุดยั้ง และทุกๆ วินาทีย่อมมีความสำคัญเมื่อองค์กรธุรกิจตกอยู่ในความเสี่ยง หากการตอบสนองช้าเกินไป หรือหากปราศจากระบบการป้องกันที่สำคัญ ผลกระทบก็จะเพิ่มสูงขึ้นอย่างรวดเร็ว จนอาจเสี่ยงต่อการสูญเสียรายได้ ข้อมูล และความเชื่อมั่นของลูกค้า ปัจจุบันมีมัลแวร์ที่แพร่กระจายอย่างรวดเร็ว และเจาะระบบองค์กรต่างๆ ได้อย่างรวดเร็วเช่นกัน

รายงานความปลอดภัยกลางปีของซิสโก้ ซึ่งวิเคราะห์ข้อมูลข่าวกรองเกี่ยวกับภัยคุกคามและแนวโน้มของไซเบอร์ซีเคียวริตี้ เปิดเผยถึงความจำเป็นที่สำคัญอย่างมากสำหรับองค์กรต่างๆ ในการ “ลดระยะเวลาการตรวจจับภัยคุกคามเพื่อแก้ไขปัญหาการโจมตีที่ซับซ้อนอย่างทันท่วงที”

ในขณะที่คนร้ายยังคงสร้างสรรค์นวัตกรรมอย่างต่อเนื่อง เพื่อเล็ดลอดเข้าสู่เครือข่ายและหลบเลี่ยงมาตรการรักษาความปลอดภัย สิ่งใหม่ที่พบก็คือ คนร้ายมีความสามารถเพิ่มมากขึ้นในการคิดค้นวิธีการโจมตีรูปแบบใหม่ๆ อย่างรวดเร็ว รวมถึงการปรับปรุงขีดความสามารถในการเจาะระบบและหลบเลี่ยงการตรวจจับ ในช่วงครึ่งแรกของปี 2558 ความสำเร็จที่สำคัญของผู้โจมตีทางออนไลน์ได้แก่ การพัฒนาเครื่องมือและกลยุทธ์ใหม่ๆ และนำเอาเครื่องมือและกลยุทธ์เดิมๆ กลับมาใช้ เพื่อหลบหลีกระบบรักษาความปลอดภัย

ด้วยการใช้เทคนิคต่างๆ เช่น การปรับเปลี่ยนโค้ดให้อ่านยากขึ้น (Obfuscation) ผู้โจมตีจึงสามารถเล็ดลอดผ่านแนวป้องกันบนเครือข่าย และดำเนินการโจมตีจนสำเร็จก่อนที่จะถูกตรวจพบ เนื่องจากซอฟต์แวร์อันตรายมีการแพร่กระจายอย่างต่อเนื่องและเพิ่มมากขึ้น โดยไม่มีมาตรการตอบโต้ที่มีประสิทธิภาพเพียงพอ ดังนั้นไม่ช้าก็เร็วองค์กรต่างๆ ก็จะต้องถูกเจาะเข้าสู่ระบบได้สำเร็จอย่างแน่นอน

ขณะเดียวกัน ผู้ผลิตเทคโนโลยีการรักษาปลอดภัยก็รับมือกับปัญหานี้ด้วยการสร้างสรรค์นวัตกรรมใหม่ๆ ตัวอย่างเช่น คณะนักวิจัยเพิ่มเติมการวิเคราะห์รูปแบบไฟล์ใหม่ เช่น .cab และ .chm เนื่องจากตรวจพบการโจมตีใหม่ๆ ที่ใช้รูปแบบไฟล์ดังกล่าว นอกจากนี้ ผู้ผลิตกำลังพัฒนาเอนจิ้นการตรวจจับใหม่ พร้อมทั้งประเมินและพัฒนาระบบวิเคราะห์พฤติกรรมอย่างต่อเนื่อง

ผู้ผลิตเทคโนโลยีการรักษาปลอดภัยทราบดีว่าตนเองจำเป็นที่จะต้องดำเนินการอย่างยืดหยุ่น หากว่าระบบป้องกันเครือข่ายมีช่องโหว่แม้เพียงช่วงสั้นๆ ผู้โจมตีก็จะเป็นฝ่ายมีชัย อย่างไรก็ตาม การสร้างสรรค์นวัตกรรมในแวดวงอุตสาหกรรมการรักษาความปลอดภัยยังไม่รวดเร็วเพียงพออย่างที่ควรเป็น รายงานของซิสโก้เน้นย้ำถึง ความจำเป็นสำหรับองค์กรธุรกิจในการปรับใช้โซลูชั่นแบบครบวงจร แทนที่จะใช้ผลิตภัณฑ์แบบติดตั้งเฉพาะจุด และควรจะทำงานร่วมกับผู้ผลิตที่ไว้ใจได้ และว่าจ้างผู้ให้บริการด้านการรักษาความปลอดภัยเพื่อทำการประเมินและให้คำแนะนำปรึกษา ยิ่งไปกว่านั้น ผู้เชี่ยวชาญด้านภูมิศาสตร์การเมืองยังระบุว่าจำเป็นที่จะต้องมีการพัฒนากรอบโครงสร้างระดับโลกสำหรับการกำกับดูแลระบบไซเบอร์ เพื่อรองรับการเติบโตทางเศรษฐกิจอย่างยั่งยืน

ข้อมูลสำคัญบางประเด็นจากรายงานความปลอดภัยประจำปี 2558 ของซิสโก้ รวมถึงรายงานความปลอดภัยกลางปี 2558 มีดังนี้:

• การโจมตีทางไซเบอร์ก่อให้เกิดค่าใช้จ่ายเพิ่มมากขึ้นและรับมือได้ยากกว่าเดิม – ในช่วงปี 2557 ค่าใช้จ่ายโดยเฉลี่ยของการละเมิดด้านความปลอดภัยเพิ่มเป็น 5.9 ล้านดอลลาร์ หรือ 213 ล้านบาท แต่ที่สำคัญกว่านั้นก็คือ เวลาเฉลี่ยที่ใช้ในการแก้ปัญหาการโจมตีทางไซเบอร์ในปัจจุบันอยู่ที่ 45 วัน ซึ่งเพิ่มขึ้นเกือบ 50 เปอร์เซ็นต์เมื่อเทียบกับหนึ่งปีที่แล้ว

• องค์กรไม่สามารถตรวจพบการละเมิดได้อย่างทันท่วงที – อาจใช้เวลากว่า 2 ปีสำหรับบางองค์กรกว่าที่จะสามารถตรวจพบการละเมิด ขณะที่บริษัทกว่าครึ่งหนึ่งของ ไม่สามารถระบุจุดที่มีการบุกรุกได้อย่างแน่ชัด

• เว็บ เครือข่าย และอีเมลคือ 3 ช่องทางหลักที่โดนโจมตีมากที่สุด – ทั้ง 3 ช่องทางนี้ได้รับการใช้งานอย่างแพร่หลายในปัจจุบัน โดยเฉพาะอย่างยิ่งในเอเชีย-แปซิฟิก ซึ่งอัตราการใช้งานอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่อยู่ในระดับที่สูง

• การแฮ็กระบบเป็นสาเหตุหลักของการเกิดช่องโหว่ – ตามมาติดๆ ด้วยมัลแวร์และโซเชียลมีเดีย โดยนักวิเคราะห์ระบุว่าโซเชียลมีเดียเป็นปัจจัยสำคัญที่ก่อให้เกิดการหยุดชะงักในโลกปัจจุบันที่มีการเชื่อมต่อถึงกันอย่างใกล้ชิด

• เมื่อปีที่แล้ว ธุรกิจค้าปลีกถูกโจมตีหนักที่สุด ความเสียหายสูงถึง 245 ล้านดอลลาร์ – รองลงมาได้แก่ ธุรกิจบริการด้านการเงิน (80 ล้านดอลลาร์) และการแพทย์ (4.5 ล้านดอลลาร์)

• โมบายล์มัลแวร์คือช่องทางใหม่สำหรับผู้โจมตี – ขณะเดียวกัน 99 เปอร์เซ็นต์ของซอฟต์แวร์อันตรายเหล่านี้พุ่งเป้าไปที่ระบบปฏิบัติการ Android ในปี 2556

• Flash กลับมาอีกครั้ง – การโจมตีช่องโหว่ของ Adobe Flash ซึ่งรวมอยู่ในชุดเครื่องมือสำหรับการโจมตี Angler และ Nuclear มีแนวโน้มเพิ่มสูงขึ้น

• วิวัฒนาการของมัลแวร์เรียกค่าไถ่ – มัลแวร์เรียกค่าไถ่ (Ransomware) ยังคงสร้างรายได้เป็นกอบเป็นกำให้แก่

แฮ็กเกอร์ และมีการเผยแพร่มัลแวร์ชนิดนี้รุ่นใหม่ๆ ออกมาอย่างต่อเนื่อง

• Dridex: การโจมตีที่ปรับเปลี่ยนอย่างต่อเนื่อง – ผู้สร้างแคมเปญการโจมตีที่กลายพันธุ์อย่างรวดเร็วนี้มีความเข้าใจอย่างลึกซึ้งเกี่ยวกับการหลบเลี่ยงมาตรการรักษาความปลอดภัย

เตรียมพร้อมรับมือกับการต่อสู้

ผู้โจมตีและผู้ผลิตเทคโนโลยีด้านความปลอดภัยกำลังแข่งขันกันอย่างดุเดือดมากขึ้นเพื่อสร้างสรรค์นวัตกรรมใหม่ๆ ขณะที่ผู้ใช้และองค์กรตกอยู่ในความเสี่ยงที่เพิ่มสูงขึ้น ผู้ผลิตจำเป็นที่จะต้องมีความตื่นตัวมากขึ้นในการพัฒนาโซลูชั่นการรักษาความปลอดภัยแบบครบวงจรที่จะช่วยให้องค์กรต่างๆ สามารถดำเนินการป้องกันเชิงรุก รวมทั้งปรับเปลี่ยนบุคลากร กระบวนการ เทคโนโลยีให้สอดคล้องกันได้ดังนี้

• การป้องกันภัยคุกคามอย่างครบวงจร – องค์กรต่างๆ เผชิญกับปัญหาท้าทายอย่างมากในการปรับใช้โซลูชั่นแบบติดตั้งเฉพาะจุด และจำเป็นที่จะต้องเปลี่ยนไปใช้สถาปัตยกรรมที่ติดตั้งระบบรักษาความปลอดภัยไว้ในทุกๆ ที่ โดยมีผลบังคับใช้ที่จุดควบคุมเท่านั้น

• บริการเติมเต็มช่องว่าง – ขณะที่แวดวงอุตสาหกรรมความปลอดภัยแก้ไขปัญหาระบบป้องกันที่แยกเป็นส่วนๆ ไม่ต่อเนื่อง รวมไปถึงสถานการณ์ภัยคุกคามที่เปลี่ยนแปลงอย่างไม่หยุดยั้ง และปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญ องค์กรธุรกิจจะต้องลงทุนในโซลูชั่นการรักษาความปลอดภัยที่มีประสิทธิภาพ ยั่งยืน และไว้ใจได้ รวมถึงบริการระดับผู้เชี่ยวชาญ

• กรอบโครงสร้างระดับโลกสำหรับการกำกับดูแลระบบไซเบอร์ – การกำกับดูแลระบบไซเบอร์ทั่วโลกในปัจจุบันไม่สามารถรองรับสถานการณ์ภัยคุกคามหรือปัญหาท้าทายใหม่ๆ ทางด้านภูมิศาสตร์การเมือง คำถามเรื่องพรมแดน เช่น รัฐบาลเก็บรวบรวมข้อมูลเกี่ยวกับประชาชน ธุรกิจและแบ่งปันข้อมูลดังกล่าวระหว่างเขตอำนาจศาลต่างๆ ในลักษณะใด ถือเป็นอุปสรรคสำคัญในการสร้างระบบกำกับดูแลไซเบอร์ ทั้งนี้เพราะความร่วมมือทั่วโลกมีลักษณะจำกัด จำเป็นที่จะต้องใช้กรอบโครงสร้างการกำกับดูแลไซเบอร์ภายใต้ความร่วมมือของหลายฝ่ายที่เกี่ยวข้อง เพื่อรองรับการสร้างสรรค์นวัตกรรมและการขยายตัวทางเศรษฐกิจที่ยั่งยืนในระดับโลก

• ผู้ผลิตเทคโนโลยีที่ไว้ใจได้ – องค์กรต่างๆ ควรเรียกร้องให้ผู้ผลิตเทคโนโลยีมีความโปร่งใสและสามารถสาธิตถึงการรักษาความปลอดภัยที่รวมไว้ในผลิตภัณฑ์ที่นำเสนอ เพื่อยืนยันถึงความน่าเชื่อถือ องค์กรเหล่านี้จะต้องมีความเข้าใจดังกล่าวในทุกแง่มุมของการพัฒนาผลิตภัณฑ์ ตั้งแต่ส่วนของซัพพลายเชน ไปจนถึงอายุการใช้งานของผลิตภัณฑ์ และจะต้องขอให้ผู้ผลิตรับรองคำกล่าวอ้างในรูปแบบของสัญญา และเรียกร้องความปลอดภัยที่ดียิ่งขึ้น

ดาวน์โหลดสำเนาของ รายงานความปลอดภัยกลางปี 2558 ของซิสโก้

คำกล่าวสนับสนุน

• คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการประจำประเทศไทยและภูมิภาคอินโดจีนของซิสโก้

“ท่ามกลางสถานการณ์ภัยคุกคามทั่วโลกในปัจจุบัน องค์กรธุรกิจและหน่วยงานราชการจำเป็นที่จะต้องมีความตื่นตัวมากขึ้น และจะต้องปรับปรุงนโยบายด้านความปลอดภัยให้ทันสมัย ขณะที่ประเทศไทยกำลังพัฒนาไปสู่เศรษฐกิจดิจิตอล ผู้บริหารฝ่ายรักษาความปลอดภัยจำเป็นที่จะต้องมีบทบาทในคณะกรรมการบริหารขององค์กร เพราะปัญหาข้อมูลรั่วไหลอาจสร้างความเสียหายอย่างมากมายมหาศาลต่อธุรกิจ ประเทศไทยครองอันดับ 3 ของโลกในแง่ภัยคุกคามทางไซเบอร์ (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย – ThaiCERT, มิถุนายน 2558) และรายงานจาก ThaiCERT ระบุว่า ในปี 2558 อาชญากรรมออนไลน์ราว 34.5 เปอร์เซ็นต์เกี่ยวข้องกับโค้ดอันตราย ขณะที่ 26.3 เปอร์เซ็นต์ และ 23.3 เปอร์เซ็นต์เกี่ยวข้องกับการฉ้อโกงและการบุกรุกระบบตามลำดับ เป็นเรื่องที่น่าเศร้าที่พบว่าองค์กรที่ถูกโจมตีมากที่สุดคือ หน่วยงานของรัฐ และสถาบันการศึกษา ที่จริงแล้ว ทุกๆ องค์กรล้วนมีความเสี่ยง และถือเป็นภารกิจระดับชาติในการสร้างระบบเศรษฐกิจที่มีความมั่นคงปลอดภัย ขณะที่ประเทศไทยกำลังพัฒนาสู่การเป็นประเทศดิจิตอลที่มีการเชื่อมต่อถึงกันอย่างทั่วถึง”

ทรัพยากรสนับสนุน

• ความคิดเห็นของจอห์น เอ็น. สจ๊วต เกี่ยวกับรายงานความปลอดภัยกลางปี 2558 ของซิสโก้
• ภาพอินโฟกราฟิกของรายงานความปลอดภัยกลางปี
• บล็อกด้านความปลอดภัยของซิสโก้
• ผลิตภัณฑ์และโซลูชั่นความปลอดภัยของซิสโก้
• Twitter @CiscoAPAC
• Facebook http://facebook.com/ciscosecurity

เกี่ยวกับ บริษัท ซิสโก้ ซีสเต็มส์ จำกัด
ซิสโก้ (NASDAQ: CSCO) เป็นผู้นำระดับโลกด้านไอทีที่ช่วยให้ธุรกิจและบริษัทต่างๆสร้างสรรค์สิ่ง มหัศจรรย์และปรากฏการณ์ใหม่ๆที่เกิดจากการเชื่อมต่อ (connect) ดูข่าวและข้อมูลเพิ่มเติมเกี่ยวกับซิสโก้ได้ที่ http://thenetwork.cisco.com ผลิตภัณฑ์ซิสโก้ในประเทศไทยจัดจำหน่ายผ่านช่องทางการจัดจำหน่ายโดยพาร์ทเนอร์ของ Cisco Systems International B.V ซึ่งเป็นเจ้าของบริษัทในเครือซิสโก้ ซีสเต็มส์ ทั้งหมด