# ซิสโก้เผยรายงานความปลอดภัย ระบุ “องค์กรมีความมั่นใจน้อยลง”

ซิสโก้เผยรายงานความปลอดภัย ระบุ “องค์กรมีความมั่นใจน้อยลง”
และผลกระทบต่ออุตสาหกรรมจากผู้บุกรุกเพิ่มมากขึ้น

องค์กรธุรกิจเสริมสร้างความแข็งแกร่งด้านความปลอดภัยเพื่อรับมือกับการโจมตีที่อาศัยจุดอ่อน
“โครงสร้างพื้นฐานรุ่นเก่า” และ “การรั่วไหลของข้อมูลผ่าเบราว์เซอร์”

กรุงเทพฯ, 27 มกราคม 2559 – รายงานด้านความปลอดภัยประจำปี 2559 ของซิสโก้ ซึ่งสำรวจตรวจสอบแนวโน้มความปลอดภัยไซเบอร์และข้อมูลเชิงลึกเกี่ยวกับภัยคุกคาม เปิดเผยว่า มีองค์กรทั่วโลกเพียง 45 เปอร์เซ็นต์เท่านั้นที่มั่นใจในสถานะความปลอดภัยของตนเอง ขณะที่ปัจจุบันผู้บุกรุกดำเนินการโจมตีอย่างซับซ้อน รุนแรง และรวดเร็ว

แม้ว่าผู้บริหารอาจไม่แน่ใจเกี่ยวกับความแข็งแกร่งด้านความปลอดภัยขององค์กร แต่ผู้บริหาร 92 เปอร์เซ็นต์เห็นพ้องต้องกันว่า หน่วยงานกำกับดูแลและนักลงทุนจะคาดหวังให้บริษัทต่างๆ จัดการความเสี่ยงด้านไซเบอร์ซีเคียวริตี้อย่างเหมาะสม ผู้บริหารเหล่านี้ดำเนินมาตรการเพิ่มมากขึ้นเพื่อรักษาอนาคตขององค์กร โดยเฉพาะอย่างยิ่งขณะที่องค์กรพยายามปรับเปลี่ยนการดำเนินงานให้เป็นรูปแบบดิจิตอล

รายงานดังกล่าวเน้นย้ำถึงปัญหาท้าทายที่องค์กรธุรกิจต้องเผชิญ โดยเป็นผลสืบเนื่องมาจากการพัฒนาก้าวหน้าอย่างรวดเร็วของผู้โจมตี ปัจจุบัน แฮ็กเกอร์ใช้ประโยชน์จากทรัพยากรที่ “ถูกกฎหมาย” เพื่อเริ่มต้นการโจมตีอย่างมีประสิทธิภาพเพื่อสร้างผลกำไร นอกจากนี้ ลำพังเพียงแค่การโจมตีโดยตรงโดยอาชญากรไซเบอร์ที่ใช้มัลแวร์เรียกค่าไถ่ (Ransomware) สามารถสร้างรายได้ถึง 34 ล้านดอลลาร์ต่อปี (หรือ 1,224 ล้านบาทต่อปี) และอาชญากรเหล่านี้ยังคงดำเนินการโจมตีอย่างต่อเนื่อง โดยไม่สะทกสะท้านต่อมาตรการป้องปรามของหน่วยงานกำกับดูแล

องค์กรธุรกิจต้องรับมือกับปัญหาท้าทายด้านความปลอดภัยที่ยับยั้งความสามารถขององค์กรในการตรวจจับการโจมตีทางไซเบอร์ รวมทั้งบรรเทาปัญหา และกู้คืนระบบภายหลังการโจมตี โครงสร้างพื้นฐานรุ่นเก่า รวมถึงโครงสร้างองค์กรและแนวทางปฏิบัติที่ล้าสมัย ทำให้องค์กรตกอยู่ในความเสี่ยงเพิ่มมากขึ้น

รายงานดังกล่าวเรียกร้องให้ทั่วโลกร่วมมือกันมากขึ้น และลงทุนในกระบวนการ เทคโนโลยี และบุคลากรเพื่อต่อสู้กับอาชญากรที่มุ่งโจมตีอุตสาหกรรมต่างๆ

ประเด็นสำคัญจากผลการศึกษาวิจัย

• ความเชื่อมั่นลดลง ความโปร่งใสเพิ่มขึ้น: ไม่ถึงครึ่งหนึ่งขององค์กรธุรกิจที่ตอบแบบสอบถามมั่นใจในความสามารถของตนเองในการระบุขอบเขตความเสี่ยงของเครือข่ายและแก้ไขความเสียหาย แต่ผู้บริหารฝ่ายการเงินและธุรกิจส่วนใหญ่เห็นพ้องต้องกันว่าหน่วยงานกำกับดูแลและนักลงทุนคาดหวังว่าบริษัทต่างๆ จะมีความโปร่งใสเพิ่มมากขึ้นในการเปิดเผยข้อมูลเกี่ยวกับความเสี่ยงทางด้านไซเบอร์ซีเคียวริตี้ในอนาคต แนวโน้มนี้แสดงให้เห็นว่าปัญหาเรื่องความปลอดภัยได้รับความสนใจจากคณะกรรมการบริหารเพิ่มมากขึ้น

• โครงสร้างพื้นฐานรุ่นเก่า: ในช่วงปี 2557 ถึง 2558 จำนวนองค์กรที่ระบุว่าโครงสร้างพื้นฐานด้านความปลอดภัยของตนเองมีความทันสมัยลดลง 10 เปอร์เซ็นต์ ผลการสำรวจชี้ว่า 92 เปอร์เซ็นต์ของอุปกรณ์อินเทอร์เน็ตมีช่องโหว่ที่รู้จัก 31 เปอร์เซ็นต์ของอุปกรณ์ทั้งหมดที่วิเคราะห์ไม่ได้รับการสนับสนุนหรือบำรุงรักษาโดยผู้ขายอีกต่อไป

• ธุรกิจขนาดกลางและขนาดเล็ก (SMB) คือจุดอ่อน: ขณะที่องค์กรต่างๆ สำรวจซัพพลายเชนและความร่วมมือกับองค์กรธุรกิจขนาดเล็กอย่างใกล้ชิด ก็พบว่าองค์กรเหล่านี้ใช้เครื่องมือและกระบวนการป้องกันภัยคุกคามน้อยกว่า ตัวอย่างเช่น ในช่วงปี 2557 ถึง 2558 จำนวน SMB ที่ใช้ระบบรักษาความปลอดภัยบนเว็บลดลงกว่า 10 เปอร์เซ็นต์ ซึ่งบ่งชี้ถึงความเสี่ยงต่อองค์กรต่างๆ อันเนื่องมาจากจุดอ่อนบนโครงสร้าง

• เอาต์ซอร์สเพิ่มขึ้นอย่างต่อเนื่อง: ภายใต้แนวโน้มในการแก้ไขปัญหาการขาดแคลนบุคลากร องค์กรทุกขนาดตระหนักถึงคุณประโยชน์ของบริการเอาต์ซอร์สที่ช่วยเสริมสร้างความปลอดภัย ไม่ว่าจะเป็นบริการให้คำปรึกษา การตรวจสอบระบบรักษาความปลอดภัย และการตอบสนองต่อกรณีปัญหาที่เกิดขึ้น ธุรกิจ SMB ซึ่งมักจะขาดแคลนทรัพยากรสำหรับการรักษาความปลอดภัยอย่างมีประสิทธิภาพ กำลังดำเนินการปรับปรุงแนวทางด้านความปลอดภัยด้วยการใช้บริการเอาต์ซอร์ส ซึ่งมากถึง 23 เปอร์เซ็นต์ในปี 2558 เปรียบเทียบกับ 14 เปอร์เซ็นต์ในปีก่อนหน้า

• การเปลี่ยนไปโจมตีเซิร์ฟเวอร์: อาชญากรออนไลน์ได้เปลี่ยนไปโจมตีเซิร์ฟเวอร์ที่มีช่องโหว่ เช่น เซิร์ฟเวอร์ของ WordPress เพื่อสนับสนุนการโจมตี โดยใช้ประโยชน์จากแพลตฟอร์มโซเชียลมีเดียเพื่อจุดประสงค์ร้าย ตัวอย่างเช่น จำนวนโดเมน WordPress ที่อาชญากรใช้เพิ่มขึ้นถึง 221 เปอร์เซ็นต์ในช่วงเดือนกุมภาพันธ์ถึงตุลาคม 2558

• การรั่วไหลของข้อมูลบนเบราว์เซอร์: แม้ว่าทีมงานฝ่ายรักษาความปลอดภัยมักจะมองว่าส่วนขยายของเบราว์เซอร์ที่เป็นอันตราย (malicious browser extensions) ถือเป็นภัยคุกคามระดับต่ำ แต่ก็อาจเป็นช่องทางที่ทำให้ข้อมูลรั่วไหล โดยส่งผลกระทบต่อองค์กรต่างๆ มากกว่า 85 เปอร์เซ็นต์ แอดแวร์ (Adware), โฆษณาที่มีมัลแวร์แฝงอยู่ (Malvertising) และแม้กระทั่งเว็บไซต์ทั่วไปหรือคอลัมน์แจ้งข่าวมรณกรรม อาจนำไปสู่ปัญหาข้อมูลรั่วไหลสำหรับผู้ใช้ที่ไม่ได้อัพเดตซอฟต์แวร์อย่างสม่ำเสมอ

• จุดบอดของ DNS (Domain Name Service) : เกือบ 92 เปอร์เซ็นต์ของมัลแวร์ “อันตราย” ใช้ DNS เป็นความสามารถหลักมักจะเป็น “จุดบอด” ด้านความปลอดภัย เพราะโดยทั่วไปแล้วทีมงานฝ่ายรักษาความปลอดภัยและผู้

เชี่ยวชาญ DNS ทำงานในกลุ่มไอทีคนละกลุ่มภายในบริษัท และไม่ค่อยได้ประสานงานร่วมกัน

• ตรวจจับได้รวดเร็วขึ้น: แวดวงอุตสาหกรรมประเมินว่าเวลาที่ใช้ในการตรวจจับอาชญากรรมไซเบอร์อยู่ที่ประมาณ 100 ถึง 200 วัน ซึ่งถือเป็นระยะเวลาที่นานเกินไปจนไม่อาจยอมรับได้ ซิสโก้ได้ลดระยะเวลาดังกล่าวจาก 46 เป็น 17.5 ชั่วโมง นับตั้งแต่ที่รายงานด้านความปลอดภัยกลางปี 2558 ของซิสโก้ถูกตีพิมพ์เผยแพร่ การลดระยะเวลาการตรวจจับจะช่วยลดความเสียหายจากการโจมตีทางไซเบอร์ ลดความเสี่ยงและผลกระทบต่อลูกค้า และโครงสร้างพื้นฐานทั่วโลก

• ความน่าเชื่อถือคือสิ่งสำคัญ: ขณะที่องค์กรต่างๆ ปรับเปลี่ยนการดำเนินงานสู่ระบบดิจิตอลเพิ่มมากขึ้น ข้อมูล อุปกรณ์ เซ็นเซอร์ และบริการต่างๆ จึงมีจำนวนเพิ่มขึ้น และก่อให้เกิดความต้องการใหม่ๆ สำหรับความโปร่งใส ความน่าเชื่อถือ และความไว้วางใจสำหรับลูกค้า

หากต้องการสำเนาฉบับสมบูรณ์ของรายงานด้านความปลอดภัยประจำปี 2559 ของซิสโก้ และอ่านรายละเอียดเพิ่มเติมเกี่ยวกับคำแนะนำของซิสโก้ในเรื่องแนวทางสำหรับองค์กรธุรกิจในการลดความเสี่ยง คลิกที่นี่

เกี่ยวกับรายงาน
รายงานด้านความปลอดภัยประจำปี 2559 ของซิสโก้ วิเคราะห์แนวโน้มและปัญหาสำคัญๆ ในด้านไซเบอร์ซีเคียวริตี้จากผู้เชี่ยวชาญด้านความปลอดภัยของซิสโก้ในประเด็นที่เกี่ยวกับความก้าวหน้าของอุตสาหกรรมการรักษาความปลอดภัยและอาชญากรที่พยายามเล็ดลอดผ่านระบบป้องกัน นอกจากนี้ รายงานฉบับนี้ยังเน้นย้ำผลการศึกษาเบนช์มาร์กเกี่ยวกับความสามารถด้านความปลอดภัย (Security Capabilities Benchmark Study) ฉบับที่สองของซิสโก้ ซึ่งมุ่งตรวจสอบการรับรู้ของบุคลากรฝ่ายรักษาความปลอดภัยในเรื่องที่เกี่ยวกับสถานะด้านความปลอดภัยขององค์กร และยังมีการกล่าวถึงแนวโน้มทางภูมิศาสตร์การเมือง ข้อมูลเชิงลึกเกี่ยวกับการรับรู้เรื่องความเสี่ยงด้านไซเบอร์ซีเคียวริตี้และความเชื่อมั่น และข้อคิดเห็นเกี่ยวกับการป้องกันภัยคุกคามอย่างครบวงจร

คำกล่าวสนับสนุน

• จอห์น เอ็นสจ๊วต, รองประธานอาวุโสฝ่ายรักษาความปลอดภัยของซิสโก้

“ระบบการรักษาความปลอดภัยควรปรับสภาพได้ตามการออกแบบ ความเป็นส่วนตัว และความรับผิดชอบที่โปร่งใส ด้วย IoT ที่เกิดขึ้นในทุกธุรกิจ ความสามารถในการใช้เทคโนโลยีจะต้องสร้าง ลงทุน และดำเนินการได้ในทุกภาคส่วน เราไม่ควรสร้างหนี้ที่เกิดจากการใช้เทคโนโลยีอีกต่อไป แต่เราต้องเผชิญความท้าทายที่เกิดขึ้นในทุกวันนี้”

• คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการประจำประเทศไทยและภูมิภาคอินโดจีนของซิสโก้

“แนวโน้ม IoT และ Digitization เข้ามามีบทบาทสำคัญในทุกธุรกิจ ด้วยเหตุนี้ความสามารถด้านการรักษาความปลอดภัยจึงต้องถูกสร้างขึ้น และใช้งานในทุกภาคธุรกิจ ขณะที่ภัยคุกคามส่วนใหญ่ยังคงมีอยู่อย่างต่อเนื่อง ข้อมูล

เชิงลึกในรายงาน Annual Security Report ของซิสโก้ชี้ให้เห็นว่าผู้โจมตีมีการสร้างสรรค์นวัตกรรมใหม่ๆ อย่างต่อเนื่อง เพื่อใช้ประโยชน์จากช่องโหว่ด้านความปลอดภัย และมีการใช้ทรัพยากรออนไลน์ที่ถูกกฎหมายเพื่อทำการโจมตีเพิ่มมากขึ้น ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (ThaiCERT) เปิดเผยว่า คนไทย 48% มีความเสี่ยงในเรื่องความปลอดภัยทางออนไลน์ และมีการรายงานปัญหาด้านไซเบอร์ซีเคียวริตี้ 2,534 กรณีในช่วง 6 เดือนที่ผ่านมา โดยครอบคลุมถึงปัญหาการปลอมแปลง การบุกรุก และโค้ดอันตราย ขณะที่การลงทุนด้านการรักษาความปลอดภัยเพิ่มขึ้น แต่ไซเบอร์ซีเคียวริตี้มีความซับซ้อนมากขึ้น และผู้โจมตีไม่เคยละความพยายามที่จะโจมตีองค์กรธุรกิจในแต่ละปี

ทุกวันนี้มาตรการด้านการรักษาความปลอดภัยจะต้องมีความสอดคล้องกับทิศทางธุรกิจ มีการปรับใช้อย่างเหมาะสมในระดับโครงสร้าง และผสานรวมเข้าด้วยกันอย่างกลมกลืน ผู้บริหารระดับสูงในองค์กรต่างๆ จำเป็นต้องรับทราบและปรับใช้กลยุทธ์ด้านความปลอดภัย เพื่อเตรียมพร้อมรับมือกับภัยคุกคามที่ไม่คาดคิด ขณะที่บริษัทไอทีจะต้องพัฒนาโซลูชั่นที่เชื่อถือได้สำหรับลูกค้า”

ทรัพยากรสนับสนุน
วิดีโอของ Cisco Security
รายงานด้านความปลอดภัยประจำปีของซิสโก้
บล็อก Cisco Security
อินโฟกราฟิกของซิสโก้
ติดตามซิสโก้บน Twitter @CiscoSecurity
กดถูกใจ Cisco Security บน Facebook

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