ซิสโก้เผยรายงานความปลอดภัยประจำปี ชี้ “การโจมตีขั้นสูงและแทรฟฟิกอันตราย” เพิ่มขึ้นอย่างที่ไม่เคยเกิดขึ้นมาก่อน

ภัยคุกคามขยายตัวโดยการโจมตี Surface ด้วยเทคนิคใหม่ๆ

กรุงเทพฯ, ประเทศไทย - 17 มีนาคม 2557 — รายงานด้านความปลอดภัยของซิสโก้ ประจำปี 2557 (Cisco 2014 Annual Security Report) เปิดเผยว่าภัยคุกคามที่ใช้ประโยชน์จากความไว้ใจในระบบของผู้ใช้ รวมถึง แอพพลิเคชั่น และเครือข่ายส่วนบุคคล มีปริมาณเพิ่มสูงขึ้นจนน่าตกใจ รายงานดังกล่าวระบุว่าปัญหาการขาดแคลนบุคลากรผู้เชี่ยวชาญด้านการรักษาความปลอดภัยเกือบหนึ่งล้านคนทั่วโลกส่งผลกระทบต่อความสามารถขององค์กรในการตรวจสอบและคุ้มครองเครือข่าย ขณะที่จุดอ่อนและภัยคุกคามโดยรวมเพิ่มขึ้นจนถึงระดับสูงสุดนับตั้งแต่ปี 2543 เป็นต้นมา

ข้อมูลที่พบในรายงานดังกล่าวนำเสนอภาพที่ชัดเจนของปัญหาและความท้าทายด้านความปลอดภัยที่มีการพัฒนาเปลี่ยนแปลงอย่างรวดเร็ว ซึ่งองค์กรธุรกิจ ฝ่ายไอที และผู้ใช้ต้องประสบพบเจอ ผู้โจมตีใช้วิธีการต่างๆ เช่น การขโมยรหัสผ่านและข้อมูลผู้ใช้ (Credentials) การแทรกซึมแบบแฝงเร้น (Hide-in-plain-sight infiltrations) และการใช้ประโยชน์จากความไว้วางใจเมื่อทำธุรกรรมทางเศรษฐกิจ บริการภาครัฐ และการติดต่อสื่อสารทางสังคม

ประเด็นสำคัญในรายงานความปลอดภัยประจำปี

- **ความซับซ้อนที่เพิ่มขึ้นและการแพร่กระจายของภัยคุกคาม** การโจมตีอย่างง่ายๆ ที่สร้างความเสียหายในระดับที่ควบคุมได้เริ่มถูกแทนที่ด้วยปฏิบัติการที่เป็นระบบของกลุ่มอาชญากรในโลกไซเบอร์ โดยมีลักษณะซับซ้อน ก้าวล้ำ มีเงินทุนสนันสนุนที่ดี และสามารถสร้างความเสียหายทางเศรษฐกิจและทำลายชื่อเสียงอย่างมากต่อองค์กรภาครัฐและภาคเอกชนที่ตกเป็นเหยื่อ
- **ความซับซ้อนของภัยคุกคามและโซลูชั่นเพิ่มมากขึ้น เนื่องจากอุปกรณ์พกพาอัจฉริยะและคลาวด์คอมพิวติ้งเติบโตอย่างรวดเร็ว ส่งผลให้มีพื้นที่การโจมตีกว้างขวางมากขึ้นอย่างที่ไม่เคยมีมาก่อ**

น อุปกรณ์ชนิดใหม่และสถาปัตยกรรมโครงสร้างแบบใหม่เปิดโอกาสให้ผู้โจมตีสามารถใช้ประโยชน์จากจุดอ่อนที่คาดไม่ถึงและทรัพยากรที่ไม่ได้รับการปกป้องอย่างเพียงพอ

- **กลุ่มอาชญากรไซเบอร์ได้เรียนรู้ว่าการใช้ประโยชน์จากพลังของโครงสร้างพื้นฐานอินเทอร์เน็ตให้ประโยชน์มากมายมหาศาล**กว่าการเข้าถึงเพียงแค่คอมพิวเตอร์หรืออุปกรณ์ของผู้ใช้ การโจมตีในระดับโครงสร้างพื้นฐานนี้มุ่งที่จะเข้าถึงเว็บโฮสติ้งเซิร์ฟเวอร์ที่สำคัญ รวมไปถึงเนมเซิร์ฟเวอร์ และดาต้าเซ็นเตอร์ โดยมีเป้าหมายที่จะแพร่กระจายการโจมตีไปสู่อุปกรณ์ของผู้ใช้ที่ใช้บริการจากทรัพยากรเหล่านี้ ด้วยการพุ่งเป้าไปที่โครงสร้างพื้นฐานอินเทอร์เน็ต ผู้โจมตี (Attackers) จะทำลายความไว้วางใจในทุกสิ่งที่เชื่อมต่อหรืออาศัยโครงสร้างพื้นฐานดังกล่าว

ข้อมูลสำคัญที่พบในรายงานด้านความปลอดภัยของซิสโก้

- **จุดอ่อนและภัยคุกคามโดยรวม<u>แตะระดับสูงสุด</u>** นับตั้งแต่ที่มีการตรวจสอบเป็นครั้งแรกเมื่อเดือนพฤษภาคม 2543 และ ณ เดือนตุลาคม 2556 **ภัยคุกคามโดยรวมแตะระดับสูงสุด**ที่ 14 **เป**อร์เซ็นต์เมื่อเทียบกับปี 2555
- **รายงานระบุถึง 'ปัญหาการขาดแคลนบุคลากรด้านความปลอดภัย' กว่าหนึ่งล้านคน**ทั่วโลกในปี 2557 ความซับซ้อนของเทคโนโลยีและเทคนิคที่อาชญากรออนไลน์ใช้ รวมถึงความพยายามอย่างไม่หยุดยั้งในการเจาะระบบเครือข่ายและโจรกรรมข้อมูล ได้แซงหน้าความสามารถของบุคลากรฝ่ายไอทีและฝ่ายรักษาความปลอดภัยในการรับมือกับภัยคุกคาม องค์กรส่วนใหญ่ไม่มีบุคลากรหรือระบบสำหรับตรวจสอบเครือข่ายขนาดใหญ่อย่างต่อเนื่อง รวมทั้งตรวจจับการแทรกซึม แล้วปรับใช้มาตรการป้องกันอย่างทันท่วงทีและมีประสิทธิภาพ
- **100 เปอร์เซ็นต์ของ 30 กลุ่มตัวอย่างที่เป็นบริษัทข้ามชาติที่ใหญ่ที่สุดในโลก สร้าง แทรฟฟิกของผู้เยี่ยมชม (visitors) ไปยังเว็บไซต์ที่มีมัลแวร์** ทั้งนี้ 96 เปอร์เซ็นต์ของบริษัทเหล่านี้มีการส่งแทรฟฟิกไปยังเซิร์ฟเวอร์ที่ถูกใช้เป็นช่องทางในการโจมตี (Hijacked Server) ในทำนองเดียวกัน 92 เปอร์เซ็นต์ส่งแทรฟฟิกไปยังเว็บเพจที่ไม่มีเนื้อหาใดๆ ซึ่งโดยปกติแล้วจะรองรับกิจกรรมที่เป็นอันตราย
- **การโจมตีแบบ Distributed Denial of Service (DDoS)**– การโจมตีนี้สามารถขัดขวางแทรฟฟิกที่ไปและมาจากเว็บไซต์เป้าหมาย และสามารถทำให้ ISP กลายเป็นอัมพาต การโจมตีนี้ได้ยกระดับสูงขึ้นทั้งในแง่ของปริมาณและความรุนแรง และบางครั้งพยายามที่จะปิดบังกิจกรรมที่ชั่วร้ายอื่นๆ เช่น ลักลอบโอนเงินก่อน / ระหว่าง หรือหลังการโจมตี DDoS ที่ใช้เป็นฉากบังหน้าหรือเบี่ยงเบนความสนใจ
- **โทรจันอเนกประสงค์ถือเป็นมัลแวร์บนเว็บที่พบเจอบ่อยครั้งที่สุด** ด้วยสัดส่วน 27 เปอร์เซ็นต์ของ

มัลแวร์ทั้งหมดที่พบในปี 2556 สคริปต์อันตราย เช่น โปรแกรมสำหรับเจาะช่องโหว่ (Exploit) และ iframe เป็นหมวดหมู่ที่พบมากที่สุดเป็นอันดับสองที่ 23 เปอร์เซ็นต์ โทรจันสำหรับโจรกรรมข้อมูล เช่น โปรแกรมขโมยรหัสผ่าน และการสร้างประตูลับ (Backdoor) ครอบคลุมสัดส่วน 22 เปอร์เซ็นต์ของมัลแวร์บนเว็บทั้งหมดที่พบ การลดลงอย่างต่อเนื่องในโฮสต์มัลแวร์และไอพีแอดเดรสที่แตกต่าง นั่นคือ ลดลง 30 เปอร์เซ็นต์ระหว่างเดือนมกราคม 2556 ถึงเดือนกันยายน 2556 แสดงให้เห็นว่ามัลแวร์มีการกระจุกตัวอยู่ในโฮสต์และไอพีแอดเดรสเพียงไม่กี่รายการ

- **Java ยังคงเป็นภาษาโปรแกรมที่ถูกใช้เป็นช่องทางการโจมตีมากที่สุด** โดยเป็นเป้าหมายหลักของอาชญากรออนไลน์ ข้อมูลจาก Sourcefire ซึ่งตอนนี้เป็นส่วนหนึ่งของซิสโก้ แสดงให้เห็นว่า Java ครองสัดส่วนเกือบทั้งหมด (91 เปอร์เซ็นต์) ของตัวบ่งชี้ความเสี่ยงของระบบคอมพิวเตอร์ (Indicators of Compromise – IOC)
- **99 เปอร์เซ็นต์ของมัลแวร์แบบโมบายล์ทั้งหมดพุ่งเป้าโจมตีอุปกรณ์ Android** ที่ 43.8 เปอร์เซ็นต์ Andr/Qdplugin-A คือโมบายล์มัลแวร์ที่พบเจอมากที่สุด โดยปกติแล้วอยู่ในรูปแบบของสำเนาที่มีการปรับเปลี่ยนของแอพที่ถูกกฎหมายซึ่งเผยแพร่ผ่านตลาดที่ไม่เป็นทางการ
- **ภาคธุรกิจที่เฉพาะเจาะจง** เช่น อุตสาหกรรมยาและเคมีภัณฑ์ และอุตสาหกรรมการผลิตชิ้นส่วนอิเล็กทรอนิกส์ มีอัตราการพบเจอมัลแวร์ที่สูงมากในอดีตที่ผ่านมา แต่ในปี 2555 และ 2556 จำนวนครั้งของการพบเจอมัลแวร์เพิ่มสูงขึ้นอย่างมากในภาคเกษตรกรรมและเหมืองแร่ ทั้งๆ ที่เมื่อก่อนนี้เป็นภาคธุรกิจที่มีความเสี่ยงต่ำ นอกจากนี้ การพบเจอมัลแวร์เพิ่มสูงขึ้นอย่างต่อเนื่องในธุรกิจพลังงาน น้ำมัน และก๊าซ

คำกล่าวสนับสนุน

- **คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการประจำประเทศไทยและอินโดจีนของซิสโก้**

"ผลการสำรวจจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ., ประเทศไทย, 2556) ชี้ว่าจำนวนผู้ใช้อินเทอร์เน็ตในประเทศไทยเพิ่มขึ้นอย่างมีนัยยะสำคัญในแต่ละปี เมื่อสิ้นปี 2556 มีผู้ใช้อินเทอร์เน็ต 25 ล้านคน และผู้ใช้โทรศัพท์เคลื่อนที่ 87 ล้านคน จากจำนวนประชากรทั้งหมด 64 ล้านคน ดังนั้นแนวโน้มดังกล่าวนี้จึงนำไปสู่ภัยคุกคามด้านความปลอดภัยทางไซเบอร์ทั้งโดยตั้งใจและไม่ตั้งใจ รายงานความปลอดภัยประจำปีของซิสโก้เน้นย้ำถึงรูปแบบภัยคุกคามทั่วโลกและแนวโน้มด้านความปลอดภัย ในช่วงเริ่มต้นของ 'Internet of Everything' (IoE) นี้ การเติบโตของ IoE จะเป็นปัจจัยหลักที่ผลักดันการขยายตัวอย่างรวดเร็วของภัยคุกคามที่ซับซ้อน โดยจะส่งผลกระทบต่อบุคคลทั่วไปและองค์กรธุรกิจ ซิสโก้ประเมินว่าภายในปี 2563 จะมีวัตถุต่างๆ ทั่วโลกกว่า 5 หมื่นล้านชิ้นถูกเชื่อมต่อเข้าด้วยกัน และเป็นไปไม่ได้ที่เราจะติดตั้งระบบรักษาความปลอดภัยไว้ในวัตถุทุกชิ้น ดังนั้นเราจึงต้องเตรียมพร้อมรับมือกับภัยคุกคามที่จะเกิดขึ้นกับอุปกรณ์ที่เชื่อมต่อ"

“ภัยคุกคามไซเบอร์สามารถพบได้ทุกที่ และเป็นภัยคุกคามหลักต่อความมั่นคงของประเทศ รวมไปถึงสังคม เศรษฐกิจ องค์กรต่างๆ และบุคคลทั่วไป วันนี้ชีวิตการทำงานและเรื่องส่วนตัวของเรามีการผสมผสานโดยใช้อุปกรณ์ที่หลากหลายในที่ทำงาน ซึ่งนอกจากจะเป็นภัยคุกคามต่อผู้ใช้ทั่วไปแล้ว ยังอาจก่อให้เกิดอันตรายต่อองค์กรด้วย รายงานความปลอดภัยประจำปีของซิสโก้ระบุถึงแนวโน้มในเรื่องความปลอดภัยที่เราจำเป็นต้องจัดการในปัจจุบัน แม้ว่ารายงานดังกล่าวจะแสดงภาพที่น่ากลัวเกี่ยวกับสถานะปัจจุบันของความปลอดภัยในโลกไซเบอร์ แต่ก็ยังพอมีความหวังสำหรับการฟื้นฟูความเชื่อมั่นเกี่ยวกับบุคลากร สถาบัน และเทคโนโลยี โดยจะต้องเริ่มต้นจากการเสริมสร้างศักยภาพของบุคลากรที่เกี่ยวข้องด้วยการให้ความรู้เกี่ยวกับพื้นที่การโจมตีที่ขยายใหญ่ขึ้นอย่างต่อเนื่อง เพื่อต่อสู้กับการโจมตีทุกรูปแบบอย่างมีประสิทธิภาพ ฝ่ายรักษาความปลอดภัยจะต้องเข้าใจเกี่ยวกับผู้โจมตี รวมถึงแรงจูงใจและวิธีการที่ใช้ ทั้งก่อน ระหว่าง และหลังการโจมตีนอกจากนี้ รายงานของโครงการจัดตั้งศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (Thai Computer Emergency Response Team หรือ ThaiCERT) ซึ่งเป็นสมาชิกของสพธอ. ระบุว่าในปี 2556, 39.6 เปอร์เซ็นต์ของอาชญากรรมออนไลน์เกี่ยวข้องกับการฉ้อโกง (Fraud) ขณะที่ 37.8 เปอร์เซ็นต์ และ 17 เปอร์เซ็นต์เกี่ยวข้องกับการบุกรุก (Intrusion) และความพยายามที่จะบุกรุก (Intrusion Attempt) ตามลำดับ ทั้งนี้ได้รับรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์เกือบ 1,800 ครั้ง โดยครอบคลุมถึงไวรัส, เวิร์ม และการดำเนินการโดยแฮคเกอร์

“ประเทศไทยสนับสนุนความร่วมมือในภูมิภาคอาเซียนอย่างเต็มที่เพื่อต่อสู้กับอาชญากรรมในโลกไซเบอร์ ซึ่งถือเป็น 1 ใน 8 ภารกิจสำคัญของอาเซียนในการปราบปรามอาชญากรรมข้ามประเทศ ในสภาพการณ์ดังกล่าวนี้ องค์กรธุรกิจของไทยจำเป็นที่จะต้องทบทวนกลยุทธ์และนโยบายด้านการรักษาความปลอดภัยที่สอดรับกับความต้องการทางด้านธุรกิจ ขณะที่หน่วยงานราชการจำเป็นที่จะต้องพัฒนากรอบนโยบายด้านความปลอดภัยทางไซเบอร์ที่ครอบคลุมประเด็นต่างๆ เช่น ธรรมาภิบาล ความพร้อมในกรณีฉุกเฉิน โครงสร้างพื้นฐานสารสนเทศระดับชาติ และการเพิ่มขีดความสามารถด้านความปลอดภัย”

ทรัพยากรสนับสนุน

- ดูรายงานด้านความปลอดภัยประจำปีของซิสโก้ได้ที่ที่นี่ : http://www.cisco.com/web/offers/lp/2014-annual-security-report/
- วิดีโอ: จอห์น เอ็น. สจ๊วต กับประเด็นเรื่องความไว้วางใจ: https://www.youtube.com/watch?v=BrsL0rJPXMk
- เข้าร่วมการสนทนาเรื่องความปลอดภัยบนทวิตเตอร์ ด้วยการติดตาม @CiscoSecurity และคลิกถูกใจ Cisco Security บนเฟซบุ๊คที่ http://facebook.com/ciscosecurity
- อ่านบล็อกของซิสโก้

เกี่ยวกับรายงาน

รายงานด้านความปลอดภัยประจำปี 2557 ของซิสโก้ระบุแนวโน้มด้านความปลอดภัยที่สำคัญที่สุดในรอบปี และแนะนำแนวทางในการดูแลเทคโนโลยีขององค์กรให้ปลอดภัยมากขึ้น ซิสโก้แบ่งปันข้อมูลเกี่ยวกับภัยคุกคามล่าสุดโดยใช้ข้อมูลข่าวกรองเรื่องภัยคุกคามในแบบเรียลไทม์จากฝ่ายปฏิบัติการด้านข้อมูลความปลอดภัย (Security Intelligence Operations – SIO) ของซิสโก้ และรายงานในปีนี้ยังผสานรวมเครื่องมือของ Sourcefire อีกด้วย Cisco SIO เป็น อีโคซิสเต็มส์ด้านความปลอดภัยที่เป็น Cloud-based ที่ใหญ่ที่สุดในโลก โดยใช้ฟีดข้อมูล (Live data) มากกว่า 75 เทราบิตจากโซลูชั่นอีเมล, เว็บ, ไฟร์วอลล์ และโซลูชั่นป้องกันการบุกรุก (IPS)

เกี่ยวกับซิสโก้:

ซิสโก้ (NASDAQ: CSCO) เป็นผู้นำระดับโลกด้านไอทีที่ช่วยให้ธุรกิจและบริษัทต่างๆสร้างสรรค์สิ่งมหัศจรรย์และปรากฏการณ์ใหม่ๆที่เกิดจากการเชื่อมต่อ (connect) ดูข่าวและข้อมูลเพิ่มเติมเกี่ยวกับ

ซิสโก้ได้ที่ http://thenetwork.cisco.com ผลิตภัณฑ์ซิสโก้ในประเทศไทยจัดจำหน่ายผ่านช่องทางการจัดจำหน่ายโดยพาร์ทเนอร์ของ Cisco Systems International B.V ซึ่งเป็นเจ้าของบริษัทในเครือซิสโก้ ซีสเต็มส์ ทั้งหมด