ทำไมการรักษาความปลอดภัยแบบ “มุ่งเน้นที่ภัยคุกคามเป็นหลัก” (Threat-Centric Security)

ทำไมการรักษาความปลอดภัยแบบ “มุ่งเน้นที่ภัยคุกคามเป็นหลัก” (Threat-Centric Security) จึงจำเป็นสำหรับองค์กร ‘ทุกขนาด’ ในวันนี้

โดย นาย วัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการซิสโก้ประจำประเทศไทย และภูมิภาคอินโดจีน

องค์กรทุกขนาดจะต้องเตรียมพร้อมรับมือกับการโจมตีที่ซับซ้อนมากขึ้น และจะต้องประเมินระบบป้องกันและมาตรการที่มีอยู่ เพื่อต่อสู้กับการโจมตีแบบเจาะจงเป้าหมายที่แพร่กระจายเป็นวงกว้าง ผู้โจมตีกำลังใช้วิธีการก้าวล้ำมากขึ้นในการแทรกซึมเข้าสู่องค์กรขนาดเล็กและขนาดใหญ่ โดยครอบคลุมตั้งแต่องค์กรขนาดเล็ก (พนักงาน 2 50-500 คน) ไปจนถึงองค์กรขนาดกลาง (พนักงาน 500-999 คน) และองค์กรขนาดใหญ่ที่มีพนักงาน 1,000 คนขึ้นไป แน่นอนว่าเราได้ยินเรื่องราวมากมายเกี่ยวกับการเจาะระบบรักษาความปลอดภัยที่ส่งผลกระทบต่อองค์กรขนาดใหญ่ที่มีชื่อเสียงตามที่ปรากฏผ่านสื่อ อย่างไรก็ตาม ผู้โจมตีมักมองหาหนทางที่จะสร้างผลตอบแทนผ่านช่องทางที่หลากหลาย เช่นเดียวกับการดำเนินธุรกิจทั่วไป และโดยมากแล้ว วิธีที่ดีที่สุดสำหรับผู้โจมตีในการสร้างผลกำไรสูงสุดและลดความเสี่ยงให้เหลือน้อยที่สุดก็คือ “การโจมตีองค์กรธุรกิจขนาดเล็กและขนาดกลางอย่างต่อเนื่อง” แทนที่จะมุ่งโจมตีองค์กรขนาดใหญ่เพียงองค์กรเดียว
จะเห็นว่าผู้โจมตีใช้วิธีการที่ซับซ้อนมากขึ้นในการโจมตีองค์กรทุกขนาด โดย รายงานความปลอดภัยประจำปี 2558 ของซิสโก้ ระบุว่า แนวโน้มที่เพิ่มมากขึ้นในขณะนี้ก็คือ ผู้โจมตีใช้ประโยชน์จากช่องโหว่ในระบบรักษาความปลอดภัย เพื่อหลบเลี่ยงการตรวจจับและปกปิดกิจกรรมที่เป็นอันตราย โดยมีประเด็นสำคัญคือ:
• Snowshoe Spam เป็นวิธีการโจมตีที่ได้รับความนิยมเพิ่มขึ้น โดยผู้โจมตีจะส่งสแปมจำนวนน้อยจากชุดไอพีแอดเดรสจำนวนมาก เพื่อหลีกเลี่ยงการตรวจจับ และเพิ่มโอกาสในการเจาะบัญชีผู้ใช้ที่มีช่องโหว่ในหลายๆ ทาง

• เครื่องมือโจมตีที่ใช้งานกันอย่างกว้างขวางมักจะถูกตรวจจับโดยบริษัทรักษาความปลอดภัย ด้วยเหตุนี้อาชญากรออนไลน์จึงหันไปใช้ “ชุดเครื่องมือที่ไม่ค่อยได้รับความนิยม” ซึ่งนับว่าเป็นวิธีการที่ยั่งยืน เพราะไม่ค่อยมีใครสนใจมากนัก

• ในอดีต Flash และ JavaScript ขาดความปลอดภัยในตัวมันเอง แต่ด้วยความก้าวหน้าในการตรวจจับและป้องกันภัยคุกคาม ผู้โจมตีจึงต้องปรับเปลี่ยน ด้วยการใช้เครื่องมือที่โจมตีจุดอ่อนหลายๆ ส่วน เช่น การเผยแพร่มัลแวร์ด้วยสองไฟล์ที่แตกต่างกัน นั่นคือ ไฟล์ Flash และไฟล์ JavaScript จะทำให้เป็นเรื่องยากมากขึ้นสำหรับอุปกรณ์การรักษาความปลอดภัยที่จะระบุและปิดกั้นภัยคุกคามดังกล่าว และวิเคราะห์ด้วยเครื่องมือถอดรหัสโปรแกรม

บุคลากรจากองค์กรต่างๆ มักจะขอให้แนะนำวิธีการต่อสู้กับภัยคุกคามที่ซับซ้อนเหล่านี้ และไม่ว่าจะเป็นองค์กรขนาดเล็กหรือใหญ่ คำตอบของเราก็ยังคงเน้นย้ำถึง 1) ความจำเป็นในการปรับใช้แนวทางที่มุ่งเน้นภัยคุกคามและการปฏิบัติงาน ซึ่งจะช่วยลดความยุ่งยากซับซ้อนและการแยกกระจัดกระจาย ควบคู่ไปกับ 2) การจัดหาเทคโนโลยีที่มีความสามารถในการตรวจสอบที่เหนือกว่า การควบคุมอย่างต่อเนื่อง และ 3) การป้องกันภัยคุกคามอย่างเหนือชั้นโดยครอบคลุมเครือข่ายและขอบเขตการโจมตีทั้งหมด โดยมากแล้ว ลูกค้ามักจะเลือกใช้ระบบรักษาความปลอดภัยที่ “ดีพอใช้” ในจุดสำคัญๆ เช่น ระบบอีเมล หรืออุปกรณ์รักษาความปลอดภัยบนเว็บ แนวทางนี้อันตรายอย่างมาก เพราะปัญหาข้อมูลรั่วไหลเพียงครั้งเดียว ก็อาจทำให้องค์กรธุรกิจขนาดกลางและขนาดเล็กที่มีสถานะแข็งแกร่งต้องเลิกกิจการ ซึ่งนับว่าไม่คุ้มค่าเลยกับการเลือกซื้อโซลูชั่นความปลอดภัยที่ถูกกว่า โดยคนร้ายก็เริ่มตระหนักและใช้ประโยชน์จากช่องโหว่นี้เพิ่มมากขึ้น

การรักษาความปลอดภัยแบบมุ่งเน้นที่ภัยคุกคามเป็นหลัก ไม่ได้เป็นเพียงแค่นโยบายหรือมาตรการควบคุมเท่านั้น การปรับใช้แนวทางนี้จะช่วยให้บุคลากรฝ่ายรักษาความปลอดภัยสามารถรับมือกับการโจมตีได้ในทุกขั้นตอน โดยครอบคลุมทุกช่องทางการโจมตี และตอบสนองได้ทุกเวลาอย่างทันท่วงที ไม่ว่าเครือข่ายที่คุ้มครองจะมีขนาดเท่าใดก็ตาม

ไม่ว่าคุณจะปกป้ององค์กรขนาดกลาง สำนักงานที่อยู่ไกลออกไป หรือองค์กรที่มีสาขาหลายแห่ง คุณจะต้องเผชิญกับการโจมตีที่ทำให้ข้อมูลสำคัญตกอยู่ในภาวะเสี่ยง และอาจก่อให้เกิดความเสียหายอย่างมาก อย่างไรก็ดี ไม่ว่าองค์กรของคุณจะมีขนาดเล็กหรือใหญ่ คุณก็มีหน้าที่ความรับผิดชอบในแง่ของกฎหมายและความไว้วางใจสำหรับการปกป้องข้อมูลที่มีค่าของลูกค้า รวมไปถึงทรัพย์สินทางปัญญา และข้อมูลลับขององค์กร

การรักษาความปลอดภัยมีความสำคัญต่อธุรกิจเพิ่มมากขึ้นอย่างที่ไม่เคยมีมาก่อน การโจมตีที่เพิ่มขึ้นอย่างมากและกฎระเบียบที่เข้มงวดมากขึ้นส่งผลให้ประเด็นเรื่องความปลอดภัยของข้อมูลถูกหยิบยกขึ้นหารือในที่ประชุมคณะกรรมการบริหารขององค์กรทุกขนาด ตามข้อมูลที่ได้รับจากผู้เชี่ยวชาญด้านความปลอดภัยใน 9 ประเทศ ผลการศึกษาเกี่ยวกับเกณฑ์การตรวจวัดความสามารถด้านการรักษาความปลอดภัยของซิสโก้ (Cisco Security Capabilities Benchmark Study) ซึ่งรวมอยู่ในรายงานความปลอดภัยประจำปี 2558 ของซิสโก้ เปิดเผยถึงช่องว่างระหว่างความคิดเห็นกับความเป็นจริง ทั้งยังระบุว่า “บริษัทขนาดกลางมีการรับรู้ที่ดีกว่าบริษัทขนาดใหญ่” ผลการศึกษาดังกล่าวชี้ว่า มีความแตกต่างน้อยมากระหว่างองค์กรขนาดกลาง (พนักงาน 500-999 คน) และองค์กรขนาดใหญ่ (พนักงาน 1000 คนขึ้นไป) ในแง่ของความพร้อมในการตอบสนองต่อปัญหาด้านความปลอดภัย องค์กรขนาดกลางมีทัศนะใกล้เคียงกับองค์กรขนาดใหญ่ อย่างไรก็ตาม ในองค์กรที่ผู้บริหารไม่ให้ความสำคัญกับเรื่องของความปลอดภัยมากนัก พบว่าระบบรักษาความปลอดภัยในองค์กรดังกล่าวก็มีความก้าวล้ำในระดับที่ต่ำกว่าองค์กรอื่นๆ เป็นอย่างมาก นอกจากนี้ ยังมีช่องว่างในเรื่องความสามารถของบริษัทในการกำหนดขอบเขตและควบคุมปัญหาความเสี่ยงภายในเวลาอันรวดเร็ว โดยเป็นผลมาจากข้อจำกัดของระบบรักษาความปลอดภัยจำนวนมากที่มุ่งเน้นการตรวจจับในช่วงเวลาปัจจุบัน องค์กรทุกขนาดควรจะมองหา “ระบบที่รองรับการวิเคราะห์ย้อนหลัง” เมื่อเกิดปัญหาการเจาะระบบ แท้จริงแล้วระบบรักษาความปลอดภัยที่ทันสมัยจะต้องรองรับการตรวจสอบอย่างรอบ

ด้าน เพื่อให้ผู้ควบคุมระบบรักษาความปลอดภัยสามารถย้อนกลับไปค้นหาสาเหตุต้นตอของปัญหา และสามารถทำความเข้าใจเกี่ยวกับขอบเขตของการเจาะระบบและแก้ไขปัญหาอย่างทันท่วงที ซึ่งจะช่วยให้องค์กรทุกขนาดสามารถขจัดภัยคุกคามและจำกัดความรุนแรงของปัญหา รวมไปถึงความเสียหายที่เป็นผลตามมา

ปัจจุบันมีเทคโนโลยีที่จำเป็นสำหรับการดำเนินการอย่างรวดเร็วทั้งก่อน ระหว่าง และหลังการโจมตี และถึงเวลาแล้วที่เราจะต้องจัดระเบียบองค์กรอย่างเหมาะสม ด้วยการปรับใช้ “แนวทางรักษาความปลอดภัยแบบมุ่งเน้นที่ภัยคุกคามเป็นหลัก” เพื่อช่วยป้องกันภัยคุกคามได้ในทุกขั้นตอนของการโจมตี โดยครอบคลุมเครือข่ายและอุปกรณ์ของผู้ใช้อย่างทั่วถึง