บทสรุปสำหรับผู้บริหาร

ภูมิภาคเอเชียแปซิฟิกเป็นภูมิภาคหนึ่งที่กำลังตื่นตัวที่ซึ่งกำลังก้าวเข้าสู่ยุคของการเปลี่ยนแปลงทางดิจิตอลที่ยิ่งใหญ่ ซึ่งเป็นภูมิภาคที่มีความหลากหลายทางเศรษฐกิจและเป็นผู้นำในการพัฒนาเมืองในอนาคตที่เชื่อมต่อกัน หรือที่เรียกว่าสมาร์ทซิตี้ หลาย ๆ ประเทศเห็นถึงประโยชน์ของการพัฒนาอย่างรวดเร็วเหล่านี้และ Internet of Things (IoT) กลายเป็นเรื่องที่พบเห็นได้ทั่วไปในองค์กรต่าง ๆ และพนักงานยังคงสามารถทำงานได้จากระยะไกลและมีคล่องตัว นอกจากนี้ยังมีอุปกรณ์ที่เชื่อมต่อกับอินเทอร์เน็ตมากขึ้น

ขณะที่สิ่งนี้เป็นการเปิดโอกาสในการเติบโตและการพัฒนามากขึ้น แต่ก็ยังสร้างความเสี่ยงด้านภัยคุกคามทางโลกไซเบอร์ที่ร้ายแรงและความเสี่ยงสำหรับธุรกิจและบุคคล ผู้โจมตีกำลังเพิ่มความซับซ้อนมากขึ้นเรื่อย ๆ และใช้เทคนิคที่ทันสมัยเพื่อทำลายองค์กร

ในปี 2017 เกิดคลื่นการโจมตีทางไซเบอร์เป็นประวัติการณ์ แต่มาตรการด้านความปลอดภัยทางไซเบอร์เป็นการโต้ตอบเชิงปฏิกิริยาที่บ่อยครั้งเกินไปแทนที่จะเป็นพื้นฐานของโครงสร้างพื้นฐานระบบดิจิตอลที่แข็งแกร่ง ในมุมมองนี้ บริษัทต่าง ๆ ในภูมิภาคเอเชียแปซิฟิกต้องเผชิญกับภัยคุกคาม 6 ครั้งในทุกนาที แต่ มีการตรวจสอบเพียง 50% ของการแจ้งเตือนเท่านั้น

การศึกษาวิจัยด้านเกณฑ์มาตรฐานการรักษาความปลอดภัยในภูมิภาคเอเชียแปซิฟิกประจำปี 2018 ของ Cisco ซึ่งดำเนินการโดยนักวิจัยบุคคลที่สามที่เป็นอิสระ - นำเสนอข้อมูลเชิงลึกเกี่ยวกับแนวทางปฏิบัติด้านความปลอดภัยจากผู้ตอบแบบสอบถามกว่า 2,000 คนใน 11 ประเทศ ซึ่งรวมถึงจีน เกาหลีและญี่ปุ่นในภูมิภาคเอเชียเหนือ เอเชียตะวันออกเฉียงใต้ได้แก่ สิงคโปร์ ไทยมาเลเซีย เวียดนาม ฟิลิปปินส์ และอินโดนีเซีย ออสเตรเลียในภาคใต้ และอินเดีย*

ในรายงานฉบับนี้ เราเน้นถึงความสูญเสียทางเศรษฐกิจที่เกิดขึ้นทั่วภูมิภาคเอเชียแปซิฟิกอันเนื่องมาจากอุบัติการณ์ความปลอดภัยทางไซเบอร์ และข้อเท็จจริงที่ว่าผู้ต้านทานการบุกรุกมีงานที่ต้องทำมากมายและท้าทายที่จะเอาชนะให้ได้ การวิจัยและข้อมูลเชิงลึกของเรามีจุดมุ่งหมายเพื่อช่วยให้องค์กรต่าง ๆ สามารถตอบโต้กับภัยคุกคามที่กำลังมีวิวัฒนาการและมีซับซ้อนเพิ่มขึ้นในปัจจุบัน

ผลลัพธ์ที่สำคัญจากรายงานฉบับนี้ ได้แก่

1. การละเมิด

   ผู้โจมตีเริ่มที่จะมีความชำชองและมุ่งร้ายมากขึ้นเรื่อย ๆ ในภูมิภาคเอเชียแปซิฟิก บริษัทต่าง ๆ ต้องเผชิญกับภัยคุกคามมากถึง 10,000 ครั้งต่อวัน ซึ่งหมายความว่าในทุกนาทีจะมีภัยคุกคาม 6 ครั้ง เกือบ 75% ของบริษัทที่ทำการสำรวจจะเผชิญกับภัยคุกคามมากกว่า 5,000 ครั้งต่อวัน

   อย่างไรก็ตาม มีการตรวจสอบเพียง 50% ของการแจ้งเตือนทั้งหมด แม้ว่าจำนวน 51% ของการแจ้งเตือนทั้งหมดจะเป็นอุบัติการณ์ที่เกิดขึ้นตามหลักการหรือกฎเกณฑ์ที่ตั้งไว้ (เป็นจริง)

2. การขาดความพร้อมในการรักษาความปลอดภัย

   การศึกษาของเราถามผู้ตอบแบบสอบถาม 2,000คน เกี่ยวกับโครงสร้างพื้นฐานด้านความปลอดภัยดิจิตอลที่ผู้ตอบแบบสอบถามมีในบริษัท ผู้ตอบแบบสอบถามมากถึง 9% บอกว่าองค์กรของพวกเขาไม่มีผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ใด ๆ เลย ในขณะที่อีก 13% ไม่มีผู้บริหารระดับสูงที่มีความรับผิดชอบโดยตรงและรับผิดชอบด้านความปลอดภัยทางไซเบอร์ขององค์กรของพวกเขา

   ในบรรดาผู้ตอบแบบสอบถาม มีเพียง 42%ที่บอกว่าผู้บริหารระดับสูงเห็นว่าความปลอดภัยทางไซเบอร์มีความสำคัญสูง และเพียง 44% ที่ยอมรับว่าบทบาทและความรับผิดชอบด้านความปลอดภัยภายในองค์กรควรมีสายการบังคับบัญชาที่ชัดเจน

3. เศรษฐกิจและชื่อเสียงที่เสียหาย

   การโจมตีทางไซเบอร์มีผลกระทบที่กว้างขวาง ซึ่งรวมถึงความสูญเสียด้านการเงินและชื่อเสียงของบริษัท ใน เอเชียตะวันออกเฉียงใต้ 51% ของการโจมตีทางไซเบอร์ทั้งหมดก่อให้เกิดความเสียหายมากกว่า 1 ล้านเหรียญสหรัฐฯ เกือบ 10% ของผู้ตอบแบบสอบถามกล่าวว่าการโจมตีสร้างความเสียหายให้กับพวกเขามากกว่า 5 ล้านเหรียญสหรัฐฯ 33% ของผู้ตอบแบบสอบถามในการศึกษากล่าวว่าการละเมิดสามารถสร้างความเสียหายให้กับพวกเขาได้ทุกที่ระหว่าง 1 ถึง 5 ล้านเหรียญสหรัฐฯ

4. การโจมตีแบบหลากหลายรูปแบบ

   รูปแบบของการโจมตีทางไซเบอร์ยังกำลังมีการเปลี่ยนแปลง ปัจจุบันผู้โจมตีไม่ได้มุ่งเป้าเพียงแค่โครงสร้างพื้นฐานด้านไอที แต่ตอนนี้ยังมุ่งเป้าไปที่เทคโนโลยีการดำเนินงาน (OT) ด้วย ซึ่งมีผลต่อการทำงานและการดำเนินธุรกิจรายวัน

   30% ขององค์กรเคยประสบปัญหาการโจมตีทางไซเบอร์ตามกระบวนการเหล่านั้นมาแล้ว, ขณะที่ 50% ขององค์กรเหล่านั้นกล่าวว่าพวกเขามีความคาดหวังว่าเรื่องนี้จะได้รับการพัฒนาขึ้น นอกจากนี้ 41% ของผู้ตอบแบบสอบถามในเอเชียแปซิฟิกกล่าวว่าธุรกิจของพวกเขาจะได้รับผลกระทบหากโครงสร้างพื้นฐานด้านการดำเนินงานของบริษัทถูกบุกรุก

5. การตรวจสอบข้อเท็จจริงที่เพิ่มขึ้นจากผู้มีส่วนได้เสีย

   นอกเหนือจากความเสียหายทางการเงินแล้ว อุบัติการณ์ด้านความปลอดภัยทางไซเบอร์ยังเป็นการบ่อนทำลายความสามารถขององค์กรในภูมิภาคเอเชียแปซิฟิกในการสร้างความเชื่อมั่นให้กับผู้บริโภคและผู้มีส่วนได้เสียอื่นด้วย 72% กล่าวว่าข้อกังวลเรื่องความเป็นส่วนตัวที่มากขึ้นจากลูกค้า จะเพิ่มเวลามากขึ้นในรอบการขายของพวกเขา เกือบครึ่งหนึ่งกล่าวว่ารอบการขายของพวกเขาล่าช้ากว่าหนึ่งเดือน

*ผู้ตอบแบบสอบถามในญี่ปุ่น, จีน, อินเดีย, ออสเตรเลียได้รับการสัมภาษณ์ในปี 2017 สิงคโปร์ อินโดนีเซีย ไทยได้รับการสัมภาษณ์ในระยะหลังของการศึกษาในเดือนมิถุนายน 2018

ในปีที่จะมาถึง ผู้บริหารยังเชื่อว่าการตรวจสอบข้อเท็จจริงจากผู้มีส่วนได้เสียเช่น นักลงทุน บริษัทประกันภัย หน่วยงานกำกับดูแล คู่ค้าทางธุรกิจ ผู้บริหาร กลุ่มผู้ควบคุมดูแล/กลุ่มที่สนใจ สื่อและพนักงานเริ่มที่จะมีมากขึ้น

คำแนะนำสำหรับผู้ต้านทานการบุกรุก

เมื่อศัตรูโจมตีองค์กรของพวกเขาอย่างหลีกเลี่ยงไม่ได้ ผู้ต้านทานการบุกรุกจะเตรียมรับมืออย่างไรและพวกเขาสามารถฟื้นตัวได้เร็วแค่ไหน ผลลัพธ์จากการศึกษาวิจัยด้านเกณฑ์มาตรฐานการรักษาความปลอดภัยในภูมิภาคเอเชียแปซิฟิกประจำปี 2018 ของ Cisco ซึ่งนำเสนอข้อมูลเชิงลึกเกี่ยวกับแนวทางการรักษาความปลอดภัยจากผู้ตอบแบบสอบถามมากกว่า 2,000 คนใน 11 ประเทศแสดงให้เห็นว่าผู้ต้านทานการบุกรุกมีความท้าทายมากมายที่จะเอาชนะได้

อย่างไรก็ตาม ผู้ต้านทานการบุกรุกจะค้นพบว่าการปรับปรุงความปลอดภัยเชิงกลยุทธ์และการปฏิบัติตามหลักปฏิบัติที่ดีที่สุดร่วมกันสามารถลดความเสี่ยงที่เกิดขึ้นใหม่ ชะลอความคืบหน้าของผู้โจมตีลง และทำให้มองเห็นภาพรวมของภัยคุกคามได้ดีขึ้น ผู้ต้านทานการบุกรุกควรที่จะพิจารณาดังนี้

- ใช้เครื่องมือป้องกันด่านแรกที่สามารถปรับขนาดได้เช่น แพลตฟอร์มรักษาความปลอดภัยระบบคลาวด์
- ยืนยันว่าปฏิบัติตามนโยบายและแนวปฏิบัติของบริษัทสำหรับการปรับปรุงแอปพลิเคชัน ระบบ และอุปกรณ์
- ใช้การแบ่งกลุ่มเครือข่ายเพื่อช่วยลด

  ความเสี่ยงจากการแพร่ระบาด
- ยอมรับเครื่องมือตรวจสอบกระบวนการปลายทางรุ่นใหม่
- เข้าถึงกระบวนการและข้อมูลข่าวกรองภัยคุกคามที่ถูกต้อง แม่นยำ ทันเวลาที่อนุญาตสำหรับข้อมูลดังกล่าวเพื่อที่จะรวมเข้าไว้ในระบบการเฝ้าติดตามและการรักษาความปลอดภัย
- ดำเนินการวิเคราะห์เชิงลึกและละเอียดยิ่งขึ้น
- ทบทวนและปฏิบัติตามขั้นตอนการตอบสนองด้านความปลอดภัย
- สำรองข้อมูลบ่อย ๆ และทดสอบขั้นตอนการกู้คืน ซึ่งเป็นกระบวนการที่สำคัญในโลกที่หนอนแรนซัมแวร์บนเครือข่ายเคลื่อนที่อย่างรวดเร็วและอาวุธทางไซเบอร์ที่ประสิทธิภาพการทำลายล้างสูง
- ตรวจสอบประสิทธิภาพของบุคคลที่สามในการทดสอบเทคโนโลยีด้านความปลอดภัยเพื่อลดความเสี่ยงของการโจมตี

  ห่วงโซ่อุปทาน
- ดำเนินการสแกนความปลอดภัยของ microservice บริการระบบคลาวด์ และระบบการจัดการแอปพลิเคชัน
- ทบทวนระบบรักษาความปลอดภัยและสำรวจการใช้

  การวิเคราะห์ SSL และการถอดรหัส SSL ถ้ามี

ผู้ต้านทานการบุกรุกควรพิจารณาการนำเทคโนโลยีการรักษาความปลอดภัยขั้นสูงมาใช้ ซึ่งรวมถึงการเรียนรู้ด้วยเครื่องและขีดความสามารถของปัญญาประดิษฐ์ ด้วยมัลแวร์ที่ซ่อนการสื่อสารไว้ภายในการรับส่งข้อมูลเว็บแบบเข้ารหัสและบุคคลภายในที่ฉ้อโกงส่งข้อมูลที่มีความสำคัญผ่านระบบคลาวด์ขององค์กร ทีมรักษาความปลอดภัยต้องการเครื่องมือที่มีประสิทธิภาพในการป้องกันหรือตรวจจับการใช้การเข้ารหัสเพื่อปกปิดกิจกรรมที่เป็นอันตราย

เกี่ยวกับรายงาน

การศึกษาวิจัยด้านเกณฑ์มาตรฐานการรักษาความปลอดภัยในภูมิภาคเอเชียแปซิฟิกประจำปี 2018 ของCiscoนำเสนอความก้าวหน้าด้านอุตสาหกรรมความปลอดภัยล่าสุดที่ออกแบบมาเพื่อช่วยให้องค์กรและผู้ใช้สามารถป้องกันการโจมตีได้ นอกจากนี้ เรายังค้นหาเทคนิคและกลยุทธ์ที่ศัตรูใช้ในการทำลายการป้องกันเหล่านั้นและหลีกเลี่ยงการตรวจจับ รายงานยังเน้นถึงผลลัพธ์ที่สำคัญจาก การศึกษาวิจัยด้านเกณฑ์มาตรฐานการรักษาความปลอดภัยในภูมิภาคเอเชียแปซิฟิกประจำปี 2018 ของCiscoซึ่งจะตรวจสอบท่าทีเกี่ยวกับการรักษาความปลอดภัยของผู้ประกอบการและการรับรู้ความพร้อมในการปกป้องของพวกเขา