การตอบสนองต่อเหตุการณ์ (Incident response): 5 ปัจจัยสำคัญที่ CISOs ควรคำนึงถึงเมื่อสร้างกระบวนการตอบสนองต่อเหตุการณ์

เนื่องจากการโจมตีจากภัยคุกคามมีความซับซ้อนและเกิดขึ้นถี่ขึ้นเรื่อย ๆ ซึ่ง 86% ของ CISOs ยืนยันว่าเหตุการณ์การโจมตีออนไลน์ที่เกิดขึ้นในองค์กรต่าง ๆ เป็นสิ่งที่หลีกเลี่ยงไม่ได้ ดังนั้นไม่น่าแปลกใจเลยว่าส่วนใหญ่ (76%) เชื่อว่าความรวดเร็วและคุณภาพของการตอบสนองต่อเหตุการณ์ (IR) เป็นปัจจัยที่สำคัญเมื่อทำการวัดประสิทธิภาพ จึงทำให้หัวหน้าฝ่ายรักษาความปลอดภัยด้านไอทีไม่ได้เพียงแค่ให้ความสำคัญกับการป้องกันการโจมตี แต่ยังต้องระบุปัญหาที่จะเกิดขึ้นเพื่อลดความเสียหายอีกด้วย

เมื่อการตอบสนองต่อเหตุการณ์กลายเป็นสิ่งสำคัญ CISOs ยังคงเผชิญกับภาวะที่ยากในการจัดการ ทั้งนี้ มี 5 ปัจจัยสำคัญ ที่หัวหน้าฝ่ายรักษาความปลอดภัยด้านไอทีควรให้ความสำคัญในการเลือกจัดการการตอบสนองต่อเหตุการณ์ในองค์กร ได้แก่

ขาดแคลนบุคลากรมืออาชีพ

การตอบสนองต่อเหตุการณ์มักจะเข้าใจผิดว่าจะควรกระโดดเข้าสู่ขั้นตอนการแก้ไขเมื่อมีเหตุการณ์เกิดขึ้น ซึ่งจริง ๆ แล้ว IR จะเกิดขึ้นก่อนที่จะมีเหตุการณ์โจมตีเกิดขึ้นและจะยังคงอยู่ถึงแม้ว่าการโจมตีจบแล้ว โดยทั่วไปขั้นตอนของ IR ประกอบด้วย 4 ขั้นตอน ได้แก่ ขั้นตอนแรกคือการเตรียมพร้อมเพื่อให้มั่นใจว่าเจ้าหน้าที่รู้วิธีการรับมือเมื่อมีการโจมตีเกิดขึ้น ขั้นตอนที่สองคือการตรวจจับเหตุการณ์การโจมตี ขั้นตอนที่สามทีม IR จะเป็นต้องกำจัดการโจมตีและกู้คืนระบบที่ได้รับผลกระทบ และขั้นตอนสุดท้าย หลังจากที่ปัญหาได้รับการแก้แล้ว กลยุทธ์ของ IR จะต้องประเมินเหตุกาณ์ที่เกิดขึ้นเพื่อจะลดปัญหาที่จะเกิดขั้นแบบเดิมอีก

โดยขั้นตอนต่าง ๆ เหล่านี้จำเป็นจะต้องใช้บุคลากรมืออาชีพในการทำงาน แต่บุคลากรในสายงานนี้มีน้อย กำลังขาดแคลนบุคลากร จากรายงานการสำรวจ Kaspersky Lab’s survey 43% ของ CISOs ยังมีความลำบากในการวิเคราะห์หามัลแวร์ โดย 20% หาผู้เชี่ยวชาญในการตอบสนองต่อการโจมตี และ 13% ไม่สามารถหาคนมากำจัดภัยคุกคามได้ ปัญหาอีกประการหนึ่งคือการรักษาพนักงาน เพราะผู้เชี่ยวชาญเหล่านี้จะรู้ว่าตัวเองมีความสำคัญและเป็นที่ต้องการ สามารถเปลี่ยนองค์กรเพื่อได้เงินเดือนที่สูงกว่าได้ตลอด ด้วยเหตุผลเหล่านี้ทำให้ บริษัทต่าง ๆ มีความยากมากขึ้นในการจัดหาทีมมาดูกระบวนการ IR ทั้งหมดได้

การเลือกบริษัทผู้ให้บริการภายนอก (outsources) ที่เหมาะสม

การเลือกบริษัทภายนอกหรือผู้รับเหมาถือเป็นงานที่ไม่ง่าย หากจะทำให้มีประสิทธิภาพ ทีมผู้ให้บริการภายนอก

(outsource) ควรจะสามารถทำงานครอบคลุมถึงความสามารถที่สำคัญต่าง ๆ ของ IR ไม่ว่าจะเป็น การวิจัยภัยคุกคาม การวิเคราะห์มัลแวร์ และนิติวิทยาศาสตร์ดิจิตัล (digital forensics) โดยผู้ให้บริการภายนอกจะต้องมีใบรับรองที่ยืนยันฐานทักษะได้ และประสบการณ์ในแต่ละหน้าที่อีกด้วย ยิ่งพวกเขาทำงานให้กับลูกค้าในหลากหลายอุตสาหกรรม ยิ่งทำให้พวกเขามีโอกาสที่ได้เจอกับเหตุการณ์การโจมตีที่แตกต่างกันไปหลากหลากหลาย และสามารถหาความคล้ายคลึงกันในแต่ละกรณีได้อีกด้วย

ในบริษัทอุตสาหกรรมต่าง ๆ ที่มีการควบคุมอย่างเข้มงวด อาจมีข้อจำกัดในการเลือกบริษัทภายนอก โดยพวกเขาจะเลือกเพียงแค่บริษัทที่ตรงตามข้อกำหนดเฉพาะเท่านั้น

ค่าใช้จ่ายของการตอบสนองต่อเหตุการณ์

การกำหนดค่าใช้จ่ายในการตอบสนองต่อเหตุการณ์ภายในองค์กร องค์กรจะต้องจ่ายเงินเดือนสำหรับพนักงานประจำที่มีทักษะที่หายากและราคาสูง และอาจจะต้องซื้อโซลูชั่นและบริการการจัดการภัยคุกคามอัจฉริยะ (threat intelligence) ที่จำเป็นสำหรับการค้นหาภัยคุกคาม การวิเคราะห์ข้อมูลและการรับมือและแก้ไขจากการโจมตี อย่างไรก็ตาม ค่าใช้จ่ายเฉลี่ยจากการประสบกับการรั่วไหลของข้อมูลทั่วโลกกำลังเพิ่มขึ้น ด้วยการละเมิดในองค์กรต่าง ๆ ที่มีค่าเฉลี่ยจำนวนสูงถึง 1.23 ล้านเหรียญสหรัฐ (สูงขึ้น 24% จาก 992,000 เหรียญสหรัฐ เมื่อปี 2560).ด้วยค่าใช้จ่ายด้านเหตุการณ์ในไอทีที่เพิ่มขึ้น องค์กรต่าง ๆ ก็ได้ตระหนักที่จะต้องให้ความสำคัญกับค่าใช้จ่ายในการรักษาความปลอดภัยออนไลน์

บางองค์กรได้ใช้บริษัทภายนอกที่มีความยืดหยุ่นในค่าใช้จ่าย และคุ้มค่าในการลงทุน เพียงแค่จ่ายในกรณีที่มีการให้บริการเท่านั้น อย่างไรก็ตามองค์กรต่าง ๆ ที่มีเหตุการณ์การโจมตีจำนวนมาก จำเป็นต้องมีทีม IR ภายในองค์กร และพวกเขายังต้องหารูปแบบที่คุ้มกับค่าใช้จ่าย เมื่อมีการตอบสนองกับเหตุการณ์ในระดับแรก ทีมภายในจำเป็นที่จะต้องวิเคราะห์เหตุการณ์ที่เกิดขึ้นก่อนและคาดการณ์ได้ว่าจะสามารถจัดการเองได้ หรือจะให้ทีมบริษัทภายนอกจัดการต่อ

การทำงานร่วมกับแผนกไอที

เมื่อมีเหตุการณ์การโจมตีเกิดขึ้น ทีมไอทีจะเลือกที่จะปิดอุปกรณ์ที่โดนโจมตีเพื่อลดผลกระทบ แต่สำหรับผู้ที่ทำหน้าที่เผชิญหรือตอบสนองต่อเหตุการณ์ จำเป็นจะต้องเก็บรวบรวมหลักฐานเป็นอันดับแรก นั่นหมายถึง จะต้องทิ้งอุปกรณ์ที่ถูกโจมตีไว้สักครู่หลังจากเกิดเหตุการณ์ การรวบรวม บันทึกและจัดเก็บหลักฐานไว้เพียง 3 เดือน และปิดอุปกรณ์ที่ถูกโจมตีจะทำให้การทำงานของทีม IR ยากขึ้น

เพื่อหลีกเลี่ยงความแตกต่างนี้ ทีม IR ภายในควรจะเตรียมแนวทางหรือคำแนะนำที่จัดทำขึ้นเป็นพิเศษเพื่อเพื่อนร่วมงานทีมไอที หรือแนะนำการอบรมพิเศษสำหรับทีมไอทีที่ต้องการมากกว่าความรู้ด้านการรักษาความปลอดภัยพื้นฐานแต่ไม่ได้เจาะลึกถึงทักษะด้านความปลอดภัย ด้วยความคิดริเริ่มนี้จะทำให้ทั้งสองทีมมั่นใจได้ว่าเข้าใจและปฏิบัติในแนวทางเดียวกัน

ความล่าช้าในการตอบสนองในเชิงปฏิบัติ

องค์กรต่าง ๆ ที่มีทีม IR จากภายนอกจะสามารถจัดการกระบวนการได้อย่างรวดเร็ว เนื่องจากทีม IR ภายนอกจะ

เข้ามาจัดการและแก้ปัญหาได้ทันทีเมื่อมีเหตุการณ์เกิดขึ้น ในทางกลับกันสิ่งนี้ก็มาพร้อมกับข้อผิดพลาดได้เช่นกัน ตัวอย่างเช่น องค์กรและบริษัทภายนอกจะต้องเซ็นต์สัญญาและข้อตกลงการจ้างงานก่อนที่จะเริ่มงานกัน ซึ่งทั้งนี้อาจจะเกิดความล่าช้าในการจัดการกับเหตุการณ์ได้

จากประสบการณ์ของเรา ทีมลูกค้ามักจะเข้ามาตรวจสอบในทุกวันจันทร์ว่ามีการละเมิดหรือข้อมูลรั่วไหลบ้างหรือไม่ในช่วงวันหยุด หลาย ๆ ครั้งที่พวกเขาจัดการกับปัญหาด้วยตัวเอง จนเมื่อพวกเขาไม่สามารถจัดการได้จึงหันไปหาผู้เชี่ยวชาญภายนอก เมื่อถึงวันศุกร์องค์กรก็จะต้องรีบจัดการเซ็นต์สัญญาข้อตกลงเพื่อจะให้ทีม IR ได้เข้ามาจัดการได้ก่อนจะถึงวันหยุด หากองค์กรไหนมีทีมภายในพวกเขาจะประเมินในแต่ละกรณีและมอบหมายความรับผิดชอบได้อย่างรวดเร็ว

***

สำหรับองค์กรขนาดใหญ่ มีการผสมผสานกันทั้งทีม IR ภายในเป็นทีมแรกในการจัดการกับเหตุการณ์ที่เกิดขึ้น และกันทีม IR ภายนอกเป็นกำลังเสริม ซึ่งการรวมกันจะเป็นประโยชน์มากที่สุดและลดปัญหาการขาดแคลน

ทั้งหมดที่กล่าวมา ไม่ได้หมายความว่า การใช้ทีม IR ภายนอกจะเป็นการยกความรับผิดชอบทั้งหมดให้ทีมผู้เชี่ยวชาญภายนอกและลดภาระของตัวเอง การวางแผนยังคงมีความสำคัญ เพื่อให้ทันท่วงที องค์กรควรจะมีการเตรียมการรับมือเบื้องต้นเมื่อมีเหตุการณ์เกิดขึ้น ควรจะมีคำแนะนำว่าจะใช้ทีมภายนอกเมื่อไหร่และแก้ปัญหาอย่างไร อีกทั้งจำเป็นต้องกำหนดหน้าที่ที่ชัดเจนให้กับผู้รับผิดชอบในองค์กรที่ทำหน้าที่จัดการ ลำดับความสำคัญ และประสานงานกับทีมภายในและภายนอกอีกด้วย