กลยุทธ์การรักษาความปลอดภัยแบบตั้งรับ เป็นความท้าทายใหญ่หลวงสำหรับประธานเจ้าหน้าที่รักษาความปลอดภัยสารสนเทศ

ผลการศึกษาจาก F5 ชี้ มีเพียง 51% ของบริษัทที่มีกลยุทธ์ด้านการรักษาความปลอดภัยไอทีทั่วถึงทั้งองค์กร

F5 เน็ตเวิร์กส์ ได้ออกรายงานระดับโลกเกี่ยวกับบทบาทของประธานเจ้าหน้าที่รักษาความปลอดภัยสารสนเทศ (CISO) และวิธีการรักษาความปลอดภัยไอที ที่องค์กรทั่วโลกใช้ดำเนินการอยู่ท่ามกลางภัยคุกคามปัจจุบันที่มีการพัฒนาไม่หยุดหย่อน รายงานดังกล่าวพบว่าเนื่องจากการรักษาความปลอดภัยไอทีกลายเป็นสิ่งสำคัญอันดับต้น จึงทำให้ซีไอเอสโอมีอิทธิพลต่อองค์กรมากขึ้น อย่างไรก็ดี กลยุทธ์ด้านการรักษาความปลอดภัยในหลายองค์กรส่วนใหญ่ยังคงเป็นในเชิงรับและยังไม่สอดคล้องไปในแนวทางเดียวกับบทบาทของธุรกิจ

ผลการศึกษาซึ่งจัดทำโดยสถาบัน Penemon โดยอาศัยข้อมูลจากการสัมภาษณ์มืออาชีพระดับอาวุโสด้านความปลอดภัยไอทีจำนวน 184 รายใน 7 ประเทศ ได้แก่ สหรัฐอเมริกา สหราชอาณาจักร เยอรมัน บราซิล แมกซิโก อินเดีย และจีน

“การวิจัยดังกล่าวให้มุมมองที่แตกต่างเกี่ยวกับสิ่งที่ ซีไอเอสโอ กำลังดำเนินการอยู่ท่ามกลางสภาพแวดล้อมที่ท้าทายในปัจจุบัน” ไมค์ คอนเวอร์ติโน ประธานเจ้าหน้าที่ฝ่ายรักษาความปลอดภัยสารสนเทศ หรือ ซีไอเอสโอ ของ F5 กล่าว “เห็นได้อย่างชัดเจนว่าซีไอเอสโอ กำลังมีความคืบหน้าในการขับเคลื่อนฟังก์ชันด้านการรักษาความปลอดภัยและบทบาทของภาวะผู้นำที่มีต่อองค์กร นอกจากนี้ ในองค์กรอีกหลายแห่ง การรักษาความปลอดภัยไอทียังไม่มีบทบาทในเชิงกลยุทธ์ เชิงรุกเพื่อปกป้องสินทรัพย์และป้องกันการโจมตีที่ซับซ้อนและต่อเนื่องอย่างเต็มรูปแบบ”

ผลสำรวจในประเด็นหลัก

• ความรับผิดชอบของซีไอเอสโอที่เพิ่มมากขึ้น – แม้ว่าซีไอเอสโอ จะมีอิทธิพลในกลุ่มผู้บริหารระดับสูงขององค์กรในระดับที่แตกต่างกันไปก็ตาม ซีไอเอสโอส่วนใหญ่จะมีอิทธิพลหรืออำนาจในการบริหารจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์ของบริษัทซึ่งสร้างผลกระทบมากขึ้น 68 เปอร์เซ็นต์ของผู้ตอบสำรวจกล่าวว่า ซีไอเอสโอเป็นผู้มีอำนาจในการตัดสินเรื่องการใช้จ่ายเกี่ยวกับการรักษาความปลอดภัยไอทีทั้งหมด ในขณะที่ในอีก 64 เปอร์เซ็นต์กล่าวว่าซีไอเอสโอนั้นมีอิทธิพลในทางตรงและมีอำนาจในการใช้จ่ายเกี่ยวกับการรักษาความปลอดภัยทั้งหมดในองค์

กร ทั้งนี้ 87 เปอร์เซ็นต์ ของผู้ตอบสำรวจกล่าวว่างบประมาณด้านการรักษาความปลอดภัยไอทีเพิ่มขึ้นอย่างมีนัย (18 เปอร์เซ็นต์) เพิ่มขึ้นบางส่วน (29 เปอร์เซ็นต์) หรือไม่มีการเปลี่ยนแปลง (40 เปอร์เซ็นต์)

• ขาดแนวทางที่สอดคล้องกับธุรกิจ – การมีกลยุทธ์ด้านการรักษาความปลอดภัยไอทีที่ครอบคลุมทั่วทั้งบริษัท นับว่าหาได้ยาก 58 เปอร์เซ็นต์ของผู้ตอบสำรวจชี้ว่าระบบรักษาความปลอดภัยไอทีนั้นเป็นฟังก์ชันแบบสแตนอโลน และมีเพียง 22 เปอร์เซ็นต์ที่กล่าวว่า มีการผสานการรักษาความปลอดภัยร่วมกับทีมธุรกิจอื่นๆ ในขณะที่ 45 เปอร์เซ็นต์กล่าวว่าฟังก์ชันด้านการรักษาความปลอดภัยไม่มีการกำหนดเส้นแบ่งความรับผิดชอบที่ชัดเจน โดย 75 เปอร์เซ็นต์ของผู้ตอบสำรวจ กล่าวว่า เนื่องจากขาดการผสานการทำงานร่วมกับฟังก์ชันทางธุรกิจ ทำให้ปัญหาเรื่องของการทำงานแบบไซโล ส่งผลอย่างมีนัย (36 เปอร์เซ็นต์) หรือส่งผลบางประการ (39 เปอร์เซ็นต์) ต่อกลยุทธ์และยุทธวิธีในการรักษาความปลอดภัยไอที

• การตระหนักเรื่องการรักษาความปลอดภัยซึ่งเป็นสิ่งที่ธุรกิจให้ความสำคัญยังเป็นเชิงรับอยู่ – 60 เปอร์เซ็นต์ของผู้ตอบสำรวจเชื่อว่าองค์กรของตนมองว่าการรักษาความปลอดภัยเป็นความสำคัญอันดับต้นของธุรกิจ ในขณะที่มีเพียง 51 เปอร์เซ็นต์ กล่าวว่าองค์กรของตนมีกลยุทธ์ด้านการรักษาความปลอดภัย และ มีเพียง 43 เปอร์เซ็นต์ กล่าวว่าผู้บริหารระดับสูงได้มีการนำกลยุทธ์มาทบทวน อนุมัติ พร้อมให้การสนับสนุนในการดำเนินการ ผลศึกษายังชี้ว่าการเปลี่ยนแปลงที่เกิดขึ้นในโปรแกรมการรักษาความปลอดภัยส่วนใหญ่จะเป็นการตั้งรับ ในเรื่องของข้อมูลรั่วไหล (45 เปอร์เซ็นต์) และช่องโหว่ของระบบรักษาความปลอดภัยไซเบอร์ (43 เปอร์เซ็นต์) ซึ่งเป็นสองเหตุการณ์หลักที่ผู้บริหารระดับอาวุโสได้ให้ความสนใจ

• วิกฤติขับเคลื่อนอำนาจด้วยภาวะผู้นำของผู้บริหาร 65 เปอร์เซ็นต์ของผู้ตอบสำรวจกล่าวว่า ซีไอเอสโอ สื่อสารโดยตรงกับผู้บริหารระดับอาวุโส แต่ไม่ค่อยเป็นการพูดคุยในเชิงกลยุทธ์ถึงภัยคุกคามทั้งหมดให้องค์กรได้รับทราบ 56 เปอร์เซ็นต์ ยอมรับว่าจะมีการสื่อสารกับซีอีโอและกรรมการบริหารก็ต่อเมื่อมีเหตุการณ์ในประเด็นของข้อมูลรั่วไหล และเกิดการโจมตีบนไซเบอร์ ในขณะที่มีเพียง 19 เปอร์เซ็นต์ ที่มีการรายงานเกี่ยวกับข้อมูลรั่วไหลทั้งหมดให้ซีอีโอและกรรมการบริหารได้รับทราบ

• ปัญญาประดิษฐ์ หรือ AI เป็นโซลูชันที่มีศักยภาพในแบบที่พนักงานต้องการ การขาดแคลนผู้มีความสามารถด้านการรักษาความปลอดภัยไอที ยังคงเป็นเรื่องสำคัญสำหรับซีไอเอสโอ บุคลากรด้านการรักษาความปลอดภัยไอทีซึ่งเป็นที่ต้องการในองค์กรโดยเฉลี่ย จะมีพนักงานทำงานแบบเต็มเวลาในจำนวนที่เพิ่มจาก 19 คนเป็น 32 (หรือเทียบเท่า) คน ภายในอีก 2 ปีข้างหน้า ซึ่งเกือบครึ่งของผู้ตอบสำรวจ (42 เปอร์เซ็นต์) รู้สึกว่าพนักงานในองค์กรไม่เพียงพอ โดย 58 เปอร์เซ็นต์ กล่าวว่า ประสบความยากลำบากในการจ้างพนักงานดูแลเรื่องความปลอดภัยที่มีคุณภาพ เนื่องจากความท้าทายที่ใหญ่ที่สุดคือการหาและว่าจ้างผู้สมัครที่มีคุณภาพ (56 เปอร์เซ็นต์) และไม่สามารถเสนอเงินเดือนเท่าราคาที่จ่ายอยู่ในตลาดได้ (48 เปอร์เซ็นต์) ความท้าทายเหล่านี้ กดดันให้บริษัทต้องหาโซลูชันจากที่อื่น ซึ่งครึ่งนึง (50 เปอร์เซ็นต์) ของผู้ตอบสำรวจเชื่อว่า การเรียนรู้ของเครื่องคอมพิวเตอร์และปัญหาประดิษฐ์ (Artificial

Intelligence) สามารถตอบโจทย์เรื่องการขาดแคลนบุคลากรได้ และ 70 เปอร์เซ็นต์ เชื่อว่าเทคโนโลยีเหล่านี้ เป็นสิ่งสำคัญยิ่งต่อบทบาทการรักษาความปลอดภัยไอทีในอีก 2 ปีข้างหน้า

ข้อมูลเพิ่มเติม

- Mike Convertino blog and full report