ประชาชาติธุรกิจ
Prachachat Turakij
Circulation: 120,000
Ad Rate: 1,350

Section: การตลาด/ไอซีที
วันที่: พุธ 23 - ศุกร์ 25 มีนาคม 2565
ปีที่: 44 **ฉบับที่:** 5447 **หน้า:** 1(ขวา), 13, 15
Col.Inch: 100.42 **Ad Value:** 135,567 **PRValue (x3):** 406,701 **คลิป:** สี่สี
หัวข้อข่าว: ภัยไซเบอร์ ปัญหาใหญ่ ปรับไมนด์เซต-เร่งสร้างการรับรู้

15 ภัยไซเบอร์ ปัญหาใหญ่
ปรับไมนด์เซต เร่งสร้างการรับรู้

ภัยไซเบอร์ ปัญหาใหญ่
15 ปรับไมนด์เซต เร่งสร้างการรับรู้

ภัยไซเบอร์ ปัญหาใหญ่

ปรับไมนด์เซต-เร่งสร้างการรับรู้

ปัจจุบันคนไทยใช้อินเทอร์เน็ต เฉลี่ย 9 ชั่วโมงต่อวัน และมีแนวโน้มจะเพิ่มขึ้นต่อเนื่อง ส่งผลให้การคุกคามทางไซเบอร์พุ่งสูงขึ้นเป็นเงาตามตัว และแฝงมาในหลายรูปแบบ ซึ่งภาครัฐก็ตระหนักถึงความเสียหายทางเศรษฐกิจที่อาจเกิดขึ้นจึงพยายามวางแนวทางป้องกัน ไม่ว่าจะเป็นการออกพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ขณะที่ภาคธุรกิจ และผู้ที่เกี่ยวข้องทั้งหลายต่างให้ความสำคัญกับการวางแนวทางป้องกัน โดยเฉพาะธุรกิจโทรคมนาคมอีกเซ็กเตอร์สำคัญที่ไม่เพียงมีส่วนต่อการขับเคลื่อนเศรษฐกิจของประเทศ ยังเกี่ยวพันกับผู้ใช้บริการจำนวนมากด้วย

ล่าสุดในงานประชุมใหญ่สำมัญประจำปี 2565 ของสมาคมโทรคมนาคมแห่งประเทศไทย ในพระบรมราชูปถัมภ์ เมื่อเร็ว ๆ นี้ได้จัดเสวนาออนไลน์ในหัวข้อ **"ความสำคัญต่อการรับมือภัยคุกคามทางไซเบอร์ในเซ็กเตอร์โทรคมนาคม"** โดยผู้เชี่ยวชาญจากภาคส่วนต่าง ๆ มาแลกเปลี่ยนมุมมอง

พลเอก ดร.ปรัชญา เฉลิมวัฒน์ เลขาธิการคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) พูดถึงภัยคุกคามทางไซเบอร์ว่า ปัจจุบันผู้ใช้อินเทอร์เน็ตเพิ่มขึ้นทั่วโลกทำให้โลกปัจจุบันของทุกคน คือ โลกสี่เหลี่ยม ที่ติดต่อสื่อสาร พูดคุยกันผ่านจอ

ภัยไซเบอร์ปัญหาลามทั่วโลก

หากดูสถิติการใช้อินเทอร์เน็ตของคนไทยพบว่า ประเทศไทยมีประชากร 70 ล้านคน แต่มีผู้ใช้โทรศัพท์มากกว่า 90 ล้านเครื่อง หมายถึง 1 คนถือครองโทรศัพท์มากกว่า 1 เครื่อง และใช้อินเทอร์เน็ตเฉลี่ย 9 ชั่วโมงต่อวัน นั่นหมายถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มสูงขึ้นในหลายรูปแบบ ส่วนผู้ที่เข้ามาโจมตีก็มีตั้งแต่ระดับแฮกเกอร์ทั่วไป ไปจนถึงการจัดตั้งทีมมีเป้าหมายทั้งด้านการเงิน สร้างชื่อเสียงหรือทางการเมือง

"ปัจจุบันภัยคุกคามไซเบอร์กลายเป็นปัญหาอันดับต้น ๆ ของโลก นอกเหนือจากเรื่องโรคระบาด การเปลี่ยนแปลงทางภูมิอากาศ ซึ่งการโจมตีทางไซเบอร์มีหลายระดับ และสามารถยกระดับได้มากที่สุดจนถึงทำให้เกิดสงครามหรืออาชญากรรมทางคอมพิวเตอร์"

อัพเดตแผนไซเบอร์ฉบับใหม่

ขณะที่การรักษาความปลอดภัยของระบบไอทีก็ตามมาด้วยความไม่สะดวกในการใช้งาน ดังนั้น องค์กรจึงต้องรักษาสมดุลเรื่องการเพิ่มมาตรการความปลอดภัย ขณะที่พนักงานหรือผู้ใช้ก็ยังสามารถใช้งานได้อย่างสะดวก

สำหรับประเทศไทยมีการออกแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ปี 2560-2564 และได้ร่วมกับสำนักงานสภาความมั่นคงแห่งชาติ (สมช.) อัพเดตแผนยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติฉบับใหม่ขึ้นมา

อย่างไรก็ตาม ปัญหาสำคัญที่เกิดขึ้นทั่วโลกด้านการป้องกันไซเบอร์ซีเคียวริตี้ คือ ปัญหาขาดแคลนบุคลากร ปัจจุบันอุตสาหกรรมนี้ต้องการคนไอทีกว่า 1 ล้านตำแหน่ง ที่ผ่านมา สกมช.ได้จัดการแข่งขันเพื่อเฟ้นหาบุคลากรด้านนี้อย่างต่อเนื่อง ขณะที่มีแนวทางการพัฒนา และ

ประชาชาติธุรกิจ
Prachachat Turakij
Circulation: 120,000
Ad Rate: 1,350

Section: การตลาด/ไอซีที
วันที่: พุธ 23 - ศุกร์ 25 มีนาคม 2565
ปีที่: 44 **ฉบับที่:** 5447 **หน้า:** 1(ขวา), 13, 15
Col.Inch: 100.42 **Ad Value:** 135,567 **PRValue (x3):** 406,701 **คลิป:** สี่สี
หัวข้อข่าว: ภัยไซเบอร์ ปัญหาใหญ่ ปรับไมนด์เซต-เร่งสร้างการรับรู้

ป้องกันในอนาคต ได้แก่ การจัดตั้งหน่วยงานที่รับผิดชอบโดยตรง พัฒนาบุคลากรด้านไซเบอร์ซีเคียวริตี้ เพิ่มงบประมาณ ประสานความร่วมมือ ปรับองค์กรใหม่

โทรคมนาคม-แบงก์พร้อมรับมือ

ด้าน **นาวาอากาศเอกอมร ชมเชย** รองเลขาธิการสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) กล่าวถึงความสำคัญต่อการรับมือภัยคุกคามทางไซเบอร์ในเซ็กเตอร์โทรคมนาคมว่า หลังประกาศใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ปี 2562 ใช้เวลาจัดตั้ง สกมช. และออกกฎหมายลูก รวมถึงกฎเกณฑ์ข้อบังคับต่าง ๆ ซึ่งในส่วนกฎหมายลูกหลัก ๆ มาครบเกือบหมดแล้ว และคาดว่าจะผลักดันส่วนที่เหลือออกมาให้ครบถ้วนในปลายปี

"พยายามสื่อสารและทำความเข้าใจว่า พ.ร.บ.ดังกล่าว จะมีส่วนทำให้ภาพการป้องกันทางไซเบอร์ของประเทศมีความเข้มแข็ง ดังนั้น สิ่งที่ต้องทำคือรัฐต้องเฝ้าระวัง ขณะที่ภาคเอกชนต้องเตรียมความพร้อมด้วย ซึ่ง 2 เซ็กเตอร์ที่มีความพร้อมสูง คือ โทรคมนาคม และธนาคาร"

กสทช.ประสานค่ายมือถือ

นายสุทธิศักดิ์ ตันตะโยธิน รองเลขาธิการสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) กล่าวว่า ประเทศไทยมีความหลากหลายทางภัยไซเบอร์ค่อนข้างมาก และมุมมองโครงสร้างพื้นฐานที่หลากหลาย ทำให้การทำงาน กสทช. บางครั้งอาจไม่ได้ดั่งใจ ที่ผ่านมามีการออกใบอนุญาตตามเงื่อนไขเท่านั้น และหากสกมช.มีไกด์ไลน์ที่ชัดเจน กสทช.ก็จะรับมาทำในเชิงปฏิบัติ ซึ่งพูดคุยกันตลอดเวลา

"ก่อนหน้านี้ กสทช.ได้ร่วมกับสมาคมโทรคมนาคมฯตั้งศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับกิจการโทรคมนาคม(TTC-CERT) เพื่อเป็นศูนย์กลางการแลกเปลี่ยนข้อมูลเฝ้าระวังภัยคุกคามไซเบอร์ สร้างความมั่นใจผู้ใช้โครงข่ายโทรคมนาคม และจะขยายขอบเขตขึ้นไปอีกในปีนี้ ด้วยการวางแนวทางการกำกับดูแลโอเปอเรเตอร์เพื่อป้องกันภัยไซเบอร์ตั้งแต่ต้นทาง โดยอยู่ศึกษารายละเอียดร่วมกัน"

ปรับไมนด์เซต-เติมความรู้

ด้าน **นายปริญญา หอมเอนก** ประธานกรรมการ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด กล่าวว่า การป้องกันภัยไซเบอร์ต้องเริ่มจากการเปลี่ยนความคิดก่อนว่าไม่มีอะไรปลอดภัย และเป็นเรื่องของคนที่มีความรู้ไม่เท่ากัน ไม่ใช่รวยหรือจน มีการศึกษาหรือไม่มี แต่เป็นเรื่องความรู้ด้านการป้องกันภัยไซเบอร์ที่ไม่เท่ากัน ทำให้เกิดปัญหา และคดีที่มาจากหลอกลวงทางไซเบอร์เพิ่มขึ้น จึงต้องเน้นสร้างการรับรู้เกี่ยวกับการป้องกัน ซึ่งไทยถือว่าทำได้ดีในระดับหนึ่ง

"ผมนั่งเก้าอี้เป็นกรรมการบริษัทจดทะเบียนหลายรายพบว่า ทุกรายเตรียมปฏิบัติตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล แต่ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ยังไม่ทำเพราะยังไม่มีกำหนดการลงโทษ แต่ต้องเข้าใจก่อนว่า พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นฐานสำคัญของ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เพราะถ้าระบบไอทีบริษัทไม่แข็งแรงก็อาจเกิดปัญหาข้อมูลรั่วได้ ท้ายที่สุดก็ต้องได้รับการลงโทษตาม พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคลจึงต้องเน้นการให้ความรู้ว่าต้องทำ ไม่ใช่ทำเพราะโดนบังคับ"

เช่นเดียวกับ **นายฐนสรณ์ ใจดี** ประธานคณะทำงานศูนย์ประสานงานรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับกิจการโทรคมนาคม (TTC-CERT) กล่าวว่า **การสร้างการรับรู้เกี่ยวกับภัยไซเบอร์เป็นสิ่งที่ต้องทำต่อเนื่อง ซึ่งองค์กรเล็ก ๆ อาจมีข้อจำกัดในการดูแลจึงต้องหาตัวช่วยเพื่อให้องค์กรเหล่านี้สามารถจัดการภัยไซเบอร์ได้ อีกทั้งต้องสื่อสารให้ผู้บริหารตระหนักว่าภัยไซเบอร์จะสร้างความเสียหายให้ธุรกิจมหาศาล ฉะนั้นต้องกระตุ้นให้ผู้บริหารตระหนักรู้ เพื่อจัดสรรงบประมาณในการลดความเสี่ยงจากภัยไซเบอร์**