กรุงเทพธุรกิจ
Krungthep Turakij
Circulation: 160,000
Ad Rate: 1,400

Section: การเงิน-ลงทุน/-
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 35 **ฉบับที่:** 12053 **หน้า:** 21(ขวา)
Col.Inch: 12.20 **Ad Value:** 17,080 **PRValue (x3):** 51,240 **คลิป:** ขาว-ดำ
คอลัมน์: Think Out: กสทช.ยึดมือถือ-แท็บเล็ตเถื่อนหมื่นเครื่อง

กรุงเทพธุรกิจ Think Out

กสทช.ยึดมือถือ-แท็บเล็ตเถื่อนหมื่นเครื่อง

นายไตรรัตน์ วิริยะศิริกุล รักษาการแทน เลขาธิการ กสทช. กล่าวว่า เมื่อวันที่ 4 ก.พ. 2565 สำนักงาน กสทช. ร่วมกับเจ้าหน้าที่ตำรวจศูนย์ปราบปรามอาชญากรรมทางเทคโนโลยีสารสนเทศ สำนักงานตำรวจแห่งชาติ (ศปอส.ตร.) ดำเนินการตรวจสอบการจำหน่ายเครื่องวิทยุคมนาคมของร้านค้าออนไลน์หรือร้านค้าบนแพลตฟอร์มออนไลน์ต่างๆ พบว่าบริษัท ดี ดัง จำกัด มีการกระทำความผิดในข้อหา มีนำเข้า และค้า ซึ่งเครื่องวิทยุคมนาคมโดยไม่ได้รับอนุญาตจากเจ้าพนักงานผู้ออกใบอนุญาต ปรากฏของกลางทั้งหมด 5 รายการทั้งโทรศัพท์มือถือ แท็บเล็ต ไอแพด จำนวน 9,195 ชิ้น รวมมูลค่า 15,825,000 บาท

ที่ผ่านมา สำนักงานฯ ได้ดำเนินการกำกับดูแลและบังคับใช้กฎหมายที่เกี่ยวข้องกับการประกอบกิจการโทรคมนาคมและวิทยุคมนาคมมาอย่างต่อเนื่อง แต่ก็ยังคงมีประชาชนหรือบุคคลทั่วไป ซึ่งอาจเป็นทั้งผู้จำหน่ายและผู้ใช้งานเครื่องวิทยุคมนาคมที่ขาดความรู้ความเข้าใจว่า อะไรเป็นเครื่องวิทยุคมนาคมที่ได้รับการยกเว้นไม่ต้องได้รับใบอนุญาต หรืออะไรเป็นเครื่องวิทยุคมนาคมที่ต้องได้รับใบอนุญาตก่อนจำหน่ายหรือใช้งาน ตามที่กฎหมายว่าด้วยวิทยุคมนาคมกำหนดไว้

เดลินิวส์
Daily News
Circulation: 500,000
Ad Rate: 2,100

Section: First Section/การเมือง-สกู๊ปหน้า 1
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: - **ฉบับที่:** 26419 **หน้า:** 3(กลาง)
Col.Inch: 22.29 **Ad Value:** 46,809 **PRValue (x3):** 140,427 **คลิป:** สี่สี
หัวข้อข่าว: กสม.แนะสื่อ-กสทช.เคารพอัตลักษณ์เพศ

กสม.แนะสื่อ-กสทช.เคารพอัตลักษณ์เพศ

เมื่อวันที่ 10 ก.พ. นายวสันต์ ภัยหลีกลี้ และ น.ส.ศยามล ไกยูรวงศ์ กรรมการสิทธิมนุษยชนแห่งชาติ (กสม.) แถลงกรณีตรวจสอบการนำเสนอข่าวสารที่กระทบศักดิ์ศรีความเป็นมนุษย์ของกลุ่มหลากหลายทางเพศ หลังได้รับเรื่องร้องเรียนระหว่างเดือน พ.ค.-ก.ค. 2564 กล่าวอ้างว่า สถานีโทรทัศน์เคเบิลทีวีแห่งหนึ่งและสำนักข่าวแห่งหนึ่งเสนอข่าวสารโดยพาดหัวข่าวด้วยถ้อยคำที่อาจกระทบต่ออัตลักษณ์และศักดิ์ศรีของกลุ่มบุคคลที่มีความหลากหลายทางเพศ เช่น "รวบสาวสอง ค้ากามเด็กอายุต่ำกว่า 18 ปี" "จับกะเทยฆ่าสาวทอม" เป็นต้น ซึ่งเป็นการเลือกปฏิบัติโดยไม่เป็นธรรมระหว่างเพศ รวมทั้งเป็นการสร้างความเกลียดชังต่อกลุ่มบุคคลที่มีความหลากหลายทางเพศในสังคม

อย่างไรก็ตามเพื่อเป็นการส่งเสริมและคุ้มครองสิทธิมนุษยชน กสม.จึงเห็นควรมีข้อเสนอแนะไปยังสถานีเคเบิลทีวีผู้ถูกร้อง สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) และรัฐสภา คือ 1.สถานีเคเบิลทีวีในฐานะผู้ประกอบวิชาชีพสื่อ ต้องไม่นำเสนอหัวข่าว ความนำ และภาพประกอบจนทำให้เกิดความเข้าใจคลาดเคลื่อนไปจากสาระสำคัญของข่าว และต้องนำเสนอข่าวโดยคำนึงถึงศักดิ์ศรีความเป็นมนุษย์ของบุคคลที่ตกเป็นข่าว โดยเฉพาะอย่างยิ่งต้องระมัดระวังการใช้ถ้อยคำเกี่ยวกับกลุ่มบุคคลที่มีความหลากหลายทางเพศด้านอัตลักษณ์ 2.สำนักงาน กสทช. จัดทำและผลักดันร่างแนวทางในการนำเสนอเนื้อหารายการเกี่ยวกับกลุ่มบุคคลที่มีความหลากหลายทางเพศ โดยให้สอดคล้องกับการเปลี่ยนแปลงของสังคมและเทคโนโลยี และ 3.ให้รัฐสภาเร่งผลักดันร่างพระราชบัญญัติส่งเสริมจริยธรรมและมาตรฐานวิชาชีพสื่อมวลชน ซึ่งมีหลักการสำคัญในการคุ้มครองเสรีภาพของผู้ประกอบวิชาชีพสื่อมวลชน และเป็นการคุ้มครองสิทธิของประชาชนไปพร้อมกัน.

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,550

Section: First Section/-
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 45 **ฉบับที่:** 16042 **หน้า:** 1(ล่าง), 2
Col.Inch: 143.76 **Ad Value:** 222,828 **PRValue (x3):** 668,484 **คลิป:** สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

พล.อ.ปรัชญา เฉลิมวัฒน์

จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

หมายเหตุ - *มติชนสัมภาษณ์พิเศษ พล.อ.ปรัชญา เฉลิมวัฒน์ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งทำหน้าที่บริหารหน่วยงานดูแลความปลอดภัยไซเบอร์แห่งชาติ ซึ่งจัดตั้งมาได้ 1 ปี เพื่อรับมือกับภัยสมัยใหม่ที่มากับเทคโนโลยีที่นับวันยิ่งก้าวหน้า สถานการณ์ด้านภัยไซเบอร์ และการรับมือเป็นอย่างไร เป็นเรื่องที่สังคมและประชาชนคนไทยควรจะได้รับรู้ ผ่านบทสัมภาษณ์พิเศษชิ้นนี้*

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานใหม่ ที่จัดตั้งขึ้นอย่างเร่งด่วนเพื่อรับมือสถานการณ์ใหม่ทางด้านภัยไซเบอร์ ที่มากับเทคโนโลยีสมัยใหม่ที่มีคุณูปการมากมาย แต่ในอีกด้านของความก้าวหน้า การใช้ระบบอินเตอร์เน็ต การใช้เทคโนโลยีด้านการสื่อสาร โดยบิดเบือนเพื่อประโยชน์เฉพาะกลุ่มหรือเพื่อก่อกวนบั่นทอนสังคม ก็กำลังเป็นปัญหาในระดับโลก และในระดับประเทศ

สกมช.เป็นหน่วยงานที่อยู่ระหว่างการสร้างความพร้อมอย่างรีบเร่ง ผู้ทำหน้าที่บุกเบิกหน่วยงานนี้คือ นายทหารสายวิทยาศาสตร์มือดี ที่แวดวงกองทัพรู้จักกันดี คือ **พล.อ.ปรัชญา เฉลิมวัฒน์** เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ลธ.กมช.)

พล.อ.ปรัชญาอธิบายที่มาที่ไปของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ว่าเกิดขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มีผลใช้บังคับเมื่อพฤษภาคม 2562 ก่อนจัดตั้งสำนักงานเมื่อ 1 มกราคม 2564

จัดตั้งขึ้นโดยศึกษารูปแบบจากต่างประเทศ และจำลองสิ่งที่จะเกิดขึ้นเพื่อเข้าไปรับมือ เกี่ยวข้องกับ 4 พันธกิจหลัก ประกอบด้วย

1.หน่วยงานกำกับดูแลการดำเนินนโยบาย ตามแนวปฏิบัติ กำหนดหน้าที่อำนาจต่างๆ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยวัตถุประสงค์หลักของกฎหมายฉบับนี้ ในการจัดตั้ง สกมช.ขึ้น เพื่อดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure)

ซึ่งกำหนดไว้ 8 ด้าน ได้แก่ ด้านความมั่นคงของรัฐ, ด้านบริการภาครัฐที่สำคัญ, ด้านการเงินการธนาคาร, ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม, ด้านการขนส่งและโลจิสติกส์, ด้านพลังงานและสาธารณูปโภค, ด้านสาธารณสุข และด้านอื่นตามที่คณะกรรมการประกาศเพิ่มเติม

"ถือเป็นเรื่องค่อนข้างใหญ่ ขอบเขตงานหรือความรู้ที่อยู่ในความรับผิดชอบเป็นวงกว้าง ดังนั้นคงต้องใช้เวลาสักระยะ ประมาณ 2 ปี สร้างความพร้อมให้ทุกเซ็กเตอร์ ราชกิจจานุเบกษาระบุไว้ชัดเจนว่าหน่วยงานใดบ้างที่จะเป็นซีไอไอ แต่เราจะเป็นผู้กำหนดลักษณะว่า หากมีบริการที่สำคัญในลักษณะนี้ หน่วยงานนั้นๆ จะเป็นซีไอไอหรือไม่ โดยหน่วยงานที่เป็นซีไอไอจะต้องปฏิบัติตามประกาศของ กมช. ซึ่งเป็นคณะกรรมการชุดใหญ่ มี พล.อ.ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี เป็นประธาน ขณะที่ สกมช.จะขึ้นตรงกับ พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี"

"ยังมีคณะกรรมการกำกับดูแลด้านความมั่นคง

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,550
Section: First Section/-
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 45 ฉบับที่: 16042 หน้า: 1(ล่าง), 2
Col.Inch: 143.76 Ad Value: 222,828 PRValue (x3): 668,484 คลิป: สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

ปลอดภัยไซเบอร์ (กกม.) มี นายชัยวุฒิ ธนาคมานุสรณ์ รัฐมนตรีว่าการกระทรวงดีอีเอส เป็นประธาน และมีปลัดกระทรวง และผู้มีหน้าที่ขับเคลื่อนองค์กรต่างๆ ที่เกี่ยวข้อง หากเกิดการโจมตีขนาดใหญ่ ที่เข้าขั้นร้ายแรงหรือวิกฤต คณะกรรมการชุดนี้จะหารือร่วมกัน เพื่อหาทางรับมือกับเรื่องนี้ และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ดังนั้น สกมช.จะเกี่ยวข้องกับกระทรวงดีอีเอส ในลักษณะการทำงานร่วมกัน เนื่องจากกระทรวงดีอีเอสเป็นผู้รับผิดชอบในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 หรือ พ.ร.บ.คอมพิวเตอร์ ที่มีการกระทำความผิดด้านการละเมิดต่างๆ แต่ส่วนของ พ.ร.บ.ไซเบอร์ จะเน้นการเสริมสร้างความแข็งแกร่งให้กับหน่วยงานที่เป็นซีไอไอ" พล.อ.ปรัชญากล่าว

2.สกมช.จะเป็นหน่วยงานหลักในการประสานงาน โดยกระทรวงดีอีเอสจะรับผิดชอบส่วนของ พ.ร.บ.คอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert : ไทยเซิร์ต) ซึ่งตอนนี้อยู่ภายใต้สังกัดของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือเอ็ตด้า ซึ่งใน พ.ร.บ.ไซเบอร์ กำหนดให้ สกมช.เป็นผู้ดูแลในระดับประเทศ มีลักษณะหน้าที่เป็นศูนย์กลางในประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีหน่วยงานในซีไอไอกว่า 300 แห่ง ต้องอาศัยศูนย์กลางในประสาน ปัจจุบันมีการจัดตั้ง 'ไทยแบงก์เซิร์ต' ซึ่งเป็นหน่วยงานในซีไอไอ ด้านการเงินการธนาคารแห่งแรก และถัดมามีการจัดตั้ง 'เทลโก้เซิร์ต' ตามคำแนะนำของเอนิซ่า องค์กรของสหภาพยุโรป (อียู) ที่ดูแลเรื่องความมั่นคงปลอดภัยทางไซเบอร์

โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ CERT มีอยู่ทั่วโลก เกิดจากมหาวิทยาลัยคาร์เนกีเมลลอน เป็นผู้กำหนดการลงทะเบียน หากแต่ละประเทศต้องการที่จัดตั้งศูนย์ประสานดังกล่าวจะต้องมีการขออนุญาต โดยศูนย์ประสาน อาทิ เจแปนเซิร์ต ยูเอสเซิร์ต จะทำหน้าที่ประสานงาน แลกเปลี่ยนข้อมูล แจ้งเตือน เฝ้าติดตาม และปฏิบัติหน้าที่ ตามที่มีการกำหนด ซึ่งหากภารกิจเยอะจำเป็นต้องใช้ทรัพยากรทั้งงบประมาณและบุคลากรจำนวนมาก

3.การพัฒนาบุคลากร แม้ไม่มีโรงเรียนที่เปิดสอนโดยตรง แต่จะมีโครงการต่างๆ อาทิ การจัดอบรม มีการสอบใบรับรอง และให้ใบรับรอง เพื่อให้บุคลากรมีความรู้ โดยปี 2564-2565 มีโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งได้รับทุนสนับสนุนจำนวน 119 ล้านบาท จากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยตั้งเป้าที่จะพัฒนาบุคลากรระดับพื้นฐาน 2,025 คน แต่คาดว่าจะได้มากกว่า เพราะปรับเปลี่ยนรูปแบบการจัดฝึกอบรมจากระบบออฟไลน์เป็นออนไลน์ และระดับผู้เชี่ยวชาญ จำนวน 300 คน ซึ่ง

ส่วนหนึ่งของจำนวนดังกล่าว จะส่งเสริมให้มีใบรับรองระดับสากล เพื่อใช้เป็นดัชนีชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ อย่างไรก็ตาม ปัจจุบันประเทศไทยมีผู้เชี่ยวชาญที่ได้รับใบรับรองระดับสากลเพียง 200 คน ขณะที่สิงคโปร์ มีถึง 1,000 คน ทั้งนี้ยังมีการจัดการแข่งขัน 'ไทยแลนด์ไซเบอร์ก็อตทาเลนต์' ใน 3 ระดับ ได้แก่ มัธยมศึกษา อุดมศึกษา และระดับบุคคลทั่วไป ซึ่งส่วนใหญ่เป็นผู้ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีประสบการณ์ด้านการทำงานและเคยผ่านการแข่งขันระดับเวทีโลก โดยส่วนนี้ได้รับความสนใจเป็นอย่างมาก เนื่องจากมีเงินรางวัลจูงใจ สูงสุดเท่าที่เคยจัดการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยความช่วยเหลือจากผู้ประกอบการ เพราะลำพังสำนักงานเองไม่มีงบประมาณเพียงพอ

และ **4.การทำความร่วมกับหน่วยงานทุกภาคส่วนทั้งในและต่างประเทศ** เพราะการป้องกันภัยด้านไซเบอร์ไม่สามารถต่อสู้ได้เพียงลำพัง ซึ่งแตกต่างจากเรื่องอื่น จึงจำเป็นต้องก้าวไปไปพร้อมกัน เช่น มีอยู่ธนาคารทั้งหมด 10 แห่ง มีธนาคาร 1 แห่งถูกโจมตีทางไซเบอร์ ธนาคารแห่งที่ 2 อาจจะถูกโจมตีในลักษณะเดียวกันได้ แต่หากมีการหารือกัน การโจมตีอาจเกิดขึ้นเพียง 1 หรือ 2 แห่งที่อาจจะไม่ระมัดระวังเท่านั้น ดังนั้น การประสานงานจึงเป็นส่วนหนึ่งในการที่จะทำให้ความมั่นคงปลอดภัยไซเบอร์แข็งแกร่งขึ้น ซึ่งนอกจากหน่วยงานในประเทศแล้ว ยังจำเป็นต้องมีการประสานงานกับหน่วยงานในต่างประเทศ เช่น สหรัฐอเมริกา อังกฤษ อิสราเอล รัสเซีย จีน เป็นต้น หรือทุกประเทศที่มีความมั่นคงปลอดภัยไซเบอร์ หรือมีพลังอำนาจด้านไซเบอร์สูงในระดับโลก

"สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ตามสถิติสูงสุดระดับชาติ พบว่า ช่องโหว่ต่างๆ เกิดขึ้นจากการพัฒนาแอพพลิเคชั่น และซอฟต์แวร์ต่างๆ ส่วนใหญ่ขาดกระบวนการในการดำเนินการให้ปลอดภัยตั้งแต่เริ่มต้น จึงเป็นเรื่องที่ต้องมีการหารือ เพื่อกำหนดแนวทางในการแก้ไขในระดับประเทศ เพราะ สกมช.ไม่สามารถที่จะตรวจสอบได้ครบทุกจุด แม้มีผู้ดูแลตลอด 24 ชั่วโมง ก็ไม่สามารถที่จะตรวจสอบได้ทั้งประเทศ การพัฒนาบุคลากร สร้างความรู้ความเข้าใจ เสริมสร้างความแข็งแกร่ง เพื่อให้เกิดความตระหนักถึงความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งสำคัญ"

"ช่องโหว่ที่มักถูกโจมตีทางไซเบอร์อย่างมากใน

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,550
Section: First Section/-
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 45 ฉบับที่: 16042 หน้า: 1(ล่าง), 2
Col.Inch: 143.76 Ad Value: 222,828 PRValue (x3): 668,484 คลิป: สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

ปัจจุบัน ได้แก่ 1.ระบบคอมพิวเตอร์ จะมีซอฟต์แวร์เป็นระบบปฏิบัติการ ซึ่งเขียนขึ้นจากผู้ที่มีความเชี่ยวชาญ และมีความระมัดระวังด้านความปลอดภัยจากการถูกโจมตีอยู่แล้ว ขณะเดียวกัน จะมีระบบปฏิบัติการอยู่ 2 โหมด คือ 1.จากผู้ที่เป็นแอดมิน และ 2.ผู้ใช้งาน แต่โดยทั่วไปคอมพิวเตอร์ของเราจะอยู่ในโหมดผู้ใช้งาน ดังนั้น อาชญากรไซเบอร์ หรือแฮกเกอร์ จึงจะพยายามโจมตีและเข้ามาอยู่ในโหมดของผู้ใช้งานก่อน จนสามารถยกระดับเป็นแอดมิน เมื่อเป็นแอดมินได้ แฮกเกอร์จะยึดเครื่อง ซึ่งเป็นอันตราย และเปรียบเหมือนบ้านที่มีช่องโหว่ นก หนู แมลงจึงจะสามารถเข้าได้ จึงต้องมีผู้ตรวจสอบ รวมถึงแฮกเกอร์เองจะหาช่องโหว่ไปพร้อมกัน และเมื่อเจอช่องโหว่จะมีการกำกับอยู่ในเว็บกลาง จึงต้องมีการตรวจสอบว่าหากมีการใช้ซอฟต์แวร์รุ่นนี้ เวอร์ชั่นนี้ คอมพิวเตอร์รุ่นนี้ หรือซีพียูนี้ จะมีช่องโหว่เรื่องนี้ ซึ่งสามารถใช้ในการโจมตีได้ เราจึงต้องติดตามประกาศอยู่เสมอว่าเรามีช่องโหว่ส่วนไหน และแนะนำให้มีการอัพเดตซอฟต์แวร์ ขณะที่ระบบปฏิบัติการแจ้งเตือน ควรดำเนินการตามคำแนะนำนั้น เพราะการอัพเดตถือเป็นการปิดช่องโหว่ต่างๆ เหล่านี้ได้ เป็นเรื่องที่ไม่ควรละเลย”

“และ 2.หลายครั้งที่แอดมินซึ่งเป็นผู้ดูแลระบบ มักจะละเลยเรื่องการอัพเดต เพราะมักจะมีปัญหา อาทิ ซอฟต์แวร์ต่างๆ ไม่ทำงานได้เหมือนเดิม จึงหลีกเลี่ยงอัพเดต ซึ่งจะเป็นภาระกับเจ้าหน้าที่ด้านไอที โดยเฉพาะอุปกรณ์ด้านการแพทย์ที่มีการอัพเดตแล้วมักมีความเสี่ยง แต่หากไม่อัพเดต ก็มีความเสี่ยงเช่นกัน เนื่องจากมีความอ่อนไหวอย่างมาก อาทิ เครื่องให้ยา เครื่องวัดต่างๆ ต้องมีการกำหนดเป็นมาตรฐาน จากผู้ที่ได้รับใบรับรอง

3.ซีโรเดย์ เป็นช่องโหว่คล้ายกัน แต่ผู้ที่พบส่วนใหญ่เป็นแฮกเกอร์ เจอแล้วจะไม่บอกใคร แอบเก็บกุญแจหรือประตูเข้าบ้านนี้ไว้ ไม่แจ้งไปที่ศูนย์กลางในการประสานงาน พอไม่แจ้งจึงเกิดช่องโหว่ที่เรียกว่าซีโรเดย์ ซึ่งหลายหน่วยงาน รวมถึงหน่วยข่าวกรองของประเทศมหาอำนาจ ก็อาศัยช่องโหว่ที่เป็นซีโรเดย์นี้ในการเข้าถึงคอมพิวเตอร์เป้าหมายเพื่อจะหาข้อมูลที่ตัวเองต้องการ เช่นเดียวกับหน่วยข่าวกรองในหลายประเทศ ทั้งนี้ ซีโรเดย์ยังเป็นสินค้าได้ด้วย โดยการนำไปประกาศในเว็บไซต์เถื่อนต่างๆ เพื่อนำซีโรเดย์นี้ใช้ในการเข้าระบบต่างๆ ที่ตกเป็นเหยื่อของช่องโหว่นั้นๆ”

พล.อ.ปรัชญากล่าวว่า บอกได้ยากว่า แฮกเกอร์หรือผู้ที่โจมตีเป็นกลุ่มใด เพราะต้องมีการสอบสวนขั้นสูง เรามีเลขไอพีคล้ายกับเลขที่บ้าน เมื่อคอมพิวเตอร์ติดต่อกันก็จะทราบถึงหมายเลขได้ ซึ่งบอกได้ว่ามาจากประเทศไหน แต่ยืนยันไม่ได้ชัดเจนว่าประเทศนั้นเป็นคนทำ ส่วนใหญ่แฮกเกอร์ที่จับกุมได้มักไม่มีประสบการณ์ ขณะเดียวกัน ก็จับกุมได้น้อยขึ้นอยู่กับหลักฐานที่แฮกเกอร์ทิ้งไว้ด้วย เพราะแฮกเกอร์ที่มีความสามารถจะลบรอยนิ้วมือ หรือไม่ทิ้งร่องรอยใดๆ ให้สามารถจับได้ ดังนั้น วิธีที่ดีที่สุด คือ การป้องกัน และการลดความเสี่ยง เพราะการติดตามต้องอาศัยทรัพยากร และคำนึงถึงความคุ้มค่าของมูลค่าของผลกระทบด้วย

“ภาพรวมสถานการณ์ความมั่นคงปลอดภัยไซเบอร์บ้านเรายังต้องพัฒนา การจะไม่ตกเป็นเหยื่อภัยทางไซเบอร์ ต้องมีความเฉลียวใจ ระมัดระวัง ระแวง คำนึงถึงความเป็นไปได้ ความตระหนัก ซึ่งเกิดจากความรู้ความเข้าใจเป็นเรื่องที่สำคัญ เปรียบเหมือนกับการฉีดวัคซีนไซเบอร์ เพื่อสร้างภูมิคุ้มกันภัยคุกคามทางไซเบอร์”

“หลายคนอาจเข้าใจว่า เมื่อมีการจัดตั้ง ‘สกมช.’ ขึ้นแล้ว เหมือนมีกองทัพที่มีความพร้อม และคอยดูแลปกป้องภัยทางไซเบอร์ ซึ่งไม่ใช่ แท้จริงแล้ว สกมช. เป็นหน่วยงานที่มีหน้าที่คล้ายกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ในการออกนโยบาย กำหนดแนวปฏิบัติ เราไม่มีกำลังคนเพียงพอที่จะดูแลทั้งประเทศ แม้อัตราโครงการของ สกมช. จะมีบุคลากรถึง 480 คน แต่ขณะนี้ยังมีพนักงานจริงๆ เพียง 40 คนเท่านั้น จึงจะดูแลเฉพาะส่วนที่มีผลกระทบร้ายแรงต่อความมั่นคง และส่งผลกระทบเป็นวงกว้างในระดับประเทศ ดังนั้น ทุกองค์กรจึงต้องป้องกันตัวเองในเบื้องต้น ก่อนที่ สกมช. จะเข้าไปช่วยเหลือ แก้ไข หากได้รับการโจมตี” พล.อ.ปรัชญากล่าว

และนั่นคือภาพรวมของหน่วยงานที่ทำหน้าที่ดูแลเฝ้าระวังภัยสมัยใหม่ ที่กำลังเร่งสร้างองค์กรเพื่อรับมือกับสถานการณ์ใหม่ ที่เชื่อว่าจะมีมากขึ้นและเพิ่มความซับซ้อนขึ้นเรื่อยๆ

บางกอกทูเดย์
Bangkok Today
Circulation: 150,000
Ad Rate: 1,000

Section: First Section/-
วันที่: ศุกร์ 11 - พฤหัสบดี 17 กุมภาพันธ์ 2565
ปีที่: 20 **ฉบับที่:** 3278 **หน้า:** 25(กลาง)
Col.Inch: 63.85 **Ad Value:** 63,850 **PRValue (x3):** 191,550 **คลิป:** สี่สี
หัวข้อข่าว: กสทช. แนะวิธีใช้งาน 'Mobile ID' สะดวก ปลอดภัย ง่ายทุกธุรกรรม

กสทช. แนะวิธีใช้งาน'Mobile ID' สะดวก ปลอดภัย ง่ายทุกธุรกรรม

สำนักงาน กสทช. เผยความสำเร็จในการเปิดลงทะเบียนสมัครใช้งาน "Mobile ID" เบอร์มือถือ แทนบัตร แทนตัวคุณ โดยมีแผนงานขยายขอบข่ายผู้ให้บริการและหน่วยงานต่างๆ เพิ่มมากขึ้น พร้อมเร่งเดินหน้าโปรโมทการใช้งาน Mobile ID ให้เข้าถึงและสร้างความเข้าใจกับประชาชนในวงกว้าง ผ่านภาพยนตร์โฆษณาชุดใหม่ ที่ถ่ายทอดเรื่องราวของเจเนอเรชั่นใหม่แห่งการยืนยันตัวตน รวมทั้งยังแนะนำวิธีสมัครใช้งาน Mobile ID เพียง 3 ขั้นตอนง่ายๆ "โชว์-แชะ-พร้อมใช้" เพื่อให้การทำธุรกรรมต่างๆ ของคุณ สะดวก ใช้งานง่าย ข้อมูลส่วนบุคคลปลอดภัย เพื่อคุณภาพชีวิตคนไทยทุกคนที่ดีขึ้น

หลังจากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) และเครือข่ายภาคี ได้เปิดให้ผู้ใช้บริการสามารถสมัครใช้บริการ "Mobile ID" เบอร์มือถือ แทนบัตร แทนตัวคุณ ตอนนี้ประชาชนคนไทยจะได้ใช้ประโยชน์จากระบบการพิสูจน์และยืนยันตัวตนด้วยรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ หรือ "Mobile ID" เพื่อใช้แสดงตนในการเข้าใช้บริการได้อย่างเป็นรูปธรรมและจริงจัง กับหลากหลายหน่วยงานทั้งภาครัฐและภาคเอกชน ตอกย้ำชัด 'หมดยุค' ยื่นเอกสารอีกต่อไปแล้ว

สำหรับระบบ Mobile ID นี้ ได้พัฒนาตามข้อกำหนดและมาตรฐานของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ ETDA ผู้ใช้งานจึงมั่นใจได้ว่าจะได้รับความสะดวกและปลอดภัย โดยมีการคุ้มครองข้อมูลส่วนบุคคล ป้องกันไม่ให้เกิดความเสี่ยงจนถูกมิจฉาชีพนำไปใช้หรือปลอมแปลงเพื่อสวมสิทธิ์ได้ ซึ่งการผลักดันให้ประชาชนหันมาใช้ Mobile ID มากขึ้นนี้ นอกจากจะช่วยขับเคลื่อนและส่งเสริมนโยบายรัฐบาลในเรื่องการใช้ดิจิทัลไอดีให้เห็นผลเป็นรูปธรรมชัดเจน ยังมีวัตถุประสงค์หลัก เพื่อสร้างสังคมดิจิทัลเต็มรูปแบบ ด้วยการเปลี่ยนสมาร์ทโฟนของทุกคนให้เป็นเครื่องมือสื่อสารยุคใหม่แห่งการทำธุรกรรมที่จะทำให้ชีวิตคนไทยทุกคนดีขึ้นอีกด้วย

ภายหลังการทดลองทดสอบ Mobile ID ในวงปิดมาระยะหนึ่งจนเป็นที่พอใจแล้ว บัดนี้ระบบมีความพร้อมที่จะให้บริการ Mobile ID อย่างเต็มรูปแบบสำหรับประชาชนทั่วไปในการเปิดบัญชีธนาคารกรุงเทพ โดยในระยะยาวสามารถใช้ Mobile ID เพื่อยืนยันตัวตนในการทำธุรกรรมได้อย่างหลากหลาย เช่น ขอใช้บริการโทรศัพท์เคลื่อนที่ ทำธุรกรรมฝาก โอน ถอน เปิดบัญชีที่ธนาคาร ยื่นขอทำใบขับขี่อิเล็กทรอนิกส์ ขอรับบริการจากรัฐและเอกชน และทำธุรกรรมออนไลน์ เป็นต้น อีกทั้งยังขยายขอบข่ายผู้ให้บริการเพิ่มมากขึ้น เพื่อให้ประชาชนได้ใช้บริการกับหน่วยงานอื่นๆ ตามที่สำนักงาน กสทช. ได้ทำข้อตกลงไว้

การใช้งาน Mobile ID ตามข้อตกลงของสำนักงาน กสทช. กับหน่วยงานต่างๆ ครอบคลุมถึงการสมัครใช้บริการใบขับขี่ดิจิทัล DLT QR License กับกรมขนส่งทางบก ติดต่อเชื่อมโยงกับกรมสรรพากรสำหรับเข้าระบบเพื่อยื่นภาษีออนไลน์ (E-FILING) เข้าสู่ระบบบริการขอใช้สิทธิประกันสังคมของสำนักงานประกันสังคม ยืนยันตัวตนในการเปิดบัญชีธนาคารกับธนาคารกรุงเทพ จำกัด (มหาชน) หรือเปิดบัญชีการลงทุนกับตลาดหลักทรัพย์แห่งประเทศไทย (SET) และใช้ได้กับ บริษัท ไปรษณีย์ไทย จำกัด เพื่อยืนยันตัวตนในการรับ-ส่ง พัสดุ เป็นต้น

นอกจากการสร้างการรับรู้ให้กับประชาชนทราบถึงนวัตกรรมใหม่ในการพิสูจน์และยืนยันตัวตนโดยไม่ต้องใช้บัตรประจำตัวประชาชน เพื่อรองรับบริการและธุรกรรมผ่านช่องทางออนไลน์ได้อย่างสะดวกสบายและปลอดภัยมากขึ้นแล้ว สำนักงาน กสทช. ยังมุ่งเน้นส่งต่อความเชื่อมั่นให้แก่ประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์กับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน โดยการสื่อสารผ่านช่องทางที่หลากหลาย ทั้งสื่อสิ่งพิมพ์และสื่อสังคมออนไลน์ (Social Media) ซึ่งได้รับการตอบรับและประชาชนได้เริ่มรับรู้เกี่ยวกับระบบดังกล่าวเพิ่มมากขึ้น

ปัจจุบัน สำนักงาน กสทช. จึงเดินหน้าต่อยอดประชาสัมพันธ์ Mobile ID เพิ่มเติมให้เป็นที่รับรู้ เข้าใจ และเกิดประโยชน์ในการใช้งานต่อไป โดยเชิญชวนให้ประชาชนสมัครใช้งาน Mobile ID พร้อมขจัดข้อสงสัยเกี่ยวกับการใช้งาน และได้รับข้อมูลอย่างครบถ้วน สำนักงาน กสทช. จึงได้จัดทำภาพยนตร์โฆษณาแนะนำการใช้งาน ซึ่งจะช่วยอธิบายขั้นตอนและวิธีการใช้งานการพิสูจน์

บางกอกทูเดย์
Bangkok Today
Circulation: 150,000
Ad Rate: 1,000

Section: First Section/-
วันที่: ศุกร์ 11 - พฤหัสบดี 17 กุมภาพันธ์ 2565
ปีที่: 20 **ฉบับที่:** 3278 **หน้า:** 25(กลาง)
Col.Inch: 63.85 **Ad Value:** 63,850 **PRValue (x3):** 191,550 **คลิป:** สี่สี
หัวข้อข่าว: กสทช. แนะวิธีใช้งาน 'Mobile ID' สะดวก ปลอดภัย ง่ายทุกธุรกรรม

และยืนยันตัวตนด้วยรูปแบบบัตรประจำตัวอิเล็กทรอนิกส์บนโทรศัพท์เคลื่อนที่ หรือ Mobile ID ผ่านช่องทางที่ประชาชนสามารถเข้าถึงง่าย ทั่วถึง สะดวก รวดเร็ว และถูกต้องมากยิ่งขึ้น

สำหรับภาพยนตร์โฆษณาได้อธิบายถึงรูปแบบการยืนยันตัวตนแบบเดิม ๆ ที่ต้องใช้เอกสารหลักฐานในรูปแบบกระดาษ หรือเอกสารหลักฐานฉบับจริง ต้องเข้าคิวเป็นเวลานาน ๆ ในการตรวจสอบเอกสารเพื่อติดต่อหรือทำธุรกรรมกับหน่วยงานต่างๆ แต่ปัญหานี้กำลังจะหมดไป พร้อมเข้าสู่เจเนอเรชั่นใหม่ในการยืนยันตัวตน ซึ่งเป็นครั้งแรกที่เราจะไม่ต้องยื่นบัตรประชาชน เอกสาร หรือแม้กระทั่งลายเซ็น และไม่จำเป็นต้องเดินทางอีกต่อไปแล้ว

นอกจากนั้น ภาพยนตร์โฆษณายังแสดงขั้นตอนสมัครใช้บริการ Mobile ID โดยเปลี่ยนบทบาทของเบอร์มือถือ ให้เป็นบัตรประจำตัวอิเล็กทรอนิกส์ ทดแทนการพกบัตรประชาชนหรือพาสปอร์ต เพื่อนำไปใช้ติดต่อสถานที่ราชการหรือเอกชนต่อไป

โดยประชาชนทุกคนสามารถเปิดใช้งาน Mobile ID เพียง 3 ขั้นตอนง่ายๆ ได้ที่ศูนย์บริการเครือข่ายโทรศัพท์มือถือ ที่ใช้งานอยู่ เพียง "โชว์" แสดงบัตรประชาชนแก่เจ้าหน้าที่ทำการตรวจสอบความถูกต้อง จากนั้น "แชะ" ด้วยการถ่ายภาพใบหน้า เพื่อลงทะเบียนเปรียบเทียบพิสูจน์ตัวตน เพียงเท่านี้ก็จะ "พร้อมใช้" มือถือเครื่องเดียวแทนบัตรเพื่อทำธุรกรรมอย่างปลอดภัย ทั้งข้อมูลและเงินไม่รั่วไหล และสามารถใช้บริการ Mobile ID ผ่านแอปพลิเคชันของเครือข่ายโทรศัพท์มือถือ กับธุรกรรมของหน่วยงานต่างๆ ทั้งภาครัฐและเอกชนได้แล้ว

ข่าวหุ้น
Khao Hoon
Circulation: 90,000
Ad Rate: 1,100

Section: First Section/บริษัทจดทะเบียน
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 28 **ฉบับที่:** 6879 **หน้า:** 1(ล่าง), 8
Col.Inch: 45.47 **Ad Value:** 50,017 **PRValue (x3):** 150,051 **คลิป:** สี่สี
หัวข้อข่าว: ITELเจรจาซื้อไอทีเอาท์ซอร์สซิ่งเล็งปิดดีลภายในไตรมาส2-3ปีนี้

ITEL 8
เจรจา
ซื้อไอทีเอาท์ซอร์สซิ่ง

ITELเจรจาซื้อไอทีเอาท์ซอร์สซิ่ง เล็งปิดดีลภายในไตรมาส2-3ปีนี้

ITEL ซุ่มเจรจาซื้อกิจการบริษัทด้าน IT out-sourcing เล็งปิดดีลภายในไตรมาส 2-3/65 ดันเข้าตลาดหลักทรัพย์ฯ ในปี 66 พร้อมเข้าลงทุน 5% ในบริษัทสตาร์ตอัพ กางแผนปี 65 รายได้พุ่ง 3,200 ล้านบาท อัตรากำไรสุทธิไม่ต่ำกว่า 10% ตุนแบ็กล็อก 3,500 ล้านบาท บุ๊กรายได้ปีนี้ 2,400-2,500 ล้านบาท จ่อเซ็นงานใหม่ปีนี้ 3,000 ล้านบาท

นายณัฐนัย อนันตรัมพร ประธานเจ้าหน้าที่บริหาร บริษัท อินเตอร์ลิ้งค์ เทเลคอม จำกัด (มหาชน) หรือ ITEL เปิดเผยว่า แผนการดำเนินงานในปี 2565 บริษัทคาดมีอัตรากำไรสุทธิไม่ต่ำกว่า 10% และตั้งเป้าหมายมีรายได้อยู่ที่ไม่ต่ำกว่า 3,200 ล้านบาท โดยปัจจุบันบริษัทมีงานในมือรอรับรู้รายได้ (Backlog) อยู่ที่ประมาณ 3,500 ล้านบาท คาดว่าจะรับรู้รายได้ในปี 2565 ประมาณ 2,400-2,500 ล้านบาท ส่วนที่เหลือทยอยรับรู้รายได้ในปีถัด ๆ ไป

ขณะที่ คาดว่าจะได้เซ็นสัญญางานใหม่เข้ามาเพิ่มเติม มูลค่ารวมไม่น้อยกว่า 3,000 ล้านบาท โดยน่าจะได้เซ็นสัญญาในไตรมาส 1/2565 มูลค่าประมาณ 1,300 ล้านบาท เช่น งานคอร์สออนไลน์ของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) มูลค่า 305 ล้านบาท และงาน USO-TOT มูลค่า 703 ล้านบาท โดย 56% เป็นงานให้บริการโครงข่าย และ 44% เป็นงานติดตั้งโครงข่าย หลังล่าสุดบริษัทได้งานติดตั้งโซลาร์เซลล์ (Solar Cell) ของผู้ให้บริการมือถือรายใหญ่ โดยเป็นงานติดตั้ง Solar Cell สำหรับสถานีฐานทั่วประเทศ (ยกเว้นกรุงเทพมหานคร) รวมมูลค่างานทั้งสิ้น 167.93 ล้านบาท (รวมภาษีมูลค่าเพิ่ม) โดยมีระยะเวลาดำเนินการโครงการ 180 วัน

นอกจากนี้ ปัจจุบันบริษัทอยู่ระหว่างเจรจากับกลุ่มลูกค้ารายใหญ่ระดับโลก (Hyperscaler) 1 ใน 4 ราย ได้แก่ Google, Facebook, Alibaba และ Amazon หลังจากได้พันธมิตรใหม่จากออสเตรเลียเข้ามา คาดว่าประมาณ 1 เดือนจากนี้ หรือประมาณเดือน ก.พ.-มี.ค. 2565 จะได้เซ็นสัญญากับลูกค้าดังกล่าว หลังจากนั้นลูกค้าน่าจะย้ายเข้ามาภายในเดือน มิ.ย.-ก.ค. 2565 โดยจะเข้ามาใช้บริการเริ่มแรกจำนวน 0.6 เมกะวัตต์ และเพิ่มเป็น 2 เมกะวัตต์ ภายใน 2 ปี ด้วยงบลงทุนรวม 200 ล้านบาท อีกทั้งบริษัทมีแผนขยายขนาดเป็น 6 เมกะวัตต์ ภายใน 2 ปีข้างหน้า โดยคาดว่าจะใช้งบลงทุนประมาณ 300-400 ล้านบาท

นายณัฐนัย กล่าวว่า บริษัทอยู่ระหว่างพิจารณาเข้าซื้อกิจการอีก 1 ดีล ซึ่งเป็นบริษัทด้าน IT outsourcing ที่มีความชำนาญด้าน Cyber Security และความชำนาญด้านซอฟต์แวร์ ปัจจุบันอยู่ระหว่างการทำ Due Diligence คาดว่าแล้วเสร็จภายในเดือน เม.ย. 2565 จากนั้นจะดำเนินการเข้าซื้อภายในไตรมาส 2-3/2565 เข้าถือหุ้นในสัดส่วนไม่น้อยกว่า 51%

ข่าวหุ้น
Khao Hoon
Circulation: 90,000
Ad Rate: 1,100

Section: First Section/บริษัทจดทะเบียน
วันที่: ศุกร์ 11 กุมภาพันธ์ 2565
ปีที่: 28 **ฉบับที่:** 6879 **หน้า:** 1(ล่าง), 8
Col.Inch: 45.47 **Ad Value:** 50,017 **PRValue (x3):** 150,051 **คลิป:** สี่สี
หัวข้อข่าว: ITELเจรจาซื้อไอทีเอาท์ซอร์สซิ่งเล็งปิดดีลภายในไตรมาส2-3ปีนี้

นอกจากนี้ หลังจากที่บริษัทจะทำ Swap Share เข้าถือหุ้น 51% ในบริษัท บลู โซลูชั่น จำกัด (BS) ผู้ให้บริการวางระบบ (System Integrator) ซึ่ง BS เป็นบริษัทย่อยที่ถือหุ้นโดยบริษัท เวทเธอเรีย อี จำกัด คาดว่าขั้นตอนจะแล้วเสร็จภายในไตรมาส 1/2565 ทำให้บริษัทมีรายได้เพิ่มขึ้น 500-700 ล้านบาท/ปี จากการรวมงบของ BS เข้ามา และมีแผนผลักดันให้บริษัทดังกล่าวเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ อย่างเร็วสุดในปี 2566 รวมทั้งบริษัทยังอยู่ระหว่างการเจรจาเข้าถือหุ้นบริษัทสตาร์ตอัพสัญชาติไทยด้านเทคโนโลยีที่เตรียมเข้าจดทะเบียนในตลาดหลักทรัพย์ฯ ในปี 2565 ในสัดส่วน 5%

ส่วนการขายสินทรัพย์เข้ากองทรัสต์ของทรัสต์เพื่อการลงทุนในสิทธิการเช่าอสังหาริมทรัพย์มูลค่า 750 ล้านบาท คาดว่าจะแล้วเสร็จและได้รับเงินภายในช่วงไตรมาส 1/2565 โดยเงินทุนดังกล่าวจะใช้ในการคืนเงินกู้ ทำให้อัตราส่วนหนี้สินต่อทุน (D/E) ปลายปี 2565 ลดลงเหลือ 0.7-0.9 เท่า จากปัจจุบัน 1.6-1.7 เท่า และลงทุนในดาต้าเซ็นเตอร์และกิจการอื่น ๆ ต่อไป ■

มติชน กรอบบ่าย
Matichon (Mid-Day)
Circulation: 950,000
Ad Rate: 1,550

Section: First Section/-
วันที่: เสาร์ 12 กุมภาพันธ์ 2565
ปีที่: 45 **ฉบับที่:** 16043 **หน้า:** 1(กลาง), 2
Col.Inch: 143.50 **Ad Value:** 222,425 **PRValue (x3):** 667,275 **คลิป:** สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

พล.อ.ปรัชญา เฉลิมวัฒน์

จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

หมายเหตุ - *มติชนสัมภาษณ์พิเศษ พล.อ.ปรัชญา เฉลิมวัฒน์ เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งทำหน้าที่บริหารหน่วยงานดูแลความปลอดภัยไซเบอร์แห่งชาติ ซึ่งจัดตั้งมาได้ 1 ปี เพื่อรับมือกับภัยสมัยใหม่ที่มากับเทคโนโลยีที่นับวันยิ่งก้าวหน้า สถานการณ์ด้านภัยไซเบอร์ และการรับมือเป็นอย่างไร เป็นเรื่องที่สังคมและประชาชนคนไทยควรจะได้รับรู้ ผ่านบทสัมภาษณ์พิเศษชิ้นนี้*

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานใหม่ ที่จัดตั้งขึ้นอย่างเร่งด่วนเพื่อรับมือสถานการณ์ใหม่ทางด้านภัยไซเบอร์ ที่มากับเทคโนโลยีสมัยใหม่ที่มีคุณูปการมากมาย แต่ในอีกด้านของความก้าวหน้า การใช้ระบบอินเตอร์เน็ต การใช้เทคโนโลยีด้านการสื่อสาร โดยบิดเบือนเพื่อประโยชน์เฉพาะกลุ่มหรือเพื่อก่อกวนบั่นทอนสังคม ก็กำลังเป็นปัญหาในระดับโลก และในระดับประเทศ

สกมช.เป็นหน่วยงานที่อยู่ระหว่างการสร้างความพร้อมอย่างรีบเร่ง ผู้ทำหน้าที่บุกเบิกหน่วยงานนี้คือ นายทหารสายวิทยาศาสตร์มือดี ที่แวดวงกองทัพรู้จักกันดี คือ **พล.อ.ปรัชญา เฉลิมวัฒน์** เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ลธ.กมช.)

พล.อ.ปรัชญาอธิบายที่มาที่ไปของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ สกมช. ว่าเกิดขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 มีผลใช้บังคับเมื่อพฤษภาคม 2562 ก่อนจัดตั้งสำนักงานเมื่อ 1 มกราคม 2564

จัดตั้งขึ้นโดยศึกษารูปแบบจากต่างประเทศ และจำลองสิ่งที่จะเกิดขึ้นเพื่อเข้าไปรับมือ เกี่ยวข้องกับ 4 พันธกิจหลัก ประกอบด้วย

1.หน่วยงานกำกับดูแลการดำเนินนโยบาย ตามแนวปฏิบัติ กำหนดหน้าที่อำนาจต่างๆ ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยวัตถุประสงค์หลักของกฎหมายฉบับนี้ ในการจัดตั้ง สกมช.ขึ้น เพื่อดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII : Critical Information Infrastructure)

ซึ่งกำหนดไว้ 8 ด้าน ได้แก่ ด้านความมั่นคงของรัฐ, ด้านบริการภาครัฐที่สำคัญ, ด้านการเงินการธนาคาร, ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม, ด้านการขนส่งและโลจิสติกส์, ด้านพลังงานและสาธารณูปโภค, ด้านสาธารณสุข และด้านอื่นตามที่คณะกรรมการประกาศเพิ่มเติม

"ถือเป็นเรื่องค่อนข้างใหญ่ ขอบเขตงานหรือความรู้ที่อยู่ในความรับผิดชอบเป็นวงกว้าง ดังนั้นคงต้องใช้เวลาสักระยะ ประมาณ 2 ปี สร้างความพร้อมให้ทุกเซ็กเตอร์ ราชกิจจานุเบกษาระบุไว้ชัดเจนว่าหน่วยงานใดบ้างที่จะเป็นซีไอไอ แต่เราจะเป็นผู้กำหนดลักษณะว่า หากมีบริการที่สำคัญในลักษณะนี้ หน่วยงานนั้นๆ จะเป็นซีไอไอหรือไม่ โดยหน่วยงานที่เป็นซีไอไอจะต้องปฏิบัติตามประกาศของ กมช. ซึ่งเป็นคณะกรรมการชุดใหญ่ มี พล.อ.ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรี เป็นประธาน ขณะที่ สกมช.จะขึ้นตรงกับ พล.อ.ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี"

"ยังมีคณะกรรมการกำกับดูแลด้านความมั่นคง

มติชน กรอบบ่าย
Matichon (Mid-Day)
Circulation: 950,000
Ad Rate: 1,550

Section: First Section/-
วันที่: เสาร์ 12 กุมภาพันธ์ 2565
ปีที่: 45 **ฉบับที่:** 16043 **หน้า:** 1(กลาง), 2
Col.Inch: 143.50 **Ad Value:** 222,425 **PRValue (x3):** 667,275 **คลิป:** สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

ปลอดภัยไซเบอร์ (กกม.) มี นายชัยวุฒิ ธนาคมานุสรณ์ รัฐมนตรีว่าการกระทรวงดีอีเอส เป็นประธาน และมีปลัดกระทรวง และผู้มีหน้าที่ขับเคลื่อนองค์กรต่างๆ ที่เกี่ยวข้อง หากเกิดการโจมตีขนาดใหญ่ ที่เข้าขั้นร้ายแรงหรือวิกฤต คณะกรรมการชุดนี้จะหารือร่วมกัน เพื่อหาทางรับมือกับเรื่องนี้ และคณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.) ดังนั้น สกมช.จะเกี่ยวข้องกับกระทรวงดีอีเอส ในลักษณะการทำงานร่วมกัน เนื่องจากกระทรวงดีอีเอสเป็นผู้รับผิดชอบในส่วนของพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 หรือ พ.ร.บ.คอมพิวเตอร์ ที่มีการกระทำความผิดด้านการละเมิดต่างๆ แต่ส่วนของ พ.ร.บ.ไซเบอร์ จะเน้นการเสริมสร้างความแข็งแกร่งให้กับหน่วยงานที่เป็นซีไอไอ" พล.อ.ปรัชญากล่าว

2.สกมช.จะเป็นหน่วยงานหลักในการประสานงาน โดยกระทรวงดีอีเอสจะรับผิดชอบส่วนของ พ.ร.บ.คอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 โดยมีศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert : ไทยเซิร์ต) ซึ่งตอนนี้อยู่ภายใต้สังกัดของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือเอ็ตด้า ซึ่งใน พ.ร.บ.ไซเบอร์ กำหนดให้ สกมช.เป็นผู้ดูแลในระดับประเทศ มีลักษณะหน้าที่เป็นศูนย์กลางในประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งมีหน่วยงานในซีไอไอกว่า 300 แห่ง ต้องอาศัยศูนย์กลางในประสาน ปัจจุบันมีการจัดตั้ง 'ไทยแบงก์เซิร์ต' ซึ่งเป็นหน่วยงานในซีไอไอ ด้านการเงินการธนาคารแห่งแรก และถัดมามีการจัดตั้ง 'เทลโก้เซิร์ต' ตามคำแนะนำของเอนิซ่า องค์กรของสหภาพยุโรป (อียู) ที่ดูแลเรื่องความมั่นคงปลอดภัยทางไซเบอร์

โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ CERT มีอยู่ทั่วโลก เกิดจากมหาวิทยาลัยคาร์เนกีเมลลอน เป็นผู้กำหนดการลงทะเบียน หากแต่ละประเทศต้องการที่จัดตั้งศูนย์ประสานดังกล่าวจะต้องมีการขออนุญาต โดยศูนย์ประสาน อาทิ เจแปนเซิร์ต ยูเอสเซิร์ต จะทำหน้าที่ประสานงาน แลกเปลี่ยนข้อมูล แจ้งเตือน เฝ้าติดตาม และปฏิบัติหน้าที่ ตามที่มีการกำหนด ซึ่งหากภารกิจเยอะจำเป็นต้องใช้ทรัพยากรทั้งงบประมาณและบุคลากรจำนวนมาก

3.การพัฒนาบุคลากร แม้ไม่มีโรงเรียนที่เปิดสอนโดยตรง แต่จะมีโครงการต่างๆ อาทิ การจัดอบรม มีการสอบใบรับรอง และให้ใบรับรอง เพื่อให้บุคลากรมีความรู้ โดยปี 2564-2565 มีโครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งได้รับทุนสนับสนุนจำนวน 119 ล้านบาท จากสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (กสทช.) โดยตั้งเป้าที่จะพัฒนาบุคลากรระดับพื้นฐาน 2,025 คน แต่คาดว่าจะได้มากกว่า เพราะปรับเปลี่ยนรูปแบบการจัดฝึกอบรมจากระบบออฟไลน์เป็นออนไลน์ และระดับผู้เชี่ยวชาญ จำนวน 300 คน ซึ่ง

ส่วนหนึ่งของจำนวนดังกล่าว จะส่งเสริมให้มีใบรับรองระดับสากล เพื่อใช้เป็นดัชนีชี้วัดด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ อย่างไรก็ตาม ปัจจุบันประเทศไทยมีผู้เชี่ยวชาญที่ได้รับใบรับรองระดับสากลเพียง 200 คน ขณะที่สิงคโปร์ มีถึง 1,000 คน ทั้งนี้ยังมีการจัดการแข่งขัน 'ไทยแลนด์ไซเบอร์ก็อตทาเลนต์' ใน 3 ระดับ ได้แก่ มัธยมศึกษา อุดมศึกษา และระดับบุคคลทั่วไป ซึ่งส่วนใหญ่เป็นผู้ปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มีประสบการณ์ด้านการทำงานและเคยผ่านการแข่งขันระดับเวทีโลก โดยส่วนนี้ได้รับความสนใจเป็นอย่างมาก เนื่องจากมีเงินรางวัลจูงใจ สูงสุดเท่าที่เคยจัดการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยความช่วยเหลือจากผู้ประกอบการ เพราะลำพังสำนักงานเองไม่มีงบประมาณเพียงพอ

และ **4.การทำความร่วมกับหน่วยงานทุกภาคส่วนทั้งในและต่างประเทศ** เพราะการป้องกันภัยด้านไซเบอร์ไม่สามารถต่อสู้ได้เพียงลำพัง ซึ่งแตกต่างจากเรื่องอื่น จึงจำเป็นต้องก้าวไปไปพร้อมกัน เช่น มีอยู่ธนาคารทั้งหมด 10 แห่ง มีธนาคาร 1 แห่งถูกโจมตีทางไซเบอร์ ธนาคารแห่งที่ 2 อาจจะถูกโจมตีในลักษณะเดียวกันได้ แต่หากมีการหารือกัน การโจมตีอาจเกิดขึ้นเพียง 1 หรือ 2 แห่งที่อาจจะไม่ระมัดระวังเท่านั้น ดังนั้น การประสานงานจึงเป็นส่วนหนึ่งในการที่จะทำให้ความมั่นคงปลอดภัยไซเบอร์แข็งแกร่งขึ้น ซึ่งนอกจากหน่วยงานในประเทศแล้ว ยังจำเป็นต้องมีการประสานงานกับหน่วยงานในต่างประเทศ เช่น สหรัฐอเมริกา อังกฤษ อิสราเอล รัสเซีย จีน เป็นต้น หรือทุกประเทศที่มีความมั่นคงปลอดภัยไซเบอร์ หรือมีพลังอำนาจด้านไซเบอร์สูงในระดับโลก

"สถานการณ์ความมั่นคงปลอดภัยไซเบอร์ ตามสถิติสูงสุดระดับชาติ พบว่า ช่องโหว่ต่างๆ เกิดขึ้นจากการพัฒนาแอพพลิเคชั่น และซอฟต์แวร์ต่างๆ ส่วนใหญ่ขาดกระบวนการในการดำเนินการให้ปลอดภัยตั้งแต่เริ่มต้น จึงเป็นเรื่องที่ต้องมีการหารือ เพื่อกำหนดแนวทางในการแก้ไขในระดับประเทศ เพราะ สกมช.ไม่สามารถที่จะตรวจสอบได้ครบทุกจุด แม้มีผู้ดูแลตลอด 24 ชั่วโมง ก็ไม่สามารถที่จะตรวจสอบได้ทั้งประเทศ การพัฒนาบุคลากร สร้างความรู้ความเข้าใจ เสริมสร้างความแข็งแกร่ง เพื่อให้เกิดความตระหนักถึงความมั่นคงปลอดภัยไซเบอร์จึงเป็นสิ่งสำคัญ"

"ช่องโหว่ที่มักถูกโจมตีทางไซเบอร์อย่างมากใน

มติชน กรอบบ่าย
Matichon (Mid-Day)
Circulation: 950,000
Ad Rate: 1,550
Section: First Section/-
วันที่: เสาร์ 12 กุมภาพันธ์ 2565
ปีที่: 45 ฉบับที่: 16043 หน้า: 1(กลาง), 2
Col.Inch: 143.50 Ad Value: 222,425 PRValue (x3): 667,275 คลิป: สี่สี
หัวข้อข่าว: พล.อ.ปรัชญา เฉลิมวัฒน์ จัดทัพ-จัดวัคซีนไซเบอร์ รับมือสงครามออนไลน์

ปัจจุบัน ได้แก่ 1.ระบบคอมพิวเตอร์ จะมีซอฟต์แวร์เป็นระบบปฏิบัติการ ซึ่งเขียนขึ้นจากผู้ที่มีความเชี่ยวชาญ และมีความระมัดระวังด้านความปลอดภัยจากการถูกโจมตีอยู่แล้ว ขณะเดียวกัน จะมีระบบปฏิบัติการอยู่ 2 โหมด คือ 1.จากผู้ที่เป็นแอดมิน และ 2.ผู้ใช้งาน แต่โดยทั่วไปคอมพิวเตอร์ของเราจะอยู่ในโหมดผู้ใช้งาน ดังนั้น อาชญากรไซเบอร์ หรือแฮกเกอร์ จึงจะพยายามโจมตีและเข้ามาอยู่ในโหมดของผู้ใช้งานก่อน จนสามารถยกระดับเป็นแอดมิน เมื่อเป็นแอดมินได้ แฮกเกอร์จะยึดเครื่อง ซึ่งเป็นอันตราย และเปรียบเหมือนบ้านที่มีช่องโหว่ นก หนู แมลงจึงจะสามารถเข้าได้ จึงต้องมีผู้ตรวจสอบ รวมถึงแฮกเกอร์เองจะหาช่องโหว่ไปพร้อมกัน และเมื่อเจอช่องโหว่จะมีการกำกับอยู่ในเว็บกลาง จึงต้องมีการตรวจสอบว่าหากมีการใช้ซอฟต์แวร์รุ่นนี้ เวอร์ชั่นนี้ คอมพิวเตอร์รุ่นนี้ หรือซีพียูนี้ จะมีช่องโหว่เรื่องนี้ ซึ่งสามารถใช้ในการโจมตีได้ เราจึงต้องติดตามประกาศอยู่เสมอว่าเรามีช่องโหว่ส่วนไหน และแนะนำให้มีการอัพเดตซอฟต์แวร์ ขณะที่ระบบปฏิบัติการแจ้งเตือน ควรดำเนินการตามคำแนะนำนั้น เพราะการอัพเดตถือเป็นการปิดช่องโหว่ต่างๆ เหล่านี้ได้ เป็นเรื่องที่ควรละเลย"

"และ 2.หลายครั้งที่แอดมินซึ่งเป็นผู้ดูแลระบบ มักจะละเลยเรื่องการอัพเดต เพราะมักจะมีปัญหา อาทิ ซอฟต์แวร์ต่างๆ ไม่ทำงานได้เหมือนเดิม จึงหลีกเลี่ยงอัพเดต ซึ่งจะเป็นภาระกับเจ้าหน้าที่ด้านไอที โดยเฉพาะอุปกรณ์ด้านการแพทย์ที่มีการอัพเดตแล้วมักมีความเสี่ยง แต่หากไม่อัพเดต ก็มีความเสี่ยงเช่นกัน เนื่องจากมีความอ่อนไหวอย่างมาก อาทิ เครื่องให้ยา เครื่องวัดต่างๆ ต้องมีการกำหนดเป็นมาตรฐาน จากผู้ที่ได้รับใบรับรอง

3.ซีโรเดย์ เป็นช่องโหว่คล้ายกัน แต่ผู้ที่พบส่วนใหญ่เป็นแฮกเกอร์ เจอแล้วจะไม่บอกใคร แอบเก็บกุญแจหรือประตูเข้าบ้านนี้ไว้ ไม่แจ้งไปที่ศูนย์กลางในการประสานงาน พอไม่แจ้งจึงเกิดช่องโหว่ที่เรียกว่าซีโรเดย์ ซึ่งหลายหน่วยงาน รวมถึงหน่วยข่าวกรองของประเทศมหาอำนาจ ก็อาศัยช่องโหว่ที่เป็นซีโรเดย์นี้ในการเข้าถึงคอมพิวเตอร์เป้าหมายเพื่อจะหาข้อมูลที่ตัวเองต้องการ เช่นเดียวกับหน่วยข่าวกรองในหลายประเทศ ทั้งนี้ ซีโรเดย์ยังเป็นสินค้าได้ด้วย โดยการนำไปประกาศในเว็บไซต์เถื่อนต่างๆ เพื่อนำซีโรเดย์นี้ไปใช้ในการเข้าระบบต่างๆ ที่ตกเป็นเหยื่อของช่องโหว่นั้นๆ"

พล.อ.ปรัชญากล่าวว่า บอกได้ยากว่า แฮกเกอร์หรือผู้ที่โจมตีเป็นกลุ่มใด เพราะต้องมีการสอบสวนขั้นสูง เรามีเลขไอพีคล้ายกับเลขที่บ้าน เมื่อคอมพิวเตอร์ติดต่อกันก็จะทราบถึงหมายเลขได้ ซึ่งบอกได้ว่ามาจากประเทศไหน แต่ยืนยันไม่ได้ชัดเจนว่าประเทศนั้นเป็นคนทำ ส่วนใหญ่แฮกเกอร์ที่จับกุมได้มักไม่มีประสบการณ์ ขณะเดียวกัน ก็จับกุมได้น้อยขึ้นอยู่กับหลักฐานที่แฮกเกอร์ทิ้งไว้ด้วย เพราะแฮกเกอร์ที่มีความสามารถจะลบรอยนิ้วมือ หรือไม่ทิ้งร่องรอยใดๆ ให้สามารถจับได้ ดังนั้น วิธีที่ดีที่สุด คือ การป้องกัน และการลดความเสี่ยง เพราะการติดตามต้องอาศัยทรัพยากร และคำนึงถึงความคุ้มค่าของมูลค่าของผลกระทบด้วย

"ภาพรวมสถานการณ์ความมั่นคงปลอดภัยไซเบอร์บ้านเรายังต้องพัฒนา การจะไม่ตกเป็นเหยื่อภัยทางไซเบอร์ ต้องมีความเฉลียวใจ ระมัดระวัง ระแวง คำนึงถึงความเป็นไปได้ ความตระหนัก ซึ่งเกิดจากความรู้ความเข้าใจเป็นเรื่องที่สำคัญ เปรียบเหมือนกับการฉีดวัคซีนไซเบอร์ เพื่อสร้างภูมิคุ้มกันภัยคุกคามทางไซเบอร์"

"หลายคนอาจเข้าใจว่า เมื่อมีการจัดตั้ง 'สกมช.' ขึ้นแล้ว เหมือนมีกองทัพที่มีความพร้อม และคอยดูแลปกป้องภัยทางไซเบอร์ ซึ่งไม่ใช่ แท้จริงแล้ว สกมช. เป็นหน่วยงานที่มีหน้าที่คล้ายกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ในการออกนโยบาย กำหนดแนวปฏิบัติ เราไม่มีกำลังคนเพียงพอที่จะดูแลทั้งประเทศ แม้อัตราโครงการของ สกมช. จะมีบุคลากรถึง 480 คน แต่ขณะนี้ยังมีพนักงานจริงๆ เพียง 40 คนเท่านั้น จึงจะดูแลเฉพาะส่วนที่มีผลกระทบร้ายแรงต่อความมั่นคง และส่งผลกระทบเป็นวงกว้างในระดับประเทศ ดังนั้น ทุกองค์กรจึงต้องป้องกันตัวเองในเบื้องต้น ก่อนที่ สกมช. จะเข้าไปช่วยเหลือ แก้ไข หากได้รับการโจมตี" พล.อ.ปรัชญากล่าว

และนั่นคือภาพรวมของหน่วยงานที่ทำหน้าที่ดูแลเฝ้าระวังภัยสมัยใหม่ ที่กำลังเร่งสร้างองค์กรเพื่อรับมือกับสถานการณ์ใหม่ ที่เชื่อว่าจะมีมากขึ้นและเพิ่มความซับซ้อนขึ้นเรื่อยๆ