ETDA (เอ็ตด้า) ตั้งรับภัยไซเบอร์-ร่วมแชร์ข้อมูลระหว่างองค์กร ระงับเหตุก่อนลุกลาม

ภัยคุกคามไซเบอร์ที่ทวีความรุนแรงมากขึ้น ก่อให้เกิดความตระหนักในหน่วยงานถึงการมีทีมงานด้าน Cybersecurity เพื่อตั้งรับภัยไซเบอร์ได้อย่างทันท่วงที รวมถึงการแชร์ข้อมูลกับทีมหรือหน่วยงานอื่น ๆ เพื่อควบคุมและระงับการแพร่ขยายของเหตุภัยคุกคามให้เร็วที่สุด

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงไอซีที โดย ThaiCERT หรือ ไทยเซิร์ต เปิดบ้านเชิญหน่วยงานที่เป็น Critical Infrastructure (CI) และผู้สนใจเข้าร่วมรับฟังและพูดคุยหัวข้อ “แนวทางการจัดตั้ง Computer Security Incident Response Team (CSIRT) เพื่อเตรียมรับมือภัยคุกคามไซเบอร์ (CSIRT Building Recommendations for Handling Cyber Threats)” ณ ห้อง Open Forum ของ ETDA โดยได้รับเกียรติจาก กำพล ศรธนะรัตน์ ผู้อำนวยการฝ่ายเทคโนโลยีและการสื่อสาร สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (กลต.) ดร.กิตติ โฆษะวิสุทธิ์ ผู้จัดการฝ่ายความปลอดภัยเทคโนโลยีสารสนเทศ ธนาคารกรุงเทพ จำกัด (มหาชน) ชูชัย วชิรบรรจง กรรมการที่ปรึกษา (ประธานชมรม IT ประกันภัย) สมาคมประกันวินาศภัยไทย เกียรติตระการ ญาณมุข ผู้ช่วยกรรมการใหญ่อาวุโส สายงานเทคโนโลยีสารสนเทศฯ บมจ.ไทยพาณิชย์ประกันชีวิต ร่วมเสวนา โดยมี ดร.สรณันท์ จิวะสุรัตน์ ผู้อำนวยการอาวุโส สำนักวิจัยและพัฒนา และรักษาการผู้อำนวยการ สำนักความมั่นคงปลอดภัย ETDA เป็นผู้ดำเนินรายการ รวมทั้งมี Martijn van der Heide CERT Specialist ของไทยเซิร์ต เป็นวิทยากรบรรยายเรื่อง “Establishing CSIRT” ก่อนการเสวนา

สุรางคณา วายุภาพ ผู้อำนวยการ ETDA กล่าวเปิดว่า สืบเนื่องจากภัยคุกคามในบ้านเรามีมากขึ้นตามลำดับ การทำงานแต่เพียงลำพังหน่วยงานเดียวคงไม่สามารถทำได้ ต้องสร้างเครือข่ายความร่วมมือแล้วทำงานให้เป็นระบบที่ยอมรับกันได้ทั่วโลก โดยไทยเซิร์ตพร้อมจะเป็นเครือข่ายสำคัญสำหรับความร่วมมือ รวมทั้งน้อมรับความเห็น ตลอดจนยินดีจะช่วย support การทำงานของหน่วยงานต่าง ๆ

Martijn เสริมว่า ไทยเซิร์ต พร้อมที่จะสนับสนุนให้หน่วยงานต่าง ๆ จัดตั้ง CERT (Computer Emergency Response Team) หรือ CSIRT โดยปัจจุบัน ETDA กำลังจัดทำคู่การจัดตั้ง CERT/CSIRT เพื่ออธิบายกระบวนการในการจัดตั้งและการปฏิบัติงานอย่างเป็นขั้นตอน ซึ่งถ้าหน่วยงานต่าง ๆ นำไปปฏิบัติ ก็ยินดีอย่างยิ่งที่จะมาร่วมเครือข่าย เพื่อแชร์ข้อมูลกันก่อนที่จะได้รับความเสียหาย โดยผู้ที่สนใจสามารถติดต่อเพื่อขอรับร่างคู่มือนี้ซึ่งใกล้เสร็จ

สมบูรณ์แล้ว และตอบแบบสำรวจกลับมายังไทยเซิร์ต เพื่อนำมาปรับปรุงร่างคู่มือฉบับนี้ให้สมบูรณ์ที่สุดก่อนเผยแพร่ต่อไป

กำพล ซึ่งเป็นตัวแทนจากฝั่งตลาดหลักทรัพย์กล่าวว่า กลต. กำลังจะประกาศ Regulation ใหม่ ที่เน้นเรื่อง Cybersecurity เพิ่มขึ้น รวมทั้งเรื่อง CERT, Governance of Enterprise IT ซึ่งอ้างอิง COBIT 5, ISO 27001, 27002 โดยจะมี Grace Period (ระยะผ่อนผัน) ให้หนึ่งปี แล้วจึงเข้าไป Audit ซึ่ง Regulation ตัวนี้มีการจัดทำเป็นปี โดยผ่านขั้นตอนต่าง ๆ รวมทั้งยังมีการรับฟังความคิดเห็นแล้ว ซึ่งจะใช้รองรับการตั้ง Sector-based CERT ระหว่าง 3 หน่วยงานด้วย คือ กลต. ธนาคารแห่งประเทศไทย และคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (คปภ.) ซึ่งภายใต้ กลต. เองก็ต้องไปหารือกันภายในระหว่างสมาชิก ว่ารูปแบบที่จะทำงาน จะแชร์ข้อมูลขนาดไหน ซึ่งหวัง ETDA จะมีส่วนช่วยในเรื่องนี้ ทั้งการสร้าง Awareness และกรอบกติกาต่าง ๆ

ทางภาคประกันวินาศภัย ชูชัย กล่าวว่า เนื่องจากกำลังจะมีการให้บริการกรมธรรม์ออนไลน์ภายในสิ้นปีนี้หรือปีหน้า Cybersecurity จึงเป็นเรื่องสำคัญ เพราะถ้าระบบ Security ไม่ดีพอ ก็จะส่งผลต่อความเชื่อมั่นและเกิดผลกระทบสูง ซึ่งที่ผ่านมา หลายองค์กรมีปัญหาเรื่องของบลงทุนด้าน Security เพราะเห็นผลลัพธ์หรือระบุตัวชี้วัดยาก หน่วยงานเล็กไม่มีเครื่องมือที่มีประสิทธิภาพ หรือผู้บริหารยังไม่ได้ให้ความสำคัญเท่าที่ควร ซึ่งหากมีการแชร์ข้อมูลระหว่าง Sector ภาคประกันวินาศภัยคงจะแข็งแกร่งขึ้น เนื่องจากธุรกิจประกันวินาศภัยมีความเชื่อมโยงกับภาคการเงินอื่น ๆ และธุรกิจประกันวินาศภัยมีคู่ค้ามากมาย ซึ่งการเชื่อมโยงผ่านอิเล็กทรอนิกส์จะทำให้เกิดประโยชน์กับธุรกิจ

ในส่วนประกันชีวิต เกียรติตระการ กล่าวว่า มีการแชร์ข้อมูลระหว่างหน่วยงานต่าง ๆ ในระดับปฏิบัติการ เช่น ข้อมูลการโจมตี โดยปัจจุบันมีการพัฒนาใช้อุปกรณ์ที่ทันสมัยขึ้น เช่น Security Information and Event Management (SIEM) แต่บางครั้งแฮกเกอร์ก็มีวิธีการโจมตีอื่น ๆ เช่น DDos ซึ่งต้องอาศัยความร่วมมือจากหน่วยงานอื่น เช่น ISP (CAT) เพื่อช่วยให้บล็อกทราฟฟิก ทำให้เห็นว่าการแชร์ข้อมูลและร่วมมือกันนั้นสำคัญมาก

ในส่วนภาคการเงินการธนาคาร ดร.กิตติ กล่าวว่า ลักษณะธุรกิจที่เปลี่ยนไปทำให้ต้องเชื่อมต่อมากขึ้น ไม่ได้เสร็จในหน่วยงานเดียว ทั้งลูกค้า คู่ค้า และฟินเทคในอนาคต เมื่อระบบเชื่อมต่อและเกิดเหตุอะไรขึ้นมาก็ต้องตามไปทั้งกระบวนการ ซึ่งระบบเชื่อมต่อแล้วก็ต้องเชื่อมต่อคน เวลาเกิดเหตุ แต่ละ Sector ก็มีความสนใจและเป้าหมายแตกต่างกัน การแชร์ข้อมูลระหว่าง Sector อาจจะยากกว่า ซึ่งต้องแชร์ข้อมูลกันภายใน Sector ก่อน หากแชร์ได้เร็วหน่วยงานที่ 2 หน่วยงานที่ 3 ก็ลดผลกระทบลงได้ และเพราะมีมุมในแง่ของการแข่งขันระหว่างหน่วยงานด้วยจึงต้องกำหนดกรอบและข้อมูลที่จะแชร์ ซึ่งจะต้องมีการวางใจหรือเชื่อใจกัน (Trust) ด้วย ซึ่งใน Sector เดียวกัน เช่น ที่ภาคการเงินได้เริ่มทำ ก็มีการทำความรู้จักกันและสร้างบรรยากาศในการแชร์ที่ทุกคนสบายใจ

ดร.สรณันท์ ในฐานะตัวแทนของไทยเซิร์ต ได้แชร์เรื่องแนวทางพัฒนา CERT ซึ่งอยู่ในเอกสารร่างคู่มือ โดยต้องการความคิดเห็นจากผู้ที่เกี่ยวข้องทุกฝ่าย เพื่อให้หน่วยงานต่าง ๆ สามารถนำไปใช้ประโยชน์ได้จริง พร้อมทั้งเชิญชวนให้มาร่วมซ้อมรับมือภัยคุกคามไซเบอร์ ซึ่งเป็นกิจกรรมที่ไทยเซิร์ตทำมาอย่างต่อเนื่อง โดยได้สรุปสาระสำคัญของ

การพูดคุยในวันนี้ใน 3 ประเด็นคือ ความสำคัญของการแชร์ข้อมูลระหว่างกัน (Information Sharing) การสร้างความไว้เนื้อเชื่อใจกัน (Trust) ในการแชร์ข้อมูล และการสร้างเครือข่ายความร่วมมือ (Human Networking) อย่างเช่น เวที Open Forum วันนี้ ก็เป็นอีกความร่วมมือหนึ่ง

ทาง ETDA Open Forum ขอขอบคุณผู้เข้าร่วมพูดคุยครั้งนี้ โดยหัวข้อการพูดคุยครั้งต่อไปจะเป็นประเด็นใด สามารถติดตามรายละเอียดได้ที่ www.etda.or.th และ http://ictlawcenter.etda.or.th