ข่าวประชาสัมพันธ์
ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์
โทรศัพท์ ๐-๒๖๑๘-๒๓๒๓ ต่อ ๑๐๑๔-๑๐๑๕
E-mail : webmaster@prd.go.th

การสัมมนาแลกเปลี่ยนประสบการณ์ด้านความมั่นคงทางไซเบอร์
ระหว่าง สำนักงาน กสทช. ร่วมกับสถานเอกอัครราชทูตไทย ณ กรุงเทลอาวีฟ ประเทศอิสราเอล

๑๙/๒๕๕๙

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) โดยสำนักงานส่งเสริมการแข่งขันและกำกับดูแลกันเอง ร่วมกับสถานเอกอัครราชทูตไทย ณ กรุงเทลอาวีฟ ประเทศอิสราเอล จัดการสัมมนาแลกเปลี่ยนประสบการณ์ด้านความมั่นคงทางไซเบอร์ หัวข้อ ความมั่นคงปลอดภัยในกิจการกระจายเสียงและโทรทัศน์บนโลกอินเทอร์เน็ต โดย ผศ.ดร.ธวัชชัย จิตรภาษ์นันท์ กรรมการ กสทช. เป็นประธานกล่าวต้อนรับคณะและผู้เข้าร่วมการสัมมนา มีพลจัตวา Moshe Markvitz และคณะอดีตเจ้าหน้าที่ทางทหารของอิสราเอลที่มีประสบการณ์ติดต่อสื่อสารด้านข่าวกรองเพื่อคุ้มครองทางไซเบอร์ของอิสราเอล เป็นผู้บรรยาย นายอภินันท์ จันทรังษี อธิบดีกรมประชาสัมพันธ์ มอบหมายให้ นายนรกิจ ศรัทธา ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์และเจ้าหน้าที่ ศสช. เข้าร่วมการสัมมนาครั้งนี้ เมื่อวันที่ ๑๗ กุมภาพันธ์ ๒๕๕๙ ณ หอประชุม ชั้น ๒ อาคารหอประชุม สำนักงาน กสทช.

การสัมมนาครั้งนี้ บรรยายเกี่ยวกับสถานภาพและกลยุทธ์การป้องกันความมั่นคงปลอดภัยเกี่ยวกับโลกไซเบอร์ในปัจจุบัน ให้ความรู้เรื่องของการเข้าโจมตีในระบบต่างๆ ระบบการกระจายเสียง การป้องกันการโจมตีเครือข่ายของรัฐบาล ป้องกันการโจมตีระบบการเงิน การป้องกันการบุกรุกและการกระทำความผิดในโลกไซเบอร์ทางด้านกฎหมาย ในปัจจุบันประเทศอิสราเอลมีการพัฒนาโลกไซเบอร์อย่างเข้มแข็ง จึงได้นำผู้เชี่ยวชาญจากอิสราเอลมาร่วมให้แนวทางกับผู้บริหารสำนักงานรัฐบาลอิเล็กทรอนิกส์ EGA ผู้บริหารสำนักงาน กสทช. และกระทรวงการต่างประเทศ เป็นโครงการความร่วมมือระหว่างประเทศไทยและประเทศอิสราเอล ในการสนับสนุนนโยบายรัฐบาล รวมถึงกระทรวงเทคโนโลยีสารสนเทศเทศและการสื่อสารในการสร้างยุทธศาสตร์ชาติเพื่อเข้าสู่ประชาคมอาเซียน ต้องมีความพร้อมทางด้านกายภาพและสารสนเทศ จะได้นำความสำเร็จของประเทศอิสราเอลในการพัฒนาด้านไซเบอร์ที่มีประสบการณ์กว่า ๕๐ ปี ประเทศอิสราเอลและประเทศไทยจะได้ช่วยกันทำงานด้านความปลอดภัยทางไซเบอร์ ปัญหาการโดนโจมตีทางไซเบอร์มีกระจายอยู่ทั่วโลก

เป็นปัญหาซับซ้อน มีการโจมตีโครงสร้างพื้นฐานเกี่ยวกับ น้ำ ไฟฟ้า การคมนาคมขนส่ง การโจมตีทางไซเบอร์ใช้ต้นทุนต่ำ เพราะใช้แฮกเกอร์ เพียง ๑๐ คน สามารถโจมตีให้ระบบไซเบอร์เสียหายได้ทั้งประเทศ โลกมีการเปลี่ยนแปลง ความสามารถการโจมตีไม่ต้องมีการสู้รบแบบเดิม แต่สามารถโจมตีทางไซเบอร์จากพิกัดต่างๆได้จากทั่วโลก โดยไม่ทราบที่มาของผู้โจมตี ซึ่งกระทบความมั่นคงของทุกประเทศ ทางสหรัฐอเมริกามีการถูกโจมตีในโลกไซเบอร์ และต่างชาติได้นำเอาแบบเครื่องบินรบมาสร้างเลียนแบบโดยไม่ต้องเสียค่าใช้จ่ายในเรื่องของการพัฒนา เกิดการล้วงความลับของรัฐบาลและเกิดความเสียหาย

การถูกโจมตีในโลกไซเบอร์ มีหลายรูปแบบ การก่อการร้าย ยาเสพติด การตัดระบบติดต่อสื่อสารระหว่างประชาชนและรัฐบาลของประเทศนั้น การโจมตีผ่านไซเบอร์ ใช้ระบบ DOS เข้าขวางการติดต่อสื่อสารระหว่างรัฐบาล ทำให้การโทรคมนาคมไม่สามารถส่งข้อมูลไปสู่ประชาชนได้ การโจมตีโลกไซเบอร์ไปรบกวนการส่งโดรน การติดต่อผ่านดาวเทียม พลังงานจากดาวเทียมค่อนข้างต่ำ การขัดขวางข้อมูลจากดาวเทียมจึงทำได้ง่าย บล็อกจากอัพลิงค์ การโจมตีทาง E-Commerce ผ่านทางการทำธุรกรรมดิจิทัล ผู้โจมตีสามารถใช้เป็นช่องทางเข้าสู่ระบบและโจรกรรมทางการเงิน สร้างความเสียหายให้กับระบบการเงิน แต่ธนาคารไม่แจ้งปัญหาที่เกิดเพราะธนาคารมีการทำประกันกับบริษัทประกันไว้

ปัจจุบันคนร้ายสามารถดึงหมายเลขโทรศัพท์ของประชาชน เพื่อใช้เข้าถึงบัญชีธนาคาร รู้ข้อมูลของผู้ใช้โทรศัพท์ได้ทุกคน รู้ความเคลื่อนไหวตลอดเวลา เพราะมีซอฟต์แวร์ที่สามารถดึงข้อมูลจากโซเชียลเน็ตเวิร์ค ทำให้รู้รายละเอียดของประชาชนได้ทุกข้อมูล เวลาซื้ออุปกรณ์ฮาร์ดแวร์ที่มีซอฟต์แวร์ฟรีมาด้วย ผู้ใช้บริการต้องเข้ารหัสเพื่อป้องกันไม่ให้เกิดอาชญากรรมได้ ปัจจุบันการย้ายข้อมูลเข้าระบบคลาวด์ หากคลาวด์ถูกโจมตี ข้อมูลที่คลาวด์จะไม่เหลือ ควรมีการทำระบบสำรองข้อมูลเสมอ หากไม่มีจะกู้คืนยาก ระบบจะต้องแจ้งเตือนทันทีจะต้องมีการฝึกฝนอบรมเจ้าหน้าที่ไอทีให้เกิดความชำนาญ เพื่อป้องกันจากภัยคุกคาม

พลจัตวา Moshe Markvitz กล่าวถึง กฎหมายเพื่อควบคุมอาชญากรรมด้านคอมพิวเตอร์สร้างความปลอดภัยให้กับสาธารณะและส่วนบุคคล มีการแก้ไขปัญหาทางด้านเทคนิคและกฎหมาย ต้องป้องกันไม่ให้เด็กและเยาวชนเข้าสู่สื่อลามกอนาจาร การล่วงละเมิดต่อเด็ก สิทธิส่วนตัว การโจมตีรัฐบาล เช่น ประเทศสิงค์โปร์ กฎหมาย มาตรา ๔๔ เมื่อปี ๒๐๑๒ สิทธิของบุคคลการคุ้มครองข้อมูลส่วนบุคคลเป็นไปอย่างเหมาะสม สหรัฐอเมริกา มีกฎหมาย cybersecurity act of 2015 เป็นเครื่องมือที่รัฐบาลและเอกชนแลกเปลี่ยนแบ่งปันข้อมูลเมื่อถูกโจมตีทางอินเตอร์เน็ต

เจ้าหน้าที่ของรัฐบาลอิสราเอล กล่าวถึง รูปแบบการหลอกลวงเมื่อประชาชนใช้โซเชียลมีเดีย ได้แก่ Executive Impersonations การหลอกลวงว่าสามารถประสานกับบุคคลสำคัญและเปิดเผยข้อมูล Account Takeover ให้ดาวโหลดส่งชื่อ ข้อมูล และทำการฉ้อโกง Customer scams ใช้คูปอง ซื้อสินค้าราคาถูกแต่เป็นคูปองปลอม มีการให้บาร์โค๊ต และ ข้อมูล สมาร์ทโฟน และทำการแฮกทีหลัง Information Leakage ข้อมูลในโซเชียลมีเดียต่างๆ อาจรั่วไหลจากบุคคลข้างเคียง เช่น ทหารถ่ายรูปการรบและส่งเข้าโซเชียลมีเดีย ทำให้ฝ่ายตรงข้ามทราบข้อมูล An Attack การให้คนในองค์กร ช่วยโจมตีระบบ ใช้โซเชียลมีเดียแทนการใช้อีเมล์