ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

น.ท.มนตรี ชลอปัญจศิลป์
หมายเลข ๔๔ สัมมนาที่ ๗

๑. บทนำ

ปัจจุบันความก้าวหน้าทางเทคโนโลยีด้านไซเบอร์ถูกนำมาใช้ประโยชน์ ในการทำธุรกรรมหรือการติดต่อสื่อสารจึงก่อให้เกิดสภาพแวดล้อมที่เอื้ออำนวยต่อภัยคุกคามและการก่ออาชญากรรมทางไซเบอร์ที่สามารถส่งผลกระทบในวงกว้างได้อย่างรวดเร็วและปัจจุบันยิ่งทวีความรุนแรงมากขึ้นสร้างความเสียหายทั้งในระดับบุคคล และ ระดับประเทศ การป้องกันหรือรับมือกับภัยคุกคามหรือความเสี่ยงทางไซเบอร์ จึงต้องอาศัยความรวดเร็วและการประสานงานกับทุกหน่วยงานที่เกี่ยวข้อง เพื่อป้องกันและรับมือได้ทันสถานการณ์และมีการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างต่อเนื่อง ดังนั้น หน่วยงานหรือผู้ใช้งาน ในระบบเครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือ ระบบที่เกี่ยวข้องกับด้านไซเบอร์ ต้องทราบถึงภัยคุกคามทางไซเบอร์ และ แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อจะได้ปฏิบัติในการป้องกันรักษาความปลอดภัยทางไซเบอร์ได้อย่างถูกต้อง

๒. คำจำกัดความ

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยง จากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป

องค์ประกอบของความปลอดภัยของข้อมูล : CIA Triad ประกอบไปด้วย

C = “Confidentiality” หมายถึง การรักษาความลับของข้อมูลในระบบสารสนเทศ

I = “Integrity” หมายถึง ความสมบูรณ์ของข้อมูล เพื่อให้เกิดความมั่นใจว่าข้อมูลจะไม่ถูกแก้ไข หรือ เปลี่ยนแปลง โดยไม่ได้รับอนุญาต

A = “Availability” หมายถึง ความพร้อมใช้งานของระบบสารสนเทศ

๓. รูปแบบภัยคุกคามทางไซเบอร์

๓.๑ มัลแวร์ (Malware) คือความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด สูญเสียความลับทางข้อมูล สูญเสียความไม่เปลี่ยนแปลงของข้อมูล สูญเสียเสถียรภาพของระบบปฏิบัติการ

๓.๒ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยาก

๓.๓ หนอนคอมพิวเตอร์ (Computer worm) หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้โดยจะคัดลอกและกระจายตัวเองข้ามเครือข่าย เช่น ระบบเครือข่าย หรือ อินเทอร์เน็ต เป็นต้น

๓.๔ ม้าโทรจัน (Trojan horse) โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบ

๓.๕ สปายแวร์ (Spyware) ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูลสถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๓.๖ ประตูหลัง (Backdoor) รูรั่วของระบบรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ที่ผู้ออกแบบหรือผู้ดูแลระบบจงใจทิ้งไว้โดยเป็นกลไกลับทางซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคงปลอดภัย แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดี สามารถเข้ามาในระบบและก่อความเสียหายได้

๓.๗ Rootkit โปรแกรมที่ออกแบบมาเพื่อซ่อนอ็อบเจ็กต์ต่าง ๆ เช่น กระบวนงาน ไฟล์หรือข้อมูล แม้จะเป็นโปรแกรมที่อาจไม่เป็นอันตรายเสมอไป แต่ก็ถูกนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากขึ้น

๓.๘ การโจมตีแบบ DoS/DDoS ความพยายามโจมตีเพื่อทำให้เครื่องคอมพิวเตอร์ปลายทางหยุดทำงานหรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

๓.๙ Botnet ภัยคุกคามทางเครือข่ายคอมพิวเตอร์ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้น ต้องการตัวนำทางเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เอง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น

๓.๑๐ Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ antispam หรือหากใช้ฟรีอีเมล์เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว

๓.๑๑ Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตโดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

๓.๑๒ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้

๓.๑๓ ข้อมูลขยะ (Spam) ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมลหรือเรียกว่า อีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับ

๓.๑๔ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรือ อาศัยโปรแกรมแฮกหลากรูปแบบ ที่หาได้ง่ายในโลกอินเทอร์เน็ต แถมยังใช้งานได้ง่าย ไม่ต้องเป็นผู้เชี่ยวชาญในคอมพิวเตอร์ก็สามารถเจาะระบบได้

๓.๑๕ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก

๔. แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๔.๑ สำหรับหน่วยงาน

๔.๑.๑ ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

๔.๑.๒ เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

๔.๑.๓ แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงาน ให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับอีเมลแนบจากคนที่ไม่รู้จัก ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่าง ๆ หรือช่องทาง Social Network ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

๔.๑.๔ หากพบพิรุธว่าระบบถูกโจมตีเช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง ๓๐ วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

๔.๑.๕ ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า ๙๐ วัน หรือตามที่กฎหมายกำหนด

๔.๒ สำหรับผู้ใช้งานทั่วไป

๔.๒.๑ เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่าง ๆ หรือช่องทาง Social Media เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวัน มัลแวร์มาจากพวกไฟล์แนบ ทาง Social Network เพิ่มมากขึ้น

๔.๒.๒ การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

๔.๒.๓ ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อตลอดจน ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

๕. สรุป

ปัญหาเรื่องภัยคุกคามทางไซเบอร์ จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์จากผู้ไม่หวังดี ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงาน อันเกิดจากสาเหตุต่าง ๆ การมุ่งทำลายชื่อเสียง การก่อกวน หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้กลุ่มแฮคเกอร์ด้วยกันได้รับรู้ ในอนาคตการโจมตีทางไซเบอร์จะมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น เนื่องจากสามารถหาเครื่องมือในการโจมตีได้ง่ายจากอินเทอร์เน็ต ดังนั้นจึงต้องตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามมาตรการรักษาวามมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานเพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้ การติดตามสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

บรรณานุกรม

ธนัญชัย ตรีภาค. เอกสารคำสอน Network Security [ออนไลน์].สืบค้น ๑๙ พฤศจิกายน ๒๕๖๓, จาก http://www.ce.kmitl.ac.th/download.php?DOWNLOAD.

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ [ออนไลน์].สืบค้น ๑๙ พฤศจิกายน ๒๕๖๓, จาก http://www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF.

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร. องค์ความรู้การป้องกันภัยคุกความทางคอมพิวเตอร์ [ออนไลน์]. สืบค้น ๑๙ พฤศจิกายน ๒๕๖๓, จาก https://www.senate.go.th/assets/portals.