ความมั่นคงปลอดภัยทางไซเบอร์

Cyber Security

เนื่องจากปัจจุบันปัญหาเรื่องภัยคุกคามทางไซเบอร์ (Cyber Security) จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์ จากผู้ไม่หวังดีทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวง ประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงาน อันเกิดจากสาเหตุ ต่างๆ ไม่ว่าจะเป็นการต้องการแสดงพลังของกลุ่มบุคคลที่ต่อต้านนโยบายของรัฐบาล การมุ่งทำลาย ชื่อเสียง การก่อกวน หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้กลุ่มแฮคเกอร์ด้วยกันได้รับรู้ ในอนาคตการโจมตีทางไซเบอร์จะมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น เนื่องจากสามารถหาเครื่องมือในการโจมตีได้ง่ายจากอินเตอร์เน็ทและเว็บไซต์ ซึ่งจะทำให้มีแฮคเกอร์หน้าใหม่เกิดขึ้นได้ง่าย รัฐบาลจะต้องให้ความสำคัญเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) อย่างเป็นรูปธรรม โดยมีการประกาศใช้พระราชบัญญัติว่าด้วยการรักษา ความมั่นคงปลอดภัยไซเบอร์ ที่ผ่านการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และ การได้รับการยอมรับจากภาคเอกชนและภาคประชาชน แต่สิ่งที่สำคัญยิ่งกว่านั้น ประชาชน โดยเฉพาะอย่างยิ่งบุคลากรของหน่วยงานภาครัฐในทุกระดับ จะต้องตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงาน เพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้การติดตามสถานการณ์ ด้านความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อนักระทบต่อความมั่น คงของรัฐความมั่น คงทางเศรษฐกิจความมั่น คงทางทหาร และความสงบ เรียบร้อยภายในประเทศ “ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำ หรือการดำเนินการใดๆ โดยมิชอบโดยใช้ คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้ เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวของและเป็นภัยอันตราย ที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ประเภทของภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคาม	คำอธิบาย
1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)
2. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
3. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
4. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
5. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

6. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสำธารณะ (CVE-Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
7. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
8. โปรแกรมไม่พึงประสงค์ (Malicious Code)	ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสำมารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ
9. ภัยคุกคามอื่นๆ นอกเหนือจากที่กาหนดไว้ข้างต้น (Other)	ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สำมารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้ำจำนวนภัยคุกคามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงกำรจัดแบ่งประเภทภัยคุกคามนี้ใหม่

การแบ่งประเภทภัยคุกคามทางไซเบอร์

ประเภทภัยคุกคาม	คำอธิบาย
1. Application/Service/ OS configuration problem	เหตุการณ์ที่เกิดจากการ Configuration แอปพลิเคชัน/การให้บริการ/ระบบปฏิบัติการ ที่ผิดพลาด
2. Denial of Service (DoS)	เหตุการณ์ที่ผู้บุกรุกส่งข้อมูล และ packet จำนวนมากไปยังเครือข่ายหรือเครื่องของหน่วยงาน เพื่อให้เครื่องให้บริการหยุดชะงัก

3. Fraud	เหตุการณ์ที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
4. Information Gathering	เหตุการณ์ที่ตรวจพบความพยายามของผู้บุกรุกในการค้นหาข้อมูลสำคัญเพื่อใช้สำหรับการโจมตีเข้าสู่ระบบ
5. Information Leak	เหตุการณ์ที่ตรวจพบการรั่วไหลของข้อมูลสำคัญจากช่องทางต่างๆ เช่น Social Media ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัย
6. Malware Detected	การบุกรุกที่เกิดจากการโจมตีของมัลแวร์ไปยังเครือข่าย และเครื่องให้บริการของหน่วยงาน ได้แก่ Backdoor, Trojan, Virus, Worm และ Botnet
7. Server Compromise	เหตุการณ์ที่ตรวจพบว่าเครื่องให้บริการ (Server) ของหน่วยงานถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต โดยผู้บุกรกเป็นที่เรียบร้อย
8. Service Unavaliable	การทำให้บริการมีปัญหาหรือเกิดเหตุขัดข้อง จนไม่สามารถให้บริการได้
9. Suspicious Activity	การเชื่อมต่อข้อมูล และ Traffic ที่ผิดปรกติ และมีความเชื่อมโยงที่จะเป็นการบุกรุกระบบ
10. Web Compromise	Web Application หรือเว็บไซต์ ถูกยึดครองโดยไม่ได้รับอนุญาต

ที่มา: ส่วนความมั่นคงปลอดภัยสารสนเทศ ฝ่ายวิศวกรรมและปฏิบัติการ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับบุคคลและหน่วยงาน

- **สำหรับบุคคล**
  - ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าไปยังเว็บไซต์ที่ไม่เหมาะสม ไม่เปิดไฟล์ที่ไม่มีการตรวจสอบแน่ชัดหรือเปิดไฟล์จาก บุคคลที่ไม่รู้จัก และระมัดระวังการเปิดไฟล์ผ่าน Social Media ทั้งนี้เพื่อหลีกเลี่ยงพวกมัลแวร์
  - ไม่ใช้รหัสผ่านบน โลก cyber เป็นรหัสชุดเดียวกันทุกระบบ
  - ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ข้อมูลต่อเพื่อป้องกันตนเองเป็นต้นตอ ต่อการส่งแพร่กระจายไวรัส

- **สำหรับหน่วยงาน**
    - ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นในการเข้าถึงระบบและข้อมูล
    - เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบป้องกันการโจมตีของ ไวรัส Web Application Firewall หรือ DDos Protection
    - แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้อินเตอร์เน็ต โดยหลีกเลี่ยงความเหมาะสม ป้องกัน ข้อความจาก Social Media
    - หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้หรือมีความล่าช้าปกติ ควรตรวจสอบ Log การ login ย้อนหลังทุกๆ เดือน
    - ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ต่างๆตามที่กฎหมายกำหนดไว้

ในการแก้ไขหรือป้องกันทางการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับบุคคลและหน่วยงาน ผู้บริหารต้องมีส่วนร่วมในการรับทราบและให้แนวทางในการแก้ปัญหาที่ให้ถูกต้อง เพื่อให้สร้างความมั่นคงให้ทางไซเบอร์และให้ผู้ใช้จำเป็นต้องมีความรู้และความเข้าใจในปัญหาจากการคุกคามว่าเกิดขึ้นได้อย่างไรต้นตอเกิดจากอะไร เพราะไม่ว่าจะมีระบบป้องกันที่ดีขนาดไหนหาก เกิดช่องโหว่ในระบบก็สามารถถูกแฮกเกอร์เจาะเข้าระบบได้เช่นกัน ผู้ใช้งานทุกคนควรมีความระมัดระวังในการใช้งานระบบ ไซเบอร์ เพื่อให้ทุกคนมีความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยและควรมีไหวพริบในขณะที่กำลังเจอกับปัญหา ถือเป็นการรู้จักป้องกันการก่อให้เกิดปัญหาทางความมั่นคงทางไซเบอร์อีกด้วยเพื่อป้องกันการเกิดเหตุการณ์ที่ไม่คาดคิดที่จะเกิดขึ้นได้ตลอดเวลา.