สรุปบทเรียนจากการพัฒนาความรู้

รอบการประเมินที่ 1 : ปีงบประมาณ พ.ศ. 2569

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

จัดทำโดย นางเกษร ชั่งเหลือ
ตำแหน่ง บรรณารักษ์ชำนาญการ

การรักษาความมั่นคงปลอดภัยบนอินเทอร์เน็ตสำหรับข้าราชการยุคดิจิทัลมุ่งเน้นการปกป้องข้อมูลของทางราชการ และข้อมูลส่วนบุคคลจากภัยคุกคามทางไซเบอร์ ซึ่งข้าราชการในยุคดิจิทัลควรมีความรู้ความเข้าใจเกี่ยวกับการใช้อินเตอร์เน็ต การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวังเพื่อให้ปลอดภัยจากภัยคุกคามและสร้างความน่าเชื่อถือให้กับองค์กรภาครัฐอย่างมีประสิทธิภาพ

1. ประเภทการกระทำความผิดทางคอมพิวเตอร์

การกระทำใด ๆ ที่มุ่งร้ายผ่านระบบเครือข่ายคอมพิวเตอร์สร้างความเสียหายต่อข้อมูลส่วนบุคคลและองค์กรอย่างมาก โดยมีประเภทของการกระทำความผิดที่เป็นภัยคุกคามทางอินเทอร์เน็ต ดังนี้

1.1 แฮกเกอร์ (Hacker) บุคคลที่มีความสนใจศึกษาเรื่องระบบปฏิบัติการคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์แล้วเผยแพร่ข้อมูลสิ่งที่ได้ค้นพบพร้อมกับทำการแจ้งเตือนไปยังระบบที่พบช่องโหว่ให้ดำเนินการแก้ไขปรับปรุง ทั้งนี้ จะมีเพียงแฮกเกอร์บางคนเท่านั้นที่นำไปกระทำการประสงค์ร้ายเพื่อทำลายระบบ

1.2 แคร็กเกอร์ (Cracker) บุคคลที่มีความสนใจศึกษาหรือนำความรู้มากระทำความผิดให้เกิดความเสียหายโดยการโจมตีเจาะระบบทำให้ระบบคอมพิวเตอร์เกิดความเสียหายเพื่อแสวงหาผลประโยชน์

1.3 สคริปต์คิดดี้ (Script Kiddy) บุคคลที่มีความอยากรู้อยากเห็น และชอบทดลองโปรแกรมสำเร็จรูปโดยการใช้เครื่องมือสคริปต์โจมตีทำให้ระบบเกิดความเสียหายส่วนใหญ่ทำเพื่อความอยากรู้อยากเห็นสนุกเพื่อก่อกวน

1.4 สปาย (Spy) บุคคลที่แอบเข้ามาในระบบคอมพิวเตอร์เพื่อล้วงข้อมูลความลับจากฝ่ายตรงข้าม เช่น ข้อมูลทางการทหาร ข้อมูลเชิงธุรกิจ ประโยชน์ด้านข่าวกรอง การลงทุน สายลับ จารชน หรือผู้สอดแนม

1.5 เอ็มพลอยอี (Employee) บุคคลในองค์กรที่สามารถเข้าระบบได้ และไม่ปฏิบัติตามกฎระเบียบขององค์กรโดยการนำเอาข้อมูลความลับขององค์กรไปเผยแพร่ เช่น ระบบการรักษาความปลอดภัยขององค์กร ซึ่งจะก่อให้เกิดความเสียหายต่อองค์กรอย่างรุนแรงได้

1.6 ผู้ก่อการร้าย (Terrorist) กลุ่มผู้ก่อการร้ายที่ก่อความไม่สงบด้านคอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต เป้าหมายเพื่อทำลายความเชื่อมั่น สร้างความเสียหายทางเศรษฐกิจ และส่งผลกระทบต่อความมั่นคงของประเทศ โดยกระทำการโจมตีระบบเว็บไซต์ภาครัฐ ระบบการเงินออนไลน์ เจาะระบบความลับเปิดเผยข้อมูลสำคัญ เรียกค่าไถ่ ปรับเปลี่ยนหน้าเว็บไซต์โจมตีทางจิตวิทยา ทำลายระบบสารสนเทศ

2. รูปแบบการกระทำความผิดทางคอมพิวเตอร์

การกระทำความผิดทางคอมพิวเตอร์มีรูปแบบหลัก ๆ ที่ส่งผลกระทบต่อสังคม ดังนี้

2.1 Social Engineering จิตวิทยาหลอกหล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ ทำให้ผู้ได้รับข้อมูลข่าวสารหลงเชื่อเปิดเผยข้อมูลสำคัญ หรือเสียทรัพย์สิน

2.2 Denial of Service (Dos) ส่งคำสั่งลวงขอใช้ระบบคราวละมาก ๆ เพื่อให้ระบบประมวลผลไม่ทันหยุดให้บริการส่งผลกระทบต่อการใช้งานของผู้อื่น

2.3 Decryption การถอดรหัส การเข้าถึงข้อมูลลับที่มีการเข้ารหัสอยู่ เพื่อล้วงความลับข้อมูลที่แท้จริง

2.4 Birthday Attacks การโจมตีที่อาศัยหลักความน่าจะเป็นข้อมูลวันเดือนปีเกิดตั้งรหัสไว้ในการหาข้อมูลสำคัญหรือเพื่อปลอมแปลงลายเซ็นดิจิทัล

2.5 Man in the Middle Attacks เป็นคนกลางดักฟัง ขโมย เปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

3. การกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 เจตนารมณ์เพื่อป้องกันและปราบปราม การกระทำด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่ง ที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูล ของบุคคลอื่นในระบบคอมพิวเตอร์ โดยมิชอบ หรือใช้ระบบคอมพิวเตอร์ เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จ หรือมีลักษณะลามกอนาจาร ดังนั้น การใช้เทคโนโลยีควรศึกษาและปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

4. การป้องกันภัยคุกคามทางอินเทอร์เน็ต

4.1 ปฏิบัติตามเจตนารมณ์ของ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และกฎหมายอื่น ๆ ที่เกี่ยวข้อง เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562, พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

4.2 ตั้งรหัสผ่านให้ปลอดภัยคาดเดาได้ง่าย เช่น เลขเรียงตามลำดับ, วันเกิด, หมายเลขโทรศัพท์

4.3 ควรมีการ Update Version ของBrowser อย่างสม่ำเสมอ ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น

4.4 ควรระมัดระวังเปิดเผยข้อมูลส่วนบุคคล เผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือใส่ร้ายผู้อื่น

4.5 ระวังโปรแกรมที่แปลกปลอมแสดงขึ้นมาพร้อมการเปิดเครื่องหรือกำลังใช้งาน

4.6 ระบบการให้บริการธุรกรรมอิเล็กทรอนิกส์จะต้องมีการสร้างรหัสการเข้าข้อมูล และใบรับรองทางอิเล็กทรอนิกส์และซอฟต์แวร์อยู่เสมอ หลังจากเสร็จสิ้นแล้วให้ล็อกเอาท์ออกจากระบบทันทีทุกครั้ง

4.7 ไม่เปิด E-mail หรือเว็บไซต์ที่น่าสงสัยผู้ส่งไม่ชัดเจนเว็บไซต์ที่เสี่ยง เช่น เว็บการพนัน เว็บลามก

4.8 ระวังการแชร์ข้อมูลส่วนตัว และไม่คลิกลิงก์ที่ไม่รู้จัก

5. ข้อสรุปและแนวคิดในการประยุกต์ใช้เพื่อพัฒนาองค์การ

สรุป การถูกโจมตีทางระบบเครือข่ายนับว่าเป็นภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อเศรษฐกิจ สังคมอย่างรุนแรง ผู้ตกเป็นเหยื่อมักพบได้จากหลายสาเหตุ เช่น เว็บไซต์หลอกลวง ถูกหลอกซื้อของออนไลน์ หรือเกิดจากตัวของเราเองโดยการโพสต์ข้อมูลที่ไม่เหมาะสม ดังนั้นควรใช้เทคโนโลยีอย่างระมัดระวัง มีสติ การปฏิบัติตนตามแนวทางหลักการใช้เทคโนโลยีเพื่อให้รู้เท่าทันภัยคุกคามทางไซเบอร์อย่างปลอดภัย นับว่าเป็นเกราะป้องกันที่ดีที่สุดในการถูกโจรกรรมข้อมูล การถูกหลอกลวงทางออนไลน์ และช่วยให้ข้าราชการยุคดิจิทัลปฏิบัติงานได้อย่างมีประสิทธิภาพ ปลอดภัย และสร้างความน่าเชื่อถือให้กับองค์การได้

โดยมีแนวคิดในเพื่อพัฒนาองค์การให้มีความมั่นคงปลอดภัยบนอินเทอร์เน็ตยุคดิจิทัล ดังนี้

1. ให้ความร่วมมือตามนโยบาย คำสั่ง และแผนว่าด้วยการรักษาตวามมั่นคงปลอดภัยไซเบอร์ขององค์กร
2. กำหนดหลักเกณฑ์การใช้เครื่องคอมพิวเตอร์ และการใช้งานอินเทอร์เน็ตสำหรับผู้ขอรับบริการห้องสมุดเพื่อควบคุมป้องกันภัยให้องค์การมีความมั่นคงปลอดภัยบนอินเทอร์เน็ตยุคดิจิทัล
3. ให้บริการเผยแพร่ข้อมูลด้วยความระมัดระวัง ไม่ทำให้องค์กรเสื่อมเสีย ปฏิบัติตามกฎหมายที่เกี่ยวข้อง
4. มีความตระหนักรู้ในการใช้เทคโนโลยี พัฒนาตนเอง เผยแพร่ความรู้ด้านความมั่นคงปลอดภัยบนอินเทอร์เน็ตยุคดิจิทัล

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
ด้านการพัฒนา : ☑ **ทักษะด้านดิจิทัล**
บรรยายโดย : อาจารย์ณัฐ พยงค์ศรี ตำแหน่ง นักวิชาการคอมพิวเตอร์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม พนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม
หน่วยงานผู้รับผิดชอบ : สำนักงานคณะกรรมการข้าราชการพลเรือน (สำนักงาน ก.พ.)
วิธีการพัฒนาตนเอง : เรียนรู้ด้วยตนเองผ่านสื่ออิเล็กทรอนิกส์ (e-Learning) สำนักงาน
วันที่ได้รับการฝึกอบรม : วันที่ 10 กุมภาพันธ์ 2569 **สถานที่ :** https://learningportal.ocsc.go.th/login/