รอบ1
ปีงบประมาณ
พ.ศ.2567

สรุปบทเรียนจากการพัฒนาความรู้

หลักสูตร ความมั่นคงปลอดภัยบนอินเทอร์เน็ต และการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

จัดทำโดย นายภูวดล แสงทอง

แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย

ปริมาณผู้ใช้งานอินเทอร์เน็ตมีแนวโน้มการใช้งานสูงขึ้น ถึงกว่า ๙ เท่า แบบก้าวกระโดด การใช้งานอินเทอร์เน็ตสามารถเข้าถึงได้เกือบ ๕๐% ของประชากรทั่วโลกทำให้อินเทอร์เน็ตนั้นค่อนข้างมีบทบาทสำคัญต่อการดำเนินชีวิตประจำวัน

ปัจจุบันแนวโน้มการใช้งานอินเทอร์เน็ตจะเป็นในรูปแบบที่เรียกว่าสื่อสังคมออนไลน์หรือ Social Media ทุกคนมีโอกาสร่วมกันสร้างสรรค์อินเทอร์เน็ตทำให้เกิดการใช้งานในรูปแบบต่าง ๆ จากปัจจัยเบื้องต้นเมื่ออินเทอร์เน็ตเป็นส่วนหนึ่งของชีวิตย่อมมีผลกระทบทั้งด้านดีและไม่ดี ผู้ไม่ประสงค์ดีหรืออาชญากรมีแนวโน้มที่จะเปลี่ยนแปลงรูปแบบให้เข้ากับสถานการณ์ หรือการใช้งานอินเทอร์เน็ตที่เป็นปัจจุบันนั่นหมายถึงสิ่งที่เกิดขึ้นกับโลกปัจจุบันที่ไม่ได้เกิดขึ้นบนอินเทอร์เน็ตมีแนวโน้มที่จะเปลี่ยนรูปแบบให้มาเกิดขึ้นบนอินเทอร์เน็ต

สถิติการใช้งานของประเทศไทย

สังคมไทยผู้ที่มีอายุระหว่าง ๒๐-๓๐ ปี เป็นกลุ่มที่ใช้งานอินเทอร์เน็ตสูง จากสถิติหลายช่วงปีที่ผ่านมามีปริมาณเกือบ ๖๐-๗๐ เปอร์เซ็นต์ ดังนั้นคนกลุ่มนี้มีโอกาสมีความเสี่ยงที่จะเผชิญโลกของอาชญากรรมค่อนข้างสูง รวมทั้งกลุ่มผู้สูงวัยหรือวัยหลังเกษียณที่เพิ่งเริ่มต้นการใช้งาน โดยประชาชนคนไทยส่วนมากใช้อินเทอร์เน็ตในช่วงเวลางาน

ความสัมพันธ์และการกระจายตัวของข้อมูลในโลกอินเทอร์เน็ต

ประเด็นหนึ่งที่ต้องคำนึงถึงในการใช้งานอินเทอร์เน็ตอย่างถูกวิธี คือ เรื่องของการเชื่อมโยงและการกระจายตัวของข้อมูล ในอดีตการใช้งานอินเทอร์เน็ตเป็นแบบที่ผู้ใช้เข้าไปในเว็บไซต์ที่สนใจเพื่ออ่านข้อมูลแต่เพียงอย่างเดียว แต่ปัจจุบันเป็นโลกของ Social Media ที่ผู้ใช้งานอินเทอร์เน็ตมีบทบาทเป็นผู้สร้างข้อมูลด้วย ส่งผลให้ข้อมูลเดิม ๆ ถูกวนซ้ำจนทำให้หลงเชื่อและตกเป็นเหยื่อได้ เช่น การหลอกรับบริจาคเงิน ที่ผู้ไม่หวังดีจะลงข่าวเก่าเพื่อขอรับเงินบริจาค นอกจากนี้การกระจายตัวของข้อมูลยังเป็นไปได้อย่างรวดเร็วและรุนแรง เพียงกด Like หรือ Share ก็สามารถกระจายข้อมูลให้คนอื่น ๆ ได้มากมาย ซึ่งนอกจากจะทำให้ข้อมูลข่าวสารกระจายตัวได้อย่างรวดเร็วแล้ว ยังส่งผลให้ Virus หรือข้อมูลที่ไม่เหมาะสมสามารถกระจายตัวได้อย่างรวดเร็วด้วยเช่นกัน

การเปลี่ยนแปลงพฤติกรรมของผู้บริโภคก็มีส่วนสำคัญต่อการใช้งานอินเทอร์เน็ต มีผู้ที่ทำงานผ่านระบบออนไลน์มากขึ้น เช่น การทำงานเอกสารแบบออนไลน์ซึ่งสามารถใช้งานร่วมกันหลายคนได้ พฤติกรรมการใช้จ่ายก็เปลี่ยนจากการใช้เงินสดเป็นบัตรเดบิต บัตรเครดิต รวมถึงสกุลเงินดิจิทัลมากขึ้น การใช้งาน PC ลดลง โดยมีการใช้งาน Smart Phone กันมากขึ้น ส่วนเว็บไซต์ต่าง ๆ ก็ปรับเปลี่ยนจากรูปแบบ Static Web เป็น Social Media วิธีการการสื่อสารก็ขยายจากเพียงการใช้ข้อความหรือเสียง กลายเป็นวิดีโอ หรือ Live Streaming ทุกคนสามารถเป็นสื่อได้ กลายเป็นการตลาดรูปแบบใหม่ สรุปคือการทำงานต่าง ๆ มีแนวโน้มเปลี่ยนแปลงเป็นรูปแบบดิจิทัลมากขึ้น

วิวัฒนาการของเว็บไซต์

ยุคของอินเทอร์เน็ต สามารถแบ่งออกได้เป็น 4 ยุค ได้แก่

1. เว็บ 1.0 (One Way Communication) เป็นการสื่อสารทางเดียว ใช้เผยแพร่เนื้อหาที่ผู้สร้างจัดทำขึ้นเพียงอย่างเดียว

2. เว็บ 2.0 (Two Way Communication) เป็นการสื่อสารสองทาง ผู้เข้าเว็บไซต์สามารถโต้ตอบกับบุคคลอื่น ๆ ได้ เช่น เว็บบอร์ด , Social Media

3. เว็บ 3.0 มีการพัฒนามากขึ้นจนทำให้แพลตฟอร์มสามารถวิเคราะห์ข้อมูลและให้คำแนะนำแก่ผู้ใช้งานได้ เช่น การเดาคำค้นของ Google การแสดงข้อมูลตามลำดับความสำคัญที่คาดว่าผู้ค้นต้องการในขณะนั้น การแนะนำเพื่อนที่ผู้ใช้อาจรู้จักของ Facebook เป็นต้น

4. เว็บ 4.0 แพลตฟอร์มมีความสามารถในการเรียนรู้พฤติกรรมของมนุษย์ผ่านประวัติการอ่าน สืบค้น และโต้ตอบบนโลกออนไลน์ และสามารถให้คำแนะนำที่ดียิ่งขึ้นไปกว่าเว็บ 3.0

ประเภทของผู้ที่กระทำความผิดทางคอมพิวเตอร์

๑. Hacker คือ คนที่มีความสนใจในระบบคอมพิวเตอร์ในเชิงลึก พยายามเจาะเข้าระบบคอมพิวเตอร์เพื่อหาจุดอ่อนของระบบ โดยมักจะแจ้งให้เจ้าของระบบทราบเพื่อปิดจุดอ่อนและมีการแบ่งปันข้อมูลให้แก่กัน

๒. Cracker คือ Hacker ที่นำความรู้ที่มีมาใช้ในเชิงทำลายเพื่อสร้างความเสียหายแก่ระบบ

๓. Script kiddy คือ บุคคลที่ยังไม่ค่อยมีความชานาญในการแฮกมากนัก ไม่สามารถเขียนโปรแกรมในการเจาะระบบได้เอง ส่วนใหญ่เป็นมือใหม่ที่อยากทดลองเป็นแฮกเกอร์

๔. Spy คือ บุคคลที่ถูกจ้างเพื่อเจาะระบบและขโมยข้อมูล

๕. Employee คือ พนักงานในองค์กรที่นำความลับขององค์การไปเผยแพร่โดยไม่เจตนา แล้วทำให้ระบบขององค์กรถูกโจมตี

๖. Terrorist บุคคลที่ก่อความไม่สงบบนเว็บไซต์หรือเครือข่ายอินเทอร์เน็ต ทำให้ไม่สามารถใช้งานได้

รูปแบบของการกระทำความผิด

๑. Social Engineering คือ ปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญ เกี่ยวกับคอมพิวเตอร์ เช่น ส่งอีเมล์หลอกลวงให้โอนเงิน

๒. Password Guessing คือ การเดา Password เพื่อเข้าสู่ระบบ

๓. Denial of Service คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

๔. Decryption คือ การถอดรหัสข้อมูล

๕. Birthday Attacks คือ การสุ่มคีย์ขึ้นมา และตรงกับที่กำหนดไว้

๖. Man In the Middle attacks คือ การพยายามที่จะทำตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

วิธีการโจมตีบนเครือข่ายอินเทอร์เน็ต

๑. ส่ง malware และ virus ให้แพร่กระจายผ่าน Social Media

๒. Zombie Attack เป็นการส่ง Malware ไปยังเครื่องคอมพิวเตอร์จำนวนมากเพื่อสั่งให้โจมตีเป้าหมายอีกทีหนึ่ง การโจมตีลักษณะนี้เป็นวิธีที่รับมือได้ยากเนื่องจากเป็นการโจมตีจำนวนมากจากบุคคลที่สามซึ่งไม่มีส่วนเกี่ยวข้อง

๓. กลลวงทางสังคม (Social Engineering) คือ การล่อหลอกหรือใช้วิธีอื่นใดเพื่อให้ได้รหัสผ่านเพื่อเข้าสู่ระบบโดยที่ไม่จำเป็นต้องใช้ความรู้หรือเทคนิคทางคอมพิวเตอร์

๔. Phishing เป็นการปลอมแปลมเว็บไซต์ขององค์กรอื่นให้เหยื่อเข้าใจว่าเป็นเว็บไซต์จริงเพื่อดักจับรหัสผ่าน หรือเพื่อติดตั้ง Malware หรือ Virus

๕. การละเมิดข้อมูลส่วนบุคคล จากข้อมูลของผู้ใช้ใน Social Media ต่าง ๆ เช่น รายชื่อเพื่อน ที่อยู่ปัจจุบัน พฤติกรรมการใช้ชีวิต

๖. ใช้ Search Engine Optimizer (SEO) เพื่อปั่นข้อมูลทำให้เข้าใจผิดเกี่ยวกับความนิยมของเรื่องต่าง ๆ

รูปแบบการกระทำผิดทางอินเทอร์เน็ต

๑. Social Engineering คือ ปฏิบัติการทางจิตวิทยาหลอกล่อให้เหยื่อติดกับโดยไม่ต้องอาศัยความชำนาญเกี่ยวกับคอมพิวเตอร์ เช่น ส่งอีเมล์หลอกลวงให้โอนเงิน

๒. Denial of Service คือ การโจมตีลักษณะหนึ่งที่อาศัยการส่งคำสั่งลวงไปร้องขอการใช้งานจากระบบและร้องขอในคราวละมาก ๆ เพื่อที่จะทำให้ระบบหยุดการให้บริการ

๓. Decryption คือ การถอดรหัสข้อมูล

๔. Birthday Attacks คือ การสุ่มคีย์ขึ้นมา และตรงกับที่กำหนดไว้

๕. Man In the middle Attacks คือ การพยายามที่จะทาตัวเป็นคนกลางเพื่อคอยดักเปลี่ยนแปลงข้อมูลโดยที่คู่สนทนาไม่รู้ตัว

สิ่งที่ต้องพึงระวังในการใช้งานบนอินเทอร์เน็ต

๑. การโจมตีของ Malware and Virus Threat รูปแบบของไฟล์ที่ส่งต่อผ่านอีเมล์ หรืออาจจะส่งผ่านสื่อสังคมออนไลน์หรือ Social Media

๒. การโจมตีของ Zombie attack เป็นรูปแบบแนวโน้มที่จะมีมากในปัจจุบัน โดยปล่อยไวรัสไปยังคอมพิวเตอร์ เครือข่ายของอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์กลายเป็น Zombie ถูกแฮกเกอร์ควบคุม

๓. การหลอกลวงเชิงจิตวิทยา (Social Engineering) เพื่อให้เปิดเผยข้อมูล Phishing เป็นรูปแบบหนึ่งของการทำ Social Engineering ซึ่งเป็นเทคนิคการหลอกลวงโดยใช้จิตวิทยาผ่านระบบคอมพิวเตอร์ ส่วนใหญ่จะมาในรูปแบบอีเมล์ เว็บไซต์ และสื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ที่จะให้ผู้ใช้กรอกข้อมูลส่วนบุคคลที่เป็นความลับ

สิ่งที่ไม่ควรใช้เป็นรหัสผ่าน

เพื่อความปลอดภัยในการใช้งานระบบคอมพิวเตอร์ ผู้ใช้งานควรตั้งรหัสผ่านที่ไม่สั้นเกินไป เป็นข้อความที่ไม่มีความหมาย ประกอบด้วย อักษรตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ และหลีกเลี่ยงการตั้งรหัสผ่านด้วยชุดอักหรือตัวเลขที่คาดเดาไว้ง่าย เช่น 9999 1111 7876 1234 abcd qwerty หรือข้อมูลส่วนตัว เช่น หมายเลขโทรศัพท์ วันเดือนปีเกิด ชื่อตัวเอง หรือผู้ใช้ของโปรแกรม

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ. ศ. ๒๕๕๐ (แก้ไขเพิ่มเติม พ.ศ. ๒๕๖๐) และได้ประกาศในราชกิจจานุเบกษา เมื่อ ๒๕ มกราคม ๒๕๖๐

คำศัพท์เกี่ยวกับคอมพิวเตอร์ ในมาตรา ๓

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทางานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดสิ่งใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในคอมพิวเตอร์ในสภาพที่ระบบอาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของการบริการหรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

ผู้ให้บริการ" หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

“พนักงานเจ้าหน้าที่” หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัตินี้

“รัฐมนตรี” หมายความว่า รัฐมนตรีผู้รักษาการตราพระราชบัญญัตินี้

สิ่งที่สำคัญที่เป็นจุดเด่นของ พ.ร.บ. ฉบับนี้ คือ ข้อมูลจราจรทางคอมพิวเตอร์ โดยถ้ามีการทำผิดทางเครือข่ายอินเตอร์เน็ตหรือเครือข่ายคอมพิวเตอร์ จะสามารถนำข้อมูลจราจรทางคอมพิวเตอร์มาทำการตรวจสอบเพื่อให้ทราบว่าผู้กระทำความผิดนั้น เป็นใคร อย่างไร ในเวลานั้น ๆ

ตัวอย่าง การกระทำความผิดตาม พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรานี้เป็นการป้องกันบุคคลที่นำข้อมูลที่เป็นความลับเกี่ยวกับมาตรการการป้องกันระบบฐานข้อมูลไปเปิดเผยโดยมิชอบ แล้วทำให้เกิดความเสียหายเกิดขึ้น เช่น นำรุ่น เวอร์ชั่นระบบรักษาความปลอดภัยขององค์กรไปเปิดเผย และมีผู้นำข้อมูลเหล่านั้นไปใช้ในการโจมตีระบบและเป็นผลสำเร็จทำให้เกิดความเสียหายถ้ามีการนำไปพูดและพิสูจน์ทราบ บุคคลนั้นจะมีความผิดตามมาตรานี้

แหล่งที่มา

หลักสูตร : ความมั่นคงปลอดภัยบนอินเทอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล
บรรยายโดย : อาจารย์ณัฐ พยงค์ศรี
สถาบัน/หน่วยงาน/ระบบ : สำนักงาน ก.พ. , ระบบฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ (LDD e-Training)
รูปแบบหลักสูตร : e-Learning
ช่วงเวลาการฝึกอบรม : ก.พ. 2567