ETDA สพธอ www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

สาขาวิชาชีพอุตสาหกรรมดิจิทัล
สาขาธุรกิจดิจิทัลและพาณิชย์อิเล็กทรอนิกส์

อาชีพนักบริหารระบบความมั่นคงปลอดภัย ด้านพาณิชย์อิเล็กทรอนิกส์ ระดับ 6

สารบัญ
CONTENT

บทที่ 4
รับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์

65

ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

72

กฎ ระเบียบ ข้อบังคับ
ในการรักษาข้อมูลจราจรทางคอมพิวเตอร์

บทที่ 5
ปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

81

จริยธรรมและจรรยาบรรณ
ในการประกอบวิชาชีพ
ด้านพาณิชย์อิเล็กทรอนิกส์

94

Data Life Cycle

98

ความเป็นส่วนตัวและ
การรักษาความลับข้อมูลส่วนบุคคล
และองค์การ

บทที่ 6
ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์

103

ข้อกำหนด ข้อบังคับ
และบทลงโทษตามกฎหมาย
พาณิชย์อิเล็กทรอนิกส์

119

พระราชบัญญัติ
คุ้มครองข้อมูลส่วนบุคคล
พ.ศ.2562

บทที่ 7
ปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

126

การเข้าใจภัยคุกคามในระบบสารสนเทศ
และวิธีการป้องกันภัยคุกคาม
และการหลอกลวงออนไลน์

129

ปฏิบัติตามหลักการ
เพื่อรักษาความปลอดภัย

บทที่

1 การบริหารจัดการระบบความมั่นคงปลอดภัยด้านเว็บไซต์

หัวข้อเนื้อหาการเรียนรู้ที่ 1
การเลือกผู้รับจดทะเบียนชื่อโดเมน

นิยาม/ความหมายของภัยคุกคาม (Threat)

เทคโนโลยีสารสนเทศย่อมาจากคำว่า ไอที (information technology: IT) ซึ่งหมายถึง การประยุกต์ใช้คอมพิวเตอร์และอุปกรณ์โทรคมนาคม เพื่อจัดเก็บ ค้นหา ส่งผ่าน และจัดดำเนินการข้อมูล ซึ่งมักเกี่ยวข้องกับธุรกิจหนึ่งหรือองค์การต่าง ๆ ซึ่งส่วนใหญ่ในความเข้าใจมักให้ความหมายสำคัญคือ เครื่องคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ และยังรวมไปถึงเทคโนโลยีการกระจายสารสนเทศอย่างอื่นด้วย เช่น โทรทัศน์และโทรศัพท์ อุตสาหกรรมหลายอย่างเกี่ยวข้องกับเทคโนโลยีสารสนเทศ ตัวอย่างเช่น ฮาร์ดแวร์ ซอฟต์แวร์ อิเล็กทรอนิกส์ อุปกรณ์กึ่งตัวนำ อินเทอร์เน็ต อุปกรณ์โทรคมนาคม การพาณิชย์อิเล็กทรอนิกส์ และบริการทางคอมพิวเตอร์

กระบวนการที่เกี่ยวข้องกับการป้องกันและตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งเรียกว่าเป็นขั้นตอนการป้องกันสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่าง ๆ ถูกใช้งาน โดยผู้ที่ไม่ได้รับสิทธิ์หรือไม่ได้รับอนุญาต หรือเรียกว่า **ความปลอดภัยของเทคโนโลยีสารสนเทศ**

ทั้งนี้ ในการตรวจสอบข้อมูลยังเกิดข้อดี คือ ทราบได้ว่ามีใครกำลังพยายามที่จะบุกรุกเข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ มีผู้บุกรุกระบบใดบ้าง รวมทั้งการป้องกันจากภัยคุกคาม (Threat) ต่าง ๆ

ความมั่นคงปลอดภัย

ความมั่นคงปลอดภัย (Security) ซึ่งหมายถึง การทำให้รอดพ้นจากอันตรายหรืออยู่ในสถานะที่มีความปลอดภัยไร้ความกังวลและความกลัวและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ โดยทั่วไปแล้วเป็นพื้นฐานสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศ (Information System Security) ซึ่งถือเป็นการป้องกันข้อมูลสารสนเทศรวมถึงองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง เช่น ระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้รอดพ้นจากอันตราย

ภัยคุกคามของเทคโนโลยีสารสนเทศ

ภัยคุกคามของเทคโนโลยีสารสนเทศ คือ สิ่งที่อาจก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่า เราเรียกว่า ภัยคุกคาม โดยอาจเกิดจากธรรมชาติหรือบุคคล อาจจะตั้งใจหรือไม่ก็ตามหากพิจารณาตามความเสียหายที่เกิดขึ้น โดยการกระทำที่เกิดขึ้นจนได้รับความเสียหายเราเรียกว่า การโจมตี (Attack) จากผู้โจมตี (Attacker) ที่เรียกว่า แฮ็กเกอร์ (Hacker) หรือแคร็กเกอร์ (Cracker) และลักษณะการโจมตีหรือบุกรุกอาจเกิดขึ้นได้หลายแบบ เช่น การพยายามเข้าใช้งาน การแก้ไขข้อมูล การทำให้เสียหาย และการทำลายข้อมูล

ภัยคุกคามแบ่งเป็น 2 ประเภท ได้แก่

1

ภัยคุกคามทางกายภาพ (Physical Threat)

ภัยคุกคามที่เกิดขึ้นกับฮาร์ดแวร์ที่ใช้ในระบบคอมพิวเตอร์และระบบเครือข่าย เช่น ฮาร์ดดิสก์เสีย หรือทำงานผิดพลาด โดยอาจเกิดจากภัยธรรมชาติ เช่น น้ำท่วม ไฟไหม้ ฟ้าผ่า แต่ในบางครั้งอาจเกิดจากการกระทำของมนุษย์ด้วยเจตนาหรือไม่เจตนาก็ตาม

2

ภัยคุกคามทางตรรกะ (Logical Threat)

ภัยคุกคามที่เกิดขึ้นกับข้อมูลสารสนเทศ หรือการใช้ทรัพยากรของระบบ เช่น การแอบลักลอบใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตการขัดขวางไม่ให้คอมพิวเตอร์ทำงานได้ตามปกติ การปรับเปลี่ยนข้อมูลหรือสารสนเทศโดยไม่ได้รับอนุญาต เช่น แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมิได้รับอนุญาต แต่ไม่มีประสงค์ร้าย หรือไม่มีเจตนาที่จะสร้างความเสียหายหรือสร้างความเดือดร้อนให้แก่ใครทั้งสิ้น แต่เหตุผลที่ทำเช่นนั้นอาจเป็นเพราะต้องการทดสอบความรู้ความสามารถของตนเองก็เป็นไปได้ ซึ่งเรียกกลุ่มคนรูปแบบนี้ว่า **แฮ็กเกอร์ (hacker)** นอกจากนี้ยังมีที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่น โดยมีเจตนาร้ายอาจจะเข้าไปทำลายระบบ หรือสร้างความเสียหายให้กับระบบ Network ขององค์กรอื่น หรือขโมยข้อมูลที่เป็นความลับทางธุรกิจ ซึ่งเรียกบุคคลกลุ่มนี้ว่า แคร็กเกอร์ (Cracker) ความแตกต่างระหว่าง Hacker กับ Cracker คือ Hacker มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าท้าย โดยการเจาะระบบให้สำเร็จ ส่วน Cracker มีจุดประสงค์คือ ต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ

ความสำคัญของนโยบาย และการจัดทำแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ตามมาตรฐานที่กำหนด

สิ่งสำคัญในการดำเนินงานความมั่นคงปลอดภัยของสารสนเทศนั้น มีสิ่งที่ต้องคำนึงถึงเป็นหลักได้แก่ ความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability) นอกจากนี้ยังต้องคำนึงถึงนโยบายการปฏิบัติงาน การให้การศึกษา และเทคโนโลยีที่จะนำมาใช้เป็นกลไกควบคุมและป้องกันที่ต้องเกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยของสารสนเทศด้วย โดยในที่นี้จะกล่าวถึงสิ่งที่ต้องคำนึงถึงเป็นหลักก่อน

1 ความลับ (Confidentiality)

เนื่องจากข้อมูลบางอย่างมีความสำคัญจำเป็นต้องเก็บเป็นความลับ หากถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตราย เช่น ข้อมูลทางการทหาร ข้อมูลทางธุรกิจ การรักษาความลับเป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัย และผู้ใช้กลไกหลักที่ใช้ในการรักษาความลับ คือ การเข้ารหัสข้อมูล (Cryptography or Encryption) โดยมีหลักการ คือ การเปลี่ยนรูปแบบข้อมูลที่อ่านออกให้อยู่ในรูปแบบที่ไม่สามารถอ่านออกหรือเข้าใจได้ โดยมีการใช้ Key (Password) ในกระบวนการเข้ารหัสและถอดรหัส ตัวอย่างเช่น การซื้อสินค้าผ่านระบบเว็บไซต์ด้วยบัตรเครดิต ซึ่งบริษัทบัตรเครดิตต้องมีการรักษาความลับของลูกค้าโดยต้องมีการกรอกข้อมูลยืนยันพร้อมรหัสผ่านจึงจะสามารถทำการซื้อสินค้าได้ สำหรับผู้ที่ใช้บริการเว็บไซต์มีสิ่งที่สามารถสังเกตได้คือ เว็บไซต์ที่มีการเข้ารหัสจะใช้โปรโตคอล https แทน http โดยโปรโตคอล https จะมีการเข้ารหัสก่อนส่งข้อมูล ทำให้แม้จะถูกดักฟังข้อมูลไปแต่หากถอดรหัสไม่ได้ก็จะไม่สามารถอ่านข้อมูลนั้นได้ ต่างจากโปรโตคอล http ซึ่งส่งข้อมูลเป็นตัวอักษรธรรมดาที่สามารถอ่านได้ทันที กลไกอื่น ๆ ที่ใช้ปกป้องความลับ ได้แก่ การควบคุมการเข้าถึง (Access Control) ที่จะต้องมีการพิสูจน์ทราบตัวตนของผู้ใช้งานก่อนว่ามีสิทธิ์ใช้งานหรือไม่ เช่น การล็อกอินก่อนเข้าใช้งาน

2 ความคงสภาพ (Integrity)

ความคงสภาพ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศจะขาดความคงสภาพเมื่อสารสนเทศนั้นถูกเปลี่ยนแปลงหรือปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกระทำในรูปแบบอื่น ๆ ซึ่งจะส่งผลต่อความเชื่อได้ของข้อมูลหรือแหล่งที่มา ผู้รับผิดชอบจึงต้องปกป้องข้อมูลให้คงสภาพเดิม ไม่ถูกดัดแปลงแก้ไขโดยผู้ที่ไม่ได้รับอนุญาตกลไกหลักที่ใช้ในการรักษาความคงสภาพประกอบด้วย 2 ส่วน คือ การป้องกัน (Prevention) และการตรวจสอบ (Detection)

2.1 การป้องกัน (Prevention)

เป็นการป้องกันไม่ให้มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต รวมถึงป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลนอกเหนือขอบเขตของผู้ได้รับอนุญาต ซึ่งอาจใช้การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ในประเด็นแรก และใช้การตรวจสอบสิทธิ์ (Authorization) ในประเด็นหลัง

2.2 การตรวจสอบ (Detection)

เพื่อดูว่าข้อมูลยังคงมีความน่าเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถตรวจเช็กวิเคราะห์เหตุการณ์ต่าง ๆ ที่เกิดขึ้นจาก Log File

3 ความพร้อมใช้ (Availability)

ความพร้อมใช้ หมายถึง ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด ความพร้อมใช้งานจัดเป็นส่วนหนึ่งของความมั่นคง ความน่าเชื่อถือ (Reliability) ของระบบ ระบบอาจถูกโจมตีโดยผู้ไม่ประสงค์ดีที่พยายามทำให้ระบบไม่สามารถใช้งานได้ แนวทางการป้องกัน เช่น การทำโหลดบาลานซ์ชิง (Load Balancing) เพื่อกระจายงานให้กับเครื่องแม่ข่ายหลายเครื่อง หรือการทำระบบสำรอง (Backup System) เพื่อให้สามารถกู้คืนข้อมูลได้หากข้อมูลเสียหาย หรือหากข้อมูลหรือสารสนเทศขาดคุณสมบัติด้านใดด้านหนึ่งหรือหลายด้าน จากทั้ง 3 คุณสมบัติ ได้แก่ความลับ ความคงสภาพ และความพร้อมใช้ จะถือว่าข้อมูลหรือสารสนเทศนั้นไม่มีความปลอดภัย

ดังนั้น การกำหนดนโยบายและการจัดทำแผนด้านความมั่นคงปลอดภัยของเว็บไซต์จะดำเนินการตามวัตถุประสงค์ ดังนี้

3.1 เพื่อกำหนดทิศทาง หลักการ และกรอบของข้อกำหนดในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์

3.2 เพื่อสร้างความรู้ความเข้าใจให้พนักงานปฏิบัติตามนโยบาย มาตรฐานกรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำรวมถึงกฎหมายที่เกี่ยวกับระบบคอมพิวเตอร์ได้อย่างถูกต้องและเหมาะสม

3.3 เพื่อให้พนักงานและผู้ที่ต้องใช้หรือเชื่อมต่อระบบคอมพิวเตอร์ขององค์กรให้สามารถใช้งานระบบคอมพิวเตอร์ของบริษัทได้อย่างถูกต้องและเหมาะสม

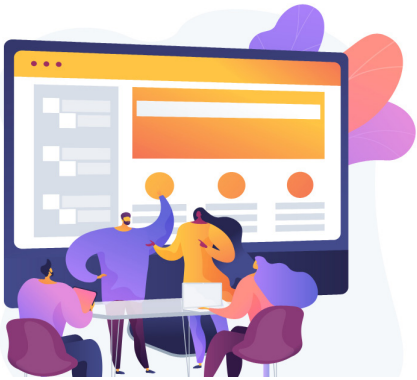
3.4 เพื่อป้องกันไม่ให้ระบบคอมพิวเตอร์และข้อมูลสารสนเทศขององค์กรโดนบุกรุก ขโมย ทำลาย แทรกแซงการทำงาน หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อการดำเนินธุรกิจขององค์กร

ขั้นตอน / แนวทาง ทางการวางแผนเพื่อ บริหารจัดการเครื่องบริการเว็บ

การวางแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ มีหลักเกณฑ์ที่ใช้สำหรับการพิจารณาเพื่อจัดทำแผน ซึ่งได้แก่ การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ ภัยคุกคาม (Threat) ที่เกี่ยวข้อง และการวางมาตรการ (Measure) เพื่อป้องกันภัยคุกคามที่มีความสำคัญ โดยมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard) มีแนวทางในการจัดทำแผนด้านความมั่นคงปลอดภัยของเว็บไซต์ ดังต่อไปนี้

1 การวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ

ก่อนที่จะมีการจัดทำเว็บไซต์ การสำรวจความต้องการทางธุรกิจหรือความต้องการของผู้ใช้บริการเป็นข้อมูลสำคัญสำหรับการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ ซึ่งบอกได้ว่าการจัดทำเว็บไซต์มีจุดประสงค์เพื่ออะไร คุณสมบัติของเครื่องบริการเว็บเป็นอย่างไร และการกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง รวมถึงการใช้เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม เพื่อตอบสนองต่อความต้องการของธุรกิจและผู้ใช้บริการ



2 จัดลำดับความเสี่ยงของภัยคุกคามที่คาดว่าจะเกิดขึ้นกับเว็บไซต์

ก่อนที่จะมีการจัดทำเว็บไซต์ การสำรวจความต้องการทางธุรกิจหรือความต้องการของผู้ใช้บริการเป็นข้อมูลสำคัญสำหรับการวางแผนเพื่อบริหารจัดการเครื่องบริการเว็บ ซึ่งบอกได้ว่าการจัดทำเว็บไซต์มีจุดประสงค์เพื่ออะไร คุณสมบัติของเครื่องบริการเว็บเป็นอย่างไร และการกำหนดหน้าที่ความรับผิดชอบของบุคลากรที่เกี่ยวข้อง รวมถึงการใช้เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยอย่างเหมาะสม เพื่อตอบสนองต่อความต้องการของธุรกิจและผู้ใช้บริการ

3 กำหนดมาตรการที่เกี่ยวข้องเพื่อป้องกันภัยคุกคามที่มีความสำคัญ

การจัดลำดับความเสี่ยงของภัยคุกคามทำให้สามารถเลือกใช้มาตรการเพื่อป้องกันหรือลดความเสี่ยงจากภัยคุกคามที่มีความสำคัญโดยมีค่าใช้จ่ายที่เหมาะสม ไม่ว่าจะเป็นเรื่องของการเตรียมความพร้อมให้กับบุคคลที่เกี่ยวข้อง การเลือกใช้เทคโนโลยีและมาตรฐานด้านความมั่นคงปลอดภัยที่เหมาะกับภัยคุกคามและสามารถขยายขอบเขตการรักษาความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพในกรณีที่เว็บไซต์มีผู้ใช้บริการมากขึ้น

หัวข้อเนื้อหาการเรียนรู้ที่ 2 เครื่องบริการเว็บ โดเมน และระบบบริหารจัดการเว็บไซต์

การเลือกผู้รับจดทะเบียนชื่อโดเมน

เครื่องบริการเว็บหรือเครื่องคอมพิวเตอร์ที่ให้บริการอยู่บนเครือข่ายอินเทอร์เน็ต ในความเป็นจริงจะถูกระบุด้วย หมายเลข IP (เช่น 165.134.170.27) แต่เนื่องจากคนเราสามารถจดจำชื่อได้ดีกว่าการจำตัวเลขยาว ๆ **ยูอาร์แอล (URL: Universal Resource Locator)** หรือ ตัวชี้แหล่งในอินเทอร์เน็ต จึงมีขึ้นเพื่ออำนวยความสะดวกในการอ้างถึงเครื่องบริการเว็บบนเครือข่ายอินเทอร์เน็ต โดยยูอาร์แอลจะมีความสัมพันธ์กับชื่อโดเมน เพราะชื่อโดเมนเป็นที่อยู่เป้าหมายและเป็นส่วนประกอบของยูอาร์แอล เช่น https://www.etda.or.th หรือ https://www.thaicert.or.th จะมีชื่อโดเมนที่มีการใช้ คือ etda.or.th และ thaicert.or.th ตามลำดับ

ดังนั้น ก่อนที่จะพัฒนาเว็บไซต์ ผู้ดูแลเครื่องบริการเว็บ จึงมีความจำเป็นจะต้องจดทะเบียนชื่อโดเมนของเว็บไซต์ตนเองเสียก่อน ชื่อโดเมนจึงมีความสำคัญเป็นอันดับแรกสำหรับเว็บไซต์ โดยเฉพาะกับการโฆษณาประชาสัมพันธ์บนอินเทอร์เน็ต ถ้าได้ชื่อที่จดจำง่าย ตรงกับกลุ่มเป้าหมายที่มีความสนใจในบริการหรือสินค้าอยู่แล้วนั้น จะทำให้ชื่อโดเมนหรือเว็บไซต์นั้น ๆ ได้รับความสนใจและเป็นที่จดจำได้ง่าย ไม่เฉพาะลูกค้าของเว็บไซต์เท่านั้น แต่ยังรวมไปถึงโปรแกรมค้นหา (Search Engine) ชื่อดังต่าง ๆ ที่จะเข้ามาทำดัชนีการค้นหา (Index) ในเว็บเพจหน้าต่าง ๆ ของเว็บไซต์ เช่น Google Yahoo และ BING

แนวทางการเลือก รูปแบบเครื่องบริการเว็บ

ผู้ให้บริการเว็บโฮสติ้ง มีส่วนสำคัญในด้านความมั่นคงปลอดภัยเว็บไซต์ เนื่องจากในรูปแบบที่นิยมกระทำกันนั้น ผู้ให้บริการจะมีฐานะเป็นผู้ดูแลระบบปฏิบัติการ (Operating System) โปรแกรมสำหรับให้บริการเว็บ (Web Server Software) ระบบบริหารจัดการเว็บไซต์ (CMS) และซอฟต์แวร์ที่เกี่ยวข้องกับเครื่องบริการเว็บทั้งหมด ทั้งในการติดตั้ง ตั้งค่า และการปรับเวอร์ชันหรือปรับปรุงระบบ (Upgrade/Update) ซึ่งในบางครั้ง ช่องโหว่ก็อาจจะเกิดขึ้นมาจากข้อผิดพลาดของระบบปฏิบัติการ (Operating System) หรือ โปรแกรมสำหรับให้บริการเว็บ หรือ ระบบบริหารจัดการเว็บไซต์ ซึ่งบางครั้งการตั้งค่าบางอย่างผู้ใช้บริการไม่สามารถแก้ไขปรับปรุงได้เอง

แนวทางในการพิจารณาเลือกผู้ให้บริการเว็บโฮสติ้ง

1 พิจารณาเลือกรูปแบบการให้บริการระหว่าง Shared หรือ Dedicated

รูปแบบการให้บริการเว็บโฮสติ้งนั้นมีหลายรูปแบบไม่ว่าจะเป็นการให้บริการแบบ Shared หรือ Dedicated ซึ่งรูปแบบการให้บริการนั้นมีข้อแตกต่างกันทั้งในเรื่องของต้นทุนค่าใช้จ่ายและสภาพแวดล้อมที่มีผลกระทบต่อความมั่นคงปลอดภัยของเว็บไซต์

การให้บริการแบบ Shared

มีค่าใช้จ่ายที่ต่ำเนื่องจากเป็นการใช้เครื่องบริการร่วมกันระหว่างผู้ใช้บริการหลาย ๆ ราย โดยมักไม่ได้มีการแบ่งแยกสิทธิ์การเข้าถึงระหว่างโปรแกรมประยุกต์ของผู้ใช้บริการแต่ละราย ดังนั้น หากเว็บไซต์ของผู้ใช้บริการรายใดรายหนึ่งมีช่องโหว่ ผู้ประสงค์ร้ายก็อาจอาศัยช่องโหว่นั้นในการเข้าโจมตีเว็บไซต์อื่น ๆ ที่อยู่ในเครื่องบริการเดียวกันได้ แม้ว่าจะเป็นเว็บไซต์ที่ไม่มีช่องโหว่เลยก็ตาม

การให้บริการแบบ Dedicated

ผู้ใช้บริการแต่ละรายจะได้เครื่องบริการเว็บแยกกันไปโดยเฉพาะ จึงทำให้มีค่าใช้จ่ายที่สูงกว่ามาก แต่ช่วยป้องกันความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่ของเว็บไซต์อื่นได้ดีกว่า ดังนั้น หากผู้ใช้บริการมีข้อจำกัดทางด้านต้นทุนและค่าใช้จ่ายก็มีความจำเป็นที่จะต้องรับทราบถึงความเสี่ยงด้านความมั่นคงปลอดภัยและเตรียมแนวทางการป้องกันหรือบรรเทาผลกระทบจากความเสี่ยงดังกล่าวไว้

หลายครั้งที่ชื่อโดเมนถูกแก้ไขให้ชี้ไปยังเว็บไซต์หลอกลวง และสาเหตุหนึ่งที่ทำให้เกิดเหตุการณ์นี้คือ การเข้าถึงบัญชีที่ใช้จดทะเบียนชื่อโดเมนโดยไม่ได้รับอนุญาต ทำให้ผู้ประสงค์ร้ายสามารถเข้าไปเปลี่ยนแปลงการตั้งค่าของชื่อโดเมนเพื่อนำไปใช้ในทางที่ผิด ซึ่งปรากฏตามรายงานของ Security and Stability Advisory Committee (SSAC) ดังนั้น แนวทางในการเลือกผู้รับจดทะเบียนชื่อโดเมนมีดังต่อไปนี้

1

มีการยืนยันการลงทะเบียน

โดยให้ผู้ขอจดทะเบียนยืนยันอีเมลของตนโดยการเข้าไปยังจุดเชื่อมโยงหลายมิติ (Hyperlink) บนเว็บเพจ ซึ่งระบุไว้ในอีเมลเปิดการใช้งาน (Activation Email) ที่ผู้รับจดทะเบียนส่งมา โดยบริการจดทะเบียนสามารถเพิ่มมาตรการความมั่นคงปลอดภัยโดยใช้การติดต่อไปยังหมายเลขโทรศัพท์ของผู้ขอจดทะเบียน เพื่อบอกหมายเลขสำหรับยืนยันการลงทะเบียน (Confirmation Number) ให้ผู้ขอจดทะเบียนนำหมายเลขมากรอกในแบบฟอร์มบนเว็บเพจ เพื่อเปิดการใช้งานบัญชีหรืออนุญาตให้ทำธุรกรรมได้

2

มีมาตรการในการเพิ่มความมั่นคงปลอดภัยให้กับรหัสผ่าน

เช่น การกำหนดค่าเริ่มต้นของรหัสผ่านที่มีความซับซ้อนคาดเดาได้ยาก (Strong Password) ระบุความยาวขั้นต่ำของรหัสผ่าน จำกัดอายุการใช้งาน

3

มีการแจ้งเตือนและยืนยันการเปลี่ยนแปลงข้อมูลลงทะเบียน

ทั้งนี้ การเปลี่ยนแปลงข้อมูลต่าง ๆ ต้องมีการกำหนดขั้นตอนสำหรับการเปลี่ยนแปลงข้อมูล ซึ่งต้องอาศัยการยืนยันจากหลายบุคคลที่เกี่ยวข้อง โดยการยืนยันการเปลี่ยนแปลงในลักษณะนี้จะช่วยป้องกันการเปลี่ยนแปลงจากผู้ประสงค์ร้ายที่อาจปลอมตัวเพื่อเข้ามาเอาข้อมูลจากบุคคลใดบุคคลหนึ่งได้

2 การพิจารณาจากรูปแบบนโยบายการจัดการช่องโหว่

เมื่อมีการค้นพบช่องโหว่ในซอฟต์แวร์ที่ใช้งานอยู่ในเครื่องบริการเว็บ ผู้ให้บริการจะต้องมีนโยบายที่ชัดเจนในการป้องกันความเสียหายที่อาจจะเกิดจากช่องโหว่นั้น ๆ เช่น การแจ้งให้ผู้ใช้ทราบในทันที การ Patch หรือแก้ปัญหาเฉพาะหน้า (Workaround) ตามที่ผู้ผลิตซอฟต์แวร์หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่เชื่อถือได้แนะนำ ตลอดจนแผนสำรองในกรณีที่เป็นช่องโหว่ที่ไม่สามารถหาวิธีแก้ไขหรือป้องกันความเสียหายในระยะเวลาอันสั้นได้ โดยต้องพิจารณาทั้งผลที่คาดว่าจะได้รับและระยะเวลาที่สามารถดำเนินการได้สำเร็จ ตลอดจนอาจต้องพิจารณาถึงความรับผิดชอบ (Liability) ที่ผู้ให้บริการอาจจะต้องชดเชยในกรณีที่เกิดความเสียหายแก่ผู้ใช้บริการ ในกรณีที่เกิดความบกพร่องในการจัดการกับช่องโหว่

3 รูปแบบการให้บริการโอนย้ายไฟล์ข้อมูล (Remote File Transfer)

ในการโอนย้ายไฟล์ข้อมูลระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ ผู้ให้บริการเว็บโฮสติ้งควรมีช่องทางการโอนย้ายที่มั่นคงปลอดภัยและมีการเข้ารหัสเพื่อรักษาความลับของข้อมูลระหว่างที่มีการโอนย้าย เช่น มีบริการ Secure Transfer Protocol (SFTP) สำหรับกระบวนการโอนย้ายไฟล์

4 การให้บริการรูปแบบการสื่อสารอย่างมั่นคงปลอดภัยสำหรับเว็บไซต์ (บริการโปรโตคอล SSL/TLS)

บริการโปรโตคอล SSL (Secure Socket Layer Protocol) และ TLS (Transport Layer Security Protocol) เป็นโปรโตคอลที่กำหนด รูปแบบการสื่อสารที่มีความมั่นคงปลอดภัย ซึ่งสามารถป้องกันการสื่อสารของโปรแกรมประยุกต์ในระบบรับ-ให้ (Client-Server System) จากการลอบฟัง (Eavesdropping) การแก้ไขให้เสียหาย (Tampering) และการปลอมแปลงข้อความที่ใช้ในการสื่อสาร (Message Forgery) เว็บไซต์ที่ไม่ได้มีการนำ SSL/TLS มาใช้งาน จะเปิดโอกาสให้ผู้ประสงค์ร้ายสามารถลอบฟัง แก้ไข และปลอมแปลงข้อมูลที่ใช้รับ-ส่งระหว่างเครื่องบริการเว็บและผู้ใช้บริการได้

ในกรณีที่มีความจำเป็นต้องใช้งานบริการ SSL/TLS ผู้ใช้บริการควรตรวจสอบว่าผู้ให้บริการเว็บโฮสติ้งมีการให้บริการ SSL/TLS หรือไม่ หากผู้ให้บริการสามารถให้บริการ SSL/TLS ผู้ใช้บริการก็จำเป็นจะต้องขอใบรับรองอิเล็กทรอนิกส์ประเภทเว็บไซต์ หรือ SSL Certificate จากผู้ให้บริการใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือ

บริการ SSL/TLS จะเป็นเครื่องมือที่สำคัญในการรักษาความมั่นคงปลอดภัยของข้อมูลสำคัญ เช่น ข้อมูลลูกค้า ข้อมูลบัตรเครดิต ซึ่งมีการรับ-ส่งกันระหว่างเครื่องของผู้ใช้บริการและเครื่องบริการเว็บ โดยเฉพาะผู้ใช้บริการที่ต้องการจะเปิดบริการเว็บไซต์สำหรับการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce Website) หรือการทำธุรกรรมทางอิเล็กทรอนิกส์สำหรับภาครัฐ

5 การสำรองข้อมูลและการดูแลรักษาเครื่องบริการเว็บ

ผู้ให้บริการต้องมีการสำรองข้อมูลของเครื่องบริการเว็บที่อยู่ในความดูแลอย่างสม่ำเสมอ นอกจากนี้ ผู้ให้บริการควรมีเครื่องมือให้กับผู้ใช้บริการสำหรับการสำรองข้อมูลของเว็บไซต์ด้วยตนเอง และผู้ใช้บริการควรตรวจสอบนโยบายที่เกี่ยวข้องกับการสำรองและกู้คืนข้อมูลของผู้ให้บริการ วิธีการสำรองข้อมูลที่ผู้ให้บริการใช้ และเครื่องมืออำนวยความสะดวกให้กับการสำรองและกู้คืนข้อมูล ว่ามีความเหมาะสมและสอดคล้องกับความต้องการใช้งานหรือไม่

6 การติดต่อผู้ให้บริการเมื่อมีเหตุฉุกเฉิน

ผู้ให้บริการควรจะมีช่องทางติดต่อเฉพาะสำหรับกรณีที่เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อใช้ในการประสานงานอย่างทันท่วงที ทั้งในกรณีที่ผู้ใช้บริการต้องการติดต่อเพื่อขอความช่วยเหลือ หรือกรณีที่มีหน่วยงานอื่นประสานเข้ามา การที่ให้ผู้บริการมีช่องทางติดต่อเฉพาะเกี่ยวกับเรื่องความมั่นคงปลอดภัยจะช่วยสะท้อนว่าผู้ให้บริการมีความเอาใจใส่ต่อปัญหาด้านความมั่นคงปลอดภัยเป็นอย่างยิ่ง

แนวทางการเลือก ระบบบริหารจัดการเว็บไซต์ (CMS)

การพัฒนาเว็บไซต์ของหน่วยงานรัฐและเอกชนในปัจจุบัน เห็นได้ชัดว่ามีแนวโน้มของการนำเอาระบบบริหารจัดการเว็บไซต์มาใช้งานกันอย่างแพร่หลาย อาจเนื่องมาจากความสะดวกสบายของการพัฒนาและบริหารจัดการเว็บไซต์ โดยรูปแบบของการพัฒนามีทั้งที่เป็นการนำ CMS ที่พัฒนามาจากผู้พัฒนาในต่างประเทศ ซึ่งอนุญาตให้ผู้ใช้บริการทั่วโลกสามารถนำไปใช้งานต่อไปฟรี หรืออีกประเภทหนึ่งคือ CMS ที่พัฒนาโดยบริษัทในประเทศไทยและมีการคิดค่าบริการหรือลิขสิทธิ์ในการใช้งาน ก็เป็นอีกหนึ่งทางเลือกของเทคโนโลยีการพัฒนาเว็บไซต์

ปัจจุบันพบว่า ระบบบริหารจัดการเว็บไซต์ที่เป็นที่นิยมและมีผู้ใช้บริการมากที่สุด ได้แก่ WordPress Joomla และ Drupal ตามลำดับ และจากสถิติของ Google Trends และสถิติเรื่องช่องโหว่ที่ National Vulnerability Database (NVD) ซึ่งเป็นองค์กรที่อยู่ภายใต้กำกับของ Nation Institute of Standards and Technology หรือ NIST พบว่า CMS ที่มีความนิยมใช้กันมากก็จะมีรายงานช่องโหว่ของระบบมากเช่นกัน แม้ว่าการนำระบบบริหารจัดการเว็บไซต์มาประยุกต์ใช้ จะถือเป็นการตอบโจทย์หน่วยงานที่ต้องการให้บริการจัดการเว็บไซต์เป็นไปอย่างง่ายดายและย่นระยะเวลาในการพัฒนา สามารถนำเวลาไปพัฒนาในส่วนเนื้อหาให้มีความสมบูรณ์ได้มากกว่า แต่เนื่องจาก CMS ที่เป็นที่นิยมมักเป็นระบบที่พัฒนาแบบโอเพนซอร์ส (Open Source) ซึ่งมีความเสี่ยงที่จะพบช่องโหว่ต่าง ๆ ได้

แนวทางในการพิจารณาเลือก ระบบบริหารจัดการเว็บไซต์ที่มีความมั่นคงปลอดภัย

1 พิจารณาจากตัวเลือกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

CMS ควรมีเอกสารแนะนำแนวทางการติดตั้งและการตั้งค่าเพื่อรักษาความมั่นคงปลอดภัย (Security Best Practice) และมี Plugin เสริมที่ติดตั้งให้เกิดความมั่นคงปลอดภัยตรงตามความต้องการของผู้ดูแลเครื่องบริการเว็บและผู้ใช้บริการ นอกจากตัวเลือกด้านความมั่นคงปลอดภัยแล้วยังมีปัจจัยอื่น ๆ ที่สามารถนำมาพิจารณาใช้เป็นแนวทางในการเลือก CMS ได้

2 พิจารณาจากคุณภาพของประชาคมนักพัฒนา CMS

ในกรณีของ CMS ที่เป็น Open Source ซึ่งต้องอาศัยประชาคมของนักพัฒนาในการปรับปรุง CMS ให้ดีขึ้น CMS ที่มีประชาคมนักพัฒนาที่มีขนาดใหญ่ มีการสื่อสารภายในและพัฒนาอย่างต่อเนื่อง (Active Developer Community) จะเป็น CMS ที่มีฟังก์ชันการทำงานตอบสนองต่อความต้องการของผู้ใช้ได้มากกว่า รวมถึงการปรับเวอร์ชันหรือปรับปรุงระบบเพื่อแก้ไขข้อบกพร่องและช่องโหว่ของ CMS เพื่อแก้ไขช่องโหว่ที่เกิดขึ้นหรือระยะเวลาใช้ในการพัฒนาตัวปรับรุ่น (Patch) เพื่อแก้ไขช่องโหว่ที่เกิดขึ้นก็จะสามารถตอบสนองความต้องการได้มากกว่าเช่นกัน

3 พิจารณาจากแหล่งข้อมูลที่เกี่ยวกับการติดตั้ง การตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัย

CMS ที่ดีควรมีแหล่งข้อมูลเอกสารสนับสนุนที่เกี่ยวข้องกับการติดตั้ง ตั้งค่า และแนวทางการรักษาความมั่นคงปลอดภัยให้กับ CMS

รูปแบบการสื่อสารอย่างมั่นคงปลอดภัยระหว่างโปรแกรมค้นดูเว็บและเครื่องบริการเว็บ

โปรโตคอล SSL (Secure Socket Layer Protocol) และ **โปรโตคอล TLS (Transport Layer Security Protocol)** เป็นโปรโตคอลที่กำหนดรูปแบบการสื่อสารที่มีความมั่นคงปลอดภัย ซึ่งสามารถป้องกันการสื่อสารของโปรแกรมประยุกต์ในระบบรับ-ให้ (Client-Server System) จากการลอบฟัง (Eavesdropping) การแก้ไขให้เสียหาย (Tampering) และการปลอมแปลงข้อความที่ใช้ในการสื่อสาร (Message Forgery) โปรโตคอล SSL ถูกนำมาใช้งานครั้งแรกในปี 1994 โดย บริษัท Netscape Communications และที่ผ่านมาได้มีการปรับปรุงเพื่อแก้ไขปัญหาความมั่นคงปลอดภัยของโปรโตคอลไป 2 ครั้ง และเวอร์ชันสุดท้ายของ SSL คือเวอร์ชัน 3 ซึ่งถูกพัฒนาในปี 1996 ตามเอกสาร RFC 6101 ขณะที่โปรโตคอล TLS ถูกพัฒนาต่อยอดเพื่อแก้ไขปัญหาความมั่นคงปลอดภัยในโปรโตคอล SSL ในปี 1999 โดย IETF ซึ่งได้มีการกำหนดเป็นมาตรฐานและได้มีการพัฒนาปรับปรุงต่อเนื่องกันมาเป็น TLS เวอร์ชัน 1.2 ในปี 2008 ตาม RFC 5246 เป็นเวอร์ชันปัจจุบันที่ได้รับการยอมรับเรื่องความมั่นคงปลอดภัยมากที่สุด

อย่างไรก็ตามในปัจจุบันเครื่องบริการเว็บและโปรแกรมค้นดูข้อมูลเว็บไม่ได้รองรับโปรโตคอล SSL/TLS ทุกเวอร์ชัน ทั้งนี้ จากผลการสำรวจเว็บไซต์ทั่วไป เมื่อเดือนมกราคม พ.ศ. 2557 พบว่า เว็บไซต์มากกว่าร้อยละ 99 รองรับโปรโตคอล TLS 1.0 และ SSL 3.0 ในขณะที่เว็บไซต์ที่รองรับ TLS 1.1 และ TLS 1.2 มีจำนวนร้อยละ 23 และร้อยละ 25 ตามลำดับ

โปรโตคอล SSL/TLS
กำหนดรูปแบบการสื่อสารที่มีความมั่นคงปลอดภัย
ด้วยกระบวนการพื้นฐานที่สำคัญ 3 กระบวนการ

1 การยืนยันตัวตนของเครื่องบริการเว็บ

โปรโตคอล SSL/TLS อนุญาตให้ผู้ใช้บริการยืนยันเอกลักษณ์ของเครื่องบริการเว็บ (Web Server's Identity) โดยใช้เทคนิคของการเข้ารหัสโดยใช้กุญแจสาธารณะตรวจสอบใบรับรองอิเล็กทรอนิกส์ของเครื่องบริการเว็บ ว่าออกโดยผู้ให้บริการออกใบรับรองอิเล็กทรอนิกส์ที่น่าเชื่อถือหรือไม่ และใบรับรองอิเล็กทรอนิกส์ดังกล่าวยังสามารถใช้งานได้ไม่หมดอายุหรืออยู่ในรายการเพิกถอนใบรับรองอิเล็กทรอนิกส์

2 การยืนยันตัวตนของผู้ใช้บริการ

เครื่องบริการเว็บสามารถยืนยันเอกลักษณ์ของผู้ใช้บริการ ด้วยการตรวจสอบใบรับรองอิเล็กทรอนิกส์ของผู้ใช้บริการด้วยเทคนิคจองการเข้ารหัสโดยใช้กุญแจสาธารณะเช่นกัน ส่วนใหญ่แล้วในกรณีที่มีการยืนยันตัวตนของผู้ใช้บริการ ผู้ใช้บริการจะมีการยืนยันตัวตนของเครื่องบริการเว็บควบคู่กันไป ซึ่งเป็นการยืนยันตัวตนของทั้งสองฝ่าย (Mutual Authentication)

3 การเข้ารหัสข้อมูลที่ใช้ในการสื่อสาร

โปรโตคอล SSL/TLS สามารถใช้ในการเข้ารหัสข้อมูลที่ใช้รับส่งกันระหว่างเครื่องบริการเว็บและโปรแกรมค้นดูเว็บ โดยการเลือกกระบวนการเข้ารหัสข้อมูลที่มีความมั่นคงปลอดภัยเหมาะสมกับการสื่อสาร นอกจากนี้ยังสามารถตรวจสอบได้ว่าข้อมูลที่มีการรับส่งนั้นมีการแก้ไขหรือปลอมแปลงหรือไม่

เว็บไซต์ที่ไม่ได้มีการนำ SSL/TLS มาใช้งาน จะเปิดโอกาสให้ผู้ประสงค์ร้ายสามารถลอบฟัง แก้ไข และปลอมแปลงข้อมูลที่ใช้รับ-ส่งระหว่างเครื่องบริการเว็บ และผู้ใช้บริการได้

การเลือกเวอร์ชันของ SSL/TLS ที่เหมาะสม

1 โปรโตคอล SSL/TLS มีหลายเวอร์ชัน แต่ละเวอร์ชันมีคุณสมบัติด้านความมั่นคงปลอดภัยไม่เหมือนกัน ซึ่งในแต่ละเวอร์ชันของ SSL/TLS มีรายละเอียด ดังนี้

SSL เวอร์ชัน 2

มีความมั่นคงปลอดภัยต่ำ และปัจจุบันไม่มีการใช้งาน

SSL เวอร์ชัน 3

พัฒนามาจาก SSL เวอร์ชัน 2 แต่ในปัจจุบันหน่วยงานส่วนใหญ่ไม่นิยมใช้งาน SSL เวอร์ชัน 3 เนื่องจากไม่มีคุณสมบัติที่สำคัญบางอย่าง อีกทั้งผู้ใช้บริการส่วนใหญ่หันไปใช้งาน TLS เวอร์ชัน 1.0

TLS เวอร์ชัน 1.0

พัฒนามาจาก SSL เวอร์ชัน 3 คุณสมบัติส่วนใหญ่มีความมั่นคงปลอดภัย เมื่อใช้งานกับองค์ประกอบอื่น ๆ อย่างระมัดระวังผ่านโปรโตคอล HTTP

TLS เวอร์ชัน 1.1 / 1.2

แก้ปัญหาในด้านความมั่นคงปลอดภัยที่เป็นที่รู้จักทั้งหมด

อย่างไรก็ตาม ตามประกาศของ NIST SP 800-52r2 หน่วยงานจะต้องสนับสนุน TLS 1.3 ภายในวันที่ 1 มกราคม 2024 หลังจากวันดังกล่าว เซิร์ฟเวอร์ จะต้อง สนับสนุน TLS 1.3 สำหรับแอปพลิเคชันทั้งภาครัฐและพลเมืองหรือธุรกิจ โดยทั่วไปเซิร์ฟเวอร์ที่รองรับ TLS 1.3 น่าได้รับการกำหนดค่าให้ใช้ TLS 1.2 เช่นกัน อย่างไรก็ตาม TLS 1.2 อาจถูกปิดใช้งานบนเซิร์ฟเวอร์ที่รองรับ TLS 1.3 หากมีการพิจารณาว่า TLS 1.2 ไม่จำเป็นสำหรับการทำงานร่วมกัน

2 แนวทางการเลือกใช้เวอร์ชันของโปรโตคอล SSL/TLS มีดังนี้

TLS เวอร์ชัน 1.2

ควรนำมาใช้เป็นโปรโตคอลหลัก เนื่องจากเวอร์ชันนี้มีองค์ประกอบและมีการแก้ปัญหาในด้านความมั่นคงปลอดภัยที่ไม่มีในโปรโตคอลเวอร์ชันก่อน ๆ ซึ่งถ้าแพลตฟอร์มของเครื่องบริการเว็บไม่รองรับ TLS 1.2 ก็ให้วางแผนเพื่อปรับปรุง หรือถ้าบริการของผู้ให้บริการไม่รองรับก็ให้เสนอไปยังผู้ให้บริการนั้น ๆ ให้อัปเดตต่อไปในอนาคต

คำแนะนำขั้นต้น

เครื่องบริการเว็บต้องรองรับ TLS 1.0/TLS 1.1 เนื่องจากยังมีเครื่องผู้ใช้บริการใช้โปรโตคอลเวอร์ชันอื่น ๆ อย่างหลากหลาย ซึ่ง TLS ของทั้ง 2 เวอร์ชันนี้ จะสามารถรองรับความมั่นคงปลอดภัยในการใช้งานที่เพียงพอสำหรับเว็บไซต์

การเลือกวิธีการเข้ารหัสของ SSL/TLS ที่เหมาะสม

ในการติดต่อสื่อสารและแลกเปลี่ยนข้อมูลอย่างมั่นคงปลอดภัย จะต้องทำให้แน่ใจได้ว่าการติดต่อสื่อสารนั้นเกิดขึ้นโดยตรงระหว่างผู้ส่งข้อมูลและผู้รับข้อมูลที่ต้องการ และไม่มีการดักฟังข้อมูลโดยบุคคลอื่น ซึ่งในโปรโตคอล SSL และ TLS ได้มีการใช้ Cipher Suite สำหรับกำหนดระดับความมั่นคงปลอดภัยของการติดต่อสื่อสารที่เกิดขึ้น โดย Cipher Suite จะประกอบด้วยหน่วยโครงสร้างต่าง ๆ ที่นำมาประกอบกันทำให้เกิดความมั่นคงปลอดภัยในระดับต่าง ๆ ซึ่งสามารถปรับเปลี่ยนหน่วยโครงสร้างหน่วยใดหน่วยหนึ่งได้หากตรวจพบว่าไม่มีระดับความมั่นคงปลอดภัยเพียงพอ โดยโปรโตคอล SSL/TLS จะมีการใช้โปรโตคอล Handshake ในการตกลงวิธีการสื่อสารระหว่างเครื่องบริการเว็บและเครื่องรับบริการเว็บด้วยการเลือก Cipher Suite ไปใช้งาน เพื่อการยืนยันตัวตนของแต่ละฝ่าย การส่งใบรับรองอิเล็กทรอนิกส์ระหว่างกันและการสร้าง Session Key ต่าง ๆ ทั้งนี้ การเลือกวิธีการเข้ารหัสของ SSL/TLS ที่เหมาะสมนั้น ขึ้นอยู่กับหลายปัจจัยตามแต่ละองค์กร ซึ่งไม่จำเป็นจะต้องใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูงสุดเสมอไป

ปัจจัยเบื้องต้นในการเลือกใช้ขั้นตอนวิธีการเข้ารหัส

1 ความมั่นคงปลอดภัยที่ต้องการ

ความสำคัญของข้อมูล

ข้อมูลที่มีความสำคัญมากควรใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูง

ระยะเวลาของข้อมูล

ข้อมูลที่มีความสำคัญในระยะเวลาสั้น (เช่น หลักวันแทนที่จะเป็นหลักปี) สามารถใช้วิธีการเข้ารหัสที่มีระดับความมั่นคงปลอดภัยลดลงมาได้

ภัยคุกคามต่อข้อมูล

ข้อมูลที่มีภัยคุกคามสูงควรใช้วิธีการเขารหัสที่มีความมั่นคงปลอดภัยสูง

มาตรการป้องกันอื่น ๆ

สามารถใช้แทนเพื่อลดความจำเป็นในการใช้วิธีการเข้ารหัสที่มีความมั่นคงปลอดภัยสูง เช่น การเลือกใช้วิธีการติดต่อสื่อสารที่มีการป้องกัน โดยอาจเป็นการใช้งานอินเทอร์เน็ตแบบจำกัดขอบเขตแทนการใช้งานอินเทอร์เน็ตสาธารณะ

2 สมรรถนะที่ต้องการ (Required Performance)

โดยหากต้องการสมรรถนะที่สูง อาจจะต้องจัดหาทรัพยากรของระบบเพิ่มเติม หรืออาจจำเป็นต้องลดระดับความมั่นคงปลอดภัยของวิธีการเข้ารหัส

3 ทรัพยากรของระบบ

โดยหากมีทรัพยากร เช่น กระบวนการหรือหน่วยความจำไม่มาก ก็สามารถใช้วิธีการเข้ารหัสที่มีระดับความมั่นคงปลอดภัยลดลงมาได้

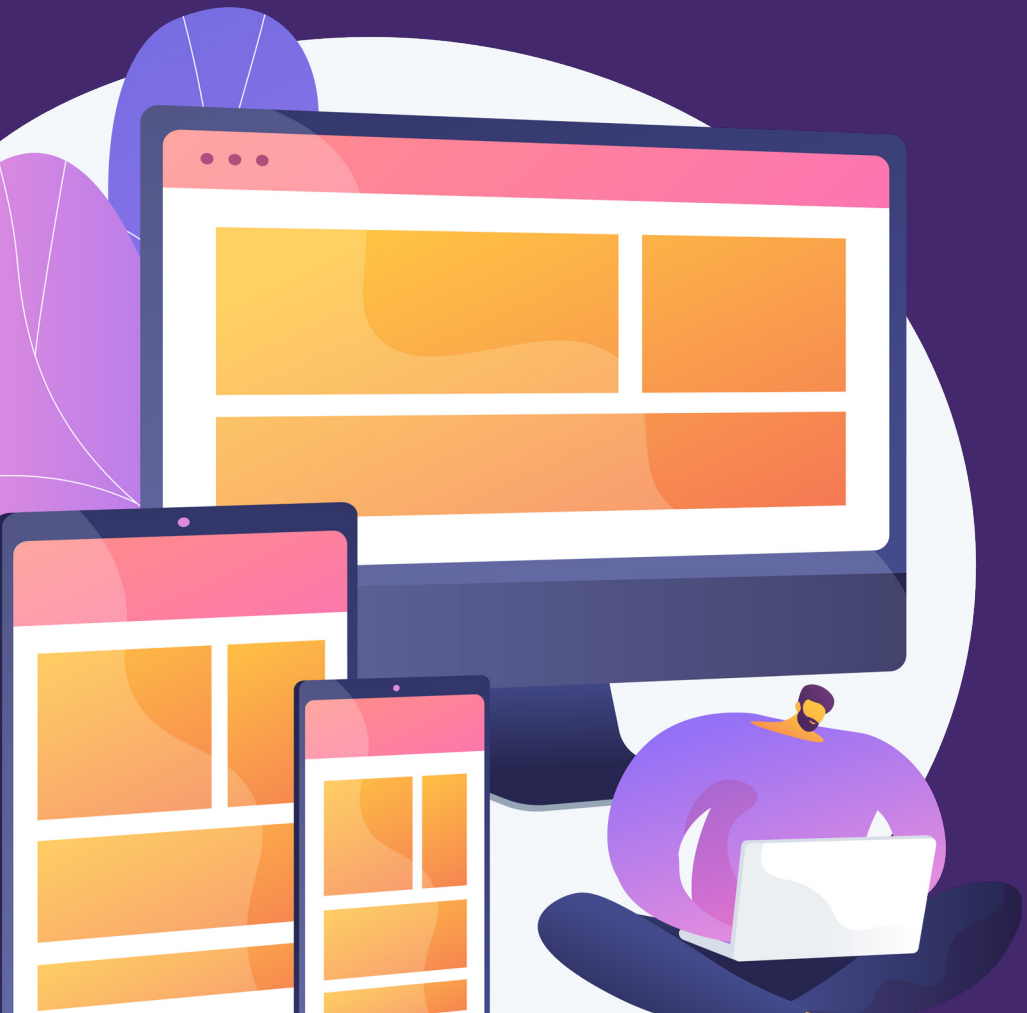
4 ข้อจำกัดด้านการนำเข้า การส่งออก และการใช้งานวิธีการเข้ารหัสของแต่ละประเทศ

5 การรองรับวิธีการเข้ารหัสแบบต่าง ๆ โดยโปรแกรมประยุกต์บนเว็บ

6 การรองรับวิธีการเข้ารหัสแบบต่าง ๆ โดยโปรแกรมค้นดูเว็บของผู้ใช้บริการเป้าหมาย

บทที่

2 การตั้งค่าความมั่นคงปลอดภัยเครื่องบริการเว็บ



หัวข้อเนื้อหาการเรียนรู้ที่ 1
การตั้งค่าโปรแกรมสำหรับการให้บริการเว็บไซต์

การติดตั้งและตั้งค่าโปรแกรมสำหรับให้บริการเว็บ (Web Server Software)

ซึ่งเป็นโปรแกรมที่มีผู้พัฒนาหลายรายและมีหลายรุ่น ทำให้ก่อนการติดตั้งโปรแกรมดังกล่าว ผู้ดูแลเครื่องบริการเว็บควรศึกษารายละเอียดของคู่มือการติดตั้ง (Installation Guideline) และการตั้งค่าพารามิเตอร์ต่าง ๆ ที่เกี่ยวข้อง เพื่อให้โปรแกรมดังกล่าวสามารถทำงานได้ตามความต้องการของผู้ให้บริการและมีความมั่นคงปลอดภัย

การติดตั้งเครื่องบริการเว็บควรทำให้เกิดความมั่นคงปลอดภัยมากที่สุด ผู้ดูแลเครื่องบริการเว็บควรศึกษาเอกสารและข้อมูลในการติดตั้งเครื่องบริการเว็บอย่างละเอียดก่อนที่จะทำการเริ่มติดตั้งจริง ซึ่งในระหว่างขั้นตอนการติดตั้งอาจมีการติดตั้งโปรแกรมหรือสคริปต์ (Script) ใด ๆ ที่ไม่จำเป็นถูกติดตั้งมาให้อย่างอัตโนมัติ ดังนั้น เมื่อพบข้อมูลใด ๆ ที่ไม่จำเป็น ผู้ดูแลเครื่องบริการควรลบออกไปทันที เพื่อไม่เป็นการเปิดช่องโหว่ให้ผู้ประสงค์ร้ายเข้ามาทำอันตรายแก่เครื่องบริการเว็บได้

ข้อกำหนดที่เกี่ยวข้องกับโปรแกรม
สำหรับให้บริการเว็บให้มีความมั่นคงปลอดภัย

1 ปรับปรุงส่วนประกอบของโปรแกรม

ปรับปรุงส่วนประกอบของโปรแกรมสำหรับให้บริการเว็บอย่างสม่ำเสมอ ส่วนใหญ่แล้วชุดปรับปรุง (Patch) จะเป็นโปรแกรมที่มีการแก้ไขข้อบกพร่อง หรือจุดอ่อนของโปรแกรมที่ตรวจพบ รวมถึงมีการพัฒนาประสิทธิภาพในการทำงานของโปรแกรมและระบบที่เกี่ยวข้องได้

2 ควบคุมข้อความแจ้งเตือน

ควบคุมข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาด (Error Message) ไม่ให้แสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย เนื่องจากผู้ประสงค์ร้ายสามารถใช้ข้อมูลจากข้อความแจ้งเตือนหรือข้อความแสดงข้อผิดพลาดเพื่อคาดเดาข้อมูลการตั้งค่าโปรแกรมและระบบที่เกี่ยวข้องได้

3 จัดหมวดหมู่ของสารบบ

จัดหมวดหมู่ของสารบบ (Directory) ที่ใช้เก็บไฟล์ข้อมูล เว็บเพจ ระบบปฏิบัติการ โปรแกรมสำหรับให้บริการเว็บ และโปรแกรมอื่น ๆ โดยจะต้องมีการกำหนดสิทธิ์ในการเข้าถึงสารบบที่เกี่ยวข้องทั้งหมดให้เหมาะสมกับการใช้งาน และคำนึงถึงความมั่นคงปลอดภัย

4 ตรวจสอบและจัดการลบ

ตรวจสอบและจัดการลบตัวอย่างโปรแกรม ตัวอย่างไฟล์ข้อมูล บัญชีผู้ใช้ที่ไม่ได้ใช้งาน เช่น บัญชีซึ่งมีการใช้งานระหว่างกระบวนการติดตั้งเครื่องบริการเว็บทั้งหมด อาทิ ไฟล์เอกสารที่มาจากบริษัทผู้ผลิตเครื่องบริการเว็บ ไฟล์ทดสอบ ไฟล์ตัวอย่างที่ติดตั้งจากเครื่องบริการเว็บ บัญชีผู้ใช้พื้นฐานที่เครื่องบริการเว็บสร้างขึ้น

5 ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้น

ตรวจสอบไม่ให้มีการใช้ค่าเริ่มต้นของชื่อสารบบ ชื่อไฟล์ข้อมูล ตำแหน่งไฟล์ข้อมูล รหัสผ่าน ที่มากับการติดตั้งเครื่องบริการเว็บ เนื่องจากผู้ประสงค์ร้ายมักจะใช้ค่าเริ่มต้นเหล่านี้เป็นข้อมูลเบื้องต้นในการโจมตีเครื่องบริการเว็บ

6 ควบคุมการเข้าถึงเครื่องบริการเว็บ

จำกัดหมายเลขไอพีปลายทางหรือยูอาร์แอลที่อนุญาตให้เครื่องบริการเว็บสามารถเชื่อมต่อ (Whitelist) ซึ่งจะช่วยให้ผู้ดูแลเครื่องบริการเว็บตรวจสอบพบความผิดปกติ หากพบว่ามีการเชื่อมต่อออกไปยังหมายเลขไอพีปลายทางหรือยูอาร์แอลที่ไม่ได้รับอนุญาต

7 ปิดบริการต่าง ๆ ที่ไม่จำเป็นบนเครื่องบริการเว็บ

โดยเฉพาะบริการประเภท Remote Access ส่วนใหญ่ เครื่องบริการเว็บไซต์มักมีการติดตั้งซอฟต์แวร์ต่าง ๆ มาให้กับผู้ดูแลเครื่องบริการเว็บ เพื่อเพิ่มความสะดวกสบายจากการเข้าจัดส่วนประกอบต่าง ๆ ของเว็บไซต์ ไม่ว่าจะเป็นบริการประเภท Remote Access เช่น Remote Desktop, VNC, SSH, Talent หรือบริการอื่น ๆ ที่มีความเกี่ยวข้องกับเว็บไซต์โดยตรง เช่น บริการฐานข้อมูล (Database) ตลอดจนบริการ FTP สำหรับจัดการไฟล์ของเว็บไซต์ การเปิดบริการต่าง ๆ ทิ้งไว้บนเครื่องบริการเว็บโดยไม่ได้ใช้งานก็เปรียบเสมือนการเปิดโอกาสให้ผู้ประสงค์ร้ายได้ทดสอบโจมตีหาช่องโหว่ตามช่องทางนั้น ๆ ซึ่งในกรณีที่รุนแรงมาก อาจถึงขั้นถูกผู้ประสงค์ร้ายเข้าถึงข้อมูลในเครื่องบริการเว็บในระดับสิทธิ์ของผู้ดูแลระบบก็เป็นได้

ข้อกำหนดหรือแนะนำแนวทางปฏิบัติ และให้คำปรึกษา การกำหนดค่าระบบบริหารจัดการเว็บไซต์ (CMS)

แนวทางในการพัฒนาเว็บไซต์มีด้วยกันหลากหลายวิธี ซึ่งการนำระบบบริหารจัดการเว็บไซต์มาประยุกต์ใช้ก็คือเป็นอีกหนึ่งทางเลือกที่ช่วยอำนวยความสะดวกในการพัฒนาและบริหารจัดการเว็บไซต์ ผู้ดูแลเครื่องบริการเว็บจึงจำเป็นต้องตั้งค่าองค์ประกอบบางอย่างก่อนที่จะใช้งานจริง เพื่อให้เว็บไซต์มีความมั่นคงปลอดภัยและป้องกันภัยคุกคามจากผู้ประสงค์ร้าย

ข้อกำหนดสำหรับการตั้งค่าระบบบริหารจัดการเว็บไซต์

1. ต้องมีการกำหนดสิทธิ์การใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ไฟล์ต่าง ๆ ให้เหมาะสมกับบทบาทหน้าที่ของผู้ใช้บริการ

2. ตรวจสอบว่ามีไฟล์หรือโปรแกรมเสริม (Plug-in Program) ที่ไม่จำเป็นหรือไม่ได้ใช้งานปรากฏอยู่หรือไม่ หากตรวจพบ ผู้ดูแลเครื่องบริการเว็บต้องลบหรือถอนการติดตั้งไฟล์ หรือโปรแกรมเสริมนั้นทันที

3. หมั่นตรวจสอบการอัปเดตเวอร์ชันของระบบบริหารจัดการเว็บไซต์อยู่เสมอ และอัปเดตเวอร์ชันให้เป็นปัจจุบัน โดยให้ดาวน์โหลดไฟล์จากเว็บไซต์หลักของผู้ให้บริการระบบบริหารจัดการเว็บไซต์เท่านั้น

4. ลบบัญชีผู้ใช้ที่มากับการติดตั้งระบบบริหารจัดการเว็บไซต์ เปลี่ยนชื่อผู้ใช้ของบัญชีผู้ใช้นั้น หรือเปลี่ยนรหัสผ่านของบัญชีผู้ใช้นั้น ให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัยแทน

5. เปลี่ยน Table Prefix ของฐานข้อมูลที่มาในระหว่างการติดตั้งระบบบริหารจัดการเว็บไซต์ เช่น ใน WordPress จะมีการใช้ Table Prefix ที่ขึ้นต้นด้วย wp_xxx ให้เปลี่ยนเป็นชื่ออื่น เนื่องจากอาจเป็นช่องทางให้ผู้ประสงค์ร้ายสามารถทราบถึงโครงสร้างและตารางในฐานข้อมูลได้

ข้อกำหนดหรือแนะนำแนวทางปฏิบัติ และให้คำปรึกษา

การกำหนดค่า Config ระบบฐานข้อมูล (Database system)

จากเอกสารเรื่อง Oracle Database Security Checklist ของ Oracle และ Making Database Security an IT Security Priority ของ SANS ที่กล่าวถึง แนวทางการรักษาความมั่นคงปลอดภัยของฐานข้อมูล นับว่ามีความน่าสนใจเป็นอย่างมาก เนื่องจากในกระบวนการทำงานของเครื่องบริการเว็บและเว็บไซต์นั้น จะต้องมีการเก็บข้อมูลต่าง ๆ ลงในฐานข้อมูลอยู่เสมอ ดังนั้น ผู้ดูแลเครื่องบริการเว็บจึงจำเป็นต้องตั้งค่าองค์ประกอบบางอย่างเพื่อรักษาความมั่นคงปลอดภัยของข้อมูล

ข้อกำหนดสำหรับการตั้งค่าฐานข้อมูล

1. ตั้งค่าฐานข้อมูล อนุญาตให้เฉพาะโปรแกรมประยุกต์ (Application) และเครื่องบริการเว็บที่เกี่ยวข้องเข้าถึงได้เท่านั้น
2. ควบคุมการเข้าถึงระบบฐานข้อมูลด้วยระบบรักษาความมั่นคงปลอดภัย เช่น ด่านกันบุกรุก หรือไฟร์วอลล์ (Firewall) เพื่อไม่ให้ผู้ใช้บริการทั่วไปเข้าถึงฐานข้อมูลได้
3. ตรวจสอบและปิดบริการ (Service) ที่ไม่จำเป็นหรือไม่ได้ใช้งานในระบบฐานข้อมูล
4. จัดให้มีการทบทวนบัญชีผู้ใช้ภายในฐานข้อมูลตามระยะเวลาที่กำหนด และลบบัญชีผู้ใช้ที่ไม่ได้มีการใช้งานออกจากระบบฐานข้อมูล
5. ปิดบัญชีผู้ใช้ที่มาพร้อมกับการติดตั้งฐานข้อมูล หรือเปลี่ยนรหัสผ่านของบัญชีดังกล่าวให้เป็นรหัสผ่านที่มีความมั่นคงปลอดภัย

6. กำหนดค่าติดตั้งระบบฐานข้อมูลเพื่อไม่อนุญาตให้ใช้งานรหัสที่มีค่าว่าง (Null Password)

7. ตรวจสอบและลบแฟ้มชั่วคราว (Temporary File) ที่ถูกสร้างขึ้นระหว่างการติดตั้งระบบฐานข้อมูล เนื่องจากไฟล์ข้อมูลดังกล่าวอาจจะมีข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย

8. ปรับปรุงเวอร์ชันของโปรแกรมระบบฐานข้อมูล หรืออัปเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดเสมอ เพื่อให้โปรแกรมมีความมั่นคงปลอดภัยมากที่สุด

9. กำหนดสิทธิ์การใช้งาน (Permission) และการควบคุมการเข้าถึง (Access Control) ให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้

10. รหัสผ่านที่เก็บในฐานข้อมูลต้องมีการเข้ารหัสเสมอ

ข้อกำหนดสำหรับการตั้งค่า Server-Side Script Engine

ปัจจุบันหลายเว็บไซต์ได้มีการใช้เทคโนโลยีในการพัฒนาเว็บไซต์แบบพลวัต (Dynamic Website) ซึ่งเนื้อหาในหน้าเว็บเพจเปลี่ยนแปลงได้ตามปัจจัยที่กำหนด โดยการพัฒนาหน้าเว็บเพจแบบพลวัตต้องอาศัยการใช้เทคโนโลยี Server-Side Script Engine เช่น PHP, ASP.NET, JSP ซึ่งผู้ดูแลเครื่องบริการเว็บต้องทำการตั้งค่าองค์ประกอบบางอย่างของ Server-Side Script Engine ให้มีความมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงของผู้ประสงค์ร้าย

ข้อกำหนดสำหรับการตั้งค่า Server-Side Script Engine

1. ควบคุมการเข้าถึงไฟล์หรือสารบบต่าง ๆ ให้เหมาะสมกับบทบาทของผู้ใช้งาน เช่น ไฟล์ Script หรือสารบบที่เก็บโปรแกรม ควรอนุญาตการเข้าถึงและให้สิทธิ์แก่ผู้ใช้งานที่เป็นเจ้าของไฟล์หรือนักพัฒนาซอฟต์แวร์เท่านั้น ผู้ใช้บริการทั่วไปจะได้รับสิทธิ์ในการอ่านแต่ไม่สามารถทำการแก้ไขได้ ส่วนผู้ดูแลเครื่องบริการเว็บได้รับสิทธิ์ทั้งการอ่าน เขียน และแก้ไขได้

2. ปรับปรุงเวอร์ชันของ Server-Side Script Engine หรืออัปเดต Patch จากบริษัทผู้พัฒนาซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุด เพื่อให้โปรแกรมมีความมั่นคงปลอดภัยมากที่สุด

3. กำหนดค่าติดตั้งไม่ให้ Server-Side Script Engine แสดงข้อมูลเวอร์ชันของ Server-Side Script Engine ที่เครื่องบริการเว็บใช้งานใน HTTP Header เนื่องจากอาจจะเป็นช่องทางให้ผู้ประสงค์ร้ายล่วงรู้เวอร์ชันที่เครื่องบริการเว็บใช้งาน และหาช่องโหว่เข้ามาทำอันตรายได้

4. กำหนดค่าติดตั้ง Server-Side Script Engine ไม่ให้มีการแสดงรายละเอียดของข้อความหรือแสดงข้อผิดพลาด (Error Message) หากจะต้องมีรายละเอียด ก็ควรแสดงข้องมูลที่จำเป็นและไม่เป็นประโยชน์กับผู้ประสงค์ร้าย

กรอบแนวคิดในการพัฒนาคน ด้าน Cybersecurity (NICE Framework)

ในปัจจุบันภัยคุกคามในโลกไซเบอร์มีความหลากหลายและล้ำหน้ามากขึ้น การที่จะรับมือกับภัยคุกคามเหล่านั้นได้อย่างมีประสิทธิภาพจำเป็นต้องมีการบริหารจัดการบุคลากรทางด้านไซเบอร์ โดยมีกรอบแนวคิดที่จะช่วยสนับสนุนคือ **“NICE Framework”**

NICE หรือ National Initiative for Cybersecurity Education เป็นแนวคิดที่ริเริ่มมาจากหน่วยงาน NIST หรือ National Institute of Standards and Technology ภายใต้การกำกับดูแลของกระทรวงพาณิชย์ ประเทศสหรัฐอเมริกา NICE เป็นความร่วมมือระหว่างหน่วยงานภาครัฐ เอกชน และสถาบันการศึกษา ที่มีจุดมุ่งหมายในการสร้างระบบเครือข่าย และส่งเสริมให้เกิดระบบนิเวศที่มีความเข้มแข็งให้กับการพัฒนากำลังคน การฝึกอบรม และการศึกษาในด้าน Cybersecurity โดยมีวิสัยทัศน์ในการสร้างมืออาชีพที่มีความเชี่ยวชาญด้าน Cybersecurity เพื่อป้องกันประเทศให้พ้นจากภัยคุกคาม รวมถึงสามารถแข่งขันได้ในเชิงเศรษฐกิจ NICE Framework อธิบายถึงหลักการ และแนวทางในการพัฒนากระบวนการ และวิธีปฏิบัติ เพื่อ “สรรหา คัดเลือก พัฒนา รวมถึงรักษาคนเก่งให้อยู่กับองค์กร”

แนวทางการพัฒนาคนด้าน Cybersecurity นั้นอาศัยองค์ประกอบหลัก ดังนี้

1 กลุ่มงาน (Categories)

หมายถึง กลุ่มงานหลักที่ครอบคลุมงานทางด้าน Cybersecurity ขององค์กร เช่น กลุ่มงานกำกับดูแล (Oversee and Govern – OV)

2 สายงานความเชี่ยวชาญ (Specialty Areas)

หมายถึง ขอบเขตความเชี่ยวชาญจำเพาะที่เกี่ยวข้องกันในแต่ละกลุ่มงานหลักของด้าน Cybersecurity เช่น กลุ่มงานกำกับดูแล (Oversee and Govern – OV) จะมีงานตามความเชี่ยวชาญ ประกอบด้วย งานด้านการให้คำปรึกษา และสนับสนุนทางกฎหมายที่เกี่ยวข้อง (Legal Advice and Advocacy - LGA) งานบริหารจัดการความปลอดภัยทางไซเบอร์ (Cybersecurity Management - MGT) และงานนโยบายและการวางแผนกลยุทธ์ (Strategic Planning and Policy – SPP)

3 บทบาทหน้าที่ (Work Roles)

ตำแหน่งงานตามความเชี่ยวชาญ เช่น ตำแหน่งผู้จัดการการรักษาความปลอดภัยระบบข้อมูลสารสนเทศ (Information Systems Security Manager) เป็นตำแหน่งงานที่อยู่ภายใต้ความเชี่ยวชาญของงานบริหารจัดการความปลอดภัยทางไซเบอร์ (Cybersecurity Management - MGT)

4 งาน (Task)

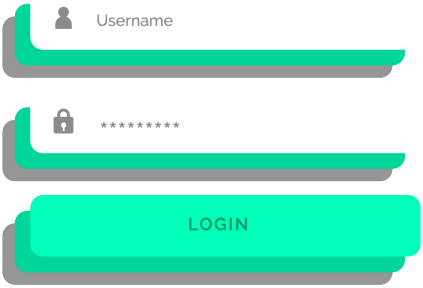
ภาระหน้าที่ที่แต่ละตำแหน่งงานจะต้องรับผิดชอบ เช่น ภาระหน้าที่ที่ผู้จัดการการรักษาความปลอดภัยระบบข้อมูลสารสนเทศ (Information Systems Security Manager) จะต้องรับผิดชอบ ได้แก่ การบริหารจัดการงบประมาณในการจัดทำโครงการให้มีประสิทธิภาพ การให้คำแนะนำแก่ฝ่ายบริหารในประเด็นระดับความเสี่ยง และความปลอดภัยของระบบข้อมูลสารสนเทศ เป็นต้น

5 ความรู้ ทักษะ และความสามารถ

ที่จำเป็นต้องใช้ในตำแหน่งงานนั้น ๆ ประกอบด้วย

ความรู้ (Knowledge): ชุดข้อมูลที่นำไปประยุกต์ใช้โดยตรงกับงานในแต่ละตำแหน่ง
ทักษะ (Skill): ความสามารถที่สังเกตเห็นได้จากการฝึกปฏิบัติในสิ่งที่ได้เรียนรู้มา
ความสามารถ (Ability): ความสามารถในการแสดงพฤติกรรมที่นำไปสู่ผลลัพธ์ที่จับต้องได้

หัวข้อเนื้อหาการเรียนรู้ที่ 2
รหัสผ่านและเทคโนโลยีการพิสูจน์ตัวตน



การกำหนดและรักษารหัสผ่าน

การเข้าใช้งานระบบต่าง ๆ ของเว็บไซต์ในปัจจุบัน เครื่องบริการเว็บจำเป็นที่จะต้องตรวจสอบและยืนยันตัวตนของผู้ใช้บริการว่าเป็นบุคคลที่ได้รับอนุญาตหรือไม่ โดยส่วนมากมักใช้ชื่อบัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) ในการตรวจสอบ ซึ่งการเข้าสู่ระบบด้วยชื่อบัญชีผู้ใช้และรหัสผ่านนั้นมีความเสี่ยงสูงต่อการถูกโจมตีจากผู้ประสงค์ร้าย และปัจจัยที่จะทำให้การโจมตีสำหรับหรือไม่นั้นมักขึ้นอยู่กับการกำหนดรหัสผ่านของผู้ใช้บริการเป็นหลัก ซึ่งหากผู้ใช้บริการกำหนดรหัสผ่านที่ไม่มีความมั่นคงปลอดภัยก็เท่ากับเป็นการเปิดโอกาสให้ผู้ประสงค์ร้ายคาดเดารหัสผ่านและข้อมูลถึงข้อมูลที่เป็นความลับของผู้ใช้บริการได้โดยง่าย และก่อให้เกิดผลกระทบมากมาย เช่น การทำธุรกรรมออนไลน์ หากมีผู้ประสงค์ร้ายสุ่มชื่อบัญชีและรหัสผ่านของผู้ใช้งานได้ ก็สามารถปลอมตัวเสมือนว่าเป็นผู้ใช้บริการเองเข้าไปทำธุรกรรมใด ๆ ได้อย่างอิสระ

รูปแบบในการโจมตีเพื่อดักเอารหัสผ่านของผู้ใช้มี 2 วิธี คือ Dictionary Attack และ Brute Force Attack การโจมตีรหัสผ่านแบบ Dictionary Attack เป็นการสุ่มเดาข้อมูลหรือรหัสผ่านจากคำศัพท์ที่อยู่ใน Dictionary และคำศัพท์ที่พบบ่อยซึ่งเรียกว่า “Word List” ในขณะที่การโจมตีรหัสผ่านแบบ Brute Force Attack จะเป็นวิธีการโจมตีด้วยการสุ่มข้อมูลหรือรหัสผ่านโดยคาดเดารหัสผ่านตามทุกความเป็นไปได้ของตัวอักษรในแต่ละหลัก ผู้ประสงค์ร้ายอาจเป็นผู้เดาสุ่มเองหรืออาจจะใช้โปรแกรมอัตโนมัติทำงานเพื่อเดาสุ่ม ซึ่ง Brute Force Attack สามารถหารหัสผ่านที่ถูกต้องได้ เพียงแต่ขึ้นอยู่กับระยะเวลาของการเดาสุ่มที่จะมากหรือน้อยขึ้นอยู่กับความซับซ้อนการของตั้งรหัสผ่าน

คำแนะนำที่เกี่ยวกับการจัดการรหัสผ่านให้มีความมั่นคงปลอดภัย

1 ตั้งค่ารหัสผ่านให้มีความมั่นคงปลอดภัย (Strong Password)

โดยรหัสผ่านควรประกอบด้วยตัวอักษรทั้งตัวเล็กตัวใหญ่ผสมกัน มีตัวเลขและสัญลักษณ์พิเศษอย่างน้อย 1 หลัก และต้องมีความยาวทั้งหมดไม่น้อยกว่า 8 หลัก

2 กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

จะช่วยลดโอกาสจากการถูกคาดเดารหัสผ่าน

3 ไม่กำหนดรหัสผ่านที่ไม่มีการเข้ารหัสลับบนเครื่องบริการเว็บ

หากจำเป็นต้องมีการเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด เช่น AES หรือ Triple DES และหากมีการเก็บอยู่ในรูปแบบของค่าแฮช (Hash Value) ควรใช้ขั้นตอนวิธี (Algorithm) ตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนดไว้ เช่น SHA-224 SHA-256 SHA-384 SHA-512

เทคโนโลยีการพิสูจน์ตัวบุคคล

การพิสูจน์ตัวตน คือ ขั้นตอนการยืนยัน (identify) ความถูกต้องของการเป็นบุคคลที่กล่าวอ้างจริง ในทางปฏิบัติจะแบ่งออกเป็น 2 ขั้นตอน

1 **การระบุตัวตน (Identification)**

คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น ชื่อผู้ใช้ (username)

2 **การพิสูจน์ตัวตน (Authentication)**

คือ ขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้าง การพิสูจน์ตัวตนจัดเป็นการตรวจสอบหลักฐานขั้นพื้นฐานที่สำคัญที่สุดของการควบคุมความปลอดภัย ดังนั้น การพิสูจน์ตัวตนที่ดีจะช่วยเพิ่มความมั่นคงปลอดภัยขั้นพื้นฐานให้กับระบบมากยิ่งขึ้น

กลไกของการพิสูจน์ตัวตน (Authentication mechanisms)

Possession factor

เช่น กุญแจหรือเครดิตการ์ด

Knowledge factor

เช่น รหัสผ่าน (passwords) หรือการใช้พิน (PINs)

Biometric factor

เช่น ลายนิ้วมือรูปแบบเรตินา (retinal patterns) หรือใช้รูปแบบเสียง (voice patterns)

การยืนยันตัวตนหลายขั้นตอน

(Multi-Factor Authentication)

คือ การใช้ปัจจัยหลาย ๆ อย่างในการตรวจสอบและยืนยันตัวบุคคล เพื่ออนุญาตเข้าใช้งานซอฟต์แวร์ ระบบ หรือข้อมูลต่าง ๆ โดยทั่วไประบบ MFA จะเป็นการใช้เครื่องมือตั้งแต่ 2 อย่างขึ้นไปในการตรวจสอบและยืนยันความถูกต้อง ดังนี้

1. **What you know (สิ่งที่คุณรู้)**
   เช่น password รหัสประจำตัว หรือคำถามเฉพาะเพื่อกู้รหัสผ่าน

2. **What you have (สิ่งที่คุณมี)**
   เช่น บัตรสมาร์ตการ์ด FIDO token, one-time password (OTP), อุปกรณ์บลูทูท, Apple Watch หรือ authenticator device อื่น ๆ

3. **Who you are (สิ่งที่คุณเป็น)**
   เช่น ลายนิ้วมือ หรือระบบจดจำใบหน้า

4. **What you do and where you are (สิ่งที่คุณทำ หรือที่ที่คุณอยู่)**
   เช่น การระบุที่อยู่ โดยใช้ GPS, IP Address หรือ Integrated Windows Authentication (IWA) และพฤติกรรมนิสัยการพิมพ์ (keystroke biometrics)

ประโยชน์ที่เห็นได้ชัดของ multi-factor authentication นั่นก็คือ **"ความปลอดภัยที่สูงขึ้น"** การเพิ่มเครื่องมือหรือปัจจัยในการรับรองความถูกต้องเข้าด้วยกัน เช่น การใช้ password, hardware token และ biometric เพื่อรับรองความถูกต้องของผู้ใช้งาน สามารถลดความเสี่ยงการละเมิดการเข้าถึงข้อมูลและซอฟต์แวร์ลงได้เป็นอย่างมาก

อย่างไรก็ตาม ในขณะที่ MFA มีประโยชน์อย่างมากในการใช้งานเพื่อความปลอดภัยในการยืนยันผู้ใช้งานเข้าระบบ ในหลายครั้งก็มักจะตามมาซึ่งความยุ่งยากในการบริหารจัดการและการใช้งาน ผู้ใช้งานจำเป็นต้องจัดเตรียม factor ที่สอง (อย่างแรกคือสิ่งที่รู้ หรือจำได้) สำหรับบางผู้ใช้งาน การต้องจัดเตรียมโทรศัพท์สมาร์ตโฟนเพื่อรับ one-time password (OTP) ผ่าน SMS อาจจะเป็นข้อจำกัด แต่ถึงอย่างนั้น MFA ก็ยังคงเป็นรูปแบบที่ปลอดภัยที่สุดสำหรับองค์กรในการล็อกระบบเครือข่ายหรือแอปพลิเคชันจากการเข้าถึงที่ไม่ได้รับอนุญาต

การยืนยันตัวตนด้วยชีวมิติ

(Biometric Authentication)

Biometric เป็นการศึกษาคุณลักษณะที่ไม่สามารถเปลี่ยนแปลงได้ ที่มีลักษณะเฉพาะตัวบุคคล เช่น ลายพิมพ์นิ้วมือ หรือม่านตา Biometric จะสามารถประยุกต์ใช้ได้หลากหลายที่ เช่น บริษัท รัฐบาล การควบคุมเขตแดน โรงพยาบาล และธนาคาร เพื่ออนุญาตให้บุคคลเข้าถึงพื้นที่จำกัด พื้นที่เฉพาะ ไฟล์เฉพาะ เขตแดนเฉพาะ หรือยืนยันตัวตนเพื่อเข้าถึงข้อมูลที่ทำการเก็บไว้ เช่น ข้อมูลอาชญากร

กระบวนการพิสูจน์ตัวตนนั้นจะนำ 3 ลักษณะข้างต้นมาใช้ในการยืนยันหลักฐานที่นำมากล่าวอ้าง ทั้งนี้ขึ้นอยู่กับระบบ วิธีการที่นำมาใช้เพียงลักษณะอย่างใดอย่างหนึ่ง (Single-factor authentication) นั้นมีข้อจำกัดในการใช้ ตัวอย่างเช่น Possession factor นั้น อาจจะสูญหายหรือถูกขโมยได้ Knowledge factor อาจจะถูกดักฟัง เดา หรือขโมยจากเครื่องคอมพิวเตอร์ Biometric factor จัดได้ว่าเป็นวิธีที่มีความปลอดภัยสูง อย่างไรก็ตามการที่จะใช้เทคโนโลยีนี้ได้นั้นจำเป็นต้องมีการลงทุนที่สูงด้วยเช่นกัน

ดังนั้น จึงได้มีการนำแต่ละคุณลักษณะมาใช้ร่วมกัน (multi-factor authentication) ตัวอย่างเช่น ใช้ Possession factor กับ Knowledge factor มาใช้ร่วมกัน เช่น การใช้ลายมือชื่อร่วมกับการใช้บัตรเครดิต หรือการใช้รหัสผ่านร่วมกับการใช้บัตร ATM การนำแต่ละลักษณะของการพิสูจน์ตัวตนมาใช้ร่วมกันมากกว่า 1 ลักษณะ จะช่วยเพิ่มประสิทธิภาพในการรักษาความปลอดภัยของข้อมูล

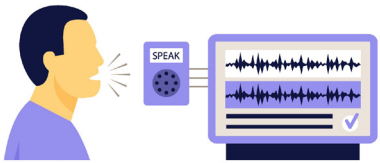
วิธีพิสูจน์ตนด้วย Biometric สามารถแบ่งได้เป็น 2 ประเภท

1 แบบที่ตรวจสอบจากลักษณะทางกายภาพ

ดูจากอัตลักษณ์ หรือลักษณะเฉพาะของร่างกายอย่างเช่น ลายนิ้วมือ ม่านตา เรตินา รวมทั้งหน้าตาและลายมือด้วย

2 การตรวจสอบจากพฤติกรรม

จากรูปแบบการกดคีย์บอร์ด ลายเซ็น และเสียง ลักษณะการทำงานของระบบ Biometric นั้นคือ ตัวเซนเซอร์จะอ่านข้อมูลดิจิทัลเกี่ยวกับ Biometric เข้ามา เช่น รูปร่างของมือของผู้ใช้ จากนั้นข้อมูลจากเซนเซอร์ก็จะได้รับการประมวลผล และมีการดึงเอาคุณลักษณะพิเศษที่ไม่เหมือนกันของแต่ละคนออกมา เช่น ขนาดของนิ้วและมือ จากนั้นข้อมูลเกี่ยวกับคุณลักษณะพิเศษนี้จะถูกใช้ในการสร้างเทมเพลต ซึ่งเป็นการสังเคราะห์ข้อมูลชิ้นใหม่ เพื่อใช้แทนตัวลายนิ้วมือจริง ๆ ที่อ่านได้จากเซนเซอร์ จากนั้น การพิสูจน์ตัวตนก็จะเปรียบเทียบเทมเพลตที่สร้างขึ้นมาใหม่นี้กับไฟล์ที่มีอยู่แล้ว ถ้าเหมือนก็จะอนุญาตหรือ accept แต่ถ้าไม่เหมือนก็จะทำการปฏิเสธ หรือ reject



บทที่

3 ใช้โปรแกรมประยุกต์ความมั่นคงปลอดภัยบนเครื่องบริการเว็บเพื่อให้บริการ

หัวข้อเนื้อหาการเรียนรู้ที่ 1
การโจมตีในระบบสารสนเทศจากเทคนิคต่าง ๆ

SQL Injection

เว็บไซต์ส่วนใหญ่ใช้คำสั่ง SQL ในการเชื่อมต่อฐานข้อมูล ผู้ประสงค์ร้ายสามารถแทรกคำสั่ง SQL ผ่านพารามิเตอร์ต่าง ๆ ของเว็บไซต์ เช่น GET POST ทำให้สามารถดำเนินการใด ๆ ก็ตามในฐานข้อมูลได้ โดยหากการโจมตีด้วยเทคนิคสำเร็จ จะทำให้ผู้ประสงค์ร้ายสามารถเข้าถึง แก้ไขเปลี่ยนแปลง ลบข้อมูลในฐานข้อมูล หรือสั่งปิดฐานข้อมูลได้ ซึ่งเว็บไซต์ที่เชื่อมต่อฐานข้อมูลโดยตรงหรือมีการเรียกฐานข้อมูลทุกครั้งที่เรียกหน้าเว็บเพจจะต้องระมัดระวังช่องโหว่นี้เป็นพิเศษ (ฐานข้อมูลที่ใช้กันโดยทั่วไป ได้แก่ MySQL, PostgreSQL, Oracle, Microsoft SQL Server และ DB2) ซึ่งช่องโหว่นี้เรียกว่า “SQL Injection Vulnerability” และการโจมตีที่อาศัยช่องโหว่นี้ เรียกว่า “SQL Injection Attack” แต่ในปัจจุบันมีฐานข้อมูลประเภท NoSQL ซึ่งไม่ได้ใช้คำสั่ง SQL ในการเข้าถึงข้อมูลในฐานข้อมูล ทำให้มีความปลอดภัยจากการโจมตีด้วยเทคนิคนี้มากขึ้น

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาศัยช่องโหว่นี้ในการดำเนินการ ดังนี้

1.1 เรียกดูข้อมูลลับ (Sensitive Data) ที่เก็บในฐานข้อมูล เช่น การเปิดเผยข้อมูลส่วนบุคคลของผู้ใช้บริการ

1.2 เพิ่ม เปลี่ยนแปลง ลบ ข้อมูลที่เก็บในฐานข้อมูล เช่น เปลี่ยนแปลงข้อมูลหน้าเว็บเพจ เปลี่ยนรหัสผ่านของผู้ใช้บริการ หรือใช้คำสั่งปิดฐานข้อมูล

1.3 หลีกเลี่ยงการยืนยันตัวตนจากระบบ Login (Login Authentication Bypass) เช่น สามารถดำเนินการคำสั่งภายใต้บัญชีผู้ใช้ที่ไม่ได้รับอนุญาตได้ โดยไม่ผ่านกระบวนการยืนยัน

1.4 อัปโหลดข้อมูลขึ้นไปยังเว็บไซต์หรือฐานข้อมูลได้

1.5 ส่งคำสั่งโดยตรงต่อระบบปฏิบัติการได้ เช่น การสั่งให้เครื่องบริการเว็บเปิดหรือปิด Firewall ของเครื่องบริการเว็บนั้น

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

โปรแกรมประยุกต์บนเว็บต้องมีการจัดทำ Prepared Statement และ/หรือ Stored Procedure – เป็นวิธีการที่จะแยกคำสั่งในการประมวลผล และค่าที่จะนำไปประมวลผลออกจากกัน จากวิธีการดังกล่าวจะช่วยป้องกันการโจมตีด้วยวิธีการ SQL Injection ได้

ไม่ควรเขียนคำสั่ง SQL โดยตรงในตัวแปร (Parameter) ที่ส่งโดยตรงไปยังโปรแกรมประยุกต์บนเว็บ เพราะจะนำไปสู่ความเสี่ยงที่ผู้ประสงค์ร้ายจะสามารถปลอมแปลงค่าตัวแปรและกระทำการใด ๆ โดยตรงกับฐานข้อมูลได้

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

ควบคุมการแสดงผลข้อมูล Error Message - ถ้า Error Message แสดงข้อมูลที่เกี่ยวข้องกับฐานข้อมูล เช่น ชื่อฐานข้อมูล ตารางฐานข้อมูล หรือคำสั่ง SQL ที่เป็นสาเหตุของการผิดพลาด ทำให้ผู้ประสงค์ร้ายสามารถนำข้อมูลเหล่านี้ไปใช้ประโยชน์ในการโจมตีเว็บไซต์ในอนาคตได้

กำหนดสิทธิ์ขั้นต่ำให้บัญชีผู้ใช้ของฐานข้อมูล – หากกำหนดสิทธิ์ของบัญชีผู้ใช้ที่สามารถเข้าถึงฐานข้อมูลมากเกินจำเป็น จะทำให้ความเสียหายที่เกิดจากการถูกโจมตีมีมากขึ้น ดังนั้น ควรกำหนดสิทธิ์ของบัญชีผู้ใช้ที่เข้าถึงฐานข้อมูลให้น้อยที่สุดแค่ที่เพียงพอกับการใช้งาน

3 การทดสอบความมั่นคงปลอดภัย

โดยปกติแล้วการพัฒนาโปรแกรมประยุกต์จะสร้างคำสั่ง SQL จาก SQL Syntax ซึ่งจะมีการรับค่าที่ได้จากโปรแกรมค้นดูเว็บ (Web Browser) มาใช้ในคำสั่ง SQL เช่น Select * from users where id=$id; ซึ่งจากตัวอย่างข้างต้น ตัวแปร $id จะรับข้อมูลจากโปรแกรมค้นดูเว็บฝั่งผู้ใช้บริการ แต่ส่วนที่เหลือเป็น Static ที่เขียนโดยผู้พัฒนาโปรแกรมประยุกต์บนเว็บ

ในกรณีปกติ ผู้ใช้บริการส่ง $id=10 คำสั่ง SQL จะเป็น “Select * from users where id=10;” ระบบจะคืนค่าข้อมูลที่มี id=10 ออกมา ซึ่งผู้ประสงค์ร้ายสามารถเปลี่ยนแปลง SQL โดยเพิ่ม “or 1=1” ที่ประโยค where เป็น “Select * from users where id=10 or 1=1;” ซึ่งเมื่อนำคำสั่งไปประมวลผลจะเป็นจริงในทุกกรณี โปรแกรมประยุกต์ก็จะแสดงข้อมูลที่ดึงจากฐานข้อมูลออกมา โดยการทดสอบนั้นพยายามป้อนค่าทดสอบเข้าไปเพื่อค้นหาข้อผิดพลาด

OS Command Injection

หากผู้พัฒนาโปรแกรมประยุกต์มีการใช้คำสั่ง OS Command เช่น exex(), Passthru(), shell_exec(), system(), popen() ร่วมกับการพัฒนาโปรแกรมประยุกต์บนเว็บ ก็จะเป็นช่องโหว่ที่ทำให้ผู้ประสงค์ร้ายโจมตีผ่านคำสั่งระดับระบบปฏิบัติการ (OS Command) เพื่อสั่งดำเนินการใด ๆ ผ่านโปรแกรมประยุกต์บนเว็บที่มีช่องโหว่ได้ ซึ่งจะนำไปสู่การรั่วไหลของข้อมูลที่สำคัญ การเข้าควบคุมเครื่องบริการเว็บ หรือใช้เป็นฐานเพื่อโจมตีเครื่องบริการเว็บอื่น ๆ

เว็บไซต์ใดก็ตามที่ใช้คำสั่ง OS Command เช่น exex(), Passthru(), shell_exec(), system(), popen() ในภาษา PHP ร่วมกับการพัฒนาโปรแกรมประยุกต์ ก็จะเป็นช่องโหว่ที่ทำให้ผู้ประสงค์ร้ายโจมตีโปรแกรมประยุกต์บนเว็บ โดยการสั่ง Run คำสั่ง OS Command เพื่อสั่งดำเนินการกับระบบผ่านโปรแกรมประยุกต์บนเว็บ ซึ่งช่องโหว่นี้เรียกว่า “OS Command Injection Vulnerability” และการโจมตีที่อาศัยช่องโหว่นี้เรียกว่า “OS Command Injection Attack”

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาศัยช่องโหว่นี้ในการดำเนินการ ดังนี้

1.1 เรียกดูข้อมูลลับ (Sensitive Data) หรือลบไฟล์ที่เก็บในเครื่องบริการเว็บ

1.2 เข้าจัดการและควบคุมเครื่องบริการเว็บ เพื่อใช้เป็นฐานโจมตีเครื่องบริการเว็บอื่น ๆ

1.3 ดาวน์โหลดและสั่งดำเนินการโปรแกรมหรือสคริปต์อันตราย

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

พัฒนาโปรแกรมประยุกต์บนเว็บ โดยให้ปิดการใช้งานคำสั่งต่าง ๆ เพื่อป้องกันการเรียกใช้ที่ไม่พึงประสงค์ เช่น ผู้ประสงค์ร้ายอัปโหลดไฟล์ Backdoor

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

หากจำเป็นต้องพัฒนาฟังก์ชันในโปรแกรมประยุกต์โดยใช้คำสั่ง OS Command ผู้พัฒนาโปรแกรมประยุกต์ต้องตรวจสอบ Variables ที่จะใช้กับตัวแปรของ OS Command ก่อนนำไปประมวลผล และต้องให้มั่นใจได้ว่า Execute แค่ค่าเท่านั้น (ถ้าเราจะใช้ OS Command ต้อง Clean ก่อนโดยการใช้ฟังก์ชันเข้าช่วย)

3 การทดสอบความมั่นคงปลอดภัย

OS Command Injection เป็นการโจมตีที่ดำเนินการผ่านหน้าเว็บไซต์เพื่อสั่งดำเนินการใด ๆ กับเครื่องบริการเว็บ เช่น ผู้ประสงค์ร้ายสามารถทำการอัปโหลดโปรแกรมอันตราย หรือดักเอารหัสผ่านได้

วิธีการทดสอบเบื้องต้น เช่น ในภาษา PHP สามารถใช้ Semicolon (;) เพื่อระบุว่าจบส่วนที่เป็น URL และตามด้วยคำสั่ง OS Command โดยคำสั่ง ‘%3B’ คือรหัสของ Semicolon ที่เข้ารหัสเรียบร้อยแล้ว

Unchecked Path Parameter / Directory Traversal

ผู้ประสงค์ร้ายเรียกชื่อไฟล์หรือข้อมูลที่เก็บบนเครื่องบริการเว็บได้โดยตรงผ่าน External Parameter เช่น ใส่คำสั่ง ?file=../../secret.txt ต่อท้าย URL ของเว็บไซต์ ก็จะเป็นการระบุชื่อไฟล์ที่ต้องการพร้อม Path ไฟล์ ทำให้ผู้ประสงค์ร้ายสามารถเข้าถึงไฟล์ที่อยู่บนเครื่องบริการเว็บโดยไม่ได้รับการอนุญาตได้ ซึ่งช่องโหว่นี้เรียกว่า “Directory Traversal Vulnerability” และการโจมตีในลักษณะนี้ เรียกว่า “Directory Traversal Attack”

ไม่ว่าเว็บไซต์ประเภทใดก็อาจตกเป็นเหยื่อได้ ถ้าโปรแกรมประยุกต์บนเว็บอนุญาตให้ระบุชื่อไฟล์ได้ด้วย External Parameter และถ้าเครื่องบริการเว็บของท่านเก็บข้อมูลที่เป็นความลับ เช่น ข้อมูลส่วนบุคคล ก็มีความเสี่ยงที่จะถูกผู้ประสงค์ร้ายเรียกเอาข้อมูลดังกล่าวไปได้

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาศัยช่องโหว่นี้ในการดู จัดการ ลบไฟล์ ในเครื่องบริการเว็บหรือในฐานข้อมูลได้

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

ไม่อนุญาตให้ใส่ Filename เพื่อระบุถึงข้อมูลได้จาก External Parameter เมื่อโปรแกรมประยุกต์บนเว็บอนุญาตให้ใส่ Filename เพื่อระบุถึงข้อมูลได้จาก External Parameter ผู้ประสงค์ร้ายจะสามารถเข้าถึงและดำเนินการใด ๆ ได้อย่างง่ายดาย และสามารถดูข้อมูลทั้งหมดที่ไม่ควรเปิดเผยแก่บุคคลภายนอกได้

ใช้ Fixed Directory ในการจัดการระบุชื่อไฟล์

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

กำหนด Permission การเข้าถึงไฟล์บนเครื่องบริการเว็บให้เหมาะสม และเครื่องบริการเว็บควรป้องกันการโจมตีได้ เมื่อโปรแกรมประยุกต์บนเว็บใด ๆ เรียกไฟล์ในเครื่องบริการเว็บโดยไม่ได้รับอนุญาต

ตรวจสอบ Filename เช่น มีการแปล String ที่ระบุ Directory ได้

Improper Session Management

การเข้าถึงเว็บไซต์ใด ๆ ของผู้ใช้บริการ วิธีในการตรวจสอบและยืนยันตัวตนของผู้ใช้บริการที่หลายเว็บไซต์นิยมใช้ คือ สร้าง Session ID ขึ้นหลังจากกระบวนการยืนยันตัวตนของผู้ใช้บริการสำเร็จ โดย Session ID นี้ จะถูกนำไปใช้ในการอ้างอิงและตรวจสอบสิทธิ์ในการเข้าถึงหน้าเว็บเพจต่าง ๆ ที่ผู้ใช้บริการเข้าเยี่ยมชม และ Session ID นี้ จะถูกใช้จนกว่าผู้ใช้บริการจะปิดหน้าต่างโปรแกรมค้นดูเว็บถึงจะทำการลบ Session ID นั้น ซึ่งจะไม่สามารถใช้ Session ID เดิมในการอ้างอิงได้อีก จากลักษณะการทำงานดังกล่าวทำให้เครื่องบริการเว็บสามารถติดตามข้อมูลทางฝั่งผู้ใช้บริการได้ตลอดตราบเท่าที่โปรแกรมค้นหาเว็บยังไม่ถูกปิด ทำให้ผู้ประสงค์ร้ายสามารถอาศัยช่องโหว่นี้ในการโจมตีเว็บไซต์ด้วยวิธี Session Hijack

หากเว็บไซต์ของท่านมีการให้บริการที่เกี่ยวข้องกับข้อมูลที่เป็นความลับและมีความแข่งขันสูง เช่น เว็บไซต์ที่ให้บริการชำระเงินทางอิเล็กทรอนิกส์ เช่น Internet Banking, Online Trading หรือ e-Commerce เว็บไซต์ที่มีข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับไม่สามารถเปิดเผยต่อบุคคลที่สามได้เด็ดขาด เช่น Job-Hunting Website, Internal Community Website หรือ Webmails เว็บไซต์ที่มีระบบการยืนยันตัวตนเพื่อเข้าใช้งานระบบ เช่น การยืนยันตัวตนเพื่อเข้าใช้งานในฐานะผู้ดูแลระบบ หรือเว็บไซต์ที่ให้เฉพาะสมาชิกเข้าถึงเท่านั้น จะต้องระมัดระวังและป้องกันเป็นพิเศษ

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาศัยช่องโหว่นี้ในการดำเนินการโดยใช้ประโยชน์จากการจัดการ Session ที่ไม่เหมาะสม คือ สามารถดักขโมย Session ID ของผู้ใช้บริการ หรือนำเอา Session ID ไปใช้ในการเข้าเว็บไซต์ด้วยสิทธิ์ของเจ้าของ Session ได้ ยกตัวอย่างเช่น

1.1 เข้าถึงและดำเนินการกับบริการต่าง ๆ ที่ผู้ใช้บริการมีสิทธิ์ เช่น สั่งโอนเงิน (Internet Banking Service), สั่งซื้อของออนไลน์

1.2 เพิ่ม แก้ไข ลบ ข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น เปลี่ยนรหัสผ่าน

1.3 เรียกดูข้อมูลตามสิทธิ์ของผู้ใช้บริการ เช่น เปิดดูข้อมูลในอีเมลส่วนตัว

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

สร้าง Session ID ที่ยากต่อการคาดเดา ไม่ใช้ Algorithm ที่ง่ายเกินไป เช่น Pseudo Random Number

ไม่ใช้ URL Parameter ในการเก็บ Session ID

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

ใช้ Session ID เป็นค่าสุ่ม

มีการกำหนดวันหมดอายุของ Cookie ที่เก็บ Session ID

3 การทดสอบความมั่นคงปลอดภัย

ผู้ทดสอบสามารถตรวจสอบว่า Cookie ที่ให้บริการสามารถป้องกันการโจมตีได้หลากหลายแค่ไหน ซึ่งเป้าหมายโดยรวมคือเพื่อให้ได้ Cookie ที่มีช่องโหว่ที่เกิดจากการโจมตี เช่น Session Hijacking อนุญาตให้ผู้ประสงค์ร้ายสามารถแก้ไขหรือเปลี่ยนแปลงสิทธิ์ของผู้ใช้บริการในระบบได้

โดยปกติรูปแบบการโจมตีจะมี ดังนี้

3.1 ดักเก็บ Cookie เพื่อให้ได้ Cookie ที่เป็นไฟล์ตัวอย่าง

3.2 วิเคราะห์ขั้นตอนและ Algorithm วิธีการสร้าง Cookie จากตัวอย่างที่ได้ สร้างไฟล์ Cookie ปลอมเพื่อใช้ในการโจมตี

Cross-Site Scripting

Cross-Site Scripting (XSS) เกิดจากช่องโหว่ของโปรแกรมประยุกต์บนเว็บที่ไม่มีการคัดกรองและตรวจสอบข้อมูลที่ได้รับจากผู้ใช้บริการว่าเป็นข้อมูลที่มีความน่าเชื่อถือหรือไม่ ทำให้ผู้ประสงค์ร้ายสามารถแทรกคำสั่งต่าง ๆ เข้าไปในเว็บเพจ เมื่อผู้ใช้บริการเรียกหน้าเว็บเพจนั้นก็อาจถูกขโมยข้อมูลสำคัญไปได้ ซึ่งผู้ประสงค์ร้ายอาจจะนำไปสวมรอยเพื่อเข้าสู่ระบบไปยังเว็บไซต์เสมือนว่าเป็นผู้ใช้บริการตัวจริง ปัญหานี้เรียกว่า “Cross-Site Scripting Vulnerability” และการโจมตีที่ใช้ประโยชน์จากช่องโหว่นี้เรียกว่า “Cross-Site Scripting Attack” ซึ่งอาจไม่เป็นอันตรายต่อเว็บไซต์ แต่จะส่งผลกระทบโดยตรงต่อความมั่นคงปลอดภัยของผู้ใช้บริการ

ทุกเว็บไซต์ควรระมัดระวังช่องโหว่ประเภทนี้ โดยเฉพาะเว็บไซต์ที่มีการจัดการ Session ID ที่เก็บในไฟล์ Cookie รวมถึงเว็บไซต์ที่ให้ผู้ใช้บริการสมัครสมาชิกและยืนยันตัวตนด้วยการ Login เพื่อเข้าสู่ระบบ ควรจะต้องระมัดระวังเป็นพิเศษ ซึ่งลักษณะของเว็บเพจที่อาจมีช่องโหว่ประเภทนี้ คือ

1. มีการรับข้อมูลจากผู้ใช้บริการผ่าน Input Form

เช่น หน้า Login เพื่อเข้าสู่ระบบ หน้าลงทะเบียนสมาชิก หรือกล่องคอมเมนต์

2. หน้าเว็บเพจที่แสดงผลจากการค้นหาข้อมูล

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาจอาศัยช่องโหว่ในการดำเนินการ ดังนี้

1.1 แสดงหน้าเว็บเพจปลอมหรือข้อมูลปลอมบนเว็บไซต์

1.2 ดักเอาไฟล์ Cookie ที่เก็บบนโปรแกรมค้นดูเว็บ โดยถ้า Session ID นั้นเก็บอยู่ใน Cookie อาจนำไปสู่การปลอมแปลง Session ID ได้ หรือถ้าเก็บข้อมูลส่วนบุคคลใน Cookie ข้อมูลก็อาจถูกเปิดเผยได้

1.3 เปลี่ยนแปลงข้อมูลใน Cookie และทำโปรแกรมประยุกต์บนเว็บบันทึก Cookie ที่ถูกเปลี่ยนแปลง โดยผู้ประสงค์ร้ายอาจแก้ไข Session ID และบันทึกใน Cookie ผู้ใช้บริการก็จะได้รับ Session ID ที่ถูกเปลี่ยนแปลงแก้ไขแทน

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

โปรแกรมประยุกต์บนเว็บต้องมีการทำ Output Validation ในลักษณะ Sanitization

การทำ HTML Entity Encoding หรือ URL Encoding กับข้อมูลที่จะแสดงผล โดยการทำ Output Validation เปรียบเสมือนการป้องกันการแสดงผลข้อมูลที่ไม่พึงประสงค์ยังฝั่งผู้ใช้บริการ เช่น การแสดงผลข้อผิดพลาด (Error Message) ที่ในบางครั้งอาจแสดงข้อมูลที่เป็นประโยชน์ต่อผู้ประสงค์ร้าย ซึ่งข้อมูลทั้งหมดนี้ผู้ประสงค์ร้ายสามารถรวบรวมมาเป็นข้อมูลที่ใช้โจมตีเว็บไซต์ได้ง่ายมากขึ้น เช่น การใช้งานฟังก์ชัน htmlentities() ในภาษา PHP เพื่อป้องกันการโจมตีด้วยเทคนิค XSS สมมติว่าผู้ประสงค์ร้ายมีการส่งค่า <script>alert(“Hacked”) </script> เข้ามายังระบบผ่านตัวแปรหนึ่ง เมื่อค่าดังกล่าวถูกนำไปประมวลผลผ่านฟังก์ชัน htmlentities() ซึ่งจะมีการ Encode ค่าต่าง ๆ ให้อยู่ในรูปแบบที่โปรแกรมคนดูเว็บมองเป็นเพียงข้อความธรรมดา กรณีนี้ผลลัพธ์ที่ได้จากการ Encode ด้วยฟังก์ชันดังกล่าวได้เป็น <script>alert(“Hacked”)</script> ในฝั่งผู้ใช้บริการได้อยู่ แต่อยู่ในรูปแบบของข้อความซึ่งไม่สามารถนำมาประมวลผลในลักษณะสคริปต์ตามที่ผู้ประสงค์ร้ายต้องการได้

ตรวจสอบ Input Validation ไม่ให้ใช้ HTML Tag ใด ๆ เช่น ไม่ Generate Content จาก Tag <script></script>

ไม่อนุญาตให้มีการเรียก Stylesheets จากเว็บไซต์ที่ไม่ได้ตรวจสอบก่อน

ตั้งค่า Charset Parameter ของ HTTP Content-Type Header

โปรแกรมประยุกต์บนเว็บต้องมีการตรวจสอบข้อมูลชุดคำสั่งในเว็บไซต์ว่ากำลังรับข้อมูลที่ผิดปกติเป็นสคริปต์ที่อันตรายหรือไม่ เช่น สคริปต์ที่มีเครื่องหมายอักขระพิเศษ เช่น < > ? & # โดยต้องคัดกรองเครื่องหมายเหล่านี้ก่อนที่จะนำไปประมวลผลที่เครื่องบริการเว็บและการกรองข้อมูลที่รับเข้าจากผู้ใช้เป็นหลัก และข้อมูลที่รับเข้าต่าง ๆ ไม่ควรถูกนำมาใช้งานในทันที แต่ต้องมีการกรองข้อมูลก่อนการใช้งานทุกครั้ง และต้องมั่นใจได้ว่าผู้ใช้ไม่สามารถวาง Script ใด ๆ ลงในเว็บได้ ควรแปลงพวก Non-Alphanumeric Data ให้กลายเป็น HTML Character เสียก่อน เช่น เครื่องหมายน้อยกว่า “<” ควรถูกแปลงเป็น “& l t ;”

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

โปรแกรมประยุกต์บนเว็บต้องมีการใช้งาน HTTPOnly Cookie Flag HTTPOnly เป็นรูปแบบการกำหนดค่าเพิ่มเติม (Flag) สำหรับป้องกันไม่ให้ฝั่งผู้ใช้บริการ สามารถเข้าถึงค่า Cookie ของระบบได้ โดยทั่วไปหากระบบมีช่องโหว่ของการโจมตีด้วยเทคนิค XSS ผู้ประสงค์ร้ายอาจส่งคำสั่งเพื่อให้โปรแกรมอ่านข้อมูล Cookie ของผู้ใช้บริการและลักลอบส่งข้อมูลออกไปยังปลายทาง รวมถึงในบางครั้งอาจสั่งให้มีการปรับเปลี่ยนค่าใน Cookie ได้ด้วย อย่างไรก็ตาม การใช้งาน HTTPOnly นั้นยังมีข้อจำกัดว่าสามารถใช้งานกับโปรแกรมค้นดูเว็บที่สนับสนุนเท่านั้น เช่น โปรแกรมค้นดูเว็บ Chrome ตั้งแต่เวอร์ชัน 1.0.154 หรือ Safari ตั้งแต่เวอร์ชัน 4 หรือ Internet Explorer ตั้งแต่เวอร์ชัน 6sp1

การตรวจสอบว่าเว็บไซต์ใช้ HTTPOnly หรือไม่ สามารถใช้เครื่องมือ Developer Tools ของโปรแกรมค้นดูเว็บตรวจสอบได้ ซึ่งหากเว็บไซต์มีการใช้ HTTPOnly จะปรากฏข้อความดังรูป

Response Header	Value
(Status-Line)	HTTP/1.1 200 OK
Server	ASP.NET Development Server/10.0.0.0
Date	Sat, 22 Oct 2011 07:14:45 GMT
X-AspNet-Version	4.0.30319
Set-Cookie	testcookie=Testcookie Value; path=/; HttpOnly
Cache-Control	private
Content-Type	text/html; charset=utf-8
Content-Length	1795
Connection	Close

3 การทดสอบความมั่นคงปลอดภัย

จุดอ่อนด้านความมั่นคงปลอดภัยของโปรแกรมประยุกต์บนเว็บส่วนใหญ่ คือ การไม่มีการตรวจสอบข้อมูลที่รับเข้ามาจากฝั่งผู้ใช้บริการก่อนที่จะนำข้อมูลนั้นไปประมวลผล ซึ่งจุดอ่อนเรื่องดังกล่าวเป็นสาเหตุของช่องโหว่สำคัญที่พบบนโปรแกรมประยุกต์บนเว็บหลายประการ เช่น Cross-Site Scripting, SQL Injection, Interpreter Injection

Cross-Site Request Forgery

Cross-Site Request Forgery (CSRF) เป็นภัยคุกคามประเภทหนึ่งที่เกิดจากการที่ผู้ประสงค์ร้ายลักลอบปลอมแปลงคำสั่งข้อมูลให้เสมือนเป็นคำสั่งจากผู้ใช้บริการระบบ เพื่อให้เครื่องบริการเว็บเข้าใจว่าเป็นคำสั่งที่มาจากผู้ใช้บริการของระบบและดำเนินการตามที่ร้องขอ เช่น ผู้ประสงค์ร้ายอาศัยช่องโหว่ของเว็บเพจปลอมแปลงคำสั่งข้อมูลให้เสมือนเป็นคำสั่งจากเจ้าของบัญชีจริง เพื่อติดต่อกับระบบธนาคารทางอินเทอร์เน็ต ทำให้ระบบเชื่อและเข้าใจว่าเจ้าของบัญชีต้องการทำธุรกรรมทางการเงินนั้น ๆ จริง ซึ่งปัญหานี้เรียกว่า “Cross-Site Request Forgery Vulnerability” และการโจมตีที่อาศัยช่องโหว่นี้เรียกว่า “Cross-Site Request Forgery Attack”

เว็บไซต์ที่ให้บริการที่มีความสำคัญสูง เช่น บริการชำระเงินออนไลน์ หรือเว็บไซต์ที่ผู้ใช้บริการต้องผ่านกระบวนการยืนยันตัวตนด้วยการเข้าสู่ระบบก่อนที่จะเข้าใช้งานเว็บไซต์ เช่น การเข้าถึงหน้าเว็บเพจของผู้ดูแลระบบ หรือเว็บไซต์ที่มีกระบวนการจัดการ Session ด้วยการจัดการหรือจัดเก็บ Session ในไฟล์ Cookie หรือใช้เทคนิคการยืนยันตัวตนด้วย Basic Authentication (การใช้ Username และ Password) ก็ควรระมัดระวังการโจมตีประเภทนี้

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาจอาศัยช่องโหว่ในการดำเนินการ ดังนี้

1.1 เข้าถึงและดำเนินการกับบริการต่าง ๆ ที่เข้าถึงได้เฉพาะผู้ใช้บริการที่ Login แล้ว เช่น สั่งโอนเงิน (internet Banking Service), สั่งซื้อของออนไลน์

1.2 เพิ่ม แก้ไข ลบ ข้อมูลส่วนบุคคลของผู้ใช้บริการ เช่น เปลี่ยนรหัสผ่าน

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

ฟังก์ชันต่าง ๆ ควรดำเนินการผ่าน POST Method และตรวจสอบความถูกต้องกับค่าที่ซ่อน อยู่ภายใน POST Method ก่อนจะดำเนินการต่อ ยกตัวอย่าง ขั้นตอนที่ต้องรับข้อมูลจากฝั่งผู้ใช้บริการและต้องได้รับข้อความยืนยันจากฝั่งผู้ใช้บริการ (Confirmation Page) ก่อน จึงจะดำเนินการโดยให้ตั้งค่าที่เป็นความลับค่าหนึ่งให้เป็น Field ที่ซ่อนอยู่ใน POST Method เมื่อทางฝั่งผู้ใช้บริการกดส่ง Confirm จาก Confirmation Page ก็ให้แทรกค่า ๆ นี้มาด้วย (ซึ่งค่าที่เป็นความลับนี้อาจจะเป็น Session ID ที่สร้างขึ้นมาเพิ่ม ตอนที่ผู้ใช้บริการ Log In) โดยเมื่อได้รับ Request ให้ตรวจสอบค่าใน Hidden Parameter ว่าเป็นค่าที่ถูกต้องแล้วจึงจะดำเนินการต่อเท่านั้น

โปรแกรมประยุกต์บนเว็บต้องมีฟังก์ชันการยืนยันตัวตนของผู้ใช้งานอีกครั้ง และให้กรอก Captcha เมื่อมีการเปลี่ยนสถานะการทำงานในฟังก์ชันที่สำคัญ ๆ เช่น การชำระเงิน การเปลี่ยนรหัสผ่าน

โปรแกรมประยุกต์บนเว็บต้องมีการใช้งาน Unique Token และ/หรือ ตรวจสอบ Referrer ร่วมกับการส่งข้อมูล หรือคำสั่งผ่านแบบฟอร์มการสร้างข้อมูลอ้างอิงเพื่อใช้ในการตรวจสอบความถูกต้องของข้อมูลที่ส่งมาประมวลผล อาจจะด้วยการสร้าง Unique Token ในแบบฟอร์ม และเพื่อให้แน่ใจว่าข้อมูลในแบบฟอร์มที่ส่งมาประกอบในแต่ละครั้งนั้นเป็นข้อมูลที่เกิดจากการที่ผู้ใช้บริการจริง ไม่ใช่โปรแกรมอัตโนมัติหรือสคริปต์ที่ใช้ในการโจมตีแต่อย่างใด ซึ่งจะเห็นตัวอย่างของวิธีการดังกล่าวได้จากการเข้าใช้งาน Online Banking ที่ในแต่ละการทำธุรกรรมจะต้องมีการยืนยันด้วยหมายเลข OTP ก่อนเสมอ เพื่อเป็นการยืนยันว่าการทำธุรกรรมนั้นเกิดจากผู้ใช้บริการจริง เมื่อตรวจสอบได้ว่ามาจาก URL ที่ถูกต้องแล้ว จึงดำเนินการต่อ

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

วิธีการลดความเสียหายที่เกิดจากการถูกโจมตีโปรแกรมประยุกต์บนเว็บต้องมีการส่งอีเมลอัตโนมัติ แจ้งผู้ใช้บริการทุกครั้ง เมื่อการดำเนินการที่สำคัญ เช่น กระบวนการสั่งโอนเงินทำสำเร็จ และต้องไม่มีข้อมูลส่วนบุคคลของผู้ใช้บริการแทรกเข้าไปในอีเมล

3 การทดสอบความมั่นคงปลอดภัย

CSRF เป็นการโจมตีที่สวมสิทธิ์ของผู้ใช้บริการและดำเนินการบางอย่างบนเว็บไซต์ ซึ่งถ้าผู้ประสงค์ร้ายสามารถโจมตีบัญชีผู้ใช้ของผู้ดูแลเครื่องบริการเว็บได้ ก็จะสามารถสั่งดำเนินการใด ๆ กับโปรแกรมประยุกต์บนเว็บด้วยสิทธิ์ของผู้ดูแลเว็บได้

HTTP Header Injection

การที่ผู้ประสงค์ร้ายสร้าง Response Header หรือปลอมแปลงแก้ไข Response Body ไว้ และเมื่อผู้ใช้บริการเข้าเว็บไซต์ดังกล่าว จะแสดงผลหน้าเว็บเพจปลอมและอาจจะ Run สคริปต์ สร้าง Cookie ปลอม และสั่งให้เก็บไว้บนโปรแกรมค้นดูเว็บของผู้ใช้บริการ ซึ่งหากขั้นตอนการสร้าง HTTP Response Header ของโปรแกรมประยุกต์ดังกล่าวมีช่องโหว่ ผู้ประสงค์ร้ายจะสามารถเพิ่มข้อมูลใน Header หรือสามารถแก้ไขเปลี่ยนแปลงข้อมูลในส่วน Response Body ซึ่งปัญหานี้เรียกว่า “HTTP Header Injection Vulnerability” และการโจมตีที่อาศัยช่องโหว่นี้ คือ “HTTP Header Injection Attack”

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาจอาศัยช่องโหว่ในการดำเนินการ ดังนี้

1.1 กระทำการใด ๆ ที่เหมือนกับการโจมตีช่องโหว่ Cross-Site Scripting เช่น โปรแกรมค้นดูเว็บของผู้ใช้บริการส่ง Request ที่ไม่ได้มาจากผู้ใช้บริการโดยตรง หรือถูกบังคับให้ Run สคริปต์ที่แทรกอยู่บนหน้าเว็บเพจ ซึ่งสิ่งเหล่านี้เป็นภัยคุกคามประเภทเดียวกับหัวข้อ Cross-Site Scripting

1.2 ผู้ประสงค์ร้ายสร้าง Cookie โดยไม่ได้รับอนุญาต เช่น เมื่อ HTTP Set-Cookie Header ถูกสร้างขึ้น ไฟล์ Cookie ที่ถูกสร้างโดยไม่ได้รับอนุญาตก็จะถูกสร้างและเก็บข้อมูลในโปรแกรมค้นดูเว็บของผู้ใช้บริการด้วย

1.3 Poison Web Cache HTTP Response Splitting จะบังคับให้เครื่องบริการเว็บสร้าง HTTP Response หลายอัน และทำให้เกิด Cache Poisoning ซึ่งจะแสดงหน้าเว็บเพจที่ผู้ประสงค์ร้ายต้องการด้วยการใช้ Proxy Server เก็บ Cache ของ HTTP Response ที่สร้างขึ้น และเก็บแทนที่ Cache เดิม เมื่อผู้ใช้บริการเข้าเว็บไซต์ของเหยื่อก็จะเห็นหน้าเว็บไซต์ที่เป็นเว็บไซต์ปลอมที่ถูกสร้างโดยผู้ประสงค์ร้าย

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

ไม่ให้แสดงข้อมูล HTTP Header โดยตรง

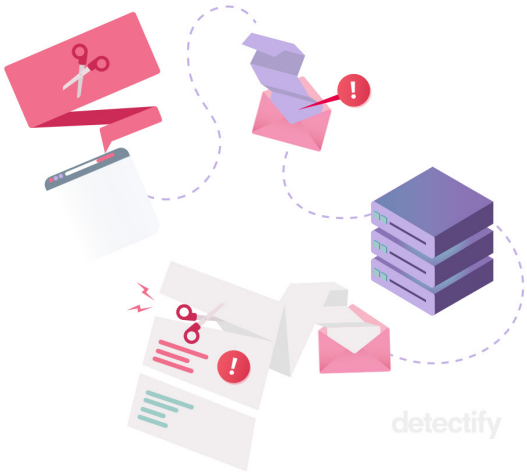
ในกรณีที่มีการใช้งาน HTTP Header – เพิ่มการป้องกัน Unexpected Line Feeds ด้วยตนเอง หากไม่มีฟังก์ชัน Line Feed Neutralization

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

ลบ Line Feed Characters ทั้งหมดที่ปรากฏใน External Text Input

3 การทดสอบความมั่นคงปลอดภัย

ในส่วนนี้จะแสดงให้เห็นถึงการโจมตีที่ใช้ประโยชน์จาก HTTP โปรโตคอล โดยอาศัยจุดอ่อนของโปรแกรมประยุกต์บนเว็บด้วย ซึ่งจะวิเคราะห์จากการโจมตี HTTP Header มี 2 รูปแบบ คือ **HTTP Splitting** และ **HTTP Smuggling**



Mail Header Injection

โปรแกรมประยุกต์บนเว็บอาจมีฟังก์ชันในการส่งอีเมลแบบเฉพาะเจาะจงไปยังผู้ใช้บริการแต่ละราย เช่น ผู้ใช้บริการที่สั่งซื้อสินค้าของเว็บไซต์ ซึ่งโดยทั่วไปแล้วอีเมลเหล่านี้จะมีเพียงผู้ดูแลเว็บ (Web Admission) ที่สามารถเข้าถึงได้เท่านั้น โดยผู้ประสงค์ร้ายอาจทำการตั้งค่า เปลี่ยนแปลง หรือเพิ่มอีเมลอื่น ๆ ได้ตามต้องการ และใช้เครื่องบริการเว็บเป็นฐานสำหรับกระจาย Spam mail ซึ่งช่องโหว่ดังกล่าวจะเรียกว่า **"Mail Header Injection Vulnerability"** และการโจมตีที่ใช้ประโยชน์จากช่องโหว่นี้เรียกว่า "Mail Header Injection Attack"

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายอาจอาศัยช่องโหว่นี้ในการใช้โปรแกรมประยุกต์ที่ถูกโจมตีเป็นฐานส่ง Spam Mail

2 แนวทางในการป้องกันการโจมตี

แนวทางในการป้องกันปัญหา มีดังต่อไปนี้

2.1 Fundamental Solutions: การป้องกันการโจมตี

กำหนดค่าคงที่ (Fixed Values) สำหรับองค์ประกอบของ Header เก็บค่าและแสดงผลที่รับมาจากผู้ใช้บริการในส่วนเนื้อความของอีเมล องค์ประกอบของ Header ที่ต้องรับค่าจากผู้ใช้บริการ เช่น To, Cc, Bcc, Subject ซึ่งหากนำค่าเหล่านี้มาใช้เป็นค่าสำหรับการส่งออกอีเมลโดยตรง ผู้ประสงค์ร้ายก็จะสามารถแทรกอีเมลอื่น ๆ และทำการแก้ไขเปลี่ยนแปลงเนื้อหาในอีเมลและส่งออกไปยังอีเมลอื่น ๆ ที่ไม่เกี่ยวข้องได้ คำแนะนำ คือ ไม่ให้ใช้ External Parameter เพื่อกำหนดค่าของอีเมล Header Element

กรณีที่ไม่สามารถกำหนดค่าคงที่ (Fixed Values) ใน Header ใช้ Email-sending API ที่สามารถใช้งานร่วมกับโปรแกรมประยุกต์บนเว็บ หรือภาษาที่ใช้ในการพัฒนาได้ หากไม่สามารถใช้ค่าคงที่กับ Email Header ได้ ควรใช้ Email-sending API โดยสามารถใช้งานร่วมกับโปรแกรมประยุกต์บนเว็บ หรือภาษาที่ใช้ในการพัฒนาได้แทน และ API ก็ยังอนุญาตให้เพิ่มข้อมูลใน Header ได้หลาย ๆ รายการ ซึ่งผู้พัฒนาโปรแกรมประยุกต์บนเว็บจะต้องทำการปรับปรุงเพิ่มเติม เพื่อไม่อนุญาตให้สามารถแบ่งบรรทัดใน Header ได้ เช่น การป้องกันการขึ้นบรรทัดใหม่ โดยเพิ่มช่องว่าง (Space) หรือ Tab หลังจากข้อมูล เพื่อเป็นสัญลักษณ์ว่าสิ้นสุดข้อมูลแล้ว และตัวอักษรหรือข้อมูลใด ๆ ที่อยู่หลังสัญลักษณ์นี้จะถูกลบออกทั้งหมด

ไม่กำหนดชื่อที่อยู่อีเมลใน HTML ไม่ระบุชื่ออีเมลของผู้รับโดยตรงใน Hidden Parameter ที่จะส่งผ่านไปยังโปรแกรมประยุกต์บนเว็บ ผู้ประสงค์ร้ายจะสามารถดักโจมตีและเปลี่ยนค่าในอีเมลได้

2.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

วิธีการลดความเสียหายที่เกิดจากการถูกโจมตี ลบ Line Feed Character ทั้งหมดที่รับข้อมูลจากผู้ใช้บริการลบบรรทัดของตัวอักขระที่รับจากผู้ใช้บริการทั้งหมดใน Input Text เนื่องจากโปรแกรมประยุกต์บนเว็บอาจลบข้อมูลไม่ทั้งหมด ซึ่งเสี่ยงต่อการเกิดช่องโหว่

3 การทดสอบความมั่นคงปลอดภัย

ภัยคุกคามในข้อนี้จะส่งผลกับโปรแกรมประยุกต์บนเว็บที่มีฟังก์ชันอีเมลในการติดต่อกับ Mail Server (IMAP/SMTP) เป้าหมายของการทดสอบนี้ คือ ตรวจสอบความสามารถในการส่งคำสั่งใด ๆ ก็ตามไปที่ Mail Server เพื่อดูผลลัพธ์จากการส่งข้อมูลที่ไม่ถูกต้อง

File Inclusion

การโจมตีโดยใช้เทคนิค File Inclusion คือการนำโปรแกรม PHP ของผู้ประสงค์ร้าย เข้าไปแทรกเพื่อรวมเข้ากับไฟล์ PHP ตัวหลักที่อยู่บนเว็บไซต์ของเป้าหมาย โดยไฟล์ PHP ตัวหลักของเป้าหมายจะทำหน้าที่ในการแสดงส่วน Header และ Footer ของหน้าเว็บไซต์ สำหรับส่วนที่เป็นเนื้อหามักทำโดยการเรียกรวม (Include) มาจากไฟล์อื่น โดยมักจะพบได้บ่อยในซอฟต์แวร์ประเภท CMS (Content Management System) ในการที่ผู้ใช้งานต้องการเรียกหน้าต่าง ๆ บนเว็บไซต์ที่มีช่องโหว่นี้ ผู้ประสงค์ร้ายมักจะพยายามโจมตีไปยังจุดที่บ่งบอกถึงข้อมูลเกี่ยวกับการเรียกไปยังหน้าอื่น และปรับเปลี่ยนค่าพารามิเตอร์ต่าง ๆ แล้วประมวลผลบนเครื่องเซิร์ฟเวอร์ของเป้าหมาย และแสดงผลลัพธ์กลับไปแสดงบนหน้าจอของผู้ประสงค์ร้าย หรือคือการควบคุมเครื่องเว็บเซิร์ฟเวอร์ของเป้าหมายจากทางไกล

1 ภัยคุกคามที่อาจเกิดขึ้น (Possible Threats)

ผู้ประสงค์ร้ายมักจะเป็นไฟล์ประเภท PHP Shell ซึ่งจะเป็นเครื่องมือที่ทำให้ผู้ประสงค์ร้ายสามารถที่จะทำการต่าง ๆ ได้ดังนี้

1.1 แสดงรายชื่อไฟล์ใน Directory ต่าง ๆ และผู้ประสงค์ร้ายสามารถคลิกที่ชื่อ Directory เพื่อย้ายเข้าไปใน Directory ที่ต้องการได้ ทำให้ผู้ประสงค์ร้ายทราบโครงสร้างของ Directory และรายชื่อไฟล์ที่สำคัญบนเครื่องของเป้าหมายได้

1.2 เปิดไฟล์บนเครื่องของเป้าหมาย ทำให้อาจทราบข้อมูลของผู้ใช้บริการระบบ รวมถึงอาจทราบถึงรหัสผ่านที่ใช้ในการเชื่อมต่อกับฐานข้อมูลได้

1.3 มีโอกาสที่ผู้ประสงค์ร้ายอาจแอบแฝงไฟล์อันตรายจากเครื่องของผู้ประสงค์ร้ายไปเก็บไว้บนเว็บเซิร์ฟเวอร์ของเป้าหมายได้

2 แนวทางในการป้องกันการโจมตี

2.1 การป้องกันโดยการใช้ตัวเลขแทนชื่อไฟล์ ช่องโหว่ที่แท้จริงของเว็บไซต์ที่สามารถถูกโจมตีด้วยเทคนิค File Inclusion คือการเขียนโปรแกรมให้มีการเรียกรวมไฟล์ที่สองเข้ามาเป็นส่วนหนึ่งของไฟล์แรก การป้องกันที่ได้ผลที่สุดคือ การให้พารามิเตอร์ที่เป็นตัวเลขที่มีเงื่อนไขในการใช้ Map ว่าหมายเลขใดคือไฟล์ใด ดังนั้นตัวเลขที่สามารถใช้ได้คือตัวเลขที่ผู้ให้บริการอนุญาตเท่านั้นมีจำนวนจำกัด ทำให้การเรียกรวมไฟล์เกิดขึ้นกับไฟล์ที่มีอยู่จำนวนจำกัดที่ผู้ให้บริการตั้งค่าไว้เท่านั้น และทำให้ผู้ประสงค์ร้ายไม่สามารถเรียกรวมไฟล์อื่นที่ไม่อยู่ในรายการเงื่อนไขได้

2.2 การป้องกันโดยการตรวจหาและแทนที่ http:// สำหรับกรณีที่ผู้ให้บริการพบว่า เว็บไซต์มีช่องโหว่ File Inclusion ผู้ให้บริการสามารถที่จะทำการป้องกันแบบชั่วคราวได้อย่างรวดเร็วโดยการตรวจสอบและกรองคำว่า http:// ซึ่งผู้ประสงค์ร้ายจะใช้อ้างอิงไปยังเว็บไซต์ที่มี PHP Shell อยู่

2.3 การป้องกันโดยไม่ให้เว็บเซิร์ฟเวอร์ติดต่อกับอินเทอร์เน็ตพอร์ต 80 เนื่องจากเว็บเซิร์ฟเวอร์จะทำการ request เอาไฟล์ PHP บนเซิร์ฟเวอร์ดังกล่าวโดยการเชื่อมต่อไปที่พอร์ตหมายเลข 80 ของเว็บเซิร์ฟเวอร์ที่เก็บไฟล์ PHP Shell ดังนั้น หากทำการสกัดกั้นไม่ให้เว็บเซิร์ฟเวอร์ติดต่อกับพอร์ต 80 กับเครื่องอื่นบนอินเทอร์เน็ตได้ก็จะสามารถป้องกันได้ โดยการตั้งค่าที่เว็บเซิร์ฟเวอร์ของผู้ให้บริการและการกำหนดที่ Firewall

3 การทดสอบความมั่นคงปลอดภัย

ภัยคุกคามนี้มักจะทำการรวมไฟล์ PHP ตัวหลักกับไฟล์อื่นที่ระบุชื่อไฟล์เพิ่มขึ้นมา ซึ่งสามารถสังเกตได้จากช่อง Address และ Status Bar ที่อยู่ด้านล่างเบราวเซอร์ไปยังไฟล์ที่อยู่บนเครื่องของผู้ประสงค์ร้าย

หัวข้อเนื้อหาการเรียนรู้ที่ 2
การไม่มีระบบพิสูจน์ตัวจริงและการกำหนดสิทธิ์
(Lack of Authentication and authorization)

การไม่มีระบบพิสูจน์ตัวจริง และการกำหนดสิทธิ์

ในการออกแบบเว็บไซต์ ควรจะตระหนักเรื่องความมั่นคงปลอดภัยเมื่อนำไปใช้งานจริง ซึ่งในบทนี้จะแสดงให้เห็นถึงแนวทางในการป้องกันของฟังก์ชันที่มีความสำคัญ ได้แก่ Authentication และ Authorization

1 Lack of Authentication

1.1 Fundamental Solutions: การป้องกันการโจมตี

โปรแกรมประยุกต์ต้องระบุวิธีการยืนยันตัวตนของผู้ใช้บริการ (Authentication) ในกรณีที่มีการกำหนด Access Control โดยปกติเมื่อเว็บไซต์มีการเก็บข้อมูลที่เป็นความลับที่อนุญาตให้เฉพาะเจ้าของข้อมูลสามารถเข้าถึง แก้ไข เปลี่ยนแปลงข้อมูลได้ จะต้องมีกระบวนการในการยืนยันตัวตน แต่พบว่าในบางเว็บไซต์อนุญาตให้ผู้ใช้บริการสามารถเข้าถึงข้อมูลที่เป็นความลับได้เพียงแค่ระบุอีเมลเท่านั้น ซึ่งอีเมลดังกล่าวเป็นข้อมูลที่สามารถพบได้ทั่วไป ดังนั้นจะต้องมีวิธีการยืนยันตัวตนที่มั่นคงปลอดภัยมากขึ้นด้วยการให้ผู้ใช้บริการระบุข้อมูลส่วนบุคคล เช่น รหัสผ่าน ร่วมด้วย

การเก็บรหัสผ่านควรอยู่ในรูปที่มีการเข้ารหัสลับตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนด เช่น AES หรือ Triple DES และหากมีการเก็บรหัสผ่านในรูปแบบของค่าแฮช (Hash Value) ควรใช้ขั้นตอนวิธี (Algorithm) ตามที่มาตรฐานด้านความมั่นคงปลอดภัยกำหนดไว้ เช่น SHA-224 SHA256 SHA-512

1.2 Mitigation Measures: การลดความเสียหายที่เกิดจากการถูกโจมตี

รหัสผ่านที่ใช้ต้องประกอบด้วย อักษรตัวเล็ก อักษรตัวใหญ่ ตัวเลขและอักขระพิเศษ ซึ่งทั้งหมดจะต้องมีความยาวรวมไม่น้อยกว่า 8 หลัก

2 Lack of Authentication

2.1 Fundamental Solutions: การป้องกันการโจมตี

โปรแกรมประยุกต์บนเว็บต้องมีกระบวนการที่ชัดเจน เพื่อให้แน่ใจว่าผู้ใช้บริการที่เข้าสู่ระบบไม่สามารถเข้าถึงบัญชีผู้ใช้และข้อมูลของผู้ใช้งานคนอื่น ๆ ได้ กระบวนการยืนยันตัวตน อนุญาตให้ผู้ใช้บริการที่เป็นเจ้าของข้อมูลสามารถเข้าถึงและแก้ไขเปลี่ยนแปลงข้อมูลได้ แต่ในกรณีที่มีผู้ใช้บริการคนอื่นเข้าสู่ระบบและใช้บริการนั้น ๆ ในเวลาเดียวกัน ผู้พัฒนาโปรแกรมประยุกต์บนเว็บจะต้องทำการตรวจสอบให้แน่ใจว่าอนุญาตให้ผู้ใช้บริการแต่ละคนเข้าถึงได้เฉพาะข้อมูลของตัวเองเท่านั้น ตัวอย่างเว็บไซต์ใช้ Session ID ในการจัดการและระบุถึงบัญชีผู้ใช้ที่เข้าสู่ระบบสำเร็จ เพื่อระบุตัวตนของผู้ใช้บริการ แต่เว็บไซต์ทั่วไปอาจใช้ User ID ซึ่งเป็นค่าค่าหนึ่งที่เก็บอยู่ในฐานข้อมูลในการอ้างอิง การเก็บ User ID ที่อ้างอิงจากฐานข้อมูลใน URL หรือ POST Parameter จะทำให้ผู้ประสงค์ร้ายสามารถใช้ User ID และเข้าถึงรวมทั้งดำเนินการใด ๆ กับฐานข้อมูลได้ โดยการปลอมตัวเป็นผู้ใช้บริการและเข้าถึงข้อมูลที่ไม่ได้รับอนุญาตได้

2.2 การทดสอบความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัย การ Authentication และ Authorization เป็นการยืนยันตัวตนของผู้ใช้บริการที่จะเข้าติดต่อกับโปรแกรมประยุกต์บนเว็บ และเป็นกระบวนการที่อนุญาตให้เฉพาะผู้ใช้บริการที่ได้รับอนุญาตสามารถทำการเข้าถึงข้อมูลได้เท่านั้น

ตัวอย่างที่พบโดยทั่วไป คือ การ Login เข้าสู่ระบบ ซึ่งการทดสอบกระบวนการ Authentication และ Authorization ก็คือการทำความเข้าใจถึงวิธีการทำงาน ขั้นตอนที่ใช้ก่อน และใช้ข้อมูลนั้นในการหาวิธีทดสอบเพื่อหลีกเลี่ยงกลไกต่าง ๆ ในการ Authentication และ Authorization

Authorization เป็นกระบวนการที่เกิดขึ้นหลังจากการ Authentication สำเร็จ ดังนั้น ผู้ทดสอบจะต้องตรวจสอบ Authorization ต่อเมื่อได้รับข้อมูลที่เกี่ยวข้องอย่างถูกต้อง เช่น ชื่อบัญชีผู้ใช้และรหัสผ่านถูกต้อง บทบาทหน้าที่พร้อมสิทธิ์ในการเข้าถึงข้อมูลต่าง ๆ ของผู้ใช้บริการคนนั้นถูกต้อง โดยผู้ทดสอบต้องตรวจสอบว่าช่องโหว่เกี่ยวกับการกำหนดสิทธิ์เข้าถึงข้อมูลด้วย

บทที่

4 รับมือสถานการณ์ภัยคุกคามที่เกิดกับเว็บไซต์

หัวข้อเนื้อหาการเรียนรู้ที่ 1
ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์

ภัยคุกคาม ที่เกิดขึ้นกับเว็บไซต์

แนวทางในการรับมือสถานการณ์ภัยคุกคามที่เกิดขึ้นกับเว็บไซต์ สามารถจำแนกออกเป็น 3 ประเภทตามรูปแบบการโจมตี ดังนี้

1 กรณีเว็บไซต์ถูกบุกรุกและควบคุม (Intrusions)

ภัยคุกคามจากการบุกรุกและควบคุมเว็บไซต์ (Intrusions) สามารถพบเห็นและทำการยืนยันได้ง่ายที่สุด เนื่องจากการโจมตีมักจะต้องการสร้างร่องรอยหรือหลักฐานที่เห็นได้อย่างชัดเจนตามแต่ละจุดประสงค์ของผู้ประสงค์ร้าย เช่น การสร้างหน้าเว็บไซต์หลอกลวง (Phishing) เพื่อหวังผลทางการเงิน การเปลี่ยนแปลงข้อมูลต่าง ๆ บนเว็บไซต์ (Web Defacement) เพื่อหวังผลในการทำลายชื่อเสียง หรือแม้กระทั่งการเผยแพร่มัลแวร์บนเว็บไซต์ (Malware) เพื่อให้ผู้เข้าชมเว็บไซต์ติดมัลแวร์ ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกบุกรุกและควบคุม สามารถดำเนินการได้ในลักษณะเดียวกันตามข้อกำหนดที่เกี่ยวข้อง ดังนี้

1.1 ปิดการเชื่อมต่อของเว็บไซต์

1.2 สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น Web Log Source code Database

1.3 ตรวจสอบช่องทางการโจมตีและช่องโหว่ของเว็บไซต์ด้วยข้อมูลที่สำเนามาในระหว่างที่ผู้ดูแลกำลังตรวจสอบช่องทางการโจมตี

1.4 ระหว่างการตรวจสอบ ให้ทำการจัดสร้างเว็บเพจแบบ Static ขึ้นมาทดแทนเป็นการชั่วคราว เพื่อชี้แจงสถานการณ์การปิดปรับปรุง รวมไปถึงเพื่อให้หน่วยงานสามารถดำเนินภารกิจได้อย่างต่อเนื่อง โดยเว็บเพจดังกล่าวควรติดตั้งในเครื่องบริการเว็บใหม่ เพื่อลดความเสี่ยงจากการที่เครื่องบริการเว็บเดิมถูกควบคุมและปรับเปลี่ยนการตั้งค่าต่าง ๆ ป้องกันไม่ให้มีผลกับข้อมูลที่อยู่บนเครื่องเดิม

1.5 กู้คืนโปรแกรมที่เกี่ยวข้องกับข้อมูลเว็บ และกู้คือฐานข้อมูลที่เกี่ยวข้องกับเว็บไซต์ให้เป็นเวอร์ชันก่อนที่จะถูกโจมตี

1.6 ตรวจสอบช่องโหว่ของเว็บไซต์ (เวอร์ชันก่อนที่จะถูกโจมตี) ด้วยการทำ Vulnerability Assessment แก้ไขช่องโหว่ของเว็บไซต์ที่ทำให้ผู้ประสงค์ร้ายสามารถเจาะเข้าคุมระบบได้

1.7 บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ในหลายครั้งที่พบว่าผู้ประสงค์ร้ายสามารถบุกรุกและเข้าควบคุมเว็บไซต์ได้มาเป็นเวลานานแล้ว แต่เพิ่งสร้างร่องรอยหรือเปลี่ยนแปลงข้อมูลในเวลาต่อมา ส่งผลให้เกิดการวิเคราะห์ข้อมูลการโจมตีและช่องโหว่ของเว็บไซต์ผ่านข้อมูล Log ทำได้ยากขึ้น เนื่องจากในบางหน่วยงานมีการเก็บข้อมูล Log ไว้เพียงชั่วขณะหนึ่ง ส่งผลให้การวิเคราะห์ข้อมูลช่วงเวลาที่เกิดการโจมตีไม่สามารถทำได้ อย่างไรก็ตาม ผู้ดูแลต้องทบทวนข้อมูล Log อย่างสม่ำเสมอเพื่อเป็นการตรวจสอบการโจมตีที่เกิดขึ้น

2 กรณีเว็บไซต์ถูกโจมตีในลักษณะ DoS (Denial of Service)

การโจมตีเว็บไซต์ในลักษณะ DoS คือ การโจมตีเพื่อมุ่งเน้นให้เว็บไซต์ไม่สามารถให้บริการต่อได้ ซึ่งเป้าประสงค์สามารถเกิดได้จากหลายส่วน เช่น การลดความน่าเชื่อถือของหน่วยงาน การลดโอกาสในการทำธุรกิจ รวมถึงปัจจุบันมีการพบว่าเป็นการทำเพื่อเป้าประสงค์ที่เกี่ยวข้องในเชิงการเมืองการบริหาร อย่างกรณีกลุ่มแฮ็กเกอร์ประกาศว่าจะมีการโจมตีหน่วยงานราชการให้ไม่สามารถเปิดบริการได้อีก

ปัจจุบัน การโจมตีขยายตัวออกไปจนถึงการโจมตีที่เรียกว่า ดีดอส หรือ DDoS (Distributed Denial of Service) โดยเป็นลักษณะการโจมตีเป็นกลุ่มที่เกิดจากเครื่องคอมพิวเตอร์หลาย ๆ เครื่อง ทำการโจมตีเป้าหมายในเวลาเดียวกัน ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกโจมตีในลักษณะ DDoS มีข้อกำหนดที่เกี่ยวข้อง ดังนี้

2.1 ปิดการเชื่อมต่อของเว็บไซต์

2.2 สำเนาข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการถูกบุกรุกเพื่อนำมาใช้ในการวิเคราะห์ เช่น Web Log หรือ Firewall Log

2.3 ตรวจสอบหมายเลขไอพีที่ต้องสงสัยว่าจะเป็นการโจมตีด้วยข้อมูลที่สำเนามา โดยปกติจะพบเห็นข้อมูลในลักษณะที่เกิดซ้ำ ๆ ในรูปแบบเดียวกัน เช่น มีการเรียกเว็บไซต์ด้วย URL หนึ่งเป็นจำนวนมาก หรือมีการส่งข้อมูลมายังบริการหนึ่งซ้ำ ๆ เป็นจำนวนมาก

2.4 ปิดกั้นการเข้าถึงจากไอพีแอดเดรสดังกล่าว และแจ้งไปยังผู้ให้บริการเครือข่ายอินเทอร์เน็ตเพื่อหามาตรการที่รองรับในกรณีที่อุปกรณ์ป้องกันของหน่วยงานไม่สามารถรองรับปริมาณข้อมูลที่มากมายได้

2.5 บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันและการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

การจัดการกับเหตุการณ์ภัยคุกคามในกรณีถูกโจมตีด้วยเทคนิค Dos หรือ DDoS สิ่งสำคัญคือผู้ดูแลต้องมีทักษะในการพิจารณาและคัดแยกไอพีแอดเดรสที่คาดว่าจะเป็นการโจมตีที่รวดเร็วและถูกต้อง เพื่อป้องกันข้อผิดพลาดจากการปิดกั้นการเชื่อมต่อ โดยอาจอาศัยการประมวลผลในลักษณะสถิติและลักษณะการเข้าใช้งานที่ผิดปกติ รวมถึงยังจำเป็นต้องมีความร่วมมือกับผู้ให้บริการอินเทอร์เน็ตเพื่อให้การป้องกันการโจมตีสามารถทำได้อย่างมีประสิทธิภาพมากยิ่งขึ้น



3 กรณีโดเมนถูกขโมย (Domain Hijack)

การโดนขโมย (Domain Hijack) เป็นหนึ่งในรูปแบบการโจมตีที่มีมานานแล้ว และดูเหมือนว่ายังคงเป็นรูปแบบการโจมตีที่พบอยู่เสมอ เหยื่อที่ถูกขโมยโดเมนสามารถเป็นได้ตั้งแต่บริษัทขนาดเล็กและไม่เว้นแม้แต่บริษัทขนาดใหญ่ที่ดำเนินธุรกิจด้านเทคโนโลยีสารสนเทศที่ยังพบว่าตกเป็นเหยื่อในหลายครั้ง โดยจุดประสงค์ของการขโมยข้อมูลส่วนใหญ่มุ่งประโยชน์ไปยังการหาผลประโยชน์ในหลายลักษณะ เช่น การขโมยโดเมนเพื่อนำไปหาประโยชน์โดยการเรียกค่าไถ่จากเจ้าของโดเมนตัวจริง นำไปใช้สร้างสถานการณ์หลอกลวงหน้า Phishing ซึ่งการรับมือสถานการณ์ภัยคุกคามในกรณีเว็บไซต์ถูกขโมยโดเมนสามารถดำเนินการได้ แต่อย่างไรก็ตามจำเป็นต้องมีข้อมูลที่เพียงพอเพื่อให้การแก้ปัญหาทำได้อย่างมีประสิทธิภาพ โดยมีข้อกำหนดที่เกี่ยวข้อง ดังนี้

3.1 เก็บรวบรวมหลักฐานที่เกิดขึ้นทั้งหมด เช่น วัน เดือน ปี ที่ข้อมูลโดเมนเปลี่ยน หน้าจอของโดเมนที่ใช้งาน

3.2 ตรวจสอบกับผู้ลงทะเบียนโดเมนถึงสาเหตุของการเปลี่ยนแปลงโดเมน ในบางครั้งพบว่าผู้ดูแลถูกขโมยข้อมูลรหัสผ่านโดยการติดมัลแวร์ ทำให้ผู้ประสงค์ร้ายสามารถเข้าสู่เว็บไซต์บริหารจัดการโดเมนและทำการเปลี่ยนแปลงข้อมูลส่วนบุคคล

3.3 แจ้งการถูกขโมยข้อมูลโดเมนกับผู้ลงทะเบียนโดเมนที่เราใช้บริการ โดยนำหลักฐานที่เกี่ยวข้องแนบไปด้วย เช่น หลักฐานการโอนเงิน หลักฐานการตอบรับ

3.4 เมื่อได้รับสิทธิ์ในการบริหารจัดการโดเมนคืนมาแล้ว ให้ตรวจสอบข้อมูลต่าง ๆ ที่ใช้ในการยืนยันตัวตน เช่น ข้อมูลอีเมลผู้จดทะเบียนโดเมน รวมถึงเปลี่ยนรหัสผ่านระบบบริหารจัดการโดเมน

3.5 บันทึกเหตุการณ์และขั้นตอนการดำเนินการที่เกิดขึ้นทั้งหมด เพื่อใช้เป็นข้อมูลในการป้องกันการประสานงานกับหน่วยงานที่เกี่ยวข้องในกรณีที่จำเป็น

ภายหลังจากถูกขโมยโดเมนแล้ว สิ่งที่ยากที่สุดสำหรับผู้ดูแล คือ การทำให้ผู้ให้บริการลงทะเบียนโดเมนเชื่อว่าโดเมนถูกขโมยจริง และยอมคืนสิทธิ์กลับคืนให้กับผู้ดูแลตัวจริง แต่อย่างไรก็ตามความสำคัญไม่น้อยไปกว่านั้นคือผู้ดูแลจำเป็นต้องทราบสาเหตุของการถูกขโมยโดเมนที่เกิดขึ้น เพื่อเป็นการป้องกันและรับมือสถานการณ์การโจมตีที่อาจเกิดซ้ำอีก

การรับมือภัยคุกคาม ที่เกิดขึ้นกับเว็บไซต์

การใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเครื่องบริการเว็บอย่างสม่ำเสมอ จะช่วยให้ผู้ดูแลเครื่องบริการเว็บในการค้นหาข้อบกพร่องของเว็บไซต์ในเบื้องต้น โดยมีข้อกำหนดที่เกี่ยวข้องกับการใช้โปรแกรมตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ ดังนี้

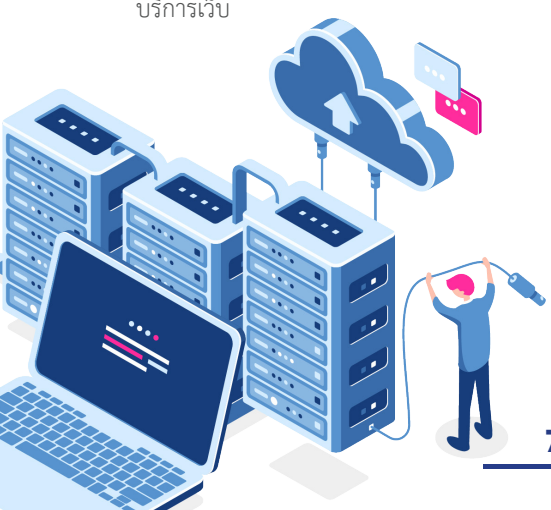
1. เลือกโปรแกรมที่น่าเชื่อถือ หรือได้รับการแนะนำจากหน่วยงานที่เกี่ยวข้อง
2. ปรับรุ่นของโปรแกรมที่ใช้ในการตรวจสอบข้อบกพร่องให้เป็นรุ่นล่าสุดเพื่อที่จะได้ตรวจสอบช่องโหว่ใหม่ ๆ ได้
3. หากการใช้โปรแกรมส่งผลกระทบกับการให้บริการของเครื่องบริการเว็บ ควรจะมีการสำรองข้อมูลทุกครั้งก่อนมีการใช้โปรแกรมตรวจสอบ
4. ควรใช้โปรแกรมมากกว่าสองโปรแกรมขึ้นไปในการตรวจสอบเพื่อเปรียบเทียบผลลัพธ์ที่ได้จากการตรวจสอบ

การสำรองข้อมูลเว็บไซต์

เพื่อให้กิจกรรมต่าง ๆ ของเว็บไซต์ดำเนินได้อย่างราบรื่น การสำรองข้อมูลต่าง ๆ ที่เกี่ยวข้องกับเว็บไซต์อาจไม่ใช่วิธีการป้องกันการโจมตีที่เกิดขึ้น แต่เป็นวิธีที่มักจะมีส่วนเกี่ยวข้องมากที่สุดเมื่อมีเหตุการณ์การโจมตีหรือเหตุการณ์ฉุกเฉินกับเว็บไซต์ เพราะเมื่อพบว่าเว็บไซต์ถูกโจมตี สิ่งที่ทำได้ในเบื้องต้นคือการกู้คืนข้อมูลเวอร์ชันก่อนที่จะพบว่าถูกโจมตี เนื่องจากหน่วยงานไม่สามารถทราบได้ว่าการโจมตีที่เกิดขึ้นส่งผลกระทบต่อข้อมูลหรือการทำงานส่วนใดของเว็บไซต์บ้าง เช่น อาจถูกแก้ไขข้อมูลในฐานข้อมูลของเว็บไซต์ในส่วนที่ยากต่อการตรวจสอบโดยปกติ

หน้าที่สำคัญอย่างหนึ่งของผู้ดูแลเครื่องบริการเว็บ คือ การดูแลรักษาความสมบูรณ์ของข้อมูลบนเครื่องบริการเว็บ เนื่องจากเครื่องบริการเว็บเป็นเครื่องบริการที่ถูกเปิดเผยและมีความสำคัญที่สุดบนระบบเครือข่ายขององค์กร โดยองค์ประกอบหลักในการสำรองข้อมูลบนเครื่องบริการเว็บ มี 2 องค์ประกอบ ได้แก่ 1) การสำรองข้อมูลระบบปฏิบัติการบนเครื่องบริการเว็บ 2) การดูแลรักษาข้อมูลสำรองที่เชื่อถือได้ (Authoritative Copy) ของเว็บไซต์ โดยมีการป้องกันแยกต่างเครื่องบริการเว็บ เพื่อให้เกิดความมั่นใจว่าจะสามารถกู้คืนเว็บไซต์ให้อยู่ในสภาพสมบูรณ์ พร้อมใช้งานได้เหมือนเดิม

ผู้ดูแลเครื่องบริการเว็บจำเป็นต้องดำเนินการสำรองข้อมูลของเครื่องบริการเว็บอย่างสม่ำเสมอ เนื่องจากอาจจะเกิดความผิดพลาดขึ้นกับเครื่องบริการเว็บจากการกระทำที่ประสงค์ร้ายหรือโดยไม่ตั้งใจ หรือจากความขัดข้องของฮาร์ดแวร์และซอฟต์แวร์ นอกจากนี้ หน่วยงานภาครัฐหรือองค์กรต่าง ๆ ได้มีการกำหนดกฎเกณฑ์ข้อบังคับในการสำรองและเก็บรักษาข้อมูลของเครื่องบริการเว็บ องค์กรต่าง ๆ จำเป็นต้องสร้างนโยบายในการสำรองข้อมูลของเครื่องบริการเว็บ



ข้อกำหนดที่เกี่ยวกับการปฏิบัติในการสำรองข้อมูลของเครื่องบริการเว็บ

ซึ่งอ้างอิงจากแนวทางมาตรฐานของ NIST มีดังต่อไปนี้

1. แนวปฏิบัติต้องสอดคล้องกับข้อกำหนดทางกฎหมาย
2. แนวปฏิบัติต้องสอดคล้องกับข้อผูกพันทางสัญญา
3. แนวปฏิบัติต้องสอดคล้องกับแนวนโยบายที่เกี่ยวข้องขององค์กร
4. จุดประสงค์และขอบเขตของแนวปฏิบัติ
5. บทบาทหน้าที่ของผู้ที่เกี่ยวข้อง
6. เครื่องบริการเว็บที่เกี่ยวข้องกับแนวปฏิบัติ
7. คำนิยามของศัพท์เฉพาะ โดยเฉพาะในทางกฎหมายและทางเทคนิค
8. รายละเอียดของกฎหมาย ข้อผูกพันสัญญา และนโยบายขององค์กรที่เกี่ยวข้อง
9. ความถี่ของการสำรองข้อมูล
10. ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองได้รับการดูแลรักษาและการป้องกันอย่างเหมาะสม
11. ขั้นตอนสำหรับยืนยันว่าข้อมูลได้รับการทำลายหรือมีการเก็บรักษา เมื่อไม่มีความจำเป็นในการใช้งาน
12. ขั้นตอนสำหรับยืนยันว่าข้อมูลที่มีการสำรองสามารถถูกเรียกออกมาใช้งานได้อย่างถูกต้องในกรณีที่มีการร้องขอ
13. ความรับผิดชอบของผู้ที่มีส่วนร่วมในการเก็บรักษา การป้องกัน และการทำลายข้อมูล
14. ระยะเวลาในการเก็บรักษาข้อมูลแต่ละประเภท
15. หน้าที่รับผิดชอบของทีมสำรองข้อมูล ในกรณีที่องค์กรมีทีมดังกล่าว

หัวข้อเนื้อหาการเรียนรู้ที่ 2
กฎ ระเบียบ ข้อบังคับในการรักษาข้อมูลจราจรทางคอมพิวเตอร์

เว็บไซต์ที่ไม่มีการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลการใช้งานของผู้ใช้ (Log) เมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุขัดข้องทางเทคนิคขึ้นระหว่างการให้บริการ จะไม่สามารถตรวจหาสาเหตุได้ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์หรือข้อมูลการเข้าใช้งานเว็บไซต์ (Log) ตามหลักสูตรนี้ให้เป็นไปตาม ข้อกำหนดในพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2560 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ

พระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ได้ประกาศใช้ในวันที่ 19 กรกฎาคม พ.ศ. 2550 และที่แก้ไขเพิ่มเติมฉบับที่ 2 ประกาศในราชกิจจานุเบกษาเมื่อวันที่ 23 มกราคม พ.ศ. 2560 โดยให้ประชาชนคำนึงถึงการดำเนินกิจกรรมต่าง ๆ ให้เกิดความถูกต้องเป็นสำคัญที่มีความครอบคลุมในด้านกฎหมาย และมีความรอบคอบในการดำเนินกิจกรรมและเพิ่มการระมัดระวังให้มากขึ้น โดยสามารถสรุปเป็นประเด็น ได้ดังนี้

1. กรณีที่มีการใช้ระบบสารสนเทศ โดยที่เจ้าของสารสนเทศไม่อนุญาต ระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 10,000 บาท
2. ล่วงรู้มาตรการป้องกันการเข้าสู่ระบบสารสนเทศของผู้อื่น แล้วนำไปเปิดเผยให้ผู้อื่น ระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท
3. กระทำการเข้าถึงข้อมูลสารสนเทศของผู้อื่นโดยมิชอบที่อยู่ในระบบสารสนเทศ ระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท
4. กระทำการโดยดักรับข้อมูลคอมพิวเตอร์ผ่านเครือข่ายสารสนเทศ ระวางโทษจำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 60,000 บาท
5. ทำให้ข้อมูลที่อยู่ในระบบสารสนเทศเสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมโดยมิชอบ ระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท

6. ทำให้การทำงานของระบบสารสนเทศผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ (การปล่อย MULTIWARE เช่น VIRUS, TROJAN, WORM) ระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท

7. ส่งข้อมูลหรือส่งจดหมายอิเล็กทรอนิกส์ที่มีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ผู้อื่น ระวางโทษปรับไม่เกิน 100,000 บาท

8. ถ้ากระทำความผิดในข้อ (1) (2) (3) (4) หรือ (7) และสร้างความเสียหายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ระวางโทษจำคุก 1 - 7 ปี และปรับตั้งแต่ 20,000 – 140,000 บาท และหากเป็นกรณี (5) หรือ (6) ระวางโทษจำคุก 3 - 15 ปี และปรับตั้งแต่ 60,000 – 300,000 บาท รวมถึงหากทำให้ผู้อื่นเสียชีวิตต้องระวางโทษจำคุกตั้งแต่ 5 – 20 ปี และปรับตั้งแต่ 100,000 – 400,000 บาท

9. ถ้าจำหน่ายเผยแพร่ที่จัดทำโดยเฉพาะเพื่อใช้เป็นเครื่องมือสนับสนุนผู้กระทำความผิด ระวางโทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หากสนับสนุนข้อ (8) ระวางโทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท

10. หากส่งข้อมูลเท็จ หลอกลวง บิดเบือน อนาจาร ทั้งผู้กระทำหรือให้การสนับสนุน ระวางโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท

11. หากมีการดัดแปลง ตัดต่อ หรือแปลงรูปภาพบุคคลอื่น และทำให้บุคคลนั้นหรือบุคคลที่เกี่ยวข้องเสียหาย ระวางโทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 200,000 บาท

ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564

ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2564 กำหนดให้เก็บข้อมูลไว้เป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่ข้อมูลเข้าสู่ระบบและสิ้นสุดการใช้บริการ แต่ทั้งนี้ไม่เกิน 2 ปี ตามคำสั่งของพนักงานเจ้าหน้าที่เป็นรายกรณี และหากเจ้าหน้าที่ขอเรียกดูข้อมูลแล้วไม่ปฏิบัติตามคำสั่ง จะถูกปรับไม่เกิน 200,000 บาท และต่อเนื่องอีกวันละไม่เกิน 5,000 บาท จนกว่าจะปฏิบัติได้ถูกต้อง ผู้ให้บริการที่ต้องจัดเก็บคือ ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นโดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น รวมถึงผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น อันได้แก่ ผู้ประกอบกิจการโทรคมนาคม และการกระจายภาพและเสียง ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ ผู้ให้บริการร้านอินเทอร์เน็ต ผู้ให้บริการโปรแกรมคอมพิวเตอร์ซอฟต์แวร์ เทคโนโลยีปัญญาประดิษฐ์ แอปพลิเคชันที่ทำให้บุคคลสามารถติดต่อสื่อสารข้อมูลระหว่างกันได้ ผู้ให้บริการสื่อสังคมออนไลน์ ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่าง ๆ ผู้ให้บริการคลาวด์ ผู้ให้บริการดิจิทัล (Digital Service Provider) ที่ใช้เครือข่ายคอมพิวเตอร์หรือระบบคอมพิวเตอร์เป็นส่วนหนึ่งของการให้บริการ

ประเภทของ Log File ที่มีความจำเป็นต้องเก็บไว้ตามกฎหมาย

แบ่งออกเป็น 7 ประเภท ดังนี้

1. Personal Computer log file

คือ การจัดเก็บข้อมูลบนคอมพิวเตอร์ส่วนบุคคล เช่น อีเมล ชื่อที่ระบุตัวตนผู้ใช้ (User ID)

2. Network Access Server or RADIUS server log file

คือ การจัดเก็บข้อมูลจากการเข้าเครือข่ายอินเทอร์เน็ตหรือขอบเขตการเข้าไปใช้ เช่น IP ของผู้ใช้ เลขหมายเรียกเข้า

3. Email Server log file (SMTP log)

คือ การจัดเก็บข้อมูลในกลุ่มของผู้ใช้บริการอินเทอร์เน็ต เช่น อีเมลของผู้รับ-ผู้ส่ง หมายเลขสมาชิกกลุ่ม

4. FTP Server log file

คือ การจัดเก็บข้อมูลบนอินเทอร์เน็ตที่เกิดจากการโอนถ่ายข้อมูล เช่น รูปภาพ ข้อความ เพลง บทความ โปรแกรมต่าง ๆ

5. Web Server (HTTP server) log file

คือ การจัดเก็บข้อมูลอินเทอร์เน็ตบนเครื่องของผู้ให้บริการเว็บ เช่น ข้อมูลการเข้าถึง วันเวลา เส้นทางการเชื่อมโยง

6. UseNet log file

คือ การจัดเก็บข้อมูลบนเครือข่ายขนาดใหญ่ เช่น ข้อมูลการเข้าถึงเครือข่าย ชื่อเครื่อง หมายเลขเครื่อง จุดประสงค์ในการเข้า

7. IRC log file

คือ การจัดเก็บข้อมูลที่เกิดจากการแลกเปลี่ยนข้อมูลการสื่อสารผ่านเครือข่ายอินเทอร์เน็ต เช่น ข้อมูล เมื่อมีการเข้าถึงเครือข่าย วันที่ เวลาเริ่มต้นและเวลาสิ้นสุดที่ใช้บริการนั้น ๆ ชื่อที่ระบุตัวตนผู้ใช้ (User ID) หมายเลข IP

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 เป็นพระราชบัญญัติที่เกี่ยวข้องกับเรื่องข้อมูลส่วนบุคคลทุกคนโดยตรง โดยเป็นกฎหมายที่จะเน้นไปที่การสร้างมาตรฐานให้กับองค์กรต่าง ๆ ที่มีการเก็บรวบรวมข้อมูลส่วนบุคคลรวมถึงการนำไปใช้ ซึ่ง พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มีขอบเขต ดังนี้

"ข้อมูลส่วนบุคคล"

หมายถึง ข้อมูลใด ๆ ที่ระบุไปถึง "เจ้าของข้อมูล" ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม

"เจ้าของข้อมูล"

หมายถึง บุคคลที่ข้อมูลส่วนบุคคลนั้นระบุไปถึง ไม่ใช่กรณีที่บุคคลมีความเป็นเจ้าของ (Ownership) ข้อมูล หรือเป็นผู้สร้างหรือเก็บรวบรวมข้อมูลนั้นเองเท่านั้น

"บุคคล" (Natural Person)

ในที่นี้หมายถึง บุคคลธรรมดาที่มีชีวิตอยู่ ไม่รวมถึง "นิติบุคคล" (Juridical Person) ที่จัดตั้งขึ้นตามกฎหมาย

"ข้อมูลส่วนบุคคล" จึงเป็น **"ข้อมูล"** ทั้งหลายที่สามารถใช้ระบุถึงบุคคลที่เป็น **"เจ้าของข้อมูล"** โดย

- แม้ว่าจะเป็นข้อมูลที่อยู่ในรูปแบบกระดาษหรือในรูปแบบอื่น ๆ แต่ได้มีไว้เพื่อจะนำไปใช้ประมวลผลต่อไป
- แม้ว่าตัวข้อมูลที่มีอยู่นั้นจะไม่สามารถใช้ระบุถึงบุคคลได้แต่หากใช้ร่วมกันกับข้อมูลหรือสารสนเทศอื่น ๆ ประกอบกันแล้วก็จะสามารถระบุถึงตัวบุคคลได้ โดยไม่จำเป็นว่าข้อมูลหรือสารสนเทศอื่นนั้นได้มีอยู่ด้วยกัน
- โดยไม่ขึ้นอยู่กับว่าข้อมูลนั้นจะเป็นจริงหรือเป็นเท็จ

โดยหลักการแล้วผู้ประกอบการมีความรับผิดชอบในข้อมูลส่วนบุคคลที่ตนเองได้เก็บรวบรวมและใช้ นอกจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลแล้ว ผู้ประกอบการยังมีความรับผิดจากการไม่บริหารจัดการข้อมูลที่ดีพอด้วย

ผู้ประกอบการจำเป็นต้องแสดงให้เห็นว่ามีขั้นตอนการกำหนดข้อมูลให้เป็นข้อมูลส่วนบุคคลในองค์กร โดยอย่างน้อยประกอบด้วย

1. การกำหนดนโยบายและนิยามความหมายของข้อมูลส่วนบุคคล
2. การกำหนดขั้นตอนการตรวจสอบข้อมูลส่วนบุคคล
3. การระบุความเชื่อมโยงและเส้นทางการส่งข้อมูลส่วนบุคคลที่จะเกิดขึ้นในองค์กร รวมถึงระบุแหล่งที่จะได้มาซึ่งข้อมูลส่วนบุคคลทั้งหลาย
4. การกำหนดความเสี่ยงของข้อมูลส่วนบุคคลชุดต่าง ๆ
5. มีมาตรการคุ้มครองข้อมูลส่วนบุคคล

การประมวลผลข้อมูลจะเกิดขึ้นอย่างถูกต้องได้เมื่อมีฐาน (basis) หรือเหตุผลในการประมวลผลข้อมูลนั้น ๆ ไม่ว่าจะเป็นการเก็บรวบรวม การใช้ การเผยแพร่ และการเก็บรักษา ในการประมวลผลข้อมูลแต่ละครั้งผู้ควบคุมข้อมูลจะต้องระบุฐานในการประมวลผลให้ได้ฐานใดฐานหนึ่ง แจ้งฐานในการประมวลผลให้เจ้าของข้อมูลทราบ และดำเนินการกับข้อมูลนั้น ๆ ตามข้อจำกัดที่แตกต่างกันของแต่ละฐาน รวมถึงเก็บบันทึกไว้ด้วยว่าใช้ฐานใด การประมวลผลข้อมูลแต่ละชุด ตามมาตรา 24 ของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลฯ ให้ความยินยอมเป็นหลักในการประมวลผลข้อมูล ซึ่งความยินยอม (consent) เป็นฐานที่มีความสำคัญที่ให้เจ้าของข้อมูลสามารถ “เลือก” จัดการข้อมูลของตนเองได้ ซึ่งมีเงื่อนไขของความยินยอม ดังนี้

ความยินยอมต้องขอก่อนจะมีการประมวลผลเกิดขึ้น

ความยินยอมต้องไม่เป็นเงื่อนไขในการให้บริการ

ความยินยอมต้องอยู่แยกส่วนกับเงื่อนไขในการให้บริการ

วัตถุประสงค์ของการประมวลผลข้อมูลต้องเฉพาะเจาะจง

ความยินยอมต้องชัดเจน ไม่คลุมเครือ

การขอความยินยอมแบบชัดแจ้ง (Explicit Consent) สำหรับข้อมูลที่อ่อนไหว

โดยพระราชบัญญัตินี้ ตามมาตรา 5 ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าการเก็บรวบรวม ใช้ หรือเปิดเผยนั้น ได้กระทำใน หรือนอกราชอาณาจักร ก็ตามในกรณีที่ผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลอยู่นอกราชอาณาจักร พระราชบัญญัตินี้ให้ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของเจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร โดยการดำเนินกิจกรรมของผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลดังกล่าว เมื่อเป็นกิจกรรม ดังต่อไปนี้

1. การเสนอสินค้าหรือบริการให้แก่เจ้าของข้อมูลส่วนบุคคลซึ่งอยู่ในราชอาณาจักร ไม่ว่าจะมีการชำระเงินของเจ้าของข้อมูลส่วนบุคคลหรือไม่ก็ตาม
2. การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

แนวปฏิบัติสำหรับฝ่ายเทคโนโลยีสารสนเทศเกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

โดยหลักการสำหรับการคุ้มครองข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่จะต้องจัดให้มีมาตรการปกป้องที่เหมาะสมเพื่อคุ้มครองสิทธิและเสรีภาพของเจ้าของข้อมูลส่วนบุคคล โดยจะต้องมีมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการองค์กร (technical and organizational measures) ในการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เพื่อประมวลผลและดำเนินการเกี่ยวกับข้อมูลส่วนบุคคลให้ถูกต้องตามกฎหมาย โดยมาตรการเชิงเทคนิคและมาตรการเชิงบริหารจัดการองค์กร ควรจัดองค์ประกอบให้ครบ 3 ส่วน ได้แก่ บุคลากร (people) กระบวนการ (process) และเทคโนโลยี (technology) ในภาพรวมที่นอกเหนือจากประเด็นด้านกฎหมายแล้วจะเป็นการดำเนินการที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศ ปัจจุบันมีนิยามและความหมายรวมถึงเทคโนโลยีดิจิทัล (digital technology) โดยครอบคลุมการกำกับดูแลและบริหารจัดการระบบเทคโนโลยีสารสนเทศและด้านมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล ทั้งในส่วนที่ดำเนินการตามกฎหมายและดำเนินการเพื่อจัดการความเสี่ยง ตลอดจนการจัดการเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

โดยงานสารสนเทศจะมีบทบาทเกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล

แบ่งออกเป็น 6 ประเภท ดังนี้

1. การบริหารสถาปัตยกรรมการพัฒนาระบบเพื่อช่วยสนับสนุนการคุ้มครองข้อมูลส่วนบุคคล โดยการวิเคราะห์ความต้องการของระบบสารสนเทศและเครื่องมือเพื่อให้การดำเนินการ บริหารจัดการสิทธิ์ และการจัดการความเสี่ยงขององค์กรสอดคล้องตามหลักการในการคุ้มครองข้อมูลส่วนบุคคล รวมถึงการรักษาความมั่นคงปลอดภัย

2. การให้ความรู้และการสร้างความตระหนักในการคุ้มครองข้อมูลส่วนบุคคลให้มีความสอดคล้องกับนโยบายและขั้นตอนในการดำเนินงานที่กำหนด

3. การพัฒนาระบบที่คำนึงถึงการคุ้มครองข้อมูลส่วนบุคคล เพื่อนำมาใช้ในการประมวลผลข้อมูลส่วนบุคคล โดยคำนึงถึงการออกแบบการคุ้มครองข้อมูลส่วนบุคคลตั้งแต่เริ่มต้นเพื่อลดผลกระทบหรือความเสียหายที่จะเกิดขึ้นกับเจ้าของข้อมูลส่วนบุคคล เช่น การประมวลผลข้อมูลเท่าที่จำเป็นและการนำมาตรการมาประยุกต์ใช้ เช่น การเข้ารหัสข้อมูล การปิดทับข้อมูล

4. การประเมินผลกระทบด้านการคุ้มครองข้อมูลส่วนบุคคล โดยการดำเนินกิจกรรมเกี่ยวกับการตรวจสอบระบบเพื่อให้มีความพร้อมในการคุ้มครองข้อมูลส่วนบุคคล เช่น การใช้ซอฟต์แวร์ในการตรวจสอบแอปพลิเคชัน การตรวจสอบช่องโหว่ของระบบ

5. การเฝ้าระวังและแจ้งเตือนเหตุการณ์ที่กระทบกับการคุ้มครองข้อมูลส่วนบุคคลเพื่อเป็นการป้องกันและลดผลกระทบจากการละเมิดข้อมูลส่วนบุคคล

6. การตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคล โดยต้องดำเนินการแก้ไขเหตุการณ์หากเหตุการณ์ละเมิดมีสาเหตุมาจากเทคโนโลยี จึงควรมีการจัดทำแผนการตอบสนองต่อเหตุการณ์ละเมิดข้อมูลส่วนบุคคลและขั้นตอนในการเก็บรวบรวมหลักฐานและวัตถุพยานอย่างเป็นระบบและมีความน่าเชื่อถือ

บทที่

5 ปฏิบัติตามจรรยาบรรณวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

หัวข้อเนื้อหาการเรียนรู้ที่ 1

จริยธรรมและจรรยาบรรณในการประกอบวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

จริยธรรมในการใช้คอมพิวเตอร์

หลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ โดยทั่วไปเมื่อพิจารณาถึงคุณธรรมจริยธรรมเกี่ยวกับการใช้เทคโนโลยีคอมพิวเตอร์และสารสนเทศแล้ว จะกล่าวถึงใน 4 ประเด็น ที่รู้จักกันในลักษณะตัวย่อว่า PAPA ประกอบด้วย

1 ความเป็นส่วนตัว (Information Privacy)

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ โดยทั่วไป หมายถึง สิทธิ์ที่จะอยู่ตามลำพังและเป็นสิทธิ์ที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธิ์นี้ใช้ได้ครอบคลุมทั้งส่วนบุคคล กลุ่มบุคคล และองค์กรต่าง ๆ โดยมีประเด็นเกี่ยวกับความเป็นส่วนตัว ดังนี้

1.1 การเข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร

1.2 การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล เช่น บริษัทใช้คอมพิวเตอร์ในการตรวจจับหรือเฝ้าดูการปฏิบัติงาน การใช้บริการของพนักงาน ถึงแม้ว่าจะเป็นการติดตามการทำงานเพื่อการพัฒนาคุณภาพการใช้บริการ แต่กิจกรรมหลายอย่างของพนักงานก็ถูกเฝ้าดูด้วย พนักงานสูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

1.3 การใช้ข้อมูลของลูกค้าจากแหล่งต่าง ๆ ที่ไม่ได้ขออนุญาตจัดเก็บเอง เพื่อผลประโยชน์ในการขยายตลาด

1.4 การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น

ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเทอร์เน็ตที่มีการให้โปรโมชัน หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต และที่อยู่อีเมล

2 ความถูกต้อง (Information Accuracy)

ในการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูลนั้น คุณลักษณะที่สำคัญประการหนึ่ง คือ ความน่าเชื่อถือของข้อมูล ทั้งนี้ ข้อมูลจะมีความน่าเชื่อถือมากน้อยเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูลด้วย ประเด็นด้านจริยธรรมที่เกี่ยวข้องกับความถูกต้องของข้อมูล โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบต่อความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่ เช่น ในกรณีที่องค์กรให้ลูกค้าลงทะเบียนด้วยตนเอง หรือกรณีของข้อมูลที่เผยแพร่ผ่านทางเว็บไซต์ อีกประเด็นคือ จะทราบได้อย่างไรว่าข้อผิดพลาดที่เกิดขึ้นนั้นไม่ได้เกิดจากความจงใจ และผู้ใดจะเป็นผู้รับผิดชอบหากเกิดข้อผิดพลาดในการจัดทำข้อมูลและสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าฐานข้อมูล รวมถึงการปรับปรุงข้อมูลให้มีความทันสมัยอยู่เสมอ นอกจากนี้ ควรให้สิทธิ์แก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลของตนเองได้

3 ความเป็นเจ้าของ (Information Property)

สิทธิ์ความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น รถยนต์ คอมพิวเตอร์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น บทเพลง โปรแกรมคอมพิวเตอร์ แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่าง ๆ ได้ เช่น สิ่งพิมพ์ เทป ซีดีรอม

4 การเข้าถึงข้อมูล (Data Accessibility)

ปัจจุบันการใช้งานโปรแกรม หรือระบบคอมพิวเตอร์มักจะมีการกำหนดสิทธิ์ตามระดับของผู้ใช้งาน ทั้งนี้ เพื่อเป็นการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษาความลับของข้อมูล ตัวอย่างสิทธิ์ในการใช้งานระบบ เช่น การบันทึก การแก้ไข ปรับปรุง และการลบ ดังนั้น ในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงของผู้ใช้ และการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ก็ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดสิทธิ์ส่วนบุคคล

จรรยาบรรณนักคอมพิวเตอร์

1 ยึดมั่นในความซื่อสัตย์สุจริต ปฏิบัติหน้าที่และดำรงชีวิตเหมาะสมตามหลักธรรมาภิบาล

1.1 ประกอบวิชาชีพนักคอมพิวเตอร์ด้วยความซื่อสัตย์ สุจริต มีความยุติธรรม ใฝ่หาความรู้ใหม่ ๆ อยู่เสมอ เป็นการพัฒนาตนเอง และงานที่รับผิดชอบ อันจะเป็นการเพิ่มศักยภาพให้ตนเองและหน่วยงานที่สังกัด

1.2 ผู้ประกอบวิชาชีพคอมพิวเตอร์ควรมีความวิริยะอุตสาหะในการปฏิบัติงาน เพื่อให้บรรลุความสำเร็จของงานสูงสุด

2 ตั้งมั่นอยู่ในความถูกต้อง มีเหตุผล และรู้รักสามัคคี

2.1 ไม่คัดลอกผลงานของผู้อื่นมาเป็นของตน เว้นแต่จะได้รับอนุญาตจากเจ้าของสิทธิ์อย่างเป็นลายลักษณ์อักษร

2.2 ให้ความยกย่องและนับถือผู้ร่วมงานและผู้ร่วมอาชีพทุกระดับ ที่มีความรู้ความสามารถ และความประพฤติดี

2.3 รักษา และแสวงหามิตรภาพระหว่างผู้ร่วมงาน และผู้ร่วมอาชีพ

3 ไม่ประพฤติหรือกระทำการใด ๆ อันเป็นเหตุให้เสื่อมเสียเกียรติศักดิ์ในวิชาชีพแห่งตน

3.1 ใช้ความรู้ความสามารถในทางสร้างสรรค์ ไม่ใช้ในทางทำลายหรือกลั่นแกล้งให้ผู้อื่นได้รับความเสียหาย

3.2 ไม่แอบอ้าง อวดอ้าง ดูหมิ่นต่อบุคคลอื่น ๆ หรือกลุ่มวิชาชีพอื่น

3.3 ให้ความร่วมมือในการปฏิบัติหน้าที่เพื่อส่งเสริมเกียรติคุณของวิชาชีพ ผู้ร่วมอาชีพ และเพื่อพัฒนาวิชาชีพ

4 ปฏิบัติหน้าที่ ปฏิบัติตน ในวิชาชีพนักคอมพิวเตอร์ที่ดี เป็นแบบอย่างที่ดีของสังคม

4.1 ไม่เรียกรับหรือยอมรับทรัพย์สินหรือผลประโยชน์อย่างใดอย่างหนึ่งสำหรับตนเองหรือผู้อื่นโดยมิชอบด้วยกฎ ระเบียบ และหลักคุณธรรม จริยธรรม

4.2 ไม่ใช้อำนาจหน้าที่โดยไม่ชอบธรรมในการเอื้อให้ตนเองหรือผู้อื่นได้รับประโยชน์หรือเสียประโยชน์

4.3 ไม่ใช้ความรู้ความสามารถไปในทางล่อลวง หลอกลวง จนเป็นเหตุให้เกิดผลเสียต่อผู้อื่น

5 เคารพในสิทธิเสรีภาพ และความเสมอภาคของผู้อื่น ปฏิบัติหน้าที่ด้วยความโปร่งใส เป็นธรรม

5.1 รับฟังความคิดเห็นอย่างเท่าเทียม แลกเปลี่ยนประสบการณ์ระหว่างบุคคล เครือข่าย และองค์กรที่เกี่ยวข้อง

5.2 เปิดโอกาสให้ประชาชนเข้ามามีส่วนร่วมและสามารถตรวจสอบการปฏิบัติงานได้

จรรยาบรรณสำหรับผู้ใช้อินเทอร์เน็ต

อินเทอร์เน็ตถือได้ว่าเป็นบริการสาธารณะและมีผู้ใช้จำนวนมาก เพื่อให้การใช้งานเป็นไปอย่างถูกต้องและมีประสิทธิภาพ ผู้ที่เข้ามาใช้ควรมีกฎกติกาที่ปฏิบัติร่วมกัน เพื่อป้องกันปัญหาที่จะเกิดขึ้นจากการใช้งานที่ผิดวิธี หรือไม่เหมาะสม ในที่นี้ขอแยกเป็น 2 ประเด็นใหญ่ คือ

1 **มารยาทของผู้ใช้อินเทอร์เน็ต ในฐานะบุคคลที่เข้าไปใช้บริการต่าง ๆ** แบ่งออกเป็น 5 ด้าน คือ

1.1 ด้านการติดต่อสื่อสารกับเครือข่าย

ในการเชื่อมต่อเข้าสู่เครือข่าย ควรใช้ชื่อบัญชี (Internet Account Name) และรหัสผ่าน (Password) ของตนเอง ไม่ควรนำของผู้อื่นมาใช้

ควรเก็บรักษารหัสผ่านของตนเองเป็นความลับ และทำการเปลี่ยนรหัสผ่านเป็นระยะ ๆ รวมทั้งไม่ควรแอบดูหรือถอดรหัสผ่านของผู้อื่น

ควรวางแผนการใช้งานล่วงหน้าก่อนการเชื่อมต่อกับเครือข่ายเพื่อเป็นการประหยัดเวลา

เลือกถ่ายโอนเฉพาะข้อมูลและโปรแกรมต่าง ๆ เท่าที่จำเป็นต่อการใช้งานจริง

ก่อนเข้าใช้บริการต่าง ๆ ควรศึกษากฎ ระเบียบ ข้อกำหนด รวมทั้งธรรมเนียมปฏิบัติของแต่ละเครือข่ายที่ต้องการติดต่อ

1.2 ด้านช่องทางการรับส่งข้อมูลบนเครือข่ายที่จะส่งผลกระทบต่อผู้อื่นในช่วงเวลาที่มีการใช้บริการบนระบบเครือข่ายจำนวนมาก

ในกรณีที่มีการใช้งานระบบเครือข่ายในองค์กรหรือสัญญาณอินเทอร์เน็ตร่วมกัน ในการปฏิบัติงาน ควรหลีกเลี่ยงการติดต่อกับแพลตฟอร์มภายนอก หรือการรับ-ส่งข้อมูลแบบเรียลไทม์ หรือการสื่อสารที่ต้องใช้ทรัพยากรทางอินเทอร์เน็ตจำนวนมาก เช่น การโหลดบิททอเรนท์ (Bit Torrent) หรือไฟล์ขนาดใหญ่ การเล่นเกมออนไลน์ หรือการรับชมการถ่ายทอดสด หรือวิดีโอสตรีมมิง (Video Streaming) ผ่าน YouTube / Twitch

1.3 ด้านการใช้ข้อมูลบนเครือข่าย

เลือกใช้ข้อมูลที่มีความน่าเชื่อถือ มีแหล่งที่มาของผู้เผยแพร่ และที่ติดต่อ

เมื่อนำข้อมูลจากเครือข่ายมาใช้ ควรอ้างอิงแหล่งที่มาของข้อมูลนั้น และไม่ควรแอบอ้างผลงานของผู้อื่นมาเป็นของตนเอง

ไม่ควรนำข้อมูลส่วนตัวของผู้อื่นไปเผยแพร่ก่อนได้รับอนุญาต

1.4 ด้านการติดต่อสื่อสารระหว่างผู้ใช้

ใช้ภาษาที่สุภาพในการติดต่อสื่อสาร และใช้คำให้ถูกความหมาย เขียนถูกต้องตามหลักไวยากรณ์

ใช้ข้อความที่สั้น กระชับ เข้าใจง่าย

ไม่ควรนำความลับ หรือเรื่องส่วนตัวของผู้อื่นมาเป็นหัวข้อในการสนทนา รวมทั้งไม่ใส่ร้ายหรือทำให้บุคคลอื่นเสียหาย

หลีกเลี่ยงการใช้ภาษาที่ดูถูก เหยียดหยามศาสนา วัฒนธรรม และความเชื่อของผู้อื่น

ในการติดต่อสื่อสารกับผู้อื่นควรสอบถามความสมัครใจของผู้ที่ติดต่อด้วย ก่อนที่จะส่งข้อมูล หรือโปรแกรมที่มีขนาดใหญ่ไปยังผู้ที่เราติดต่อด้วย

ไม่ควรส่งไปรษณีย์อิเล็กทรอนิกส์ (e-Mail) ที่ก่อความรำคาญ และความเดือดร้อนแก่ผู้อื่น เช่น จดหมายลูกโซ่

1.5 ด้านระยะเวลาในการใช้บริการ

ควรคำนึงถึงระยะเวลาในการติดต่อกับเครือข่าย เพื่อเปิดโอกาสให้ผู้ใช้คนอื่น ๆ บ้าง

ควรติดต่อกับเครือข่ายเฉพาะช่วงเวลาที่ต้องการใช้งานจริงเท่านั้น

2 **มารยาทของผู้ใช้อินเทอร์เน็ต ในฐานะบุคคลที่ทำหน้าที่เผยแพร่ข้อมูล ข่าวสารต่างๆ** ลงบนอินเทอร์เน็ต ประกอบด้วย

2.1 ควรตรวจสอบความถูกต้องของข้อมูล และข่าวสารต่าง ๆ
ก่อนนำไปเผยแพร่บนเครือข่าย เพื่อให้ได้ข้อมูลที่เป็นจริง

2.2 ควรใช้ภาษาที่สุภาพ และเป็นทางการในการเผยแพร่สิ่งต่าง ๆ บนอินเทอร์เน็ต
และควรเผยแพร่ข้อมูลข่าวสารต่าง ๆ ทั้งภาษาไทยและภาษาอังกฤษ เพื่อให้เป็นมาตรฐานสากล และเพื่อให้ผู้เข้ารับชมสื่อสามารถเข้าถึงเนื้อหาได้มากขึ้น โดยไร้ข้อจำกัดด้านภาษา

2.3 ควรเผยแพร่ข้อมูล และข่าวสารที่เป็นประโยชน์ในทางสร้างสรรค์
ไม่ควรนำเสนอข้อมูลข่าวสารที่ขัดต่อศีลธรรมและจริยธรรมอันดี รวมทั้งข้อมูลที่ก่อให้เกิดความเสียหายต่อผู้อื่น

2.4 ควรบีบอัดภาพหรือข้อมูลขนาดใหญ่
ก่อนนำไปเผยแพร่บนอินเทอร์เน็ต เพื่อประหยัดเวลาในการดึงข้อมูลของผู้ใช้

2.5 ควรระบุแหล่งที่มา
วันเดือนปีที่ทำการเผยแพร่ข้อมูล ที่อยู่ เบอร์โทรศัพท์ของผู้เผยแพร่ รวมทั้งควรมีคำแนะนำ และคำอธิบายการใช้ข้อมูลที่ชัดเจน

2.6 ควรระบุข้อมูล ข่าวสารที่เผยแพร่ให้ชัดเจน
ว่าเป็นโฆษณา ข่าวลือ ความจริง หรือความคิดเห็น

2.7 ไม่ควรเผยแพร่ข้อมูล ข่าวสาร รวมทั้งโปรแกรมของผู้อื่นก่อนได้รับอนุญาตจากเจ้าของ
และที่สำคัญคือ ไม่ควรแก้ไข เปลี่ยนแปลงข้อมูลของผู้อื่นที่เผยแพร่บนเครือข่าย

2.8 ไม่ควรเผยแพร่โปรแกรมที่นำความเสียหาย
เช่น ไวรัสคอมพิวเตอร์เข้าสู่ระบบเครือข่าย และควรตรวจสอบแฟ้มข้อมูล ข่าวสาร หรือโปรแกรม ว่าปลอดไวรัส ก่อนเผยแพร่เข้าสู่ระบบอินเทอร์เน็ต

ความรับผิดชอบในการสื่อสาร และแลกเปลี่ยนข้อมูลอย่างมีมารยาท

อินเทอร์เน็ตช่วยให้เราสามารถติดต่อสื่อสารและมีปฏิสัมพันธ์กับผู้อื่นได้อย่างสะดวก เพื่อให้เกิดการแลกเปลี่ยนข่าวสารระหว่างกัน หรือมีส่วนร่วมแลกเปลี่ยนความเห็น ตามการสื่อสารที่เกิดขึ้นอย่างรวดเร็ว และบางครั้ง การไม่แสดงตัวตนที่แท้จริง ก็อาจทำให้เกิดการสื่อสารที่ขาดมารยาทที่ดีได้ง่าย ซึ่งควรมีความตระหนักถึงมารยาทในการใช้อินเทอร์เน็ต (netiquette) สื่อสารกับผู้อื่นอย่างสุภาพ คำนึงถึงผลกระทบที่จะเกิดกับผู้อื่น และเป็นแบบอย่างที่ดีในโลกออนไลน์ ดังนี้

1. อย่ากระพือความขัดแย้ง หลีกเลี่ยงการใช้ภาษารุนแรงและก้าวร้าว
2. หลีกเลี่ยงการประชดประชัน เราต้องเข้าใจว่าการสื่อสารผ่านอินเทอร์เน็ตนั้นไม่เห็นภาษากายและสีหน้า ซึ่งช่วยในการสื่อสาร ดังนั้น การแสดงความเห็นเชิงประชดประชันอาจทำให้เกิดความเข้าใจผิดได้ง่าย
3. อย่าโกหก ซื่อสัตย์ต่อผู้อื่นและไม่เสแสร้งปลอมตัวเป็นคนอื่น เว้นแต่กรณีที่จำเป็นต้องปกปิดอัตลักษณ์
4. ใช้อินเทอร์เน็ตโดยคำนึงถึงผลกระทบที่มีต่อผู้อื่น เช่น ไม่แชร์ข้อมูลส่วนบุคคลของคนอื่นในสื่อสาธารณะ ไม่ส่งต่ออีเมลส่วนตัวของผู้อื่นให้บุคคลที่สามโดยไม่ได้รับอนุญาต
5. อย่าโพสต์หรือแชร์ข้อมูลส่วนบุคคลทั้งของตนเองและผู้อื่น ที่อาจนำภัยอันตรายมาได้ โดยเฉพาะกับคนไม่รู้จักและเว็บไซต์ที่ดูน่าสงสัย และไม่รองรับการเข้ารหัส เช่น ไม่แชร์แผนการท่องเที่ยวที่อาจทำให้ผู้ประสงค์ร้ายรู้ว่าเราจะไม่อยู่บ้านเวลาไหน
6. ใช้อินเทอร์เน็ตให้เหมาะสมกับสถานการณ์และบริบท เช่น ไม่ส่งข้อความหรือเล่นโทรศัพท์มือถือระหว่างที่สนทนากับผู้อื่น หรือขณะร่วมโต๊ะอาหาร หรือเรียนรู้กฎของชุมชนออนไลน์ที่เราสนใจก่อนเข้าร่วม

7. อย่าโพสต์ความรู้สึกส่วนตัวเกี่ยวกับงานหรือความสัมพันธ์ หากต้องการสื่อสารในเรื่องที่มีอารมณ์ความรู้สึกเข้ามาเกี่ยวข้องมาก ๆ พยายามสื่อสารกับคนที่เกี่ยวข้องโดยตรงด้วยช่องทางที่มีความเป็นส่วนตัว

8. อย่าแชร์ข้อมูลหรือข่าวสารโดยไม่ได้ตรวจสอบให้ดีก่อน โดยเฉพาะในกรณีที่อาจทำให้บุคคลหรือองค์กรใดเสื่อมเสียชื่อเสียง

ความรับผิดชอบ
ในการใช้และอ้างอิงผลงานของผู้อื่น

อินเทอร์เน็ตกลายเป็นแหล่งข้อมูลสำคัญในการเรียนรู้ แต่การที่อินเทอร์เน็ตช่วยให้เราเข้าถึง แชร์ รวมถึงคัดลอกผลงานของผู้อื่นได้ง่าย ไม่ได้แปลว่าเรามีสิทธิ์ใช้ผลงานของผู้อื่นโดยไม่ต้องขออนุญาต ก่อนจะใช้ผลงานของผู้อื่น ถือเป็นความรับผิดชอบที่จะต้องตรวจสอบว่า ผลงานชิ้นนั้นยังติดลิขสิทธิ์หรือได้ตกเป็นของสาธารณะ (public domain) เนื่องจากความคุ้มครองลิขสิทธิ์ได้หมดลงแล้ว เป็นผลงานของรัฐบาลที่ใช้เงินสาธารณะสร้างขึ้นมา หรือผู้สร้างสรรค์เลือกที่จะมอบผลงานให้เป็นของสาธารณะ ในกรณีที่ติดลิขสิทธิ์ เราต้องตรวจสอบว่าการใช้งานนั้นถือเป็นการใช้อย่างเป็นธรรมหรือไม่ ถ้าไม่ก็ถือเป็นหน้าที่ของเราในการขออนุญาต ตัวอย่างกรณีที่ถือว่าละเมิดลิขสิทธิ์ เช่น การนำผลงานทั้งหมดของผู้อื่น ไม่ว่าจะเป็นหนังสือ บทความ ภาพ วิดีโอ เพลง กราฟิก โพสต์ความเห็น หรือผลงานสร้างสรรค์ของผู้อื่น ไปเผยแพร่ในเว็บไซต์ อีเมล หรือโซเชียลมีเดียโดยไม่ได้รับอนุญาต

นอกจากการละเมิดลิขสิทธิ์ซึ่งเป็นปัญหาด้านกฎหมาย การขโมยผลงานของผู้อื่น (plagiarism) ก็ถือเป็นปัญหาเชิงจริยธรรมในแวดวงวิชาการ นักเรียน/นักศึกษา/นักวิจัย ต้องมีความรับผิดชอบในการอ้างอิงผลงานของผู้อื่น ไม่ว่าแหล่งที่มาจะมาจากในออนไลน์หรือออฟไลน์ก็ตาม เช่น ไม่นำคำพูด แนวคิด ข้อค้นพบในผลงานของผู้อื่นมาใช้โดยไม่อ้างอิงให้เหมาะสม

โดยสามารถสรุป 5 ขั้นตอนในการใช้และอ้างอิงผลงานสร้างสรรค์อย่างรับผิดชอบ คือ 1) ตรวจสอบว่าใครเป็นเจ้าของผลงาน 2) ขออนุญาตก่อนใช้ 3) ให้เครดิตกับเจ้าของผลงาน 4) ซื้อสิทธิ์การใช้ (ถ้าจำเป็น) และ 5) ใช้อย่างมีความรับผิดชอบ

ความรับผิดชอบ ในการปฏิบัติตามกฎหมาย

พลเมืองดิจิทัลที่ดีควรศึกษาว่ามีกฎหมายและข้อบังคับอะไรบ้างที่กำกับการใช้อินเทอร์เน็ตของเรา เช่น กฎหมายลิขสิทธิ์ กฎหมายกำกับดูแลเนื้อหาออนไลน์ กฎหมายว่าด้วยความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ รวมถึงตระหนักถึงผลกระทบจากการละเมิดกฎหมายด้วย

ข้อควรระวังด้านกฎหมายมี ดังนี้

1. ไม่ขโมยอัตลักษณ์ออนไลน์
2. ไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น
3. ไม่ดาวน์โหลดเพลง ภาพยนตร์ หรือผลงานสร้างสรรค์ของผู้อื่นผ่านช่องทางที่ผิดกฎหมาย รวมถึงไม่เผยแพร่งานที่ติดลิขสิทธิ์ไปตามช่องทางที่ผิดกฎหมาย
4. อย่าสร้างหรือเผยแพร่มัลแวร์ ซอฟต์แวร์ เว็บไซต์ หรือแอปพลิเคชันที่ขโมยข้อมูลสำคัญของผู้อื่นหรือทำลายระบบ
5. ไม่โพสต์หรือแชร์เนื้อหาที่สุ่มเสี่ยงผิดกฎหมาย เช่น สื่อลามก อนาจาร ประทุษวาจา ข้อความหมิ่นประมาท
6. ไม่ละเมิดความเป็นส่วนตัวของผู้อื่น เช่น การดักจับอีเมลของผู้อื่น หรือแอบขโมยรหัสผ่าน เพื่อเข้าไปดูบัญชีเฟซบุ๊กของผู้อื่นโดยไม่ได้รับอนุญาต

ความรับผิดชอบ ในการรักษาความปลอดภัย

อินเทอร์เน็ตเต็มไปด้วยความเสี่ยง เช่น อาชญากรรมคอมพิวเตอร์ ภัยคุกคามไซเบอร์ การขโมยอัตลักษณ์ออนไลน์ พลเมืองดิจิทัลจำเป็นต้องเรียนรู้วิธีป้องกันตัวเองจากความเสี่ยงออนไลน์ อาทิเช่น

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัปเดตให้เป็นเวอร์ชันใหม่อย่างสม่ำเสมอ
2. ตรวจสอบเวลาเปิดไฟล์แนบทางอีเมล และระมัดระวังก่อนจะกดคลิกลิงก์เชื่อมไปยังส่วนอื่น ๆ
3. เปิดใช้การพิสูจน์ตัวตนสองระดับ
4. ติดตั้งใช้งานแอปพลิเคชันสำหรับติดตามและล็อกโทรศัพท์มือถือระยะไกล ในกรณีที่อุปกรณ์สูญหาย
5. สำรองข้อมูลไว้หลายแห่งเพื่อป้องกันข้อมูลสูญหาย
6. การตั้งล็อกหน้าจอบนคอมพิวเตอร์หรืออุปกรณ์เคลื่อนที่ต่าง ๆ ด้วยรหัสผ่าน พินโค้ด ลายนิ้วมือ ฯลฯ
7. การเข้ารหัสป้องกันการเข้าถึงข้อมูลที่อยู่ในอุปกรณ์เชื่อมต่อภายนอก เช่น ยูเอสบีไดร์ฟ

จริยธรรมการทำธุรกิจออนไลน์

ปัจจุบันเทคโนโลยีสารสนเทศมีการขยายตัวอย่างรวดเร็ว มีช่องทางในการเข้าใช้งานได้ง่ายขึ้น ผลของการพัฒนา ส่งผลให้มีการประยุกต์ใช้งานเทคโนโลยีสารสนเทศกันอย่างกว้างขวาง โดยเฉพาะการทำธุรกิจออนไลน์หรือธุรกิจทาง e-Commerce ซึ่งมีการทำธุรกิจประเภทนี้กันอย่างแพร่หลาย ทำให้เกิดผลทั้งด้านที่เป็นประโยชน์และด้านที่เป็นโทษในการแสวงหาผลประโยชน์จากทำธุรกิจออนไลน์ ดังนั้น การหาประโยชน์จากทางใดทางหนึ่ง จึงต้องเกี่ยวข้องกับการมีจรรยาบรรณและจริยธรรม ซึ่งการมีจรรยาบรรณและจริยธรรมนี้เป็นเรื่องสำคัญที่ต้องมีการปลูกฝังให้กับผู้ที่ประกอบธุรกิจออนไลน์ เพื่อให้ผู้ประกอบการเหล่านี้มีการทำธุรกิจที่แสวงหาประโยชน์อย่างเหมาะสมและสร้างสรรค์ มิใช่จะหาประโยชน์ที่มิชอบอย่างเดียว

การทำพาณิชย์อิเล็กทรอนิกส์ หรือการค้าขายสินค้าบนอินเทอร์เน็ตนี้ ผู้ขายจะนำเสนอสินค้าเป็นรูปภาพและราคา มีการบรรยายรายละเอียดและสรรพคุณของสินค้ากำกับไว้ หากผู้ซื้อมีความประสงค์จะซื้อสินค้าและสินค้านั้นตรงความต้องการของผู้ซื้อ ก็จะเกิดการติดต่อแลกเปลี่ยนเพื่อซื้อขายสินค้านั้น ๆ แต่การติดต่อซื้อขายลักษณะนี้ส่วนใหญ่ทางผู้ซื้อจะไม่สามารถเห็นสินค้าที่ต้องการซื้อได้ ผู้ซื้อจะต้องมีความไว้วางใจและมีความมั่นใจในตัวผู้ขาย ว่าสินค้าจะถูกต้องตามที่บรรยายรายละเอียดไว้ และจะไม่หลอกลวงขายสินค้าให้ผู้ซื้อ ผู้ขายก็ต้องมีความมั่นใจในตัวผู้ซื้อว่าจะทำการชำระเงินตามที่ตกลงกันไว้ ซึ่งในสังคมปัจจุบันมีการหลอกลวงผู้บริโภคอยู่จำนวนไม่น้อย และมีการฉ้อโกงร้านค้าจำนวนมาก แสดงให้เห็นว่า มีทั้งผู้ขาย/ผู้ซื้อ สินค้าที่ไม่มีจริยธรรมอยู่จำนวนมาก

จริยธรรมทางธุรกิจสารสนเทศ หมายถึง หลักเกณฑ์ในการประพฤติตนร่วมกันในการทำธุรกิจออนไลน์ โดยบุคคลต้องประพฤติปฏิบัติตามเพื่อให้เกิดความเชื่อมั่นและความพึงพอใจในการซื้อขายสินค้าระหว่างกันและกัน การดำเนินธุรกิจออนไลน์ เมื่อมีกลุ่มคนจำนวนมากทั้งในและนอกประเทศในการติดต่อซื้อขายกัน อาจมีความเสี่ยงต่อการฉ้อโกง การหลอกลวง หรือการนำเสนอให้บิดเบือนไปจากความเป็นจริง จริยธรรมทางธุรกิจออนไลน์จะช่วยให้การดำเนินธุรกิจเป็นไปตามแนวทางที่ดี ที่ถูกต้อง และเกิดปัญหาในการซื้อขายกันน้อยที่สุด หากบุคคลแต่ละคนนั้นปฏิบัติตามจริยธรรมที่กำหนดไว้

เมื่อปี ค.ศ. 2001 ศูนย์สหประชาชาติเพื่อการอำนวยความสะดวกด้านการค้าและธุรกรรมอิเล็กทรอนิกส์ (United Nations Centre for Trade Facilitation and Electronic Business : UN/CEFACT) ได้มีข้อเสนอแนะฉบับที่ 32 เกี่ยวกับเรื่องเครื่องมือในการกำกับดูแลตนเองของพาณิชย์อิเล็กทรอนิกส์ – จริยธรรมทางธุรกิจ “e-Commerce Self-Regulatory Instruments (Codes of Conducts)” โดยมีความเห็นว่าการจัดทำ “Codes of Conducts” หรือจริยธรรมทางธุรกิจ สามารถดำเนินการได้ทันที รวดเร็วกว่าการออกกฎหมาย มีความยืดหยุ่นสามารถนำไปปรับใช้ได้ตามความเหมาะสมของแต่ละบุคคลและองค์กร โดยต้องคำนึงถึงหลักการพื้นฐานที่สำคัญ คือ ความเป็นธรรมต่อทุกฝ่าย โดยจริยธรรมมีองค์ประกอบ ดังนี้

1 ความเชื่อถือได้ (Reliability)

โดยข้อมูลที่เผยแพร่จะต้องมีความเชื่อถือได้ และเป็นที่ยอมรับในการติดต่อสื่อสารทางอิเล็กทรอนิกส์ ความเชื่อถือได้ของระบบองค์กร และความเชื่อถือได้ของชนิดของลายมือชื่ออิเล็กทรอนิกส์

2 ความโปร่งใส (Transparency)

ข้อมูลที่มีอยู่จะต้องมีความโปร่งใสอย่างสูงสุด เช่น ข้อมูลการติดต่อ ข้อมูลทะเบียนการค้า หมายเลขประจำตัวผู้เสียภาษี รายละเอียดสินค้า รายละเอียดค่าใช้จ่ายรูปแบบและเงื่อนไขการชำระเงิน ระยะเวลาการจัดส่งสินค้า การรับประกันสินค้า กฎหมายเกี่ยวกับการทำธุรกรรม

3 ความลับและความเป็นส่วนตัว (Confidentiality and Privacy)

ต้องมีการเคารพสิทธิ์ความเป็นส่วนตัวของผู้อื่น เช่น ข้อมูลส่วนบุคคลต้องเก็บเป็นความลับ และนำไปใช้เมื่อได้รับการยินยอมจากอีกฝ่ายเท่านั้น มีมาตรการรักษาข้อมูลที่เป็นความลับ และมีการคุ้มครองสิทธิ์ในทรัพย์สินทางปัญญา

หัวข้อเนื้อหาการเรียนรู้ที่ 2 Data Life Cycle

Data Life Cycle

Data Life Cycle คือ ลำดับขั้นตอนของข้อมูลโดยเริ่มตั้งแต่ การเกิดขึ้นของข้อมูล วิธีเก็บข้อมูล การนำไปใช้ การแชร์ข้อมูล การจัดเก็บถาวร และการทำลายข้อมูล หรือเราก็อาจจะมองได้ว่า ถ้าเปรียบ Data Life Cycle กับสิ่งมีชีวิตแล้ว ก็จะคล้ายกับ Life Cycle ของสิ่งมีชีวิตที่มีจุดเริ่มต้น คือ การเกิด ถ้ามองในมุมของข้อมูล ก็คือ การสร้างสรรค์ให้ข้อมูลเกิดขึ้น หรือ Create และจุดสุดท้าย คือ การเสียชีวิต ก็คือ การทำลายทิ้งหรือ Destroy นั่นเอง

1. Create

การสร้างสรรค์ให้ข้อมูลเกิดขึ้น ไม่ว่าจะมาจากวิธีใด ๆ ก็ตาม รวมไปถึงการซื้อข้อมูล หรือการรับข้อมูลจากหน่วยอื่นมาใช้จัดเก็บภายหลัง

2. Store

เมื่อเราได้ข้อมูลมาแล้วจะเลือกการจัดเก็บวิธีใด เพื่อให้ข้อมูลที่เราได้มีความเป็นระเบียบ ใช้งานได้ง่าย ไม่สูญหายหรือถูกทำลายได้ และให้ผู้ที่นำไปใช้ต่อ สามารถนำไปใช้ได้อย่างรวดเร็ว ไม่ว่าจะเก็บลงในรูปแบบ File หรือ Database

3. Use

เมื่อเรามีการจัดเก็บข้อมูลลงไปในรูปแบบที่ต้องการแล้ว ก็จะเป็นการนำข้อมูลนั้นมาใช้ให้เกิดประโยชน์สูงสุด เช่น การวิเคราะห์ข้อมูลเพื่อหามุมมองที่น่าสนใจ การจัดทำเป็นรายงานสรุปผล แต่เราก็ต้องสำรองข้อมูลไว้ด้วย เพื่อป้องกันเหตุที่ข้อมูลเกิดความเสียหายหรือสูญหาย

4. Share

การแชร์ข้อมูลกัน โดยเฉพาะระหว่างหน่วยงาน ต้องตระหนักด้วยว่า ข้อมูลบางประเภทไม่ใช่ว่าทุกคนจะสามารถเข้าถึงได้ หรือข้อมูลบางประเภทก็ควรจะรู้แค่ในหน่วยงานนั้น ๆ ขั้นตอนนี้จึงต้องกำหนดการเข้าถึงข้อมูล และถ้าหน่วยงานนั้นมีการนำข้อมูลไปใช้ เจ้าของข้อมูลก็ต้องมีการกำหนดเงื่อนไข (Condition) ในการใช้งานให้ชัดเจน

5. Archive

เมื่อข้อมูลมีการนำใช้ไปในช่วงระยะเวลาที่เหมาะสมหรือไม่ได้ใช้งานแล้ว ก็ต้องมีการจัดเก็บถาวร โดยข้อมูลนั้นจะต้องไม่มีการลบ ปรับปรุง หรือแก้ไขอีก และสามารถนำกลับมาใช้งานใหม่ได้ตามต้องการ

6. Destroy

เมื่อข้อมูลที่ได้มีการจัดเก็บถาวรแล้ว หากจัดเก็บในระยะเวลาที่นานหรือเกินกว่าระยะที่กำหนดแล้ว ก็ต้องมีการทำลายข้อมูลนั้นทิ้งไป

การปฏิบัติตามแนวปฏิบัติของ Data Life Cycle

Data Governance หรือการจัดทำธรรมาภิบาลข้อมูล เป็นการวางนโยบายเพื่อใช้ในการกำกับดูแลข้อมูล โดยรวมทั้งกระบวนการข้อมูลทั้งหมด บุคคลที่เกี่ยวข้อง เครื่องมือในการจัดการข้อมูลและป้องกันข้อมูล เพื่อให้องค์กรเกิดความมั่นใจว่าข้อมูลที่นำมาใช้มีความถูกต้อง สมบูรณ์ มั่นคงปลอดภัย เชื่อถือได้ และนำไปใช้งานได้ง่าย หรือเรียกได้ว่า การที่องค์กรมีการจัดทำ Data Governance ขึ้นมาก็เพื่อสร้าง Life Cycle ให้กับข้อมูลขององค์กรนั่นเอง

1. Data Architecture

เป็นการอธิบายถึงโครงสร้างและการเชื่อมโยงของข้อมูลทั้งหมดภายในองค์กร รวมไปถึงทิศทางการไหลของข้อมูลในระดับต่าง ๆ ทั้งหมด เพื่อให้คนในองค์กรเข้าใจภาพรวมทั้งหมดขององค์กร

2. Data Modeling & Design

เป็นการสร้างแบบจำลองข้อมูลเพื่อนำแนวคิดต่าง ๆ มานำเสนอในรูปแบบจำลองที่อธิบายได้เข้าใจง่าย และเพื่อสร้างความเข้าใจระหว่าง ผู้ออกแบบฐานข้อมูล ผู้เขียนโปรแกรม และผู้ใช้งานระบบฐานข้อมูล อาจเป็นในรูปแบบของไดอะแกรม (Diagram) หรือตาราง โดยแบ่งออกเป็นได้ 3 ระดับคือ Conceptual Data Model, Logical Data Model และ Physical Data Model

3. Data Storage & Operations

เป็นการดำเนินการจัดการข้อมูลภายในองค์กรตลอด Life Cycle โดยเริ่มตั้งแต่การวางแผนการใช้งาน การสำรองข้อมูล (Backup) การกู้คืนข้อมูล (Restore) การจัดเก็บถาวร (Archive) และกระบวนการต่าง ๆ ที่เกี่ยวกับข้อมูล เพื่อให้ข้อมูลมีความถูกต้องและไม่สูญหาย

4. Data Security

เป็นขั้นตอนการสร้างความมั่นคงปลอดภัยของข้อมูลในบริบทของการรักษาความลับ ความถูกต้องของข้อมูล ความพร้อมใช้งานของข้อมูล โดยต้องดำเนินงานตั้งแต่การวางแผน การจัดทำ การปฏิบัติตาม และการบังคับใช้นโยบายและขั้นตอนในการรักษาความมั่นคงปลอดภัย

5. Data Integration & Interoperability

เป็นขั้นตอนการรวบรวมข้อมูลมาจากแหล่งต่าง ๆ ในรูปแบบที่สอดคล้องกันเข้ามาอยู่ในแหล่งเดียวกัน เพื่อนำไปใช้ในการจัดทำ Master Data, Data Warehouse และ Data Lake สิ่งที่จะได้มาจากขั้นตอนนี้เพิ่มเติมคือการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน ซึ่งเป็นการทำงานร่วมแบบข้ามหน่วยงาน ทำให้เกิดการกำหนดมาตรฐานหรือข้อตกลงร่วมกันระหว่างหน่วยงานหรือระบบขึ้น เพื่อให้เกิดการควบคุมและจัดการคุณภาพของข้อมูลได้ดียิ่งขึ้น

6. Reference & Master Data

เป็นการบริหารจัดการข้อมูลเพื่อให้ทุกหน่วยงานสามารถเข้าถึงและใช้ข้อมูลร่วมกันได้ โดยข้อมูลอาจเก็บไว้แหล่งเดียวหรือมีระบบที่ใช้จัดเก็บเพื่อลดความซ้ำซ้อนกันของข้อมูลที่มีอยู่ในระบบ ด้วยการกำหนดมาตรฐานต่าง ๆ โดยข้อมูลที่เป็น ข้อมูลหลัก (Master Data) หมายถึง ข้อมูลที่สร้างและได้รับการใช้งานอยู่ภายในขอบเขตองค์กร เช่น ข้อมูลพนักงาน ข้อมูลสินค้า ข้อมูลผู้ขาย ส่วน ข้อมูลอ้างอิง (Reference Data) หมายถึง ข้อมูลที่มีความเป็นสากลและมีการใช้งานโดยทั่วไป เช่น ข้อมูลชื่อจังหวัด ข้อมูลรหัสไปรษณีย์

7. Data Warehousing & Business Intelligent

เป็นการดำเนินการรวบรวมข้อมูลจากแหล่งข้อมูลที่หลากหลาย รวมถึงรูปแบบที่หลากหลายมาเก็บในคลังข้อมูล โดยผ่านกระบวนการและจัดทำให้อยู่ในรูปแบบที่เหมาะสม เพื่อนำไปวิเคราะห์ข้อมูลต่อไป

8. Document & Content

เป็นการวางแผนการจัดการ การเข้าถึง การใช้งาน และการควบคุมกิจกรรมต่าง ๆ ที่เกี่ยวกับข้อมูลที่ไม่มีโครงสร้างหรือแบบกึ่งโครงสร้าง เช่น การจัดเก็บ การป้องกันความเสียหาย การเข้าถึงข้อมูล ทั้งที่เก็บอยู่ในรูปแบบกระดาษ และไฟล์อิเล็กทรอนิกส์ มีข้อความ รูปภาพ เสียง ภาพเคลื่อนไหว ฯลฯ

9. Metadata Management

เป็นการบริหารจัดการและกำหนดมาตรฐานข้อมูลที่ใช้กำกับและอธิบายข้อมูลหลักหรือข้อมูลอื่น ๆ ซึ่งรายละเอียดใน Metadata จะทำให้ทราบถึงคุณลักษณะของข้อมูล เพื่อทำให้ผู้ใช้งานเข้าใจข้อมูลและระบบ รวมถึงขั้นตอนการทำงานได้อย่างถูกต้องและตรงกัน

10. Data Quality Management

เป็นการวางแผนการดำเนินการและการควบคุมกิจกรรมต่าง ๆ รวมถึงการปรับปรุงเพื่อให้ข้อมูลมีคุณภาพตลอดเวลา โดยต้องทำให้ข้อมูลมีความถูกต้อง (Accuracy) ครบถ้วน (Completeness) สอดคล้องกัน (Consistency) เป็นปัจจุบัน (Timeliness) ตรงตามความต้องการของผู้ใช้ (Relevancy) และพร้อมใช้ (Availability) ซึ่งอาจมีเครื่องมือหรือซอฟต์แวร์ที่ใช้ในการวัดระดับคุณภาพของข้อมูลและประสิทธิภาพของการนำข้อมูลไปใช้

หัวข้อเนื้อหาการเรียนรู้ที่ 3
ความเป็นส่วนตัวและการรักษาความลับข้อมูลส่วนบุคคลและองค์กร

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ โดยทั่วไป หมายถึง สิทธิ์ที่จะอยู่ตามลำพังและเป็นสิทธิ์ที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธิ์นี้ใช้ได้ครอบคลุมทั้งส่วนบุคคล กลุ่มบุคคล และองค์กรต่าง ๆ ปัจจุบันมีประเด็นเกี่ยวกับความเป็นส่วนตัวที่เป็นข้อน่าสังเกต ดังนี้

1. การเข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร

2. การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล เช่น บริษัทใช้คอมพิวเตอร์ในการตรวจจับหรือเฝ้าดูการปฏิบัติงาน การใช้บริการของพนักงาน ถึงแม้ว่าจะเป็นการติดตามการทำงานเพื่อการพัฒนาคุณภาพการให้บริการ แต่กิจกรรมหลายอย่างของพนักงานก็ถูกเฝ้าดูด้วย พนักงานสูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

3. การใช้ข้อมูลของลูกค้าจากแหล่งต่าง ๆ เพื่อผลประโยชน์ในการขยายตลาด

4. การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น

ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิ์ความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเทอร์เน็ตที่มีการให้โปรโมชัน หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต และที่อยู่อีเมล

สิทธิในความเป็นส่วนตัว และในการคุ้มครองข้อมูลส่วนบุคคล

มาตรา 12 ในปฏิญญาสากลว่าด้วยสิทธิมนุษยชนบัญญัติว่า “บุคคลใดจะถูกแทรกแซงในความเป็นส่วนตัว ครอบครัว ที่อยู่อาศัย หรือการสื่อสาร หรือจะถูกลบหลู่เกียรติยศและชื่อเสียงตามอำเภอใจหรือโดยผิดกฎหมายไม่ได้ ทุกคนมีสิทธิ์ที่จะได้รับความคุ้มครองต่อการแทรกแซงสิทธิ์หรือการลบหลู่ดังกล่าวนั้น” ในโลกดิจิทัลที่มีการเก็บข้อมูลส่วนบุคคลไว้มากมาย พลเมืองมีสิทธิ์เรียกร้องชีวิตส่วนตัวในอินเทอร์เน็ต รวมถึงความเป็นส่วนตัวในการสื่อสารถึงกัน นอกจากนั้น พลเมืองมีสิทธิ์รับรู้ว่าข้อมูลส่วนบุคคลอะไรบ้างที่ถูกบันทึกไว้ จะถูกใช้อย่างไร และเราจะจัดการอะไรกับมันได้บ้าง สิทธิ์ในความเป็นส่วนตัวครอบคลุมสิทธิต่าง ๆ ดังนี้

1 การออกกฎหมายความเป็นส่วนตัว

รัฐมีพันธะหน้าที่ในการจัดทำและบังคับใช้กฎหมายคุ้มครองความเป็นส่วนตัวและข้อมูลส่วนบุคคลของประชาชน โดยกฎหมายดังกล่าวจะต้องสอดคล้องกับหลักสิทธิมนุษยชนสากลและมาตรการการคุ้มครองผู้บริโภค และต้องระบุถึงการป้องกันการละเมิดความเป็นส่วนตัวโดยรัฐและบริษัทเอกชนด้วย

เจ้าหน้าที่รัฐและบริษัทเอกชนมีพันธะที่จะต้องปฏิบัติตามกฎระเบียบและกระบวนการในการจัดการกับข้อมูลส่วนบุคคล การเก็บ ใช้ เปิดเผย และรักษาข้อมูลส่วนบุคคลจะต้องทำโดยโปร่งใสและได้มาตรฐาน และการนำข้อมูลส่วนบุคคลไปใช้ต้องได้รับความยินยอมจากเจ้าของข้อมูลก่อน พลเมืองทุกคนมีสิทธิ์รับรู้ว่ามีข้อมูลส่วนบุคคลอะไรบ้างที่ถูกนำไปใช้หรือส่งต่อให้กับบุคคลที่สามด้วยวัตถุประสงค์อะไร รวมถึงมีสิทธิ์ควบคุมข้อมูลส่วนบุคคลของเราเอง ไม่ว่าจะเป็นการเข้าถึง ตรวจสอบความถูกต้อง การกู้คืน การขอให้ลบข้อมูลส่วนบุคคล และมีสิทธิ์ได้รับแจ้งเมื่อข้อมูลของตนถูกส่งต่อให้บุคคลที่สาม ถูกนำไปใช้ในทางที่ผิด หาย หรือถูกขโมย

เมื่อผู้ให้บริการออนไลน์หรือหน่วยงานรัฐมีความจำเป็นต้องขอข้อมูลส่วนบุคคล ควรเก็บข้อมูลเท่าที่จำเป็นจริง ๆ และต้องเก็บภายในระยะเวลาที่จำเป็นต่อการใช้งานเท่านั้น โดยเมื่อใช้ข้อมูลเสร็จเรียบร้อยแล้วจะต้องลบข้อมูลนั้นทิ้ง การคุ้มครองข้อมูลส่วนบุคคลควรอยู่ภายใต้การกำกับดูแลขององค์กรอิสระที่สามารถทำงานอย่างโปร่งใสโดยปราศจากอิทธิพลทางการเมืองหรือผลประโยชน์เชิงพาณิชย์

2 นโยบายและการตั้งค่าความเป็นส่วนตัว

ผู้ให้บริการออนไลน์ต้องประกาศนโยบายความเป็นส่วนตัวที่ชัดเจนและให้ผู้ใช้เข้าถึงได้ง่าย รวมถึงการตั้งค่าความเป็นส่วนตัวต้องทำได้ง่าย ครอบคลุมรอบด้าน และคำนึงผลประโยชน์ของผู้ใช้เป็นหลัก เช่น การตั้งค่าตั้งต้นให้ปกป้องความเป็นส่วนตัวของผู้ใช้ให้มากที่สุด แล้วหากผู้ใช้ต้องการเปิดเผยข้อมูลมากขึ้น ก็ให้เป็นทางเลือกของผู้ใช้เอง (ไม่ใช่ตั้งค่าตั้งต้นให้เปิดเผยข้อมูล แล้วค่อยให้ผู้ใช้เลือกปิดได้ในภายหลัง)

ผู้ให้บริการออนไลน์ต้องแจ้งให้ผู้ใช้ทราบทุกครั้งหากมีการเปลี่ยนแปลงเงื่อนไขการให้บริการ โดยเฉพาะนโยบายการเก็บข้อมูลผู้ใช้และการตั้งค่าความเป็นส่วนตัว

3 มาตรฐานการรักษาความลับและบูรณภาพของระบบ

ระบบไอทีต้องมีมาตรฐานการรักษาความลับ (confidentiality) และบูรณภาพของระบบ (integrity หมายถึง การรักษาความปลอดภัยเพื่อป้องกันไม่ให้ซอฟต์แวร์อันตรายเข้ามาปรับเปลี่ยนข้อมูลหรือไฟล์ของเราได้) เพื่อป้องกันไม่ให้บุคคลอื่นเข้าสู่ระบบโดยปราศจากความยินยอม

4 การคุ้มครองตัวตนออนไลน์

ประชาชนทุกคนมีสิทธิ์ที่จะสร้างตัวตนในโลกออนไลน์และได้รับความเคารพในตัวตนนั้น ๆ ซึ่งรวมถึงการเลือกไม่เปิดเผยตัวตนแท้จริง ทว่าสิทธิ์ดังกล่าวจะต้องไม่ถูกใช้ในทางที่ผิดหรือเป็นภัยต่อผู้อื่น นอกจากนั้น ข้อมูลการพิสูจน์ตัวตนจะต้องไม่ถูกนำไปใช้หรือเปลี่ยนแปลงโดยปราศจากความยินยอมของเจ้าของ

5 สิทธิ์ในการไม่เปิดเผยตัวและใช้การเข้ารหัส

พลเมืองทุกคนมีสิทธิ์ในการสื่อสารแบบนิรนามในโลกออนไลน์ และมีสิทธิ์ในการใช้เทคโนโลยีการเข้ารหัสเพื่อรักษาความเป็นส่วนตัว ความปลอดภัย และการสื่อสารแบบนิรนาม

6 เสรีภาพจากการสอดแนม

พลเมืองทุกคนมีเสรีภาพที่จะสื่อสารโดยปราศจากการสอดแนมตามอำเภอใจในโลกออนไลน์ เช่น การติดตามข้อมูลพฤติกรรมการใช้อินเทอร์เน็ตของเรา

7 ความเป็นส่วนตัวในที่ทำงาน

ประชาชนมีสิทธิ์ในความเป็นส่วนตัวในที่ทำงาน เช่น การส่งอีเมลส่วนตัวในบริษัท ผู้ว่าจ้างมีหน้าที่แจ้งให้ทราบถึงการตรวจสอบและติดตามข้อมูลการสื่อสารในที่ทำงาน หากไม่มีการแจ้งล่วงหน้า ให้ถือว่าพนักงานมีความเป็นส่วนตัวในการใช้อินเทอร์เน็ตในที่ทำงาน

บทที่

6 ปฏิบัติตามกฎหมายพาณิชย์อิเล็กทรอนิกส์

หัวข้อเนื้อหาการเรียนรู้ที่ 1
ข้อกำหนด ข้อบังคับ และบทลงโทษตามกฎหมายพาณิชย์อิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 (ฉบับแก้ไขเพิ่มเติม) เป็นกฎหมายกลางที่รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ ให้มีผลผูกพันและใช้บังคับได้ตามกฎหมายเพื่อรับรองการใช้ลายมือชื่ออิเล็กทรอนิกส์ด้วยกระบวนการใด ๆ ทางเทคโนโลยีให้เสมอด้วยการลงลายมือชื่อธรรมดาอันส่งผลต่อความเชื่อมั่นมากขึ้นในการทำธุรกรรมทางอิเล็กทรอนิกส์ และกำหนดให้มีการกำกับดูแลการให้บริการเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการให้บริการอื่นที่เกี่ยวข้องกับลายมือชื่ออิเล็กทรอนิกส์

"ธุรกรรม"

หมายถึง การกระทำใด ๆ ที่เกี่ยวกับกิจกรรมในทางแพ่งและพาณิชย์ หรือในการดำเนินงานของรัฐตามที่กำหนดในกฎหมายนี้

"อิเล็กทรอนิกส์"

หมายถึง การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น

"ธุรกรรมทางอิเล็กทรอนิกส์"

หมายถึง ธุรกรรมที่กระทำขึ้นโดยใช้วิธีการทางอิเล็กทรอนิกส์ทั้งหมดหรือแค่บางส่วน

ทั้งนี้ พ.ร.บ. ว่าด้วยว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ ประกอบด้วย **6 หมวดสำคัญ** ได้แก่

หมวด 1 ธุรกรรมทางอิเล็กทรอนิกส์

รองรับการทำธุรกรรมในรูปแบบข้อมูลอิเล็กทรอนิกส์ในเรื่องต่าง ๆ

หมวด 2 ลายมือชื่ออิเล็กทรอนิกส์

รองรับลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

หมวด 3 ธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์

รองรับการกำกับดูแลธุรกิจบริการที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำคัญและมีผลกระทบวงกว้าง

หมวด 3/1 ระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัล

รองรับให้บุคคลสามารถพิสูจน์และยืนยันตัวตนผ่านระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลได้ โดยมีกลไกการควบคุมดูแลผู้ประกอบธุรกิจบริการที่เกี่ยวข้อง เพื่อให้ระบบดังกล่าวมีความน่าเชื่อถือและมั่นคงปลอดภัย

หมวด 4 ธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ

รองรับการให้บริการภาครัฐด้วยวิธีการทางอิเล็กทรอนิกส์

หมวด 5 คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (คธอ.)

รองรับการมีคณะกรรมการเพื่อส่งเสริมและพัฒนาการทำธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

หมวด 6 บทกำหนดโทษ

กำหนดไว้สำหรับหมวดที่ 3 และหมวดที่ 3/1 ในส่วนธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ และระบบการพิสูจน์และยืนยันตัวตนทางดิจิทัลเท่านั้น

สิ่งสำคัญของการลงลายมือชื่อ คือ การทำให้เกิดหลักฐาน ที่สามารถระบุตัวเจ้าของลายมือชื่อ และสามารถแสดงเจตนาของเจ้าของลายมือชื่อเกี่ยวกับข้อความที่ตนเองลงลายมือชื่อได้

สาระสำคัญของ พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

การอนุมัติเห็นชอบ หรือยอมรับข้อความ เช่น การลงลายมือชื่อเพื่อยอมรับข้อกำหนดที่ปรากฏในสัญญา

การรับรองหรือยืนยันความถูกต้องของข้อความ เช่น การลงลายมือชื่อเพื่อรับรองว่าข้อความในแบบแสดงรายการภาษีเงินได้เป็นรายการที่ถูกต้องสมบูรณ์และเป็นความจริง

การตอบแจ้งการเข้าถึงหรือการรับข้อความ (acknowledgement) เช่น การลงลายมือชื่อเพื่อตอบแจ้งการรับเอกสาร

การเป็นพยานให้กับการลงลายมือชื่อหรือการทำธุรกรรมของบุคคลอื่น เช่น การลงลายมือชื่อเพื่อรับรองเอกสาร หรือรับรองลายมือชื่อ (notarization)

พระราชบัญญัติว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และที่แก้ไขเพิ่มเติม

กฎหมายเกี่ยวกับอาชญากรรมทางคอมพิวเตอร์ หรือ **พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์** เพื่อกำหนดมาตรการทางอาญาในการลงโทษผู้กระทำผิดต่อระบบการทำงานของคอมพิวเตอร์ ระบบข้อมูล และระบบเครือข่าย ซึ่งในปัจจุบันยังไม่มีบทบัญญัติของกฎหมายฉบับใดกำหนดว่าเป็นความผิด ทั้งนี้ เพื่อเป็นหลักประกัน สิทธิเสรีภาพและการคุ้มครองการอยู่ร่วมกันของสังคม ทั้งนี้ ได้ยกประเด็นสำคัญของการละเมิดกฎหมาย ทั้ง 13 ตัวอย่างการกระทำ ดังนี้

1. เข้าถึงระบบ หรือข้อมูลของผู้อื่นโดยไม่ชอบ
2. แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย
3. ส่งข้อมูลหรืออีเมลก่อกวนผู้อื่น หรือส่งอีเมลสแปม
4. เข้าถึงระบบ หรือข้อมูลทางด้านความมั่นคงโดยมิชอบ
5. จำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด
6. นำข้อมูลที่ผิด พ.ร.บ. เข้าสู่ระบบคอมพิวเตอร์
7. ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด
8. ตัดต่อ เติม หรือดัดแปลงภาพ
9. เผยแพร่ข้อมูลเกี่ยวกับเยาวชน ต้องกระทำโดยปกปิดไม่ให้ทราบตัวตน
10. เผยแพร่เนื้อหาลามก อนาจาร
11. กด Like & Share ถือเป็นวิธีหนึ่งในการเผยแพร่ข้อมูล
12. แสดงความคิดเห็นที่ผิด พ.ร.บ. คอมพิวเตอร์
13. ละเมิดลิขสิทธิ์ นำผลงานของผู้อื่นมาเป็นของตนเอง

พระราชบัญญัติว่าด้วย ระบบการชำระเงิน พ.ศ. 2560

เพื่อกำหนดกลไกสำคัญทางกฎหมายในการรองรับระบบการโอนเงินทางอิเล็กทรอนิกส์ ทั้งที่เป็นการโอนเงินระหว่างสถาบันการเงินและระบบการชำระเงินรูปแบบใหม่ในรูปของเงินอิเล็กทรอนิกส์ก่อให้เกิดความเชื่อมั่นต่อระบบการทำธุรกรรมทางการเงินและการทำธุรกรรมทางอิเล็กทรอนิกส์มากยิ่งขึ้น

สาระสำคัญเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

1. รูปแบบและเจตนา และการพิสูจน์ในการชำระเงิน
2. สิทธิ์ของเจ้าหนี้ และลูกหนี้ ที่ไม่สามารถชำระเงินได้
3. คำสั่งให้ชำระ ยกเลิกการชำระ
4. รับผิดชอบในความเสียหายจากการโอนเงิน

ปัญหาเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์

1. เงื่อนไขสัญญาส่วนมากมักเป็นสัญญาสำเร็จรูป หรือเป็นสัญญาจำยอม ผู้บริโภคขาดอำนาจการต่อรอง
2. การโอนเงินยังไม่มีกฎหมายเฉพาะในเรื่องพยานหลักฐานทางอิเล็กทรอนิกส์
3. ในการบอกยกเลิกการชำระเงิน
4. วัน เวลา สถานที่ ในการทำธุรกรรม
5. การละเมิดสิทธิส่วนบุคคล
6. เครื่องคอมพิวเตอร์เกิดบกพร่อง

กฎหมายทรัพย์สินทางปัญญา

ทรัพย์สินทางปัญญา (Intellectual Property) หมายถึง ผลงานอันเกิดจากการประดิษฐ์ คิดค้น หรือการสร้างสรรค์ของมนุษย์ ซึ่งเน้นที่ผลผลิตของสติปัญญาและความชำนาญ โดยไม่จำกัดชนิดของการสร้างสรรค์ หรือวิธีการแสดงออกในรูปแบบของสิ่งที่จับต้องได้ เช่น สินค้าต่าง ๆ หรือในรูปแบบของสิ่งของที่จับต้องไม่ได้ เช่น บริการ แนวคิดในการดำเนินธุรกิจ กรรมวิธีการผลิตในอุตสาหกรรม

ทรัพย์สินทางปัญญา แบ่งออกเป็น 2 ประเภท ได้แก่ **ลิขสิทธิ์ (Copyright)** และ **ทรัพย์สินทางอุตสาหกรรม (Industrial Property)** ดังนี้

1 ลิขสิทธิ์ (Copyright)

หมายถึง สิทธิ์แต่เพียงผู้เดียวของเจ้าของลิขสิทธิ์ที่จะกระทำการใด ๆ กับงานที่ผู้สร้างสรรค์ได้ทำขึ้น ไม่ว่างานดังกล่าวจะแสดงออกในรูปแบบอย่างใด โดยประเภทของงานอันมีลิขสิทธิ์ที่กฎหมายกำหนดไว้ ได้แก่

1. วรรณกรรม (รวมถึงโปรแกรมคอมพิวเตอร์)
2. นาฏกรรม
3. ศิลปกรรม
4. ดนตรีกรรม
5. โสตทัศนวัสดุ
6. ภาพยนตร์
7. สิ่งบันทึกเสียง
8. งานแพร่เสียงแพร่ภาพ
9. งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ

นอกจากนี้ กฎหมายลิขสิทธิ์ยังให้ความคุ้มครองถึงสิทธิ์ของนักแสดงด้วย ทั้งนี้ การคุ้มครองลิขสิทธิ์ไม่ครอบคลุมถึงความคิด ขั้นตอน กรรมวิธี ระบบ วิธีใช้ วิธีทำงาน แนวความคิด หลักการ การค้นพบ ทฤษฎีทางวิทยาศาสตร์หรือคณิตศาสตร์

2 ทรัพย์สินทางอุตสาหกรรม (Industrial Property)

หมายถึง ความคิดสร้างสรรค์ที่เกี่ยวกับสินค้าอุตสาหกรรมต่าง ๆ ความคิดสร้างสรรค์นี้ อาจเป็นความคิดในการประดิษฐ์คิดค้น ซึ่งอาจจะเป็นกระบวนการหรือเทคนิคในการผลิต ที่ได้ปรับปรุงหรือคิดค้นขึ้นใหม่ หรือการออกแบบผลิตภัณฑ์อุตสาหกรรมที่เป็นองค์ประกอบและรูปร่างของตัวผลิตภัณฑ์ นอกจากนี้ยังรวมถึง เครื่องหมายการค้า ความลับทางการค้า การคุ้มครองพันธุ์พืช แบบผังภูมิของวงจรรวม และสิ่งบ่งชี้ทางภูมิศาสตร์ เป็นต้น ทรัพย์สินทางอุตสาหกรรม แบ่งออกได้ดังนี้

2.1 สิทธิบัตร (Patent) เป็นการคุ้มครองการคิดค้นสร้างสรรค์ที่เกี่ยวกับการประดิษฐ์ (Invention) หรือการออกแบบผลิตภัณฑ์ (Industrial Design) ที่มีลักษณะตามที่กฎหมายกำหนด ซึ่งแบ่งออกเป็น 3 ประเภท ได้แก่

สิทธิบัตรการประดิษฐ์ (Invention Patent)

หมายถึง การให้ความคุ้มครองการคิดค้นที่เกี่ยวกับลักษณะองค์ประกอบโครงสร้าง หรือกลไกของผลิตภัณฑ์ รวมทั้งกรรรมวิธีในการผลิต การเก็บรักษา หรือการปรับปรุงคุณภาพของผลิตภัณฑ์

อนุสิทธิบัตร (Petty Patent)

หมายถึง การให้ความคุ้มครองการประดิษฐ์จากความคิดสร้างสรรค์ที่มีระดับการพัฒนาเทคโนโลยีไม่สูงมาก โดยอาจเป็นการประดิษฐ์คิดค้นขึ้นใหม่ หรือปรับปรุงจากการประดิษฐ์ที่มีอยู่ก่อนเพียงเล็กน้อย

สิทธิบัตรการออกแบบผลิตภัณฑ์ (Design Patent)

การให้ความคุ้มครองความคิดสร้างสรรค์ที่เกี่ยวกับรูปร่างลักษณะภายนอกของผลิตภัณฑ์ องค์ประกอบของลวดลายหรือสีของผลิตภัณฑ์ ซึ่งสามารถใช้เป็นแบบสำหรับผลิตภัณฑ์อุตสาหกรรมรวมทั้งหัตถกรรมได้ และแตกต่างไปจากเดิม

ผู้ทรงสิทธิบัตรการประดิษฐ์ ผู้ทรงอนุสิทธิบัตร หรือผู้ทรงสิทธิบัตรการออกแบบผลิตภัณฑ์ มีสิทธิ์เด็ดขาด หรือสิทธิ์แต่เพียงผู้เดียวในการแสวงหาผลประโยชน์จากการประดิษฐ์หรือการออกแบบผลิตภัณฑ์ที่ได้รับสิทธิบัตร หรืออนุสิทธิบัตรนั้น ภายในระยะเวลาที่กฎหมายกำหนด

2.2 **แบบผังภูมิของวงจรรวม (Layout-Design of Integrated Circuits)** หมายถึง แบบแผนผัง หรือภาพที่ทำขึ้น ไม่ว่าจะปรากฏในรูปแบบหรือวิธีใด เพื่อแสดงถึงการจัดวาง และการเชื่อมต่อของวงจรไฟฟ้า เช่น ตัวนำไฟฟ้า หรือตัวต้านทาน

2.3 **เครื่องหมายการค้า (Trademark)** หมายถึง เครื่องหมาย สัญลักษณ์ หรือตรา ที่ใช้กับสินค้าหรือบริการ แบ่งออกเป็น 4 ประเภท ได้แก่

เครื่องหมายการค้า (Trademark)

หมายถึง เครื่องหมายที่ใช้ หรือจะใช้กับสินค้าเพื่อแสดงให้เห็นว่า สินค้าที่ใช้เครื่องหมายนั้น แตกต่างกับสินค้าที่ใช้เครื่องหมายการค้าของบุคคลอื่น เช่น กระทิงแดง M-150 มาม่า ไวไว

เครื่องหมายบริการ (Service Mark)

เครื่องหมายที่ใช้ หรือจะใช้กับบริการเพื่อแสดงว่า บริการที่ใช้เครื่องหมายนั้นแตกต่างกับบริการที่ใช้เครื่องหมายบริการของบุคคลอื่น เช่น การบินไทย ธนาคารกรุงไทย

เครื่องหมายรับรอง (Certification Mark)

หมายถึง เครื่องหมายที่เจ้าของเครื่องหมายรับรองใช้ หรือจะใช้เป็นเครื่องหมายที่เกี่ยวข้องกับสินค้าหรือบริการของบุคคลอื่น เพื่อรับรองเกี่ยวกับสินค้าหรือบริการนั้น เช่น ตลาดต้องชม หนูณิชย์บอกต่อความอร่อย ฮาลาล

เครื่องหมายร่วม (Collective Mark)

หมายถึง เครื่องหมายการค้าหรือเครื่องหมายบริการที่ใช้ หรือจะใช้โดยบริษัทหรือวิสาหกิจในกลุ่มเดียวกัน หรือโดยสมาชิกของสมาคม สหกรณ์ สหภาพ สมาพันธ์ กลุ่มบุคคล หรือองค์กรอื่นใดของรัฐ หรือเอกชน เช่น ตราช้างของบริษัท ปูนซีเมนต์ไทย จำกัด (มหาชน)

2.4 ความลับทางการค้า (Trade Secret) หมายถึง ข้อมูลการค้าซึ่งยังไม่เป็นที่รู้จักกันโดยทั่วไป โดยเป็นข้อมูลที่มีมูลค่าในเชิงพาณิชย์ เนื่องจากข้อมูลนั้นเป็นความลับ และมีการดำเนินการตามสมควรเพื่อทำให้ข้อมูลนั้นปกปิดเป็นความลับ

2.5 ชื่อทางการค้า (Tradename) หมายถึง ชื่อที่ใช้ในการประกอบกิจการ เช่น ไทยประกันชีวิต ขนมบ้านอัยการ

2.6 สิ่งบ่งชี้ทางภูมิศาสตร์ (Geographical Indication) หมายถึง สัญลักษณ์หรือสิ่งอื่นใดที่ใช้เรียก หรือใช้แทนแหล่งภูมิศาสตร์และสามารถบ่งบอกว่า สินค้าที่เกิดจากแหล่งภูมิศาสตร์นั้น เป็นสินค้าที่มีคุณภาพ ชื่อเสียง หรือคุณลักษณะเฉพาะของแหล่งภูมิศาสตร์ ดังกล่าว เช่น ข้าวหอมมะลิ ทุ่งกุลาร้องไห้ ผ้าไหมยกดอกลำพูน ส้มโอนครชัยศรี ไข่เค็มไชยา

ในปัจจุบัน มีกฎหมายที่อยู่ในความรับผิดชอบของกรมทรัพย์สินทางปัญญา จำนวน 7 ฉบับ ได้แก่

1. พระราชบัญญัติสิทธิบัตร พ.ศ. 2522 และที่แก้ไขเพิ่มเติม
2. พระราชบัญญัติเครื่องหมายการค้า พ.ศ. 2534 และที่แก้ไขเพิ่มเติม
3. พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 และที่แก้ไขเพิ่มเติม
4. พระราชบัญญัติคุ้มครองแบบของผังภูมิวงจรรวม พ.ศ. 2543
5. พระราชบัญญัติความลับทางการค้า พ.ศ. 2545
6. พระราชบัญญัติคุ้มครองสิ่งบ่งชี้ทางภูมิศาสตร์ พ.ศ. 2546
7. พระราชบัญญัติการผลิตผลิตภัณฑ์ซีดี พ.ศ. 2548

ซึ่งหากละเมิดกฎหมายที่คุ้มครองทรัพย์สินทางปัญญา จะต้องรับโทษตามรายละเอียดกฎหมายที่เกี่ยวกับการป้องปรามการละเมิดทรัพย์สินทางปัญญา ตามระเบียบ **"กฎหมายที่เกี่ยวกับการป้องปรามการละเมิดทรัพย์สินทางปัญญา"**

กฎหมายการจดทะเบียน พาณิชยอิเล็กทรอนิกส์

เพื่อให้ธุรกิจมีความน่าเชื่อถือจากการมีสถานะตัวตนทางกฎหมายเพื่อประโยชน์ในการทำธุรกรรมกับหน่วยงานต่าง ๆ และสร้างความมั่นใจให้ผู้บริโภค กรมพัฒนาธุรกิจการค้าอาศัยอำนาจตามกฎหมายทะเบียนพาณิชย์ให้ผู้ขายสินค้าหรือบริการทางอินเทอร์เน็ต ทั้งเว็บไซต์ ร้านค้าออนไลน์หรือ Social Media ต้องจดทะเบียนพาณิชย์การประกอบธุรกิจพาณิชย์อิเล็กทรอนิกส์เพื่อให้ผู้ประกอบการแสดงตนอย่างเปิดเผยต่อทางราชการ

กรมพัฒนาธุรกิจการค้า ได้จัดทำเกณฑ์มาตรฐานคุณภาพธุรกิจพาณิชย์อิเล็กทรอนิกส์ไทย ซึ่งเทียบเคียงกับเกณฑ์มาตรฐานคุณภาพระดับสากลของ World Trustmark Alliance ที่มีสมาชิกประเทศต่าง ๆ ไม่น้อยกว่า 30 ประเทศ เพื่อเป็นหลักเกณฑ์การจัดทำเว็บไซต์ร้านค้าออนไลน์ที่ดีมีการให้ข้อมูลที่ถูกต้อง ชัดเจน มีความปลอดภัยของระบบการซื้อขายสินค้าเป็นการเพิ่มระดับความน่าเชื่อถือของเว็บไซต์ร้านค้าออนไลน์ไทยให้แก่ผู้บริโภคในการตัดสินใจเลือกซื้อสินค้า/บริการจากร้านค้าออนไลน์

โดยหลักสำคัญ ประกอบด้วย

1. ด้านการเปิดเผยข้อมูลของธุรกิจและรายละเอียดของสินค้าหรือบริการด้วยความถูกต้อง ชัดเจน และเข้าถึงได้ง่าย
2. ด้านเงื่อนไขทางการค้าวิธีการยกเลิกหรือคืนสินค้าและวิธีการติดต่อสื่อสารกับลูกค้า
3. ด้านความปลอดภัยของระบบการใช้งานบนเว็บไซต์ร้านค้าออนไลน์
4. ด้านความปลอดภัยของการเก็บรักษา และใช้งานข้อมูลส่วนบุคคล การจัดเก็บข้อมูลส่วนบุคคล
5. ด้านกลไกการแก้ปัญหาข้อร้องเรียนและการระงับข้อพิพาทจากการซื้อขายสินค้า หรือบริการ ที่ยุติธรรม รวดเร็วทันเวลา

แบ่งเป็น 3 ระดับ ได้แก่ ระดับ Silver ระดับดี Gold ระดับดีมาก และระดับ Platinum ระดับดีเด่น โดยออกให้แก่ผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ที่จดทะเบียนและมีคุณสมบัติครบถ้วนตามหลักเกณฑ์ที่กำหนด เป็นการบ่งบอกว่าเว็บไซต์นั้น ๆ มีคุณภาพผ่านเกณฑ์ประเมินตามมาตรฐานคุณภาพธุรกิจ e-Commerce ของกรมพัฒนาธุรกิจการค้า ซึ่งเมื่อผ่านการตรวจประเมินแล้วจะได้รับเครื่องหมายรับรอง การยื่นขออนุญาตใช้เครื่องหมาย **สามารถยื่นผ่านทาง www.trustmarkthai.com หรือกองพาณิชย์อิเล็กทรอนิกส์กรมพัฒนาธุรกิจการค้า โทร. 02-547-5961 หรืออีเมล dbdverified@dbd.go.th** ศึกษารายละเอียดเพิ่มเติมได้ที่ www.trustmarkthai.com สร้างความน่าเชื่อถือ โดยให้นำไปติดตั้งแสดงบนหน้าเว็บไซต์ร้านค้าออนไลน์

1 ผู้มีหน้าที่จดทะเบียนพาณิชย์

1.1 บุคคลธรรมดา (กิจการเจ้าของคนเดียว)

1.2 ห้างหุ้นส่วนสามัญ

1.3 นิติบุคคลที่ตั้งขึ้นตามกฎหมายต่างประเทศที่มาตั้งสำนักงานสาขาในประเทศไทย

1.4 ห้างหุ้นส่วนสามัญนิติบุคคล ห้างหุ้นส่วนจำกัด

1.5 บริษัทจำกัด บริษัทมหาชนจำกัด

โดยบุคคลตาม 1.1 - 1.5 ต้องประกอบกิจการค้าซึ่งเป็นพาณิชยกิจตามที่รัฐมนตรีว่าการกระทรวงพาณิชย์กำหนดตาม 2

2 กิจการค้าที่เป็นพาณิชยกิจที่ต้องจดทะเบียนพาณิชย์

2.1 บุคคลธรรมดา (กิจการเจ้าของคนเดียว) ห้างหุ้นส่วนสามัญ และนิติบุคคลที่ตั้งขึ้นตามกฎหมายต่างประเทศที่มาตั้งสำนักงานสาขาในประเทศไทย ตาม 1.1-1.3 ซึ่งประกอบกิจการดังต่อไปนี้ ต้องจดทะเบียนพาณิชย์

ผู้ประกอบกิจการโรงสีข้าวและโรงเลื่อยที่ใช้เครื่องจักร

ผู้ประกอบกิจการขายสินค้าไม่ว่าอย่างใด ๆ อย่างเดียวหรือหลายอย่าง คิดรวมทั้งสิ้นในวันหนึ่งขายได้เป็นเงินตั้งแต่ 20 บาทขึ้นไป หรือมีสินค้าดังกล่าวไว้เพื่อขายมีค่ารวมทั้งสิ้นเป็นเงินตั้งแต่ 500 บาทขึ้นไป

นายหน้าหรือตัวแทนค้าต่างซึ่งทำการเกี่ยวกับสินค้าไม่ว่าอย่างใด ๆ อย่างเดียวหรือหลายอย่างก็ตาม และสินค้านั้นมีค่ารวมทั้งสิ้นในวันหนึ่งวันใดเป็นเงินตั้งแต่ 20 บาทขึ้นไป

ผู้ประกอบกิจการหัตถกรรมหรืออุตสาหกรรมไม่ว่าอย่างใด ๆ อย่างเดียวหรือหลายอย่างก็ตาม และขายสินค้าที่ผลิตได้ คิดราคารวมทั้งสิ้นในวันหนึ่งวันใดเป็นเงินตั้งแต่ 20 บาทขึ้นไปหรือในวันหนึ่งวันใดมีสินค้าที่ผลิตได้มีราคารวมทั้งสิ้นตั้งแต่ 500 บาทขึ้นไป

ผู้ประกอบกิจการขนส่งทางทะเล การขนส่งโดยเรือกลไฟหรือเรือยนต์ประจำทาง การขนส่งโดยรถไฟ การขนส่งโดยรถราง การขนส่งโดยรถยนต์ประจำทาง การขายทอดตลาด การรับซื้อขายที่ดิน การให้กู้ยืมเงิน การรับแลกเปลี่ยนหรือซื้อขายเงินตราต่างประเทศ การซื้อหรือขายตั๋วเงิน การธนาคาร การโพยก๊วน การทำโรงรับจำนำ และการทำโรงแรม

ขาย ให้เช่า ผลิต หรือรับจ้างผลิต แผ่นซีดี แถบบันทึก วีดิทัศน์ แผ่นวีดิทัศน์ ดีวีดี หรือแผ่นวีดิทัศน์ระบบดิจิทัล เฉพาะที่เกี่ยวกับการบันเทิง

ขายอัญมณี หรือเครื่องประดับซึ่งประดับด้วยอัญมณี

ซื้อขายสินค้าหรือบริการโดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

บริการอินเทอร์เน็ต

ให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย

บริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

การให้บริการเครื่องคอมพิวเตอร์เพื่อใช้อินเทอร์เน็ต

การให้บริการเครื่องเล่นเกม

การให้บริการฟังเพลงและร้องเพลงโดยคาราโอเกะ

การให้บริการตู้เพลง

โรงงานแปรสภาพ แกะสลัก และการหัตถกรรมจากงาช้าง การค้าปลีก การค้าส่งงาช้างและผลิตภัณฑ์จากงาช้าง

2.2 ห้างหุ้นส่วนสามัญนิติบุคคล ห้างหุ้นส่วนจำกัด บริษัทจำกัด และบริษัทมหาชนจำกัด ซึ่งประกอบกิจการดังต่อไปนี้ ต้องจดทะเบียนพาณิชย์

ขาย ให้เช่า ผลิต หรือรับจ้างผลิต แผ่นซีดี แถบบันทึก วีดิทัศน์ แผ่นวีดิทัศน ดีวีดี หรือแผ่นวีดิทัศน์ระบบดิจิทัล เฉพาะที่เกี่ยวกับการบันเทิง

ขายอัญมณี หรือเครื่องประดับซึ่งประดับด้วยอัญมณี

ซื้อขายสินค้าหรือบริการโดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

บริการอินเทอร์เน็ต

ให้เช่าพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย

บริการเป็นตลาดกลางในการซื้อขายสินค้าหรือบริการ โดยวิธีการใช้สื่ออิเล็กทรอนิกส์ผ่านระบบเครือข่ายอินเทอร์เน็ต

การให้บริการเครื่องคอมพิวเตอร์เพื่อใช้อินเทอร์เน็ต

การให้บริการเครื่องเล่นเกม

การให้บริการฟังเพลงและร้องเพลงโดยคาราโอเกะ

การให้บริการตู้เพลง

โรงงานแปรสภาพ แกะสลัก และการหัตถกรรมจากงาช้าง การค้าปลีก การค้าส่งงาช้างและผลิตภัณฑ์จากงาช้าง

3 กำหนดระยะเวลาการจดทะเบียนพาณิชย์

3.1 จดทะเบียนพาณิชย์ตั้งใหม่ ต้องจดทะเบียนภายใน 30 วันนับแต่วันเริ่มประกอบพาณิชยกิจ

3.2 การเปลี่ยนแปลงรายการจดทะเบียน ต้องจดทะเบียนภายใน 30 วันนับแต่วันที่มีการเปลี่ยนแปลง ตามรายการเปลี่ยนแปลง ดังนี้

เปลี่ยนชื่อที่ใช้ในการประกอบพาณิชยกิจ

เลิกประกอบพาณิชยกิจบางส่วน หรือเพิ่มใหม่

เพิ่มหรือลดเงินทุน

ย้ายสำนักงานใหญ่

เปลี่ยนผู้จัดการ

เจ้าของ/ผู้จัดการเปลี่ยนที่อยู่

ย้าย เลิก หรือเพิ่มสาขา โรงเก็บสินค้า หรือตัวแทนค้าต่าง

แก้ไขเพิ่มเติมผู้เป็นหุ้นส่วน (หุ้นส่วนเข้า/ออก) เงินลงหุ้น จำนวนเงินลงทุนของห้าง

จำนวนเงินทุน จำนวนหุ้น และมูลค่าหุ้นของบริษัทจำกัด จำนวนและมูลค่าหุ้นที่บุคคลแต่ละสัญชาติถืออยู่

รายการอื่น ๆ เช่น แก้ไขชื่อเว็บไซต์ ชื่ออักษรโรมัน ฯลฯ

3.3 เลิกประกอบพาณิชยกิจ ต้องจดทะเบียนภายใน 30 วันนับแต่วันที่เลิกประกอบพาณิชยกิจ

3.4 ใบทะเบียนพาณิชย์สูญหายต้องยื่นขอใบแทนภายใน 30 วันนับแต่วันสูญหาย

4 หน้าที่ของผู้ประกอบพาณิชยกิจ

4.1 ต้องขอจดทะเบียนต่อนายทะเบียนภายใน 30 วัน นับแต่วันที่เริ่มประกอบ เปลี่ยนแปลง หรือเลิกกิจการ

4.2 ต้องแสดงใบทะเบียนพาณิชย์ หรือใบแทนใบทะเบียนพาณิชย์ไว้ ณ สำนักงาน ในที่เปิดเผยและเห็นได้ง่าย

4.3 ต้องจัดให้มีป้ายชื่อที่ใช้ในการประกอบพาณิชยกิจไว้หน้าสำนักงานแห่งใหญ่และสำนักงานสาขา โดยเปิดเผยภายในเวลา 30 วันนับแต่วันที่จดทะเบียนพาณิชย์ ป้ายชื่อให้เขียนเป็นอักษรไทย อ่านง่ายและชัดเจน จะมีอักษรต่างประเทศในป้ายชื่อด้วยก็ได้ และจะต้องตรงกับชื่อที่จดทะเบียนไว้ หากเป็นสำนักงานสาขาจะต้องมีคำว่า “สาขา” ไว้ด้วย

4.4 ต้องยื่นคำขอใบแทนใบทะเบียนพาณิชย์ ภายใน 30 วัน นับแต่วันที่สูญหาย หรือชำรุด

4.5 ต้องไปให้ข้อเท็จจริงเกี่ยวกับรายการจดทะเบียนตามคำสั่งของนายทะเบียน

4.6 ต้องอำนวยความสะดวกแก่นายทะเบียนและพนักงานเจ้าหน้าที่ ซึ่งเข้าทำการตรวจสอบในสำนักงานของผู้ประกอบกิจการ

หัวข้อเนื้อหาการเรียนรู้ที่ 2
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ขอบเขตการบังคับใช้ พ.ร.บ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

ใช้บังคับแก่การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักรมีผลใช้บังคับ กรณีผู้ควบคุมข้อมูลส่วนบุคคล ผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักร หากมีกิจกรรม ดังนี้

1. เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลส่วนบุคคลที่อยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่ก็ตาม
2. เฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลส่วนบุคคลที่เกิดขึ้นในราชอาณาจักร

ข้อยกเว้นการใช้บังคับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

1. การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลของบุคคลที่ทำการเก็บรวบรวมข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนตนหรือเพื่อกิจกรรมในครอบครัวของบุคคลนั้นเท่านั้น
2. การดำเนินการของหน่วยงานของรัฐที่มีหน้าที่ในการรักษาความมั่นคงของรัฐ ซึ่งรวมถึงความมั่นคงทางการคลังของรัฐหรือการรักษาความปลอดภัยของประชาชน รวมทั้งหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน นิติวิทยาศาสตร์ หรือการรักษาความมั่นคงปลอดภัยไซเบอร์
3. บุคคลหรือนิติบุคคลซึ่งใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ทำการเก็บรวบรวมไว้เฉพาะเพื่อกิจการสื่อมวลชนและศิลปกรรมหรืองานวรรณกรรมอันเป็นไปตามจริยธรรมแห่งการประกอบวิชาชีพหรือเป็นประโยชน์สาธารณะเท่านั้น
4. สภาผู้แทนราษฎร วุฒิสภา และรัฐสภา รวมถึงคณะกรรมการที่แต่งตั้งโดยสภาดังกล่าว ซึ่งเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลในการพิจารณาตามหน้าที่และอำนาจของสภาผู้แทนราษฎร วุฒิสภา รัฐสภา หรือคณะกรรมการ แล้วแต่กรณี

5 การพิจารณาพิพากษาคดีของศาลและการดำเนินงานของเจ้าหน้าที่ ในกระบวนการพิจารณาคดี การบังคับคดี และการวางทรัพย์ รวมทั้งการดำเนินงานตามกระบวนการยุติธรรมทางอาญา

6 การดำเนินการกับข้อมูลของบริษัทข้อมูลเครดิต และสมาชิกตามกฎหมายว่าด้วยการประกอบธุรกิจข้อมูลเครดิต

ข้อมูลส่วนบุคคล (Personal Data)

"ข้อมูลส่วนบุคคล" หมายถึง ข้อมูลใด ๆ ที่ระบุไปถึง "เจ้าของข้อมูล" ไม่ว่าทางตรงหรือทางอ้อม โดยไม่รวมถึงข้อมูลของผู้ที่ถึงแก่กรรม ข้อมูลเกี่ยวกับบุคคลที่ทำให้ระบุตัวบุคคลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ที่อยู่ เบอร์โทรศัพท์ อีเมล ข้อมูลทางการเงิน เชื้อชาติ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ

บุคคลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

1 **เจ้าของข้อมูลส่วนบุคคล (Data Subject)**

2 **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller)**
บุคคลหรือนิติบุคคลที่มีอำนาจหน้าที่ตัดสินใจเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

3 **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor)**
บุคคลหรือนิติบุคคลที่ดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล

การเก็บรวบรวม ใช้ หรือเปิดเผย ข้อมูลส่วนบุคคล

1. **Consent ได้รับการยินยอม**
2. **Scientific or Historical Research การจัดทำเอกสารประวัติศาสตร์** หรือจดหมายเหตุเพื่อประโยชน์สาธารณะ หรือที่เกี่ยวกับการศึกษา วิจัย หรือสถิติ
3. **Contract จำเป็นเพื่อการปฏิบัติตามสัญญา**
4. **Public Task จำเป็นเพื่อประโยชน์สาธารณะ หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐ**
5. **Legitimate Interest จำเป็นเพื่อประโยชน์โดยชอบด้วยกฎหมายของผู้ควบคุมข้อมูลส่วนบุคคล** หรือของบุคคล หรือนิติบุคคลอื่น
6. **Legal Obligations การปฏิบัติตามกฎหมาย**
7. **ความยินยอม (Consent)**
8. **ต้องได้รับความยินยอมก่อน หรือขณะเก็บรวบรวมข้อมูลส่วนบุคคล**
9. **ต้องทำโดยชัดแจ้งเป็นหนังสือ หรือทำผ่านระบบอิเล็กทรอนิกส์**
10. **ต้องแจ้งวัตถุประสงค์ในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**
11. **ต้องแยกส่วนใช้ภาษาที่อ่านง่ายและไม่เป็นการหลอกลวง**
12. **ความอิสระในการให้ความยินยอม**
13. **ถอนความยินยอมเมื่อใดก็ได้ เว้นแต่มีข้อจำกัดสิทธิ์**

ความยินยอมของผู้เยาว์

คนไร้ความสามารถ และคนเสมือนไร้ความสามารถ

เนื่องจากโดยทั่วไปแล้วผู้เยาว์มีความสามารถในการเข้าใจวัตถุประสงค์และรายละเอียดของการประมวลผลข้อมูลไม่เท่ากับบุคคลที่บรรลุนิติภาวะแล้ว หรืออาจยังไม่มีความสามารถในเลือกหรือตัดสินใจตามความต้องการของตนเองได้อย่างเต็มที่ รวมถึงการประเมินผลกระทบจากการให้ความยินยอมต่อผู้เยาว์ในอนาคตนั้นก็ทำได้ยาก ทำให้ความยินยอมที่ได้มาจากผู้เยาว์นั้นอาจกลายเป็นความยินยอมที่ไม่สมบูรณ์

นอกเหนือจากการใช้ภาษาที่ผู้เยาว์สามารถเข้าใจได้ง่ายแล้ว ยังอาจพิจารณาใช้เครื่องมือในการป้องกันไม่ให้เกิดการเก็บข้อมูลสงวนบุคคลของผู้เยาว์โดยไม่สมควร เช่น สอบถามว่าผู้ใช้บริการอายุเกินเกณฑ์แล้วหรือไม่ หรือแจ้งเตือนให้มีผู้ปกครองให้ความยินยอม หรือกำหนดให้มีการตั้งค่าโดยผู้ปกครอง (parental setting หรือ parental mode) ในการใช้บริการ เพื่อป้องกันมิให้ผู้เยาว์ให้ข้อมูลส่วนบุคคลโดยรู้เท่าไม่ถึงการณ์ ข้อจำกัดเกี่ยวกับความสามารถในการให้ความยินยอมของผู้เยาว์นั้นเป็นเรื่องที่มีความสำคัญมาก

จึงให้ความคุ้มครองผู้เยาว์เป็นพิเศษในกรณีของการใช้ความยินยอมเป็นฐานในการประมวลผลสำหรับการบริการออนไลน์ประเภท Information Society Services เช่น บริการเกมออนไลน์ การขายสินค้าออนไลน์ ที่มุ่งให้บริการแก่ผู้เยาว์โดยตรง โดยให้ผู้ควบคุมข้อมูลต้องได้รับความยินยอมจากผู้ปกครองจากผู้เยาว์ที่อายุต่ำกว่า 16 ปี หรือต่ำกว่า 13 ปีหากมีกฎหมายภายในของประเทศนั้น ๆ กำหนดไว้

ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (sensitive personal data)

ข้อมูลที่มีความละเอียดอ่อน ได้แก่ เชื้อชาติเผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนา หรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใดที่กระทบต่อเจ้าของข้อมูลส่วนบุคคลนายทำนองเดียวกันตามที่คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลประกาศกำหนด

การเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (sensitive personal data) จะชอบด้วยกฎหมายเมื่อทำตามหลักการหนึ่งหลักการได้ ดังนี้

1. **Explicit consent ได้รับการยินยอมโดยชัดเจน**
2. **Vital Interest ป้องกันหรือระงับอันตรายต่อชีวิต ร่างกาย หรือสุขภาพของบุคคล** ซึ่งเจ้าของข้อมูลส่วนบุคคลไม่สามารถให้ความยินยอมได้
3. **Social protection and non-profit การดำเนินกิจกรรมโดยชอบด้วยกฎหมายที่มีการคุ้มครองที่เหมาะสมของมูลนิธิ สมาคม หรือองค์กรที่ไม่แสวงหากำไร**
4. **Manifestly made public ข้อมูลที่เปิดเผยต่อสาธารณะด้วยความยินยอมโดยชัดแจ้งของเจ้าของข้อมูลส่วนบุคคล**
5. **Legal claims เพื่อการก่อตั้งสิทธิ์เรียกร้องตามกฎหมาย การปฏิบัติตามหรือการใช้สิทธิ์เรียกร้องตามกฎหมาย หรือการยกขึ้นต่อสู้สิทธิ์เรียกร้องตามกฎหมาย**
6. **Legal Obligations จำเป็นในการปฏิบัติตามกฎหมายเฉพาะที่เกี่ยวกับหัวข้อดังนี้**

6.1 preventive or Occupational Medicine

เวชศาสตร์ป้องกันหรืออาชีวเวชศาสตร์ การประเมินความสามารถในการทำงานของลูกจ้าง การวินิจฉัยโรคทางการแพทย์ การให้บริการด้านสุขภาพด้านสังคม การรักษาทางการแพทย์ การจัดการด้านสุขภาพ หรือระบบและการให้บริการด้านสังคมสงเคราะห์

6.2 Public health

ประโยชน์สาธารณะด้านการสาธารณสุข

6.3 Health or social care systems

การคุ้มครองแรงงาน การประกันสังคม หลักประกันสุขภาพแห่งชาติ สวัสดิการเกี่ยวกับการรักษาพยาบาลของผู้มีสิทธิ์ตามกฎหมายความคุ้มครองผู้ประสบภัยจากรถหรือการคุ้มครองทางสังคม

6.4 Archiving, Scientific or historical Research

การศึกษาวิจัยทางวิทยาศาสตร์ ประวัติศาสตร์ หรือสถิ หรือประโยชน์สาธารณะอื่น

6.5 Substantial public interest

ประโยชน์สาธารณะที่สำคัญ

บทที่

7 ปฏิบัติความปลอดภัยในวิชาชีพด้านพาณิชย์อิเล็กทรอนิกส์

หัวข้อเนื้อหาการเรียนรู้ที่ 1
การเข้าใจภัยคุกคามในระบบสารสนเทศ และวิธีการป้องกันภัยคุกคาม และการหลอกลวงออนไลน์

สแกม (Scam)

สแกม (Scam) คือ ลักษณะการหลอกลวงในรูปแบบต่าง ๆ ผ่านระบบอินเทอร์เน็ต แบ่งได้หลายประเภท ยกตัวอย่างเช่น

1 Scam บัตรเครดิต

เป็นลักษณะการหลอกลวงไม่ว่าจะส่งผ่านทางอีเมลเพื่อให้ยืนยันข้อมูลบัตรเครดิตจากธนาคาร เพื่อมิให้ถูกยกเลิกบัตร หรืออาจใช้การโทรศัพท์มาสอบถามข้อมูลโดยอ้างว่าเป็นผู้ให้บริการเครดิตบูโร เพื่อให้ยืนยันบัตรและข้อมูลบนบัตร ซึ่งการหลอกลวงรูปแบบนี้จะทำให้ผู้กระทำความผิดได้ข้อมูลหมายเลขบัตร ชื่อ และรวมถึงข้อมูลเลขหลังบัตร และจะสามารถนำไปใช้ในการซื้อสินค้าหรือบริการออนไลน์ได้

2 Scam ถูกรางวัล

เป็นลักษณะการส่งอีเมลมายังผู้รับโดยมีเนื้อความเกี่ยวกับการที่ผู้รับอีเมลนั้นได้รับการจับฉลากและถูกรางวัลโดยมีจำนวนเงินมหาศาล แต่จะต้องมีการจัดส่งข้อมูลส่วนบุคคล เช่น หน้าพาสปอร์ต หรือหน้าบัตรประชาชน เพื่อยืนยันตัวบุคคล หรือแม้แต่การโอนค่าธรรมเนียมในการรับรางวัลดังกล่าว

3 Scam ค่าธรรมเนียมศุลกากร

เป็นลักษณะการติดต่อสื่อสารหลายช่องทางกับเหยื่อ เช่น การติดต่อทาง Facebook หรือสื่อสังคมออนไลน์ประเภทอื่น ๆ หรือแม้แต่การติดต่อกันผ่านอีเมล โดยเมื่อผู้ไม่หวังดีทำความคุ้นเคยกับเหยื่อได้แล้ว ก็จะมีการเสนอว่าจะส่งของมาให้เช่น เงิน หรือของมีค่า แต่พัสดุติดกระบวนการทางศุลกากร ซึ่งต้องจ่ายค่าธรรมเนียมหรือค่าปรับต่าง ๆ โดยการโอนเงินอาจกระทำโดยโอนไปยังบัญชีธนาคารของคนไทย หรือการโอนเงินผ่านระบบการเงินรูปแบบอื่น เช่น Western Union

4 โรแมนซ์สแกม (Romance Scam)

โรแมนซ์สแกม มีลักษณะที่คล้ายคลึงกับ Scam ค่าธรรมเนียมศุลกากร ซึ่งจะมีผู้ที่เข้ามาติดต่อทำความรู้จักกันไม่ว่าจะเป็นสื่อสังคมออนไลน์ หรือเว็บไซต์หาคู่ ซึ่งการหลอกลวงนั้นจะใช้ความเชื่อใจระหว่างชายหญิง โดยจะมีการสัญญาว่าจะส่งเงิน หรือสิ่งของมาให้ แต่ติดปัญหาเรื่องศุลกากร ซึ่งจะให้เหยื่อทำการโอนเงินให้เป็นค่าธรรมเนียม หรืออาจเป็นกรณีที่มีการถ่ายคลิปวิดีโอไม่ว่าจะตั้งใจหรือถูกแอบถ่าย โดยฝ่ายผู้กระทำความผิดข่มขู่ผู้เสียหายให้โอนเงิน มิเช่นนั้นคลิปวิดีโอนั้นจะถูกเผยแพร่สู่สาธารณะ

การป้องกัน

กระบวนการเกี่ยวกับการหลอกลวงในรูปแบบ Scam นี้ จุดประสงค์หลัก คือ การหลอกเอาเงินจากเหยื่อ โดยใช้ความรัก ความโลภ และความกลัว เป็นเครื่องมือในการทำให้เหยื่อหลงเชื่อ ซึ่งเรื่องดังกล่าวเป็นการตัดสินใจเฉพาะบุคคล ดังนั้น เพื่อเป็นการป้องกันการกระทำความผิดในลักษณะดังกล่าว ผู้ใช้งานอินเทอร์เน็ตควรมีความยับยั้งชั่งใจไม่ให้หลงเชื่อคำชักชวนให้โอนเงินโดยผู้ที่ไม่สามารถยืนยันได้ว่าเป็นใคร โดยดำเนินการในเบื้องต้น ดังนี้

1 การตรวจสอบหัวอีเมล

หากเป็นอีเมลที่ส่งมาจากหน่วยงานที่อ้างว่าเป็นเครดิตบูโร ธนาคาร หรือการอ้างถึงเชื้อชาติจากผู้ส่ง เช่น อีเมลจากกงสุลสหรัฐอเมริกา ผู้ได้รับอีเมลสามารถตรวจสอบข้อมูลหัวอีเมล (e-Mail Header) ในเบื้องต้นเพื่อตรวจสอบว่าปรากฏ IP Address ต้นทางหรือไม่ เพื่อตรวจสอบแหล่งที่มาในเบื้องต้น ได้แก่ ชื่อ ISP รวมถึงประเทศที่ ISP ตั้งอยู่ โดยกระบวนการตรวจสอบหัวอีเมลจะมีความแตกต่างกันขึ้นอยู่กับผู้ให้บริการ เช่น Gmail Yahoo Hotmail ฯลฯ

2 การยืนยันหน่วยงาน/เจ้าหน้าที่

หากมีเจ้าหน้าที่จากหน่วยงาน เช่น เจ้าหน้าที่ศุลกากร ตำรวจ หรือเจ้าหน้าที่ธนาคาร ส่งอีเมลหรือโทรศัพท์มาเพื่อให้ทำการโอนเงินต่าง ๆ เพื่อไม่ให้พัสดุติดค้าง หรือเพื่อป้องกันไม่ให้มีความผิดทางการเงิน ควรขอชื่อ ตำแหน่ง หมายเลขโทรศัพท์ที่ทำงาน ก่อนทำการโอนเงินทุกกรณี และโทรศัพท์สอบถามไปยังหน่วยงานที่เกี่ยวข้องโดยใช้หมายเลขโทรศัพท์ที่ค้นหาเอง และคุยกับเจ้าหน้าที่ที่อ้างชื่อดังกล่าวโดยตรง (มิใช่เพียงแค่สอบถามว่ามีเจ้าหน้าที่ชื่อดังกล่าวอยู่ในหน่วยงานหรือไม่) เพื่อยืนยันตัวตนเจ้าหน้าที่

3 การดำเนินการหากถูกละเมิด

หากรู้ตัวว่าถูกหลอกลวงและหลงเชื่อโดยทำการโอนเงินเป็นที่เรียบร้อยแล้ว ให้ผู้เสียหายจัดเก็บหลักฐาน ได้แก่ รายละเอียดการโอนเงิน เช่น เลขบัญชีธนาคาร ชื่อบัญชี สาขาที่โอน หรือรูปแบบการโอนเงินอื่น ๆ ที่มีหลักฐานการโอน ข้อมูลหัวอีเมล หรือข้อมูลทางคอมพิวเตอร์ใด ๆ ที่มีการติดต่อสื่อสารกับผู้กระทำความผิด

รวบรวมข้อมูลข้างต้น แจ้งสถานีตำรวจใกล้ที่เกิดเหตุ โดยการแจ้งนั้นหากเป็นกรณีการส่งอีเมลและวิธีการใด ๆ ทางคอมพิวเตอร์ ให้ระบุว่าเป็นการถูกหลอกลวงทางอินเทอร์เน็ตอันทำให้เสียทรัพย์ ซึ่งอาจเข้าข่ายเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่แก้ไขเพิ่มเติม

ข้อจำกัดในการตรวจสอบ

เนื่องจากหัวอีเมลเป็นการแสดงผลตามนโยบายการให้บริการของผู้ให้บริการอีเมล ดังนั้น IP Address ที่ปรากฏอาจไม่ใช่ข้อมูลของ “ผู้ส่ง” แต่เป็นเพียงข้อมูลของเครื่องคอมพิวเตอร์แม่ข่ายของผู้ให้บริการอีเมลเท่านั้น

หัวข้อเนื้อหาการเรียนรู้ที่ 2
ปฏิบัติตามหลักการเพื่อรักษาความปลอดภัย

ปฏิบัติตามหลักการเพื่อรักษาความปลอดภัย

กระบวนการที่เกี่ยวข้องกับการป้องกันและตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ซึ่งเรียกว่าเป็นขั้นตอนการป้องกันสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่าง ๆ ถูกเข้าใช้งานโดยผู้ที่ไม่ได้รับสิทธิ์หรือไม่ได้รับอนุญาต หรือเรียกว่า **ความปลอดภัยของเทคโนโลยีสารสนเทศ**

ความมั่นคงปลอดภัย (Security) หมายถึง การทำให้รอดพ้นจากอันตราย หรืออยู่ในสถานะที่มีความปลอดภัยไร้ความกังวล และความกลัวและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือโดยบังเอิญ โดยทั่วไปแล้วเป็นพื้นฐานสำคัญของความมั่นคงปลอดภัยของระบบสารสนเทศ (Information System Security) ซึ่งถือเป็นการป้องกันข้อมูลสารสนเทศรวมถึงองค์ประกอบอื่น ๆ ที่เกี่ยวข้อง เช่น ระบบและฮาร์ดแวร์ที่ใช้ในการจัดเก็บและถ่ายโอนข้อมูลสารสนเทศนั้นให้รอดพ้นจากอันตราย

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ได้กำหนดแนวคิดขึ้นเรียกว่า The CIA triad นั้นมีองค์ประกอบด้วยกัน 3 ประการ ได้แก่ ความลับ (Confidentiality) ความคงสภาพ (Integrity) และความพร้อมใช้งาน (Availability)

1 Confidentiality (ความลับ)

เป็นการรับประกันว่า ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ สารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาตจะถือเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรต้องมีมาตรการป้องกัน เช่น

- การจัดประเภทของสารสนเทศ
- การรักษาความปลอดภัยให้กับแหล่งข้อมูล
- การกำหนดนโยบายความมั่นคงปลอดภัยและนำไปใช้งาน
- การให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัย และนำไปใช้

2 Integrity (ความคงสภาพ)

บูรณภาพของข้อมูล คือ ความถูกต้องสมบูรณ์ ความครบถ้วน และไม่มีสิ่งปลอมปนทั้งก่อน-ระหว่าง-และภายหลังการกระทำการใด ๆ กับข้อมูลชุดนั้น ดังนั้น สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน เช่น ไม่ถูกทำให้เสียหาย หรือไฟล์หายเนื่องจาก virus, worm หรือ Hacker ที่ทำการปลอมปน สร้างความเสียหายให้กับข้อมูลองค์การได้ เช่น แก้ไขยอดเงินในบัญชีธนาคารหรือแก้ไขราคาในการสั่งซื้อ

Integrity ในหลักการของ CIA Triad ทาง Security นั้น เป็นหัวใจสำคัญของการวางกลยุทธ์ด้านความมั่นคงปลอดภัยในยุคที่มีเครือข่ายเชื่อมต่อกัน โดยแบ่งออกเป็นสองประเภท คือ

1. ความน่าเชื่อถือในการทำงานอย่างถูกต้องของระบบ ในภาวะที่มีปัญหา (หรือเรียกว่าปัญหาที่เกิดจาก Soft Error) ตัวอย่างของ Integrity ในลักษณะนี้คือการที่ระบบอาจจะมีปัญหา เช่น ถ้าเป็นการส่งข้อความผ่าน medium อาจจะเกิดปัญหา ทำให้มี error ขึ้น จาก noise หรือ interference ของระบบ หรืออาจเกิด bit flip ซึ่งอาจเกิดขึ้นได้ใน memory หรือ storage จากการทำงานผิดพลาดของระบบเอง (hard disk ทั้งแบบ solid state หรือแบบ spinning disk นั้นมีโอกาสเขียนพลาดได้ตลอดเวลา โดยเฉพาะถ้า storage medium เริ่มมีอายุ) Error ประเภทนี้ จำนวนมากสามารถทำการตรวจสอบได้ด้วยการทำ Error Correction Code (เช่น CRC32) แต่ในหลายกรณี ก็ต้องมีการควบคุมที่ต่างออกไป

2. ความน่าเชื่อถือในการทำงานอย่างถูกต้องของระบบ ในภาวะที่อาจมีคนร้าย (In presence of Adversary) (ในหัวข้อนี้จะพูดถึง Integrity ในลักษณะนี้เป็นหลัก เพราะ หากระบบเราสามารถรับมือกับ Integrity Requirement ในลักษณะนี้ได้ ก็จะสามารถรับมือจากปัญหา Soft Error ได้เช่นกัน)

3 Availability (ความพร้อมใช้งาน)

สารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้ระบบที่ไม่ได้รับอนุญาต การเข้าถึงก็จะล้มเหลวถูกขัดขวาง เช่น การป้องกันให้เครื่องและระบบให้บริการพาณิชย์อิเล็กทรอนิกส์มีสภาพพร้อมใช้งาน สามารถให้บริการได้เสมอ ป้องกัน รับมือ ตอบสนอง และบรรเทาความเสียหายเมื่อถูกโจมตีได้ ดังนั้น จึงต้องมีการระบุตัวตน (Identification) ว่าเป็นสมาชิกและพิสูจน์ได้ว่าได้รับอนุญาตจริง (Authorization)

บรรณานุกรม
REFERENCES

- สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ. (2562). **หลักสูตรการเข้าใจดิจิทัล (Digital Literacy) พ.ศ. 2562**. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. เข้าถึง URL: https://www.dlbaseline.org/explore
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2559). **ข้อเสนอแนะมาตรฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารที่จำเป็นต่อธุรกรรมทางอิเล็กทรอนิกส์ ETDA Recommendation on ICT Standard for Electronic Transactions ขมธอ. 4 – 2559**. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. เข้าถึง URL: https://standard.etda.or.th/wp-content/uploads/2018/09/20150405-ER-WAS-V07-33-R1.pdf
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2559). **ทรัพย์สินทางปัญญากับการใช้เทคโนโลยีสารสนเทศ**. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. เข้าถึง URL: https://www.etda.or.th/publishing-detail/intellectual-property-and-the-use-of-information-technology.html
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2560). **กฎหมายเทคโนโลยีสารสนเทศ (พิมพ์ครั้งที่ 8 ฉบับปรับปรุง)**. กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. เข้าถึง URL: https://www.etda.or.th/publishing-detail/information-technology-law-8th-edition.html
- ศูนย์วิจัยกฎหมายและการพัฒนา (2564). **Thailand Data Protection Guidelines 3.0 แนวปฏิบัติเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล**. คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. เข้าถึง URL: https://www.law.chula.ac.th/event/9705/

ETDA สพธอ
www.etda.or.th

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 21
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310
โทร 0 2123 1234 โทรสาร 0 2123 1200
www.etda.or.th