หน่วยที่ 14

ความมั่นคงปลอดภัยระบบคอมพิวเตอร์

อาจารย์ นาวาโท กรกช วิไลลักษณ์

ชื่อ อาจารย์ นาวาโท กรกช วิไลลักษณ์
วุฒิ วท.บ. (บริหารศาสตร์) โรงเรียนนายเรือ
วท.ม. (เทคโนโลยีการจัดการระบบสารสนเทศ)
มหาวิทยาลัยมหิดล
ตำแหน่ง ประจำกรมกำลังพลทหารเรือ
กรมกำลังพลทหารเรือ
หน่วยที่ปรับปรุง หน่วยที่ 14

มสธ

แผนการสอนประจำหน่วย

ชุดวิชา คอมพิวเตอร์เบื้องต้น

หน่วยที่ 14 ความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ตอนที่

14.1 หลักการสำคัญของการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

14.2 แนวทางการจัดการความมั่นคงปลอดภัยระบบคอมพิวเตอร์

แนวคิด

1. การรักษาความมั่นคงปลอดภัย เป็นการบริหารจัดการความเสี่ยงที่เกิดขึ้นกับระบบคอมพิวเตอร์ให้สามารถรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ กระบวนการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ได้แก่ การพิสูจน์ตัวจริง การกำหนดสิทธิ์ การเฝ้าตรวจความมั่นคงปลอดภัย การกำหนดนโยบายการรักษาความมั่นคงปลอดภัย โดยกระบวนการต่างๆ เหล่านี้หากได้กระทำอย่างถูกต้องสมบูรณ์จะทำให้มั่นใจได้ว่าระบบคอมพิวเตอร์ที่ใช้งานอยู่นั้นถูกใช้งานอย่างมั่นคงปลอดภัย ในการจัดการความมั่นคงปลอดภัยนิยมประยุกต์ใช้แบบจำลองการรักษาความมั่นคงปลอดภัยเพื่อกำหนดนโยบาย วิธีการ ตลอดจนเทคโนโลยีที่จำเป็นสำหรับการบริหารความมั่นคงปลอดภัย
2. ภัยคุกคาม หมายถึง ชุดของเหตุการณ์ที่เกิดขึ้นแล้วจะส่งผลต่อความมั่นคงปลอดภัยของทรัพยากรสารสนเทศ ชุดของเหตุการณ์เหล่านั้นมีวัตถุประสงค์หลักเพื่อการสร้าง การสกัดกั้น การขัดจังหวะ การดัดแปลงแก้ไข และการปลอมแปลง เพื่อทำลายความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ทรัพยากรสารสนเทศที่เป็นเป้าหมาย การประยุกต์ใช้งานเทคโนโลยีร่วมกับการบริหารจัดการความมั่นคงปลอดภัยอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการกำหนดนโยบาย การประยุกต์ใช้งานเทคโนโลยีที่เกี่ยวข้อง และควบคุมการปฏิบัติให้เป็นไปตามที่กำหนดในนโยบายจะสร้างความมั่นใจได้ว่าการผลิต ประมวลผล จัดเก็บ และแสดงผลทรัพยากรสารสนเทศนั้นๆ มีความมั่นคงปลอดภัย

วัตถุประสงค์

เมื่อศึกษาหน่วยที่ 14 จบแล้ว นักศึกษาสามารถ

1. อธิบายแนวคิดเกี่ยวกับหลักการรักษาความมั่นคงปลอดภัยได้
2. อธิบายหลักการใช้งานแบบจำลองความมั่นคงปลอดภัยได้

3. อธิบายแนวคิดเกี่ยวกับภัยคุกคามและการโจมตีได้
4. อธิบายแนวคิดเกี่ยวกับการจัดการความมั่นคงปลอดภัยได้
5. วิเคราะห์แนวทางการประยุกต์ใช้แบบจำลองรักษาความมั่นคงปลอดภัยได้
6. วิเคราะห์แนวทางการจัดการรักษาความมั่นคงปลอดภัยได้

กิจกรรมระหว่างเรียน

1. ทำแบบประเมินผลตนเองก่อนเรียนหน่วยที่ 14
2. ศึกษาเอกสารการสอนตอนที่ 14.1–14.2
3. ปฏิบัติกิจกรรมตามที่ได้รับมอบหมายในเอกสารการสอนแต่ละเรื่อง
4. ทำกิจกรรมประจำชุดวิชา (ถ้ามี)
5. ชมรายการสอนเสริมผ่านทางอินเทอร์เน็ตหรือเข้ารับบริการสอนเสริม (ถ้ามี)
6. ชมสื่ออิเล็กทรอนิกส์ประจำชุดวิชา
7. ทำแบบประเมินผลตนเองหลังเรียนหน่วยที่ 14

สื่อการสอน

1. เอกสารการสอน
2. แบบฝึกปฏิบัติ
3. สื่ออิเล็กทรอนิกส์ประจำชุดวิชา
4. การสอนเสริมทางอินเทอร์เน็ตหรือเอกสารสอนเสริม (ถ้ามี)

การประเมินผล

1. ประเมินผลจากแบบประเมินผลตนเองก่อนเรียนและหลังเรียน
2. ประเมินผลจากกิจกรรมและแนวตอบท้ายเรื่อง
3. ประเมินผลจากกิจกรรมประจำชุดวิชา (ถ้ามี)
4. ประเมินผลจากการสอบไล่ประจำภาคการศึกษา

เมื่ออ่านแผนการสอนแล้ว ขอให้ทำแบบประเมินผลตนเองก่อนเรียน หน่วยที่ 14 ในแบบฝึกปฏิบัติ แล้วจึงศึกษาเอกสารการสอนต่อไป

มสธ

ตอนที่ 14.1
หลักการสำคัญของการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

โปรดอ่านหัวเรื่อง แนวคิด และวัตถุประสงค์ของตอนที่ 14.1 แล้วจึงศึกษารายละเอียดต่อไป

หัวเรื่อง

14.1.1 ความหมายและหลักการรักษาความมั่นคงปลอดภัย

14.1.2 ภัยคุกคามและการโจมตี

แนวคิด

1. ความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หมายถึง การรักษาสภาพความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของระบบคอมพิวเตอร์ นับตั้งแต่ฮาร์ดแวร์ไปจนถึงข้อมูลที่ถูกจัดเก็บในระบบคอมพิวเตอร์นั้น กระบวนการสำคัญที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ได้แก่ การพิสูจน์ตัวจริง การกำหนดสิทธิ์ การเฝ้าตรวจความมั่นคงปลอดภัย การกำหนดนโยบายการรักษาความมั่นคงปลอดภัย โดยกระบวนการต่างๆ เหล่านั้นหากได้กระทำอย่างถูกต้องสมบูรณ์จะทำให้มั่นใจได้ว่าระบบคอมพิวเตอร์ที่ใช้งานอยู่นั้นถูกใช้งานอย่างมั่นคงปลอดภัย แม้ว่าจะมีผู้ละเมิดมาตรการการรักษาความมั่นคงปลอดภัยก็จะสามารถตรวจสอบสาเหตุและค้นหาผู้รับผิดชอบได้
2. ภัยคุกคามคือ ชุดของเหตุการณ์ที่เกิดขึ้นแล้วจะส่งผลต่อความมั่นคงปลอดภัยของทรัพยากรสารสนเทศ โดยมีลักษณะสำคัญคือ การสกัดกั้น การขัดจังหวะ การดัดแปลงแก้ไข และการปลอมแปลง เพื่อทำลายความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ทรัพยากรสารสนเทศที่ตกเป็นเป้าหมาย กล่าวได้ว่าทรัพยากรสารสนเทศที่ภัยคุกคามในหลายๆ รูปแบบแต่มีความเสี่ยงของเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยแตกต่างกันออกไป และภัยคุกคามต่อทรัพยากรสารสนเทศจะไม่ส่งผลใดๆ ต่อทรัพยากรสารสนเทศหากปราศจากการโจมตีต่อทรัพยากรสารสนเทศนั้น

วัตถุประสงค์

เมื่อศึกษาตอนที่ 14.1 จบแล้ว นักศึกษาสามารถ

1. อธิบายหลักการรักษาความมั่นคงปลอดภัยได้
2. อธิบายความหมายและหลักการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ได้
3. อธิบายภัยคุกคามรูปแบบต่างๆ ได้
4. อธิบายหลักการโจมตีได้
5. อธิบายความสัมพันธ์ระหว่างช่องโหว่และการโจมตีได้

เรื่องที่ 14.1.1
ความหมายและหลักการรักษาความมั่นคงปลอดภัย

เมื่อกล่าวถึงการรักษาความมั่นคงปลอดภัย สิ่งที่ผู้คนโดยทั่วไปคำนึงถึงเป็นสิ่งแรกคือ การค้นหาการบุกรุกของผู้ไม่ประสงค์ดีกับระบบคอมพิวเตอร์ซึ่งนิยมเรียกว่า “แฮกเกอร์” รวมถึงการกำจัดโปรแกรมที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของคอมพิวเตอร์ หรือมัลแวร์ประเภทต่างๆ โดยไม่ตระหนักรู้ถึงความหมายที่แท้จริงของ “ความมั่นคงปลอดภัย” ของระบบคอมพิวเตอร์ ซึ่งแท้จริงแล้วมีความหมายครอบคลุมถึง การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรในระบบคอมพิวเตอร์ในทุกๆ ระดับ เริ่มต้นตั้งแต่อุปกรณ์ฮาร์ดแวร์ ระบบปฏิบัติการ ซอฟต์แวร์ต่างๆ ที่ถูกติดตั้ง และการเชื่อมต่อกันเป็นเครือข่าย และรวมถึงข้อมูลหรือสารสนเทศซึ่งถูกจัดเก็บและประมวลผลโดยอุปกรณ์และซอฟต์แวร์ที่เชื่อมต่อเป็นระบบ ความหมายของการรักษาความมั่นคงปลอดภัยในระบบคอมพิวเตอร์จึงมีขอบเขตมากกว่าการรักษาความมั่นคงปลอดภัยให้กับคอมพิวเตอร์หรืออุปกรณ์เพียงอย่างเดียว

1. ทรัพยากรสารสนเทศ

ทรัพยากรสารสนเทศ มีความหมายครอบคลุมถึงเครื่องคอมพิวเตอร์ และอุปกรณ์เชื่อมต่อต่างๆ และครอบคลุมถึงองค์ประกอบอื่นๆ ดังต่อไปนี้

1.1 มนุษย์ (people) ได้แก่ ผู้ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ เช่น ผู้ใช้งาน ผู้ดูแลระบบ ทั้งนี้โดยปกติแล้วมนุษย์จะถูกประเมินเป็นภัยคุกคามหลักต่อทรัพยากรสารสนเทศเนื่องจากมีเป็นทรัพยากรที่เป็นมีจุดอ่อนมากที่สุดในการรักษาความมั่นคงปลอดภัย แม้ว่าทรัพยากรอื่นๆ จะถูกปกป้องและกำหนดมาตรการอย่างรัดกุมที่สุดแล้ว หากผู้คนที่เกี่ยวข้องกับทรัพยากรนั้นละเลยหรือขาดความตระหนักรู้ก็จะส่งผลให้ทรัพยากรนั้นถูกโจมตีสำเร็จ เช่น การให้บริการรับฝากไฟล์ผ่านอินเทอร์เน็ตซึ่งเลือกใช้เทคโนโลยีการรักษาความมั่นคงปลอดภัยที่เข้มแข็งมาก แต่ผู้ใช้งานบันทึกข้อมูลสำหรับใช้พิสูจน์ตัวจริงและกำหนดสิทธิ์โดยเขียนลงบนกระดาษแปะไว้ที่หน้าจอมอนิเตอร์ ย่อมเป็นการเพิ่มความเสี่ยงที่จะมีผู้ไม่ประสงค์ดีใช้ข้อมูลดังกล่าวเข้าถึงข้อมูลที่ถูกจัดเก็บในระบบนั้น โดยอาจเปลี่ยนแปลง แก้ไข หรือลบข้อมูลนั้นโดยไม่ได้รับอนุญาต เป็นต้น นอกจากนี้มนุษย์ยังเป็นองค์ประกอบสำคัญของการโจมตีความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ด้วยเหตุจูงใจที่หลากหลาย เช่น ความต้องการชื่อเสียง ความโลภ แนวทางทางการเมือง โดยเมื่อโจมตีสำเร็จอาจได้รับค่าจ้างหรือการยอมรับจากสังคมที่เขาต้องการ เป็นต้น

1.2 ฮาร์ดแวร์และอุปกรณ์ต่อเชื่อมต่าง ๆ (hardware and its peripheral) ในที่นี้มีความหมายรวมถึงเครื่องคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟนซึ่งมีความสามารถในการรับข้อมูล ประมวลผล แสดงผล และเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ได้ ความไม่มั่นคงปลอดภัยของอุปกรณ์เหล่านี้อาจเกิดขึ้นเนื่องจากมีภัยคุกคามเกิดขึ้นกับอุปกรณ์โดยตรง เช่น การขโมย ซึ่งส่งผลให้เจ้าของไม่สามารถใช้งานได้

หรือนำข้อมูลส่วนบุคคลในอุปกรณ์นั้นไปเปิดเผยทำให้ความลับของข้อมูลนั้นถูกทำลายลง หรืออาจเกิดจากไฟฟ้ากระชากและทำให้ข้อมูลที่จัดเก็บในอุปกรณ์นั้นๆ เสียหาย นอกจากนี้ยังรวมถึงการที่ฮาร์ดแวร์นั้นๆ ถูกทำลายหรือทำให้ใช้การไม่ได้โดยมีสาเหตุจากธรรมชาติ เช่น น้ำท่วม ฟ้าผ่าอุปกรณ์ เป็นต้น

1.3 ซอฟต์แวร์ (software) ที่ถูกพัฒนาขึ้นมักมีข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัย เนื่องจากคุณสมบัตินี้มักถูกละเลยในระหว่างขั้นตอนการวิเคราะห์และพัฒนาซอฟต์แวร์นั้นๆ ทำให้เมื่อมีการนำมาใช้งานมักจะมีช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น อุปกรณ์เราเตอร์สำหรับใช้งานอินเทอร์เน็ตสำหรับเชื่อมต่อผ่านระบบเอดีเอสแอลบางรุ่นมีข้อบกพร่องเกี่ยวกับความมั่นคงปลอดภัย และเมื่อผู้ไม่ประสงค์ดีโจมตีระบบสำเร็จจะสามารถปลอมแปลงกระบวนการสอบถามโดเมนเนมได้ เป็นต้น ดังนั้นผู้ใช้งานหรือผู้ดูแลระบบจะต้องดำเนินการการปรับปรุงคุณสมบัติซอฟต์แวร์ตามหลังอยู่เสมอๆ ทั้งนี้การปรับปรุงคุณสมบัติดังกล่าว ผู้พัฒนาซอฟต์แวร์อาจสร้างช่องโหว่ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยเพิ่มมากขึ้นโดยไม่ได้ตั้งใจก็เป็นได้

1.4 ข้อมูลและสารสนเทศ (data and information) เป็นทรัพยากรที่สำคัญต่อบุคคลหรือองค์กรที่เป็นผู้สร้าง ประมวลผล และรับส่งข้อมูลสารสนเทศนั้นๆ ด้วยเหตุนี้ทรัพยากรนี้จึงเป็นเป้าหมายหลักของการโจมตีของผู้ไม่ประสงค์ดีโดยผลเสียหายที่เกิดขึ้นมักจะเกิดขึ้นในสามลักษณะสำคัญคือ การเปิดเผยความลับ การแก้ไขข้อมูลโดยไม่มีสิทธิ์ และการทำให้ข้อมูลนั้นๆ ไม่สามารถเข้าถึงได้ เช่น ถูกลบ เปลี่ยนแปลงสิทธิ์ หรือถูกเข้ารหัสลับเพื่อเรียกค่าไถ่ เป็นต้น

1.5 ขั้นตอนระเบียบวิธีปฏิบัติ (procedure) ขั้นตอนการดำเนินการกับข้อมูลมักถูกละเลยจากผู้ที่เกี่ยวข้องทำให้มีช่องโหว่ที่อาจทำให้เกิดการละเมิดความมั่นคงปลอดภัยได้ เช่น องค์กรต่างๆ มักมีการฝึกอบรมพนักงานให้ดำเนินการอย่างใดอย่างหนึ่งกับซอฟต์แวร์ที่ใช้ในองค์กรในรูปแบบของคู่มือการทำงาน ทำให้พนักงานที่มีหน้าที่คล้ายคลึงกันสามารถใช้งานซอฟต์แวร์ได้เหมือนๆ กัน โดยมักละเลยการสร้างความตระหนักรู้เกี่ยวกับการใช้งานซอฟต์แวร์อย่างมั่นคงปลอดภัยเป็นผลให้เกิดช่องโหว่ของการรักษาความมั่นคงปลอดภัยได้ เช่น พนักงานบัญชีคนหนึ่งอาจเข้าใช้งานระบบเงินเดือนค้างไว้โดยไม่ได้ล็อกหน้าจอขณะพักรับประทานอาหารกลางวัน ผู้ไม่ประสงค์ดีอาจเข้าใช้งานซอฟต์แวร์และปรับเปลี่ยนข้อมูลในระบบบัญชีได้ เป็นต้น

1.6 เครือข่าย (network) ระบบสารสนเทศในปัจจุบันถูกเชื่อมต่อเข้าด้วยกันผ่านเครือข่ายการรับส่งข้อมูลไม่ว่าจะเป็นเครือข่ายส่วนตัว เครือข่ายเฉพาะบริเวณ และมักเชื่อมต่อกับเครือข่ายอินเทอร์เน็ต แม้ว่าการเชื่อมต่อกันดังที่ได้กล่าวมาจะสร้างความสามารถในการใช้งานทรัพยากรสารสนเทศร่วมกันจากระยะทางไกล และทำให้เกิดการใช้งานทรัพยากรอย่างมีประสิทธิภาพมากยิ่งขึ้น การเชื่อมต่อกันเป็นเครือข่ายยิ่งมีขนาดมากเท่าไรย่อมเป็นการเพิ่มความเสี่ยงที่ทรัพยากรจะถูกโจมตี และเพิ่มความยากในการรักษาความมั่นคงปลอดภัยมากยิ่งขึ้น

เมื่อกล่าวโดยนัยแล้วจะเห็นว่า ทรัพยากรสารสนเทศมีองค์ประกอบสำคัญๆ ดังที่ได้กล่าวมา อย่างไรก็ดีทรัพยากรสารสนเทศอาจถูกนิยามได้ในความหมายที่ใกล้เคียงกันแต่ถูกนิยามขึ้นมาในระยะเริ่มต้น คือ ระบบคอมพิวเตอร์ ซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ มนุษย์ และข้อมูล ซึ่งจะขาดองค์ประกอบสำคัญคือ เครือข่ายและขั้นตอนวิธีปฏิบัติซึ่งเป็นองค์ประกอบที่สำคัญในปัจจุบัน เนื่องจากการประยุกต์ใช้

งานเทคโนโลยีสารสนเทศและการสื่อสารในปัจจุบันมีการแลกเปลี่ยนทรัพยากรกันผ่านช่องทางการสื่อสารและระบบเครือข่าย ตลอดจนการประมวลผลข้อมูลในปัจจุบันมีความซับซ้อนมากขึ้นกว่าในอดีต ดังนั้นเมื่อกล่าวถึงระบบคอมพิวเตอร์ในปัจจุบันจึงนิยมใช้คำว่าทรัพยากรสารสนเทศซึ่งมีความหมายครอบคลุมถึงทรัพยากรเครือข่ายและขั้นตอนวิธีปฏิบัติที่เกี่ยวข้อง

2. การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

การรักษาความมั่นคงปลอดภัย หมายถึง การทำให้มั่นใจได้ว่าทรัพยากรสารสนเทศที่มีอยู่มีความถูกต้องสมบูรณ์ และพร้อมใช้งานสำหรับผู้ใช้งานที่ได้รับสิทธิ์ในการเข้าถึงทรัพยากรนั้นๆ ในที่นี้จะยกตัวอย่างการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจัดเก็บข้อมูลซึ่งอาจมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ ตลอดจนต้องการรักษาความครบถ้วนสมบูรณ์ของไฟล์ต่างๆ ที่ถูกจัดเก็บไว้ในคอมพิวเตอร์ไม่ให้ถูกทำลายโดยมัลแวร์[1] และป้องกันการแพร่ระบาดของหนอนอินเทอร์เน็ต[2] ซึ่งอาจทำให้เครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ นักศึกษาอาจพิจารณาตั้งพาสเวิร์ดเพื่อควบคุมการเข้าถึงเข้าถึงเครื่องคอมพิวเตอร์ จัดการเข้ารหัสลับฮาร์ดดิสก์ ติดตั้งซอฟต์แวร์ตรวจจับคอมพิวเตอร์ไวรัส และเปิดการใช้งานไฟร์วอลล์ส่วนบุคคล[3] เป็นต้น โดยทั่วไปการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศสามารถจำแนกตามเป้าหมายของการรักษาความมั่นคงปลอดภัยได้ดังต่อไปนี้

2.1 ความมั่นคงปลอดภัยเชิงกายภาพ (physical security) เพื่อป้องกันอุปกรณ์ สิ่งของ หรือบริเวณให้ปราศจากการเข้าถึงโดยไม่ได้รับอนุญาต และการใช้งานที่ไม่ถูกต้อง เช่น การตั้งรหัสผ่านเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล สร้างห้องปฏิบัติการสำหรับระบบคอมพิวเตอร์และเครือข่าย การจัดให้มีระบบไฟสำรอง การจัดให้มีระบบดับเพลิง การจัดให้มีการพิสูจน์ตัวจริงก่อนเข้าถึงฮาร์ดแวร์หรือห้องที่ใช้จัดเก็บฮาร์ดแวร์ตลอดจนทรัพยากรเครือข่ายที่เกี่ยวข้อง เป็นต้น

2.2 ความมั่นคงปลอดภัยส่วนบุคคล (personnel security) เพื่อรักษาบุคลากร หรือกลุ่มของผู้ใช้งานที่ได้รับสิทธิ์ให้เข้าถึงและดำเนินงานได้อย่างมั่นคงปลอดภัย เช่น การกำหนดสิทธิ์ให้กับเจ้าหน้าที่ตามความรับผิดชอบ โดยกำหนดให้เจ้าหน้าที่ทั่วไปไม่สามารถอ่านข้อมูลที่ถูกสร้างขึ้นโดยหัวหน้างานของตนเอง แต่สามารถแก้ไขและตรวจสอบผู้ทำการแก้ไขทรัพยากรนั้นๆ ได้ การบังคับให้ผู้ใช้งานเปลี่ยนรหัสผ่านเมื่อเข้าสู่ระบบในครั้งแรกและทุกๆ สามเดือน เป็นต้น

2.3 ความมั่นคงปลอดภัยของการดำเนินงาน (operation security) เพื่อปกป้องหรือป้องกันกระบวนการทำงาน ตลอดจนกิจกรรมอื่นๆ ที่เกี่ยวข้อง เช่น สหกรณ์ออมทรัพย์ควรการจัดให้มีกลไกการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลที่จัดเก็บ ประมวลผล เมื่อสมาชิกดำเนินธุรกรรมกับสหกรณ์

---

[1] มัลแวร์ (malware) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบให้โจมตีต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ แบ่งเป็นหลายชนิดขึ้นอยู่กับลักษณะเฉพาะของซอฟต์แวร์นั้น ๆ เช่น คอมพิวเตอร์ไวรัส หนอนอินเทอร์เน็ต โทรจัน เป็นต้น

[2] หนอนอินเทอร์เน็ต (worms) หมายถึง มัลแวร์หรือซอฟต์แวร์ไม่พึงประสงค์ประเภทหนึ่งที่แพร่กระจายตัวเองผ่านเครือข่ายคอมพิวเตอร์ โดยใช้ประโยชน์จากช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของซอฟต์แวร์หรือบริการต่างๆ เช่น ช่องโหว่ของการแชร์ไฟล์ร่วมกันของระบบปฏิบัติการ เป็นต้น

[3] ไฟร์วอลล์ส่วนบุคคล (personal firewall) หมายถึง ซอฟต์แวร์ที่ถูกออกแบบติดตั้งบนเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทำหน้าที่ป้องกันคอมพิวเตอร์เครื่องนั้นจากการโจมตีทางเครือข่ายด้วยการวิเคราะห์ข้อมูลที่เข้าและออกจากคอมพิวเตอร์นั้นๆ

การกำหนดห้ามเจ้าหน้าที่เขียนรหัสผ่านสำหรับเข้าใช้งานระบบลงบนกระดาษ หรือการตรวจสอบสิทธิ์ในการเข้าถึงทรัพยากรก่อนการเข้าถึง การทำให้มั่นใจได้ว่าเอกสารลับถูกจัดเก็บหรือทำลายตามที่กำหนดในนโยบายการรักษาความมั่นคงปลอดภัย เป็นต้น

2.4 ความมั่นคงปลอดภัยของการสื่อสาร (communication security) เพื่อป้องกันสื่อนำสัญญาณข้อมูลต่างๆ ที่รับส่งผ่านช่องทางการสื่อสาร โดยมุ่งเน้นการรักษาความมั่นคงปลอดภัยของอุปกรณ์ต่างๆ ที่เชื่อมต่อกันเป็นระบบสื่อสาร รวมถึงการแพร่สัญญาณให้มีความมั่นคงปลอดภัย เช่น การกำหนดมาตรการเฝ้าตรวจการดักรับข้อมูล การเข้ารหัสข้อมูลที่มีการรับส่งกันในเครือข่ายหรือระหว่างเครือข่าย การใช้บริการวีพีเอ็นในการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างสาขาซึ่งทำให้มั่นใจได้ว่าการรับส่งข้อมูลระหว่างจุดจะถูกเข้ารหัสทำให้ผู้ไม่ประสงค์ดีที่ดักรับข้อมูลได้ไม่สามารถวิเคราะห์หรือแปลความหมายข้อมูลที่ดักรับได้ เป็นต้น

2.5 ความมั่นคงปลอดภัยของเครือข่าย (network security) เพื่อป้องกันการเข้าถึงอุปกรณ์เครือข่ายต่างๆ และอุปกรณ์ที่นำมาเชื่อมต่อเข้ากับเครือข่าย เช่น การแบ่งเครือข่ายออกเป็นเครือข่ายย่อยๆ เพื่อจำแนกกลุ่มผู้ใช้งานและระบบบริการต่างๆ รวมถึงการจัดให้มีการเฝ้าตรวจความมั่นคงปลอดภัย และการจัดให้มีการพิสูจน์ตัวจริงของผู้ใช้งานก่อนจึงจะสามารถใช้งานเครือข่ายได้ จะเห็นได้ว่ามีความแตกต่างจากความมั่นคงปลอดภัยของการสื่อสารโดยมีขอบเขตที่แคบกว่าและพิจารณาที่การเชื่อมต่อในบริเวณที่เกี่ยวข้อง เช่น ระบบเครือข่ายภายในบ้าน ระบบเครือข่ายภายในบริษัท เป็นต้น

2.6 ความมั่นคงปลอดภัยของข้อมูลข่าวสาร (information security) เพื่อรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ขององค์ประกอบต่างๆ ที่ถูกผนวกรวมเข้าเป็นระบบสารสนเทศ นับตั้งแต่กระบวนการสร้าง ประมวลผล และการรับส่งสารสนเทศนั้นๆ

3. หลักการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์

ในการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ประกอบด้วย 2 หลักการ ได้แก่ หลักการพื้นฐาน และหลักการอื่นๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.1 หลักการพื้นฐาน การรักษาความมั่นคงปลอดภัยจะสำเร็จได้ก็ต่อเมื่อองค์กรหรือบุคคลนั้นๆ ได้มีการจัดการกำหนดนโยบายที่เกี่ยวข้อง การควบคุมการดำเนินการให้เป็นไปตามนโยบาย การเสริมสร้างความรู้ความเข้าใจที่เกี่ยวข้อง การฝึกอบรม การสร้างความตระหนักรู้ และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องอย่างเหมาะสม

3.1.1 การรักษาความลับ (confidentiality) หมายถึง กระบวนการ มาตรการและการจัดการที่เกี่ยวข้องกับการรักษาความลับของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้สามารถเข้าถึงและเข้าใจความหมายได้เฉพาะผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นๆ ตัวอย่างข้อมูลที่ควรมีการจัดเก็บและมีการกำหนดมาตรการควบคุมการเข้าถึงเพื่อรักษาความลับของข้อมูลที่สำคัญเช่น ข้อมูลผู้ป่วยในระบบสารสนเทศของโรงพยาบาล ข้อมูลส่วนบุคคลอื่นๆ เช่น หมายเลขประจำตัวประชาชน กำหนดการของบุคคลสำคัญ รายชื่อผู้โดยสารของเที่ยวบินต่างๆ เป็นต้น

3.1.2 การรักษาความครบถ้วนสมบูรณ์ (integrity) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการตรวจสอบความครบถ้วนสมบูรณ์ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความถูกต้องสมบูรณ์ และสามารถตรวจสอบความครบถ้วนสมบูรณ์นั้นได้ เช่น หากมีการแก้ไขไฟล์ที่ถูกสร้างขึ้นแล้วมีการส่งผ่านไฟล์นั้นเข้าสู่เครือข่ายคอมพิวเตอร์ ผู้ที่เกี่ยวข้องจะต้องสามารถตรวจสอบได้ว่าไฟล์นั้นว่าถูกแก้ไขเปลี่ยนแปลงไประหว่างการส่งผ่านช่องทางการสื่อสารหรือไม่ เป็นต้น

3.1.3 การรักษาความพร้อมใช้ (availability) หมายถึง กระบวนการ มาตรการ และการจัดการที่เกี่ยวข้องกับการรักษาความพร้อมใช้ของสารสนเทศที่ถูกประมวลผล ส่งต่อ และจัดเก็บให้มีความพร้อมใช้อยู่เสมอ ทำให้ผู้ใช้ที่มีสิทธิ์เข้าถึงและใช้งานทรัพยากรสารสนเทศนั้นๆ สามารถเข้าใช้งานได้ เช่น เมื่อกล่าวถึงความพร้อมใช้ของระบบบริการธนาคารอิเล็กทรอนิกส์ อาจหมายถึงลูกค้าสามารถเข้าถึงและใช้งานบริการนั้นได้เสมอตลอด 24 ชั่วโมง และอาจหมายรวมถึงเจ้าหน้าที่ๆ เกี่ยวข้องสามารถเข้าถึงและบริหารจัดการซอฟต์แวร์นั้นได้ เป็นต้น

ภาพที่ 14.1 องค์ประกอบสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

จากภาพที่ 14.1 จะเห็นว่าทรัพยากรสารสนเทศที่ต้องการให้มีความมั่นคงปลอดภัยนั้นอาจถูกจัดเก็บอยู่ในฮาร์ดแวร์ (hardware) ซอฟต์แวร์ (software) หรือถูกส่งผ่านระบบการสื่อสาร (communication) ก็เป็นได้ และการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรสารสนเทศนั้นจะมีความเกี่ยวเนื่องกับการรักษาความมั่นคงปลอดภัยทางกายภาพ (physical security) ในทุกระดับโดยการจัดให้มีเทคโนโลยีและกระบวนการที่เหมาะสมสำหรับการเข้าถึงทางกายภาพต่อฮาร์ดแวร์ ซอฟต์แวร์ และระบบการสื่อสาร นอกจากนี้ยังมีความจำเป็นต้องสร้างการรักษาความมั่นคงปลอดภัยส่วนบุคคล (personal security) เนื่องจากมนุษย์เป็นจุดอ่อนที่สุดของระบบการรักษาความมั่นคงปลอดภัย และมักละเมิดกฎเกณฑ์ที่จำเป็น ทั้งนี้ อาจแก้ไขได้โดยการสร้างความตระหนักรู้ถึงเหตุผลและความสำคัญของการรักษาความมั่นคงปลอดภัย เป็นต้น ทั้งนี้มาตรการและเทคโนโลยีที่นำมาใช้จะต้องมีการกำหนดให้สอดคล้องกับการจัดการรักษาความมั่นคงปลอดภัยในระดับองค์กรโดยการกำหนดยุทธศาสตร์ นโยบายและกฎระเบียบที่เกี่ยวข้อง ตลอดจนมีการกำกับดูแลอย่างเหมาะสม

3.2 หลักการอื่น ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย การรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศจึงเป็นกระบวนการเชิงบริหารที่นำเอานโยบาย การดำเนินงาน และการประยุกต์ใช้เทคโนโลยีที่เกี่ยวข้องเพื่อป้องกันและจำกัดผลเสียหายต่อการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของทรัพยากรสารสนเทศนั้นๆ

3.2.1 ช่องโหว่ (vulnerability) คือ ความบกพร่องหรือจุดอ่อนที่มีอยู่ในทรัพยากรสารสนเทศโดยเป็นผลมาจากการออกแบบ การพัฒนาซอฟต์แวร์ การจัดการกระบวนการทำงาน หรือการบำรุงรักษาระบบนั้นๆ เช่น ช่องโหว่ของระบบปฏิบัติการ ช่องโหว่ของซอฟต์แวร์เว็บเบราว์เซอร์ การอนุญาตให้ผู้ไม่มีบัตรเข้าถึงห้องสำคัญๆ ที่เกี่ยวข้องกับกระบวนการทำงานโดยไม่มีการตรวจสอบ หรือการไม่ควบคุมให้มีการตรวจสอบเอกสารลับก่อนการทิ้งขยะ เป็นต้น เมื่อพิจารณาตามกลุ่มของทรัพยากรจะสามารถจำแนกประเภทของช่องโหว่ได้ 3 ลักษณะ ดังต่อไปนี้

1) ช่องโหว่ที่เกี่ยวข้องกับฮาร์ดแวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยของฮาร์ดแวร์ เช่น ช่องโหว่ของการเข้ารหัสของระบบขายปลีกครบวรจร (Point of Sale; POS) ซึ่งส่งผลให้ผู้โจมตีสามารถขโมยข้อมูลบัตรเครดิตของผู้ใช้บริการ[4] หรือช่องโหว่ของระบบสมองกลที่ใช้ควบคุมรถยนต์ที่เมื่อถูกโจมตีผ่านเครือข่ายแล้วจะทำให้ผู้โจมตีสามารถควบคุมการระบบควบคุมภายในรถยนต์คันนั้นๆ ได้[5] เป็นต้น

2) ช่องโหว่ที่เกี่ยวข้องกับซอฟต์แวร์ หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับซอฟต์แวร์ต่างๆ ที่เมื่อเกิดการโจมตีต่อซอฟต์แวร์นั้นๆ แล้วจะส่งผลกระทบต่อความมั่นคงปลอดภัยของซอฟต์แวร์และซอฟต์แวร์ระบบอื่นๆ ที่เกี่ยวข้อง เช่น ช่องโหว่ของระบบปฏิบัติการที่เกี่ยวข้องกับการแชร์ไฟล์ผ่านระบบเครือข่ายคอมพิวเตอร์ที่หากผู้ไม่ประสงค์ดีโจมตีต่อบริการแชร์ไฟล์สำเร็จอาจทำการลบโฟลเดอร์ หรือไฟล์ต่างๆ โดยไม่ได้รับอนุญาต เป็นต้น

3) ช่องโหว่ที่เกี่ยวข้องกับการบริหารจัดการข้อมูล หมายถึง ข้อบกพร่องที่เกี่ยวข้องกับการจัดการข้อมูลต่างๆ ทั้งที่เป็นข้อมูลที่ไม่ได้จัดเก็บในรูปแบบดิจิทัล และข้อมูลในรูปแบบดิจิทัล เช่น หากองค์กรหรือบุคคลจัดเก็บข้อมูลซึ่งใช้ในการพิสูจน์ตัวจริงอย่างไม่เหมาะสม เมื่อข้อมูลนั้นรั่วไหลออกไปอาจส่งผลให้เกิดการโจมตีต่อองค์กรนั้นๆ ได้ หรือเปิดโอกาสให้มีการโจมตีต่อทรัพยากรอื่นๆ เป็นต้น

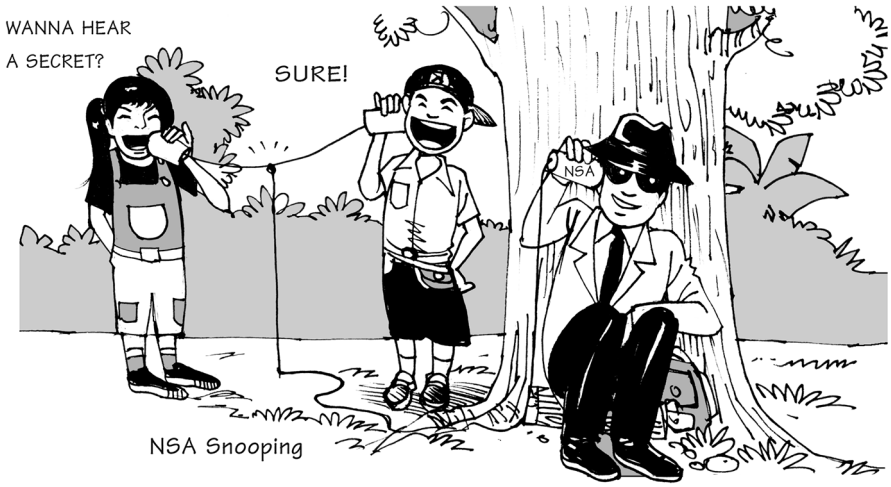
3.2.2 ภัยคุกคาม (threat) คือ บุคคลหรือผู้ใดก็ตามที่สามารถใช้ประโยชน์จากช่องโหว่ที่มีเข้าถึงและทำลายความมั่นคงปลอดภัยของทรัพยากรสารสนเทศได้ ภัยคุกคามต่อทรัพยากรสารสนเทศจำแนกได้ 4 ลักษณะคือ

1) การดักรับ (interception) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีเข้าถึงหรือดักรับข้อมูลโดยปราศจากสิทธิ์โดยถูกต้อง เช่น การดักรับที่รับส่งกันระหว่างผู้รับและผู้ส่งในระบบเครือข่ายคอมพิวเตอร์ (sniffing) การแอบอ่านข้อมูลจากหน้าจอของผู้อื่น การแอบฟังผู้อื่นพูดคุยกันเพื่อให้ได้ข้อมูลที่ตนเองไม่มีสิทธิ์เข้าถึง ดังภาพที่ 14.2 เป็นต้น

---

[4] http://blogs.cisco.com/security/detecting-payment-card-data-breaches-today-to-avoid-becoming-tomorrows-headline/ สืบค้นเมื่อ 20 มีนาคม 2559.

[5] http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/ สืบค้นเมื่อ 20 มีนาคม 2559.



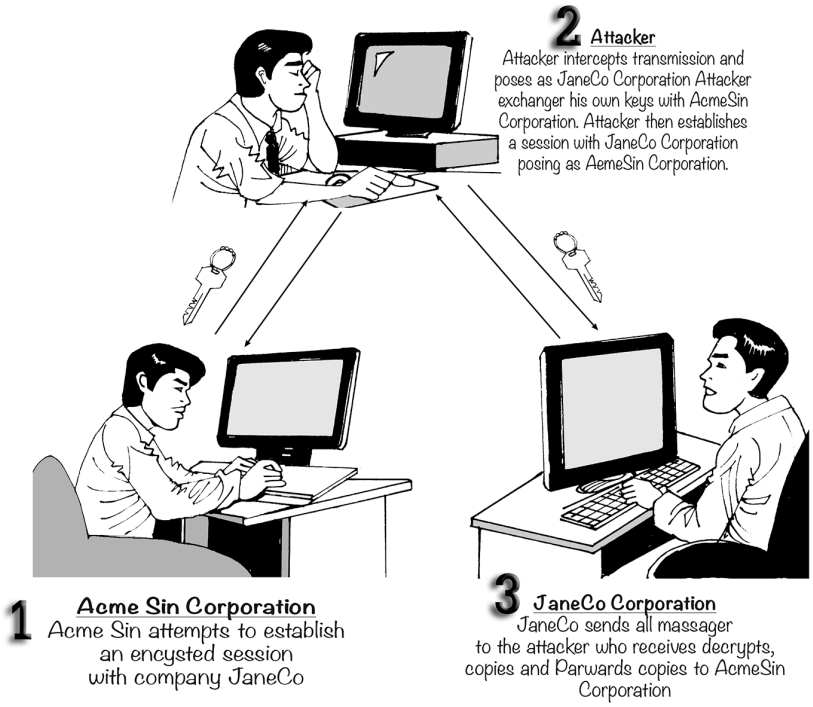
ภาพที่ 14.2 การดักรับข้อมูล

2) การขัดจังหวะ (interruption) หมายถึง เหตุการณ์ที่ผู้ไม่ประสงค์ดีกระทำแล้วส่งผลให้ผู้ใช้งานที่มีสิทธิ์ไม่สามารถเข้าถึง หรือใช้งานทรัพยากรนั้นๆ ได้ เช่น การตัดสายสัญญาณเครือข่าย การลบไฟล์ข้อมูล การทำลายคอมพิวเตอร์ ดังที่แสดงในภาพที่ 14.3 หรือการนำเข้าข้อความที่ระบบประมวลผลแล้วทำให้ระบบปฏิเสธการให้บริการ เป็นต้น

"It's not the most sophisticated Spam blocker
I've tried, but it's the only one that works:"

ภาพที่ 14.3 การทำลายคอมพิวเตอร์ส่งผลให้ผู้มีสิทธิ์ใช้งานไม่สามารถใช้งานได้

3) การดัดแปลงแก้ไข (modification) หมายถึง การเข้าถึงและแก้ไขทรัพยากรสารสนเทศโดยไม่มีสิทธิ์ เช่น การเปลี่ยนแปลงการปรับตั้งค่าต่างๆ ของระบบปฏิบัติการ การอนุญาตให้มีการเข้าถึงจากระยะไกลโดยไม่มีการพิสูจน์ตัวจริง ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัย การดักรับโดยการเปลี่ยนเส้นทางและการเปลี่ยนแปลงข้อมูลที่ถูกรับส่งผ่านเครือข่าย ดังแสดงในภาพที่ 14.4 เป็นต้น โดยการดัดแปลงแก้ไขดังกล่าวอาจกระทำได้ในกรณีอื่นๆ เช่น เพื่อนของนักศึกษาอาจแก้ไขไฟล์รายงานของนักศึกษาที่ถูกบันทึกไว้ในสื่อจัดเก็บข้อมูล เช่น แฟลชไดร์ฟโดยที่นักศึกษาไม่ทราบ เมื่อนักศึกษาส่งรายงานไปยังอาจารย์จึงพบว่าข้อมูลนั้นไม่ใช่ข้อมูลที่ถูกต้อง เป็นต้น



ภาพที่ 14.4 การโจมตีที่มีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่มีสิทธิ์

4) การปลอมแปลง (fabrication) หมายถึง การสร้างข้อมูลหรือสิ่งแปลกปลอมเข้าสู่ระบบสารสนเทศ เช่น การเพิ่มข้อมูลลงในระบบจัดการฐานข้อมูล การตั้งเครือข่ายไร้สายที่มีชื่อสถานีเหมือนกับเครือข่ายเป้าหมาย เพื่อดักรับข้อมูลต่างๆ และการปลอมแปลงหมายเลขไอพีเพื่อหลบเลี่ยงกลไกพิสูจน์ตัวจริงเพื่อเข้าใช้งานเครือข่าย การปลอมแปลงตนเองเป็นบุคคลอื่นเพื่อหลอกถามข้อมูลดังที่แสดงในภาพที่ 14.5 เป็นต้น วัตถุประสงค์หลักของการปลอมแปลงจึงเกี่ยวข้องกับการล่อลวงให้เหยื่อเข้าใจผิดว่าข้อมูลหรือสารสนเทศนั้นเป็นข้อมูลหรือตัวตนจริงๆ ของผู้นั้น หากเหยื่อตายใจและให้ข้อมูลหรือเปิดเผยข้อมูลสำคัญจะทำให้เกิดการละเมิดความมั่นคงปลอดภัยต่อเหยื่อนั้นๆ เช่น การส่งจดหมายโดยอ้างว่าผู้ส่งเป็นหัวหน้างานและให้ส่งความลับขององค์กรไปยังอีเมล หรือให้จัดพิมพ์เอกสารแล้วส่งไปยังผู้โจมตี เป็นต้น

ภาพที่ 14.5 การปลอมแปลง

3.2.3 การโจมตี (attack) คือ การกระทำหรือผลที่เกิดขึ้นเมื่อเกิดภัยคุกคามต่อช่องโหว่ต่างๆ ที่มีอยู่ในทรัพยากรสารสนเทศ ทั้งนี้การโจมตีอาจไม่ได้มีต้นกำเนิดจากผู้ไม่ประสงค์ดีแต่เพียงอย่างเดียวก็เป็นได้ เช่น ทรัพยากรสารสนเทศหนึ่งมีความลับไม่ควรถูกเผยแพร่ให้ผู้ไม่มีหน้าที่เกี่ยวข้องรับทราบ แต่ไม่ถูกกำหนดมาตรการควบคุมการเข้าถึงอย่างเหมาะสม อาจถูกเข้าถึงโดยผู้ใช้งานทั่วไป และนำข้อมูลนั้นไปเผยแพร่ อันเป็นการทำลายความลับของทรัพยากรนั้นๆ ทั้งนี้ การกระทำดังกล่าวอาจเกิดขึ้นโดยเจตนาหรืออาจเกิดขึ้นจากอุบัติเหตุ การโจมตีอีกลักษณะหนึ่งที่ได้รับความนิยมคือ การโจมตีต่อโครงสร้างพื้นฐานที่สำคัญของเป้าหมาย เช่น การทำให้ระบบปฏิเสธการให้บริการ และการโจมตีด้วยเทคนิคเชิงสังคมอื่นๆ เช่น การแอบอ้างเป็นพนักงานคอลเซนเตอร์เพื่อล่อลวงเป้าหมายให้กระทำการอย่างใดอย่างหนึ่งโดยเปิดเผยข้อมูลพิสูจน์ตัวจริง หรือการหลอกลวงให้ทำรายการบัญชีผ่านเอทีเอ็ม เป็นต้น

3.2.4 ผู้ไม่ประสงค์ดี (attacker) คือ บุคคลหรือกระบวนการที่เกิดขึ้นจากมนุษย์เพื่อกระทำการโจมตีต่อทรัพยากรสารสนเทศเป้าหมาย จากนิยามดังกล่าวจะเห็นได้ว่ามีความหมายใกล้เคียงกับภัยคุกคามแต่จำกัดสาเหตุไว้ที่มนุษย์เท่านั้น ซึ่งผู้ไม่ประสงค์ดีอาจมีแรงจูงใจในการโจมตีต่อระบบที่แตกต่างกันออกไป เช่น ความประมาท ค่าตอบแทน และความสะใจ เป็นต้น ในปัจจุบันนิยมใช้คำว่า แฮกเกอร์ (hacker) สามารถจำแนกประเภทจากแรงจูงใจในการโจมตีต่อระบบได้หลายลักษณะ เช่น แฮกเกอร์สมัครเล่น แฮกเกอร์หมวกขาว แฮกเกอร์หมวกดำ เป็นต้น

1) แฮกเกอร์มือสมัครเล่น (script kiddy) หมายถึง บุคคลทั่วไปที่โจมตีต่อช่องโหว่ของระบบด้วยเครื่องมือหรือซอฟต์แวร์ที่ผู้ไม่ประสงค์ดีคนอื่นเผยแพร่ไว้โดยปราศจากความเข้าใจถึงกระบวนการทำงานของซอฟต์แวร์นั้นๆ รวมไปถึงบุคคลทั่วๆ ไปที่ล่วงรู้ช่องโหว่ของการรักษาความมั่นคงปลอดภัยที่เข้าถึงหรือแก้ไขทรัพยากรที่ไม่มีสิทธิ์โดยไม่ได้ตั้งใจ เช่น การลบไฟล์เอกสารที่ใช้งานร่วมกันผ่านเครือข่ายได้เนื่องจากผู้ดูแลระบบกำหนดสิทธิ์ไว้ผิด เป็นต้น

2) แฮกเกอร์หมวกขาว (white hat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาช่องโหว่ และการโจมตีต่อระบบคอมพิวเตอร์ในเชิงป้องกันและรักษาความมั่นคงปลอดภัยให้กับระบบแล้วรายงานช่องโหว่หรือการโจมตีดังกล่าวต่อเจ้าของหรือผู้มีหน้าที่รับผิดชอบเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการปรับปรุงความมั่นคงปลอดภัยและแก้ไขข้อบกพร่องนั้นๆ ก่อนที่ช่องโหว่หรือข้อบกพร่องดังกล่าวจะถูกตรวจพบหรือถูกประกาศให้ทราบในที่สาธารณะ เช่น เว็บบอร์ดหรืออินเทอร์เน็ต เป็นต้น

3) แฮกเกอร์หมวกดำ (black hat) หมายถึง ผู้เชี่ยวชาญระบบคอมพิวเตอร์ที่ใช้ความสามารถดังกล่าวในการค้นหาและโจมตีต่อระบบคอมพิวเตอร์ เพื่อการทำลายความมั่นคงปลอดภัยโดยมีผลประโยชน์ส่วนตัวเป็นแรงจูงใจ เช่น ค่าตอบแทนจากองค์กรอาชญากรรม การล้างแค้น หรือความคิดเห็นทางการเมือง เป็นต้น

3.2.5 เอกซ์พลอยต์ (exploit) คือ แม้ว่าเอกซ์พลอยต์จะมีความหมายตามพจนานุกรมว่า “การใช้ประโยชน์หรือการทำประโยชน์” แต่เอกซ์พลอยต์ในที่นี้จะหมายถึงการโจมตีต่อช่องโหว่ที่มีในระบบสารสนเทศ เพื่อทำลายความมั่นคงปลอดภัยหรือเข้าใช้ประโยชน์จากช่องโหว่ที่มีอยู่ เช่น ช่องโหว่ของระบบจัดการเนื้อหาผ่านเว็บที่ถูกค้นพบและรายงาน อาจมีผู้ไม่ประสงค์ดีพัฒนาโปรแกรมที่สามารถโจมตีต่อช่องโหว่ดังกล่าวสำเร็จ แล้วแจกจ่ายให้กับผู้ที่สนใจนำโปรแกรมนี้ไปโจมตีต่อช่องโหว่นั้น นอกจากนี้ยังหมายถึงเทคนิควิธีที่ใช้ในการโจมตีด้วยเทคนิควิศวกรรมเชิงสังคม เช่น การพยายามตีสนิทกับเหยื่อซึ่งทำหน้าที่สำคัญในระบบสารสนเทศเพื่อให้ได้มาซึ่งข้อมูลที่เป็นประโยชน์ต่อการโจมตี หรือการล่อลวงเพื่อใช้ประโยชน์จากเหยื่อในการเข้าถึงทรัพยากรสารสนเทศ เป็นต้น

3.2.6 เป้าหมาย (target) คือ บุคคล องค์กร ทรัพยากรสารสนเทศที่มีช่องโหว่และได้รับผลกระทบโดยตรงจากการการโจมตีที่อาจเกิดขึ้น

3.2.7 วิธีการโจมตี (attack vector) คือ กระบวนการ วิธีการ เครื่องมือและเทคนิคที่ใช้โจมตีต่อช่องโหว่ที่มีในเป้าหมายของการโจมตี

ดังที่ได้กล่าวข้างต้นแล้วว่า วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยคือ การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาความพร้อมใช้ของทรัพยากรสารสนเทศ ซึ่งมีความหมายนับตั้งแต่เครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นๆ เพียงเครื่องเดียว ซอฟต์แวร์ต่างๆ ไปจนถึงระบบสารสนเทศที่เชื่อมต่อกันผ่านเครือข่าย ฉะนั้นหากต้องการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรจึงมีแนวทางคล้ายคลึงกับการบริหารงาน โดยนอกจากจะต้องกำหนดแนวทางการจัดการทรัพยากรในภาพรวมแล้ว จะต้องดำเนินการพิจารณาความเหมาะสม ความสะดวกในการใช้งาน การกำหนดสิทธิ์และการเข้าถึง การสร้างนโยบายการรักษาความมั่นคงปลอดภัย ตลอดจนคัดเลือกเทคโนโลยีที่เกี่ยวข้องโดยคำนึง

ถึงความต้องการที่เกี่ยวข้องกับความมั่นคงปลอดภัย และความง่ายในการใช้งาน ให้สอดคล้องกับความต้องการขององค์กร นโยบาย และผู้ใช้งานเป็นสำคัญ

กิจกรรม 14.1.1

1. สมมติเหตุการณ์ว่าเครื่องคอมพิวเตอร์แบบพกพาของนักศึกษาสูญหาย โดยที่นักศึกษาไม่ได้ทำการสำรองไฟล์ข้อมูลสำคัญใดๆ ไว้แต่นักศึกษาได้ดำเนินการเข้ารหัสฮาร์ดดิสก์และกำหนดให้ระบบปฏิบัติการลบข้อมูลทั้งหมดหากมีการป้อนรหัสผ่านผิดเกินสามครั้ง เหตุการณ์นี้ส่งผลที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างไร

2. สมมติเหตุการณ์ว่านักศึกษาเขียนรหัสผ่านสำหรับเข้าใช้งานคอมพิวเตอร์ส่วนตัวไว้บนจอคอมพิวเตอร์ ต่อมาพบว่า มีผู้ไม่ประสงค์ดีเข้าใช้งานเครื่องคอมพิวเตอร์เครื่องนั้นผ่านระบบเครือข่ายและได้ทำการเปลี่ยนพาสเวิร์ดสำหรับเข้าใช้งาน และลบไฟล์สำคัญไป อยากทราบว่าเหตุการณ์นี้ส่งผลอย่างไรต่อความมั่นคงปลอดภัย

แนวตอบกิจกรรม 14.1.1

1. โดยปกติเมื่อเครื่องคอมพิวเตอร์สูญหายย่อมมีโอกาสถูกเปิดขึ้นใช้งานจากขโมยจึงมีโอกาสที่ข้อมูลที่เป็นความลับจะถูกเปิดเผย แต่ในกรณีนี้ผลกระทบจะเกี่ยวข้องกับความพร้อมใช้ของข้อมูลเป็นหลัก เนื่องจากนักศึกษาผู้นี้ไม่ได้ดำเนินการสำรองข้อมูลไว้ในแหล่งข้อมูลอื่นๆ เลย

2. การเปลี่ยนรหัสผ่านสำหรับเข้าใช้งานคอมพิวเตอร์ส่งผลให้นักศึกษาที่มีสิทธิ์เข้าใช้ไม่สามารถเข้าใช้งานได้ จึงส่งผลต่อความพร้อมใช้ของเครื่องคอมพิวเตอร์เครื่องนั้นๆ ในขณะเดียวกันหากนักศึกษาที่เป็นเจ้าของเครื่องสามารถกู้คืนสภาพและสามารถเข้าใช้งานได้จะพบว่าข้อมูลสำคัญของตนถูกเปลี่ยนแปลงไป ซึ่งหมายถึงความครบถ้วนสมบูรณ์นั้นเสียหาย และหากมีข้อมูลที่ไม่ต้องการให้ผู้อื่นล่วงรู้ถูกจัดเก็บไว้ก็มีความเสี่ยงที่ข้อมูลนั้นจะถูกเข้าถึงได้จึงอาจส่งผลต่อการรักษาความลับเช่นเดียวกัน

มสธ

เรื่องที่ 14.1.2
ภัยคุกคามและการโจมตี

ภัยคุกคาม หมายถึง ชุดของเหตุการณ์ที่หากเกิดขึ้นแล้วจะเกิดผลเสียหายต่อความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และสารสนเทศที่จัดเก็บ ประมวลผล และส่งผ่านระบบคอมพิวเตอร์นั้นๆ เอ็ม วิทแมน (M. Whitman) จำแนกประเภทของภัยคุกคามที่มีต่อทรัพยากรสารสนเทศออกเป็นหมวดหมู่เพื่อความสะดวกในการบริหารจัดการภัยคุกคามต่อทรัพยากรสารสนเทศซึ่งประกอบด้วย บุคลากร ระบบงานประยุกต์ โครงสร้างพื้นฐานของระบบสารสนเทศและข้อมูลต่างๆ ที่มีในองค์กรนั้นๆ

1. ประเภทของภัยคุกคาม

ภัยคุกคาม หมายถึง ชุดของเหตุการณ์ที่เกิดขึ้นแล้วจะส่งผลต่อความมั่นคงปลอดภัยของทรัพยากรสารสนเทศ ชุดของเหตุการณ์เหล่านี้มีวัตถุประสงค์หลักเพื่อการสร้าง การสกัดกั้น การขัดจังหวะ การดัดแปลงแก้ไข และการปลอมแปลง เพื่อทำลายความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ทรัพยากรสารสนเทศที่เป็นเป้าหมาย โดยสามารถจำแนกประเภทของภัยคุกคามตามทรัพยากรที่เป็นเป้าหมายได้ ดังต่อไปนี้

1.1 ภัยคุกคามต่อทรัพย์สินทางปัญญา คือ ภัยคุกคามที่เกิดขึ้นโดยหวังผลทำลายความมั่นคงปลอดภัยของทรัพย์สินทางปัญญาของเป้าหมาย เช่น ในระดับองค์กรต่างๆ ซึ่งโดยทั่วไปแล้ว การดำเนินกิจกรรมต่างๆ ภายในองค์กรมักทำให้เกิดกระบวนการและสร้างองค์ความรู้ต่างๆ เพื่อใช้ในการแก้ปัญหาและดำเนินกิจการภายในองค์กร ข้อมูลต่างๆ เหล่านี้จึงเป็นทรัพย์สินทางปัญญาขององค์กรนั้นๆ รวมไปถึงผลการวิจัย ความลับทางการค้าซึ่งอาจทำให้องค์กรนั้นได้เปรียบคู่แข่งขัน ในกรณีของการใช้งานส่วนบุคคล ภัยคุกคามที่อาจเกิดขึ้นต่อทรัพยากรส่วนบุคคล เช่น การคัดลอกผลงาน หรือการคัดลอกลิขสิทธิ์ของซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนบุคคลเพื่อนำไปใช้งานโดยไม่ได้รับอนุญาต เป็นต้น

1.2 ภัยคุกคามจากการโจมตีโดยซอฟต์แวร์ คือ ภัยคุกคามที่เกิดขึ้นจากการโจมตีของซอฟต์แวร์ต่อระบบเป้าหมาย ไม่ว่าจะเป็นต่อเครื่องคอมพิวเตอร์ส่วนบุคคล ระบบบริการที่ทำงานบนเซิร์ฟเวอร์ หรือโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศอื่นๆ เช่น เครือข่าย ซอฟต์แวร์ที่ใช้โจมตีดังที่ได้กล่าวมานิยมเรียกว่า “มัลแวร์” ซึ่งหมายถึง ซอฟต์แวร์ที่ถูกออกแบบและพัฒนาขึ้นเพื่อสร้างความเสียหายต่อระบบเป้าหมาย และสามารถแบ่งออกเป็นหลายประเภทตามวิธีการโจมตีเป็น คอมพิวเตอร์ไวรัส (computer virus) หนอนอินเทอร์เน็ต (internet worms) โทรจัน (trojan) และแบคดอร์ (backdoor) เป็นต้น

1.3 ภัยคุกคามต่อคุณภาพของบริการ คือ ภัยคุกคามที่ก่อกวนทำให้ความพร้อมใช้ของทรัพยากรสารสนเทศขององค์กรไม่สามารถให้บริการต่อผู้ใช้งานได้อย่างมีประสิทธิภาพ เนื่องจากการทำงานขององค์กรในปัจจุบันมีแนวโน้มการประยุกต์ใช้เทคโนโลยีสารสนเทศและการสื่อสารในการทำงานมากยิ่งขึ้น เช่น องค์กรหนึ่งๆ อาจเปิดให้บริการต่างๆ ผ่านอินเทอร์เน็ตเพื่อให้ลูกค้าสามารถสั่งซื้อ และดำเนินธุรกรรม

กับองค์กร เมื่อเกิดการโจมตีต่อเครือข่ายของผู้ให้บริการอินเทอร์เน็ตโดยการก่อวินาศกรรมกับระบบเครือข่าย ทำให้ผู้บริการต้องใช้เครือข่ายสำรองซึ่งมีประสิทธิภาพต่ำกว่า ย่อมส่งผลให้ความพร้อมใช้ของระบบให้บริการต่างๆ ที่เชื่อมต่อกับผู้ให้บริการรายนี้ลดลง เป็นต้น

1.4 ภัยคุกคามต่อข้อมูลและสารสนเทศ คือ ภัยคุกคามที่มีต่อการรักษาความลับของข้อมูลบุคคลและโครงสร้างพื้นฐานระบบสารสนเทศ โดยมักเกิดขึ้นเมื่อผู้ไม่ประสงค์ดีประสบความสำเร็จในการเข้าถึงบริการต่างๆ โดยไม่ได้รับอนุญาตจากนั้นอาจทำการนำข้อมูลต่างๆ ไปเปิดเผย หรือขายให้กับองค์กรคู่แข่ง นอกจากนี้ยังรวมถึงการแอบดักรับข้อมูลสำหรับการพิสูจน์ตัวจริงต่างๆ เช่น ชื่อผู้ใช้งาน และรหัสผ่านสำหรับเข้าถึงเครือข่ายหรือแม้กระทั่งความพยายามในการแอบดูรหัสผ่านสำหรับเข้าใช้เครื่องคอมพิวเตอร์ส่วนบุคคลดังที่แสดงในภาพที่ 14.6 การเก็บขยะที่เกิดขึ้นในองค์กรเพื่อค้นหารหัสผ่านที่ผู้ใช้งานอาจเขียนหรือพิมพ์แล้วทิ้งโดยไม่ได้ทำลาย ตลอดจนการลักลอบจำรหัสเอทีเอ็มของเป้าหมาย เป็นต้น

Take care about shoulder surfing

ภาพที่ 14.6 การแอบดูรหัสผ่านของผู้ไม่ประสงค์ดี

1.5 ภัยคุกคามที่เกิดจากธรรมชาติ คือ ภัยคุกคามที่เกิดขึ้นโดยธรรมชาติ เช่น เมื่อเกิดแผ่นดินไหวอาจทำให้สายไฟฟ้าหรือสายใยแก้วนำแสงที่เชื่อมโยงเครือข่ายเสียหาย ทำให้โครงสร้างพื้นฐานสารสนเทศต่างๆ ไม่สามารถใช้การได้ตามปกติ การเกิดอุทกภัยฉับพลันอาจส่งผลให้องค์กรไม่สามารถดำเนินกิจกรรมได้ตามปกติ รวมไปถึงเหตุการณ์ไฟไหม้ที่เกิดขึ้นกับทรัพยากรสารสนเทศต่างๆ ที่มี ตลอดจนการสะสมของฝุ่นที่อาจทำให้เกิดไฟฟ้าลัดวงจรบนแผงวงจรไฟฟ้า ภัยธรรมชาติที่สำคัญๆ เช่น ฟ้าผ่า แผ่นดินไหว น้ำท่วม พายุไต้ฝุ่น สึนามิ ดังที่เคยเกิดขึ้นกับองค์กรสำคัญๆ ในประเทศที่สูญเสียข้อมูลสำคัญขององค์กรอันเนื่องมาจากอุทกภัย เป็นต้น

1.6 ภัยคุกคามจากความผิดพลาดของมนุษย์ คือ ภัยคุกคามที่มีสาเหตุมาจากความผิดพลาดของผู้ใช้งานที่มีสิทธิ์เข้าถึงและบริหารจัดการระบบในทุกระดับ เช่น ผู้ใช้งานทั่วไปนิยมเขียนรหัสผ่านสำหรับเข้าใช้งานระบบต่างๆ แล้วแปะไว้บนจอคอมพิวเตอร์ ส่งผลให้ข้อมูลที่ใช้ในการพิสูจน์ตัวจริงอาจถูกผู้ไม่ประสงค์ดีนำไปใช้ และใช้สิทธิ์ของผู้ใช้คนนั้นในการโจมตีต่อความมั่นคงปลอดภัยของทรัพยากรสารสนเทศ ข้อผิดพลาดอื่นๆ เช่น การปรับแต่งการตั้งค่าของอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องผิดพลาด การใช้งานคอมพิวเตอร์ส่วนบุคคลผู้ใช้งานอาจปรับตั้งค่าการทำงานซอฟต์แวร์ป้องกันคอมพิวเตอร์ไวรัสผิดพลาดทำให้ไม่มีการปรับปรุงฐานข้อมูลของซอฟต์แวร์ เมื่อเวลาผ่านไปซอฟต์แวร์นั้นก็ไม่สามารถตรวจจับคอมพิวเตอร์ไวรัสใหม่ๆ ได้ ส่งผลให้เกิดปัญหาที่เกี่ยวข้องกับความมั่นคงปลอดภัยกับคอมพิวเตอร์เครื่องนั้นๆ เป็นต้น

1.7 ภัยคุกคามจากการข่มขู่และการเปิดเผยข้อมูล คือ ภัยคุกคามที่เกิดขึ้นเมื่อผู้ไม่ประสงค์ดีหรือบุคลากรในองค์กรโจรกรรมข้อมูลจากระบบสารสนเทศแล้วทำการเรียกค่าไถ่กับเจ้าของข้อมูลหรือเจ้าของระบบ เช่น การโจรกรรมหมายเลขบัตรเครดิตจากระบบบริการร้านค้าออนไลน์ต่างๆ ทั้งนี้หากผู้ไม่ประสงค์ดีดำเนินการสำเร็จแล้วนำข้อมูลดังกล่าวเผยแพร่ต่อสาธารณะจะทำให้เกิดผลเสียหายต่อองค์กรนั้นๆ อย่างมาก เพื่อแลกเปลี่ยนกับความเสียหายที่อาจเกิดขึ้นจึงเกิดการเจรจาต่อรองและเรียกค่าไถ่ เป็นต้น

1.8 ภัยคุกคามจากการบริหารจัดการที่หละหลวม คือ ภัยคุกคามที่เกิดขึ้นจากการกำหนดแผนงานและจัดการนโยบายการใช้งานทรัพยากรสารสนเทศอย่างไม่เหมาะสมทำให้เกิดช่องโหวในการบริหารจัดการจนส่งผลให้หากเกิดการโจมตีต่อทรัพยากรสารสนเทศในองค์กรนั้นๆ เช่น การกำหนดนโยบายการเข้าถึงและการกำหนดสิทธิ์ที่ไม่รอบคอบรัดกุม การไม่กำหนดให้มีการพิสูจน์ตัวจริงก่อนการเข้าถึงทรัพยากร เป็นต้น

1.9 ภัยคุกคามจากมาตรการควบคุมที่ไม่เหมาะสม คือ ภัยคุกคามที่เกิดขึ้นจากการควบคุมและการปรับตั้งค่าอุปกรณ์ในโครงสร้างพื้นฐานสารสนเทศไม่เหมาะสมอันเป็นผลมาจากการออกแบบ การทำงานที่ด้อยประสิทธิภาพ เช่น การปล่อยให้ผู้ใช้ทั่วไปสามารถเข้าถึงเน็ตเวิร์กสวิตช์สามารถทำการปรับตั้งค่าให้มีการดักรับข้อมูลได้ เนื่องจากไม่มีการปรับตั้งชื่อรหัสผ่านผู้ใช้เพื่อจำแนกเจ้าหน้าที่ดูแลระบบออกจากผู้ใช้งานทั่วไป ผู้ใช้งานที่ไม่ประสงค์ดีอาจค้นรหัสผ่านมาตรฐานของอุปกรณ์นั้นๆ แล้วเข้าไปรับตั้งค่าต่างๆ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของทรัพยากรต่างๆ ในองค์กรได้ เป็นต้น

1.10 ภัยคุกคามจากการก่อการร้ายและการบ่อนทำลาย คือ ภัยคุกคามที่เกิดขึ้นโดยมีแรงจูงใจในในการบ่อนทำลายความมั่นคงปลอดภัยของทรัพยากรพื้นฐานขององค์กร เช่น ความพยายามในการเข้าควบคุมระบบควบคุมต่างๆ ของโรงไฟฟ้าหรือศูนย์โทรคมนาคมเพื่อสร้างความสับสนวุ่นวายให้กับสังคมและส่งผลกระทบต่อผู้คนในวงกว้าง เพื่อตอบสนองต่อแรงจูงใจทางการเมือง ศาสนา และความเชื่อของกลุ่ม เป็นต้น

1.11 ภัยคุกคามจากการขโมย คือ การโจรกรรมต่างๆ เกิดขึ้นต่อทรัพย์สินขององค์กรไม่ว่าจะเป็นในรูปของข้อมูล ฮาร์ดแวร์ โดยอาจมีแรงจูงใจที่หลากหลาย เช่น การนำสินค้านั้นๆ ไปขายทอดตลาด หรือการนำทรัพย์สินนั้นๆ ไปเพื่อค้นหาข้อมูลที่ต้องการแล้วนำข้อมูลนั้นๆ ไปใช้ประโยชน์ต่อไป เช่น การขโมยคอมพิวเตอร์โน้ตบุ๊กของวิศวกรองค์กรคู่แข่งเพื่อนำไปสืบค้นข้อมูลที่เกี่ยวข้อง เป็นต้น

1.12 ภัยคุกคามจากความผิดพลาดของฮาร์ดแวร์ คือ ภัยคุกคามที่เกิดขึ้นเนื่องจากข้อบกพร่องของฮาร์ดแวร์จนอาจทำให้ส่งกระทบต่อความมั่นคงปลอดภัย เช่น ความผิดพลาดในการออกแบบหน่วยประมวลผลกลาง (Central Processing Unit; CPU) ซึ่งส่งผลให้มีข้อบกพร่องเกี่ยวกับการคำนวณเลขจุดทศนิยม อาจส่งผลเสียต่อความครบถ้วนสมบูรณ์ของข้อมูลและสารสนเทศที่ถูกประมวลผล หรือความผิดพลาดด้านการรักษาความมั่นคงปลอดภัยของอุปกรณ์เราเตอร์ที่หากผู้ไม่ประสงค์ดีทำการโจมตีต่อข้อผิดพลาดดังกล่าวจะสามารถเข้าโจมตีอุปกรณ์อื่นๆ ที่เชื่อมต่อกับเราเตอร์ได้ เป็นต้น

1.13 ภัยคุกคามจากความผิดพลาดของซอฟต์แวร์ คือ ภัยคุกคามที่เกิดจากความผิดพลาดของซอฟต์แวร์ เช่น ข้อผิดพลาดในขั้นตอนการพัฒนาซอฟต์แวร์ที่ไม่ได้รับการทดสอบ ทั้งนี้อาจกล่าวได้ว่าซอฟต์แวร์ที่ถูกใช้งานเกือบทุกชนิดมีช่องโหว่ที่หากผู้ไม่ประสงค์ดีทำการโจมตีต่อช่องโหว่นั้นๆ สำเร็จ จะเป็นภัยคุกคามต่อความมั่นคงปลอดภัยสารสนเทศได้ ผู้สนใจสามารถข้อผิดพลาดที่เกิดขึ้นกับซอฟต์แวร์เพิ่มเติมได้จากเว็บไซต์ www.securityfocus.com

1.14 ภัยคุกคามจากเทคโนโลยีที่ล้าสมัย คือ ภัยคุกคามที่เกิดจากการใช้งานเทคโนโลยีที่ล้าสมัยซึ่งอาจให้สารสนเทศที่ถูกสร้าง ประมวลผล และจัดเก็บขึ้นมีความไม่มั่นคงปลอดภัยโดยเป็นผลสืบเนื่องจากโครงสร้างพื้นฐานของเทคโนโลยีล้าสมัย อันเกิดจากผู้ผลิตเทคโนโลยีดังกล่าวได้ยกเลิกการให้การสนับสนุนหลังการขายเนื่องจากได้มีการพัฒนาเทคโนโลยีใหม่ๆ ขึ้นมาทดแทนเรียบร้อยแล้ว ตัวอย่างที่สำคัญเช่นการใช้งานระบบปฏิบัติการที่ถูกยกเลิกสายการผลิตไปแล้วย่อมไม่ได้รับการปรับปรุงคุณสมบัติ (update) ที่สำคัญๆ ซึ่งหมายความว่าช่องโหว่ที่มีอยู่ในระบบปฏิบัติการนั้นจะไม่ได้รับการแก้ไขจะเป็นการเพิ่มโอกาสของการโจมตีสำเร็จหากคอมพิวเตอร์เครื่องนั้นตกเป็นเป้าหมายของการโจมตี

2. การโจมตี

การโจมตี หมายถึง กิจกรรมต่างๆ ที่กระทำขึ้นต่อช่องโหว่ของทรัพยากรสารสนเทศเพื่อทำลายความมั่นคงปลอดภัยของทรัพยากรนั้นๆ ตลอดจนทรัพยากรอื่นๆ ที่เกี่ยวข้องการโจมตีแตกต่างจากภัยคุกคามในมุมมองที่ว่าภัยคุกคามนั้นจะมีอยู่เสมอนับตั้งแต่องค์กรใช้งานทรัพยากรสารสนเทศ เช่น ภัยคุกคามที่เกี่ยวข้องกับฝนฟ้าคะนองจะเกิดขึ้นก็ต่อเมื่อมีพายุฝนจำนวนมาก แต่ว่าการโจมตีและผลเสียหายที่เกิดขึ้นจากฝนฟ้าคะนองจะเกิดขึ้นก็ต่อเมื่อเกิดฟ้าผ่าทรัพยากรที่เกี่ยวข้องจริงๆ เป็นต้น ในที่นี้จะกล่าวถึงการโจมตีหลักๆ ดังต่อไปนี้

2.1 มัลแวร์ (malware) หมายถึง การโจมตีที่เกิดขึ้นอันเป็นผลจากซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เช่น ไวรัสคอมพิวเตอร์ หนอนอินเทอร์เน็ต โทรจัน หรือซอฟต์แวร์เรียกค่าไถ่ต่างๆ โดยซอฟต์แวร์เหล่านั้นมักมีความสามารถในการดักรับ ทำลาย ขโมย หรือจำกัดการเข้าถึงทรัพยากรสารสนเทศของผู้มีสิทธิ์ใช้งาน

2.2 โฮกส์ (hoax) หมายถึง การโจมตีต่อทรัพยากรสารสนเทศโดยการหลอกผู้ใช้งานว่าซอฟต์แวร์นั้นๆ สามารถกำจัดมัลแวร์ต่างๆ ได้ แต่ในความเป็นจริงแล้วซอฟต์แวร์นั้นถูกพัฒนาขึ้นโดยมีการซ่อนการทำงานพิเศษที่ถูกออกแบบมาให้ทำงานอย่างใดอย่างหนึ่ง เช่น การดักรับข้อมูลจากคีย์บอร์ด ส่งผลต่อ

ความมั่นคงปลอดภัยของทรัพยากรของเป้าหมาย ผู้ใช้งานอาจติดตั้งและแจกจ่ายซอฟต์แวร์นั้นให้กับเพื่อนร่วมงานอื่นๆ ทำให้เกิดการแพร่กระจายมากขึ้น เป็นต้น

2.3 แบคดอร์ (back door) นิยมเรียกอีกอย่างหนึ่งว่าประตูลับโดยมีลักษณะเป็นซอฟต์แวร์ที่ผู้พัฒนาซอฟต์แวร์พัฒนาไว้เพื่อบริหารจัดการซอฟต์แวร์ระหว่างการพัฒนา สำหรับแก้ปัญหาที่เกิดขึ้นจากที่บ้านโดยที่ไม่มีผู้อื่นล่วงรู้ซึ่งอาจเป็นช่องทางที่ถูกใช้ในการโจรกรรมหรือทำลายข้อมูลที่สำคัญขององค์กร นอกจากนี้ยังหมายรวมถึงการติดตั้งซอฟต์แวร์ที่ทำหน้าที่รองรับการเชื่อมต่อจากผู้ไม่ประสงค์ดี เมื่อระบบถูกโจมตีสำเร็จโดยซอฟต์แวร์ดังกล่าวจะทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบได้โดยไม่จำเป็นต้องดำเนินการโจมตีอีกครั้ง แบคดอร์บางชนิดถูกออกแบบให้ทำงานในระดับฮาร์ดแวร์โดยมีวัตถุประสงค์หลักในการดักรับข้อมูลสำคัญ เช่น กุญแจรหัสลับ แล้วส่งข้อมูลนั้นไปยังผู้ไม่ประสงค์ดี

2.4 การแครกรหัสผ่าน (password crack) หมายถึง การดำเนินการวิศวกรรมย้อนกลับเพื่อคำนวณรหัสผ่านที่ใช้ในการพิสูจน์ตัวจริง ผู้ไม่ประสงค์ดีนิยมวิเคราะห์รหัสสำหรับเข้าใช้งานระบบด้วยเทคนิคการวิเคราะห์ไฟล์ฐานข้อมูลผู้ใช้งานซึ่งนิยมเรียกว่า SAM (Security Account Maneger) ที่ถูกจัดเก็บในระบบซึ่งจัดเก็บข้อมูลรหัสในรูปของข้อมูลแฮช

2.5 บรูทฟอร์ซ (brute force) หมายถึง การโจมตีด้วยการคาดเดารหัสผ่านที่เป็นไปได้เข้าสู่บริการที่ต้องการโจมตี โดยการใช้ชื่อผู้ใช้พื้นฐานของระบบหรือชื่อผู้ใช้ที่ตกเป็นเป้าหมายของการโจมตีผ่านฐานข้อมูลรหัสผ่าน ซึ่งนิยมเรียกว่า ดิคชันนารี (dictionary) ซึ่งจัดเก็บรหัสผ่านที่ผู้ใช้งานนิยมเลือกใช้

2.6 การทำให้ระบบปฏิเสธการให้บริการ (Denial of Service; DoS) หมายถึงการโจมตีต่อระบบโดยมุ่งหวังผลทำให้ระบบนั้นไม่สามารถใช้การได้ เทคนิคการโจมตีเพื่อหวังผลดังกล่าวอาจแบ่งแยกได้หลายระดับ เช่น การโจมตีแบบปิงออฟเดด (ping of death) ซึ่งเป็นการโจมตีหวังผลโจมตีต่อเป้าหมายด้วยการส่งข้อมูลไอซีเอ็มพีแพ็กเก็ตขนาดใหญ่ไปยังเครื่องเป้าหมาย หากแฮกเกอร์โจมตีด้วยเทคนิคนี้ต่อเครื่องเป้าหมายนั้นมีช่องโหว่นี้จะส่งผลทำให้เครื่องเป้าหมายไม่สามารถใช้งานเครือข่ายได้ นอกจากนี้ยังมีเทคนิคการโจมตีอื่นๆ เช่น การโจมตีต่อระบบงานเว็บ (web application) ด้วยการส่งข้อมูลที่เมื่อระบบงานประมวลผลแล้วเกิดข้อผิดพลาดอย่างร้ายแรง ไม่สามารถทำงานต่อไปได้ ส่งผลให้ผู้ใช้ที่มีสิทธิ์ใช้งานอื่นๆ ไม่สามารถเข้าใช้งานระบบได้ เป็นต้น

2.7 สปูฟฟิง (spoofing) หมายถึง การปลอมแปลงเป็นบุคคลหรือสิ่งอื่นๆ โดยทำให้เชื่อว่าเป้าหมายกำลังปฏิสัมพันธ์กับบุคคลหรือสิ่งอื่นๆ นั้นจริงๆ เช่น เทคนิคการโจมตีแบบไอพีสปูฟฟิง (IP spoofing) จะหมายถึงการโจมตีที่ผู้โจมตีทำการการปลอมแปลงไอพีแพ็กเก็ตเฮดเดอร์ให้เสมือนกับว่าได้รับอนุญาตให้เข้าใช้งานทรัพยากรบนเครือข่าย เทคนิคการโจมตีที่เกี่ยวข้องกับการปลอมแปลงอื่นๆ เช่น การโจมตีโดยการปลอมแปลงข้อมูลที่เกี่ยวข้องกับบริการสอบถามโดเมน (DNS spoofing)โดยมีรายงานการโจมตีต่อช่องโหว่ของโมเด็มระบบเอดีเอสแอลบางรุ่นที่เมื่อโจมตีสำเร็จจะอนุญาตให้ผู้ไม่ประสงค์ดีสามารถกำหนดไอพีแอดเดรสของโดเมนเนมเซิร์ฟเวอร์เป็นไอพีแอดเดรสที่ผู้ไม่ประสงค์ดีสร้างไว้ เมื่อเครื่องที่เชื่อมต่อกับโมเด็มนั้นสอบถามหมายเลขไอพีแอดเดรสก็จะได้รับไอพีแอดเดรสที่ถูกกำหนดขึ้นโดยผู้ไม่ประสงค์ดี และเพิ่มโอกาสให้เหยื่อสูญเสียข้อมูลพิสูจน์ตัวจริงแก่ผู้ไม่ประสงค์ดีเป็นต้น

2.8 การโจมตีแบบคนกลาง (man-in-the-middle) หมายถึง การโจมตีที่เกิดขึ้นเมื่อผู้ไม่ประสงค์ดีทำการดักรับข้อมูลบนเครือข่ายที่ทำการเปลี่ยนแปลงข้อมูลนั้น จากนั้นจึงส่งข้อมูลที่เปลี่ยนแปลงดังกล่าวไปยังปลายทาง จะเห็นว่าการโจมตีลักษณะนี้จะเกี่ยวข้องกับการปลอมแปลง และควบคุมเส้นทางการเดินทางของข้อมูลให้มีการไหลผ่านผู้ไม่ประสงค์ดี หากเปรียบเทียบจะคล้ายคลึงกับวรรณคดีไทยเกี่ยวกับฤาษีแปลงสาร ที่ผู้ไม่ประสงค์ดีจะดักรับ เข้าถึงและเปลี่ยนแปลงข้อมูลก่อนที่จะส่งไปยังปลายทาง เป็นต้น การลดผลสำเร็จของการโจมตีแบบคนกลางสามารถกระทำให้โดยใช้โครงสร้างพื้นฐานกุญแจสาธารณะ (public key infrastructure) ซึ่งหากผู้ใช้งานมีความตระหนักรู้ถึงวิธีการใช้งานอย่างถูกต้องจะสามารถป้องกันการโจมตีลักษณะนี้ได้เป็นอย่างดี

2.9 สแปม (spam) หมายถึง ลักษณะการได้รับข้อมูลที่ผู้รับไม่ต้องการ เช่น การได้รับจดหมายอิเล็กทรอนิกส์หรือข้อความสั้น (Short Message Service; SMS) ต่างๆ โดยที่ผู้ใช้งานไม่ได้ต้องการรับทราบข้อมูลซึ่งอาจสร้างความรำคาญใจให้กับผู้ใช้งาน หรือในบางกรณีอาจทำให้เกิดการใช้ช่องสัญญาณการสื่อสารมากผิดปกติ เป็นต้น

2.10 การดักรับ/ดักฟัง (sniffing) หมายถึง การโจมตีโดยการดักรับ หรือดักฟังข้อมูลที่รับส่งกันโดยไม่ได้รับสิทธิ์โดยมุ่งหวังการเปิดเผย และแปรความหมายข้อมูลเหล่านั้น ทั้งนี้การดักรับหรือดักฟังสามารถกระทำได้ทั้งในเครือข่ายแบบใช้สายสัญญาณ เช่น อีเธอร์เน็ต (ethernet) สายใยแก้วนำแสง หรือเครือข่ายไร้สายอื่นๆ เช่น เครือข่ายไร้สายเฉพาะบริเวณที่สร้างขึ้นบนโทรศัพท์โดยไม่มีการกำหนดให้มีการเข้ารหัสข้อมูล เป็นต้น

2.11 วิศวกรรมทางสังคม (social engineering) หมายถึง การโจมตีโดยใช้ทักษะที่เกี่ยวข้องกับการเข้าสังคมในการโจมตีต่อเป้าหมายเพื่อให้ได้มาซึ่งข้อมูลที่ใช้ในการพิสูจน์ตัวจริง หรือข้อมูลที่สำคัญอื่นๆ เพื่อใช้ในการพิสูจน์ตัวจริงและได้รับสิทธิ์ในการเข้าใช้งานในระบบ เช่น การโทรศัพท์โดยเลียนเสียงเป้าหมาย หรือการปลอมแปลงเป็นผู้บังคับบัญชาของเหยื่อ เพื่อสอบถามข้อมูลที่ต้องการ ตลอดจนการล่อลวงให้เป้าหมายเข้าใจผิดแล้วกระทำการอย่างใดอย่างหนึ่งเพื่อให้บรรลุเป้าหมายของผู้โจมตี เช่น การหลอกให้เหยื่อโอนเงินผ่านตู้เอทีเอ็ม โดยทำทีเป็นพนักงานของธนาคารซึ่งจะสนทนากับเหยื่อโดยล่อลวงให้กระทำโดยขาดความตระหนักรู้ เทคนิคการโจมตีที่เกี่ยวข้องกับวิศวกรรมทางสังคมที่สำคัญได้แก่ การโจมตีแบบฟิชชิ่งซึ่งมีลักษณะการโจมตีโดยการส่งจดหมายอิเล็กทรอนิกส์หาเหยื่อโดยมีเนื้อหาที่ทำให้เหยื่อกระทำการที่ผู้ไม่ประสงค์ดีต้องการ เช่น แจ้งเตือนว่าบัญชีผู้ใช้งานของเหยื่อถูกโจมตีให้เหยื่อเข้าไปแก้ไขข้อมูลโดย โดยการล่อลวงไปยังเว็บไซต์ปลอมที่มีลักษณะคล้ายคลึงกับเว็บไซต์ของผู้ให้บริการจริงๆ เป็นต้น

2.12 ฟาร์มมิ่ง (pharming) หมายถึง การโจมตีโดยการควบคุมเส้นทางการส่งข้อมูลของผู้ใช้งานไปยังเป้าหมายหลอก โดยมีวัตถุประสงค์หลักในการได้มาซึ่งข้อมูลที่ใช้ในการพิสูจน์ตัวจริงต่อบริการต่างๆ โดยปกติการโจมตีลักษณะนี้จะกระทำผ่านโทรจัน หรือการโจมตีบริการสอบถามโดเมน (DNS cache poisoning) โดยเมื่อผู้ใช้งานเรียกใช้งานบริการที่ต้องการ โทรจันจะเปลี่ยนเส้นทางจากปลายทางที่แท้จริงไปยังเว็บไซต์ปลอมที่ถูกสร้างขึ้นมาสำหรับรับข้อมูลพิสูจน์ตัวจริง เป็นต้น

กิจกรรม 14.1.2

1. จงอธิบายลักษณะของผลกระทบต่อความมั่นคงปลอดภัยที่เกิดจากภัยคุกคามที่เกิดขึ้นตามธรรมชาติ

2. จงอธิบายผลกระทบของสแปมเมลต่อการให้บริการจดหมายอิเล็กทรอนิกส์ และความเกี่ยวข้องกับการโจมตีด้วยเทคนิคทางสังคม

แนวตอบกิจกรรม 14.1.2

1. โดยปกติภัยคุกคามตามธรรมชาติมักส่งผลโดยตรงต่อความพร้อมใช้ของทรัพยากรนั้นๆ เช่น เมื่อเกิดฟ้าผ่าต่ออุปกรณ์สื่อสาร อาจทำให้อุปกรณ์นั้นๆ เสียหายไม่สามารถใช้งานได้ เป็นต้น

2. จดหมายอิเล็กทรอนิกส์ส่งผลโดยตรงต่อผู้ใช้งานที่เป็นเจ้าของอีเมลนั้นๆ นอกจากนี้ยังส่งผลทำให้มีการใช้งานเครือข่ายมากขึ้น ในกรณีที่ช่องสัญญาณการสื่อสารมีไม่มากพออาจส่งผลให้ช่องสัญญาณเต็มหรือใช้พื้นที่ในระบบเต็มและไม่สามารถรับจดหมายที่ควรได้ เป็นต้น และมีความเกี่ยวข้องกับการโจมตีด้วยเทคนิคทางสังคมเนื่องจากเป็นช่องทางหนึ่งในการเข้าถึงเหยื่อ โดยหากเหยื่อหลงเชื่อและดำเนินการตามข้อความที่ปรากฏในจดหมายนั้นอาจทำให้การโจมตีต่อๆ มาสำเร็จได้ เป็นต้น

มสธ

ตอนที่ 14.2
แนวทางการจัดการความมั่นคงปลอดภัยระบบคอมพิวเตอร์

โปรดอ่านหัวเรื่อง แนวคิด และวัตถุประสงค์ของตอนที่ 14.2 แล้วจึงศึกษารายละเอียดต่อไป

หัวเรื่อง

14.2.1 แบบจำลองความมั่นคงปลอดภัย

14.2.2 แนวทางบริหารจัดการความมั่นคงปลอดภัย

แนวคิด

1. แบบจำลองการรักษาความมั่นคงปลอดภัยถูกพัฒนาขึ้นเพื่อใช้ในการกำหนดนโยบาย วิธีการ ตลอดจนเทคโนโลยีที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยทรัพยากรนั้นๆ แบบจำลองที่นิยมใช้อย่างแพร่หลายในการรักษาความมั่นคงปลอดภัยคือ แบบจำลองของจอห์น แมคคิวเบอร์ ซึ่งกำหนดเป้าหมายหลักของการรักษาความมั่นคงปลอดภัยซึ่งประกอบด้วยการรักษาความลับ การรักษาความครอบถ้วนสมบูรณ์ และความพร้อมใช้ โดยครอบคลุมถึงสถานะของทรัพยากรที่ต้องการรักษาความมั่นคงปลอดภัย ตลอดจนแนวทางการป้องกันที่เหมาะสม
2. การประยุกต์ใช้งานเทคโนโลยีร่วมกับการบริหารจัดการความมั่นคงปลอดภัยอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการกำหนดนโยบาย การประยุกต์ใช้งานเทคโนโลยีที่เกี่ยวข้อง และควบคุมการปฏิบัติให้เป็นไปตามที่กำหนดในนโยบายจะสร้างความมั่นใจได้ว่าการผลิต ประมวลผล จัดเก็บ และแสดงผลทรัพยากรสารสนเทศนั้นๆ มีความมั่นคงปลอดภัยกล่าวได้ว่าความสำเร็จของการรักษาความมั่นคงปลอดภัยขึ้นอยู่กับการวางแผนและกำหนดนโยบายการรักษาความมั่นคงปลอดภัย การปฏิบัติตามแผนการ การตรวจสอบการปฏิบัติตามวงรอบ และการปรับเปลี่ยนแผนนโยบายให้สอดคล้องกับเหตุการณ์ที่เปลี่ยนแปลง

วัตถุประสงค์

เมื่อศึกษาตอนที่ 14.2 จบแล้ว นักศึกษาสามารถ

1. ประยุกต์ใช้หลักการรักษาความมั่นคงปลอดภัยได้
2. วิเคราะห์ความสำคัญของมนุษย์ต่อการรักษาความมั่นคงปลอดภัยได้
3. วิเคราะห์ความสำคัญของนโยบายการรักษาความมั่นคงปลอดภัยได้
4. วิเคราะห์ผลกระทบของการโจมตีต่อทรัพยากรสารสนเทศได้
5. กำหนดมาตรการป้องกันที่เหมาะสมสำหรับรักษาความมั่นคงปลอดภัยได้
6. วิเคราะห์ข้อจำกัดของมาตรการป้องกันได้

เรื่องที่ 14.2.1
แบบจำลองความมั่นคงปลอดภัย

แบบจำลองความมั่นคงปลอดภัย (computer security model) เป็นเครื่องมือที่ถูกพัฒนาขึ้นสำหรับการบริหารความมั่นคงปลอดภัยของสารสนเทศ มีขอบเขตรวมถึงการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ และการจัดการนโยบายที่เกี่ยวข้องอื่นๆ โดยมีวัตถุประสงค์หลักในการกำหนดมาตรการควบคุม แนวทางการป้องกัน การกำหนดนโยบายและกฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

1. แบบจำลองความมั่นคงปลอดภัยของแมคคิวเบอร์

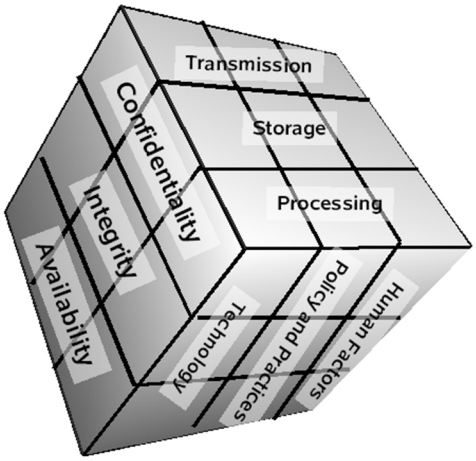
มีผู้เสนอแบบจำลองความมั่นคงปลอดภัยไว้หลากหลาย เช่น แบบจำลองของแกรมและเดนนิ่ง[6] แบบจำลองของคลากและวินสัน[7] แบบจำลองของบริวและแนช[8] เป็นต้น แต่แบบจำลองความมั่นคงปลอดภัยที่ได้รับการยอมรับอย่างกว้างขวางในการปรับใช้กับการรักษาความมั่นคงปลอดภัยสารสนเทศถูกพัฒนาขึ้นโดยจอห์น แมคคัมเบอร์ (John McCumber) โดยนำเสนอเป็นแผนภาพดังที่แสดงในภาพที่ 14.7 และได้รับความนิยมเรียกว่า แมคคัมเบอร์คิวบ์ (McCumber Cube) โดยแสดงองค์ประกอบที่จำเป็นในการรักษาความมั่นคงปลอดภัยของข้อมูลข่าวสาร ได้แก่ เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย (desired goal) สถานะของสารสนเทศ (information state) และแนวทางป้องกัน (safe guard)

---

[6] Graham–Denning model นำเสนอแบบจำลองที่กำหนดกระบวนการและวิธีการสำหรับการสร้าง ลบสารสนเทศ และการกำหนดมาตรการควบคุมการเข้าถึงและกำหนดสิทธิ์อย่างเหมาะสม

[7] Clark–Wilson model นำเสนอแบบจำลองที่กำหนดกระบวนการ วิธีการและแนวทางการวิเคราะห์ความครบถ้วนสมบูรณ์ของสารสนเทศ

[8] Brewer and Nash model นำเสนอแบบจำลองการควบคุมการเข้าถึงสารสนเทศที่สามารถปรับเปลี่ยนได้หากมีการกำหนดมาตรการที่มีการทับซ้อนกันระหว่างทรัพยากร



ภาพที่ 14.7 แมคคัมเบอร์คิวบ์

ที่มา: http://en.wikipedia.org/wiki/McCumber_cube สืบค้นเมื่อ 20 กันยายน 2558.

โดยในแต่ละองค์ประกอบหลักจะมีรายละเอียดที่เกี่ยวข้องดังต่อไปนี้

1.1 เป้าหมายหลักของการรักษาความมั่นคงปลอดภัย

1.1.1 การรักษาความลับ (confidentiality) หมายถึง การจัดการให้ทรัพยากรนั้นถูกล่วงรู้และแปลความหมายได้จากผู้ที่มีสิทธิ์

1.1.2 การรักษาความครบถ้วนสมบูรณ์ (integrity) หมายถึง การจัดการให้ทรัพยากรนั้นมีความครบถ้วนสมบูรณ์ มีกลไกตรวจสอบการถูกเปลี่ยนแปลงแก้ไข

1.1.3 การรักษาความพร้อมใช้ (availability) หมายถึง การจัดการให้ทรัพยากรนั้นถูกเข้าถึงและใช้งานได้จากผู้มีสิทธิ์อยู่เสมอ

1.2 สถานะของสารสนเทศ

1.2.1 การจัดเก็บ (storage) หมายถึง ทรัพยากรสารสนเทศใดๆ ที่ถูกจัดเก็บในแหล่งจัดเก็บข้อมูล เช่น สภาวะที่สารสนเทศนั้นถูกจัดเก็บในหน่วยความจำ ฮาร์ดดิสก์ เป็นต้น

1.2.2 การประมวลผล (processing) หมายถึง ทรัพยากรสารสนเทศใดๆ ที่ถูกกำลังถูกประมวลผล

1.2.3 การรับส่ง (transmission) หมายถึง ทรัพยากรสารสนเทศใดๆ ที่กำลังถูกรับ–ส่งผ่านตัวกลางการสื่อสาร เช่น การส่งข้อมูลพิสูจน์ตัวจริงผ่านเครือข่าย เป็นต้น

1.3 แนวทางป้องกัน

1.3.1 การจัดการนโยบาย (policy) หมายถึง การกำหนดระเบียบ วิธีปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศต่างๆ

1.3.2 ทรัพยากรมนุษย์ (human factor) หมายถึง บุคคลที่มีส่วนเกี่ยวข้องกับทรัพยากรสารสนเทศนั้นๆ

1.3.3 เทคโนโลยี (technology) หมายถึง เทคโนโลยีที่เกี่ยวข้องและสามารถนำมาประยุกต์ใช้ในการรักษาความมั่นคงปลอดภัยทรัพยากรสารสนเทศ เช่น เทคโนโลยีการเข้ารหัสลับ เทคโนโลยีที่เกี่ยวข้องกับการพิสูจน์ตัวจริง เป็นต้น

จากแบบจำลองนี้เมื่อต้องการรักษาความมั่นคงปลอดภัยให้กับทรัพยากรใดๆ ผู้มีส่วนเกี่ยวข้องจะต้องพิจารณาเป้าหมายหลักของการรักษาความมั่นคงปลอดภัยร่วมกับมุมมองอื่นๆ คือ สถานะของสารสนเทศ และแนวทางป้องกัน เช่น พื้นผิวที่เป็นจุดตัดกันระหว่าง การรับส่งข้อมูล การรักษาความลับและเทคโนโลยี แสดงให้เห็นถึงความจำเป็นที่จะต้องมีการเลือกใช้เทคโนโลยีที่เหมาะสมสำหรับการรักษาความลับของข้อมูลข่าวสารที่ถูกรับส่งระหว่างกัน ซึ่งเทคโนโลยีที่เกี่ยวข้องในกรณีนี้อาจเกี่ยวข้องกับการเข้ารหัสข้อมูลข่าวสารนั้นๆ กระบวนการพิสูจน์ตัวจริงของอุปกรณ์สื่อสารเพื่อให้มั่นใจได้ว่าการรับส่งข้อมูลนั้นจะไม่ถูกส่งต่อไปยังอุปกรณ์ที่ไม่ได้รับสิทธิ์ ทั้งนี้แบบจำลองนี้จะถูกใช้ในการพิจารณากำหนดนโยบายและข้อกำหนดที่เกี่ยวข้องกับการควบคุม การประยุกต์ใช้งานเทคโนโลยีต่างๆ เพื่อรักษาความมั่นปลอดภัยของข้อมูลข่าวสาร ซึ่งจะถูกกล่าวถึงต่อๆ ไปในหน่วยการเรียนการสอนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

2. ตัวอย่างการประยุกต์ใช้งานแบบจำลอง

2.1 การโจมตีของซอฟต์แวร์ไม่พึงประสงค์ ซอฟต์แวร์ไม่พึงประสงค์ในปัจจุบันมีความสามารถในการโจมตีต่อทรัพยากรของระบบคอมพิวเตอร์ได้หลากหลาย โดยในที่นี้เป็นการยกตัวอย่างการใช้งานแบบจำลองของแมคคัมเบอร์ในการรักษาความมั่นคงปลอดภัยจากการโจมตีของคีย์ล็อกเกอร์ซึ่งเป็นซอฟต์แวร์ไม่พึงประสงค์ที่ถูกออกแบบมาสำหรับการดักรับข้อมูลการใช้งานคอมพิวเตอร์ผ่านคีย์บอร์ด แบบจำลองของแมคคัมเบอร์สามารถนำมาประยุกต์ใช้ในการรักษาความมั่นคงปลอดภัยจากการโจมตีของซอฟต์แวร์ไม่พึงประสงค์ดังที่แสดงตารางที่ 14.1

ตารางที่ 14.1 การประยุกต์ใช้แบบจำลองแมคคัมเบอร์สำหรับการโจมตีของซอฟต์แวร์ไม่พึงประสงค์

เป้าหมายหลัก	สถานะ	แนวทางการป้องกัน
ความลับ	การจัดเก็บ ประมวลผล	นโยบาย : การติดตั้งและปรับปรุงฐานข้อมูลมัลแวร์ : การกำหนดตารางการตรวจสอบมัลแวร์ตามช่วงระยะเวลา เทคโนโลยี : ระบบตรวจจับผู้บุกรุกสำหรับโฮสต์ : ระบบตรวจจับมัลแวร์ ทรัพยากรบุคคล : พัฒนาความตระหนักรู้ : เสริมสร้างความรู้ความเข้าใจ

2.2 การโจมตีด้วยเทคนิคการทำให้ระบบปฏิเสธการให้บริการแบบ DDoS การโจมตีด้วยเทคนิคการทำให้ระบบปฏิเสธการให้บริการ (Denial of Service) เป็นภัยคุกคามที่สำคัญประการหนึ่งของการให้บริการอินเทอร์เน็ตที่ส่งผลให้ผู้ที่มีสิทธิ์ใช้งานไม่สามารถใช้งานเครือข่ายได้ ในทีนี้เป็นตัวอย่างการประยุกต์ใช้แบบจำลองของแมคคัมเบอร์ในการรักษาความมั่นคงปลอดภัยต่อการโจมตีด้วยเทคนิค DDoS ซึ่งเป็นการโจมตีจากผู้ไม่ประสงค์ดีหลายๆ รายพร้อมๆ กัน เมื่อพิจารณาภัยคุกคามและแนวทางการจัดการต่อภัยคุกคามดังที่แสดงในตารางที่ 14.2

ตารางที่ 14.2 การประยุกต์ใช้แมคคัมเบอร์โมเดลสำหรับจัดการ DDoS

เป้าหมายหลัก	สถานะ	แนวทางการป้องกัน
ความพร้อมใช้	การรับส่ง	นโยบาย : การเฝ้าตรวจเครือข่าย เทคโนโลยี : ระบบตรวจจับผู้บุกรุกทางเครือข่าย (IDS) ทรัพยากรบุคคล : พัฒนาความสามารถให้ตอบสนองต่อสถานการณ์

2.3 การโจมตีด้วยเทคนิคบรู๊ทฟอร์ซต่อบริการเอฟทีพี การโจมตีด้วยเทคนิคบรู๊ทฟอร์ซจะสุ่มรหัสผ่านจากฐานข้อมูลรหัสผ่านที่ได้รับความนิยมตั้งแล้วส่งเข้าสู่บริการโดยมีวัตถุประสงค์หลักเพื่อเข้าใช้งานบริการโดยไม่ได้รับอนุญาตหากรหัสผ่านที่ตั้งไว้เป็นรหัสผ่านที่ตรงกับฐานข้อมูลจะทำให้ผู้ไม่ประสงค์ดีสามารถเข้าใช้งานระบบได้ และอาจทำให้ผู้ไม่ประสงค์ดีสามารถเปลี่ยนรหัสผ่าน เปลี่ยนแปลงแก้ไขข้อมูลในเซิร์ฟเวอร์ และปลอมแปลงเป็นเจ้าของบัญชีผู้ใช้นั้นได้

ตารางที่ 14.3 การประยุกต์ใช้แบบจำลองแมคคัมเบอร์สำหรับจัดการ FTP Bruteforcing

เป้าหมายหลัก	สถานะ	แนวทางการป้องกัน
ความลับ ความครบถ้วนสมบูรณ์ ความพร้อมใช้	การจัดเก็บ	นโยบาย : การตั้งรหัสผ่าน การจำนวนความผิดพลาดในการพิสูจน์ตัวจริง การเฝ้าตรวจเหตุการณ์ผิดปกติ เทคโนโลยี : ระบบตรวจจับผู้บุกรุก ทรัพยากรบุคคล : ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดาและไม่ปรากฏในฐานข้อมูลรหัสผ่าน

จะเห็นว่าการนำเทคโนโลยีที่ดีที่สุดประกอบกับการกำหนดนโยบายการรักษาความมั่นคงปลอดภัยที่ดีที่สุด ยังไม่อาจกล่าวได้ว่าการสร้างความมั่นคงปลอดภัยให้กับทรัพยากรสารสนเทศแบบสมบูรณ์นั้นเป็นไปได้ ไม่ว่าจะในระดับองค์กรหรือระดับบุคคลทั้งนี้เนื่องจากการรักษาความมั่นคงปลอดภัยเป็นกระบวนการ และการดำเนินการให้มั่นใจได้ว่าทรัพยากรเหล่านั้นถูกใช้งานอย่างมั่นคงปลอดภัย อย่างไรก็ดีการนำแบบจำลองของแมคคิวเบอร์มาประยุกต์ใช้ในการจัดการความเสี่ยง และบริหารความเสี่ยงจะเป็นเครื่องมือ และตัวชี้วัดพื้นฐานที่สำคัญสำหรับการรักษาความมั่นคงปลอดภัย

กิจกรรม 14.2.1

1. จงประยุกต์ใช้แบบจำลองแมคคัมเบอร์สำหรับการแอบดูรหัสผ่าน
2. จงประยุกต์ใช้แบบจำลองแมคคัมเบอร์สำหรับการดักรับข้อมูลพิสูจน์ตัวจริงต่อระบบจดหมายอิเล็กทรอนิกส์ผ่านเว็บ

แนวตอบกิจกรรม 14.2.1

1.

เป้าหมายหลัก	สถานะ	แนวทางการป้องกัน
ความลับ	การรับส่ง	นโยบาย : ไม่เปิดเผยรหัสผ่านต่อผู้อื่น ไม่ติดรหัสผ่านบนหน้าจอ เทคโนโลยี : ใช้เทคโนโลยีสำหรับการพิสูจน์ตัวจริงเช่น ยูเอสบีโทเคน ทรัพยากรบุคคล : ผู้ใช้งานได้รับการอบรมชี้แจงให้ตระหนักถึงรูปแบบและวิธีการป้องกันการแอบดูรหัสผ่าน

2.

เป้าหมายหลัก	สถานะ	แนวทางการป้องกัน
ความลับ	การรับส่ง	นโยบาย : บังคับใช้การเทคนิคการเข้ารหัสสำหรับการใช้งานบริการจดหมายอิเล็กทรอนิกส์ เทคโนโลยี : HTTPS ทรัพยากรบุคคล : ผู้ใช้งานได้รับการอบรมชี้แจงให้ตระหนักถึงรูปแบบข้อบ่งชี้และเหตุผิดปกติที่เป็นผลของการโจมตี

เรื่องที่ 14.2.2
แนวทางบริหารจัดการความมั่นคงปลอดภัย

การประยุกต์ใช้งานเทคโนโลยีร่วมกับการบริหารจัดการความมั่นคงปลอดภัยอย่างเหมาะสม โดยเฉพาะอย่างยิ่งการกำหนดนโยบาย การประยุกต์ใช้งานเทคโนโลยีที่เกี่ยวข้อง และควบคุมการปฏิบัติให้เป็นไปตามที่กำหนดในนโยบายจะสร้างความมั่นใจได้ว่าการผลิต ประมวลผล จัดเก็บ และแสดงผลทรัพยากรสารสนเทศนั้นๆ มีความมั่นคงปลอดภัย

1. การควบคุมการเข้าถึงทรัพยากร

การควบคุมการเข้าถึงทรัพยากรสารสนเทศจะถูกดำเนินการโดยการกำหนดและใช้งานมาตรการควบคุม (access control) ซึ่งหมายถึง กระบวนการ วิธีการ หรือระบบซึ่งจะทำการตรวจสอบผู้ใช้งานก่อนอนุญาตให้ผู้ใช้งานที่ผ่านการตรวจสอบนั้นเข้าถึงทรัพยากรสารสนเทศใดๆ ได้ ยกตัวอย่าง มาตรการควบคุมสำหรับการเข้าใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทั่วไปที่นิยมใช้คือ การป้อนรหัสผู้ใช้งานและรหัสผ่าน มาตรการควบคุมสำหรับการผ่านเข้าออกห้องอาจมีการติดตั้งระบบคีย์การ์ดให้เฉพาะผู้ที่มีการ์ดเท่านั้นจึงจะสามารถเข้าออกได้ หรือแม้กระทั่งการแจกจ่ายกุญแจเฉพาะเจ้าหน้าที่ผู้มีหน้าที่เกี่ยวข้องในการเข้าถึงห้องใดห้องหนึ่ง ก็จัดเป็นมาตรการการควบคุม ทั้งนี้มาตรการควบคุมสามารถจำแนกเป็น 3 ประเภท คือ

1.1 การควบคุมการเข้าถึงภาพบังคับ (mandatory access control) หมายถึง หลักการควบคุมการเข้าถึงแบบที่ผู้ใช้งานไม่สามารถเปลี่ยนแปลงสิทธิ์การเข้าถึงทรัพยากรได้ด้วยตนเอง เหมาะสำหรับการควบคุมทรัพยาการที่มีข้อมูลและสิทธิ์ของผู้ใช้งานมีความชัดเจน เนื่องจากผู้ใช้งานแต่ละคนจะถูกแบ่งมอบสิทธิ์ในการเข้าถึงทรัพยากรเป็นกลุ่มๆ (class or category) ในแต่ละกลุ่มจะมีการจัดลำดับความมั่นคงปลอดภัย เช่น การแบ่งข้อมูลออกแบบลับที่สุด ลับมาก ลับ และไม่จัดลำดับชั้นความลับ เป็นต้น

1.2 การควบคุมการเข้าถึงโดยผู้ใช้ (discretionary access control) มีหลักการการควบคุมการเข้าถึงทรัพยากรในลักษณะของการให้สิทธิ์แก่เจ้าของหรือผู้ได้รับสิทธิ์นั้น เมื่อมีการร้องขอการพิสูจน์สิทธิ์จากผู้ใช้งาน กลไกการตรวจสอบสิทธิ์ที่ได้รับอนุญาตของผู้ใช้งานจะถูกตรวจสอบ และกลไกนี้จะเป็นผู้ส่งต่อสิทธิ์ที่ผู้ใช้งานได้รับให้สามารถเข้าถึงทรัพยากรได้อีกต่อหนึ่ง ซึ่งกลไกนี้เป็นกลไกมาตรฐานที่ระบบฐานข้อมูลนิยมใช้ในการควบคุมการเข้าถึง โดยทั่วไปเป็นที่เข้าใจได้ว่าผู้ใดสร้างหรือเป็นเจ้าของทรัพยากรผู้นั้นจะสามารถเข้าถึงและมอบสิทธิ์การเข้าถึงให้แก่ผู้อื่นได้

1.3 การควบคุมการเข้าถึงตามบทบาท (role-based access control) เป็นการควบคุมการเข้าถึงทรัพยากรตาม “หน้าที่” ที่ผู้ใช้งานมีต่อทรัพยากรสารสนเทศ กลไกควบคุมการเข้าถึงแบบนี้มีความเหมาะสมต่อการควบคุมการเข้าถึงทรัพยากรในระบบสารสนเทศ หรือโครงสร้างพื้นฐานระบบสารสนเทศที่มีความซับซ้อนเนื่องจากในระบบที่มีความซับซ้อนมากๆ มักมีความต้องการควบคุมทรัพยากรที่หลากหลาย หน้าที่

ของผู้ใช้งานจึงถูกนำมาพิจารณาในการกำหนดสิทธิ์ ทำให้มั่นใจได้ว่าจะไม่มีผู้ใช้งานคนใดที่สามารถเข้าถึงหรือบริหารระบบได้ทั้งหมด การที่มีผู้สามารถเข้าถึงหรือบริหารระบบได้แต่เพียงผู้เดียวย่อมมีความเสี่ยงในการที่ข้อมูลหรือสารสนเทศในระบบนั้นจะถูกเปลี่ยนแปลงแก้ไขอย่างไม่ถูกต้อง ตัวอย่างหนึ่งของการควบคุมการเข้าถึงตามบทบาทคือ การควบคุมการเข้าถึงซอฟต์แวร์ที่ใช้ในการปรับแต่งคุณสมบัติของระบบปฏิบัติการซึ่งกำหนดให้ผู้ใช้งานต้องได้รับสิทธิ์เป็นผู้ดูแลระบบ (administrator) เป็นต้น

2. กลไกการควบคุมการเข้าถึงทรัพยากร

โดยปกติมาตรการการควบคุมที่ได้กล่าวมา มักถูกใช้ร่วมกับกลไกสำคัญต่อไปนี้ การแสดงตน การพิสูจน์ตัวจริง การกำหนดสิทธิ์ และการกำหนดความรับผิดชอบ ในกรณีนี้จะยกตัวอย่าง มาตรการควบคุมการเข้าถึงและใช้บริการธุรกรรมผ่านอินเทอร์เน็ตของสถาบันการเงินแห่งหนึ่ง ซึ่งลูกค้าสามารถเข้าใช้งานได้ผ่านเว็บเบราว์เซอร์ และซอฟต์แวร์ที่ทำงานบนโทรศัพท์เคลื่อนที่

2.1 การแสดงตน (identification) เป็นกลไกที่ใช้ในการควบคุมผู้ใช้งานที่ต้องการเข้าถึงทรัพยากรตามช่องทางที่ทรัพยากรนั้นๆ กำหนดขึ้น ในกรณีนี้ ผู้ใช้งานจะต้องใช้งานอาจถูกร้องขอให้ใช้งานผ่านเว็บเบราว์เซอร์ที่ได้รับความนิยมใช้งาน (เช่น ไฟร์ฟอกซ์ กูเกิ้ลโครม) และซอฟต์แวร์ที่ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้นเท่านั้น หากการร้องขอใช้งานจากซอฟต์แวร์อื่นๆ เช่น โอเปราเบราว์เซอร์ หรือซอฟต์แวร์ที่ไม่ได้ถูกพัฒนาขึ้นโดยสถาบันการเงินแห่งนั้นจะไม่เข้าถึงและพิสูจน์ตัวจริงได้

2.2 การพิสูจน์ตัวจริง (authentication) เป็นกลไกที่ใช้ในการตรวจสอบความถูกต้องของผู้ที่มาแสดงตนขอเข้าถึงทรัพยากรสารสนเทศ การพิสูจน์ตัวจริงนิยมกระทำด้วยการตรวจสอบ “ความถูกต้อง” ของข้อมูลสำหรับการพิสูจน์ตัวจริง โดยแบ่งลักษณะของข้อมูลนั้นได้ 3 ลักษณะ คือ

1) ข้อมูลที่ผู้แสดงตนทราบ (something you know) เช่น ชื่อผู้ใช้งาน รหัสผ่าน หมายเลขพินสำหรับใช้งานเอทีเอ็ม เป็นต้น

2) ข้อมูลที่ผู้แสดงตนมี (something you has) เช่น บัตรเอทีเอ็ม หมายเลขบัตร เป็นต้น

3) ข้อมูลที่ผู้แสดงตนเป็น (something you are) เช่น ข้อมูลลายนิ้วมือ ข้อมูลม่านตา เป็นต้น

สำหรับกรณีการเข้าถึงบริการธนาคารอิเล็กทรอนิกส์ในปัจจุบันนิยมใช้กลไกในการพิสูจน์ตัวจริงโดยใช้แหล่งที่มาของข้อมูลร่วมกันเพื่อให้มั่นใจได้ว่าผู้ที่แสดงตนนั้นเป็นผู้ที่มีสิทธิ์เข้าถึงทรัพยากรนั้นจริงๆ โดยการใช้ข้อมูลชื่อผู้ใช้งาน รหัสผ่าน ร่วมรหัสผ่านแบบใช้ครั้งเดียว (One-Time Password; OTP) ที่ระบบจะเป็นผู้ส่งรายละเอียดไปยังโทรศัพท์มือถือเป็นครั้งๆ ไป เป็นต้น

2.3 การกำหนดสิทธิ์ (authorization) คือ กลไกในการตรวจสอบและส่งมอบสิทธิ์สำหรับการเข้าถึงทรัพยากรสารสนเทศให้กับผู้ใช้งานที่ผ่านการพิสูจน์สิทธิ์ตามที่ได้กำหนดไว้ในมาตรการการควบคุมการเข้าถึงสารสนเทศสำหรับผู้ใช้งานรายนั้นๆ ซึ่งการกำหนดสิทธิ์ก็จะสอดคล้องกับประเภทของการควบคุมการเข้าถึงดังที่ได้กล่าวมาแล้วในตอนต้น

2.4 การกำหนดความรับผิดชอบ (accountability) เป็นกลไกที่ทำให้มั่นใจได้ว่าผู้ใช้งานที่เข้าใช้งานตลอดจนผู้ไม่ประสงค์ดีที่พยายามเข้าใช้งานจะสามารถถูกตรวจสอบและเป็นผู้รับผิดชอบผลของการกระทำที่มีต่อทรัพยากรสารสนเทศนั้นๆ ได้ วิธีการและเทคโนโลยีสำคัญที่ใช้ในการตรวจสอบและกำหนดความรับผิดชอบคือการจัดเก็บข้อมูลการจราจร การจัดเก็บประวัติการใช้งานหรือที่นิยมเรียกว่า ล็อก (log) ของทรัพยากรต่างๆ ที่มี

3. มาตรฐานที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัย

เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศเป็นไปอย่างสอดคล้องกันตามคุณลักษณะเฉพาะและรูปแบบการดำเนินงานขององค์กร และสอดคล้องกับกฎหมายที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย องค์กรที่ทำหน้าที่คิดค้นและกำหนดมาตรฐานต่างๆ จึงกำหนดมาตรการและแนวทางที่เกี่ยวข้องเพื่อให้องค์กรต่างๆ นำไปประยุกต์ใช้สร้างความมั่นคงปลอดภัยให้กับทรัพยากรต่างๆ ขององค์กร ทั้งนี้หากองค์กรที่นำแนวทางที่กำหนดขึ้นไปใช้และผ่านการตรวจสอบมาตรฐานย่อมส่งผลดีต่อภาพลักษณ์ขององค์กรซึ่งเป็นการสร้างความน่าเชื่อถือและความมั่นใจต่อผู้มีส่วนได้เสียต่างๆ เช่น ผู้ถือหุ้น พนักงาน และตัวชี้วัดการจัดการความมั่นคงปลอดภัยของทรัพยากรสารสนเทศในองค์กรไปพร้อมๆ กัน ทั้งนี้มาตรฐานต่างๆ ที่กำหนดขึ้นเป็นมาตรฐานสากลย่อมมีความน่าเชื่อถือสูงเนื่องจากเป็นที่ยอมรับและถูกนำไปใช้อย่างแพร่หลาย มาตรฐานสำคัญๆ เช่น ชุดมาตรฐาน ISO 27000, COBIT เป็นต้น

3.1 ชุดมาตรฐาน ISO 27000 เป็นชุดมาตรฐานที่พัฒนาโดยองค์กรระหว่างประเทศว่าด้วยการมาตรฐาน (International Organization for Standardization; ISO) ต่อจากมาตรฐาน ISO 17799 โดยมีการรวบรวมมาตรการพื้นฐานหลากหลายมาตรฐาน ได้แก่ BS 7799-1, BS 7799-2, BS 7799-3 โดยมีเนื้อหาสำคัญเกี่ยวข้องกับการจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัย เช่น ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยของข้อมูล วิธีและกระบวนการประเมินความเสี่ยง การปฏิบัติเพื่อลดความเสี่ยงและการบริหารจัดการความเสี่ยง ขั้นตอนวิธีการดำเนินการบริหารความเสี่ยง เป็นต้น ในชุดมาตรฐานนี้จะประกอบด้วยมาตรฐานที่สำคัญๆ เช่น

- ISO 27000 เป็นชุดมาตรฐานที่รวบรวมนิยามศัพท์ต่างๆ ที่เกี่ยวข้องกับการจัดการความมั่นคงปลอดภัยสารสนเทศ
- ISO 27001 เป็นมาตรฐานที่กำหนดคุณลักษณะเฉพาะที่เกี่ยวข้องกับการบริหารจัดการรักษาความมั่นคงปลอดภัยโดยวัตถุประสงค์หลักในการสร้างมาตรการควบคุมที่จำเป็นในการรักษาความมั่นคงปลอดภัยที่ถูกเรียกว่าระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System; ISMS)
- ISO 27002 เป็นมาตรฐานที่กำหนดหลักปฏิบัติ แนวทางการจัดการความมั่นคงปลอดภัยที่มีการรวบรวมวัตถุประสงค์ วิธีการสร้างมาตรการควบคุม และรายละเอียดการปฏิบัติที่เกี่ยวข้องในการควบคุมความมั่นคงปลอดภัย
- ISO 27003 เป็นแนวทางการประยุกต์ใช้งานมาตรฐานในชุด ISO 27000

- ISO 27004 กำหนดแนวทางการตรวจวัดประสิทธิภาพการจัดการรักษาความมั่นคงปลอดภัย เพื่อช่วยในการประเมินผลหรือตรวจวัดประสิทธิภาพ
- ISO 27005 กำหนดแนวทางการจัดการความเสี่ยงที่เกี่ยวข้องกับทรัพยากรสารสนเทศ
- ISO 27006 กำหนดแนวทางการออกใบรับรองและการลงทะเบียนให้กับหน่วยงานต่างๆ ที่เกี่ยวข้อง

จะเห็นได้ว่าหลักสำคัญของชุดมาตรฐานนี้คือ การสร้างระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISMS) โดยผู้ที่จะนำมาตรฐานนี้มาประยุกต์ใช้จะต้องมีการกำหนดแผน และการปฏิบัติหลายประการในการสร้างการบริหารจัดการที่เหมาะสม โดยมีการดำเนินการเป็นวงรอบประกอบด้วยการวางแผน การปฏิบัติตามแผน การตรวจสอบ และการปรับปรุง ดังแสดงในภาพที่ 14.8

ภาพที่ 14.8 วงรอบการจัดการระบบบริหารจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ ISO 27001

3.2 มาตรฐาน COBIT (Control Objective for Information and Related Technology) เป็นมาตรฐานที่ถูกกำหนดขึ้นโดยสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ (Information System Audit and Control Association; ISACA) โดยรวบรวมแนวคิดและเฟรมเวิร์คเพื่อสร้างการควบคุมภายในที่เกี่ยวข้องกับเทคโนโลยีที่ถูกใช้งานในองค์กรเพื่อควบคุมคุณภาพของทรัพยากรสารสนเทศโดยมุ่งเน้นการตรวจวัดประสิทธิผล ประสิทธิภาพ การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ ความพร้อมใช้ การปฏิบัติตามกฎระเบียบและกฎหมาย และความน่าเชื่อถือของทรัพยากรสารสนเทศซึ่งประกอบด้วย ข้อมูลหรือสารสนเทศ กระบวนการทำงานและซอฟต์แวร์ที่เกี่ยวข้อง เทคโนโลยี สถานที่และโครงสร้างพื้นฐานทางกายภาพ และบุคลากร ที่มีส่วนเกี่ยวข้องกับองค์กรนั้นๆ มาตรฐานนี้มีแนวความคิดที่คล้ายคลึงกับมาตรฐาน ISO 27001 แต่มีการออกแบบให้เหมาะสมสำหรับกระบวนการทางธุรกิจโดยประกอบวัตถุประสงค์หลักของการควบคุมจำนวน 34 วัตถุประสงค์ที่สามารถจำแนกตามกระบวนการหลักๆ 4 ด้าน คือ

1) การวางแผนและการจัดการองค์กร (Planning and Organization; PO) ประกอบด้วย การจัดทำแผนยุทธศาสตร์ การกำหนดโครงสร้างด้านสารสนเทศ การกำหนดทิศทางแนวโน้มของเทคโนโลยี การกำหนดโครงสร้างองค์กร การบริหารการลงทุน การประชาสัมพันธ์เป้าหมายและทิศทาง การจัดการทรัพยากรบุคคลด้านไอที การจัดการคุณภาพการบริหาร การประเมินและบริหารความเสี่ยง และการบริหารโครงการ

2) การจัดหาและการติดตั้งใช้งาน (Acquisition and Implementation; AI) ประกอบด้วย การเลือกใช้ระบบอัตโนมัติ การจัดหาและบำรุงรักษาซอฟต์แวร์ประยุกต์ การจัดหาและบำรุงรักษาโครงสร้างพื้นฐานที่เกี่ยวข้อง การปฏิบัติและใช้งาน การจัดหาทรัพยากร การบริหารความเปลี่ยนแปลง การติดตั้งและการปรับเปลี่ยนความพร้อมของระบบ

3) การส่งมอบและการบริการ (Delivery and Support; DS) ประกอบด้วยการกำหนดและการจัดการระดับการให้บริการ การจัดการการให้บริการบุคคลภายนอก การจัดการที่เกี่ยวกับประสิทธิภาพการให้บริการ การสร้างความต่อเนื่องในการให้บริการ การรักษาความมั่นคงปลอดภัย การกำหนดและจัดสรรต้นทุน การอบรมให้ความรู้ผู้ใช้งาน การสนับสนุนการบริการ การจัดทำการคอนฟิกูเรชัน การจัดการแก้ไขปัญหา การจัดการข้อมูล การจัดการทางกายภาพของทรัพยากร และการจัดการด้านการปฏิบัติการ

4) การเฝ้าติดตามและประเมินผล (Monitor and Evaluate; ME) ประกอบด้วยการเฝ้าติดตามและประเมินกระบวนการใช้งานทรัพยากรสารสนเทศ การเฝ้าติดตามประเมินผลการควบคุมภายในการปฏิบัติตามข้อกำหนดและนโยบาย และการให้บริการตามหลักการธรรมาภิบาล

4. เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย

4.1 เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางกายภาพ เป็นเทคโนโลยีใช้ในสร้างสภาพแวดล้อมทางกายภาพที่เหมาะสมสำหรับการใช้งานคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ โดยเมื่อพิจารณาเหตุการณ์ที่กระทบต่อความมั่นคงปลอดภัยทางกายภาพจะพบว่า เกิดจากสภาพแวดล้อมที่คอมพิวเตอร์หรืออุปกรณ์นั้นๆ ติดตั้งอยู่ เช่น การเข้าถึงอุปกรณ์โดยไม่มีสิทธิ์ อุณหภูมิ ความชื้น และความผิดปกติที่เกี่ยวข้องกับแหล่งจ่ายพลังงานไฟฟ้า อาจแบ่งย่อยๆ ไปหลากหลาย เช่น

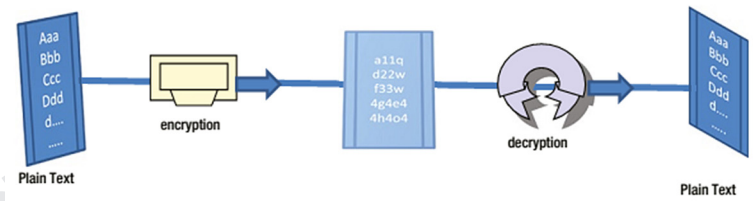
– เทคโนโลยีการป้องกันการเข้าถึงคอมพิวเตอร์หรืออุปกรณ์เชื่อมต่ออื่นๆ ซึ่งมีวัตถุประสงค์ในการป้องกันการทำลาย การขโมย การเข้าใช้งานโดยไม่ได้รับอนุญาต ซึ่งเมื่อเกิดขึ้นย่อมส่งผลต่อการรักษาความลับ ความครบถ้วนสมบูรณ์ และความพร้อมใช้ของอุปกรณ์และสารสนเทศที่ถูกจัดเก็บในอุปกรณ์นั้นๆ

– เทคโนโลยีที่เกี่ยวข้องกับการพิสูจน์ตัวจริง เป็นเทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อพิสูจน์ตัวจริงผู้ใช้ก่อนให้สิทธิ์เข้าใช้งานคอมพิวเตอร์ เช่น เทคโนโลยีการพิสูจน์เอกลักษณ์จากเสียง (voice recognition) เทคโนโลยีการตรวจสอบเอกลักษณ์ลายนิ้วมือ (fingerprint biometric) ดังที่แสดงในภาพที่ 14.9 เป็นต้น

ภาพที่ 14.9 แสดงอุปกรณ์พิสูจน์ตัวจริงด้วยลายนิ้วมือ

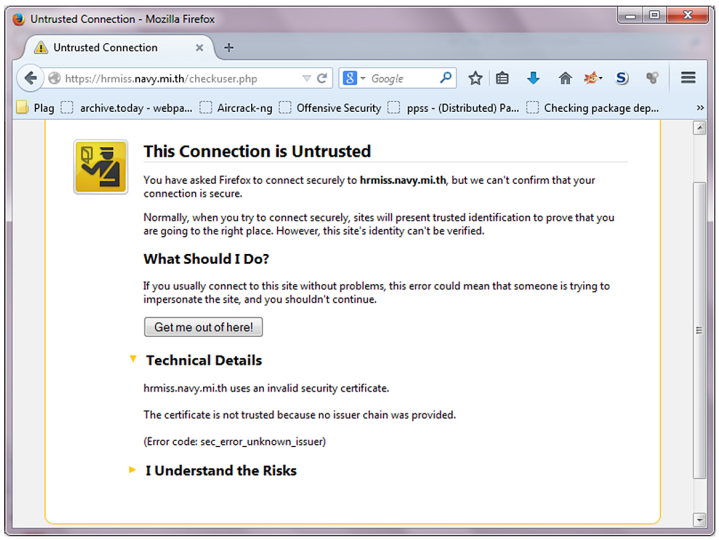
– เทคโนโลยีที่เกี่ยวการสร้างสภาพแวดล้อมที่เหมาะสมอื่นๆ เช่น ระบบสำรองไฟฟ้า ระบบปรับอากาศ เป็นต้น เนื่องจากการใช้งานคอมพิวเตอร์ในห้องที่มีฝุ่น อุณหภูมิสูงหรือมีความชื้นไม่เหมาะสมอาจส่งผลเสียหายต่อวงจรไฟฟ้าได้ เช่น หากมีความชื้นสูงและอุณหภูมิสูงอาจส่งผลให้เกิดการกลั่นตัวของไอน้ำในอากาศซึ่งเป็นสาเหตุที่ทำเกิดการลัดวงจรของแผงวงจรไฟฟ้า

4.2 วิทยาการรหัสลับ (cryptography) เป็นเทคโนโลยีที่ถูกประยุกต์เพื่อตอบสนองต่อภัยคุกคามต่อทรัพยากรสารสนเทศที่เกี่ยวข้องกับการแอบดักรับข้อมูล การแอบแก้ไขข้อมูล และการปลอมแปลงหรือหลอกลวง โดยหลักพื้นฐานของวิทยาการรหัสลับคือ การทำให้ทรัพยากรสารสนเทศที่ผ่านการเข้ารหัสนั้นสามารถเข้าถึงและแปลความหมายได้จากผู้ที่ได้รับสิทธิ์เท่านั้น เช่น การเข้ารหัสข้อความด้วยอัลกอริธึมที่ทำหน้าที่เปลี่ยนแปลงข้อความนั้นเป็นข้อความที่ไม่สามารถอ่านทำความเข้าใจได้โดยปราศจากกุญแจถอดรหัส ดังภาพที่ 14.10 ซึ่งแสดงกระบวนการเข้าและถอดรหัสไฟล์ข้อมูล



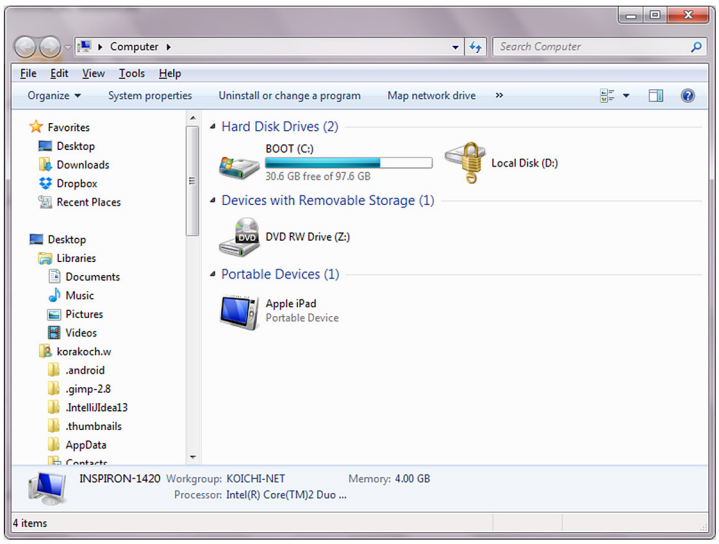
ภาพที่ 14.10 การประยุกต์ใช้งานวิทยาการรหัสลับในการรักษาความลับของข้อมูล

ทั้งนี้ วิทยาการรหัสลับถูกนำมาใช้อย่างกว้างขวาง เช่น การใช้งานโครงสร้างพื้นฐานกุญแจสาธารณะ สำหรับการป้องกันการโจมตีแบบคนกลาง (MITM) ซึ่งจะมีการแจ้งเตือนผู้ใช้งานหากตรวจพบข้อผิดพลาดที่เกี่ยวข้องกับการเข้ารหัส เป็นต้น ดังที่แสดงในภาพที่ 14.11



ภาพที่ 14.11 การแจ้งเตือนผู้ใช้งาน

การจัดเก็บข้อมูลลงบนฮาร์ดดิสก์โดยมีการเข้ารหัสลับ เพื่อป้องกันการเข้าถึงข้อมูลที่เป็นความลับจากผู้ไม่ประสงค์ดี ในกรณีที่เครื่องคอมพิวเตอร์ถูกขโมย หรือเข้าถึงได้ทั้งทางกายภาพหรือถูกบุกรุกทางเครือข่าย ดังแสดงในภาพที่ 14.12 โดยรูปกุญแจที่ไดรฟ์ดีแสดงให้เห็นว่าข้อมูลในไดร์ฟนั้นถูกเข้ารหัสข้อมูลไว้หากผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องคอมพิวเตอร์นี้ได้แต่ไม่สามารถป้อนรหัสที่ถูกต้อง ก็จะไม่สามารถเข้าถึงทรัพยากรที่ถูกจัดเก็บไว้ในนั้นได้ เป็นต้น



ภาพที่ 14.12 การประยุกต์ใช้วิทยาการรหัสลับในการเข้ารหัสข้อมูลบนดิสก์

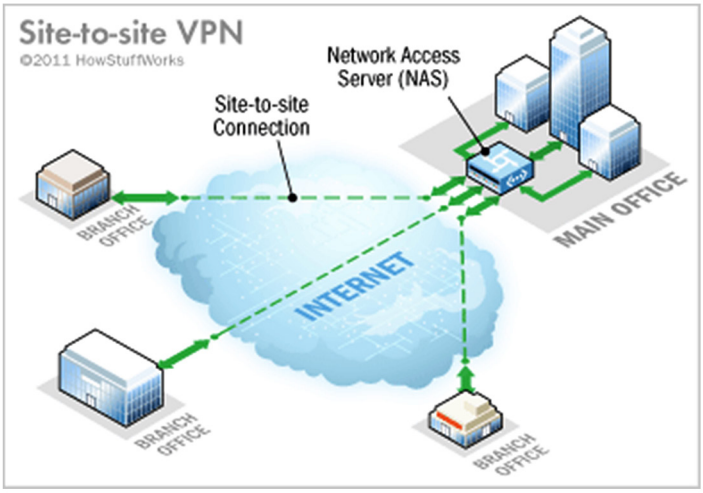
นอกจากนี้วิทยาการรหัสลับยังถูกใช้ในการตรวจสอบความครบถ้วนสมบูรณ์ของทรัพยากรสารสนเทศได้เช่นเดียวกันการตรวจสอบความครอบถ้วนสมบูรณ์ของไฟล์สามารถทำได้ด้วยการประยุกต์ใช้งานแฮชชิ่งอัลกอริธึม เช่น MD5 และ SHA1 เป็นต้น

ไฟร์วอลล์ (firewall) เป็นเทคโนโลยีที่ถูกสร้างขึ้นเพื่อป้องกันภัยคุกคามและการโจมตีทางเครือข่าย หลักทั่วไปของการใช้งานไฟร์วอลล์คือ การป้องกันภัยคุกคามที่มาจากภายนอก (ซึ่งอาจหมายถึงเครือข่ายภายนอก หรือเครือข่ายที่เครื่องคอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งเชื่อมต่อด้วยก็ได้) สามารถจำแนกชนิดของไฟร์วอลล์ตามลักษณะการใช้งานได้สองลักษณะคือ ไฟร์วอลล์สำหรับเครือข่าย (network firewall) และไฟร์วอลล์ส่วนบุคคล (personal firewall) ดังภาพที่ 14.13

ภาพที่ 14.13 ซอฟต์แวร์ไฟร์วอลล์ส่วนบุคคล

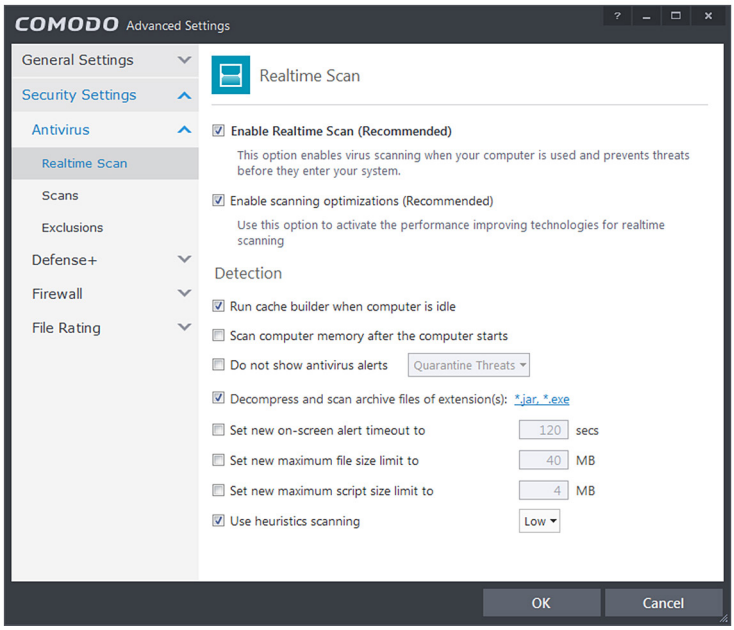
ระบบตรวจจับผู้บุกรุก (intrusion detection system) เป็นเทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อเฝ้าตรวจเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของทรัพยากรสารสนเทศ สามารถวิเคราะห์ข้อมูลทั้งในระดับเครือข่ายและข้อมูลอื่นๆ เพื่อค้นหาเหตุการณ์ที่อาจเป็นการละเมิดนโยบายการรักษาความมั่นคงปลอดภัยที่ถูกกำหนดไว้ โดยมีคุณสมบัติที่สำคัญ เช่น สามารถเฝ้าตรวจและวิเคราะห์เหตุการณ์ที่เกิดขึ้นในระบบ รายงานระดับมาตรฐานความมั่นคงปลอดภัยและติดตามสถานการณ์ การจัดการรายงานสถานการณ์ของทรัพยากรนั้นๆ เป็นต้น ระบบตรวจจับผู้บุกรุกถูกจำแนกประเภทตามลักษณะการใช้งานได้สองลักษณะคือ ระบบตรวจจับผู้บุกรุกสำหรับเครือข่าย (network-based intrusion detection system) และระบบตรวจจับผู้บุกรุกบนโฮสต์ (host-based intrusion detection system)

เครือข่ายเสมือนส่วนตัวหรือวีพีเอ็น (Virtual Private Network; VPN) เป็นเทคโนโลยีที่ถูกพัฒนาขึ้นเพื่อสร้างการเชื่อมต่อเสมือนเครือข่ายส่วนบุคคล จากเทคนิคการสร้างอุโมงค์เสมือนสำหรับการรับส่งข้อมูลระหว่างกันโดยการประยุกต์ใช้วิทยาการรหัสลับในการเข้ารหัสข้อมูลดังกล่าว ทำให้การสื่อสารบนช่องทางสาธารณะอย่างอินเทอร์เน็ต มีความมั่นคงปลอดภัยจากการโจมตีด้วยการดักรับข้อมูลมากยิ่งขึ้น เนื่องจากแม้ผู้ไม่ประสงค์ดีจะสามารถดักรับข้อมูลที่รับส่งระหว่างกันได้ ผู้ไม่ประสงค์ดีก็ยังคงไม่สามารถถอดหรือทำความเข้าใจความหมายของข้อมูลที่ดักรับได้ เทคนิคการใช้งานวีพีเอ็นมีหลายลักษณะ เช่น รีโมตแอคเซสวีพีเอ็น (remote access VPN) ซึ่งเป็นรูปแบบการเชื่อมต่อจากเครือข่ายหลักไปยังอุปกรณ์ต่างๆ และไซต์ทูไซต์วีพีเอ็น (site-to-site VPN) ซึ่งเป็นการเชื่อมต่อกันระหว่างอุปกรณ์วีพีเอ็นสำหรับเชื่อมต่อเครือข่ายหลายๆ เครือข่ายเข้าหากัน เป็นต้น ภาพที่ 14.14 แสดงแนวทางการประยุกต์ใช้งานวีพีเอ็นในการเชื่อมต่อเครือข่ายเฉพาะบริเวณที่อยู่ห่างไกลกันเข้าด้วยกันเป็นเครือข่ายภายในเสมือน



ภาพที่ 14.14 การเชื่อมต่อเครือข่ายอย่างมั่นคงปลอดภัยด้วยเทคโนโลยีวีพีเอ็น

แอนตี้ไวรัสซอฟต์แวร์ (anti-virus software) เป็นซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อค้นหา ป้องกันและกำจัดมัลแวร์หลากหลายประเภท เช่น คอมพิวเตอร์ไวรัส หนอนอินเทอร์เน็ต เป็นต้น ปัจจุบันซอฟต์แวร์ลักษณะดังกล่าวผนวกรวมความสามารถในการตรวจจับมัลแวร์ที่มีความสามารถในการโจรกรรมข้อมูล เช่น โทรจัน คีย์ล็อกเกอร์ และซอฟต์แวร์โฆษณาเข้าด้วยกัน ดังแสดงในภาพที่ 14.15 เป็นต้น



ภาพที่ 14.15 แสดงคุณสมบัติของซอฟต์แวร์กำจัดมัลแวร์

โดยปกติแอนตี้ไวรัสซอฟต์แวร์จะตรวจจับมัลแวร์ต่างๆ โดยการเปรียบเทียบสัญลักษณ์ประจำตัวของมัลแวร์ที่นิยมเรียกกันว่า ซิกเนเจอร์ (signature) ประยุกต์การใช้งานวิทยาการรหัสลับโดยการตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้นกับไฟล์สำคัญๆ ของระบบ

กิจกรรม 14.2.2

1. ในการใช้งานระบบเอทีเอ็มเพื่อทำธุรกรรมกับธนาคารมีกลไกในการพิสูจน์ตัวจริงลักษณะใด
2. การใช้งานวีพีเอ็นสามารถรักษาความลับของข้อมูลที่ส่งผ่านระบบการสื่อสารได้อย่างไร

แนวตอบกิจกรรม 14.2.2

1. การทำธุรกรรมผ่านเอทีเอ็มมีการพิสูจน์ตัวจริงโดยใช้แนวทางที่เรียกว่า two-factor authentication ซึ่งประกอบด้วย
   a. ข้อมูลในบัตรเอทีเอ็ม (something you have)
   b. รหัสผ่าน (something you know)
2. ข้อมูลที่รับ-ส่งในเครือข่ายเสมือนส่วนตัว มีการประยุกต์ใช้งานวิทยาการรหัสลับในการเข้ารหัสข้อมูล

บรรณานุกรม

จตุชัย แพงจันทร์. (2012). *Master in Security* (2nd ed.). นนทบุรี: ไอดีซีฯ.

Charles P., Pfleeger and Shari L. Pfleeger. (2007). *Security in Computing* (4th ed.).

Joseph, Migga Kizza. (2009). *A Guide to Computer Network Security.* London, UK: Springer-Verlag.

Krawetz, Neal. (2007). *Introduction to Network Security.* Massachusetts, USA: Charles River Media.

McCumber, John. (2004). *Assessing and Managing Security Risk in IT System: A Structure Methodology.* Boston, MA, USA: Auerbach Publication.

Solomon, David. (2010). *Elements of Computer Security.* London, UK: Springer-Verlag.

มสธ