บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

การศึกษาครั้งนี้มุ่งศึกษาวิเคราะห์ความรู้และความเข้าใจของบุคลากรใน กองบัญชาการกองทัพไทย เกี่ยวกับพฤติกรรม ความเสี่ยง และความรู้ความเข้าใจ ของบุคลากรในการใช้ระบบงานสารสนเทศ ว่ามีพฤติกรรมความเสี่ยงต่อภัยคุกคามในการใช้ระบบงานสารสนเทศของ กองบัญชาการกองทัพไทย มากน้อยเพียงไร มีความเสี่ยงมากแค่ไหน และไปในทิศทางด้านใด เพื่อนำผลประโยชน์ที่ได้รับสำหรับข้อมูลนี้ ไปจัดการฝึกอบรมเจ้าหน้าที่ในการรักษาความมั่นคงปลอดภัยสารสนเทศ บุคลากร ของ กองบัญชาการกองทัพไทย ต่อไป เพื่อพัฒนาหลักสูตรให้ตรงกับกลุ่มเป้าหมาย และขอบเขตความรู้ ความเข้าใจ ที่บุคลากร ใน กองบัญชาการกองทัพไทย ต้องการรู้เพิ่มเติม และความคิดเห็นต่าง ๆ เพื่อที่เป็นแนวทางให้กับ กองรักษาความปลอดภัยสารสนเทศ ผู้รับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ นำข้อมูลที่ได้ไปศึกษาและอุดช่องโหว่ ด้านบุคลกร ใน กองบัญชาการกองทัพไทย ผู้จัดทำได้รวบรวมทฤษฎีและความรู้ ความเข้าใจในด้านต่าง ๆ เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ รวบรวมข้อมูลจากการศึกษาทฤษฎี ทบทวนวรรณกรรม รวมถึงการค้นคว้าเอกสารทางวิชาการที่เกี่ยวข้องกับงานที่ทำการศึกษาโดยสรุปเป็นหัวข้อต่างๆ ดังนี้

แนวคิดทางทฤษฎีที่เกี่ยวข้อง

1) แนวคิดทฤษฎีเรื่องความรู้ (Knowledge) และความเข้าใจ (Understanding)

2) พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

3) แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองทัพไทย พ.ศ.2553 – 2556

4) ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย พ.ศ. 2547

5) ทฤษฎีความปลอดภัยคอมพิวเตอร์

บทความและงานวิจัยที่เกี่ยวข้อง

1) บทความและงานความมั่นคงปลอดภัยสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อีสเทอร์น

2) บทความภัยคุกคามความมั่นคงระบบสารสนเทศ ของ พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ พ.ศ. 2552

3) ภัยคุกคาม ช่องโหว่ และการโจมตี ของ มหาวิทยาลัยฟาร์อิสเทอร์น

4) ผลงานวิจัยที่เกี่ยวกับพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ ของนักศึกษา สุพรรษา เกษสีแก้ว จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2552

5) ผลงานวิจัยที่เกี่ยวกับ ความรู้ ทัศนคติต่อพฤติกรรมด้านความปลอดภัยของพนักงานอู่ทหารเรือ พระจุลจอมเกล้า กรมอู่ทหารเรือ กรณีศึกษา : ในสายงานฝ่ายผลิต ของนักศึกษา ศิริพงศ์ ศรีสุขกาญจน์ จากมหาวิทยาลัย ธุรกิจบัณฑิตย์ ปีการศึกษา 2553

6) ผลงานวิจัยที่เกี่ยวกับการใช้ประโยชน์และความพึงพอใจต่อระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร กรณีศึกษา : ข้าราชการโรงพยาบาลพระมงกุฎเกล้า ของนักศึกษา วรรณษา บุนนาค จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2554

7) ผลงานวิจัยที่เกี่ยวกับความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์ กรณีศึกษาในเขต กรุงเทพมหานคร ของนักศึกษา นวรัตน์ พัฒโนทัย จาก มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี ปีการศึกษา 2555

8) ผลงานวิจัยที่เกี่ยวกับการวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์การเรียนรู้ ICT ชุมชน กรณีศึกษา ศูนย์การเรียนรู้ ICT ชุมชนตำบลบางเพรียง อำเภอบางบ่อ จังหวัดสมุทรปราการ ของนักศึกษา ปิยะนาถ คล่องดี จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ ปีการศึกษา 2556

2.1 แนวคิดทางทฤษฎีที่เกี่ยวข้อง

ทฤษฎีเรื่องความรู้ (Knowledge) และความเข้าใจ (Understanding)

ความรู้ เป็นการรับรู้เบื้องต้น ซึ่งบุคคลส่วนมากจะได้รับผ่านประสบการณ์ โดยการเรียนรู้จากการตอบสนองต่อสิ่งเร้า (S-R) แล้วจัดระบบเป็นโครงสร้างของความรู้สร้างสรรค์ให้ระหว่างความจำ (ข้อมูล) กับสภาพจิตวิทยา ด้วยเหตุนี้ ความรู้ จึงเป็นความจำเป็นที่สร้างสรรค์ให้สอดคล้องกับสภาพจิตใจของตนเอง ความรู้จึงเป็นกระบวนการภายใน อย่างไรก็ตามความรู้ก็อาจส่งผลต่อพฤติกรรมที่แสดงออกของมนุษย์ได้ (สุรพงษ์ โสธนะเสถียร, 2553, น. 120)

ความรู้เป็นพฤติกรรมเบื้องต้นที่ผู้เรียนสามารถจดจำได้ หรือระลึกได้โดยการมองเห็น หรือได้ยิน ซึ่งความรู้ในที่นี้ คือ ข้อเท็จจริง กฎเกณฑ์ คำจำกัดความ เป็นต้น โดยทั้งนี้ความรู้จึงเป็นพฤติกรรมขั้นต้นที่คนเราเพียงแต่จำได้โดยนึกได้ ความรู้ขั้นนี้ ได้แก่ ความรู้เกี่ยวกับคำจำกัดความ ความหมาย ข้อเท็จจริง กฎโครงสร้าง และวิธีการแก้ปัญหา ดังนั้นอาจกล่าวรวม ๆ ได้ว่า ความรู้หมายถึง การเรียนรู้ที่เน้นความจำและการระลึกถึงได้ของคนเราที่มีความคิด ปรากฏการณ์หรือวัตถุต่าง ๆ ความจำนี้อาจจะเริ่มจากสิ่งที่ง่ายไม่ซับซ้อนไปจนถึงเรื่องยุ่งยากซับซ้อนหลายขั้นได้ (สุตชาติ วงษ์หุ่น, 2539, น. 28)

ความเข้าใจ หมายถึง เป็นขั้นตอนของความรู้ (Knowledge) ขั้นตอนนี้จะต้องใช้ความสามารถทางสมอง และทักษะที่สูงขึ้นจนถึงกับที่สื่อความหมาย ซึ่งมักเกิดขึ้นหลักจากที่บุคคลได้รับข่าวสารต่าง ๆ และความเข้าใจนี้เองจะแสดงออกในรูปของทักษะต่าง ๆ ซึ่งแยกได้เป็น 3 ลักษณะ ดังนี้ (อรรวรรณ ปิลันธน์โอวาท, 2549, น. 40)

1) การแปลความหมาย หมายถึง เป็นการจับใจความให้ถูกต้องเกี่ยวกับสิ่งที่สื่อความหมายหรือภาษาหนึ่งของการสื่อสารไปสู่อีกรูปแบบหนึ่ง

2) การตีความหมาย หมายถึง เป็นการอธิบายความหมายหรือสรุปเรื่องราว โดยการจัดระเบียบใหม่ รวบรวมเรียบเรียงเนื้อหาใหม่

3) การขยายความ เป็นการขยายเนื้อหาที่เหนือไปกว่าขอบเขตที่รู้เป็นการขยายขีดการอ้างอิงหรือแนวโน้มที่เกินเลยจากข้อมูล

Rosenberg and Hovland (1960, p. 4) อธิบายความหมายของ การเข้าใจ ไว้ว่า ความรับรู้ ความนึกคิด และความเชื่อ ตามแนวทัศนคติ ซึ่งสิ่งเหล่านี้สามารถแสดงออกมาได้ โดยคำถามที่อยู่ในรูปการพิมพ์หรือคำพูด เช่น ถ้าผู้ที่สนใจอยากรู้ว่าประชาชนมีความเข้าใจและมีทัศนคติต่อเรื่องใด ๆ ผู้นั้นสามารถสำรวจความคิดเห็นได้ โดยการสัมภาษณ์ หรือกรอกแบบสอบถามได้ เป็นต้น

Bertrang Russell (1926) ได้ให้ความหมายของความรู้ ซึ่งหมายถึง อาจกำหนดไว้ให้เชื่อสิ่งที่อยู่ในข้อตกลงกับข้อเท็จจริง แต่ปัญหาคือการที่ไม่มีใครรู้ในสิ่งที่เชื่อ คือ ไม่มีผู้ใดรู้สิ่งที่เป็นจริงและไม่มีผู้ใดรู้ในสิ่งที่จัดเรียงไว้ตามข้อตกลง

Bloom el al. (1956, PP.28-80) ได้ให้คำนิยามว่า

ความรู้ (Knowledge) เป็นสิ่งที่เกี่ยวข้องกับการระลึกถึงเฉพาะเรื่องหรือเรื่องทั่ว ๆ ไป ระลึกถึงวิธี กระบวนการหรือสถานการณ์ต่าง ๆ โดยเน้นความจำและการเกิดความรู้ไม่ว่าระดับใดย่อมมีความสัมพันธ์กับความรู้สึก ซึ่งส่งผลให้เชื่อมโยงกับสภาพจิตใจของบุคคล โดยปัจจัยที่ทำให้ส่งผลนี้ คือ สภาพแวดล้อม ประสบการณ์ที่สะสม จึงทำให้แสดงออกต่อการกระทำของบุคคล

ความเข้าใจ (Comprehension Or Understand) หมายถึง บุคคลสามารถทำบางสิ่งบางอย่างได้มากกว่าข้อมูลที่ได้รับ สามารถเขียนเรียบเรียงใหม่ พร้อมแสดงความคิดเห็นเพิ่มเติมแปลความเปรียบเทียบความเห็นอื่น ๆ หรือคาดผลของเหตุการณ์ที่จะเกิดได้เป็นพฤติกรรมในขั้นที่ต่อจากความรู้ เป็นขั้นตอนที่สมอง และความสามารถของทักษะ ได้เข้ามาเกี่ยวข้องด้วย จะส่งผลต่อการสื่อสารตีความ แปลความ ขยายความของเหตุเหล่านั้นที่สัมพันธ์กันอีกระดับหนึ่ง โดยความรู้ต้องเกิดจากข้อมูลหรือประสบการณ์ที่เพียงพอ ดังนั้น ความรู้ สามารถกล่าวได้ว่าเป็นการวัดความรู้และความเข้าใจไปด้วยกัน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ในปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ จึงมีผู้ไม่หวังดีเกิดขึ้นอย่างแน่นอน โดยการกระทำใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารทำงานหรือให้ทำงานผิดพลาด ย่อมก่อให้เกิดความเสียหาย กระทบกระเทือนต่อเศรษฐกิจ สังคม และความมั่นคง สมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำดังกล่าว ประเทศไทยจึงมีการออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ขึ้นมาโดยมีบทลงโทษดังนี้

มาตรา 5 ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจาคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 6 ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้ อื่นจัดทาขึ้นเป็นการเฉพาะถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นต้องระวางโทษจาคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 7 ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา 8 ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ตองระวางโทษจาคุกไม่เกินสามปีหรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 9 ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมด หรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาทหรือทั้งจำทั้งปรับ

มาตรา 10 ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจาคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา 11 ผู้ใดส่งข้อมูลคอมพิวเตอร์ หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

มาตรา 12 หากมีการกระทำความผิดตาม มาตรา 9 หรือมาตรา 10

1) ก่อให้เกิดความเสียหายแก่ประชาชนเกิดขึ้นทันทีหรือภายหลัง ต้องระวางโทษปรับไม่เกินสองแสนบาท หรือต้องระวางโทษจำไม่เกิน 10 ปี

2) น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศและเศรษฐกิจ ต้องระวางโทษจำคุกตั้งแต่สามปี ถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

3) ถ้าการกระทำความผิดตาม 2) เป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่สิบปี ถึงยีสิบปีมาตรา 13 ผู้ใดจำหน่ายหรือเผยแพร่ ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 มาตรา 9 มาตรา 10 หรือมาตรา 11 ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 14 ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

1) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน

2) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนักแก่ประชาชน

3) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็น ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4) นำเข้าสู่ ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์ นั้นประชาชนทั่วไปอาจเข้าถึงได้

5) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม 1) 2) 3) หรือ 4)

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14

มาตรา 16 ผู้ใดนำเข้าสู่ ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ถ้าการกระทำตามวรรคหนึ่ง เป็นการนำเข้าข้อมูลคอมพิวเตอร์ โดยสุจริต ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งเป็นความผิดอันยอมความได้ ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

มาตรา 17 ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษหรือ

2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

แผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสาร ของ กองทัพไทย พ.ศ.2553 – 2556

แผนแม่บทการปฏิบัติการต่อเครือข่ายคอมพิวเตอร์ กองทัพไทย เป็นการเริ่มต้นในการกำหนดกรอบ แนวทางในการปฏิบัติ เพื่อให้ทุกส่วนราชการสามารถที่จะแลกเปลี่ยนข้อมูลและปฏิบัติงานด้านการปฏิบัติการต่อเครือข่ายคอมพิวเตอร์ ร่วมกันได้อย่างมีประสิทธิภาพ ซึ่งเป็นไปตามแผนแม่บท การปฏิบัติการต่อเครือข่ายต่อคอมพิวเตอร์ จำเป็นอย่างยิ่งในการทำให้การแลกเปลี่ยนข้อมูลระหว่าง ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีความปลอดภัย และเชื่อถือได้ ดังนั้นจึงมีความจำเป็นที่ต้องอาศัยความร่วมมือจากบุคลากร ในทุกระดับ โดยจะต้องยึดถือและปฏิบัติตาม กฎ ระเบียบ ข้อบังคับ ต่างๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านสารสนเทศ และระเบียบอื่นๆ ที่เกี่ยวข้อง อย่างเคร่งครัด

จุดมุ่งหมายของแผนแม่บทเพื่อให้ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ กองทัพอากาศ ยึดถือเป็นแนวทางในการปฏิบัติต่อเครือข่ายคอมพิวเตอร์ ตามหลักนิยมการปฏิบัติการข่าวสาร กองทัพไทย

วัตถุประสงค์ เพื่อให้ข้าราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีจิตสำนึกในการรักษาความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้ส่วนราชการ บก.กองทัพไทย กองทัพบก กองทัพเรือ และกองทัพอากาศ มีแนวทางในการดำเนินงานเกี่ยวกับการปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่เป็นรูปธรรมและสามารถวัดผลการปฏิบัติได้ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ ของ ส่วนราชการ บก.กองทัพไทย กองทัพบกกองทัพเรือ และกองทัพอากาศ มีความปลอดภัยจากภัยคุกคาม สามารถปฏิบัติงานตลอดเวลารวมทั้งสนับสนุนการปฏิบัติการทางทหารได้อย่างมีประสิทธิภาพ

ระเบียบ กองบัญชาการทหารสูงสุด ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ กองทัพไทย พ.ศ.2547

ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศ ของกองบัญชาการทหารสูงสุด และเหล่าทัพ

ความมุ่งหมายของระเบียบนี้ เพื่อกำหนดหลักการและมาตรการในการรักษาความปลอดภัยระบบสารสนเทศ ของกองทัพไทย พิทักษ์รักษาและป้องกัน มิให้ข้อมูลและสิ่งที่เป็นความลับของทางราชการ รั่วไหลหรือรู้ไปถึง หรือตกไปอยู่ในมือของฝ่ายตรงข้ามหรือบุคคลผู้ไม่มีอำนาจหน้าที่ป้องกันการจารกรรมทั้งจากบุคคลภายในและภายนอกส่วนราชการ พิทักษ์รักษาและป้องกันการก่อวินาศกรรม แก่ เครื่องจักรคำนวณ อุปกรณ์ เครื่องใช้ อาคาร สถานที่ และเอกสาร เป็นต้น หัวหน้าส่วนราชการสามารถกำหนดมาตรการรักษาความปลอดภัยให้ระบบสารสนเทศของส่วนราชการ และแต่งตั้งเจ้าหน้าที่ควบคุมการรักษาความปลอดภัยระบบสารสนเทศ ของ ส่วนราชการเพิ่มเติมได้โดยให้สอดคล้อง และไม่ขัด หรือ แย้งกับระเบียบนี้

เหตุผลในการประกาศใช้ระเบียบนี้ คือ วางระเบียบ กองบัญชาการทหารสูงสุด ในการรักษาความปลอดภัยระบบสารสนเทศของกองทัพไทย เกี่ยวกับระบบคอมพิวเตอร์ ระบบสื่อสาร สารสนเทศเครือข่ายระบบสารสนเทศ เพื่อให้ใช้บังคับแก่ส่วนราชการ ข้าราชการ และลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมทั้งบุคคลภายนอก ที่เข้ามาดำเนินการ เกี่ยวกับระบบสารสนเทศ ของ กองบัญชาการทหารสูงสุด และเหล่าทัพ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตาม พรบ. ข้อมูลข่าวสาร ของ ทางราชการ พ.ศ.๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ หรืออื่น ๆ ที่ได้ประกาศใช้ทดแทน

1) การรักษาความปลอดภัยเกี่ยวกับบุคคล

2) การรักษาความปลอดภัย สถานที่

3) การรักษาความปลอดภัยระบบสารสนเทศ

4) การรักษาความปลอดภัยในการพัฒนาระบบสารสนเทศ

5) การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยระบบสารสนเทศ

ทฤษฎีความมั่นคงปลอดภัยสารสนเทศ

สารสนเทศ (information) เป็นผลลัพธ์ของการประมวลผล การจัดดำเนินการ และการเข้าประเภทข้อมูลโดยการรวมความรู้เข้าไปต่อผู้รับสารสนเทศนั้น สารสนเทศ มีความหมายหรือแนวคิดที่กว้าง และหลากหลาย ตั้งแต่การใช้คำว่าสารสนเทศ ในชีวิตประจำวัน จนถึงความหมายเชิงเทคนิค ตามปกติในภาษาพูด แนวคิดของสารสนเทศใกล้เคียงกับความหมายของการสื่อสาร

ความมั่นคงปลอดภัยของสารสนเทศคืออะไร

1) ความมั่นคงปลอดภัย (Security) คือ สถานะที่มีความปลอดภัย ไร้กังวลอยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตรายทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ

2) การรักษาความปลอดภัยทางข้อมูล Information Security คือ ผลที่เกิดขึ้นจากการใช้ระบบของนโยบายและ/หรือ ระเบียบปฏิบัติที่ใช้ในการพิสูจน์ทราบ ควบคุม และป้องกันการเปิดเผยข้อมูล (ที่ได้รับคำสั่งให้มีการป้องกัน) โดยไม่ได้รับอนุญาต : นิยามโดย ThaiCERT (ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย)

2.2 บทความและงานวิจัยที่เกี่ยวข้อง

บทความและงานความมั่นคงปลอดภัยสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อีสเทอร์น

ความมั่นคงปลอดภัยขององค์กร

1) ความมั่นคงปลอดภัยทางกายภาย Physical Security

2) ความมั่นคงปลอดภัยส่วนบุคคล Personal Security

3) ความมั่นคงปลอดภัยในการปฏิบัติงาน Operations Security

4) ความมั่นคงปลอดภัยในการติดต่อสื่อสาร Communication Security

5) ความมั่นคงปลอดภัยของเครือข่าย Network Security

6) ความมั่นคงปลอดภัยของสารสนเทศ Information Security

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้นประกอบด้วย

1) ความลับ Confidentiality

2) ความสมบูรณ์ Integrity

3) ความพร้อมใช้ Availability

4) ความถูกต้องแม่นยำ Accuracy

5) เป็นของแท้ Authenticity

6) ความเป็นส่วนตัว Privacy

ความลับ Confidentiality เป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น การจัดประเภทของสารสนเทศ การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล กำหนดนโยบายรักษาความมั่นคงปลอดภัย และนำไปใช้ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้ ภัยคุกคามที่เพิ่มมากขึ้นในปัจจุบัน มีสาเหตุมาจากความก้าวหน้าทางเทคโนโลยี ประกอบกับความต้องการความสะดวกสบายในการสั่งซื้อสินค้าของลูกค้า โดยการยอมให้สารสนเทศส่วนบุคคลแก่ website เพื่อสิทธิ์สนการทำธุรกรรมต่าง ๆ โดยลืมไปว่าเว็บไซต์ เป็นแหล่งข้อมูลที่สามารถขโมยสารสนเทศไปได้ไม่ยากนัก

ความสมบูรณ์ Integrity ความสมบูรณ์ คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลกปลอม สารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องครบถ้วน สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ เพื่อขัดขวางการพิสูจน์การเป็นสารสนเทศจริง

ความพร้อมใช้ Availability ความพร้อมใช้ หมายถึง สารสนเทศจะถูกเข้าถึงหรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้หรือระบบอื่นที่ได้รับอนุญาตเท่านั้นหากเป็นผู้ใช้หรือระบบที่ไม่ได้รับอนุญาต การเข้าถึงหรือเรียกใช้งานจะถูกขัดขวางและล้มเหลวในที่สุด

ความถูกต้องแม่นยำ Accuracy หมายถึง สารสนเทศต้องไม่มีความผิดพลาด และต้องมีค่าตรงกับความคาดหวังของผู้ใช้เสมอ เมื่อใดก็ตามที่สารสนเทศมีค่าผิดเพี้ยนไปจากความคาดหวังของผู้ใช้ ไม่ว่าจะเกิดจากการแก้ไขด้วยความตั้งใจหรือไม่ก็ตาม เมื่อนั้นจะถือว่าสารสนเทศ “ไม่มีความถูกต้องแม่นยำ”

ความเป็นของแท้ Authenticity คือ สารสนเทศที่ถูกจัดทำขึ้นจากแหล่งที่ถูกต้อง ไม่ถูกทำซ้ำโดยแหล่งอื่นที่ไม่ได้รับอนุญาต หรือแหล่งที่ไม่คุ้นเคยและไม่เคยทราบมาก่อน

ความเป็นส่วนตัว Privacy คือ สารสนเทศที่ถูกรวบรวม เรียกใช้ และจัดเก็บโดยองค์กรจะต้องถูกใช้ในวัตถุประสงค์ที่ผู้เป็นเข้าของสารสนเทศรับทราบ ณ ขณะที่มีการรวบรวมสารสนเทศนั้นมิฉะนั้นจะถือว่าเป็นการละเมิดสิทธิส่วนบุคคลด้านสารสนเทศ

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

1) Software ย่อมต้องอยู่ภายใต้เงื่อนไขของการบริหารโครงการ ภายใต้เวลา ต้นทุน และกำลังคนที่จำกัด ซึ่งมักจะทำภายหลังจากการพัฒนาซอฟต์แวร์เสร็จแล้ว

2) Hardware จะใช้นโยบายเดียวกับสินทรัพย์ที่จับต้องได้ขององค์กร คือการป้องกันจากการลักขโมยหรือภัยอันตรายต่าง ๆ รวมถึงการจัดสถานที่ที่ปลอดภัยให้กับอุปกรณ์หรือฮาร์ดแวร์

3) Data ข้อมูล/สารสนเทศ เป็นทรัพยากรที่มีค่าขององค์กร การป้องกันที่แน่นหนาก็มีความจำเป็นสำหรับข้อมูลที่เป็นความลับ ซึ่งต้องอาศัยนโยบายความปลอดภัยและกลไกป้องกันที่ดีควบคู่กัน

4) People บุคลากร คือภัยคุกคามต่อสารสนเทศที่ถูกมองข้ามมากที่สุด โดยเฉพาะบุคลากรที่ไม่มีจรรยาบรรณในอาชีพ ก็เป็นจุดอ่อนต่อการโจมตีได้ จึงได้มีการศึกษากันอย่างจริงจังเรียกว่า Social Engineering ซึ่งเป็นการป้องการการหลอกหลวงบุคลากร เพื่อเปิดเผยข้อมูลบางอย่างเข้าสู่ระบบได้

5) Procedure ขั้นตอนการทำงาน เป็นอีกหนึ่งองค์ประกอบที่ถูกมองข้าม หากมิจฉาชีพทราบขั้นตอนการทำงาน ก็จะสามารถค้นหาจุดอ่อนเพื่อนกระทำการอันก่อนให้เกิดความเสียหายต่อองค์กรและลูกค้าขององค์กรได้

6) Network เครือข่ายคอมพิวเตอร์ การเชื่อมต่อระหว่างคอมพิวเตอร์และระหว่างเครือข่ายคอมพิวเตอร์ ทำให้เกิดอาชญากรรมและภัยคุกคามคอมพิวเตอร์ โดยเฉพาะการเชื่อมต่อระบบสารสนเทศเข้ากับเครือข่ายอินเตอร์เน็ต

อุปสรรคของงานความมั่นคงปลอดภัยของสารสนเทศ

1) ความมั่นคงปลอดภัย คือ ความไม่สะดวก เนื่องจากต้องเสียเวลาในการป้อน password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวผู้ใช้

2) มีความซับซ้อนบางอย่างในคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Registry , Port, Service ที่เหล่านี้จะทราบในแวดวงของ Programmer หรือผู้ดูแลระบบ

3) ผู้ใช้คอมไม่ระแวดระวัง

4) การพัฒนาซอฟต์แวร์ไม่คำนึงถึงความปลอดภัยภายหลัง

5) แนวโน้มเทคโนโลยีสารสนเทศคือการแบ่งปัน ไม่ใช่ การป้องกัน

6) มีการเข้าถึงข้อมูลได้จากทุกสถานที่

7) ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟแวร์และฮาร์ดแวร์เพียงอย่างเดียว

8) มิจฉาชีพมีความเชี่ยวชาญ (ในการเจาะข้อมูลของผู้อื่นมากเป็นพิเศษ)

9) ฝ่ายบริหารมักจะไม่ให้ความสำคัญแก่ความมั่นคงปลอดภัย

บทความภัยคุกคามความมั่นคงระบบสารสนเทศ ของ พ.อ.รศ.ดร.เศรษฐพงค์ มะลิสุวรรณ

ประมาณ 500 ปี ก่อนคริตศักราช ชาวจีนชื่อ ซัน ซุน วู ได้เขียนเรื่อง Art of war ให้ความสำคัญกับการรู้จักตัวเองรวมถึงภัยคุกคามที่ต้องเผชิญ เพื่อจะได้รู้ว่าควรปกป้องข้อมูลขององค์กรอย่างไร สิ่งที่ควรรู้ คือ

1) รู้จักตัวเอง คือ รู้จักการปกป้องข้อมูลและระบบให้มีความมั่นคง ระบบขนส่ง และขั้นตอนต่างๆ

2) การรู้ถึงภัยคุกคามที่ต้องเผชิญ ศึกษาจากแหล่งข้อมูลที่น่าเชื่อถือทำให้สามารถตัดสินใจจัดการกับภัยคุกคามต่างๆที่มีผลกับ พนักงาน โปรแกรม ข้อมูล และระบบสารสนเทศขององค์กร การรักษาความปลอดภัยข้อมูล กล่าวถึงอันตรายจากภัยคุกคามที่ส่งผลกับคน และทรัพย์สิน

มีการสำรวจประเภทของภัยคุกคาม เมื่อการเชื่อมต่ออินเตอร์เน็ตขยายไปทั่วโลก ศึกษาถึงแนวทางปฏิบัติในการป้องกันภัยคุกคามต่างๆ มีการสำรวจเปรียบเทียบประเภทของภัยคุกคามทำให้เกิดความเข้าใจร่วมกันว่าภัยคุกคามที่เพิ่มขึ้นมาจากการที่องค์กรเชื่อมต่ออินเตอร์เน็ต โดยจำนวนผู้ใช้อินเตอร์เน็ตเพิ่มขึ้นเรื่อยๆ คิดเป็น 17% ของคนทั้งโลก หรือ จากคนทั่วโลก 6.6 พันล้านคน มีคนที่เข้าใช้งานอินเตอร์เน็ตถึง 1.1 พันล้านคน

ข้อผิดพลาดจากการกระทำของมนุษย์ (Acts of human error or failure) ประเภทนี้มีการกระทำโดยเจตนา หรือ มีเจตนามุ่งร้ายโดยผู้ใช้ที่มีสิทธิเข้าใช้ระบบ เมื่อผู้ใช้ระบบทำงานผิดพลาด เนื่องจากขาดความชำนาญ ขาดการฝึกอบรม และการสันนิษฐานไม่ถูกต้อง สิ่งเล็กน้อยเหล่านี้สามารถสร้างความเสียหายอย่างมากการคุกคามที่อันตรายที่สุดต่อความปลอดภัยของข้อมูลองค์กร คือ พนักงานขององค์กรเองเพราะพนักงานใช้ข้อมูลในการดำเนินกิจกรรมทางธุรกิจขององค์กรทุกวัน สิ่งที่พนักงานจะต้องปฏิบัติอย่างเคร่งครัดคือ การรักษาความลับของข้อมูล ข้อมูลมีความถูกต้องครบถ้วน และข้อมูลพร้อมใช้งานได้ทุกเมื่อ รูปต่อไปเป็นการแนะนำเกี่ยวกับการคุกคามจาภายนอก เพราะความผิดพลาดเพียงเล็กน้อยของพนักงาน เช่น ไม่ได้ปิดประตูหน้าต่างทำให้หัวขโมยเข้ามาในองค์กรได้ การลบหรือแก้ไขข้อมูลที่เป็นเอกสารสำคัญ

นโยบายและกลยุทธ์ด้านเทคโนโลยีสารสนเทศ เพื่อสนับสนุนข้อมูลสารสนเทศ ซึ่งการโจมตีระบบข้อมูลสารสนเทศเป็นเหตุการณ์ที่เกิดขึ้นเป็นประจำทุกวัน และต้องการการรักษาความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มมากขึ้นพร้อมกับการโจมตีที่มีความซับซ้อนมากขึ้น ดังนั้นองค์กรต้องเข้าใจในสิ่งแวดล้อมของการทำงานของระบบข้อมูลสารสนเทศ และกลยุทธ์ป้องกันภัยข้อมูลสารสนเทศจึงจะสามารถจัดการปัญหาต่างๆ ได้ ซึ่งเป็นต้นเหตุที่เกิดขึ้นกับข้อมูลสารสนเทศในองค์กร

ภัยคุกคาม ช่องโหว่ และการโจมตี ของ มหาวิทยาลัยฟาร์อิสเทอร์น

ภัยคุกคาม ช่องโหว่ และการโจมตี

1) ภัยคุกคาม

2) ช่องโหว่

3) การโจมตี

4) มัลแวร์

ภัยคุกคาม Threat คือ วัตถุ สิ่งของ ตัวบุคคล หรือสิ่งอื่นใดที่เป็นตัวแทนของการะทำอันตรายต่อทรัพย์สิน ภัยคุกคามมีหลายกลุ่ม เช่น ภัยคุกคามที่เกิดขึ้นโดยเจตนา หรือบางกลุ่มเป็นภัยคุกคามที่เกิดขึ้นโดยไม่ได้เจตนา เช่ยภัยคุกคามจากธรรมชาติ หรือจากผู้ใช้ในองค์กรเอง ภัยคุกคามที่สามารถทำลายช่องโหว่ ได้เท่านั้น จึงจะสามารถสร้างความเสียหายแก่ระบบได้ และจัดว่าภัยคุกคามนั้นเป็นความเสี่ยง Risk ที่อาจสร้างความเสียหายแก่สารสนเทศได้

ตารางที่ 2.1 ตารางสรุปประเภทของภัยคุกคาม

ประเภทของภัยคุกคาม	ตัวอย่างภัยคุกคาม
1) การทำลายหรือทำให้เสียหาย Subotage or Vandalism	1) การทำลายระบบหรือสารสนเทศ
2) การลักขโมย Theft	2) การลักขโมยหรือการโจรกรรมอุปกรณ์คอมพิวเตอร์หรือสารสนเทศ
3) ซอฟต์แวร์โจมตี Software Attack	3) ไวรัส เวิร์ม มาโคร Dos
4) ภัยธรรมชาติ Force of Nature	4) น้ำท่วม ไฟไหม้ แผ่นดินไหว ไฟดับ

ตารางที่ 2.1 (ต่อ)

ประเภทของภัยคุกคาม	ตัวอย่างภัยคุกคาม
5) คุณธรรมของการบริการที่เบี่ยงเบนไป Deviation in Quality of Service	5) ISP, WAN, Service, Provider
6) ความผิดพลาดทางด้านเทคนิคฮาร์แวร์ Hardware	6) อุปกรณ์ทำงานผิดพลาด
7) ความผิดพลาดทางด้านเทคนิคซอฟต์แวร์ Technical Hardware Failures/Error	7) Bugs, ปัญหาของโค๊ด ลูปไม่รู้จบ
8) ความล้าสมัยของเทคโนโลยี Technological Obsolescence	8) เทคโนโลยีที่ใช้บางอย่างล้าสมัยไปแล้ว

ความผิดพลาดที่เกิดจากบุคคล Human Error/Failures

1) เป็นความผิดพลาดที่เกิดจากพนักงานหรือบุคคลที่ได้รับอนุญาตให้เข้าถึงสารสนเทศขององค์กรได้

2) อาจเกิดจากความไม่ได้ตั้งใจ เนื่องจากไม่มีประสบการณ์ หรือขาดการฝึกอบรม หรือคาดเดา เป็นต้น

3) ป้องกันภัยคุกคาม โดยการให้ความรู้ด้านความมั่นคงปลอดภัยของสารสนเทศ การฝึกอบรมอย่างสม่ำเสมอ

4) มีมาตรการควบคุม

ภัยร้ายต่อทรัพย์สินทางปัญญา Comromises to Intellectual Property

1) ทรัพย์สินทางปัญญา Intellectual Property คือทรัพย์สินที่จับต้องไม่ได้ ที่ถูกสร้างขึ้นมาโดยบุคคลหรือองค์กรใด ๆ หากต้องการนำทรัพย์สินทางปัญญาของผู้อื่นไปใช้ อาจต้องเสียค่าใช้จ่าย และจะต้องระบุแหล่งที่มาของทรัพย์สินดังกล่าวไว้อย่างชัดเจน

2) ในทางกฎหมาย การให้สิทธิในความเป็นเจ้าของทรัพย์สินทางปัญญา มี 4 ประเภทคือ ลิขสิทธิ์ (copyrights) ความลับทางการค้า (Trade Secrets) เครื่องหมายการค้า (Trade Marks) สิทธิบัตร (Patents)

3) การละเมิดความคุ้มครองทรัพย์สินทางปัญญาที่มากที่สุดคือ การละเมิดลิขสิทธิ์ซอฟต์แวร์

การจารกรรมหรือการรุกล้ำ Espionage or Trespass

1) การจารกรรมหรือการรุกล้ำ (Espionage or Trespass) การจารกรรม Espionage เป็นการที่กระทำซึ่งใช้อุปกรณ์อิเลคทรอนิกส์ หรือตัวบุคคลในการจารกรรมสารสนเทศที่เป็นความลับ

2) ผู้จารกรรมจะใช้วิธีการต่าง ๆ เพื่อให้ถึงซึ่งสารสนเทศที่จัดเก็บไว้ และรวมรวมสารสนเทศนั้น โดยไม่ได้รับอนุญาต

3) Industrial Espionage วิธีนี้เป็นการใช้เทคนิคที่ถูกกฎหมายแต่ก้ำกึ่งความไม่ชอบธรรม เพื่อรวบรวมสารสนเทศที่สำคัญหรือความลับทางการค้าของคู่แข่งเพื่อนำมาหาผลประโยชน์

4) Shoulder Surfing คือการแอบดูข้อมูลส่วนตัวของผู้อื่นขณะทำธุรกรรมผ่านตู้ ATM

5) การรุกล้ำ Trespass คือ การกระทำที่ทำให้ผู้อื่นสามารถเข้าสู่ระบบเพื่อรวมรวมสารสนเทศที่ต้องการ โดยไม่ได้รับอนุญาต

ประเภทของ Espionage และ Trespass

1) Hacker บุคคลผู้ซึ่งสร้างซอฟต์แวร์คอมพิวเตอร์ขึ้นมา เพื่อให้ตนสามารถเข้าถึงสารสนเทศของผู้อื่นอย่างผิดกฎหมาย

แบ่งออกได้เป็น 2 ประเภท

Expert Hacker เป็นแฮคเกอร์ที่มีทักษะสูง ทำการพัฒนาโปรแกรมขนาดเล็กหรือซอฟต์แวร์สคริปต์ที่ใช้ในการเข้าถึงสารสนเทศในระบบของผู้อื่น ให้พวก Unskilled Hacker ใช้

Unskill Hacker คือ พวกแฮคเกอร์ที่มีทักษะน้อย ไม่สามารถสร้างโปรแกรมเจาะระบบได้เอง จึงเป็นผู้นำโปรแกรมไปเจาะระบบ หรือเข้าถึงสารสนเทศของผู้อื่น

2) Script Kiddies คือ แฮคเกอร์มือใหม่ ที่ไม่มีความชำนาญ เป็นผู้นำ ซอฟต์แวร์ของ Expert Hacker มาใช้ในการโจมตีหรือก่อกวนระบบของผู้อื่น

3) Packet Monkeys คือ script Kiddies ที่ใช้โปรแกรมอัตโนมัติโจมตีระบบแบบปฏิเสธการให้บริการ Distributed Denial of Service ทำให้ระบบไม่สามารถให้บริการทำตามคำร้องขอที่ส่งมาได้ ซึ่งอาจทำให้ผู้ใช้เข้าใจว่าระบบล้มเหลว

4) Cracker คือผู้ที่ทำลายหรือทำซ้ำซอฟต์แวร์รักษาความมั่นคงปลอดภัยของระบบอื่น

ความแตกต่างระหว่าง Hacker / Cracker

Hacker มีเป้าหมายเพื่อทดสอบความสามารถหรือต้องการท้าท้ายโดยการเจาะระบบให้สำเร็จ

Cracker มีจุดประสงค์คือ ต้องการทำลายระบบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์หรือระบบสารสนเทศ

5) Phreaker คือ ผู้เจาะระบบเครือข่ายโทรศัพท์สาธารณะ เพื่อให้ตนเองใช้โทรศัพท์โดยไม่เสียค่าใช้จ่าย หรือเพื่อรบกวนสัญญาณโทรศัพท์

การกรรโชกสารสนเทศInformation Extortion คือ การที่มีผู้ขโมยข้อมูลหรือ สารสนเทศที่เป็นความลับจากคอมพิวเตอร์ แล้วต้องการเงินเป็นค่าตอบแทน เพื่อแลกกับการคืนสารสนเทศนั้นหรือแลกกับการไม่เปิดเผยสารสนเทศดังกล่าว เรียกว่า Blackmail

การทำลายหรือทำให้เสียหาย

1) เป็นการทำลายหรือก่อให้เกิดความเสียหายต่อระบบคอมพิวเตอร์เว็บไซต์ ภาพลักษณ์ ธุรกิจ และทรัพย์สินขององค์กร ซึ่งอาจเกิดจากผู้อื่นที่ไม่หวังดี หรือแม้กระทั่งจากพนักงานขององค์กรเอง

2) การทำลายเช่น การขีดเขียนทำลายหน้าเว็บไซต์

3) ภัยคุกคามประเภทนี้เรียกว่า ปฏิบัติการ Hacktivist หรือ Cyberactivist เป็นปฏิบัติการที่แซกแทรง หรือสร้างความสับสนให้กับระบบการทำงานบางอย่างในองค์กร เพื่อคัดค้านการดำเนินงาน นโยบาย หรือกิจกรรมบางอย่างขององค์กร หรือหน่วยงานของรัฐ

4) การก่อการร้ายบนโลกไซเบอร์ Cyberterrorism เป็นภัยคุกคามอีกรูปแบบหนึ่ง เป็นการก่อการร้ายผ่านระบบเครือข่ายหรือระบบอินเตอร์เน็ต

5) FBI ได้ให้นิยามของ Cybertierriorsm ว่า เป็นการโจมตีแบบไตร่ตรองไว้ก่อนต่อสารสนเทศ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ และข้อมูลซึ่งจะก่อให้เกิดความรุนแรงหรือทำลายเป้าหมาย โดยกลุ่มบุคคล หรือตัวแทนที่ไม่เปิดเผยนาม ที่มีเหตุจูงใจจากประเด็นการเมือง

การลักขโมย Theif คือการถือเอาของผู้อื่นโดยผิดกฎหมาย เช่นอุปกรณ์ต่าง ๆ ทั้งแบบธรรมดาและแบบอิเล็คทรอนิค แล้ว ยังรวมถึง สารสนเทศขององค์กร และทรัพย์สินทางปัญญาอื่น ๆ

ซอฟต์แวร์โจมตี Software Attack

1) เรียกว่า การโจมตีโดยซอฟต์แวร์ เกิดจากบุคคลหรือกลุ่มบุคคลออกแบบซอฟต์แวร์ให้ทำหน้าที่โจมตีระบบ เรียกว่า Malicious Code หรือ Malicious Software หรือ Malware

2) มัลแวร์ Malware ถูกออกแบบเพื่อสร้างความเสียหาย ทำลาย หรือระงับ การให้บริการของระบบเป้าหมาย มีหลายชนิด เช่น virus worm, Zombie, Trojan Horse, Logic Bomb, Back door เป็นต้น

ภัยธรรมชาติ Force of Nature

ภัยธรรมชาติต่าง ๆ สามารถสร้างความเสียหายให้กับสารสนเทศขององค์กรได้ หากไม่มีการป้องกันหรือวางแผนรับมือกับภัยธรรมชาติ อาจก่อให้เกิดความเสียหายแก่องค์กรได้อย่างมหาศาล สามารถป้องกันหรือจำกัดความเสียหาย โดยการวางแผนรับสถานการณ์ฉุกเฉินและภัยพิบัติ Contingency Plan

คุณภาพของการบริการที่เบี่ยงเบนไป Deviations in Quality of Service

เกิดขึ้นจากการที่องค์กรรับมาเพื่อการทำงานของระบบสารสนเทศไม่เป็นไปตามความคาดหวัง ซึ่งอาจเกิดจากความผิดพลาดของการให้บริการ ที่อาจจะเกี่ยวเนื่องจากอุปกรณ์ในระบบให้บริการผิดพลาด อาจกล่าวได้ว่า เป็นภัยคุกคามต่อความพร้อมใช้ Availability Disruption

ความผิดพลาดทางเทคนิคฮาร์แวร์ (Technical Hardware Failure / Error)

เกิดขึ้นเมื่อผู้ผลิตปล่อยฮาร์ดแวร์ที่มีข้อบกพร่องออกสู่ตลาด ทำให้องค์กรได้ฮาร์ดแวร์ดังกล่าวมา ได้รับผลกระทบจากการทำงานที่บกพร่องของฮาร์ดแวร์ อาจทำให้ระบบงานหยุดชะงักไม่สามารถให้บริการแก่ลูกค้าได้ องค์กรอาจสูญเสียยอดการสั่งซื้อ และที่สำคัญความน่าเชื่อถือในที่สุด

ความผิดพลาดทางเทคนิคด้านซอฟต์แวร์ Technical Software Failures/Error

เกิดจากองค์ซื้อ ซอฟต์แวร์ โดยไม่รู้ว่า ซอฟต์แวร์นั้นมีความผิดพลาด ซึ่งก็สามารถสร้างความเสียหายแก่องค์กร เช่นเดียวกันกับความผิดพลาดทางเทคนิคด้านฮาร์ดแวร์ เช่น ความผิดพลาดที่พบส่วนใหญ่ คือ Bug ในซอฟต์แวร์

ความล้าสมัยของเทคโนโลยี Technical Obsolescence

เทคโนโลยีพื้นฐานของคอมพิวเตอร์ หรือระบบสารสนเทศ ล้าสมัยจะส่งผลให้ระบบไม่น่าไว้ใจ และอาจเกิดความเสี่ยงต่อการรักษาความมั่นคงของสารสนเทศ เนื่องจากอาจถูกโจมตีได้โดยง่ายด้วยเทคโนโลยีที่ทันสมัยกว่า

ช่องโหว่

ช่องโหว่ Vulnerabilities หรือ ความล่อแหลม ซึ่งหมายถึง ความอ่อนแอของระบบคอมพิวเตอร์ หรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงสารสนเทศในระบบได้ ซึ่งจะนำไปสู่ความเสียหายแก่สารสนเทศ หรือแม้แต่การทำงานของระบบ

การถูกโจมตี

การโจมตี Attack คือการกระทำบางอย่างที่อาศัยความได้เปรียบจากช่องโหว่ของระบบ เพื่อเข้าควบคุมการทำงานของระบบ เพื่อให้ระบบเกิดความเสียหาย หรือเพื่อโจรกรรมสารสนเทศ

รูปแบบการโจมตีของ Malicious Code

1) สแกนหมายเลข IP Adress เพื่อหาหมายเลขช่องโหว่ แล้วทำการติดตั้ง Back door

2) ท่องเว็บไซต์ ระบบที่มี Malicious ฝังตัวอยู่ จะสร้างเว็บเพจชนิดต่าง ๆ เมื่อผู้ใช้เข้าได้เยี่ยมชมเว็บเพจที่มีอันตรายดังกล่าว ก็จะได้รับ Malicious Code ไปได้

3) Virus คัดลอกตัวเองไปอยู่กับโปรแกรม ที่ผู้ใช้รันโปรแกรมนั้นๆ

4) Email ส่งอีเมล์ที่มี Malicious Code ซึ่งทันทีที่เปิดเมลอ่าน Malicious Code ก็จะทำงานทันที

รูปแบบการโจมตี

เครื่องมือที่ใช้โจมตี แบบ Distributed Denial of Service (DDoS) DDoS มีใช้กันอย่างแพร่หลายมานานหลายปีแล้วย้อนหลังเป็น 10 ปี มาแล้ว (แต่บรรดาผู้ผลิตอุปกรณ์คอมพิวเตอร์ต่างก็มีวิธีป้องกันการโจมตีเช่นเดียวกัน)

รูปแบบการโจมตีที่นิยมใช้กันก็มีอย่าง SYN flood, UDP flood, ICMP flood, Smurf, Fraggle เป็นต้น

การโจมตีแบบ SYN Flood เป็นการโจมตีโดยการส่ง แพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ (ผู้โจมตีสามารถปลอมไอพีของ source address ได้) เครื่องที่เป็นเป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมายัง source IP address ที่ระบุไว้ ซึ่งผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source IP address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ขึ้นที่เครื่องเป้าหมาย หากมีการส่ง SYN flood จำนวนมาก ก็จะทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้ นอกจากนี้ SYN flood ที่ส่งไปจำนวนมาก ยังอาจจะทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่อีกด้วย

การโจมตีแบบ ICMP Flood เป็นการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

การโจมตีแบบ UDP Flood เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่ และหรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด โดยจะส่ง UDP packet ไปยัง port ที่กำหนดไว้ เช่น 53 (DNS)

การโจมตีแบบ Teardrop โดยปกติ เราเตอร์จะไม่ยอม ให้แพ็กเก็ตขนาดใหญ่ผ่านได้ จะต้องทำ Fragment เสียก่อนจึงจะยอมให้ผ่านได้ และเมื่อผ่านไปแล้วเครื่องของผู้รับปลายทาง จะนำแพ็กเก็ตที่ถูกแบ่งออกเป็น ชิ้นส่วนต่าง ๆ ด้วยวิธีการ Fragment มารวมเข้าด้วยกันเป็น แพ็กเก็ตที่สมบูรณ์ การที่สามารถนำมารวมกันได้นี้จะต้องอาศัยค่า Offset ที่ปรากฏอยู่ในแพ็กเก็ต แรกและแพ็กเก็ตต่อๆ ไป สำหรับการโจมตีแบบ Teardrop นี้ ผู้โจมตีจะส่งค่า Offset ในแพ็กเก็ตที่ สองและต่อ ๆ ไปที่จะทำให้เครื่องรับปลายทางเกิดความสับสน หากระบบปฏิบัติการไม่สามารถ รับมือกับปัญหานี้ก็จะทำให้ระบบหยุดการทำงานใน ทันที

การโจมตีแบบ Land Attack ลักษณะการโจมตีประเภทนี้ เป็นการส่ง SYN ไปที่ เครื่องเป้าหมายเพื่อขอการเชื่อมต่อ ซึ่งเครื่องที่เป็นเป้าหมายจะต้องตอบรับคำขอการเชื่อมต่อด้วย SYN ACK ไปที่เครื่องคอมพิวเตอร์ต้นทางเสมอ แต่เนื่องจากว่า IP Address ของเครื่องต้นทางกับ เครื่องที่เป็น เป้าหมายนี้มี IP Address เดียวกัน โดยการใช้วิธีการสร้าง IP Address ลวง (โดยข้อเท็จจริงแล้วเครื่องของ Hacker จะมี IP Address ที่ต่างกับเครื่องเป้าหมายอยู่แล้ว แต่จะใช้ วิธีการทางซอฟต์แวร์ในการส่งแพ็กเก็ตที่ประกอบด้วยคำขอการเชื่อมต่อ พร้อมด้วย IP Address ปลอม) ซึ่งโปรโตคอลของเครื่องเป้าหมายไม่สามารถแยกแยะได้ว่า IP Address ที่เข้ามาเป็นเครื่อง ปัจจุบันหรือไม่ ก็จะทำการตอบสนองด้วย SYN ACK ออกไป หากแอดเดรสที่ขอเชื่อมต่อเข้ามา เป็นแอดเดรสเดียวกับเครื่องเป้าหมาย ผลก็คือ SYN ACK นี้จะย้อนเข้าหาตนเอง และเช่นกันที่การ ปล่อย SYN ACK แต่ละครั้งจะต้องมีการปันส่วนของหน่วยความจำเพื่อการนี้ จำนวนหนึ่ง ซึ่งหาก ผู้โจมตีส่งคำขอเชื่อมต่อออกมาอย่างต่อเนื่องก็จะเกิดปัญหาการจัดสรร หน่วยความจำ

การโจมตี แบบ Smurf ผู้โจมตีจะส่ง ICMP Echo Request ไปยัง broadcast address ในเครือข่ายที่เป็นตัวกลาง (ปกติจะเรียกว่า amplifier) โดยปลอม source IP address เป็น IP address ของระบบที่ต้องการโจมตี ซึ่งจะทำให้เครือข่ายที่เป็นตัวกลางส่ง ICMP Echo Reply กลับไปยัง IP address ของเป้าหมายทันที ซึ่งทำให้มีการใช้งานแบนด์วิดธ์อย่างเต็มที่ความเสียหายที่เกิด โดยการโจมตีในรูปแบบ DoS ความเสียหายที่เกิดจาก DoS ส่งผลให้ผู้ใช้งานแต่ละส่วนไม่ เหมือนกัน แล้วแต่ว่าเขาจะอยู่ในส่วนใด เช่น เป็นผู้เข้าไปใช้งาน เป็นพนักงานในองค์กรที่ โดนโจมตีหรือเป็น เจ้าของเครื่องที่ถูกใช้ในการโจมตี หรือจะมองในแง่ขององค์กรที่โดนโจมตี ทุกๆ ฝ่ายล้วนแล้วแต่เป็นฝ่ายเสียทั้งนั้น ยกเว้นคนที่ทำให้เหตุการณ์นี้ เกิดขึ้น หรือคนที่เป็นคน บงการอยู่เบื้องหลังเท่านั้นที่ได้ประโยชน์จากการโจมตีนั้น จะจัดความเสียหาย ของ DoS นั้น ก็สามารถจัดได้ตามประเภทของการทำงานของตัว DoS เอง ซึ่งสามารถแบ่งได้เป็นสองประเภท ด้วยกันคือ

ความเสียหายกับเครื่องคอมพิวเตอร์ ในส่วนความเสียหายของ เครื่องคอมพิวเตอร์นั้น เราก็สามารถมองได้สองมุมด้วยกันคือ ในมุมของเครื่องที่ถูกใช้ในการโจมตีกับในมุมของเครื่องที่โดนโจมตี

1) เครื่องที่ถูกใช้เป็นเครื่องมือในการโจมตี อันดับแรกคือเราสูญเสียการควบคุมของเครื่องเราเองทำให้คนอื่นสามารถเข้ามาบงการเครื่องของเราให้ไปทำอย่างโน้นทำอย่างนี้ตามที่เขาต้องการได้ อันดับสองคือการเสียทรัพยากรของเครื่องเองไม่ว่าจะเป็น ซีพียู เมโมรี หรือแบนด์วิดธ์ เป็นต้น ทรัพยากรต่าง ๆ ของเครื่องที่กล่าวไปแล้วนั้นจะถูกใช้ไปรันโปรแกรมที่จะใช้ในการเข้าไปโจมตี เครื่องเหยื่อ ทำให้เครื่องคอมพิวเตอร์ของเรานั้นไม่สามารถใช้งานได้อย่างเต็มที่

2) เครื่องที่เป็นเหยื่อในการโจมตีครั้งนี้ แน่นอนว่าทำให้เครื่องนั้นไม่สามารถให้บริการต่อไปได้ เพราะจุดประสงค์หลักของ DoS ก็คือสิ่งนี้ เพราะเครื่องนั้นมัวแต่ประมวลผล Request จำนวนมากที่ถูกส่งเข้ามาทำให้เครื่องนั้นทำงานหนักจนไม่สามารถรับงานได้อีกต่อไปบางเครื่องอาจจะแฮงก์ไปเฉย ๆ หรือระบบอาจจะ Crash เลยก็เป็นไปได้ทำให้เครื่องนั้นไม่สามารถให้บริการได้อีก

ความเสียหายกับระบบเน็ตเวิร์ก ความเสียหายที่เกิดขึ้น กับระบบเน็ตเวิร์กนั้น เราก็สามารถมองได้สองมุมเช่นกัน คือ มองในมุมของผู้ที่ถูกใช้เป็นเครื่องมือในการโจมตี และผู้ที่ถูกโจมตี มุมที่ผู้ถูกใช้เป็นเครื่องมือ ทำให้แบนด์วิดธ์ที่เราควรจะมีเหลือไว้ ใช้นั้นถูกใช้ไปกับการโจมตีเสียหมด บางครั้งก็กินแบนด์วิดธ์ทั้งหมด ที่เรามีอยู่เพื่อใช้ในการโจมตีทำให้เครื่อง หรือระบบที่ถูกใช้เป็นเครื่องมือในการโจมตีนั้นไม่สามารถใช้งานระบบ เน็ตเวิร์กได้อีกต่อไป มุมที่ผู้ถูกโจมตี เช่นเดียวกับแบนด์วิดธ์ของผู้ที่ถูกโจมตีนั้นก็จะใช้ไปอย่างรวดเร็วจนหมด ทำให้บริการที่เตรียมไว้ที่เครื่องที่ถูกโจมตีนั้นไม่สามารถใช้งานได้อีกต่อไป เครื่องที่ต้องการที่จะติดต่อเข้ามาที่เครื่องนี้ หรือผ่านเครื่องนี้เพื่อเข้าไปในระบบข้างใน (ในกรณีที่เป็นไฟร์วอลล์) ไม่สามารถใช้งานได้ ผู้ที่อยู่ด้านในของระบบก็จะไม่สามารถเชื่อมต่อกับ ระบบภายนอกได้เช่นเดียวกัน แต่ระบบ LAN ภายในก็ยังสามารถใช้งานได้ตามปกติ

ความเสียหายกับองค์กร เมื่อเกิดการโจมตีขึ้นแล้วก็มีแต่เสียกับเสียเท่านั้น ยิ่งองค์กรที่ถูกโจมตีด้วยแล้วความเสียหายนั้นก็เกิดขึ้นอย่างมากมายทีเดียว เริ่มตั้งแต่ความเสียหายของตัวเครื่องคอมพิวเตอร์หรือระบบที่โดนโจมตีเองทำให้ ต้องเสียเวลาเสียค่าใช้จ่ายในการซ่อมแซม เพื่อที่ให้สามารถกลับมาให้บริการได้อย่างเดิม เสียโอกาสทางธุรกิจโอกาสที่จะทำธุรกรรมกับเครื่องที่โดนโจมตี หรือการทำธุรกรรมอื่นๆ กับระบบภายในที่จำเป็นต้องต่อเชื่อมกับอินเตอร์เน็ตสูญเสียโอกาสที่จะทำธุรกรรมทางอินเตอร์เน็ต โอกาสที่ลูกค้าจะเข้ามาในเว็บโอกาสที่จะปิด การขาย โอกาสที่จะสร้างรายได้ และอีกหลาย ๆ โอกาสที่ทางองค์กรจะต้องเสียไป

เสียภาพลักษณ์ขององค์กร องค์กรที่ถูกโจมตีด้วยการโจมตีประเภท DoS นั้น ทำให้การบริการที่องค์กรนั้นเตรียมพร้อมไว้ให้บริการไม่สามารถให้บริการ ได้ทำให้ภาพลักษณ์ขององค์กรนั้นเสียไป เพราะไม่สามารถป้องกัน เหตุที่เกิดขึ้นได้ หรือไม่มีวิธีการแก้ไขที่รวดเร็วจนทำให้เกิดความ เสียหายขึ้น ทำให้ลูกค้าขาดความเชื่อมั่นในองค์กรว่าจะสามารถตอบสนอง ความต้องการของตนได้ อาจเป็นเหตุให้ลูกค้าเปลี่ยนใจไปใช้บริการของ องค์กรอื่นแทนในที่สุด

วงจรชีวิตของไวรัสคอมพิวเตอร์ มี 4 ระยะ คือ

1) ระยะไม่เคลื่อนไหว Dormant Phase เป็นระยะที่โปรแกรมไวรัสจะหยุดนิ่งไม่กระทำการใดๆ เป็นระยะที่ยังไม่ถูกกระตุ้นให้ทำงานนั่นเอง

2) ระยะแพร่กระจาย Propagation Phase เป็นระยะที่โปรแกรมไวรัสคัดลอกตัวเองหรือฝังตัวอยู่กับโปรแกรมอื่น หรือหน่วยความจำ ใด ๆ ขึ้นอยู่กับหน้าที่ของไวรัส สำหรับโปรแกรมที่ติดไวรัส ก็คือโปรแกรมที่มีโค๊ดไวรัสฝังอยู่หรือแนบอยู่ ก็จะเข้าสู่ระยะแพร่กระจายต่อไป

3) ระยะถูกกระตุ้น Triggering Phase เป็นระยะที่โปรแกรมไวรัสดถูกกระตุ้นให้ทำงานตามคำสั่ง โดยเหตุการณ์ต่าง ๆ ที่จะเป็นตัวกระตุ้นการทำงาน เช่น ถึงวันที่ที่ถูกกำหนดไว้ในโปรแกรมไวรัส

4) ระยะทำงาน Execution Phase เป็นระยะทำงานของโปรแกรมไวรัส เป็นระยะที่เห็นผลของการทำงาน เช่นมีข้อความปรากฏบนจอภาพ หรือ รูปภาพในโฟลเดอร์หายไป เป็นต้น

ประเภทของไวรัส

1) Memory Resident Virus เป็นไวรัสที่ฝังตัวอยู่ในหน่วยความจำหลัก

2) Program File Virus เป็น ไวรัส ที่ฝังตัวอยู่ในโปรแกรมใด ๆ เช่น File ที่มี นามสกุล .exe, .com, .sys เป็นต้น

3) Polymorphic Virus เป็นไวรัสที่สามารถซ่อนลักษณะและเปลี่ยนพฤติกรรมไปเรื่อยๆ เพื่อหลีกเลี่ยงการตรวจจับของซอฟต์แวร์ AntiVirus

4) Boot Sector เป็นไวรัสที่ฝังตัวอยู่ในส่วนของ Boot Sector ของ Hard disk ที่จัดเก็บโปรแกรมระบบปฏิบัติการ ซึ่งจะถูกอ่านเมื่อเริ่มต้นเปิดเครื่อง การทำงานของไวรัสชนิดนี้ จะทำการเคลื่อนย้ายชุดคำสั่งที่อยู่บริเวณ Boot Sector ไปไว้บริเวณอื่น จากนั้นโปรแกรมไวรัสจะวางโค๊ดของตนไว้ใน Boot Sector แทน เมื่อระบบเริ่มทำงาน คือเริ่มเปิดเครื่อง โค๊ดโปรแกรมไวรัสจะถูกโหลดไปไว้ที่หน่วยความจำหลัก เพื่อเริ่มทำการประมวลผลตามคำสั่งมุ่งร้ายที่ได้กำหนดไว้ และขณะเดียวกันไวรัสก็ได้ถูกฝังตัวอยู่ในหน่วยความจำหลักเรียบร้อยแล้ว

5) Macro Virus มาโคร คือชุดคำสั่ง ที่ทำงานได้เองอัตโนมัติ บนโปรแกรมหรือ application เฉพาะ นั่นคือในกลุ่ม Microsoft Office แบ่งออกเป็น Auto Execute, Auto Macro, Command Macro

6) E-mail Virus เป็นไวรัสที่แนบตัวเองไปกับอีเมล์ เช่น อาจแบบไปกับเนื้อหาอีเมล์ หรือฝังตัวไปกับไฟล์ที่แนบไปกับอีเมล์

ปัญหาจากสปายแวร์ เมื่อสปายแวร์ได้แอบเข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของคุณแล้ว มันจะพยายามรัน process พิเศษบางอย่างซึ่งจะเป็นผลให้เครื่องคอมพิวเตอร์ของคุณทำงานช้าลงหรืออาจทำการเข้าสู่เว็บไซต์ต่างๆได้ช้า หรืออาจเข้าสู่เว็บไซต์ที่ต้องการไม่ได้เลย นอกจากนี้ ยังส่งผลเกี่ยวเนื่องกับเรื่องของข้อมูลส่วนบุคคล (privacy) ในประเด็นต่อไปนี้ด้วย ไม่สามารถทราบได้เลยว่าข้อมูลที่ถูกนำไปมีอะไรบ้างไม่อาจทราบได้เลยว่าใครเป็นผู้นำข้อมูลเหล่านั้นไปและจะไม่ทราบเช่นกันว่า ข้อมูลเหล่านั้นจะถูกนำไปใช้อย่างไรบ้าง

ข้อสังเกตเมื่อมีสปายแวร์เข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ มีหน้าต่างเล็กๆ ที่เป็นโฆษณาป๊อบอัพขึ้นมาเองบ่อยครั้งจนนับไม่ถ้วน เมื่อต้องการเข้าสู่เว็บไซต์ใดเว็บไซต์หนึ่งและพิมพ์ที่อยู่แอดเดรส (URL) ลงไปอย่างถูกต้องแล้วแต่เว็บบราวเซอร์จะเข้าสู่เว็บไซต์ที่สปายแวร์ได้ตั้งไว้และแสดงหน้าเว็บเหล่านั้น แทนที่จะเข้าไปยังเว็บไซต์ที่ต้องการสังเกตเห็นว่ามีแถบเครื่องมือใหม่ๆ ที่ไม่เคยเห็น หรือไม่คุ้นเคยเกิดขึ้นบนเว็บบราวเซอร์ บริเวณ task tray ในส่วนแสดงการเปิดโปรแกรมที่กำลังรันอยู่ด้านล่างของหน้าต่างวินโดว์จะปรากฏแถบแสดงเครื่องมือหรือไอคอนที่ไม่เคยเห็นมาก่อน หรือไอคอนแปลกๆ หน้าหลักของบราวเซอร์ที่คุณเซ็ตค่าไว้ถูกเปลี่ยนไปในทันที เมื่อเรียก search engine ที่เคยใช้ในการค้นหาขึ้นมา และทำการค้นหา หรือทันทีที่คลิกปุ่ม search เว็บบราวเซอร์จะไปเรียกหน้าเว็บที่แตกต่างไปจากเดิมฟังก์ชั่นบนคีย์บอร์ดบางอย่างที่เคยใช้งานจะเกิดอาการผิดปกติ เช่น เคยกดปุ่ม tab เพื่อเลื่อนไปยังช่องกรอกข้อความในฟิลด์ถัดไปบนหน้าเว็บจะไม่สามารถใช้ในการเลื่อนตำแหน่งได้เหมือนเดิม เป็นต้น ข้อความแสดงความผิดพลาดของซอฟต์แวร์วินส์โดว์จะเริ่มปรากฏบ่อยมากขึ้น เครื่องคอมพิวเตอร์ของคุณจะทำงานช้าลงอย่างเห็นได้ชัดเมื่อสั่งเปิดโปรแกรมหลายโปรแกรม หรือทำงานหลายอย่าง โดยเฉพาะในระหว่างการบันทึกแฟ้มข้อมูล เป็นต้น

การป้องกันสปายแวร์ ไม่คลิ๊กลิ้งบนหน้าต่างเล็กๆ ที่ปรากฏขึ้นมาอัตโนมัติหรือโฆษณาที่ป๊อบอัพขึ้นมา เพราะป๊อบอัพเหล่านั้นมักจะมีตัวสปายแวร์ฝังอยู่ การคลิ๊กลิ้งเหล่านั้นจะทำให้สปายแวร์ถูกนำเข้ามาติดตั้งบนเครื่องของคุณผ่านวินโดวส์ได้ในทันที ส่วนวิธีการปิดหน้าต่างป๊อบอัพเหล่านั้นควรคลิ๊กที่ปุ่ม “X” บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar) ควรเลือกที่คำตอบ “No” ทุกครั้งที่มีคำถามต่างๆ ถามขึ้นมาจากป๊อบอัพเหล่านั้น คุณต้องระมัดระวังเป็นอย่างมากกับคำถามที่ปรากฏขึ้นมาเป็นไดอะล็อกบ็อกซ์ต่างๆ แม้ว่าไดอะล็อกบ๊อกซ์เหล่านั้นจะเกิดขึ้นตอนคุณกำลังรันโปรแกรมเฉพาะที่คุณจะใช้งาน หรือใช้โปรแกรมอื่นอยู่ก็ตาม ควรปิดหน้าต่างป๊อบอัพเหล่านั้นด้วยวิธีคลิ๊กที่ปุ่ม “X” บนแถบเมนู Title bar แทนที่จะปิดด้วยคำสั่ง close บนแถบแสดงเครื่องมือมาตรฐานของวินโดว์ (standard toolbar) ควรระมัดระวังอย่างมากในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี เพราะมีหลายเว็บไซต์ที่จัดหาแถบเครื่องมือแบบที่ให้ผู้ใช้ปรับแต่งเองหรือมีคุณสมบัติอื่นๆ ที่เหมาะสำหรับผู้ใช้ให้ปรับแต่งเองไว้ให้ดาวน์โหลดบนอินเทอร์เน็ต สำหรับท่านที่ต้องการใช้คุณสมบัติของเครื่องมือเหล่านี้ ไม่ควรจะดาวน์โหลด เครื่องมือเหล่านี้มาจากเว็บไซต์ที่ไม่น่าเชื่อถือ และต้องตระหนักเสมอว่ามันเป็นการปล่อยให้สปายแวร์ผ่านเข้ามายังเครื่องคุณได้ด้วย ไม่ควรติดตามอีเมล์ลิ้งที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกันสปายแวร์ เหมือนกับอีเมล์ที่ให้ข้อมูลว่า มีการเสนอซอฟต์แวร์ป้องกันไวรัส ซึ่งอันที่จริงลิ้งเหล่านั้นจะนำไปสู่แนวทางที่ตรงกันข้าม คือเป็นการถามเพื่อให้คุณคลิ๊กอนุญาตให้สปายแวร์เข้ามาดำเนินการติดตั้งในเครื่องโดยไม่ถูกขัดขวาง

วิธีกำจัดสปายแวร์ ทำการสแกนเครื่องคอมพิวเตอร์อย่างถี่ถ้วน ด้วยโปรแกรมแอนติไวรัส ซึ่งแอนติไวรัสบางยี่ห้อจะมีคุณสมบัติในการค้นหาและกำจัดสปายแวร์ แต่แอนติไวรัสอาจไม่สามารถมองหาสปายแวร์พบแบบ real time ได้ ดังนั้นควรกำหนดให้โปรแกรมแอนติไวรัสของคุณทำการสแกนหาไวรัสเมื่อเครื่องอยู่ในสภาวะปลอดจากการใช้งานใดๆ และควรทำการสแกนอย่างถี่ถ้วนและสม่ำเสมอ เช่น วันละครั้งหลังเลิกงาน เป็นต้น) ทำการติดตั้งโปรแกรมแอนติสปายแวร์ที่มีลิขสิทธิ์และถูกออกแบบมาเพื่อกำจัดสปายแวร์โดยเฉพาะมีผู้ผลิตหลายรายที่เสนอผลิตภัณฑ์ที่มีคุณสมบัตินี้ ซึ่งจะสแกนหาสปายแวร์บนเครื่องและกำจัดสปายแวร์ออกจากเครื่องได้ สำหรับผลิตภัณฑ์แอนติสปายแวร์ที่เป็นที่นิยม ได้แก่ LavaSoft’Adaware,Webroot’s SpySweeper, PestPatrol, Spybot Search and Destroy (ตามลิ้งก์ด้านล่าง) สร้างความรำคาญ ให้กับผู้ที่รู้ว่ามันคือของปลอม เพราะต้องเปลืองแรงลบเมล์ในอินบ็อกซ์ (Inbox) อยู่เสมอๆ แต่สำหรับผู้ที่หลงเชื่ออาจสร้างความตื่นตระหนก จนต้องรีบตรวจสอบเครื่องตัวเองอย่างเร่งด่วน เมื่อตรวจสอบพบตามที่ข้อความในอีเมล์แจ้งมาแล้ว จะให้ผู้ดูแลระบบมาจัดการกำจัดไวรัสโดยด่วน เมื่อผู้ดูแลระบบมาถึง แล้วบอกว่านี่ไม่ใช่ไวรัส แต่มันเป็นแค่จดหมายหลอกลวง ก็กลับไม่เชื่อ และ ที่ร้ายแรงกว่านั้นคือ เมื่อตนเองได้รับอีเมล์นั้น ก็หวังดีส่งต่อ

ข้อความไปเรื่อยๆทำให้เปลืองทรัพยากรของระบบเครือข่ายโดยไม่จำเป็น และอาจกลายเป็นจดหมายลูกโซ่ที่ไม่มีวันจบสิ้นในที่สุด

วิธีการสังเกตมีดังนี้

1) อีเมล์ดังกล่าวจะไม่มีไฟล์แนบ

2) ส่วนใหญ่อ้างว่าได้ข้อมูลมาจากแหล่งข่าวที่มีชื่อเสียง แต่ไม่มีลิงค์ไปยังแหล่งข้อมูลนั้น

3) ประกอบไปด้วยข้อความอวดอ้างเกินจริง เน้นย้ำว่ามีอันตรายมาก

4) เนื้อความในตอนท้ายเน้นว่าต้องส่งอีเมล์นี้ต่อให้ผู้อื่น เป็นต้น

5) พบเห็นจดหมายอิเล็กทรอนิกส์ที่มีข้อความในทำนองที่กล่าวข้างต้น ชื่อเรื่อง หรือเนื้อหาที่มีในรายการดังต่อไปนี้ ควรลบทิ้งทันทีและไม่ควรส่งต่อให้ผู้อื่น เนื่องจากเป็นข่าวที่ไม่เป็นความจริง และอาจก่อให้เกิดความเสียหายต่อผู้อื่นที่ได้รับข้อความเหล่านี้

ผลงานวิจัยที่เกี่ยวกับพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ ของนักศึกษา สุพรรษา เกษสีแก้ว (2552) จาก มหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาพฤติกรรมการใช้สังคมออนไลน์เวลาจริงของนักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ และเปรียบเทียบพฤติกรรมการใช้สังคมออนไลน์เวลาจริง จำแนกตามปัจจัยส่วนบุคคลของนักศึกษา กลุ่มตัวอย่างเป็นนักศึกษาปริญญาตรีมหาวิทยาลัยธุรกิจบัณฑิตย์ จำนวน 400 คน พบว่าส่วนใหญ่ ใช้สังคมออนไลน์เวลาจริงด้วยโปรแกรม msn เพื่อแลกเปลี่ยนข่าวสาร ที่บ้าน ส่วนใหญ่รู้จักสังคมออนไลน์จากเพื่อน ด้านประโยชน์ของสังคมออนไลน์เวลาจริงที่พอใจมากที่สุด ช่วงเวลาที่ใช้ คือ 18.01 – 24.00 น. ใช้ในการติดต่อกับบุคคลที่รู้จัก

ผลงานวิจัยที่เกี่ยวกับ ความรู้ ทัศนคติต่อพฤติกรรมด้านความปลอดภัยของพนักงานอู่ทหารเรือพระจุลจอมเกล้า กรมอู่ทหารเรือ กรณีศึกษา : ในสายงานฝ่ายผลิต ของนักศึกษา ศิริพงศ์ ศรีสุขกาญจน์ (2553) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาพฤติกรรมด้านความปลอดภัยของพนักงาน เปรียบเทียบความรู้และทัศนคติของพนักงานที่มีลักษณะส่วนบุคคลแตกต่างกันและความสัมพันธ์ระหว่างความรู้ ทัศนคติ และพฤติกรรมด้านความปลอดภัย กลุ่มตัวอย่างคือพนักงานที่ปฏิบัติงานในสายงานฝ่ายผลิตของ อู่ทหารเรือพระจุลจอมเกล้า กรมอู่ทหารเรือ จำนวน 277 คน พนักงานมีระดับความรู้ด้านความปลอดภัยอยู่ในระดับปานกลาง ทัศนคติด้าน ความปลอดภัยอยู่ในระดับที่ดี และพฤติกรรมด้านความปลอดภัยอยู่ในระดับปานกลาง

ผลงานวิจัยที่เกี่ยวกับการใช้ประโยชน์และความพึงพอใจต่อระบบอินทราเน็ต การใช้ประโยชน์และความพอใจต่อระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร กรณีศึกษา : ข้าราชการโรงพยาบาลพระมงกุฎเกล้า ของนักศึกษา วรรณยา บุนนาค (2554) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาเรื่อง การศึกษาพฤติกรรมการใช้อินทราเน็ตเพื่อการสื่อการภายในองค์กร การใช้ประโยชน์ความพึงพอใจต่อการใช้ระบบอินทราเน็ตเพื่อการสื่อสารภายในองค์กร โดยใช้แบบสอบถามกับกลุ่มตัวอย่าง 358 คนแล้วนำมาวิเคราะห์ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน ค่าไคสแควร์ และความแปรปรวนทางเดียว จากการสุ่มตัวอย่างดังกล่าว โรงพยาบาลพระมงกุฎเกล้าในการให้บริการบนระบบอินทราเน็ตและคอมพิวเตอร์ยังมีประสิทธิภาพต่ำ

ผลงานวิจัยที่เกี่ยวกับความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคล ของนักศึกษา นวรัตน์ พัฒโนทัย (2555) นักศึกษามหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี เป็นการศึกษาเรื่อง ทางระบบคอมพิวเตอร์ กรณีศึกษาในเขต กรุงเทพมหานคร เป็นการศึกษาระดับความรู้ ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลในเขตกรุงเทพมหานคร จากกลุ่มตัวอย่างที่ใช้ในการศึกษา คือประชาชน ที่ใช้คอมพิวเตอร์ ในเขตกรุงเทพมหานคร โดยใช้แบบสอบถาม เป็นเครื่องมือในการสำรวจ สรุปได้ว่า ประชาชนที่ใช้คอมพิวเตอร์ในเขตกรุงเทพมหานคร ส่วนใหญ่มีระดับความรู้อยู่ในเกณฑ์มีความรู้ร้อยละ 68.6 ผลการทดสอบสมมติฐานพบว่า ปัจจัยส่วนบุคคลที่มีความแตกต่างกัน ด้านเพศ อายุ ระดับการศึกษา อาชีพ ประสบการณ์การทำงาน มีผลต่อความรู้ ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์แตกต่างกัน ยกเว้นปัจจัยส่วนบุคคลด้านรายได้ ซึ่งไม่ส่งผลต่อความรู้ความเข้าใจในความปลอดภัยของข้อมูลส่วนบุคคลทางระบบคอมพิวเตอร์

ผลงานวิจัยที่เกี่ยวกับการวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์ ของนักศึกษา ปิยะนาถ คล่องดี (2556) นักศึกษามหาวิทยาลัยธุรกิจบัณฑิตย์ เป็นการศึกษาเรื่อง การวิเคราะห์ความคุ้มทุนและประโยชน์ที่ชุมชนได้รับในการจัดตั้งศูนย์การเรียนรู้ ICT ชุมชน กรณีศึกษา ศูนย์การเรียนรู้ ICT ชุมชนตำบลบางเพรียง อำเภอบางบ่อ จังหวัดสมุทรปราการ เป็นการศึกษาความคุ้มค่าในการลงทุนจัดตั้งศูนย์การเรียนรู้ ICT ชุมชนของภาครัฐกับมูลค่าการลงทุนที่เสียไป โดยมีการวิเคราะห์เป็น 2 แบบ คือ 1) การวิเคราะห์ข้อมูลเชิงปริมาณ โดยนำการวิเคราะห์ ทางการเงินมาใช้ 2) การวิเคราะห์แบบพรรณนา เป็นการวิเคราะห์ให้ทราบถึงผลประโยชน์ที่ชุมชนได้รับ และจากการเครื่องมือดังกล่าวพบว่า ผู้ใช้บริการส่วนใหญ่มีความพึงพอใจในการให้บริการของศูนย์การเรียนรู้ ICT ชุมชนร้อยละ 70 มีความพึงพอใจในการเข้าถึง สถานที่ตั้งศูนย์