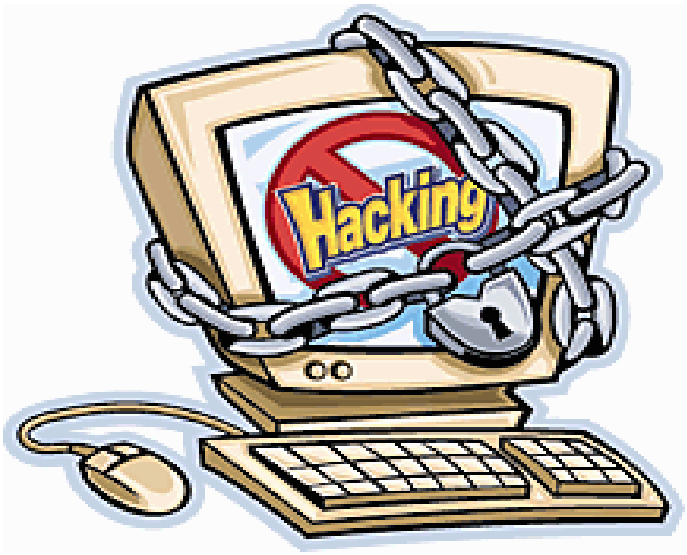
การป้องกันภัยคุกคามทางคอมพิวเตอร์



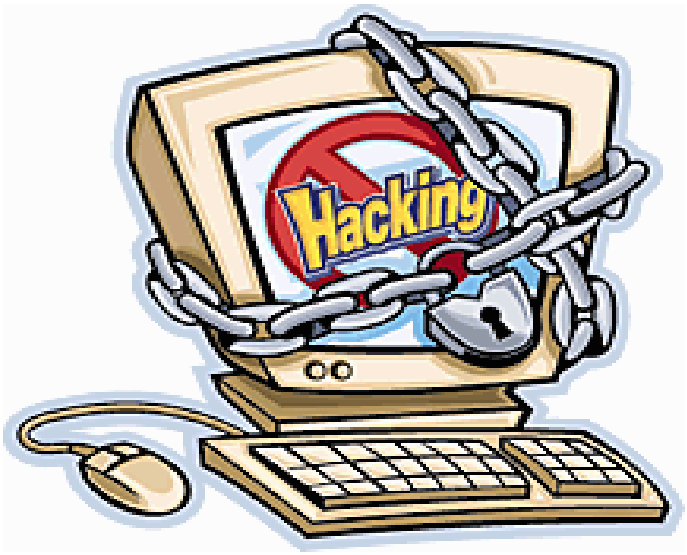
เอกสารเป็นส่วนหนึ่งประกอบการจัดการความรู้

(Knowledge Management)

โดย
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา

องค์ความรู้

เรื่อง การป้องกันภัยคุกคามทางคอมพิวเตอร์



เอกสารเป็นส่วนหนึ่งประกอบการจัดการความรู้

(Knowledge Management)

โดย
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร
คณะทำงานการจัดการความรู้ สำนักงานเลขาธิการวุฒิสภา

สรุปสาระสำคัญ
เรื่อง
การป้องกันภัยคุกคามทางคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์ ครอบคลุมทั้งการคุกคามทางระบบฮาร์ดแวร์ ระบบซอฟต์แวร์ และข้อมูล โดยสาเหตุของภัยคุกคามอาจจะมาจากทางกายภาพ เช่น อัคคีภัย ปัญหาวงจรไฟฟ้า ระบบสื่อสาร ความผิดพลาดของฮาร์ดแวร์ ความผิดพลาดของซอฟต์แวร์ หรือภัยคุกคามที่เกิดจากคนหรือผู้ใช้ระบบ เช่น การบุกรุกจากผู้ที่ไม่ได้รับอนุญาต หรือผู้ใช้ไม่เข้าใจระบบทำให้ระบบเกิดความเสียหาย ภัยคุกตามเหล่านี้เป็นสาเหตุให้ข้อมูลในระบบเสียหาย สูญหาย ถูกขโมย หรือแก้ไขบิดเบือน โดยจำแนกภัยคุกคามทางระบบคอมพิวเตอร์แบ่งออกเป็น ๓ ประเภทดังนี้

1. ภัยคุกคามทางระบบฮาร์ดแวร์ (Hardware Security Threats) คือ ภัยที่มีต่อระบบการจ่ายไฟฟ้า ภัยที่เกิดจากการทำลายทางกายภาพโดยตรงต่อระบบคอมพิวเตอร์นั้นๆ และภัยจากการลักขโมยโดยตรง

2. ภัยคุกคามทางระบบซอฟต์แวร์ (Software Security Threats) การลบซอฟต์แวร์ หรือการลบเพียงบางส่วนของซอฟต์แวร์นั้น ๆ การขโมยซอฟต์แวร์ (Software Theft) การเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Software Modification) และการขโมยข้อมูล (Information Leaks)

3.ภัยคุกคามที่มีต่อระบบข้อมูล (Data Threats) การที่ข้อมูลอาจถูกเปิดเผยโดยมิได้รับอนุญาต การที่ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขเพื่อผลประโยชน์ โดยมิได้มีการตรวจสอบแก้ไข การที่ข้อมูลนั้นถูกทำให้ไม่สามารถนำมาใช้งานได้

รูปแบบภัยคุกคามทางคอมพิวเตอร์

1. มัลแวร์ (Malware) คือความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด สูญเสียความลับทางข้อมูล สูญเสียความไม่เปลี่ยนแปลงของข้อมูล สูญเสียเสถียรภาพของระบบปฏิบัติการ

2. ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยาก

3. หนอนคอมพิวเตอร์ (computer worm) หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่น ระบบเครือข่าย หรืออินเทอร์เน็ต เป็นต้น

4. ม้าโทรจัน (Trojan horse) โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนาไปใช้ในการเจาะระบบ

5. สปายแวร์ (Spyware) ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์ และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

6. ประตูหลัง (Backdoor) รูรั่วของระบบรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ที่ผู้ออกแบบหรือผู้ดูแลระบบจงใจทิ้งไว้โดยเป็นกลไกลับทางซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคงปลอดภัย แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้

7. Rootkit โปรแกรมที่ออกแบบมาเพื่อซ่อนอ็อบเจ็กต์ต่างๆ เช่น กระบวนงาน ไฟล์ หรือข้อมูล แม้จะเป็นโปรแกรมที่อาจไม่เป็นอันตรายเสมอไป แต่ก็ถูกนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากขึ้น

8. การโจมตีแบบ DoS/DDoS ความพยายามโจมตีเพื่อทาให้เครื่องคอมพิวเตอร์ปลายทางหยุดทางานหรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

9. BOTNET ภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการตัวนำทางเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เอง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น

10. Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล์ เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

11. Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สาคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตโดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทาให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

12. Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้

13. ข้อมูลขยะ (Spam) ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมล์หรือเรียกว่า อีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับ

14. Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ ไม่ว่าจะกระทำด้วยมนุษย์ หรือ อาศัยโปรแกรมแฮก หลากรูปแบบ ที่หาได้ง่ายในโลกอินเทอร์เน็ต แถมยังใช้งานได้ง่าย ไม่ต้องเป็นผู้เชี่ยวชาญในคอมพิวเตอร์ก็สามารถเจาะระบบได้

15. ผู้บุกรุก (Hacker)

หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก

<u>แนวทางแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัย</u>

<u>สำหรับหน่วยงาน</u>

1. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

2. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

3. แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงาน ให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับเมลแนบจากคนที่ไม่รู้จัก , ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่างๆ หรือช่องทาง Social Network ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

4. หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง 30 วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

5. ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน หรือตามที่กฎหมายกำหนด

6. หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามไซเบอร์มายัง**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย** : ThaiCERT (ไทยเซิร์ต)

<u>แนวทางแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัย</u>

<u>สำหรับผู้ใช้อินเทอร์เน็ตทั่วไป</u>

1. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่างๆ หรือช่องทาง Social Media เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวันมัลแวร์มาจากพวกไฟล์แนบ ทาง Social Network เพิ่มมากขึ้น

2. การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

3. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจน ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

****

คำนำ

ในปัจจุบันเรื่องของการรักษาความปลอดภัยของข้อมูลถือเป็นส่วนสำคัญของการนำระบบสารสนเทศเข้ามาใช้ในองค์กร เนื่องจากระบบสารสนเทศใช้คอมพิวเตอร์เป็นหลักในการเก็บรักษาข้อมูล และใช้ระบบเครือข่ายเป็นกลางในการติดต่อสื่อสาร จึงเป็นเรื่องง่ายต่อการคุกคามข้อมูลจากผู้ไม่ประสงค์ สำหรับภัยคุกคามต่อระบบคอมพิวเตอร์จะหมายความครอบคลุมทั้งการคุกคามทางฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล โดยสาเหตุของภัยคุกคามอาจจะมาจากทางกายภาพ เช่น อัคคีภัย ปัญหาวงจรไฟฟ้า ระบบสื่อสาร ความผิดพลาดของฮาร์ดแวร์ ความผิดพลาดของซอฟต์แวร์ หรือภัยคุกคามที่เกิดจากคนหรือผู้ใช้ระบบ เช่น การบุกรุกจากผู้ที่ไม่ได้รับอนุญาต หรือผู้ใช้ไม่เข้าใจระบบทำให้ระบบเกิดความเสียหาย ภัยคุกตามเหล่านี้เป็นสาเหตุให้ข้อมูลในระบบเสียหาย สูญหาย ถูกขโมยหรือแก้ไขบิดเบือน

ดังนั้น การนำระบบสารสนเทศเข้ามาใช้ จึงต้องเพิ่มในเรื่องของระบบการรักษาความปลอดภัยของข้อมูลควบคู่ไปด้วยอย่างหลีกเลี่ยงไม่ได้ ความรู้เกี่ยวกับกระบวนการป้องกันและตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ขั้นตอนการป้องกันจะช่วยให้ ผู้ที่ใช้งานสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่าง ๆ ถูกเข้าใช้งานโดยผู้ที่ไม่ได้รับสิทธิ์ ส่วนการตรวจสอบจะทำให้ทราบได้ว่ามีใครกำลังพยายามที่จะบุกรุก เข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ ผู้บุกรุก ทำอะไรกับระบบบ้าง รวมทั้งการป้องกันจากภัยคุกคาม (Threat) ต่างๆ อาชญากรรมคอมพิวเตอร์ การกระทำที่ผิดต่อกฎหมายโดยการใช้คอมพิวเตอร์ หรือทำลายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่น จึงมีความสำคัญต่อผู้ใช้งาน และผู้ดูแลระบบคอมพิวเตอร์เป็นอย่างมาก

สำนักเทคโนโลยีสารสนเทศและการสื่อสาร

กรกฎาคม 2559

สารบัญ

หน้า

๒. เนื้อหา

๒.๑ บทนำ/หลักการและเหตุผล

ด้วยมีพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ โดยสำนักงานเลขาธิการวุฒิสภา ประกาศใช้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อเป็นเครื่องมือสำหรับผู้ใช้บริการ ผู้ดูแลระบบงานและผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของวุฒิสภา และสำนักงานเลขาธิการวุฒิสภา ดังนั้น จึงจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติฯ เพื่อให้ความมั่นคงปลอดภัยด้านสารสนเทศของวุฒิสภาเป็นไปอย่างยั่งยืน ดังในรายละเอียดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักงานเลขาธิการวุฒิสภา

ระบบเทคโนโลยีสารสนเทศ สำนักเทคโนโลยีสารสนเทศและการสื่อสารซึ่งมีหน้าที่มีหน้าที่ดำเนินการเกี่ยวกับการเสนอแนะนโยบาย การกำกับ ดูแล การสนับสนุน ส่งเสริม วางแผนและติดตามผลการนำเทคโนโลยีสารสนเทศมาใช้พัฒนาระบบงานและกระบวนการพิจารณาทางด้านนิติบัญญัติของวุฒิสภา และของสำนักงานเลขาธิการวุฒิสภา ดำเนินการเกี่ยวกับการประสานงานและปฏิบัติตามแนวนโยบายเทคโนโลยีสารสนเทศภาครัฐ และดำเนินการเกี่ยวกับการบริหาร ควบคุม ดูแลและบำรุงรักษา ระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย ระบบฐานข้อมูล และโปรแกรมต่าง ๆ ของวุฒิสภา ตลอดจนพิจารณาข้อกำหนดมาตรฐานเทคโนโลยีสารสนเทศของวุฒิสภา และของสำนักงานเลขาธิการวุฒิสภา เพื่อสนองตอบตามวิสัยทัศน์ขององค์กร ซึ่งเป็นการดำเนินงานเพื่อสนองตอบแผนยุทธศาสตร์ของสำนักงานเลขาธิการวุฒิสภา (ฉบับที่ ๓) พ.ศ. ๒๕๕๕ – ๒๕๕๙ ซึ่งเกี่ยวข้องการดำเนินการด้านเทคโนโลยีสารสนเทศ ประเด็นยุทธศาสตร์ที่ ๒ พัฒนาฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ เป้าประสงค์หลัก ข้อมูล และระบบเทคโนโลยีสารสนเทศที่เชื่อถือได้ ถูกต้อง รวดเร็ว เป็นปัจจุบัน ผู้ใช้เข้าถึงได้ง่าย และเชื่อมโยงกับเครือข่ายทั้งในและต่างประเทศ

ทั้งนี้ การนำระบบสารสนเทศเข้ามาใช้จึงต้องเพิ่มในเรื่องของระบบการรักษาความปลอดภัยของข้อมูลควบคู่ไปด้วยอย่างหลีกเลี่ยงไม่ได้ ความรู้เกี่ยวกับกระบวนการป้องกันและตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ขั้นตอนการป้องกันจะช่วยให้ผู้ที่ใช้งานสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่าง ๆ ถูกเข้าใช้งานโดยผู้ที่ไม่ได้รับสิทธิ์ ส่วนการตรวจสอบทำให้ทราบได้ว่ามีใครกำลังพยายามที่จะบุกรุก เข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ ผู้บุกรุกทำอะไรกับระบบบ้าง รวมทั้งการป้องกันจากภัยคุกคาม (Threat) ต่างๆ อาชญากรรมคอมพิวเตอร์ การกระทำที่ผิดต่อกฎหมายโดยการใช้คอมพิวเตอร์ หรือทำลายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่น จึงมีความสำคัญต่อผู้ใช้งานและผู้ดูแลระบบคอมพิวเตอร์เป็นอย่างมาก

2.2 วิธีดำเนินการ/ขั้นตอนการจัดทำองค์ความรู้

รายละเอียดของวิธีการดำเนินการ/ขั้นตอนในการจัดทำองค์ความรู้ ที่จะเกิดขึ้นภายในองค์กร ซึ่งมีดังนี้

ลำดับ	วิธีการ	วิธีการดำเนินงาน
1	วิธีการบ่งชี้ความรู้	๑. ตั้งคณะทำงานภายในสำนักเพื่อดำเนินการจัดทำองค์ความรู้
2	วิธีการสร้างและแสวงหาความรู้	๒. รวบรวมความรู้ที่เกี่ยวข้องกับองค์ความรู้ที่ดำเนินการ ศึกษาขั้นตอน/กระบวนการปฏิบัติงาน เอกสารที่เกี่ยวข้อง - วิทยากรภายนอก - การเสวนาเกี่ยวกับการภัยคุกคามทางคอมพิวเตอร์สำหรับผู้ใช้งานในองค์กร
3	วิธีการแลกเปลี่ยนเรียนรู้	ประชุมระดมสมอง หลังจากการรวบรวมและวิเคราะห์ข้อมูลที่เกี่ยวข้องมาประมวลกลั่นกรองเป็นเอกสารองค์ความรู้หรือคู่มือการปฏิบัติงาน ที่มีความครบถ้วน ถูกต้อง ทันสมัย สามารถนำไปใช้เป็นแนวทางในการปฏิบัติงานและเผยแพร่ได้
4	การมีส่วนร่วมดำเนินการ	บุคลากรสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ร่วมกันประชุมแสดงความคิดเห็นหลังจากจัดทำเอกสารร่างองค์ความรู้
5	วิธีการประมวลและกลั่นกรองความรู้	การตรวจสอบกลั่นกรองโดยคณะทำงานภายในสำนักฯ และผู้บังคับบัญชาตามลำดับชั้น
6	วิธีการจัดเก็บองค์ความรู้	จัดเก็บองค์ความรู้ในรูปแบบเอกสารและรูปแบบเอกสารอิเล็กทรอนิกส์ เพื่อให้ง่ายและสะดวกต่อการค้นหาและใช้งาน
7	วิธีการเผยแพร่และถ่ายทอดองค์ความรู้	การเผยแพร่และถ่ายทอดองค์ความรู้ในระบบ Intranet

2.3 รายละเอียดเนื้อหาองค์ความรู้

การป้องกันภัยคุกคามทางคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์

ภัยคุกคามต่อระบบคอมพิวเตอร์ ครอบคลุมทั้งการคุกคามทางระบบฮาร์ดแวร์ ระบบซอฟต์แวร์ และข้อมูล โดยสาเหตุของภัยคุกคามอาจจะมาจากทางกายภาพ เช่น อัคคีภัย ปัญหาวงจรไฟฟ้า ระบบสื่อสาร ความผิดพลาดของฮาร์ดแวร์ ความผิดพลาดของซอฟต์แวร์ หรือภัยคุกคามที่เกิดจากคน หรือผู้ใช้ระบบ เช่น การบุกรุกจากผู้ที่ไม่ได้รับอนุญาต หรือผู้ใช้ไม่เข้าใจระบบทำให้ระบบเกิดความเสียหาย ภัยคุกตามเหล่านี้เป็นสาเหตุให้ข้อมูลในระบบเสียหาย สูญหาย ถูกขโมย หรือแก้ไขบิดเบือน โดยจำแนกภัยคุกคามทางระบบคอมพิวเตอร์แบ่งออกเป็น ๓ ประเภทดังนี้

1. **ภัยคุกคามทางระบบฮาร์ดแวร์ (Hardware Security Threats)** สามารถจำแนกได้เป็น ๓ ประเภทใหญ่ๆ ดังนี้ คือ
    1.1 ภัยที่มีต่อระบบการจ่ายไฟฟ้า
    1.2 ภัยที่เกิดจากการทำลายทางกายภาพโดยตรง ต่อระบบคอมพิวเตอร์นั้นๆ
    1.3 ภัยจากการลักขโมยโดยตรง

๒. ภัยคุกคามทางระบบซอฟต์แวร์ (Software Security Threats) แบ่งได้เป็น ๔ ประเภทดังนี้
    2.1 การลบซอฟต์แวร์ หรือการลบเพียงบางส่วน ของซอฟต์แวร์นั้นๆ
    2.2 การขโมยซอฟต์แวร์ (Software Theft)
    2.3 การเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (Software Modification)
    2.4 การขโมยข้อมูล (Information Leaks)

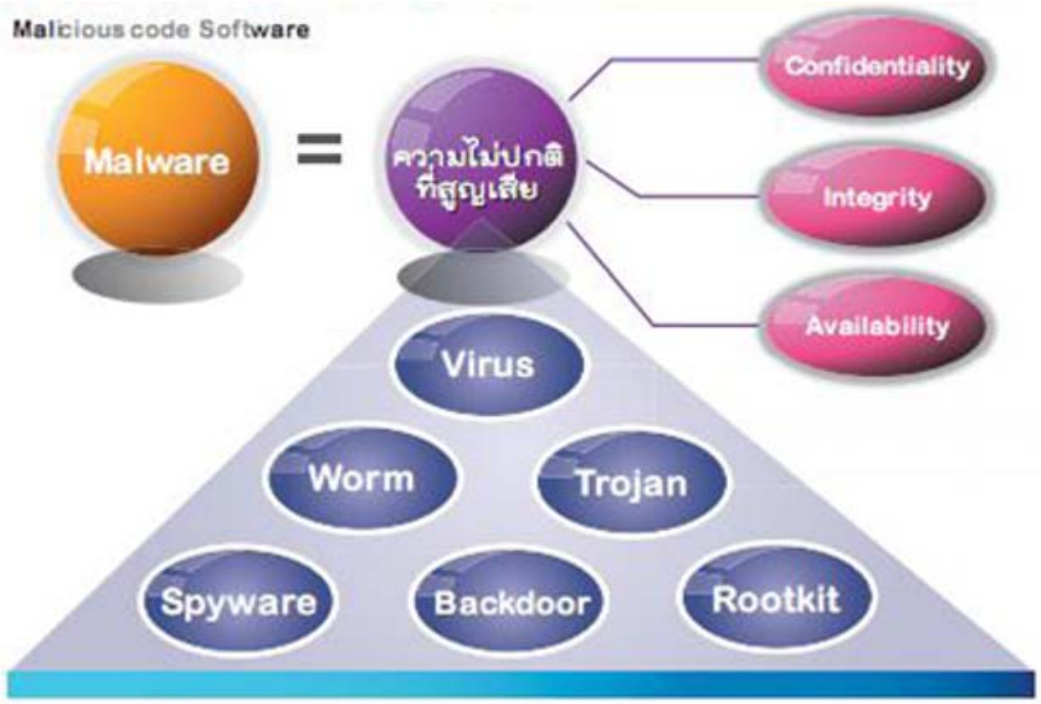
๓.ภัยคุกคามที่มีต่อระบบข้อมูล (Data Threats) แบ่งได้เป็น ๓ ประเภทดังนี้
    3.1 การที่ข้อมูลอาจถูกเปิดเผยโดยมิได้รับอนุญาต
    3.2 การที่ข้อมูลอาจถูกเปลี่ยนแปลงแก้ไขเพื่อผลประโยชน์ โดยมิได้มีการตรวจสอบแก้ไข
    3.3 การที่ข้อมูลนั้นถูกทำให้ไม่สามารถนำมาใช้งานได้

รูปแบบภัยคุกคามทางคอมพิวเตอร์

1. มัลแวร์ (Malware)

คือความไม่ปกติทางโปรแกรม ที่สูญเสีย C (Confidentiality) I (Integrity) และ A (Availability) อย่างใดอย่างหนึ่ง หรือทั้งหมด จนเกิดเป็นไวรัส เวิร์ม โทรจัน สปายแวร์ Backdoor และ Rootkit

- การสูญเสีย C (Confidentiality) คือ สูญเสียความลับทางข้อมูล
- การสูญเสีย I (Integrity) คือ สูญเสียความไม่เปลี่ยนแปลงของข้อมูล นั่นคือ ข้อมูลถูกเปลี่ยนแปลงแก้ไข
- การสูญเสีย A (Availability) คือ สูญเสียเสถียรภาพของระบบปฏิบัติการ



2. ไวรัสคอมพิวเตอร์ (Computer Virus)

เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยาก ไวรัสคอมพิวเตอร์มีหลายประเภทและก่อให้เกิดความเสียหายต่อระบบได้หลายรูปแบบ ตั้งแต่สร้างความรำคาญ มีข้อความแปลก ๆ ปรากฏขึ้นมาเรื่อย ๆ บนหน้าจอหรือแม้กระทั่งทำลายไฟล์ข้อมูลต่าง ๆ ให้ได้รับความเสียหาย รูปแบบของไวรัสคอมพิวเตอร์มี ๗ ประเภท ดังนี้

1. ไวรัสเลียนแบบ (Companion Virus) จะแอบแฝงตามไฟล์ต่างๆ และคอยสร้างไฟล์ขึ้นมาใหม่โดยเลียนแบบไฟล์ในระบบเดิม แล้วหลอกให้ระบบเรียกไฟล์ที่สร้างเลียนแบบขึ้นมาใช้งานแทนไฟล์จริง

2. ไวรัสโปรแกรม (Program Virus) ถ้ามีการเรียกใช้ไฟล์ที่ติดไวรัสประเภทนี้ ก็จะทำให้ไวรัสแพร่เชื้อไปยังทุกไฟล์ที่สามารถติดต่อไปได้

3. ไวรัสบู๊ต (Boot Virus) เป็นไวรัสที่คอยก่อกวนไฟล์สำคัญ ๆ ที่สำหรับเปิดเครื่องในตอนแรก ทำให้เราไม่สามารถบู๊ตเข้าสู่วินโดว์ได้

4. ไวรัสสองหน้า (Multipartite Virus) สามารถติดเชื้อได้ทั้งโปรแกรมและบู๊ตเซ็กเตอร์ได้พร้อม ๆ กัน ถือเป็นไวรัสที่มีความสามารถสูง

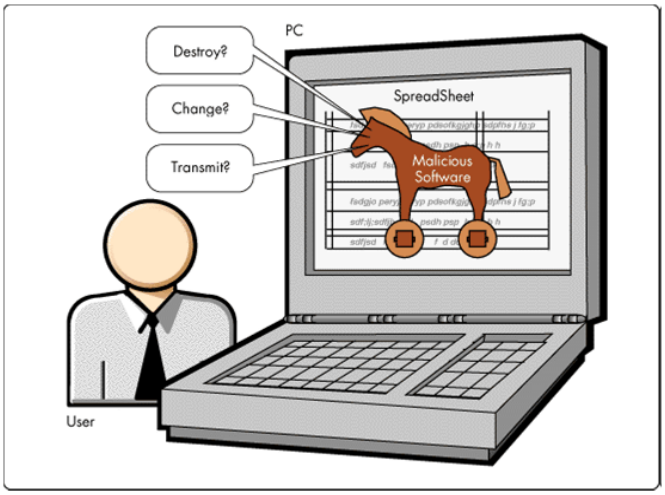
5. ไวรัสมาโคร (Macro Virus) ทำการแพร่กระจายเชื้อเฉพาะไฟล์ที่เป็นเอกสารเท่านั้น เพื่อทำให้ข้อมูลที่เก็บไว้ในไฟล์เกิดความเสียหายหรือเปลี่ยนแปลงไป

3. หนอนคอมพิวเตอร์ (computer worm)

หนอนคอมพิวเตอร์จะแพร่กระจายโดยไม่ผ่านการใช้งานของผู้ใช้ โดยมันจะคัดลอกและกระจายตัวมันเองข้ามเครือข่าย เช่น ระบบเครือข่ายหรืออินเทอร์เน็ต เป็นต้น หนอนคอมพิวเตอร์สามารถทำลายข้อมูลและสร้างความเสียหายให้กับคอมพิวเตอร์รวมไปถึงการทำให้คอมพิวเตอร์หยุดทำงาน

4. ม้าโทรจัน (Trojan horse)

โปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ โดยส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนาไปใช้ในการเจาะระบบ และเพื่อโจมตีคอมพิวเตอร์, เซิร์ฟเวอร์, หรือระบบเครือข่ายอีกที ซึ่งเป็นที่รู้จักกันในชื่อการโจมตีเพื่อ "ปฏิเสธการให้บริการ" (Denial of Services)



5. สปายแวร์ (Spyware)

ประเภทโปรแกรมคอมพิวเตอร์ที่บันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์ และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม ซึ่งส่วนใหญ่แล้วบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึง และส่งไปยังบริษัทโฆษณาต่างๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต

6. ประตูหลัง (Backdoor)

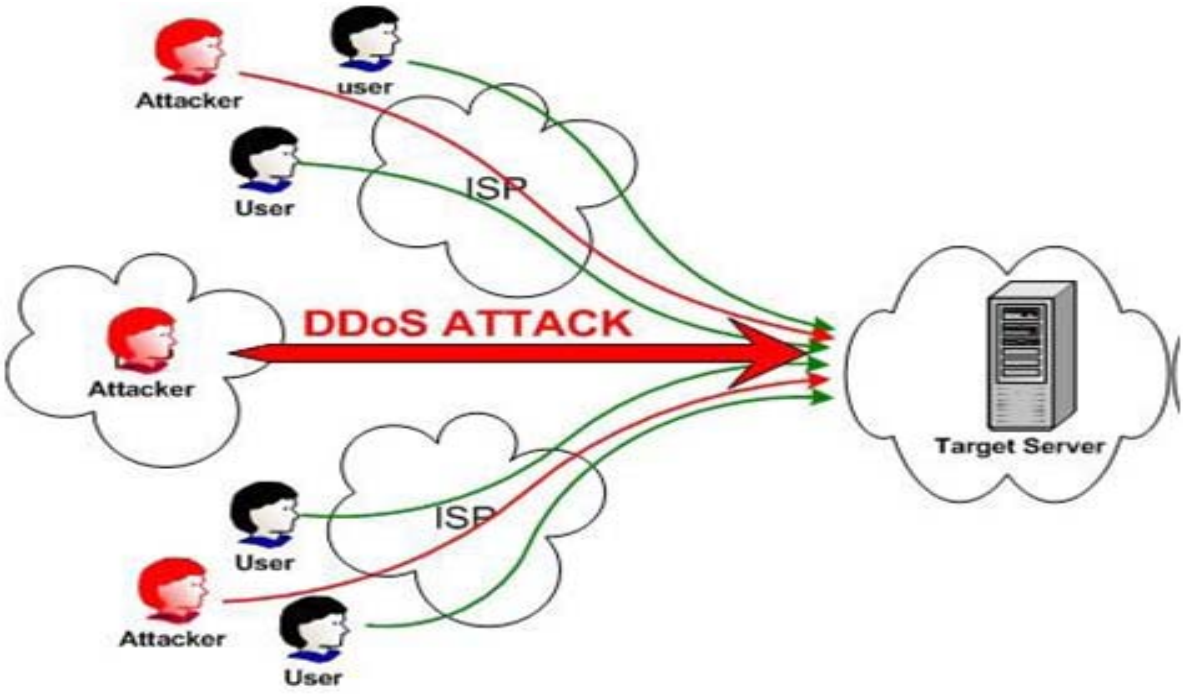
รูรั่วของระบบรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ ที่ผู้ออกแบบหรือผู้ดูแลระบบจงใจทิ้งไว้ โดยเป็นกลไกลลับทางซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้ข้ามผ่านการควบคุมความมั่นคงปลอดภัย แต่อาจเปิดทางให้ผู้ไม่ประสงค์ดีสามารถเข้ามาในระบบและก่อความเสียหายได้

7. Rootkit

โปรแกรมที่ออกแบบมาเพื่อซ่อนอ็อบเจ็กต์ต่างๆ เช่น กระบวนงาน ไฟล์ หรือข้อมูล แม้จะเป็นโปรแกรมที่อาจไม่เป็นอันตรายเสมอไป แต่ก็ถูกนำมาใช้ในการซ่อนกิจกรรมที่เป็นอันตรายมากขึ้นในปัจจุบัน ทำให้คอมพิวเตอร์ใดๆ สามารถส่งสแปมหรือทำการโจมตีคอมพิวเตอร์เครื่องอื่นๆ ได้โดยที่ผู้ใช้เป้าหมายไม่สามารถล่วงรู้และโปรแกรมด้านความปลอดภัยทั่วไปไม่สามารถตรวจจับได้

8. การโจมตีแบบ DoS/DDoS

ความพยายามโจมตีเพื่อทาให้เครื่องคอมพิวเตอร์ปลายทางหยุดทางาน หรือสูญเสียเสถียรภาพ หากเครื่องต้นทาง (ผู้โจมตี) มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากผู้โจมตีมีมากและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS) ด้วยเทคโนโลยีที่ก้าวล้าในปัจจุบัน ซึ่งมีภัยคุกคามมากมาย และแพร่กระจายอย่างรวดเร็ว ทาให้ปัจจุบันการโจมตีส่วนใหญ่ในโลกออนไลน์ มักเป็นการโจมตีแบบ DDoS



9. BOTNET

ภัยคุกคามทางเครือข่ายคอมพิวเตอร์ ด้วยมัลแวร์ทั้งหลายที่กล่าวในตอนต้นต้องการตัวนำทางเพื่อต่อยอดความเสียหาย และทำให้ยากแก่การควบคุมมากขึ้น ตัวนำทางที่ว่านี้ก็คือ Botnet ซึ่งก่อให้เกิดภัยคุกคามที่ไม่สามารถเกิดขึ้นได้เอง เช่น Spam, DoS/DDoS และ Phishing เป็นต้น

10. Spam Mail

หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล์ เช่น hotmail, yahoo ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

11. Phishing

คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สาคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิตโดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทาให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น มักจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing แผลงมาจากคำว่า fishing แปลว่าการตกปลา ซึ่งมีความหมายถึง การปล่อยให้ปลามากินเหยื่อที่ล่อไว้

12. Sniffing

เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่นักโจมตีระบบนิยมใช้

13. ข้อมูลขยะ (Spam)

ภัยคุกคามส่วนใหญ่ที่เกิดจากอีเมล์หรือเรียกว่า อีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับโดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่างๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti-spam หรือใช้บริการคัดกรองอีเมล์ของเว็บไซต์ที่ให้บริการอีเมล์ หลายคนอาจจะสงสัยว่า spammer รู้อีเมล์เราได้อย่างไร คำตอบคือได้จากเว็บไซต์ ห้องสนทนา ลิสต์รายชื่อลูกค้า รวมทั้งไวรัสชนิดต่างๆ ที่เป็นแหล่งรวบรวมอีเมล์และถูกส่งต่อกันไปเป็นทอดๆ ซึ่งหากจำเป็นต้องเผยแพร่อีเมล์ทางอินเทอร์เน็ตโดยป้องกันการถูกค้นเจอจาก Botnet สามารถทำได้โดยเปลี่ยนวิธีการสะกดโดยเปลี่ยนจาก “@” เป็น “at” แทน

14. Hacking

เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ ไม่ว่าจะกระทำด้วยมนุษย์ หรือ อาศัยโปรแกรมแฮก หลากรูปแบบ ที่หาได้ง่ายในโลกอินเทอร์เน็ต แถมยังใช้งานได้ง่าย ไม่ต้องเป็นผู้เชี่ยวชาญในคอมพิวเตอร์ก็สามารถเจาะระบบได้ จึงควรที่ผู้ใช้งานอินเทอร์เน็ตจะเฝ้าระวังและป้องกันตนเองให้ปลอดภัย

15. ผู้บุกรุก (Hacker)

หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก ดังนั้น องค์กรส่วนใหญ่ที่ใช้อินเทอร์เน็ตจึงให้ความสำคัญกับมาตรการป้องกัน Hacker

<u>ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไวรัสคอมพิวเตอร์ สปายแวร์</u>

1. ตรวจสอบซอฟต์แวร์ที่ใช้งานปลอดภัยหรือยัง

2. การแชร์ไฟล์ และการรับ-ส่งไฟล์ต่างๆ

3. การสำรองข้อมูล

๔. ติดตามข่าวสารต่างๆ

4. เช็คที่มาที่ไปของไฟล์ที่จะดาวน์โหลดมาจากอินเตอร์เน็ต และควรทำการแสกนไวรัสทุกครั้ง

5. หลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่มาที่ไม่ใช่เว็บไซต์ ที่เราไม่รู้จัก

6. หมั่นอัพเดทโปรแกรมป้องกันไวรัสอย่างสม่าเสมอ เพราะไวรัส สปายแวร์ มีการปรับปรุงและเกิดใหม่อยู่เสมอ

7. หมั่นทำการ backup สำรองข้อมูล สำรองไฟล์ที่สำคัญบ่อยๆ ซึ่งอาจจะเขียนลง CD,DVD หรือใส่ External HD สารองก็ได้

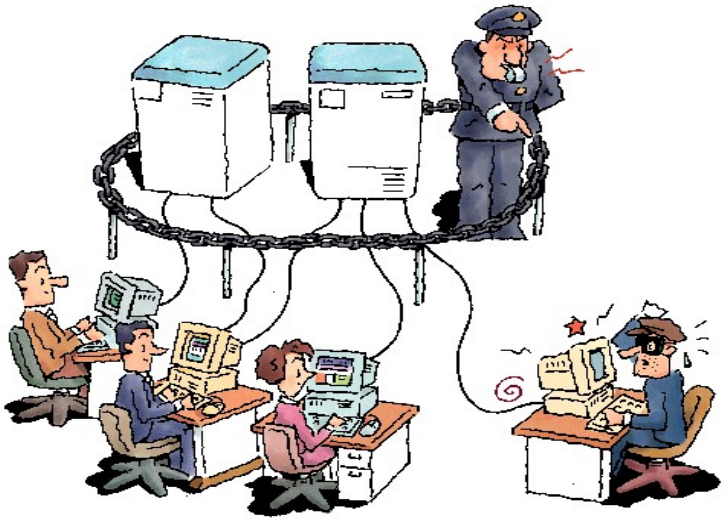
8. หมั่นอัพเดทวินโดวส์หรือระบบปฏิบัติการที่เราใช้ รวมไปถึงโปรแกรมเบราเซอร์และโปรแกรมเมล์ไครเอนต์

9. ให้รอบคอบอย่าประมาทในการทำธุรกรรมใดๆผ่านอินเตอร์เน็ต

10. ห้ามเปิดข้อความ หรือคลิกลิงค์ใดๆ ที่ส่งผ่านมาทางโปรแกรมสื่อสังคมออนไลน์ (Social Media) ที่เราไม่รู้จักที่มาหรือคนที่ส่งมาหาเรา

11. หมั่นตรวจสอบการทำธุรกรรมทางอินเตอร์เน็ต เช่น การจับจ่าย ซื้อของผ่านเน็ต หรือการจ่ายค่าสาธารณูปโภคต่างๆ รวมไปถึงดูรายงาน statement การเข้า - ออก ของเงินหรือเครดิต เพราะถ้าหากเกิดปัญหาใดๆ จะได้แก้ไขได้ทันท่วงที

แนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต



เมื่อได้ทำความรู้จักกับภัยคุกคามรูปแบบต่างๆ แล้ว จึงขอสรุป 10 วิธีป้องกันภัยคุกคามทางอินเทอร์เน็ต สำหรับการใช้งานส่วนบุคคล

1. ตั้งสติก่อนเปิดเครื่องก่อน Login เข้าใช้งานคอมพิวเตอร์ ต้องมั่นใจว่าไม่มีใครแอบดู Password เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ ควรล็อคหน้าจอให้อยู่ในสถานะที่ต้องใส่ค่า Login อย่าประมาทในการใช้งานอินเทอร์เน็ต ตระหนักไว้ว่าข้อมูลความลับ อาจถูกเปิดเผยได้เสมอในโลกออนไลน์

2. กำหนด Password ที่ยากแก่การคาดเดาควรมีความยาวไม่ต่ากว่า 8 ตัวอักษร และใช้อักขระพิเศษ ไม่ตรงกับความหมายในพจนานุกรมเช่น ASDFG@# เพื่อให้เดาได้ยากมากขึ้นและการใช้งานอินเทอร์เน็ตทั่วไป เช่น การ Login ระบบ e-mail ระบบสนทนาออนไลน์ (Chat) หรือระบบเว็บไซต์ที่เราเป็นสมาชิกอยู่ ทางที่ดีควรใช้ Password ที่ต่างกันบ้างพอให้จำได้ หรือมีเครื่องมือช่วยจำ Password เข้ามาช่วย

3. สังเกตขณะเปิดเครื่องสังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์รัน มาพร้อมๆ กับการเปิดเครื่องหรือไม่ ถ้าดูไม่ทัน ให้ สังเกตระยะเวลาบูตเครื่อง หากนานผิดปกติ อาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือปัญหาอื่นๆได้

4. หมั่นตรวจสอบและอัพเดทระบบปฏิบัติการ (Operating System) เช่น Window ซอฟต์แวร์ที่ใช้มั่นตรวจสอบและอัพเดต OS หรือซอฟต์แวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่อง เช่น โปรแกรมป้องกันไวรัส หรือโปรแกรมไฟร์วอลล์ และควรใช้ระบบปฏิบัติการ และซอฟต์แวร์ที่มีลิขสิทธิ์ นอกจากนี้ควรอัพเดตอินเทอร์เน็ตบราวเซอร์ให้ทันสมัยอยู่เสมอ เนื่องจาก Application Software สมัยใหม่มักพึ่งพาอินเทอร์เน็ตบราวเซอร์ ก่อให้เกิดช่องโหว่ใหม่ ๆ

5. ไม่ลงซอฟต์แวร์มากเกินจำเป็นเช่น Internet Browser E-Mail โปรแกรมทางด้านเอกสาร ตกแต่งภาพ เสียง วีดีโอ โปรแกรมป้องกันไวรัส และโปรแกรมไฟร์วอลล์ เป็นต้น

6. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เช่น เว็บไซต์ลามกอนาจาร เว็บไซต์การพนัน เว็บไซต์แนบไฟล์ .EXEเว็บไซต์ที่ Pop-up หลายเพจ เว็บไซต์ที่มี Linkไม่ตรงกับชื่อ

7. สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการ ธุรกรรมออนไลน์Web e-Commerce ที่ปลอดภัยควร มีลักษณะดังนี้ มีการทำ HTTPS เนื่องจาก HTTPS จะมีการเข้ารหัสข้อมูล มีใบรับรองทางอิเล็กทรอนิกส์ CA (Certificate Authority) เช่น https://www.facebook.com

8. ไม่เปิดเผยข้อมูลส่วนตัวผ่าน Social Network เลขที่บัตรประชาชน หนังสือเดินทาง ประวัติการทำงาน เบอร์โทรศัพท์ส่วนตัว ข้อมูลทางการแพทย์ หมายเลขบัตรเครดิต

9. ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้อินเทอร์เน็ต ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเทอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยไม่ส่งต่อภาพลามกอนาจร ภาพที่ตัดต่อทำให้ผู้อื่นได้รับความเสียหายอับอาย

10. ไม่หลงเชื่อโดยง่ายอย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเทอร์เน็ต ควรหมั่นศึกษาหาความรู้จากเทคโนโลยีอินเทอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนเชื่อในสิ่งที่ได้รับรู้

<u>แนวทางแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงาน</u>

7. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล

8. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS

9. แจ้งเจ้าหน้าที่ของหน่วยงานและพนักงาน ให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนหรือไม่รับเมลแนบจากคนที่ไม่รู้จัก , ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่างๆ หรือช่องทาง Social Network ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์

10. หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง 30 วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

11. ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน หรือตามที่กฎหมายกำหนด

12. หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามไซเบอร์มายัง**ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย** : ThaiCERT (ไทยเซิร์ต)

<u>แนวทางแนวทางป้องกันภัยคุกคามทางอินเทอร์เน็ต เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ใช้อินเทอร์เน็ตทั่วไป</u>

4. เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม เว็บผิดกฎหมาย ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกัน หรือไม่รู้จักกันมาก่อน ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชตต่างๆ หรือช่องทาง Social Media เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งนับวันมัลแวร์มาจากพวกไฟล์แนบ ทาง Social Network เพิ่มมากขึ้น

5. การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮกเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่น ๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

6. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจน ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

****

2.4 ประโยชน์ที่ได้รับจากการจัดทำองค์ความรู้

1. ช่วยเพิ่มประสิทธิภาพขององค์กร
2. ป้องกันการสูญหายของความรู้ ในกรณีที่บุคคลากรเกษียณอายุ ลาออก หรือเสียชีวิต
3. เพิ่มศักยภาพในการดำเนินงานด้านเทคโนโลยีสารนเทศและการสื่อสาร
4. มีการพัฒนาความสามารถที่จะแบ่งปันความรู้ที่ได้เรียนรู้มาให้กับคนอื่นๆ ในองค์กร และนำความรู้ไปปรับใช้กับงานที่ทำอยู่ให้เกิดประสิทธิผลมากยิ่งขึ้น
5. ช่วยเพิ่มขีดความสามารถในการตัดสินใจและวางแผนดำเนินงานให้รวดเร็ว และดีขึ้น เพราะมีสารสนเทศ หรือแหล่งความรู้เฉพาะที่มีหลักการ เหตุผล และน่าเชื่อถือช่วยสนับสนุนการตัดสินใจ
6. เมื่อพบข้อผิดพลาดจากการปฏิบัติงาน ก็สามารถหาวิธีแก้ไขได้ทันท่วงที
7. บุคลากรในองค์ มีความรู้ด้านการป้องกันภัยคุมคามทางคอมพิวเตอร์

2.5 ปัญหาและอุปสรรค

-

2.6 ข้อเสนอแนะ

การนำระบบสารสนเทศเข้ามาใช้จึงต้องเพิ่มในเรื่องของระบบการรักษาความปลอดภัยของข้อมูลควบคู่ไปด้วยอย่างหลีกเลี่ยงไม่ได้ การเสริมสร้างความรู้เกี่ยวกับกระบวนการป้องกัน และตรวจสอบการเข้าใช้งานเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต ขั้นตอนการป้องกันจะช่วยให้ ผู้ที่ใช้งานสกัดกั้นไม่ให้เทคโนโลยีสารสนเทศต่าง ๆ ถูกเข้าใช้งานโดยผู้ที่ไม่ได้รับสิทธิ์ ส่วนการตรวจสอบทำให้ทราบได้ว่ามีใครกำลังพยายามที่จะบุกรุก เข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ ผู้บุกรุก ทำอะไรกับระบบบ้าง รวมทั้งการป้องกันจากภัยคุกคาม (Threat) ต่างๆ อาชญากรรมคอมพิวเตอร์ การกระทำที่ผิดต่อกฎหมายโดยการใช้คอมพิวเตอร์ หรือทำลายคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่น จึงมีความสำคัญต่อผู้ใช้งานและผู้ดูแลระบบคอมพิวเตอร์เป็นอย่างมาก อีกทั้งการ Update ข้อมูลเกี่ยวกับภัยคุมคามทางคอมพิวเตอร์ให้ทันสมัย ก้าวทันต่อยุคของโลกแห่งดิจิทัลต่อไป