เอกสารรวบรวมความรู้เพื่ออ่านประกอบการสอนวิชา CP101

โดย อาจารย์สาโรช เมาลานนท์

บทเรียน ที่ 12 การรักษาความปลอดภัยคอมพิวเตอร์ที่ใช้งานบนเครือข่าย

การรักษาความปลอดภัยคอมพิวเตอร์

ในปัจจุบันการใช้งานคอมพิวเตอร์เป็นสิ่งจำเป็นสำหรับทุกองค์กร การเชื่อมโยงถึงกันของคอมพิวเตอร์ให้เป็นเครือข่าย และการเชื่อมต่อสู่อินเทอร์เน็ตกลายเป็นสิ่งจำเป็นสำหรับมนุษย์ โดยเฉพาะในสังคมเมืองที่จะขาดเสียไม่ได้ การใช้คอมพิวเตอร์และเครือข่ายไม่ได้จำกัดอยู่เฉพาะภายในองค์กรใหญ่ๆ เท่านั้น แต่ได้ขยายตัวเข้าไปในหน่วยงานทุกขนาด และกำลังขยายตัวเข้าไปยังบ้านพักอาศัยด้วย เทคโนโลยีสารสนเทศและการสื่อสารกำลังกลายเป็นสิ่งแวดล้อมที่สำคัญสิ่งหนึ่งของมนุษย์

เนื่องจาก สิ่งที่มีค่ามากที่สุดของระบบคอมพิวเตอร์ คือ ข้อมูลและสารสนเทศ ดังนั้น ถ้าข้อมูลถูกจารกรรม ถูกปรับเปลี่ยน ถูกเข้าถึงโดยเจ้าของไม่รู้ตัว ถูกปิดกั้นขัดขวางให้ไม่สามารถเข้าถึงข้อมูลได้ หรือถูกทำลายเสียหายไป สิ่งต่าง ๆ เหล่านี้เป็นเรื่องที่จะสามารถเกิดขึ้นได้อย่างไม่ยากบนโลกของเครือข่าย โดยเฉพาะเมื่ออยู่ออนไลน์บนอินเทอร์เน็ต ดังนั้นสิ่งที่จะต้องคำนึงถึงเรื่องหนึ่ง คือ การรักษาความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ในทุกๆ เครื่อง รวมถึงการรักษาไว้ซึ่งข้อมูลส่วนตัวของแต่ละบุคคล ที่ทุกๆ คนจำเป็นจะต้องมีความรู้ ความเข้าใจ ให้สามารถป้องกันผู้ประสงค์ร้ายที่มีอยู่ทั่วไปบนเครือข่ายคอมพิวเตอร์ รวมทั้งความเสียหายที่อาจเกิดจากการรู้เท่าไม่ถึงการณ์ของตัวเองด้วย

องค์ประกอบด้านความปลอดภัยของข้อมูล

หลักการสำคัญที่ใช้เป็นแนวทางในการพิจารณาถึงคุณสมบัติด้านความปลอดภัยของข้อมูลที่จะต้องคำนึงถึงซึ่งประกอบด้วยองค์ประกอบ 3 ด้าน นิยมเรียกกันเป็นชื่อย่อว่า CIA มี ดังนี้

1. ความลับ (Confidentiality) หมายถึง การรักษาไว้ซึ่งความลับของข้อมูลตามที่ควรจะเป็น ซึ่งหมายรวมถึงการทำให้ข้อมูลสามารถเข้าถึงได้ หรือเปิดเผยได้ เฉพาะผู้มีสิทธิที่ได้รับอนุญาตเท่านั้น และหากเป็นข้อมูลส่วนบุคคลองค์กรจะต้องธำรงไว้ซึ่งความเป็นส่วนบุคคล (Privacy)

2. ความคงสภาพ (Integrity) หมายถึง การดำรงรักษาไว้ซึ่งความถูกต้องของข้อมูล ถึงแม้ว่าข้อมูลจะต้องส่งผ่านเครือข่ายคอมพิวเตอร์ไปยังอีกที่หนึ่ง การทำให้ข้อมูลมีความน่าเชื่อถือจะต้องประกอบด้วย 2 ส่วน คือ ข้อมูลนั้นไม่ถูกแก้ไขจากแหล่งเดิมที่มา และความหน้าเชื่อถือของแหล่งที่มา

3. ความพร้อมใช้งาน (Availability) หมายถึง ระบบและกลไกต่างๆ ต้องพร้อมใช้งาน เพื่อให้สามารถเข้าถึงข้อมูลได้เมื่อต้องการภายในเงื่อนไขที่ได้กำหนดไว้

ในระบบงานที่สำคัญจำเป็นต้องมีระบบงานย่อยเพื่อดูแลจัดการในด้านการรักษาความปลอดภัยของข้อมูลในระบบ ตัวอย่างเช่น การพิสูจน์ทราบตัวตนของผู้ใช้ การตรวจสอบสิทธิ์การใช้งาน และความสามารถในการตรวจสอบได้ ยกตัวอย่างเช่น นิสิตได้รับบัวศรีไอดี ซึ่งประกอบด้วยยูสเซอร์เนม (Username) และรหัสผ่าน (Password) โดยบัวศรีไอดีนี้จะเป็นการระบุตัวตนของนิสิตแต่ละคน (Identification) นิสิตจะใช้บัวศรีไอดีในการเข้าใช้ระบบงานต่าง ๆ เช่น ระบบเว็บอีเมลของมหาวิทยาลัย ระบบ SUPREME2004 เพื่อลงทะเบียนเรียนและดูผลการเรียน เป็นต้น

- การพิสูจน์ทราบตัวตน (Authentication) ระบบพิสูจน์ทราบตัวตนเป็นกลไกที่ใช้ตรวจสอบผู้ใช้ที่ต้องการล็อกอินเข้าใช้งานระบบหรือเครือข่าย ในการตรวจสอบเพื่อพิสูจน์ทราบนั้นอาจใช้ยูสเซอร์เนมและรหัสผ่าน หรือสมาร์ทการ์ด (Smart cards) หรือระบบไบโอเมติก (Biometrics) เช่น การสแกนลายนิ้วมือ การสแกนม่านตา เป็นต้น ก็ได้ ทุกระบบที่สำคัญจำเป็นต้องมีระบบพิสูจน์ตัวตน ดังนั้น ผู้ใช้แต่ละคนก็จำเป็นต้องมีความรู้ความเข้าใจในการเข้าใช้งานระบบนี้ รวมถึงการดูแลรักษาสิ่งที่ใช้ระบุตัวตนของเราอย่างดี ทั้งในปัจจุบันได้มีกฎหมายเป็นพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มีผลบังคับใช้เมื่อ 18 กรกฎาคม 2550 ได้ระบุโทษสำหรับบุคคลที่พยายามเข้าใช้งานระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตนต้องระวางโทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

- การตรวจสอบสิทธิ์การใช้งาน (Authorization) หลังจากที่ผ่านการพิสูจน์ทราบตัวตนแล้ว ขั้นตอนต่อไปจะเป็นการตรวจสอบสิทธิ์ของผู้เข้าใช้ ว่าได้มีการกำหนดสิทธิ์ให้เข้าใช้งานได้ในระดับไหน มีการกำหนดระดับชั้นความลับเพื่อให้ผู้ใช้มีความสามารถในการเข้าถึงที่ชั้นความลับแตกต่างกันตามบทบาทหน้าที่ของแต่ละคน และมีการกำหนดสิทธิ์ในการ

ดำเนินการกับข้อมูลอย่างไรได้บ้าง เช่น การเข้าถึงหรืออ่าน การเขียน การแก้ไข หรือการลบข้อมูล

- การตรวจสอบได้ (Accountability) ในทุกระบบงานจำเป็นจะต้องมีความสามารถในการตรวจสอบการเข้าใช้งานระบบของผู้ใช้ เช่น การเก็บล็อก (logs) ซึ่งเป็นการจัดเก็บเวลาและกิจกรรมต่างๆ ที่ผู้ใช้แต่ละคนเข้าใช้งานในระบบ ซึ่งในปัจจุบันตามกฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ได้กำหนดให้ผู้ให้บริการ จะต้องจัดเก็บข้อมูลการจราจรบนเครือข่ายไว้ สำหรับให้เจ้าพนักงานตามกฎหมายตรวจสอบได้ เมื่อมีการกระทำความผิดเกิดขึ้น และหากไม่มีสิ่งนี้ให้ตรวจสอบ ก็ถือเป็นความผิดของผู้ให้บริการซึ่งมีการระวางโทษไว้แล้วด้วย

ภัยคุกคาม (Threat)

ภัยคุกคาม หมายถึง สิ่งที่อาจก่อให้เกิดความเสียหายต่อคุณสมบัติด้านความปลอดภัยของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ตามที่ได้กล่าวไว้ข้างต้น การกระทำที่อาจก่อให้เกิดการเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายเราจะเรียกว่าการโจมตี (Attack) ผู้โจมตี (Attacker) เราเรียกว่า **แฮคเกอร์ (Hacker)** ซึ่งใช้ในความหมายสำหรับผู้โจมตีที่มิได้ประสงค์ร้ายต่อเป้าหมาย ส่วนผู้โจมตีทีประสงค์ร้ายโดยก่อให้เกิดวามเสียหายต่อเป้าหมายเราจะเรียกว่า **แคร็คเกอร์ (Cracker)** โดยสามารถแบ่งภัยคุกคามที่อาจเกิดขึ้นได้เป็น 4 ประเภท คือ

1. การเปิดเผย (Disclosure) คือ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือข้อมูลนั้นถูกเปิดเผยให้กับผู้ที่ไม่ได้รับอนุญาต
2. การหลอกลวง (Deception) คือ การให้ข้อมูลที่เป็นเท็จ
3. การขัดขวาง (Disruption) คือ การทำลายข้อมูล หรือกันไม่ให้กระทำต่อข้อมูลอย่างถูกต้อง
4. การควบคุมระบบ (Usurpation) การควบคุมบางส่วนหรือทั้งระบบโดยไม่ได้รับอนุญาต

เนื่องจากภัยคุกคามมีความหลากหลาย การทำความเข้าใจพื้นฐานกับภัยคุกคามประเภทต่างๆ จะทำให้เข้าใจระบบการรักษาความปลอดภัยมากขึ้น ตัวอย่างของภัยคุกคามที่อาจเกิดขึ้นได้ ดังนี้

- การสอดแนม (Snooping) บางครั้งใช้คำว่า สนิฟฟิง (Sniffing) หมายถึง การดักเพื่อแอบดูข้อมูล จัดอยู่ในภัยคุกคามประเภท การเปิดเผย การสอดแนมเป็นการโจมตีแบบพาสซีฟ

(Passive) คือ เป็นการกระทำที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล ตัวอย่างเช่น การดักอ่านข้อมูลในระหว่างที่ส่งผ่านเครือข่าย หรือการอ่านไฟล์ที่จัดเก็บอยู่ในระบบ แพ็กเก็ตสนิฟเฟอร์ (Packet Sniffer) เป็นรูปแบบหนึ่งของการโจมตีแบบสอดแนม ลักษณะของการโจมตีแบบนี้ เนื่องจากข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกตัดแบ่งออกเป็นส่วนย่อยๆ เรียกว่า แพ็กเก็ต (Packet) และโดยปกติจะอยู่ในลักษณะที่เรียกว่า Clear Text คือ เป็นตัวอักษรตามจริง ดังนั้นหากข้อมูลในแพ็กเก็ต ณ ขณะนั้นเป็นยูสเซอร์เนมและรหัสผ่าน หากดักจับไปได้ก็จะสามารถทราบความลับของรหัสผ่านได้ และสิ่งที่ควรทราบไว้ คือ โปรแกรมแพ็กเก็ตสนิฟเฟอร์มีให้ดาวน์โหลดกันบนอินเทอร์เน็ต วิธีการแก้ปัญหาเพื่อป้องกันภัยคุกคามประเภทนี้ได้แก่การรักษาความลับของข้อมูลโดยการเข้ารหัสลับข้อมูล (Encryption) ที่ต้นทาง และทำการถอดรหัสลับข้อมูลกลับที่ปลายทาง

- การเปลี่ยนแปลงข้อมูล (Modification) หมายถึง การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต จัดอยู่ในภัยคุกคามประเภท การหลอกลวง การเปลี่ยนแปลงข้อมูลเป็นการโจมตีแบบแอ็คทีฟ (Active) ตัวอย่างเช่น การโจมตีแบบผ่านคนกลาง (Man-in-the-middle attack) ซึ่งผู้บุกรุกดักข้อมูลจากผู้ส่งระหว่างทาง แล้วทำการแก้ไขก่อนส่งต่อไปให้ผู้รับ วิธีการแก้ปัญหาเพื่อป้องกันภัยคุกคามประเภทนี้ได้แก่การใช้โปรแกรมที่มีความสามารถในการรักษาความคงสภาพของข้อมูล (Integrity) ซึ่งเมื่อข้อมูลไปถึงปลายทางหากมีการเปลี่ยนแปลงโปรแกรมนี้ที่ปลายทางจะแจ้งให้ทราบได้

- การปลอมตัว (Spoofing) หมายถึง การทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นอีกบุคคลหนึ่ง จัดอยู่ในภัยคุกคามประเภท การหลอกลวง ตัวอย่างเช่น การปลอมอีเมลของผู้ส่งเพื่อให้ผู้รับเข้าใจผิด การปลอมแปลงอีเมลมักมีวัตถุประสงค์ที่จะหลอกให้เหยื่อกระทำการที่อาจก่อให้เกิดความเสียหาย หรือบอกข้อมูลที่มีความสำคัญออกมา เช่น รหัสผ่านหรือข้อมูลส่วนตัว นอกจากนี้ก็อาจเป็น การปลอมหมายเลขไอพีแอดเดรสให้เป็นเครื่องคอมพิวเตอร์ที่เชื่อถือได้ เพื่อหลอกให้เหยื่อเข้ามาดำเนินการบนเครื่องดังกล่าว แล้วล้วงเอาความลับของผู้ใช้ไป

- การโจมตีเพื่อให้เกิดการปฏิเสธการให้บริการ (Denial of Service) เรียกเป็นคำย่อว่า DoS หมายถึง การขัดขวางการให้บริการของเซิร์ฟเวอร์ โดยการทำให้มีการใช้ทรัพยากรของเซิร์ฟเวอร์จนหมดหรือถึงขีดจำกัดของมัน ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ หรือ อีเมลเซิร์ฟเวอร์ การโจมตีจะทำโดยการเปิดการเชื่อมต่อกับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้

ผู้ใช้คนอื่นๆ ไม่สามารถเข้ามาใช้บริการได้ การโจมตีอาจมุ่งไปที่การทำให้ประสิทธิภาพของเครือข่ายลดลงโดยการส่งแพ็กเก็ตขยะจำนวนมากเข้าไปในเครือข่าย ปัจจุบันมีการโจมตีแบบแยกกระจาย เรียกย่อว่า DDoS (Distributed Denial of Service) โดยใช้คอมพิวเตอร์หลายแสนเครื่องเพื่อโจมตีเป้าหมายเดียวกัน โดยขั้นตอนแรกจะมีการปล่อยเวิร์มไปฝังตัวในเครื่องต่างๆ ที่อยู่บนอินเทอร์เน็ต เครื่องเหล่านี้จะถูกเรียกว่า ซอมบี้ (Zombie) เมื่อถึงเวลาที่กำหนดซอมบี้ก็จะโจมตีพร้อมกันไปยังเครื่องเป้าหมาย การโจมตีแบบนี้ทำให้ยากต่อการป้องกันและหยุดยั้งการโจมตี

- โปรแกรมประสงค์ร้าย (Malicious program) หรือเรียกย่อๆ ว่า มัลแวร์ (malware) เป็นโปรแกรมที่ถูกสร้างขึ้นมาเพื่อทำการก่อกวน ทำลาย หรือทำความเสียหายกับระบบคอมพิวเตอร์และเครือข่าย โปรแกรมประสงค์ร้ายในปัจจุบันที่แพร่หลายมี 3 ประเภท คือ ไวรัส เวิร์ม และม้าโทรจัน ความเป็นมาของโปรแกรมประสงค์ร้ายที่พอจะสืบสาวได้นับแต่ปี พ.ศ. 2526 นายเฟร็ด โคเฮน (Fred Cohen) ได้บันทึกว่ามีโปรแกรมขนาดเล็กบางตัวสามารถสำเนาตัวเองจากโปรแกรมหนึ่งไปยังอีกโปรแกรมหนึ่ง และเรียกโปรแกรมลักษณะแบบนี้ว่า ไวรัสคอมพิวเตอร์ และเขาเป็นคนแรกที่เขียนเอกสารทางวิชาการเรื่องไวรัสคอมพิวเตอร์ในปี พ.ศ. 2530 (Cohen, F., 1987. "Computer Viruses Theory and Experiments," Computers and Security, vol. 6, pp. 22--35.) (ข้อมูลจาก http://en.wikipedia.org/wiki/Computer_virus#History และ http://en.wikipedia.org/wiki/Fred_Cohen ค้นเมื่อวันที่ 31 สิงหาคม พ.ศ. 2550) จากนั้นไวรัสคอมพิวเตอร์ก็มีเพิ่มมากขึ้น แต่ไม่ได้กระทบกับผู้คนส่วนใหญ่ที่ไม่ได้อยู่ในแวดวงคอมพิวเตอร์ ในปี พ.ศ. 2542 ไวรัสคอมพิวเตอร์ชื่อ Melissa ทำความเสียหายโดยตรงต่อเครือข่ายอินเทอร์เน็ต โดยการแพร่ตัวเองไปอย่างรวดเร็วผ่านเครือข่ายอินเทอร์เน็ต จากนั้นมาคนทั่วไปเริ่มตระหนักถึงภัยคุกคามจากไวรัสคอมพิวเตอร์ พร้อมกันนั้นไวรัสคอมพิวเตอร์ก็เริ่มมีความซับซ้อนมากยิ่งขึ้น มัลแวร์ที่มีความร้ายแรงทวีจำนวนมากขึ้น นับแต่ Code Red, Nimda, MyDoom และ SQL Slammer

- สแปม (Spam) คือ การส่งอีเมลไปยังผู้ใช้จำนวนมาก โดยมีจุดประสงค์เพื่อการโฆษณา สแปมจัดอยู่ในสิ่งที่ก่อให้เกิดความรำคาญไม่ใช่มัลแวร์ อย่างไรก็ตามการส่งสแปมเมลจำนวนมหาศาลในปัจจุบันได้สร้างความเสียหายให้เกิดขึ้นกับองค์กรที่ต้องเสียค่าใช้จ่ายในการจัดเก็บข้อมูลอีเมลขยะในเมลเซิร์ฟเวอร์ เสียแบนด์วิดธ์จำนวนมากในเครือข่ายขององค์กรไปกับแพ็กเก็ตขยะ รวมทั้งทำให้คนในองค์กรต้องมาเสียเวลาจัดการกับอีเมลขยะที่

ไม่พึงประสงค์นี้ มีข้อมูลจาก http://en.wikipedia.org/wiki/E-mail_spam ค้นเมื่อวันที่ 31 สิงหาคม พ.ศ. 2550 แสดงจำนวนอีเมลขยะใน เดือนกุมภาพันธ์ พ.ศ. 2550 จำนวน 90 พันล้านฉบับต่อวัน

- สปายแวร์ (Spyware) คือ ซอฟต์แวร์ใดๆ ที่ใช้ช่องทางการเชื่อมต่อกับอินเทอร์เน็ตเพื่อแอบส่งข้อมูลส่วนตัวของผู้ใช้นั้นไปให้กับบุคคลหรือองค์กรหนึ่งโดยที่ผู้ใช้ไม่ทราบ สปายแวร์สามารถเข้าสู่เครื่องคอมพิวเตอร์ของผู้ใช้ได้โดยผ่านทางไวรัสคอมพิวเตอร์ เว็บเพจที่เข้าไปดู หรืออีเมลที่เปิดอ่าน

ปัญหาความปลอดภัยที่ใกล้ตัวเรา

ไวรัส เวิร์ม และโทรจันฮอร์ส

ไวรัส เวิร์ม และโทรจันฮอร์ส เป็นโปรแกรมอันตรายที่สามารถทำความเสียหายต่อเครื่องคอมพิวเตอร์ และข้อมูลในเครื่องคอมพิวเตอร์ ทำให้การเข้าใช้งานเครือข่ายหรืออินเทอร์เน็ตช้าลง และอาจใช้คอมพิวเตอร์ของเราในการแพร่กระจายตัวเอง ไปยังเพื่อนฝูง ครอบครัว เพื่อนร่วมงานของเรา จนถึงตลอดทั่วทั้งเว็บ แต่ถึงอย่างไรก็ตามหากเรามีความรู้ความเข้าใจถึงวิธีป้องกันเพียงเล็กน้อย รวมทั้งสามัญสำนึกที่ดี โอกาสที่นิสิตจะตกเป็นเหยื่อของภัยคุกคามเหล่านี้ก็จะลดน้อยลง รวมทั้งจะทำให้เครือข่ายที่เราใช้งานอยู่มีความมั่นคงปลอดภัย และพร้อมใช้งานอยู่ตลอดเวลา ในปัจจุบันเรารวมเรียกโปรแกรมประสงค์ร้ายที่ออกแบบมาเพื่อเจาะเข้าทำลาย หรือสร้างความเสียหายให้แก่ระบบคอมพิวเตอร์และเครือข่ายว่า **มัลแวร์** (Malware) หรือบางทีเรียกว่า มัลลิเชียสโค้ด (Malicious Code) มาทำความรู้จักภัยคุกคามที่ใกล้ตัวเราอย่างมากในปัจจุบัน

ไวรัส คือ โปรแกรมคอมพิวเตอร์ชุดหนึ่งที่ถูกสร้างขึ้นโดยผู้ประสงค์ร้าย ให้ฝังตัวเองในโปรแกรมหรือไฟล์หนึ่ง เพื่อที่จะแพร่กระจายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ โดยทำความเสียหายแก่เครื่องในขณะที่มันแพร่กระจาย ไวรัสสามารถสร้างความเสียหายให้แก่ซอฟต์แวร์ ฮาร์ดแวร์ และไฟล์ของเราได้ ความร้ายแรงของไวรัสคอมพิวเตอร์มีตั้งแต่ ก่อให้เกิดความรำคาญจนถึงขั้นทำความเสียหายอย่างร้ายแรง ซึ่งคล้ายกับไวรัสของคนที่มีความร้ายแรงมาก เช่น ไวรัส Ebola ไข้หวัดนก ลงมาถึงรุนแรงน้อย เช่น ไวรัสโรคหวัด เป็นต้น สำหรับไวรัสคอมพิวเตอร์ที่แท้จริงแล้วจะไม่สามารถแพร่กระจายได้เอง ต้องอาศัยการกระทำจากมนุษย์ เช่น การแบ่งปันการใช้ไฟล์ หรือเปิดอีเมลที่มีไวรัส เป็นการแพร่ขยายตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง

เวิร์ม มีลักษณะคล้ายไวรัส แต่มีความแตกต่างที่สำคัญคือเป็นโปรแกรมที่ถูกออกแบบมาเพื่อคัดลอกตัวเองจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งโดยอัตโนมัติ จากการเข้าควบคุม

คุณสมบัติบางอย่างของคอมพิวเตอร์ที่ใช้ส่งถ่ายไฟล์หรือข้อมูล เมื่อเวิร์มเข้ามาอยู่ในระบบของเราแล้ว จะสามารถแพร่กระจายด้วยตัวเองได้ สิ่งที่เป็นอันตรายที่สุดของเวิร์มก็คือ ความสามารถในการแพร่กระจายอย่างรวดเร็วได้เป็นจำนวนมาก ตัวอย่างเช่น เวิร์มสามารถส่งสำเนาของเวิร์มไปยังทุกคนที่มีรายชื่อในสมุดบันทึกอีเมลแอดเดรสของเรา และคอมพิวเตอร์ของเจ้าของรายชื่อเหล่านั้นก็จะดำเนินการเช่นเดียวกัน เกิดเป็นผลกระทบแบบต่อเนื่องจากการส่งข้อความในเครือข่ายอย่างหนักจนทำให้การทำงานของเครือข่ายช้าลง รวมทั้งมีผลต่ออินเทอร์เน็ตด้วย เมื่อมีการปล่อยเวิร์มออกมาใหม่ๆ เวิร์มจะแพร่กระจายอย่างรวดเร็ว ทำให้เครือข่ายติดขัด ต้องรอเป็นเวลานานในการเข้าเว็บเพจบนอินเทอร์เน็ต และเนื่องจากเวิร์มไม่ต้องอาศัยโปรแกรมที่เป็น "โฮสต์" หรือไฟล์ในการเคลื่อนย้ายตัวเอง จึงสามารถฝังตัวเองในระบบของเรา และทำให้ผู้อื่นสามารถเข้าควบคุมคอมพิวเตอร์ของเราจากระยะไกลได้ ตัวอย่างเช่น เวิร์ม MyDoom ที่เกิดขึ้นเมื่อเร็วๆ นี้ ได้รับการออกแบบมาให้เปิด "ประตูหลัง" ของระบบที่ติดเวิร์มดังกล่าว และใช้ระบบนั้นโจมตีเว็บไซต์ต่างๆ

โทรจันฮอร์สหรือม้าโทรจัน เป็นคำที่มาจากสงครามโทรจันระหว่างทรอยและกรีก ที่ชาวกรีกสร้างม้าเป็นโครงไม้ขนาดใหญ่ทิ้งไว้ โดยซ่อนทหารไว้ภายในแล้วถอยทัพกลับ พอชาวโทรจันออกมาดูเห็นม้าโครงไม้ทิ้งไว้ คิดว่าเป็นของขวัญที่ทหารกรีกทิ้งไว้ให้ จึงนำกลับเข้าเมืองไป ตกดึกทหารกรีกที่ซ่อนตัวอยู่ ก็ออกมาเปิดประตูเมืองให้ทหารกรีกเข้ามายึดกรุงทรอยได้สำเร็จ ม้าโทรจันในยุคปัจจุบันเป็นโปรแกรมคอมพิวเตอร์ที่ดูเหมือนเป็นซอฟต์แวร์ที่มีประโยชน์ แต่จริงๆ แล้วสามารถทำลายระบบการรักษาความปลอดภัย และสร้างความเสียหายได้อย่างมากมาย ม้าโทรจันปัจจุบันแฝงกายมาในรูปของอีเมลที่มีเอกสารแนบซึ่งอ้างว่าเป็นโปรแกรมปรับปรุงด้านการรักษาความปลอดภัยแต่กลับเป็นตัวทำลายซอฟต์แวร์ป้องกันไวรัสและไฟร์วอลล์ หรือม้าโทรจันอาจแฝงมากับซอฟต์แวร์ประเภทที่ให้เราดาวน์โหลดได้โดยไม่เสียค่าใช้จ่าย จึงไม่ควรดาวน์โหลดซอฟต์แวร์จากแหล่งที่มาซึ่งคุณไม่รู้จัก

การไม่เข้าใจเกี่ยวกับแพตช์ (Patch)

ยังเป็นที่เข้าใจกันไม่มากว่าซอฟต์แวร์ที่ถูกติดตั้งไว้ในเครื่องคอมพิวเตอร์ใดๆ โดยเฉพาะโปรแกรมระบบปฏิบัติ และโปรแกรมเว็บเบราเซอร์ หรือชุดออฟฟิค นั้น โดยปกติจะยังไม่มีความสมบูรณ์ มักจะมีจุดอ่อนหรือช่องโหว่ที่อาจค้นพบได้ในภายหลัง โดยเฉพาะช่องโหว่ทางด้านความปลอดภัยอันเป็นช่องทางให้ไวรัส หรือเวิร์ม สามารถโจมตี และเข้ามาติดตั้งอยู่ในเครื่องคอมพิวเตอร์ได้โดยผู้ใช้ไม่รู้ตัว บริษัทผู้ผลิตซอฟต์แวร์จะต้องมีทีมวิจัย เพื่อค้นหาช่องโหว่ทางด้านความปลอดภัย ซึ่งเมื่อค้นพบก็จะออกสิ่งที่ เรียกว่า แพตช์ ซึ่งจะเป็นซอฟต์แวร์ที่ใช้ปิดช่องโหว่ที่พบ เพื่อให้ผู้ใช้งาน

นำมาติดตั้งในเครื่องของตน ในปัจจุบันมีคำที่ใช้เรียกแพตช์อยู่หลายคำ เช่น Security Patch, Hotfix และ Service Pack (SP1, SP2) เป็นต้น ดังนั้นสำหรับในกรณีเครื่องคอมพิวเตอร์ที่แม้โปรแกรมป้องกันไวรัสจะตรวจพบและกำจัดไวรัสหรือเวิร์มออกไปได้ แต่หากยังไม่ได้ปิดช่องโหว่ไวรัสหรือเวิร์มตัวเดิมที่ใช้ช่องโหว่นี้ก็จะกลับเข้ามาอย่างไม่จบสิ้น อย่างไรก็ตามการจัดการเกี่ยวกับแพตช์ที่ผู้ใช้ต้องรู้ว่าจะต้องติดตั้งแพตช์ไหนบ้างกลายเป็นสิ่งที่ยากและซับซ้อน และการโจมตีที่สำเร็จในปัจจุบันโดยส่วนใหญ่นั้นเกิดจากการที่ผู้ใช้ไม่ได้ติดตั้งแพตช์ที่ได้ออกมานานแล้ว

การไม่รู้จักใช้ไฟร์วอลล์ส่วนบุคคล (Personal Firewall)

ไฟร์วอลล์จะเป็นอุปกรณ์พิเศษหรือเป็นซอฟต์แวร์ที่ติดตั้งบนเครื่องคอมพิวเตอร์เฉพาะ ในอดีตไฟร์วอลล์มีราคาแพงจึงใช้กันเฉพาะในองค์กรใหญ่ๆ โดยจะติดตั้งขวางอยู่ระหว่างเครือข่ายภายในขององค์กรกับเครือข่ายอินเทอร์เน็ต ทำหน้าที่ตรวจสอบข้อมูลที่วิ่งเข้าและออกจากเครือข่ายขององค์กรไปยังเครือข่ายอินเทอร์เน็ต ซึ่งเป็นสิ่งที่จำเป็นอย่างมากสำหรับองค์กรเพื่อรักษาความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์และเครือข่ายขององค์กร

สำหรับไฟร์วอลล์ส่วนบุคคลเป็นซอฟต์แวร์ที่สามารถติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัว ทำหน้าที่ช่วยป้องกันผู้บุกรุกเข้ามาในเครื่องคอมพิวเตอร์ของเรา ไฟร์วอลล์ทำงานโดยการตรวจสอบข้อมูลทั้งหมดที่เข้าหรือออกจากเครื่องคอมพิวเตอร์ของเรา และจะอนุญาตให้ผ่านไปได้ก็ต่อเมื่อตรวจสอบแล้วพบว่าไม่ละเมิดกับกฎเกณฑ์ของไฟร์วอลล์ที่กำหนดไว้ และหากมีการละเมิดกฎเกณฑ์ก็จะไม่อนุญาตให้ผ่านไป

เนื่องจากในปัจจุบันมีซอฟต์แวร์ไฟร์วอลล์ส่วนบุคคลออกมาหลายตัว และสำหรับระบบปฏิบัติการ Windows ทั้งแต่เวอร์ชั่น Windows XP เป็นต้นมา ได้มีการติดตั้งซอฟต์แวร์ไฟร์วอลล์ส่วนบุคคลมาให้แล้ว ดังนั้นผู้ใช้ที่ใช้ระบบปฏิบัติการดังกล่าว จึงสมควรอย่างยิ่งที่จะรู้จักการเปิดใช้งานซอฟต์แวร์ไฟร์วอลล์ส่วนบุคคล ทั้งนี้เพื่อเพิ่มความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ส่วนตัวของเรา และถึงแม้ว่าองค์กรของเราจะได้มีการติดตั้งไฟร์วอลล์ในระดับองค์กรอยู่แล้ว ก็ยังมีความจำเป็นที่จะต้องติดตั้งใช้งานไฟร์วอลล์ส่วนบุคคล เพราะเครือข่ายภายในองค์กรก็ยังคงมีผู้บุกรุกแอบแฝงตัวอยู่หลังไฟร์วอลล์ขององค์กรได้

แนวทางการป้องกันตัวให้ปลอดภัยจากภัยคุกคาม

แม้ว่าไวรัส เวิร์ม และม้าโทรจัน หรือภัยคุกคามอื่นๆ จะมีลักษณะที่แตกต่างกัน แต่มีวิธีการในการช่วยให้ปลอดภัยจากสิ่งอันตรายเหล่านี้ได้ ดังนี้

1. ติดตั้งโปรแกรมตรวจจับไวรัส ในปัจจุบันเครื่องคอมพิวเตอร์ทุกเครื่องที่ต่ออยู่กับเครือข่ายคอมพิวเตอร์ โดยเฉพาะเครือข่ายอินเทอร์เน็ต จำเป็นอย่างยิ่งที่จะต้องมีการติดตั้ง

โปรแกรมตรวจจับไวรัส ที่มีให้เลือกใช้หลายผลิตภัณฑ์ ในปัจจุบันโปรแกรมตรวจจับไวรัสจะมีทั้งประเภทที่ติดตั้งและดูแลเฉพาะเครื่องคอมพิวเตอร์แต่ละเครื่อง กับประเภทที่เป็นโปรแกรมตรวจจับไวรัสสำหรับองค์กร ซึ่งในกรณีหลังที่เป็นระบบสำหรับองค์กร จะมีทั้งโปรแกรมตรวจจับไวรัสที่ติดตั้งไว้ที่ประตูทางเข้าออกยังเครือข่ายขององค์กร และยังมีกระบวนการที่จะให้สามารถติดตั้งไปยังเครื่องทุกเครื่องภายในองค์กรได้อย่างสะดวกและรวดเร็วด้วย เช่น กรณีของมหาวิทยาลัยของเราก็จะมีการติดตั้งโปรแกรมตรวจจับไวรัสสำหรับองค์กรไว้แล้วด้วย แต่สำหรับเครื่องคอมพิวเตอร์ส่วนตัวที่บ้านของนิสิต ก็จำเป็นที่จะต้องติดตั้งโปแกรมป้องกันไวรัสส่วนตัวเอง

2. ปรับปรุงฐานข้อมูลไวรัสให้กับโปรแกรมตรวจจับไวรัสที่ใช้อยู่ตลอดเวลา โปรแกรมป้องกันไวรัสจำเป็นต้องมีการปรับปรุงฐานข้อมูลไวรัสตัวใหม่ๆ ที่จะเกิดขึ้น อาจเรียกว่าไวรัสซิกเนเจอร์ (Virus Signature) โดยบริษัทผู้ผลิตโปรแกรมป้องกันไวรัสจะมีทีมวิจัยของตัวเองในการค้นหาเพื่อปรับปรุงฐานข้อมูลไวรัสตัวใหม่ๆ อยู่เสมอ และเราจะต้องติดตามเพื่อปรับปรุงแฟ้มข้อมูลไวรัสซิกเนเจอร์ให้ทันสมัยอยู่เสมอจากบริษัทผู้ผลิตโปรแกรมตรวจจับไวรัสที่เราใช้งานอยู่ สำหรับโปรแกรมตรวจจับไวรัสสำหรับองค์กรกระบวนการปรับปรุงแฟ้มข้อมูลไวรัสซิกเนเจอร์จะดำเนินการให้โดยอัตโนมัติ

3. สั่งให้โปรแกรมตรวจจับไวรัสที่ใช้อยู่ตรวจสอบไวรัสอย่างเต็มรูปแบบอย่างน้อยสัปดาห์ละหนึ่งครั้ง

4. ทำการติดตั้งไฟร์วอลล์ส่วนบุคคลบนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ด้วย

5. ไม่ดาวน์โหลดโปรแกรมที่มาจากแหล่งที่ไม่น่าเชื่อถือ

6. ไม่เปิดเอกสารแนบทางอีเมลที่ส่งจากบุคคลที่คุณไม่รู้จัก ควรสแกนแฟ้มกลุ่มนี้ก่อนทุกครั้งหากไม่แน่ใจให้ลบโปรแกรมนั้นออกไป

7. ปรับปรุงระบบปฏิบัติการและซอฟต์แวร์ เช่น โปรแกรมเบราเซอร์ ชุดออฟฟิค ให้ทันสมัยอยู่เสมอด้วยการใช้แหล่งข้อมูลที่น่าเชื่อถือ

8. เนื่องจากเราไม่สามารถสร้างระบบที่มีความมั่นคงปลอดภัยได้ 100 % ดังนั้นการทำสำเนาแฟ้มข้อมูลที่สำคัญของเราเก็บแยกไว้ในที่ปลอดภัยอีกชุดหนึ่งจึงเป็นสิ่งที่จะต้องตระหนักและดำเนินการให้ติดเป็นนิสัยเสมอ

บรรณานุกรม

Timothy J. O'Leary and Linda I. O'Leary. Computing Essentials 2006, Complete Edition. Singapore: McGraw-Hill, 2006.

เชลลี. การี บี. การสื่อสารข้อมูลระดับพื้นฐาน. กรุงเทพฯ: ทอมสัน, 2544. 468 หน้า. (สัลยุทธ์ สว่างวรรณ, ผู้แปล)

จตุชัย แพงจันทร์. Master in Security. นนทบุรี: ไอดีซี, 2550. 524 หน้า.