ความปลอดภัยของคอมพิวเตอร์ ตอนที่ 1

ผศ.สุพล พรหมมาพันธุ์

ภาควิชาคอมพิวเตอร์ธุรกิจ คณะสารสนเทศศาสตร์ มหาวิทยาลัยศรีปทุม

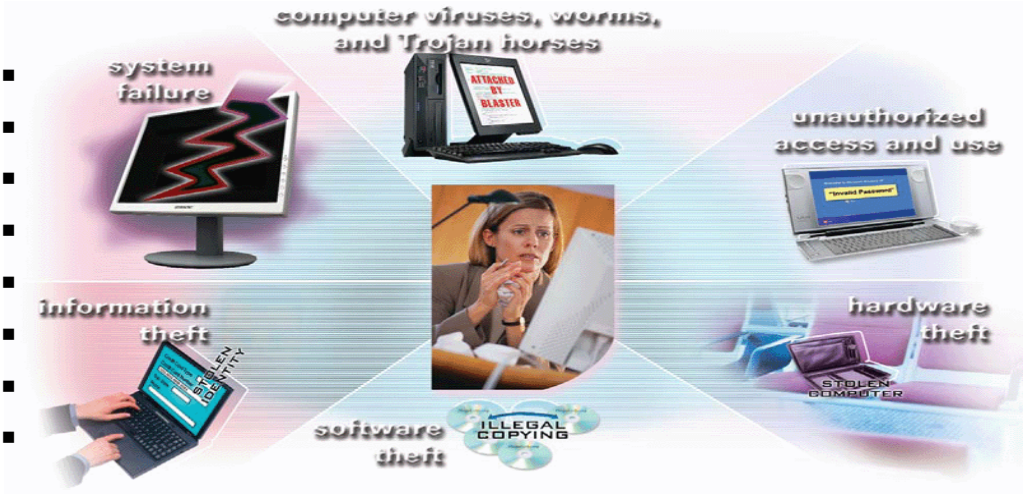
ลงตีพิมพ์ในหนังสือพิมพ์ Transport Journal ฉบับที่ 508 วันที่ 8-14 ธันวาคม พ.ศ.2551 หน้า 16

ปัจจุบันเราได้พึงพาอาศัยเครื่องคอมพิวเตอร์ช่วยในการทำงานอยู่ในชีวิตประจำวันเป็นจำนวนมาก ไม่ว่าจะเป็นการสร้างสารสนเทศ, การจัดเก็บข้อมูล, การจัดการสารสนเทศที่จำเป็นสำหรับการปฏิบัติงานต่างๆ ดังนั้นคอมพิวเตอร์จึงมีความสำคัญในการจัดเก็บข้อมูลสารสนเทศที่จำเป็นต่อการเรียกใช้งาน ผู้ใช้คอมพิวเตอร์จำนวนมากไม่ได้ตระหนักถึงความปลอดภัยและความเสียหายที่จะเกิดขึ้นกับข้อมูลบนคอมพิวเตอร์กันมากเท่าใดนัก ตัวอย่างเช่น ในทางธุรกิจ ต้องมีความมั่นใจในการจัดเก็บสารสนเทศเกี่ยวกับระเบียนของสินเชื่อ, ข้อมูลพนักงาน ข้อมูลของลูกค้า,สารสนเทศในการจัดซื้อสินค้าต่างๆ ต้องเป็นความลับ และมีความปลอดภัยสูง ส่วนผู้ใช้งานอยู่ที่บ้าน ต้องมั่นใจว่า หมายเลขบัตรเครดิตของเขา ต้องมีการักษาความปลอดภัยที่ดี มิให้ผู้อื่นสามารถล่วงรู้ได้เมื่อมีการซื้อสินค้าหรือการบริการผ่านทางอินเตอร์เน็ต

ความเสี่ยงด้านความปลอดภัยของคอมพิวเตอร์ในปัจจุบัน มีอยู่หลายกรณีด้วยกัน ไม่ว่าจะเป็นความเสียหายของฮาร์ดแวร์, ซอฟต์แวร์, ข้อมูล, สารสนเทศ หรือความสามารถในการประมวลผล หรือบางกรณีอาจเกิดจากอุบัติเหตุทำให้เครื่องคอมพิวเตอร์เกิดการแตกหัก หรืออาจเกิดจากการบุกรุกล่วงล้ำ หรือบางทีผู้บุกรุกนั้นอาจไม่ได้ต้องการก่อให้เกิดความเสียหาย แต่เขาอาจจะเข้ามาใช้ข้อมูล, เปิดดูสารสนเทศ, หรือโปรแกรมต่างๆในเวลาที่คอมพิวเตอร์นั้นยังไม่ได้ปิดล็อก ผู้บุกรุกบางคนได้แสดงหลักฐานทิ้งเอาไว้หรือไม่ก็ฝากข้อความทิ้งเอาไว้ แต่บางคนก็ไม่ทิ้งหลักฐานอะไรไว้ ซึ่งบางทีอาจทำให้คอมพิวเตอร์เสียและข้อมูลเสียหาย เป็นต้น

บริษัทที่ทำธุรกิจระหว่างประเทศ ต้องมีความรอบคอบในเรื่องการดูแลรักษาความปลอดภัยเป็นกรณีพิเศษ ซึ่งเรื่องที่พบโดยส่วนใหญ่เป็นเรื่องของ**อาชญากรรมคอมพิวเตอร์** (Computer Crime or Cybercrime) ซึ่งเป็นการกระทำผิดกฎหมายเกี่ยวกับบนอินเตอร์เน็ตเป็นหลัก จากการตรวจติดตามของ FBI ทำให้ทราบว่าอาชญากรรมคอมพิวเตอร์ที่พบมากที่สุด 3 อย่าง จากทั้งหมด 7 อย่างได้แก่ (1). นักเจาะระบบ (Hacker), (2). พวกบ้าคลั่ง (Cracker), (3). พวกประสาทอ่อนๆ (Script Kiddie), (4). นักสืบของบริษัท (Corporate spy), (5). พนักงานไม่ศีลธรรมจริยธรรม (Unethical employee), (6). พวกชอบขู่เข็ญว่าร้ายทางอินเตอร์เน็ต (Cyberextortionist), และ (7). พวกผู้ก่อการร้ายทางอินเตอร์เน็ต (Cyberterrorist) ดังมีรายละเอียดคือ

- **การเจาะระบบ (Hacking)** ส่วนนักเจาะระบบเรียกกันว่าแฮกเกอร์ (Hacker) ถึงแม้ว่า ความหมายดั้งเดิมของคำว่า Hacker จะหมายถึง ผู้มีความกระตือรือร้นหรือมีศรัทธาอย่างแก่กล้าต่อการทำงาน และเป็นคำที่ได้รับการยกย่องชมเชย แต่ความหมายของคำว่า Hacker ในปัจจุบันได้แปรเปลี่ยนไปในทางที่ไม่ดี **ซึ่งหมายถึงผู้เจาะระบบหรือผู้บุกรุกเข้าไปเพื่อเข้าถึงข้อมูลในคอมพิวเตอร์หรือบนเครือข่ายคอมพิวเตอร์อย่างผิดกฎหมาย** ซึ่งตัวของ Hacker เองก็ได้เรียกร้องว่า พวกเขาเข้าไปในระบบคอมพิวเตอร์นั้น ก็เพื่อปรับปรุงเรื่องความปลอดภัยของคอมพิวเตอร์ตามหน้าที่ซึ่งได้รับมอบหมาย อย่างไรก็ดี มีบางบริษัทบางองค์กรก็ได้รับความเสียหายจากพวก Hacker มามากต่อมากแล้ว


computer viruses, worms, and Trojan horses
ATTACKED BY BLASTER
system failure
unauthorized access and use
"Invalid Password"
information theft
STOLEN IDENTITY
hardware theft
STOLEN COMPUTER
software theft
ILLEGAL COPYING

✪✪✪✪✪