การจัดการความเสี่ยงของระบบงานคอมพิวเตอร์

โดย ดร. ครรชิต มาลัยวงศ์

21 ธันวาคม 2542

คอมพิวเตอร์เป็นเครื่องมือสำคัญของมนุษย์ในยุคปัจจุบันนี้ ไม่ว่าเราจะไปที่ไหนก็จะพบว่ามีผู้ใช้เครื่องคอมพิวเตอร์ทำงานต่าง ๆ มากมาย นับตั้งแต่การพิมพ์เอกสาร ไปจนถึงการให้บริการที่ซับซ้อนอย่างเช่นการเก็บค่าโดยสารรถไฟฟ้า การตรวจรักษาผู้ป่วย การให้บริการฝากถอนเงินด้วยระบบเอทีเอ็ม แม้แต่ตามหนังสือพิมพ์แทบทุกฉบับก็ยังตีพิมพ์คอลัมน์ที่เกี่ยวกับคอมพิวเตอร์ หรือ ระบบอินเทอร์เน็ตกันเป็นประจำทุกวัน

การใช้คอมพิวเตอร์จึงกลายเป็นเรื่องจำเป็นไปเสียแล้ว ถ้าเราไม่ใช้คอมพิวเตอร์งานการต่าง ๆ ก็คงจะไม่สามารถดำเนินไปได้อย่างราบรื่นและสะดวกรวดเร็วเหมือนที่เป็นอยู่ ยกตัวอย่างง่าย ๆ ก็คือการถอนเงินผ่านตู้เอทีเอ็ม ทำให้เราไม่จำเป็นต้องพกพาเงินสดทีละมาก ๆ หากต้องการใช้ก็เพียงแต่แวะเข้าไปกดปุ่มถอนเงินที่ตู้เอทีเอ็มเท่านั้น ถ้าไม่มีระบบแบบนี้ก็ยังคิดไม่ออกเหมือนกันว่าสภาวะการซื้อขายสินค้าต่าง ๆ ในประเทศไทยของเราจะยังคงเหมือนเมื่อสี่สิบห้าสิบปีก่อนนี้หรือไม่

อย่างไรก็ตาม การที่มีผู้ใช้คอมพิวเตอร์ในด้านต่าง ๆ มากขึ้นนั้นก็อาจทำให้เกิดปัญหาได้เหมือนกัน เพราะคอมพิวเตอร์ก็เหมือนเครื่องมืออื่น ๆ คืออาจมีผู้นำไปใช้ผิดได้ หรือมิฉะนั้นก็อาจจงใจนำไปใช้ในทางที่ผิดได้อีกเหมือนกัน

การกระทำผิดประเภทหนึ่งก็คือการทำให้ผู้เป็นเจ้าของระบบคอมพิวเตอร์เดือดร้อน ด้วยวิธีการต่าง ๆ สมัยเมื่อผมเป็นคณบดีอยู่ที่เอไอทีนั้น คอมพิวเตอร์พีซีในห้องปฏิบัติการที่ผมดูแลอยู่หายไปหนึ่งเครื่อง ไม่มีใครทราบว่าหายไปได้อย่างไร เพราะห้องปฏิบัติการนั้นเปิดให้นักศึกษาทำงานจนดึกถึงเท่าใดก็ได้ ช่วงนั้นเป็นระยะที่บริษัทไอบีเอ็มเพิ่งจะผลิตเครื่องพีซีออกมาใช้ใหม่ ๆ จึงกลายเป็นเครื่องที่คงจะมีคนหลายคนอยากนำไปใช้ที่บ้าน แต่การทำเช่นนั้นก็ทำให้ผมเดือดร้อนต้องถูกอธิการบดีเรียกไปดุ แม้ผมจะอธิบายว่าเรามีประกันไว้แล้ว และ ผมก็ไม่เดือดร้อนเท่าใดนัก เพราะเมื่อเครื่องพีซีหายไปผมก็ใช้เงินที่บริษัทประกันชดใช้ให้ไปซื้อเครื่องรุ่นใหม่ที่ดีกว่ามาแทนได้ แต่อธิการบดีก็ยังไม่สบายใจอยู่นั่นเองเนื่องจากเห็นว่าการถูกโจรกรรมไปนั้นทำให้ชื่อเสียงของสถาบันเสียหาย

ความเดือดร้อนที่เล่ามานี้ยังเป็นเรื่องเล็กน้อยมาก เรื่องที่ใหญ่กว่านั้นก็คือกรณีของธนาคารกรุงไทยซึ่งเคยมีข่าวเมื่อหลายปีก่อนว่ามีผู้มาถอนเงินเอทีเอ็มแล้วคอมพิวเตอร์เกิดใจดีจึงปล่อยเงินให้ผู้ถอนไปมากมายหลายแสนบาท ลงท้ายผู้ถอนเกิดสำนึกผิดจึงไปแจ้งขอคืนเงินกับตำรวจจึงกลายเป็นข่าวใหญ่โตไป เรื่องความผิดพลาดนี้เกิดขึ้นจริง แต่จะมีรายละเอียดอย่างไรขอยกเว้นไว้ไม่เล่า เอาแต่เพียงว่าปัญหานี้ทำให้เกิดความเดือดร้อนไปทั่ว ผู้บริหารและผู้ปฏิบัติ

งานเกี่ยวกับคอมพิวเตอร์ก็ต้องตรวจสอบว่าเกิดอะไรขึ้นและจะต้องหาทางแก้ไขปิดรอยรั่วไม่ให้เกิดขึ้นอีกในอนาคต ฝ่ายบัญชีลูกค้าก็ต้องตรวจสอบว่ามีลูกค้ากี่คนที่ได้เงินไปโดยมิชอบ แล้วก็ต้องติดตามลูกค้าเหล่านั้นมาเจรจาให้คืนเงิน นั่นก็คือเกิดความยุ่งยากไปทั้งธนาคาร

เมื่อสามสิบกว่าปีมาแล้วผมพัฒนาโปรแกรมสำหรับใช้ลงทะเบียนนักศึกษา และ คิดคะแนนสอบของนักศึกษาที่เอไอที โปรแกรมและข้อมูลของผมนั้นไม่ได้มีการป้องกันอะไรเลย เพราะระบบแรก ๆ เป็นงานแบบเอกเทศ ไม่ได้ยุ่งกับใคร ไม่ได้เก็บข้อมูลลงในจานแม่เหล็ก เมื่อต้องการใช้งานเมื่อใดก็หยิบโปรแกรมกับแฟ้มข้อมูลมาใช้ ผมเองก็ไม่ได้คาดคิดมาก่อนว่าจะมีใครแอบเข้ามาแก้ไขโปรแกรมและแฟ้มข้อมูลของผมได้ ต่อมาเมื่อเอไอทีขยายตัวขึ้นได้เครื่องไอบีเอ็มขนาดใหญ่มาใช้ มีนักศึกษาและอาจารย์มากขึ้น ปัญหาที่ผมไม่ได้คาดคิดก็เริ่มจะเกิดขึ้น

อาจารย์คนหนึ่งในคณะวิทยาการคอมพิวเตอร์ ได้ออกข้อสอบเก็บไว้ในระบบคอมพิวเตอร์เมนเฟรมเพื่อเตรียมไปให้นักศึกษาใช้สอบกลางภาค ปรากฏว่าเมื่อนำข้อสอบไปสอบจริง ๆ นักศึกษาก็เฮฮากันทั่วหน้า เพราะก่อนหน้านี้มีนักศึกษามือดีแอบเจาะแฟ้มข้อมูลของอาจารย์ได้แล้วก็นำเอาข้อสอบมาแบ่งกันดูไปเรียบร้อยแล้ว เมื่อถูกลูบคมเช่นนี้ บรรดาอาจารย์ก็ไม่มีทางเลือกนอกจากหาวิธีต่าง ๆ ในการป้องกันไม่ให้ลูกศิษย์ที่ตนเองสอนจนเก่งเข้ามาล้วงตับอาจารย์อีกต่อไป

จากที่กล่าวมานี้จะเห็นว่า คอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์นั้นได้ช่วยให้เราทำงานสะดวกมากขึ้นก็จริง แต่เราก็จะต้องเริ่มคิดว่าจะใช้กันอย่างไรจึงจะไม่มีปัญหา หรือไม่เกิดผลกระทบในทางลบจากการใช้นั้นได้ เรื่องนี้เป็นเรื่องใหญ่และมีความสำคัญอย่างยิ่งต่อหน่วยงานทุกแห่ง หากหน่วยงานที่มีคอมพิวเตอร์ไม่สนใจคอยป้องกันปัญหาทำนองนี้อย่างต่อเนื่องแล้วเมื่อเกิดปัญหาขึ้นก็อาจจะแก้ไขไม่ได้ และ หากเป็นปัญหาที่รุนแรงอาจทำให้หน่วยงานถึงกับต้องปิดตัวเองไปก็ได้

บทความนี้จะเล่าให้ท่านผู้อ่านทราบเกี่ยวกับวิธีการในการวิเคราะห์ความเสี่ยงเพื่อหาจุดอ่อนที่ต้องการให้มีมาตรการรักษาความมั่นคงปลอดภัยของระบบงานคอมพิวเตอร์ โดยเราจะเริ่มด้วยการพิจารณาว่ามีงานลักษณะใดบ้างที่อาจเป็นปัญหา

งานที่อาจเกิดปัญหาความเสี่ยง

อันที่จริงแล้ว คอมพิวเตอร์ทุกเครื่องย่อมมีโอกาสเสียหายได้ด้วยกันทั้งสิ้น คอมพิวเตอร์บางเครื่องอาจจะหายไปเหมือนเครื่องที่ผมเล่าให้ฟัง แต่ที่ร้ายกว่าก็คือข้อมูลที่เก็บไว้ในฮาร์ดดิสก์และมีเพียงชุดเดียวโดยไม่ได้ทำสำเนาเอาไว้นั้น อาจจะอันตรธานไปอย่างเรียกกลับมาอีกไม่ได้ และหากเป็นข้อมูลทางด้านบัญชีสำคัญ ๆ ละก็ ท่านอาจจะต้องปิดบริษัทไปเลยก็ได้ บางเครื่องอาจจะเชื่อมต่อกับระบบอินเทอร์เน็ต และ ท่านอาจจะชอบไปดึงเอาโปรแกรมของคนอื่นมาใช้โดยไม่ทราบว่าจะได้ไวรัสคอมพิวเตอร์แถมมาด้วย และเจ้าไวรัสนั้นก็อาจจะแผลงฤทธิ์ลบฮาร์ดดิสก์ของท่านได้อีกเหมือนกัน แต่ถึงท่านจะไม่ไปดึงเอาโปรแกรมใครมาใช้ ท่านก็ยังอาจจะ

ได้รับไวรัสคอมพิวเตอร์อยู่ดี เพราะเวลานี้มีผู้ส่งไวรัสคอมพิวเตอร์ไปกับจดหมายอิเล็กทรอนิกส์กันมากขึ้น เมื่อท่านเปิดจดหมายออกอ่าน เจ้าไวรัสเหล่านี้ก็จะแทรกซึมเข้าไปเริ่มบ่อนทำลายระบบของท่าน

อ่านแล้วก็ไม่ต้องไปแค้นเคืองหรอกครับ เพราะเหตุการณ์อย่างนี้เป็นธรรมดาของโลกที่มีทั้งคนดีและคนเลวคละกันอยู่ ไม่ใช่มีแต่คนดีไปหมด หรือ คนเลวไปหมด เมื่อมีคนคอยจ้องจะแกล้ง ก็เป็นหน้าที่ของเราจะต้องคอยป้องกันเอาไว้เช่นกัน คิดว่าเป็นเกมอย่างหนึ่งของโลกก็แล้วกันจะได้สบายใจ

โดยทั่วไปเราแบ่งปัญหาความมั่นคงปลอดภัยของคอมพิวเตอร์ออกเป็นกลุ่มต่าง ๆ ดังนี้

1. ความมั่นคงปลอดภัยทางกายภาพ หมายความถึงความปลอดภัยของตัวเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ อย่างเช่นในกรณีที่คอมพิวเตอร์ของผมหายไปนั้นก็เป็นเรื่องในกลุ่มนี้ ในการออกแบบระบบคอมพิวเตอร์และการกำหนดที่ตั้งของศูนย์คอมพิวเตอร์หรือการวางตัวเครื่องนั้น เรื่องที่จะต้องพิจารณาเป็นอันดับแรกก็คือเรื่องความมั่นคงปลอดภัยของเครื่องนี้เอง เราจะต้องหลีกเลี่ยงไม่ตั้งวางเครื่องไว้ในจุดที่มีความเสี่ยงสูง เช่น วางคอมพิวเตอร์ไว้ใกล้มือคนภายนอก หากใครเคยดูภาพถ่ายจากกล้องวีดิโอที่นำมาฉายทางเคเบิลทีวีช่อง 37 จะพบบ่อย ๆ ว่ามีภาพของคนร้ายเอื้อมมือมากระชากเอาเครื่องบันทึกเงินสดออกไปได้ง่าย ๆ คอมพิวเตอร์และอุปกรณ์ที่ตั้งในห้องปฏิบัติการหรือชั้นเรียนก็มีความเสี่ยงทำนองนี้ค่อนข้างมาก ตามสถานศึกษานั้นมักจะมีอุปกรณ์คอมพิวเตอร์ต่าง ๆ หายไปอยู่เสมอ

   อย่างไรก็ตามสถานที่ตั้งของศูนย์คอมพิวเตอร์และตัวเครื่องนั้นยังคงเป็นเพียงส่วนหนึ่งของปัญหาเท่านั้น การดูแลความมั่นคงปลอดภัยยังจะต้องพิจารณาให้กว้างไปกว่านี้อีก เช่นจะต้องระวังไม่ตั้งเครื่องในจุดที่มีความสั่นสะเทือนมากเกินไป หรืออยู่ใกล้กับบริเวณที่ได้รับคลื่นเรดาร์ ไมโครเวฟ คลื่นอัลตราซาวนด์ หรือ แม้แต่ได้รับแสงอินฟราเรดมากเกินไป คลื่นที่มองไม่เห็นเหล่านี้อาจทำให้ระบบของเราทำงานผิดพลาดได้โดยไม่สามารถหาสาเหตุพบ

   บริเวณที่ตั้งของศูนย์คอมพิวเตอร์ที่ควรหลีกเลี่ยงยังมีอีกมาก เช่นไม่อยู่ในบริเวณที่เสี่ยงต่อภัยพิบัติต่าง ๆ เช่น น้ำท่วม หรือ เพลิงไหม้ได้ง่าย ไม่อยู่ใกล้แหล่งที่จะมีผู้บุกรุกได้ง่าย ฯลฯ
2. ความมั่นคงปลอดภัยของบุคลากร เรื่องนี้มีอยู่สองประเด็น ประเด็นแรกก็คือเราจะต้องพยายามตรวจสอบการว่าจ้างบุคลากรเข้าทำงานให้ถี่ถ้วน เพื่อให้มั่นใจว่าบุคลากรเหล่านี้ไว้วางใจได้จริง และ ประเด็นที่สองก็คือ บุคลากรของเราอาจจะต้องทำงานจนถึงเวลาค่ำคืน เราจะมีวิธีป้องกันไม่ให้บุคลากรเหล่านี้ได้รับอันตรายได้อย่างไร ไม่ว่าอันตรายนั้นจะมาจากบุคคลอื่นในหน่วยงานเดียวกัน หรือ จากบุคคลภายนอก

เรื่องนี้อาจจะฟังดูแปลก ๆ แต่จริง ๆ แล้วสำคัญมาก เมื่อเร็ว ๆ นี้เองก็มีข่าวว่าข้าราชการหญิงผู้หนึ่งที่มาทำงานในวันหยุดถูกกระทำลวนลามจนเกือบจะเสียที แล้วงานคอมพิวเตอร์ในบางแห่งนั้นจำเป็นจะต้องทำงานจนดึกจนดื่นทั้งหญิงและชาย หากหน่วยงานไม่ออกแบบห้องทำงานหรือควบคุมการเข้าออกให้ดีแล้ว พนักงานก็อาจจะรู้สึกไม่ปลอดภัยและไม่อยากทำงานด้วยก็ได้

3. ความมั่นคงปลอดภัยของอุปกรณ์คอมพิวเตอร์ เรื่องนี้ก็ไม่แคล้วการป้องกันไม่ให้อุปกรณ์ถูกโจรกรรมไปเป็นหลัก แต่การโจรกรรมนั้นก็อาจทำให้ข้อมูลสูญหายไปได้ดังกล่าวมาแล้ว ดังนั้นอย่าคิดแต่เพียงจะประกันเครื่องเอาไว้เท่านั้น ต้องคิดให้รอบด้าน ตั้งแต่การป้องกันการเคลื่อนย้ายตัวเครื่อง การเคลื่อนย้ายอุปกรณ์ การติดตั้งอุปกรณ์ไว้ในที่ซึ่งเข้าถึงได้ยาก นอกจากนั้นเวลานี้ยังมีการทำลายอุปกรณ์บางอย่างด้วยไวรัสคอมพิวเตอร์ได้ด้วย ดังนั้นขอบเขตของความปลอดภัยของอุปกรณ์จึงขยายตัวออกไปอย่างกว้างขวางมากขึ้น
4. ความมั่นคงปลอดภัยของซอฟต์แวร์ ซอฟต์แวร์เป็นสิ่งที่เรายังสนใจในเรื่องความมั่นคงปลอดภัยกันน้อย เพราะซอฟต์แวร์สำเร็จส่วนใหญ่นั้นเรามักจะหาซื้อมาได้ง่าย ส่วนซอฟต์แวร์ที่พัฒนาขึ้นเองนั้นเราก็เชื่อว่าคงจะไม่มีใครมาสนใจจะเข้ามายุ่งเกี่ยวด้วย แต่นี่ก็คือความเข้าใจผิด หากเราไม่มีกระบวนการเก็บต้นฉบับซอฟต์แวร์ที่เหมาะสมแล้ว ซอฟต์แวร์ต้นฉบับของเราเองก็มีโอกาสถูกทำลายเสียหายได้ และเมื่อถึงตอนนั้นเราจะไปเรียกร้องให้บริษัทซอฟต์แวร์ส่งมาให้อีกหนึ่งชุดก็คงไม่ได้ หรือในกรณีของซอฟต์แวร์ที่พัฒนาเองก็เช่นกัน เราจะทราบได้อย่างไรว่าจะไม่มีใครเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งภายใน ในอเมริกานั้นช่วงแรก ๆ ที่นำคอมพิวเตอร์มาใช้ในธนาคาร มีนักโปรแกรมแอบแก้ไขเปลี่ยนแปลงคำสั่งเพื่อดักเอาเศษของเซนต์ที่โปรแกรมเดิมปัดทิ้งมาเก็บเอาไว้ นาน ๆ เข้าก็เป็นเงินมากเหมือนกัน โปรแกรมประเภทนี้เรียกกันว่า salami program หรือ โปรแกรมเศษเนื้อ นอกจากนั้นก็ยังอาจจะมีคนสร้างโปรแกรมอื่น ๆ เข้ามาดักเก็บข้อมูลเราไปด้วยก็ได้ เมื่อปีก่อนมีข่าวว่ามีคนจากประเทศจีนหนึ่งส่งบัตร สคส. มาให้ใครต่อใครทางไปรษณีย์อิเล็กทรอนิกส์แฟ้มบรรจุสคส.นั้นมีโปรแกรมบางอย่างแอบแฝงอยู่ เมื่อผู้รับเรียกบัตรนี้ขึ้นมาดูทางจอภาพ โปรแกรมที่ซ่อนอยู่ก็ออกฤทธิ์ด้วยการอ่านแฟ้มข้อมูลต่าง ๆ แล้วส่งกลับไปให้แก่ผู้ส่ง สคส. ทางอินเทอร์เน็ต ด้วยเหตุนี้เองเมื่อคิดดูแล้วก็จะเห็นว่าการรักษาความมั่นคงปลอดภัยของซอฟต์แวร์ในยุคปัจจุบันนั้นไม่ใช่เรื่องง่ายเลย
5. ความมั่นคงปลอดภัยของระบบเครือข่าย แต่ก่อนนี้เวลาเราใช้เครือข่ายคอมพิวเตอร์นั้น เราก็ระวังแต่เพียงป้องกันอย่าให้ใครมาคอยดักฟังสัญญาณข้อมูลจากสายเคเบิลของเราเท่านั้น แต่ขณะนี้เทคโนโลยีได้เปลี่ยนแปลงไปมาก ยิ่งระบบอินเทอร์เน็ตได้

รับความสนใจอย่างกว้างขวางด้วยแล้วยิ่งทำให้การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายของเรายากมากขึ้น เพราะไป ๆ มา ๆ ไม่ใช่ว่าจะมีแต่พนักงานของเราเท่านั้นที่เข้าถึงเครือข่ายได้ แม้แต่เด็กแถวเอกิฮาบารา ซิมลิมเทาเวอร์ หรือ แม่น้ำวอลกา ก็สามารถเข้ามาแอบดูเราได้ว่ามีอะไรอยู่ในระบบคอมพิวเตอร์ของเราบ้าง

6. ความมั่นคงปลอดภัยของระบบข้อมูล เมื่อเราพูดถึงระบบคอมพิวเตอร์นั้น สิ่งที่เรามองข้ามไม่ได้ก็คือข้อมูลและระบบข้อมูล ในบรรดาองค์ประกอบทั้งหมดของระบบคอมพิวเตอร์นั้น ข้อมูลเป็นส่วนที่สำคัญที่สุด เพราะข้อมูลนั้นหากเสียหายหรือถูกทำลายไปแล้วเราจะเรียกกลับคืนมาอีกไม่ได้ ยกเว้นแต่เมื่อได้สำรองเก็บเอาไว้ก่อนแล้ว ดังนั้นการรักษาความมั่นคงปลอดภัยของข้อมูลจึงเป็นเรื่องที่มีความสำคัญสุดยอดยิ่งกว่าการรักษาความมั่นคงปลอดภัยขององค์ประกอบอื่น ๆ การปกป้องรักษาข้อมูลนั้นมีทั้งการป้องกันไม่ให้ผู้อื่นเข้ามาอ่านข้อมูล หรือแอบคัดลอกข้อมูลไปใช้ หรือลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูลจนทำให้การตัดสินใจที่ใช้ข้อมูลนั้นผิดพลาดจนเกิดความเสียหายขึ้นได้

หลักการของการรักษาความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ให้ได้ผลนั้นจำเป็นจะต้องเข้าใจหลักการพื้นฐานที่เกี่ยวข้องเอาไว้บ้าง มิฉะนั้นแล้วก็จะไม่สามารถจับประเด็นที่จะดำเนินการได้ถูกต้อง และทำให้การดำเนินงานไม่ได้ผล

หลักการพื้นฐานทางด้านนี้อาจแยกออกได้เป็นประเด็นต่าง ๆ ดังนี้

1. ประเด็นด้านการคุกคาม (Threat) การคุกคามนั้นหมายถึงสิ่งใด ๆ หรือเหตุการณ์ใด ๆ ที่อาจมีผลร้ายต่อการปฏิบัติงานของหน่วยงาน การที่พนักงานไม่พอใจแล้วคิดสไตรค์ไม่ทำงานก็ตาม หรือ การที่มีบริษัทคู่แข่งจ้องจะหาทางล้วงเอาความลับของเราไปก็ตาม ล้วนแล้วแต่เรียกได้ว่าเป็นการคุกคามทั้งสิ้น ขอให้สังเกตว่าการคุกคามนั้นมีอยู่เป็นปกติธรรมดา ไม่ได้ขึ้นอยู่กับวิธีการที่เราติดตั้งศูนย์คอมพิวเตอร์ หรือ ตัวเครื่องและอุปกรณ์ ไม่ได้ขึ้นอยู่กับความมุ่งร้ายของคนอื่นและไม่ได้ขึ้นอยู่กับว่าจะมีคนจงใจคุกคามเราจริง ๆ หรือไม่ ดังนั้นเหตุการณ์ไฟฟ้าดับระยะยาว หรือ ฝนตกหนักจนน้ำท่วมก็เป็นการคุกคามได้
2. ประเด็นด้านสภาพที่เอื้อหรืออาจประสบการคุกคาม (Vulnerability) หมายถึงลักษณะของการติดตั้งระบบคอมพิวเตอร์ หรือ อุปกรณ์ที่อาจจะทำให้ประสบการคุกคามได้มากน้อยเพียงใด การเชื่อมต่อคอมพิวเตอร์ของเราเข้ากับระบบอิน

เทอร์เน็ตก็ทำให้เราอยู่ในสภาพที่อาจประสบกับการคุกคามจากผู้อื่นได้ง่ายขึ้น ในขณะที่ถ้าหากเราไม่สนใจเชื่อมต่อเลย เราก็จะไม่ประสบกับการคุกคามนั้น

3. ประเด็นด้านความเสี่ยง (Risk) หมายถึงความประจวบเหมาะที่การคุกคามกับสภาพที่เอื้อต่อการคุกคามมาพร้อมกันพอดี ยกตัวอย่างเช่น มีการคุกคามที่จะเข้ามาแก้ไขคะแนนสอบของนักศึกษาในมหาวิทยาลัยแห่งหนึ่ง และมหาวิทยาลัยแห่งนั้นได้จัดทำฐานข้อมูลคะแนนสอบของนักศึกษาเอาไว้ในระบบอินเทอร์เน็ต จึงเอื้อต่อการที่จะประสบการคุกคามพอดี เช่นนี้มหาวิทยาลัยแห่งนั้นก็เกิดความเสี่ยงขึ้น เมื่อมีความเสี่ยงขึ้นแล้วผู้ที่เข้ามาฉวยโอกาสทำเช่นนั้นก็เรียกว่าผู้โจมตี (Attacker) ขอให้สังเกตด้วยว่าการโจมตีหรือการพยายามเข้ามาแก้ไขคะแนนสอบนั้นอาจจะเกิดจากผู้จู่โจมหลายคนก็ได้
4. มาตรการป้องกัน (Countermeasure) หมายถึงกระบวนการที่ช่วยลดความเสียหายที่อาจจะเกิดขึ้นจากปัญหาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ อาจจะด้วยการลดโอกาสในการเข้าโจมตีด้วยการลดสภาพที่เอื้อต่อการคุกคาม หรือลดความสูญเสียที่อาจจะเกิดจากการโจมตี

เมื่อผมสอนเรื่องการรักษาความมั่นคงปลอดภัยเป็นส่วนหนึ่งของวิชาการบริหารศูนย์คอมพิวเตอร์นั้น ผมได้ให้หลักการเอาไว้ง่าย ๆ ว่า

1. พยายามจัดวางอุปกรณ์หรือกำหนดมาตรการดูแลเพื่อไม่ให้คนนอกหรือคนที่ไม่ประสงค์ดีเข้าถึงระบบคอมพิวเตอร์
2. หากคนนอกนั้นเข้าถึงระบบคอมพิวเตอร์ได้ก็ต้องหาทางป้องกันไม่ให้ใช้คอมพิวเตอร์ได้ นั่นคือมีวิธีป้องกันไม่ให้เปิดสวิตช์เครื่อง หรือ Login ได้
3. หาก Login ได้ก็ต้องพยายามอย่าให้เข้าถึงแฟ้มข้อมูลสำคัญได้
4. หากเข้าถึงแฟ้มข้อมูลได้และสามารถก็อปปี้แฟ้มได้ก็อย่าให้อ่านแฟ้มออก
5. ต้องจับคนบุกรุกให้ได้

หลักการง่าย ๆ มีแค่นี้เอง แต่การปฏิบัติตามหลักการไม่ใช่เรื่องง่ายเลย อย่างไรก็ตามผมขอเสนอขั้นตอนในการดำเนินงานรักษาความมั่นคงปลอดภัยดังต่อไปนี้

ขั้นตอนในการวิเคราะห์ความเสี่ยงและรักษาความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยขององค์ประกอบต่าง ๆ ที่กล่าวมาข้างต้นนั้นเป็นเรื่องละเอียดอ่อน และจะต้องดำเนินการอย่างจริงจังและรอบคอบ ทุกหน่วยงานควรพิจารณาความจำเป็นที่จะต้องจัดการในเรื่องนี้แล้ว จะรอจนกว่าจะเกิดปัญหาขึ้นแล้วจึงดำเนินการเข้าทำนอง วัว

หายแล้วล้อมคอกไม่ได้ เพราะปัญหานั้นอาจจะร้ายแรงจนถึงกับทำให้เกิดความสูญเสียอย่างมหาศาลได้

ก่อนที่จะพิจารณาขั้นตอนในการรักษาความปลอดภัย ควรเข้าใจไว้เป็นพื้นฐานก่อนว่าในการดำเนินการใด ๆ นั้นล้วนแล้วแต่จะต้องใช้ทุนทรัพย์ทั้งนั้น เพียงแต่จะใช้มากหรือใช้น้อยเท่านั้น มีกฎง่าย ๆ อยู่ว่าการใช้ทุนทรัพย์นั้นควรจะคุ้มกับสิ่งที่จะได้รับ ทางด้านการรักษาความมั่นคงปลอดภัยก็เช่นกัน หากเราลงทุนไปร้อยบาทก็หมายความว่าผลเสียหายที่เราป้องกันได้นั้นคุ้มกับการลงทุน หากสิ่งที่เราต้องการป้องกันมีมูลค่าของความเสียหายเพียงสิบบาท แต่เราต้องลงทุนไปร้อยบาท เช่นนี้ก็นับว่าเปล่าประโยชน์ ไม่คุ้มการลงทุน

ขั้นตอนในการวิเคราะห์ความเสี่ยงและรักษาความมั่นคงปลอดภัยของระบบงานคอมพิวเตอร์จึงควรจะมีดังต่อไปนี้

1. ผู้บริหารระดับสูงจะต้องมีนโยบายในด้านการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์อย่างชัดเจน อีกนัยหนึ่งผู้บริหารจะต้องเข้าใจปัญหาที่อาจจะเกิดขึ้นจากการมีระบบที่ไม่มั่นคงปลอดภัย และจะต้องจัดสรรงบประมาณให้ดำเนินการด้วย
2. แต่งตั้งให้มีผู้รับผิดชอบงานทางด้านความมั่นคงปลอดภัย หน่วยงานส่วนมากไม่มีผู้ที่ทำหน้าที่นี้โดยตรง แต่มอบหมายให้ทำกันหลายคน นักวิเคราะห์ระบบอาจช่วยดูการป้องกันรักษาความปลอดภัยของฐานข้อมูล วิศวกรสื่อสารอาจดูแลงานด้านเครือข่าย ฯลฯ วิธีนี้ทำให้การรักษาความมั่นคงปลอดภัยไม่เป็นเอกภาพ และไม่ทราบแน่ชัดว่าใครทำอะไรบ้าง หากหน่วยงานมีขนาดใหญ่และกิจการกว้างขวางก็ควรจัดให้เป็นฝ่ายขึ้นมาได้โดยจัดสรรให้มีบุคลากรมากพอ แต่ถ้าหากเป็นหน่วยงานขนาดเล็กก็เพียงแต่มอบหมายให้วิศวกรระบบสักหนึ่งหรือสองคนเป็นผู้ดูแล เหตุผลที่ควรเป็นวิศวกรระบบหรือนักเขียนโปรแกรมระบบก็เพราะจะต้องศึกษาลึกลงไปถึงระดับภาษาสัญลักษณ์หรือภาษาเครื่องของระบบต่าง ๆ
3. วิเคราะห์ภัยคุกคามระบบว่ามีอะไรบ้าง ในที่นี้จะต้องพิจารณาภัยคุกคามทุกประเด็นต่อหน่วยงานและต่อระบบคอมพิวเตอร์ให้ละเอียดที่สุดเท่าที่จะทำได้ ยกตัวอย่างเช่น การสูญเสียลูกค้า การสูญเสียตลาด การถูกโจรกรรม การเกิดอุบัติภัยกับอุปกรณ์ต่าง ๆ ไปจนถึงกรณีที่พนักงานเจ็บป่วยมาทำงานไม่ได้ ในกรณีที่เกิดภัยคุกคามแต่ละอย่างขึ้นนั้นให้พิจารณาด้วยว่าจะเกิดผลกระทบเป็นความเสียหายมากน้อยสักเพียงใด การพิจารณาส่วนนี้ถ้าคิดเป็นวงเงินจะทำให้เห็นภาพได้ชัดเจนขึ้นดังแสดงในตารางที่ 1 เมื่อได้รายละเอียดแล้วให้บันทึกเป็นตารางเก็บไว้ดังนำตัวอย่างง่าย ๆ มาแสดงในตารางที่ 2
4. วิเคราะห์สภาพที่เอื้อต่อการคุกคาม ในที่นี้ให้พิจารณาการติดตั้งเครื่องและอุปกรณ์ตลอดจนซอฟต์แวร์ และระบบเครือข่ายต่าง ๆ แล้ววิเคราะห์ว่ามีโอกาสที่จะเกิด

ปัญหาภัยคุกคามได้มากเพียงใด ในการวิเคราะห์นี้เราจะต้องพิจารณาองค์ประกอบของระบบคอมพิวเตอร์ให้ครบถ้วน ไม่ว่าในด้าน ฮาร์ดแวร์ ซอฟต์แวร์ บุคลากร ข้อมูล ระบบเครือข่าย สถานที่ติดตั้งอุปกรณ์ต่าง ๆ ตลอดจนสิ่งแวดล้อมของระบบคอมพิวเตอร์ของเรา ให้พิจารณาแต่ละองค์ประกอบเป็นประเด็น ๆ ไป เช่น กรณีของเครื่องพีซี ให้พิจารณาว่าการตั้งเครื่องพีซีในสำนักงานของเรานั้นมีโอกาสที่จะถูกผู้อื่นโจรกรรมไปมากน้อยเพียงใด หรือในกรณีของแฟ้มข้อมูลลูกค้าที่เราบันทึกไว้ในระบบคอมพิวเตอร์ของเรานั้นมีโอกาสที่ผู้ไม่หวังดีจะโจรกรรมไปหรือลักลอบแก้ไขเปลี่ยนแปลงไปได้มากน้อยเพียงใด หรือ ถูกนำไปเปิดเผย หรือ มีโอกาสที่จะทำบางส่วนหายไปได้มากน้อยเพียงใด ในเรื่องแฟ้มข้อมูลนี้เราอาจจะพิจารณาสามแบบ คือ ถูกโจรกรรมหรือเปลี่ยนแปลง ถูกนำไปเปิดเผย หรือ ถูกทำให้บางส่วนหายไปได้มากน้อยเพียงใด เราอาจจะพิจารณาโอกาสที่จะเกิดขึ้นโดยกำหนดว่าอาจเกิดขึ้นได้บ่อยครั้งแค่ไหน เช่น อาจเกิดขึ้นได้ทุกวัน ทุกสัปดาห์ ทุกเดือน ทุกปี หรือ มากกว่านั้น ดังแสดงในตารางที่ 3 เมื่อพิจารณาแล้วให้จัดทำตารางแสดงสถานการณ์ที่เอื้อต่อการคุกคามเอาไว้ดังที่เห็นในตารางที่ 4

5. ขั้นต่อมาเป็นการพิจารณาขนาดของความเสี่ยง เริ่มต้นด้วยนำเอาตารางการคุกคามและตารางแสดงสถานการณ์ที่จะเกิดการคุกคามมาจัดทำเป็นตารางเดียวกัน คงจำได้ว่าความเสี่ยงนั้นเกิดขึ้นเมื่อมีการคุกคาม และ มีสถานภาพที่เอื้อให้เกิดการคุกคาม หากมีการคุกคามแต่ไม่มีสถานภาพที่เอื้อ หรือมีสภาพที่เอื้อให้เกิดการคุกคาม แต่ไม่มีการคุกคาม ก็ต้องสรุปว่าไม่มีความเสี่ยงในกรณีนั้น ๆ วิธีการพิจารณาจัดรวมเป็นตารางก็คือ ให้พิจารณาภัยคุกคามแต่ละอย่างก่อน จากนั้นให้ตรวจสอบว่าภัยนั้นจะเกิดกับองค์ประกอบอย่างใดบ้างของระบบงานคอมพิวเตอร์ ในการตรวจสอบนี้จะดีมากถ้าหากเรามีแผนภูมิกระแสข้อมูลของระบบงานคอมพิวเตอร์ เพราะจะช่วยให้เราไล่ตามกระแสข้อมูลได้ว่าเกี่ยวข้องกับกิจกรรมอะไรบ้าง เมื่อตรวจพบแล้วว่าเกี่ยวข้องกับองค์ประกอบอะไร ก็ให้พิจารณาว่าองค์ประกอบนั้น ๆ มีสถานการณ์ที่เอื้อต่อภัยคุกคามมากน้อยแค่ไหน ถ้าหากไม่พบสถานการณ์ก็หมายความว่าไม่เกิดความเสี่ยง แต่ถ้าพบว่ามีสถานการณ์ที่เอื้อต่อภัยคุกคาม ก็ให้กำหนดรายละเอียดพร้อมกับโอกาสที่จะเกิดภัยนั้นไว้ในตารางใหม่ จากนั้นให้คำนวณว่าความเสี่ยงนั้นมีโอกาสเกิดขึ้นมากน้อยเพียงใดในหนึ่งปี และ จะทำให้เกิดผลกระทบมากน้อยเพียงใด ต่อจากนั้นจึงค่อยแปลงกลับเป็นจำนวนเงินที่จะทำให้เกิดการสูญเสีย ตารางที่ 5 แสดงการผสมผสานตารางที่ 2 และ 4 เข้าด้วยกันตามคำแนะนำข้างต้น

แนวทางจัดการกับความเสี่ยง

เมื่อทราบสถานภาพความเสี่ยงของระบบงานคอมพิวเตอร์โดยรวมแล้ว ต่อไปก็เป็นการพิจารณาหาทางจัดการกับความเสี่ยง ซึ่งเรามีวิธีการทำได้สามวิธีดังนี้

1. **ย้ายความเสี่ยง** วิธีนี้ก็คือย้ายความเสี่ยงที่เรามีอยู่ไปให้คนอื่นรับภาระแทน เช่นทำประกันเอาไว้กับบริษัทประกันภัย (เหมือนตัวอย่างที่ผมได้อ้างถึงแล้ว) หรือ ย้ายไปให้บริษัทผู้ให้บริการรับผิดชอบแทน การใช้วิธีนี้ต้องพิจารณาให้ดีเพราะอาจจะไม่ได้ลดผลกระทบทั้งหมดได้
2. **ลดความเสี่ยง** วิธีนี้ก็คือการจัดสิ่งแวดล้อมทางเทคโนโลยีของระบบใหม่ เช่น การใช้อุปกรณ์อื่น ๆ ทั้งฮาร์ดแวร์ และ ซอฟต์แวร์เข้าช่วยเพื่อลดโอกาสที่จะเกิดการคุกคาม
3. **เลี่ยงความเสี่ยง** วิธีนี้ก็คือการเปลี่ยนรูปแบบการดำเนินงานของหน่วยงาน อาจจะเปลี่ยนแปลงบุคลากร เปลี่ยนการจัดองค์กร เปลี่ยนรูปแบบการดำเนินธุรกิจ หรือ แม้แต่เปลี่ยนแบบจำลองทางธุรกิจที่ใช้ในการพัฒนาระบบงานคอมพิวเตอร์นั้น

การจัดการกับความเสี่ยงนั้นเป็นเรื่องที่จะต้องพิจารณาดำเนินการกลับไปกลับมาหลายหน เพราะสถานการณ์ที่เอื้อให้เกิดภัยคุกคามแต่ละประเภทนั้นอาจทำให้เกิดความเสี่ยงได้หลายลักษณะด้วยกัน เราควรพิจารณาสถานการณ์ที่ทำให้เกิดความเสี่ยงสูง ๆ ก่อนแล้วหาทางที่จะจัดการกับความเสี่ยงในรูปแบบต่าง ๆ ให้ได้ผล

สรุป

ความมั่นคงปลอดภัยของระบบงานคอมพิวเตอร์ และ การจัดการกับความเสี่ยงที่ทำให้ระบบงานไม่ปลอดภัยนั้นเป็นเรื่องสำคัญมากยิ่งขึ้น โดยเฉพาะในเมื่อการใช้งานระบบคอมพิวเตอร์ของหน่วยงานต่าง ๆ เริ่มมีลักษณะเป็นเครือข่ายแบบอินเทอร์เน็ตมากยิ่งขึ้น ระบบเครือข่ายเช่นนี้เปิดโอกาสให้คนภายนอกที่มีความรู้ทางด้านคอมพิวเตอร์สูงบุกรุกเข้ามาตรวจสอบแฟ้มข้อมูลในเครื่องแม่ข่ายของเราได้ง่ายขึ้น หากผู้ที่บุกรุกเข้ามานั้นมีประสงค์ร้ายก็อาจจะบ่อนทำลายระบบงานคอมพิวเตอร์ของเราได้โดยง่าย และอาจส่งผลกระทบอย่างรุนแรงต่อหน่วยงานของเราได้

การจัดการกับความเสี่ยงจะต้องดำเนินการอย่างเป็นระบบ ด้วยการพิจารณาภัยคุกคาม สถานการณ์ที่เอื้อให้เกิดภัยคุกคาม แล้วนำข้อมูลที่ได้มาจัดทำเป็นตารางความเสี่ยง ต่อจากนั้นจะต้องพิจารณาจัดการกับความเสี่ยงด้วยการย้าย ลด หรือเลี่ยงความเสี่ยงที่มีอยู่ในระบบงานคอมพิวเตอร์ของเราตามความเหมาะสมของสถานการณ์

บรรณานุกรม

1. David G.W. Birch and Neil A. McEvay, Risk Analysis for Information Systems, ใน Investing in Information Systems, Leslie Wilcocks บรรณาธิการ, Chapman & Hall, UK, 1996.

2. Karen A. Forcht, Computer Security Management, International Thompson Publishing, 1994.

ตารางที่ 1 ผลกระทบคิดเป็นเงิน

ความสูญเสียมากที่สุด	ระดับผลกระทบ
0 บาท	0
10 บาท	1
100 บาท	2
1000 บาท	3
10000 บาท	4
100000 บาท	5
1000000 บาท	6
ฯลฯ	ฯลฯ

ตารางที่ 2 ตัวอย่างการคุกคาม

รายการ	ชื่อ	การคุกคาม	คำอธิบาย	ระดับผลกระทบ
1	ข้อมูลลูกค้า	R1	ข้อมูลลูกค้าสูญหาย/ถูกแก้	5
2	ข้อมูลลูกค้า	R2	ข้อมูลถูกเปิดเผย	6
3	ข้อมูลลูกค้า	R3	ใช้ข้อมูลไม่ได้	6
4	การสั่งซื้อสินค้า	S1	ข้อมูลการสั่งซื้อสูญหาย/แก้	4
5	การสั่งซื้อสินค้า	S2	ข้อมูลการสั่งซื้อถูกเปิดเผย	4
6	การสั่งซื้อสินค้า	S3	ใช้ข้อมูลไม่ได้	5

ตัวอย่างที่ 3 โอกาสที่เกิดปัญหา

ความถี่	ระดับความถี่
ไม่เกิด	0
เกิดทุกวัน	1
เกิดทุกสัปดาห์	2
เกิดทุกเดือน	3
เกิดทุกปี	4
เกิดทุกสิบปี	5
เกิดทุก 100 ปี	6

ตารางที่ 4 สถานการณ์ที่เอื้อต่อการคุกคาม

รายการที่	ชื่อ	สถานการณ์	ระดับความถี่	คำอธิบาย
1	พีซีสำหรับคำสั่งซื้อ	A1	3	พีซีถูกใช้งานโดยไม่ได้รับอนุญาต
2	พีซีสำหรับคำสั่งซื้อ	A2	5	พีซีถูกอุบัติภัย
3	พีซีสำหรับคำสั่งซื้อ	A3	3	พีซีถูกไวรัสก่อกวน
4	เครื่องแม่ข่าย	B1	3	เครื่องแม่ข่ายถูกใช้งานโดยไม่ได้รับอนุญาต
5	เครื่องแม่ข่าย	B2	4	เครื่องแม่ข่ายถูกอุบัติภัย
6	เครื่องแม่ข่าย	B3	3	เครื่องแม่ข่ายถูกไวรัสทำลาย

ตารางที่ 5 ความเสี่ยง

รายการ	การคุกคาม	สถานการณ์	ระดับความถี่	ระดับผลกระทบ	คำอธิบาย
1	R1	A1	3	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะพีซีถูกใช้งานโดยไม่ได้รับอนุญาต
2	R1	A2	5	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะพีซีถูกอุบัติภัย
3	R1	A3	3	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะพีซีถูกไวรัสก่อกวน
4	R1	B1	3	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะถูกใช้งานโดยไม่ได้รับอนุญาต
5	R1	B1	4	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะเครื่องแม่ข่ายถูกอุบัติภัย
6	R1	A3	3	5	ข้อมูลลูกค้าสูญหาย/ถูกแก้เพราะเครื่องแม่ข่ายถูกไวรัสทำลาย