การรักษาความปลอดภัยบนระบบเครือข่ายสารสนเทศสำหรับองค์กร

(How to Save the Information Network System for Organization)

นายนรินทร์ พนาวาส

(ผู้ช่วยอธิการบดีฝ่ายบริหาร มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี)

e-Mail: narin.pa@east.spu.ac.th

ด้วยปัจจุบันเป็นยุคของข้อมูลสารสนเทศ (Information Age) การใช้งานคอมพิวเตอร์เครือข่าย ผ่านระบบอินเทอร์เน็ตในองค์กรต่างๆ ได้มีการใช้งานเพิ่มมากขึ้นเป็นลำดับ เพื่อเป็นช่องทาง ในการติดต่อสื่อสารแลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว รวมไปถึงการทำธุรกิจออนไลน์และการพาณิชย์ในด้านต่างๆ โดยเฉพาะทางด้านธุรกิจ ซึ่งปัจจุบันมีการแข่งขันกันสูงมาก องค์กรต่างๆจึงพยายามแสวงหาเทคโนโลยีสารสนเทศเข้ามาใช้เพื่อช่วยการบริหารจัดการงานต่างๆ ภายในองค์กร และสนับสนุนการแข่งขันในธุรกิจ ให้ประสบความสำเร็จ เพื่อให้เกิดข้อได้เปรียบทางด้านการแข่งขัน กับธุรกิจในประเภทเดียวกัน แต่ถ้าองค์กรใด พิจารณาเฉพาะเรื่องการจัดทำระบบเทคโนโลยีสารสนเทศให้สำเร็จเพียงอย่างเดียว โดยอาจมองข้ามเรื่องระบบรักษาความปลอดภัยบนระบบเครือข่ายสารสนเทศภายในองค์กรที่ดี อาจจะทำให้ผู้ที่ไม่หวังดีจากภายนอกหรือบุคคลภายในองค์กรเข้ามาก่อกวนการทำงาน พยายามหาวิธีการหรือหาช่องโหว่และจุดอ่อนของระบบ เพื่อแอบลักลอบเข้าสู่ระบบหรือแอบดูข้อมูลข่าวสาร เพื่อให้ระบบเครือข่ายหยุดชะงักไม่สามารถให้บริการได้ ในบางครั้งอาจมีการทำลายข้อมูล ซึ่งทำให้เกิดความเสียหายให้กับองค์กรได้ เนื่องจากระบบเครือข่ายอินเทอร์เน็ตได้เชื่อมโยงถึงกันทั่วโลก ทำให้เกิดปัญหาในเรื่องอาชญากรรมทางด้านเทคโนโลยีตลอดเวลา โดยเฉพาะในเรื่องของการโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ตก็มีให้เห็นมากยิ่งขึ้น โดยผู้ที่แอบลักลอบเข้าสู่ระบบของผู้อื่นสามารถมาได้จากทั่วโลก ส่วนใหญ่จะทำการเจาะระบบผ่านช่องโหว่ของระบบปฏิบัติการ (Operation System) Windows ,Unix , Linux เป็นต้น หรือจากช่องโหว่ของโปรแกรมที่เปิดให้บริการ เช่น WWW, DNS, Mail และ FTP เป็นต้น และจากระบบฐานข้อมูล (Database) ขององค์กร

ดังนั้น ทุกองค์กรควรตระหนักถึงเรื่องการนำระบบรักษาความปลอดภัยบนระบบเครือข่ายในรูปแบบต่างๆมาใช้งาน เพื่อการลดความเสี่ยงทางด้านระบบสารสนเทศขององค์กร โดยขอแนะนำวิธีการป้องกันเบื้องต้น ที่ทุกองค์กรสามารถนำไปพิจารณา ตรวจสอบ หรือจัดซื้อจัดหาอุปกรณ์รักษาความปลอดภัย เข้าไปเสริมความแข็งแกร่ง ให้กับระบบเครือข่ายของท่าน ดังนี้

1. การนำอุปกรณ์ระบบรักษาความปลอดภัย เข้ามาช่วยป้องกันและตรวจสอบการโจมตีบนระบบเครือข่าย เช่น ไฟร์วอล (Firewall) ที่ทำหน้าที่เป็นเสมือนยามเฝ้าหน้าประตู โดยทำการตรวจสอบทุกคนที่จะเข้าสู่ระบบ มีการจดบันทึกข้อมูลการเข้าออก ติดตามพฤติกรรมการใช้งานในระบบ รวมทั้งสามารถกำหนดกฎเกณฑ์ที่จะอนุญาตให้ใช้ระบบในระดับต่างๆ ได้ ซึ่งจะสามารถลดปัญหาการบุกรุกจากภายนอกได้ และถ้าต้องการเพิ่มความแข็งแกร่ง ให้กับไฟร์วอลในด้านการตรวจจับผู้บุกรุกได้อย่างมีประสิทธิภาพมากขึ้น ควรนำระบบ IDS (Intrusion Detection System) และ IPS (Intrusion Prevention System) เข้ามาใช้ซึ่งจะสามารถเพิ่มระบบรักษาความปลอดภัยบนระบบเครือข่ายได้มากขึ้น และถ้าองค์กรของเรายังไม่สามารถลงทุนอุปกรณ์ประเภทเหล่านี้ได้ อาจจะใช้ประโยชน์จากอุปกรณ์ Router ในองค์กรเพื่อเปิด - ปิด Port ที่อนุญาตให้เข้าและออกภายในเบื้องต้น หรืออาจนำระบบปฏิบัติการ Linux มาติดตั้งทำหน้าที่เป็น Firewall และ IDS ขององค์กรได้โดยไม่ต้องเสียค่าใช้จ่ายโปรแกรมในการติดตั้ง (ติดตามเรื่องการทำงานของระบบปฏิบัติการ Linux ได้ในบทความต่อไป)

2. การติดตั้งระบบป้องกันการเข้าเว็บไซต์ลามก หรือเว็บไซต์ที่ ไม่พึงประสงค์ และป้องกันโปรแกรมดาวน์โหลดข้อมูล หรือควบคุมการใช้งานที่ไม่จำเป็นประเภท P2P, Multimedia, FTP เป็นต้น

3. การติดตั้งระบบ Enterprise Anti-Virus เพื่อป้องกันไวรัสที่อาจจะเข้ามากระจายและโจมตี ผ่านทางเข้า-ออกระบบเครือข่ายอินเทอร์เน็ตขององค์กร เช่น การรับ-ส่งอีเมล์ การเปิดเข้าเว็บไซต์ที่มีไวรัส และป้องกันไวรัสที่จะเข้ามาโจมตีบนเครื่องคอมพิวเตอร์ เป็นต้น

4. ออกแบบระบบให้สามารถรองรับตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (สามารถอ่านบทความเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ฉบับต่อไป)

5. การตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล และช่องโหว่ของโปรแกรมที่เปิดให้บริการในปัจจุบันเพื่อไม่มีช่องโหว่หรือพยายามให้มีน้อยที่สุด โดยอาจเพิ่มความปลอดภัยให้กับระบบขององค์กรได้ ดังนี้

5.1 แก้ไขค่าพื้นฐาน (Default) ที่เกิดจากการติดตั้งระบบปฏิบัติการ หรือโปรแกรมในครั้งแรกบนเครื่องแม่ข่าย (Server) เนื่องจากอาจจะทำให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาได้

5.2 ทำการลง Patch หรือการลง Hotfix หลังการติดตั้งระบบปฏิบัติการและโปรแกรมทุกครั้งอย่างสม่ำเสมอจากเว็บไซต์ของเจ้าของผลิตภัณฑ์

5.3 ทำการปิด Port Service อื่นๆที่ไม่มีความจำเป็นต้องใช้ในการเปิดให้บริการบนเครื่อง Server

5.4 จัดหาโปรแกรมที่ใช้ตรวจสอบหาช่องโหว่ต่างๆบนเครื่อง Server ที่เปิดให้บริการ เช่น Nessus , Eye Retina , ISS Internet Scanner, Microsoft MBSA, GFI LAN guard และ Shadow Security Scanner เป็นต้น

5.5 สามารถติดตามข่าวสารและหาข้อมูลเพิ่มเติมทางด้านระบบรักษาความปลอดภัยได้ที่เว็บไซต์ www.cert.org ,www.sans.org , www.isaca.org, www.isc2.org และ www.thaicert.nectec.or.th เป็นต้น

6. มีการกำหนดนโยบายระบบการรักษาความปลอดภัยภายในองค์กร ดังนี้

6.1 มีคณะกรรมการบริหารจัดการด้านความปลอดภัยเครือข่ายสารสนเทศเพื่อการวางแผนและการป้องกันทางด้านระบบการรักษาความปลอดภัย

6.2 มีระเบียบ ข้อตกลงด้านการรักษาความปลอดภัยสารสนเทศ ในการจัดจ้าง หรือดำเนินงานด้านสารสนเทศ กับบุคคลภายนอก

6.3 มีการจัดทำระบบบัญชีรายการทรัพย์สินทางด้าน ICT และทำการติดตามและตรวจสอบอย่างสม่ำเสมอ

6.4 มีการจำกัดสิทธิ และการแบ่งชั้นความลับในการเข้าถึงระบบและฐานข้อมูลของพนักงาน ตามตำแหน่ง หน้าที่ และความรับผิดชอบ

6.5 มีการกำหนดหน้าที่ความรับผิดชอบทางด้านสารสนเทศของบุคลากรในองค์กรอย่างเป็นลายลักษณ์อักษร

6.6 มีขั้นตอนการปฏิบัติงานที่ชัดเจน สำหรับรับมือกับเหตุการณ์ การละเมิดความปลอดภัย คอมพิวเตอร์ เป็นลายลักษณ์อักษร

6.7 มีการกำหนดหน้าที่ความรับผิดชอบ ทางด้านสารสนเทศของบุคลากรในองค์กรอย่างเป็นลายลักษณ์อักษร

6.8 มีนโยบายและการตรวจสอบรหัสผ่านของผู้ใช้ เช่น ต้องมีมากกว่า 8 ตัวอักษร ที่คาดเดาได้ยาก และต้องกำหนดการหมดอายุการใช้งานของรหัสผ่านของผู้ใช้งาน

6.9 มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้ในองค์กรมีลิขสิทธิ์ถูกต้องตามกฎหมาย

6.10 กำหนดนโยบายการเข้าใช้งานระบบเครือข่ายของอุปกรณ์เคลื่อนที่ชนิดต่างๆ เช่น Notebook ,Palm เป็นต้น โดยจะต้องมีการ Login เข้าใช้งานเครือข่ายอินเทอร์เน็ตทุกครั้งที่เข้าใช้งาน เพื่อการป้องกันไม่ให้บุคคลภายนอกเข้ามาใช้งานระบบเครือข่ายขององค์กร

6.11 มีการตั้งเวลา เครื่องคอมพิวเตอร์ทุกเครื่องในองค์กรให้มีเวลา ตรงกัน กับมาตรฐานกลาง

6.12 มีระบบติดตามการใช้งานของผู้ใช้งานภายในองค์กร

6.13 มีระบบสำรองสารสนเทศ กรณีสารสนเทศเกิดมีปัญหา

6.14 มีข้อกำหนด และบทลงโทษแก่ผู้ที่ละเลยต่อการปกป้องข้อมูลส่วนบุคคล การก่อกวนและโจมตีระบบเครือข่ายภายในขององค์กร

สุดท้าย องค์กรที่เล็งเห็นความสำคัญ ในเรื่องการนำระบบรักษาความปลอดภัย มาใช้งานบนระบบเครือข่ายภายในองค์กร จะสามารถช่วยลดความเสี่ยงของการถูกโจมตี ก่อกวน การหยุดชะงักของระบบอันจะเป็นการป้องกัน มิให้เกิดความเสียหายขึ้นทางด้านการให้บริการต่างๆ ขององค์กรในอนาคต โดยการพิจารณาลงทุนทางด้านระบบรักษาความปลอดภัยนี้ควรพิจารณาบนพื้นฐานของความจำเป็นของธุรกิจท่านเป็นเกณฑ์การตัดสินใจลงทุน