เตรียมรับมือ Big Data Crisis ด้วย Data Management

วิชญ์คุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

รูปแบบวิธีการประมวลผลข้อมูล

การใช้ระบบคอมพิวเตอร์ช่วยในการประมวลผลข้อมูลนั้น มีวิธีการประมวลผลได้หลายรูปแบบ ดังนี้

1. **การประมวลผลแบบชุด** (Batch processing) คือ การประมวลผลโดยผู้ใช้จะทำการรวบรวมข้อมูลที่ต้องการจะประมวลผลไว้เป็นชุดๆ ซึ่งแต่ละชุดจะมีการกำหนดจำนวนรายการข้อมูลไว้เท่าๆ กัน แล้วนำเข้าสู่ระบบ จากนั้นจึงเรียกใช้คำสั่งให้ประมวลผลชุดข้อมูล ซึ่งจะสามารถทำพร้อมกันได้มากน้อยขึ้นอยู่กับข้อกำหนดของโปรแกรม และศักยภาพของระบบคอมพิวเตอร์ที่ใช้ประมวลผล

การประมวลผลแบบชุด (Batch processing) เหมาะสำหรับองค์การที่มีปริมาณงานมาก แต่ไม่จำเป็นต้องบริการข้อมูลในทันทีทันใด เนื่องจากการประมวลผลข้อมูลจะทำเป็นช่วงเวลา บางกรณีอาจกำหนดเป็นตารางเวลาประมวลผลว่าจะประมวลผลทุกๆ เวลาเท่าไหร่ในแต่ละวัน ง่ายต่อการตรวจสอบข้อผิดพลาดของข้อมูลเนื่องจากมีการรวบรวม และแยกเป็นชุดๆ

2. **การประมวลผลแบบโต้ตอบ** (Interactive) **หมายถึง** การทำงานในลักษณะที่ระบบประมวลผลมีการโต้ตอบกับผู้ใช้ โดยผู้ใช้สามารถที่จะตรวจสอบข้อมูลได้ตลอดเวลา

การประมวลผลแบบโต้ตอบ (Interactive) นั้น จะให้ผลลัพธ์ได้ทันต่อความต้องการของผู้ใช้ในทันที แต่มีโอกาสผิดพลาดมากกว่าการประมวลผลแบบชุด (Batch processing) หากข้อมูลที่นำมาประมวลผลมีปริมาณมาก ซึ่งภาระจะตกอยู่ที่ผู้ใช้เป็นผู้ตรวจสอบซึ่งโอกาสผิดพลาดอาจมีสูงขึ้น และการแก้ไขข้อผิดพลาดของข้อมูลทำได้ยากกว่า

3. **การประมวลผลแบบออนไลน์** (Online processing) **คือ** การประมวลผลร่วมกันระหว่างคอมพิวเตอร์ที่เชื่อมต่อกันผ่านระบบเครือข่ายทั้งภายในองค์การแบบ Intranet หรือระหว่างองค์การผ่าน WAN หรือผ่าน Internet ซึ่งจะทำการประมวลผลในลักษณะแบบชุด (Batch processing) หรือแบบโต้ตอบ (Interactive) ขึ้นอยู่กับจำนวนข้อมูล และความต้องการของผู้ใช้งาน

การจัดการระบบรักษาความปลอดภัยข้อมูล

ระบบการรักษาความปลอดภัยข้อมูล ถือเป็นส่วนที่มีความสำคัญ องค์การต้องมีการดำเนินการอย่างเหมาะสมโดยอ้างอิงมาตรฐานด้านความมั่นคงปลอดภัยทางสารสนเทศ เพราะความเสียหายที่เกิดขึ้นอาจไม่สามารถที่จะคาดเดาขอบเขต และผลกระทบได้

การจัดการระบบการรักษาความปลอดภัยข้อมูลที่อาศัย Information Security Management Framework มีขั้นตอนต่างๆ ดังนี้

ขั้นตอนที่ 1 การบริหารความเสี่ยง การทำ Vulnerability Assessment **และ** Penetration Testing

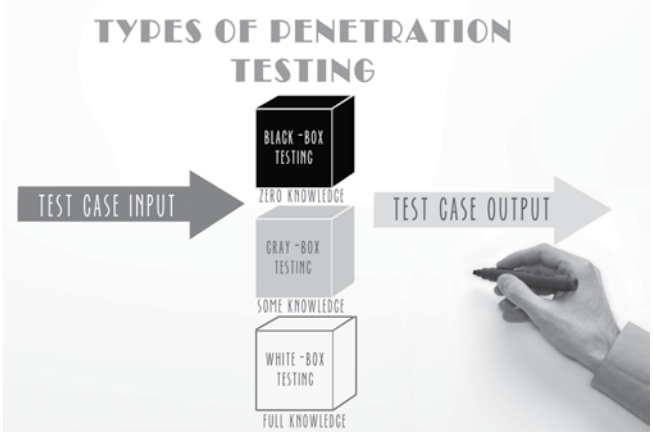
ขั้นตอนแรกในการจัดการระบบการรักษาความปลอดภัยข้อมูล คือ การบริหารความเสี่ยง การทำ Vulnerability Assessment และ การทำ Penetration Testing ซึ่งวัตถุประสงค์ในขั้นตอนแรกนี้คือการหาข้อมูลคุณลักษณะของระบบสารสนเทศ และฐานข้อมูลที่องค์การใช้งานในมุมมองด้านการรักษาความปลอดภัย โดยผลลัพธ์ที่ได้คือปัญหาด้านความปลอดภัยที่จะเกิดขึ้นกับระบบ และแนวทางในการแก้ไขปัญหาต่างๆ

การทำ Vulnerability Scanner คือ การวิเคราะห์ตรวจสอบหาช่องโหว่ต่างๆ ในระบบโดยใช้ Security Tools ต่างๆ เช่น Acunetix Web Vulnerability Scanner, GFI LANguard Network Security Scanner, Nessus™ vulnerability scanner เป็นต้น

การทำ Penetration Testing คือ การทดสอบเจาะระบบเพื่อโจรกรรมข้อมูลสำคัญ เช่น บัญชีผู้ใช้พร้อมทั้ง รหัสผ่าน รวมถึงข้อมูลอื่นๆ ที่สำคัญ โดยการทดสอบในลักษณะนี้จะดำเนินการเหมือนกับการเจาะระบบโดยแฮกเกอร์ การทำ Penetration Testing แบ่งออกเป็น 2 รูปแบบ คือ Black-Box Penetration Testing และ White-Box Penetration Testing Black-Box Penetration Testing คือ กระบวนการทดสอบการเจาะระบบ โดยผู้ทดสอบจะไม่ได้รับข้อมูลรายละเอียดของระบบ จะได้รับข้อมูลเพียง URL หรือ IP Address เท่านั้น ซึ่งผู้ทดสอบระบบจะดำเนินการแฮกระบบผ่าน Internet

ในการทดสอบจะได้ผลลัพธ์เชิงรายละเอียดมากน้อยเพียงใดขึ้นอยู่กับความสามารถของผู้ทำการทดสอบ ข้อดีของการทำ Black-Box Penetration Testing คือ สามารถประเมินความแข็งแกร่งของระบบได้จากภายนอกระบบโดยข้อสรุปที่ได้จะเป็นข้อสรุปในลักษณะความยากง่าย และความเป็นไปได้ในการเจาะระบบผ่าน Internet ข้อเสียของการทำ Black Box Penetration Testing คือ การเจาะระบบจากภายนอก อาจไม่สามารถเจาะเข้าระบบได้ เพราะข้อมูลมีน้อย หรือผู้ทดสอบระบบมีความสามารถไม่มากพอ และผลลัพธ์ที่ได้ไม่ได้บ่งบอกว่าระบบย่อยต่างๆ ที่ทำงานร่วมกันในระบบทดสอบ มีช่องโหว่มากน้อยเพียงใด และต้องดำเนินการกับระบบย่อยเหล่านั้นอย่างไรบ้าง

ส่วน White Box Penetration Testing คือ การทดสอบการเจาะระบบ โดยผู้ทดสอบจะดำเนินการเจาะระบบจากภายในระบบที่



ต้องการทดสอบ ข้อดีของการทำ White Box Penetration Testing คือ ผู้ทดสอบระบบจะสามารถประเมินความเสี่ยงได้ใกล้เคียงกับความเป็นจริงมากกว่าแบบ Black Box Testing เนื่องจากผู้ทดสอบระบบจะทราบข้อมูลภายในของระบบได้มากกว่า ข้อเสียของการทำ White Box Penetration Testing คือ การเจาะระบบจากภายในจะให้ผลลัพธ์ คือ ความปลอดภัยของระบบย่อยต่างๆ แต่ไม่สามารถระบุปัญหาในกรณีที่มีแฮกเกอร์โจมตีจากภายนอกระบบได้ ดังนั้นถ้าสามารถดำเนินการได้ควรทำทั้ง 2 รูปแบบ แล้วนำข้อมูลมาประมวลผลร่วมกันจึงจะให้ผลลัพธ์ คือช่องโหว่ต่างๆ ที่สำคัญพร้อมทั้งแนวทางในการแก้ไขช่องโหว่ดังกล่าวที่ครบถ้วน

ขั้นตอนที่ 2 การทำ Critical Hardening / Patch และ Fixing

หลังจากที่ทำการหาช่องโหว่โดยกระบวนการ Scan และกระบวนการ Penetration Testing ขั้นตอนต่อมาจะเป็นการจัดลำดับความสำคัญของช่องโหว่ที่พบว่าช่องโหว่ใดที่มีความจำเป็นเร่งด่วนที่ต้องแก้ไข โดยสามารถจัดเป็นลำดับ หรือจัดเป็นกลุ่ม เช่น กลุ่มช่องโหว่ที่ทำให้เกิดความเสี่ยงในระดับ สูง กลาง ต่ำ เป็นต้น สำหรับกระบวนการค้นหาช่องโหว่ในระบบโดยใช้โปรแกรม Vulnerability Scanner เช่น Nessus, Retina, Internet Scanner และ Shadow Security Scanner จะสามารถจัดลำดับความสำคัญได้โดยอัตโนมัติจากช่องโหว่ต่างๆ ในระบบนั้น และจำเป็นต้องมีการทำ Hardening เพื่อปิดช่องโหว่ต่างๆ โดยจะเน้นไปที่ช่องโหว่ที่มีนัยสำคัญในระดับสูงก่อนกระบวนการทำ Hardening ที่สำคัญได้แก่

- ปิด Port ของบริการต่างๆ ที่ไม่จำเป็นต้องใช้งานของ Host/Server ต่างๆ ในระบบ
- แก้ไขการตั้งค่าระบบที่เป็นค่า Default ในการติดตั้งระบบครั้งแรก
- ทำการติดตั้ง Patch หรือ Hotfix
- ติดตั้ง และใช้งานโปรแกรม Personal Firewall ในการป้องกัน และตรวจจับ IP Address ของผู้บุกรุก
- ปิด Port หรือบริการต่างๆ ที่ Border Firewall และ Border Router ACL

อ่านต่อฉบับหน้า