เตรียมรับมือ Big Data Crisis ด้วย Data Management จบ

วิชญ์คุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ขั้นตอนที่ 6 การทำ Internal และ external audit และการทำ Re-assessment และ Re-hardening

ในกระบวนการที่ดำเนินการตามขั้นตอนตั้งแต่ขั้นตอนแรกนั้น จะมีการดำเนินการตรวจสอบหาช่องโหว่ในระบบแล้วจึงปิดช่องโหว่ด้วยกระบวนการต่างๆ มากมาย แต่ผู้ดูแลระบบจะแน่ใจได้อย่างไรว่าระบบที่ผ่านกระบวนการ Hardening แล้วจะมีช่องโหว่หลงเหลืออยู่หรือไม่ ดังนั้นจึงต้องมีกระบวนการในการตรวจสอบอีกครั้ง โดยขั้นตอนนี้จะเป็นการดำเนินการซ้ำในขั้นตอน Assessment และมีการทำ Hardening ในส่วนของช่องโหว่ที่ยังค้างอยู่ในระบบ นอกจากนี้ยังต้องดำเนินการประเมินความเสี่ยงที่เกิดขึ้นกับระบบ (Risk Assessment) หรือแม้กระทั่งขององค์การทั้งหมด ซึ่งมีขั้นตอนที่ต้องปฏิบัติคือ

- การระบุปัจจัยที่มีผลต่อความเสี่ยง และการระบุความเสี่ยงต่างๆ ที่มีโอกาสเกิดขึ้น (Risk Identification)
- การวิเคราะห์ความเสี่ยง (Risk Analysis)
- การบริหารจัดการกับความเสี่ยง (Risk Management)

กระบวนการที่ทำให้ทราบข้อมูลเกี่ยวกับระบบได้ดีที่สุดคือกระบวนการตรวจสอบ (Audit) โดยกระบวนการตรวจสอบต่างๆ นั้นจำเป็นต้องพิจารณาถึงการควบคุมการทำงานต่างๆ ว่าทำได้ถูกต้องหรือไม่ โดยการควบคุมต่างๆ ในระบบแบ่งออกได้เป็น 3 ประเภทคือ

- การควบคุมแบบป้องกันล่วงหน้า (Preventive Control)
- การควบคุมแบบค้นหาประวัติเหตุการณ์ที่เกิดขึ้น (Detective Control)
- การควบคุมแบบแก้ไขปัญหาจากเหตุการณ์ที่เกิดขึ้น (Corrective Control)

สำหรับการตรวจสอบระบบสารสนเทศ (IT Audit) ควรพิจารณาการควบคุมใน 3 มุมมองพร้อมๆ กัน ได้แก่

- มุมมองด้านการบริหารจัดการ (Administrative Control)
- มุมมองด้านเทคนิค (Technical Control)
- มุมมองด้านกายภาพ (Physical Control)

ประเภทของ IT Audit สามารถแบ่งออกเป็น 7 ประเภทได้แก่

- การตรวจสอบระบบปฏิบัติการ
- การตรวจสอบอุปกรณ์เครือข่าย
- การตรวจสอบอุปกรณ์รักษาความปลอดภัย
- การตรวจสอบโปรแกรมฐานข้อมูล
- การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการทางเครือข่ายต่างๆ (Server)
- การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control)
- การตรวจสอบด้านกายภาพ (Physical Control)

ขั้นตอนที่ 7 การทำ Managed Security Service (MSS) และ Real-time Monitoring โดยใช้ระบบ IDS และ IPS

สำหรับระบบที่ต้องการการดูแลจากผู้เชี่ยวชาญ และยังไม่มีทีมผู้ดูแลระบบที่สามารถดูแลระบบทั้งหมดได้ การจัดจ้าง Outsource ด้านการรักษาความปลอดภัยในระบบโดยเฉพาะ เป็นแนวคิดที่ต้องการให้ Outsource มาช่วยในการบริหารความเสี่ยงที่อาจจะเกิดขึ้นในระบบ และช่วยลดความเสี่ยงในระบบโดยรวม การเลือก Managed Security Service Provider (MSSP) จึงเป็นหัวใจสำคัญในการบริหารระบบ ขณะเดียวกันต้องมีการกำหนดข้อตกลงเกี่ยวกับระดับการให้บริการ และการรับผิดชอบ (Service Level Agreement) ให้ชัดเจน โดยควรมีรายละเอียดให้มากที่สุดเท่าที่จะทำได้ เช่น

- ขอบเขตในการให้บริการของ MSSP
- ระยะเวลาในการให้บริการ และการตอบสนองของ MSSP
- ค่าใช้จ่ายที่เกิดขึ้นในแต่ละเดือน
- ความรับผิดชอบของ MSSP ในแง่กฎหมาย และบทปรับ

สำหรับหน้าที่ความรับผิดชอบของ MSSP ควรให้บริการครอบคลุมหัวข้อต่างๆ ดังต่อไปนี้

- บริหารจัดการ และเฝ้าระวัง ดำเนินการเกี่ยวกับ Network Perimeter Security ที่ External Firewall, Border Router, IDS/IPS, VPN ตลอดจน Server บริเวณ DMZ
- บริหารจัดการ Vulnerability ให้กับระบบขององค์การอย่างต่อเนื่อง เช่นการทำ Vulnerability Assessment และทำ Penetration Testing รายเดือน เป็นต้น
- เฝ้าระวัง Internal Network จาก Virus และ Hacker
- เฝ้าระวัง Internal Firewall และ Server Farm ภายในระบบ LAN ขององค์การ
- รับปรึกษาในกรณีที่เกิดปัญหาความปลอดภัย รับแก้ปัญหาในลักษณะ Incident Response และ Digital Forensic (การพิสูจน์หลักฐานทางอิเล็กทรอนิกส์)
- บริหารจัดการ Centralize Log Management และ Centralize Patch Management อย่างเป็นระบบ
- บริการแจ้งข่าวความเคลื่อนไหวด้าน Information Security โดยเฉพาะเรื่องเกี่ยวกับช่องโหวใหม่ๆ ไวรัสที่กำลังแพร่ระบาดในขณะนั้น ให้ทราบในลักษณะวันต่อวัน

ข้อดีในการที่องค์การจัดจ้าง MSSP คือ

- สามารถช่วยลดต้นทุนการดำเนินการในองค์การด้านอัตรากำลัง ของบุคลากรเชี่ยวชาญได้รวมถึง Hardware/ Software ต่างๆ
- สามารถได้รับข่าวสารใหม่ๆ ด้าน Information Security
- ได้รับคำปรึกษาเมื่อเกิดปัญหา
- คอยเตือนภัยทาง Internet ให้องค์การทราบอยู่ตลอดเวลา

ข้อเสียของการจัดจ้าง MSSP

- ถ้าสัญญาไม่รัดกุมพอจะทำให้เกิดปัญหาในทางปฏิบัติได้
- หาก MSSP ไม่มีความเชี่ยวชาญพอ จะทำให้ไม่คุ้มค่าในการลงทุน
- อาจเกิดกรณีที่ระบบเกิดปัญหาแต่ MSSP ไม่สามารถแก้ไขปัญหาหรือให้คำปรึกษาที่เหมาะสมได้ตามที่คาดหวังไว้

ถึงแม้ว่าจะมีข้อเสียในการจัดจ้าง MSSP แต่ข้อดีก็มีมากกว่า การตกลงทำงานร่วมกันกับ MSSP ในลักษณะที่ช่วยเหลือซึ่งกันและกัน โดยงานที่ต้องใช้ความสามารถเฉพาะทางจะมอบให้ MSSP เป็นผู้ดูแล ส่วนองค์การจะเป็นผู้ตรวจสอบการทำงานของ MSSP ว่าปฏิบัติตาม Service Level Agreement หรือไม่ โดยปัจจุบันในประเทศไทยมีผู้ให้บริการ MSSP แล้วหลายเจ้า และได้รับการรับรองมาตรฐานในระดับสากล

โดยสรุปแล้ว การบริหารจัดการข้อมูลที่มีปริมาณมากนั้น ถึงแม้องค์การอาจจะมองว่าส่วนใหญ่จะเป็นเรื่องทางเทคนิคก็เลยมอบหมายให้ฝ่ายเทคโนโลยีสารสนเทศเป็นผู้ดูแลรับผิดชอบ ซึ่งความจริงแล้วหน่วยงานย่อยภายในองค์การ หรือแม้แต่ตัวบุคลากรผู้ที่เป็นผู้ผลิตข้อมูล ผู้นำเข้า หรือใช้ประโยชน์จากข้อมูลเป็นผู้ที่มีบทบาทสำคัญอย่างยิ่งต่อการบริหารจัดการข้อมูล เนื่องจากต้องมีการสร้างความเข้าใจร่วมกันในทิศทางการทำงาน แนวปฏิบัติขั้นตอนที่มีความเหมาะสมกับข้อมูลประเภทต่างๆ ซึ่งองค์การใช้นโยบาย ระเบียบ และแนวปฏิบัติเป็นเครื่องมือในการกำหนดกรอบ และทิศทางการทำงานให้เป็นไปในทิศทางเดียวกันทั้งองค์การ แล้วจึงให้ความสำคัญกับการเลือกใช้เทคโนโลยีการจัดเก็บ บริหารจัดการ และประมวลผลข้อมูลที่เหมาะสม และสมประโยชน์ร่วมกันทั้งองค์การ กำหนดระดับการเข้าถึง การใช้งาน และมาตรการรักษาความปลอดภัยในระดับที่สร้างให้เกิดความน่าเชื่อถือของข้อมูล ลดความเสี่ยง และผลกระทบหากเกิดความเสียหาย รวมถึงการวางแผนเพื่อรับมือกับสถานการณ์ที่ไม่อาจคาดเดาได้

ซึ่งในข้อเท็จจริงที่ผ่านๆ มา ความเสียหายเกี่ยวกับข้อมูลที่เกิดขึ้นกับองค์การทั่วโลกนั้น เกิดจากการไม่ให้ความสำคัญกับการบริหารจัดการที่รัดกุม และเหมาะสม ขาดการรักษาความมั่นคงปลอดภัยที่ดี ซึ่งจริงๆ แล้วองค์การไม่ต้องลงทุนสูง เพียงแค่บุคลากรภายในองค์การมีความตระหนัก และช่วยกันปฏิบัติตามนโยบายอย่างเคร่งครัด ก็สามารถสร้างความมั่นคงด้านข้อมูลให้กับองค์การได้เป็นอย่างดี แต่ทั้งนี้ก็ขึ้นอยู่กับความสามารถของผู้บริหาร และวัฒนธรรมขององค์การ เพราะคงไม่มีใครอยากให้เกิดกรณีของ Panama Paper ขึ้นกับองค์การเป็นแน่ ด้วยเทคโนโลยีที่พัฒนาอย่างต่อเนื่องเพื่อรองรับความต้องการ รวมถึงการพัฒนาแนวทางเพื่อแก้ไขปัญหาด้านเทคนิคอย่างมีประสิทธิภาพทำให้ไม่ว่าจะมีข้อมูลปริมาณมหาศาลเพียงใดก็ไม่ยากเกินกว่าที่จะบริหารจัดการได้ TPA news

ข้อมูลอ้างอิง:

www.visioncritical.com
www.crisistextline.org
www.somkiat.cc
www.koonnapab.com
datasecuritymanagement.com
oodbms-ict.blogspot.com
www.bigcrisisdata.org
www.trendmicro.com