ระบบความปลอดภัยข้อมูลของคุณใช้การได้ดีอยู่หรือไม่?

ทูลด้านการรักษาความปลอดภัยไม่ใช่เป็นแบบที่ “กำหนดค่าครั้งเดียว แล้วใช้งานไปได้ตลอด”

ไม่ต้องสงสัยเลยว่าระบบรักษาความปลอดภัยข้อมูลกำลังมีอัตราการขยายตัวอย่างก้าวกระโดด แต่เนื่องจากอุปกรณ์ด้านการรักษาความปลอดภัยรวมทั้งเทคนิควิธีการต่างๆ มีความซับซ้อนและมีจำนวนเพิ่มขึ้น คุณจะแน่ใจได้อย่างไรว่าระบบรักษาความปลอดภัยของคุณได้รับการปรับปรุงที่ดีพอแล้ว? และถูกต้องตามกฎระเบียบหรือไม่? เราสามารถวิ่งตามแนวโน้มต่างๆ ตามที่ได้ตั้งใจไว้ได้ดีแค่ไหน?

ป้องกันให้ครอบคลุมและทั่วถึง

หากถามเจ้าหน้าที่ผู้ดูแลระบบการรักษาความปลอดภัยข้อมูลว่ารู้สึกกังวลเกี่ยวกับเรื่องใด เกือบทั้งหมดจะตอบว่ากังวลกับจุดอ่อนในระบบซึ่งยังไม่มีเวลาแก้ไข อาจเป็นสิ่งที่มองข้ามไปหรือช่องโหว่ที่คิดว่าใช่แน่ๆ แต่ไม่มีข้อพิสูจน์ ทั้งหมดนี้เป็นสิ่งที่ผู้เชี่ยวชาญระบบรักษาความปลอดภัยข้อมูลไม่อยากพบเจอ

ผู้เชี่ยวชาญระบบความปลอดภัยข้อมูลยอมรับความจริงในข้อนี้และพยายามหาทางลดความเสี่ยงลงโดยใช้ระบบป้องกันที่ครอบคลุมและทั่วถึงเพื่อลดความเสี่ยงขององค์กรจากจุดอ่อนต่างๆ

ระบบป้องกันที่ครอบคลุมและทั่วถึงคือแนวความคิดของการติดตั้งแนวป้องกันหลายชั้น (layer) เพื่อเป็นการลดความเสี่ยง หากอุปกรณ์ตัวใดตัวหนึ่งหรือเลเยอร์ใดเลเยอร์หนึ่งใน DMZ ถูกบุกรุก ก็ยังมีเลเยอร์อื่นป้องกันได้อยู่ การที่จะใช้วิธีการนี้ได้ดีจำเป็นต้องมีพนักงานที่ได้รับการฝึกอบรมมาเป็นอย่างดี เครื่องมือและกระบวนการที่มีประสิทธิภาพ มีนโยบายที่ชัดเจน และมีการฝึกอบรมผู้ใช้ แม้ว่าไม่สามารถขจัดความเสี่ยงออกไปได้ทั้งหมด แต่ระบบนี้ก็นับว่าเป็นวิธีการที่มีประสิทธิภาพมากที่สุดในการลดความรุนแรงของปัญหา

มีความตั้งใจดี

การตรวจสอบระบบและปฏิบัติตามข้อกำหนดกฎเกณฑ์ต่างๆ เริ่มได้รับความนิยมแพร่หลายยิ่งขึ้น องค์กร และอุตสาหกรรมต่างๆ กำลังพยายามปฏิบัติตนให้สอดคล้องกับกฎหมาย และกฎเกณฑ์ด้านการรักษาความปลอดภัยอื่นๆ ยกตัวอย่างเช่น Sarbanes-Oxley Act, HIPAA และ FISMA เป็นเพียงส่วนหนึ่งของข้อกำหนดกฎเกณฑ์ที่ทำให้องค์กรต่างๆ ต้องเพิ่มการควบคุมระบบรักษาความปลอดภัยข้อมูลมากขึ้น ความสำเร็จจากการติดตั้งระบบควบคุมเหล่านี้ล้วนต้องการระบบความปลอดภัยข้อมูลเพิ่มขึ้นและต้องเสริมด้วยการป้องกันเชิงลึก (Defense in Depth) และต้องทำด้วยความเร่งรีบอีกด้วย

เน้นหนักในรายละเอียด

เจ้าหน้าที่ระบบความปลอดภัยข้อมูลมีเป้าหมายเดียวกันคือปกป้องค์กรของตน แต่ประสบการณ์ทำงานของแต่ละคนมักแตกต่างกันมาก ไม่ว่าจะเป็น

- ผู้ดูแลระบบวินโดวส์
- ผู้ดูแลระบบยูนิกซ์
- ผู้ดูแลระบบเครือข่าย/ไฟร์วอลล์
- นักพัฒนา และผู้ตรวจสอบนโยบาย

ประสบการณ์ทำงานในแต่ละสาขานี้มีคุณค่าเป็นอย่างยิ่งต่อการสร้างระบบความปลอดภัยข้อมูลที่มีประสิทธิภาพ แต่โดยธรรมชาติแล้วทุกๆ คนมักสนใจแต่ในระบบที่ตนมีความถนัดหรือมีความเข้าใจอยู่เท่านั้น จึงมักส่งผลให้ทำการติดตั้งระบบความปลอดภัยในระบบนั้นๆ ก่อน

หลายๆ เลเยอร์ของการป้องกันเชิงลึกมักรวมอยู่ในสาขาเดียวกัน ผู้ดูแลระบบยูนิกซ์อาจกำหนดการควบคุมระบบรักษาความปลอดภัยไว้หลากหลาย แต่ถ้าบริษัทไม่มี

ความปลอดภัยข้อมูลนั้นต้องพิจารณาโดยชั่งน้ำหนักระหว่างระบบความปลอดภัยข้อมูลราคาแพงกับบทเรียนราคาแพงของการถูกเจาะระบบ

นโยบายกำหนดให้ใช้รหัสผ่าน ระบบเหล่านั้นก็ยังมีความเสี่ยงสูงที่จะถูกบุกรุกอยู่ดี

ความจริงข้อนี้เองทำให้มีการกำหนดให้ผู้ดูแลระบบรักษาความปลอดภัยสามารถปฏิบัติงานได้ในทุกๆ ที่ในองค์กรอย่างไม่จำกัด โดยไปแบ่งสรรกันในทีมงานว่าแต่ละคนถนัดในการทำงานในพื้นที่ใด

จะรันเครื่องไม้เครื่องมือต้องใช้คน

ในขณะที่บริษัทต่างๆ ยังคงเพิ่มงบประมาณสำหรับเครื่องไม้เครื่องมือ (ทูล) ด้านการรักษาความปลอดภัยข้อมูล แต่บางทีก็ไม่ยอมเพิ่มงบประมาณจัดจ้างพนักงานเพื่อทำการติดตั้งและบริหารจัดการเครื่องไม้เครื่องมือเหล่านั้น ทุกๆ ปีบริษัทต่างๆ อนุมัติงบประมาณสำหรับซื้อหาเครื่องไม้เครื่องมือเหล่านี้เพราะได้รับแรงกดดันมาจากการถูกตรวจสอบ หรือเครือข่ายถูกบุกรุกในปีก่อนหน้า

แต่เครื่องไม้เครื่องมือด้านการรักษาความปลอดภัยข้อมูลก็ใช้งานไม่ง่ายนัก เช่น การติดตั้งและปรับใช้ให้สอดรับกับสภาพของแต่ละบริษัท การติดตั้งใหม่ต้องใช้ทรัพยากรเป็นจำนวนมากและหากสภาพการใช้งานเปลี่ยนแปลงบ่อยก็ต้องปรับปรุงเครื่องไม้เครื่องมือบ่อยๆ ตามไปด้วย ที่สำคัญที่ก็คือมีช่องโหว่ใหม่ๆ เกิดขึ้นทุกสัปดาห์ ทำให้ต้องปรับปรุงซิกเนเจอร์ และเครื่องไม้เครื่องมือต่างๆ ด้วย

หากมีระยะเวลาติดตั้งน้อยเกินไปหรือทรัพยากรไม่เพียงพอ โซลูชันต่างๆ เหล่านี้อาจกลายเป็น shelfware ไปได้ เป็นเรื่องธรรมดาที่เราต้องพึ่งพาเทคโนโลยีในการแก้ปัญหา อย่างไรก็ตามในเรื่องของระบบความปลอดภัยข้อมูลและการบริหารจัดการเครือข่ายจำเป็นอย่างยิ่งที่ต้องมีคน เวลา และการผนวก/ปรับแต่งระบบ ซึ่งถือเป็นส่วนประกอบสำคัญของโซลูชันที่มีประสิทธิภาพสูง

มีคำถามข้อหนึ่งที่ผมมักจะถามเจ้าหน้าที่ระบบความปลอดภัยข้อมูลอยู่เสมอก็คือ “เหตุใดจึงคอยเฝ้าตรวจสอบไฟร์วอลล์ ระบบ และล็อกของระบบตรวจจับการบุกรุก (IDS log)” คำตอบที่ได้มักเป็นว่า “เนื่องจากผมกำลังหาทางแก้ปัญหาข้อหนึ่งอยู่” เราใช้เครื่องไม้เครื่องมือเหล่านี้เพื่อติดตามผล ป้องกัน และเตือนพวกเราในกรณีระบบความปลอดภัยข้อมูล

กับดักของการตรวจสอบ

มีข้อโต้แย้งกันว่า การตรวจสอบ (Audit) คือสิ่งที่ดีที่สุดสำหรับการสร้างความตระหนักในเรื่องเกี่ยวกับระบบความปลอดภัยข้อมูล การตรวจสอบมักก่อให้เกิดการพัฒนานโยบาย การให้ความรู้แก่ผู้ใช้ การปรับปรุงแพตช์ และการเสริมสร้างทัศนคติทางด้านระบบความปลอดภัยทั่วทั้งองค์กร แย่หน่อยตรงที่การตรวจสอบได้ปลูกฝังให้บริษัทต่างๆ กลายเป็น “บริษัทมุสาฯ” กันไปหมด

ความจำเป็นของการต้องผ่านการตรวจสอบกลายเป็นสิ่งสำคัญที่บริษัทต่างๆ ต้องปฏิบัติ ส่งผลให้เกิดความกดดันว่าต้องผ่านไม่ว่าจะต้องเสียค่าใช้จ่ายมากน้อยเพียงใด แม้ว่าจะต้องปกปิดปัญหาและหมกเม็ดเอาไว้ก็ตาม เมื่อถึงคราวทำการตรวจสอบก็มีการใช้เครื่องไม้เครื่องมือจำนวนมากเพื่อการนี้ เจ้าหน้าที่ไอทีแจ้งว่าขณะที่กำลังตรวจสอบและวิเคราะห์ข้อมูล หน้าจอระบบป้องกันการบุกรุกของผู้ตรวจสอบแสดงคำเตือนขึ้น (แต่จริงๆ แล้วเป็นเพียงฟังก์ชันตรวจสอบธรรมดาๆ เท่านั้น) เนื่องจากผู้ตรวจสอบครอบคลุมเรื่องต่างๆ กว้างมาก จึงมักไม่ได้เป็นผู้เชี่ยวชาญในสาขานั้นๆ

> “บทสรุปก็คือระบบความปลอดภัยข้อมูลนั้นเกี่ยวข้องกับการควบคุมและการรันกระบวนการต่างๆ”

หลังจากการตรวจสอบเสร็จสิ้นไปแล้วเมื่อมาพิจารณาผลลัพธ์เรามักจะพบว่าเกิดสิ่งต่างๆ ดังนี้:

1. หากยังไม่มีข้อสรุปที่ชัดเจน บริษัทดังกล่าวจะดำเนินธุรกิจไปตามปกติ โดยมีความรู้สึกผิดว่ายังคงมีปัญหาอยู่เช่นเดิม
2. หากตรวจพบปัญหา ผลการตรวจก็จะไม่ส่งผลเปลี่ยนแปลงแต่อย่างใด โดยจะมีการอ้างว่าต้องการงบประมาณเพิ่มเติมเพื่อซื้อเครื่องไม้เครื่องมืออื่นๆ มาเสริมระบบเพื่อให้สามารถผ่านการตรวจในครั้งต่อไป

แล้วคุณจะหลับสบายหายกังวล

เรายังคงมีปัญหาจำนวนหนึ่งที่รอการแก้ไขแม้ว่าจะมีการปรับปรุงไปแล้วบางส่วน หลักการของระบบความปลอดภัยคือความรู้ความเข้าใจต่อความเสี่ยงและการนำนโยบายไปปฏิบัติ การขาดแคลนทักษะ พนักงานมีไม่เพียงพอ และความกดดันจากการตรวจสอบ ส่งผลให้ปัญหาต่างๆ ไม่ได้รับการประเมินและแก้ไขในแนวทางที่เหมาะสม

ที่ปรึกษามักให้การช่วยเหลือในช่วงเฟสแรกของการติดตั้งผลิตภัณฑ์ใหม่ ช่วยให้มั่นใจได้ว่าผลิตภัณฑ์ดังกล่าวจะได้รับการติดตั้งและผนวกเข้าด้วยกันอย่างเหมาะสม อย่างไรก็ตามต้องมีการส่งมอบและฝึกอบรมที่มีประสิทธิภาพ และที่สำคัญที่สุดคือต้องมีเจ้าหน้าที่แบบเต็มเวลาอย่างเพียงพอสำหรับการบริหารจัดการเครื่องไม้เครื่องมือเหล่านั้น

สรุปได้ว่าระบบความปลอดภัยข้อมูลนั้นเกี่ยวข้องกับการควบคุมและการรันกระบวนการที่มีการปรับปรุงเปลี่ยนแปลงอยู่ตลอดเวลา, ต้องพิจารณากันโดยชั่งน้ำหนักระหว่างระบบความปลอดภัยข้อมูลราคาแพงกับบทเรียนราคาแพงของการถูกเจาะระบบ ไม่มีเครื่องไม้เครื่องมือชนิดใดซึ่งสามารถแก้ปัญหาด้านระบบความปลอดภัยได้ทั้งหมด เราจำเป็นต้องเน้นไปที่ “คนและกระบวนการ”

กุญแจสำคัญของการป้องกันเชิงลึกคือการนำเอามืออาชีพทางด้านระบบความปลอดภัย เครือข่าย ระบบ และการปฏิบัติตามกฎหมายที่มีความรู้ความเข้าใจทรัพยากรทั้งหมดอย่างกระจ่างแจ้งมาร่วมมือกันหาทางแก้ไขปัญหาอย่างเต็มที่ ■