ความปลอดภัยของฐานข้อมูล

วัตถุประสงค์ในการรักษาความปลอดภัย

ความปลอดภัยของระบบฐานข้อมูล (database security) เป็นการป้องกันผู้ไม่มีสิทธิเข้ามาใช้ หรือแก้ไขข้อมูล และความสามารถในการป้องกันข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์ เช่น ข้อมูลที่ถูกเปลี่ยนแปลงให้ผิดพลาดได้โดยง่าย แสดงว่าข้อมูลมีความปลอดภัยต่ำ เป็นต้น ทั้งนี้ความปลอดภัยของระบบฐานข้อมูลมีความสำคัญต่อความสำเร็จขององค์กรเป็นอย่างมาก ผู้บริหารฐานข้อมูลจึงจำเป็นที่จะต้องรักษาฐานข้อมูลให้ปลอดภัย

1. ความหมายของการรักษาความปลอดภัย

การรักษาความปลอดภัยของฐานข้อมูลหมายถึงการดูแลจัดการและรักษาข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์ พร้อมสำหรับผู้ที่มีสิทธิในการใช้ข้อมูลสามารถใช้งานได้อยู่เสมอ การเสียหายของระบบฐานข้อมูลซึ่งเกิดจากข้อบกพร่องของความปลอดภัย เช่น

- เครื่องเสียในระหว่างทำงาน ถ้าไม่มีการจัดการที่ดีอาจทำให้ข้อมูลผิดพลาดได้ เช่นการโอนเงินจากบัญชี ก ไปบัญชี ข เราสามารถทำได้ 2 แบบ คือ ถอนเงินบัญชี ก ก่อนแล้วฝากเงินเข้าบัญชี ข หรือฝากเงินเข้าบัญชี ข ก่อนถอนเงินจากบัญชี ก ในแบบแรกถ้าเครื่องเกิดมีปัญหาหลังจากถอนเงินเรียบร้อยแล้ว แต่ยังไม่ได้ฝากเงิน ก็จะทำให้ผลรวมของยอดเงินหายไป ส่วนแบบหลังยอดเงินก็จะมากเกินไป ทั้งสองแบบนี้ไม่เป็นที่ต้องการ ระบบรักษาความปลอดภัยของฐานข้อมูลจึงจำเป็นต้องมีขบวนการควบคุมการทำงานในลักษณะรายการ (transaction) คือการที่ถ้าทำรายการใดไม่สำเร็จทุกขั้นตอนจะต้องเสมือนยังไม่ได้ทำขั้นตอนใดเลย

- การใช้งานพร้อมกัน อาจทำให้เกิดปัญหา ดังตัวอย่าง ถ้านาย ก ทำการถอนเงินด้วยสมุดเงินฝาก ในเวลาเดียวกับที่นาย ข ทำการถอนเงินด้วยบัตรเอทีเอ็ม จากบัญชีเดียวกัน ถ้าการทำงาน 2 รายการนี้ ไม่เป็นอิสระจากกัน คือต่างอ่านได้ยอดเงินคงเหลือก่อนถอนเท่ากัน แล้วทำการถอนเงิน จะทำให้ได้ยอดคงเหลือของบัญชีผิดพลาดได้

โดยทั่วไปการป้องกันความผิดพลาดสามรถทำได้โดยง่าย เนื่องจากระบบ DBMS ส่วนใหญ่จะมีองค์ประกอบที่ช่วยป้องกันความผิดพลาดดังตัวอย่างข้างต้นได้อยู่แล้ว จึงไม่เป็นภาระของผู้ใช้งาน

2.วัตถุประสงค์ของการรักษาความปลอดภัย

วัตถุประสงค์ของการรักษาความปลอดภัยของระบบฐานข้อมูล ก็เพื่อลดปัจจัยเสี่ยงที่เกี่ยวกับ ความเสียหายกับฐานข้อมูล เนื่องจากความผิดพลาดในการทำงานของผู้ใช้ระบบฐานข้อมูล แฟ้มข้อมูลเสียหาย ความผิดพลาดในการทำงานของเครื่องหรือเครื่องคอมพิวเตอร์ไม่สามารถทำงานได้ การปฏิบัติงานที่ไม่เหมาะสมหรือผิดปกติ เนื่องจากการใช้คำสั่งในระบบโดยไม่ได้รับอนุญาติ การทุจริต และการเปิดเผยข้อมูลที่เป็นความลับ โดยสามารถแยกวัตถุประสงค์โดยรวมของการรักษาความปลอดภัยในระบบฐานข้อมูลได้ 4 ประการ คือ

2.1 เพื่อให้สามารถรักษาข้อมูลเป็นความลับได้ (secrecy) ระบบจะต้องปกป้องข้อมูลไม่ให้ผู้ไม่มีสิทธิในการใช้ข้อมูลเข้าใช้ข้อมูลได้ และจะต้องสามารถกำหนดให้ผู้ใช้งานแต่ละคนสามารถใช้งานได้ตามสิทธิที่กำหนดเท่านั้นด้วย ควรมีการกำหนดสิทธิไว้ชัดเจน อยู่ในห้องเครื่อง มีการรักษาความปลอดภัยโดยใช้บัตรผ่าน มีการควบคุมสิทธิผู้ใช้งานอย่างรอบคอบ มีความปลอดภัยในการใช้งานในระบบเครือข่าย และมีระบบสำรองกู้คืนข้อมูลที่ดี สามารถใช้งานได้สะดวก

2.2 เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ (integrity) นั่นคือจะต้องสามารถรักษาข้อมูลให้มีความถูกต้องตามกฎเกณฑ์หรือเงื่อนไขที่ได้กำหนดไว้ตอนสร้างฐานข้อมูล ข้อมูลต้องไม่ผิดเพี้ยน รวมทั้งความถูกต้องของข้อมูลในการประมวลผลข้อมูลพร้อมกันด้วย

2.3 เพื่อให้มีฐานข้อมูลพร้อมใช้งานอยู่เสมอ (availability) สามารถทำงานได้ตามปกติและเต็มประสิทธิภาพตามจุดมุ่งหมายในการใช้ และมีขีดความสามารถปฏิบัติงานได้ตามที่ต้องการเนื่องถ้าการใช้งานระบบฐานข้อมูลมักจะมีข้อขัดข้องอยู่เสมอ เช่นเครื่องเสีย หรือไฟดับ หรือข้อมูลสูญหาย ถ้ามีการรักษาความปลอดภัยที่ดีจะทำให้ผู้ใช้งานมีความเชื่อถือในระบบฐานข้อมูลนั้น

2.4 เพื่อลดความเสี่ยง (Risk Assessment) การรักษาความปลอดภัยที่ดีจะช่วยลดความเสี่ยงในค่าใช้จ่ายที่จะเกิดขึ้นจากการเสียหายของข้อมูล การวางแผนด้านการรักษาความปลอดภัยได้อย่างเหมาะสมจะช่วยลดความเสี่ยงในการเกิดความเสียหายของข้อมูลค่าใช้จ่าย มีการประเมินความสมดุลระหว่างค่าใช้จ่ายหรือต้นทุนคุ้มค่ากับประโยชน์ที่จะได้รับจากการรักษาความปลอดภัย

3.ข้อคำนึงในการรักษาความปลอดภัยระบบฐานข้อมูล

ในการรักษาความปลอดภัยของระบบฐานข้อมูลนั้น จะต้องคำนึงถึงนโยบาย(policy)ขององค์การและสถานภาพของระบบการรักษาความปลอดภัยในปัจจุบัน(current state)

3.1.นโยบายขององค์การ นโยบายขององค์การมีผลสำคัญอย่างยิ่งต่อการรักษาความปลอดภัยของข้อมูล นโยบายขององค์การจะต้องมุ่งเน้นที่จุดมุ่งหมายและการทำงานที่ดี การกำหนดนโยบายด้านการรักษาความปลอดภัยก็เพื่อให้องค์กรสามารถดูแลรักษาระบบความปลอดภัย องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของพนักงาน พร้อมทั้งระเบียบวิธีปฏิบัติให้พนักงานใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนให้ปฏิบัติตามกฎระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ

การกำหนดนโยบายด้านการรักษาความปลอดภัย เพื่อให้องค์กรสามารถดูแลรักษาระบบความปลอดภัย องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของพนักงาน พร้อมทั้งระเบียบวิธีปฏิบัติให้พนักงานใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนปฏิบัติตามกฎ ระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ โดยต้อง

กำหนดให้แน่นอนว่าระบบรักษาความปลอดภัยนี้ใครเป็นผู้ปฏิบัติ (who) ใช้กับส่วนใดบ้างในระบบ(to what resources) มีวิธีการปฏิบัติอย่างไร(how) ผู้ใช้ผู้ใดสามารถเข้าถึงข้อมูลส่วนใดได้บ้าง รวมทั้งต้องกำหนดสิทธิว่าใครมีสิทธิกำหนดที่จะเปลี่ยนแปลงแก้ไขข้อมูลนั้นๆ

3.2.สถานภาพของระบบการรักษาความปลอดภัย โดยมีการตรวจสอบว่าในปัจจุบันสถานภาพของระบบการรักษาความปลอดภัยอยู่ในระดับใดและต้องการปรับปรุงหรือเปลี่ยนแปลงอันใดบ้าง ความต้องการในการใช้ข้อมูลที่ปลอดภัยและคำแนะนำจากส่วนต่างๆที่ใช้งานภายในระบบ การแจกงานไปสู่ผู้ที่รับผิดชอบ มีตารางเวลาที่กำหนดว่าส่วนใดของระบบจะต้องปรับปรุงอะไรบ้าง ณ เวลาใด มีการจัดทำแผนฉุกเฉิน เพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น แผนฉุกเฉินนี้อาจทำรวมเป็นแผนเดียวทั้งองค์กรหรือแยกตามงานก็ได้ แผนนี้ควรจะระบุ ชื่อคนที่จะต้องติดต่อเมื่อเกิดเหตุ อุปกรณ์หรือเครื่องมือสำรอง ตลอดจนขบวนการทำงานอย่างละเอียด บุคลากรที่เกี่ยวข้องควรจะคุ้นเคยกับแผนเหล่านี้และมีการทดสอบให้มั่นใจว่าสามารถใช้งานได้- การจัดทำแผนฉุกเฉิน เพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น แผนฉุกเฉินนี้อาจทำรวมเป็นแผนเดียวทั้งองค์กร หรือแยกตามงานก็ได้ แผนนี้ควรจะระบุ ชื่อคนที่จะต้องติดต่อเมื่อเกิดเหตุ อุปกรณ์หรือเครื่องมือสำรอง ตลอดจนขบวนการทำงานอย่างละเอียด บุคลากรที่เกี่ยวข้องควรจะคุ้นเคยกับแผนเหล่านี้และมีการทดสอบให้มั่นใจว่าสามารถใช้งานได้

ที่มา http://sot.swu.ac.th/Portals/156/sot/CP342/lesson12/ms1t1.htm