มหาวิทยาลัยราชภัฏนครปฐม
Nakhon Pathom Rajabhat University

การวางแผนและจัดการระบบความปลอดภัยในระบบฐานข้อมูล

เนื้อหา

- ความหมายของการรักษาความปลอดภัย
- วัตถุประสงค์ของการรักษาความปลอดภัย
- ข้อคำนึงถึงในการรักษาความปลอดภัยระบบฐานข้อมูล
- การควบคุมความคงสภาพของฐานข้อมูล (Database Integrity)
- การรักษาความปลอดภัยของระบบฐานข้อมูล (Database Security)
- การโจมตีข้อมูล

ความหมาย

- **การรักษาความปลอดภัยของฐานข้อมูล** หมายถึง การดูแลจัดการและรักษาข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์พร้อมสำหรับผู้ที่มีสิทธิในการใช้ข้อมูลสามารถใช้งานได้อยู่เสมอ การเสียหายของระบบฐานข้อมูลซึ่งเกิดจากข้อบกพร่องของความปลอดภัย

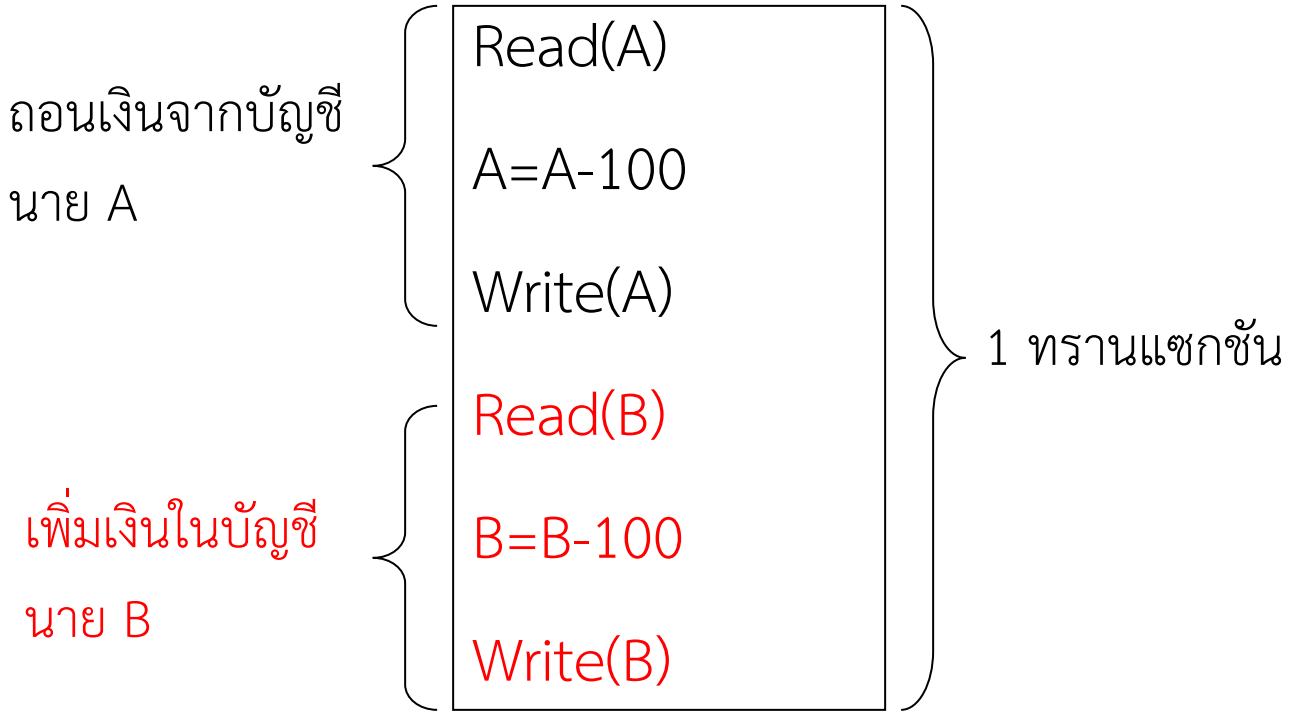
ตัวอย่าง>>เหตุการณ์ฮาร์ดแวร์เสีย

- ในระหว่างการโอนเงินจากบัญชี ก ไปบัญชี ข
  - ถอนเงินบัญชี ก ก่อนแล้วฝากเงินเข้าบัญชี ข หรือฝากเงินเข้าบัญชี ข ก่อนถอนเงินจากบัญชี ก ในแบบแรกถ้าเครื่องเกิดมีปัญหาหลังจากถอนเงินเรียบร้อยแล้ว แต่ยังไม่ได้ฝากเงิน ก็จะทำให้ผลรวมของยอดเงินหายไป ส่วนแบบหลังยอดเงินก็จะมากเกินไป ทั้งสองแบบนี้ไม่เป็นที่ต้องการ

- ระบบรักษาความปลอดภัยของฐานข้อมูลจึงจำเป็นต้องมีขบวนการควบคุมการทำงานในลักษณะรายการ (transaction) คือการที่ถ้าทำรายการใดไม่สำเร็จทุกขั้นตอนจะต้องเสมือนยังไม่ได้ทำขั้นตอนใดเลย

ตัวอย่าง>>เหตุการณ์การใช้งานพร้อมกัน

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



ความปลอดภัยของระบบฐานข้อมูล (Database Security)

- เป็นการป้องกันผู้ไม่มีสิทธิเข้ามาใช้ หรือแก้ไขข้อมูลและความสามารถในการป้องกันข้อมูลให้ถูกต้องครบถ้วนสมบูรณ์

วัตถุประสงค์ของการรักษาความปลอดภัย

- **เพื่อให้สามารถรักษาข้อมูลเป็นความลับได้ (Secrecy)** ระบบจะต้องปกป้องข้อมูลไม่ให้ผู้ไม่มีสิทธิในการใช้ข้อมูลเข้าใช้ข้อมูลได้
- **เพื่อให้ข้อมูลในฐานข้อมูลมีความถูกต้องครบถ้วนสมบูรณ์ (Integrity)** นั่นคือจะต้องสามารถรักษาข้อมูลให้มีความถูกต้องตามกฎเกณฑ์หรือเงื่อนไขที่ได้กำหนดไว้ตอนสร้างฐานข้อมูล
- **เพื่อให้มีฐานข้อมูลพร้อมใช้งานอยู่เสมอ (Availability)** สามารถทำงานได้ตามปกติและเต็มประสิทธิภาพตามจุดมุ่งหมายในการใช้
- **เพื่อลดความเสี่ยง (Risk Assessment)**

ข้อคำนึงถึงในการรักษาความปลอดภัยระบบฐานข้อมูล

- **นโยบายขององค์การ**
  - องค์กรจำเป็นต้องมีการกำหนดนโยบายด้านความปลอดภัยให้ชัดเจน โดยประกอบด้วยกฎ ข้อบังคับ และหน้าที่ความรับผิดชอบของพนักงาน พร้อมทั้งระเบียบวิธีปฏิบัติให้พนักงานใช้เป็นหลักในการทำงาน รวมทั้งการติดตามตรวจสอบให้ทุกคนปฏิบัติตามกฎ ระเบียบ มาตรฐานที่วางไว้อย่างเคร่งครัด และสม่ำเสมอ

- **สถานภาพของระบบการรักษาความปลอดภัย**
  - ความต้องการในการใช้ข้อมูลที่ปลอดภัยและคำแนะนำจากส่วนต่างๆที่ใช้งานภายในระบบ
  - การแจกงานไปสู่ผู้ที่รับผิดชอบ มีตารางเวลาที่กำหนดว่าส่วนใดของระบบจะต้องปรับปรุงอะไรบ้าง ณ เวลาใด
  - มีการจัดทำแผนฉุกเฉิน เพื่อให้องค์กรสามารถดำเนินการต่อไปได้เมื่อมีวิกฤตการณ์เกิดขึ้น
  - มีการทดสอบให้มั่นใจว่าสามารถใช้งานได้

การควบคุมความคงสภาพของฐานข้อมูล (Database Integrity)

การควบคุมความคงสภาพของฐานข้อมูล (Database Integrity)

- หมายถึง การควบคุมข้อมูลที่เป็นคีย์หลัก (Primary Key : PK) ของรีเลชันให้มีข้อมูลที่ไม่ซ้ำกันและมีค่าที่ไม่เป็นค่าว่าง ทำให้ข้อมูลที่ถูกเก็บอยู่ในฐานข้อมูลที่อยู่ต่างรีเลชันกันมีความสัมพันธ์กัน สามารถอ้างอิงถึงกันและกันอย่างถูกต้อง มีความสอดคล้องกัน (Consistency) ตลอดเวลาของการประมวลผล เพื่อให้ข้อมูลของระบบงานในฐานข้อมูลมีความถูกต้อง น่าเชื่อถือ และไม่มีความขัดแย้งใด ๆ เกิดขึ้น
  - **กฎความคงสภาพของข้อมูล (Integrity Constraint)**
  - **การจัดการรายการเปลี่ยนแปลง (Transaction Management)**
  - **การควบคุมการใช้งานฐานข้อมูลโดยผู้ใช้หลายคน (Database Concurrency Control)**
  - **การสำรองข้อมูลและการกู้คืนข้อมูล (Backup and Recovery)**

กฎควบคุมความคงสภาพของข้อมูล (Integrity Constraint)

- **กฎความคงสภาพของ** Entity (Entity Integrity Rule)

> “**ค่าข้อมูลของคีย์หลักจะต้องไม่เป็นค่าว่าง**(Null Value)”

เพราะจะไม่สามารถนำ Primary Key มาใช้เข้าถึงข้อมูลในแต่ละแถวได้

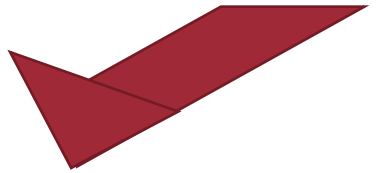
ตัวอย่าง

ค่าว่าง

รหัสนักศึกษา	รหัสวิชา	เกรด
	โดม	B
50000002	ญาญ่า	A

ค่าว่าง

รหัสนักศึกษา	รหัสวิชา	เกรด
50000001	โดม	
50000002	ญาญ่า	A



กฎควบคุมความคงสภาพของข้อมูล (Integrity Constraint)

- **กฎความคงสภาพของการอ้างอิง** (Referential Integrity Rule)

> “**ถ้า** Relation **ใดมี** Attribute **ที่เป็นคีย์นอกอยู่ ข้อมูลที่เป็นคีย์นอกนั้นจะต้องเป็นข้อมูลที่มีอยู่ในคีย์หลักอีก** Relation **หนึ่ง**”

เนื่องจากจะต้องมีการอ้างถึงค่าในตารางที่เป็นคีย์นอก

ตัวอย่าง

ตารางสินค้า

คีย์หลัก

รหัสสินค้า	ชื่อสินค้า	จำนวน
bk00198	เสื้อยืด	100
cd00034	กางเกงขายาง	250

ตารางยอดขาย

คีย์หลัก **คีย์นอก**

รหัสพนักงาน	รหัสสินค้า	ยอดขาย
HY001	bk00198	80
HY002	cd00034	200

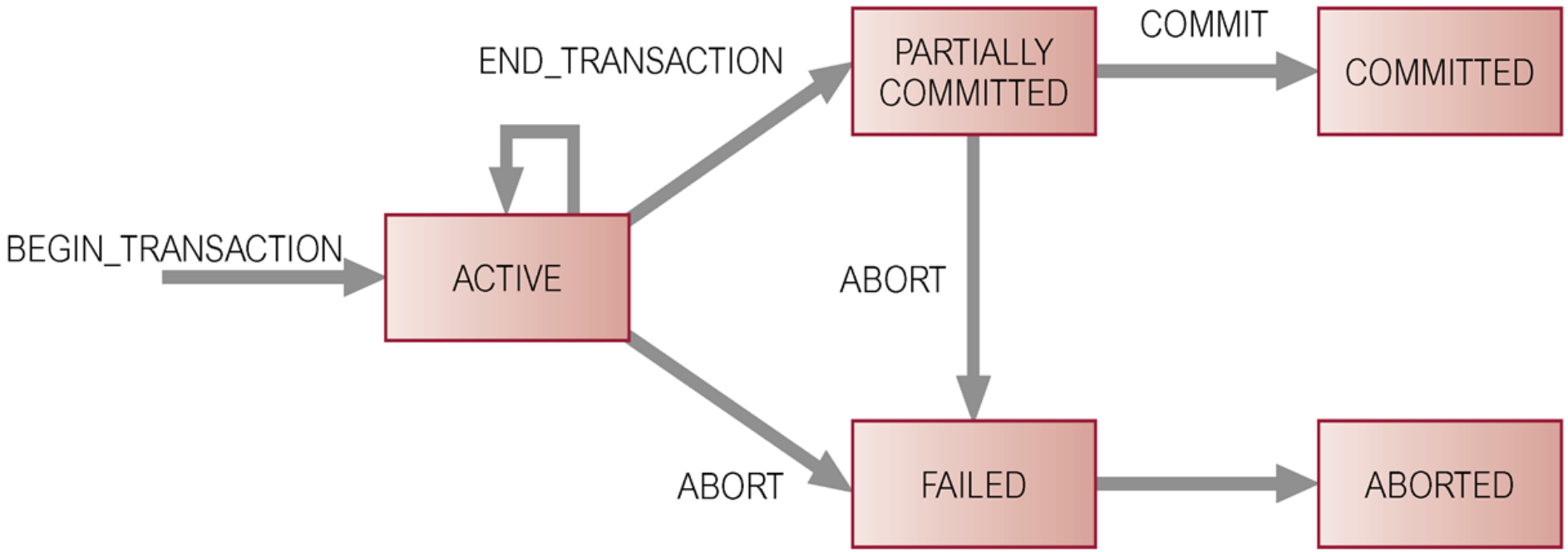
กฎการควบคุมความถูกต้องของข้อมูล (Data Integrity)

ฐานข้อมูลไม่สามารถรู้ได้เองว่าข้อมูลที่เก็บอยู่นั้นสอดคล้องกับความเป็นจริงหรือไม่ เราจึงต้องบอกให้ฐานข้อมูลรู้ด้วยสิ่งที่เรียกว่า กฎการควบคุมความถูกต้องของข้อมูล หรือ Data Integrity

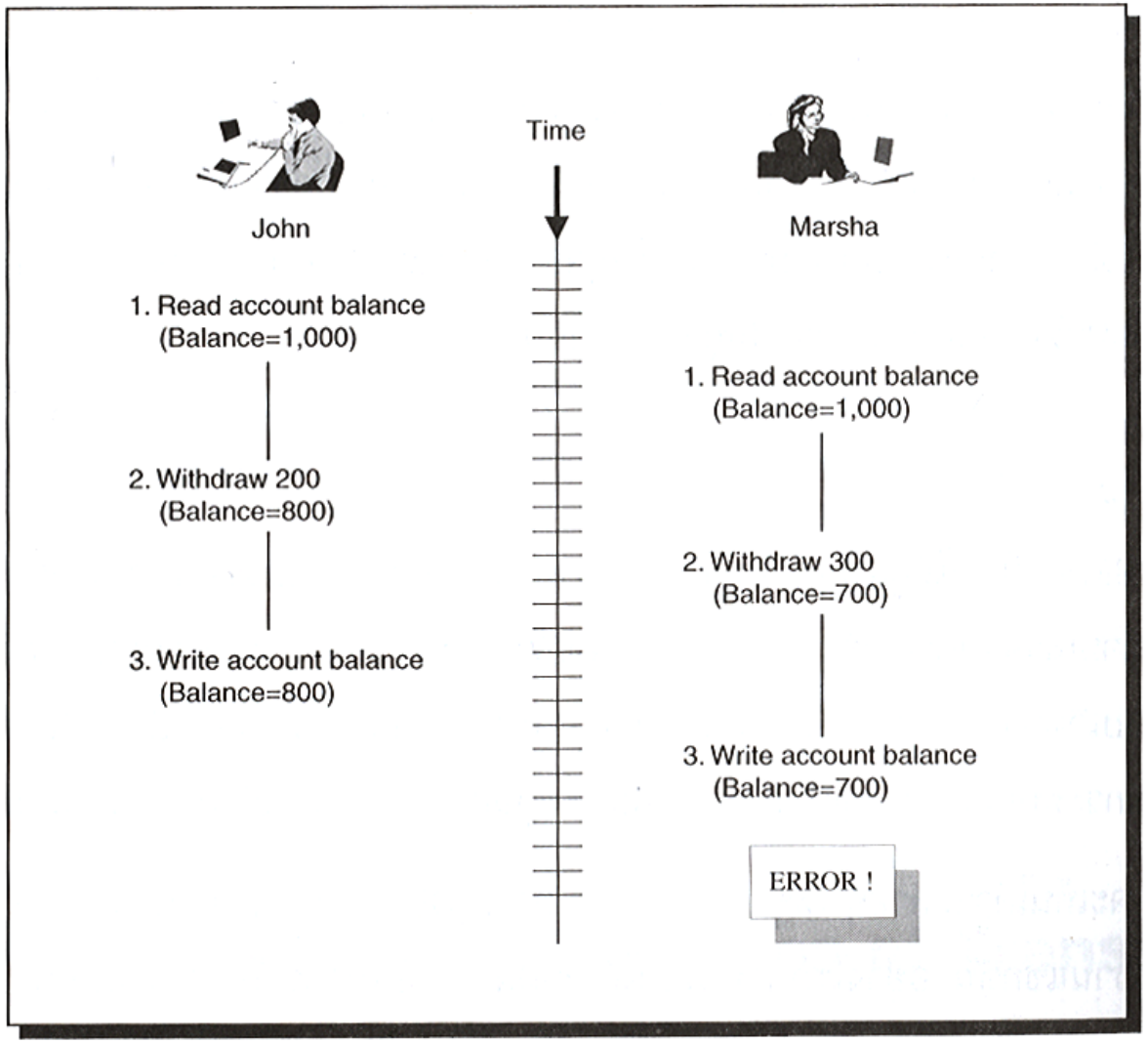
ตัวอย่างงานระบบทะเบียนนักศึกษาจะมี Integrity Rule ดังต่อไปนี้

- นักศึกษาทุกคนต้องสังกัดคณะที่มีอยู่เท่านั้น
- วิชาที่ลงทะเบียนต้องเป็นวิชาที่เปิดสอนเท่านั้น
- เกรดเฉลี่ยแต่ละเทอมจะอยู่ระหว่าง 0.00-4.00 เท่านั้น
- เกรดที่ได้จะต้องเป็น A,B+,B,C+,C,D+,D หรือ F เท่านั้น เป็นต้น

การจัดการรายการเปลี่ยนแปลง (Transaction Management)



การควบคุมการใช้งานฐานข้อมูลโดยผู้ใช้หลายคน (Database Concurrency Control)



แสดงการใช้งานทรานแซกชันระหว่าง John และ Marsha ที่เกิดภาวะพร้อมกัน

ที่มา https://courses.ischool.berkeley.edu/i257/f15/Lectures/Lecture15_257.pptx.pdf

การสำรองข้อมูลและการกู้คืนข้อมูล (Backup and Recovery)

- ควรทำการสำรองข้อมูลและเก็บใน CD-RW, DVD-RW, Magnetic Tape และ Hard Disk เป็นต้น

- วิธีการทำสำเนา
  - Full Backup หรือ Archival Backup เป็นการทำสำเนาทุก โปรแกรม ทุก File ไว้ทั้งหมด การทำ Full Backup ควรทำทุกสัปดาห์ หรือทุกสิ้นเดือน
  - Differential Backup เป็นการทำสำเนาข้อมูลเฉพาะข้อมูลที่มีการเปลี่ยนแปลงหลังจากทำ Full Backup

การรักษาความปลอดภัยของระบบฐานข้อมูล (Database Security)

การรักษาความปลอดภัยของระบบฐานข้อมูล (Database Security)

- หมายถึง การป้องกันข้อมูลในฐานข้อมูลจากผู้ที่ไม่มีสิทธิ์เกี่ยวข้องกับข้อมูลนั้น (Unauthorized Users) ไม่ให้สามารถเข้ามาใช้งานฐานข้อมูลได้ เพื่อเป็นป้องกันผู้ที่ไม่หวังดีเข้ามาทำการแก้ไข ทำลาย หรือแม้แต่การขโมยข้อมูล เพื่อนำไปใช้ประโยชน์ส่วนตัวได้
  - ความปลอดภัยระดับโครงสร้างฐานข้อมูล
  - ความปลอดภัยระดับข้อมูล

ความปลอดภัยระดับโครงสร้างฐานข้อมูล

- ความปลอดภัยระดับโครงสร้างฐานข้อมูล หมายถึง การควบคุมและดูแลในเรื่องของการเปลี่ยนแปลงโครงสร้างของข้อมูล เช่น การเพิ่ม ลบ แก้ไขคอลัมน์หรือตารางของฐานข้อมูล โดยใช้ภาษานิยามข้อมูล (DLL) เช่น CREATE ALTER และ DROP

- ดังนั้น การปรับเปลี่ยนโครงสร้างของฐานข้อมูลจะต้องกระทำโดย DBA เท่านั้น ผู้ใช้ทั่วไปจะไม่มีสิทธิเข้ามาแก้ไขโครงสร้างฐานข้อมูลนี้ได้

ความปลอดภัยระดับข้อมูล

- ความปลอดภัยระดับข้อมูล หมายถึง การควบคุมและดูแลให้แต่ละกลุ่มผู้ใช้ฐานข้อมูล (Database User) ให้สามารถทำงานหรือเกี่ยวข้องกับข้อมูลในฐานข้อมูลตามสิทธิ์ที่ DBA จะกำหนดไว้ให้เท่านั้น การกระทำของผู้ใช้ที่จะเข้ามาทำงานประกอบด้วย INSERT UPDATE และ DELETE
- ความปลอดภัยระดับข้อมูล สามารถควบคุมได้หลายวิธี ดังนี้
  - การสร้างวิว (View)
  - การกำหนดสิทธิการจัดการฐานข้อมูล
  - การเข้ารหัสข้อมูล

การสร้างระบบรักษาความปลอดภัยสำหรับผู้ใช้

- **การสร้างสิทธิผู้ใช้ในการเข้าถึงข้อมูล**
  - การยืนยันตัวบุคคล (Authentication)
  - การให้สิทธิ (Authorization)
- **การสร้างข้อมูลให้เป็นความลับ**

การยืนยันตัวบุคคล (Authentication)

- **การใช้รหัสผ่าน (password) ในการเข้าสู่ระบบคอมพิวเตอร์** ผู้ใช้งานแต่ละคนจะต้องป้อนรหัสผ่านจึงจะมีสิทธิเข้าถึงข้อมูลได้ ซึ่งเป็นระบบการรักษาความปลอดภัยในระดับพื้นฐานอย่างหนึ่ง การตั้งรหัสผ่านควรจะมีกฎเกณฑ์ เพื่อให้เดาได้ยาก เช่นควรจะมีความยาวไม่น้อยกว่า 6 ตัวอักษร และควรจะมีทั้งตัวเลข ตัวอักษร และสัญลักษณ์พิเศษรวมกัน ไม่ควรเป็นคำที่มีความหมาย หรือเป็นชื่อ เช่น ชื่อคน ชื่อจังหวัด เวลาป้อนรหัสผ่านจะต้องไม่แสดงบนจอ โดยทั่วไปจะแสดงเป็นค่าดาว * แทน และที่สำคัญที่สุดจะต้องมีการบังคับให้มีการเปลี่ยนรหัสเป็นระยะด้วย

- **การใช้บัตรสมาร์ทการ์ด (smartcard)** ผู้ใช้จะมีบัตรสำหรับเข้าระบบคอมพิวเตอร์ บัตรสมาร์ทการ์ดคล้ายกับบัตรเอทีเอ็ม และต้องป้อนรหัสส่วนตัว (Personnel Identification Number) หรือพิน (PIN)

- **การใช้การตรวจสอบจากร่างกายมนุษย์ (biometric)** เช่น ม่านตา เสียง ลายนิ้วมือ การตรวจสอบในลักษณะนี้จะต้องนำลักษณะของผู้ที่ต้องการเข้าไปใช้ฐานข้อมูลไปเปรียบเทียบกับลักษณะข้อมูลของผู้ใช้ที่มีอยู่ในเครื่องคอมพิวเตอร์ ถ้าตรงกันจึงจะมีสิทธิเข้าใช้ข้อมูล

การให้สิทธิ (Authorization)

- สิทธิในการอ่านข้อมูลหรือเรียกดูข้อมูล (read)
- สิทธิในการเพิ่มข้อมูล (insert)
- สิทธิในการเปลี่ยนแปลงข้อมูล (update)
- สิทธิในการลบข้อมูล (delete)
- สิทธิในการสร้างดัชนี (index)
- สิทธิในการสร้างตารางหรือวิว (resource)
- สิทธิในการเปลี่ยนแปลงโครงสร้างข้อมูล (alteration)
- สิทธิในการลบตารางหรือวิว (drop)

การสร้างข้อมูลให้เป็นความลับ

- การเข้ารหัส (coding) เป็นกระบวนการแปลงรูปแบบของข้อมูลให้อยู่ในรูปที่บุคคลอื่นๆไม่สามารถรู้เนื้อหาของข้อมูล ยกเว้นบุคคลที่เป็นผู้รับ ซึ่งจะต้องมีตัวถอดรหัสทำการแปลงข้อมูลนั้นกลับมาเป็นข้อมูลต้นฉบับ การเข้ารหัสจะใช้วิธีแทนค่าแต่ละค่าด้วยค่าอื่น ซึ่งเป็นการป้องกันข้อมูลในระดับหนึ่ง สามารถป้องกันผู้ที่ไม่ทราบวิธีการเข้ารหัสใช้ข้อมูลได้อย่างง่ายๆ

- การยุบตัวซ้ำ (compression) มักจะใช้กับข้อมูลประเภทตัวเลข หรือข้อมูลที่แปลงเป็นเลขฐานสองแล้ว เช่นการแปลงข้อมูล 01111100011 เป็น 1532 ประโยชน์ที่จะได้รับนอกจากเพิ่มความปลอดภัยแล้ว เทคนิคนี้มักจะนำไปประยุกต์ใช้กับการบีบอัดข้อมูลเพื่อประหยัดที่ในการเก็บข้อมูล และเวลาในการส่งข้อมูลด้วย

- การแทนค่า (substitution) มีหลักการทำงานคล้ายกับการเข้ารหัสโดยมีการกำหนดค่าที่จะแทนไว้ล่วงหน้า ส่วนการเข้ารหัสจะเป็นการกำหนดหลักการเข้ารหัสไว้

- การสลับตำแหน่งข้อมูล (transposition) ทำโดยไม่ได้เปลี่ยนข้อมูล แต่ใช้วิธีการสลับตำแหน่งของข้อมูลแทน

- ในการใช้งานจริงในการรักษาความปลอดภัยของฐานข้อมูลมักจะเป็นการนำเทคนิคต่างๆ หลายเทคนิคมาประยุกต์ใช้งานร่วมกัน เพื่อให้ระบบความปลอดภัยนั้นมั่นคงและเชื่อถือได้

การโจมตีข้อมูล (Data Security)

10 อันดับการโจมตีข้อมูลในปี 2025

- การโจมตีแบบ Injection
- การตรวจสอบสิทธิและการควบคุมการเข้าถึงที่บกพร่อง
- การรั่วไหลของข้อมูล
- การโจมตีด้วยมัลแวร์และแรนซัมแวร์
- ภัยคุกคามจากบุคคลภายใน
- การเข้ารหัสที่อ่อนแอ
- การจัดการข้อมูลที่ไม่ปลอดภัย
- การรักษาความปลอดภัยจากบุคคลที่สามไม่เพียงพอ
- การจัดทำบัญชีข้อมูลและการจัดการข้อมูล
- การไม่ปฏิบัติตามกฎระเบียบการคุ้มครองข้อมูลส่วนบุคคล

การโจมตีแบบ Injection

- **การโจมตีแบบ Injection** ทำให้ผู้ไม่ประสงค์เข้าถึงระบบฐานข้อมูลได้ถึงแม้ว่าจะไม่มีสิทธิ์ โดยการใส่คำสั่งที่เป็นอันตรายผ่านช่องทางเชื่อมต่อกับฐานข้อมูล เช่น เว็บแอพพลิเคชัน แต่แอบแฝงด้วยคำสั่งที่ก่อให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ต่อระบบฐานข้อมูล เช่น บายพาสการพิสูจน์ตัวตน หรือการแก้ไขฐานข้อมูล เป็นต้น
- การโจมตีในลักษณะนี้จะเป็นการสร้างปัญหาใหญ่ให้กับองค์กรได้มากมาย เนื่องจากภายในเซิร์ฟเวอร์ของแต่ละองค์กรมักจะรวบรวมข้อมูลลูกค้า ข้อมูลส่วนบุคคล หมายเลขบัตรเครดิต และระบบการเงิน และจะสร้างปัญหาได้ในระยะยาว หากไม่มีการแก้ไขอย่างทันท่วงที

- ดังนั้น องค์กรควรมีการตรวจสอบอินพุต (Input Validation) การส่งค่าผ่านตัวแปรแทนการต่อสตริงคำสั่งโดยตรง และหลักการสิทธิ์การเข้าถึงฐานข้อมูลขั้นต่ำ (Least Privilege) เท่าที่จำเป็น

การตรวจสอบสิทธิและการควบคุมการเข้าถึงที่บกพร่อง

- **การยืนยันตัวตนที่บกพร่อง (Broken Authentication)** คือ การที่ระบบมีข้อผิดพลาดในการออกแบบฟังก์ชันยืนยันตัวตนและการจัดการเซสชัน (Session Management)

- **การควบคุมการเข้าถึงที่บกพร่อง (Broken Access Control)** คือการที่ระบบไม่สามารถบังคับใช้ข้อจำกัดในการเข้าถึงทรัพยากรหลังจากที่ผู้ใช้ล็อกอินเข้ามาแล้ว

- **ตัวอย่างเช่น** ผู้โจมตีสามารถเข้าถึงฟังก์ชันหรือข้อมูลที่ไม่มีสิทธิ์ เช่น การเปิดดูไฟล์ส่วนตัวของผู้อื่น, การแก้ไขข้อมูลของบุคคลอื่น หรือการยกระดับสิทธิ์ตัวเองเป็นผู้ดูแลระบบ (Privilege Escalation)
- ดังนั้น องค์กรควรใช้มาตรฐาน 802.1x ร่วมกับเซิร์ฟเวอร์ RADIUS สำหรับควบคุมการเข้าถึงเครือข่าย และหมั่นทำการทดสอบเจาะระบบ (Penetration Testing) เพื่อค้นหาช่องโหว่เหล่านี้ก่อนถูกโจมตี

การรั่วไหลของข้อมูล

- **การรั่วไหลของข้อมูล (Data Breach)** คือเหตุการณ์ละเมิดความมั่นคงปลอดภัยที่ทำให้ข้อมูลสำคัญ ข้อมูลที่ได้รับความคุ้มครอง หรือข้อมูลส่วนบุคคล ถูกคัดลอก ส่งต่อ เข้าถึง หรือใช้งานโดยบุคคลที่ไม่มีสิทธิ์. เหตุการณ์นี้ส่งผลกระทบโดยตรงต่อความลับ (Confidentiality), ความถูกต้อง (Integrity) หรือความพร้อมใช้ (Availability) ของข้อมูลองค์กร

- **ตัวอย่างที่พบบ่อยเช่น** การเจาะระบบ (Hacking) มัลแวร์เรียกค่าไถ่ (Ransomware) หรือเกิดขึ้นจากพนักงานส่งข้อมูลให้ผิดคน เป็นต้น
- องค์กรควรมีการควบคุมความเสียหาย สืบสวน แจ้งเตือนหน่วยงานที่เกี่ยวข้องตามที่พรบ.การคุ้มครองข้อมูลส่วนบุคคล และกู้คืนระบบกลับมาให้ได้

การโจมตีด้วยมัลแวร์และแรนซัมแวร์

- **มัลแวร์ (Malware)** คือ ซอฟต์แวร์ที่ถูกสร้างขึ้นเพื่อวัตถุประสงค์ร้าย เช่น การขัดขวางการทำงานของคอมพิวเตอร์ รวบรวมข้อมูลที่ละเอียดอ่อน หรือเข้าถึงระบบส่วนตัวโดยไม่ได้รับอนุญาต. ประเภทที่พบบ่อยได้แก่ ไวรัส (Virus) ที่ต้องอาศัยการแนบตัวกับไฟล์อื่นเพื่อแพร่กระจาย, เวิร์ม (Worm) ที่สามารถสำเนาตัวเองและแพร่กระจายได้เองผ่านเครือข่าย, และม้าโทรจัน (Trojan Horse) ที่หลอกลวงว่าเป็นโปรแกรมปกติเพื่อทำอันตรายระบบภายหลัง

- **แรนซัมแวร์ (Ransomware)** คือ มัลแวร์เรียกค่าไถ่ที่จะทำการเข้ารหัสไฟล์ของเหยื่อจนไม่สามารถใช้งานได้ และจะเรียกร้องเงิน (มักเป็น Bitcoin) เพื่อแลกกับคีย์ในการถอดรหัส

- องค์กรควรใช้ซอฟต์แวร์ Antivirus ที่รองรับการสแกนแบบ Real-time หมั่นอัปเดต Patch ของระบบปฏิบัติการ และการสำรองข้อมูล (Backup) ที่สำคัญไว้อย่างสม่ำเสมอเพื่อใช้ในการกู้คืนระบบ

ภัยคุกคามจากบุคคลภายใน

- **ภัยคุกคามจากบุคคลภายใน (Insider Threat)** คือภัยคุกคามที่เกิดจากบุคคลที่ได้รับความไว้วางใจภายในองค์กร เช่น พนักงาน ผู้รับเหมา หรืออดีตพนักงาน ซึ่งใช้สิทธิ์การเข้าถึงระบบที่ถูกต้องเพื่อสร้างความเสียหายต่อข้อมูลหรือทรัพยากร

- ภัยคุกคามจากคนภายในองค์กรนั้นอันตรายกว่าคนนอกเพราะพวกเขารู้จักโครงสร้างเครือข่ายและมีรหัสผ่านในการเข้าถึงระบบอยู่แล้ว
- องค์กรควรใช้หลักการให้สิทธิ์เท่าที่จำเป็น และแบ่งแยกหน้าที่เพื่อตรวจสอบกันเอง ดำเนินการยกเลิกสิทธิ์การเข้าถึงทันทีเมื่อพนักงานลาออก จัดอบรม Security Awareness และใช้ระบบตรวจสอบพฤติกรรมผู้ใช้และระบบ Log เพื่อตรวจจับสิ่งผิดปกติ

การเข้ารหัสที่อ่อนแอ

- **การเข้ารหัสที่อ่อนแอ (Weak Cryptography)** คือ อัลกอริทึมหรือการนำเทคนิคการเข้ารหัสมาใช้งานที่มีข้อบกพร่อง มีความยาวกุญแจ (Key length) สั้นเกินไป หรือมีช่องโหว่ที่ทำให้ผู้โจมตีสามารถถอดรหัสข้อมูลได้โดยไม่ต้องรู้กุญแจ

- องค์กรเปลี่ยนไปใช้อัลกอริทึมมาตรฐานปัจจุบัน อัปเกรดฟังก์ชันแฮช (Hashing) เพิ่มความยาวกุญแจ และปรับปรุงความปลอดภัยบนเครือข่ายแลนไร้สาย

การจัดการข้อมูลที่ไม่ปลอดภัย

- **การจัดการข้อมูลที่ไม่ปลอดภัย (Insecure Data Handling)** คือ กระบวนการหรือการกระทำที่ทำให้ข้อมูลสำคัญรั่วไหล ถูกเข้าถึง หรือถูกแก้ไขโดยไม่ได้รับอนุญาต ซึ่งมักเกิดจากความประมาทหรือการขาดมาตรการป้องกันที่เหมาะสม

- องค์กรควรทำการจัดประเภทข้อมูล (Data Classification) เพื่อกำหนดระดับความสำคัญ บังคับใช้หลักการให้สิทธิ์เท่าที่จำเป็น และใช้เทคนิคการลบข้อมูลอย่างปลอดภัย (Data Wiping) เมื่อเลิกใช้งานอุปกรณ์

การรักษาความปลอดภัยจากบุคคลที่สามไม่เพียงพอ

- **การรักษาความปลอดภัยจากบุคคลที่สามไม่เพียงพอ (Inadequate Third-Party Security)** คือ ความเสี่ยงที่เกิดจากบุคคลภายนอก เช่น คู่ค้า หรือผู้รับเหมา มีมาตรการป้องกันที่อ่อนแอจนกลายเป็นช่องทางการโจมตี ปัญหาที่พบบ่อยคือ การไม่ยกเลิกสิทธิ์การเข้าถึงของพนักงานชั่วคราวหรือผู้รับเหมาหลังจากเสร็จสิ้นภารกิจ การจ้างพัฒนาซอฟต์แวร์จากภายนอกอาจนำไปสู่การแทรกซึมของช่องโหว่ เช่น back doors หรือ injection attacks เข้าสู่ระบบ จนถึงอุปกรณ์ของเวนเดอร์ที่ติดมัลแวร์สามารถกลายเป็นพาหะนำเชื้อเข้าสู่เครือข่ายองค์กรได้ แม้จะมีข้อตกลงระดับการให้บริการ (SLA) ก็ตาม

- องค์กรควรระบุข้อกำหนดความปลอดภัยในสัญญาและกำหนดความรับผิดชอบทางกฎหมายให้ชัดเจน ดำเนินการตรวจสอบความปลอดภัยของเวนเดอร์ (Third-party assessment) อย่างสม่ำเสมอเพื่อประเมินความเสี่ยง และบังคับใช้หลักการสิทธิ์ขั้นต่ำเพื่อจำกัดการเข้าถึงข้อมูลของบุคคลภายนอกเท่าที่จำเป็นเท่านั้น

การจัดทำบัญชีข้อมูลและการจัดการข้อมูล

- **การจัดทำบัญชีข้อมูล (Data Inventory)** คือการจัดทำบัญชีรายชื่อทรัพย์สินข้อมูลทั้งหมด เพื่อให้องค์กรทราบว่ามีข้อมูลอะไรบ้าง จัดเก็บอยู่ที่ไหน และใครเป็นผู้รับผิดชอบ, โดยข้อมูลที่บันทึกควรประกอบด้วย ชื่อข้อมูล ประเภท สถานที่จัดเก็บ (Local หรือ Hosted) และชื่อผู้เป็นเจ้าของ
- **การจัดการข้อมูล (Data Management)** คือการบริหารจัดการข้อมูลอย่างเป็นระบบตลอดวงจรชีวิตข้อมูล (Data Life Cycle) เพื่อรักษาความปลอดภัยและความถูกต้อง

- องค์กรควรรวบรวม จัดเก็บ และเลือกใช้ฐานข้อมูลหรือเซิร์ฟเวอร์ที่มีประสิทธิภาพ การใช้งานและป้องกัน: กำหนดสิทธิ์เข้าถึงตามหลักการสิทธิ์ขั้นต่ำ (Least Privilege) การเข้ารหัสข้อมูล การสำรองข้อมูลสม่ำเสมอ และการทำลายข้อมูล (Destruction) เมื่อข้อมูลหมดความจำเป็น

การไม่ปฏิบัติตามแนวทาง กฎระเบียบ และพ.ร.บ.การคุ้มครองข้อมูลส่วนบุคคล

- การไม่ปฏิบัติตามแนวทาง กฎระเบียบ และพ.ร.บ.การคุ้มครองข้อมูลส่วนบุคคล องค์กรอาจถูกสั่งปิดกิจการถาวรหากมีการละเมิดที่รุนแรง นอกจากนี้ยังต้องเผชิญกับต้นทุนทางอ้อม เช่น การสูญเสียความเชื่อมั่นจากลูกค้า (Customer Churn), ความเสียหายต่อชื่อเสียง และค่าใช้จ่ายในการสืบสวน

เอกสารอ้างอิง

- **OWASP Data Security Top 10.** ค้นเมื่อ 25 กุมภาพันธ์ 2569, จาก https://owasp.org/www-project-data-security-top-10/


Q
&
A

คำถามทบทวน บทที่ 2