@ Post

ฉบับที่ 7/2556 ประจำเดือน กรกฎาคม พ.ศ. 2556 Free Copy

การพิสูจน์ตัวตน (Authentication)

ในปัจจุบันมีการใช้ระบบยืนยันตัวตนมากขึ้น โดยเฉพาะการยืนยันตัวตนในการใช้งานอินเทอร์เน็ตภายในองค์กร ซึ่งเป็นไปตาม พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550

การพิสูจน์ตัวตน (Authentication) คือการยืนยันความถูกต้องของหลักฐานที่แสดงว่าเป็นบุคคลนั้นจริง ซึ่งมีการทำงานเป็น 2 ขั้นตอน คือ การระบุตัวตน โดยผู้ใช้งานจะต้องแสดงว่าตนเองคือใคร เช่น รหัสผู้ใช้ (Username) และการพิสูจน์ตัวตน (Authentication) ซึ่งเป็นการตรวจสอบหลักฐานว่าเป็นบุคคลที่อ้างถึงจริงหรือไม่

สิ่งที่ใช้สำหรับพิสูจน์ตัวตน แบ่งออกเป็น 3 คุณลักษณะ คือ

1. สิ่งที่มี (Possession factor) เช่น กุญแจ หรือเครดิตการ์ด เป็นต้น

2. สิ่งที่รู้ (Knowledge factor) เช่น รหัสผ่าน (Password) หรือการใช้พิน (PIN) คือชุดตัวเลขหรือตัวอักษรที่กำหนดขึ้นเป็นรหัสลับเฉพาะส่วนบุคคล เพื่อใช้เป็นรหัสผ่านเข้าสู่ระบบงาน ภายใต้ข้อกำหนดหรือรูปแบบของหน่วยงานผู้ให้บริการจะกำหนดขึ้น

3. สิ่งที่เป็น (Biometric factor) เช่น ลายนิ้วมือ หรือม่านตา (Retinal patterns) คือ การยิงแสงเลเซอร์ หรือแสงอินฟราเรดพลังงานต่ำเข้าไปยังลูกตา ใช้การสแกนม่านตา ในระบบรักษาความปลอดภัยในการระบุตัวตน

กระบวนการพิสูจน์ตัวตนจะนำ 3 คุณลักษณะดังกล่าว มาใช้ในการยืนยันตัวตน เช่น การใช้Username และ Password เพื่อเข้าใช้งานระบบอินเทอร์เน็ต เป็นต้น

ระบบยืนยันตัวตน มีการทำงาน 3 ส่วน คือ

1. **การพิสูจน์ตัวตน** (Authentication) คือส่วนที่เป็นขั้นตอนแรกของการเข้าใช้งานระบบ ซึ่งผู้เข้าใช้งานระบบต้องถูกยอมรับจากระบบว่าสามารถเข้าใช้งานระบบได้ โดยจะตรวจสอบจาก Username และ Password

2. **การอนุญาต** (Authorization) คือขั้นตอนในการตรวจสอบสิทธิ์ในการใช้งานว่าสามารถเข้าถึงข้อมูลใดได้บ้างหรือระบบใดได้บ้าง เมื่อได้รับการพิสูจน์ว่าสามารถเข้าสู่ระบบได้

3. **การตรวจสอบได้** (Accountability) คือการบันทึกรายละเอียดของการใช้ระบบและรวมถึงข้อมูลต่างๆ ที่ผู้ใช้กระทำลงไปในระบบ ซึ่งสามารถตรวจสอบได้ว่า ผู้ใช้งานทำอะไรส่วนใดบ้าง

จากที่กล่าวมาข้างต้นจะพบว่าในระบบยืนยันตัวตนที่ใช้อยู่โดยทั่วไป นอกจากจะเก็บข้อมูลชื่อผู้ใช้งาน รหัสผ่าน และสิทธิ์ในการเข้าถึงข้อมูล โดยข้อมูลเหล่านี้จะทำให้ทราบว่าผู้ที่เข้ามาในระบบ คือใคร ทำอะไร ที่ไหน อย่างไร และเมื่อใด ถ้าไปใช้กระทำความผิด เช่น โพสต์ข้อความหมิ่นประมาทผู้อื่นในอินเทอร์เน็ต บุคคลซึ่งเป็นเจ้าของ Username นั้นก็มีอาจปฏิเสธการกระทำนั้นได้ เพราะระบบยืนยันตัวตนที่กำหนดให้ผู้ใช้งานต้อง Login เข้าสู่ระบบก่อนเข้าใช้งานอินเทอร์เน็ตจะจัดเก็บข้อมูลและเป็นตัวพิสูจน์ว่า “คุณคือใคร” ที่เข้าใช้งานระบบอินเทอร์เน็ตขององค์กร

สำหรับกรมส่งเสริมการปกครองท้องถิ่น (สถ.) ได้มีการนำระบบยืนยันตัวตนมาใช้ในการพิสูจน์ตัวตนว่าเป็นข้าราชการของ สถ. และมีสิทธิ์ในการใช้งานอินเทอร์เน็ตผ่านระบบเครือข่ายทั้งแบบมีสาย (LAN) และไร้สาย (Wireless LAN) ซึ่งเป็นไปตามนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ สถ. พ.ศ. 2554 หมวดที่ 1 ว่าด้วยการใช้งานระบบสารสนเทศอย่างถูกต้อง ข้อ 1.1 การพิสูจน์ตัวตนที่กำหนดให้ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้งานระบบสารสนเทศของ สถ. โดยต้องป้องกัน ดูแลรักษาข้อมูลบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) ห้ามทำให้ผู้อื่นล่วงรู้ และต้องรับผิดชอบการกระทำใดๆ ที่เกิดจากบัญชีชื่อผู้ใช้งาน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม