ก4895

มติชน

วันอังคารที่ 7 มกราคม พุทธศักราช 2546 ปีที่ 25 ฉบับที่ 9069 หน้า 19

เทคนิคการตั้งรหัสผ่านให้ปลอดภัย

แม้ความลับจะไม่มีในโลก แต่การป้องกันความลับรั่วไหลก็เป็นสิ่งที่ทุกคนพึงระวัง โดยเฉพาะอย่างยิ่งบนโลกแห่งเน็ตเวิร์ก องค์กรต่างๆ หรือแม้แต่ผู้ใช้งานคอมพิวเตอร์ทั่วไปจึงจำเป็นที่จะต้องหามาตรการสกัดการเข้าถึงข้อมูลสำคัญจากผู้ไม่หวังดีมาใช้หลายวิธี รหัสผ่านถือเป็นกลไกสำคัญในการป้องกันและใช้ในการทำงานร่วมกันบนระบบเน็ตเวิร์กที่มีการนำมาใช้ ดังนั้น การตั้งรหัสผ่านนั้นจึงควรมีเทคนิคในการตั้งซึ่งจะช่วยให้คนอื่นไม่สามารถคาดเดาและเจาะรหัสผ่านได้โดยง่าย

แต่ขอย้ำว่าไม่มีระบบเน็ตเวิร์กใดที่สามารถรับประกันความปลอดภัยได้ 100 เปอร์เซ็นต์ แม้แต่ระบบเครือข่ายของเอฟบีไอที่เชื่อกันว่ามีความปลอดภัยสูงสุดก็ยังเคยถูกเจาะระบบมาแล้ว สิ่งสำคัญนอกจากการติดตั้งระบบรักษาความปลอดภัยแล้ว กฎเกณฑ์การใช้งานในระบบเครือข่ายก็เป็นเรื่องที่ไม่ควรมองข้าม

●เทคนิคการใช้งานรหัสผ่าน

ถ้าจะลองเดารหัสเอทีเอ็มของคุณผู้อ่านเชื่อได้ว่ามีผู้อ่านมากกว่าครึ่งจะใช้ปีเกิดของตนเองมาตั้งเป็นรหัสเอทีเอ็ม บางคนก็ไม่เคยเปลี่ยนรหัสผ่านเลยตั้งแต่ได้รับมา

รหัสผ่านเป็นวิธีการรักษาความปลอดภัยด่านแรกที่นิยมใช้กันมากที่สุดแต่ก็มีโอกาสถูกผู้ไม่หวังดีบุกเจาะรหัสได้ การใช้รหัสผ่านจึงต้องมีเทคนิคง่ายๆ ดังนี้

1.อย่าใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน

วิธีนี้เป็นที่นิยมอย่างยิ่งสำหรับผู้ใช้งานเพราะกลัวว่าจะจำรหัสผ่านต่างๆ ไม่ได้หรือเพื่อให้จำง่าย เช่น ใช้ชื่อสำหรับการล็อกอินเป็น PUM ก็ตั้งรหัสผ่านว่า PUM เลย หรือไม่ก็ตั้งเป็น PUM 2003 เป็นต้น หากใครตั้งรหัสผ่านแบบนี้ก็เหมือนการแจกรหัสฟรีให้กับผู้ที่ต้องการ

2.อย่าใช้คำที่มีอยู่ในดิกชันนารี

สำหรับบางคนที่ไม่อยากคิดมากก็เปิดดิกชันนารีดู แล้วเลือกคำศัพท์ที่จำได้ง่ายๆ มาตั้งเป็นรหัสผ่าน บางคนก็สุ่มเปิดดิกชันนารีขึ้นมาแล้วสุ่มเลือกคำที่ 5 ของหน้านั้นมาตั้งเป็นรหัสผ่านแบบง่ายๆ (ไปหน่อย)

การตั้งรหัสผ่านในลักษณะนี้ต้องระวังมากเช่นกันเพราะมีโปรแกรมที่สามารถสุ่มรหัสผ่านจากดิกชันนารีได้และจะสามารถค้นหารหัสผ่านที่ถูกต้องได้ภายในเวลาไม่กี่นาที

3.อย่าใช้คำธรรมดาสามัญทั่วไป

เมื่อคำที่อยู่ในดิกชันนารีไม่ปลอดภัย บางคนจึงคิดหาคำอื่นๆ ที่ไม่มีอยู่ในดิกชันนารีมาใช้แทน แต่คำที่นำมาใช้นั้นอาจง่ายเกินไป เช่น 1234,abc123,passwd, nopasswd เป็นต้น คำพื้นฐานในลักษณะนี้ก็มีคนรวบรวมไว้เป็นโปรแกรมสำหรับเดารหัสผ่านเช่นกัน

4.อย่าใช้ตัวอักษรอย่างเดียว

รหัสผ่านที่ดีไม่ควรใช้ตัวอักษรอย่างเดียวควรจะใช้ตัวเลข ตัวอักษรพิเศษหรือสัญลักษณ์ต่างๆ ในการตั้งรหัสผ่านด้วย เช่น +,# $ % ^ & -_ เช่น ตั้งรหัสผ่านเป็น abk%432*(#! ที่สำคัญต้องมีหลักในการจำรหัสของตนเองเพื่อป้องกันหลงลืมและไม่สามารถเข้าไปใช้งานได้

5.อย่าตั้งรหัสผ่านสั้นเกินไป

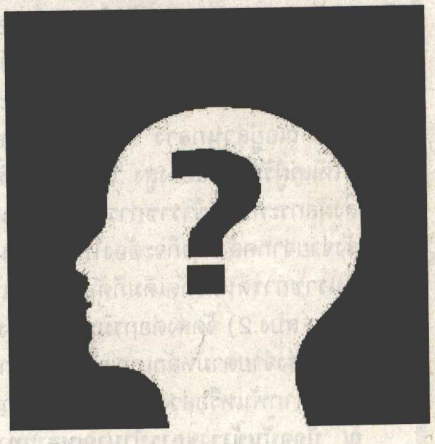
สุดท้าย โปรแกรมเดารหัสผ่านจะใช้ตัวอักษรทั้งหมดที่มีอยู่ในการเดา ดังนั้น ไม่ว่ารหัสผ่านจะตั้งไว้อย่างไรก็สามารถใช้โปรแกรมเดาออกได้ทั้งสิ้น เพียงแต่ว่าจะใช้เวลาเท่าไร ถ้าใช้คำที่มีอยู่ในดิกชันนารีหรือข้อมูลส่วนตัวตั้งเป็นรหัสผ่าน ก็อาจจะใช้เวลาเพียงห้าหรือสิบนาทีแต่ถ้าทำตามคำแนะนำข้างต้นคือไม่ใช้คำเหล่านี้ก็จะใช้เวลานานขึ้น อาจจะเป็นหนึ่งปีหรือสิบปีขึ้นไปถึงจะเดาได้ ซึ่งกว่าจะถึงเวลานั้นผู้ใช้ก็คงเปลี่ยนรหัสผ่านไปเรียบร้อยแล้ว

ความยาวของรหัสผ่านจะสัมพันธ์กับระยะเวลาในการเดา เป็นเงื่อนไขอย่างหนึ่งที่ทำให้การเดารหัสผ่านยากขึ้น ไม่ว่าจะตั้งรหัสผ่านสั้นเกินไปเช่นมีแค่ 2 ตัวอักษร โปรแกรมค้นหารหัสผ่านก็สามารถเดาได้โดยใช้เวลาไม่นานนัก รหัสผ่านควรจะมีความยาวอย่างน้อย 6 ตัวอักษรขึ้นไปเพื่อให้โปรแกรมเดารหัสผ่านทำงานได้ยากขึ้น

6.เปลี่ยนรหัสผ่านในเวลาที่เหมาะสม

เมื่อต้องการทำงานเกี่ยวกับความปลอดภัยบนเน็ตเวิร์ก ผู้ที่สามารถใช้งานได้จะมีชื่อที่ใช้สำหรับทำการล็อกอินเข้าระบบพร้อมกับรหัสผ่าน สำหรับรหัสผ่านนั้นควรมีการเปลี่ยนในกรณีต่อไปนี้

- เปลี่ยนรหัสผ่านทันทีในการใช้งานครั้งแรก
- เปลี่ยนรหัสผ่านเป็นระยะ เช่น 3 เดือน เป็นต้น
- เปลี่ยนเมื่อต้องแจ้งรหัสผ่านให้ผู้อื่นทราบ



มาตรการทั้ง 6 นี้จะช่วยป้องกันการเจาะข้อมูลได้อย่างน่าพอใจ หรืออย่างน้อยก็ทำให้ผู้ไม่หวังดีต้องใช้เวลาและความยากลำบากกว่าเดิมหากจะสืบค้นรหัสผ่านของเรา ซึ่งวิธีที่ดีที่สุดในการรักษาความปลอดภัยก็คือ "ความไม่ประมาท" นั่นเอง

ที่มาของข้อมูล : นิตยสาร CHIP SPECIAL เรื่อง "จัดการเน็ตเวิร์ก แค่ปลายนิ้ว"