



--- EDITOR'S TALK ---

เปิดศักราชใหม่ 2552 ทางทีมงาน บริษัท โกลบอล เทคโนโลยี อินทีเกรเทด ตั้งใจมอบสิ่งดีๆ ให้ทุกท่าน จึงจัดทำ SRAN e-Newsletter ขึ้น เพื่อเผยแพร่ความรู้ด้าน IT Security ทั้งในมุมมองด้านเทคโนโลยี ภัยคุกคาม และแนวทางการปฏิบัติเพื่อความปลอดภัยของข้อมูลสารสนเทศ โดยตั้งหวังให้ผู้อ่านรู้เท่าทัน และสามารถป้องกันภัยร้ายที่แฝงเร้นเข้ามาในโลกไซเบอร์ได้

สำหรับฉบับแรกนี้ เปิดตัวด้วยเรื่องราวเกี่ยวกับ ธุรกรรมออนไลน์ ที่เข้ามามีบทบาทต่อชีวิตประจำวันของเราท่านๆ มากขึ้นทุกขณะ นำเสนอด้วยบทความของบริษัทฯ ที่ตีพิมพ์ในหนังสือพิมพ์สยามธุรกิจ ฉบับวันที่ 26-28 พฤศจิกายน 2551 ผนวกข้อมูลเสริมด้านการป้องกันอย่างรู้เท่าทัน และการรับมือภัยคุกคาม เพื่อมุมมองที่ชัดเจนในการป้องกันปัญหาที่เกิดจากการทำธุรกรรมทางอินเทอร์เน็ต

หากมีข้อเสนอแนะติดต่อได้ที่ info@gbtech.co.th ค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

access

ธุรกรรมออนไลน์ ภัยร้าย! แฝงเงามืด

เมื่อหลายเดือนก่อนได้เกิดคดีที่เกี่ยวข้องกับการทำธุรกรรมทางอินเทอร์เน็ต โดยผู้เสียหายได้ใช้บริการ Internet Banking และตกเป็นเหยื่อโดยไม่รู้ตัว ซึ่งเมื่อตรวจสอบพบว่ามีผู้ดักข้อมูลโดยใช้โปรแกรม Key Logger ซึ่งคอยเก็บข้อมูลจากแป้นคีย์บอร์ดขณะใช้งาน และส่งผ่านระบบอินเทอร์เน็ตให้กับแฮกเกอร์ ซึ่งนำข้อมูลที่ได้สวมรอยเป็นผู้ใช้งาน เข้าทำธุรกรรมทางการเงิน สร้างความเสียหายมูลค่าไม่น้อย เหตุการณ์นี้สามารถป้องกันได้ หากผู้ใช้งานและผู้ให้บริการระบบธุรกรรมออนไลน์ตระหนักและรู้เท่าทันภัยคุกคาม ตลอดจนเสริมสร้างเทคโนโลยีให้ปลอดภัยมากยิ่งขึ้น

อ่านต่อ...หน้า 2

ป้องกัน อยากรู้เท่าทัน

เมื่อการทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นการซื้อขายสินค้าหรือบริการทางอินเทอร์เน็ต, การทำธุรกรรมทางการเงินผ่านเว็บไซต์ธนาคาร เข้ามามีบทบาทในชีวิตประจำวันของผู้คนมากขึ้น จึงจำเป็นอย่างยิ่งที่ต้องให้ความสำคัญกับการพิสูจน์ตัวตนผู้ใช้งาน ซึ่งถือเป็นด่านแรกของการเข้าใช้งานระบบออนไลน์ เพื่อตรวจสอบให้แน่ชัดว่าเป็นบุคคลผู้นั้นจริง การพิสูจน์ตัวตนสามารถทำได้หลายรูปแบบ เช่น การใช้รหัสผ่าน, PIN Code, ระบบ Token, ลักษณะเฉพาะทางชีวภาพ, การเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-Key Cryptography) เป็นต้น ...

อ่านต่อ...หน้า 3



ในปัจจุบันแฮกเกอร์ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคารหรือผู้ให้บริการธุรกรรมออนไลน์ เพื่อเข้าถึงชั้นความลับของลูกค้าเพียงอย่างเดียว แต่เปลี่ยนเป้าหมายเป็นผู้ใช้งาน (User) อินเทอร์เน็ต ซึ่งเข้าถึงได้ง่ายกว่าแทนโดยอาศัยความรู้เท่าไม่ถึงการณ์



ต่อจากหน้า 01 ธุรกรรมออนไลน์... ภัยร้ายแฝงเงามืด

เนื่องจากมีการใช้งานอินเทอร์เน็ตอย่างทั่วถึงมากยิ่งขึ้นบางครั้งผู้ใช้งานอาจพยายามดาวน์โหลดโปรแกรมหรือข้อมูลบางอย่างที่แฮกเกอร์ได้เผยแพร่ไว้ตามเว็บไซต์สาธารณะโดยโปรแกรมดังกล่าวมักมีชื่อที่ดึงดูดให้ดาวน์โหลด เช่น clip ฉาว, โปรแกรมเร่งความเร็ว, โปรแกรม crack serial number, โปรแกรมเกมส์ เป็นต้น เมื่อผู้ใช้งานหลงดาวน์โหลดโปรแกรมดังกล่าวมาติดตั้งในเครื่อง อาจมีมัลแวร์แฝงมากับไฟล์ ทำให้ผู้ใช้ตกเป็นเหยื่อมิจฉาชีพที่จ้องดักข้อมูลได้

ในแง่ผู้ใช้งานทั่วไป : ต้องป้องกันภัยคุกคามที่เกิดขึ้นโดยตระหนักรู้ และควบคุมพฤติกรรมตนเองในการใช้งานอินเทอร์เน็ตบนเครื่องคอมพิวเตอร์

ส่วนตัว, ไม่ดาวน์โหลดโปรแกรมที่ไม่มั่นใจในความปลอดภัย, หมั่นดูแลเครื่องคอมพิวเตอร์ให้มีการอัปเดตทั้งซอฟต์แวร์ป้องกัน และ Patch, ตั้งรหัสผ่านที่ยากต่อการคาดเดา หากต้องทำธุรกรรมทางอินเทอร์เน็ต เช่น ซื้อสินค้า หรือทำธุรกรรมทางการเงิน ให้ทำบนเครื่องตนเองที่คิดว่าปลอดภัยแล้ว เลือกช่องทางการใช้งานให้ถูกต้อง เช่น เมื่อมีการ Login ผ่านเว็บไซต์ให้ดูว่าเป็นการผ่าน HTTPS หรือไม่ หากไม่ใช้ก็ไม่ควรใช้ โดยเฉพาะหากอยู่ในวง LAN ไม่ว่าจะ เป็นร้านอินเทอร์เน็ตคาเฟ่ หรือบริษัท เพราะอาจมีการดัก User / Password ผ่านระบบเครือข่ายได้ และควรเลือกใช้บริการธุรกรรมอินเทอร์เน็ตจากผู้ให้บริการที่น่าเชื่อถือเท่านั้น

ในแง่ผู้ให้บริการ : ผู้ให้บริการต้องให้ความสำคัญกับเทคโนโลยีในการระบุตัวตน ผู้ใช้งาน, ดูแลความปลอดภัยของข้อมูลและวิธีการใช้งานเมื่อลูกค้าต้องทำธุรกรรมผ่านระบบอินเทอร์เน็ต ตลอดจนให้ความรู้แก่ลูกค้าให้รู้เท่าทันภัยคุกคามในปัจจุบัน

ในที่นี้ผมขอเน้นเรื่องการใช้เทคโนโลยีการพิสูจน์ตัวตนของลูกค้าที่ทำธุรกรรมผ่านอินเทอร์เน็ต ซึ่งที่ใช้กันอยู่มีสามรูปแบบคือ

- ❖ สิ่งที่คุณมี (Something you have) เช่น กุญแจไขประตู, บัตรอิเล็กทรอนิกส์ หรือระบบ Token เป็นต้น
- ❖ สิ่งที่คุณรู้ (Something you know) คือ รหัสผ่านหรือชุดตัวเลขเฉพาะ
- ❖ สิ่งที่คุณเป็น (Something you are) เป็นการพิสูจน์ตัวตนแบบชีวมาตร เช่น ลายนิ้วมือ ระบบรู้จำเสียง ระบบสแกนม่านตา เป็นต้น

อย่างไรก็ดี ผู้ให้บริการด้านพาณิชย์อิเล็กทรอนิกส์ เช่น สถาบันการเงิน, ผู้ประกอบธุรกิจ E-Commerce ควรนำเทคโนโลยีการพิสูจน์ตัวตนแบบ Two-Factor Authentication มาใช้เป็นอย่างน้อย ตลอดจนให้ความรู้แก่ลูกค้าในการทำธุรกรรมผ่านระบบอินเทอร์เน็ต เพื่อไม่ให้ตกเป็นเหยื่อพวกมิจฉาชีพที่นับวันจะมีวิธีการที่ซับซ้อนแยบยลขึ้นทุกที

เมื่อ การทำธุรกรรมออนไลน์ ไม่ว่าจะเป็นการซื้อขายสินค้าหรือบริการทางอินเทอร์เน็ต, การทำธุรกรรมทางการเงินผ่านเว็บไซต์ธนาคาร เข้ามามีบทบาทในชีวิตประจำวันของผู้คนมากขึ้น จึงจำเป็นอย่างยิ่งที่ต้องให้ความสำคัญกับการพิสูจน์ตัวตนผู้ใช้ งาน ซึ่งถือเป็นด่านแรกของการเข้าใช้งานระบบออนไลน์ เพื่อตรวจสอบให้แน่ชัดว่าเป็นบุคคลผู้นั้นจริง การพิสูจน์ตัวตนสามารถทำได้หลายรูปแบบเช่น การใช้รหัสผ่าน, PIN Code, ระบบ Token, ลักษณะเฉพาะทางชีวภาพ, การเข้ารหัสโดยใช้กุญแจสาธารณะ (Public-Key Cryptography) เป็นต้น



นอกจากให้ความสำคัญกับเทคโนโลยีที่ใช้ในการพิสูจน์ตัวตนแล้ว ยังต้องอาศัยนโยบายด้านความมั่นคงปลอดภัยข้อมูล ตลอดจนวิธีการปฏิบัติและการควบคุมที่เหมาะสม ในเรื่องนี้องค์กรต่าง ๆ อาจต้องนำมาตรฐาน MSA ISO/IEC 27001:2005 ซึ่งเป็นกฎเกณฑ์ที่เกี่ยวข้องกับการจัดการความปลอดภัยสารสนเทศมาใช้ ผู้บริหารควรให้การสนับสนุนเต็มที่เพื่อให้แน่ใจว่าได้มีการสร้างระบบอย่างถูกต้องและยึดมั่นกับนโยบายดังกล่าว

ในแง่ของสถาบันการเงิน ควรประเมินความสามารถของเทคนิคการพิสูจน์ตัวตนที่ใช้ถือว่าสามารถรับมือกับภัยคุกคามและความเสี่ยงใหม่ ๆ ที่เกิดขึ้นได้หรือไม่ จากข้อมูลเปิดเผยโดยสมาคม ICISA (International Computer Security Association) ร้อยละ 80 ของระบบที่ได้รับความเสียหายเกิดขึ้นจากภายในองค์กรเอง โดยสถาบัน Basel Committee on Banking Supervision แนะนำให้สถาบัน การเงินพิจารณาถึงความเสี่ยงที่เห็นได้ชัดของการให้บริการธนาคารผ่านอินเทอร์เน็ตที่อาศัยหมายเลขใช้เฉพาะเพียงอย่างเดียว การพิสูจน์ตัวตนแบบปัจจัยเดียว อาจไม่เหมาะสมสำหรับการใช้งานเชิงพาณิชย์หรือเพียงพอสำหรับแอปพลิเคชันและธุรกรรมที่มีความเสี่ยงสูงจึงควรหันมาให้ความสำคัญกับการประเมินความเสี่ยงระบบอย่างสม่ำเสมอควบคู่ไปด้วย จะช่วยลดความเสี่ยงภายในระบบลงได้



← ต่อจากหน้า **01 ปกกันอย่างไรรู้เท่าทัน**

สำหรับการทำธุรกรรมทางอินเทอร์เน็ตนั้น การพิสูจน์ตัวตนแบบปัจจัยเดียว (single-factor) อาจไม่รัดกุม และไม่เพียงพอต่อการให้บริการธุรกรรมอิเล็กทรอนิกส์ ซึ่งมีแนวโน้มขยายตัวขึ้น ควบคู่กับความเสี่ยงที่สูงขึ้นเป็นเงาตามตัว จึงควรใช้การพิสูจน์ตัวตนแบบสองปัจจัย (two-factor) ตัวอย่างที่เห็นเด่นชัดคือ เครื่องเอทีเอ็มที่ใช้บัตรพลาสติก (สิ่งที่คุณมี) ควบคู่กับหมายเลขเฉพาะสี่หลัก (สิ่งที่คุณรู้) เปรียบเทียบกับการพิสูจน์ตัวตนทางระบบเครือข่ายคือ การใช้ระบบ Token ร่วมกับรหัสผ่านนั่นเอง วิธีนี้จะช่วยยกระดับความปลอดภัยให้สูงขึ้นอีกขั้น และผู้ใช้บริการรายนั้นไม่อาจปฏิเสธความรับผิดชอบในการทำธุรกรรมของตนได้ ซึ่งระบบที่มีประสิทธิภาพจะช่วยให้โครงสร้างด้านความปลอดภัยแข็งแกร่งขึ้น ลดปัญหาการฉ้อฉลลงได้อีกทางหนึ่ง

อีกประเด็นหนึ่งที่ควรให้ความสนใจในระบบการทำธุรกรรมออนไลน์ คือ การป้องกันการดักข้อมูลหรือการเปลี่ยนแปลงการจราจรของเครือข่าย เส้นทางของเครือข่ายได้รับการป้องกันโดยใช้ช่องทางที่มีการรักษาความปลอดภัย เช่น การใช้ SSL (Secure Socket Layer Protocol) ซึ่งเข้ารหัสลับข้อมูลก่อนที่จะส่งข้อมูลนั้นสู่อินเทอร์เน็ต หากผู้ไม่ประสงค์ดีดักข้อมูลระหว่างทาง ก็ไม่อาจตีความหมายของข้อมูลนั้นได้

นอกจากกลุ่บายออนไลน์ดังกล่าว ยังมีวิธีการแบบกายรูปแบบอื่นอีกสารพัดวิธีที่จะดึงทรัพย์ออกจากกระเป๋าเหยื่อ หากเรารู้เท่าทันก็จะช่วยปกป้องตนเองให้พ้นภัยได้ ซึ่งทีมงานจะได้นำเสนอใน SRAN e-Newsletter ฉบับต่อไป โปรดติดตามค่ะ

กรณี Key Logger ในบทความข้างต้น หากผู้ให้บริการธุรกรรมทางการเงินกำหนดให้ลูกค้าใช้ Token ควบคู่กับรหัสผ่านแล้ว มิจฉายพิก็ไมอาจสวมรอยเป็นเหยื่อ ลักลอบนำเงินออกจากบัญชี สร้างความเสียหายให้ผู้อื่นได้อย่างไรก็ตาม เมื่อธุรกรรมออนไลน์ในประเทศไทยยังใช้รหัสผ่านเป็นหลักในการพิสูจน์ตัวตนผู้ใช้งานเพียงปัจจัยเดียว ผู้ใช้จึงควรป้องกันตนเองเบื้องต้นโดยการกำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร และใช้อักขระพิเศษ เพื่อให้ยากต่อการคาดเดา เช่น สมมติตั้งรหัสว่า globaltech แทนที่จะระบุตรงตัว อาจกำหนดรหัสเป็น G10b@1tEc# (สำคัญคือต้องจำให้ได้!!) ควบคู่กับการไม่ดาวน์โหลดไฟล์ส่มสี่ สุ่มห้าจากอินเทอร์เน็ต เพราะมีโอกาสได้โปรแกรมไม่พึงประสงค์แฝงมาด้วย เช่น Key Logger (ที่มีเผยแพร่ทั่วไปในโลกออนไลน์) หากติดกับแล้วแม้จะตั้งรหัสผ่านที่เดายากเพียงใด ก็ไม่อาจรอดพ้นเงื้อมมือมิจฉาชีพไปได้