ธนาคารแห่งประเทศไทย
BANK OF THAILAND

Consultation Paper

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (cyber hygiene)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย
มิถุนายน 2563

1. เหตุผลในการออกประกาศ

ปัจจุบันผู้ให้บริการ e-payment ใช้เทคโนโลยีและระบบเทคโนโลยีสารสนเทศ เป็นกลไกหลักในการขับเคลื่อนธุรกิจ ทำให้เผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) มากขึ้น ผู้ให้บริการ e-payment จึงควรมีการรักษาความมั่นคงปลอดภัยที่เข้มงวด รัดกุม ต่อการรับมือกับภัยคุกคามทางไซเบอร์ ธนาคารแห่งประเทศไทยจึงได้กำหนดแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (cyber hygiene) ที่จะช่วยยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญของผู้ให้บริการ e-payment เพื่อลดความเสี่ยงหรือผลกระทบต่อลูกค้า ผู้ให้บริการ e-payment และต่อระบบชำระเงินโดยรวมเมื่อเกิดภัยคุกคามทางไซเบอร์ขึ้น

2. ขอบเขตการบังคับใช้

ประกาศฉบับนี้ให้ใช้บังคับกับผู้ประกอบธุรกิจการชำระเงินภายใต้การกำกับตามกฎหมายที่มิใช่สถาบันการเงิน

3. เนื้อหา

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (cyber hygiene) ประกอบด้วย

(1) การกำหนดมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ผู้ให้บริการ e-payment ต้องจัดให้มีการกำหนดการรักษาความมั่นคงปลอดภัยขั้นต่ำ (minimum security baseline) และตั้งค่าการรักษาความมั่นคงปลอดภัยสอดคล้องกับการให้บริการ (security hardening) ให้**ครอบคลุมระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่ายที่<u>รองรับระบบงานสำคัญ</u>** ให้ชัดเจนเป็นลายลักษณ์อักษร รวมทั้งดำเนินการและสอบทานตามที่ได้กำหนดไว้

กรณีผู้ให้บริการ e-payment ไม่สามารถปฏิบัติตามมาตรฐานที่กำหนดไว้ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

(2) การป้องกันภัยจาก malware (malware protection) ผู้ให้บริการ e-payment ต้องจัดให้มีเครื่องมือสำหรับป้องกันภัยจาก malware รวมทั้งติดตามให้มีการปรับปรุง (update) ให้เป็นปัจจุบันและเท่าทันภัยคุกคามใหม่อย่างสม่ำเสมอ เพื่อเป็นการลดความเสี่ยงจากการถูกโจมตีโดย malware

(3) การบริหารจัดการ security patch (security patch management) ผู้ให้บริการ e-payment มีกระบวนการบริหารจัดการ security patch (security patch management) ในทุกระบบงานและอุปกรณ์ เพื่อเป็นการลดความเสี่ยงที่ระบบเทคโนโลยีสารสนเทศจะถูกโจมตีจากช่องโหว่ใหม่ ๆ โดยผู้ให้บริการ e-payment ดำเนินการให้แล้วเสร็จในระยะเวลาที่เหมาะสมตามระดับความเสี่ยงของช่องโหว่และระดับความสำคัญของระบบงาน

สำหรับกรณีที่ผู้ผลิตยังไม่ออก security patch เพื่อปิดช่องโหว่ใหม่ ๆ ที่เพิ่งค้นพบ ผู้ให้บริการ e-payment ต้องหาการควบคุมอื่นทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีจากช่องโหว่นั้น ๆ

(4) การบริหารจัดการบัญชีผู้ใช้งานที่มีสิทธิ์สูง (privilege user) ผู้ให้บริการ e-payment ต้องจัดให้มีมาตรการควบคุมและจำกัดการใช้บัญชีผู้ใช้งานที่มีสิทธิ์สูงอย่างเข้มงวด เช่น การมอบหมายสิทธิ์ การเบิกใช้ กำหนดระยะเวลาการใช้งาน การสอบทานหลังการใช้ การกำหนดรหัสผ่านที่รัดกุม เป็นต้น **ของระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่าย และอุปกรณ์รักษาความปลอดภัยเครือข่าย** เพื่อป้องกันการนำบัญชีผู้ใช้งานที่มีสิทธิ์สูงไปใช้โดยไม่ได้รับอนุญาต

(5) การพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการ e-payment ต้องจัดให้มีการพิสูจน์ตัวตนแบบ multi-factor authentication ในกรณีดังต่อไปนี้

(5.1) บัญชีผู้ใช้งานที่มีสิทธิ์สูงทุกบัญชีของระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย

(5.2) บัญชีผู้ใช้งานทุกบัญชีที่สามารถเข้าถึงข้อมูลลูกค้า (customer information) ของระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย **ที่เชื่อมต่อกับเครือข่ายสาธารณะ (Internet facing)**

สำหรับกรณีที่ระบบปฏิบัติการ (operating system) ระบบฐานข้อมูล (database system) ระบบงาน (application) อุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยเครือข่าย ไม่รองรับการพิสูจน์ตัวตนแบบ multi-factor authentication ผู้ให้บริการ e-payment สามารถใช้วิธีการอื่นใดที่มีประสิทธิภาพเทียบเท่าทดแทน เพื่อลดความเสี่ยงจากการถูกโจมตีการพิสูจน์ตัวตนได้โดยง่าย

กรณีผู้ให้บริการ e-payment ไม่สามารถปฏิบัติตามได้ในบางระบบหรืออุปกรณ์ ต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (exception) เพื่อประเมินความเสี่ยงและพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอเหมาะสมก่อนดำเนินการ

(6) การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (vulnerability management and penetration testing) ผู้ให้บริการ e-payment ต้องจัดให้มีการบริหารจัดการช่องโหว่ (vulnerability assessment) สำหรับทุกระบบงานตามระดับความเสี่ยงอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมทั้งจัดให้มีการทดสอบเจาะระบบ (penetration test) โดยผู้เชี่ยวชาญภายในหรือภายนอกที่มีความเป็นอิสระ ครอบคลุมระบบงานและระบบเครือข่ายที่มีการเชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (Internet facing) สม่ำเสมออย่างน้อยปีละ 1 ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

4. กำหนดการรับฟังความคิดเห็น

ธนาคารแห่งประเทศไทยเปิดรับฟังความคิดเห็นและข้อเสนอแนะต่อแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต้นที่จำเป็น (cyber hygiene) ผ่านทางเว็บไซต์ของธนาคารแห่งประเทศไทย (www.bot.or.th) ตั้งแต่ วันที่ 17 มิถุนายน 2563 จนถึงวันที่ 15 กรกฎาคม 2563

ผู้ประสานงาน :
ทีมเกณฑ์การกำกับความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
Email: ITSupervision@bot.or.th