ธนาคารแห่งประเทศไทย

4 กันยายน 2562

เรียน ผู้จัดการ

ธนาคารพาณิชย์ทุกแห่ง

ที่ ธปท.ฝตท.(01) ว. 1252 /2562 เรื่อง แนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (iPentest)

ธนาคารแห่งประเทศไทย (ธปท.) ร่วมกับศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) จัดทำแนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (iPentest) ซึ่งเป็นแนวทางในการทดสอบเจาะระบบในลักษณะ Red Teaming ที่ผู้ทดสอบ (Ethical Hacker หรือ Red Team) ทดสอบเจาะระบบเพื่อประเมินความพร้อมในการรับมือของสถาบันการเงิน (สง.) ในด้านการป้องกัน (Protection) การตรวจจับ (Detection) การตอบสนองต่อเหตุการณ์และการรับมือภัยคุกคามทางไซเบอร์ (Response) ทั้งความพร้อมด้านบุคลากร กระบวนการ และเทคโนโลยี การทดสอบเจาะระบบแบบ iPentest จะช่วยยกระดับความเข้มแข็งด้านความมั่นคงปลอดภัยเพิ่มเติมจากการทดสอบเจาะระบบเชิงเทคนิค ที่ สง. ดำเนินการเป็นประจำอยู่แล้ว เพื่อให้มั่นใจว่า สง. มีการป้องกันที่แข็งแรง ตรวจจับภัยคุกคามทางไซเบอร์ได้ทันการณ์ และสามารถตอบสนองต่อเหตุการณ์ได้รวดเร็ว

ทั้งนี้ ธปท. กำหนดให้ สง. ที่มีความสำคัญเชิงระบบ (Domestic Systemically Important Banks: D-SIBs) หรือมีความเสี่ยงตั้งต้นทางไซเบอร์ (Cyber Inherent Risk) อยู่ในระดับสูง ดำเนินการตามแนวปฏิบัติ iPentest ภายในปี 2563 สำหรับ สง. อื่น ให้พิจารณาตามระดับความเสี่ยงและความพร้อมของ สง. โดยขอให้หน่วยงานที่รับผิดชอบดูแลและบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT Risk Management) และหน่วยงานกำกับการปฏิบัติตามหลักเกณฑ์ (Compliance) มีส่วนร่วมในการกำกับดูแลการปฏิบัติตามแนวปฏิบัติดังกล่าว

จึงเรียนมาเพื่อโปรดทราบและถือปฏิบัติ

ขอแสดงความนับถือ

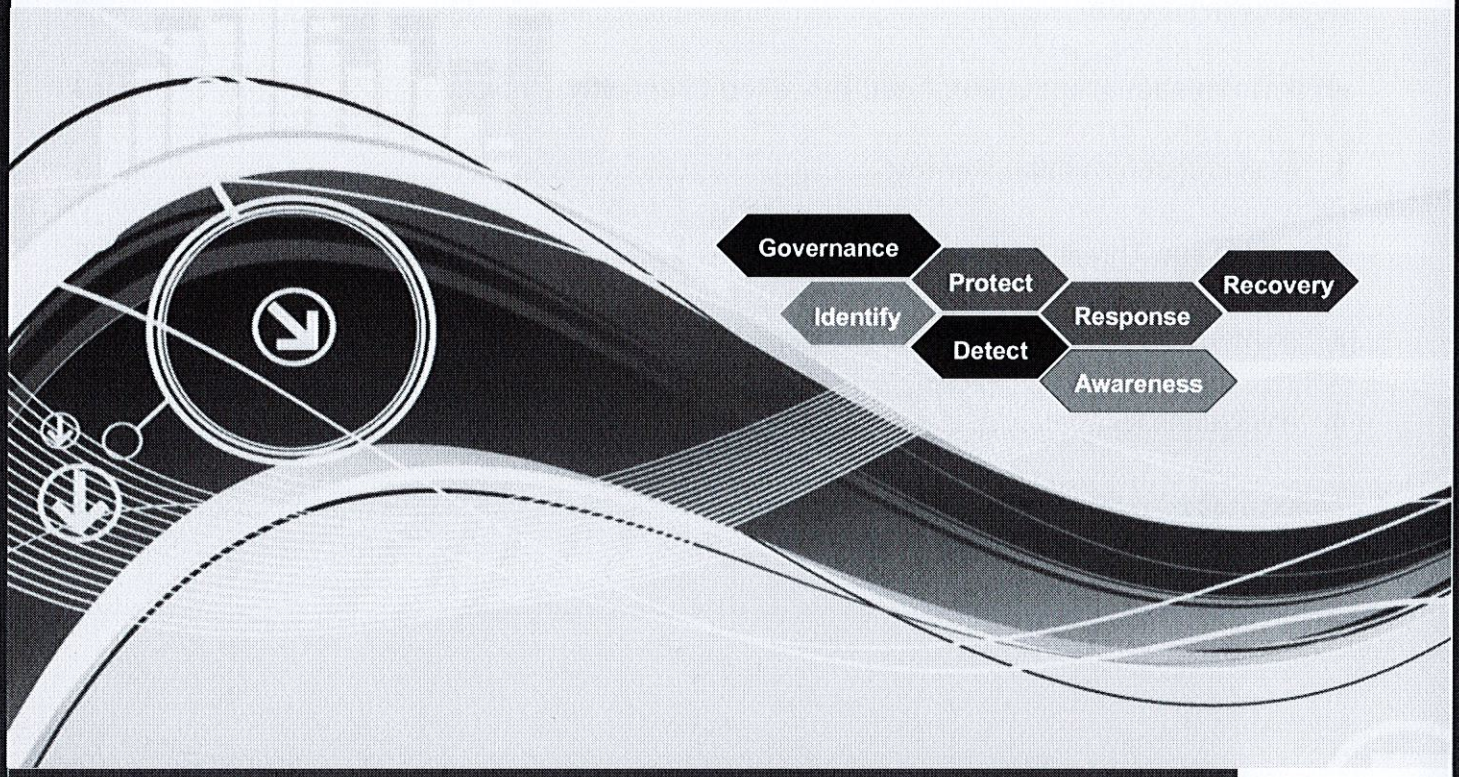
(นายจาตุรงค์ จันทรังษ์)
ผู้ช่วยผู้ว่าการ สายกำกับสถาบันการเงิน
ผู้ว่าการแทน

สิ่งที่ส่งมาด้วย แนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (iPentest)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
โทรศัพท์ 0 2283 5827 หรือ 0 2283 6577
E-Mail ITSupervision@bot.or.th

หมายเหตุ [X] ธนาคารได้จัด Workshop เพื่อสื่อสารและรับฟังความเห็นในวันที่ 26 เมษายน 2562 ณ ธปท.
[ ] ไม่มีการประชุมชี้แจง

ธนาคารแห่งประเทศไทย



แนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (Intelligence-led Penetration Testing Guideline: iPentest)

ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สายนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน

สารบัญ

แนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led

เหตุผลและความจำเป็น

สถาบันการเงินและผู้ให้บริการชำระเงิน ใช้เทคโนโลยีเป็นกลไกหลักในการขับเคลื่อนธุรกิจเพื่อตอบโจทย์การให้บริการลูกค้าและเพิ่มประสิทธิภาพในการบริหารจัดการธุรกิจ การใช้เทคโนโลยีทำให้สถาบันการเงินเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีความซับซ้อนและส่งผลกระทบแพร่กระจายในวงกว้างได้อย่างรวดเร็วมากขึ้น นอกเหนือจากการวางระบบป้องกันแล้ว การตรวจจับภัยไซเบอร์ที่คุกคามองค์กรเป็นสิ่งจำเป็นในการรับมือภัยไซเบอร์ได้อย่างทันการณ์ การทดสอบเจาะระบบเป็นหนึ่งในขั้นตอนสำคัญของการตรวจจับภัยไซเบอร์ผ่านการตรวจหาช่องโหว่ของระบบและบริหารจัดการเพื่อลดความเสี่ยงจากช่องโหว่ดังกล่าว ธนาคารแห่งประเทศไทยได้ออกประกาศที่ สนส. 19/2560 เรื่อง หลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ (Information Technology Risk) กำหนดให้สถาบันการเงินทดสอบเจาะระบบงาน (application) และระบบเครือข่าย (network) ที่เชื่อมต่อกับเครือข่ายสื่อสารสาธารณะ (internet facing) เป็นประจำอย่างน้อยปีละ 1 ครั้ง และเมื่อมีการเปลี่ยนแปลงระบบอย่างมีนัยสำคัญ

การทดสอบเจาะระบบที่สถาบันการเงินดำเนินการในปัจจุบัน เน้นการตรวจหาช่องโหว่ระบบเชิงเทคนิคเป็นหลัก อย่างไรก็ตาม การรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบันที่มีรูปแบบที่หลากหลายและซับซ้อน การทดสอบเจาะระบบเพื่อตรวจหาช่องโหว่ระบบเชิงเทคนิคอาจไม่เพียงพอสำหรับประเมินความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ ดังนั้น สถาบันการเงินจึงควรมีการทดสอบเจาะระบบที่สะท้อนความสามารถในการรับมือภัยคุกคามทางไซเบอร์ที่ครอบคลุมทั้งด้านบุคลากร กระบวนการ และเทคโนโลยี

ธนาคารแห่งประเทศไทยร่วมกับศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) จัดทำแนวปฏิบัติการทดสอบเจาะระบบแบบ Intelligence-led (Intelligence-led Penetration Testing Guideline: iPentest) ซึ่งเป็นการทดสอบการเจาะระบบภายใต้สถานการณ์เสมือนจริงในลักษณะ Red Teaming ที่มีการนำข้อมูล Threat Intelligence มากำหนดสถานการณ์จำลอง โดยผู้ทดสอบเจาะระบบใช้ทักษะและประสบการณ์หาแนวทางบุกรุกระบบเพื่อประเมินความพร้อมในการรับมือของสถาบันการเงิน ทั้งด้าน protection detection และ response ครอบคลุมทั้งด้านบุคลากร กระบวนการ และเทคโนโลยี การทดสอบในลักษณะดังกล่าวเป็นสิ่งที่สถาบันการเงินควรดำเนินการเพิ่มเติมจากการทดสอบเจาะระบบเชิงเทคนิคที่ทำอยู่แล้วโดยปกติ เพื่อให้สถาบันการเงินยกระดับความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ ให้มั่นใจว่ามีการป้องกันที่แข็งแรง การตรวจจับและการตอบสนองต่อภัยคุกคามทางไซเบอร์ได้ทันการณ์ และเพื่อเสริมสร้างความมั่นใจให้กับผู้บริหารระดับสูงและคณะกรรมการสถาบันการเงินในการกำกับดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของสถาบันการเงินด้วย

แนวทางการทดสอบเจาะระบบแบบ Intelligence-led (iPentest)

การทดสอบ iPentest เป็นการทดสอบการเจาะระบบภายใต้สถานการณ์เสมือนจริงในลักษณะ Red Teaming ที่ต้องอาศัยการสนับสนุนและมีส่วนร่วมของผู้บริหารและหน่วยงานที่เกี่ยวข้องภายในสถาบันการเงิน โดยแนวทางการดำเนินการประกอบด้วย 4 ส่วนสำคัญ คือ

1. **การกำกับดูแลการทดสอบให้ครอบคลุม และป้องกันความเสี่ยงที่อาจเกิดขึ้น** โดยการกำหนดบทบาทหน้าที่และความรับผิดชอบ และกระบวนการที่เกี่ยวข้องอย่างชัดเจน มีเกณฑ์การคัดเลือกผู้ทดสอบ รวมทั้งควบคุมดูแลการทดสอบอย่างรัดกุมและป้องกันความเสี่ยงที่อาจกระทบต่อการดำเนินธุรกิจ
2. **การใช้ข้อมูล Threat Intelligence กำหนดสถานการณ์จำลอง** โดยสถานการณ์จำลองที่กำหนดควรสอดคล้องกับความเสี่ยงที่สถาบันการเงินเผชิญ และรูปแบบภัยคุกคามทางไซเบอร์ในปัจจุบัน เพื่อให้การทดสอบใกล้เคียงสถานการณ์จริงมากที่สุด
3. **การดูแลการทดสอบเจาะระบบให้เป็นไปตามแผนที่กำหนด และได้ผลการทดสอบที่เป็นประโยชน์** เพื่อป้องกันความเสี่ยงและลดผลกระทบที่อาจเกิดขึ้นขณะทดสอบ ผู้ที่เกี่ยวข้องมีการสรุปและสอบทานผลการทดสอบร่วมกัน ตลอดจนจัดทำแผนและกำหนดระยะเวลาการปรับปรุงแก้ไขอย่างเหมาะสม
4. **การนำเสนอผลการทดสอบ** รายงานผลการทดสอบมีรายละเอียดครบถ้วน และนำเสนอต่อคณะกรรมการผู้บริหารและผู้ที่เกี่ยวข้องตามกระบวนการรายงานความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน

1. การกำกับดูแลการทดสอบ iPentest

1.1 **การทดสอบควรดำเนินการในแนวทางเดียวกับการบริหารจัดการโครงการ** คือ มีการกำหนดขอบเขต ระยะเวลา บทบาทหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องให้ชัดเจน ทั้งบุคลากรด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านอื่นที่เกี่ยวข้อง เช่น ด้านกฎหมาย ด้านสื่อสาร เป็นต้น ครอบคลุมทั้งในระดับบริหารและระดับปฏิบัติการ โดยดำเนินการร่วมกันในกระบวนการสำคัญ เช่น การกำหนดขอบเขต การประเมินความเสี่ยง การติดตามความคืบหน้า และการปรับปรุงแก้ไขช่องโหว่ที่พบจากการทดสอบ

1.2 **กำหนดบทบาทหน้าที่และความรับผิดชอบ**ของบุคลากรที่เกี่ยวข้อง ประกอบด้วย

1.2.1 **Control group** ทำหน้าที่ควบคุมดูแลกระบวนการทดสอบอย่างใกล้ชิด เพื่อป้องกันความเสี่ยงและลดผลกระทบที่อาจเกิดขึ้นจากการทดสอบ เช่น ข้อมูลรั่วไหล ระบบขัดข้อง รวมทั้งป้องกันไม่ให้มีการส่งต่อเหตุการณ์ผิดปกติ (escalation) ไปยังผู้ที่ไม่เกี่ยวข้องในระหว่างการทดสอบ จนนำไปสู่ความเข้าใจผิดต่อเหตุการณ์ที่เกิดขึ้น (false alarm) โดย Control group ควรประกอบด้วยบุคลากรที่รับผิดชอบดูแลงานที่เกี่ยวข้องกับระบบและบริการภายใต้ขอบเขตการทดสอบ ทั้งจากด้านเทคโนโลยีสารสนเทศ ด้านธุรกิจ และด้านอื่นที่เกี่ยวข้อง เช่น ด้านบริหารความเสี่ยง ด้านกำกับดูแลการปฏิบัติตามกฎหมายและหลักเกณฑ์ ด้านบริหารจัดการเหตุการณ์ผิดปกติ ด้านบริหารความต่อเนื่องทางธุรกิจและด้านสื่อสาร เป็นต้น

1.2.2 **ผู้รับผิดชอบรวบรวม Threat Intelligence** เพื่อใช้เป็นข้อมูลในการสร้างสถานการณ์จำลองในการทดสอบ

1.2.3 **ผู้ทดสอบ** ทำหน้าที่ทดสอบตามแผนการทดสอบ โดยผู้ทดสอบมีคุณสมบัติตามเกณฑ์ที่สถาบันการเงินกำหนด แบ่งเป็น 2 ระดับ ได้แก่ ระดับบริหารจัดการ (security management level) ทำหน้าที่บริหารจัดการเหตุการณ์ผิดปกติที่เกิดขึ้นและดูแลภาพรวมการดำเนินการทดสอบเจาะระบบ และระดับปฏิบัติการ (penetration tester level) ทำหน้าที่ทดสอบเจาะระบบ โดยผู้ทดสอบอาจเป็นผู้ทดสอบภายในสถาบันการเงินหรือว่าจ้างผู้ทดสอบจากภายนอก

1.3 **กำหนดขอบเขตและระยะเวลาการทดสอบ** โดยกำหนดขอบเขตการทดสอบให้ครอบคลุมระบบและบริการที่สำคัญ (critical functions) รวมถึงช่องโหว่ที่เกี่ยวข้องกับบุคลากร และกระบวนการป้องกัน ตรวจจับและรับมือเหตุการณ์ผิดปกติ โดยขอบเขตและระยะเวลาควรเก็บเป็นความลับและแจ้งในวงจำกัดเท่านั้น เพื่อให้การประเมินความสามารถในการป้องกัน ตรวจจับและรับมือเหตุการณ์ผิดปกติที่สถาบันการเงินจำลองสถานการณ์ มีประสิทธิผลและสามารถสะท้อนได้ใกล้เคียงสถานการณ์จริงมากที่สุด

1.4 **ทดสอบบนระบบในสภาพแวดล้อมจริง (production)** เพื่อให้การจำลองสถานการณ์โจมตีเสมือนจริงและสามารถสะท้อนความพร้อมของระบบ บุคลากร และกระบวนการป้องกัน ตรวจจับและรับมือเหตุการณ์ผิดปกติด้านภัยไซเบอร์ของสถาบันการเงินได้อย่างมีประสิทธิผล อย่างไรก็ตาม ในบางขั้นตอนของการทดสอบที่อาจส่งผลให้เกิดความเสี่ยงสูงต่อการดำเนินธุรกิจหรือส่งผลกระทบต่อลูกค้าในวงกว้าง อาจทดสอบบนสภาพแวดล้อมเสมือนจริง (UAT / pre-production environment) ทดแทน ทั้งนี้ควรระบุสภาพแวดล้อมที่ใช้ทดสอบให้ชัดเจนในรายงานผลการทดสอบด้วย

1.5 **ประเมินความเสี่ยงจากการทดสอบให้รัดกุม ครอบคลุมผลกระทบที่อาจเกิดขึ้นในทุกด้าน** เช่น ความเสี่ยงด้านปฏิบัติการ ความเสี่ยงด้านกฎหมายและกฎเกณฑ์ ความเสี่ยงด้านข้อมูล ความเสี่ยงจากบุคคลภายนอก (third-party risk) และความเสี่ยงด้านชื่อเสียง เป็นต้น เนื่องจากการทดสอบส่วนใหญ่ดำเนินการบนสภาพแวดล้อมจริง

1.6 **กำหนดเกณฑ์การคัดเลือกผู้ทดสอบที่ชัดเจน** โดยเกณฑ์ควรระบุคุณสมบัติผู้ทดสอบที่สถาบันการเงินมั่นใจว่าสามารถดำเนินการทดสอบได้อย่างมีประสิทธิผล มีประสิทธิภาพ เชื่อถือได้ และควรจัดทำเป็นลายลักษณ์อักษรเพื่อใช้อ้างอิงได้ โดยการกำหนดเกณฑ์พิจารณาปัจจัยเหล่านี้ประกอบกัน ได้แก่

1.6.1 **การได้รับประกาศนียบัตรการรับรองมาตรฐานความรู้ความสามารถ (certification)** เพื่อให้มั่นใจว่าผู้ทดสอบมีความรู้พื้นฐานด้านการทดสอบและมาตรฐานสากลที่ยอมรับโดยทั่วไป โดยตัวอย่างการรับรองมาตรฐานผู้ทดสอบระดับบริหารจัดการ และระดับปฏิบัติการที่ยอมรับโดยทั่วไป มีดังนี้

ระดับบริหารจัดการ (security management level) เช่น Certified Information Systems Security Professional (CISSP) Certified Information Security Manager (CISM)

ระดับปฏิบัติการ (penetration tester level) เช่น (1) ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester (2) ประกาศนียบัตรการรับรองจากสถาบัน Offensive Security เช่น OSCP, OSWP, OSCE, OSEE และ OSWE และ (3) ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GCIH, GMOB, GPEN, GXPN, GAWN และ GWAPT โดยสถาบันการเงินอาจพิจารณาประกาศนียบัตรการรับรองอื่นที่เทียบเคียงกับข้างต้นได้

1.6.2 **ประสบการณ์และผลงานของผู้ทดสอบ** เพื่อให้สถาบันการเงินมั่นใจว่าผู้ทดสอบมีประสบการณ์เพียงพอและมีผลงานที่แสดงความสามารถในการทดสอบเจาะระบบได้อย่างมีประสิทธิผลและประสิทธิภาพตามเป้าหมายและขอบเขตที่สถาบันการเงินวางไว้

1.6.3 **จรรยาบรรณในวิชาชีพ (ethics)** เพื่อให้มั่นใจว่าผู้ทดสอบปฏิบัติตามข้อกำหนดหรือเงื่อนไขการว่าจ้างงาน นโยบายการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและข้อตกลงการไม่เปิดเผยข้อมูลของสถาบันการเงินได้อย่างเคร่งครัด ตลอดจนไม่มีประวัติที่เสื่อมเสียที่กระทบต่อการรักษาความมั่นคงปลอดภัย เช่น ประวัติอาชญากรรมหรือการทุจริต เป็นต้น

1.7 **ควรพิจารณาปรับเปลี่ยนผู้ทดสอบอย่างต่อเนื่องตามความเหมาะสม** เพื่อให้เกิดความหลากหลายในด้านมุมมอง วิธีการหรือเทคนิคการทดสอบ เช่น กรณีที่สถาบันการเงินดำเนินการทดสอบโดยใช้ผู้ทดสอบของสถาบันการเงินเอง ควรพิจารณาปรับเปลี่ยนผู้ทดสอบหรือว่าจ้างผู้ทดสอบภายนอกดำเนินการทดสอบเพิ่มเติมด้วย

2. การใช้ข้อมูล Threat Intelligence

2.1 **มีการนำข้อมูล Threat Intelligence กำหนดสถานการณ์ในการทดสอบ** โดยข้อมูล Threat Intelligence เป็นข้อมูลวิธีการ เทคนิค และกระบวนการที่ผู้ไม่ประสงค์ดีใช้ในการพยายามเข้าถึงระบบของสถาบันการเงิน ซึ่งมักเรียกโดยย่อว่า TTP (Tactics, Techniques and Procedures) โดยเป็นข้อมูลที่สถาบันการเงินอาจจัดให้มีเอง หรือจ้างผู้ให้บริการ Threat Intelligence ดำเนินการให้ ทั้งนี้ ข้อมูลที่ใช้ต้องสอดคล้องกับความเสี่ยงภัยไซเบอร์ที่สถาบันการเงินเผชิญ และรูปแบบภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในปัจจุบัน เพื่อให้การทดสอบใกล้เคียงสถานการณ์จริงมากที่สุด

2.2 **การสร้างสถานการณ์จำลอง** ควรประกอบด้วย

2.2.1 **ภาพรวมภัยคุกคามที่สถาบันการเงินเผชิญ** (cyber threat landscape) ควรระบุภัยคุกคามที่สำคัญ รายละเอียดของภัยคุกคามที่มีโอกาสเกิดสูง และสถานการณ์ที่อาจเกิดขึ้นกับสถาบันการเงิน

2.2.2 **ช่องโหว่ของสถาบันการเงิน** รวมถึงช่องโหว่ของระบบ กระบวนการ และบุคลากร โดยเฉพาะช่องโหว่ของกระบวนการบริหารจัดการข้อมูล

2.3 **ควรปรับปรุงแก้ไขช่องโหว่สำคัญที่พบทันที** ในระหว่างการรวบรวมข้อมูล Threat Intelligence หากหน่วยงานหรือผู้ที่รับผิดชอบด้าน Threat Intelligence พบช่องโหว่หรือภัยคุกคามที่สำคัญที่อาจเกิดขึ้นกับสถาบันการเงิน ต้องรีบแจ้งให้ Control group รับทราบโดยเร็ว เพื่อปรับปรุงแก้ไขช่องโหว่ดังกล่าวอย่างทันท่วงที

3. การทดสอบเจาะระบบ

3.1 **แผนการทดสอบ** ควรครอบคลุมอย่างน้อย ต่อไปนี้

3.1.1 **สถานการณ์จำลอง** (scenarios) ที่การทดสอบสามารถปฏิบัติได้จริงและมีประสิทธิผลในการประเมินการรับมือภัยคุกคามทางไซเบอร์

3.1.2 **เป้าหมายของการโจมตี** (threat actor goals) หรือ flag ที่ผู้ทดสอบต้องพยายามเข้าถึงและดำเนินการตามที่กำหนดไว้ (capture)

3.1.3 **หลักฐานจากการทดสอบ** (validated evidence) ที่สะท้อนผลกระทบทางธุรกิจเพื่อจัดทำแนวทางในการปรับปรุงหลังการทดสอบ

3.1.4 **การบริหารความเสี่ยงจากการทดสอบ** โดยควรมีผลการประเมินความเสี่ยงและแผนการควบคุมและบริหารความเสี่ยงที่เกิดจากการทดสอบ เพื่อป้องกันและลดผลกระทบที่อาจเกิดขึ้นขณะทดสอบ

3.2 **ผู้ทดสอบดำเนินการทดสอบ**ตามสถานการณ์จำลองที่กำหนด โดยพยายามเข้าถึงและดำเนินการตามเป้าหมายการโจมตีที่กำหนดไว้

3.3 **จัดให้ผู้ทดสอบและผู้ที่เกี่ยวข้องสอบทานผลการทดสอบร่วมกัน (test review workshop)** เพื่อหารือถึงช่องโหว่ที่ตรวจพบ รายละเอียดวิธีการหรือเทคนิคที่ใช้ทดสอบ รวมถึงผลกระทบอื่นที่อาจเกิดขึ้นหากไม่มีข้อจำกัดเรื่องเวลาและทรัพยากร รวมทั้งการปรับปรุงแก้ไขหรือวิธีการลดความเสี่ยง

3.4 **จัดทำแผนและกำหนดระยะเวลาปรับปรุงแก้ไข** จากผลการทดสอบและผลสรุปจาก test review workshop เพื่อให้การปรับปรุงแก้ไขช่องโหว่อย่างเหมาะสมและสอดคล้องกับระดับความเสี่ยงที่สถาบันการเงินยอมรับได้

4. การสรุปผลการทดสอบ

4.1 **รายงานผลการทดสอบ** (iPentest report) อย่างน้อยควรครอบคลุม ดังนี้

- บทสรุปผู้บริหาร (executive summary)
- ขอบเขตการทดสอบเจาะระบบ
- สภาพแวดล้อมการทดสอบเจาะระบบ
- วิธีการและขั้นตอนดำเนินการทดสอบเจาะระบบ
- ผลการทดสอบเจาะระบบที่ครอบคลุมช่องโหว่ทั้งด้านบุคลากร กระบวนการ และเทคโนโลยี
- ผลประเมินความสามารถด้านการป้องกัน ตรวจจับและรับมือเหตุการณ์ผิดปกติของสถาบันการเงิน
- แผนการปรับปรุงแก้ไขปัญหา และการปิดช่องโหว่ ตามระดับความเสี่ยง

4.2 **นำเสนอผลการทดสอบและแผนการปรับปรุงแก้ไข** ต่อคณะกรรมการระดับบริหารที่เกี่ยวข้อง เช่น คณะกรรมการบริหารจัดการและกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Steering Committee) เพื่อให้ผู้บริหารระดับสูงรับทราบและมีพิจารณาการบริหารจัดการความเสี่ยงที่เกี่ยวข้อง

4.3 **จัดให้มีผู้รับผิดชอบติดตามการปรับปรุงแก้ไข** อย่างต่อเนื่องและรายงานความคืบหน้าการดำเนินการต่อคณะกรรมการที่เกี่ยวข้อง เช่น อาจมอบหมายหน่วยงานตรวจสอบภายในดำเนินการดังกล่าว

4.4 **นำเสนอผลการทดสอบต่อคณะกรรมการระดับกำกับดูแล** ได้แก่ คณะกรรมการสถาบันการเงิน คณะกรรมการบริหารความเสี่ยง และคณะกรรมการตรวจสอบ โดยอาจนำเสนอประกอบกับภาพรวมความเสี่ยงด้านไซเบอร์ เพื่อให้คณะกรรมการดังกล่าวรับทราบและพิจารณาให้มีการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับนโยบาย รวมทั้งตระหนักถึงความสำคัญและสนับสนุนให้มีการทดสอบอย่างต่อเนื่องต่อไป

เอกสารอ้างอิง

- CBEST Intelligence-Led Testing, Council for Registered Ethical Security Testers (CREST) associated with Bank of England, 2016
- A Framework for the Regulatory use of Penetration Testing in the Financial Services Industry, Global Financial Markets Association (GFMA), March 2018
- Cyber Resilience Assessment Framework, Hong Kong Monetary Authority, December 2016
- Red Team: Adversarial Attack Simulation Exercises, Monetary Authority of Singapore, November 2018

ธนาคารแห่งประเทศไทย