R0Cyber

CYBER LAW & STANDARDS · 2.2 ตอนที่ 2

พ.ร.บ.คอมพิวเตอร์ และขอบเขตทางกฎหมาย

อะไรคือความผิด ผู้ให้บริการมีหน้าที่อะไร และทีมไซเบอร์ทำงานอย่างไรให้อยู่ในกรอบกฎหมาย

ม.5–14 | log 90 วัน | ได้รับอนุญาต

CYBER ACT	พ.ร.บ.ไซเบอร์ 2562 · CII	สกมช.
COMPUTER	พ.ร.บ.คอมพิวเตอร์	ม.5–14, 26
PDPA	คุ้มครองข้อมูลส่วนบุคคล	สคส.
POLICY	นโยบายความปลอดภัยองค์กร	ISO 27001
REPORT	รายงานเหตุ · ประสานงาน	72 ชม.
EXERCISE	Tabletop · ซ้อมตัดสินใจ	Workshop

CYBER LAW · POLICY · RESPONSE

อ้างอิง พ.ร.บ.ไซเบอร์ 2562 · พ.ร.บ.คอมพิวเตอร์ 2550/2560 · PDPA 2562 · เนื้อหาเพื่อการศึกษา ไม่ใช่คำปรึกษาทางกฎหมาย

R0Cyber

ตอนนี้มี 5 หัวข้อ

01	ภาพรวมกฎหมาย	ฉบับ 2550 · แก้ไข 2560 · ใช้กับใคร
02	ความผิดสำคัญ	ม.5–10 ต่อระบบและข้อมูล · ม.11–14
03	หน้าที่ผู้ให้บริการ	ม.26 เก็บข้อมูลจราจร 90 วัน
04	ขอบเขตงานไซเบอร์	งานที่ถูกกฎหมาย · หลักฐาน · กฎหมายใหม่
05	ทบทวนและสรุป	Quick check · สรุปตอน

R0Cyber

พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ฉบับ 2550

กำหนดความผิดต่อระบบและข้อมูลคอมพิวเตอร์ และหน้าที่ผู้ให้บริการ

แก้ไข 2560

ปรับบทความผิด เพิ่มเรื่องสแปม ปรับหน้าที่เก็บข้อมูลจราจร และการระงับเนื้อหา

ใช้กับใคร

ผู้กระทำความผิด · ผู้ให้บริการ · พนักงานเจ้าหน้าที่ที่มีอำนาจสืบสวน

มุมผู้กระทำ

ห้ามเข้าถึง ดักรับ แก้ไข หรือรบกวนระบบโดยไม่ได้รับอนุญาต

มุมผู้ให้บริการ

เก็บข้อมูลจราจร และให้ความร่วมมือกับเจ้าหน้าที่ตามกฎหมาย

มุมผู้เสียหาย

เก็บหลักฐาน แจ้งความ และประสานเจ้าหน้าที่

มุมทีมไซเบอร์

ทุกการทดสอบต้องมีอนุญาต — เครื่องมือเดียวกัน ต่างกันที่อนุญาต

R0Cyber

ความผิดต่อระบบและข้อมูลคอมพิวเตอร์

มาตรา	การกระทำ	โทษสูงสุด
ม.5	เข้าถึงระบบที่มีมาตรการป้องกัน โดยมิชอบ	จำคุก 6 เดือน หรือปรับ 10,000 บาท
ม.6	นำมาตรการป้องกันการเข้าถึงที่รู้มา ไปเปิดเผยโดยมิชอบ	จำคุก 1 ปี หรือปรับ 20,000 บาท
ม.7	เข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกัน โดยมิชอบ	จำคุก 2 ปี หรือปรับ 40,000 บาท
ม.8	ดักรับข้อมูลที่อยู่ระหว่างการส่ง โดยมิชอบ	จำคุก 3 ปี หรือปรับ 60,000 บาท
ม.9	ทำให้ข้อมูลเสียหาย ถูกทำลาย แก้ไข เปลี่ยนแปลง	จำคุก 5 ปี หรือปรับ 100,000 บาท
ม.10	ทำให้ระบบถูกระงับ ชะลอ ขัดขวาง ทำงานไม่ได้ตามปกติ	จำคุก 5 ปี หรือปรับ 100,000 บาท

คำสำคัญ: "โดยมิชอบ" = ไม่ได้รับอนุญาต — ผู้ดูแลระบบที่ทำนอกหน้าที่ หรือทดสอบเกินขอบเขตที่ได้รับอนุญาต ก็เข้าข่ายได้

R0Cyber

ความผิดอื่นที่คนทำงานไซเบอร์ต้องรู้

ม.11 ส่งข้อความรบกวน (สแปม)

ส่งโดยไม่เปิดให้ผู้รับบอกเลิกหรือปฏิเสธได้ง่าย — ปรับไม่เกิน 200,000 บาท

ม.12 กระทบระบบสำคัญ

ถ้าการกระทำตาม ม.5–11 เกิดกับระบบที่เกี่ยวกับความมั่นคงหรือบริการสาธารณะ โทษหนักขึ้นมาก

ม.13 จำหน่าย/เผยแพร่ชุดคำสั่ง

ที่จัดทำขึ้นเฉพาะเพื่อใช้กระทำผิดตาม ม.5–11 — จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท

ม.14 นำเข้าข้อมูลเท็จ/ผิดกฎหมาย

ข้อมูลปลอม เท็จ ที่น่าจะเกิดความเสียหาย หรือกระทบความมั่นคง — จำคุกไม่เกิน 5 ปี

ข้อควรระวัง: เครื่องมือทดสอบความปลอดภัยใช้ได้ถูกกฎหมาย แต่การแจกจ่ายมัลแวร์หรือชุดเจาะระบบให้ผู้อื่นใช้โจมตี เข้าข่ายมาตรา 13

R0Cyber

หน้าที่ผู้ให้บริการ: เก็บข้อมูลจราจรคอมพิวเตอร์

≥ 90 วัน

นับแต่ข้อมูลเข้าสู่ระบบ
เจ้าหน้าที่สั่งให้เก็บนานขึ้นได้ ไม่เกิน 2 ปี

ใครคือผู้ให้บริการ และต้องเก็บอะไร

- ผู้ให้บริการอินเทอร์เน็ต · โฮสติ้ง · ผู้ให้บริการแอป และองค์กรที่ให้บุคคลอื่นใช้เครือข่าย เช่น Wi-Fi สำนักงาน โรงแรม
- แหล่งกำเนิด ปลายทาง วันเวลา ปริมาณ ระยะเวลา ชนิดบริการ และข้อมูลระบุผู้ใช้เท่าที่จำเป็น
- ไม่ปฏิบัติตาม: ปรับไม่เกิน 500,000 บาท

ทำให้เป็นหลักฐานได้: ซิงก์เวลา (NTP) · เก็บแบบแก้ไขไม่ได้ · จำกัดผู้เข้าถึง · ตรวจว่าเก็บครบจริง

log เป็นข้อมูลส่วนบุคคลด้วย — ต้องปฏิบัติตาม PDPA ควบคู่: แจ้งวัตถุประสงค์ จำกัดสิทธิ์ และลบเมื่อพ้นระยะ

R0Cyber

งานไซเบอร์ที่ถูกกฎหมาย: อนุญาต · ขอบเขต · หลักฐาน

ทำได้เมื่อมีสิ่งเหล่านี้

- หนังสืออนุญาตจากเจ้าของระบบที่มีอำนาจ
- ขอบเขตชัดเจน: ระบบ ช่วงเวลา วิธีการ (RoE)
- นโยบายองค์กรรองรับงานเฝ้าระวังของ SOC
- บันทึกทุกกิจกรรมและรายงานผล

เส้นที่ห้ามข้าม

- โจมตีกลับ (hack back) ระบบของผู้โจมตี
- สแกนหรือทดสอบระบบที่ไม่ได้รับอนุญาต
- เปิดอ่านอีเมล/แชตพนักงานโดยไม่มีนโยบายและเหตุจำเป็น
- เก็บข้อมูลที่พบเกินจำเป็น หรือนำไปเผยแพร่

หลักจำ: เครื่องมือเดียวกัน ทำงานเดียวกัน — ต่างกันที่ "ได้รับอนุญาตหรือไม่" และ "อยู่ในขอบเขตหรือไม่"

R0Cyber

สถานการณ์ที่ต้องคิดให้รอบ

สถานการณ์	แนวทางที่ปลอดภัย
พบช่องโหว่ในเว็บของบริษัทอื่นโดยบังเอิญ	หยุดทดสอบ · ไม่ดึงข้อมูล · แจ้งเจ้าของผ่านช่องทางทางการ หรือ ThaiCERT
SOC ต้องตรวจทราฟฟิกของพนักงาน	มีนโยบายแจ้งพนักงาน · ทำเท่าที่จำเป็นต่อความปลอดภัย · จำกัดผู้เข้าถึง (PDPA)
ทีม IR ต้องทำสำเนาดิสก์เครื่องที่ถูกเจาะ	ได้รับอนุมัติ · ทำ hash · บันทึกห่วงโซ่การครอบครองหลักฐาน
ผู้รับจ้างทดสอบเจาะ เจอระบบนอกขอบเขต	หยุด แจ้งผู้ว่าจ้าง ขออนุญาตเพิ่มเป็นลายลักษณ์อักษรก่อน
ค้นข้อมูล OSINT ของผู้โจมตี	ใช้ข้อมูลสาธารณะ ไม่ล็อกอินบัญชีผู้อื่น ไม่ปลอมตัวตนเพื่อเข้าถึงระบบ

ไม่แน่ใจ = หยุดและถามฝ่ายกฎหมาย/DPO ก่อน — ความรวดเร็วไม่คุ้มกับการกลายเป็นผู้กระทำผิดเสียเอง

R0Cyber

เก็บหลักฐานและแจ้งความเมื่อถูกโจมตี

1

เก็บก่อนล้าง

log · ภาพหน้าจอ · สำเนาดิสก์/หน่วยความจำ

2

ทำ hash

พิสูจน์ว่าหลักฐานไม่ถูกแก้ไข

3

ห่วงโซ่การครอบครอง

ใคร รับ ส่ง เก็บ เมื่อไร

4

แจ้งความ

ตำรวจไซเบอร์ · แจ้งความออนไลน์

5

ประสานต่อเนื่อง

ผู้ให้บริการ · ธนาคาร · ThaiCERT

พ.ร.ก.มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (2566 · แก้ไข 2568)

ระงับบัญชีต้องสงสัย/บัญชีม้า แลกเปลี่ยนข้อมูลระหว่างธนาคาร ผู้ให้บริการ และเจ้าหน้าที่ · ฉบับ 2568 (มีผล 13 เม.ย. 2568) ให้สถาบันการเงิน ผู้ให้บริการโทรคมนาคม และแพลตฟอร์มต้องร่วมรับผิดชอบความเสียหายเมื่อไม่ปฏิบัติตามมาตรการ

เหตุหลอกลวงทางการเงิน: แจ้งธนาคารให้ระงับบัญชีโดยเร็ว แล้วแจ้งความ — ยิ่งเร็ว โอกาสติดตามเงินคืนยิ่งสูง

R0Cyber

เหตุเดียว ใช้กฎหมายสามฉบับพร้อมกัน

ตัวอย่าง: แรนซัมแวร์เข้ารหัสระบบ และขโมยข้อมูลลูกค้าออกไป

พ.ร.บ.คอมพิวเตอร์

ผู้โจมตีมีความผิด ม.5, 7, 9, 10 ⟶ เก็บหลักฐานและแจ้งความ · ผู้ให้บริการส่ง log ให้เจ้าหน้าที่

PDPA

ข้อมูลส่วนบุคคลรั่ว ⟶ ประเมินความเสี่ยง แจ้ง สคส. ภายใน 72 ชม. และแจ้งเจ้าของข้อมูลถ้าเสี่ยงสูง

พ.ร.บ.ไซเบอร์

ถ้าเป็น CII ⟶ แจ้ง สกมช. และหน่วยงานควบคุม · ถ้าไม่ใช่ ขอความช่วยเหลือ ThaiCERT ได้

ต่อในตอนที่ 3: รวมทุกหน้าที่ไว้ใน "เมทริกซ์การรายงานเหตุ" และนโยบายเดียวขององค์กร

QUICK CHECK

R0Cyber

ทบทวนสั้น ๆ: จริงหรือไม่จริง?

1. ทดสอบระบบเกินขอบเขตที่ได้รับอนุญาต อาจผิด ม.5 หรือ ม.7	✓ จริง	เข้าถึงโดยมิชอบ
2. ผู้ให้บริการต้องเก็บข้อมูลจราจรอย่างน้อย 90 วัน	✓ จริง	มาตรา 26
3. ถูกโจมตีแล้ว โจมตีกลับระบบผู้โจมตีได้ถูกกฎหมาย	✗ ไม่จริง	ห้าม hack back
4. ควรล้างเครื่องทันทีก่อนเก็บหลักฐาน	✗ ไม่จริง	เก็บหลักฐานก่อน

SUMMARY · ตอนที่ 2

สรุป: พ.ร.บ.คอมพิวเตอร์

- ✓ ความผิดต่อระบบ ม.5–10 · สแปม ระบบสำคัญ ชุดคำสั่ง ม.11–13
- ✓ ผู้ให้บริการเก็บข้อมูลจราจร ≥ 90 วัน (ม.26)
- ✓ งานไซเบอร์ต้องมีอนุญาตและขอบเขต — ห้าม hack back
- ✓ เก็บหลักฐาน + hash + ห่วงโซ่การครอบครอง แล้วแจ้งความ
- ✓ เหตุเดียวอาจต้องใช้กฎหมายหลายฉบับพร้อมกัน

ทำแบบทดสอบท้ายตอน แล้วพบกันในตอนถัดไป

ตอนถัดไป

ตอนที่ 3

นโยบาย การรายงานเหตุ และการประสานงาน

- ลำดับชั้นเอกสารนโยบาย
- การรายงานเหตุภายใน
- เมทริกซ์รายงานภายนอก
- บทบาทและการสื่อสาร