การสร้างทีมรักษาความปลอดภัยไซเบอร์ สำหรับหน่วยงานระดับกลางถึงเล็ก

ผศ.อัครเดช วัชระภูพงษ์

ผู้ช่วยอธิการบดีฝ่ายสารสนเทศและความปลอดภัยทางไซเบอร์ สจล.

จุดสังเกตการรักษาความปลอดภัยไซเบอร์ (1/2)

- งาน..ล้น..มือ
  - ไซเบอร์ฯ ไม่ใช่งานหลัก แถมเพิ่มความยุ่งยากในการทำงาน
- ไม่มีใครเข้าใจระบบไอทีทั้งหมด
  - ต่างคนต่างก็รู้เฉพาะระบบ/บริการที่ตัวเองใช้
- ไม่มีทีมชำนาญโดยเฉพาะ/เต็มเวลา
  - ไม่มีอัตรา ตำแหน่งไม่ก้าวหน้า งานไม่ท้าทาย ที่อื่นให้ค่าตัวสูงกว่า ฯลฯ

จุดสังเกตการรักษาความปลอดภัยไซเบอร์ (2/2)

- ไม่มีการตรวจประเมินความเสี่ยงภัยไซเบอร์อย่างจริงจัง
  - เป็นแค่งานกระดาษรูทีน ไม่อัปเดตการเปลี่ยนแปลงระบบไอทีที่เกิดขึ้น
- เน้นการใช้งานได้เหนือการรักษาความปลอดภัยไซเบอร์
  - ไม่ได้ให้ความสำคัญการรักษาความปลอดภัยตั้งแต่ขั้นตอนการออกแบบและสร้าง
- ไม่มีแนวทางบำรุงรักษาระบบสารสนเทศเดิมได้ดีพอ
  - ของบซ่อมบำรุงยาก ส่งมอบระบบอย่างไรก็ใช้ไปอย่างนั้นเรื่อยมาไม่กล้าเปลี่ยน

วัฒนธรรมองค์กรที่ควรสร้างให้เกิดขึ้นเพื่อรับมือภัยจากไซเบอร์

- หัวหน้าต้องเป็นแบบอย่างที่ดีแก่ลูกน้อง
- ลำบากขึ้นหน่อยแต่ปลอดภัยขึ้นมาก
- ความผิดพลาดคือบทเรียน

ทีมที่จำเป็นต้องมี – ทีมความปลอดภัยไซเบอร์ (1/2)
Cyber-Security Committee

- ตัวแทนผู้บริหาร
  - ผ่านการสร้างความตระหนักรู้ความปลอดภัยไซเบอร์ระดับผู้บริหาร
  - ทำตัวเป็นแบบอย่างที่ดีในการรักษาความปลอดภัยไซเบอร์
- ตัวแทนฝ่ายกฎหมาย
  - ผ่านการอบรมด้านกฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ อาทิ พรบ.ไซเบอร์ พรบ. คอม พรบ.ข้อมูลส่วนบุคคล

ทีมที่จำเป็นต้องมี – ทีมความปลอดภัยไซเบอร์ (2/2)
Cyber-Security Committee

- ตัวแทนฝ่ายประชาสัมพันธ์
  - ผ่านการอบรมด้านภาพลักษณ์องค์กรและสื่อสังคมออนไลน์
- ตัวแทนฝ่ายปฏิบัติการ
  - ผ่านการสร้างความตระหนักรู้ความปลอดภัยไซเบอร์ระดับปฏิบัติการ
  - ควรมีทั้งที่ทราบระบบงานและที่ทราบเชิงเทคนิค
  - ได้รับการอบรมทักษะและความรู้ด้านความปลอดภัยไซเบอร์เป็นประจำ

ทีมที่จำเป็นต้องมี – ทีมรับมือเหตุฉุกเฉินทางไซเบอร์

Cyber-Security Incident Response Team (CSIRT)

- ผู้มีอำนาจตัดสินใจ/ประสานงานได้ทันท่วงที
  - ผ่านการซักซ้อมแผนรับมือเหตุฉุกเฉินทางไซเบอร์
  - พร้อมประสานงานทุกเมื่อ
- ผู้ปฏิบัติงาน
  - ผ่านการซักซ้อมแผนรับมือเหตุฉุกเฉินทางไซเบอร์
  - พร้อมทุกเมื่อที่เหตุเกิดหรือตรวจจับความผิดปกติได้

แผนที่ควรมีสำหรับหน่วยงานขนาดกลางถึงเล็ก (1/2)

- แผนตรวจสอบสินทรัพย์และประเมินความเสี่ยงความปลอดภัยไซเบอร์
  - รายการอุปกรณ์ โปรแกรม และบริการสารสนเทศ ทั้งที่ใช้ปฏิบัติงานและสนับสนุนงาน
  - ตารางความเสี่ยง ผลกระทบ และกลวิธีรับมือ
- แผนรับมือเหตุฉุกเฉินทางไซเบอร์
  - วิธีการรายงานและระงับเหตุ
  - วิธีการติดต่อประสานงาน

แผนที่ควรมีสำหรับหน่วยงานขนาดกลางถึงเล็ก (2/2)

- แผนสร้างความตระหนักรู้และเท่าทัน
  - เป้าหมายคือทุกคน อย่างน้อยปีละ 1 ครั้ง
  - ผลิตสื่อประชาสัมพันธ์เป็นระยะ อย่างน้อยเดือนละ 1 ครั้ง
- แผนอบรมและพัฒนาบุคลากร
  - เป้าหมายคือบางคน อย่างน้อยปีละ 1 ครั้ง
  - ควรครอบคลุมทั้งกลุ่มบริหารจัดการและกลุ่มเทคนิค

การเตรียมพร้อมเชิงนโยบาย (1/4)

- พันธมิตร
  - NCSA/ThaiCERT
  - Brotherhood
  - Vendors
  - Universities
  - Volunteers

การเตรียมพร้อมเชิงนโยบาย (2/4)

- ส่วนกลางสนับสนุน
  - **Practical** Plans and Checklists
    - … and NOT one-size-fits-all!
  - Dedicated Cyber-Security Teams
    - CSOC & Hotline
    - Experts
  - BYOD Approach

การเตรียมพร้อมเชิงนโยบาย (3/4)

- เครือข่ายข่าวสาร/องค์ความรู้
- ปรับสัญญาจัดซื้อจัดจ้างให้สอดคล้องกับการรักษาความปลอดภัยไซเบอร์
  - คุณสมบัติผู้เข้าร่วมประมูล ที่มีความใส่ใจต่อการรักษาความปลอดภัยไซเบอร์
  - คุณลักษณะอุปกรณ์หรือโปรแกรม ที่เอื้อต่อการตรวจจับเหตุผิดวิสัยทางไซเบอร์
  - เกณฑ์คะแนน **VS** เกณฑ์ราคา

การเตรียมพร้อมเชิงนโยบาย (4/4)

- ผูกกับระบบตรวจสอบ (ประเมินหน่วยงาน)
  - ต้องส่งรายงานการตรวจสอบสินทรัพย์และประเมินความเสี่ยงความปลอดภัยไซเบอร์
  - ต้องส่งรายงานการสร้างความตระหนักรู้และพัฒนาบุคลากรด้านความปลอดภัยไซเบอร์
- ผูกกับระบบเลื่อนขั้น (ประเมินบุคลากร)
  - ให้คะแนนเพิ่มพิเศษหากเข้าร่วม 2 ทีมข้างต้น
  - ให้คะแนนเพิ่มพิเศษหากผ่านการอบรมที่จำเป็นต่อการรักษาความปลอดภัยไซเบอร์

การเตรียมพร้อมเชิงเทคนิค (1/2)

- เครื่องมือ/แพลตฟอร์มตรวจจับเหตุผิดปกติ
  - Message Logging System
  - Endpoint Detection and Response (EDR)
    - … not only anti-virus!
  - SEIM/SOAR
    - … not only centralized log servers!

การเตรียมพร้อมเชิงเทคนิค (2/2)

- ออกแบบให้ AAA แข็งแกร่ง
  - Authentication : 2FA & Zero-Trust
  - Authorization : Access Control Matrix
  - Auditing : What/Where/When/How/Who/Whom
- ไม่สนใจเพียงเครื่องคอมพิวเตอร์ แต่ต้องสนใจสิ่งที่ไม่ใช่คอมพิวเตอร์ด้วย

"Security is a process, not a product. Products provide some protection, but the only way to effectively do business in an insecure world is to put processes in place that recognize the inherent insecurity in the products. The trick is to reduce your risk of exposure regardless of the products or patches."

Bruce Schneier