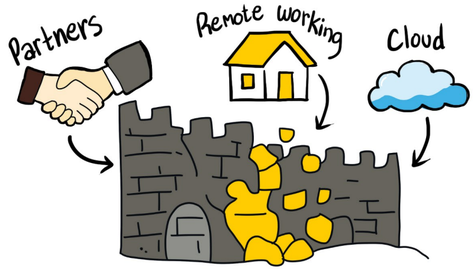
Seminar

CYBERSECURITY x CYBERSECURITY

Shift the Core, Know the Unknown

CYFENCE



Old : เชื่อใจทุกอย่างในเครือข่ายภายใน ❌
New : ไม่มี “ภายใน” อีกต่อไป ✅

IMPLICIT TRUST =WEAKNESS

Data Breach / Ransomware / API Attack

Zero Trust

ไม่เชื่อใจโดยปริยาย ตรวจสอบทุกการเข้าถึงเสมอ ไม่ว่ามาจากที่ใด

Shift Up Process - Zero Trust

กระบวนการ 5 ขั้นตอนสู่ Zero Trust

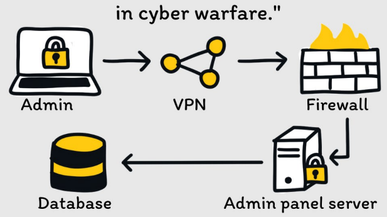
Step 1: Define Your Protect Surface

ถามว่า:"เรากำลังปกป้องอะไร?"มุ่งเน้นที่ “ของมีค่า"(DAAS):

Data	Application	Asset	Service
ข้อมูลสำคัญ	แอปพลิเคชันสำคัญ	ทรัพย์สินสำคัญ	บริการสำคัญ

Step 2: Map the Transaction Flows

"Mapping is the most critical weapon in cyber warfare."



Step 3: Build a Zero Trust Architecture

- สร้าง"Micro-perimeter" รอบ Protect Surface แทนที่จะป้องกันทั้งเครือข่าย ให้สร้างกำแพงเล็กๆรอบสิ่งที่สำคัญที่สุด
- ใช้ Segmentation/Micro-segmentation แบ่งเครือข่าย
- เป้าหมาย:จำกัด "Blast Radius"

Step 4: Create a Zero Trust Policy

“Deny All” by defult
ปฏิเสธทุกการเข้าถึงเป็นค่าเริ่มต้น แล้วค่อยๆ อนุญาตเฉพาะที่จำเป็น

- WHO (ใคร)

กลุ่ม Content Editors ต้อง ยืนยันตัวตนด้วย MFA

- WHAT (ทำอะไร)

เข้าถึง WordPress Admin Panel

- WHEN (เมื่อไหร่)

เฉพาะเวลาทำการ 09.00 – 18.00 น.

- WHERE (จากที่ไหน)

เฉพาะ IP ของออฟฟิศ

- WHY (เพื่ออะไร)

เพื่อแก้ไข / จัดการ เนื้อหาเว็บไซต์

- HOW (อย่างไร)

ผ่าน Protocol ที่ปลอดภัย (เช่น HTTPS, VPN, SSH)

Step 5: Monitor and Maintain

- การตรวจสอบอย่างต่อเนื่อง Continuously Monitor ตรวจสอบการรับส่งข้อมูลและ Log ทั้งหมดอย่างต่อเนื่อง
- A Look for Anomalies มองหาการละเมิดนโยบายและพฤติกรรมที่ผิดปกติ
- Anti-fragile System เป้าหมายคือระบบที่พัฒนาขึ้นเมื่อเวลาผ่านไป ไม่ใช่แค่ทนต่อการโจมตี

Quick Wins

1. บังคับใช้ MFA
เพิ่มความปลอดภัยด้วยการยืนยันตัวตนหลายปัจจัย

2. กำหนด Protect Surface ให้ชัดเจน
ระบุว่า “สิ่งที่ต้องปกป้องที่สุด” คืออะไร เช่น ข้อมูลลูกค้า/ระบบหลัก/Admin Panel

3. ตรวจสอบ Log การเข้าถึงอย่างจริงจัง
เฝ้าดูว่าใครเข้ามา/จากที่ไหน/ทำอะไร

คำถามเริ่มต้นสำคัญ

“Protect Surface ของเราคืออะไร?”

แนวคิดหลัก: เริ่มเล็กๆ แต่มีเป้าหมายชัด เมื่อรู้ว่าอะไรสำคัญที่สุด เราจะปกป้องได้ตรงจุดมากขึ้น

คุณเกษมนัส ไม้เรียง
ผู้จัดการส่วนประจำ ฝ่ายผลิตภัณฑ์ความปลอดภัยไซเบอร์
บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน)