23-IP-09-GE-TRC-A

Training Course on Cybersecurity Management Systems

ระหว่างวันที่ 16-19 พฤษภาคม 2566

ผ่านระบบการประชุมออนไลน์

จัดทำโดย อนุชา เกษมวัฒนากุล

วิศวกรอาวุโส สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

วันที่ 12 กรกฎาคม 2566

ส่วนที่ 1 เนื้อหา/องค์ความรู้จากการเข้าร่วมโครงการ

1.1 ที่มาหรือวัตถุประสงค์ของโครงการโดยย่อ

หลักสูตรนี้มีจุดประสงค์เพื่อให้ผู้เข้ารวมโครงการสามารถเข้าใจหลักการ แนวทางของ Cybersecurity Management เพื่อนำไปประยุกใช้ในการวางกลยุทธ์ นโยบาย และใช้เป็นเครื่องมือในการรับมือกับภัยคุกคามที่เกิดขึ้นในปัจจุบัน

ตามรายงานของ McKinsey และ CISCO ที่เผยแพร่ในปี ค.ศ. 2021 และ 2022 นั้น ความเสียหายที่เกิดจาก Cyberattacks นั้นจะขึ้นสูงถึง 10.5 ล้านล้าน USD ต่อปีใน 2025 ซึ่งเป็นสามเท่าของปี 2015 ดังนั้น Cybersecurity จึงเป็นเรื่องที่ไม่อาจมองข้ามได้สำหรับทุกหน่วยงาน โดยเฉพาะจากวิกฤติ COVID-19 ที่ทำให้เกิดความเปลี่ยนแปลงอย่างมากในการทำงาน อย่างการ Remote เข้าทำงานจากภายนอกหน่วยงาน ที่หลายหน่วยงานไม่ยังไม่พร้อมรับมือ และปัจจุบัน Cybercrime นั้นได้ถูกจัดให้เป็นปัญหาระดับโลกอย่างหนึ่งที่เป็นภัยต่อมนุษย์

ดังนั้น Cybersecurity management ที่มีประสิทธิภาพจึงเป็นสิ่งที่ช่วยให้หน่วยงานมีความปลอดภัย

1.2 เนื้อหา/องค์ความรู้ที่ได้จากกิจกรรม

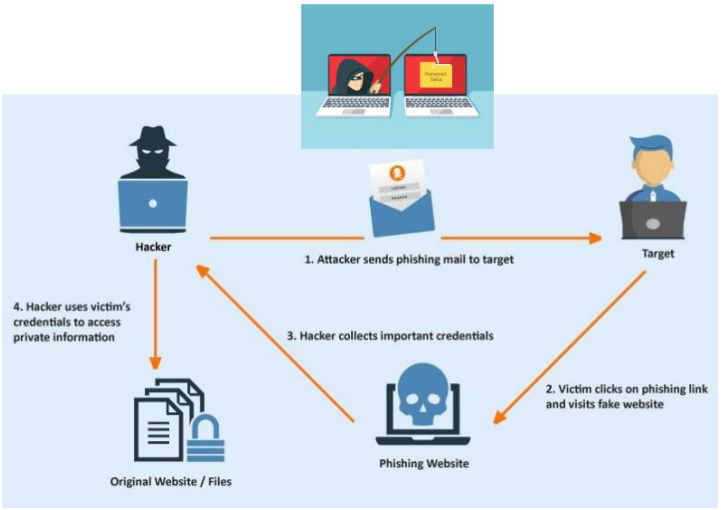
Cybersecurity มีเป้าหมายในการรักษา C : confidential, I: integrity, A: availability ของ ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อุปกรณ์ต่างๆ รวมถึงข้อมูลจาก Cyberattack และลดผลกระทบที่จะเกิดขึ้น

Cyberattack คือ การโจมตีเพื่อเข้าถึง เปลี่ยนแปลง ทำลาย ระบบคอมพิวเตอร์ เครือข่ายคอมพิวเตอร์ อุปกรณ์ต่างๆ รวมถึงข้อมูล ด้วยวิธีการต่างๆ โดยมักทำโดย Hacker, อาชญากรไซเบอร์ หรือ กลุ่มที่ได้รับการสนับสนุนโดยรัฐใดๆ หนุนหลัง โดยมีเป้าหมายตั้งแต่ บุคคล ธุรกิจ หน่วยงานรัฐ หรือโครงสร้างพื้นฐานที่สำคัญ มีผลทำให้ ข้อมูลเสียหาย เกิดความเสียหายทางการเงิน หรือทำลายชื่อเสียง

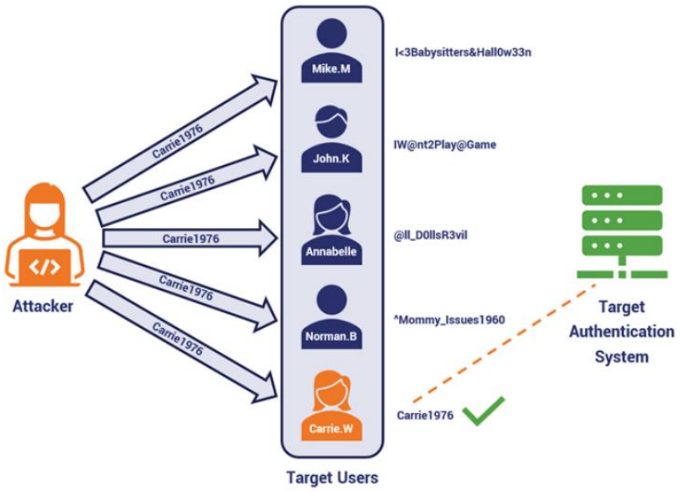
ประเภทของ Cyberattack โดยย่อ

- Malware : ซอฟต์แวร์ไม่พึงประสงค์ เช่น worm, spyware, ransomware, adware, trojan ที่อาจโจมตีผ่านช่องโหว่ต่างๆ, การกด link, การ Download

- Phishing : การโจมตีโดยหลอกเหยื่อให้หลงเชื่อทำสิ่งที่ต้องการ การโจมตีนี้ถูกใช้อย่างแพร่หลาย ถูกจัดอยู่ในกลุ่ม Social Engineering Attack โดยการโจมตีอาจจะมาในรูปแบบ การส่ง email หลอกลวงไปยังเหยื่อ เมื่อเหยื่อกด link ที่พาไปยัง fake website แล้วถูกหลอกใส่ข้อมูลสำคัญ อย่าง credential คนร้ายก็จะได้รับข้อมูลดังกล่าวไปใช้ในการเข้าถึงข้อมูลส่วนตัวอื่นๆ

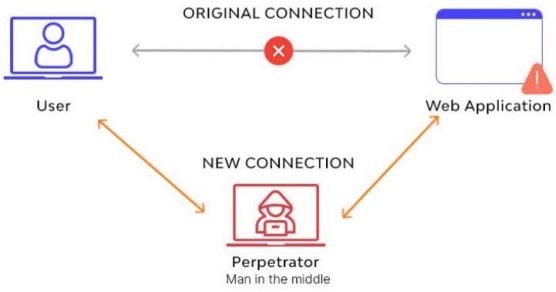


- Password : โจมตีเพื่อให้ได้ password ของเหยื่อด้วยวิธีการต่างๆ เช่น password spraying, Brute force, dictionary, keylogger



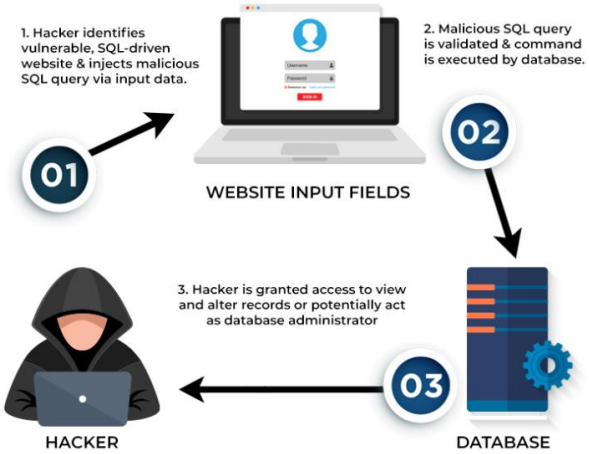
Password Spraying

- Man-in-the-Middle : การขโมยหรือแก้ไขข้อมูลโดยการที่ผู้ไม่ประสงค์ดีแทรกเข้ามาอยู่ระหว่างกลางระหว่างการสื่อสาร



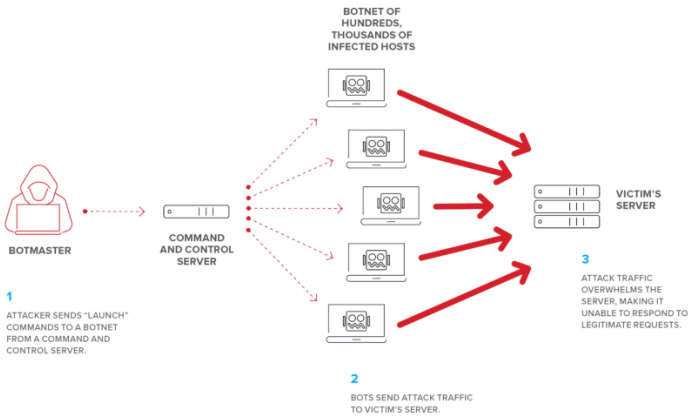
Man-in-the-Middle Attack

- SQL Injection : การส่ง malicious code เข้าไปที่เหยื่อที่มีช่องโหว่เพื่อให้ได้สิ่งต้องการ ไม่ว่าจะเป็นข้อมูล หรือแม้แต่สิทธิระดับ Administrator ของ DB



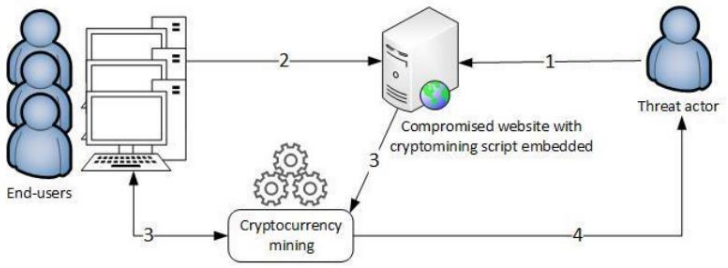
SQL Injection Attack

- Denial-of-Service : การโจมตีเพื่อให้เหยื่อไม่สามารถให้บริการได้ บางกรณีผู้ไม่ประสงค์ดีได้ควบคุม bot จำนวนมากให้ส่ง traffic ปริมาณมหาศาลไปยังเหยื่อจนเหยื่อไม่สามารถให้บริการได้ทันหรือ shutdown ลง (หรือเรียกว่าการทำ DDoS)



- Insider Threat การโจมตีจากคนในด้วยแรงจูงใจต่างๆ

- Crytojacking : การโจมตีเพื่อเข้าใช้ทรัพยากรของเหยื่อในการขุด cryptocurrency

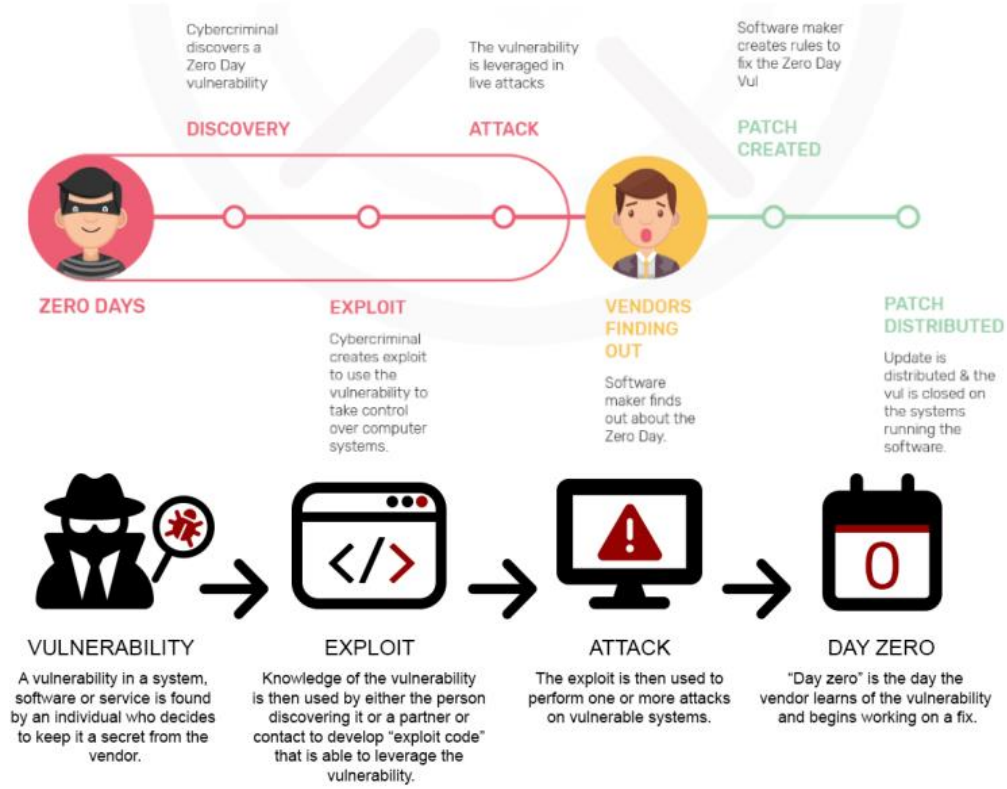


Steps

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

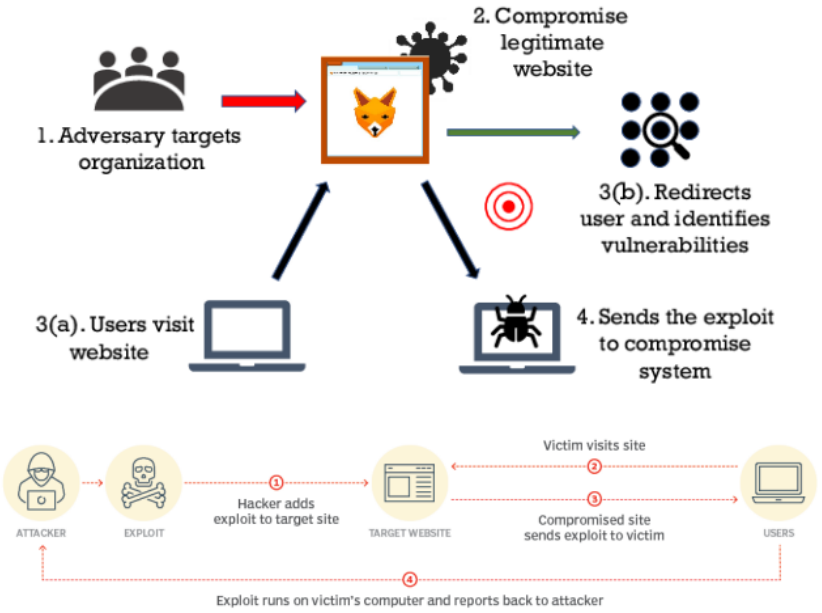
Cryptojacking

- Zero-Day Exploit : การโจมตีไปยังช่องโหว่ที่ยังไม่มีวิธีการแก้ไข



Zero-Day Exploit

- Watering Hole : การโจมตีเว็บที่ได้รับความนิยม เพื่อฝัง code ที่ใช้ในการโจมตีเหยื่อที่เข้าเยี่ยมเว็บดังกล่าวต่อไป



Watering Hole Attack

Cybersecurity threats และ การรับมือ โดยย่อ

- Supply Chain Attack คือการที่ ผู้ไม่ประสงค์ดีเข้าโจมตีผู้ให้บริการ หรือเจ้าของผลิตภัณฑ์ เพื่อโจมตีเหยื่อที่ใช้บริการหรือผลิตภัณฑ์ดังกล่าว การโจมตีนี้สำหรับผู้ใช้งานสามารถรับมือโดยการใช้ endpoint detection and response solution ในการตรวจจับและแก้ไขเหตุการณ์ที่ผิดปกติ
- Internet of Medical things (IoMT) เกิดจากการขาดเข้ารหัสข้อมูลที่ดี, มีการ hard code credential รวมถึงขาดการควบคุมด้าน security ที่ดี การโจมตีนี้รับมือโดยการใช้หลักการ Zero Trust, การแบ่ง segment ที่เหมาะสม รวมถึงกำหนดแนวทางการจัดการอุปกรณ์ต่างๆ และบริหารจัดการช่องโหว่ของ Medical IoT
- Router และ infrastructure security ผู้ไม่ประสงค์ดีโจมตีอุปกรณ์ดังกล่าวแล้วยกระดับสิทธิของตนแล้วเข้าถึง private services/data การโจมตีนี้รับมือโดยใช้ Firewall, penetration testing, network monitoring, VPN, encryption และ การให้ความรู้กับบุคลากร
- Spyware เป็น malware ที่มุ่งเป้าที่ข้อมูลต่างๆ ของเหยื่อ แนวทางป้องกันได้แก่ใช้ anti-malware ที่มีความสามารถป้องกัน spy-ware
- Macro viruses เป็น macro program ไม่ประสงค์ดีที่ฝังลงในไฟล์เอกสาร มีคุณสมบัติที่ตรวจสอบได้ยาก มักแพร่ผ่าน e-mail หรือ link ต่างๆ แนวทางป้องกัน ใช้ Anti-malware ที่สามารถตรวจจับการ download file หรือ เปิด link ไม่ปลอดภัยได้, มีการ update OS. เป็นประจำ และไม่เปิดไฟล์จาก email หรือ link ที่น่าสงสัย รวมถึงไม่ click pop-ups
- Command and control หรือ C&C เป็นการโจมตีที่ผู้ไม่ประสงค์ดีสามารถส่งคำสั่งควบคุมเหยื่อให้ทำตามได้ รวมทั้งส่งข้อมูลหรือผลการโจมตีกลับทางช่องทางที่สร้างไว้ แนวการรับมือ ใช้

Intrusion detection system (IDS), Intrusion Prevention system (IPS), Firewall หรืออื่นๆ ที่สามรถป้องกันการ run app หรือ code ได้, ใช้ 2-Factor authentication และ digital code signing

Cyber security ที่มีต่ออุตสาหกรรมแต่ละประเภท

ภัยต่อ SME ได้แก่

1) Phishing Attack เป็นภัยที่มีการขยายตัวถึง 65% เมื่อเทียบกับปี 2022
2) Malware Attack
3) Ransomware
4) Weak passwords จากสถิติพบว่าเฉลี่ยแต่ละองค์กรมีผู้ใช้ password อ่อนแออยู่ถึง 19%

ภัยต่อคมนาคมทางราง

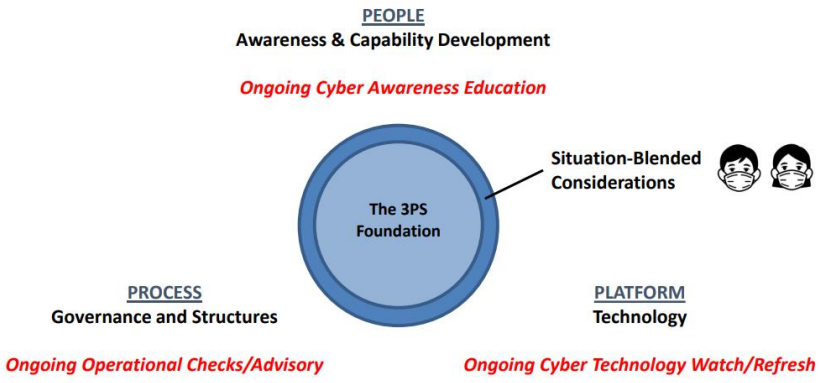
1) ปริมาณ IoT ที่เชื่อมกับระบบที่สูงทำให้มีช่องโหว่ให้ถูกโจมตีมากขึ้น
2) การส่งสัญญาณควบคุมผ่านระบบไร้สายที่ใช้ protocol ที่ไม่ปลอดภัย
3) ransomware
4) การโจมตีทางกายภาพต่ออุปกรณ์ต่างๆ

ภัยต่อ Smart City เช่น IoT ถูกเข้าควบคุม ผ่านช่องโหว่ต่างๆ หรือ password ที่ถูกใช้ซ้ำกัน นำไปสู่การถูกสอดแนม รวมถึงควบคุมอุปกรณ์อื่นๆ ที่อาจเข้าถึงได้ต่อไป

ภัยต่อ Healthcare ได้แก่ ransomware ที่เพิ่มมากขึ้นกระทบต่อการให้บริการ

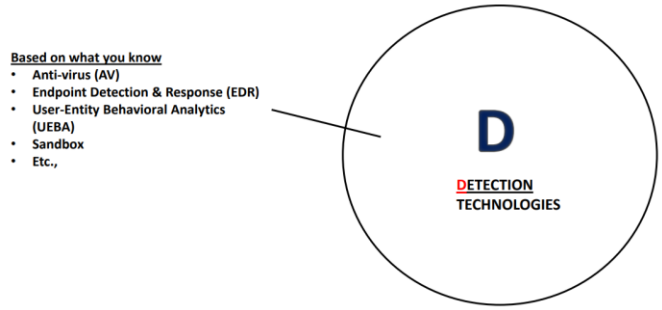
แนวทางการรับมือภัย Cyber จะตั้งอยู่บนพื้นฐาน 3 สิ่งคือ

1) People ต้องได้รับคำแนะนำให้ระแวดระวังและพัฒนาความสามารถ
2) Process มีกรอบให้ปฏิบัติที่ดี
3) Platform ตัว technology ที่นำมาใช้ต้องดูแลให้ปลอดภัย

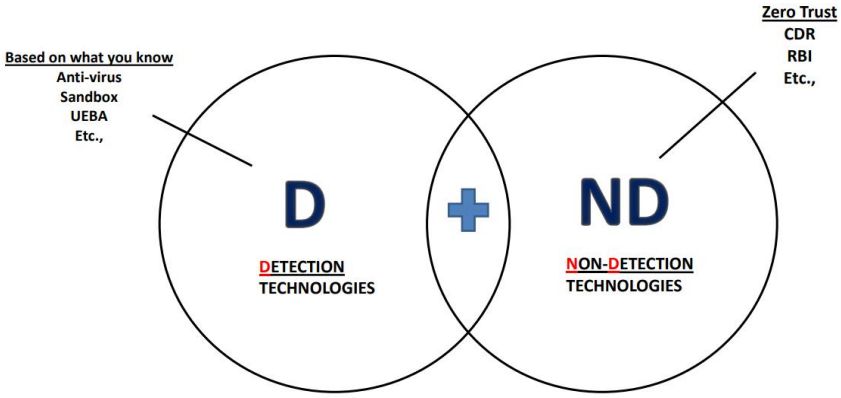


ช่องโหว่ของการป้องกันในปัจจุบันและการอุดช่องโหว่

การป้องกันในปัจจุบันอยู่บนพื้นฐานของการตรวจจับ (Detection) สิ่งที่รู้ว่าเป็นภัย ซึ่งเท่ากับว่าการตรวจไม่พบไม่ได้แปลว่าไม่มีภัยนั้นอยู่จริง อย่างเช่น Anti-virus, Endpoint Protection, Endpoint Detection, User & Entity Behavior Analytics (UEBA) Sandbox ทั่ว ๆ ไปนั้นที่ทำงานด้วยการตรวจจับ definition หรือ พฤติกรรมอันตราย หรือ พฤติกรรมที่ผิดปกติ ซึ่งผู้ไม่ประสงค์ดีย่อมหาทางหลบหลีกกระบวนการตรวจจับด้วยวิธีการต่างๆ ไม่ว่าจะ ใส่ password กับ file zipped , ใช้ Zero-day โจมตี ซึ่งอาจรวมถึงการใช้ AI เข้าช่วยอีกด้วย

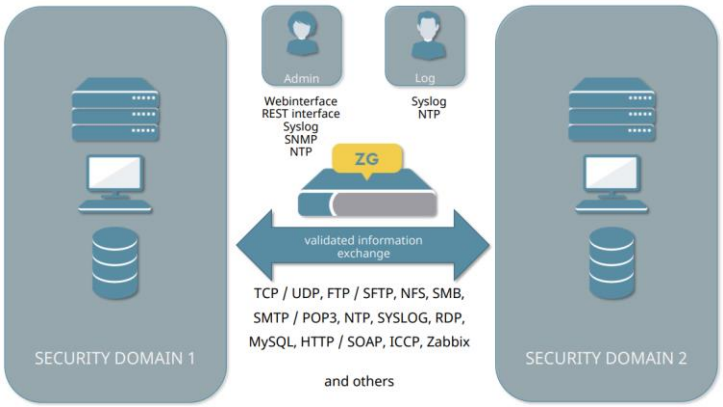


การอุดช่องโหว่นั้นทำได้โดยนำ Zero-Trust เข้ามาใช้ ซึ่ง Zero-trust คือ การที่ต้องตรวจสอบทุกสิ่งให้แน่ใจว่าปลอดภัยก่อนเสมอ ซึ่งเครื่องมือที่ยกตัวอย่างในโครงการอบรมนี้ได้แก่



1) Remote Browsing Isolation (BRI) ที่การท่องเว็บ หรือบริการผ่าน Browser ใดๆ จะทำผ่าน virtual container บน cloud ซึ่งจะป้องกันผู้ใช้จากการถูกโจมตีโดยตรง

2) Content Disarm & Reconstruction (CDR) สำหรับ file จะเป็นการตัดส่วนที่ไม่เกี่ยวข้องหรือเป็นอันตรายออกจาก file ก่อนที่จะถึงผู้ใช้ แต่สำหรับ Network จะเป็นการทำ white-listing ที่จะ reconstruct packet มาตรวจสอบก่อนส่งผ่านไป

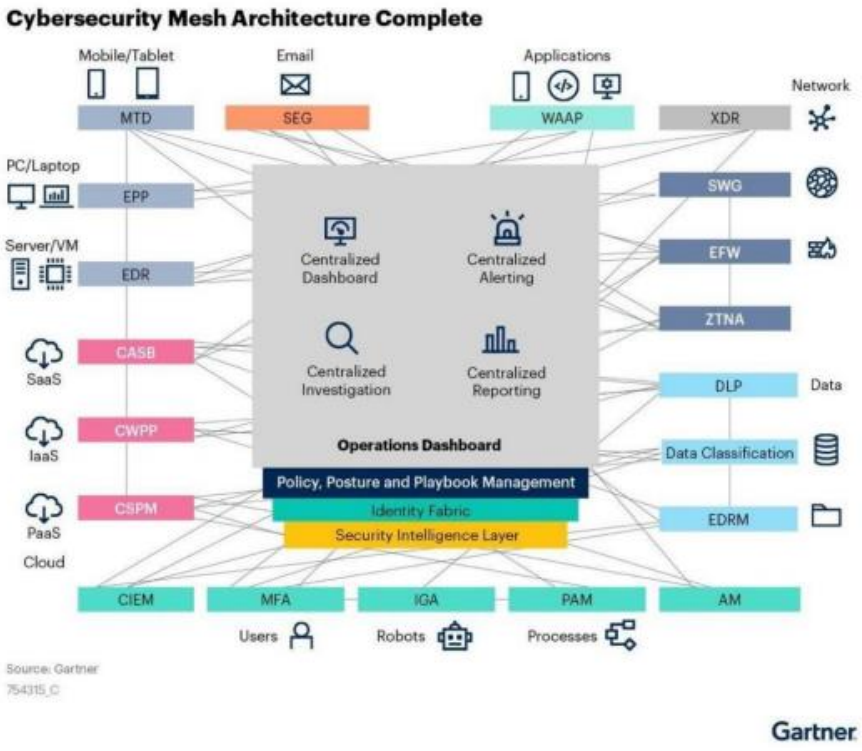


3) Robotic VAPT ทำการ ตรวจสอบช่องโหว่ทั้ง Vulnerability assessment และ penetration test โดยอัตโนมัติอย่างสม่ำเสมอ

Cybersecurity สำหรับ Cloud เช่นเดียวกับ onsite แต่เพิ่มความซับซ้อนมากกว่าเนื่องจากช่องทางการเข้าใช้ที่เปลี่ยน รวมถึงโครงสร้างหลายส่วนที่ไม่สามารถควบคุมได้ด้วยตัวเอง ทำให้ต้องใช้แนวคิด Zero-trust เข้ามาช่วยด้วยเช่นกัน เพื่อให้องค์กรสามารถดำเนินกิจกรรมหลักได้ต่อไป นอกจากนั้นสิ่งเหล่านี้ยังเป็นสิ่งที่ต้องให้ความสำคัญสำหรับการใช้ Cloud คือ network ต้องสามารถใช้งานได้เสมอ มีการป้องกัน มีการตรวจจับ มีการจำกัดความเสียหาย หรือสามารถกู้กลับมาได้ทันท่วงที

Cybersecurity Mesh Architecture (CSMA) คือ แนวคิดที่เชื่อมโยงสอดประสานเครื่องมือควบคุมความปลอดภัยต่างๆ เข้าด้วยกันให้มีความยืดหยุ่น ทำให้มีความปลอดภัยยิ่งขึ้นและใช้ทรัพยากรน้อยลง โดยมีคุณสมบัติดังนี้

1) security analytic และ Intelligence
2) Identity และ access management
3) ควบคุม policy ให้กับอุปกรณ์ต่างๆ ได้
4) Dashboard ที่รวมข้อมูลเข้าด้วยกันทำให้ตรวจสอบและตอบสนองได้ทัน



ข้อดีของ CSMA คือ

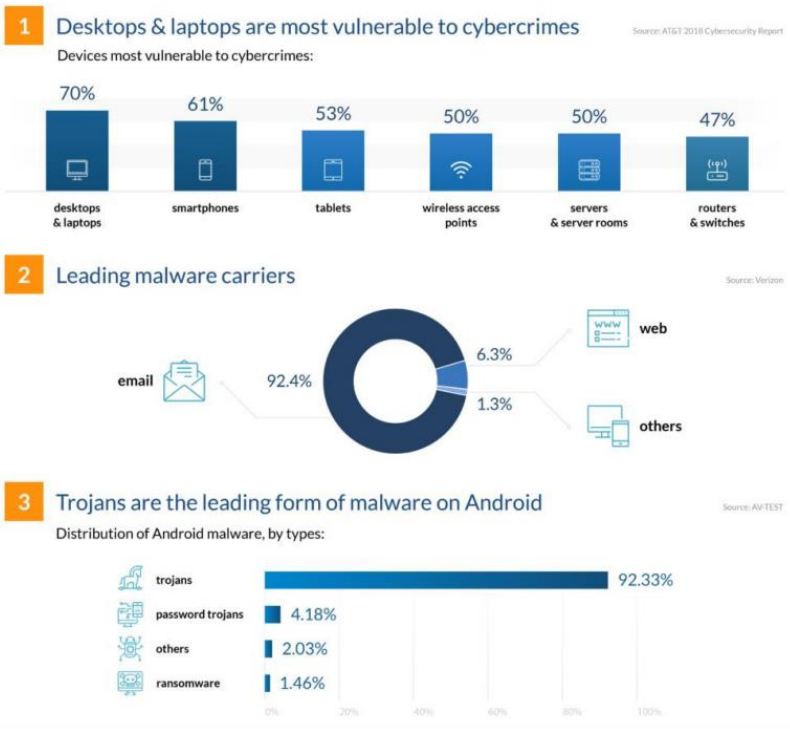
1) รองรับ Identity and Access Management (IAM)
2) การเชื่อมโยงสื่อสารระหว่าง third-party services ทำได้ง่าย ทำให้แต่ละเครื่องมือทำงานร่วมกันได้ดี
3) ง่ายในการจัดทำระบบตรวจสอบตัวตนในอนาคต
4) รองรับ Decentralized Identity standards ทำให้ identity data ได้รับการดูแล
5) การติดตั้งและจัดการ security tools ใหม่ทำได้ง่ายและยืดหยุ่น

คำแนะนำสำหรับการ Balancing ระหว่าง Cybersecurity และ Productivity ว่าเครื่องมือ หรือ policy ด้าน cybersecurity ใดที่ก่อให้ให้เกิดคอขวดต่อ productivity มากให้พิจารณาที่นั่นก่อน รวมทั้งหาเครื่องมือที่เหมาะสมที่ให้ทั้งความปลอดภัยและสร้างสรรค์งานดีได้

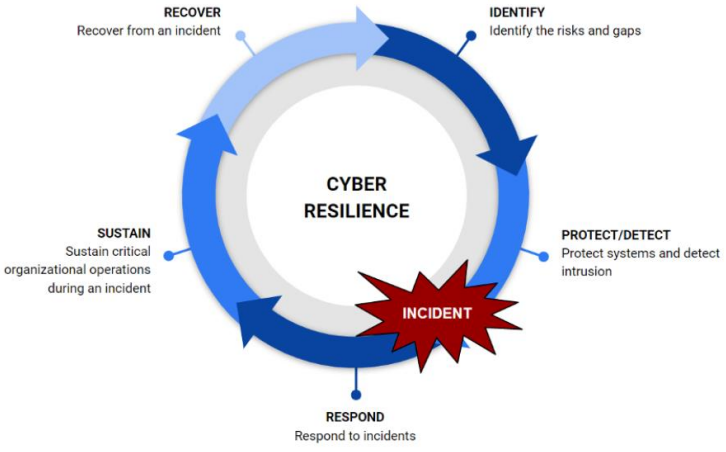
พัฒนาการของ Cyberattack และ solution

Cyberattack	Solution
Gen.1 Virus	Anti-virus
Gen.2 Network	Firewall, IDS
Gen.3 Application	IPS
Gen.4 Payload	Anti-bot and sandboxing products
Gen.5 Mega	Real Time Threat intelligence

สถิติด้าน Cyberattack



Cyber Resilience คือ แนวคิดที่จะให้องค์กรสามารถอยู่รอดได้

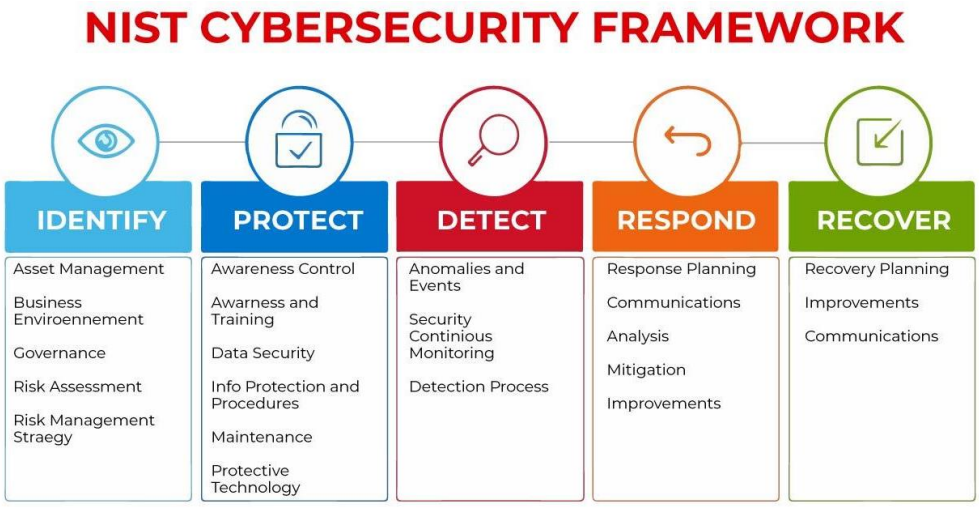


The 5 stages of cyber resilience can be adopted by any public sector organization seeking to protect themselves from cyber attacks.

1) Identify risk และ gap ที่มี
2) Protect / Detect จากการบุกรุก
3) Respond ตอบสนองต่อ incident ที่เกิดขึ้น
4) Sustain งานหรือสิ่งสำคัญขององค์กรต้องยังทำงานได้ในระหว่างเกิด incident
5) Recover กู้คืนจาก incident

NIST : Cybersecurity Framework (CSF)

1) Identify
2) Protect
3) Detect
4) Respond
5) Recover



ISO 27001 : เป็นมาตรฐานที่เป็นที่อย่างกว้างขวาง โดยมีกระบวนการ PDCA ประกอบด้วย

Plan

1) Objective
2) Scope
3) Asset inventory
4) Risk management framework
5) Identify risks และกำหนด scope
6) Define risk treatment plans
7) Validate controls – Annex A
8) Write document

Do

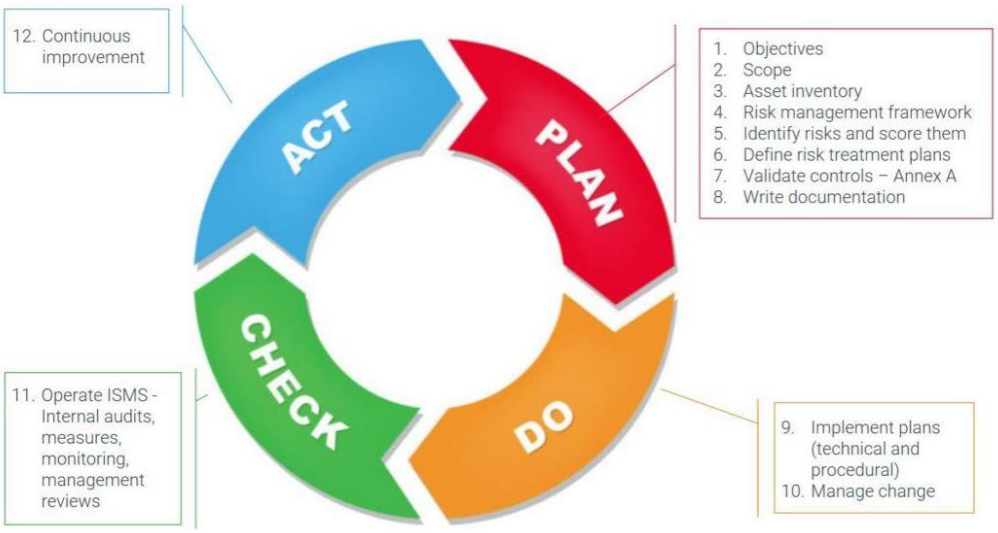
9) Implement plans
10) Manage change

Check

11) Operate ISMS internal audit, monitor และ management review

ACK

12) Continuous improvement



จากทั้ง 2 แนวทางข้างต้นมีความเป็นไปได้ในการนำมาประยุกต์ใช้ และจะได้ผลลัพธ์ที่ดีจากการนำทั้ง CFS และ ISO 27001 มาใช้ร่วมกัน

Digital Policy นั้นใช้ทั้งเพื่อควบคุมเพื่อให้ได้ผลตามเป้าหมาย เช่น การแข่งขันที่ยุติธรรม ประชาชนได้ประโยชน์ หรือ สร้างส่งเสริมให้เกิด หรือพัฒนาบางสิ่งเพื่อผลลัพธ์ที่ดี เช่น ในประเทศเกาหลีของผู้บรรยายได้มีการจัดทำ Cybersecurity Policy for Digital Transformation ที่ช่วยตอบสนองในด้านต่างๆ เช่น

ยกระดับความปลอดภัยให้ทันสมัย

1) สร้างความร่วมมือระหว่าง Public-private ในการตอบสนองภัย
2) สร้างการสนับสนุนให้กับ SME เช่น ให้คำแนะนำ และบริการรักษาความปลอดภัยข้อมูล
3) สนับสนุนให้ประชาชนรับมือกับภัยไซเบอร์ เช่น บริการ My PC care service, checklist ความปลอดภัย

Cybersecurity ด้าน R&D มีการลงงบประมาณในส่วนต่างๆ เพื่อสนับสนุน R&D เช่น

1) Data Protection
2) Physical security
3) Network protection
4) Convergence security (การใช้ชีวิตและสุขภาพ)
5) Convergence service protection (บริการ เช่น web, mail, blockchain หรือ e-transaction)
6) International joint research

และยังมีด้านอื่นๆ เช่น สร้างความปลอดภัยสำหรับการให้บริการที่ไม่ต้องมาแสดงตัวด้วยตัวเอง การสร้างแรงงานที่มีความสามารถ สร้างเครือข่ายความร่วมมือระหว่างประเทศ ผ่านการให้ความรู้

ตัวอย่างการสร้างคนใน ประเทศเกาหลี

ประเทศเกาหลี นั้นมีการสร้างทั้งคนให้มีความสามารถด้านนี้จากสถาบันการศึกษาเอง การให้การสนับสนุนเพิ่มแก่สถานศึกษา และผ่านโปรแกรมเฉพาะทางอื่นๆ รวมทั้งสร้างใบรับรองงานด้าน cybersecurity แขนงต่างๆ ภายในประเทศ เพิ่มเติม นอกจากที่สนับสนุนให้ได้รับใบรับรองจากสากล

ข้อมูลเบื้องต้นเกี่ยวกับ Cybersecurity Certifications

1) ISC^2 เป็นองค์กรที่ตั้งขึ้นปี 1989 ไม่แสวงหาผลกำไร มีกิจกรรมให้ความรู้ และใบรับรองสำหรับผู้ทำงานด้าน IT โดยมีใบรับรองหลายรายการ เช่น
    - CISSP
    - SSCP
    - CCSP
    - CAP
    - CSSLP
    - HCISPP

    โดยที่กำลังเป็นที่นิยมได้แก่ CISSP และ CCSP

    CISSP : Certified Information Systems Security Professional เป็นใบรับรองที่เน้นด้าน Information Technology Security, Cybersecurity โดยครอบคลุมความรู้ดังต่อไปนี้
    - Security and Risk Management
    - Asset Security
    - Security Architecture and Engineering
    - Communication and Network Security
    - Identity and Access Management (IAM)
    - Security Assessment and Testing
    - Security Operations
    - Software Development Security

    CCSP : Certified Cloud Security Professional เป็นใบรับรองที่เน้น Secure cloud infrastructure โดยครอบคลุมความรู้ดังต่อไปนี้
    - Cloud Concepts, Architecture and Design
    - Cloud Data Security
    - Cloud Platform and infrastructure Security
    - Cloud Application Security
    - Cloud Security Operations
    - Legal, Risk and Compliance

ความแตกต่างระหว่าง CISSP กับ CCSP

CISSP เหมาะกับสายงานบริหาร เช่น

- Chief Information Security Officer
- Director of Security
- Chief Information Officer
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Consultant
- Security Auditor
- Security Manager
- Security Architect
- Network Architect

CCSP เหมาะกับสายงาน Technical

- Enterprise Architect
- Security Administrator
- Security Architect
- Systems Engineer
- Security Manager
- Security Consultant
- Security Engineer
- Systems Architect

2) CompTIA เป็นองค์กรให้ความรู้ และใบรับรองเช่นกันมีใบรับรองหลายรายการ เช่น
    a. Security+
    b. CySA+
    c. CASP

ส่วนที่ 2 ประโยชน์ที่ได้รับและการขยายผลจากการเข้าร่วมโครงการ

- ประโยชน์ต่อตนเอง : ได้รับความรู้เกี่ยวกับการโจมตีรูปแบบต่างๆ พร้อมวิธีการรับมือ ตั้งแต่ก่อนเกิดเหตุ ระหว่างเกิดเหตุ และหลังเกิดเหตุ อีกทั้งการแชร์ประสบการณ์จากผู้บรรยาย ที่สามารถนำถ่ายทอดให้ผู้ร่วมงานและทีมที่เกี่ยวข้อง
- ประโยชน์ต่อหน่วยงานต้นสังกัด : นำความรู้ที่ได้มาวางแผนรับมือตั้งแต่ก่อนเกิดเหตุ ระหว่างเกิดเหตุ และหลังเกิดเหตุได้
- ประโยชน์ต่อสายงานหรือวงการวิชาชีพในหัวข้อนั้นๆ : สามารถนำความรู้ที่ได้มาถ่ายทอดต่อไป ทำให้เกิดความปลอดภัยผู้ที่เกี่ยวข้อง
- กิจกรรมการขยายผลที่ได้ดำเนินการภายในระยะเวลา 60 วันนับจากวันสุดท้ายของโครงการ : นำความรู้ที่ได้มาใช้ในการบรรยายสร้างความตระหนักให้กับพนักงานในองค์กร
- กิจกรรมการขยายผลที่จะดำเนินการภายใน 6 เดือนหลังเข้าร่วมโครงการ : นำความรู้ที่ได้มานำเสนอในการปรับปรุงงานด้านต่างๆ เช่น ISMS

ส่วนที่ 3 เอกสารแนบ

- รายชื่อผู้เข้าร่วมโครงการและประเทศที่เข้าร่วมโครงการ
- กำหนดการฉบับล่าสุด (Program)
- เอกสารประกอบการประชุม/สัมมนา (Training Materials)
