รายงานการเข้าร่วมโครงการเอพีโอ
23-IP-09-GE-TRC-A
ระหว่างวันที่ 16-19 พฤษภาคม 2566
ผ่านระบบการประชุมออนไลน์
จัดทำโดยนางสาวณัฐวดี โพธิ์กะสังข์
นักวิชาการคอมพิวเตอร์ชำนาญการ สำนักงานเศรษฐกิจอุตสาหกรรม
กระทรวงอุตสาหกรรม
วันที่ 22 มิถุนายน พ.ศ. 2566

ส่วนที่1 เนื้อหา/องค์ความรู้จากการเข้าร่วมโครงการ

1.1 ที่มาและวัตถุประสงค์ของโครงการ

เทคโนโลยีสารสนเทศและเครือข่าย internet มีความก้าวหน้าเป็นอย่างมากโดยปัจจุบันได้มีการนำเทคโนโลยีสารสนเทศเหล่านี้มาประยุกต์ใช้ประโยชน์เป็นจำนวนมากและมีแนวโน้มการใช้งานเพิ่มขึ้นอย่างต่อเนื่องสอดคล้องกับจำนวนผู้ใช้อินเทอร์เน็ตที่เพิ่มขึ้น ในปัจจุบันโลกของ internet มีการเชื่อมต่อเข้าด้วยกันเป็นโครงข่ายและมีความซับซ้อนอย่างมาก ซึ่งส่งผลให้มีผู้ไม่ประสงค์ดีหรือ hacker พยายามหาช่องทางในการเข้าถึงข้อมูลของผู้อื่นเพื่อนำข้อมูลเหล่านั้นไปแสวงหาประโยชน์ส่วนตน หรือการหลอกลวงเพื่อลักทรัพย์ต่าง ๆ

การโจมตีทางไซเบอร์ทำให้เกิดการสูญเสียอย่างมากมายทั้งทางด้านการเงิน ทางกฎหมายรวมถึงมีการละเมิดข้อมูลส่วนตัวและก่อให้เกิดความเสียหายต่อชื่อเสียงของบุคคลและหน่วยงาน ดังนั้น จึงเป็นเรื่องยากสำหรับการบริหารจัดการด้าน Cyber Security ในรูปแบบดังเดิมที่ไม่สามารถตอบสนองต่อเหตุการณ์การโจมตีที่ซับซ้อนที่อาจเกิดขึ้นในอนาคต

หลักสูตรนี้ เป็นโครงการสำหรับการบริหารจัดการ Cyber Security สำหรับเจ้าหน้าที่หน่วยงานของรัฐเพื่อรับมือกับการโจมตีทาง Cyber ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น รวมถึงเพื่อแนะนำแนวคิดหลักและแนวโน้มในการบริหารจัดการรักษาความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น อีกทั้งจะช่วยให้ผู้เข้าร่วมอบรมได้เรียนรู้กลยุทธ์ นโยบาย และเครื่องมือทาง Cyber Security พร้อมทั้งช่วยให้สามารถใช้เครื่องมือดังกล่าวได้อย่างสอดคล้องกัน และเพื่อเป็นการหารือเกี่ยวกับมาตรฐานและ certification programs เพื่อเสริมสร้างประสิทธิภาพด้าน Cyber Security ในการบริหารจัดการในระดับองค์กร

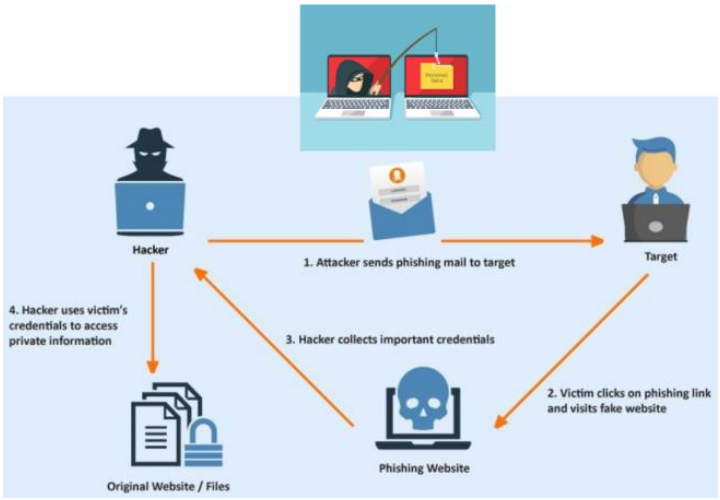
1.2 เนื้อหา/องค์ความรู้ที่ได้รับ

1.2.1 ความรู้ด้านการโจมตีทางไซเบอร์

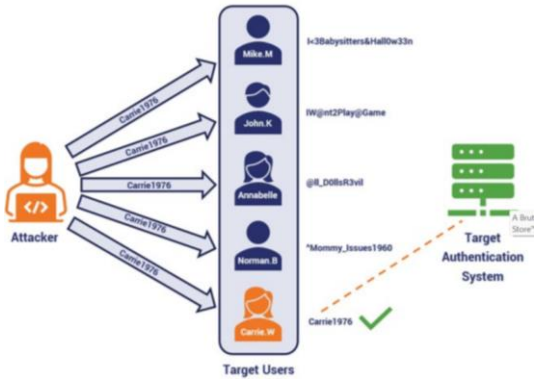
Cyberattack คือ การโจมตีทางไซเบอร์ โดยหมายถึงการที่ hacker พยายามรบกวนหรือทำให้ระบบคอมพิวเตอร์ เครือข่ายหรืออุปกรณ์อิเล็กทรอนิกส์มีปัญหาในการใช้งานหรือมีความผิดปกติหรือการขโมยข้อมูลที่ละเอียดอ่อน เช่น ข้อมูลส่วนตัวของบุคคล ข้อมูลทางการเงิน ข้อมูลการรักษาพยาบาล ข้อมูลขององค์กรหรือทรัพย์สินทางปัญญา หรือก่อกวนบริการที่สำคัญ ส่งผลให้สูญเสียข้อมูล สูญเสียทางการเงิน สูญเสียทางธุรกิจและความเสียหายต่อชื่อเสียง โดยใช้เทคนิคและวิธีการต่างๆ โดยมีตัวอย่างเป้าหมายการโจมตี ดังนี้ บุคคล ธุรกิจ รัฐบาล หน่วยงานหรือโครงสร้างพื้นฐานที่สำคัญ ชนิดของ Cyberattacks ประกอบด้วย 10 ชนิด ดังนี้

1. Malware Attack หมายถึงซอฟต์แวร์ที่เป็นอันตราย รวมถึงไวรัส เวิร์ม สปายแวร์ แรนซัมแวร์ แอดแวร์ และโทรจัน เป็นต้น โดยไวรัสโทรจันสามารถปลอมตัวเป็นไวรัส โดยซอฟต์แวร์ Ransomware อาจบล็อกการเข้าถึงระบบหลักของเครือข่าย แต่สปายแวร์คือซอฟต์แวร์ที่ขโมยข้อมูลลับทั้งหมดโดยที่ผู้ใช้งานไม่รู้ตัว ซึ่งมัลแวร์เจาะระบบเครือข่ายผ่านช่องโหว่ เมื่อมีผู้ใช้คลิกที่ลิงค์ที่อันตรายจากนั้นจะดาวน์โหลดไฟล์แนบจากอีเมลหรือเมื่อใช้ Flash Drive ที่ติดไวรัส

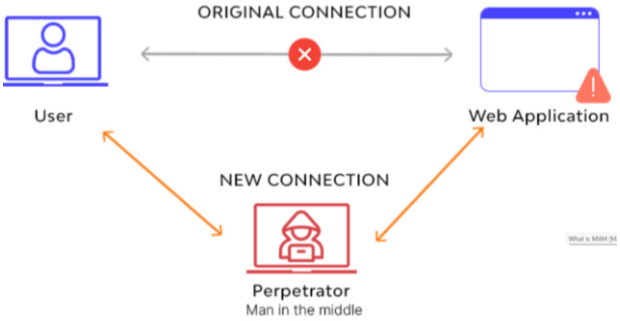
2. Phishing Attack การโจมตีแบบฟิชชิ่งเป็นหนึ่งในการโจมตีที่โดดเด่นที่สุดประเภทหนึ่งจากการโจมตีทางไซเบอร์ที่แพร่หลาย ซึ่ง Phishing Attack เป็นประเภทการโจมตีทาง social media ซึ่งผู้โจมตีจะปลอมตัวเป็นผู้ติดต่อที่เชื่อถือได้และส่งเมล์ปลอมให้กับเหยื่อ เมื่อเหยื่อเปิดเมล์และคลิกที่ลิงค์ที่เป็นอันตรายหรือเปิดจดหมายสิ่งที่แนบมา ผู้โจมตีจะสามารถเข้าถึงข้อมูลลับและข้อมูลของบัญชีนั้น ๆ ได้ นอกจากนี้ยังสามารถติดตั้งมัลแวร์ผ่านฟิชชิงได้อีกด้วย



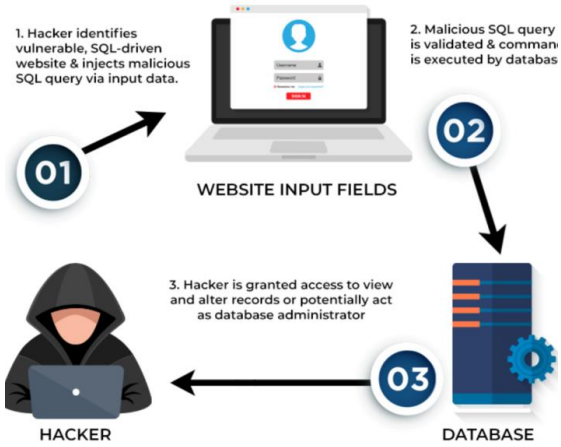
3. Password Attack เป็นรูปแบบหนึ่งของการโจมตีโดย Hacker จะถอดรหัสรหัสผ่านของผู้ใช้งานด้วยวิธีที่หลากหลายด้วยโปรแกรมและเครื่องมือ crack รหัสผ่าน เช่น Aircrack, Cain, Abel, John the Ripper, Hashcat และ อื่น ๆ การโจมตีด้วยรหัสผ่านมีหลายประเภท เช่น Password Spraying, brute force attacks, dictionary attacks, and keylogger attacks เป็นต้น



4) Man-in- the Middle Attack (MITM) คือการดักฟังการโจมตีโดยในการโจมตีผู้โจมตีจะเข้ามาระหว่างการสื่อสารของสองฝ่าย กล่าวคือ ผู้โจมตีทำการโจมตีเซสชันระหว่างไคลเอ็นต์และโฮสต์ โดย Hacker จะขโมยและจัดการข้อมูล โดยตัดหรือปิดการสื่อสารระหว่างไคลเอนต์กับเซิร์ฟเวอร์ในช่องทางปกติ และสายสื่อสารจะถูกแทนที่ด้วย Hacker ซึ่งจะทำให้ Hacker สามารถดังจับข้อมูลทุกอย่างของผู้ใช้งานได้โดยที่ผู้ใช้งานไม่รู้ตัว

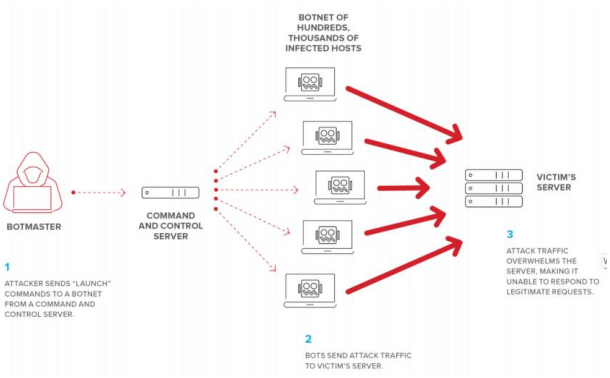


5. SQL Injection Attack การโจมตีนี้เกิดขึ้นบนเว็บไซต์ที่ขับเคลื่อนด้วยฐานข้อมูล กล่าวคือเมื่อ Hacker จัดการ standard SQL query Hacker จะดำเนินการโดยการส่ง malicious code ไปในช่องโหว่หรือช่องค้นหาเว็บไซต์ เช่น website search box ที่มีช่องโหว่จึงทำให้เซิร์ฟเวอร์เปิดเผยข้อมูลสำคัญให้กับ Hacker

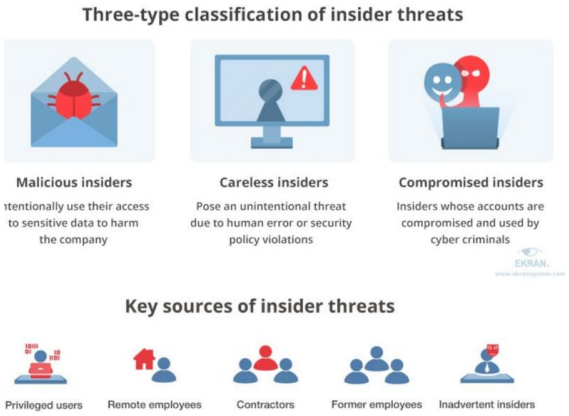


6. Denial-of-Service Attack เป็นภัยคุกคามที่สำคัญโดยผู้โจมตีจะกำหนดเป้าหมายของระบบที่จะโจมตี เช่น เซิร์ฟเวอร์ หรือเครือข่าย และจะโจมตีโดยทำให้ทรัพยากรและแบนด์วิธใช้งานได้อย่างไม่มี

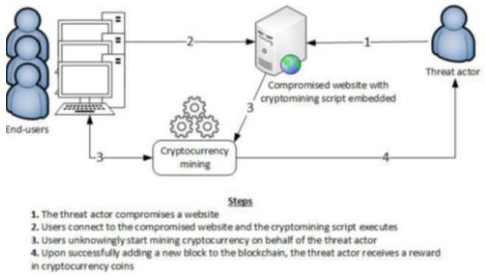
ประสิทธิภาพ เช่น มีการส่งคำขอเข้าใช้งานเซิร์ฟเวอร์เป็นจำนวนมากส่งผลให้เว็บไซต์ที่เป็นโฮสต์ Down หรือช้าลง หรือระบบไม่สามารถใช้งานได้



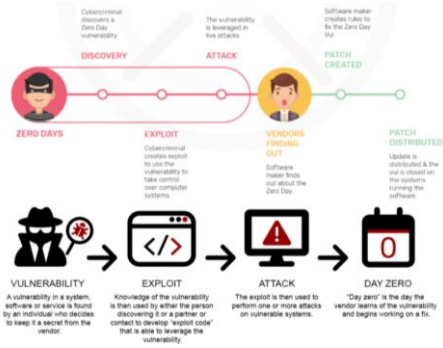
7. Insider Treat เป็นเป็นภัยคุกคามจากภายใน เช่น บุคคลจากภายในองค์กรที่รู้ทุกอย่างเกี่ยวกับองค์กรซึ่งเป็นประเภทการโจมตีที่มีโอกาสที่จะก่อให้เกิดความเสียหายอย่างมาก ส่วนใหญ่การโจมตีนี้พบในธุรกิจขนาดเล็ก เช่น พนักงานมีการเข้าถึงข้อมูลได้หลายบัญชี



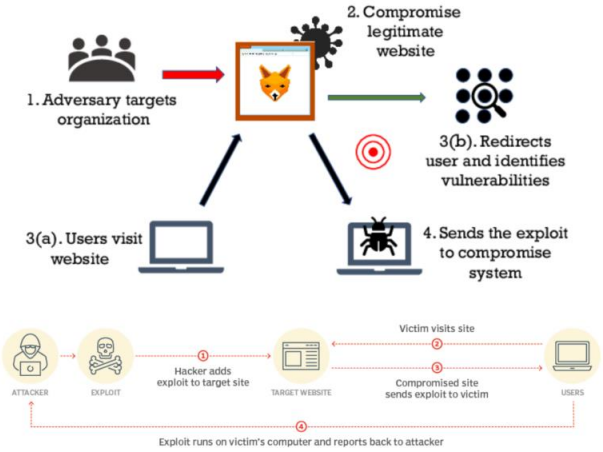
8. Cryptojacking เป็นภัยคุกคามที่มีความเกี่ยวข้องอย่างมากเกี่ยวกับสกุลเงินดิจิทัล Cryptojacking เกิดขึ้นเมื่อผู้โจมตีเข้าถึงคอมพิวเตอร์ของผู้อื่นโดยการเข้าถึงนั้นได้มาจากการเผยแพร่เว็บไซต์หรือหลอกล่อเหยื่อให้คลิกลิงก์อันตรายผู้โจมตียังใช้โฆษณาออนไลน์ด้วยรหัส JavaScript โดยผู้ที่ตกเป็นเหยื่อไม่ทราบว่าสิ่งนี้เป็นการขุด Crypto Currency



9. Zero-Day Exploit เกิดขึ้นหลังจากมีช่องโหว่ในเครือข่าย ส่วนใหญ่ไม่มีวิธีแก้ไขสำหรับช่องโหว่ในกรณีนี้ ดังนั้นผู้ขายจึงแจ้งช่องโหว่ดังกล่าวให้ผู้ใช้งานทราบผู้ขายหรือผู้พัฒนาระบบจะต้องใช้ระยะเวลาในการแก้ไขปัญหา ในขณะเดียวกัน ผู้โจมตีกำหนดเป้าหมายในการโจมตีช่องโหว่ และพวกเขาแน่ใจว่าจะสามารถโจมตีจากช่องโหว่เหล่านี้ได้ก่อนที่จะมีแพตช์หรือโซลูชั่นมาปิดช่องโหว่เหล่านี้



10. Watering Hole Attack ผู้โจมตีกำหนดเป้าหมายเว็บไซต์ที่มีการใช้งานความถี่จำนวนมาก หรือสุ่มโจมตีจากกลุ่มเป้าหมาย หรือสุ่มโจมตีโดยการคาดเดา โดยผู้โจมตีจะทำให้เว็บไซต์เหล่านี้ติดมัลแวร์และทำให้ระบบมีปัญหา ซึ่งมัลแวร์ในการโจมตีดังกล่าวมีเป้าหมายที่ผู้ใช้ เช่น ข้อมูลส่วนบุคคล โดย Hacker จะ remote ไปยังเครื่องที่ถูก hack เพื่อควบคุมเครื่อง



ความมั่นคงปลอดภัยสำหรับ Supply Chain

มีการตรวจสอบระบบภายในด้วยการทดสอบเพิ่มเหตุการณ์โจมตีโดยใช้ช่องโหว่ของ Supply Chain เพื่อหาวิธีในการปิดช่องโหว่ดังกล่าวและมีมาตรการเชิงรุกเพื่อป้องกันการโจมตี Supply Chain เป็นการเพิ่มความปลอดภัยทางไซเบอร์ตามแนวทางของสหรัฐอเมริกาเพื่อความแข็งแกร่งโดยเน้นความร่วมมือระหว่างกันขององค์กรเพื่อปกป้องโครงสร้างพื้นฐานที่สำคัญ และยังเป็นการรักษาความปลอดภัยของ Supply Chain ที่มีความครอบคลุมมากขึ้นในแง่ของการดูแลความปลอดภัยจากการโจมตีทางไซเบอร์ตลอดทั้งกระบวนการ supply chain

การโจมตี Supply Chain มี Attact Classification คือ Initial Access ซึ่งจะใช้กระบวนการที่ซับซ้อนและแนบเนียนเพื่อให้สามารถเข้าถึงข้อมูลขององค์กรโดยกำหนดเป้าหมายเป็นซอฟต์แวร์ที่มีการจ้างพัฒนาอาจมีการฝังโค้ดหรืออัพเดตบางอย่างเพื่อให้ตรวจสอบได้ยาก โดยโจมตีที่ช่องโหว่ของระบบ จากนั้นส่งมัลแวร์ไปยังเครือข่ายของผู้ใช้งานจากนั้นผู้ใช้งานสามารถถูกเจาะผ่านการอัปเดตของซอฟต์แวร์หรือแอปพลิเคชั่น

วิธีป้องกันการโจมตี Supply Chain

- เขียนโปรแกรมอย่างรัดกุมไม่ให้มีช่องโหว่และอนุญาตให้แอปที่ได้รับอนุญาตทำงานเท่านั้น
- ใช้โซลูชัน endpoint detection และมีการตรวจจับและแก้ไขกิจกรรมที่น่าสงสัยโดยอัตโนมัติ

ความมั่นคงปลอดภัย โดย Cyber Resilience

1. การระบุความเสี่ยง (Identify) คือการทำความเข้าใจในการบริหารจัดการภายในองค์กร ตั้งแต่เรื่องบุคลากร ความสามารถ ข้อมูลและระบบภายในต่าง ๆ ตลอดจนทรัพย์สินทั้งหมดขององค์กร เพื่อที่จะได้นำมาประเมินความเสี่ยงและวางแผนในการจัดการภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อองค์กรได้อย่างเหมาะสม

2. การป้องกัน (Protect) คือการป้องกันจะเริ่มตั้งแต่การวางกลไกและขั้นตอนเพื่อรักษาความปลอดภัย การติดตั้งอุปกรณ์ เช่น Firewall การบำรุงรักษาอุปกรณ์ กระบวนการจัดการข้อมูล และการควบคุมการเข้าถึงและการใช้ระบบ นอกจากนี้ยังรวมถึงการฝึกอบรมและสร้างความตระหนักให้บุคลากรถึงเรื่องความสำคัญของความปลอดภัยเทคโนโลยีสารสนเทศอีกด้วย

3. การตรวจจับ (Detect) คือการเฝ้าระวังและติดตามเหตุการณ์หรือกิจกรรมน่าสงสัยที่อาจก่อให้เกิดภัยคุกคามทางไซเบอร์ซึ่งมีผลกระทบต่อองค์กร รวมถึงการตรวจสอบหาช่องโหว่ของระบบเพื่อที่จะได้พัฒนาระบบให้มีความต้านทานต่อภัยคุกคามทางไซเบอร์ได้มากขึ้น

4. การตอบสนอง (Respond) หลังจากตรวจพบความผิดปกติที่อาจส่งผลต่อความปลอดภัยเทคโนโลยีสารสนเทศแล้วทางองค์กรจำเป็นต้องมีการตอบสนองต่อเหตุการณ์ดังกล่าวอย่างเหมาะสม โดยการวางแนวทางปฏิบัติให้ชัดเจน มีการวิเคราะห์หาสาเหตุ และมีการสื่อสารกันระหว่างองค์กร ในกรณีที่อาจต้องขอความช่วยเหลือจากหน่วยงานภายนอก เพื่อที่จะได้หาแนวทางการป้องกันและลดโอกาสเกิดปัญหาแบบเดิมได้ในอนาคต

5. รักษา สนันสนุน (sustain) รักษาระบบหรือข้อมูลที่สำคัญไว้ระหว่างที่เกิดเหตุการณ์เพื่อป้องกันเหตุการณ์ที่อาจก่อให้เกิดความเสียหายมากกว่าเดิม

6. การกู้คืน (Recover) เมื่อถูกโจมตีทางไซเบอร์ ทางองค์กรจำเป็นต้องทำให้ระบบกลับมาใช้งานได้เป็นปกติอย่างรวดเร็วที่สุด เพื่อให้ธุรกิจดำเนินต่อไปได้อย่างต่อเนื่อง และลดความสูญเสียทั้งด้านการเงินและด้านชื่อเสียงขององค์กร ดังนั้นจึงต้องมีการวางแผนการกู้คืนอย่างมีระบบ และมีการติดต่อสื่อสารที่ดีทั้งภายในและภายนอกองค์กร

ระบบความปลอดภัยใหม่ Zero trust Framework

1. ความน่าเชื่อถือของอุปกรณ์ คือผู้ดูแลระบบไอทีองค์กรจะต้องมีข้อมูลอุปกรณ์ทั้งหมดของบริษัท เช่น ข้อมูลผู้ใช้งาน ฮาร์ดแวร์ ซอฟต์แวร์ แพทช์ ระบบปฏิบัติการ รวมถึงมีโซลูชันที่ตรวจสอบจัดการและควบคุมอุปกรณ์เหล่านี้ได้ โดยสามารถตรวจสอบว่าอุปกรณ์มีความน่าเชื่อถือหรือไม่ และเป็นไปตามข้อกำหนดนโยบายความปลอดภัยที่กำหนดไว้ล่วงหน้าหรือไม่ ซึ่งการใช้โซลูชันการจัดการปลายทาง unified endpoint management (UEM) แบบครบวงจรช่วยให้ผู้ดูแลระบบสามารถจัดการตรวจสอบและควบคุมอุปกรณ์ทั้งหมด เช่น มือถือ เดสก์ท็อป แล็ปท็อป และ อุปกรณ์ IoT ต่าง ๆ ได้ในทุกแพลตฟอร์มจากอุปกรณ์ควบคุมของผู้ดูแลระบบเพียงเครื่องเดียว

2. ความน่าเชื่อถือของผู้ใช้ การพิสูจน์ตัวตนโดยใช้รหัสผ่านร่วมกับการตรวจสอบผู้ใช้งานให้มีความปลอดภัยมากยิ่งขึ้น เช่น การใช้ Biometric หรือการใช้ Certificate หรือ การยืนยันตนแบบหลายปัจจัย (MFA)

3. Transport/Session Trust องค์ประกอบที่สำคัญอีกอย่างหนึ่งของ Zero trust คือการเข้าถึงให้น้อยที่สุด คือผู้ใช้งานหรือระบบควรมีสิทธิ์เข้าถึงทรัพยากรเท่าที่จำเป็นสำหรับการทำงานโดยเฉพาะเท่านั้น ต้องไม่มากหรือไม่น้อยเกินไป

4. ความน่าเชื่อถือของแอปพลิเคชัน ช่วยให้เจ้าหน้าที่สามารถเข้าถึงแอปพลิเคชันต่าง ๆ รวมถึงแอปพลิเคชัน Windows แบบดั้งเดิมได้อย่างปลอดภัยจากอุปกรณ์ใด ๆ ดังนั้นจึงเป็นกุญแจสำคัญในการสร้างพื้นที่ทำงานดิจิทัล ด้วยความทันสมัยของการตรวจสอบผู้ใช้งานที่ช่วยให้การลงชื่อเพียงครั้งเดียว Single Sign On (SSO)

5. Data Trust สร้างความน่าเชื่อถือของข้อมูลป้องกันการรั่วไหลของข้อมูลและตรวจสอบให้แน่ใจว่าเป็นข้อมูลที่ถูกต้องและไม่ได้ถูกแก้ไขระหว่างผู้ใช้และด้วยเทคโนโลยีต่าง ๆ เช่น การป้องกันการสูญหายของข้อมูล

Zero Trust ประกอบด้วย 1) Remote Browsing Isolation (RBI) 2) Content Disarm & Reconstruction (CDR) 3) Robotic VAPT (Continuous testing)

Remote Browsing Isolation (RBI)

คือการโหลดเนื้อหาเว็บบนคอนเทนเนอร์ให้เป็นเว็บเสมือนแล้วจัดเก็บที่คลาวด์ ป้องกันไม่ให้มัลแวร์เข้าถึงคอมพิวเตอร์ของผู้ใช้โดยตรง ซึ่งระบบจะสามารถแยกเว็บเสมือนเหล่านี้ได้ เช่น การท่องอินเตอร์เน็ตโดยใช้เว็บเบราว์เซอร์ การใช้งานอีเมล การประชุมเสมือน การ Chat การใช้แอปพลิเคชั่นบนเว็บ ซึ่งวิธีนี้เป็นวิธีที่มีประสิทธิภาพสูงในการปกป้องคอมพิวเตอร์ทุกเครื่องในองค์กรรวมถึงเครือข่ายภาครัฐ

Content Disarm & Reconstruction (CDR) – Files

ช่วยป้องกันเนื้อหาอันตรายที่ฝังอยู่ภายในไฟล์ Microsoft Office และ Adobe โดยจะจัดการกับรูปแบบของไฟล์ที่มักจะถูกใช้กระจายมัลแวร์ซึ่งจะช่วยลดโอกาสของการติดมัลแวร์ในการโจมตีแบบ Social Engineering หรือจากความผิดพลาดของผู้ใช้งานเอง เนื่องจากการโจมตีจากไฟล์คิดเป็น 75% ของเหตุการณ์ทั้งหมดเนื้อหาที่ซ่อนไฟล์ที่อันตรายและหลบเลี่ยงการตรวจจับการสแกนได้มากกว่า 90% ของการโจมตีที่เป็นอันตรายเกิดขึ้นทุกวันผ่านช่องทาง (Email, web downloads, supply chain file-shares and USB devices).

vulnerability assessment and penetration testing (VAPT)

เทคโนโลยีการทดสอบความปลอดภัยที่สามารถทำการ Hack อย่างมีจริยธรรมโดยอัตโนมัติ (ผ่านทุกขั้นตอนตามปกติการประเมินช่องโหว่และการทดสอบการเจาะระบบ

Anti-virus/Endpoint Protection Platform (EPP)

• รูปแบบการป้องกันแบบดั้งเดิมส่วนใหญ่ต้องการการดูแลจากผู้เชี่ยวชาญโดยมีการปรับใช้บนอุปกรณ์ปลายทางตรวจหากิจกรรมหรือไฟล์ที่เป็นอันตราย

• Anti-virus ยุคถัดไปที่ใช้โมเดลการเรียนรู้ของเครื่องพร้อมใช้งานแล้วเช่นกัน โดยจะมีการตรวจจับไวรัสให้ด้วย

Endpoint Detection & Response (EDR)

คือเครื่องมือในการตรวจสอบภัยคุกคามโดยมีวิธีการตรวจจับโดยผู้เชี่ยวชาญทำการตรวจจับเมื่อภัยคุกคามเข้ามาใกล้

User & Entity Behavior Analytics (UEBA)

คือการตรวจจับพฤติกรรมปลายทางที่ผิดปกติ

Sandbox

คือการแยกสภาพแวดล้อมเพื่อตรวจสอบพฤติกรรมของไฟล์และสังเกตพฤติกรรมเพื่อตรวจสอบว่าไฟล์นั้นเป็นอันตรายหรือไม่ โดยภัยคุกคามจะหาวิธีหลีกเลี่ยงการตรวจจับอย่างต่อเนื่อง เช่น การ Encrypted zip file , malware รูปแบบใหม่ Zero-day, Sandbox evasion

The Internet of Medical Things (IoMT)

Internet of Medical Things (IoMT) Attact Classification คือ Excution ในยุคของ COVID-19 ในปี 2020 กว่า 25% ของการโจมตีทางไซเบอร์ในองค์กรที่ให้บริการด้านสุขภาพเกี่ยวข้องกับ IoMT อุปกรณ์และซอฟต์แวร์ที่ล้าสมัยกำลังสร้างช่องโหว่ด้านความปลอดภัยทางไซเบอร์ที่ร้ายแรงสำหรับทั้งโรงพยาบาลและผู้ป่วย การขาดการเข้ารหัสข้อมูลส่วนบุคคล และมีการควบคุมความปลอดภัยที่หละหลวม องค์กรด้านการดูแลสุขภาพจึงลดความเสี่ยงได้เพียงเล็กน้อยในกรณีที่อุปกรณ์ล้าสมัย

วิธีการป้องกันภัยคุมคามจาก IoMT

- ปรับใช้แนวทาง Zero Trust กับอุปกรณ์ทางการแพทย์
- แบ่งกลุ่มของอุปกรณ์ตามบริบทการใช้งานและจัดทำโปรไฟล์แบบเชิงลึก โดยการประเมินและการบังคับใช้นโยบายของอุปกรณ์แต่ละอุปกรณ์
- เสริมความแข็งแกร่งให้กับกลยุทธ์การจัดการช่องโหว่ด้วย Medical IoT Security

Router and Infrastructure Security

Router and Infrastructure Security มี Attact Classification คือ Privilege Escalation อุปกรณ์เครือข่าย เช่น เราเตอร์และสวิตช์ มักจะเป็นทรัพยากรที่ผู้โจมตีจะใช้เพื่อล้มล้างองค์กร ผู้โจมตีบุกรุกอุปกรณ์เครือข่ายและจากนั้นผู้โจมตีจะสามารถเข้าถึงโครงสร้างพื้นฐานภายในของบริษัทได้โดยตรงและสามารถเข้าถึงบริการและข้อมูลส่วนตัวของผู้ใช้งานได้

วิธีการป้องกัน Router and Infrastructure Security

- นำ Firewall มาใช้งาน ,มีการทดสอบระบบด้วย penetration testing, มีการ network monitoring, และมีการใช้งาน virtual private networks (VPNs), รวมถึงการเขารหัสข้อมูล (encryption technologies), และการอบรมความรู้ด้านเทคโนโลยีใหม่

Spyware

Spyware มี Attact Classification คือ Credential Access สปายแวร์เป็นมัลแวร์ประเภทหนึ่งที่มีจุดประสงค์เพื่อรวบรวมข้อมูลส่วนบุคคลหรือข้อมูลองค์กร ติดตามหรือขายกิจกรรมบนเว็บของเหยื่อ (เช่น การค้นหา ประวัติ และการดาวน์โหลด) เก็บข้อมูลบัญชีธนาคาร และขโมยข้อมูลส่วนบุคคล ท้ายที่สุดสปายแวร์จะสามารถเข้าควบคุมอุปกรณ์กรองข้อมูลหรือส่งข้อมูลส่วนบุคคลไปยังบุคคลอื่นที่ไม่รู้จักโดยปราศจากความยินยอมล่วงหน้าของเจ้าของข้อมูล สปายแวร์สามารถติดตั้งตัวเองบนอุปกรณ์ของเหยื่อด้วยวิธีการต่างๆแต่โดยทั่วไปจะทำการหลอกล่อเป้าหมายหรือใช้ประโยชน์จากช่องโหว่ของระบบ ได้แก่ ผู้ใช้

ยอมรับพรอมต์หรือป๊อปอัปแบบสุ่มโดยไม่ได้ตั้งใจ ดาวน์โหลดซอฟต์แวร์หรืออัปเกรดจากแหล่งที่ไม่น่าเชื่อถือ เปิดไฟล์แนบอีเมลจากผู้ส่งที่ไม่รู้จักหรือละเมิดลิขสิทธิ์ภาพยนตร์และเพลง เป็นต้น

วิธีการป้องกัน Spyware

- ใช้ antivirus software และ anti-malware ที่มีลิขสิทธิ์ที่น่าเชื่อถือ
- หลีกเลี่ยงการ chat กับบุคคลแปลกหน้า
- ไม่เปิด Email ที่เป็นอันตราย ไม่คลิ๊ก link ที่เป็นอันตราย ไม่คลิ๊ก online pop-ups

Macro Viruses

Macro Viruses มี Attact Classification คือ Lateral Movement ไวรัสมาโครคือไวรัสคอมพิวเตอร์ที่เขียนด้วยภาษามาโครเดียวกันกับที่ใช้กับซอฟต์แวร์แอปพลิเคชันบางอย่าง เช่น Microsoft Office, Excel และ PowerPoint อนุญาตให้โปรแกรมแมโครฝังอยู่ในเอกสารได้ เช่น มาโครจะทำงานโดยอัตโนมัติเมื่อเปิดเอกสาร และลักษณะนี้เป็นกลไกที่ชัดเจนซึ่งคำสั่งคอมพิวเตอร์ที่เป็นอันตรายสามารถแพร่กระจายได้ และสิ่งนี้เป็นสาเหตุหนึ่งที่การเปิดไฟล์แนบที่ไม่คาดคิดในอีเมลหรืออีเมลจากผู้ส่งที่ไม่รู้จักอาจเป็นอันตรายได้ โปรแกรมป้องกันไวรัสจำนวนมากสามารถตรวจจับมาโครไวรัสได้ อย่างไรก็ตาม พฤติกรรมของมาโครไวรัสยังคงตรวจจับได้ยาก

วิธีการป้องกัน Macro Viruses

- ใช้ antivirus software ที่มีลิขสิทธิ์ที่น่าเชื่อถือ
- update ระบบปฏิบัติการ window อย่างสม่ำเสมอ
- ไม่เปิด Email ที่เป็นอันตราย ไม่คลิ๊ก link ที่เป็นอันตราย ไม่คลิ๊ก online pop-ups

Command and Control

Command and Control มี Attact Classification คือ Command and Control การโจมตีนี้แฮ็กเกอร์ส่วนใหญ่จะใช้อีเมลฟิชชิ่งติดตั้งมัลแวร์ ซึ่งสิ่งนี้สร้างช่องทางคำสั่งและการควบคุมที่ใช้พร็อกซีในการโจมตี ช่องทางเหล่านี้ถ่ายทอดคำสั่งไปยังปลายทางที่ถูกบุกรุกและส่งออกคำสั่งเหล่านั้นกลับไปยังผู้โจมตี จากนั้นผู้โจมตีจะสอดแนมโดยมุ่งโจมตีไปที่ระบบเครือข่ายเพื่อรวบรวมข้อมูลที่ละเอียดอ่อนและสร้างเซิร์ฟเวอร์ที่จะสื่อสารกับอุปกรณ์ต่าง ๆ การโจมตีเหล่านี้มักเรียกว่าการโจมตีแบบ C2 หรือ C&C

วิธีการป้องกัน Command and Control

- นำระบบ intrusion detection system (IDS), intrusion prevention system (IPS) และ Firewalls หรืออุปกรณ์อื่น ๆ ที่มีความสามารถในการป้องกันได้มาใช้งาน
- นำระบบ Two-factor authentication และ digital code signing มาใช้งาน

การโจมตีด้านโครงสร้างพื้นฐาน Industry-specific cybersecurity (Railways)

โครงสร้างพื้นฐานของรถไฟและระบบการปฏิบัติงานทั่วทั้งพื้นที่ Onboard, Wayside, Station หรือ Control Center ระบบเหล่านี้สามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ หากระบบเหล่านี้ได้รับผลกระทบจากการโจมตีทางไซเบอร์จะทำให้เกิดกลไกรักษาความปลอดภัยของรถขนส่งทางรางซึ่งจะทำให้บริษัทรถไฟหยุดดำเนินการชั่วคราว

1) จำนวนที่เพิ่มขึ้นของอุปกรณ์ IoT ทำให้ผู้โจมตีมีโอกาสมากขึ้นในการดำเนินการหาช่องโหว่หรือถอดรหัส รหัสผ่านบนระบบที่สำคัญ

2) เมื่อระบบควบคุมอาณัติสัญญาณใช้โปรโตคอล WLAN ที่มีความปลอดภัยต่ำ ผู้โจมตีสามารถดำเนินการโจมตีโดยใช้คนกลางและแทรกคำสั่งที่เป็นอันตรายเข้าไปในระบบ

3) แม้ว่าระบบรางทั่วโลกจะตกเป็นเป้าหมายของการโจมตีด้วยแรนซัมแวร์ แต่อย่างไรก็ตามระบบรถไฟได้รับการออกแบบโดยคำนึงถึงความปลอดภัยทางกายภาพและความน่าเชื่อถือแทนความปลอดภัยทางไซเบอร์ สถิติระหว่างปี 2556-2564 แสดงให้เห็นว่าอุตสาหกรรมการขนส่งมีเหตุการณ์การโจมตีด้วยแรนซัมแวร์ 4% บริษัทรถไฟของอิตาลีและเดนมาร์กยังต้องหยุดดำเนินการเนื่องจากการโจมตีของแรนซัมแวร์ในเดือนมีนาคมและตุลาคม 2565 ตามลำดับ

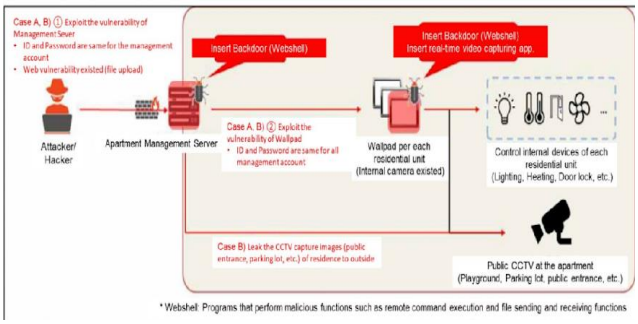
4) ตำแหน่งทางภูมิศาสตร์ของสิ่งอำนวยความสะดวกนั้นยากต่อการจัดการทำให้ผู้โจมตีสามารถเข้าถึงอุปกรณ์เครือข่ายได้ เช่น เราเตอร์หรือคอนโทรลเลอร์และทำให้ระบบในอุตสาหกรรมรถไฟเสี่ยงต่อการถูกคุกคามจากการปลอมแปลงข้อมูลหรือการหยุดชะงักของบริการ

Industry-specific cybersecurity (Smart City)

ในประเทศเกาหลี ระบบอัจฉริยะถูกนำไปใช้กับอพาร์ทเมนท์เป็นหลักโดยอพาร์ทเมนท์ที่สร้างขึ้นใหม่ซึ่งเป็นส่วนหนึ่งของการก่อสร้างเมืองอัจฉริยะในช่วงไม่กี่ปีที่ผ่านมา ลิฟต์ เครื่องปรับอากาศ ระบบควบคุมการเข้าออกที่จอดรถ และ wallpad ในแต่ละยูนิตได้รับการติดตั้งเป็นระบบอัจฉริยะในอพาร์ตเมนต์อย่างไรก็ตาม คุณลักษณะด้านความปลอดภัยของระบบอัจฉริยะเหล่านี้ค่อนข้างต่ำ ทำให้ตกเป็นเป้าหมายของการโจมตีทางไซเบอร์จำนวนมากในเดือนเมษายน พ.ศ. 2564 ในพาร์ตเมนต์ใหม่ในพื้นที่ของประเทศหนึ่ง ระบบ wallpad ที่ผู้อยู่อาศัยใช้ถูกแฮ็กข้อมูลส่วนบุคคลรั่วไหลและประตูอาคารถูกเปิดออก

Industry-specific cybersecurity (Smart City)

เหตุการณ์ Hack Wallpad และ CCTV



Industry-specific cybersecurity (Healthcare)

ความถี่และความรุนแรงที่เพิ่มขึ้นของการโจมตีด้วยแรนซัมแวร์โรงพยาบาลและองค์กรด้านการดูแลสุขภาพสามารถขัดขวางการปฏิบัติงานและการเข้าถึงของผู้ป่วยเป็นเวลาหลายสัปดาห์หรือหลายเดือน หรือการให้บริการหยุดชะงัก รวมถึงการหยุดทำงานของระบบอิเล็กทรอนิกส์ 41.7% การยกเลิกการนัดหมาย 10.2% และการเบี่ยงเบนความสนใจของรถพยาบาล 4.3% ในเดือนกันยายน 2020 การโจมตีด้วยแรนซัมแวร์ที่โรงพยาบาลในเยอรมนีทำให้ผู้หญิงเสียชีวิตนอกจากนี้ ศูนย์ความปลอดภัยทางไซเบอร์แห่งชาติของสหราชอาณาจักร (NCSC) ยังรายงานการโจมตีโดยแฮ็กเกอร์ที่เป็นที่รู้จักอย่าง APT29 ซึ่งกำหนดเป้าหมายข้อมูลเกี่ยวกับการพัฒนาของ COVID-19 ในสหราชอาณาจักร แคนาดา และสหรัฐอเมริกาและนอกจากนี้มหาวิทยาลัยแห่งแคลิฟอร์เนียต้องจ่ายค่าไถ่ 1.14 ล้านดอลลาร์ให้กับ NetWalker หลังจากที่เซิร์ฟเวอร์ของคณะแพทยศาสตร์ได้รับผลกระทบจากแรนซัมแวร์

NIST Cyber Security Framework(CSF) (U.S. cyber security framework)

1) อธิบายสถานะความปลอดภัยทางไซเบอร์ในปัจจุบัน

2) อธิบายเป้าหมายสำหรับความปลอดภัยทางไซเบอร์

3) ระบุและจัดลำดับความสำคัญของโอกาสในการปรับปรุงภายในบริบทของกระบวนการที่ต่อเนื่องและทำซ้ำได้

4) ประเมินความก้าวหน้าไปสู่สถานะเป้าหมายของความปลอดภัยทางไซเบอร์

5) สื่อสารระหว่างผู้มีส่วนได้ส่วนเสียภายในและภายนอกเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์

องค์ประกอบหลักของ CSF

1. แกนหลัก: ผลลัพธ์ด้านความปลอดภัยในโลกไซเบอร์ที่ต้องการจะจัดตามลำดับชั้นและสอดคล้องกับคำแนะนำและการควบคุมที่ดียิ่งขึ้น

2. โปรไฟล์: สอดคล้องกับความต้องการขององค์กรและวัตถุประสงค์ ความเสี่ยงที่ยอมรับได้ และการใช้ทรัพยากรที่ต้องการ

3. ระดับการดำเนินการ: มาตรการเชิงคุณภาพสำหรับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ขององค์กร

The Framework Core ประกอบด้วย 5 function

Function1: Identify

• พัฒนาความเข้าใจในองค์กรเพื่อจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ต่อระบบ บุคลากร สินทรัพย์ ข้อมูล และความสามารถ

• การทำความเข้าใจบริบททางธุรกิจ ทรัพยากรที่สนับสนุนการทำงานที่สำคัญ และความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง ช่วยให้องค์กรสามารถมุ่งเน้นและจัดลำดับความสำคัญของสิ่งที่ต้องดำเนินการได้ โดยสอดคล้องกับกลยุทธ์การจัดการความเสี่ยงและความต้องการทางธุรกิจ

• ตัวอย่างของหมวดหมู่ผลลัพธ์ภายในฟังก์ชันนี้ ได้แก่: การจัดการสินทรัพย์ สภาพแวดล้อมทางธุรกิจ ธรรมาภิบาล การประเมินความเสี่ยง และกลยุทธ์การบริหารความเสี่ยง

Function2: Protect

• พัฒนาและดำเนินการป้องกันที่เหมาะสมเพื่อให้แน่ใจว่าได้ส่งมอบบริการที่มีคุณภาพ

• ฟังก์ชันป้องกันรองรับความสามารถในการจำกัดหรือควบคุมผลกระทบของเหตุการณ์ความปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น

• ตัวอย่างของหมวดหมู่ผลลัพธ์ภายในฟังก์ชันนี้ ได้แก่ การจัดการข้อมูลประจำตัวและการควบคุมการเข้าถึง ความตระหนัก และการฝึกอบรม ความปลอดภัยของข้อมูล การป้องกันข้อมูล กระบวนการและขั้นตอน การซ่อมบำรุง และเทคโนโลยีป้องกัน

Function3: Detect

• พัฒนาและดำเนินกิจกรรมที่เหมาะสมเพื่อระบุเหตุการณ์ความปลอดภัยทางไซเบอร์

• ฟังก์ชั่น Detect ช่วยให้สามารถค้นพบเหตุการณ์ความปลอดภัยทางไซเบอร์ได้ทันท่วงที

• ตัวอย่างของหมวดหมู่ผลลัพธ์ภายในฟังก์ชันนี้ ได้แก่ ความผิดปกติ และเหตุการณ์ผิดปกติ การตรวจสอบความปลอดภัยอย่างต่อเนื่อง และกระบวนการตรวจจับ

Function4: Respond

• พัฒนาและดำเนินกิจกรรมที่เหมาะสมเพื่อดำเนินการเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ที่ตรวจพบ

• ฟังก์ชั่นการตอบสนองต่อเหตุการณ์ถูกโจมตีทางไซเบอร์

• ตัวอย่างของหมวดหมู่ผลลัพธ์ภายในฟังก์ชันนี้ ได้แก่ การวางแผนการตอบสนอง การสื่อสาร การวิเคราะห์ บรรเทา และการปรับปรุง

Function5: Recover

• พัฒนาและดำเนินกิจกรรมที่เหมาะสมเพื่อรักษาแผนสำหรับความยืดหยุ่นและเพื่อฟื้นฟูความสามารถหรือบริการใดๆที่บกพร่องเนื่องจากเหตุการณ์ความปลอดภัยทางไซเบอร์

• ฟังก์ชั่นการกู้คืนรองรับการกู้คืนอย่างทันเวลาเพื่อให้สามารถกลับมาทำงานได้อย่างปกติ เพื่อลดผลกระทบจากเหตุการณ์การโจมตีทางไซเบอร์

• ตัวอย่างของหมวดหมู่ผลลัพธ์ภายในฟังก์ชันนี้ ได้แก่ การวางแผนการกู้คืน การปรับปรุง และการสื่อสาร

ISO 27001

ISO/IEC 27001 เป็นมาตรฐานการรักษาความปลอดภัยของข้อมูลซึ่งเผยแพร่ในปี 2005 และแก้ไขครั้งล่าสุดในปี 2022 ซึ่งเผยแพร่โดยองค์การระหว่างประเทศว่าด้วยการมาตรฐาน เป็นที่ยอมรับในหลายประเทศว่าเป็นกรอบหลักสำหรับการดำเนินการด้านความปลอดภัยข้อมูลและความปลอดภัยทางไซเบอร์ โดยจะอธิบายถึงระบบการจัดการความปลอดภัยของข้อมูล และวางความปลอดภัยไว้ในบริบทของการจัดการและกระบวนการโดยรวมในบริษัท เหมาะสำหรับการใช้งานโดยองค์กรทุกขนาดหรือทุกอุตสาหกรรม

การเปรียบเทียบระหว่าง CSF และ ISO 27001

• Cybersecurity Framework เป็นไปตามนโยบายของผู้บริหารของประเทศสหรัฐเมริกา คำสั่งการปรับปรุงความปลอดภัยทางไซเบอร์โครงสร้างพื้นฐานที่สำคัญเมื่อปี 2013 และในตอนแรกมีไว้สำหรับบริษัทในสหรัฐอเมริกาที่ถือว่าเป็นส่วนหนึ่งของโครงสร้างพื้นฐานที่สำคัญ เหมาะสำหรับการใช้งานโดยองค์กรทั่วไปที่เผชิญกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ โดยไม่คำนึงถึง ขนาด หรืออุตสาหกรรม

นวัตกรรมใหม่สำหรับ Cyber-protection techniques

Cybersecurity Mesh Architecture

CSMA คือ frame work หนึ่งที่ช่วยบริหารจัดการด้านความปลอดภัย โดยหลายๆบริษัทปรับใช้กลยุทธ์ ต่าง ๆ ในการรักษาความปลอดภัยที่มีเป้าหมายในการแก้ปัญหาความเสี่ยงด้านความปลอดภัโดยเฉพาะเป็นผลให้สถาปัตยกรรมด้านความปลอดภัยกลายเป็นเรื่องซับซ้อนและยากต่อการตรวจสอบและนำไปสู่การตรวจสอบปัญหาที่ผิดพลาดและล่าช้า

Federated Identity Management

Federated Identity Management คือ การจัดการข้อมูลแบบศูนย์รวม โดยจะมีการแบ่งปัน Digital Identities กับ Partner ที่เชื่อถือได้ซึ่งทำให้ User สามารถใช้งานได้หลากหลายธุรกิจแต่ใช้เพียงแค่ Credential ชุดเดียว

Cyber Resilience in the Cloud Environment

ความยืดหยุ่นทางไซเบอร์ในสภาพแวดล้อมคลาวด์ คือเครือข่ายที่ยืดหยุ่น และจำกัดกิจกรรมของผู้ที่ไม่ได้รับอนุญาต เป็นเครือข่ายที่ได้รับการออกแบบมาเพื่อลดโอกาสที่จะเกิดความเสียหาย โดยมีลักษณะเฉพาะที่สำคัญที่สุดคือความสามารถในการทำให้ระบบที่มีความสำคัญกลับมาทำงานได้อย่างรวดเร็วหลังจากถูกโจมตี

Ransomware ที่โจมตีกลุ่มประเทศอาเซี่ยน

Ransomware Maze

เป็น Ransomware ชนิดหนึ่งที่ถูกออกแบบมาเพื่อเข้ารหัสไฟล์บน PC หรือ Laptop ของเหยื่อ และทำการเรียกค่าไถ่หากเหยื่อต้องการจะเปิดไฟล์นั้น

ช่องทางการโจมตี

1. อีเมลขยะ มักใช้ลิงก์หรือไฟล์แนบที่เป็นอันตราย (ส่วนใหญ่ไฟล์ Word หรือ Excel)
2. การโจมตีด้วย RDP brute force
3. การใช้ช่องโหว่ที่มีในการโจมตี

Ransomware REvil

REvil ransomware เป็นไวรัสบล็อกไฟล์ที่ถือว่าเป็นภัยคุกคามร้ายแรงที่เข้ารหัสไฟล์หลังจากการติดไวรัสและมีการเรียกค่าไถ่ข้อมูลที่ได้เข้ารหัสไว้ โดยข้อความจะอธิบายว่าเหยื่อต้องจ่ายค่าไถ่เป็นบิตคอยน์ และเมื่อค่าไถ่จ่ายไม่ตรงเวลา จะมีการเรียกค่าไถ่เพิ่มขึ้นเป็นสองเท่า REvil ransomware เป็น ransomware บริษัทสัญชาติรัสเซีย โดยมีการดำเนินการแรนซัมแวร์ในลักษณะของบริการ (ransomware as a Service)

ช่องทางการโจมตี

REvil ransomware ทำงานเหมือนกับแรนซัมแวร์อื่น ๆ โดยหลังจากเข้าไปในอุปกรณ์ของเหยื่อแล้ว มันจะเข้ารหัสไฟล์ของพวกเขาด้วยกุญแจที่แฮ็กเกอร์เท่านั้นที่มี และจะเรียกค่าไถ่เพื่อให้เหยื่อได้รับไฟล์คืน

Regnar ransomware

Ragnar Locker เป็นแรนซั่มแวร์สำหรับ Windows และ Linux ซึ่งเป็น Ramsomware ที่แฮกเกอร์สร้างเทคนิคใหม่ขึ้นมา เพื่อหลบเลี่ยงการตรวจจับจาก security programs Ragnar Locker ถูกใช้โจมตีในการเข้ารหัสไฟล์เหยื่อ โดยหลาย ๆ องค์กรพยายามป้องกันระบบเครือข่ายตัวเองด้วยการเพิ่มเทคนิคใหม่ ๆ ขึ้นมาเพื่อหยุด Ragnar Locker Ransomware นี้

ช่องทางการโจมตี

หลักการทำงานโดยทั่วไปของ ransomware คือจะพยายามหยุดการทำงานของโปรแกรม security แล้วจึงเข้ารหัสไฟล์ (encrypting) แต่ Ragnar Locker จะใช้คอมพิวเตอร์เสมือน (virtual machines) ในการหลบเลี่ยงและเข้ารหัสไฟล์ (encrypting)

NetWalker

แรนซัมแวร์ NetWalker จะแพร่ระบาดเฉพาะคอมพิวเตอร์ที่ใช้ Windows และเป้าหมายหลักคือสถานพยาบาลและสถานศึกษา ระบบนี้จะขโมยข้อมูลและนำข้อมูลไปแชร์บน Dark เว็บไซต์ ทำให้หัวข้อของข้อมูลนั้นเป็นเป้าหมายของมัลแวร์เพิ่มเติมและเสี่ยงต่อการถูกโจมตีจากกลุ่มแฮ็กเกอร์อื่นๆ แรนซั่มแวร์นี้มักมาทางอีเมลฟิชชิ่ง ซึ่งมักมาพร้อมกับข้อความเกี่ยวกับ COVID-19 ซึ่งมีไฟล์แนบหรือลิงก์ที่เป็นอันตราย

Overview of Cybersecurity Certifications

Certifications ประกอบด้วย

CISSP	SSCP	CCSP
IT security, cybersecurity	IT infrastructure security	Secure cloud infrastructure
CAP	**CSSLP**	**HCISPP**
IT information security, information assurance, risk management framework	Software development lifecycle security	Healthcare cybersecurity privacy

CISSP (Certificate Information System Security Professional)

เหมาะสำหรับผู้ที่มีประสบการณ์อย่างน้อย 2 ปีในงานด้าน Security เนื่องจากข้อสอบ Certification (CISSP CAT Examination) นั้นมีความยากและท้าทายผู้เข้าสอบสูง โดยข้อสอบมีจำนวน 100 - 150 ข้อ และต้องใช้เวลาประมาณ 3 ชั่วโมงในการสอบ นอกจากนั้นผู้สอบยังต้องได้คะแนนอย่างน้อย 70% ในการผ่าน Examination โดยสิ่งที่ต้องเรียนคือ

1) Security and Risk Management
2) Asset Security
3) Security Architecture and Engineering
4) Communication and Network Security
5) Identity and Access Management (IAM)
6) Security Assessment and Testing
7) Security Operations
8) Software Development Security

CCSP (Certified Cloud Security Professional Preparation) Secure cloud infrastructure)

เหมาะสำหรับผู้ที่มีประสบการณ์อย่างน้อย 5 ปีในงานด้าน Cloud Security เนื่องจากข้อสอบนั้นมีความยากและท้าทายผู้เข้าสอบสูง โดยข้อสอบมีจำนวน 125 ข้อ และต้องใช้เวลาประมาณ 4 ชั่วโมงในการสอบ นอกจากนั้นผู้สอบยังต้องได้คะแนนอย่างน้อย 70% ในการผ่าน Examination โดยสิ่งที่ต้องเรียนคือ

1) loud Concepts, Architecture and Design
2) Cloud Data Security
3) Cloud Platform and infrastructure Security
4) Cloud Application Security
5) Cloud Security Operations
6) Legal, Risk and Compliance

ความแตกต่างระหว่าง CISSP กับ CCSP

CISSP เป็นสิ่งรับรองว่าช่วยให้ผู้สอบสามารถเปลี่ยนอาชีพไปเป็น Manager ได้ และเหมาะสำหรับตำแหน่งดังนี้

- 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

CISSP เป็นสิ่งรับรองว่าช่วยให้ผู้สอบยังคงอยู่ในตำแหน่งด้าน technical ได้ โดยปฏิบัติงานตำแหน่ง ดังนี้

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

ComTIA Security+ ข้อสอบจะประกอบด้วย

- ภัยคุกคาม ช่องโหว่ และการโจมตี
- เทคโนโลยีและเครื่องมือต่างๆ
- สถาปัตยกรรมและการออกแบบ
- ตัวตนและการเข้าถึงการจัดการ
- การบริหารความเสี่ยง
- การเข้ารหัสและรหัสสาธารณะ

นโยบายดิจิทัล

นโยบายดิจิทัลคือการกระทำทั้งหมดที่หน่วยงาน รวมถึงรัฐบาล กระทำเพื่อป้องกันการถูกโจมตีทางไซเบอร์ ซึ่งประกอบด้วยชุดความคิดหรือแผนการว่าจะทำอย่างไรในสถานการณ์เฉพาะที่ได้รับการตกลงอย่างเป็นทางการจากกลุ่มบุคคล องค์กรธุรกิจ โดยมีปัจจัยดังต่อไปนี้

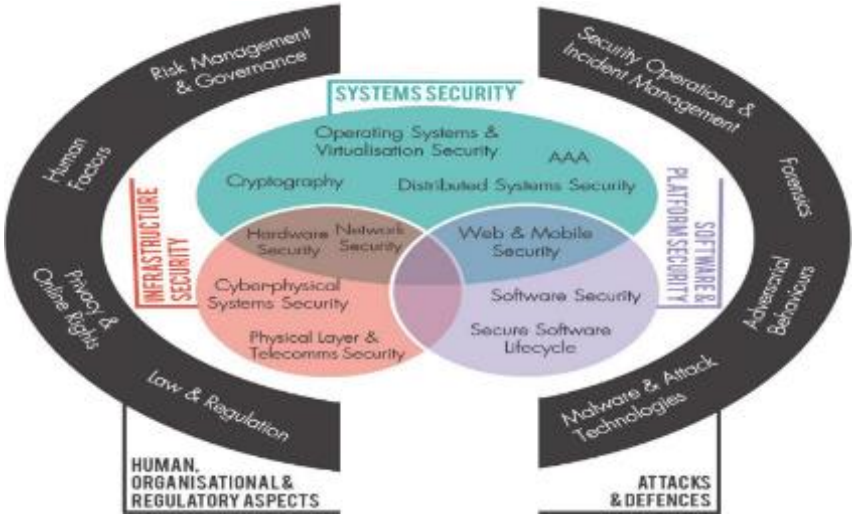
1) จะต้องใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์สูงสุด

2) นโยบายจะต้องสะท้อนถึงความต้องการจากหน่วยงานต่างๆ เช่น การเมือง ธุรกิจ ภาคประชาสังคม และกระแสโลกหรือมีมาตรการจำกัดกิจกรรมทางธุรกิจเพื่อประสิทธิภาพในการบริหารจัดการ

3) มีนโยบายควบคุมธุรกิจแต่ละประเภท

4) มีนโยบายที่รองรับการเปลี่ยนแปลงทางดิจิทัลและกระตุ้นให้ธุรกิจลงทุนในเทคโนโลยีใหม่ ๆ เช่น AI และ เมตาเวิร์ส

Cybersecurity Policy Framework



องค์ประกอบหลักของยุทธศาสตร์ความปลอดภัยทางไซเบอร์แห่งชาติ (McKinsey, 2020)

1.หน่วยงานความมั่นคงทางไซเบอร์แห่งชาติ (NCA)

• ทักษะและความเชี่ยวชาญทางเทคนิคภายในองค์กรพร้อมความร่วมมือกับหน่วยงานอื่น

2. แผนป้องกันโครงสร้างพื้นฐานที่สำคัญระดับชาติ

• จัดลำดับความสำคัญตามมาตรฐานสากลและการกำกับดูแลที่แข็งแกร่ง

3. แผนเผชิญเหตุและฟื้นฟูระดับชาติ

• ขั้นตอนการรายงาน, การตรวจสอบเชิงรุก การป้องกันเชิงรุก,การประเมินที่เป็นมาตรฐานและแผนการที่แข็งแกร่ง

4. กฎหมายที่กำหนดเกี่ยวกับอาชญากรรมทางไซเบอร์ทั้งหมด

• ความร่วมมือระหว่างประเทศที่สำคัญและเป็นขั้นตอน

5. ระบบนิเวศความปลอดภัยทางไซเบอร์

• ผู้ประกอบการและธุรกิจ แรงงาน พลเมืองที่รู้เท่าทันโลกไซเบอร์

Cybersecurity for Digital Tranform

Modernize Cybersecurity

• ตรวจจับและแบ่งปันความรู้ด้านภัยคุกคาม โดยควรมีการตรวจจับภัยคุกคามตลอดเวลา

• มี ai ตรวจจับ domain ที่เป็นอันตราย

• การปกป้องข้อมูล

• Anti spam/Anti mulware

• intrusion prevention

• backup ข้อมูลอย่างสม่ำเสมอ

• มีการเข้ารหัสข้อมูลและกู้คืนข้อมูล

Cybersecurity R&D Convergense Security

• มีการเข้ารหัสข้อมูล

• login เข้าสู่ระบบด้วย user password ที่แข็งแรงหรือใช้การยื่นยันตัวตนด้วยในหน้าหรือลายนิ้วมือ

• มีระบบเฝ้าระวัง

• มีระบบ cloud Security

• มี web, email ฐานข้อมูลที่เป็นประโยชน์

วิวัฒนาการของการโจมตีทาง Cyber

• Generation I: การเปลี่ยนแปลงของเทคโนโลยีสมัยใหม่ มีการพัฒนาผลิตภัณฑ์ป้องกันไวรัส

• Generation II: มี Firewall ตัวแรกพร้อมกับระบบตรวจจับการบุกรุก (IDS)

• Generation III: เน้นการป้องกันและเปิดตัวผลิตภัณฑ์ระบบป้องกันการบุกรุก (IPS)

• Generation IIII: ผลิตภัณฑ์ต่อต้านบอทและแซนด์บ็อกซ์ (APT) เพื่อจัดการกับการโจมตีที่ไม่เคยมีมาก่อนและการโจมตีซีโร่เดย์

• Generation V: ข้อมูลภัยคุกคามแบบเรียลไทม์ ป้องกันการโจมตีบนอินสแตนซ์เสมือน คลาวด์ การปรับใช้ อุปกรณ์ปลายทาง สำนักงานระยะไกล และอุปกรณ์เคลื่อนที่

สถิติการโจมตีทางไซเบอร์ล่าสุด

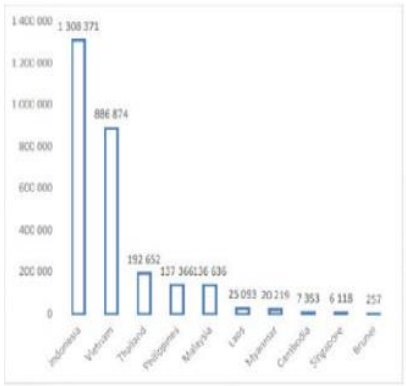
• อุปกรณ์ไอทีที่ถูกโจมตีมากที่สุด คอมพิวเตอร์และแล็ปท็อป โดยเส้นทางที่ใช้สำหรับการโจมตีมากที่สุดของมัลแวร์คืออีเมล และการโจมตีทางไซเบอร์บนมือถือกำลังเพิ่มขึ้น โทรจันก็เพิ่มขึ้นและเริ่มมีมากขึ้นในโทรศัพท์ที่ใช้ Android สถิติการโจมตีทางไซเบอร์ล่าสุดในประเทศกลุ่ม AESAN

• การโจมตีทางไซเบอร์ครั้งใหญ่ในอาเซียนประเทศส่วนใหญ่ถูกละเมิดข้อมูลและโดนโจมตีด้วยแรนซัมแวร์

• มีความสูญเสียต่อเศรษฐกิจของประเทศ สูญเสียความมั่นใจในบริการที่สำคัญของประชาชน

• การหยุดชะงักของเศรษฐกิจในระดับประเทศหรือระดับโลก และความเสียหายด้านชื่อเสียง

Ransomware ในกลุ่มประเทศอาเซียน



Ransomware Detection Count

Ransomware family	Target country	Target sector
Maze	Singapore	Aerospace
	Thailand	State enterprise
	Thailand	Beverage company
	Vietnam	Manufacturing and trading (steel)
REvil	Indonesia	Palm products and others
	Singapore	Engineering
Ragnar	Singapore	Aerospace
NetWalker	Malaysia	IT services
	Thailand	Hotels and accommodation

อันดับที่หนึ่งคือประเทศ อินโดนีเซีย 1,308,317 อันดับที่สอง เวียตนาม 886,874 อันดับที่สาม ไทย 192,652 อันดับที่สี่ฟิลิปปิน 137,366 อันดับที่ห้า มาเลเซีย 136,636 อันดับที่หก ลาว 25,093 อันดับที่เจ็ด เมียนม่า 20,219 อันดับที่แปด กัมพูชา 7,353 อันดับที่เก้าสิงคโป 6,118 และอันดับที่สิบบรูไน 257

ตัวอย่าง Cyberattacks

ภัยคุมคามทาง Cyber มีจำนวนสูงขึ้นมากเมื่อเปรียบเทียบกับผู้ติดเชื้อ Covid 19 ในเดือนมีนาคมปี 2020 พบว่ามีภัยคุมคามด้านไฟล์ที่เป็นอันตราย ลิงค์ที่เป็นอันตราย และ Email ที่เป็นอันตราย โดยเหตุการณ์ Email ที่เป็นอันตรายสูงที่สุด 8,091,193 เหตุการณ์ เพิ่มสูงขึ้นจากเดือนมกราคม -เดือนมีนาคม 2020 โดยเกิด

ที่ประเทศ United State 38.4% ประเทศอื่น ๆ 29% Germany 14.7% France 9.2% Belgium 4.7% และ United Kingdom 4.1% และเป็นชนิดของการโจมตีอันดับ 1 คือ Ransomware อันดับ 2 Trojan อันดับ 3 RAT เป็นต้น

ส่วนที่ 2 ประโยชน์ที่ได้รับและการขยายผลจากการเข้าร่วมโครงการ

• ประโยชน์ต่อตนเอง ได้ทราบรายละเอียดการโจมตีทางไซเบอร์ในรูปแบบต่างๆ รวมถึงได้ทราบวิธีการแก้ปัญหาหากโดนโจมตี โดยสามารถนำแนวคิดและองค์ความรู้มาเสริมสร้างทักษะในการวางแผนกลยุทธ์ของการบริหารจัดการความมั่นคงทางไซเบอร์ได้ ทั้งในด้านของการบริหารจัดการก่อนเผชิญเหตุ การบริหารจัดการระหว่างเผชิญเหตุ และการบริหารจัดการหลังจากเผชิญเหตุให้แก่หน่วยงานได้ โดยสามารถนำมาปรับใช้ได้กับหน่วยงานในแต่ละประเภทได้อย่างมีประสิทธิภาพ

• ประโยชน์ต่อหน่วยงานต้นสังกัด สามารถนำแนวคิดและองค์ความรู้มาเสริมสร้างทักษะในการวางแผนกลยุทธ์ของการบริหารจัดการความมั่นคงทางไซเบอร์ได้ ทั้งในด้านของการบริหารจัดการก่อนเผชิญเหตุ การบริหารจัดการระหว่างเผชิญเหตุ และการบริหารจัดการหลังจากเผชิญเหตุให้แก่หน่วยงานได้

• ประโยชน์ต่อสายงาน สามารถนำแนวคิดและองค์ความรู้มาเสริมสร้างทักษะในการวางแผนกลยุทธ์ของการบริหารจัดการความมั่นคงทางไซเบอร์ได้ ทั้งในด้านของการบริหารจัดการก่อนเผชิญเหตุ การบริหารจัดการระหว่างเผชิญเหตุ และการบริหารจัดการหลังจากเผชิญเหตุ โดยสามารถนำมาปรับใช้ได้กับทุกหน่วยงาน โดยเป็นโอกาสในการเพิ่มพูนความรู้ให้กับผู้เข้าร่วมอบรมรวมถึงช่วยให้มีความก้าวหน้าในสายงาน

• กิจกรรมการขยายผลที่ได้ดำเนินการภายในระยะเวลา 60 วันนับจากวันสุดท้ายของโครงการ มีการแบ่งปันองค์ความรู้ที่ได้รับให้แก่พนักงานในหน่วยงานเพื่อเสริมสร้างทักษะในการบริหารจัดการความมั่นคงทางไซเบอร์

• กิจกรรมการขยายผลที่จะดำเนินการภายใน 6 เดือนหลังเข้าร่วมโครงการ จะพัฒนาแนวทางในการการวางแผนกลยุทธ์ของการบริหารจัดการความมั่นคงทางไซเบอร์ทั้งด้านการบริหารจัดการก่อนเผชิญเหตุ การบริหารจัดการระหว่างเผชิญเหตุ และการบริหารจัดการหลังจากเผชิญเหตุ ให้มีประสิทธิภาพมากยิ่งขึ้น โดยมีการศึกษาถึงวิธีการโจมตีรูปแบบใหม่อย่างสม่ำเสมอ รวมทั้งหาวิธีการในการป้องกันการโจมตีตามเทคโนโลยีใหม่ๆ เพื่อเพิ่มประสิทธิภาพในการปฏิบัติงาน