เอกสารเสนอบทความวิชาการ

เรื่อง

แนวทางการพัฒนา
สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.
ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force

โดย

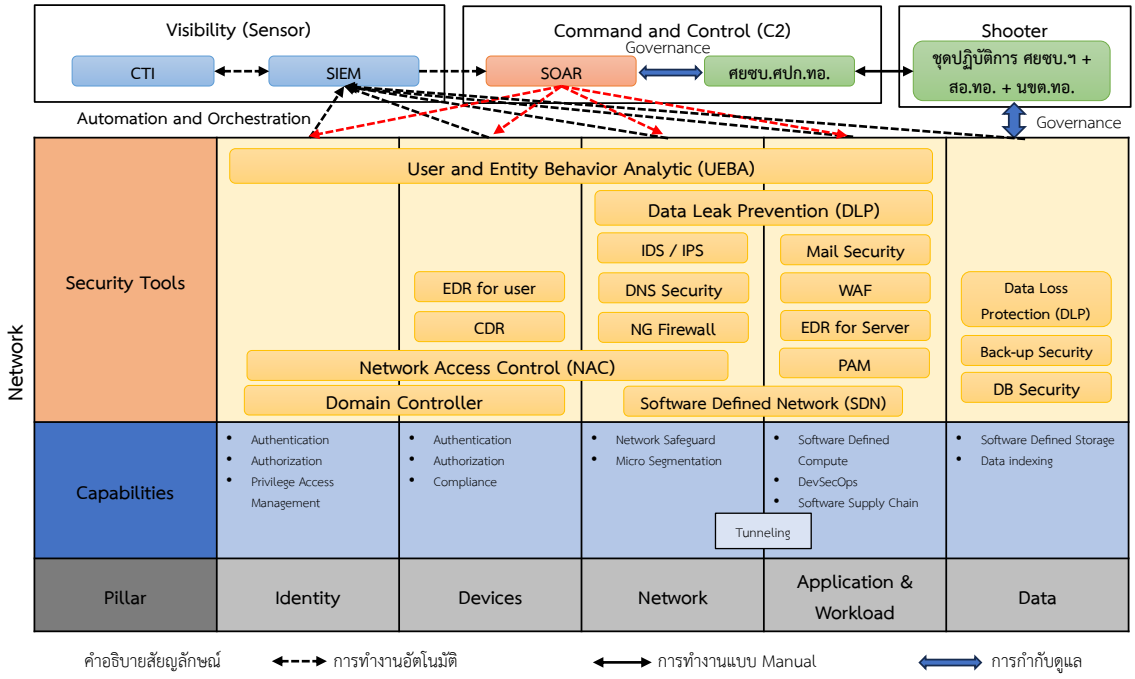
นาวาอากาศเอก เอกชัย สิงห์ทอง

นายทหารฝ่ายเสนาธิการ กองรักษาความมั่นคงปลอดภัยไซเบอร์
ศูนย์ไซเบอร์กองทัพอากาศ

พ.ศ.๒๕๖๗

บทคัดย่อ

กองทัพอากาศ (ทอ.) มีการพัฒนาหน่วยโดยใช้แนวคิดกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง Network Centric Air Force (NCAF) ย่อมต้องมีความเสี่ยงต่อภัยคุกคามทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้ จำเป็นต้องมีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ได้มาตรฐานและมีประสิทธิภาพเข้ากันได้ดีกับบริบทของ ทอ. สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการยอมรับในระดับสากลอย่างแพร่หลายในปัจจุบันคือ Zero Trust แต่ ทอ.มีการจัดโครงสร้างหน่วยงาน และมีหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เฉพาะเจาะจงตามบริบทของ ทอ.เอง การนำสถาปัตยกรรม Zero Trust มาประยุกต์ใช้งานจึงควรปรับให้เข้ากับบริบทของ ทอ.และสอดคล้องกับ NCAF กลายเป็นแนวทางการพัฒนาสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.เองดังนี้



หน้านี้ตั้งใจเว้นว่างไว้

คำนำ

ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) ก่อตั้งเมื่อ ๑ ต.ค.๖๓ มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านไซเบอร์ของกองทัพอากาศ (ทอ.) หนึ่งในหน้าที่สำคัญคือการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ ทอ.ซึ่งต้องมีการวางตำแหน่งและหน้าที่การทำงานของเครื่องมือในการรักษาความมั่นคงปลอดภัยไซเบอร์ต่าง ๆ ใน ทอ.ให้ถูกต้องเหมาะสม สามารถทำงานประสานสอดคล้อง เพื่อให้เกิดประสิทธิภาพในการป้องกันอย่างเต็มที่ ในทางปฏิบัติองค์กรต่าง ๆ จะยึดตามสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีมาตรฐานและได้รับการยอมรับอย่างแพร่หลาย มีความทันสมัยตอบสนองต่อความต้องการใช้งานเครือข่าย ซึ่งในปัจจุบันสถาปัตยกรรมที่เป็นที่ยอมรับอย่างแพร่หลายคือ Zero Trust แต่การจะนำสถาปัตยกรรมนี้มาใช้งานใน ทอ.เลยนั้นอาจจะทำให้ไม่ได้ประสิทธิภาพอย่างเต็มที่ เนื่องจาก ทอ.มีบริบทของการจัดหน่วย รวมถึงมีหน่วยงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในแบบของ ทอ.เอง อีกทั้งยังยึดแนวทางในการปฏิบัติงานที่ใช้เครือข่ายเป็นศูนย์กลาง หรือ Network Centric Air Force (NCAF) อีกด้วย ทอ.จึงควรมีแนวทางการพัฒนาสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แบบ Zero Trust ให้เข้ากันได้กับบริบทของ ทอ.และแนวคิด NCAF ของ ทอ.ด้วย ในบทความนี้จึงเป็นการนำเสนอแผนภาพสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.ที่มีความสอดคล้องกับสถาปัตยกรรม Zero Trust และเข้ากันได้กับแนวคิด NCAF

หน้านี้ตั้งใจเว้นว่างไว้

กิตติกรรมประกาศ

บทความเรื่อง “แนวทางการพัฒนาสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ. ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force” สำเร็จลุล่วงไปด้วยดี เกิดจากการสนับสนุนทั้งจากบุคคลและหน่วยงานต่าง ๆ ผู้เขียนขอขอบคุณมา ณ โอกาสนี้ ขอขอบคุณผู้บังคับบัญชาและผู้ร่วมงาน ณ ศูนย์ไซเบอร์กองทัพอากาศ ที่ให้การสนับสนุนเป็นอย่างดี ขอขอบคุณครอบครัวที่สนับสนุนและเป็นแรงใจในการเขียนบทความ ตลอดจนผู้แต่งหรือเรียบเรียบตำราหรือเนื้อหาต่าง ๆ ที่ผู้เขียนนำมาใช้อ้างอิงในบทความนี้ ขอกราบขอบพระคุณบุพการี ครูอาจารย์ ที่ฟูมฟักอบรมสั่งสอนจนมาถึงทุกวันนี้ ผู้เขียนหวังว่าบทความนี้จะเป็นประโยชน์ต่อ ทอ.ในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หากมีข้อผิดพลาดประการใดผู้เขียนยินดีน้อมรับคำแนะนำเพื่อแก้ไขต่อไป

นาวาอากาศเอก เอกชัย สิงห์ทอง
ศูนย์ไซเบอร์กองทัพอากาศ
เมษายน ๒๕๖๗

หน้านี้ตั้งใจเว้นว่างไว้

สารบัญ

หน้านี้ตั้งใจเว้นว่างไว้

สารบัญภาพ

หน้านี้ตั้งใจเว้นว่างไว้

คำย่อที่ใช้และความหมาย

CDR	Content Disarm and Reconstruction เครื่องมือหรือระบบที่ใช้ในการลบรหัสที่อาจเป็นอันตรายออกจากไฟล์ แล้วประกอบไฟล์กลับให้สามารถทำงานได้อย่างปลอดภัย
CTI	Cyber Threat Intelligence เครื่องมือหรือระบบที่ให้บริการข้อมูลของภัยคุกคามทางไซเบอร์ เช่น ลายเซ็นต์ดิจิตอลของไฟล์ที่อันตราย ที่อยู่ไอพีที่ไม่น่าเชื่อถือ หรือ ที่อยู่เว็บไซต์หลอกลวงต่าง ๆ เป็นต้น
DLP	Data Leak Prevention เครื่องมือหรือระบบที่ใช้ในการป้องกันข้อมูลสำคัญขององค์กรรั่วไหล ซึ่งเกิดจากการกำกับดูแลที่ไม่เพียงพอ หรือการใช้งานของผู้ใช้ที่ขาดความตระหนักรู้ Data Lost Protection เครื่องมือป้องกันข้อมูลสารสนเทศสูญหาย ที่เกิดจากการถูกขโมยข้อมูล ทำลายข้อมูล หรือการเข้ารหัสเพื่อเรียกค่าไถ่
IDS	Intrusion Detection System ระบบตรวจจับการโจมตีทางไซเบอร์
IPS	Intrusion Prevention System ระบบป้องกันการโจมตีทางไซเบอร์
EDR	End-point Detection and Response เครื่องมือหรือระบบที่ช่วยให้องค์กรสามารถตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นบนอุปกรณ์ปลายทาง เช่น แล็ปท็อป คอมพิวเตอร์เดสก์ท็อป เซิร์ฟเวอร์ และอุปกรณ์พกพา ต่าง ๆ
NAC	Network Access Control เครื่องมือควบคุมการเข้าถึงเครือข่าย ของอุปกรณ์ต่าง ๆ
PAM	Privilege Access Management เครื่องมือหรือระบบที่บริหารจัดการและควบคุมสิทธิ์ในการเข้าใช้งานระบบหรือเครื่องแม่ข่าย
PAS	Privilege Access Security เครื่องมือรักษาความปลอดภัยบัญชีผู้ใช้และควบคุมสิทธิ์การเข้าใช้งานระบบสารสนเทศหรือเครื่องแม่ข่าย
SDN	Software Defined Network ระบบเครือข่ายสารสนเทศ ที่สามารถบริหารจัดการด้วยซอฟต์แวร์จากส่วนกลาง สามารถสร้างเครือข่ายเสมือนใช้งานได้แบบพลวัต

SIEM	Security Information and Event Management ระบบที่ช่วยให้ผู้ปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สามารถเฝ้าระวังและตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยสามารถรวบรวม log จากเครื่องมือต่าง ๆ มาปรับแต่งเพื่อสามารถแสดงผลร่วมกันได้
SOAR	Security Orchestration Automation and Response ระบบที่ใช้สำหรับตอบสนองต่อเหตุการณ์ทางไซเบอร์ได้โดยอัตโนมัติ ผ่านการเขียนกระบวนการทำงานให้มีการสั่งการเครื่องมือต่าง ๆ ให้ทำงานประสานกันอย่างมีประสิทธิภาพ
UEBA	User and Entity Behavior Analytic เครื่องมือวิเคราะห์พฤติกรรมในเครือข่ายสารสนเทศของผู้ใช้หรืออุปกรณ์ต่าง ๆ เพื่อตรวจจับพฤติกรรมที่เป็นภัยคุกคาม
WAF	Web Application Firewall เครื่องมือหรือระบบที่ใช้ในการตรวจจับและป้องกันการโจมตีเว็บไซต์โดยเฉพาะ

เนื้อเรื่อง

๑. ที่มา

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ถูกท้าทายเพิ่มขึ้นอย่างมากในช่วงที่เกิดการแพร่ระบาดของเชื้อ Covid 19 ในห้วงปี พ.ศ.๒๕๖๓ - ๒๕๖๕ เนื่องจากในช่วงดังกล่าวบุคลากรของหน่วยงานหรือองค์กรต่าง ๆ ถูกกักตัวตามมาตรการป้องกันการแพร่ระบาดของเชื้อ Covid 19 ทำให้ต้องทำงานจากระยะไกลเพื่อใช้งานระบบสารสนเทศต่าง ๆ ของที่ทำงาน เป็นการเพิ่มช่องทางและโอกาสที่จะถูกโจมตีทางไซเบอร์เป็นอย่างมาก นักรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงได้นำสถาปัตยกรรม Zero Trust มาใช้ในการออกแบบและดำเนินการป้องกันทางไซเบอร์ ซึ่งตอบสนองต่อสถานการณ์ในห้วงนั้นได้เป็นอย่างดี จึงทำให้สถาปัตยกรรมการป้องกันทางไซเบอร์แบบ Zero Trust ได้รับการยอมรับและใช้งานอย่างแพร่หลายจนกลายเป็นมาตรฐานในระดับสากลจนถึงทุกวันนี้

ถึงแม้สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ Zero Trust จะได้รับการยอมรับอย่างแพร่หลายแต่การนำมาประยุกต์ใช้กับ ทอ.ยังต้องมีการปรับให้เข้ากับบริบท ข้อจำกัด ของ ทอ.ที่มีอยู่ด้วย สถาปัตยกรรม Zero Trust จึงจะได้ผลตามที่ควรจะเป็น ซึ่งปัจจุบัน ทอ.ยังไม่มีแนวทางในการปรับสถาปัตยกรรม Zero Trust มาใช้งานในการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเข้ากันได้กับแนวทางปฏิบัติที่ ทอ.ดำเนินอยู่ คือกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force : NCAF)

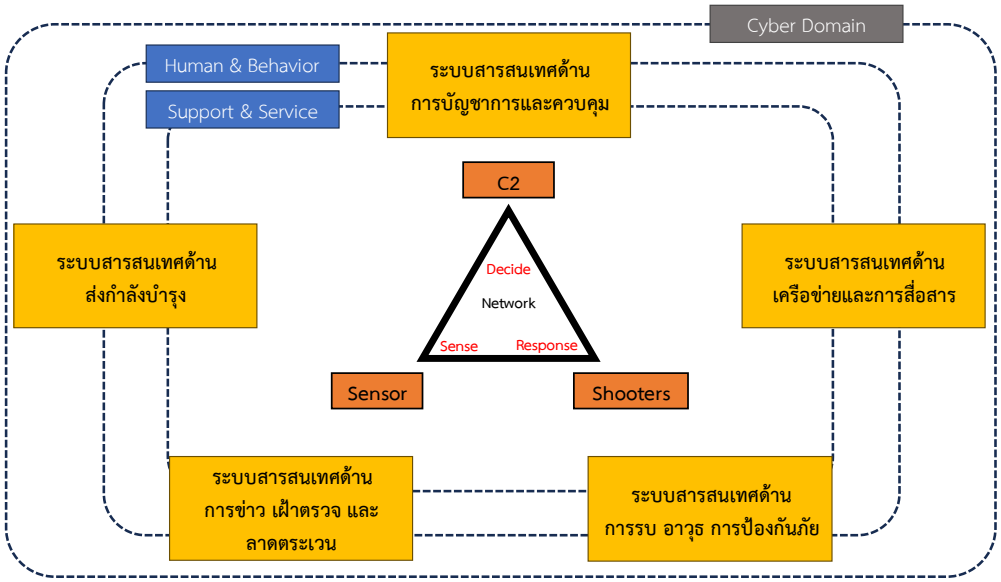
นอกจากนี้ในการดำเนินโครงการเสริมสร้างขีดความสามารถด้านไซเบอร์ของ ทอ. จะต้องมีการจัดหาหรือพัฒนาเครื่องมือรักษาความมั่นคงปลอดภัยทางไซเบอร์มาใช้งาน ซึ่งมีหลากหลายชนิด แต่ละชนิดก็ทำหน้าที่แตกต่างกันซึ่ง ทอ.ยังขาดแผนภาพที่จะช่วยบ่งบอกถึงความสัมพันธ์ของเครื่องมือกับสถาปัตยกรรม Zero Trust ซึ่งจะทำให้สามารถ ติดตาม ตรวจสอบ สถานะภาพโดยรวมของการดำเนินโครงการได้

จากเหตุผลข้างต้นจึงทำให้ ทอ.ควรมีแนวทางการพัฒนาสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ. ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force ขึ้นเพื่อใช้เป็นเครื่องมือในการดำเนินการพัฒนาขีดความสามารถการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทอ.

๒. แนวคิด Network Centric Air Force

แนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง หรือ Network Centric Air Force (NCAF) เป็นแนวคิดที่ ทอ.นำมาพัฒนาประยุกต์ใช้เป็นแนวคิดในการทำงานของ ทอ.ปรากฏอยู่ในยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) (ฉบับปรับปรุง พ.ศ.๒๕๖๓) ตามภาพที่ ๑ ซึ่งถูกขับเคลื่อนมาจากกระแสการเปลี่ยนแปลงทางเทคโนโลยี ที่มีการนำระบบสารสนเทศมาใช้งานและทำงานผ่านเครือข่าย เป็นผลทำให้การทำงานมีประสิทธิภาพ รวดเร็ว ถูกต้อง ช่วยให้การตัดสินตกลงใจทำได้อย่างรวดเร็ว สามารถรับรู้สถานการณ์ต่าง ๆ ได้อย่างทันทีทันใด หน่วยปฏิบัติก็สามารถรับคำสั่งไปปฏิบัติได้อย่างรวดเร็ว ทำให้วงรอบการตัดสินตกลงใจ (Observe, Orient, Decide and

Act : OODA) ทำได้อย่างรวดเร็ว ซึ่งเป็นปัจจัยสำคัญต่อความสำเร็จในการปฏิบัติภารกิจตามหลักนิยมของกองทัพอากาศ



ภาพที่ ๑ แนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force) ของ ทอ.[๑]

๒.๑ องค์ประกอบของ NCAF

NCAF จะมีแกนกลางเป็นขีดความสามารถในการปฏิบัติการทางอากาศของ ทอ.ซึ่งเป็นภารกิจหลักตามกฎหมาย โดยจะมีสามส่วนสำคัญคือ

๒.๑.๑ Network คือเครือข่ายที่เชื่อมโยงส่วนต่าง ๆ เข้าด้วยกันเพื่อให้สามารถ รับ-ส่งข้อมูลถึงกันได้อย่างรวดเร็ว

๒.๑.๒ Sensor คือหน่วยงานที่ทำหน้าที่ในการตรวจจับ เฝ้าระวัง และการข่าวของ ทอ.

๒.๑.๓ C2 คือส่วนบัญชาการและควบคุม เป็นส่วนที่รับข้อมูลข่าวสารต่าง ๆ จาก Sensor แล้วนำมากลั่นกรอง ตัดสินตกลงใจ แล้วจึงสั่งการไปที่ Shooters

๒.๑.๔ Shooters คือส่วนปฏิบัติ เป็นหน่วยที่มีชุดปฏิบัติการต่าง ๆ รองรับคำสั่งที่ C2 สั่งการมา

๒.๒ ระบบสารสนเทศใน NCAF

NCAF ใช้เครือข่ายในการประสานการปฏิบัติร่วมกัน นอกจากการปฏิบัติการทางอากาศแล้ว ก็ยังมีระบบสนับสนุนการปฏิบัติการ และมีกำลังพลของ ทอ.เป็นส่วนที่ขับเคลื่อนภารกิจ ในแง่ของระบบสารสนเทศแล้ว ยังแยกออกเป็นกลุ่ม ๆ ได้อีก ๕ กลุ่มคือ

๒.๒.๑ ระบบสารสนเทศด้านการบัญชาการและควบคุม

๒.๒.๒ ระบบสารสนเทศด้านการข่าวกรอง เฝ้าตรวจและลาดตระเวน

---

[๑] กรมยุทธการทหารอากาศ. (๒๕๖๓). “การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO)” ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) (ฉบับปรับปรุง พ.ศ.๒๕๖๓) พิมพ์ครั้งที่ ๑. กรุงเทพฯ : กรมยุทธการทหารอากาศ. หน้า ๓๔.

๒.๒.๓ ระบบสารสนเทศด้านการยุทธ และการป้องกันภัยทางอากาศ

๒.๒.๔ ระบบสารสนเทศด้านการส่งกำลังบำรุง

๒.๒.๕ ระบบสารสนเทศด้านเครือข่ายและการสื่อสาร

เนื่องจากแนวคิด NCAF นี้มีการเชื่อมโยงการปฏิบัติผ่านเครือข่ายทั้งเครือข่ายภายใน ทอ.และเครือข่ายอินเทอร์เน็ต ดังนั้นทุกภาคส่วนของ NCAF จึงอยู่ภายใต้มิติไซเบอร์ด้วย ทำให้แนวคิด NCAF ต้องมีการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเข้มแข็งและมีประสิทธิภาพ เหมาะสมกับแนวคิดและบริบทของ ทอ.

๓. หน่วยงานที่รับผิดชอบการปฏิบัติการไซเบอร์ของ ทอ.

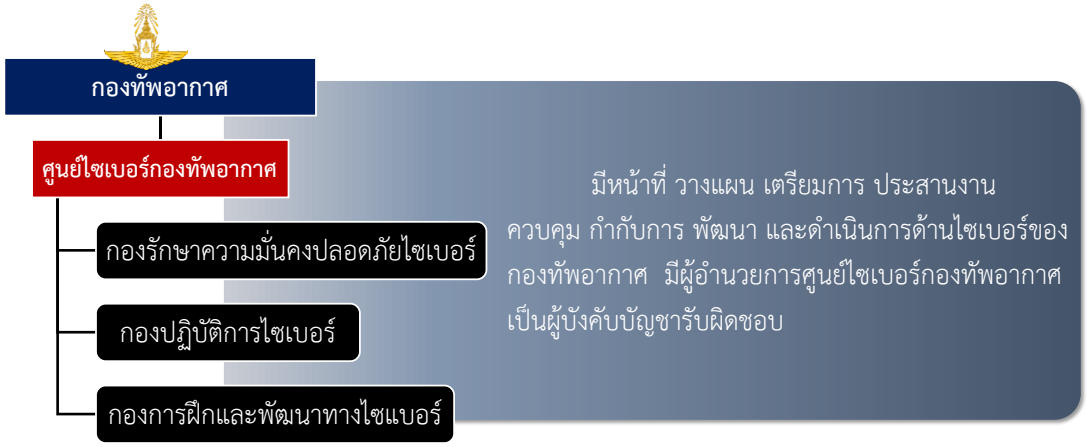
๓.๑ หน่วยตามโครงสร้างเตรียมกำลัง

ทอ.ได้ตั้ง ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) ขึ้นมาเมื่อ ๑ ต.ค.๖๓ เพื่อเป็นหน่วยงานที่รับผิดชอบภารกิจทางไซเบอร์ทั้งปวงของ ทอ.ในโครงสร้างเตรียมกำลัง ตามภาพที่ ๒ โดยมีหน่วยขึ้นตรงหลักประกอบด้วย

๓.๑.๑ กองรักษาความมั่นคงปลอดภัยไซเบอร์ (กรซ.ศซบ.ทอ.) รับผิดชอบภารกิจด้านการป้องกันทางไซเบอร์ของ ทอ.

๓.๑.๒ กองปฏิบัติการไซเบอร์ (กปซ.ศซบ.ทอ.) รับผิดชอบภารกิจด้านการป้องปรามและการข่าวกรองเฝ้าตรวจและลาดตระเวนของ ทอ.

๓.๑.๓ กองการฝึกและพัฒนาทางไซเบอร์ รับผิดชอบการฝึกและพัฒนากำลังพลทางไซเบอร์ รวมถึงการสนับสนุนการปฏิบัติการทางไซเบอร์



ภาพที่ ๒ โครงสร้างและภารกิจของ ศซบ.ทอ.

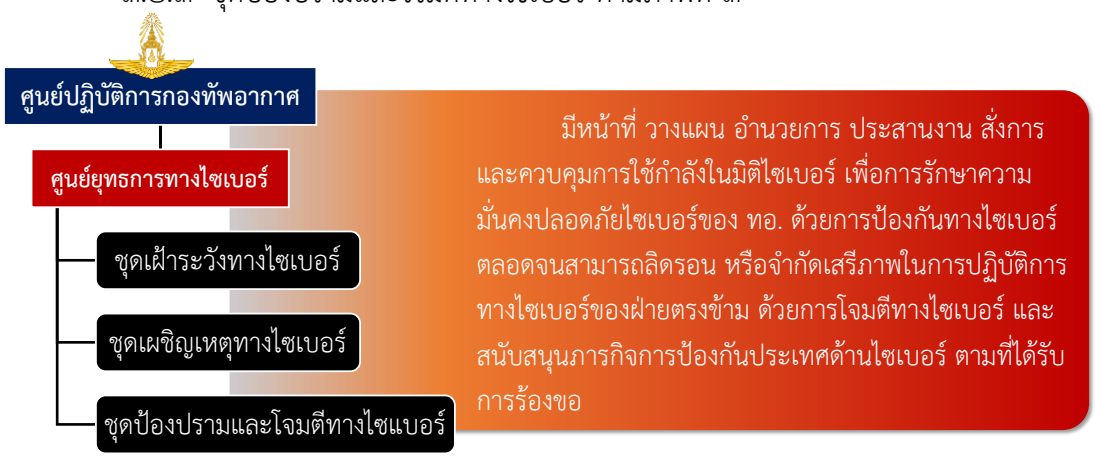
๓.๒ หน่วยตามโครงสร้างใช้กำลัง

ศซบ.ทอ. ยังกำกับดูแล จัดการ หน่วยงานในโครงสร้างใช้กำลังคือ ศูนย์ยุทธการทางไซเบอร์ ศูนย์ปฏิบัติการกองทัพอากาศ (ศยซบ.ศปก.ทอ.) มีชุดปฏิบัติการประกอบด้วย

๓.๒.๑ ชุดเฝ้าระวังทางไซเบอร์

๓.๒.๒ ชุดเผชิญเหตุทางไซเบอร์

๓.๒.๓ ชุดป้องปรามและโจมตีทางไซเบอร์ ตามภาพที่ ๓



ภาพที่ ๓ โครงสร้างและภารกิจของ ศยซบ.ศปก.ทอ.

๓.๓ หน่วยงานที่ต้องร่วมมือในการรักษาความมั่นคงปลอดภัยไซเบอร์

นอกจาก ศซบ.ทอ. หรือ ศยซบ.ศปก.ทอ. แล้ว ยังมีหน่วยงานอื่น ๆ ทั้งใน ทอ.และนอก ทอ.ที่จะต้องร่วมมือกันในการปฏิบัติภารกิจรักษาความมั่นคงปลอดภัยไซเบอร์ด้วยดังนี้

๓.๓.๑ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ทำหน้าที่เป็นฝ่ายอำนวยการด้านเทคโนโลยีสารสนเทศและการสื่อสารรวมถึงด้านไซเบอร์ของ ทอ.เป็นหน่วยกำหนดนโยบายต่าง ๆ ทางไซเบอร์ กำกับดูแลให้เป็นไปตามระเบียบต่าง ๆ ทางไซเบอร์ อีกทั้งยังเป็นฝ่ายเสนาธิการด้านไซเบอร์ให้กับผู้บังคับบัญชาของ ทอ.ด้วย

๓.๓.๒ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) เป็นหน่วยงานที่รับผิดชอบโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศของ ทอ. เช่น เครือข่ายสารสนเทศ การเชื่อมต่ออินเทอร์เน็ต การเชื่อมต่อเครือข่ายไร้สาย (Wi-Fi) การให้บริการเครื่องแม่ข่ายสำหรับระบบสารสนเทศของหน่วยต่าง ๆ ของ ทอ.

๓.๓.๓ หน่วยเจ้าของระบบเทคโนโลยีสารสนเทศ เป็นหน่วยที่จัดหาหรือพัฒนาระบบเทคโนโลยีสารสนเทศขึ้นมาใช้งานภายใต้กรอบแนวคิด NCAF โดยทำหน้าที่เป็นผู้ดูแลระบบเทคโนโลยีสารสนเทศนั้น ๆ ควบคุมสิทธิ์และกลุ่มผู้ใช้งานของระบบ การสำรองข้อมูลระบบ ฯลฯ

๓.๓.๔ หน่วยงานกำกับดูแลตามกฎหมาย พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้แก่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ ศูนย์ไซเบอร์ กรมเทคโนโลยีสารสนเทศและอวกาศกลาโหม (ศซบ.ทสอ.กห.)

๓.๓.๕ หน่วยงานทางด้านไซเบอร์อื่น ๆ ภายนอก ทอ. เช่น ศูนย์ไซเบอร์ภายใต้กระทรวงกลาโหม ได้แก่ ศูนย์ไซเบอร์ กองบัญชาการกองทัพไทย (ศซบ.ทท.) ศูนย์ไซเบอร์กองทัพบก (ศซบ.ทบ.) และ ศูนย์ไซเบอร์ กรมการสื่อสารและเทคโนโลยีสารสนเทศทหารเรือ (ศซบ.สสท.ทร.) หน่วยงานด้านไซเบอร์ขององค์กรภาครัฐ รัฐวิสาหกิจ หรือเอกชน เพื่อประสานความร่วมมือในการรับมือกับภัยคุกคามทางไซเบอร์ของประเทศ

๔. สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ Zero Trust

หลังจากที่ ทอ. ได้ใช้แนวคิด NCAF เพื่อเพิ่มประสิทธิภาพในการปฏิบัติภารกิจ ทำให้สามารถเชื่อมโยงข้อมูล ประสานการทำงานผ่านเครือข่ายได้อย่างรวดเร็ว มีเอกภาพ แต่ก็มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์อย่างหลีกเลี่ยงไม่ได้ ทอ.เองจำเป็นต้องมีการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ แต่ก็ต้องเข้ากันได้กับแนวคิด NCAF อีกทั้งยังต้องเหมาะสมกับบริบทของ ทอ.อีกด้วย ทอ.จึงจำเป็นต้องมีการประยุกต์ใช้สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ได้รับการยอมรับ เป็นสถาปัตยกรรมที่เข้ากันได้กับกระแสการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศของโลก

สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ Zero-Trust เป็นสถาปัตยกรรมที่ถูกพัฒนาขึ้นมาบนหลักความคิดที่ว่า ไม่มีส่วนใด ๆ ในมิติไซเบอร์ที่จะสามารถเชื่อมั่นในความปลอดภัยได้อย่างสมบูรณ์ ซึ่งเป็นที่มาของคำว่า Zero-Trust (ความเชื่อมั่นเท่ากับ 0 หรือไม่เชื่อมั่นอะไรเลย) โดยถูกนำไปใช้ในการเชื่อมต่อจากระยะไกลเพื่อเข้าใช้งานเครือข่ายภายในองค์กรก่อน ซึ่งมีการใช้งานและได้รับการยอมรับจนเป็นพื้นฐานสำคัญที่ขาดไม่ได้ ในห้วงที่มีการแพร่ระบาดของไวรัส Covid-19 ทั่วโลกมีการปรับพฤติกรรมการทำงานมาใช้การทำงานนอกสถานที่ในห้วงที่ทุกคนต้องปฏิบัติตามมาตรการกักตัวเพื่อป้องกันการแพร่ระบาดของ Covid-19 ความต้องการมาตรการหรือสถาปัตยกรรมในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ถูกยกระดับและพัฒนาขึ้น มีการผนวกรวมส่วนอื่น ๆ ในมิติไซเบอร์เข้าไปในสถาปัตยกรรม ทำให้ได้สถาปัตยกรรม Zero-Trust ที่ครอบคลุมและสมบูรณ์มากยิ่งขึ้น ไม่เฉพาะเจาะจงที่การเชื่อมต่อเครือข่ายเหมือนในยุคแรกอีกต่อไป

๔.๑ หลักการของ Zero Trust

Zero Trust เป็นกรอบและแนวทางด้านความปลอดภัยที่เน้นการควบคุมการเข้าถึงที่เข้มงวด และการตรวจสอบผู้ใช้และอุปกรณ์ที่พยายามเข้าถึงทรัพยากรภายในเครือข่ายหรือระบบสารสนเทศอย่างต่อเนื่อง หลักการสำคัญของ Zero Trust ได้แก่

๔.๑.๑ ยืนยันก่อนเชื่อถือ : คำขอเข้าถึงทุกรายการจะได้รับการตรวจสอบสิทธิ์และอนุญาตอย่างละเอียดก่อนที่จะให้สิทธิ์การเข้าถึง

๔.๑.๒ การเข้าถึงสิทธิ์น้อยที่สุด : ผู้ใช้และอุปกรณ์จะได้รับสิทธิ์เข้าถึงขั้นต่ำที่จำเป็นในการทำงานที่ต้องการเท่านั้น จะไม่มีการให้สิทธิ์แบบเปิดกว้างแบบเก่าอีก

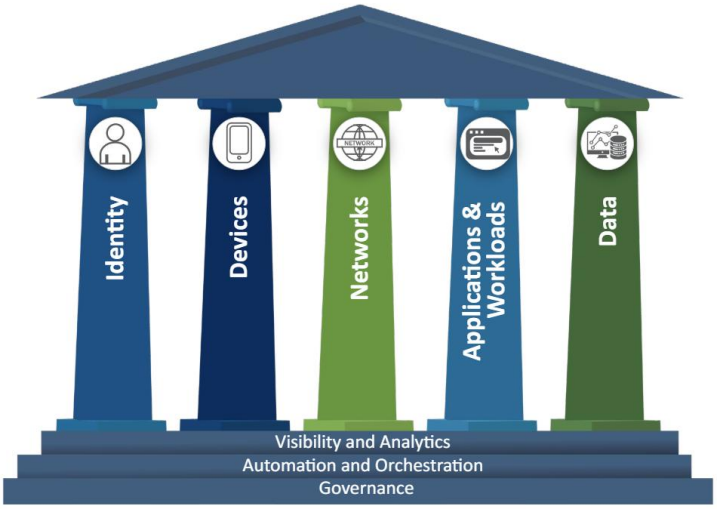
๔.๑.๓ การตรวจสอบสิทธิ์อย่างต่อเนื่อง : มีการตรวจสอบและวิเคราะห์พฤติกรรมของการรับส่งข้อมูลเครือข่ายและรูปแบบการเข้าถึงเพื่อตรวจจับและตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นแบบทันที

๔.๑.๔ การแบ่งส่วนย่อย : เครือข่ายและทรัพยากรแบ่งออกเป็นส่วนเล็ก ๆ และการเข้าถึงระหว่างส่วนย่อยเหล่านี้ได้รับการควบคุมอย่างเข้มงวด ไม่สามารถเข้าถึงส่วนย่อยอื่น ๆ ที่ไม่มีสิทธิ์ได้ ซึ่งช่วยป้องกันการโจมตีภายในเพิ่มเติมของแฮกเกอร์ได้

๔.๑.๕ การควบคุมการเข้าถึงแบบพลวัต : การควบคุมการเข้าถึงได้รับการดัดแปลงและปรับเปลี่ยนตามข้อมูลบริบท เช่น ตำแหน่งของผู้ใช้ ความสมบูรณ์ของอุปกรณ์ และพฤติกรรม เป็นต้น แบบทันทีอย่างต่อเนื่องตลอดเวลา

๔.๒ องค์ประกอบของ Zero Trust

สถาปัตยกรรม Zero Trust ที่เป็นที่ยอมรับในระดับสากลนั้นมีหลากหลายสถาปัตยกรรม ในบทความนี้ขอใช้สถาปัตยกรรม Zero Trust ของ หน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน (CISA) ของสหรัฐอเมริกาเนื่องจากมีความกระชับสามารถทำความเข้าใจได้ง่ายซึ่งมีการจัดเสาหลัก (Pillars) และการจัดการดังแสดงในภาพที่ ๔



ภาพที่ ๔ สถาปัตยกรรม Zero-Trust ของ CISA[๑]

ที่มา : Zero Trust Maturity Model ของ หน่วยงานรักษาความปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน (CISA)

๔.๒.๑ เสาหลักของ Zero Trust ประกอบด้วย

๔.๒.๑.๑ Identity หรือ ตัวตนทางไซเบอร์ เป็นตัวตนที่ใช้ในการติดต่อ เข้าถึงระหว่างกันของอุปกรณ์ หรือระบบสารสนเทศต่าง ๆ โดยหมายถึงตัวตนของผู้ใช้งานและตัวตนอื่น ๆ ด้วย ในเสานี้จะต้องมีขีดความสามารถในการยืนยันตัวตนก่อนเข้าถึงเครือข่าย การยืนยันระดับสิทธิ์ของการใช้งาน และการบริหารจัดการตัวตนและสิทธิ์การใช้งานเหล่านั้น

๔.๒.๑.๒ Devices หรือ อุปกรณ์ คืออุปกรณ์ที่ใช้ในการเชื่อมต่อหรือเข้าถึงเครือข่ายหรือระบบสารสนเทศ โดยรวมทั้งอุปกรณ์ประจำตัวของผู้ใช้งาน และอุปกรณ์สำนักงาน เช่น เครื่องพิมพ์ กล้องวงจรปิด เป็นต้น ในเสานี้จะต้องมีความสามารถในการอนุมัติการเข้าถึงของอุปกรณ์ การควบคุมระดับสิทธิ์การเข้าถึงอิงจากอุปกรณ์ที่ใช้งาน และการบริการจัดการการเข้าถึงและสิทธิ์เหล่านั้น

๔.๒.๑.๓ Networks หรือ เครือข่าย เป็นเสาที่เป็นเสมือนเส้นทางสำหรับใช้สัญจรในมิติไซเบอร์ ซึ่งมีการแบ่งแยกขอบเขตตามเลขหมายไอพี สามารถกำจัดการเข้าถึงในแต่ละขอบเขตของเลขไอพีได้ผ่านทางอุปกรณ์บริหารจัดการเครือข่ายหรือซอฟต์แวร์บริหารจัดการเครือข่าย (Software Defined Network) ในเสานี้จะต้องมีขีดความสามารถในการป้องกันการเข้าถึงเครือข่าย

---

[๑] Cybersecurity and Infrastructure Security Agency. (2023). “Zero Trust Maturity Model” Version 2.0. April 2023. Page 7.

โดยไม่ได้รับอนุญาต สามารถแบ่งแยกเป็นเครือข่ายขนาดเล็กมาก ๆ ตามสิทธิ์การใช้งานที่เฉพาะเจาะจง

๔.๒.๑.๔ Applications & Workloads หรือแอพพลิเคชันและส่วนที่แบกรับการทำงานของแอพพลิเคชัน ในบริบทที่ไม่ใช้คลาวด์ (Cloud) จะเป็นเครื่องแม่ข่าย ทั้งแบบทางกายภาพและแบบเสมือน ในเสานี้จะมีการควบคุมการเข้าถึงผ่านบัญชีผู้ใช้งานของแอพพลิเคชัน และอาจจะมีการยืนยันตัวตนแบบหลายเงื่อนไข (Multi-Factor Authentication) ร่วมด้วย ในเสานี้จะต้องมีขีดความสามารถในการกำหนดขีดความสามารถในการประมวลผลของแอพพลิเคชันได้ตามสิทธิ์ของผู้ใช้ มีการพัฒนาที่ปลอดภัยไม่มีช่องโหว่ให้ผู้ไม่หวังดีหลบหลีกกลไกการรักษาความมั่นคงปลอดภัย และยังต้องสามารถสร้างช่องทางใช้งาน (Tunneling) ร่วมกับเสา Networks ได้ด้วย

๔.๒.๑.๕ Data หรือ ข้อมูล ในเสานี้จะหมายถึงข้อมูลของแอพพลิเคชันใช้งานหรือข้อมูลที่องค์กร มีการใช้งานโดยมีการกำหนดสิทธิ์ในการใช้งานผ่านบัญชีผู้ใช้ โดยบัญชีผู้ใช้แต่ละบัญชีจะมีระดับสิทธิ์สูง-ต่ำ ไม่เท่ากัน จึงทำให้การเข้าถึงข้อมูลในแต่ละส่วนไม่เท่ากัน ในเสานี้จะต้องมีขีดความสามารถในการกำหนดพื้นที่จัดเก็บข้อมูลที่ควบคุมด้วยซอฟต์แวร์เพื่อให้สามารถบริหารจัดการได้ง่ายและรองรับการตอบสนองอัตโนมัติ และควรมีการจัดทำดัชนีอย่างต่อเนื่อง

๔.๒.๒ การจัดการของ Zero Trust

ทั้ง ๕ เสาหลัก จะต้องมีการจัดการในภาพรวมซึ่งมี ๓ ส่วนดังนี้

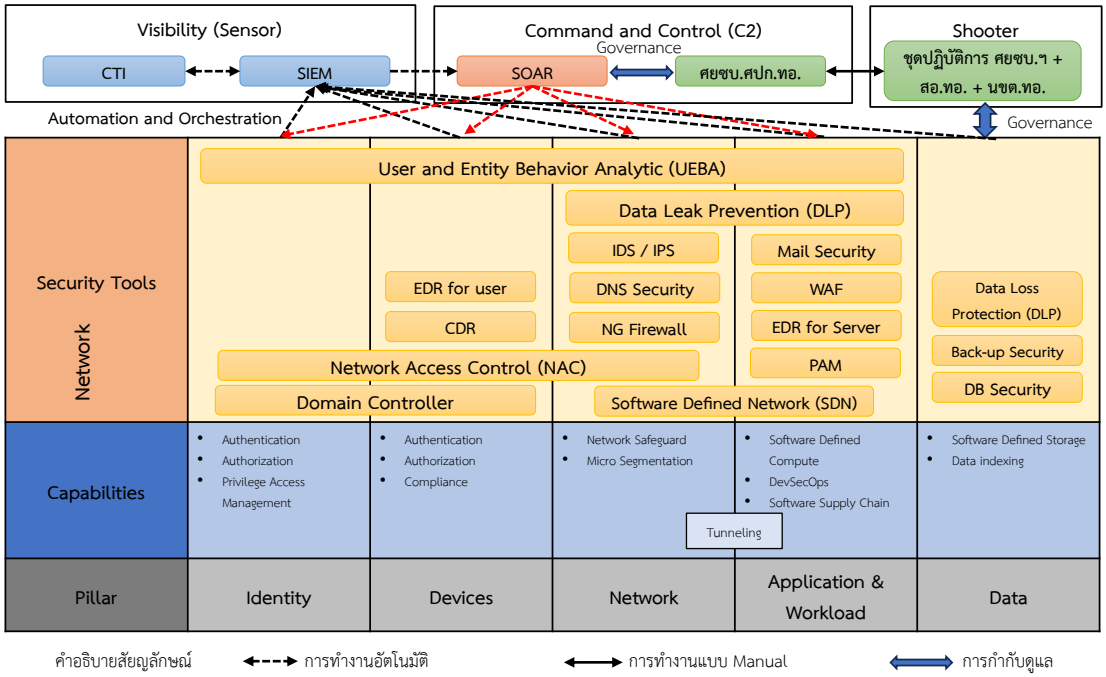
๔.๒.๒.๑ Visibility and Analytics หรือ ความสามารถในการมองเห็นและการวิเคราะห์ ในส่วนนี้องค์กรจะต้องจัดการให้สามารถมองเห็นกิจกรรมที่เกิดขึ้นในแต่เสาหลัก แล้วทำการวิเคราะห์พฤติกรรมในภาพรวมของทั้งองค์ ไม่ใช่เฉพาะเสาใดเสาหนึ่ง เช่น จะต้องเห็นและวิเคราะห์พฤติกรรมของผู้ใช้งานได้ตั้งแต่การใช้อุปกรณ์ใดในการเข้าถึงเครือข่ายด้วยบัญชีผู้ใช้ใด มีการเข้าถึงเครือข่ายในส่วนไหนบ้าง มีการเข้าถึงแอพพลิเคชันใดบ้าง และเข้าถึงข้อมูลใดไปแล้วบ้าง เข้ามูลเหล่านี้จะต้องมีการสานสัมพันธ์เป็นเนื้อเดียวกันในส่วนนี้ ข้อดีที่เห็นได้ชัดของส่วนนี้คือจะทำให้สามารถตรวจจับภัยคุกคามทางไซเบอร์ได้อย่างแม่นยำ ลดการตรวจจับผิดพลาด และยังสามารถยับยั้งการโจมตีแบบ 0-Day หรือการโจมตีที่ยังไม่เป็นที่รู้จักได้อีกด้วย

๔.๒.๒.๒ Automation and Orchestration หรือ การดำเนินการอัตโนมัติอย่างเหมาะสมลงตัว ในส่วนนี้เป็นการจัดการภายหลังจากที่ตรวจจับภัยคุกคามได้จากส่วนก่อนหน้านี้ โดยที่สถาปัตยกรรมจะต้องมีการตอบสนองภัยคุกคามเหล่านั้นอย่างอัตโนมัติและมีความเหมาะสมลงตัว กล่าวคือ ในการตอบสนองนั้น จะต้องมีการสั่งการกลับไปยังเครื่องมือด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ ที่องค์กรมี เครื่องมือเหล่านั้นจะต้องมีการตอบสนองตามลำดับก่อน-หลังอย่างเหมาะสมลงตัว การตอบสนองจึงจะได้ผลและมีประสิทธิภาพ

๔.๒.๒.๓ Governance หรือ การกำกับดูแล เป็นส่วนที่ผู้ใช้งานหรือผู้ดูแลระบบหรือผู้กำกับดูแลในภาพรวมของสถาปัตยกรรม จะเข้ามาตรวจสอบ ตั้งค่า ปรับปรุงประสิทธิภาพ การทำงานใน สองส่วนก่อนหน้านี้

๕. สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ. ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force

ในการนำสถาปัตยกรรม Zero Trust มาใช้งานใน ทอ. จึงควรมีการปรับสถาปัตยกรรมให้เข้ากับบริบทของ ทอ.โดยเฉพาะอย่างยิ่งแนวคิดการปฏิบัติงานที่ใช้เครือข่ายเป็นศูนย์กลางหรือ NCAF เสียก่อน จึงได้สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force ตามภาพที่ ๕



ภาพที่ ๕ สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force

๕.๑ อธิบายสถาปัตยกรรม ฯ

ในส่วนของ Network ตาม NCAF จะเทียบเคียงกับทั้ง ๕ เสาหลักของ Zero Trust ในสถาปัตยกรรมนี้ จะมีการจัดเครื่องมือหรือระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่าง ๆ ลงไปในแต่ละเสาหลักอิงตามขีดความสามารถที่ต้องการในแต่ละเสา

ในส่วนของ Sensor ตาม NCAF จะเทียบเคียงกับการจัดการ Visibility and Analytics จะใช้เครื่องมือ Security Information and Events Management (SIEM) ซึ่งทำงานร่วมกับ Cyber Threat Intelligence (CTI) เครื่องมือต่าง ๆ ที่อยู่ในแต่ละเสาหลัก จะส่งข้อมูลการทำงานไปที่ระบบ SIEM เพื่อให้เห็นสถานการณ์ในภาพรวม แล้วทำการตรวจจับโดยตรวจสอบข้อมูลร่วมกับ CTI ให้เกิดความแม่นยำและรวดเร็ว

ในส่วนของ C2 ตาม NCAF จะใช้เครื่องมือ Security Orchestration Automation and Response (SOAR) ในการบัญชาการตอบสนองเหตุการณ์โดยอัตโนมัติอย่างเหมาะสมลงตัว ซึ่งตรงกับการจัดการ Automation and Orchestration ของ Zero Trust ในส่วนนี้ SOAR จะรับ

ข้อมูลการโจมตีมาจาก SIEM แล้วทำการสั่งการตอบสนองอัตโนมัติกลับไปยังเครื่องมือต่าง ๆ ในแต่ละเสาอย่างเหมาะสมลงตัว

ในส่วนของ Shooters ตาม NCAF จะแยกเป็น ๒ มิติ ในมิติไซเบอร์จะเป็นเครื่องมือการรักษาความมั่นคงปลอดภัยไซเบอร์ต่าง ๆ ที่อยู่ในแต่ละเสาหลัก ที่รับคำสั่งมาจาก SOAR ในมิติกายภาพ จะมีชุดปฏิบัติการของ ศยซบ.ศปก.ทอ. ทำการตอบสนองเหตุการณ์ ร่วมกับ สอ.ทอ. และ นขต.ทอ. เจ้าของระบบที่ได้รับผลกระทบ นอกจากนี้ ชุดปฏิบัติการของ ศยซบ.ศปก.ทอ. ยังทำหน้าที่กำกับดูแลการทำงานของ SOAR ซึ่งสอดคล้องกับการจัดการ Governance ของ Zero Trust

๕.๒ ประโยชน์ของสถาปัตยกรรม ฯ

๔.๒.๑ ช่วยให้การนำ Zero Trust มาประยุกต์ใช้ใน ทอ.มีความกระชับ เข้ากันได้กับแนวคิด NCAF

๔.๒.๒ ช่วยให้สามารถดำเนินการได้อย่างรวดเร็วเนื่องจาก ทอ.มีความคุ้นชินกับแนวคิด NCAF อยู่ก่อนแล้ว เพียงแค่ทำความเข้าใจเครื่องมือที่ต้องใช้ก็สามารถดึงประโยชน์ของ Zero Trust มาใช้ได้อย่างเต็มประสิทธิภาพ

๔.๒.๓ ใช้เป็นแนวทางในการดำเนินโครงการพัฒนาขีดความสามารถการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ ทอ.และช่วยในการสื่อสารทำความเข้าใจกับหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการจัดทำโครงการ

๔.๒.๔ ช่วยให้การพัฒนาขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.มีมาตรฐาน เป็นที่ยอมรับในระดับสากล

๕.๓ แนวทางการพัฒนาในอนาคต

ด้วยความก้าวหน้าด้านปัญญาประดิษฐ์เชิงสรรค์สร้าง (Generative AI : Gen-AI) หรือโมเดลภาษาขนาดใหญ่ (Large Language Model : LLM) ทำให้เทคโนโลยีสามารถเข้ามาช่วยงานคนในระดับที่สูงขึ้นได้อย่างมาก ซึ่ง ทอ.เองก็ประสบปัญหาขาดแคลนบุคลากรที่จะปฏิบัติหน้าที่ในศูนย์ยุทธการทางไซเบอร์ ฯ การนำ AI มาใช้ร่วมกับสถาปัตยกรรมนี้ จะช่วยแก้ปัญหานี้ของ ทอ.ได้

หน้านี้ตั้งใจเว้นว่างไว้

บรรณานุกรม

กรมยุทธการทหารอากาศ. (๒๕๖๓) ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๑ - ๒๕๘๐) (ฉบับปรับปรุง พ.ศ.๒๕๖๓). กรมยุทธการทหารอากาศ. กรุงเทพมหานคร.

Rose, S. & Borchert, O. & Mitchell, S. & Connelly, S (2020). Zero Trust Architecture. NIST Special Publication 800-207. https://doi.org/10.6028/NIST.SP.800-207.

Badhwar, R. (2022). The CISO Guide to Zero Trust Security.

Garbis, J & Chapman, W. J. (2021) Zero Trust Security: An Enterprise Guide. Apress.

Department of Defense. (2022). Zero Trust Reference Architecture. [Accessed: March 22, 2024]. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf.

Cybersecurity Division, CISA. (2023). Zero Trust Maturity Model [Accessed: March 10, 2024]. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

หน้านี้ตั้งใจเว้นว่างไว้

ภาคผนวก

ชื่อผู้แต่ง	นาวาอากาศเอก เอกชัย สิงห์ทอง
คุณวุฒิ	วิทยาศาสตรบัณฑิต (ทอ.) (วิทยาการคอมพิวเตอร์) โรงเรียนนายเรืออากาศ
ตำแหน่ง	นายทหารฝ่ายเสนาธิการประจำกอง กองรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ
หมายเลขโทรศัพท์	๐๖ ๔๒๙๕ ๕๕๕๓

ผนวก ง

ประกอบระเบียบกองทัพอากาศว่าด้วยการให้รางวัลผลงานประดิษฐ์คิดค้นและบทความทางวิชาการ พ.ศ.๒๕๖๔

การสรุปสาระสำคัญของบทความทางวิชาการและบทความทางวิชาการที่แปลมาจากภาษาต่างประเทศ

๑. ชื่อของบทความทางวิชาการ

ภาษาไทย สถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ. ที่สอดคล้องกับ Zero Trust และ Network Centric Air Force

ภาษาอังกฤษ (ถ้ามี) -

๒. ประเภทของผลงาน

☑ บทความทางวิชาการ

☐ บทความทางวิชาการที่แปลมาจากภาษาต่างประเทศ

๓. รายชื่อผู้เขียน/แปลบทความ และผู้ร่วมงาน

ยศ-ชื่อ-สกุล น.อ.เอกชัย สิงห์ทอง ตำแหน่ง ฝสธ.กรซ.ศซบ.ทอ. สังกัด ศซบ.ทอ.

๔. บทความนี้เกี่ยวข้องกับสายวิทยาการใด

สายวิทยาการ เทคโนโลยีสารสนเทศ (ไซเบอร์)

๕. ให้ระบุข้อมูลของสาระสำคัญโดยย่อดังต่อไปนี้

๕.๑ ที่มาหรือแรงจูงใจที่ทำให้เกิดความคิดในการเขียน-แปลบทความทางวิชาการ ทอ.ยังขาดสถาปัตยกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมกับบริบทและหลักนิยมของ ทอ.

๕.๒ ระยะเวลาในการเขียน/แปล ตั้งแต่ ม.ค.๖๗ ถึง เม.ย.๖๗ รวมใช้เวลา ๐ ปี ๔ เดือน

๕.๓ ลักษณะของบทความทางวิชาการ / แปลบทความ

☑ เป็นผลงานที่เขียนขึ้นโดยใช้ความรู้และประสบการณ์

☑ เป็นผลงานที่ได้รวบรวมและเรียบเรียงขึ้น

☐ เป็นผลงานที่ได้แปลขึ้น

๕.๔ เคยได้รับรางวัลอันดับที่.....จาก.....

☐ เป็นเงินรางวัล จำนวน.....บาท เมื่อ.....

☐ เป็นของรางวัล.....(ระบุประเภท) เมื่อ.....

๕.๕ กองทัพอากาศได้รับประโยชน์และผลกระทบจากผลงานนี้อย่างไร นำสถาปัตยกรรมนี้ไปใช้เป็นแนวทางในการดำเนินการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของ ทอ.

๕.๖ มีการรับรองผลงานไปใช้ประโยชน์หรือไม่

☑ ไม่มี

☐ มี รายละเอียดตามเอกสารอ้างอิงที่แนบ จำนวน.....แผ่น

๕.๗ งบประมาณที่ใช้ในการจัดทำ

☐ จำนวนเงิน .....บาท

☐ แหล่งที่ได้รับงบประมาณ .....

๕.๘ มีการเผยแพร่ผลงานนี้หรือไม่

☐ ไม่มี

☑ มี โดยวิธี เผยแพร่ออนไลน์ ที่ใด เว็บไซต์ ศซบ.ทอ. เมื่อ พ.ค.๖๗

๕.๙ อื่น ๆ (ถ้ามี) .....

หน้านี้ตั้งใจเว้นว่างไว้