ระเบียบกองทัพบก
ว่าด้วย การกำหนดมาตรฐานอุปกรณ์และระบบภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๓

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของกองทัพบกเป็นไปด้วยความเรียบร้อย มีประสิทธิภาพ เป็นมาตรฐานในการกำหนดประเภทเครือข่ายสื่อสารข้อมูลที่ใช้งานในกองทัพบก ข้อมูล แนวทางการรักษาและเสริมสร้างความแข็งแกร่งในการรักษาความมั่นคงทางปลอดภัย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า “ระเบียบกองทัพบก ว่าด้วยการกำหนดมาตรฐานอุปกรณ์และระบบภายในศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๓”

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ บรรดาระเบียบและคำสั่งอื่นใดในส่วนที่กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน โดยยึดถือภายใต้ กรอบนโยบายด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศกระทรวงกลาโหม และระเบียบกองทัพบก ว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพบก (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ ที่ได้ประกาศขึ้น

ข้อ ๔ ระเบียบนี้ให้ใช้บังคับแก่ส่วนราชการในสังกัดกองทัพบก

ข้อ ๕ คำจำกัดความในระเบียบนี้

๕.๑ เครือข่ายสื่อสารข้อมูล (Network) หมายถึง กลุ่มของคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่าง ๆ ที่นำมาเชื่อมต่อกันเพื่อให้ผู้ใช้ในเครือข่าย สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และใช้อุปกรณ์ต่าง ๆ ร่วมกันในเครือข่ายได้

๕.๒ ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) หมายถึง ข้อมูลที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ แสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

๕.๓ ระบบเครือข่ายเสมือนส่วนตัว (Virtual Private Network : VPN) หมายถึง เทคโนโลยีการเชื่อมต่อครือข่ายเพื่อสร้างช่องทางส่วนตัวเฉพาะเชื่อมต่อกันระหว่าง ๒ หน่วยงาน ผ่านเครือข่ายสาธารณะ แต่ยังสามารถคงความเป็นเครือข่ายเฉพาะขององค์กรได้ด้วยการเข้ารหัสแพ็กเก็ตก่อนส่งเพื่อให้ข้อมูลมีความปลอดภัยมากขึ้น

๕.๔ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) หมายถึง เครื่องมือที่ใช้ในการป้องกันเครือข่ายคอมพิวเตอร์จากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต

/๕.๕ ระบบบริหาร...

๕.๕ ระบบบริหารจัดการข้อมูลและเหตุการณ์ทางด้านความมั่นคงปลอดภัย (Security Information and Event Management : SIEM) หมายถึง ระบบที่ทำหน้าที่รวบรวมและจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (log) จากอุปกรณ์ต่าง ๆ นำมาวิเคราะห์หาความสัมพันธ์ แนวโน้มของข้อมูล log เพื่อค้นหาต้นตอและเป้าประสงค์ของการโจมตีรูปแบบต่างๆ ได้ทั้งแบบ Real-time และการตรวจสอบย้อนหลัง รวมทั้งสามารถบริหารจัดการภัยคุกคาม (Incident Management) ได้

๕.๖ ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Operation Center : CSOC) หมายถึง ศูนย์กลางในการเฝ้าระวังและรับมือภัยคุกคามทางไซเบอร์ของหน่วย รับผิดชอบในการ ติดตาม เฝ้าระวัง ตรวจสอบ วิเคราะห์เหตุการณ์ และภัยคุกคามทางไซเบอร์

๕.๗ ส่วนเฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ (ระดับที่ ๑ หรือ Tier 1) หมายถึง ส่วนเฝ้าระวังและแจ้งเตือนภัยคุกคามอย่างต่อเนื่อง ตรวจสอบความพร้อมของอุปกรณ์รักษาความมั่นคงปลอดภัยไซเบอร์ ตรวจสอบและรวบรวมข้อมูลภัยคุกคามในเบื้องต้นและประสานไปยัง ส่วนเผชิญเหตุภัยคุกคามทางไซเบอร์ (Tier 2)

๕.๘ ส่วนเผชิญเหตุภัยคุกคามทางไซเบอร์ (ระดับที่ ๒ หรือ Tier 2) หมายถึง ส่วนวิเคราะห์ภัยคุกคามเชิงลึก หาความสัมพันธ์ของข้อมูลที่เกี่ยวกับการโจมตีที่ได้รับจากแหล่งต่าง ๆ ประเมินผลกระทบของระบบและข้อมูลสำคัญ รวมถึงอัปเดตระบบอย่างต่อเนื่องเพื่อให้สามารถตรวจจับภัยคุกคามใหม่ได้อย่างมีประสิทธิภาพ

๕.๙ ส่วนงานความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (ระดับ ๓ หรือ Tier 3) หมายถึง ส่วนงานของกำลังพลกองทัพบกที่มีความเชี่ยวชาญในด้านต่าง ๆ เช่น เครือข่าย การตรวจพิสูจน์พยานหลักฐานดิจิทัล การวิเคราะห์มัลแวร์ หรือเชี่ยวชาญเกี่ยวกับซอฟต์แวร์หรือระบบเฉพาะที่ใช้ในหน่วยงาน

หมวด ๑ การแบ่งประเภทเครือข่ายและระดับการรักษาความมั่นคงปลอดภัย

ข้อ ๖ ประเภทเครือข่ายสื่อสารข้อมูลที่ใช้งานในกองทัพบก แบ่งออกเป็น ๔ ประเภท ได้แก่

๖.๑ เครือข่ายสื่อสารข้อมูลประเภทที่ ๑ โครงสร้างพื้นฐานวิกฤตแบบปิด

๖.๒ เครือข่ายสื่อสารข้อมูลประเภทที่ ๒ เครือข่ายสื่อสารข้อมูลแบบปิดของหน่วยต่าง ๆ

๖.๓ เครือข่ายสื่อสารข้อมูลประเภทที่ ๓ เครือข่ายสื่อสารข้อมูลที่เชื่อมต่อกับอินเตอร์เน็ตของหน่วยต่าง ๆ

๖.๔ เครือข่ายสื่อสารข้อมูลประเภทที่ ๔ เครือข่ายที่มีการเชื่อมต่อกันระหว่างเครือข่ายสื่อสารข้อมูลประเภทที่ ๑ และเครือข่ายสื่อสารข้อมูลประเภทที่ ๓

ข้อ ๗ การจัดระดับการรักษาความมั่นคงปลอดภัยของหน่วยกองทัพบก

๗.๑ ระดับสูง มีคุณลักษณะอย่างใดอย่างหนึ่งดังนี้

๗.๑.๑ จำนวนเครื่องแม่ข่าย/ให้บริการ (Server) ไม่ต่ำกว่า ๑๐ เครื่อง

๗.๑.๒ จำนวนเครื่องผู้ใช้บริการ (Client) ไม่ต่ำกว่า ๕๐๐ เครื่อง

๗.๑.๓ จำนวนผู้ใช้บริการ (User) จำนวนไม่ต่ำกว่า ๕๐๐ นาย

/๗.๒ ระดับปาน...

๗.๒ ระดับปานกลาง มีคุณลักษณะอย่างใดอย่างหนึ่งดังนี้

๗.๒.๑ จำนวนเครื่องแม่ข่าย/ให้บริการ (Server) ไม่ต่ำกว่า ๕ เครื่อง แต่ไม่เกิน ๙ เครื่อง

๗.๒.๒ จำนวนเครื่องผู้ใช้บริการ (Client) ไม่ต่ำกว่า ๒๕๐ เครื่อง แต่ไม่เกิน ๔๙๙ เครื่อง

๗.๒.๓ จำนวนผู้ใช้บริการ (User) จำนวนไม่ต่ำกว่า ๒๕๐ นาย แต่ไม่เกิน ๔๙๙ นาย

๗.๓ ระดับต่ำ มีคุณลักษณะอย่างใดอย่างหนึ่งดังนี้

๗.๒.๑ จำนวนเครื่องแม่ข่าย/ให้บริการ (Server) ตั้งแต่ ๑ เครื่อง แต่ไม่เกิน ๔ เครื่อง

๗.๒.๒ จำนวนเครื่องผู้ใช้บริการ (Client) น้อยกว่า ๒๕๐ เครื่อง

๘.๒.๓ จำนวนผู้ใช้บริการ (User) น้อยกว่า ๒๕๐ เครื่อง

หมวด ๒ มาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ ๘ กำหนดมาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแบ่งออกเป็น ๔ ระดับ ดังนี้

๘.๑ มาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับ ๑ จำเป็นต้องรักษาความมั่นคงปลอดภัยระดับสูงสุด ได้แก่ ศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ประจำเครือข่ายประเภทที่ ๔ มีจำนวน ๑๒ รายการ ดังนี้ (รูปที่ ๑ ผนวก ก)

๘.๑.๑ ระบบบริหารจัดการข้อมูลและเหตุการณ์ทางด้านความมั่นคงปลอดภัย (SIEM)

๘.๑.๒ ระบบวิเคราะห์และตรวจสอบความปลอดภัยระบบคอมพิวเตอร์ (Enterprise Security)

๘.๑.๓ ระบบบริหารจัดการข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management) ได้แก่ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Logging) และระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ให้บริการ (Log Correlation)

๘.๑.๔ ระบบป้องการโจมตีโดยปฏิเสธการให้บริการ (Denial-of-Service (DoS) attack)

๘.๑.๕ ระบบป้องกันการโจมตีของระบบเครือข่าย (Network Intrusion Prevention System : IPS)

๘.๑.๖ ระบบตรวจสอบมัลแวร์ขั้นสูง (Advance Malware)

๘.๑.๗ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ระดับโปรแกรมประยุกต์หรือแอปพลิเคชัน (NGF)

๘.๑.๘ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ระดับเฉพาะเว็บไซต์ (WAF)

๘.๑.๙ ระบบบริหารการจัดการจัดเก็บข้อมูล (Enterprise Storage Management System)

๘.๑.๑๐ ระบบใบรับรองดิจิตอล (Certificate Authority)

๘.๑.๑๑ ระบบเครือข่ายเสมือนส่วนตัว (VPN)

๘.๑.๑๒ ระบบพิสูจน์และยืนยันตัวบุคคลในระบบเครือข่าย (Authentication System)

/๘.๒ มาตรฐาน...

๘.๒ มาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับ ๒ สำหรับเครือข่ายสื่อสารข้อมูลที่ใช้งานใน ทบ. ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยระดับสูง มีจำนวน ๗ รายการ ดังนี้ (รูปที่ ๒ ผนวก ก)

๘.๒.๑ ระบบบริหารจัดการข้อมูลและเหตุการณ์ทางด้านความมั่นคงปลอดภัย (SIEM)

๘.๒.๒ ระบบบริหารจัดการข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management) ได้แก่ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Logging) และระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ให้บริการ (Log Correlation)

๘.๒.๓ ระบบป้องกันการโจมตีของระบบเครือข่าย (IPS)

๘.๒.๔ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ระดับปกติ

๘.๒.๕ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ระดับเฉพาะเว็บไซต์ (WAF)

๘.๒.๖ ระบบเครือข่ายเสมือนส่วนตัว (VPN)

๘.๒.๗ ระบบพิสูจน์และยืนยันตัวบุคคลในระบบเครือข่าย (Authentication System)

๘.๓ มาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับ ๓ สำหรับเครือข่ายสื่อสารข้อมูลที่ใช้งานใน ทบ. ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยระดับปานกลาง มีจำนวน ๔ รายการ ดังนี้ (รูปที่ ๓ ผนวก ก)

๘.๓.๑ ระบบบริหารจัดการข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management) ได้แก่ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Logging) และระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ให้บริการ (Log Correlation)

๘.๓.๒ ระบบป้องกันการโจมตีของระบบเครือข่าย (IPS)

๘.๓.๓ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ระดับปกติ

๘.๓.๔ ระบบพิสูจน์และยืนยันตัวบุคคลในระบบเครือข่าย

๘.๔ มาตรฐานอุปกรณ์และระบบประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ ระดับ ๔ สำหรับเครือข่ายสื่อสารข้อมูลที่ใช้งานใน ทบ. ที่จำเป็นต้องรักษาความมั่นคงปลอดภัยระดับต่ำ มีจำนวน ๓ รายการ ดังนี้ (รูปที่ ๔ ผนวก ก)

๘.๔.๑ ระบบบริหารจัดการข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management) ได้แก่ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Logging) และระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ให้บริการ (Log Correlation)

๘.๔.๒ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) ในระดับปกติ

๘.๔.๓ ระบบพิสูจน์และยืนยันตัวบุคคลในระบบเครือข่าย (Authentication System)

/ข้อ ๙ คุณลักษณะ...

ข้อ ๙ คุณลักษณะและขีดความสามารถของระบบงาน

๙.๑ ระบบบริหารจัดการข้อมูลและเหตุการณ์ทางด้านความมั่นคงปลอดภัย (SIEM)

๙.๑.๑ จัดเก็บและวิเคราะห์ข้อมูลความปลอดภัยของระบบเครือข่ายขององค์กร

๙.๑.๒ รวบรวมข้อมูลการจราจรทางคอมพิวเตอร์ (Log) เพื่อนำเสนอรายงานความสอดคล้องตามกฎเกณฑ์มาตรฐาน (การทำ Compliance ภายในหน่วย) เช่น ISO 27001, PCI, FISMA เป็นต้น

๙.๑.๓ วิเคราะห์ข้อมูลการจราจรทางคอมพิวเตอร์ (Log) จากอุปกรณ์รักษาความปลอดภัยเครือข่าย, อุปกรณ์เครือข่าย, ระบบงานต่าง ๆ และ Application

๙.๑.๔ ดำเนินการนำข้อมูลทั้งหมดนี้มาจัดทำรูปแบบมาตรฐาน และลดความซ้ำซ้อน (Normalization) และความสามารถในการหาความสัมพันธ์ของข้อมูล (Correlate)

๙.๑.๕ สามารถค้นหาต้นตอและเป้าประสงค์ของการโจมตีในรูปแบบต่าง ๆ ได้ทั้งในแบบ Real-time และตรวจสอบย้อนหลัง

๙.๑.๖ สามารถแจ้งเตือนไปยังผู้ดูแลระบบ เมื่อตรวจพบข้อมูลการจราจรทางคอมพิวเตอร์ (Log) ที่สอดคล้องกับเงื่อนไขที่ตั้งไว้

๙.๑.๗ นำเสนอกระดานแสดงสถานะข้อมูลระบบ เพื่อให้ผู้ดูแลระบบบริหารจัดการข้อมูลได้สะดวก

๙.๒ ระบบวิเคราะห์และตรวจสอบความปลอดภัยระบบคอมพิวเตอร์ (Enterprise Security)

๙.๒.๑ ระบบต้องสามารถทำงานร่วมกันกับระบบบริหารจัดการข้อมูลและเหตุการณ์ทางด้านความมั่นคงปลอดภัย (SIEM) ที่บริษัทนำเสนอได้อย่างมีประสิทธิภาพ

๙.๒.๒ สามารถแสดงภาพรวมความปลอดภัยระบบคอมพิวเตอร์ในรูปแบบของกระดานแสดงข้อมูลทางคอมพิวเตอร์(Dashboard) ได้

๙.๒.๓ สามารถวิเคราะห์ความเสี่ยงที่เกิดขึ้นในองค์กร (Risk Analysis) ในรูปแบบของ Dashboard ได้

๙.๒.๔ สามารถตรวจสอบเหตุการณ์จากภัยคุกคามที่เกิดขึ้น (Incident Audit) ในรูปแบบของ Dashboard ได้

๙.๒.๕ สามารถรองรับการทำ Incident Response และ การทำ Investigation ได้

๙.๒.๖ สามารถมอนิเตอร์และตรวจจับเหตุการณ์ต่าง ๆ ที่มาจากอุปกรณ์ เช่น Firewalls, Routers, Wireless Access Points, Intrusion Detection และ นำข้อมูลจากอุปกรณ์เหล่านี้มาสร้างความสัมพันธ์หรือเชื่อมโยงร่วมกันได้

๙.๒.๗ สามารถทำการค้นหาข้อมูลที่ถูกเก็บไว้ในระบบในรูปแบบต่าง ๆ เช่น การค้นหาข้อมูลย้อนหลัง, การค้นหาข้อมูลแบบกำหนดช่วงเวลา, การค้นหาข้อมูลในรูปแบบ Real Time

๙.๒.๘ สามารถนำข้อมูลมาแสดงผลในลักษณะ ตาราง แผนภูมิเส้น แผนภูมิแท่ง หรือแผนภูมิรูปวงกลมได้

/๙.๓ ระบบบริหาร...

๙.๓ ระบบบริหารจัดการข้อมูลการจราจรทางคอมพิวเตอร์ (Log Management)

๙.๓.๑ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง (Centralized Logging)

๙.๓.๑.๑ การปฏิบัติงานเป็นตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๙.๓.๑.๑.๒ สามารถรวบรวม Log จัดเก็บไว้ในเซิร์ฟเวอร์ส่วนกลาง เพื่อความปลอดภัยของข้อมูล

๙.๓.๑.๑.๓ สามารถป้องกันการทำลายและการเปลี่ยนแปลงข้อมูลที่ได้รับมาตรฐาน

๙.๓.๒ ระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ของเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ให้บริการ (Log Correlation) : สามารถจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์จากอุปกรณ์ แล้วส่งไปจัดเก็บยังระบบจัดเก็บบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ส่วนกลาง

๙.๔ ระบบป้องการโจมตีโดยปฏิเสธการให้บริการ (Denial-of-Service (DoS) attack) : สามารถป้องกันและกลั่นกรองแพ็กเกจที่มีการใช้ปริมาณข้อมูลมากผิดปกติ เพื่อป้องกันการโจมตีโดยปฏิเสธการให้บริการ

๙.๕ ระบบป้องกันการโจมตีของระบบเครือข่าย (Network Intrusion Prevention System)

๙.๕.๑ สามารถตรวจสอบแพ็กเกจที่ รับ - ส่ง บนเครือข่าย และทำการยับยั้งหรือหยุดการเชื่อมต่อเมื่อมีพฤติกรรมเข้าข่ายภัยคุกคาม

๙.๕.๒ สามารถตรวจจับโดยการเปรียบเทียบ Signature ของข้อมูลการจราจรทางคอมพิวเตอร์กับ Signature ของการโจมตีในแต่ละรูปแบบในฐานองค์ความรู้ (Signature - based)

๙.๖ ระบบตรวจสอบมัลแวร์ขั้นสูง (Advance Malware)

๙.๖.๑ สามารถตรวจจับ วิเคราะห์ไฟล์ที่มีพฤติกรรมเป็นมัลแวร์และทำการสกัดกั้นแบบเรียลไทม์

๙.๖.๒ สร้างรูปแบบพฤติกรรม (Behavior - based) โดยใช้วิธีการทางสถิติเป็นตัวชี้วัดความผิดปกติ ด้วยการสร้างค่ามาตรฐานหรือค่าปกติ (Normal) จากเหตุการณ์ที่เป็นปกติ แล้วสุ่มเหตุการณ์ที่เกิดขึ้นในแต่ละวันขึ้นมาเปรียบเทียบกับค่าปกติ (Normal) หากมีการเบี่ยงเบนไปจากเดิมให้ถือว่ามีการบุกรุกหรือมีความผิดปกติขึ้น

๙.๗ ระบบรักษาความปลอดภัยบนเครือข่าย (Firewall) แบ่งออกเป็น ๓ ระดับ ดังนี้

๙.๗.๑ ระบบรักษาความปลอดภัยบนเครือข่ายระดับปกติ : สามารถกำหนดกฎระเบียบการเข้าถึงเครือข่ายจากภายนอก ควบคุมการจราจรในระดับไอพีและพอร์ต

๙.๗.๒ ระบบรักษาความปลอดภัยบนเครือข่ายระดับโปรแกรมประยุกต์หรือแอปพลิเคชัน (Next Generation Firewall : NGF) : สามารถควบคุมการจราจรบนเครือข่ายถึงระดับแอปพลิเคชัน

๙.๗.๓ ระบบรักษาความปลอดภัยบนเครือข่ายระดับเฉพาะเว็บไซต์ (Web Application Firewall : WAF) : สามารถป้องกันการโจมตีทางเว็บไซต์ ติดตามการใช้งาน และเก็บ Log การใช้งาน Web Server

/๙.๘ ระบบบริหาร...

๙.๘ ระบบบริหารการจัดการจัดเก็บข้อมูล (Enterprise Storage Management System) : สามารถสำรองและจัดเก็บไฟล์ข้อมูลอย่างเป็นระเบียบ ลดความซ้ำซ้อนของข้อมูล และเข้าถึงข้อมูลได้จากทุกที่

๙.๙ ระบบใบรับรองดิจิตอล (Certificate Authority) : สามารถประกันความถูกต้องของข้อมูลและแหล่งที่มาของข้อมูล

๙.๑๐ ระบบเครือข่ายเสมือนส่วนตัว (VPN) : สามารถเชื่อมต่อเครือข่ายภายในของหน่วย โดยผ่านเครือข่ายอินเตอร์เน็ต ที่มีการเข้ารหัสข้อมูลเพื่อความมั่นคงปลอดภัย

๙.๑๑ ระบบพิสูจน์และยืนยันตัวบุคคลในระบบเครือข่าย (Authentication System) : สามารถพิสูจน์ตัวตน โดยมีหน้าที่หลัก ๓ ประการ ได้แก่ การตรวจสอบชื่อผู้ใช้และรหัสผ่าน (Authentication) การกำหนดสิทธิ์ในการเข้าใช้งานของผู้ใช้ (Authorization) การเก็บข้อมูลรายละเอียดการใช้งานของผู้ใช้ (Accounting)

หมวด ๓ หน้าที่และความรับผิดชอบ

ข้อ ๑๐ หน้าที่และความรับผิดชอบของเจ้าหน้าที่ประจำศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๐.๑ เจ้าหน้าที่เฝ้าระวังและแจ้งเตือนภัยคุกคามทางไซเบอร์ (Tier 1) มีหน้าที่

๑๐.๑.๑ รับแจ้งเหตุภัยคุกคามทางไซเบอร์

๑๐.๑.๒ เฝ้าระวังทางเทคนิคด้านการรักษาความปลอดภัยไซเบอร์

๑๐.๑.๓ บันทึกสิ่งบอกเหตุที่คาดว่าจะเกิดภัยคุกคามไซเบอร์ และจัดทำรายงานให้ผู้บังคับบัญชาทราบถึงเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น

๑๐.๑.๔ ตรวจสอบและแก้ปัญหาภัยคุกคามทางไซเบอร์ในเบื้องต้น

๑๐.๑.๕ ให้คำแนะนำเกี่ยวกับการปฏิบัติต่อภัยคุกคามด้านไซเบอร์เชิงรับให้มีความมั่นคงปลอดภัย

๑๐.๒ เจ้าหน้าที่เผชิญเหตุภัยคุกคามทางไซเบอร์ (Tier 2) มีหน้าที่

๑๐.๒.๑ วิเคราะห์เหตุภัยคุกคามที่มีความซับซ้อน

๑๐.๒.๒ ประสานการปฏิบัติกับหน่วยงานต่างๆ ในการแก้ปัญหาเหตุภัยคุกคามทางไซเบอร์

๑๐.๒.๓ ให้ความช่วยในการซ่อมบำรุงและกู้คืนระบบสารสนเทศของหน่วยที่ได้รับความเสียหายจากการภัยคุกคามทางไซเบอร์

๑๐.๒.๔ บันทึกสิ่งบอกเหตุที่คาดว่าจะเกิดภัยคุกคามไซเบอร์ และจัดทำรายงานให้ผู้บังคับบัญชาทราบถึงเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น

๑๐.๒.๕ ให้คำแนะนำเกี่ยวกับการปฏิบัติต่อภัยคุกคามด้านไซเบอร์เชิงรับให้มีความมั่นคงปลอดภัย

๑๐.๓ เจ้าหน้าที่ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ (Tier 3) มีหน้าที่

๑๐.๓.๑ วิเคราะห์เหตุภัยคุกคามที่มีความซับซ้อน

๑๐.๓.๒ ดำเนินการพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics)

/๑๐.๓.๓ วิเคราะห์...

๑๐.๓.๓ วิเคราะห์มัลแวร์ (Malware Reverse Engineering) และรูปแบบการโจมตีต่าง ๆ ที่เกิดขึ้น

๑๐.๓.๔ บันทึกสิ่งบอกเหตุที่คาดว่าจะเกิดภัยคุกคามไซเบอร์ และจัดทำรายงานให้ผู้บังคับบัญชาทราบถึงเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น

๑๐.๓.๕ ให้คำแนะนำเกี่ยวกับการปฏิบัติต่อภัยคุกคามด้านไซเบอร์เชิงรับให้มีความมั่นคงปลอดภัย

๑๐.๔ ผู้บริหารศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ (CSOC Manager) มีหน้าที่

๑๐.๔.๑ ควบคุมบังคับบัญชาเจ้าหน้าที่ของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และรับผิดชอบการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรให้เป็นไปตามนโยบายและระเบียบที่เกี่ยวข้อง

๑๐.๔.๒ วางแผนกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของศูนย์ปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑๐.๔.๓ จัดการฝึกอบรมการปฏิบัติงานให้กับเจ้าหน้าที่ศูนย์รักษาความมั่นคงปลอดภัยไซเบอร์

๑๐.๔.๔ ดำเนินการตามแผนการสื่อสารในภาวะวิกฤติ ประสานงานหน่วยงานข้างเคียงและภายนอกในการแก้ปัญหาเหตุการณ์ฉุกเฉินทางไซเบอร์

๑๐.๔.๕ รายงานให้ผู้บังคับบัญชาทราบถึงเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น

๑๐.๔.๖ ให้คำแนะนำเกี่ยวกับการปฏิบัติต่อภัยคุกคามด้านไซเบอร์เชิงรับให้มีความมั่นคงปลอดภัย

ข้อ ๑๑ ให้ ผู้อำนวยการศูนย์ไซเบอร์กองทัพบก เป็นผู้รักษาการให้เป็นไปตามระเบียบนี้ และให้ทบทวนระเบียบ วงรอบทุก ๒ ปี

ประกาศ ณ วันที่ สิงหาคม พ.ศ. ๒๕๖๓

พลเอก

(อภิรัชต์ คงสมพงษ์)

ผู้บัญชาการทหารบก

กรมยุทธการทหารบก