การป้องปรามทางไซเบอร์

พ.ศ.๒๕๖๖

โดย

กองปฏิบัติการไซเบอร์

ศูนย์ไซเบอร์กองทัพอากาศ

บันทึกข้อความ

ส่วนราชการ ทสส.ทอ.(สนผ.โทร.๒-๒๔๖๗)

ที่ กห ๐๖๐๙.๓/ ๑๒๒๕ **วันที่** ๑๙ ก.ย.๖๖

เรื่อง ส่งคู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เสนอ ศชบ.ทอ.

๑. ตามอนุมัติ จก.ทสส.ทอ.เมื่อ ๑๓ ก.ย.๖๖ ท้ายหนังสือ สนผ.ทสส.ทอ.ที่ กห ๐๖๐๙.๓(๒)/๒๐๓ ลง ๑๒ ก.ย.๖๖ ให้ใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ นั้น

๒. ทสส.ทอ.จึงขอส่งคู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ เพื่อใช้ในการฝึกความชำนาญของจำพวกทหารไซเบอร์ รายละเอียดตามแนบ

จึงเสนอมาเพื่อดำเนินการต่อไป

พล.อ.ต.

ผอ.สนผ.ทสส.ทอ.ทำการแทน

จก.ทสส.ทอ.

บันทึกข้อความ

ส่วนราชการ สนผ.ทสส.ทอ.(กนผ.โทร.๒-๑๐๕๖)

ที่ กห ๐๖๐๙.๓(๒)/ ๒๐๓ **วันที่** ๑๒ ก.ย.๖๖

เรื่อง ขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ จำพวกทหารไซเบอร์

เรียน จก.ทสส.ทอ.

๑. ตามหนังสือ ศชบ.ทอ.ที่ กห ๐๖๕๐.๑/๗๔๖ ลง ๒๘ ส.ค.๖๖ ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์ นั้น

๒. สนผ.ทสส.ทอ.ตรวจสอบแล้ว มีข้อมูล ดังนี้

๒.๑ ระเบียบ ทอ.ว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓ และฉบับแก้ไขเพิ่มเติม ข้อ ๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้ (แนบ ๑)

๒.๒ ทสส.ทอ.เป็นหน่วยรับผิดชอบสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์และสายวิทยาการไซเบอร์ ได้จัดทำคู่มือการฝึกงานในหน้าที่ เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญการปฏิบัติงานในสายวิทยาการไซเบอร์ จำนวน ๕ วิชา (แนบ ๒) ประกอบด้วย

๒.๒.๑ วิชา การป้องปรามทางไซเบอร์
๒.๒.๒ วิชา การป้องกันทางไซเบอร์
๒.๒.๓ วิชา การข่าวกรองทางไซเบอร์
๒.๒.๔ วิชา การพิสูจน์หลักฐานทางดิจิทัล
๒.๒.๕ วิชา ความรู้พื้นฐานสำหรับปฏิบัติการทางไซเบอร์

๓. สนผ.ฯ พิจารณาแล้ว เพื่อให้การดำเนินการฝึกงานในหน้าที่ของสายวิทยาการไซเบอร์เป็นไปด้วยความเรียบร้อย จึงขออนุมัติใช้คู่มือการฝึกงานในหน้าที่ของจำพวกทหารไซเบอร์ สำหรับการฝึกความชำนาญของจำพวกทหารไซเบอร์ต่อไป

จึงเรียนมาเพื่ออนุมัติตามข้อ ๓

พล.อ.ต.
ผอ.สนผ.ทสส.ทอ.

- อนุมัติตามข้อ ๓

พล.อ.ท.
จก.ทสส.ทอ.
๑๙ ก.ย.๖๖

ทสส.ทอ.
เลขรับ ๕๕๔๐
วันที่ ๒๔ ส.ค. ๒๕๖๖
เวลา ๑๓๔๘

บันทึกข้อความ

ส่วนราชการ ศชบ.ทอ.(นกพ.ฯ โทร.๒-๒๗๑๒)

ที่ กห ๐๖๕๐.๑/ ๗๔๖ วันที่ ๒๔ ส.ค.๖๖

เรื่อง ขอให้พิจารณาตำราของหลักสูตรสายวิทยาการไซเบอร์

สนผ.ทสส.ทอ.
เลขรับ ๒๗๗๑
วันที่ ๒๔ ส.ค.๖๖
เวลา ๑๓๕๗

เสนอ ทสส.ทอ.

สนผ-๖
๒๔ ส.ค. ๒๕๖๖

๑. ตามหนังสือ ทสส.ทอ.ที่ กห ๐๖๐๙.๓/๑๐๘๙ ลง ๙ ส.ค.๖๖ ให้ ศชบ.ทอ.ปรับปรุงเนื้อหาตำราของหลักสูตรสายวิทยาการไซเบอร์จำนวน ๕ วิชา นั้น

๒. ศชบ.ทอ.ตรวจสอบและพิจารณาแก้ไขเนื้อหา รายละเอียดตามความเหมาะสม ร่วมกับ ร.อ.หญิง สุธิดา บทสันเทียะ นมฐ.ผมทส.กนผ.สนผ.ทสส.ทอ.แล้วเมื่อวันที่ ๒๓ ส.ค.๖๖ ดังมี รายละเอียดตามแนบ

จึงเสนอมาเพื่อพิจารณาดำเนินการให้ต่อไป

พล.อ.ต.
ผอ.ศชบ.ทอ.

กนผ.สนผ.ทสส.ทอ.
เลขรับ ๒๑๐๕
วันที่ ๒๘ ส.ค. ๖๖
เวลา ๑๓๕๗

ทราบแล้ว
- รอง ผอ.กนผ.สนผ.ทสส.ทอ.ทราบ
- ผสส.๑ ดำเนินการในส่วนที่เกี่ยวข้อง

น.อ.
ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ทราบแล้ว

น.อ.
รอง ผอ.กนผ.สนผ.ทสส.ทอ.
๒๘ / ส.ค. / ๖๖

ระเบียบกองทัพอากาศ
ว่าด้วยการฝึกงานในหน้าที่
พ.ศ.๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงแก้ไขแนวทางปฏิบัติเกี่ยวกับการฝึกงานในหน้าที่ของกองทัพอากาศ ให้เป็นไปด้วยความเรียบร้อย จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่บัดนี้เป็นต้นไป

ข้อ ๓ ให้ยกเลิก ระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๕๔

บรรดาระเบียบและคำสั่งอื่นใด ในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือซึ่งขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ในระเบียบนี้

๔.๑ "การฝึกงานในหน้าที่" หมายความว่า การให้นายทหารประทวนเข้ารับการฝึกงานตามตำแหน่งหรือหน้าที่ที่ได้รับมอบหมาย เพื่อเพิ่มพูนความรู้ ความสามารถ และความชำนาญให้สูงขึ้น ตามลักษณะความชำนาญทหารอากาศของเหล่าทหารหรือจำพวกทหาร โดยใช้ตามมาตรฐานการฝึกความชำนาญ และหนังสือคู่มือการฝึกงานในหน้าที่เป็นแนวทางการฝึก

๔.๒ "การฝึก" หมายความว่า การฝึกงานในหน้าที่

๔.๓ "นายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร ที่แต่งตั้งขึ้นให้มีหน้าที่รับผิดชอบ และดำเนินการ ควบคุม กำกับ ดูแล เกี่ยวกับการฝึกงานในหน้าที่ของหน่วยขึ้นตรงกองทัพอากาศ ให้ใช้คำย่อว่า "นฝน."

๔.๔ "ผู้ช่วยนายทหารฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตรจำพวกทหารกำลังพลที่แต่งตั้งขึ้น ให้มีหน้าที่ช่วยเหลือนายทหารฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "ผช.นฝน."

๔.๕ "เจ้าหน้าที่ฝึกงานในหน้าที่" หมายความว่า นายทหารสัญญาบัตร หรือนายทหารประทวน หรือลูกจ้างที่แต่งตั้งขึ้น ให้มีหน้าที่ด้านธุรการเกี่ยวกับการฝึกงานในหน้าที่ ให้ใช้คำย่อว่า "จนท.ฝน."

๔.๖ "ผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่เป็นเหล่าหรือจำพวกทหารเดียวกันกับผู้รับการฝึกที่แต่งตั้งขึ้น ให้มีหน้าที่ดำเนินการ ควบคุม กำกับ ดูแลการฝึกงานในหน้าที่ภาคปฏิบัติประจำปีให้เป็นไปตามมาตรฐานการฝึกความชำนาญ

๔.๗ "ผู้ช่วยผู้ควบคุมการฝึก" หมายความว่า นายทหารสัญญาบัตรที่แต่งตั้งขึ้นให้มีหน้าที่ช่วยเหลือผู้ควบคุมการฝึก

๔.๘ "ครูฝึก"...

๓๑.๑๘.๒.๒ ระดับ ๕๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ไม่เกินร้อยละ ๘๐ ของจำนวนชั่วโมงรวมในระดับ ๗๐

๓๑.๑๘.๒.๓ ระดับ ๗๐ จำนวนชั่วโมงรวมของการเรียนการสอนของภาคปฏิบัติและภาคบรรยาย ตรงกับความมุ่งหมายเฉพาะและวัตถุประสงค์การเรียนรู้ในระดับ ๗๐

๓๑.๑๙ หนังสือคู่มือการฝึกงานในหน้าที่ เป็นเอกสารอธิบายความรู้ในวิทยาการและวิธีปฏิบัติงานของเหล่าทหารหรือจำพวกทหารซึ่งส่วนราชการหัวหน้าสายวิทยาการจัดทำขึ้น เพื่อใช้ประกอบการฝึกงานในหน้าที่ตามระดับความชำนาญ โดยมีความสัมพันธ์และสอดคล้องกับเรื่องและหัวข้อวิชาในมาตรฐานการฝึกความชำนาญ ให้เรียกโดยย่อว่า "หนังสือคู่มือการฝึก" และให้จัดทำตามผนวก ๗ แนบท้ายระเบียบนี้

หมวด ๖
การควบคุมกำกับดูแล

ข้อ ๓๒ หน่วยฝึกจะต้องดำเนินการฝึกตามระยะเวลาที่กำหนดไว้ในวงรอบการฝึก

ข้อ ๓๓ ผู้รับการฝึก จะต้องทำการฝึกครบทุกหัวข้อวิชา หรือหมวดวิชาที่เป็นวิชาหลักของจำพวกทหารตามที่กำหนดในมาตรฐานการฝึกความชำนาญ

ข้อ ๓๔ เมื่อผู้รับการฝึกย้ายสังกัด ในระหว่างการฝึกภาคปฏิบัติ หรือรอการทดสอบภาควิชาการ ให้ส่วนราชการต้นสังกัดเดิมแจ้งให้ส่วนราชการต้นสังกัดใหม่ทราบถึงสถานภาพการฝึกที่ผ่านมา และเรื่องที่จะต้องดำเนินการต่อไป พร้อมกับส่งประวัติการฝึก กับมาตรฐานการฝึกความชำนาญไปยังส่วนราชการต้นสังกัดใหม่ โดยส่วนราชการต้นสังกัดใหม่จะต้องแต่งตั้งผู้รับผิดชอบในขั้นตอนที่ยังเหลืออยู่ เพื่อดำเนินการฝึกต่อไปให้ครบตามหัวข้อที่กำหนดไว้ หากจะให้ทำการฝึกที่ส่วนราชการเดิมต่อไป ให้ประสานตกลงกันแล้วแจ้งการเปลี่ยนแปลงให้ กรมกำลังพลทหารอากาศทราบ เพื่อแก้ไขเปลี่ยนแปลงหลักฐานการควบคุมการฝึกงานในหน้าที่ให้ถูกต้อง

ข้อ ๓๕ ผู้ที่ไม่สามารถทำการฝึกได้ครบตามที่กำหนด และอยู่ในกรณีที่จะต้องพ้นจากการฝึก ให้ส่วนราชการต้นสังกัดรายงานพร้อมหลักฐานประกอบให้กรมกำลังพลทหารอากาศ ดำเนินการนำเรียนขออนุมัติผู้บัญชาการทหารอากาศ หากจะเข้ารับการฝึกในปีต่อไปจะต้องเริ่มดำเนินการใหม่ ซึ่งการพ้นจากการฝึกจะต้องอยู่ในกรณี ดังนี้

๓๕.๑ ลาออก ให้ออก ปลดออก

๓๕.๒ ต้องหาคดีอาญา ยกเว้นความผิดลหุโทษ หรือความผิดตามกฎหมายอื่นที่มีอัตราโทษไม่สูงกว่าความผิดลหุโทษ

๓๕.๓ ย้าย โอน ไปสังกัดนอกกองทัพอากาศ

๓๕.๔ มีราชการจำเป็นเร่งด่วนและสำคัญ

๓๕.๕ มีเวลาการฝึกภาคปฏิบัติไม่ถึงร้อยละ ๘๕ ของเวลาการฝึกทั้งหมด โดยมีเหตุผลอันสมควร

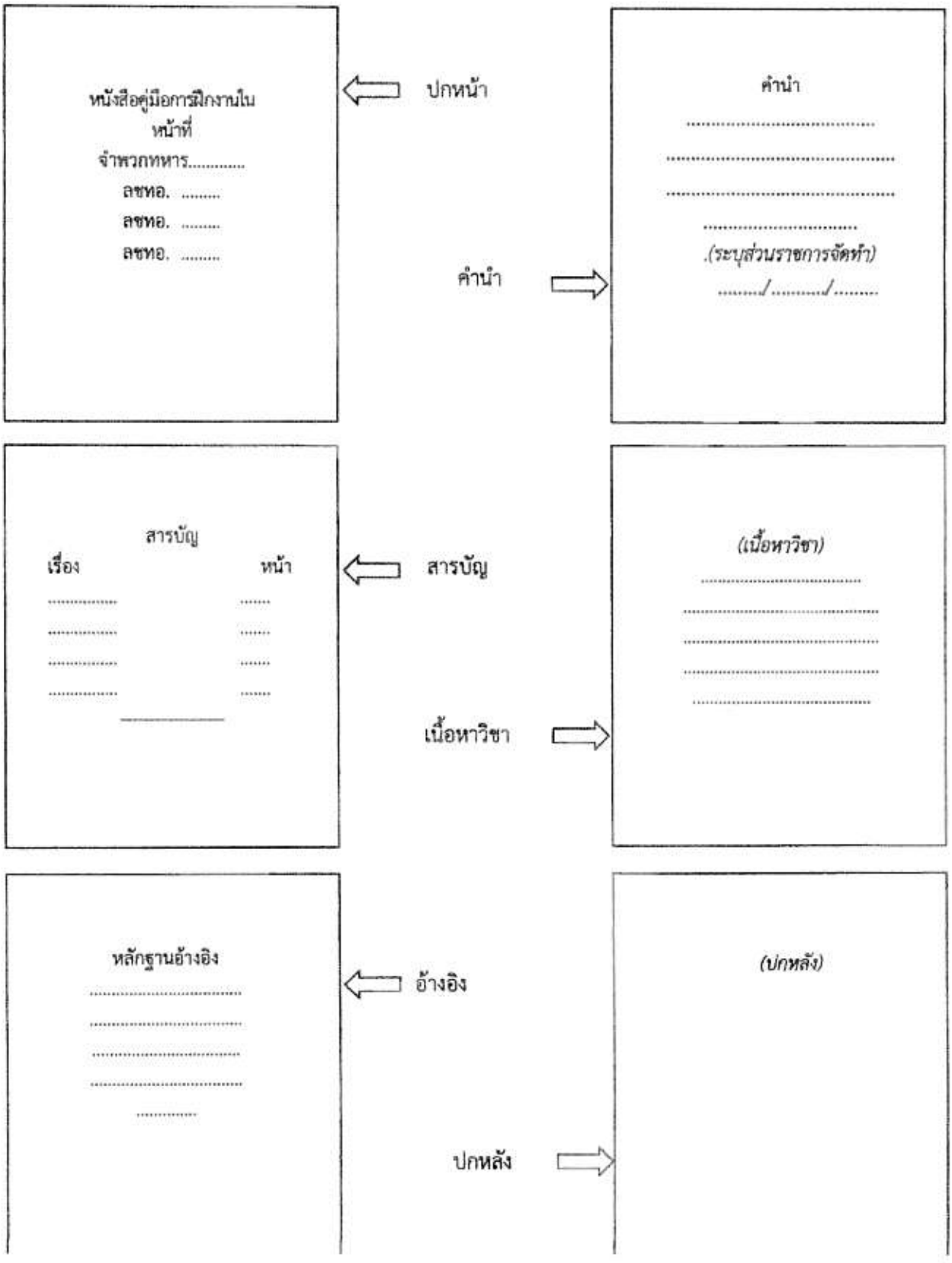
๓๕.๖ ป่วยจนมีเวลาการฝึกไม่เพียงพอตามข้อ ๓๕.๕

๓๕.๗ ขาดการทดสอบความรู้ภาคปฏิบัติตามระยะเวลาที่กำหนด โดยมีเหตุผลอันสมควร

ข้อ ๓๖ การลา ...

ผนวก ๗ ประกอบระเบียบกองทัพอากาศว่าด้วยการฝึกงานในหน้าที่ พ.ศ.๒๕๖๓

หนังสือคู่มือการฝึกงานในหน้าที่



คู่มือการฝึกงานในหน้าที่
จำพวกทหารไซเบอร์

ลชทอ.๒๘๑๓๐

ลชทอ.๒๘๑๕๐

ลชทอ.๒๘๑๗๐

กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

คำนำ

คู่มือการฝึกงานในหน้าที่วิชาการป้องปรามทางไซเบอร์ จัดทำขึ้นเพื่อประกอบการฝึกความชำนาญตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของสายวิทยาการไซเบอร์ เนื้อหาความรู้ของคู่มือเล่มนี้กล่าวถึงการป้องปรามทางไซเบอร์ ได้แก่ ความหมาย หลักการ มาตรฐานหลัก Cyber Kill Chain การตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค ตลอดจนแนวทางการดำเนินการปฏิบัติงานของกองปฏิบัติการไซเบอร์ เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่ มีความรู้ความเข้าใจและทักษะในการนำไปปฏิบัติงานในสายวิทยาการไซเบอร์ และสามารถนำองค์ความรู้ที่ได้รับ ไปประยุกต์เพื่อให้เกิดความปลอดภัยสูงสุดต่อผู้ปฏิบัติงานระบบคอมพิวเตอร์ และระบบสารสนเทศของกองทัพอากาศ

หวังเป็นอย่างยิ่งว่าคู่มือเล่มนี้ จะเป็นประโยชน์ต่อผู้เข้ารับการฝึกงานในหน้าที่และขอขอบคุณเจ้าหน้าที่ทุกท่านที่มีส่วนในการจัดทำคู่มือเล่มนี้จนเสร็จสมบูรณ์

กองปฏิบัติการไซเบอร์ ศูนย์ไซเบอร์กองทัพอากาศ

๒๘ สิงหาคม ๒๕๖๖

สารบัญ

สารบัญภาพ

บทที่ ๑ ความหมาย หลักการ และมาตรฐาน

๑.๑ ความหมาย

การปฏิบัติการเชิงรุก คือ การระงับ ลดทอน แทรกแซง ทำลาย หรือหลอกล่อ ขโมย ความสามารถของศัตรูที่ใช้ในไซเบอร์ รวมถึงการใช้งานอุปกรณ์อิเล็กทรอนิกส์ เน็ตเวิร์ค ในสภาพแวดล้อมทางไซเบอร์ โดยการปฏิบัติการเชิงรุกนั้น จะขึ้นตามรูปแบบหลัก ๆ อยู่ ๗ ขั้นตอน เป็นไปตามลำดับ ประกอบไปด้วย

๑.๑.๑ การลาดตระเวน

๑.๑.๒ การเตรียมหาวิธีเจาะระบบ

๑.๑.๓ การส่ง Payload

๑.๑.๔ การเจาะระบบ

๑.๑.๕ การติดตั้งมัลแวร์

๑.๑.๖ การสร้างช่องทางส่งคำสั่ง

๑.๑.๗ การดำเนินตามเป้าหมายตนเอง

๑.๒ หลักการ

การปฏิบัติการเชิงรุก มีหลักการปฏิบัติทั้งหมด ๗ ขั้นตอน ซึ่งประกอบไปด้วย การลาดตระเวน การเตรียมหาวิธีเจาะระบบ การส่ง Payload การเจาะระบบ การติดตั้งมัลแวร์ การสร้างช่องทางส่งคำสั่ง และการดำเนินตามเป้าหมายตนเอง ตามลำดับ

โดยขั้นตอนแรก ของการปฏิบัติการไซเบอร์เชิงรุกคือ ทำการสำรวจช่องโหว่ในแอปพลิเคชัน เครื่องเป้าหมาย หรือโครงสร้างของเครือข่ายและทดสอบเชื่อมต่อผ่านช่องโหว่เหล่านั้น ช่องโหว่ที่อยู่ภายในองค์ประกอบโครงสร้างหลาย ๆ แอปพลิเคชันนั้น สามารถตรวจสอบได้เพราะแอปพลิเคชันเหล่านั้นมีขายอยู่ในท้องตลาดออนไลน์และสามารถหาซื้อขายได้ทั่วไป เส้นทางที่เชื่อมต่อนั้น บ่อยครั้งจะถูกเปิดเผยโดยเทคโนโลยีที่สูงขึ้น ซึ่งวิศวกรทางด้านไอทีก็ต้องคอยดูแลระบบเฉพาะทางเหล่านั้น และพยายามจัดการปัญหาที่เกิดขึ้นใหม่อย่างต่อเนื่อง

๑.๓ มาตรฐาน

๑.๓.๑ ISO/IEC 27001 : Information Technology - Security Techniques - Information Security Management Systems - Requirements คือมาตรฐานหลักในหมวดระบบมาตรฐานความปลอดภัยสารสนเทศ ซึ่งแนะแนวทางและสนับสนุนให้องค์กรเข้าใจความเสี่ยงและจุดอ่อนด้านการคุ้มครองข้อมูลอย่างเป็นระบบ การดำเนินการให้สอดคล้องกับ ISO 27001 ช่วยเพิ่มความแข็งแกร่งให้กับระบบความปลอดภัยของข้อมูล ลดความเสี่ยง และปกป้องข้อมูลจากการถูกโจรกรรม

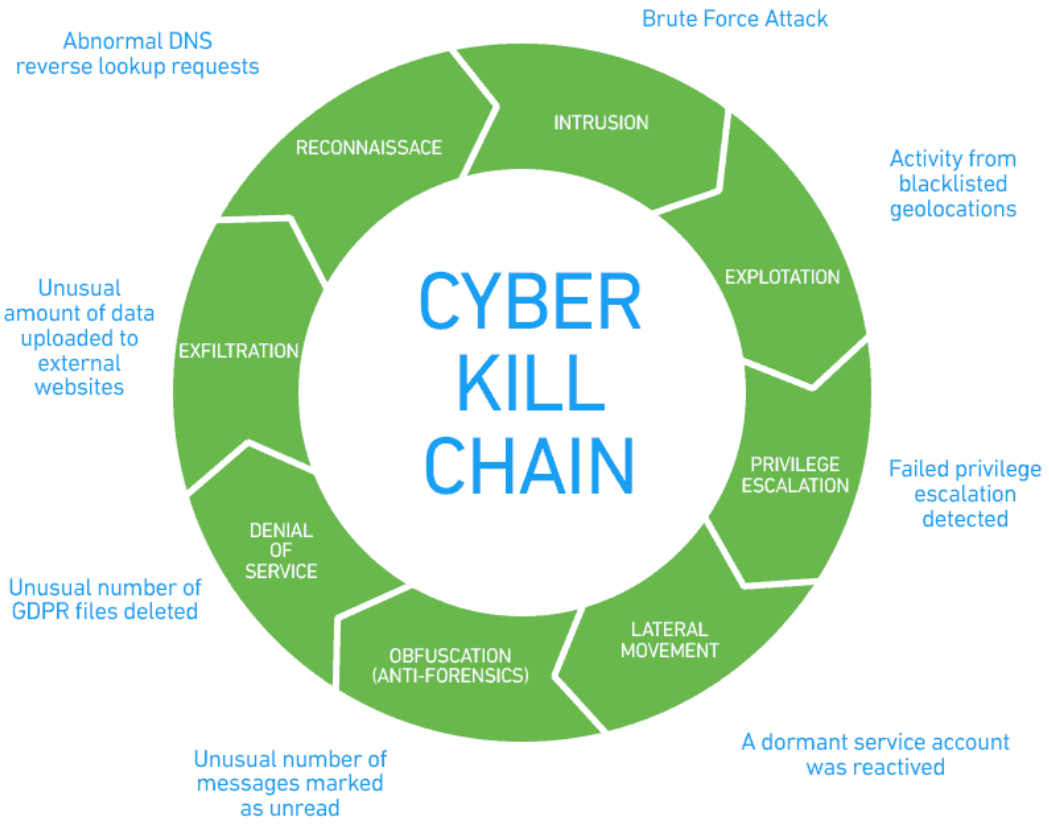
๑.๓.๒ ISO/IEC 27002 : Information Technology - Security Techniques - Code of Practice for Information Security Controls คือแนวทางที่ใช้เป็นข้อมูลอ้างอิงสำหรับการเลือกดำเนินการ และจัดการการควบคุมสำหรับทั้งสององค์กรที่มีระบบการจัดการความปลอดภัยของข้อมูล (ISMS) ตาม ISO/IEC 27001 โดยมีรายละเอียดใน Annex A รายการควบคุม และสำหรับทุกองค์กร

ที่มีแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยของข้อมูล ซึ่งต้องการใช้การควบคุมความปลอดภัยของข้อมูลที่เป็นที่ยอมรับโดยทั่วไป

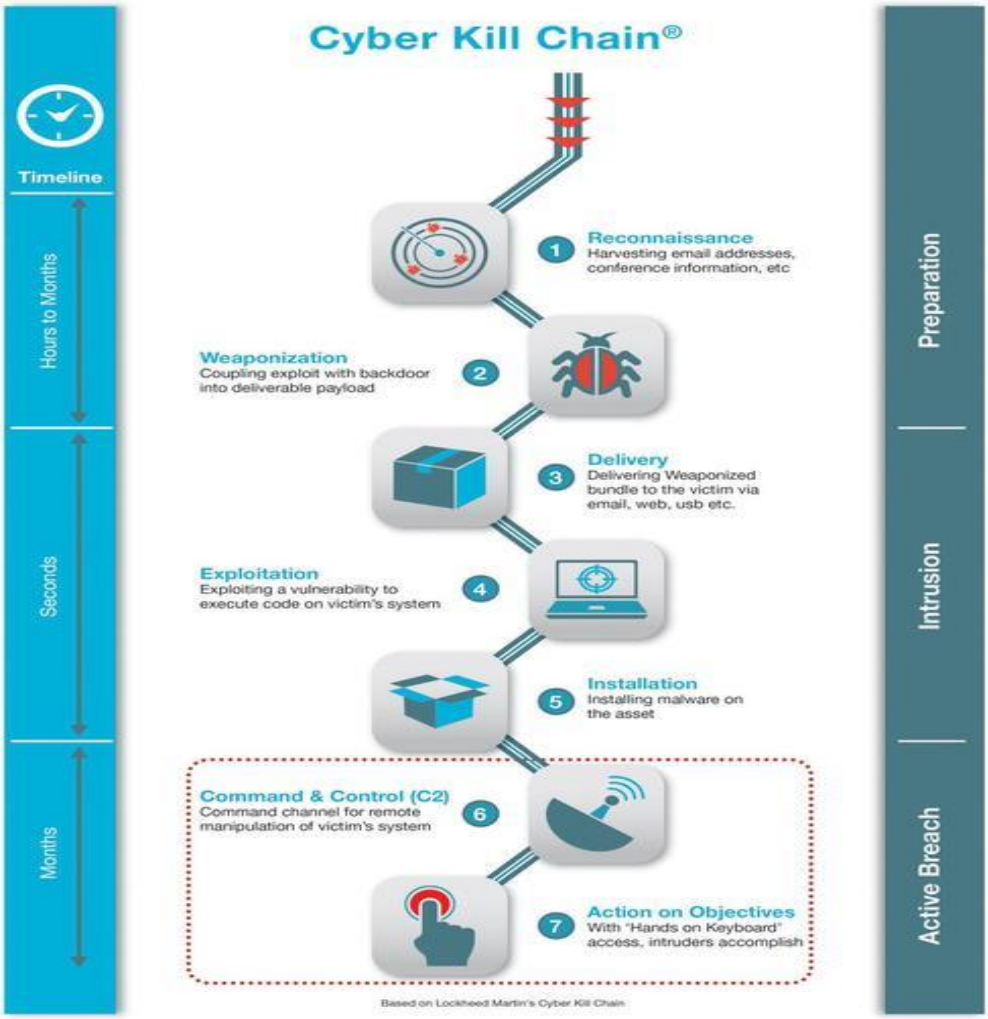
บทที่ ๒ Cyber Kill Chain

๒.๑ Cyber Kill Chain

Cyber Kill Chain ถูกคิดค้นโดย Lockheed Martin ซึ่งเป็นบริษัทด้านอากาศยาน การป้องกันความมั่นคงปลอดภัย และเทคโนโลยีระดับสูงชื่อดังของสหรัฐอเมริกา ซึ่งศัพท์คำนี้ถูกใช้กันอย่างแพร่หลายในวงการการรักษาความมั่นคงปลอดภัย เพื่อบรรยายถึงขั้นตอนของการเจาะระบบเพื่อโจมตีไซเบอร์ ที่น่าสนใจและเข้าใจได้ง่าย แบ่งขั้นตอนการโจมตีออกเป็น ๓ เฟสใหญ่ ๗ ขั้นตอนย่อย ดังนี้



ภาพที่ ๑ ตัวอย่าง Cyber Kill Chain



ภาพที่ ๒ ขั้นตอน Cyber Kill Chain

๒.๑.๑ เฟสที่ ๑ - เตรียมการโจมตี แบ่งเป็น ๒ ขั้นตอน คือ

๒.๑.๑.๑ Reconnaissance : การลาดตระเวน คือ แฮ็กเกอร์จะเริ่มต้นเก็บรวบรวมข้อมูลของเป้าหมายก่อนเริ่มการโจมตี โดยอาจค้นหาข้อมูลจากโลกอินเทอร์เน็ต หรือโซเชียลเน็ตเวิร์ค

๒.๑.๑.๒ Weaponization : เตรียมอาวุธสำหรับโจมตี โดยแฮ็กเกอร์จะเตรียมหาวิธีเจาะระบบและเตรียม Malicious Payload เพื่อส่งไปยังเหยื่อที่เล็งไว้ ขั้นตอนนี้ยังคงกระทำที่ฝั่งแฮ็กเกอร์ เหยื่อยังไม่รู้ตัวว่าจะถูกโจมตี

๒.๑.๒ เฟสที่ ๒ – บุกรุกโจมตี

๒.๑.๒.๑ Delivery : แฮ็กเกอร์ส่ง Malicious Payload ไปยังเหยื่อผ่านทางอีเมล เว็บไซต์ หรือ USB ซึ่งใน Payload นี้จะประกอบไปด้วยวิธีการบุกรุกโจมตีมากมายเพื่อใช้เจาะเข้าระบบของเหยื่อ

๒.๑.๒.๒ Exploitation : แฮ็กเกอร์ทำการเจาะระบบของเหยื่อด้วยวิธีต่าง ๆ ตาม Payload ที่ส่งมา

๒.๑.๒.๓ Installation : ติดตั้งมัลแวร์บนเครื่องของเหยื่อ (ในกรณีที่แฮ็กเกอร์ใช้มัลแวร์) หรืออะไรบางอย่างเพื่อให้คอยรับคำสั่งและทำการบางอย่างตามที่แฮ็กเกอร์ต้องการ

๒.๑.๓ เฟสที่ ๓ - เก็บเกี่ยวผลลัพธ์

๒.๑.๓.๑ Command & Control : แฮ็กเกอร์สร้างช่องทางในการรับส่งคำสั่งกับมัลแวร์ที่ติดตั้งไว้ เพื่อให้สามารถจัดการและควบคุมมัลแวร์ให้ทำตามความต้องการ

๒.๑.๓.๒ Action on Objectives : เก็บเกี่ยวผลประโยชน์ตามที่ตนเองต้องการจากระบบเครือข่ายของเหยื่อ เช่น ขโมยข้อมูล เปลี่ยนแปลงแก้ไขข้อมูล หรือทำลายระบบ เป็นต้น

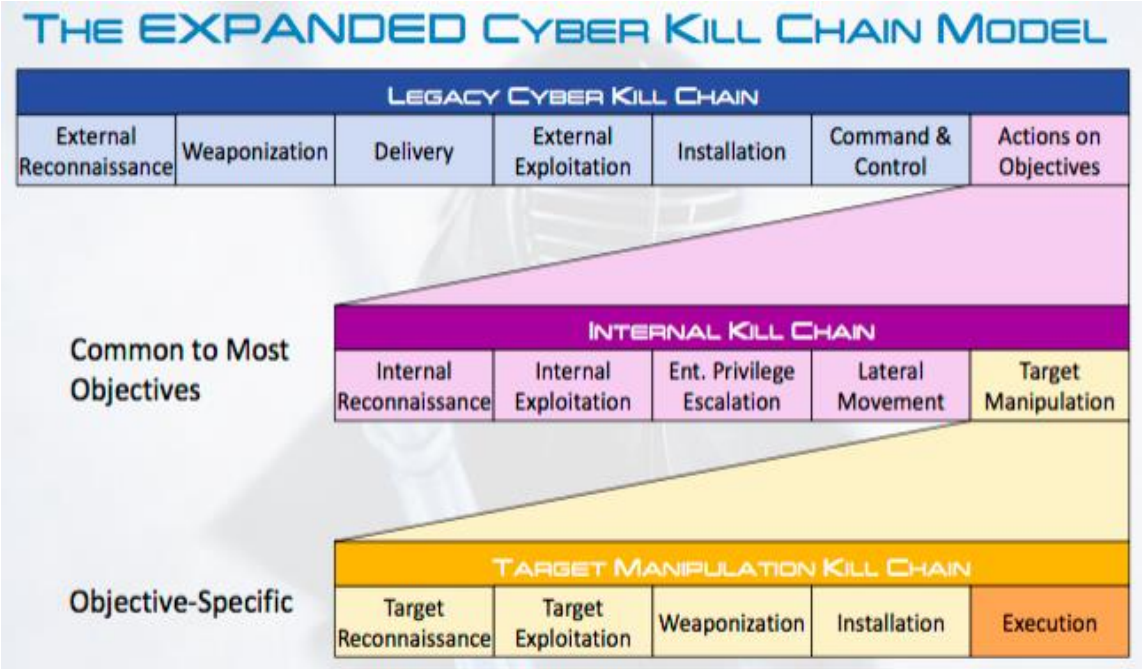
โดยปกติแล้วเฟสที่ ๑ จะใช้เวลาเตรียมการตั้งแต่หลักชั่วโมงถึงหลายเดือน เพื่อให้สามารถเจาะระบบได้เป็นผลสำเร็จ ส่วนในเฟสที่ ๒ ที่เป็นการบุกรุกโจมตีเพื่อแฝงตัวเข้าไปนั้นใช้เวลาดำเนินการเพียงไม่กี่วินาที (หรือนาที) เท่านั้น ส่วนเฟสที่ ๓ เป็นเฟสที่นานที่สุด เนื่องจากเป็นเฟสที่ค่อย ๆ แทรกซึม ทำงานตามคำสั่งจนสามารถเก็บเกี่ยวผลลัพธ์ได้ตามที่ตนเองต้องการ

๒.๒ วิธีหยุดยั้ง Cyber Kill Chain

เนื่องจาก Cyber Kill Chain เป็นขั้นตอนที่ดำเนินการอย่างต่อเนื่องเป็นลูกโซ่ นั่นหมายความว่าถ้าเราทำให้ลูกโซ่ขาดไปก็จะทำให้การโจมตีไม่เป็นผลสำเร็จทันที ซึ่งส่วนใหญ่แล้วเราจะใช้หลากหลายวิธีเข้าช่วยเพื่อพยายามตัดห่วงโซ่ทิ้งให้ได้ทุกจุด (Defense in Depth) เช่น มีระบบความปลอดภัยทางอีเมล/ต่อต้านฟิชชิ่ง (Email Security/Anti-phishing) เพื่อตรวจจับข้อมูลที่เป็นอันตราย (Malicious Payload) ในขั้นตอนที่ ๓ มีระบบ NGFW/IPS สำหรับป้องกันการแสวงหาผลประโยชน์ (Exploitation) หรือมีการป้องกันเครื่อง/โปรแกรมป้องกันไวรัส (Endpoint Protection/Antivirus) สำหรับป้องกันการติดตั้งมัลแวร์ เป็นต้น นอกจากการป้องกันแล้ว ควรมีกระบวนการ การตรวจจับ (Detection) และ การตอบสนองของเหตุการณ์ (InCIAent Response) สำหรับตรวจจับและรับมือหลังถูกบุกรุกโจมตีเข้ามาในเฟสที่ ๓ ด้วยเช่นกัน เพื่อให้สามารถกักกันระบบที่ถูกโจมตีเข้ามา และจัดการทุกอย่างให้กลับไปเป็นเหมือนเดิมได้อย่างรวดเร็ว ที่สำคัญคือการอุดช่องโหว่ที่แฮ็กเกอร์ใช้เจาะเข้ามา

๒.๓ ขั้นตอนที่เกิดขึ้นภายในระบบ The Expanded Cyber Kill Chain

เนื่องจากโมเดล Cyber Kill Chain ที่ใช้อธิบายการโจมตีไซเบอร์นั้น ล้าสมัยเกินไปแล้วในปัจจุบัน เนื่องจากไฟร์วอลล์ (Firewall) ไม่ใช่ระบบรักษาความมั่นคงปลอดภัยเดียวอีกต่อไป ควรเน้นโฟกัสสิ่งที่แฮ็กเกอร์จะทำหลังจากที่เข้ามายังระบบเครือข่ายภายในได้แล้วด้วย สมมติฐานของ Cyber Kill Chain คือ ระบบเครือข่ายมีไฟร์วอลล์ (Firewall) เป็นอุปกรณ์หลักในการป้องกันผู้บุกรุกโจมตี จึงเน้นเฉพาะการโจมตีจากภายนอกเข้าสู่ภายใน ซึ่งในปัจจุบันนี้ระบบรักษาความมั่นคงปลอดภัยมีการพัฒนาปรับเปลี่ยนไปมากไฟร์วอลล์ (Firewall) ไม่ใช่เป็นหนทางแก้ไขเดียวสำหรับรับมือกับการโจมตีไซเบอร์อีกต่อไป องค์กรควรมีการเพิ่มการป้องกันภายในระบบเครือข่ายของตนหลังจากที่แฮ็กเกอร์หลุดเข้ามาได้อีกด้วย นั่นหมายความว่า ควรมีการเพิ่มขั้นตอนให้ชัดเจนหลังจากที่แฮ็กเกอร์สามารถเจาะทะลุเข้ามาในระบบเครือข่ายได้แล้ว นั่นคือ “The Expanded Cyber Kill Chain”



ภาพที่ ๓ ตัวอย่าง The Expanded Cyber Kill Chain Model

The Expanded Cyber Kill Chain แบ่งออกเป็น ๓ เฟสใหญ่ คือ ภายนอก ภายใน และการจัดการเป้าหมาย (External, Internal and Target Manipulation)

๒.๓.๑ External (Legacy) Kill Chain คือ Cyber Kill Chain แบบดั้งเดิมที่นิยามกัน เป็นขั้นตอนการเจาะระบบเครือข่ายจากภายนอกเพื่อเข้าถึงระบบเครือข่ายภายใน แล้วจึงดำเนินกิจกรรมตามต้องการ

๒.๓.๒ Internal Kill Chain : ขั้นตอนการโจมตีของแฮ็กเกอร์หลังจากเข้ามายังระบบเครือข่ายได้แล้ว โดยแบ่งเป็น ๕ ขั้นตอนย่อย คือ

๒.๓.๒.๑ Internal Reconnaissance - ตรวจสอบระบบภายในพร้อมหาช่องโหว่อาจใช้เวลา ๑ - ๒ สัปดาห์ หรือนานกว่านั้น โดยใช้เครื่องมือล้ำสมัย เช่น Nmap, Zenmap และเพิ่มการตรวจสอบ Port ที่เปิดอยู่ของเครื่องเป้าหมายและทำการบันทึกข้อมูลเพื่อใช้ในโอกาสต่อไป เป็นต้น

๒.๓.๒.๒ Internal Exploitation - เจาะระบบภายในผ่านช่องโหว่ภายใน เช่นเดียวกับการทำ Cyber Kill Chain เช่น การใช้เครื่องมือ Metasploit เป็นต้น

๒.๓.๒.๓ Enterprise Privilege Escalation - ยกระดับสิทธิ์ของตนและสร้างความเชื่อใจ (Trust) เพื่อให้ได้สิทธิ์การเข้าถึงที่สูงยิ่งขึ้น โดยใช้เทคนิค Privilege Escalation ตามระบบปฏิบัติการของเครื่องเป้าหมาย เช่น Windows Privilege Escalation, Linux Privilege Escalation โดยใช้เครื่องมือ WinPEA และ LinPEA เป็นต้น

๒.๓.๒.๔ Lateral Movement - เมื่อได้สิทธิ์ระดับสูงแล้ว ก็ทำการค้นหาเป้าหมายที่ต้องการในพื้นที่หวงห้าม โดยการเข้าถึงจุดยุทธศาสตร์ด้านความมั่นคงปลอดภัยทางไซเบอร์ของกลุ่มเป้าหมายและทำการเข้าถึงสิ่งที่สำคัญ เช่น Credential Files เป็นต้น

๒.๓.๒.๕ Target Manipulation ทำการโจมตีเป้าหมายที่ต้องการ โดยการยิงข้อมูล (Payload) เข้าไปในพื้นที่หวงห้ามของเป้าหมาย เพื่อยกระดับสิทธิ์การเข้าถึงให้มากขึ้นและเพิ่มขีดความสามารถด้านไซเบอร์อย่างถาวร

๒.๓.๓ Target Manipulation Kill Chain : ขั้นตอนการโจมตีเป้าหมายโดยเฉพาะเจาะจงของแฮ็กเกอร์ หลังจากที่ค้นหาเป้าหมายเจอแล้ว แบ่งเป็น ๕ ขั้นตอนย่อย คือ

๒.๓.๓.๑ Target Reconnaissance ตรวจสอบและทำความเข้าใจระบบของเป้าหมาย โดยการตรวจสอบเอกสารด้านเทคโนโลยีสารสนเทศของผู้จำหน่าย การฝึกอบรมภายในซอร์สโค้ด ยูทิลิตี้ผู้ดูแลระบบมาตรฐาน

๒.๓.๓.๒ Target Exploitation - เจาะเข้าระบบเป้าหมายโดยอาศัยความเชื่อใจ (Trust) หรือเจาะผ่านช่องโหว่ โดยใช้ข้อมูลประจำตัว ระบบที่ใช้ระบบตรวจสอบสิทธิ์ส่วนกลาง

๒.๓.๓.๓ Weaponization - สร้างมัลแวร์เฉพาะสำหรับโจมตีเป้าหมายหรือหยุดกระบวนการเชิงยุทธศาสตร์ ทดสอบในสภาพแวดล้อมเป้าหมายในห้องปฏิบัติการ และแยก ถอดรหัสซอฟต์แวร์

๒.๓.๓.๔ Installation - ติดตั้งมัลแวร์บนระบบเป้าหมาย พร้อมกับการทำลายระบบตรวจจับภัยคุกคามของเครื่องเป้าหมาย

๒.๓.๓.๕ Execution - โจมตีเป้าหมายตามวัตถุประสงค์ที่ตนต้องการ และเปิดใช้งานมัลแวร์เพื่อล้มล้างการทำงานของระบบเป้าหมายให้เกิดผลลัพธ์ที่ต้องการ

หน่วยงานควรวางแผนรับมือกับ Cyber Kill Chain ในทุก ๆ ขั้นตอน เนื่องจากถ้าหยุดยั้งขั้นตอนใดขั้นตอนหนึ่งได้ ก็จะหยุดห่วงโซ่การโจมตีทั้งหมด หรือถึงแม้จะหยุดยั้งไม่ได้ ก็ยังช่วยให้แฮ็กเกอร์สามารถโจมตีได้ช้าลง และต้องลงทุนค่าใช้จ่ายมากขึ้น นอกจากนี้ทีมความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานควรวางแผนสำหรับการรายงานการถูกเจาะระบบออกสื่อต่าง ๆ การดำเนินงานกิจกรรมเกี่ยวกับกฎหมาย และรับมือกับเหตุการณ์ที่เกิดขึ้น

๒.๔ Internal Cyber Kill Chain สำหรับภัยคุกคามจากภายใน

๒.๔.๑ประเภทของ Internal Cyber Kill Chain สำหรับภัยคุกคามจากภายใน

๒.๔.๑.๑ ภัยคุกคามจากภายใน แบ่งเป็น ๒ ประเภท คือ

๒.๔.๑.๑ (๑) Flight Risks บุคลากรที่เตรียมลาออก เช่น ชอบเข้าเว็บไซต์หางาน โดยอาจเป็นเหตุให้องค์กรเกิดความเสียหายไม่ว่าจะตั้งใจหรือเริ่มละเลยต่อการรักษาความปลอดภัย

๒.๔.๑.๑ (๒) Persistent Insider เกิดจากคนที่ไม่ได้มีความประสงค์จะลาออกแต่ตั้งใจที่จะอยู่เพื่อทำความเสียหายซึ่งอาจจะมีพฤติกรรมใช้งานเว็บไซต์ผ่านตัวแทน (Proxy) หรืออื่นๆ เพื่ออำพรางการลักลอบย้ายข้อมูล เป็นต้น

๒.๔.๒ ขั้นตอนของ Internal Cyber Kill Chain สำหรับภัยคุกคามจากภายใน

เมื่อองค์กรรับทราบว่าบุคลากรมีแนวโน้มความเสี่ยงก็ควรจะต้องดูแลอย่างใกล้ชิด เช่น เมื่อบุคลากรที่เข้าเว็บไซต์สมัครงานพยายามเข้าถึงข้อมูลที่สำคัญ หรือทำการส่งข้อมูลไปยังที่แปลก ๆ เป็นต้น ดังนั้นจึงมีงานวิจัยที่พัฒนา Cyber Kill Chain เพื่อให้เหมาะสมกับภัยคุกคามจากภายในและสามารถหยุดยั้งลำดับการกระทำอันตรายได้ก่อนเกิดเหตุจริง ซึ่งมีขั้นตอนดังนี้

๒.๔.๒.๑ Reconnaissance : การโจมตีแบบสอดแนม หมายถึง ความพยายามของผู้คุกคามในการได้รับข้อมูลเกี่ยวกับเครือข่ายมากที่สุดเท่าที่จะเป็นไปได้ก่อนที่จะเริ่มการโจมตีประเภทอื่นที่ร้ายแรงกว่า การโจมตีสอดแนมจะดำเนินการโดยใช้ข้อมูลที่หาได้ง่าย ในกรณีของ Cyber Kill Chain เป็นการรวบรวมข้อมูลเกี่ยวกับสินทรัพย์เครือข่าย ไฟล์ ฐานข้อมูล และเนื้อหาอื่น ๆ ที่การโจมตีอาจต้องใช้ข้อมูลนั้นเพื่อตัดสินใจ

๒.๔.๒.๒ Access : เพื่อให้ผู้โจมตีดำเนินการโจมตีได้ พวกเขาต้องได้รับสิทธิ์ในการเข้าถึงข้อมูลที่ต้องการขโมย หากไม่สามารถเข้าถึงได้ตามข้อมูลประจำองค์กร ผู้โจมตีจะมองหาการป้องกันจากทีมไอทีเพื่อป้องกันไม่ให้ผู้อื่นเข้าถึงข้อมูลที่พวกเขาไม่ได้รับอนุญาต

๒.๔.๒.๓ Aggregation : เมื่อผู้โจมตีสามารถเข้าถึงข้อมูลเป้าหมายได้ พวกเขาสามารถรวมข้อมูลเป้าหมายและเตรียมพร้อมสำหรับการดึงข้อมูลเป้าหมายออกจากระบบฐานข้อมูลในสภาพแวดล้อมที่แตกต่างกัน

๒.๔.๒.๔ Assembly : เป็นขั้นตอนการเตรียมการข้อมูล เช่น เตรียมการส่งข้อมูลผ่านการเชื่อมต่อเข้ารหัสหากต้องการนำออกไปภายนอก หรือเอาไดรฟ์มาเสียบเพื่อเตรียมส่งข้อมูลออก เป็นต้น

๒.๔.๒.๕ Encryption : การย้ายข้อมูลไปยังที่เก็บข้อมูลชั่วคราว เพื่อเข้ารหัสข้อมูลและเตรียมข้อมูลที่จะส่งผ่านอินเทอร์เน็ตเพื่ออัปโหลดไปยังที่เก็บนอกสถานที่

๒.๔.๒.๖ Obfuscation : กลบเกลื่อนร่องรอยโดยอาจใช้ข้อมูลประจำตัว (Credentials) ที่ถูกแชร์หรือบุคคลอื่นเพื่อตามกลับได้ยาก หรือแม้กระทั่งเข้าไปแก้ไข Log เพื่อทำลายร่องรอย

๒.๔.๒.๗ Exfiltration : เริ่มนำข้อมูลออกจากองค์กรได้จากหลายกรณี เช่น Flash Drive, External Hard Drive, เครื่องคอมพิวเตอร์ส่วนตัวที่เข้าถึงเครือข่ายได้, Cloud Storage, อีเมลหรืออื่น ๆ เป็นต้น

สำหรับแฮ็กเกอร์ที่ชาญชลาดมักจะไม่เร่งรีบในการนำข้อมูลออก เพราะอาจถูกพบได้ง่าย เนื่องจากมีพฤติกรรมการใช้งานที่ผิดปกติแต่จะเลือกจังหวะที่เหมาะสมหรือทยอยนำข้อมูลออกอย่างแนบเนียน อย่างไรก็ตามทั้งสองรูปแบบ Cyber Kill Chain มีจุดประสงค์เดียวกันนั่นคือหากหยุดยั้งแค่ขั้นตอนใดขั้นตอนหนึ่งได้ ก็สามารถหยุดการโจมตีได้

๒.๕ การรับมือ Cyber Kill Chain ด้วย Cyber Resilience

๒.๕.๑ ความหมายของ Cyber Resilience

Cyber Resilience หมายถึง ความสามารถในการเตรียมตัวและการปรับตัวต่อการเปลี่ยนแปลง และความทนทานต่อการบุกรุก โจมตี รวมถึงความสามารถในการคืนสภาพของระบบ

จากคำนิยามศัพท์ในเอกสาร Presidential Policy Practice : Critical Infrastructure. Security and Resilience (PPD- 21) โดยทำเนียบขาว รัฐบาลสหรัฐได้ให้คำจำกัดความคำว่า “Security” แตกต่างจากคำว่า “Resilience” ดังนี้

๒.๕.๑.๑ Security หมายถึง การลดความเสี่ยงให้กับโครงสร้างพื้นฐานทั้งทางกายภาพและทางไซเบอร์ มุ่งเน้นไปที่การบริหารจัดการ การบุกรุก การโจมตี รวมทั้งภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้นทั้งตั้งใจและไม่ได้ตั้งใจ เช่น การก่อการร้าย หรือการโจมตีทางไซเบอร์ เป็นต้น

๒.๕.๑.๒ Resilience หมายถึง ความสามารถในการเตรียมตัวและการปรับตัวต่อการเปลี่ยนแปลง รวมทั้งความสามารถในการทนทานต่อการบุกรุก การโจมตี รวมถึงความสามารถในการคืนสภาพของระบบ ไม่ว่าจะเป็นการโจมตีที่เกิดจากภัยธรรมชาติและภัยที่มนุษย์ได้ก่อขึ้นทั้งตั้งใจและไม่ได้ตั้งใจ

ดังนั้น จะเห็นได้ว่าความหมายของคำว่า Resilience มีความหมายลึกซึ้งกว่าคำว่า Security และเมื่อพูดถึง “Cybersecurity” ก็ไม่ได้มีคำจำกัดความอย่างชัดเจนมาก่อน (แต่ในปัจจุบัน MITRE Corporation ได้นิยามไว้ในเอกสาร Cyber Resiliency Design Principles, January 2017) ซึ่งเข้าใจโดยรวมว่า “Cybersecurity” หมายถึง ความมั่นคงปลอดภัยทางไซเบอร์ ที่ไม่ใช่ความมั่นคงปลอดภัยทางกายภาพ เช่น ประตูรั้ว การล็อคประตูบ้าน ประตูรถ หากแต่หมายถึงความมั่นคงปลอดภัยในการนำคอมพิวเตอร์และระบบสารสนเทศมาใช้ รวมถึงความมั่นคงปลอดภัยในการใช้งานอินเทอร์เน็ตผ่านอุปกรณ์เคลื่อนที่ต่าง ๆ ในปัจจุบัน ดังเช่น สมาร์ทโฟน เป็นต้น โดยสภาวะไซเบอร์นั้นยากที่จะควบคุมได้ ไม่เหมือนกับทางกายภาพที่สามารถกำหนดขอบเขตในการควบคุมได้อย่างชัดเจน ดังนั้น “Cybersecurity” จึงบริหารจัดการยากกว่า “Physical Security” หรือ “Conventional Security”

๒.๕.๒ กระบวนการรับมือ Cyber Kill Chain ด้วย Cyber Resilience

ในปัจจุบันภัยไซเบอร์มีความสลับซับซ้อนมากขึ้น เนื่องจากมีการโจมตีในลักษณะ APT (Advanced Persistent Threat) ที่สนับสนุนโดยรัฐบาลของประเทศต่าง ๆ ในทางลับ ที่เรียกกันว่า “State- Sponsored Attack” และมีการขายช่องโหว่ที่ผู้ผลิตยังไม่ถูกค้นพบ ซึ่งเรียกว่า “Zero-Day Exploit” ในตลาดมืด หรือในดาร์กเว็บ (Dark Web) อีกทั้งหลายผลิตภัณฑ์ยังฝังประตูหลัง (Backdoor) มาจากโรงงาน โดยการร่วมมือกับรัฐบาลในประเทศผู้ผลิต และยังไม่รวมโปรแกรมเจาะช่องโหว่ผู้ผลิตยังไม่ถูกค้นพบที่หลุดออกมาจากกลุ่มแฮ็กเกอร์ ที่นำมาปล่อยให้ดาวน์โหลดกันทั่วไป ซึ่งจะเห็นได้ว่าในปัจจุบันและอนาคตไม่ใช่แค่ “IT Security” หรือ “Information Security” แต่รวมถึง “OT Security” (Operational Security) ที่ครอบคลุมไปถึงระบบ SCADA/ICS ตลอดจน IoT Security (Internet of Thing Security) ที่มีการเจาะระบบกัน แม้กระทั่งการเจาะกล้องวงจรปิด เช่น มัลแวร์ Mirai Botnet ที่เจาะ CCTV มาทำการโจมตีในรูปแบบ DDoS Attack เป็นต้น จึงไม่มีระบบออนไลน์ระบบใดที่ปลอดภัย ๑๐๐% ทุกระบบมีสิทธิ์ถูกเจาะตลอดเวลา ดังนั้นองค์กรจึงควรเตรียมการรับมืออยู่เสมอ จึงเป็นที่มาของแนวคิด “Cyber Resilience” ในที่สุด

กระบวนการเพื่อให้เกิด Cyber Resilience โดยเฉพาะองค์กรที่มีความเกี่ยวข้องกับโครงสร้างพื้นฐานที่สำคัญ (Critical Infrastructure) นั้นควรให้ความสำคัญกับ ๓ เรื่องใหญ่ ๆ ได้แก่

๒.๕.๒.๑ Threat Models จะเน้นไปที่ Cyber Attack Lifecycle หรือ Cyber Kill Chain ซึ่งเจ้าหน้าที่ทางไซเบอร์ควรจะทำความเข้าใจกับภัยไซเบอร์ให้ถ่องแท้ รวมถึงกระบวนการที่จะเกิดการโจมตีทางไซเบอร์

๒.๕.๒.๒ Threat Information หมายถึง การติดตามข่าวสารภัยไซเบอร์ต่าง ๆ และติดตามเทคนิคใหม่ ๆ ของแฮ็กเกอร์ และการหาประโยชน์จากช่องโหว่วันแรก (Zero Day Exploit) ที่หลุดออกมา ตลอดจนเรื่อง CTI (Cyber Threat Intelligence) รวมถึงเรื่องการแชร์ Threat Information ในรูปแบบการรวมตัวกันเป็น ISAC (Information Sharing and Analysis Center)

๒.๕.๒.๓ Frameworks หมายถึง การนำ NIST Cybersecurity Framework และ Cyber Resiliency Engineering Framework (CREF) มาใช้ในการบริหารจัดการปัญหาภัยไซเบอร์ที่มีความสลับซับซ้อนและรุนแรงขึ้น จะเห็นได้ว่าการบริหารจัดการกับภัยไซเบอร์ในปัจจุบันนิยมบริหารจัดการในลักษณะ “Threat Orientated Approach” ที่กำลังเป็นทิศทางของหลายองค์กรในโลกนี้ โดยมี Security Mindset ที่ว่า “ไม่มีระบบใดในโลกนี้ที่ปลอดภัยทั้งหมด” จึงต้องมีการนำหลักการ Cyber Resilience หรือ Cyber Resiliency เข้ามาใช้ในการเตรียมรับมือกับภัยไซเบอร์ของวันนี้และอนาคต

บทที่ ๓ การตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค

๓.๑ นิยามและความหมาย

การตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค (Red Teaming) เป็นการตรวจสอบความปลอดภัยของสินทรัพย์ (Asset) ด้านสารสนเทศของหน่วยงานที่รับการตรวจสอบแบบเสมือนจริง โดยไม่จำกัดขอบเขตหรือวิธีการ ซึ่งทางเจ้าหน้าที่ผู้ดำเนินการทดสอบจะดำเนินการค้นหาจุดอ่อนของระบบและจำลองการโจมตี ด้วยวิธีการที่ใกล้เคียงกับสถานการณ์จริงของฝ่ายตรงข้าม (แฮ็กเกอร์) เพื่อยกระดับมาตรการรักษาความปลอดภัยและลดความเสี่ยงให้แก่ระบบสารสนเทศที่สำคัญขององค์กร

๓.๒ วัตถุประสงค์

๓.๒.๑ เพื่อให้เป็นไปตาม พ.ร.บ.ความมั่นคงไซเบอร์ พ.ศ.๒๕๖๒ ซึ่งกำหนดให้หน่วยงานด้านความมั่นคงของรัฐบาลเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องมีการเฝ้าระวังรับมือและแก้ไขภัยคุกคามทางไซเบอร์ ซึ่ง กห., บก.ทท. และ เหล่าทัพ ได้มีการกำหนดความรับผิดชอบงานด้านการปฏิบัติการไซเบอร์ และรับมือภัยคุกคามทางไซเบอร์ระดับวิกฤต โดยเป็นส่วนหนึ่งของการปฏิบัติการร่วมทางไซเบอร์ในภาพรวมของ กห.ใช้ขีดความสามารถทางไซเบอร์เพื่อตอบสนองความต้องการทางยุทธการและปกป้องมิติไซเบอร์ของเหล่าทัพ

๓.๒.๒ เพื่อสร้างขีดความสามารถของหน่วยงานไซเบอร์ให้สามารถดำเนินการ ประเมินและตรวจสอบความมั่นคงปลอดภัยเครือข่ายระบบสารสนเทศของหน่วยขึ้นตรง

๓.๒.๓ เพื่อให้หน่วยมีขีดความสามารถในการจัดการกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบสารสนเทศของหน่วย

๓.๒.๔ เพื่อให้หน่วยรับรู้ถึงช่องโหว่ในระบบสารสนเทศ และดำเนินการแก้ไขเพื่อให้ระบบสารสนเทศเกิดความมั่นคงปลอดภัยพร้อมใช้งาน ส่งผลให้กองทัพอากาศมีความมั่นคงปลอดภัยด้านไซเบอร์

๓.๒.๕ เสริมสร้างขีดความสามารถกำลังพลกองทัพอากาศ ให้มีองค์ความรู้ในการปฏิบัติการข่าวกรองทางไซเบอร์ และการปฏิบัติการไซเบอร์เชิงรุก รองรับการปฏิบัติการหลายมิติ และพัฒนาระบบบริหารจัดการข่าวกรองไซเบอร์ (Cyber Threat Intelligence: CTI) ตลอดจนจัดการฝึกบังคับบัญชาและสั่งการต่อสถานการณ์สมมุติด้านการป้องกันระบบสารสนเทศที่สำคัญของกองทัพอากาศจากภัยคุกคามทางไซเบอร์

๓.๓ การรักษาความมั่นคงปลอดภัยไซเบอร์

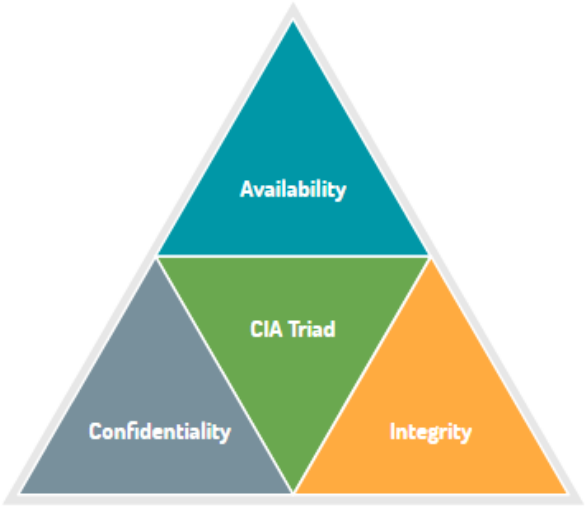
การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า“มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ”

ซึ่งการตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค (Red Teaming) นั้น จะเป็นการตรวจสอบเพื่อให้ระบบสารสนเทศของหน่วยรับตรวจ มีความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วยคุณลักษณะ ๓ ประการ ได้แก่

๓.๓.๑ Confidentiality คือ สิทธิ์ในการเข้าถึงข้อมูล ข้อมูลจะต้องเข้าถึงได้โดยผู้ที่มีสิทธิ์เท่านั้น

๓.๓.๒ Integrity คือ ความถูกต้องของข้อมูล ข้อมูลที่ถูกส่ง หรือจัดเก็บ จะต้องไม่ถูกแก้ไขโดยผู้ที่ไม่มีสิทธิ์

๓.๓.๓ Availability คือ ความพร้อมใช้งาน ไฟล์ หรือ ข้อมูลต้องเข้าถึงได้ตลอดเวลา จากบุคคลที่มีสิทธิ์



ภาพที่ ๔ CIA TRIAD

๓.๔ เอกสารและมาตรฐานที่เกี่ยวข้อง

เพื่อให้การตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิคมีความเป็นมาตรฐานในระดับสากล จึงดำเนินการโดยยึดหลักการตามเอกสารและมาตรฐานต่าง ๆ ดังนี้

๓.๔.๑ ระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ เป็นระเบียบที่ใช้บังคับแก่หน่วยขึ้นตรงกองทัพอากาศ บุคคลในสังกัดกองทัพอากาศ รวมทั้งบุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของกองทัพอากาศ

๓.๔.๒ National Institute of Standards and Technology (NIST) 800-115 : Technical Guide to Information Security Testing and Assessment เป็นคู่มือสำหรับองค์กรในการวางแผนและดำเนินการทางเทคนิคที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล ใช้เพื่อประเมิน ทดสอบ วิเคราะห์ ค้นหา และสร้างแผนบรรเทาภัยโดยสามารถนำไปใช้ได้ในหลาย ๆ จุดประสงค์ เช่น การหาช่องโหว่ในระบบหรือในเครือข่าย และการตรวจสอบอุปกรณ์กับนโยบายหรือความต้องการต่าง ๆ เป็นต้น ซึ่งจะเน้นไปที่ภาพรวมขององค์ประกอบหลักของการทดสอบและการประเมินความปลอดภัย

๓.๔.๓ MITRE ATT&CK : Design and Philosophy เป็นแพลตฟอร์มจัดการและจัดหมวดหมู่ของกลยุทธ์ เทคนิค และกระบวนการ (Tactics, Techniques, and Procedures : TTP) ที่แฮ็กเกอร์ใช้ในโลกดิจิทัล ช่วยให้หน่วยงานสามารถเพิ่มความปลอดภัยไซเบอร์ได้

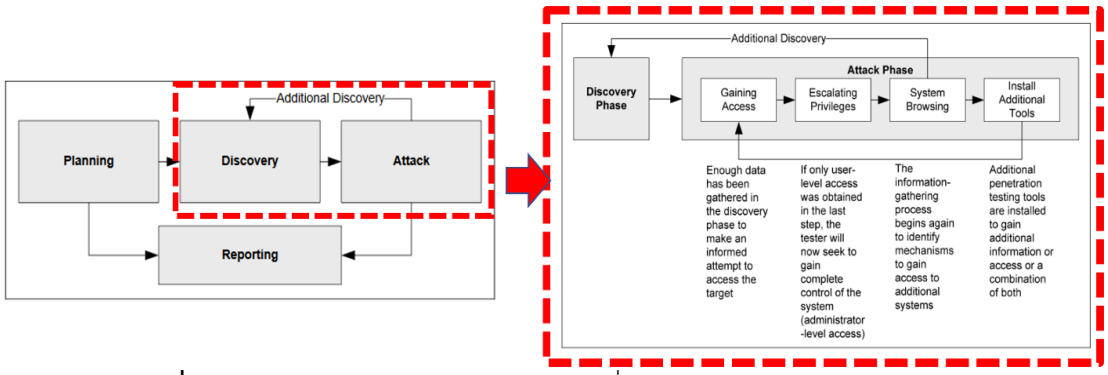
๓.๔.๔ The Penetration Testing Execution Standard (PTES) เป็นกรอบการปฏิบัติงานที่อธิบายในการทำทดสอบเจาะระบบ ทั้งในมุมมองทางธุรกิจและด้านความปลอดภัย โดยจะแบ่งเป็น ๗ หัวข้อหลัก แยกเนื้อหาทางทฤษฎีและคำแนะนำการปฏิบัติทางเทคนิค รวบรวมจากบุคลากร

ที่ทำงานด้านความมั่นคงปลอดภัยไซเบอร์จากหลายบริษัทชั้นนำ (Tenable Security, Lares Consulting และอื่น ๆ) รวมถึงบุคลากรจาก SANS ที่มาร่วมสร้างและตรวจสอบ PTES โดยตัวกรอบการปฏิบัติงานนี้ได้รับการกล่าวถึงจากหน่วยงานความปลอดภัย เช่น OWASP, CREST และหน่วยงานอื่น ๆ ทำให้เอกสารนี้มีความน่าเชื่อถือสูง ส่วนการแบ่งหัวข้อและข้อความต่าง ๆ ของ PTES นั้น มีการแบ่งข้อความที่ดูง่ายแบ่งหัวข้อชัดเจน

๓.๔.๕ OWASP Web Security Testing Guide เป็นมาตรฐานความปลอดภัยของเว็บไซต์แอปพลิเคชัน จัดทำขึ้นโดยองค์กรไม่แสวงหากำไรที่ให้ความรู้เพื่อทำให้ระบบคอมพิวเตอร์มีความปลอดภัยมากยิ่งขึ้นและเน้นวิจัยทางด้านความมั่นคงปลอดภัยเว็บไซต์แอปพลิเคชัน โดยจะมีชุมชนในด้านการแลกเปลี่ยนข่าวสาร เอกสารทางเทคนิค และเครื่องช่วยเหลือต่าง ๆ ซึ่งตัว OWASP จะมีโครงการหนึ่งที่จัดอันดับ ๑๐ ความเสี่ยงด้านความปลอดภัย เช่น การโจมตีทั้งแอปพลิเคชัน IoT และ Cloud ต่าง ๆ เป็นต้น ที่ถูกเรียกว่า OWASP TOP 10

๓.๕ แนวทางการดำเนินการ

การตรวจสอบจะประกอบด้วย ๒ ห้วง ได้แก่ Discovery Phase และ Attack Phase ซึ่งสามารถแยกเป็นกระบวนการย่อยได้ตามภาพที่ ๕ โดยมีรายละเอียดดังนี้



ภาพที่ ๕ แผนการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค

๓.๕.๑ การค้นหาเป้าหมาย (Discovery Phase) ดำเนินการด้วยเครื่องมือประเภท Host Discover ได้แก่ Netdiscover, Nmap, Advanced IP Scanner และ SoftPerfect Network Scanner รวมถึงการเก็บข้อมูลเชิงลึก เช่น ระบบปฏิบัติการของเป้าหมาย และช่องทางการให้บริการ เป็นต้น

๓.๕.๒ การเข้าสู่ระบบ (Gaining Access) ดำเนินการโดยนำข้อมูลที่ได้รวบรวมจากเป้าหมายมาพิจารณาหนทางการโจมตี (Attack Vector) และเลือกใช้ช่องโหว่ที่มีความเป็นไปได้ เพื่อกำหนดอาวุธ (Payload) ที่จะกระทำกับเป้าหมาย

๓.๕.๓ การยกระดับสิทธิ์ (Escalating Privileges) ในขั้นตอนนี้สามารถดำเนินการได้ก็ต่อเมื่อสิทธิ์ที่ได้รับหลังจากการเข้าสู่ระบบเป็นสิทธิ์ผู้ใช้งานปกติ และดำเนินการด้วยการนำช่องโหว่หรืออาวุธอื่น เข้ากระทำกับเป้าหมายเพื่อให้ได้รับสิทธิ์ที่สูงขึ้น เช่น สิทธิ์ของผู้ดูแลระบบ (Administrator) เป็นต้น ซึ่งจะสามารถดำเนินการกับเป้าหมายได้มากขึ้น เช่น การปิดระบบป้องกันไวรัสเพื่อคงสภาพการเข้าถึงระบบ หรือแก้ไขการตั้งค่าภายในระบบ/โปรแกรมอื่น เป็นต้น

๓.๕.๔ การค้นหาข้อมูลเพิ่มเติมภายในเครื่อง (System Browsing) เป็นการดำเนินการเพื่อรวบรวมข้อมูลเพิ่มเติม เช่น ข้อมูลระบบ (System Information) ข้อมูลการแชร์ไฟล์ ข้อมูลด้านเครือข่ายและการเชื่อมต่อ เป็นต้น ซึ่งจะเป็นประโยชน์ในการค้นหาและโจมตีเป้าหมายอื่น ๆ โดยอาศัยข้อมูลที่ได้จากการดำเนินการในขั้นตอนนี้

๓.๕.๕ การติดตั้งเครื่องมือเสริม (Install Additional Tools) ดำเนินการโดยการติดตั้งโปรแกรมเพิ่มเติม เช่น การติดตั้งโปรแกรมดูประวัติการเข้าใช้งานเว็บไซต์ ติดตั้งโปรแกรมดูรหัสผ่านที่จัดเก็บในระบบ หรือ ติดตั้งโทรจันเพื่อคงสภาพการเข้าถึงระบบ เป็นต้น

๓.๖ ประเภทของการตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค

๓.๖.๑ การตรวจสอบเครือข่ายอินเทอร์เน็ตไร้สายเป็นการตรวจสอบด้วยวิธีการขับรถไปในอาณาบริเวณที่ต้องการตรวจสอบเพื่อหาจุดปล่อยสัญญาณ Wifi ที่ไม่ปลอดภัย (Wardriving)

๓.๖.๒ การตรวจสอบเครื่องคอมพิวเตอร์ภายในหน่วยงาน

๓.๖.๒.๑ การตรวจสอบด้วยชุดคำสั่ง (Scripts) เพื่อค้นหาเครื่องคอมพิวเตอร์ที่ไม่ปลอดภัย จะดำเนินการด้วยการสุ่มตรวจเครื่องด้วยชุดคำสั่งที่ทาง ศซบ.ทอ.ได้พัฒนาขึ้นเพื่อรวบรวมข้อมูลหาเครื่องคอมพิวเตอร์ที่ไม่ปลอดภัย เช่น ใช้วินโดว์ที่ล้าสมัย และไม่มีการติดตั้งโปรแกรม Antivirus เป็นต้น

๓.๖.๒.๒ การตรวจสอบด้วยวิธีจำลองการเจาะระบบ ดำเนินการด้วยวิธีการจำลองตนเองเสมือนเป็นแฮ็กเกอร์ หรือข้าศึก เพื่อเข้ากระทำกับทรัพยากรสารสนเทศของหน่วยงาน

๓.๖.๓ การตรวจสอบ Web Application ภายในหน่วยงาน ดำเนินการตามมาตรฐาน OWASP Web Security Testing Guide เพื่อค้นหาช่องโหว่ของเว็บไซต์ที่ใช้ในหน่วยงาน

ภาพที่ ๖ ตัวอย่างการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์เชิงเทคนิค

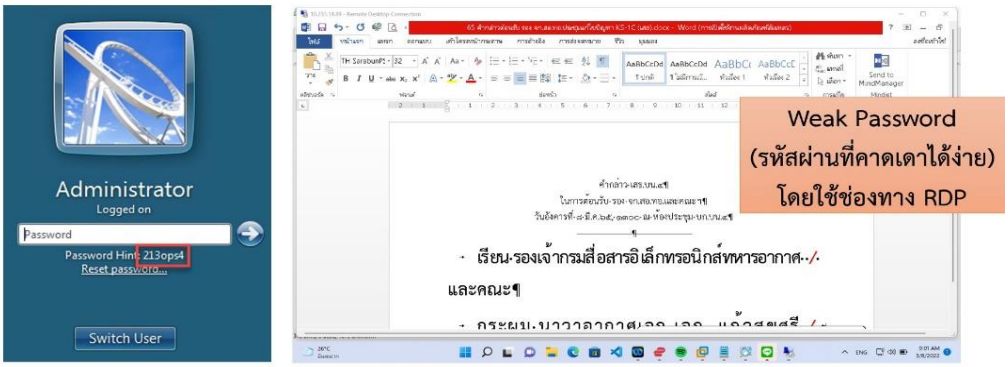
๓.๗ แนวทางการสรุปผล

๓.๗.๑ การค้นพบช่องโหว่ของระบบ (Findings) เช่น รายละเอียดของช่องโหว่ที่พบว่ามีช่องโหว่อะไรบ้าง ช่องโหว่ที่พบมีระดับความปลอดภัยอยู่ที่เท่าไหร่ เป็นต้น

๓.๗.๒ การประเมินความรุนแรงและผลกระทบ (Severities & Impacts) ควรประเมินความรุนแรงของความเสี่ยงที่เกิดจากช่องโหว่ โดยประเมินว่าแต่ละปัจจัยเสี่ยงนั้น มีโอกาสที่จะเกิดมากน้อยเพียงใด และหากเกิดขึ้นแล้วจะส่งผลกระทบต่อหน่วยงานรุนแรงมากน้อยเพียงใด

๓.๗.๓ การแก้ไขและคำแนะนำเพิ่มเติม (Recommendations) คือการลดความเสี่ยงโดยรวมของหน่วยงานโดยการลดช่องโหว่ให้ได้มากที่สุด เพราะว่าทรัพยากรสำหรับการแก้ไขที่มีอยู่จำกัด การจัดการช่องโหว่ควรเป็นกระบวนการต่อเนื่องเพื่อคอยตามภัยคุกคามใหม่และที่กำลังเกิดขึ้นและสภาพแวดล้อมที่เปลี่ยนแปลง

เมื่อพบช่องโหว่ในระหว่างดำเนินการตรวจสอบ เจ้าหน้าที่จะดำเนินการบันทึกภาพหน้าจอ (Screenshot) เพื่อยืนยันถึงวิธีในการค้นพบช่องโหว่นั้น (ภาพที่ ๗)



ภาพที่ ๗ ตัวอย่างการค้นพบช่องโหว่ของเครื่องเป้าหมาย

หากช่องโหว่นั้นสามารถสร้างความเสียหายหรือมีผลกระทบให้เจ้าหน้าที่ดำเนินการเพิ่มเติมได้ เจ้าหน้าที่จะดำเนินการบันทึกภาพหน้าจอเพิ่มเติมด้วย เช่น ช่องโหว่ MS17- 010 EternalBlue ที่เป็นช่องโหว่ที่มีความรุนแรงสูง เมื่อโจมตีสำเร็จ ผู้โจมตีจะได้สิทธิ์ในการเข้าควบคุมเครื่องโดยสมบูรณ์ (Fully Compromised) และสามารถดำเนินการเพิ่มเติมได้ ได้แก่ ลักลอบสำเนาข้อมูลของเป้าหมายไว้ในเครื่องตนเอง หรือลักลอบจับภาพจากกล้อง Web Camera เป็นต้น (ภาพที่ ๘)

MS17-010

ภาพที่ ๘ ตัวอย่างผลกระทบจากช่องโหว่ MS17- 010 EternalBlue

ในส่วนของการแก้ไขและคำแนะนำเพิ่มเติม จะดำเนินการในลักษณะสรุปเป็นตาราง แยกตามช่องโหว่ที่พบ (ภาพที่ ๙)

ช่องโหว่	วิธีการแก้ไข
Weak Password (รหัสผ่านที่คาดเดาได้ง่าย)	- ทำการตั้งรหัสผ่านให้ยากต่อการเข้าถึง โดยผู้ที่ไม่มีสิทธิ์ - เปลี่ยนรหัสผ่านให้มีความซับซ้อนยิ่งขึ้น - หากเครื่องใดมีความสำคัญต่อระบบโดยรวม ควรตั้งรหัสผ่านแยกโดยเฉพาะ - ทำการเปลี่ยนรหัสผ่านเป็นระยะ
SQL Injection	- ตรวจสอบระบบที่ใช้งานหรือกำลังพัฒนา ให้มีการตรวจสอบการกรอกข้อมูล ในช่องรับข้อมูลต่าง ๆ ก่อนจะส่งข้อมูลนั้นไปประมวลผลที่เครื่องแม่ข่าย
MS17-010 EternalBlue	- อัพเดทเวอร์ชั่นระบบปฏิบัติการให้มีความทันสมัย - ปิดการใช้งาน SMBv1 หากไม่มีความจำเป็นในการใช้งาน - ติดตั้งโปรแกรมป้องกันไวรัส

ภาพที่ ๙ ตัวอย่างการแก้ไขและคำแนะนำเพิ่มเติม แยกตามช่องโหว่

เอกสารอ้างอิง

Techtalkthai. (2559). ทำความรู้จัก Cyber Kill Chain ขั้นตอนการเจาะระบบเพื่อโจมตีเป้าหมาย. สืบค้น 5 มกราคม 2566, จาก https://www.techtalkthai.com/introduction-to-cyber-kill-chain/

Blackhat USA. (2559). Using An Expanded Cyber Kill Chain Model To Increase Attack Resiliency. สืบค้น 5 มกราคม 2566, จาก https://www.seantmalone.com/docs/us-16-Malone-Using-an-Expanded-Cyber-Kill-Chain-Model-to-Increase-Attack-Resiliency.pdf

Techtalkthai. (2559). Cyber Kill Chain แบบเดิมล้าสมัยแล้ว ควรเพิ่มขั้นตอนที่เกิดขึ้น “ภายใน” เข้าไปด้วย. สืบค้น 5 มกราคม 2566, จาก https://www.techtalkthai.com/cyber-kill-chain-should-focus-on-internal-activities/

Giora Engel. (2557). Deconstructing The Cyber Kill Chain. สืบค้น 5 มกราคม 2566, จาก https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain

Blackhat USA. (2559.Using An Expanded Cyber Kill Chain Model To Increase Attack Resiliency. สืบค้น 5 มกราคม 2566, จาก https://www.seantmalone.com/docs/us-16-Malone-Using-an-Expanded-Cyber-Kill-Chain-Model-to-Increase-Attack- Resiliency.pdf

Tim Greene. (2559). Why the ‘cyber kill chain’ needs an upgrade. สืบค้น 5 มกราคม 2566, จาก https://www.networkworld.com/article/3104542/why-the-cyber-kill-chain-needs-an-upgradesecurity-pros-need-to-focus-more-on-catching-attackers-aft.html

หนังสือพิมพ์กรุงเทพธุรกิจ. (2561). ทำความรู้จัก Cyber Kill Chain ขั้นตอนการเจาะระบบเพื่อโจมตีเป้าหมาย. สืบค้น 5 มกราคม 2566, จาก https://www.prinya.org/2022/02/11/cyber-resilience

Techtalkthai. (2562). โมเดล Cyber Kill Chain สำหรับภัยคุกคามจากภายใน. สืบค้น 5 มกราคม 2566, จาก https://www.techtalkthai.com/introduction-internal-cyber-kill-chain-model-byalienvault/

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. (2563). ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.2563. สืบค้นเมื่อ 2566, จาก https://dict.rtaf.mi.th/index.php/

NIST SP 800-115. (2564). National Institute of Standards and Technology (NIST). สืบค้น 5 มกราคม 2566, จาก https://www.nist.gov/privacy-framework/nist-sp-800-115

BLAKE STROM. (2563). MITRE ATT&CK: Design and Philosophy. สืบค้น 5 มกราคม 2566, จาก https://www.mitre.org/news-insights/publication/mitre-attck-design-andphilosophy

Penetration Testing Execution Standard. (2555). PTES Technical Guidelines. สืบค้น 5 มกราคม 2566, จาก http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines

Web Security Testing Guide project. (2566). WSTG-v4.2. สืบค้น 5 มกราคม 2566, จาก https://owasp.org/www-project-web-security-testing-guide/v42/