มาตรการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ บก.ทท. และ ศบท.

ผบ.ทสส. ได้กรุณาสั่งการในการประชุมหัวหน้าส่วนราชการ ครั้งที่ ๗/๖๓ (พ.ค.๖๓) ให้ ศซบ.ทหาร เปลี่ยนข้อพึงระวังที่จะไม่ให้เกิดเหตุการณ์ด้านไซเบอร์ขึ้น ไปเป็นข้อปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ บก.ทท. โดยให้ ศซบ.ทหาร นำเสนอในที่ประชุม หน.ส่วนราชการ ครั้งที่ ๘/๒๕๖๓

ศซบ.ทหาร ได้จัดการประชุมร่วมกับหน่วยงานต่าง ๆ ภายใน บก.ทท. ที่เกี่ยวข้องเมื่อ ๑๕ พ.ค.๖๓ เพื่อร่วมกันพิจารณากำหนดมาตรการในการดำเนินการที่เกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศ เพื่อไม่ให้เกิดช่องโหว่ที่จะนำไปสู่ภัยคุกคามทางไซเบอร์ต่อ บก.ทท. และได้นำเรียน ผบ.ทสส. ในการประชุมหัวหน้าส่วนราชการ ครั้งที่ ๘/๖๓ (มิ.ย.๖๓) โดยสรุปเป็นมาตรการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ นขต.บก.ทท. จะต้องปฏิบัติตาม จำนวนทั้งสิ้น ๑๐ ข้อ ดังนี้

๑. ให้ นขต.บก.ทท. ทุกหน่วยทำบัญชีสถานภาพเครื่องคอมพิวเตอร์และโปรแกรมปฏิบัติการหลักของเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วย ทั้งที่จัดหาโดยทางราชการ และที่หน่วยจัดหาเอง รวมทั้งเครื่องคอมพิวเตอร์ส่วนตัวของกำลังพลที่จะนำมาเชื่อมต่อกับระบบ C4I และ MIS ทั้งนี้ ผู้ที่ทำหน้าที่นายทหารรักษาความมั่นคงปลอดภัยทางไซเบอร์หรือ Cyber Security Officer หรือ CSO ของหน่วย จะต้องทำการรวบรวมข้อมูลตามแบบฟอร์มที่ ศซบ.ทหาร กำหนดส่งให้กับ ศซบ.ทหาร อีกทั้งให้เก็บข้อมูลดังกล่าวไว้รับการตรวจประเมินมาตรฐานฯ จาก ศซบ.ทหาร ต่อไป

๒. คอมพิวเตอร์ทุกเครื่องของ นขต.บก.ทท. จะต้องติดตั้งซอฟต์แวร์รักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างน้อย ๒ ชนิด ได้แก่ McAfee Antivirus, Threat Protection System (TPS) Endpoint Security โดยดำเนินการดังนี้

๒.๑ นายทหารรักษาความมั่นคงปลอดภัยทางไซเบอร์หรือ CSO ของหน่วย ภายใต้การกำกับดูแลของผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูงหรือ Chief Information Security Officer หรือ CISO ของหน่วย จะต้องวางแผนการติดตั้งซอฟต์แวร์ในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้เรียบร้อย

๒.๒ ทั้งนี้ นขต.บก.ทท. ทุกหน่วย สามารถดาวน์โหลดและติดตั้งซอฟต์แวร์เพื่อการรักษาความปลอดภัยทางไซเบอร์ ตามคู่มือที่ ศซบ.ทหาร กำหนดให้ ได้ที่เว็บไซต์หลักของ บก.ทท.

๒.๓ ให้นายทหารรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วย รายงานผลการติดตั้งฯ ถึง ผบ.หน่วย พร้อมทั้งสำเนาผลการติดตั้งให้ ศซบ.ทหาร ทราบ

๓. ห้ามเชื่อมต่อหน่วยความจำภายนอก เช่น External Hard Disk, Thumb Drive เข้ากับเครื่องคอมพิวเตอร์ในระบบ C4I และ MIS ที่มิได้ติดตั้งซอฟต์แวร์รักษาความปลอดภัยโดยเด็ดขาด โดย สส.ทหาร จะต้องจัดเตรียมระบบ Shared Drive ระบบ Cloud Storage และระบบอีเมล เพื่อทดแทนการเชื่อมต่อหน่วยความจำภายนอก

๔. ห้ามเชื่อมต่อเครื่องคอมพิวเตอร์ในระบบ C4I เข้าสู่เครือข่ายอินเทอร์เน็ตโดยเด็ดขาด

๕. ห้ามเปิดอีเมลที่ไม่ทราบแหล่งที่มา พร้อมทั้งไฟล์ต่าง ๆ ที่แนบมากับอีเมลโดยเด็ดขาด โดย ศซบ.ทหาร จะเฝ้าระวังและติดตามการเปิดอีเมลที่ไม่ทราบแหล่งที่มาที่ส่งผลให้เกิดภัยคุกคามทางไซเบอร์ต่อระบบเครือข่ายของ บก.ทท. และรายงานให้ ผบ.หน่วย ต้นสังกัดของ นขต.บก.ทท. ทราบ โดยเร็วที่สุดภายหลังการตรวจพบ

๖. ห้ามดาวน์โหลดซอฟต์แวร์จากเว็บไซต์ที่ไม่น่าเชื่อถือโดยเด็ดขาด โดยเฉพาะคอมพิวเตอร์ที่เชื่อมต่อกับระบบ C4I และ MIS ซึ่ง นขต.บก.ทท. ทุกส่วนงานควรกำหนดให้กำลังพลของหน่วยมีการติดตั้งได้เฉพาะซอฟต์แวร์ที่จำเป็นต่อการปฏิบัติงานจริง ๆ เท่านั้น ทั้งนี้ ศซบ.ทหาร จะดำเนินการเฝ้าระวังและติดตามภัยคุกคามทางไซเบอร์ที่สืบเนื่องมาจากการดาวน์โหลดซอฟต์แวร์จากเว็บไซต์ที่ไม่น่าเชื่อถือของกำลังพลของ นขต.บก.ทท. และรายงานให้ ผบ.หน่วย ของ นขต.บก.ทท. ทราบโดยเร็วที่สุดภายหลังการตรวจพบ

๗. ผู้ดูแลระบบและผู้ให้บริการด้านสารสนเทศของหน่วย ต้องปรับปรุงซอฟต์แวร์และระบบเทคโนโลยีสารสนเทศของหน่วย (Update Software) ให้มีความทันสมัยอยู่เสมอ ประกอบด้วย

๗.๑ ผู้ดูแลระบบและผู้ให้บริการด้านสารสนเทศของหน่วย ตรวจสอบสถานภาพเครื่องคอมพิวเตอร์ในความรับผิดชอบ ว่าใช้ระบบปฏิบัติการ หรือซอฟต์แวร์ เป็นเวอร์ชันล่าสุดหรือมีความปลอดภัยแล้วหรือไม่

๗.๒ ผู้ดูแลระบบและผู้ให้บริการด้านสารสนเทศของหน่วย จะต้องมีการจัดทำแผนการปรับปรุงระบบเทคโนโลยีสารสนเทศของหน่วย (Update Software) ดังนี้

๗.๒.๑ กำหนดวงรอบในการตรวจสอบและปรับปรุงระบบซอฟต์แวร์ของหน่วยเป็นวงรอบอย่างต่อเนื่อง

๗.๒.๒ ติดตามข่าวสารเกี่ยวกับการปรับปรุงระบบ (Update Software) จากผู้ผลิตอย่างต่อเนื่อง เช่น Microsoft, Adobe, Cisco, Dell เป็นต้น

๗.๒.๓ ติดตามข่าวสารเกี่ยวกับช่องโหว่ของระบบ (Vulnerability) จากนายทหารรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วย หรือจาก ศซบ.ทหาร ตลอดจนแหล่งข่าวต่าง ๆ ที่น่าเชื่อถือได้ เช่น ThaiCERT หรือบริษัทเจ้าของซอฟต์แวร์ เป็นต้น

๗.๒.๔ ทดสอบการใช้งานโปรแกรมปรับปรุงระบบ (Patch) ก่อนการติดตั้งโปรแกรมดังกล่าวต่อไป

๗.๓ ให้ ศซบ.ทหาร แจ้งเตือนช่องโหว่ใหม่ๆ ของระบบ (Vulnerability) ที่สำคัญ ให้กับ นขต.บก.ทท. ทราบอย่างต่อเนื่อง

๗.๔ ให้ ศซบ.ทหาร จัดทำเป็นแผนการประเมินช่องโหว่ (Vulnerability Assessment) ประจำปีในภาพรวมให้กับ บก.ทท. ในลักษณะของการสุ่มตรวจ หรือการตรวจประเมินตามการร้องขอโดยตรงจาก นขต.บก.ทท.

๘. เครื่องคอมพิวเตอร์ในระบบ C4I และ MIS ต้องเชื่อมต่อเข้ากับ Active Directory (AD) โดย สส.ทหาร จะทำหน้าที่รับผิดชอบในการดำเนินการในเรื่องการเชื่อมต่อดังกล่าวให้ครอบคลุมต่อไป

๙. ศซบ.ทหาร ดำเนินการเพิ่มหัวข้อตรวจตามข้อ ๑ และ ๒ ตามแผนการตรวจประเมินมาตรฐานฯ ประจำปีของหน่วย

๑๐. กรณีมีการละเมิดมาตรการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ภายในหน่วยขึ้นตรงของ บก.ทท. จนนำมาสู่ความเสียหายและความเสื่อมเสียชื่อเสียงของ บก.ทท. ถือเป็นความรับผิดชอบของ หน.ส่วนราชการของ นขต.บก.ทท.

****