บทที่ 3

สถานภาพด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดสุรินทร์

การสำรวจและวิเคราะห์สถานภาพด้านการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบเทคโนโลยีสารสนเทศของจังหวัดสุรินทร์ในปัจจุบัน มีรายละเอียดในด้านต่างๆ ประกอบด้วย

1. สถานภาพด้านเทคโนโลยีสารสนเทศ
2. สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์

3.1 หลักการและเหตุผลสถานภาพด้านเทคโนโลยีสารสนเทศ

กลุ่มยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด สำนักงานจังหวัดสุรินทร์ เป็นหน่วยงานภายในจังหวัดฯ มีหน้าที่รับผิดชอบในการจัดทำนโยบายและพัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศของจังหวัดฯ การบริหารจัดการและดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ การพิจารณา จัดซื้อจัดหาระบบคอมพิวเตอร์ อุปกรณ์ต่อพ่วง และระบบเครือข่ายขององค์กรปกครองส่วนท้องถิ่น เพื่อรองรับการปฏิบัติงานของเจ้าหน้าที่จังหวัดฯ ให้ได้รับความสะดวก รวดเร็ว รวมถึงการพัฒนาระบบงานอิเล็กทรอนิกส์ที่ช่วยอำนวยความสะดวกและเพิ่มประสิทธิภาพในการปฏิบัติงาน อีกทั้งยังได้ติดตามผลการทำงานอย่างต่อเนื่องเพื่อพัฒนาระบบงานสารสนเทศ ให้มีประสิทธิภาพมากยิ่งขึ้น โดยจากการสำรวจสถานภาพด้านเทคโนโลยีสารสนเทศของจังหวัดฯ ในปัจจุบัน สามารถสรุปรายละเอียดได้ ดังนี้

3.1.1 ฮาร์ดแวร์และซอฟต์แวร์ด้านความปลอดภัย ดังนี้

ตารางที่ 3-1 แสดงฮาร์ดแวร์ และซอฟต์แวร์ด้านความปลอดภัยของ จังหวัดฯ

ลำดับ	รายการ/อุปกรณ์	ยี่ห้อ/รุ่น	สถานที่ติดตั้ง	จำนวน
1	อุปกรณ์ป้องกันระบบเครือข่าย (Firewall)	ยี่ห้อ Fortinet รุ่น Fortigate 600C	ห้อง Server	1 ชุด
2	อุปกรณ์สำหรับป้องกันระบบเครือข่าย (Firewall)	ยี่ห้อ Sangfor รุ่น M5300F-I	ห้อง Server	1 ชุด
3	ระบบป้องกันไวรัส แบบ Client & Server	Kaspersky Security Center (Client & Server)	ห้อง Server	1 ระบบ
4	อุปกรณ์ป้องกันภัย Web Application Firewall	ยี่ห้อ F5	ห้อง Server	1 ชุด
5	โปรแกรมสำรองข้อมูล Arcserve	Arcserve UDP	ห้อง Server	1 ระบบ

3.1.2 ระบบเครือข่ายอินเทอร์เน็ต

จังหวัดสุรินทร์มีการเชื่อมโยงสัญญาณเครือข่ายอินเทอร์เน็ต เพื่อให้บริการสัญญาณอินเทอร์เน็ต ภายในจังหวัดฯ จำนวน 3 เครือข่าย ดังนี้

3.1.2.1 สัญญาณเครือข่ายจาก บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ความเร็ว 1,000 Mbps เพื่อให้บริการบนโครงข่ายสายสัญญาณ (LAN) และให้บริการระบบอินเทอร์เน็ตไร้สาย (WiFi)

3.1.2.2 สัญญาณเครือข่ายจากโครงข่าย MOTNET สำนักงานปลัดกระทรวงมหาดไทย ความเร็ว 16 Mbps เพื่อเชื่อมโยงระบบสารสนเทศของจังหวัดฯ

3.1.2.3 สัญญาณเครือข่าย GIN (Government Information Network) จากสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) ความเร็ว 20 Mbps เพื่อเชื่อมโยงข้อมูลภาครัฐและระบบบริหารสำนักงานอัตโนมัติของจังหวัดฯ (e-Office)

3.1.3 บุคลากรด้านเทคโนโลยีสารสนเทศ

ในการมอบหมายบุคลากรให้ปฏิบัติหน้าที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯได้มอบหมายให้กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร ซึ่งเป็นกลุ่มงาน ที่ดูแลรับผิดชอบ งานด้านระบบ คอมพิวเตอร์ และระบบเครือข่าย และงานด้านความมั่นคง ปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศและข้อมูลสารสนเทศด้วย ซึ่งกลุ่มพัฒนาระบบ คอมพิวเตอร์ และเครือข่าย มีกรอบอัตรากำลัง ดังนี้

1) หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย ตำแหน่ง นักวิชาการคอมพิวเตอร์ ระดับชำนาญการพิเศษ จำนวน 1 อัตรา

2) ตำแหน่ง นักวิชาการคอมพิวเตอร์ ระดับปฏิบัติการ/ชำนาญการ จำนวน 6 อัตรา

3.2 สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์

สถานภาพด้านมาตรการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ สามารถสรุปรายละเอียดได้ ดังนี้

3.2.1 สถานภาพระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของจังหวัดฯ

1) ระบบรักษาความมั่นคงปลอดภัย Internet Security สำหรับการใช้งานระบบอินเทอร์เน็ตจะใช้เส้นทางออกอินเทอร์เน็ต จำนวน 3 เส้นทาง โดยกำหนดเส้นทางหลัก ได้แก่ อินเทอร์เน็ตความเร็วสูง ความเร็ว 1000/1000 Mbps และอินเทอร์เน็ตเส้นทางสำรอง ได้แก่ MOTNET ความเร็ว 16/16 Mbps และเครือข่าย GIN ความเร็ว 20/20 Mbps ซึ่งจะมีการรักษาความปลอดภัยสำหรับผู้ใช้งานระบบ Internet ประกอบด้วย

- Next Generation-Firewall
- Web Application Firewall
- การพิสูจน์ตัวตนผ่านระบบ Domain Name (Authentication)
- ระบบคัดกรองและปิดกั้นเว็บไซต์ (Web filter)
- ระบบตรวจสอบและเฝ้าระวัง (Monitoring)
- ระบบป้องกันการโจมตีหลายรูปแบบจากผู้ไม่ประสงค์ดี (Intrusion Protection)

2) ระบบพิสูจน์ตัวตน (Authentication)

ระบบพิสูจน์ตัวตน สำหรับเข้าสู่ระบบอินเทอร์เน็ตและระบบงานอิเล็กทรอนิกส์ต่าง ๆ ของจังหวัดฯ ให้สามารถใช้งานได้อย่างสะดวก รวดเร็ว และปลอดภัย ด้วยรหัสผู้ใช้งานชุดเดียว สามารถเข้าสู่ระบบสารสนเทศ จำนวน 8 ระบบงาน ได้แก่ ระบบเครือข่ายสายสัญญาณ ระบบเครือข่ายไร้สาย ระบบเชื่อมต่อ เครือข่ายนทราเน็ตจากภายนอก ระบบบริหารจัดการข้อมูลส่วนบุคคลเพื่อการบูรณาการ ระบบบริหารจัดการ เอกสาร จังหวัดฯ

3) การกำหนดและใช้งาน Internet Protocol Address (IP Address) ภายใน จังหวัดฯ สำหรับระบบเครือข่ายภายใน จังหวัดฯ ได้มีการกำหนดหมายเลข IP Address เป็นลักษณะ Vlan (Virtual Local Area Network) เพื่อเข้าถึงระบบเครือข่ายภายใน และเป็นการรักษาความมั่นคงปลอดภัย ในการเข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายของจังหวัดฯ

4) การป้องกันการบุกรุกโจมตีระบบคอมพิวเตอร์และเครือข่าย (Firewall) มีการกำหนดให้เปิดช่องทาง (Port) ในการเข้าถึงข้อมูล ของแต่ละโครงข่ายเท่าที่จำเป็น เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ปลอดภัย เช่น การเข้าถึงระบบสารสนเทศภายใน จังหวัดฯ ที่ให้บริการประเภท Web Application แก่บุคคลภายนอก โดยจะเปิด Port เฉพาะประเภท HTTP และ HTTPS รวมถึงมีการปิดกั้นการเข้าถึง เว็บไซต์ประเภทที่มีความเสี่ยงต่อภัยคุกคามทางไซเบอร์ เช่น ประเภทเกมส์ ประเภทสื่อลามกอนาจาร ประเภทพนัน และเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม เป็นต้น

5) ระบบรักษาความมั่นคงปลอดภัยสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server Security) โดยจะมีระบบรักษาความมั่นคงปลอดภัยเครื่องคอมพิวเตอร์แม่ข่าย ประกอบด้วย

- การรักษาความปลอดภัยด้วยระบบสแกนลายนิ้วมือห้องศูนย์ข้อมูลจังหวัดฯ
- Antivirus Client & Server สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและลูกข่าย
- Web App Firewall
- การตั้งค่า Firewall ของเครื่องคอมพิวเตอร์แม่ข่าย และการอัพเดตแพทช์ (Patch) ด้านความปลอดภัยต่างๆ อย่างสม่ำเสมอ

3.2.2 สถานภาพที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์

หลักการปฏิบัติพื้นฐานของการรักษาความมั่นคงปลอดภัย ประกอบด้วย 3 ด้าน เรียกว่า “CIA Triad” ประกอบด้วย ความมั่นคงปลอดภัย (Security) เป็นการปกป้องทรัพย์สิน (Asset) ให้พ้นจากภัยคุกคาม (Threat) หลักการของความมั่นคงปลอดภัยที่จะได้กล่าวต่อไปนี้ จะสามารถใช้ได้กับทรัพย์สินทุกประเภท ไม่ว่าจะเป็นทรัพย์สินที่จับต้องได้หรือไม่ก็ตาม เช่น คอมพิวเตอร์ เงินทอง เครื่องประดับต่าง ๆ องค์ความรู้ สิทธิบัตร ข้อมูลลูกค้า ความลับทางการค้า และข้อมูลอื่น ๆ หลักการของความมั่นคงปลอดภัย การปกป้องทรัพย์สิน ขององค์กรนั้น ตั้งอยู่บนหลักความมั่นคงปลอดภัย 3 ขา (Security Triads) อันประกอบด้วย CIA ดังนี้

ภาพที่ 3–2 หลักการ CIA

ความลับ หรือ Confidentiality : เป็นการปกป้องข้อมูลไม่ให้รั่วไหลไปสู่ภายนอกองค์กร หรือบุคคลที่ต้องการเข้าถึงข้อมูลขององค์กร เนื่องจากข้อมูลข่าวสารที่หลุดออกไปจะส่งกระทบต่อองค์กรเป็นอย่างมาก จึงต้องมีการดำเนินการต่าง ๆ เพื่อปกป้องข้อมูลขององค์กร และรักษาความลับของข้อมูล เช่น การเข้ารหัส (Encryption) เทคโนโลยีที่มีการเชื่อมต่อกับเครือข่ายภายนอก (Virtual Private Network) มาตรฐานการรักษาความปลอดภัยของข้อมูลที่รับส่งผ่านอินเตอร์เน็ต (Secure Socket Layer) การเข้ารหัสและถอดรหัสข้อมูลด้วยกุญแจส่วนตัว (Public Key Infrastructure) เป็นต้น

ความถูกต้อง หรือ Integrity : เป็นการป้องกันการปลอมแปลงข้อมูลไม่ให้ถูกแก้ไขโดยที่ไม่ได้รับอนุญาต หรือไม่ถูกเปลี่ยนแปลงโดยแฮกเกอร์หรือผู้บุกรุก โดยเฉพาะข้อมูลสำคัญที่เกี่ยวข้องกับองค์กร หรือมีผลต่อองค์กร หากข้อมูลถูกเปลี่ยนแปลงแก้ไขไปแล้วจะส่งผลกระทบให้กับองค์กรอย่างมาก จึงต้องมีการตรวจสอบความถูกต้อง (Checker) ของข้อมูลอยู่เสมอ

สภาพพร้อมใช้งาน หรือ Availability : เป็นการทำให้มีความพร้อมในการใช้งานระบบคอมพิวเตอร์ได้ตลอดเวลา หรือเมื่อเกิดปัญหาระบบล่มแล้ว การไม่มีระบบสำรองไว้ใช้งานหรือการรอจนกว่าจะสามารถกู้ระบบได้จะทำให้เกิด “downtime” เป็นอย่างมาก ซึ่งเป็นต้นเหตุทำให้การดำเนินงานขององค์กรติดขัด ไม่สามารถดำเนินงานได้อย่างต่อเนื่อง จึงควรมีแผนการป้องกัน ตัวอย่างเช่น แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Planning) แผนกู้คืนระบบเทคโนโลยีสารสนเทศและดิจิทัล (Disaster Recovery Planning) เป็นต้น

หลักการของความมั่นคงปลอดภัยทั้ง 3 มิติ นั้น เป็นสิ่งที่จำเป็นและไม่สามารถแยกขาดจากกันได้นอกจากนี้ยังมีประเภทของความมั่นคงปลอดภัย ดังนี้

3.2.2.1 ความปลอดภัยทางกายภาพ (Physical Security) ได้แก่ ความปลอดภัยด้านอาคาร สถานที่การตรวจสอบคนที่ต้องผ่านเข้าออกอาคารสถานที่ เป็นต้น

3.2.2.2 ความปลอดภัยทางงานอำนวยการ (Administrative Security) ได้แก่

นโยบาย มาตรฐาน คำสั่ง กระบวนการ ข้อเสนอแนะ เป็นต้น ตัวอย่างการสร้างความปลอดภัยทางงานอำนวยการ ได้แก่ การแบ่งอำนาจ ความรับผิดชอบ การหมุนเวียนงาน การบังคับให้ลาพักผ่อน การตรวจสอบภูมิหลังก่อนการจ้างงาน

3.2.2.3 ความปลอดภัยทางเทคนิค ได้แก่ การนำเทคโนโลยีมาช่วยสร้างความปลอดภัย ตัวอย่างของการสร้างความมั่นคงปลอดภัยทางเทคนิค ได้แก่ ระบบ Access Control List ระบบ Firewall ระบบ Intrusion Detection System (IDS) เป็นต้น