รายงานด้านความมั่นคงปลอดภัยไซเบอร์
มหาวิทยาลัยราชภัฏมหาสารคาม

ในปีงบประมาณ พ.ศ. 2568 – 2569 มหาวิทยาลัยราชภัฏมหาสารคามได้ดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อรองรับภัยคุกคามที่มีความซับซ้อนและเพิ่มขึ้นอย่างต่อเนื่อง โดยมุ่งเน้นการยกระดับความพร้อมขององค์กรใน 3 ด้านหลัก ได้แก่ 1) การพัฒนาบุคลากร เพื่อเสริมสร้างความรู้ ทักษะ และความตระหนักด้านไซเบอร์ 2) การติดตั้งและพัฒนาเทคโนโลยีป้องกันภัยคุกคาม เช่น ระบบป้องกันเว็บไซต์และข้อมูลสำคัญ 3) การพัฒนาระบบเฝ้าระวังและตรวจสอบความมั่นคงปลอดภัยเว็บไซต์

การดำเนินงานดังกล่าวช่วยเพิ่มประสิทธิภาพในการป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์ พร้อมทั้งสร้างความเชื่อมั่นในการให้บริการด้านสารสนเทศของมหาวิทยาลัยแก่ผู้ใช้งานทุกภาคส่วน

1. การปรับปรุงระบบเครื่องแม่ข่ายเพื่อรองรับเทคโนโลยีใหม่และการเฝ้าระวังความปลอดภัย (Server Modernization & SOC)

ในปีงบประมาณ พ.ศ. 2568 – 2569 มหาวิทยาลัยราชภัฏมหาสารคามได้ดำเนินการ ปรับปรุงและพัฒนาระบบเครื่องแม่ข่าย (Server Infrastructure) เพื่อรองรับระบบสารสนเทศและเทคโนโลยีสมัยใหม่ ควบคู่กับการยกระดับความมั่นคงปลอดภัย โดยมีการนำระบบ Security Operations Center (SOC) จากผู้ประกอบการภายนอก และ ศูนย์สำรองข้อมูล (Disaster Recovery Site: DR Site) มาใช้งานร่วมกัน

1.1 การดำเนินงาน

1) ปรับปรุงเครื่องแม่ข่ายให้รองรับเทคโนโลยีใหม่

- Virtualization / Cloud Integration
- Container-based Applications (เช่น Docker)

2) เพิ่มประสิทธิภาพด้านการประมวลผล การจัดเก็บข้อมูล และความเสถียรของระบบ

3) ปรับปรุงระบบสำรองข้อมูล (Backup) และการกู้คืนระบบ (Disaster Recovery)

1.2 การเฝ้าระวังและความมั่นคงปลอดภัย (SOC)

1) มีการใช้บริการ SOC เพื่อเฝ้าระวังเหตุการณ์ผิดปกติที่เกิดขึ้นกับเครื่องแม่ข่ายตลอด 24x7

2) ตรวจจับพฤติกรรมที่มีความเสี่ยง เช่น

- การเข้าถึงระบบโดยไม่ได้รับอนุญาต
- การทำงานผิดปกติของระบบ (Anomaly Detection)
- แจ้งเตือนเหตุการณ์แบบ Real-time และสนับสนุนการตอบสนองเหตุการณ์ (Incident Response)
- จัดทำรายงานสรุปสถานะความปลอดภัยของเครื่องแม่ข่ายอย่างสม่ำเสมอ

1.3 การจัดตั้งศูนย์สำรองข้อมูล (DR Site)

1) จัดให้มี DR Site สำหรับรองรับกรณีระบบหลักเกิดเหตุขัดข้องหรือภัยพิบัติ

2) มีการสำรองและทำซ้ำข้อมูล (Data Replication) ไปยังศูนย์สำรอง

3) รองรับการกู้คืนระบบ (Failover) เพื่อให้บริการสามารถดำเนินต่อได้อย่างต่อเนื่อง

4) กำหนดค่า RTO (Recovery Time Objective) และ RPO (Recovery Point Objective) ให้เหมาะสมกับระบบสำคัญ

2. การติดตั้งระบบป้องกันและรักษาความปลอดภัยข้อมูลสารสนเทศ (Web Application Firewall: WAF)

มหาวิทยาลัยราชภัฏมหาสารคามได้ดำเนินการติดตั้งระบบ Web Application Firewall (WAF) เพื่อป้องกันภัยคุกคามที่เกิดขึ้นกับระบบเว็บไซต์และบริการออนไลน์ของมหาวิทยาลัย ควบคู่กับการใช้บริการ ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ (Security Operations Center: SOC) จากผู้ประกอบการภายนอก เพื่อเสริมศักยภาพในการเฝ้าระวังและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยตลอด 24 ชั่วโมง ดังนี้

2.1 ป้องกันการโจมตีเว็บไซต์ของมหาวิทยาลัย

2.1.1 ป้องกันการโจมตีประเภท

- SQL Injection
- Cross-Site Scripting (XSS)
- Remote Code Execution

2.1.2 ปกป้องระบบสำคัญ เช่น

- เว็บไซต์ มหาวิทยาลัยราชภัฏมหาสารคาม
- ระบบทะเบียนนักศึกษา
- ระบบสารสนเทศบุคลากร
- ระบ MIS
- เว็บไซต์บริการนักศึกษา

2.2 ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

- ตรวจจับพฤติกรรมผิดปกติ (Anomaly Detection)
- กรอง Traffic ที่เป็นอันตราย

2.3 เพิ่มความพร้อมใช้งานของระบบ (Availability)

- ลดความเสี่ยงจากการโจมตีแบบ DDoS (บางระดับ)
- ทำให้บริการออนไลน์ของมหาวิทยาลัยมีความต่อเนื่อง

2.4 สนับสนุนการปฏิบัติตามมาตรฐานความปลอดภัย

สอดคล้องกับแนวทางของ

- OWASP
- ISO/IEC 27001 (Information Security Management)

2.5 การบันทึกและวิเคราะห์เหตุการณ์ (Logging & Monitoring)

- เก็บ Log การโจมตี
- ใช้เป็นข้อมูลในการวิเคราะห์และพัฒนาระบบความปลอดภัยเพิ่มเติม

2.6 การเฝ้าระวังและตอบสนองเหตุการณ์ (SOC)

- มีหน่วยงาน SOC จากผู้ประกอบการ ทำหน้าที่เฝ้าระวัง (Monitoring) ตลอด 24x7
- ตรวจจับพฤติกรรมผิดปกติและวิเคราะห์เหตุการณ์ด้านความปลอดภัย
- แจ้งเตือนเหตุการณ์ (Alert) แบบ Real-time ไปยังผู้ดูแลระบบ
- จัดทำ รายงานผลการเฝ้าระวัง (Security Monitoring Report) เป็นระยะ
- สนับสนุนการตอบสนองเหตุการณ์ (Incident Response) ร่วมกับ แผนรับมือภัยคุกคามไซเบอร์ (Incident Response Plan) มหาวิทยาลัยราชภัฏมหาสารคาม

3. การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

มหาวิทยาลัยราชภัฏมหาสารคามได้มีการส่งเสริม สนุบสนุนในการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ดังนี้

3.1 โครงการพัฒนาขีดความสามารถในการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ หน่วยงานผู้จัด สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มหาวิทยาลัยราชภัฏมหาสารคามได้ส่งบุคลากรเข้าร่วมโครงการดังกล่าว เพื่อเสริมสร้างศักยภาพในการจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) ให้สอดคล้องกับมาตรฐานระดับประเทศ โดยเน้นการบริหารจัดการเหตุการณ์ในระดับต่าง ๆ เช่น ระดับหน่วยงาน ระดับโครงสร้างพื้นฐานสำคัญ และระดับประเทศ

รายชื่อผู้เข้ารับการอบรม

1) ดร.ทรงพล นามคุณ
2) นายวินัย โกหลำ
3) นายวุฒิศักดิ์ ชมดวงทิพย์

ผลลัพธ์

- จัดทำแผนรับมือภัยคุกคามไซเบอร์ (Incident Response Plan) มหาวิทยาลัยราชภัฏมหาสารคาม

3.2 โครงการพัฒนาผู้บริหารและบุคลากรด้านกฎหมายสำหรับการปฏิบัติราชการของ บุคลากรสายวิชาการและสายสนับสนุนภายในมหาวิทยาลัยราชภัฏมหาสารคาม จำนวน 600 คน โครงการนี้มีวัตถุประสงค์เพื่อพัฒนาความรู้ด้านกฎหมายที่เกี่ยวข้องกับการปฏิบัติงานภาครัฐ โดยเฉพาะด้านข้อมูลและไซเบอร์ เช่น

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ผลลัพธ์

- บุคลากรมีความตระหนักด้านกฎหมายไซเบอร์ (Cyber Law Awareness)
- ลดความเสี่ยงในการละเมิดข้อมูลส่วนบุคคล
- สนับสนุนการกำกับดูแลด้าน IT Governance ภายในมหาวิทยาลัย

4. การเข้าร่วมโครงการ Government Web Protection (GWP) (สรุป)

ในปีงบประมาณ พ.ศ. 2568 – 2569 มหาวิทยาลัยราชภัฏมหาสารคามได้เข้าร่วมโครงการ Government Web Protection (GWP) เพื่อยกระดับความมั่นคงปลอดภัยของเว็บไซต์และระบบสารสนเทศของมหาวิทยาลัยให้เป็นไปตามมาตรฐานภาครัฐ

โดยมหาวิทยาลัยได้นำ ระบบสารสนเทศและเว็บไซต์เข้าร่วมโครงการ จำนวน 5 ระบบ ตามโควต้า ที่ได้รับ เพื่อให้ได้รับการป้องกันและเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

การดำเนินงานดังกล่าวช่วยเสริมการป้องกันการโจมตีเว็บไซต์ในรูปแบบต่าง ๆ เช่น การโจมตีแบบ DDoS พร้อมทั้งมีระบบเฝ้าระวัง แจ้งเตือน และวิเคราะห์ภัยคุกคามแบบเชิงรุก

ผลลัพธ์ที่สำคัญ

- เพิ่มระดับความปลอดภัยของระบบสารสนเทศและเว็บไซต์สำคัญ
- ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
- สนับสนุนการดำเนินงานตามนโยบายความมั่นคงปลอดภัยไซเบอร์ภาครัฐ

5. การพัฒนาระบบเฝ้าระวังและตรวจสอบความมั่นคงปลอดภัยเว็บไซต์ ตามมาตรฐาน OWASP Top 10

ศูนย์เทคโนโลยีดิจิทัลและนวัตกรรม มหาวิทยาลัยราชภัฏมหาสารคามได้พัฒนาระบบ เฝ้าระวังและตรวจสอบความมั่นคงปลอดภัยเว็บไซต์ เพื่อสนับสนุนผู้ดูแลระบบ (Webmaster) และนักพัฒนาเว็บไซต์ ให้สามารถตรวจสอบช่องโหว่ เพื่อให้สามารถแก้ไขและปรับปรุง ให้สามารถลดความเสี่ยงจากภัยคุกคามไซเบอร์

มาตรฐานที่ใช้ตรวจสอบ

- OWASP
- OWASP Top 10
- MITRE CWE

คุณสมบัติของระบบที่พัฒนา

5.1 การสแกนช่องโหว่อัตโนมัติ (Automated Vulnerability Scanning)

- ตรวจสอบช่องโหว่ของเว็บไซต์ภายในมหาวิทยาลัยแบบอัตโนมัติ
- แจ้งเตือนเมื่อพบความเสี่ยง

5.2 Dashboard สำหรับผู้ดูแลระบบ/ผู้พัฒนาระบบและเว็บไซต์

- แสดงสถานะความปลอดภัยของเว็บไซต์แต่ละหน่วยงาน
- จัดอันดับความเสี่ยง (Risk Level)

5.3 ระบบแจ้งเตือน (Alert System)

- แจ้งเตือนผ่าน Email / Dashboard
- รองรับการแจ้งเตือนแบบ Real-time

5.4 ระบบรายงาน (Reporting System)

- สรุปรายงานช่องโหว่ ตามมาตรฐาน OWASP และ MITRE CWE พร้อทแนะนำแนวทางในการแก้ไข
- รองรับการใช้เป็นหลักฐานในการตรวจประเมิน โดยอ้างอิงตามมาตรฐาน

ประโยชน์ที่ได้รับ

- เพิ่มความมั่นคงปลอดภัยของเว็บไซต์มหาวิทยาลัย
- ลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์
- สนับสนุนการทำงานของ Web Developer และ Webmaster
- รองรับการประเมินมาตรฐานภาครัฐและระดับประเทศ
- สร้างความเชื่อมั่นให้กับนักศึกษา บุคลากร และประชาชน