รายงานความก้าวหน้าการพัฒนาเว็บไซต์ตามเกณฑ์ของ Webometrics

ประเด็นที่ 1 ผลการดำเนินงานของกลุ่มผู้ดูแลเว็บไซต์

กิจกรรมแลกเปลี่ยนเรียนรู้การพัฒนาเว็บไซต์ ครั้งที่ 5 วันที่ 27 กุมภาพันธ 2569 เวลา 09.00-12.00 น. ณ ห้องประชุมดอกสัก สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มรภ.กพ.

สาระสำคัญ

1. แนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)
2. หารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย
3. ประเด็นความเสี่ยงด้านความปลอดภัยทางไซเบอร์และสถิติการโจมตี
4. ข้อเสนอแนะและแนวทางการดำเนินงานในอนาคต

1. แนะนำเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

ตามคำสั่งมหาวิทยาลัยราชภัฏกำแพงเพชรที่ 2363/2568 ลงวันที่ 24 ธันวาคม 2568 ได้แต่งตั้ง นางสาวนฤชล เขื่อนยัง อาจารย์ประจำหลักสูตรโปรแกรมวิชานิติศาสตร์ เป็นเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล โดยมีวัตถุประสงค์ เพื่อรองรับการเป็นมหาวิทยาลัยดิจิทัลและปฏิบัติตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) อย่างถูกต้อง ซึ่งกำหนดให้มีหน้าที่และอำนาจในการให้คำแนะนำและวางแนวทางปฏิบัติ ผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลในแต่ละหน่วยงาน ตรวจสอบการดำเนินงานด้านการคุ้มครองข้อมูลขององค์กรให้เป็นไปตามกฎหมาย ประสานงานกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) กรณีมีเหตุละเมิดข้อมูล การรักษาความลับของข้อมูลส่วนบุคคลที่ล่วงรู้จากการปฏิบัติหน้าที่

โดยสรุป แจ้งให้ทีมแอดมินเข้าใจถึงบทบาทหน้าที่ของ DPO และบทบาทของทีมแอดมินในฐานะผู้ประมวลข้อมูลส่วนบุคคล ซึ่งเป็นบุคลากรที่สำคัญจะต้องปฏิบัติหน้าที่ภายในกรอบของกฎหมาย PDPA

2. หารือเกี่ยวกับการบริหารจัดการข้อมูลส่วนบุคคลในมหาวิทยาลัย

จากการสอบถามและหารือระหว่างทีมแอดมินที่ปฏิบัติงานในหน่วยงานต่าง ๆ ภายในมหาวิทยาลัย เกี่ยวกับแนวทางการบริหารจัดการข้อมูลส่วนบุคคล (PDPA) มาตรการควบคุมการเข้าถึงข้อมูล และสถานะความปลอดภัยทางไซเบอร์ในปัจจุบัน สาระสำคัญครอบคลุมถึงระบบฐานข้อมูลนักศึกษาและบุคลากร แนวทางปฏิบัติเกี่ยวกับกล้องวงจรปิด (CCTV) และความเสี่ยงจากการตั้งรหัสผ่านที่คาดเดาง่าย ซึ่งเป็นช่องโหว่สำคัญในการโจมตีระบบโดยมหาวิทยาลัยมุ่งเน้นการสร้างมาตรฐานการปฏิบัติงานที่ชัดเจนเพื่อคุ้มครองเจ้าหน้าที่ผู้ปฏิบัติงานและป้องกันการละเมิดข้อมูลส่วนบุคคลในวาระนี้ อาจารย์นฤชล เขื่อนยัง (DPO) ได้กำหนดประเด็นในการแลกเปลี่ยนข้อมูล เพื่อที่จะนำไปออกแบบจัดอบรมเชิงปฏิบัติการให้กับบุคลากรกลุ่มที่เป็นทีมแอดมิน เกี่ยวกับบทบาทและหน้าที่ของเจ้าหน้าที่แอดมิภายใต้กรอบของกฎหมาย PDPA เพื่อสร้างความรู้และความเข้าใจ รวมถึงสอบถามปัญหาที่ทีมแอดมินเคยพบเจอจากการปฏิบัติงาน และส่วนสุดท้ายคือการสร้างความเข้าใจเกี่ยวกับการจัดทำสัญญา NDA โดยมีหัวข้อในการหารือ ดังนี้

2.1 วิธีการจัดเก็บข้อมูลส่วนบุคคลในแต่ละหน่วยงาน เพื่อเป็นการสำรวจความเสี่ยง พฤติกรรม และปัญหาที่อาจพบในการจัดเก็บข้อมูลของทีมแอดมิน การให้สิทธิเข้าถึงข้อมูล กรณีเจ้าหน้าที่แอดมิน โยกย้ายงาน หรือลาออกมีวิธีการจำกัดการเข้าถึงข้อมูล หรือทำลายข้อมูลหรือไม่ อย่างไร

2.2 การตรวจสอบความรับผิดชอบของเจ้าหน้าที่แอดมิน/มหาวิทยาลัย ระบบต่าง ๆ สามารถตรวจสอบย้อนหลังได้หรือไม่ว่า ใครเข้าไปดู / แก้ไขข้อมูล รวมถึงความพร้อมในการรับมือกรณีเกิดเหตุละเมิดข้อมูลส่วนบุคคล

มีการกำหนดเจ้าหน้าที่แอดมินที่เป็นผู้ประมวลผลข้อมูลส่วนบุคคลไว้ชัดเจนหรือไม่ หรือเจ้าหน้าที่แอดมินบางคนเป็นเพียงคณะทำงาน มีการจัดทำคำสั่ง หรือระบุหน้าที่ของทีมแอดมินไว้ชัดเจนหรือไม่ ว่าเกี่ยวข้องกับการประมวลผลข้อมูลส่วนบุคคลอย่างไร

2.3 สอบถามประเด็นความเสี่ยงในการปฏิบัติงาน เพื่อที่จะนำไปออกแบบเป็น Case Study ในการจัดการอบรมให้ทีมแอดมินต่อไป จากประเด็นที่ อาจารยนฤชล เขื่อนยัง (DPO) กำหนดหัวขอในการประชุมวาระนี้ไว สามารถสรุปรายละเอียดพอสังเขปไดดังตอไปนี้

2.1 วิธีการจัดเก็บข้อมูลส่วนบุคคลในแต่ละหน่วยงาน

สำหรับการบริหารจัดการข้อมูลและระบบฐานข้อมูลในแต่ละหน่วยงาน จะมีฐานการจัดเก็บข้อมูลที่แตกต่างกัน กรณีตัวอย่างสำนักส่งเสริมวิชาการและงานทะเบียน มีการจัดเก็บข้อมูลตั้งแต่แรกเข้าจนถึงสำเร็จการศึกษา โดยแบ่งระดับการเข้าถึงและการจัดเก็บออกเป็น 2 ส่วนหลัก

- ฐานข้อมูลหลัก (ฐานดำ) เป็นระบบปิดที่ใช้งานภายใน (Offline) เก็บข้อมูลทุกอย่างที่เกี่ยวข้องกับการรายงานตัวและการส่งข้อมูลให้กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม (อว.) จะไม่มีการเชื่อมต่อออนไลน์เพื่อความปลอดภัย

- ระบบเผยแพร่ข้อมูลออนไลน์ แสดงผลเฉพาะข้อมูลเบื้องต้น เช่น รายชื่อและสถานะการศึกษา เพื่อให้บุคคลภายนอก ผู้ปกครอง หรือศิษย์เก่าสามารถตรวจสอบและยืนยันสถานะได้ โดยระบบมีการจัดเก็บ Log สามารถตรวจสอบได้ว่าใครเป็นผู้เข้ามาดูข้อมูล

- นโยบายการจัดเก็บและทำลายข้อมูล

(1) ข้อมูลนักศึกษา เก็บข้อมูลไว้จนสำเร็จการศึกษา หากพ้นสภาพนักศึกษาจะมีการ Disable บัญชีผู้ใช้งานเบื้องตัน โดยจะเก็บข้อมูลไว้ในระบบประมาณ 2 ปี ก่อนพิจารณาดำเนินการตามระเบียบ

(2) ข้อมูลบุคลากร สำหรับบุคลากรทั่วไปจะเก็บข้อมูลไว้ 2 ปีหลังลาออก แต่กรณีอาจารย์ที่เป็นข้าราชการจะคงบัญชีอีเมลไว้ตลอดชีวิต เนื่องจากมีความจำเป็นในการใช้เป็นชื่อผู้ประสานงานในผลงานวิจัย

นอกจากการจัดเก็บข้อมูลส่วนบุคคลผ่านระบบและฐานข้อมูลต่าง ๆ แล้ว ยังมีกรณีการจัดเก็บข้อมูลส่วนบุคคลจากกล้องวงจรปิด (CCTV) มหาวิทยาลัยฯ และมีมาตรการควบคุมและเข้าถึงกล้องวงจรปิด (CCTV) โดยการบริหารจัดการภาพจากกล้องวงจรปิดภายในมหาวิทยาลัย มีการแบ่งความรับผิดชอบระหว่างส่วนกลาง ซึ่งอยู่ภายใต้การกำกับและดูแล โดยทีมแอดมินของสำนักวิทยบริการฯ และส่วนงานคณะ/สำนัก/สถาบัน จะอยู่ภายใต้การดูแลของหน่วยงานนั้น ๆ เอง

(1) การจัดเก็บและระยะเวลา

การจัดเก็บภาพขึ้นอยู่กับความจุของ Hard Disk (NVR) เมื่อข้อมูลเต็มระบบจะทำการบันทึกวนทับอัตโนมัติ งานพัฒนาระบบเครือข่ายและการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ดูแลกล้องพื้นที่สาธารณะส่วนภายในอาคารเป็นความรับผิดชอบของแต่ละคณะ

(2) ขั้นตอนการขอเข้าถึงข้อมูลภาพ

แนวปฏิบัติดำเนินการขอตามประกาศมหาวิทยาลัยฯ ซึ่งมีแนวทาง ขั้นตอน และวิธีการขอดูภาพ และขอสำเนาภาพไว้อย่างชัดเจน ซึ่งหน่วยงานภายในสามารถนำไปใช้ได้ สรุปแนวทางการขอดู ภาพและขอสำเนาภาพได้ ดังนี้

- การขอดูภาพ ควรระบุวัตถุประสงค์และช่วงเวลาที่ชัดเจน (วินาที/นาที)

- การขอสำเนาภาพ (ไฟล์วิดีโอ) หากต้องการนำภาพออกไปประกอบคดี ต้องมีบันทึกประจำวัน หรือหลักฐานการแจ้งความจากสถานีตำรวจมาแนบ เพื่อป้องกันความรับผิดชอบของเจ้าหน้าที่แอดมินจากการเปิดเผยภาพบุคคลอื่นที่ไม่เกี่ยวข้อง

- หน่วยงานควรจัดทำป้ายเตือน "พื้นที่บันทึกภาพกล้องวงจรปิด" ตามกฎหมาย เพื่อแจ้งให้ผู้ใช้บริการทราบ ข้อสรุป ประเด็นนี้ จึงขอความอนุเคราะห์ให้แอดมินแต่ละหน่วยงาน นำส่งข้อมูลเกี่ยวกับวิธีการจัดเก็บข้อมูลตามแบบฟอร์มการบันทึกข้อมูลระบบสารสนเทศ ประกอบไปด้วย ชื่อระบบ ข้อมูลที่จัดเก็บ ระยะเวลาการจัดเก็บสิทธิการเข้าถึงข้อมูล เจ้าหน้าที่ประมวลผลข้อมูล เป็นต้น ภายในวันที่ 5 มีนาคม 2569

2.2 การตรวจสอบความรับผิดชอบของเจ้าหน้าที่แอดมิน/มหาวิทยาลัย จากการสอบถามทีมแอดมินในแต่ละหนวยงาน สามารถระบุตัวตนไดวาใครเขามา ดู/แกไข ในระบบตาง ๆ มหาวิทยาลัยฯ มีประกาศเชิงนโยบายเกี่ยวกับมาตรการคุมครองขอมูลสวนบุคคล แตยังไมมีแนวปฏิบัติกรณีเกิดเหตุละเมิดขอมูลสวนบุคคล และขั้นตอน/วิธีการรายงานมหาวิทยาลัย และแจงเหตุละเมิดมายัง DPO

ข้อสรุป

DPO ได้ให้ข้อเสนอแนะหน่วยงานว่า ควรกำหนดหน้าที่ของเจ้าหน้าที่แอดมินให้ชัดเจนว่าใครเป็น Data Processor หรือใครบ้างที่เป็นเพียงคณะทำงานช่วยเหลือ Data Processor เพื่อกำหนดกรอบหน้าที่และความรับผิดชอบให้ชัดเจนตามกฎหมาย PDPA

2.3 สอบถามประเด็นความเสี่ยงในการปฏิบัติงาน เพื่อนำมาเป็นกรณีศึกษาในการออกแบบกิจกรรมการจัดอบรมสำหรับแอดมิน โดยได้มีการแลกเปลี่ยนประสบการณ์การทำงาน และสอบถามวิธีการดำเนินการในประเด็นดังนี้

(1) การขอข้อมูลส่วนตัวจากบุคคลภายนอก มีกรณีผู้ปกครองโทรศัพท์ติดต่อมาขอเบอร์โทรศัพท์ และข้อมูลติดต่อของอาจารย์ เจ้าหน้าที่ไม่ให้ข้อมูลติดต่อส่วนตัว แต่ให้แจ้งขั้นตอนการติดตามงานหรือผลการเรียนตามระเบียบแทนแบบนี้ถูกต้องหรือไม่

(2) การยืนยันสถานะบุคลากรทางโทรศัพท์ การให้ข้อมูลว่าใครทำงานอยู่ที่ไหนผ่านทางโทรศัพท์ มีความเสี่ยงเจ้าหน้าที่ควรดำเนินการอย่างไร

(3) การจัดการข้อมูลที่ละเอียดอ่อน การฝากเจ้าหน้าที่ธุรการจัดการเรื่องการจัดทำบันทึกข้อความในระบบซึ่งต้องให้ข้อมูลส่วนตัวแก่เจ้าหน้าที่ กรณีนี้เจ้าหน้าที่รู้สึกลำบากใจที่ต้องรู้ข้อมูลส่วนบุคคล เป็นจุดเสี่ยงที่อาจทำให้ข้อมูลรั่วไหลได้ หากไม่มีการจัดการที่รัดกุม และเจ้าหน้าที่ที่ช่วยเหลือในการจัดทำเอกสารอาจจะต้องรับผิดชอบจึงเกิดความกังวลในการปฏิบัติงาน

(4) การใช้ข้อมูลเพื่อประกอบการเรียนการสอน/การเป็นวิทยากร การนำระบบที่มีข้อมูลนักศึกษาจริงไปแสดงเป็นตัวอย่าง โดยไม่ปิดบังรายชื่อหรือเกรด ถือเป็นพฤติกรรมสุ่มเสี่ยงที่อาจถูกร้องเรียนหรือไม่

(5) การที่มีบุคคลภายนอกมาขอใช้ server ของหน่วยงานในการประชาสัมพันธ์ ควรมีขอบเขตอย่างไร หากมีการประชาสัมพันธ์หรือใช้พื้นที่ทำเรื่องส่วนตัว ซึ่งอาจมีข้อมูลที่สุ่มเสี่ยง ควรมีแนวทางการป้องกัน อย่างไร

(6) การแจ้งให้บุคลากร/นักศึกษา เปลี่ยนรหัสผ่านแต่ไม่เปลี่ยนตามที่ประชาสัมพันธ์ ควรมีแนวทางการดำเนินการอย่างไร หากข้อมูลรั่วไหลหรือถูกละเมิด เจ้าหน้าที่จะต้องรับผิดชอบหรือไม่

ข้อสรุป

จากการรับฟังปัญหาและข้อกังวลในการปฏิบัติงานต่าง ๆ DPO ได้แนะนำวิธีการดำเนินการให้รัดกุมไปเบื้องต้น แต่เพื่อให้มีมาตรการและแนวทางที่ชัดเจน จึงจะนำเป็นกรณีศึกษาที่จะนำไปปรับใช้ในการออกแบบกิจกรรมที่จะจัดอบรมในทีมแอดมินต่อไป

3. ประเด็นความเสี่ยงด้านความปลอดภัยทางไซเบอร์และสถิติการโจมตี

รายงานสถิติความปลอดภัยทางไซเบอร์ (ช่วงเดือนมกราคม - กุมภาพันธ์) พบประเด็นที่น่ากังวลดังนี้

รายการความเสี่ยง	รายละเอียด
รายการความเสี่ยง	พบการโจมตีประมาณ 18.8 ล้านครั้ง (ระบบป้องกันได้ 100%)
จำนวนการโจมตี	พบ 54 รายการ โดยเป็นระดับสูง 30 รายการ
ช่องโหว่ที่เป็นอันตราย	ตรวจพบเครื่องในเครือข่ายถูกฝังมัลแวร์หรือเป็น "ซอมบี้" ประมาณ 800 เครื่อง
เครื่องที่ติดมัลแวร์	ส่วนใหญ่มาจากประเทศจีนและสวิตเซอร์แลนด์
แหล่งที่มาการโจมตี	98% ของผู้ใช้งานตั้งรหัสผ่านที่คาดเดาง่าย เช่น เบอร์โทรศัพท์ ชื่อ หรือวันเกิด

ข้อเสนอแนะ

ควรมีนโยบายบังคับเปลี่ยนรหัสผ่านทุก 3 เดือน หรือกำหนดรูปแบบรหัสผ่านที่ซับซ้อน (เช่น ผสมตัวอักษรพิเศษ หรือรหัสหน่วยงาน) ตั้งแต่การลงทะเบียนครั้งแรกเพื่อลดความเสี่ยงจากการถูกสุ่มรหัส (Brute Force)

4. ข้อเสนอแนะและแนวทางการดำเนินงานในอนาคต

4.1 ข้อเสนอแนะในการปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA)

จากการประชุมทีมแอดมิน มีประเด็นสำคัญที่เกี่ยวข้องกับการดำเนินการเพื่อคุ้มครองผู้ปฏิบัติงานเบื้องต้น และปฏิบัติตามกฎหมาย PDPA ดังนี้

(1) ทีมแอดมินมีลักษณะการปฏิบัติงานในบทบาทของผู้ประมวลผลข้อมูล (Data Processor) เจ้าหน้าที่แอดมินจึงมีสถานะเป็นผู้ประมวลผลข้อมูลตามกฎหมาย PDPA ดังนั้น จึงจำเป็นต้องมีคำสั่งแต่งตั้งหรือเอกสารที่กำหนดหน้าที่ความรับผิดชอบ ซึ่งระบุภาระงานและชื่อรายบุคคลที่ชัดเจน เพื่อให้มหาวิทยาลัยสามารถคุ้มครองทางกฎหมายแก่เจ้าหน้าที่ได้ หากเกิดเหตุละเมิดที่เกิดจากการปฏิบัติหน้าที่ตามปกติ

(2) การจัดทำข้อตกลงรักษาความลับ (NDA) อยู่ระหว่างการพิจารณาจัดทำสัญญาหรือข้อตกลงรักษาความลับเพิ่มเติม เพื่อเป็นเกราะป้องกันให้ทีมแอดมินและสร้างมาตรฐานการทำงานที่เป็นระบบ

4.2 แนวทางการดำเนินงานในอนาคต

(1) การจัดอบรมเชิงปฏิบัติการ (Workshop) สำหรับทีมแอดมิน ซึ่งมุ่งเน้นการจำลองเหตุการณ์จริง (Case Study) ให้ทีมแอดมินได้ทดลองแก้ปัญหามากกว่าการบรรยายข้อกฎหมายเพียงอย่างเดียว

(2) การจัดทำ Checklist เพื่อพัฒนาการประเมินความเสี่ยงและภาระงานที่เกี่ยวข้องกับข้อมูลส่วนบุคคลสำหรับแต่ละหน่วยงาน รวมถึงการจัดทำข้อตกลงรักษาความลับ (NDA) ให้ตรงตามบทบาทหน้าที่และมีความกระชับเพื่อไม่ให้เป็นภาระต่อผู้ปฏิบัติงานจนเกินไป

(3) การทบทวนคำสั่งแต่งตั้งคณะกรรมการ/คณะทำงานตามกฎหมาย PDPA เพื่อเป็นการปรับปรุงรายชื่อคณะกรรมการและผู้รับผิดชอบระบบให้เป็นปัจจุบัน และสอดคล้องตามกฎหมาย

ภาพกิจกรรม

ประเด็นที่ 2 รายงานผลการดำเนินงานการตรวจสอบและป้องกันการโจมตีบนเว็บไซต์

2.1 สรุปเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ที่ตรวจพบ

<u>เหตุการณ์ที่ 1</u> เมื่อวันที่ 18 - 19 กุมภาพันธ์ 2569 ตรวจพบการโจมตีประเภทการเข้าถึงทรัพยากรที่ไม่ถูกต้องหรือผิดกฎหมาย (Illegal Resource Access) โดยมีเป้าหมายหลักคือเว็บไซต์ของหน่วยงาน kpru.ac.th เหตุการณ์นี้เกิดขึ้นอย่างรุนแรงในช่วงเวลาสั้นๆ จากการตรวจสอบพบว่าการโจมตีดังกล่าวมีแหล่งที่มาจากที่อยู่ไอพี (Source IP) ซึ่งจดทะเบียนในประเทศออสเตรเลีย (Australia) โดยเครื่องมือที่ใช้ในการโจมตีถูกระบุว่าเป็นโปรแกรมอัตโนมัติที่ไม่ทราบประเภท (Unknown Bot) ที่มีความพยายามในการร้องขอข้อมูลสูงถึง 838 ครั้งในช่วงเวลาดังกล่าว ความรุนแรงของเหตุการณ์นี้ถูกจัดอยู่ในระดับวิกฤต(Critical) เนื่องจากเป็นลักษณะความพยายามในการเจาะจงเข้าถึงส่วนประกอบสำคัญของระบบที่อาจนำไปสู่การรั่วไหลของข้อมูลหรือการข้ามผ่านกลไกการพิสูจน์ตัวตน

อย่างไรก็ตาม ระบบ Cloud WAF สามารถปฏิบัติการป้องกันได้อย่างมีประสิทธิภาพสูงสุด และการร้องขอที่ผิดปกติทั้ง 838 รายการถูกสกัดกั้น (Blocked) โดยสมบูรณ์ 100% ทำให้ไม่เกิดความเสียหายต่อข้อมูล ไม่มีการบุกรุกเข้าสู่ระบบหลังบ้านได้สำเร็จ และไม่มีผลกระทบต่อเสถียรภาพหรือความพร้อมใช้งานของเว็บไซต์สำหรับผู้ใช้ทั่วไปในระหว่างเกิดเหตุการณ์และหลังเกิดเหตุการณ์ หน่วยงานจึงยังคงสถานะความปลอดภัยที่มั่นคงจากการป้องกันเชิงรุกในครั้งนี้

<u>เหตุการณ์ที่ 2</u> เมื่อวันที่ 20 - 23 กุมภาพันธ์ 2569 จากการเฝ้าระวังและตรวจสอบระบบรักษาความปลอดภัยสารสนเทศของหน่วยงาน พบความพยายามในการโจมตีทางไซเบอร์ในลักษณะที่เป็นอันตรายร้ายแรงระดับวิกฤต (Critical) โดยมีเป้าหมายหลักไปที่เครื่องแม่ข่ายมุ่งเน้นการให้บริการด้านการศึกษาออนไลน์ภายใต้ชื่อโดเมน mooc.kpru.ac.th ซึ่งเหตุการณ์ดังกล่าวเกิดขึ้นในวันที่ 23 กุมภาพันธ์ 2569 โดยประเภทการโจมตีหลักที่ตรวจพบคือการพยายามเข้าถึงทรัพยากรโดยไม่ได้รับอนุญาต (Illegal Resource Access) ผ่านการใช้เครื่องมืออัตโนมัติประเภท Hacking Tool มีต้นทางความพยายามในการโจมตีมาจากหมายเลขไอพีอยู่ที่ประเทศสิงคโปร์ (Singapore) ทั้งนี้สามารถตรวจจับและดำเนินการสกัดกั้น (Blocked) การเชื่อมต่อที่ผิดปกติได้ทั้งหมด 100% คิดเป็นจำนวนเหตุการณ์ทั้งสิ้น 449 รายการ ส่งผลให้การโจมตีในครั้งนี้ล้มเหลวโดยสิ้นเชิง และไม่เกิดผลกระทบใดๆ ต่อเสถียรภาพของระบบบริการของหน่วยงานยังคงสามารถดำเนินต่อไปได้ตามปกติ และความถูกต้องของข้อมูลภายในฐานข้อมูลไม่ได้รับความเสียหายแต่อย่างใด

โดยสรุปแล้ว ระบบยังมีความมั่นคงปลอดภัยสูง อย่างไรก็ตาม ข้อเสนอแนะที่สำคัญที่สุดคือการเร่งตรวจสอบและอัปเดต Patch ของซอฟต์แวร์ให้เป็นปัจจุบันที่สุด และการเพิ่มความเข้มข้นในการวิเคราะห์ทราฟฟิกจากต่างประเทศ เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการโจมตีในลักษณะที่ซับซ้อนยิ่งขึ้นในอนาคต

<u>เหตุการณ์ที่ 3</u> เมื่อวันที่ 4 - 5 มีนาคม 2569 พบช่องโหว่ใน IceWarp (IceWarp14) เป็นช่องโหว่ Sandbox Escape / Code Injection ใน n8n (แพลตฟอร์ม Workflow Automation แบบโอเพนซอร์ส) โดยในเวอร์ชันต่ำกว่า 2.10.1 / 2.9.3 / 1.123.22 ผู้ใช้ที่ล็อกอินแล้ว และมีสิทธิ์ สร้างหรือแก้ไข Workflow สามารถใช้ช่องโหว่ใน JavaScript Task Runner sandbox เพื่อรันโค้ดนอกขอบเขต sandbox (sandbox escape) ซึ่งจากการตรวจสอบพบหมายเลข IP Address ของ 2 หน่วยงานภายในมหาวิทยาลัย อาจได้รับผลกระทบจากช่องโหว่ดังกล่าว ทั้งนี้ส่วนกลางได้ประสานแจ้งผู้ดูแลไปเรียบร้อยแล้ว กรณีนี้หากหน่วยงานใดที่ใช้โอเพนซอร์ส ควรเร่งตรวจสอบและอัปเดตเวอร์ชั่นให้เป็นปัจจุบันที่สุด

<u>เหตุการณ์ที่ 4</u> เมื่อวันที่ 4 - 5 มีนาคม 2569 พบภัยคุกคามจากการป้องกันการโจมตีเว็บไซต์ระบบสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชร และมีการพุ่งเป้าโจมตีมายังระบบสารสนเทศหลัก การโจมตีส่วนใหญ่มีลักษณะเป็นการพยายามเข้าถึงทรัพยากรของระบบโดยไม่ได้รับอนุญาต (Illegal Resource Access) ซึ่งคาดว่าเป็นการดำเนินการผ่านระบบอัตโนมัติหรือบอทที่ไม่สามารถระบุตัวตนได้ (Unknown Bot) ทั้งนี้ แหล่งที่มาของการโจมตี (Top Attackers) พบว่าหมายเลขไอพีที่มีพฤติกรรมโจมตีสูงสุดจดทะเบียนอยู่ในประเทศเยอรมนี (Germany) โดยมีค่าคะแนนความเสี่ยงของไอพี (IP Score) อยู่ที่ระดับ 68 จากการประเมินระดับความรุนแรงของเหตุการณ์พบว่าอยู่ในระดับวิกฤต (Critical) เนื่องจากมีจำนวนเหตุการณ์การโจมตีรวมทั้งสิ้น 9,111 เหตุการณ์ (Events)

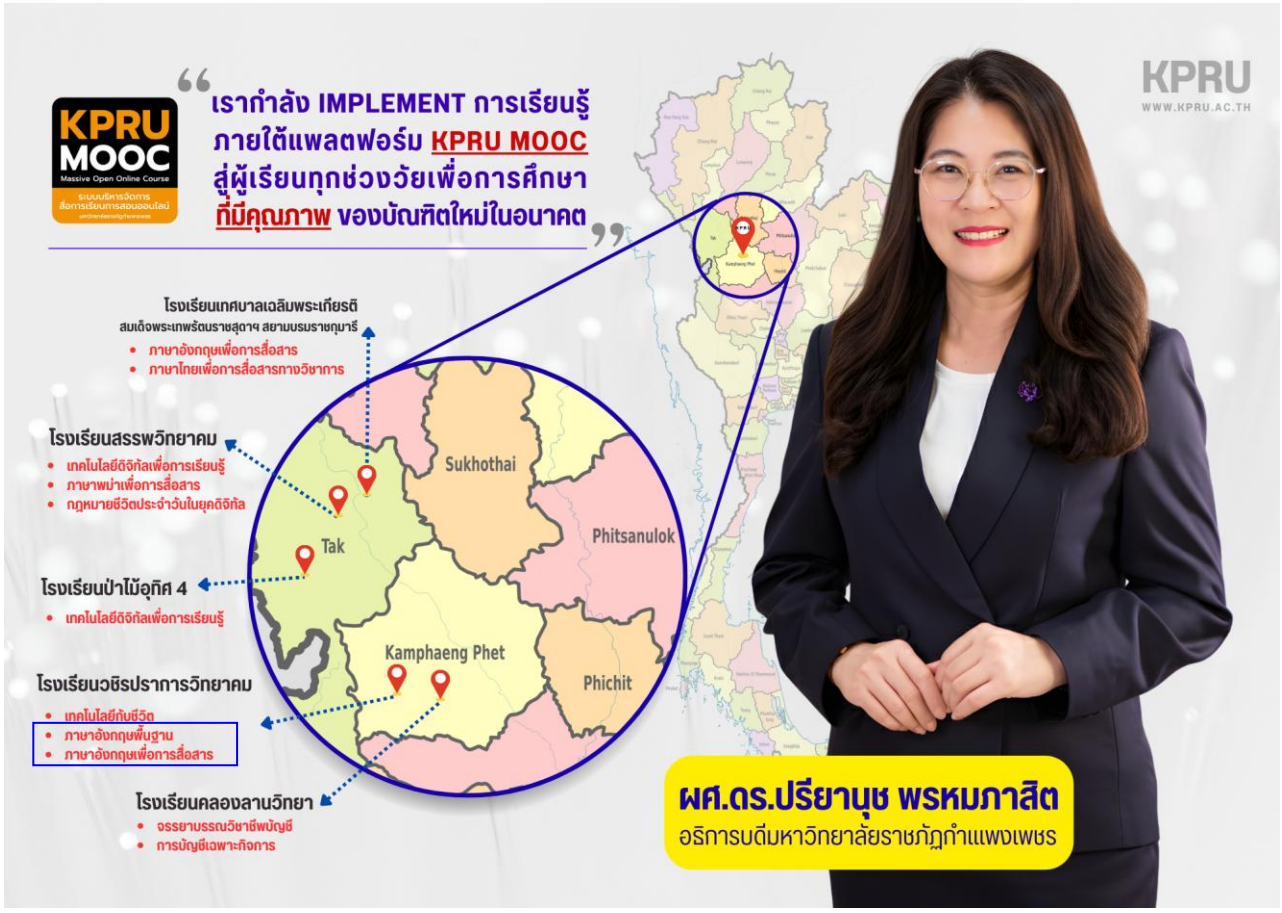
โดยสรุป กรณีพบเหตุการณ์หรือสถานการณ์ฉุกเฉิน อาจต้องขออนุญาตเชิญประชุม/อบรมเชิงปฏิบัติการ Admin เร่งด่วนโดยมิได้จัดทำบันทึกข้อความไปยังหน่วยงาน ทั้งนี้เพื่อให้ระงับป้องกันภัยคุกคามจากการป้องกันการโจมตีเว็บไซต์และระบบสารสนเทศของมหาวิทยาลัยราชภัฏกำแพงเพชร ได้อย่างทันท่วงที จึงขออภัยไว้ ณ ที่นี้

ประเด็นที่ 3 ความก้าวหน้าเกี่ยวกับการเรียนการสอนผ่านระบบ KPRU MOOC

3.1 หลักสูตร Online ส่งเสริมการเรียนรู้ ประจำปีงบประมาณ 2569 จำนวน 12 รายวิชา ดังนี้

(1) ศิลปะการจัดการอาหาร
(2) พื้นฐานการเขียนโปรแกรมเชิงสร้างสรรค์และปัญญาประดิษฐ์
(3) แคลคูลัส 1
(4) วิทยาศาสตร์โลกทั้งระบบ
(5) ความรู้พื้นฐานกฎหมายและระบบกฎหมาย
(6) การช่วยเหลือดูแลสุขภาพบุคคลที่บ้านและในชุมชน
(7) การออกแบบและโปรแกรมเชิงวัตถุ
(8) การออกแบบอินโฟกราฟิก
(9) การเขียนแบบและออกแบบด้วยคอมพิวเตอร์
(10) การยกระดับการทำงาน ด้วยปัญญาประดิษฐ์
(11) กฎหมายและจริยธรรม ในยุคดิจิทัล
(12) แนวคิดและทฤษฎีการบริหารท้องถิ่นสมัยใหม่

3.2 การจัดการเรียนการสอนรายวิชาศึกษาทั่วไป ผ่านแพลตฟอร์ม KPRU MOOC สำหรับโรงเรียนมัธยมศึกษา



วันที่ 13 กุมภาพันธ์ 2569 ผู้ช่วยศาสตราจารย์ ดร.พจน์ธรรม ณรงค์วิทย์ รองคณบดีฝ่ายวิชาการ คณะเทคโนโลยีอุตสาหกรรม ได้จัดส่งข้อมูลความก้าวหน้า เรื่องการขออนุมัติเปิดรายวิชาพื้นฐานของระบบบริหารจัดการสื่อการเรียนการสอนออนไลน์ (KPRU MOOC) ภาคเรียนที่ 1/2569

ด้วยคณะเทคโนโลยีอุตสาหกรรม ได้จัดการเรียนการสอนภายใต้ระบบบริหารจัดการสื่อการเรียน การสอนออนไลน์ (KPRU MOOC) รายวิชาพื้นฐาน วิชา เทคโนโลยีกับชีวิต ในปีการศึกษา 2/2568 ให้กับนักเรียนชั้นมัธยมศึกษาปีที่ 5/1 จำนวน 34 คน บัดนี้ การดำเนินการเรียนออนไลน์ได้ดำเนินการถึงการจัดการสอบกลางภาคในปีการศึกษา 2/2568 ลุล่วงไปด้วยดีและจะมีการจัดสอบปลายภาครายวิชาของ KPRU MOOC ให้กับนักเรียนกลุ่มดังกล่าวในวันที่ 6 มีนาคม 2569 นี้

ในการนี้ ทางคณะฯได้ปรึกษาหารือร่วมกันระหว่างผู้อำนวยการโรงเรียนวชิรปราการวิทยาคมและครูผู้รับผิดชอบประจำห้องเรียน ในการเปิดรายวิชาพื้นฐานของระบบบริหารจัดการสื่อการเรียนการสอน ออนไลน์ (KPRU MOOC) จำนวน 2 รายวิชา สำหรับการเรียนการสอน ในปีการศึกษา 1/2569 ให้กับนักเรียนชั้นมัธยมศึกษาปีที่ 6/1 จำนวน 34 คน รายวิชาพื้นฐาน วิชา ภาษาอังกฤษพื้นฐาน และวิชาภาษาอังกฤษเพื่อการสื่อสาร โดยประสงค์ขอเปิดระบบในการเข้าเรียนออนไลน์ รายวิชาดังกล่าว ตั้งแต่วันที่ 6 มีนาคม 2569 ซึ่งเป็นวันสอบปลายภาคที่ทางคณะเทคโนโลยีอุตสาหกรรมได้จัดสอบ เพื่อปฐมนิเทศและให้นักเรียนเริ่มเรียนออนไลน์ได้ ในช่วงวันหยุดปิดเทอม ภายใต้การกำกับและติดตามจากครูผู้รับผิดชอบประจำห้องเรียน