ที่ ศธ ๐๗๐๔๕/ว ๔๙๒

สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด
๓๔๗ ถนนสุขุมวิท ต.วังกระแจะ
อ.เมืองตราด จ.ตราด ๒๓๐๐๐

๑๙ พฤษภาคม ๒๕๖๙

เรื่อง แนวทางการป้องกันและคำแนะนำการรับมือภัยคุกคามจากโมเดลปัญญาประดิษฐ์ (AI)

เรียน ผู้อำนวยการศูนย์ส่งเสริมการเรียนรู้ระดับอำเภอทุกแห่งในสังกัด

สิ่งที่ส่งมาด้วย เอกสารแจ้งเตือนกรณี Mythos ความเสี่ยงรูปแบบใหม่ จำนวน ๑ ฉบับ

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หรือ ThaiCERT ได้ดำเนินการเฝ้าระวัง ติดตามพัฒนาการของเทคโนโลยีปัญญาประดิษฐ์ที่มีแนวโน้มส่งผลกระทบต่อภูมิทัศน์ภัยคุกคามทางไซเบอร์อย่างใกล้ชิด และพบว่า Mythos เป็นโมเดล AI ที่ถูกพัฒนาโดยบริษัท Anthropic ซึ่งมีขีดความสามารถในการค้นหาช่องโหว่แบบ Zero – day ในระบบปฏิบัติการและเว็บบราวเซอร์หลักรวมถึงสามารถช่วยปรับปรุง exploit สำหรับโจมตีช่องโหว่บางประเภทได้ โดยเทคโนโลยีดังกล่าวอาจทำให้การโจมตีทางไซเบอร์เกิดขึ้นเร็วขึ้นหรือมีประสิทธิภาพมากขึ้น สกมช. จึงได้จัดทำเอกสารแจ้งเตือนพร้อมแนวทางการป้องกันและคำแนะนำสำหรับหน่วยงาน เพื่อมิให้กระทบต่อโครงสร้างพื้นฐานสำคัญระบบสารสนเทศหรือประชาชนที่มาใช้บริการ

สำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด จึงขอให้สถานศึกษาทุกแห่งจำเป็นต้องรับทราบและนำแนวทางการป้องกันดังกล่าวไปดำเนินการในส่วนที่เกี่ยวข้องโดยเร่งด่วน ดังนี้

๑. ศึกษาและดำเนินการตามแนวทางการป้องกันและคำแนะนำของ ThaiCERT รายละเอียดตามสิ่งที่ส่งด้วย ครอบคลุม ๗ มาตรการ ๒๓ รายการ โดยเฉพาะมาตรการเร่งด่วน ได้แก่

๑.๑ เร่งตรวจสอบและแก้ไขช่องโหว่ระบบสารสนเทศที่เปิดให้บริการจากภายนอกเพื่อลดความเสี่ยงจากการถูกค้นหาและโจมตีโดยอัตโนมัติ

๑.๒ บังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีผู้ดูแลระบบ ระบบบริหารจัดการ อุปกรณ์สำคัญ และบริการคลาวด์ที่เกี่ยวข้อง

๑.๓ ทบทวนและปรับสิทธิ์การเข้าถึงของผู้ใช้งาน บัญชีบริการ และการเชื่อมต่อระหว่างระบบ ให้เป็นไปตามหลัก Least Privlege พร้อมยกเลิกบัญชีที่ไม่ใช้งาน

๒. จัดทำหรือทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan) ให้ครอบคลุมสถานการณ์การโจมตีโดยใช้ AI เป็นเครื่องมือ และกำหนดผู้รับผิดชอบในแต่ละขั้นตอนอย่างชัดเจน

๓. ตรวจสอบการสำรองข้อมูลให้เป็นไปตามหลัก ๓-๒-๑ Backup (สำเนาข้อมูลบนสื่อบันทึก ๒ ประเภท และเก็บนอกสถานที่ ๑ ชุด) และทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

๔.กำหนด....

๔. กำหนดนโยบายการใช้งาน AI สำหรับบุคลากร โดยเฉพาะการห้ามนำข้อมูลส่วนบุคคลของผู้เรียนและข้อมูลภายใต้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ไปป้อนในระบบ AI นอกองค์กร และให้มีผู้เชี่ยวชาญกำกับดูแลในจุดตัดสินใจสำคัญตลอด

๕. ดำเนินการลด Attack Surface โดยปิดพอร์ต โปรโตคอล และบริการที่ไม่จำเป็น พิจารณาดำเนินการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อจำกัดการเคลื่อนย้ายของผู้โจมตีภายในระบบ รวมทั้งจัดให้มีการเฝ้าระวังและบันทึกเหตุการณ์ (Log) จากระบบสำคัญอย่างต่อเนื่อง

๖. รายงานผลการดำเนินการตามมาตรการข้างต้นพร้อมข้อจำกัดและแผนดำเนินการมายังสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด ภายในวันที่ ๒๕ พฤษภาคม ๒๕๖๙

จึงเรียนมาเพื่อทราบ และดำเนินการต่อไป

ขอแสดงความนับถือ

(นางสาวสุวรรณา สิงห์ภู่)
นักจัดการงานทั่วไปชำนาญการ รักษาการในตำแหน่ง
ผู้อำนวยการสำนักงานส่งเสริมการเรียนรู้ประจำจังหวัดตราด

กลุ่มส่งเสริมและพัฒนาการเรียนรู้
งานส่งเสริมการเรียนรู้ตลอดชีวิต
โทรศัพท์ ๐ ๓๙๕๑ ๘๐๙๑
โทรสาร ๐ ๓๙๕๑ ๘๐๙๒

“เรียนดี มีคุณธรรม”

แบบประเมิน Checklist รับมือภัยคุกคาม Mythos

กรณีการใช้ปัญญาประดิษฐ์ (AI) เป็นเครื่องมือโจมตีระบบสารสนเทศ | ThaiCERT TLP:CLEAR

กลุ่มเทคโนโลยีดิจิทัลและสารสนเทศ กรมส่งเสริมการเรียนรู้ | ประเมิน ณ วันที่ 30 เมษายน 2569

สรุปผลการประเมิน (Executive Summary)

☑ ดำเนินการแล้ว 0 รายการ	⚠ ดำเนินการบางส่วน 11 รายการ	✗ ยังไม่ดำเนินการ 12 รายการ	รวมทั้งหมด 23 รายการ
ความเสี่ยงสูงมาก: 7 รายการ	ความเสี่ยงสูง: 11 รายการ	ความเสี่ยงกลาง: 5 รายการ	ข้อสังเกต: สกร. ยังมีช่องว่างด้าน Security อยู่มาก

ข้อสังเกตสำคัญ: สกร. ยังไม่ได้ดำเนินการ 12 รายการ (52%) และมีรายการที่ความเสี่ยงสูงมากถึง 7 รายการ ซึ่งต้องเร่งดำเนินการโดยด่วน ข้อจำกัดหลักคือกำลังบุคลากร IT ที่มีเพียง 5 คน ดูแลระบบมากกว่า 11 แพลตฟอร์ม จึงแนะนำให้ Prioritize มาตรการเร่งด่วน (MFA, Patch, IRP) ก่อน และพิจารณาจ้าง MSSP สำหรับงาน Security Monitoring

---

มาตรการที่ 1 — มาตรการเร่งด่วน ระดับความสำคัญ : เร่งด่วน — ดำเนินการทันที

1.1 ตรวจสอบและแก้ไขช่องโหว่ โดยเฉพาะระบบที่เปิดให้บริการจากภายนอก เพื่อลดความเสี่ยงจากการถูกค้นหาและโจมตีโดยอัตโนมัติ	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	สกร. มีการตรวจสอบช่องโหว่เป็นครั้งคราว แต่ยังไม่เป็นระบบอย่างต่อเนื่อง ระบบที่เปิดบริการจากภายนอก ได้แก่ DOLEdemy, DOLE ZD, เว็บไซต์กรม (dole.go.th) และ API endpoints ต่าง ๆ ยังไม่ผ่านกระบวนการ Vulnerability Assessment อย่างครบถ้วนและสม่ำเสมอ	
หลักฐาน/เหตุผล	กลุ่ม กย. มีบุคลากร IT เพียง 5 คน ดูแลระบบมากกว่า 11 แพลตฟอร์ม ทำให้ขาดทรัพยากรสำหรับ Vulnerability Assessment อย่างสม่ำเสมอ นอกจากนี้ Legacy systems บางส่วน เช่น ระบบทะเบียน สกร. เดิม ยังคงใช้งานอยู่และอาจมีช่องโหว่สะสม	
ข้อเสนอแนะ	เร่งจัดทำ Internet-facing asset inventory และทำ VA/PT (Vulnerability Assessment/Penetration Testing) ภายใน พ.ค. 69 เน้น DOLEdemy และ DOLE ZD ก่อนเป็นลำดับแรก พิจารณาจ้างบุคคลภายนอกทำ Pentest หากทรัพยากรภายในไม่เพียงพอ	

1.2 บังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) สำหรับบัญชีผู้ดูแลระบบ ระบบบริหารจัดการ และบริการ Cloud ในกรณีที่ไม่รองรับ MFA ให้จำกัดการเข้าถึงด้วยการกำหนด IP Whitelist	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	ระบบส่วนใหญ่ของ สกร. ยังใช้ Username/Password เป็นหลักในการเข้าถึงสำหรับผู้ดูแลระบบ MFA ยังไม่ได้บังคับใช้อย่างเป็นระบบ สกร. ใช้ Server HCI-Nutanix ที่เป็น On-premise และบางส่วนเช่า Server เอกชน จำนวน 15 VM ซึ่งการจัดการ MFA บน On-premise hypervisor และ VM เหล่านี้มีความซับซ้อนกว่าระบบ Cloud และยังไม่ได้รับการกำหนดนโยบายที่ชัดเจน		
หลักฐาน/เหตุผล	สกร. ใช้ Nutanix HCI (On-premise) เป็น infrastructure หลัก และเช่า VM จาก Private Cloud เอกชน 15 VM ทั้งสองส่วนยังไม่มีนโยบายบังคับ MFA สำหรับ Admin accounts บัญชีผู้ดูแลระบบของแพลตฟอร์มต่าง ๆ เช่น DOLEdemy (Moodle), DOLE ZD บน VM เหล่านี้ยังไม่มีการบังคับ MFA และ Nutanix Prism (Console บริหาร HCI) เองก็ยังไม่ได้เปิด MFA		
ข้อเสนอแนะ	ดำเนินการเปิดใช้ MFA ทันทีในลำดับต่อไปนี้: (1) Nutanix Prism Central — เปิด MFA สำหรับ Admin ทุกบัญชีก่อนเป็นลำดับแรก, (2) VM ทั้ง 15 ตัวที่เช่า Server เอกชน — ตั้ง MFA หรือ IP Whitelist, (3) DOLEdemy และ DOLE ZD บน VM ทั้งหมด ดำเนินการให้เสร็จภายใน 2 สัปดาห์ สำหรับระบบที่ไม่รองรับ MFA ให้จำกัดการเข้าถึงด้วย IP Whitelist เฉพาะ IP ของ สกร. เท่านั้น		

1.3 ตรวจสอบและจำกัดการเข้าถึงระบบพัฒนา (dev) ระบบทดสอบ และระบบ staging ที่สามารถเข้าถึงได้จากอินเทอร์เน็ต รวมถึงส่วนบริหารจัดการระบบดังกล่าว	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	ระบบใหม่ที่พัฒนาด้วย Agile/Microservices มี CI/CD pipeline ซึ่งระบบ staging บางส่วนอาจเข้าถึงได้จากภายนอกเพื่อความสะดวกในการทดสอบ ยังไม่มีนโยบายชัดเจนที่ห้ามเปิดระบบ dev/test สู่ Internet		
หลักฐาน/เหตุผล	การพัฒนาระบบ DOLE ZD และ DOLE OOSCY ใช้แนวทาง Microservices ซึ่งมักมี staging environment ที่เปิดเพื่อให้ทีมทดสอบจากภายนอกสำนักงานเข้าถึงได้ ระบบเหล่านี้อาจไม่ได้รับการป้องกันเท่าระบบ production		
ข้อเสนอแนะ	สำรวจและปิดการเข้าถึง staging/dev ทุกระบบจากอินเทอร์เน็ตภายใน 1 สัปดาห์ หากจำเป็นต้องเข้าถึงจากภายนอก ให้ใช้ VPN หรือ SSH Tunnel เท่านั้น กำหนดนโยบาย: 'No dev/staging on public internet' อย่างเป็นทางการ		

1.4 ทบทวนการตั้งค่าด้านความมั่นคงปลอดภัยของระบบ Cloud โดยเฉพาะทรัพยากรที่เปิดเผยสู่สาธารณะ การตั้งค่าสิทธิ์ที่เกินความจำเป็น และส่วนบริหารจัดการที่อาจเข้าถึงได้จากภายนอก	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	สกร. ใช้ Server HCI-Nutanix (On-premise) เป็น infrastructure หลัก และเช่า Server เอกชน 15 VM โดย configuration ด้านความปลอดภัยของแต่ละ VM ขึ้นอยู่กับทีมพัฒนาและผู้ดูแลระบบแต่ละคน ยังไม่มีการทบทวนการตั้งค่า security ระดับ VM อย่างเป็นระบบ โดยเฉพาะ Network policies, Firewall rules และ Service exposure ของแต่ละ VM	
หลักฐาน/ เหตุผล	Nutanix HCI ที่ใช้อยู่มี Nutanix Prism Central เป็น management plane และแต่ละ VM บน On-premise หรือ VM เช่าเอกชนทั้ง 15 ตัว อาจมีการ expose ports หรือ services ที่ไม่จำเป็นโดยไม่ตั้งใจ เนื่องจากไม่มีกระบวนการ review configuration อย่างสม่ำเสมอ	
ข้อเสนอแนะ	ทำ VM Security Configuration Review สำหรับ VM ทั้งหมดบน Nutanix และ VM เช่าเอกชน 15 ตัว ภายใน พ.ค.-มิ.ย. 69 ตรวจสอบ: Network ACL / Firewall rules ของแต่ละ VM, Database ports (ห้าม expose สู่ภายนอก), API endpoint authorization, User accounts และ SSH keys บน VM ทุกตัว ใช้ Nutanix Flow (Network Security ใน Nutanix) ช่วยกำหนด micro-segmentation ระหว่าง VM	

1.5 ทบทวนและปรับสิทธิ์การเข้าถึงของผู้ใช้งาน บัญชีบริการ และการเชื่อมต่อระหว่างระบบ ให้เป็นไปตามหลัก Least Privilege พร้อมยกเลิกบัญชีที่ไม่ใช้งาน	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	ยังไม่มีกระบวนการทบทวนสิทธิ์การเข้าถึง (Access Review) อย่างเป็นระบบและสม่ำเสมอ บัญชีผู้ใช้งานเดิมที่ลาออก โอนย้าย หรือไม่ได้ใช้งานแล้ว อาจยังคงมีสิทธิ์เข้าถึงระบบอยู่ และ service accounts สำหรับการเชื่อมต่อระหว่างแพลตฟอร์ม (เช่น API ระหว่าง DOLE ZD กับ DOLE OOSCY) อาจมีสิทธิ์เกินความจำเป็น	
หลักฐาน/ เหตุผล	สกร. มีการเชื่อมต่อ API ระหว่าง 4 แพลตฟอร์มหลัก (ข้อมูลผู้เรียน / สอบเทียบ / ธนาคาร หน่วยกิต / บริหารสำนักงาน) และ DOLEdemy เชื่อมกับ ThaiD ซึ่ง service accounts เหล่านี้มักได้รับสิทธิ์กว้างเพื่อความสะดวกในการพัฒนา	
ข้อเสนอแนะ	จัดทำ User Access Review ภายใน พ.ค.-มิ.ย. 69 ครอบคลุม: (1) บัญชีบุคลากรที่ลาออก/โอนย้าย, (2) service accounts ทุกตัว, (3) สิทธิ์ Admin ที่ไม่จำเป็น กำหนดให้ทบทวนสิทธิ์ทุก 6 เดือน และกำหนดนโยบาย auto-disable บัญชีที่ไม่ active เกิน 90 วัน	

1.6 ตรวจสอบและเปิดใช้มาตรการป้องกันการโจมตีแบบ DDoS Protection สำหรับระบบที่เปิดให้บริการจากภายนอก	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	สกร. ใช้ Nutanix HCI (On-premise) และ VM เช่าเอกชน 15 VM ซึ่งยังไม่มีการเปิดใช้ DDoS Protection ในระดับแอปพลิเคชัน (WAF) อย่างเป็นระบบ ระบบที่รับ traffic จากอินเทอร์เน็ตโดยตรงยังพึ่งพาเพียง Firewall ของผู้ให้บริการ Server เช่าเป็นหลัก	
หลักฐาน/ เหตุผล	DOLEdemy และ DOLE ZD ซึ่งเป็นระบบที่เปิดให้ประชาชนเข้าถึง มีความเสี่ยงสูงต่อการถูก DDoS โดยเฉพาะในช่วงเปิดภาคเรียนหรือช่วงสำรวจเด็กนอกระบบ ระบบที่รันบน Nutanix On premises และ VM เช่า รับ traffic จากภายนอกโดยตรงโดยยังไม่มี WAF หน้า	
ข้อเสนอแนะ	ติดตั้ง WAF สำหรับ DOLEdemy และ DOLE ZD โดยเร็ว: พิจารณา Cloudflare (มีแผนฟรีสำหรับภาครัฐ) หรือ WAF open-source เช่น ModSecurity บน Nginx สำหรับ VM เช่าเอกชน ติดต่อผู้ให้บริการ Server เช่าเพื่อขอ DDoS Protection ระดับ Network (L3/L4) และตั้ง Rate Limiting บน Application Layer	

มาตรการที่ 2 — ลด Attack Surface ระดับความสำคัญ : สำคัญสูง

2.1 จัดทำและปรับปรุงบัญชีทรัพย์สินสารสนเทศ (Asset Inventory) ให้ครบถ้วนและเป็นปัจจุบัน เพื่อให้มองเห็นจุดเสี่ยงภายในองค์กรได้อย่างต่อเนื่อง	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	มีการทำบัญชีทรัพย์สิน IT บางส่วนในรูปแบบ spreadsheet แต่ไม่ครบถ้วน โดยเฉพาะ Shadow IT (อุปกรณ์และบริการที่บุคลากรใช้งานเองโดยไม่ผ่าน กย.) และ Software dependencies ของแต่ละระบบ ยังไม่มีระบบ CMDB (Configuration Management Database) อย่างเป็นทางการ	
หลักฐาน/เหตุผล	สกร. มีแพลตฟอร์มหลักมากกว่า 11 ระบบ บวกกับ API integrations กับ ThaiD, DGA, กสศ. และระบบภายนอกอื่น ๆ การติดตาม dependencies และ 3rd-party components ยังทำด้วยมือและไม่สม่ำเสมอ	
ข้อเสนอแนะ	จัดทำ Asset Inventory อย่างเป็นทางการภายใน พ.ค.-มิ.ย. 69 ครอบคลุม: Hardware (Nutanix HCI nodes, network devices), Software & licenses, VM ทั้งหมดบน Nutanix + VM เช่าเอกชน 15 ตัว (ระบุ IP, OS, Service, Owner), API integrations กับระบบภายนอก, Third-party dependencies พิจารณาใช้ tool ช่วย เช่น Netbox หรือ spreadsheet ที่มีการอัปเดต monthly	

2.2 ลดการเปิดเผยบริการที่ไม่จำเป็นสู่ภายนอก โดยปิดพอร์ต โปรโตคอล และบริการที่ไม่ได้ใช้งาน พร้อมปรับการตั้งค่าความปลอดภัยของระบบ (Hardening)	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	Firewall rules พื้นฐานมีอยู่ แต่ยังไม่ได้ดำเนินการ Hardening อย่างเป็นระบบสำหรับทุกระบบ โดยเฉพาะ Legacy systems บางระบบอาจยังเปิดพอร์ตหรือบริการที่ไม่จำเป็น เช่น Telnet, FTP, หรือ Remote Desktop (RDP) ที่เปิดสู่ภายนอก	
หลักฐาน/เหตุผล	ระบบ legacy ที่ใช้มานานมักมีการสะสม services ที่เปิดทิ้งไว้ การ scan port จาก external perspective จะพบบริการที่ไม่ได้ตั้งใจเปิดได้บ่อยครั้งในองค์กรที่ไม่ได้ทำ regular hardening	
ข้อเสนอแนะ	ทำ Port Scan (ใช้ Nmap) จากภายนอกสำหรับ IP ทุกตัวที่ expose สู่ Internet ภายใน พ.ค. 69 ปิดพอร์ต/บริการที่ไม่จำเป็นทันที ทำ Hardening ตาม CIS Benchmark สำหรับ OS และ Web server ที่ใช้งาน (Linux, Windows Server, Apache, Nginx)	

2.3 ดำเนินการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อลดความสามารถในการเคลื่อนย้ายภายในเครือข่ายจากผู้โจมตี (Lateral Movement)	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	โครงสร้างเครือข่ายของ สกร. ยังเป็นแบบ Flat Network เป็นหลัก ไม่มีการแบ่งแยก network zone อย่างชัดเจนระหว่าง Production / Development / Administration / User network ทำให้หากถูกเจาะระบบหนึ่ง ผู้โจมตีสามารถ Lateral Move ไปยังระบบอื่นได้ง่าย	
หลักฐาน/เหตุผล	สกร. มีระบบสำคัญหลายระบบที่อยู่บนเครือข่ายเดียวกัน รวมถึง DOLE ZD ที่เก็บข้อมูลเด็ก 603,095 คน หากถูกเจาะจะเสี่ยงต่อการ Lateral Move ไปยังระบบ Credit Bank และระบบบริหารสำนักงานได้	
ข้อเสนอแนะ	วางแผน Network Segmentation ภายใน มิ.ย.-ส.ค. 69 แบ่ง Zone อย่างน้อย 4 ส่วน: (1) Internet-facing DMZ (DOLEdemy, DOLE ZD), (2) Internal Application Zone, (3) Database Zone, (4) Management Zone กำหนด Firewall rules ควบคุม traffic ระหว่าง Zone อย่างเข้มงวด	

2.4 ตรวจสอบซอฟต์แวร์ที่มีการพึ่งพาจากผู้ให้บริการภายนอก (3rd-party Software) และประเมินความเสี่ยงจากผู้ให้บริการอย่างสม่ำเสมอ	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	ยังไม่มีกระบวนการ formal ในการทบทวนและประเมิน 3rd-party software อย่างสม่ำเสมอ DOLEdemy ที่ใช้ Moodle เป็นฐาน และระบบต่าง ๆ ที่ใช้ Open Source components มีความเสี่ยงจาก Supply Chain Attack ซึ่งยังไม่มีการ track อย่างเป็นระบบ	
หลักฐาน/เหตุผล	DOLEdemy ใช้ Moodle ซึ่งมี plugin หลายตัวจาก 3rd party มีประวัติช่องโหว่สำคัญ เช่น CVE-2023-xxx series ระบบ Microservices ของ DOLE ZD ใช้ npm/pip packages จำนวนมากซึ่งแต่ละตัวอาจมีช่องโหว่	
ข้อเสนอแนะ	จัดทำ Software Bill of Materials (SBOM) สำหรับระบบหลักทุกระบบ ใช้ tool เช่น Snyk หรือ OWASP Dependency-Check เพื่อ scan vulnerabilities ใน dependencies อัตโนมัติ กำหนดนโยบาย: ต้องตรวจสอบ security ก่อน approve 3rd-party library ใหม่ทุกตัว	

มาตรการที่ 3 — เฝ้าระวังและตรวจจับ ระดับความสำคัญ : สำคัญสูง

3.1 จัดให้มีการเฝ้าระวังเส้นทางโจมตีที่สำคัญอย่างต่อเนื่อง ครอบคลุมระบบ เครือข่าย และบัญชีสิทธิ์สูง	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	ยังไม่มีระบบ Security Monitoring อัตโนมัติหรือ SOC (Security Operations Center) สำหรับ สกร. การตรวจจับเหตุการณ์ด้านความปลอดภัยยังเป็น Reactive (รอแจ้งปัญหา) ไม่ใช่ Proactive monitoring ด้วยทีม IT เพียง 5 คน การเฝ้าระวัง 24/7 ไม่สามารถทำได้ด้วยกำลังคนปัจจุบัน	
หลักฐาน/เหตุผล	กรอบอัตรากำลัง 19 ตำแหน่ง จริง 12 คน (IT 5 คน) ดูแล 11+ แพลตฟอร์ม ไม่มีตำแหน่ง dedicated Security Analyst หรือ SOC Analyst ในโครงสร้างปัจจุบัน หากเกิดเหตุการณ์โจมตีนอกเวลาราชการ อาจไม่มีผู้รับผิดชอบตอบสนองทันที	
ข้อเสนอแนะ	ระยะสั้น: กำหนดผู้รับผิดชอบ on-call rotation สำหรับเหตุการณ์ security และตั้ง alert พื้นฐานบน Nutanix Prism Central สำหรับ VM anomaly (CPU spike, network flood) ระยะกลาง: พิจารณาจ้าง Managed Security Service Provider (MSSP) หรือใช้บริการ SOC ของ ThaiCERT/ETDA สำหรับการ monitoring 24/7	

3.2 จัดเก็บและวิเคราะห์บันทึกเหตุการณ์ (Log) จากหลายแหล่ง เพื่อสนับสนุนการตรวจจับและตอบสนองเหตุการณ์ได้อย่าง ทันท่วงที	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	ระบบต่าง ๆ ของ สกร. มีการเก็บ Log อยู่แล้วในระดับ Application Log และ Server Log แต่ยังเป็น Silo ไม่มี Centralized Log Management หรือ SIEM system ที่รวบรวม Log จากหลายแหล่ง ทำให้ไม่สามารถ Correlate events ข้ามระบบได้ และ Log retention อาจไม่เพียงพอสำหรับการสืบสวนย้อนหลัง	
หลักฐาน/ เหตุผล	Nutanix HCI มี Prism Central ที่เก็บ infrastructure logs แต่ Application logs ของ DOLEdemy, DOLE ZD, DOLE OOSCY ที่รันบน VM แต่ละตัว ยังเก็บแยกกัน โดยไม่มี central aggregation และ VM เช่าเอกชน 15 ตัวก็ส่ง logs ออกมาแยกกันทั้งหมด	
ข้อเสนอแนะ	จัดตั้ง Centralized Log Management ภายใน มิ.ย.-ก.ค. 69 โดยติดตั้ง ELK Stack หรือ Graylog บน VM หนึ่งตัวของ Nutanix On-premise รวบรวม logs จาก: Nutanix Prism, VM ทั้ง 15 ตัว (เช่า), DOLEdemy, DOLE ZD, DOLE OOSCY กำหนด Log retention อย่างน้อย 90 วัน และตั้ง alert rules สำหรับพฤติกรรมผิดปกติ เช่น failed login > 5 ครั้ง/นาที	

มาตรการที่ 4 — เสริมการป้องกันของระบบ ระดับความสำคัญ : ระดับกลาง

4.1 ใช้แนวทางการป้องกันแบบหลายชั้น (Defence-in-Depth) เช่น Firewall/IPS, MFA, Network Segmentation และ Endpoint Detection and Response (EDR)	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง

สถานะปัจจุบัน	สกร. มี Firewall พื้นฐานและ Antivirus บน Endpoints แต่ยังขาดองค์ประกอบสำคัญของ Defence-in-Depth ได้แก่ IPS (Intrusion Prevention System), EDR ที่ครอบคลุมทุก endpoint, และ Network Segmentation ดังที่กล่าวไว้ในข้อ 2.3
หลักฐาน/เหตุผล	Nutanix HCI มี Nutanix Flow ที่ช่วยทำ micro-segmentation ระหว่าง VM ได้แต่ยังไม่ได้เปิดใช้งาน ไม่มี IPS ระดับ Application Layer หน้าระบบ internet-facing ไม่มี EDR solution สำหรับ endpoint ของบุคลากร กย. ที่ครอบคลุมเพียงพอ การป้องกันจึงยังเป็นแบบ Single-layer เป็นหลัก
ข้อเสนอแนะ	วางแผน Defence-in-Depth roadmap ภายใน มิ.ย.-ส.ค. 69 ลำดับความสำคัญ: (1) เปิดใช้ Nutanix Flow เพื่อทำ micro-segmentation ระหว่าง VM บน On-premise, (2) ติดตั้ง IPS/WAF หน้าระบบ internet-facing (DOLEdemy, DOLE ZD), (3) EDR บน workstations ของทีม IT และ Dev, (4) Network Segmentation ตามข้อ 2.3 จัดสรรงบประมาณ ~500,000 บาทสำหรับ EDR solution

4.2 บูรณาการมาตรการด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบและซอฟต์แวร์ ตามแนวทาง Secure Software Development Life Cycle (Secure SDLC)	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง กลาง

สถานะปัจจุบัน	ทีม Dev ของ สกร. ใช้ Agile/Scrum ในการพัฒนาระบบใหม่ มีการทำ Code Review บ้าง แต่ยังไม่มี formal Secure SDLC process ที่ครอบคลุม Security Requirements ตั้งแต่ต้น, Static Analysis (SAST), Dynamic Analysis (DAST), หรือ Security testing ใน CI/CD pipeline
หลักฐาน/เหตุผล	การพัฒนาระบบ DOLE ZD และ DOLE OOSCY ใช้ Microservices architecture ซึ่งมี attack surface กว้าง หากไม่มี Secure SDLC จะมีความเสี่ยงสูงจาก injection flaws, broken authentication และ insecure deserialization
ข้อเสนอแนะ	นำ Secure SDLC เข้าสู่กระบวนการพัฒนาใหม่ทุกโปรเจกต์ภายใน ก.ค.-ก.ย. 69 เริ่มจาก: (1) กำหนด Security Requirements ใน Sprint 0, (2) เพิ่ม SAST scan (เช่น SonarQube) ใน CI/CD pipeline, (3) ทำ OWASP Top 10 checklist ก่อน go-live ทุกครั้ง, (4) อบรม Developer ด้าน Secure Coding

4.3 พิจารณานำแนวคิด Zero Trust Architecture มาใช้ เพื่อเสริมการควบคุมการเข้าถึงและการตรวจสอบอย่างต่อเนื่อง	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง กลาง
สถานะปัจจุบัน	Zero Trust ยังอยู่ในขั้นศึกษาและรับรู้ ยังไม่มีการวางแผนหรือ implementation ใด ๆ สำหรับ สกร. ซึ่งเป็นเรื่องปกติสำหรับองค์กรภาครัฐที่ยังอยู่ในช่วงเปลี่ยนผ่าน	
หลักฐาน/เหตุผล	DGA กำลังผลักดัน Zero Trust สำหรับภาครัฐ แต่ยังไม่มี mandate สำหรับหน่วยงานระดับกรม การ implement Zero Trust ต้องการการเปลี่ยนแปลงโครงสร้างพื้นฐานและวัฒนธรรมองค์กรที่ใช้เวลาและทรัพยากรสูง	
ข้อเสนอแนะ	ดำเนินการเป็นระยะยาว (ก.ย.-ต.ค. 69 เริ่มศึกษา) โดย: (1) ศึกษา Zero Trust framework ของ NIST SP 800-207, (2) ประสานกับ DGA เพื่อขอ guidance สำหรับภาครัฐ, (3) กำหนด Zero Trust roadmap 3 ปี เริ่มจาก Identity-centric Zero Trust ก่อน	

มาตรการที่ 5 - บริหารจัดการช่องโหว่และการแก้ไข (Patch Management) ระดับความสำคัญ : ระดับกลาง

5.1 เพิ่มความถี่ในการตรวจสอบช่องโหว่และติดตามผลการแก้ไขอย่างใกล้ชิด โดยเฉพาะช่องโหว่ที่มีความเสี่ยงสูง	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	การตรวจสอบช่องโหว่ของ สกร. ยังเป็นแบบ ad-hoc ไม่มีตารางเวลา (Schedule) ที่แน่นอน ไม่มีระบบ automated vulnerability scanning ที่ดำเนินการอย่างสม่ำเสมอ การรับรู้ช่องโหว่มักมาจากประกาศ ThaiCERT หรือ vendor notification มากกว่าการค้นพบเชิงรุก	
หลักฐาน/เหตุผล	ทีม IT 5 คนไม่มีเวลาเพียงพอสำหรับ manual vulnerability scanning อย่างสม่ำเสมอ ยังไม่มี license หรือ deployment ของ Vulnerability Scanner เช่น Nessus, Qualys หรือ Tenable ในองค์กร	
ข้อเสนอแนะ	จัดซื้อ/ติดตั้ง Vulnerability Scanner (พิจารณา Tenable.io หรือ OpenVAS สำหรับ open source) ภายใน มิ.ย. 69 กำหนดตาราง scan อัตโนมัติรายสัปดาห์สำหรับ internet-facing systems และรายเดือนสำหรับระบบภายใน กำหนด SLA การแก้ไขตาม severity: Critical ≤ 7 วัน, High ≤ 30 วัน	

5.2 ปรับปรุงกระบวนการตรวจสอบและติดตั้ง Patch ให้ทันสมัย เพื่อลดช่วงเวลาที่ระบบอยู่ในภาวะเสี่ยง (Vulnerability Exposure Window)	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	มีการ patch ระบบบ้าง แต่ยังไม่มี formal Patch Management Policy ที่กำหนด: ความถี่การ patch, กระบวนการทดสอบก่อน deploy, rollback procedure, และ SLA การ patch ตาม severity ทำให้บางครั้ง patch ล่าช้าเกิน 90 วัน โดยเฉพาะ Legacy systems ที่กังวลเรื่อง compatibility	
หลักฐาน/เหตุผล	ระบบ Legacy บางส่วนไม่ได้รับการ patch เป็นเวลานานเนื่องจากกังวลว่าจะกระทบ production ไม่มี staging environment ที่สมบูรณ์สำหรับทดสอบ patch ก่อน deploy จริง	
ข้อเสนอแนะ	จัดทำ Patch Management Policy อย่างเป็นทางการภายใน พ.ค.-มิ.ย. 69 กำหนด: (1) Patch Tuesday ทุกวันอังคารที่ 2 ของเดือนสำหรับ routine patches, (2) Emergency patching ≤ 24 ชม. สำหรับ Critical CVE, (3) กระบวนการ patch testing บน staging ก่อน production เสมอ, (4) Rollback plan สำหรับทุก patch สำคัญ	

มาตรการที่ 6 — ตอบสนองและฟื้นฟู (Incident Response & Recovery) ความสำคัญ : ระดับกลาง

6.1 จัดทำและทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan: IRP) ให้รองรับสถานการณ์โจมตีที่ซับซ้อน รวมถึงกรณีที่ใช้ AI เป็นเครื่องมือโจมตี	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	ยังไม่มีเอกสาร Incident Response Plan อย่างเป็นทางการสำหรับ สกร. ที่ครอบคลุมทุกระบบ อาจมีแนวทางคร่าว ๆ แต่ไม่ได้รับการอนุมัติอย่างเป็นทางการ ไม่มี Playbook สำหรับสถานการณ์โจมตีที่ซับซ้อน เช่น Ransomware, Data Breach, หรือ AI-assisted attack	
หลักฐาน/เหตุผล	สกร. มีข้อมูลบุคคลสำคัญ ได้แก่ ข้อมูลเด็กนอกระบบ 603,095 คน ข้อมูลผู้เรียน ข้อมูลบุคลากร ซึ่งอยู่ภายใต้ PDPA หากเกิด Data Breach โดยไม่มี IRP จะไม่สามารถตอบสนองได้ทันภายใน 72 ชั่วโมงตามที่ PDPA กำหนด	
ข้อเสนอแนะ	จัดทำ IRP ครอบคลุม 5 ขั้นตอน (Preparation, Identification, Containment, Eradication, Recovery) ภายใน มิ.ย.-ก.ค. 69 เน้นสถานการณ์: (1) Ransomware attack บนระบบ DOLE ZD, (2) Data breach ข้อมูลผู้เรียน DOLEdemy, (3) PDPA breach notification process ใน 72 ชม. กำหนดผู้รับผิดชอบแต่ละขั้นตอนอย่างชัดเจน	

6.2 ซักซ้อมการตอบสนองเหตุการณ์ (Tabletop Exercise) และการฟื้นฟูระบบอย่างสม่ำเสมอ	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง สูง
สถานะปัจจุบัน	ยังไม่เคยจัดการซักซ้อมการตอบสนองเหตุการณ์ด้านไซเบอร์อย่างเป็นทางการ บุคลากรของ สกร. ยังไม่คุ้นเคยกับขั้นตอนการรับมือเหตุการณ์จริง ซึ่งจะทำให้เมื่อเกิดเหตุการณ์จริงเกิดความสับสนและล่าช้า	
หลักฐาน/เหตุผล	หน่วยงานที่ไม่เคย drill มักใช้เวลาตอบสนองนานกว่า 10 เท่าเมื่อเกิดเหตุจริง เทียบกับหน่วยงานที่ฝึกซ้อมสม่ำเสมอ สกร. มีข้อมูลสำคัญของเด็กนอกระบบซึ่งเป็น sensitive data ที่ต้องการการตอบสนองที่รวดเร็วและถูกต้อง	
ข้อเสนอแนะ	จัดซักซ้อม Tabletop Exercise ครั้งแรกภายใน ส.ค. 69 สถานการณ์: 'ระบบ DOLE ZD ถูก Ransomware' โดยเชิญ ThaiCERT เป็น facilitator กำหนดตาราง drill ปีละ 2 ครั้ง (ก.พ. และ ส.ค.) และบันทึก Lessons Learned เพื่อปรับปรุง IRP	

6.3 จัดให้มีการสำรองข้อมูลตามหลัก 3-2-1 Backup (3 copies, 2 media types, 1 offsite) พร้อมแยกเก็บข้อมูลสำรองออกจากระบบหลัก	⚠ ดำเนินการบางส่วน	ระดับความเสี่ยง สูงมาก
สถานะปัจจุบัน	สกร. มีการสำรองข้อมูลอยู่แล้ว 2 ลักษณะ คือ (1) VM-level backup ผ่าน Nutanix Data Protection (snapshot + replication) บน Nutanix HCI On-premise และ (2) ผู้รับจ้างที่พัฒนาแพลตฟอร์มแต่ละส่วนรับผิดชอบ backup app ระบบ แพลตฟอร์ม และฐานข้อมูลของตัวเองอยู่แล้ว ซึ่งถือว่ามี backup coverage ในระดับหนึ่ง แต่ยังขาดองค์ประกอบสำคัญของ 3-2-1 ได้แก่ offsite/air-gapped copy ที่แยกออกจากเครือข่ายหลักโดยสมบูรณ์ และยังไม่มีนโยบาย backup กลางที่กำกับทั้ง 2 tier ให้มีมาตรฐานเดียวกัน	
หลักฐาน/เหตุผล	Tier 1 — Nutanix Data Protection: snapshot และ replication ระดับ VM บน Nutanix cluster มีอยู่แล้ว แต่ snapshot ที่อยู่บน cluster เดียวกันยังไม่นับเป็น offsite ในบริบท Ransomware เพราะผู้โจมตีที่เข้าถึง Nutanix Prism อาจโจมตีทั้ง primary VM และ snapshot พร้อมกันได้ Tier 2 — Contractor backup: ผู้รับจ้างแต่ละรายจัดการ backup ของ app/platform/DB ตัวเองอยู่แล้ว แต่ยังไม่มีนโยบายกลางกำหนด retention period, ความถี่ backup, และมาตรฐาน restore testing ที่สม่ำเสมอ ช่องว่างหลัก: ยังไม่มี offsite/air-gapped copy ที่แยกออกจากเครือข่ายทั้งสอง tier และยังไม่มีการทดสอบ restore แบบ cross-tier เพื่อยืนยันว่าข้อมูลสามารถกู้คืนได้จริงในกรณีฉุกเฉิน	
ข้อเสนอแนะ	ดำเนินการทันที: (1) ตรวจสอบว่า backup ทุกระบบสำคัญเป็นไปตาม 3-2-1 จริงหรือไม่, (2) ทดสอบ restore จาก backup อย่างน้อยทุก 3 เดือน, (3) จัดให้มี air-gapped backup (ไม่เชื่อมต่อเครือข่าย) สำหรับข้อมูลสำคัญ เช่น DOLE ZD database, (4) ตั้ง budget ~120,000 บาทสำหรับ offsite storage solution	

มาตรการที่ 7 — กลยุทธ์เชิงรุกในยุค AI - ยุทธศาสตร์ระยะกลาง

7.1 ทบทวนสมมติฐานด้านภัยคุกคาม (Threat Model) โดยคำนึงถึงผู้โจมตีที่อาจใช้ AI เพิ่มขีดความสามารถในการโจมตีได้เร็วและซับซ้อนมากขึ้น	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง กลาง

สถานะปัจจุบัน	ยังไม่มีการทบทวน Threat Model ของ สกร. ให้ครอบคลุมภัยคุกคามที่ใช้ AI เป็นเครื่องมือ กรณี Mythos เป็นสัญญาณว่า Threat Landscape เปลี่ยนแปลงอย่างมีนัยสำคัญ การที่ AI สามารถค้นหาช่องโหว่ zero-day อัตโนมัติทำให้ระยะเวลาระหว่าง vulnerability disclosure กับ exploitation สั้นลงมาก
หลักฐาน/เหตุผล	สกร. เป็นหน่วยงานที่เก็บข้อมูลเด็กและเยาวชนกว่า 1 ล้านคน ซึ่งเป็น High Value Target สำหรับผู้ไม่หวังดี การที่ Mythos หรือ AI รุ่นถัดไปสามารถค้นหาช่องโหว่ใน Moodle (DOLEdemy) หรือ API ของ DOLE ZD ได้อัตโนมัติ ทำให้ความเสี่ยงเพิ่มขึ้นหลายเท่า
ข้อเสนอแนะ	จัดทำ AI-era Threat Model ภายใน ก.ค.-ส.ค. 69 อ้างอิง MITRE ATLAS (Adversarial Threat Landscape for AI Systems) และ NIST AI RMF ระบุ attack scenarios ที่ AI ช่วยผู้โจมตีได้ เช่น automated vulnerability discovery, AI-generated phishing, AI-assisted social engineering ปรับ security controls ตามภัยคุกคามใหม่นี้

7.2 พิจารณานำ AI มาช่วยสนับสนุนการตรวจจับภัยคุกคาม วิเคราะห์ช่องโหว่ และประเมินความเสี่ยง	✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง กลาง

สถานะปัจจุบัน	ยังไม่มีการนำ AI มาช่วยด้าน Security สำหรับ สกร. การใช้ AI เพื่อ Defense จะช่วยชดเชยข้อจำกัดด้านกำลังคน โดยเฉพาะในงาน log analysis, anomaly detection และ threat intelligence ที่ทีม 5 คนไม่สามารถทำได้ด้วยมือตลอด 24/7
หลักฐาน/เหตุผล	ทีม IT 5 คนดูแล 11+ ระบบบน Nutanix HCI On-premise และ VM เช่าเอกชน 15 VM ถ้าต้องวิเคราะห์ security logs ด้วยมือจะใช้เวลามากเกินไป AI-powered security tools เช่น Wazuh (open-source SIEM + XDR ที่ deploy On-premise ได้), หรือ Elastic Security บน ELK Stack ที่ติดตั้งบน Nutanix VM ตัวหนึ่งได้เลย
ข้อเสนอแนะ	ระยะสั้น (ก.ย. 69): Deploy Wazuh หรือ Elastic Security บน Nutanix VM เพื่อรวบรวม log และ detect anomaly จาก VM ทุกตัว (On-premise และเช่าเอกชน) โดยไม่ต้องพึ่ง External Cloud ระยะกลาง: พิจารณาใช้ AI-powered SIEM เพื่อ automate log analysis และ threat detection ลดภาระทีม IT กำหนดงบประมาณในแผนปี 2570

7.3 กำหนดแนวทางกำกับดูแลการใช้งาน AI (AI Governance Policy) อย่างเหมาะสม โดยยังคงมีผู้เชี่ยวชาญกำกับดูแลในจุดตัดสินใจที่สำคัญ		✗ ยังไม่ดำเนินการ	ระดับความเสี่ยง กลาง
สถานะปัจจุบัน	ยังไม่มี AI Governance Policy อย่างเป็นทางการสำหรับ สกร. บุคลากรของกรมเริ่มใช้ AI tools (ChatGPT, Claude, Copilot ฯลฯ) ในการทำงานมากขึ้น แต่ยังขาดนโยบายที่ชัดเจนว่าข้อมูลใดที่ห้ามป้อนเข้า AI ทั่วไป โดยเฉพาะข้อมูลเด็กนอกระบบที่อยู่ภายใต้ PDPA		
หลักฐาน/ เหตุผล	ข้อมูล DOLE ZD (ชื่อ ที่อยู่ สถานะของเด็ก) ถือเป็น sensitive personal data ภายใต้ PDPA หากบุคลากรนำข้อมูลเหล่านี้ไปใช้กับ AI tools ภายนอก (cloud-based) จะเป็นการละเมิด PDPA และ data residency requirements ของภาครัฐ		
ข้อเสนอแนะ	จัดทำ AI Use Policy สำหรับบุคลากร สกร. ภายใน ส.ค.-ต.ค. 69 ครอบคลุม: (1) ข้อมูลที่ห้ามป้อนเข้า AI tools ภายนอก (เด็กนอกระบบ ข้อมูลส่วนบุคคลผู้เรียน), (2) AI tools ที่อนุมัติให้ใช้งาน, (3) การใช้ AI ใน workflow อย่างถูกต้อง, (4) ผู้รับผิดชอบ review outputs ที่สำคัญ ประสาน สำนักงาน ก.พ.ร. เพื่อให้สอดคล้องกับ AI governance ระดับชาติ		

จึงเสนอมาเพื่อโปรดพิจารณา และเห็นชอบให้ดำเนินมาตรการตามผลการประเมินข้างต้น

ลงชื่อ .....

(ดร.วรพงษ์ น่วมอินทร์)

รักษาการผู้เชี่ยวชาญเฉพาะด้านเผยแพร่ทางการศึกษา

ปฏิบัติหน้าที่ผู้อำนวยการกลุ่มเทคโนโลยีดิจิทัลและสารสนเทศ

กรมส่งเสริมการเรียนรู้ กระทรวงศึกษาธิการ

วันที่ 30 / พ.ย. / 2569

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์

(ตามหนังสือ สกมช. TLP:CLEAR)

หน่วยงาน: ..... วันที่: ..... / ..... / ๒๕๖๙

แบบตอบรับการตรวจสอบแนวทางการรับมือกรณี AI ถูกใช้เป็นเครื่องมือโจมตีทางไซเบอร์			
ลำดับ	**หัวข้อและแนวทางปฏิบัติ**	**รายละเอียดดำเนินการ**	**ดำเนินการเรียบร้อย**
1. มาตรการเร่งด่วน			
1	**มาตรการเร่งด่วน**	ตรวจสอบและแก้ไขช่องโหว่ โดยเฉพาะระบบที่เปิดให้บริการจากภายนอก เพื่อลดความเสี่ยงจากการถูกค้นหาและโจมตีโดยอัตโนมัติ	☐
		บังคับใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) สำหรับบัญชีผู้ดูแลระบบ ระบบบริหารจัดการ อุปกรณ์สำคัญ และบริการคลาวด์ที่เกี่ยวข้อง ในกรณีที่ไม่รองรับ MFA ให้จำกัดการเข้าถึงด้วยการกำหนดแหล่งที่มา IP ที่ได้รับอนุญาต	☐
		ตรวจสอบและจำกัดการเข้าถึงระบบพัฒนา ระบบทดสอบ และระบบ staging ที่สามารถเข้าถึงได้จากอินเทอร์เน็ต รวมถึงส่วนบริหารจัดการของระบบดังกล่าว โดยกำหนดมาตรการควบคุมการเข้าถึงอย่างเข้มงวด หรือแยกออกจากเครือข่ายภายนอกหากไม่จำเป็น	☐
		ทบทวนการตั้งค่าด้านความมั่นคงปลอดภัยของระบบคลาวด์ โดยเฉพาะทรัพยากรที่เปิดเผยสู่สาธารณะ การตั้งค่าสิทธิ์ที่เกินความจำเป็น และส่วนบริหารจัดการที่อาจเข้าถึงได้จากภายนอก	☐
2. มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี			
2	**มาตรการลด Attack Surface และจำกัดเส้นทางการโจมตี**	จัดทำและปรับปรุงบัญชีทรัพย์สินสารสนเทศ (Asset Inventory) ให้ครบถ้วนและเป็นปัจจุบัน เพื่อให้สามารถมองเห็นจุดเสี่ยงภายในองค์กรได้อย่างต่อเนื่อง	☐
		ลดการเปิดเผยบริการที่ไม่จำเป็นสู่ภายนอก โดยปิดพอร์ต โปรโตคอล และบริการที่ไม่ได้ใช้งาน พร้อมปรับการตั้งค่าความปลอดภัยของระบบ (Hardening)	☐
		ดำเนินการแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อลดความสามารถในการเคลื่อนย้ายภายในเครือข่ายจากผู้โจมตี (Lateral Movement)	☐
		ตรวจสอบซอฟต์แวร์ที่มีการพึ่งพาจากผู้ให้บริการภายนอก และประเมินความเสี่ยงจากผู้ให้บริการอย่างสม่ำเสมอ	☐

3. มาตรการเฝ้าระวังและตรวจจับ			
3	**มาตรการเฝ้าระวังและตรวจจับ**	จัดให้มีการเฝ้าระวังเส้นทางโจมตีที่สำคัญอย่างต่อเนื่อง ครอบคลุมระบบ เครือข่าย และบัญชีสิทธิ์สูง	☐
		จัดเก็บและวิเคราะห์บันทึกเหตุการณ์ (Log) จากหลายแหล่ง เพื่อสนับสนุนการตรวจจับและตอบสนองเหตุการณ์ได้อย่างทันท่วงที	☐
4. มาตรการเสริมการป้องกันของระบบ			
4	**มาตรการเสริมการป้องกันของระบบ**	ใช้แนวทางการป้องกันแบบหลายชั้น (Defence-in-Depth) เช่น Firewall/IPS, MFA, Network Segmentation และ Endpoint Detection and Response (EDR)	☐
		บูรณาการมาตรการด้านความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบและซอฟต์แวร์ ตามแนวทาง Secure Software Development Life Cycle (Secure SDLC)	☐
		พิจารณานำแนวคิด Zero Trust Architecture มาใช้ เพื่อเสริมการควบคุมการเข้าถึงและการตรวจสอบอย่างต่อเนื่อง	☐
5. มาตรการบริหารจัดการช่องโหว่และการแก้ไข			
5	**มาตรการบริหารจัดการช่องโหว่และการแก้ไข**	เพิ่มความถี่ในการตรวจสอบช่องโหว่และติดตามผลการแก้ไขอย่างใกล้ชิด โดยเฉพาะช่องโหว่ที่มีความเสี่ยงสูง	☐
		ปรับปรุงกระบวนการตรวจสอบและติดตั้ง Patch ให้ทันสมัย เพื่อลดช่วงเวลาที่ระบบอยู่ในภาวะเสี่ยง	☐
6. มาตรการตอบสนองและฟื้นฟู			
6	**มาตรการตอบสนองและฟื้นฟู**	จัดทำและทบทวนแผนตอบสนองเหตุการณ์ (Incident Response Plan) ให้รองรับสถานการณ์โจมตีที่ซับซ้อน	☐
		ซักซ้อมการตอบสนองเหตุการณ์และการฟื้นฟูระบบอย่างสม่ำเสมอ	☐
		จัดให้มีการสำรองข้อมูลตามหลัก 3-2-1 Backup และแยกเก็บข้อมูลสำรองออกจากระบบหลัก	☐
7. มาตรการเชิงกลยุทธ์ในยุค AI			
7	**มาตรการเชิงกลยุทธ์ในยุค AI**	ทบทวนสมมติฐานด้านภัยคุกคาม โดยคำนึงถึงผู้โจมตีที่อาจใช้ AI เพิ่มขีดความสามารถในการโจมตี	☐
		พิจารณานำ AI มาช่วยสนับสนุนการตรวจจับภัยคุกคาม วิเคราะห์ช่องโหว่ และประเมินความเสี่ยง	☐
		กำหนดแนวทางกำกับดูแลการใช้งาน AI อย่างเหมาะสม โดยยังคงมีผู้เชี่ยวชาญกำกับดูแลในจุดตัดสินใจที่สำคัญ	☐

หมายเหตุ / ข้อจำกัด: .....

.....

.....

.....

.....

.....

ลงชื่อ.....

(.....)

ตำแหน่ง.....

วันที่ ..... / ..... / 2569

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)