แนวทางปฏิบัติงานมาตรฐาน

Standard Operating Procedure

การสแกนช่องโหว่และการติดตามแก้ไขช่องโหว่

ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเชียงใหม่

แนวทางปฏิบัติงานมาตรฐาน
Standard Operating Procedure
การสแกนช่องโหว่และการติดตามแก้ไขช่องโหว่

1. วัตถุประสงค์

เพื่อจัดการทรัพย์สินสารสนเทศ ตรวจสอบและระบุช่องโหว่ด้านความมั่นคงปลอดภัยในระบบสารสนเทศ แล้วดำเนินการแก้ไขช่องโหว่อย่างเป็นระบบ เพื่อลดความเสี่ยงจากการถูกโจมตีด้านไซเบอร์จากทั้งภายในและภายนอกระบบเครือข่ายของมหาวิทยาลัย

2. ขอบเขตการดำเนินงาน

ครอบคลุมระบบเครื่องแม่ข่าย, แอปพลิเคชัน, ฐานข้อมูล, อุปกรณ์เครือข่าย และระบบ Private Cloud ที่อยู่ภายใต้การดูแลของส่วนงานภายในมหาวิทยาลัย

3. ผู้รับผิดชอบและหน้าที่

ฝ่ายความมั่นคงปลอดภัยไซเบอร์ มีหน้าที่ อำนวยความสะดวกในการจัดการทรัพย์สินสารสนเทศ ดำเนินการสแกนช่องโหว่ วิเคราะห์ผล ให้คำแนะนำในการแก้ไข และติดตามผลการแก้ไขช่องโหว่

เจ้าหน้าที่ระบบไอทีส่วนงาน มีหน้าที่ ให้ข้อมูลทรัพย์สินสารสนเทศ รับทราบรายงานผลการสแกนช่องโหว่ ดำเนินการวางแผนและแก้ไขช่องโหว่ที่สำคัญสูงตามคำแนะนำ

ผู้บริหารไอทีส่วนงาน มีหน้าที่ รับทราบรายการทรัพย์สินสารสนเทศและผลการสแกนช่องโหว่ ตรวจสอบและอนุมัติการดำเนินการการแก้ไขช่องโหว่

4. เครื่องมือที่ใช้ วิธีการสแกนช่องโหว่ และคำนิยามของความรุนแรงของช่องโหว่

เครื่องมือที่ใช้

เครื่องมือที่เกี่ยวข้อง ได้แก่ ซอฟต์แวร์ Nessus Professional ระบบรายงานและติดตามการแก้ไขช่องโหว่ VTS (Vulnerability Tracking System) ระบบการสื่อสารผ่านระบบอีเมลและ Microsoft Team

วิธีการสแกนช่องโหว่

วิธีการสแกนช่องโหว่แบบการสแกนประจำปี (Annual Vulnerability Assessment)

ดำเนินการอย่างน้อยปีละ 1 ครั้ง ครอบคลุมระบบสารสนเทศที่สำคัญสูงทั้งหมดของส่วนงาน

โดยใช้เครื่องมือสแกนแบบเชิงลึก (Deep Scan) ด้วยการใช้ซอฟต์แวร์ Nessus Professional มีรูปแบบการสแกน 3 แบบคือ

4.1 Basic Scan เป็นการตรวจสอบช่องโหว่พื้นฐานเบื้องต้นในมุมมองจากภายนอกเครือข่ายของส่วนงาน เป็นการตรวจสอบช่องโหว่ในภาพรวมกว้างๆ ของระบบสารสนเทศ เหมาะสำหรับส่วนงานที่มีเว็บไซต์ในลักษณะ static ทั่วไป หรือระบบทั่วไปที่มีความสำคัญปานกลาง เช่น เว็บไซต์ข้อมูลข่าวสารซึ่งไม่จำเป็นต้องมีการตั้งค่าใดๆ ในระบบของส่วนงานเพิ่มเติม

4.2 Open Firewall เป็นการตรวจสอบช่องโหว่ในมุมมองที่เสมือนเชื่อมต่อภายในระบบเครือข่ายของส่วนงานเอง เหมาะกับส่วนงานที่มีระบบ firewall ป้องกันระบบเครือข่ายของส่วนงาน รวมถึงมีระบบที่ใช้กันภายในหน่วยงานที่มีความสำคัญสูงขึ้น เช่น ระบบเครื่องแม่ข่ายที่มีข้อมูลที่สำคัญที่ใช้ในการบริหารจัดการระบบงานภายในส่วนงาน จำเป็นต้องมีการตั้งค่าเพิ่มเติมบนระบบ firewall เพื่ออนุญาตให้เครื่องที่ใช้ตรวจสอบช่องโหว่สามารถผ่านเข้าไปในระบบเครือข่ายของส่วนงานได้

4.3 Credential Scan เป็นการตรวจสอบช่องโหว่ในมุมมองที่เสมือนเชื่อมต่อจากภายในระบบเครื่องแม่ข่าย (Server) เหมาะกับส่วนงานที่มีระบบ firewall ป้องกันระบบเครือข่ายของส่วนงาน รวมถึงมีระบบที่ใช้กันภายในหน่วยงาน ที่มีความสำคัญสูงมากในระดับวิกฤติ เช่น ระบบเครื่องแม่ข่ายที่มีข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคลที่สำคัญมากหรือข้อมูลสำคัญที่ใช้ในการบริหารจัดการระบบงานภายในส่วนงาน จำเป็นต้องมีการตั้งค่าเพิ่มเติมบนระบบเครื่องแม่ข่ายเพื่ออนุญาตให้เครื่องที่ใช้ตรวจสอบช่องโหว่สามารถผ่านเข้าไปในตรวจสอบภายในระบบเครื่องแม่ข่ายอย่างละเอียดได้

คำนิยามของความรุนแรงของช่องโหว่

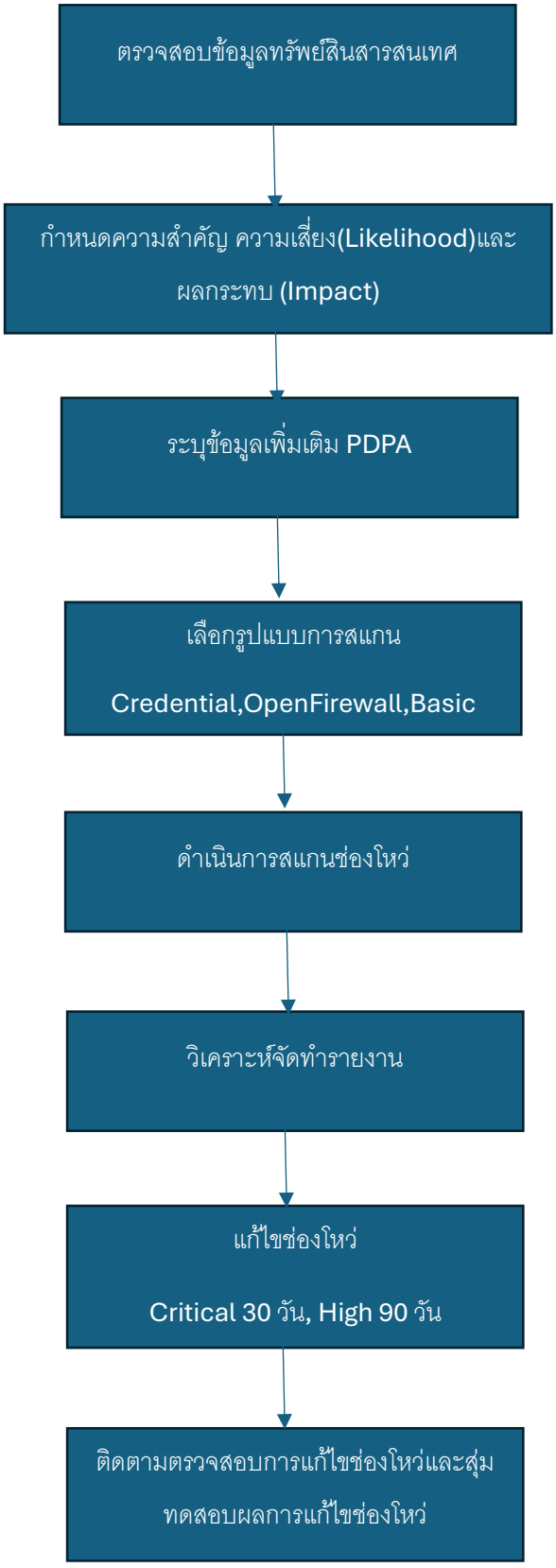
ตามนิยามของ Tenable/Nessus ซึ่งใช้ระบบ CVSS (Common Vulnerability Scoring System) เป็นพื้นฐานในการจัดระดับความรุนแรงของช่องโหว่ ช่องโหว่จะถูกจัดระดับเป็น Critical, High, Medium, Low ตามคะแนน CVSS ดังนี้

ระดับ	คะแนน CVSS	ความหมาย
Critical	9.0 – 10.0	ช่องโหว่ที่มีความรุนแรงสูงสุด มีโอกาสถูกโจมตีได้ง่ายและส่งผลกระทบรุนแรงสูงมากต่อระบบ เช่น การเข้าถึงระบบโดยไม่ต้องยืนยันตัวตน หรือสามารถรันโค้ดจากระยะไกลได้
High	7.0 – 8.9	ช่องโหว่ที่มีความรุนแรงสูง อาจต้องมีการยืนยันตัวตนหรือการโต้ตอบจากผู้ใช้ แต่ยังสามารถถูกโจมตีได้ง่ายและส่งผลกระทบต่อความมั่นคงของระบบ
Medium	4.0 – 6.9	ช่องโหว่ที่มีความรุนแรงปานกลาง อาจต้องมีเงื่อนไขเฉพาะในการโจมตี เช่น การตั้งค่าผิดพลาด หรือการเข้าถึงเฉพาะบางส่วนของระบบ
Low	0.1 – 3.9	ช่องโหว่ที่มีความรุนแรงต่ำ โอกาสในการถูกโจมตีต่ำ หรือผลกระทบต่อระบบไม่รุนแรง

หมายเหตุ: ช่องโหว่ที่มีคะแนน 0.0 จะถูกจัดเป็น Informational (Info) ซึ่งไม่ถือว่าเป็นช่องโหว่ที่ต้องแก้ไขเร่งด่วน

5. ขั้นตอนการดำเนินงาน

แผนภาพด้านล่างแสดงภาพรวมของขั้นตอนการดำเนินงานในการสแกนและติดตามการแก้ไขช่องโหว่ ตั้งแต่การกรอกข้อมูลทรัพย์สินสารสนเทศไปจนถึงการติดตามและสุ่มทดสอบช่องโหว่ของระบบ


ตรวจสอบข้อมูลทรัพย์สินสารสนเทศ
กำหนดความสำคัญ ความเสี่ยง(Likelihood)และ ผลกระทบ (Impact)
ระบุข้อมูลเพิ่มเติม PDPA
เลือกรูปแบบการสแกน Credential,OpenFirewall,Basic
ดำเนินการสแกนช่องโหว่
วิเคราะห์จัดทำรายงาน
แก้ไขช่องโหว่ Critical 30 วัน, High 90 วัน
ติดตามตรวจสอบการแก้ไขช่องโหว่และสุ่ม ทดสอบผลการแก้ไขช่องโหว่

5.1 การกรอกข้อมูลสินทรัพย์เทคโนโลยีสารสนเทศ

5.1.1 สำนักฯ ส่งบันทึกข้อความพร้อมรายการทรัพย์สินสารสนเทศที่สำคัญสูงของส่วนงานล่าสุดให้ผู้บริหารส่วนงานรับทราบ

5.1.2 เจ้าหน้าที่ไอทีส่วนงานเข้าระบบ VTS (Vulnerability Tracking System) ภายใต้เมนู จัดการทรัพย์สินสารสนเทศ เพื่อตรวจสอบรายการทรัพย์สินสารสนเทศและทำรายการทรัพย์สินสารสนเทศให้เป็นปัจจุบัน โดยปรับค่า ลำดับความสำคัญ โอกาสการถูกโจมตี(Likelihood) และ ผลกระทบ(Impact) ของทรัพย์สินให้เหมาะสมกับทรัพย์สินสารสนเทศแต่ละรายการ ตามคู่มือการใช้งานระบบ VTS หน้าที่ 10

5.1.3 เจ้าหน้าที่ไอทีส่วนงานกรอกข้อมูลระบุว่ารายการทรัพย์สินสารสนเทศใดมีข้อมูลส่วนบุคคลหรือไม่และเลือกรูปแบบของการสแกนช่องโหว่ทั้ง 3 รูปแบบ คือ Credential Scan , Open Firewall Scan และ Basic Scan ตามความเหมาะสม โดยหากทรัพย์สินสารสนเทศรายการใดมีข้อมูลส่วนบุคคล และ/หรือ มีค่าความเสี่ยงเกิน 15 จะถูกเลือกการสแกนช่องโหว่แบบ Credential Scan โดยอัตโนมัติ (ตามมติ กบม) ซึ่งบางระบบอาจมีข้อจำกัดในการดำเนินการสแกนช่องโหว่แบบ Credential Scan ให้สามารถเลือกรูปแบบการสแกนแบบ Open Firewall หรือ Basic Scan ทดแทนได้ และสุดท้ายให้ทำการยืนยันรายการทรัพย์สินสารสนเทศ ตามคู่มือการใช้งานระบบ VTS หน้าที่ 13

5.2 การสแกนช่องโหว่

หลังจากเจ้าหน้าที่ไอทีส่วนงานได้ทำการยืนยันรายการทรัพย์สินสารสนเทศของส่วนงานแล้ว เจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยไซเบอร์จะทำการจัดลำดับการดำเนินการสแกนช่องโหว่ของแต่ละส่วนงาน และจะมีการประสานงานเพื่อนัดหมายและติดต่อขอความร่วมมือจากเจ้าหน้าที่ไอทีส่วนงานเป็นรายส่วนงาน เพื่อขอข้อมูลเพิ่มเติมในกรณีที่ต้องมีการสแกนช่องโหว่แบบ Open Firewall และ Credential Scan โดยเจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยไซเบอร์จะเริ่มดำเนินการสแกนช่องโหว่ตามลำดับตามส่วนงานที่ได้วางแผนและประสานแจ้งไปแล้ว

5.3 การวิเคราะห์และจัดทำรายงาน

หลังจากที่เจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยไซเบอร์ดำเนินการสแกนช่องโหว่ของทรัพย์สินสารสนเทศของส่วนงานตามรายการที่เจ้าหน้าที่ไอทีส่วนงานยืนยันมาจนครบแล้วจะมีการวิเคราะห์ผลการสแกนเพื่อจัดลำดับความสำคัญ (Critical, High, Medium, Low) และจะมีการจัดทำบันทึกข้อความรายงาน

ช่องโหว่พร้อมคำแนะนำในการแก้ไขช่องโหว่ ส่งรายงานให้ผู้บริหารส่วนงาน และรายงานช่องโหว่ในภาพรวมของมหาวิทยาลัยรายงานในที่ประชุมกรรมการบริหารมหาวิทยาลัย โดยเจ้าหน้าที่ไอทีส่วนงานสามารถดูผลรายงานช่องโหว่ และคำแนะนำในการแก้ไขผ่านระบบ VTS ตามคู่มือการใช้งานระบบ VTS หน้าที่ 7

5.4 การแก้ไขช่องโหว่

ช่องโหว่ที่ตรวจพบของแต่ละส่วนงานในระดับ Critical ให้ส่วนงานดำเนินการแก้ไขช่องโหว่ให้แล้วเสร็จภายใน 30 วัน เนื่องจากเป็นช่องโหว่ที่มีความเสี่ยงสูงมากอาจถูกโจมตีได้อย่างรวดเร็วหากไม่ทำการแก้ไขอย่างเร่งด่วน ส่วนช่องโหว่ในระดับ High ควรได้รับการแก้ไขให้แล้วเสร็จภายใน 90 วัน นับจากวันที่รายงานผลโดยสำนักฯ ทั้งนี้ส่วนงานควรมีการจัดลำดับความสำคัญของช่องโหว่ และมีแผนการแก้ไขโดยผู้ดูแลระบบไอทีส่วนงานโดยผู้ดูแลระบบไอทีส่วนงานให้ดำเนินการแก้ไขตามแผนที่วางไว้ และควรได้รับการรับทราบและอนุมัติแผนการแก้ไขช่องโหว่โดยผู้บริหารไอทีส่วนงาน พร้อมทั้งบันทึกผลการแก้ไขช่องโหว่เป็นรายช่องโหว่ในระบบติดตามการแก้ไขช่องโหว่ VTS ตามคู่มือการใช้งานระบบ VTS หน้าที่ 9

5.5 การติดตามและตรวจสอบ

เจ้าหน้าที่ฝ่ายความมั่นคงปลอดภัยไซเบอร์จะดำเนินการประสานเจ้าหน้าที่ไอทีส่วนงานตรวจสอบความคืบหน้าเป็นรายสัปดาห์หลังจากที่ได้มีการรายงานผลการสแกนช่องโหว่ของแต่ละส่วนงาน ซึ่งหากเกินระยะเวลาแก้ไขช่องโหว่โดยเฉพาะช่องโหว่ในระดับ Critical ตามที่กำหนด 30 วัน นับจากวันรายงานผล หากส่วนงานไม่แก้ภายในเวลาที่กำหนด สำนักฯ จะดำเนินการรายงานผู้บริหารส่วนงานให้รับทราบถึงการแก้ไขที่ล่าช้าซึ่งอาจทำให้ระบบของท่านมีความเสี่ยงสูงมากในการถูกโจมตี ทั้งนี้หากดำเนินการแก้ไขแล้วสำนักฯ อาจต้องมีการสุ่มทดสอบระบบหลังการแก้ไข เพื่อยืนยันว่าไม่มีช่องโหว่ในระดับ Critical เดิมหลงเหลืออยู่ และเมื่อเจ้าหน้าที่ไอทีส่วนงานได้ดำเนินการแก้ไขช่องโหว่แล้วให้เจ้าหน้าที่ไอทีส่วนงานทำการบันทึกผลการแก้ไขช่องโหว่ในระบบติดตามการแก้ไขช่องโหว่ VTS ตามคู่มือการใช้งานระบบ VTS หน้าที่ 9

ภาคผนวก

แผนผังบทบาท

ขั้นตอน	เจ้าหน้าที่ IT ส่วนงาน	ฝ่ายความมั่นคงไซเบอร์	ผู้บริหารส่วนงาน
กรอกข้อมูล	รับผิดชอบ (R)	สนับสนุน (S)	รับทราบ (I)
สแกนช่องโหว่และวิเคราะห์ผล	สนับสนุน (S)	รับผิดชอบ (R)	รับทราบ (I)
วางแผนแก้ไขช่องโหว่	รับผิดชอบ (R)	สนับสนุน (S)	รับทราบ (I)
อนุมัติแผนแก้ไขช่องโหว่	-	-	รับผิดชอบ (R)

ตัวชี้วัด

SLA สำหรับการตอบสนองและแก้ไขช่องโหว่

ช่องโหว่ในระดับ Critical: แก้ไขภายใน 30 วัน

ช่องโหว่ในระดับ High: แก้ไขภายใน 90 วัน

KPI

อัตราการแก้ไขช่องโหว่ Critical ภายใน SLA ≥ 80%

จำนวนช่องโหว่ที่ตรวจพบซ้ำในรอบถัดไป ≤ 10%