

กระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์ กรณีเว็บไซต์พนัน
Incident Response Process in case gambling web

นายโอภาส หมีนแสน

สำนักบริการเทคโนโลยีสารสนเทศ

opas.m@cmu.ac.th

1. แนวปฏิบัติที่ดีในด้าน

กระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์

2. บทนำ/ที่มาและความสำคัญ

ในโลกไอทียุคปัจจุบันที่เทคโนโลยีสารสนเทศได้มีบทบาทและความสำคัญอย่างยิ่งต่อสังคมปกติในปัจจุบัน ภัยคุกคามทางไซเบอร์ในทุกแง่มุมที่หลากหลายและรุนแรงไม่ว่าจะเป็นภัยพื้นฐานที่สุดจากไวรัสหรือมัลแวร์ การขโมยข้อมูลอันมีค่า หรือถ้าเป็นมุมมองต่อองค์กรก็มีภัยจากการโจมตีทำลายระบบ การทำให้ระบบไม่สามารถใช้งานได้อย่างปกติ หรือภัยร้ายขั้นสูงสุดการจู่โจมเจาะช่องโหว่ทางเทคนิคเพื่อผลประโยชน์ใดๆ ก็ตาม ความเสียหายด้านไซเบอร์ทั้งหมดเหล่านี้จะสามารถแก้ไขได้โดยกระบวนการที่เรียกว่าแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan) สำหรับองค์กรยุคใหม่ในปัจจุบันถือว่าเป็นหนึ่งในกระบวนการที่สำคัญอย่างยิ่งที่องค์กรจะต้องมีและขาดไม่ได้เพื่อการตอบสนอง แก้ไขและป้องกันเหตุการณ์ที่อาจเกิดขึ้นซ้ำได้อีกในอนาคตได้อย่างมีประสิทธิภาพ

ในการศึกษาวิจัยนี้จะยกตัวอย่างกรณีศึกษาด้านการรับมือภัยคุกคามทางไซเบอร์แบบหนึ่งในลักษณะที่เรียกว่าเป็นการโจมตีแบบแก้ไขเปลี่ยนแปลงเว็บไซต์หรือ Web Defacement เป็นการโจมตีทางไซเบอร์ในรูปแบบหนึ่งที่ผู้ไม่ประสงค์ดีทำการโจมตีไปยังเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ของหน่วยงานเพื่อทำการแก้ไขเปลี่ยนแปลงเนื้อหาของเว็บไซต์ในรูปแบบต่างๆ ทั้งการแก้ไขข้อความ หรือ รูปภาพ ทั้งนี้อาจเพื่อทำลายชื่อเสียงขององค์กรหรือผลประโยชน์อื่นๆ ในกรณีศึกษานี้จะจำเพาะเจาะจงการรับมือภัยคุกคามในลักษณะของการแก้ไขเปลี่ยนแปลงเว็บไซต์โดยเป็นการแอบแฝงการโฆษณาเว็บพนันผ่านเว็บไซต์ของส่วนงาน เพื่อความน่าจะเป็นในการให้ผลการค้นหาข้อมูลจากการใช้เว็บค้นหาข้อมูลอาทิเช่น google.com ขึ้นแสดงผลเว็บพนันในอัตราที่เพิ่มขึ้นเพื่อการโฆษณา จึงใจให้คนเข้าไปยังเว็บไซต์ดังกล่าวผ่านเว็บไซต์ขององค์กรด้วยสาเหตุที่ว่าเว็บไซต์ขององค์กรที่ตกเป็นเหยื่อนั้นมักจะมีค่าคะแนนเว็บไซต์ที่ค่อนข้างดีจึงทำให้ผลการค้นหาปรากฏเว็บพนันในอันดับต้นๆ ได้ง่ายขึ้นทำให้เว็บพนันมีโอกาสมากขึ้นทำให้คนที่ใช้เว็บค้นหาข้อมูลพบเจอเว็บพนันได้บ่อยขึ้น ซึ่งปัญหานี้ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมากและเป็นรูปแบบภัยคุกคามที่พบมากที่สุด ตามสถิติที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ได้แจ้งเป็นประจำ

3. วัตถุประสงค์

1. เพื่อให้มีกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์ กรณีเว็บไซต์พนัน อันเป็นการลดความเสียหายในด้านชื่อเสียงและความเสี่ยงต่อการกระทำผิดตามกฎหมาย พรบ.ความมั่นคงปลอดภัยไซเบอร์ 2562

2. เพื่อหามาตรการแก้ไขระบบเว็บไซต์ของส่วนงานภายในมหาวิทยาลัยที่ถูกโจมตีและฟื้นฟูให้กลับมาทำงานเป็นปกติ
3. เพื่อป้องกันปัญหาของเว็บไซต์ส่วนงานที่ถูกโจมตีไม่ให้เกิดเหตุการณ์โจมตีในลักษณะดังกล่าวซ้ำอีกในอนาคต

4. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง (ถ้ามี)

ภัยคุกคามด้านไซเบอร์

การใช้ระบบเทคโนโลยีสารสนเทศหรือระบบไอทีในด้านลบที่ก่อให้เกิดผลเสียต่อข้อมูลหรือระบบที่อยู่ในองค์ประกอบของระบบเทคโนโลยีสารสนเทศใดๆ โดยคำว่า “ไซเบอร์” นั้นหมายถึง การเชื่อมโยงสื่อสารข้อมูลในลักษณะต่างๆ บนระบบเครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือเครือข่ายโทรคมนาคมอื่นใด ซึ่งปัจจุบันภัยคุกคามทางไซเบอร์ในทุกรูปแบบนั้นก่อให้เกิดผลกระทบต่อสังคม เศรษฐกิจ และความมั่นคงของประเทศ ซึ่งการโจมตีหรือภัยคุกคามทางไซเบอร์โดยทั่วไปมีหลายรูปแบบ อาทิเช่น การเจาะระบบ (Hacking) การดักจับข้อมูล (Sniffing) การโจมตีด้วยซอฟต์แวร์ไม่พึงประสงค์ (Malware) การร่วมโจมตีทำให้ระบบไม่สามารถใช้งานได้ (Distributed Denial of Service Attack : DoS) หรือการเจาะช่องโหว่ของระบบเพื่อเข้าสู่ระบบเพื่อไปแก้ไขเปลี่ยนแปลงข้อมูลบางอย่างในระบบ (Vulnerabilities) เป็นต้น (ชรินทร์ทิพย์ ปันสุวรรณ, 2565, น. 41)

การบริหารจัดการความมั่นคงปลอดภัยไซเบอร์

ด้วยโลกปัจจุบันอยู่ในยุคเศรษฐกิจดิจิทัล ดังนั้นเรื่องภัยคุกคามและความมั่นคงปลอดภัยไซเบอร์ รวมถึงการให้ความสำคัญเรื่องข้อมูลอันมีค่าที่อยู่ในระบบนั้นทุกองค์กรต้องให้ความสำคัญเป็นอันดับต้นๆ ของภารกิจที่สำคัญขององค์กร ด้วยการดำเนินการบริหารจัดการความเสี่ยงตั้งแต่ความเสี่ยงระดับองค์กร (Enterprise Risk Management) ที่ผู้บริหารองค์กรต้องคำนึงถึงเป็นอย่างยิ่ง โดยความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศนั้นมันไม่ใช่แค่ความเสี่ยงด้านประเด็นแค่เรื่องของอุปกรณ์หรือเทคโนโลยีแต่เพียงอย่างเดียวเท่านั้น แต่มันมีความเสี่ยงในด้านอื่นๆ ที่จะต้องให้ความสำคัญด้วยได้แก่ ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ความเสี่ยงด้านกระบวนการ (Process) ความเสี่ยงด้านการเงิน (Financial Risk) ความเสี่ยงด้านการให้บริการ (Services Risk) ความเสี่ยงด้านบุคลากร (Employee Risk) ความเสี่ยงด้านกฎหมาย (Law Risk) ความเสี่ยงด้านชื่อเสียงองค์กร (Reputational Risk) และยังมีความเสี่ยงด้านอื่นๆ อีกมากมายขึ้นอยู่กับลักษณะและการให้ความสำคัญของแต่ละองค์กร (อนาวิต แก้วสอาด และณัฐวี อุตกฤษฎี, 2564, น.12)

ด้วยการใช้กรอบมาตรฐาน NIST ซึ่งสร้างขึ้นโดยหน่วยงาน National Institute of Standards and Technology ซึ่งเป็นหน่วยงานหนึ่งของรัฐบาลสหรัฐอเมริกา สังกัดกระทรวงพาณิชย์สหรัฐอเมริกา (U.S. Department of Commerce) หน้าที่หลักในการพัฒนาและส่งเสริมมาตรฐานต่างๆ รวมถึงมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ที่เรียกว่า NIST Cybersecurity Framework (CSF) ซึ่งหลายองค์กรและแม้กระทั่ง พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ก็นำมาประยุกต์ใช้ในการวางแผนและจัดการความมั่นคงปลอดภัยไซเบอร์ด้วยเช่นเดียวกัน

ภายใต้กรอบมาตรฐาน NIST CSF นั้นนำมาใช้เพื่อวางแผนด้านความมั่นคงปลอดภัยไซเบอร์ โดยแต่ละองค์กรจะต้องนำไปปรับประยุกต์ใช้ให้เหมาะสมกับแต่ละองค์กร เพื่อให้เกิดภาวะที่เรียกว่า Cyber Resilience ซึ่งหมายถึง ความสามารถในการเตรียมตัวพร้อมต่อการเปลี่ยนแปลงต่างๆ มีขีดความสามารถในการทนต่อการบุกรุกโจมตีในทุกรูปแบบ รวมถึงภัยธรรมชาติ และภัยที่อาจเกิดขึ้นโดยตั้งใจและอาจไม่ตั้งใจได้ โดยกรอบมาตรฐานดังกล่าวประกอบไปด้วย 5 กระบวนการหลักด้วยกัน คือ

1. การระบุหรือ Identify เป็นขั้นแรกที่จะต้องดำเนินการเพื่อเข้าใจในตัวเององค์กรเอง ให้รู้ว่าจะองค์กรมีทรัพยากรและกระบวนการที่สำคัญอะไรบ้างเพื่อนำมาบริหารจัดการความเสี่ยงได้ต่อไป

2. การป้องกันหรือ Protect เป็นการสร้างหรือนำมามาตรการควบคุมทรัพยากรที่สำคัญ เพื่อลดผลกระทบของเหตุภัยคุกคามที่อาจเกิดขึ้นกับทรัพยากรขององค์กรได้
3. การตรวจจับหรือ Detect เพื่อตรวจสอบเหตุด้านภัยคุกคามที่อาจเกิดได้ มีกระบวนการในการเฝ้าระวังและติดตามอย่างเป็นประจำ
4. การตอบสนองหรือ Respond เป็นการวางแผนเพื่อเตรียมตอบสนองต่อเหตุการณ์ร้ายด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจพบ ประกอบกับกระบวนการสื่อสารที่มีประสิทธิภาพมีกระบวนการในการวิเคราะห์หาสาเหตุภัยคุกคาม พยายามลดผลกระทบที่อาจเกิดขึ้นต่อระบบ
5. การคืนสภาพหรือ Recover เป็นขั้นตอนเพื่อให้การดำเนินงานขององค์กรสามารถดำเนินต่อไปได้อย่างต่อเนื่อง เป็นการฟื้นฟูระบบภายหลังการถูกโจมตีให้คืนสู่สภาพปกติได้อย่างรวดเร็วที่สุด (ณัฐวี ฤกษ์ภูมิ และอนาวิล แก้วสะอาด, 2566, น.97-98)

การบริหารจัดการการรับมือภัยคุกคามไซเบอร์

เมื่อองค์กรได้ประเมินความเสี่ยงในแต่ละด้านแล้วดำเนินการตามกรอบมาตรฐาน NIST CSF ตั้งแต่การระบุ (Identify) เพื่อสำรวจทรัพยากรและประเมินความเสี่ยง การป้องกัน (Protect) เพื่อหามาตรการในการลดหรือบรรเทาปัญหาที่อาจจะเกิดขึ้นได้แล้วขั้นตอนต่อไปคือต้องคอยตรวจจับหรือตรวจสอบ (Detect) ระบบต่างๆ ที่มีอยู่ในองค์กรอย่างเป็นระบบเพื่อให้รู้ปัญหาที่อาจจะเกิดขึ้นได้ และถ้าหากว่าการป้องกันไม่ได้ผลก็อาจจะทำให้เกิดภัยคุกคามต่อระบบทำให้จำเป็นต้องมีการตอบสนอง (Respond) ต่อเหตุปัญหที่เกิดขึ้น และท้ายสุดต้องพิจารณาว่า จะต้องมีการดำเนินการคืนสภาพหรือกู้คืนระบบ (Recover) หรือไม่ ซึ่งกระบวนการ 3 ลำดับท้ายสุดคือ Detect Respond และ Recover นั้นเป็นกระบวนการสำคัญที่อยู่ภายใต้กระบวนการที่เรียกว่าการรับมือภัยคุกคามนั่นเอง

การรับมือภัยคุกคามทางไซเบอร์ตามกรอบมาตรฐาน NIST CSF จะอ้างอิงเอกสารแนวทางในการจัดการภัยคุกคามที่เรียกว่า Computer Security Incident Handling Guide ภายใต้รหัส Special Publication 800-61 Revision 2 ซึ่งกระบวนการดังกล่าวเป็นหนึ่งในองค์ประกอบที่สำคัญขององค์กรยุคใหม่ในปัจจุบัน ด้วยที่ว่าภัยคุกคามทางไซเบอร์นั้นวันจะยิ่งหลากหลายและก่อให้เกิดความเสียหายสูง การป้องกันบนพื้นฐานของการระบุและประเมินความเสี่ยงระดับองค์กรและทางเทคนิคสามารถบรรเทาเบาบางภัยคุกคามที่อาจเกิดขึ้นได้แต่ทั้งหมดก็อาจไม่สามารถป้องกันได้ ทำให้ต้องมีการเพิ่มความสามารถในการรับมือภัยคุกคามโดยเริ่มตั้งแต่การตรวจจับเหตุการณ์เพื่อลดโอกาสของความเสียหาย พยายามลดช่องโหว่ให้ได้มากที่สุด และฟื้นฟูระบบให้เป็นปกติได้อย่างรวดเร็วที่สุด ซึ่งการรับมือภัยคุกคามจะต้องมีกระบวนการในการวิเคราะห์หาสาเหตุและหาแนวทางในการจัดการกับปัญหาที่เกิดขึ้น (Cichonski et al., 2012a)

เนื่องจากกระบวนการรับมือภัยคุกคามไซเบอร์ที่มีคุณภาพเป็นกระบวนการที่ค่อนข้างซับซ้อนจะต้องมีการวางแผนและทรัพยากรที่ดี ควรต้องเริ่มจากการให้ความสำคัญกับการตรวจจับหรือตรวจสอบระบบที่เป็นประจำสม่ำเสมอ ต้องมีขั้นตอนในการประเมินและจัดการภัยที่ชัดเจนด้วยการเก็บรวบรวม วิเคราะห์ และรายงานผลข้อมูล ทั้งยังต้องประกอบไปด้วยกระบวนการในการสื่อสารที่เหมาะสมทั้งภายในและภายนอกองค์กร (Cichonski et al., 2012a)

กระบวนการจัดการการรับมือภัยคุกคามไซเบอร์

การวางแผนเพื่อสร้างกระบวนการในการรับมือภัยคุกคามไซเบอร์ทั่วไปมีขั้นตอน ดังนี้

- สร้างนโยบายและแผนรับมือภัยคุกคาม
- พัฒนาระบบการจัดการภัยคุกคามและการรายงานผล
- สร้างแนวปฏิบัติในการสื่อสารภัยคุกคามที่เกิดขึ้นกับหน่วยงานภายนอก
- แต่งตั้งทีมรับมือเหตุการณ์

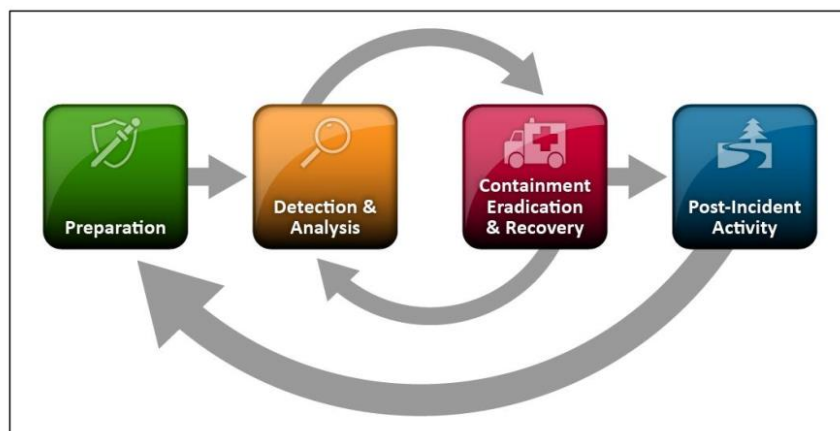
- กำหนดช่องทางการสื่อสารระหว่างทีมรับมือฯ กับหน่วยงานภายในและภายนอก
- กำหนดขอบเขตในการทำงานของทีมรับมือฯ ที่จะให้บริการ
- อบรมให้ความรู้กับทีมรับมือฯ (Cichonski et al., 2012a)

5.วิธีการ/กระบวนการ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 44 กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบไปด้วยเรื่อง

1. แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจ ประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
2. แผนการรับมือภัยคุกคามทางไซเบอร์

มหาวิทยาลัยเชียงใหม่จึงได้มีประกาศมหาวิทยาลัยเชียงใหม่ เรื่อง นโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2567 ประกาศ ณ วันที่ 3 กรกฎาคม พ.ศ. 2567 ที่ผ่านมามาตามนโยบายที่ 2 นโยบายการรักษาสภาพความพร้อมใช้งานของการให้บริการ แนวปฏิบัติข้อ 2 การตรวจสอบและรับมือภัยคุกคาม ทางไซเบอร์ (Detect & Response) ซึ่งแนวคิดหลักตามกรอบมาตรฐาน NIST CSF ในเรื่องกระบวนการรับมือฯ แสดงได้ดังภาพที่ 1 ดังนี้



ภาพที่ 1 วงจรชีวิตกระบวนการรับมือภัยคุกคามทางไซเบอร์

ขั้นตอนในการเตรียมความพร้อม (Preparation) ถือว่าเป็นขั้นตอนแรกที่มีความสำคัญมากที่สุดโดย หน่วยงานจะต้องมีการจัดทำแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ โดยจะต้องให้ความรู้แก่บุคลากร โดยมีการใช้ เครื่องมือช่วยในการตรวจสอบ (Detection) และแจ้งเตือนเหตุการณ์ผิดปกติที่เกิดขึ้น มีทีมงานและหน้าที่ของ บุคลากรในแต่ละภาระงานต้องชัดเจนในการปฏิบัติการในการตอบสนองต่อเหตุการณ์ มีกระบวนการหาข้อมูลจาก แหล่งต่างๆ หรือที่เรียกว่าการหาข่าวกรองภัยคุกคาม (Threat Intelligence) ประกอบในการช่วยวิเคราะห์ เพื่อจะ ได้รู้ถึงวิธีการโจมตีที่ผู้ไม่ประสงค์ดีใช้ แล้วจึงดำเนินการเข้าควบคุมจำกัดความเสียหายเพื่อลดผลกระทบของระบบ (Containment) ต่อจากนั้นทำการกำจัดสาเหตุที่ทำให้เกิดเหตุการณ์ให้สิ้นซาก (Eradication) พยายามนำระบบ กลับมาใช้งานเป็นปกติให้ได้อย่างรวดเร็วที่สุด (Recovery) และจะต้องมีกระบวนการในการบันทึกเหตุการณ์ที่ เกิดขึ้นเพื่อให้เป็นบทเรียนในการรับมือเหตุการณ์ในครั้งต่อไป (Post-Incident Activity) (Cichonski et al.,

2012b) ถ้าองค์กรสามารถดำเนินการได้ดังนี้ก็จะสามารถทำให้รับมือกับภัยคุกคามทางด้านไซเบอร์ได้อย่างมีประสิทธิภาพและเกิดความมั่นใจต่อระบบเทคโนโลยีสารสนเทศที่สำคัญขององค์กรต่อผู้มีส่วนได้เสียทุกภาคส่วนได้

สำนักบริการเทคโนโลยีสารสนเทศ โดยฝ่ายความมั่นคงปลอดภัยไซเบอร์ จึงได้มีการวางแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์มหาวิทยาลัยเชียงใหม่ขึ้นมาเพื่อเป็นแนวปฏิบัติในการรับมือภัยคุกคามทางไซเบอร์ให้แก่ทุกส่วนงานภายในมหาวิทยาลัยได้ใช้ร่วมกัน ดังนี้

ขั้นตอนการกำหนดบทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

กระบวนการหลักของแผนรับมือฯ เริ่มจากส่วนของ การกำหนดบทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยเริ่มจากการระบุชื่อผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ในกรณีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยจะมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และมีการเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองในกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้

ต่อไปจะทำการกำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT) โดยการใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (Centralize) โดยจะมีการระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ

ส่วนสุดท้ายของโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT) คือการกำหนดโครงสร้างรายงานเหตุการณ์ (Incident Reporting Structure) เพื่อให้บุคลากรที่อยู่ในทีมรับมือฯ ปฏิบัติเป็นขั้นเป็นตอนมีมาตรฐานในแนวทางเดียวกัน ดังนี้

1. ผู้พบเหตุการณ์แจ้งเหตุไปยังฝ่ายความมั่นคงปลอดภัยไซเบอร์ ผ่านระบบ CMU Ticket Management
2. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ วิเคราะห์เหตุการณ์และผลกระทบ พร้อมประเมินระดับความรุนแรง และทำการกำหนดหมวดหมู่ภัยคุกคาม
3. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ ประสานงานกับผู้ที่เกี่ยวข้อง เช่น ฝ่ายโครงสร้างพื้นฐาน เทคโนโลยีสารสนเทศ ฝ่ายพัฒนาระบบสารสนเทศหรือส่วนงานเจ้าของ Asset
4. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ รายงานผู้บังคับบัญชาทราบตามลำดับชั้น หากเหตุการณ์อยู่ในระดับความรุนแรงสูง (High) หรือวิกฤต (Critical)
5. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ ประสานงานผู้เกี่ยวข้อง ตอบสนองต่อเหตุการณ์ เพื่อป้องกันไม่ให้เกิดการแพร่กระจาย และกู้คืนระบบ
6. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ ดำเนินการตรวจสอบหลักฐาน เพื่อระบุสาเหตุและที่มาของปัญหาภัยคุกคาม
7. ฝ่ายความมั่นคงปลอดภัยไซเบอร์ แนะนำแนวทางในการป้องกันและแก้ไขปัญห และนำเสนอผู้บริหาร เพื่อนำไปสู่แนวนโยบายและมาตรการในการป้องกันต่อไป
8. ฝ่ายความมั่นคงปลอดภัยไซเบอร์สรุปรายงานแจ้งหน่วยงานภายนอกที่เกี่ยวข้อง (หากมีการแจ้งเหตุการณ์ดังกล่าวจากหน่วยงานภายนอก เช่น สกมช.)

6.ผลกระทบที่เป็นประโยชน์หรือสร้างคุณค่า

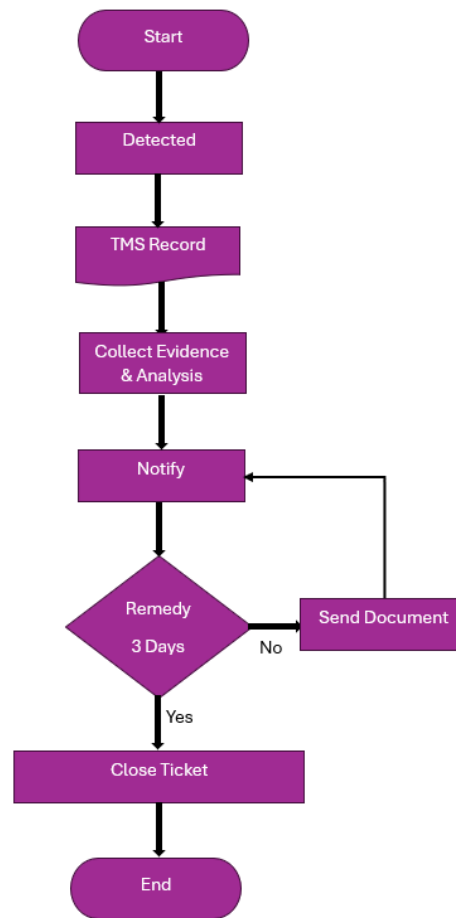
การสร้างกระบวนการรับมือภัยคุกคามไซเบอร์ กรณีเว็บไซต์ถูกแก้ไขเปลี่ยนแปลง (Web Defacement) ให้เป็นเว็บพอร์ทัลที่มีกระบวนการชัดเจนและมาตรฐานดังกล่าวช่วยเพิ่มประสิทธิภาพในการทำงานจากที่ก่อนหน้านี้

ขั้นตอนในการปฏิบัติงานไม่ชัดเจนทำให้ผู้ปฏิบัติงานเกิดความสับสนและปฏิบัติงานไม่เป็นมาตรฐานเดียวกัน ทั้งยังเป็นการช่วยเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ให้แก่ทุกส่วนงานภายในมหาวิทยาลัยเพื่อป้องกันความเสียหายที่อาจเกิดการสูญเสียชื่อเสียงของมหาวิทยาลัยและความมั่นใจในการเข้าใช้ระบบของนักศึกษา บุคลากรและผู้คนภายนอกมหาวิทยาลัยในภาพรวม ทั้งนี้กระบวนการดังกล่าวยังสามารถสร้างมาตรฐานที่ดีในการปฏิบัติงานของบุคลากรภายในฝ่ายความมั่นคงปลอดภัยไซเบอร์อันจะเป็นกรณีตัวอย่างที่ดีทำให้เจ้าหน้าที่ที่มีความตระหนักถึงมาตรฐานในการปฏิบัติงานที่ดีมีการเรียนรู้และปรับตัวกับกระบวนการที่เป็นมาตรฐานสากล ทำให้ในอนาคตสามารถเพิ่มขีดความสามารถในการทำงานในลักษณะที่ซับซ้อนมากขึ้น ซึ่งจะเป็นการเพิ่มคุณค่าให้กับเจ้าหน้าที่ของฝ่ายฯ ในระยะยาวได้เป็นอย่างดี

7.แผนการดำเนินงาน / การนำไปใช้

กระบวนการรับมือภัยคุกคามไซเบอร์ กรณีเว็บไซต์ถูกแก้ไขเปลี่ยนแปลง (Web Defacement) ให้เป็นเว็บพนัน

จากที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ดำเนินการเฝ้าระวัง ติดตาม วิเคราะห์ รวมถึงให้การแจ้งเตือนในการตรวจพบภัยคุกคามทางไซเบอร์โดยในปัจจุบันจากสถิติการเกิดปัญหาภัยคุกคามทางไซเบอร์ พบว่าหน่วยงานภาคการศึกษาในประเทศไทยตกเป็นเป้าหมายของการโจมตีด้วยการฝังเว็บพนันออนไลน์บนเว็บไซต์ของหน่วยงาน (Website Gambling) ซึ่งส่งผลกระทบต่อชื่อเสียง ภาพลักษณ์ และความน่าเชื่อถือของหน่วยงานภาคการศึกษา มหาวิทยาลัยเชียงใหม่ได้ให้ความสำคัญกับปัญหาดังกล่าวทำให้ฝ่ายความมั่นคงปลอดภัยไซเบอร์ สำนักบริการเทคโนโลยีสารสนเทศ จึงได้กำหนดกระบวนการในการจัดการกับปัญหาดังกล่าวที่มักเกิดขึ้นกับเว็บไซต์ของส่วนงานต่างๆ ภายในมหาวิทยาลัย โดยให้มีความสอดคล้องกับกระบวนการจัดการการรับมือภัยคุกคามไซเบอร์ที่กล่าวไปข้างต้น สามารถแสดงแผนผังกระบวนการทำงานได้ ดังนี้



ภาพที่ 2 ฝั่งแสดงกระบวนการรับมือภัยคุกคามเว็บพนันออนไลน์
โดยแต่ละกระบวนการย่อยสามารถอธิบายได้ ดังนี้

1. **Detected** เป็นการตรวจสอบการถูกแก้ไขเปลี่ยนแปลงเว็บไซต์เป็นประจำทุกวันโดยมี 2 วิธีการหลัก คือ

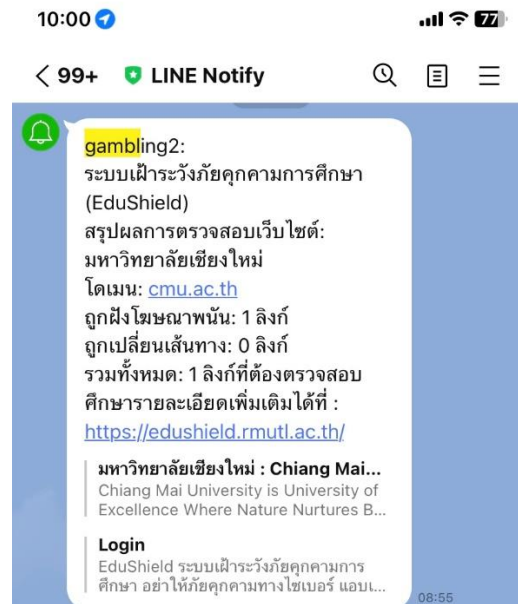
- 1.1 วิธีการใช้ Google Search Engine

ด้วยวิธีนี้จะใช้การค้นหาผ่าน Google Search บนเว็บไซต์ www.google.com โดยใช้รูปแบบคำค้นหาที่จำเพาะเจาะจงถึงคำค้น (Keyword) ที่เกี่ยวข้องกับเว็บพนันทั้งหมดภายใต้เว็บไซต์ในโดเมนของมหาวิทยาลัย หรืออาจจะจำเพาะเจาะจงส่วนงานใดส่วนงานหนึ่งก็ได้ตามรูปแบบ ดังนี้
“คำค้น (Keyword) site:ชื่อโดเมน (Domain)” และการใช้งานจริงจะเป็นตัวอย่าง ดังนี้
“slot daftar casino betting baccarat gambling site:cmu.ac.th”

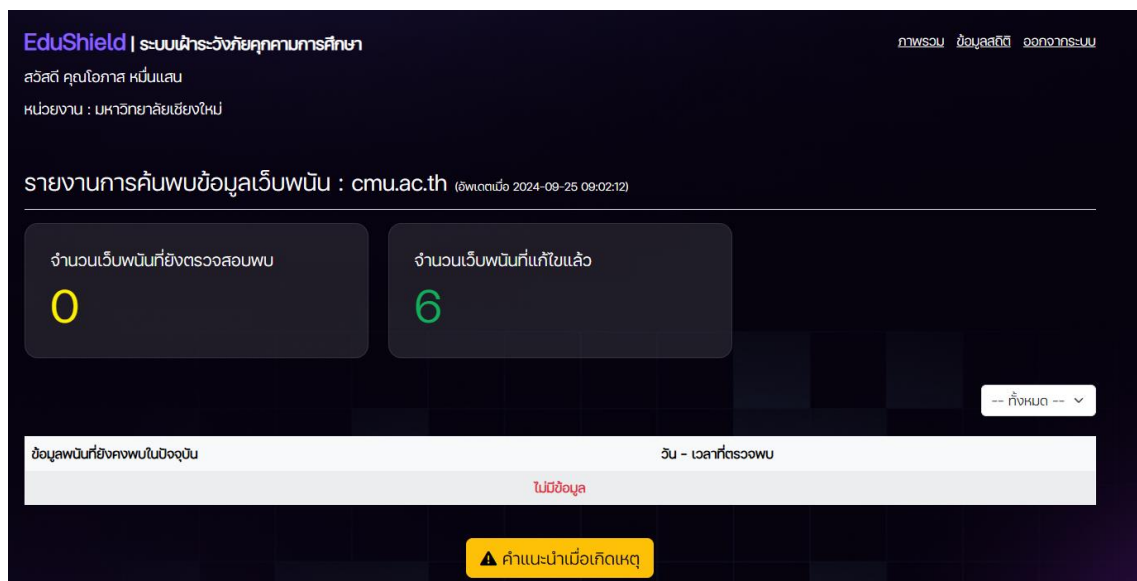
- 1.2 วิธีการใช้บริการระบบเฝ้าระวังภัยคุกคามการศึกษา EduShield

โดยระบบดังกล่าวสำนักงานคณะกรรมการการรักษามั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ร่วมกับมหาวิทยาลัยเทคโนโลยีราชมงคลล้านนา ร่วมกันจัดโครงการ เว็บไซต์การศึกษาปลอดภัยพนันออนไลน์ โดยได้มีการทำระบบเฝ้าระวังภัยคุกคามการศึกษา (EduShield) ที่พัฒนาขึ้นมาเฉพาะสำหรับหน่วยงานการศึกษาในการใช้งานระบบนี้เท่านั้น พร้อมทั้งมีระบบแจ้งเตือนทันทีเมื่อพบความพยายามโจมตีหรือการฝังเว็บพนันออนไลน์ ซึ่งจะช่วยให้หน่วยงานสามารถตอบสนองได้อย่างรวดเร็วและปกป้องเว็บไซต์ของหน่วยงานได้อย่างมีประสิทธิภาพ โดยเครื่องมือนี้จะมีการแจ้ง

เตือนทันทีเมื่อพบเว็บพนันของมหาวิทยาลัยเชียงใหม่ภายใต้โดเมน cmu.ac.th ผ่าน 2 ช่องทาง
คือ Line Notify และบนหน้าเว็บไซต์ของระบบ EduShield ดังรูป



ภาพที่ 3 การแจ้งเตือนเว็บพนันผ่าน Line Notify



ภาพที่ 4 การแจ้งเตือนเว็บพนันผ่านระบบ EduShield

2. TMS Record

เมื่อทำการตรวจพบเว็บไซต์ของส่วนงานที่ถูกแก้ไขเป็นหน้าเว็บพนันออนไลน์แล้วผู้รับแจ้งเหตุการณ์
ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงานซึ่งเป็นเจ้าหน้าที่ของฝ่ายความมั่นคงปลอดภัยไซเบอร์จะทำการ
การลงบันทึกแจ้งเหตุในระบบ TMS : Ticket Management System เพื่อเป็นการบันทึกเหตุที่ตรวจพบ
ในการที่จะติดตามตรวจสอบได้ต่อไป

แบบบันทึกเหตุการณ์คุกคามทางไซเบอร์

ข้อมูลผู้แจ้งเหตุ

ชื่อ-สกุล: โสมมา พันธ์สม
 ส่วนงาน/สังกัด: สำนักงานเทคโนโลยีสารสนเทศ

อีเมล: opas.m@cmu.ac.th

ข้อมูลเหตุการณ์คุกคามทางไซเบอร์

หมวดหมู่ภัยคุกคามทางไซเบอร์

☒ Vulnerability ☐ Spyware ☐ Flood ☐ Malware ☐ Phishing ☐ Admin Information Sharing ☐ Network Scanning
☐ Web Application Threat ☐ Denial of Service ☐ Unauthorized Access ☐ Website Defacement ☐ Malicious Redirects
☐ Email Alert ☐ Information leakage ☐ Insecure Design ☐ Credential leakage ☐ End User Information Sharing

หัวข้อภัยคุกคามทางไซเบอร์ (Subject)

คำอธิบายภัยคุกคามทางไซเบอร์

คำอธิบายเพิ่มเติมเหตุการณ์

คำอธิบายเพิ่มเติมของระบบ

ส่วนงานที่ได้รับผลกระทบ

กรุณาระบุชื่อระบบ

ภาพที่ 5 หน้าจอบันทึกเหตุการณ์ที่ตรวจพบในระบบ TMS

3. Collect Evidence & Analysis

เมื่อเจ้าหน้าที่รับแจ้งเหตุฯ ได้ทำการบันทึกเหตุเว็บไซต์ที่ถูกโจมตีแล้วเจ้าหน้าที่ที่รับผิดชอบภัยคุกคามไซเบอร์จะทำการใช้เครื่องมือที่มี คือ Burp Suite ในการเก็บหลักฐานและตรวจสอบสาเหตุหรือช่องโหว่ของเว็บไซต์ที่ถูกโจมตีและวิเคราะห์เหตุการณ์การโจมตีเว็บไซต์ที่เกิดขึ้นเพื่อหาแนวทางในการแก้ไขปัญหาตัวอย่างเครื่องมือ ดังรูป

Time	Source	Issue type	Issue	Path	Insertion point	Severity	Confidence	Comment
11:04:15 30 Oct 2024	Task 3	XPath injection		/cron.php	form_id parameter	High	Firm	
10:15:22 30 Oct 2024	Task 3	XPath injection		/demoweb/	q parameter	High	Firm	
10:05:52 30 Oct 2024	Task 3	XPath injection		/	q parameter	High	Firm	
10:20:58 30 Oct 2024	Task 3	XML injection		/	q parameter	Medium	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/sites/all/modules/jquery_update/replace/ui/ui.min.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/sites/all/modules/jquery_update/replace/ui/ui.min.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/sites/all/modules/jquery_update/replace/ui/ui.min.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/misc/jquery.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/sites/all/modules/jquery_update/replace/ui/ui.min.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/sites/all/modules/jquery_update/replace/ui/ui.min.js		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	Vulnerable JavaScript dependency		/		Low	Tentative	
10:01:01 30 Oct 2024	Task 3	TLS cookie without secure flag set		/		Medium	Firm	
10:00:58 30 Oct 2024	Task 3	TLS certificate		/		Information	Certain	

ภาพที่ 6 หน้าจอเครื่องมือ Burp Suite

4. Notify

เมื่อทราบสาเหตุของปัญหาช่องโหว่ของระบบเว็บไซต์ที่ถูกโจมตีแล้วจะทำการประสานแจ้งและให้คำแนะนำในการแก้ไขปัญหาให้ผู้ดูแลเว็บไซต์ของส่วนงานเพื่อให้แก้ไขปัญห

5. Remedy 3 Days

เมื่อแจ้งปัญหาเว็บไซต์ถูกโจมตีแก้ไขเปลี่ยนแปลงเป็นหน้าเว็บพบนอนไลน์แก่เจ้าหน้าที่ผู้ดูแลระบบเว็บไซต์ของส่วนงานแล้วจะทำการรอเพื่อให้เวลาเจ้าหน้าที่ผู้ดูแลเว็บไซต์ของส่วนงานดำเนินการลบเนื้อหาและแก้ไขปัญห

6. Send Document

หากพ้นกำหนดเวลา 3 วันแล้วเจ้าหน้าที่ผู้ดูแลเว็บไซต์ส่วนงานยังไม่ดำเนินการแก้ไขเนื้อหาเว็บพบนอนไลน์ดังกล่าวออกพร้อมทั้งแก้ไขช่องโหว่ที่ตรวจพบแล้วหัวหน้าฝ่ายความมั่นคงปลอดภัยไซเบอร์จะทำการร่างบันทึกข้อความเพื่อแจ้งเตือนปัญหาดังกล่าว ลงนามโดยผู้อำนวยการสำนักบริการเทคโนโลยีสารสนเทศ และทำการส่งไปยังผู้บริหารของส่วนงานนั้นเพื่อให้รับทราบและดำเนินการแก้ไขต่อไป

7. Close Ticket

หากพ้นกำหนดเวลา 3 วันแล้วปรากฏว่าเจ้าหน้าที่ผู้ดูแลเว็บไซต์ส่วนงานได้ดำเนินการแก้ไขหาเนื้อหาเว็บพจนานออนไลน์ดังกล่าวออกพร้อมทั้งแก้ไขช่องโหว่ที่ตรวจพบเป็นที่เรียบร้อยแล้วเจ้าหน้าที่รับมือฯ แล้ว จะดำเนินการปิด Ticket เพื่อจบกรณีหรือเหตุดังกล่าวภายในระบบ TMS โดยเหตุที่เคยเกิดขึ้นดังกล่าวจะถูกบันทึกไว้ในระบบเพื่อสามารถจะนำมาเป็นกรณีศึกษา เรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมาทั้งหมด และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต

8.วิเคราะห์และสรุปสาระสำคัญ

ภัยไซเบอร์มีอยู่อย่างหลากหลายและรุนแรงในปัจจุบันไม่สามารถป้องกันได้ทั้งหมด สามารถแก้ปัญหาและรับมือได้ด้วยกระบวนการรับมือภัยคุกคามทางไซเบอร์ที่ดีมีมาตรฐานแนวปฏิบัติชัดเจนเพื่อให้ผู้ปฏิบัติงานได้ดำเนินการได้อย่างมีมาตรฐานเดียวกันทุกคนเพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้น การโจมตีเพื่อแก้ไขเปลี่ยนแปลงเว็บไซต์โดยเฉพาะกรณีเว็บโฆษณาการพจนานออนไลน์มีจำนวนมากตามสถิติของ สกมช. ฝ่ายความมั่นคงปลอดภัยไซเบอร์จึงได้ร่างแนวปฏิบัติเฉพาะกรณีภัยการโจมตีแก้ไขเปลี่ยนแปลงหน้าเว็บไซต์ให้เป็นเว็บพจนานขึ้นมาเพื่อจัดการในกรณีเฉพาะนี้ โดยหวังว่าจะช่วยป้องกันความเสียหายที่ทำให้เกิดการสูญเสียชื่อเสียงของมหาวิทยาลัยและความมั่นใจในการใช้ระบบเว็บไซต์ของนักศึกษา บุคลากรและผู้นอกมหาวิทยาลัย

9.เอกสารอ้างอิง

ชรินทร์ทิพย์ ปั้นสุวรรณ. (2565). แนวทางการกำกับดูแลการรับมือภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ขององค์กรในยุคดิจิทัล. Chulalongkorn University Theses and Dissertations (Chula ETD). 6715.

อนาวิล แก้วสะอาด และณัฐวี อุตกฤษฎ์. (2564). แนวทางบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. วารสารสถาบันวิชาการป้องกันประเทศ.

ณัฐวี อุตกฤษฎ์,อนาวิล แก้วสะอาด (2566), บทปฏิบัติตนอย่างเป็นระบบว่าด้วยแนวทางการเตรียมพร้อมขององค์กร เพื่อยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์, วารสารเทคโนโลยีสารสนเทศ, Volume 19, Issue 1, pp. 94-102.

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*.

<https://doi.org/10.6028/NIST.SP.800-61r2>