คณะครุศาสตร์
รับเลขที่ 9194
วันที่ ๑๙ ธ.ค. ๒๕๖๕
เวลา .... น.

ที่ อว ๐๒๑๙/๑๑๐๕

สำนักงานปลัดกระทรวงการอุดมศึกษา
วิทยาศาสตร์ วิจัยและนวัตกรรม
ถนนศรีอยุธยา เขตราชเทวี กรุงเทพฯ ๑๐๔๐๐

๑๔ ธันวาคม ๒๕๖๕

เรื่อง การแจ้งเตือนกรณีตรวจพบการโจมตีต่อเว็บไซต์ของคณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช ด้วยการทำ Website Defacement

เรียน คณบดีคณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช

สิ่งที่ส่งมาด้วย ๑. สำเนาหนังสือที่ สกมช ๐๘๑๐/ว๑๓๑๑ ลงวันที่ ๒๘ พฤศจิกายน ๒๕๖๕
๒. เอกสารแจ้งเตือนกรณีตรวจพบการโจมตีต่อเว็บไซต์ของหน่วยงานการศึกษาด้วยการทำ Website Defacement

ด้วย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีหนังสือแจ้งเตือนกรณีตรวจพบเว็บไซต์ของคณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช ถูกโจมตีด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ Website Defacement ที่ URL : hxxps://edu๒.nstru.ac[.]th/net.html รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ๑

ในการนี้ สำนักงานปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม โดยสำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา จึงขอส่งสรุปข้อมูลเกี่ยวกับเหตุการณ์และคำแนะนำในการแก้ไขเบื้องต้นแจ้งเตือน มหาวิทยาลัยราชภัฏนครศรีธรรมราช เพื่อดำเนินการแก้ไขป้องกันการนำไปใช้ในการหลอกลวงอันจะส่งผลให้เกิดความเสียหายได้ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ๒ ทั้งนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามเพิ่มเติมได้ที่ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หมายเลขโทรศัพท์ ๐ ๒๑๑๔ ๓๕๓๑ หรืออีเมล ncert@ncsa.or.th

จึงเรียนมาเพื่อโปรดทราบ

เรียน คณบดี
● เพื่อโปรดทราบ
● เห็นควรมอบ ผู้ช่วยคณบดี...

ขอแสดงความนับถือ

(ผู้ช่วยศาสตราจารย์ประมา ศาสตระรุจิ)
ผู้อำนวยการ
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา

(นางสาววิจิตรา ขุนไชย)
นักวิชาการศึกษา ปฏิบัติการ
๑๙ ธ.ค. ๒๕๖๕

19/12/65

สำนักงานปลัดกระทรวงการอุดมศึกษาฯ
สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา
ฝ่ายบริหารระบบเครือข่าย
โทรศัพท์ ๐ ๒๒๓๒ ๔๐๐๐ ต่อ ๕๖๙๐ (สุพัชรพงษ์)
อีเมล supachapong.b@mhesi.go.th

สำนักงานปลัดกระทรวงการอุดมศึกษา
วิทยาศาสตร์ วิจัยและนวัตกรรม
เลขรับ ๑๑๕๗/๒๕๖๕
วันที่ ๓๐ พ.ย. ๒๕๖๕
เวลา ๑๖.๓๕ น.

ลับมาก

NCSA สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๑๒๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด
ที่ สกมช ๐๘๑๐/ว๑๓๑๑

๒๘ พฤศจิกายน ๒๕๖๕

เรื่อง การแจ้งเตือนกรณีตรวจพบการโจมตีต่อเว็บไซต์ของ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช ด้วยการทำ Website Defacement

เรียน ปลัดกระทรวงกระทรวงการอุดมศึกษา วิทยาศาสตร์วิจัยและนวัตกรรม

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย เอกสารการแจ้งเตือนกรณีตรวจพบการโจมตีต่อเว็บไซต์ของหน่วยงานการศึกษา

ตามอ้างถึง มาตรา ๒๒ (๖) ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์” นั้น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้ตรวจพบเว็บไซต์ของคณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช ถูกโจมตีด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ Website Defacement ที่ URL : hxxps://edu2.nstru.ac[.]th/net.html โดยรายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้สรุปข้อมูลเกี่ยวกับเหตุการณ์และได้จัดทำคำแนะนำในการแก้ไขเบื้องต้นแจ้งเตือน มหาวิทยาลัยราชภัฏนครศรีธรรมราช ดำเนินการแก้ไขเพื่อป้องกันการนำไปใช้อันจะส่งผลให้เกิดความเสียหายและเสื่อมเสียชื่อเสียงได้ ทั้งนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามเพิ่มเติมได้ที่ สำนักปฏิบัติการ หมายเลขโทรศัพท์ ๐-๒๑๑๔-๓๕๓๑ หรือ อีเมล ncert@ncsa.or.th

จึงเรียนมาเพื่อโปรดทราบ

มอบ สบทม. พิจารณา

ขอแสดงความนับถือ

พลอากาศตรี อมร ชมเชย

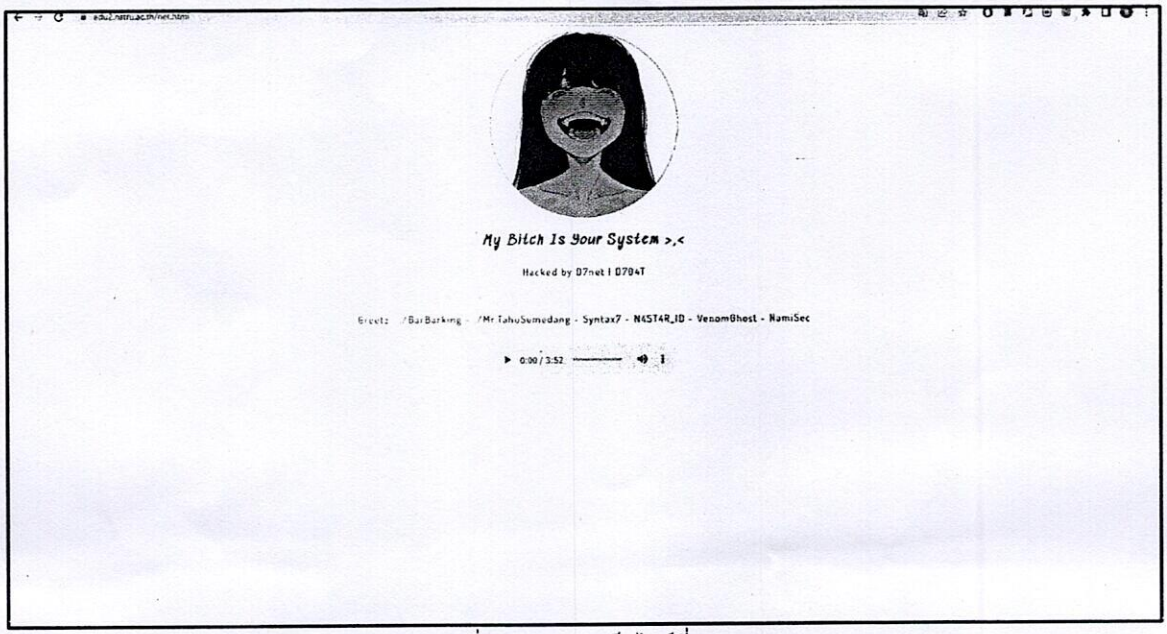
(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

(รองศาสตราจารย์พาสิทธิ์ หล่อธีรพงศ์)
รอง ปอว. รักษาราชการแทน
ปอว.
๑๖ ธ.ค. 2565
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทรศัพท์ ๐ – ๒๑๔๒- ๖๘๘๕ อีเมล ncert@ncsa.or.th

ลบมาก

เอกสารรายงานแจ้งเตือนกรณีการโจมตีต่อเว็บไซต์ของหน่วยงานราชการ ด้วยการทำ Website Defacement

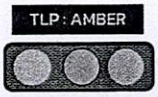
1. เมื่อวันที่ 18 พฤศจิกายน 2565 เวลาประมาณ 22.00 น. ได้ตรวจพบเว็บไซต์ของหน่วยงานการศึกษา ถูกโจมตีด้วยการเปลี่ยนแปลงหน้าเว็บไซต์ Website Defacement ที่ URL : hxxps://edu2.nstru.ac[.]th /net.html โดยได้มีการเปลี่ยนแปลงหน้าเว็บไซต์ดังกล่าวจากแฮ็กเกอร์ที่มีชื่อว่า D7net ตามภาพที่ 1



ภาพที่ 1 แสดงภาพเว็บไซต์ที่ถูกพบ

2. ทำการตรวจสอบ URL พบว่าเป็นเว็บไซต์ของ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช ตามภาพที่ 2

ภาพที่ 2 แสดงภาพเว็บไซต์ของ คณะครุศาสตร์ มหาวิทยาลัยราชภัฏนครศรีธรรมราช



<u>คำแนะนำในการดำเนินการเบื้องต้นสำหรับกรณีนี้</u>

1. ให้ตรวจสอบข้อมูลตามที่ปรากฏบนหน้าเว็บข้อมูลคอมพิวเตอร์ในระบบข้อมูล log file และพฤติการณ์แวดล้อมในระบบ เพื่อประเมินว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากพบว่ามีเหตุการณ์เกิดขึ้นให้ดำเนินการเพื่อป้องกันรับมือและลดความเสี่ยงตาม พ.ร.บ.ไซเบอร์ฯ หรือแนวทางด้าน cybersecurity เช่น NIST Cybersecurity Framework[1] เป็นต้น ทั้งนี้ สกมช. ยินดีให้การสนับสนุนในการดำเนินการดังกล่าว

2. ดำเนินการแจ้งความกับหน่วยงานบังคับใช้กฎหมายที่รับผิดชอบในทันที เช่น บช.สอท. ตั้งอยู่ภายในเมืองทองธานี จว.นนทบุรี หรือสถานีตำรวจในพื้นที่ เพื่อจะได้เป็นการแจ้งเหตุการกระทำผิดทางอาญาในฐานะผู้เสียหาย และเริ่มกระบวนการตรวจพิสูจน์ได้อย่างถูกต้องตามกฎหมาย

3. ดำเนินการตรวจสอบข้อมูลที่มีความละเอียดอ่อนที่ถูกทำให้เผยแพร่ไป โดยได้อ้างว่าเป็นของหน่วยงานหรือบุคคลอื่น เพื่อพิจารณาแนวทางป้องกันและรับมือกับข้อกฎหมายและความเสียหายที่อาจจะเกิดขึ้น

4. ในการดำเนินการเรื่องรับมือและตอบสนองเหตุการณ์ดังกล่าว นอกจากการกู้คืนระบบให้สามารถทำงานได้ตามปกติโดยเร็วแล้ว ควรจะดำเนินการหาสาเหตุและแหล่งที่มาของภัยคุกคามที่แท้จริง สามารถระบุร่องรอยได้ตามพยานหลักฐานที่ปรากฏได้อย่างชัดเจน ทั้งนี้เพื่อเป็นการตรวจหาภัยคุกคามที่ยังคงแฝงอยู่ในระบบและเป็นการป้องกันไม่ให้เกิดเหตุซ้ำจากช่องโหว่ที่มีอยู่ในระบบ

<u>คำแนะนำในการปฏิบัติเพื่อลดความเสี่ยงที่จะถูกโจมตีเว็บไซต์โดยทั่วไป สำหรับผู้ดูแลระบบ</u>

สำหรับกรณีนี้ผู้ที่เป็นเจ้าของเว็บไซต์ควรจะต้องดำเนินการตรวจสอบว่าเว็บไซต์มีช่องโหว่ที่จุดใดและควรดำเนินการแก้ไขเพื่อไม่ให้ผู้ที่ไม่หวังดีใช้เป็นที่กระทำความผิดต่อไป โดยทั่วไปแล้วในเบื้องต้น ผู้ดูแลระบบควรจะเปลี่ยนรหัสผ่านของผู้ใช้ทั้งหมด ลบลิงก์ที่ไม่ได้ใช้งานออกจากเว็บไซต์ กำหนดสิทธิ์ในการเข้าถึงเว็บไซต์ใหม่ทั้งหมด จากนั้นจึงดำเนินการทดสอบหาช่องโหว่ของเว็บไซต์เพื่อป้องกันการโจมตีต่อไป

คำแนะนำสำหรับจัดทำเว็บไซต์โดยทั่วไปนั้นมีคำแนะนำจาก OWASP TOP 10 Project[2] ซึ่งเป็นขององค์กรที่ชื่อ OWASP เป็นองค์กรที่ไม่แสวงหาผลกำไรที่ให้ความรู้ เพื่อการปรับปรุงในการจัดทำเว็บไซต์ให้ปลอดภัย ซึ่งมีคำแนะนำหลายเรื่อง เช่น การเขียนโปรแกรม การใช้เครื่องมือในการตรวจสอบการรักษาความมั่นคงปลอดภัย เทคโนโลยีที่ใช้ในการรักษาความมั่นคงปลอดภัยของเว็บไซต์ ซึ่งสามารถไปศึกษาและดาวน์โหลดเอกสารได้ที่ https://owasp.org/

<u>ตาม พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562</u> มาตรา 58[3] กรณีเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ในการดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงาน เพื่อประเมินภัยคุกคาม ดำเนินการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งมายังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

<u>อ้างอิง</u>

1. https://www.nist.gov/cyberframework
2. https://owasp.org/www-project-top-ten/
3. https://drive.ncsa.or.th/s/XtCz2kFkcwkaz9Y