



องค์การบริหารส่วนตำบลโคกสว่าง
รับเลขที่ ๖๓๗ / ๒๕๖๙
วันที่ ๒๑ / ๖๓๗ / ๒๕๖๙

ที่ รอ ๑๑๑๘/ว ๓๕๖๙

ที่ว่าการอำเภอหนองพอก

ถนนทรงบาดาล รอ ๔๕๒๑๐

๒๑ เมษายน ๒๕๖๙

เรื่อง แจ้งเตือนกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak)

เรียน นายกเทศมนตรีตำบล หุ่นแห่ง และนายกองค์การบริหารส่วนตำบล ทุกแห่ง

สิ่งที่ส่งมาด้วย สำเนาหนังสือจังหวัดร้อยเอ็ด ด่วนที่สุด ที่ รอ ๐๐๑๗๒/ว ๓๕๘๙ ลงวันที่ ๑๖ เมษายน ๒๕๖๙

ด้วยอำเภอหนองพอก ได้รับแจ้งจากจังหวัดร้อยเอ็ดว่า สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ว่าได้ติดตามสถานการณ์ด้านข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่ากรณีการรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยมีการเผยแพร่ข้อมูลบัญชีผู้ใช้งาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในแหล่งต่าง ๆ ซึ่งอาจถูกนำไปใช้เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต และเป็นจุดเริ่มต้นในการเข้าถึงข้อมูลสำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายในระบบเครือข่าย (Lateral Movement) ของหน่วยงาน ทั้งนี้ สกมช. ได้แจ้งสรุปข้อมูลเหตุการณ์ ความเสี่ยง และจัดส่งแนวทางการป้องกันและลดผลกระทบเพื่อให้หน่วยงานใช้เป็นแนวทางและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย อำเภอหนองพอก จึงขอจัดส่งเอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์ กรณีข้อมูลส่วนบุคคลรั่วไหล เพื่อใช้เป็นแนวทางในการปฏิบัติ พร้อมทั้งให้ดำเนินการตรวจสอบ ปรับปรุง เสริมสร้างมาตรการรักษาความมั่นคงสารสนเทศของหน่วยงานตามแนวทางที่กำหนด รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและดำเนินการในส่วนที่เกี่ยวข้อง

ขอแสดงความนับถือ

เรียน นายกองค์การบริหารส่วนตำบลโคกสว่าง

อำเภอหนองพอก เพื่อแจ้งเตือนกรณี
ข้อมูลส่วนบุคคลรั่วไหล (Data Leak)

เมื่อไปเดือนตุลาคม

(นางสาวสิริลักษณ์ ภาพลงาม)

เจ้าพนักงานธุรการปฏิบัติงาน

(นายจักรพงศ์ สิริมงคลกรม)

นายอำเภอหนองพอก

จาก

(บุญฤทธิ์ กลางประพันธ์)

หัวหน้าสำนักปลัดอบต.โคกสว่าง

๒๑/๓/๒๕๖๙

ที่ทำการปกครองอำเภอ

สำนักงานอำเภอ

ฝ่ายบริหารงานทั่วไป

โทร. ๐-๔๓๕๗-๙๐๗๑

(นายศรีศักดิ์ เวียงนันท)

ปลัดองค์การบริหารส่วนตำบลโคกสว่าง

(นายสงวน ชมภูทิพย์)

นายกองค์การบริหารส่วนตำบลโคกสว่าง

5๕๖

ด่วนที่สุด

ที่ รอ ๐๐๑๗.๒/ว ๓๕๖๙



ที่ว่าการอำเภอหนองพอก

เลขที่ 1523

วันที่ 17 เม.ย. 2569

เวลา 12.10 น.

ศาลากลางจังหวัดร้อยเอ็ด

ถนนเทวาภิบาล รอ. ๕๕๐๐๐

๑๖ เมษายน ๒๕๖๙

เรื่อง แจ้งเตือนกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak)

เรียน หัวหน้าส่วนราชการ หัวหน้าหน่วยงานรัฐวิสาหกิจ นายอำเภอ ทุกอำเภอ นายกองค้การบริหารส่วนจังหวัดร้อยเอ็ด และนายกเทศมนตรีเมืองร้อยเอ็ด

สิ่งที่ส่งมาด้วย ๑. สำเนาหนังสือ สกมช. ที่ สกมช ๐๘๑๐/ว ๑๓๗๕ จำนวน ๑ ฉบับ ลงวันที่ ๓ เมษายน ๒๕๖๙

๒. เอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์ฯ จำนวน ๑ ชุด

ด้วยจังหวัดร้อยเอ็ดได้รับแจ้งจากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ว่าได้ติดตามสถานการณ์ด้านข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบว่ากรณีการรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยมีการเผยแพร่ข้อมูลบัญชีผู้ใช้งาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในแหล่งต่าง ๆ ซึ่งอาจถูกนำไปใช้เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต และเป็นจุดเริ่มต้นในการเข้าถึงข้อมูลสำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายภายในระบบเครือข่าย (Lateral Movement) ของหน่วยงาน ทั้งนี้ สกมช. ได้แจ้งสรุปข้อมูลเหตุการณ์ ความเสี่ยง และจัดส่งแนวทางการป้องกันและลดผลกระทบ เพื่อให้หน่วยงานใช้เป็นแนวทางและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ รายละเอียดตามสิ่งที่ส่งมาด้วย

เพื่อให้การดำเนินการเป็นไปด้วยความเรียบร้อย จังหวัดร้อยเอ็ดจึงขอจัดส่งเอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์ กรณีข้อมูลส่วนบุคคลรั่วไหล เพื่อใช้เป็นแนวทางในการปฏิบัติ พร้อมทั้งให้ดำเนินการตรวจสอบ ปรับปรุง เสริมสร้างมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานตามแนวทางที่กำหนด สำหรับอำเภอขอให้แจ้งองค์กรปกครองส่วนท้องถิ่นในพื้นที่ทราบและถือปฏิบัติด้วย ทั้งนี้ สามารถดาวน์โหลดสิ่งที่ส่งมาด้วยได้ที่ QR Code ท้ายหนังสือฉบับนี้

จึงเรียนมาเพื่อพิจารณาดำเนินการต่อไป

ขอแสดงความนับถือ

(นายชัชวาลย์ เบญจสิริวงศ์)
ผู้ว่าราชการจังหวัดร้อยเอ็ด



สำนักงานจังหวัดร้อยเอ็ด

กลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

โทรศัพท์/โทรสาร. ๐ ๔๓๕๑ ๙๑๖๔

๗ เม.ย. ๒๕๖๙ ๐๙:๐๖



สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ ชั้น ๗ อาคารซี ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพมหานคร ๑๐๒๑๐ โทร. ๐๒-๒๕๖๙-๖๖๖๖

ด่วนที่สุด เลขที่รับ ๕๖๔
สภมช ๐๘๑๐/๖๑๕๖๙
วันที่ ๗ เม.ย. ๒๕๖๙
เวลา ๑๓:๓๐ น.

๓ เมษายน ๒๕๖๙

ศาลากลางจังหวัดร้อยเอ็ด
เลขที่รับ 4-556
ลงวันที่ ๗ เม.ย. ๒๕๖๙
โทรสาร โทร. ๐๔๕-๖๑๒๑๑๑ โทรสาร โทร. ๐๔๕-๖๑๒๑๑๑
e-mail: sra@nicsa.or.th

สำนักงานจังหวัดร้อยเอ็ด
เลขที่รับ 2069
ลงวันที่ ๗ เม.ย. ๒๕๖๙
เวลา

เรื่อง แจ้งเตือนกรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak)
เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์กรมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงาน
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
สิ่งที่ส่งมาด้วย เอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์ กรณีข้อมูลส่วนบุคคล
รั่วไหล (Data Leak)

ตามอ้างถึง มาตรา ๔๕ และ มาตรา ๒๒ (๖) สำนักงานคณะกรรมการการรักษาความมั่นคง
ปลอดภัยไซเบอร์แห่งชาติ (สภมช.) มีหน้าที่และอำนาจ “เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์
ติดตามวิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์และการแจ้งเตือนเกี่ยวกับภัยคุกคาม
ทางไซเบอร์” ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ
ทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ นั้น

สภมช. ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวข้อง
กับการรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยพบว่าผู้ข้อมูลบัญชี
ผู้ใช้งานของหน่วยงาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ถูกเผยแพร่ในแหล่งต่าง ๆ
เป็นจำนวนมาก ซึ่งข้อมูลที่รั่วไหลดังกล่าวสามารถถูกนำไปใช้ในการเข้าถึงระบบสารสนเทศ เว็บไซต์ สื่อสังคม
ออนไลน์ หรือแพลตฟอร์มที่เกี่ยวข้องโดยไม่ได้รับอนุญาต และอาจถูกใช้เป็นจุดเริ่มต้นในการเข้าถึงข้อมูล
สำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายภายในระบบเครือข่าย
(Lateral Movement) ของหน่วยงาน ทั้งนี้ สภมช. จึงได้สรุปข้อมูลเกี่ยวกับเหตุการณ์และความเสี่ยง
ที่อาจจะเกิดขึ้นแนวทางการป้องกันและลดกระทบ (รายละเอียดตามสิ่งที่ส่งมาด้วย)

จึงเรียนมาเพื่อโปรดทราบ

ขอแสดงความนับถือ

พลอากาศตรี
(อมร ชมเชย)

เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๔๒ ๖๘๘๕
ไปรษณีย์อิเล็กทรอนิกส์ : thaicert@ncsa.or.th

เอกสารการแจ้งเตือนและแนะนำแนวทางป้องกันความเสี่ยงทางไซเบอร์ กรณีข้อมูลส่วนบุคคลรั่วไหล (Data Leak)

ปัจจุบันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ การรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยพบว่ามีข้อมูลบัญชีผู้ใช้งานของหน่วยงาน เช่น ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ถูกเผยแพร่ในแหล่งต่าง ๆ เป็นจำนวนมาก ซึ่งข้อมูลที่รั่วไหลดังกล่าวสามารถถูกนำไปใช้ในการเข้าถึงระบบสารสนเทศ เว็บไซต์ สื่อสังคมออนไลน์ หรือแพลตฟอร์มที่เกี่ยวข้องโดยไม่ได้รับอนุญาต และอาจถูกใช้เป็นจุดเริ่มต้นในการเข้าถึงข้อมูลสำคัญ การยกระดับสิทธิ์ (Privilege Escalation) หรือการเคลื่อนย้ายภายในระบบเครือข่าย (Lateral Movement) ของหน่วยงาน

จากการเฝ้าระวังและติดตามสถานการณ์ พบว่าการเกิด Data Leak อาจมีสาเหตุมาจากหลายปัจจัย เช่น การโจมตีผ่านห่วงโซ่อุปทาน (Supply Chain Attack) การตั้งค่าระบบหรือเว็บไซต์ที่ไม่ปลอดภัย การขาดมาตรการป้องกันสำหรับระบบที่เปิดให้บริการจากภายนอก การติดมัลแวร์ประเภทขโมยข้อมูล (Infostealer) รวมถึงการรั่วไหลของข้อมูลผ่านระบบเชื่อมต่อ โปรแกรมประยุกต์ หรือผู้ให้บริการภายนอก เช่น การบริหารจัดการ Application Programming Interface (API) หรือการจัดเก็บข้อมูลรับรอง (Credentials) สำหรับการเชื่อมต่อที่ไม่เหมาะสม ซึ่งล้วนเป็นปัจจัยสำคัญที่นำไปสู่การรั่วไหลของข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์กร

นอกจากนี้ ยังพบว่าหลายหน่วยงานมีช่องโหว่ด้านการบริหารจัดการข้อมูลและสิทธิ์การเข้าถึง เช่น การกำหนดสิทธิ์ไม่เหมาะสม การมีบัญชีผู้ใช้งานที่ไม่ได้ใช้งานแต่ยังคงเปิดใช้งานอยู่ การไม่เพิกถอนสิทธิ์เมื่อมีการเปลี่ยนแปลงหน้าที่หรือพ้นสภาพการปฏิบัติงาน รวมถึงการขาดระบบบริหารจัดการบัญชีผู้ใช้งานแบบรวมศูนย์ (Identity and Access Management: IAM) ซึ่งเป็นปัจจัยเสริมที่ทำให้ข้อมูลส่วนบุคคลที่รั่วไหลสามารถถูกนำไปใช้ได้อย่างมีประสิทธิภาพโดยผู้ไม่ประสงค์ดี และเพิ่มความเสี่ยงต่อการละเมิดข้อมูล (Data Breach) ในวงกว้าง

ทั้งนี้ ประเด็นความเสี่ยงสำคัญที่หน่วยงานควรให้ความสำคัญ มีดังนี้

1. ความเสี่ยงด้านการควบคุมบุคลากรและสิทธิ์การเข้าถึง

ทั้งนี้ ในหลายหน่วยงานยังพบปัญหาด้านการบริหารจัดการสิทธิ์การเข้าถึงและบัญชีผู้ใช้งาน ซึ่งอาจก่อให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของระบบสารสนเทศ โดยมีประเด็นสำคัญ ดังนี้

- การกำหนดสิทธิ์การเข้าถึงไม่เหมาะสม หรือให้สิทธิ์เกินความจำเป็นต่อหน้าที่
- การมีบัญชีผู้ใช้งานที่ไม่ได้ใช้งานแต่ยังคงเปิดใช้งานอยู่ (บัญชีค้าง)
- การไม่ปรับสิทธิ์ให้สอดคล้องกับการเปลี่ยนแปลงหน้าที่ความรับผิดชอบ
- การไม่เพิกถอนสิทธิ์โดยทันทีเมื่อบุคลากรพ้นสภาพการปฏิบัติงาน หรือหมดความจำเป็นในการเข้าถึงระบบ
- ความเสี่ยงจากการใช้งานบัญชีโดยไม่เหมาะสมจากบุคลากรภายใน ผู้รับจ้าง ที่ปรึกษา หรือผู้ให้บริการภายนอก
- การขาดการควบคุมและติดตามการใช้งานบัญชีผู้ดูแลระบบหรือบัญชีสิทธิ์ระดับสูงอย่างเพียงพอ

ทั้งนี้ ปัจจัยดังกล่าวอาจส่งผลให้ผู้ไม่ประสงค์ดีสามารถนำบัญชีผู้ใช้งานไปใช้ในการเข้าถึงข้อมูลหรือระบบสำคัญของหน่วยงานโดยไม่ได้รับอนุญาต หรือใช้งานเกินขอบเขตหน้าที่ที่กำหนด

ดังนั้น หน่วยงานควรกำหนดมาตรการควบคุมบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงอย่างเป็นระบบ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- การกำหนดและอนุมัติสิทธิ์เมื่อเริ่มปฏิบัติงาน
- การปรับเปลี่ยนสิทธิ์เมื่อมีการโยกย้ายหรือเปลี่ยนแปลงหน้าที่

- การแยกหน้าที่ความรับผิดชอบที่สำคัญออกจากกัน (Segregation of Duties)
- การควบคุมและติดตามการใช้งานบัญชีสิทธิ์ระดับสูง
- การระงับหรือเพิกถอนสิทธิ์โดยทันทีเมื่อพบสภาพการปฏิบัติงาน
- กำหนดนโยบายรหัสผ่านที่ปลอดภัย เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำ กำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (Password Manager)
- กำหนดกระบวนการเปลี่ยนและกู้คืนรหัสผ่านอย่างปลอดภัย เช่น การยืนยันตัวตนก่อนรีเซ็ตรหัสผ่าน และจำกัดการใช้งานรหัสผ่านเดิม

2. ความเสี่ยงจากการรั่วไหลของข้อมูลและการควบคุมการส่งออกข้อมูลไม่เพียงพอ

นอกจากนี้ สภาพแวดล้อมการใช้งานระบบสารสนเทศในปัจจุบันมีความซับซ้อนและเชื่อมโยงกันหลายระบบ ทำให้มีการรับส่ง จัดเก็บ และใช้งานข้อมูลผ่านหลายช่องทาง ทั้งระบบภายใน ระบบคลาวด์ อีเมล เว็บแอปพลิเคชัน ระบบแชร์ไฟล์ อุปกรณ์พกพา และโปรแกรมเว็บเบราว์เซอร์ หากหน่วยงานขาดมาตรการกำกับดูแลข้อมูลอย่างเหมาะสม อาจส่งผลให้ข้อมูลสำคัญถูกเปิดเผย เข้าถึง ใช้งาน หรือส่งออกไปยังภายนอกโดยไม่ได้รับอนุญาต

โดยความเสี่ยงที่พบบ่อย มีดังนี้

- การกำหนดสิทธิ์เข้าถึงข้อมูลไม่เหมาะสม หรือเปิดให้เข้าถึงกว้างเกินความจำเป็น
- การจัดเก็บข้อมูลสำคัญในระบบหรือพื้นที่ที่ไม่ปลอดภัย
- การรับส่งข้อมูลโดยไม่มี การเข้ารหัส หรือใช้ช่องทางที่ไม่ปลอดภัย
- การใช้งานระบบคลาวด์ อีเมล หรือระบบแชร์ไฟล์ โดยไม่มีมาตรการควบคุมที่เพียงพอ
- การขาดมาตรการควบคุมและเฝ้าระวังการนำข้อมูลออกจากระบบ
- การใช้รหัสผ่านซ้ำ หรือจัดเก็บข้อมูลบัญชี และกุญแจสำหรับเชื่อมต่อระบบในลักษณะที่ไม่เหมาะสม
- ความเสี่ยงจากโปรแกรมเว็บเบราว์เซอร์ เช่น การบันทึกรหัสผ่าน การถูกขโมย session token หรือ cookie และการใช้งานส่วนขยายที่ไม่ปลอดภัย
- การติดตั้งแวร์ประเภทขโมยข้อมูลที่สามารถดึงข้อมูลบัญชีผู้ใช้งานหรือข้อมูลสำคัญจากเครื่องผู้ใช้งาน

ดังนั้น หน่วยงานควรกำหนดมาตรการป้องกันการรั่วไหลของข้อมูลอย่างเป็นระบบ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- จำแนกประเภทข้อมูลตามระดับความสำคัญ (Data Classification) และกำหนดแนวทางการใช้งานข้อมูลอย่างเหมาะสม
- จำกัดสิทธิ์การเข้าถึงข้อมูลตามหน้าที่และความจำเป็น (Least Privilege)
- เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะรับส่ง (Encryption at Rest และ In Transit)
- ควบคุมการใช้งานอีเมล ระบบคลาวด์ ระบบแชร์ไฟล์ และช่องทางรับส่งข้อมูลอื่นอย่างรัดกุม
- หลีกเลี่ยงการจัดเก็บรหัสผ่านหรือข้อมูลรับรองไว้ในเว็บเบราว์เซอร์หรือพื้นที่ที่เข้าถึงได้ง่าย
- ควบคุมการติดตั้งและใช้งานส่วนขยายของเว็บเบราว์เซอร์เท่าที่จำเป็น
- เฝ้าระวัง ตรวจสอบ และควบคุมการนำข้อมูลออกจากระบบ (Data Loss Prevention)
- ตรวจสอบและป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลจากอุปกรณ์ผู้ใช้งานอย่างสม่ำเสมอ

3. ความเสี่ยงจากการตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอกไม่เหมาะสม

ทั้งนี้ ระบบเว็บไซต์ เว็บเซิร์ฟเวอร์ และระบบสารสนเทศที่เปิดให้บริการจากภายนอก มักเป็นเป้าหมายหลักของการโจมตีจากผู้ไม่ประสงค์ดี หากมีการตั้งค่าที่ไม่เหมาะสม หรือขาดการดูแลรักษาความ

มั่นคงปลอดภัยอย่างต่อเนื่อง อาจส่งผลให้เกิดความเสี่ยงต่อการถูกโจมตีและเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยมีประเด็นสำคัญ ดังนี้

- การตั้งค่าระบบไม่เหมาะสม หรือเปิดใช้งานบริการและพอร์ตที่ไม่จำเป็น
- การไม่ปรับปรุงซอฟต์แวร์ ระบบจัดการเนื้อหา (CMS) เฟรมเวิร์ก หรือปลั๊กอินให้เป็นปัจจุบัน
- การขาดมาตรการเสริมความมั่นคงปลอดภัยสำหรับระบบที่เปิดให้บริการจากภายนอก
- การกำหนดสิทธิ์ของบัญชีบริการหรือบัญชีผู้ดูแลระบบไม่เหมาะสม
- ความเสี่ยงจากการถูกโจมตีผ่านช่องทางเว็บ เช่น การสแกนช่องโหว่ การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือการแก้ไขหน้าเว็บไซต์
- การถูกใช้ระบบเป็นช่องทางแพร่กระจายมัลแวร์ หรือขโมยข้อมูลของหน่วยงานและผู้ใช้งาน ทั้งนี้ ความเสี่ยงดังกล่าวอาจส่งผลให้ระบบของหน่วยงานถูกบุกรุก ถูกแก้ไขข้อมูล หรือถูกใช้เป็นจุดเริ่มต้นในการโจมตีระบบภายในของหน่วยงาน ดังนั้น หน่วยงานควรดำเนินการเสริมความมั่นคงปลอดภัยของระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอกอย่างสม่ำเสมอ โดยครอบคลุมประเด็นสำคัญ ดังนี้

- ปิดบริการหรือพอร์ตที่ไม่จำเป็น และจำกัดการเข้าถึงเฉพาะที่จำเป็น
- ปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสม (Secure Configuration)
- อัปเดตซอฟต์แวร์ ระบบจัดการเนื้อหา เฟรมเวิร์ก และส่วนประกอบที่เกี่ยวข้องให้เป็นปัจจุบันอยู่เสมอ
- จำกัดสิทธิ์ของบัญชีบริการและบัญชีผู้ดูแลระบบตามหลักความจำเป็น
- แยกส่วนระบบที่เปิดบริการภายนอกออกจากระบบภายใน (Network Segmentation)
- ทดสอบใช้มาตรการป้องกันการโจมตีผ่านช่องทางเว็บ เช่น Web Application Firewall (WAF) หรือมาตรการที่เทียบเท่า

4. ความเสี่ยงจากการรั่วไหลผ่านระบบเชื่อมต่อและ API

จากการเฝ้าระวังและติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ พบว่าการรั่วไหลของบัญชีผู้ใช้งานอาจเกิดจากความเสี่ยงของระบบเชื่อมต่อและการใช้งาน Application Programming Interface (API) ซึ่งใช้ในการแลกเปลี่ยนข้อมูลระหว่างระบบทั้งภายในและภายนอกหน่วยงาน โดยมีประเด็นสำคัญ ดังนี้

- การกำหนดสิทธิ์การเข้าถึง API ไม่เหมาะสม หรือให้สิทธิ์เกินความจำเป็น
- การจัดเก็บข้อมูลรับรองสำหรับการเชื่อมต่อ เช่น API key, access token, secret key หรือบัญชีบริการ ในลักษณะที่ไม่ปลอดภัย
- การเปิดเผยข้อมูลรับรองในซอร์สโค้ด ไฟล์ตั้งค่า หรือระบบที่สามารถเข้าถึงได้โดยไม่จำเป็น
- การขาดการควบคุมและจำกัดการเข้าถึงระบบเชื่อมต่อกับผู้ให้บริการภายนอกหรือระบบคู่สัญญา
- การขาดการเฝ้าระวังการใช้งาน API ทำให้ไม่สามารถตรวจจับพฤติกรรมผิดปกติได้
- ความเสี่ยงจากการนำข้อมูลรับรองไปใช้เชื่อมต่อระบบ เข้าถึงข้อมูล หรือส่งการผ่าน API โดยไม่ได้รับอนุญาต

ทั้งนี้ ความเสี่ยงดังกล่าวอาจส่งผลให้เกิดการเข้าถึงข้อมูลสำคัญ การใช้สิทธิ์เกินขอบเขต หรือการโจมตีระบบผ่านช่องทางการเชื่อมต่อระหว่างระบบ ดังนั้น หน่วยงานควรกำหนดมาตรการควบคุมความมั่นคงปลอดภัยของระบบเชื่อมต่อและ API อย่างเหมาะสม โดยครอบคลุมประเด็นสำคัญ ดังนี้

- กำหนดสิทธิ์การเข้าถึง API ตามหลักความจำเป็น (Least Privilege)
- จัดเก็บ API key, token และข้อมูลรับรองในรูปแบบที่ปลอดภัย และหลีกเลี่ยงการฝังไว้ในซอร์สโค้ด

- ใช้กลไกการยืนยันตัวตนและการอนุญาตที่เหมาะสมสำหรับการเชื่อมต่อระหว่างระบบ
- จำกัดการเข้าถึง API ตามแหล่งที่มา เช่น IP address หรือ network ที่เชื่อถือได้
- เฝ้าระวังและตรวจสอบการใช้งาน API อย่างต่อเนื่อง เพื่อป้องกันและตรวจจับพฤติกรรมที่ผิดปกติ
- ทบทวนและยกเลิกข้อมูลรับรองหรือสิทธิ์การเข้าถึงที่ไม่จำเป็นอย่างสม่ำเสมอ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงขอให้หน่วยงานในประเทศไทยยกระดับการเฝ้าระวังและติดตามสถานการณ์ภัยคุกคามทางไซเบอร์อย่างใกล้ชิด โดยเฉพาะภัยคุกคามที่เกี่ยวข้องกับบัญชีผู้ใช้งาน ระบบที่เปิดให้บริการจากภายนอก การเชื่อมต่อกับระบบหรือผู้ให้บริการภายนอก และความเสี่ยงจากการรั่วไหลของข้อมูล ซึ่งถือเป็นปัจจัยสำคัญที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลสำคัญของหน่วยงานโดยรวม

แนวทางป้องกันและลดความเสี่ยงเบื้องต้น

จากการวิเคราะห์ประเด็นความเสี่ยงด้านการควบคุมบุคลากรและสิทธิ์การเข้าถึง การรั่วไหลของข้อมูล การตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอก รวมถึงความเสี่ยงจากระบบเชื่อมต่อและการแลกเปลี่ยนข้อมูลระหว่างระบบ หน่วยงานควรดำเนินการป้องกันและลดความเสี่ยงอย่างเป็นระบบ ครอบคลุมทั้งด้านเทคโนโลยี กระบวนการ และบุคลากร เพื่อป้องกันการนำข้อมูลบัญชีผู้ใช้งานไปใช้โดยมิชอบ และลดผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศของหน่วยงาน

ทั้งนี้ สามารถดำเนินการได้ ดังนี้

1. ดำเนินการตรวจสอบและปิดช่องโหว่ของระบบสารสนเทศอย่างเร่งด่วน โดยเฉพาะระบบเว็บไซต์และบริการที่เปิดให้เข้าถึงจากภายนอก รวมถึงปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสม ปิดบริการหรือพอร์ตที่ไม่จำเป็น และกำหนดมาตรการป้องกันการโจมตีผ่านช่องทางเว็บอย่างเหมาะสม

2. สำรองข้อมูลอย่างน้อย 3 ชุด และจัดเก็บข้อมูลสำรองในลักษณะที่แยกออกจากระบบหลัก รวมถึงมีการสำรองแบบออฟไลน์ เพื่อรองรับกรณีระบบถูกโจมตีหรือเกิดเหตุขัดข้องที่กระทบต่อความต่อเนื่องในการให้บริการ

3. ตรวจสอบการเข้าถึงระบบจากระยะไกล เช่น Remote Desktop Protocol (RDP) และ Virtual Private Network (VPN) พร้อมเฝ้าระวังพฤติกรรมการใช้งานที่ผิดปกติ และกำหนดมาตรการยืนยันตัวตนที่เหมาะสมสำหรับการเข้าถึงจากภายนอก

4. บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับระบบสำคัญ ระบบที่เปิดให้บริการจากภายนอก และบัญชีผู้ใช้งานที่มีสิทธิ์ระดับสูง พร้อมกำหนดรหัสผ่านให้มีความซับซ้อนและยากต่อการคาดเดา และควรกำหนดนโยบายรหัสผ่าน เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำ กำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (Password Manager)

5. อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ อุปกรณ์ และส่วนประกอบของระบบต่าง ๆ ให้เป็นปัจจุบัน อยู่เสมอ โดยเฉพาะระบบที่เชื่อมต่อกับเครือข่ายภายนอก ระบบเว็บไซต์ ระบบจัดการเนื้อหา และซอฟต์แวร์ที่มีความเสี่ยงสูง

6. ติดตั้งและปรับปรุงระบบป้องกันมัลแวร์ให้มีความทันสมัยอยู่เสมอ โดยเฉพาะการป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลบัญชีผู้ใช้งาน ข้อมูลรับรองสำหรับเชื่อมต่อระบบ และข้อมูลสำคัญอื่นของหน่วยงาน

7. ตรวจสอบอุปกรณ์ของผู้ใช้งาน โดยเฉพาะกรณีการปฏิบัติงานจากภายนอกหน่วยงาน อุปกรณ์ของผู้ดูแลระบบ และอุปกรณ์ที่ใช้เข้าถึงระบบสำคัญ เพื่อให้มั่นใจว่ามีมาตรการป้องกันที่เหมาะสม และไม่ตกอยู่ในภาวะเสี่ยงต่อการรั่วไหลของข้อมูล

8. เผื่อระวังและวิเคราะห์บันทึกการใช้งานระบบ (Log) อย่างต่อเนื่อง และนำข้อมูลที่เกี่ยวข้องกับภัยคุกคามมาใช้ในการตรวจจับและป้องกัน โดยเฉพาะความผิดปกติของการเข้าสู่ระบบ การเรียกใช้งานระบบจากตำแหน่งที่ไม่คุ้นเคย การใช้งานบัญชีสิทธิ์สูง และการเข้าถึงข้อมูลสำคัญที่ผิดไปจากปกติ

9. ตรวจสอบและควบคุมการเข้าถึงของระบบหรือผู้ให้บริการภายนอกอย่างรัดกุม รวมถึงกำหนดสิทธิ์การเข้าถึงสำหรับระบบเชื่อมต่อ โปรแกรมประยุกต์ และ Application Programming Interface (API) ตามความจำเป็น จัดเก็บข้อมูลรับรอง คุกกี้ และโทเคนสำหรับการเชื่อมต่ออย่างปลอดภัย และเผื่อระวังการใช้งานที่ผิดปกติอย่างสม่ำเสมอ

10. จัดให้มีระบบบริหารจัดการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงแบบรวมศูนย์ เพื่อควบคุมวงจรชีวิตบัญชีผู้ใช้งานอย่างเป็นระบบ ครอบคลุมการสร้าง การแก้ไข การระงับ และการยกเลิกบัญชี รวมถึงการเพิกถอนสิทธิ์ทันทีเมื่อมีการเปลี่ยนแปลงหน้าที่หรือพื้นสภาพการปฏิบัติงาน รวมถึงกำหนดกระบวนการยืนยันตัวตน (Identity Proofing) สำหรับการสร้างบัญชี การกู้คืนบัญชี และการเปลี่ยนแปลงข้อมูลสำคัญ เพื่อป้องกันการแอบอ้างตัวตน

11. ควบคุมการกำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็นของการปฏิบัติงาน พร้อมทบทวนสิทธิ์ของผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องภายนอกเป็นระยะ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบเกินความจำเป็น รวมทั้งลดความเสี่ยงจากการใช้งานโดยไม่เหมาะสมจากบุคคลากรภายใน

12. กำหนดมาตรการป้องกันข้อมูลรั่วไหลอย่างเหมาะสม โดยจำแนกประเภทข้อมูลสำคัญ จำกัดการเข้าถึงตามระดับความจำเป็น เข้มงวดข้อมูลทั้งหมดที่จัดเก็บและขณะรับส่ง และควบคุมการส่งออกข้อมูลผ่านระบบอีเมล เว็บแอปพลิเคชัน ระบบคลาวด์ และอุปกรณ์พกพา เพื่อป้องกันการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต รวมถึงควบคุมการใช้งานข้อมูลผ่านเว็บเบราว์เซอร์ และป้องกันการจัดเก็บข้อมูลรับรองในลักษณะที่ไม่ปลอดภัย

13. จัดให้มีการทดสอบความมั่นคงปลอดภัยของระบบอย่างสม่ำเสมอ เช่น การประเมินช่องโหว่ การทดสอบเจาะระบบ และการตรวจสอบความมั่นคงปลอดภัยของเว็บไซต์ ระบบเชื่อมต่อ และบริการภายนอก เพื่อค้นหาและลดความเสี่ยงก่อนเกิดเหตุการณ์จริง รวมถึงกำหนดมาตรการควบคุมการใช้งาน session เช่น การกำหนดระยะเวลาหมดอายุของ session และการยกเลิก session เมื่อพบพฤติกรรมผิดปกติ

14. สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้อง โดยให้ความรู้เกี่ยวกับการตั้งรหัสผ่านอย่างปลอดภัย การใช้งาน MFA การระวังภัยจากการหลอกลวงทางอิเล็กทรอนิกส์ การดูแลข้อมูลรับรองสำหรับเชื่อมต่อระบบ และแนวทางการปฏิบัติที่ปลอดภัยในการใช้งานระบบสารสนเทศของหน่วยงาน

คำแนะนำทั่วไปสำหรับกรณีนี้

1. ให้ตรวจสอบข้อมูลตามที่ปรากฏบนหน้าเว็บข้อมูลคอมพิวเตอร์ในระบบข้อมูล log file และพฤติกรรมแวดล้อมในระบบ เพื่อประเมินว่ามีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นให้ดำเนินการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ดังกล่าว ตาม พ.ร.บ. ไซเบอร์ฯ หรือแนวทางด้าน cybersecurity เช่น NIST Cybersecurity Framework^[2] เป็นต้น ทั้งนี้ สกมช. ยินดีให้การสนับสนุนในการดำเนินการดังกล่าว

2. หากเกิดความเสียหาย ควรดำเนินการแจ้งความกับหน่วยงานบังคับใช้กฎหมายในทันที เช่น บช.สอท. ตั้งอยู่ภายในเมืองทองธานี จว.นนทบุรี หรือสถานีตำรวจในพื้นที่ เพื่อจะได้เป็นการแจ้งเหตุการณ์กระทำผิดทางอาญาในฐานะผู้เสียหาย และเริ่มกระบวนการตรวจพิสูจน์ได้อย่างถูกต้องตามกฎหมาย

3. ดำเนินการตรวจสอบข้อมูลต่าง ๆ เช่น ข้อมูลส่วนบุคคล ข้อมูลที่มีความละเอียดอ่อนที่ถูกทำให้เผยแพร่ไป โดยได้อ้างว่าเป็นของหน่วยงานหรือบุคคลอื่น เพื่อพิจารณาแนวทางป้องกันและรับมือกับข้อกฎหมายและความเสียหายที่อาจจะเกิดขึ้น

4. ในการดำเนินการเรื่องรับมือและตอบสนองเหตุการณ์ดังกล่าว นอกจากการกู้คืนระบบให้สามารถทำงานได้ตามปกติโดยเร็วแล้ว ควรจะดำเนินการหาสาเหตุและแหล่งที่มาของภัยคุกคามที่แท้จริงสามารถระบุร่องรอยได้ตามพยานหลักฐานที่ปรากฏได้อย่างชัดเจน ทั้งนี้ เพื่อเป็นการตรวจหาภัยคุกคามที่ยังคงแฝงอยู่ในระบบและเป็นการป้องกันไม่ให้เกิดเหตุซ้ำจากช่องโหว่ที่มีอยู่ในระบบ

5. ดำเนินการตรวจสอบข้อมูลส่วนบุคคลที่หน่วยงานได้เผยแพร่บนเว็บไซต์ให้เหมาะสมและสอดคล้องตามที่ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ในส่วนที่เกี่ยวกับการเก็บรวบรวมการใช้ และการเปิดเผยข้อมูลส่วนบุคคลที่กำหนด เนื่องจากการเปิดเผยข้อมูลส่วนบุคคลบางข้อมูลบนหน้าเว็บไซต์อาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลนั้นได้ เช่น เลขที่บัตรประจำตัวประชาชน เบอร์โทรศัพท์ หรือที่อยู่ เป็นต้น หากหน่วยงานพิจารณาแล้วปรากฏว่า ข้อมูลส่วนบุคคลใดไม่จำเป็นต้องเผยแพร่และเป็นข้อมูลที่หากเผยแพร่แล้วอาจก่อให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคลให้หน่วยงานดำเนินการเผยแพร่ข้อมูลเท่าที่จำเป็นตามที่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคลเท่านั้น กรณีหน่วยงานจำเป็นต้องเผยแพร่ข้อมูลส่วนบุคคลดังกล่าว ให้หน่วยงานดำเนินการกำหนดสิทธิในการเข้าถึงข้อมูลส่วนบุคคลหรือดำเนินการอื่นใด เพื่อเป็นการป้องกันไม่ให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคลได้อีกทั้งเป็นการลดความเสี่ยงจากการละเมิดข้อมูลส่วนบุคคลนั้นด้วย

อนึ่ง หากหน่วยงานมิได้ดำเนินการให้สอดคล้องและเป็นไปตามที่พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 กำหนด อาจถือได้ว่าเป็นการฝ่าฝืนหรือไม่ปฏิบัติ อันอาจมีความรับผิดชอบทางแพ่งทางอาญา หรือทางปกครองตามที่พระราชบัญญัติดังกล่าวกำหนดไว้

ข้อกฎหมายที่เกี่ยวข้อง

พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา ๔๕ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้าง พื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละ หน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรา 58⁽¹⁾ กรณีเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศ ในการดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน เพื่อประเมินภัยคุกคาม ดำเนินการป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามตามแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งมายังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37 (4)⁽²⁾ กรณีแจ้งเหตุการณ์ละเมิดข้อมูลส่วนบุคคลแก่สำนักงานคุ้มครองข้อมูลส่วนบุคคลโดยไม่ชักช้าภายใน 72 ชั่วโมง นับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้ เว้นแต่การละเมิดดังกล่าวไม่มีความเสี่ยงที่จะมีผลกระทบต่อ สิทธิและเสรีภาพของบุคคล ในกรณีที่การละเมิดมีความเสี่ยงสูงที่จะมีผลกระทบต่อสิทธิและเสรีภาพ ของบุคคล ให้แจ้งเหตุการณ์ละเมิดให้เจ้าของข้อมูลส่วนบุคคลทราบพร้อมกับแนวทางการเยียวยา โดยไม่ชักช้า ทั้งนี้ ได้มีกำหนดโทษตามพระราชบัญญัตินี้ ดังนี้

- 1) ความรับผิดชอบทางแพ่ง บัญญัติไว้ในมาตรา 77 ถึงมาตรา 78
- 2) โทษอาญา บัญญัติไว้ในมาตรา 79 ถึงมาตรา 81
- 3) โทษทางปกครอง บัญญัติไว้ในมาตรา 82 ถึงมาตรา 90



ทั้งนี้ ขอให้หน่วยงานติดตามสถานการณ์ภัยคุกคามทางไซเบอร์จากแหล่งข้อมูลที่เกี่ยวข้องอย่างต่อเนื่อง และดำเนินการด้านความมั่นคงปลอดภัยอย่างเคร่งครัด เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นต่อระบบสารสนเทศ ข้อมูลสำคัญ และการให้บริการของหน่วยงาน

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งานและผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ <https://webboard-nsoc.ncsa.or.th/> หรือ Scan QR Code



<https://webboard-nsoc.ncsa.or.th/>

อ้างอิง

1. <https://drive.ncsa.or.th/s/XtCz2kFkcwkaz9Y>
2. <https://ratchakitcha.soc.go.th/documents/17082307.pdf>

