

สำนักงานเขตพื้นที่การศึกษา
ประถมศึกษานครสวรรค์ เขต ๓
เลขที่รับ ๒๙/๒๕๖๙
วันที่ 14 ตุลาคม 25๖๙
เวลา 14.๒๐ น.

ลับมาก



สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
กระทรวงศึกษาธิการ กทม. ๑๐๓๐๐

๑๔ ตุลาคม ๒๕๖๙

ด่วนที่สุด

ที่ ศธ ๐๔๐๐๕/๖๔๒๔

เรื่อง ดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล
เรียน ผู้อำนวยการสำนักงานเขตพื้นที่การศึกษา

สิ่งที่ส่งมาด้วย มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล จำนวน ๑ ชุด

ด้วยสำนักงานปลัดกระทรวงศึกษาธิการ แจ้งให้หน่วยงานในสังกัดและองค์กรในกำกับดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้มีมติเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับการยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication : MFA) เช่น การใช้ Digital Identity (ThalD) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย เป็นต้น ทั้งนี้ ในส่วนของมาตรการเร่งด่วนขอให้ทุกหน่วยงานถือปฏิบัติในการเปลี่ยนรหัสผ่านเป็นประจำ ตลอดจนระงับบัญชีที่ไม่มีความจำเป็น และทบทวนสิทธิ์การเข้าถึงอย่างเคร่งครัด

ในการนี้ สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ขอให้สำนักงานเขตพื้นที่การศึกษา ดำเนินการและแจ้งสถานศึกษาในสังกัด ดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล เพื่อป้องกันภัยคุกคามทางไซเบอร์และคุ้มครองข้อมูลส่วนบุคคล มิให้รั่วไหลจากระบบงานภายในหน่วยงาน รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อทราบและดำเนินการในส่วนที่เกี่ยวข้องอย่างเคร่งครัด

ขอแสดงความนับถือ

(นางชาติทยา บุญญา)

ผู้อำนวยการศูนย์การศึกษานานาชาติขั้นพื้นฐาน ปฏิบัติราชการแทน
เลขาธิการคณะกรรมการการศึกษาขั้นพื้นฐาน

สำนักเทคโนโลยีเพื่อการเรียนการสอน
กลุ่มบริการเทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๒๘๘ ๕๙๐๖

ลับมาก

มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์

และมาตรการคุ้มครองข้อมูลส่วนบุคคล

ปัจจุบันภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับ การรั่วไหลของข้อมูลส่วนบุคคล (Data Leak) มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่อง โดยพบว่าข้อมูลบัญชีผู้ใช้งานของหน่วยงาน เช่น ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (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 การติดตั้งแวร์ประเภทสปายแวร์ (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

ประเด็นความเสี่ยงสำคัญที่หน่วยงานควรให้ความสำคัญ มีดังนี้

๑. 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
- การระงับหรือเพิกถอนสิทธิ์โดยทันทีเมื่อพ้นสภาพการปฏิบัติงาน
- กำหนดนโยบายรหัสผ่านที่ปลอดภัย เช่น หลีกเลี่ยงการใช้รหัสผ่านซ้ำ กำหนดรายการรหัสผ่านต้องห้าม (Blacklist) และส่งเสริมการใช้เครื่องมือจัดการรหัสผ่าน (Password Manager)
- กำหนดกระบวนการเปลี่ยนและกู้คืนรหัสผ่านอย่างปลอดภัย เช่น การยืนยันตัวตนก่อนรีเซ็ตรหัสผ่าน และจำกัดการใช้งานรหัสผ่านเดิม

๒. ความเสี่ยงจากการรั่วไหลของข้อมูลและการควบคุมการส่งออกข้อมูลไม่เพียงพอ

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

โดยความเสี่ยงที่พบบ่อย มีดังนี้

- การกำหนดสิทธิ์เข้าถึงข้อมูลไม่เหมาะสม หรือเปิดให้เข้าถึงกว้างเกินความจำเป็น
- การจัดเก็บข้อมูลสำคัญในระบบหรือพื้นที่ที่ไม่ปลอดภัย
- การรับส่งข้อมูลโดยไม่มีการเข้ารหัส หรือใช้ช่องทางที่ไม่ปลอดภัย
- การใช้งานระบบคลาวด์ อีเมล หรือระบบแชร์ไฟล์ โดยไม่มีมาตรการควบคุมที่เพียงพอ
- การขาดมาตรการควบคุมและเฝ้าระวังการนำข้อมูลออกจากระบบ
- การใช้รหัสผ่านซ้ำ หรือจัดเก็บข้อมูลบัญชีและกุญแจสำหรับเชื่อมต่อระบบในลักษณะที่ไม่เหมาะสม
- ความเสี่ยงจากโปรแกรมเว็บเบราว์เซอร์ เช่น การบันทึกรหัสผ่าน การถูกขโมย session token หรือ cookie และการใช้งานส่วนขยายที่ไม่ปลอดภัย
- การคิดมัลแวร์ประเภทขโมยข้อมูลที่สามารถดึงข้อมูลบัญชีผู้ใช้งานหรือข้อมูลสำคัญจากเครื่องผู้ใช้งาน

ดังนั้น หน่วยงานควรกำหนดมาตรการป้องกันการรั่วไหลของข้อมูลอย่างเป็นระบบ โดยครอบคลุมประเด็นสำคัญ ดังนี้

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

๓. ความเสี่ยงจากการตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอกไม่เหมาะสม

ทั้งนี้ ระบบเว็บไซต์ เว็บเซิร์ฟเวอร์ และระบบสารสนเทศที่เปิดให้บริการจากภายนอก มักเป็นเป้าหมายหลักของการโจมตีจากผู้ไม่ประสงค์ หากมีการตั้งค่าที่ไม่เหมาะสม หรือขาดการดูแลรักษาความมั่นคงปลอดภัยอย่างต่อเนื่อง 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)
- พิจารณาใช้มาตรการป้องกันการโจมตีผ่านช่องทางเว็บ เช่น Web Application Firewall (WAF) หรือมาตรการที่เทียบเท่า

๔. ความเสี่ยงจากการรั่วไหลผ่านระบบเชื่อมต่อและ API

จากการเฝ้าระวังและติดตามสถานการณ์ภัยคุกคามทางไซเบอร์ พบว่าการรั่วไหลของบัญชีผู้ใช้งานอาจเกิดจากความเสี่ยงของระบบเชื่อมต่อและการทำงาน Application Programming Interface (API) ซึ่งใช้ในการแลกเปลี่ยนข้อมูลระหว่างระบบทั้งภายในและภายนอกหน่วยงาน โดยมีประเด็นสำคัญ ดังนี้

- การกำหนดสิทธิ์การเข้าถึง API ไม่เหมาะสม หรือให้สิทธิ์เกินความจำเป็น
- การจัดเก็บข้อมูลรับรองสำหรับการเชื่อมต่อ เช่น API key, access token, secret key หรือ บัญชีบริการ ในลักษณะที่ไม่ปลอดภัย
- การเปิดเผยข้อมูลรับรองในซอร์สโค้ด ไฟล์ตั้งค่า หรือระบบที่สามารถเข้าถึงได้โดยไม่จำเป็น
- การขาดการควบคุมและจำกัดการเข้าถึงระบบเชื่อมต่อกับผู้ให้บริการภายนอกหรือระบบคู่สัญญา
- การขาดการเฝ้าระวังการใช้งาน API ทำให้ไม่สามารถตรวจจับพฤติกรรมผิดปกติได้
- ความเสี่ยงจากการนำข้อมูลรับรองไปใช้เชื่อมต่อบนเข้าถึงข้อมูล 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

แนวทางการดำเนินการตามมาตรการ

จากการวิเคราะห์ประเด็นความเสี่ยงด้านการควบคุมบุคลากรและสิทธิ์การเข้าถึง การรั่วไหลของข้อมูล การตั้งค่าระบบเว็บไซต์และระบบที่เปิดให้บริการจากภายนอก รวมถึงความเสี่ยงจากระบบเชื่อมต่อและการแลกเปลี่ยนข้อมูลระหว่างระบบ หน่วยงานควรดำเนินการป้องกันและลดความเสี่ยงอย่างเป็นระบบ ครอบคลุมทั้งด้านเทคโนโลยี กระบวนการ และบุคลากร เพื่อป้องกันการนำข้อมูลบัญชีผู้ใช้งานไปใช้โดยมิชอบ และลดผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศของหน่วยงาน สามารถดำเนินการได้ ดังนี้

๑. ดำเนินการตรวจสอบและปิดช่องโหว่ของระบบสารสนเทศอย่างเร่งด่วน โดยเฉพาะระบบเว็บไซต์และบริการที่เปิดให้เข้าถึงจากภายนอก รวมถึงปรับแต่งค่าความมั่นคงปลอดภัยของระบบให้เหมาะสม ปิดบริการหรือพอร์ตที่ไม่จำเป็น และกำหนดมาตรการป้องกันการโจมตีผ่านช่องทางเว็บอย่างเหมาะสม

๒. สำรองข้อมูลอย่างน้อย ๓ ชุด และจัดเก็บข้อมูลสำรองในลักษณะที่แยกออกจากระบบหลัก รวมถึงมีการสำรองแบบออฟไลน์ เพื่อรองรับกรณีระบบถูกโจมตีหรือเกิดเหตุขัดข้องที่กระทบต่อความต่อเนื่องในการให้บริการ

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

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

๕. อัปเดตระบบปฏิบัติการ ซอฟต์แวร์ อุปกรณ์ และส่วนประกอบของระบบต่าง ๆ ให้เป็นปัจจุบันอยู่เสมอ โดยเฉพาะระบบที่เชื่อมต่อกับเครือข่ายภายนอก ระบบเว็บไซต์ ระบบจัดการเนื้อหา และซอฟต์แวร์ที่มีความเสี่ยงสูง

๖. ติดตั้งและปรับปรุงระบบป้องกันมัลแวร์ให้มีความทันสมัยอยู่เสมอ โดยเฉพาะการป้องกันมัลแวร์ที่มุ่งขโมยข้อมูลบัญชีผู้ใช้งาน ข้อมูลรับรองสำหรับเชื่อมต่อระบบ และข้อมูลสำคัญอื่นของหน่วยงาน

๗. ตรวจสอบอุปกรณ์ของผู้ใช้งาน โดยเฉพาะกรณีการปฏิบัติงานจากภายนอกหน่วยงาน อุปกรณ์ของผู้ดูแลระบบ และอุปกรณ์ที่ใช้เข้าถึงระบบสำคัญ เพื่อให้มั่นใจว่ามีมาตรการป้องกันที่เหมาะสม และไม่ตกอยู่ในภาวะเสี่ยงต่อการรั่วไหลของข้อมูล

๘. เฝ้าระวังและวิเคราะห์บันทึกการใช้งานระบบ (Log) อย่างต่อเนื่อง และนำข้อมูลที่เกี่ยวข้องกับภัยคุกคามมาใช้ในการตรวจจับและป้องกัน โดยเฉพาะความผิดปกติของการเข้าสู่ระบบ การเรียกใช้งานระบบจากตำแหน่งที่ไม่คุ้นเคย การใช้งานบัญชีสิทธิ์สูง และการเข้าถึงข้อมูลสำคัญที่ผิดไปจากปกติ

๙. ตรวจสอบและควบคุมการเข้าถึงของระบบหรือผู้ให้บริการภายนอกอย่างรัดกุม รวมถึงกำหนดสิทธิ์การเข้าถึงสำหรับระบบเชื่อมต่อ โปรแกรมประยุกต์ และ Application Programming Interface (API) ตามความจำเป็น จัดเก็บข้อมูลรับรอง กุญแจลับ และโทเคนสำหรับการเชื่อมต่ออย่างปลอดภัย และเฝ้าระวังการใช้งานที่ผิดปกติอย่างสม่ำเสมอ

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

๑๑. ควบคุมการกำหนดสิทธิ์การเข้าถึงตามหน้าที่และความจำเป็นของการปฏิบัติงาน พร้อมทบทวนสิทธิ์ของผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องภายนอกเป็นระยะ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบเกินความจำเป็น รวมทั้งลดความเสี่ยงจากการใช้งานโดยไม่เหมาะสมจากบุคลากรภายใน

๑๒. กำหนดมาตรการป้องกันข้อมูลรั่วไหลอย่างเหมาะสม โดยจำแนกประเภทข้อมูลสำคัญ จำกัดการเข้าถึงตามระดับความจำเป็น เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะรับส่ง และควบคุมการส่งออกข้อมูลผ่านระบบอีเมล เว็บแอปพลิเคชัน ระบบคลาวด์ และอุปกรณ์พกพา เพื่อป้องกันการนำข้อมูลออกจากระบบโดยไม่ได้รับอนุญาต รวมถึงควบคุมการใช้งานข้อมูลผ่านเว็บเบราว์เซอร์ และป้องกันการจัดเก็บข้อมูลรับรองในลักษณะที่ไม่ปลอดภัย

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

๑๔. สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้อง โดยให้ความรู้เกี่ยวกับการตั้งรหัสผ่านอย่างปลอดภัย การใช้งาน MFA การระวังภัยจากการหลอกลวงทางอิเล็กทรอนิกส์ การดูแลข้อมูลรับรองสำหรับเชื่อมต่อระบบ และแนวทางการปฏิบัติที่ปลอดภัยในการใช้งานระบบสารสนเทศของหน่วยงาน

๑๕. เมื่อพบหรือสงสัยว่ารหัสผ่านรั่วไหลให้แจ้งให้ผู้ใช้งานเปลี่ยนทันทีโดยใช้รหัสผ่านใหม่ที่ปลอดภัย ไม่ให้ใช้รหัสผ่านเดิม

ลับมาก



ปลัดกระทรวงศึกษาธิการ
รับ 562 คืบ
วันที่ 10 ส.ค. 2569
เวลา 00.02 น.

กระทรวงศึกษาธิการ
เลขรับ ก. 210
วันที่ 7 ส.ค. 2569
เวลา 15.28

อ. ก. 5

ด่วนที่สุด

ที่ ดศ ๐๒๐๖/ว ๒๓๘๖

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๒๕๖๒-๒๕๖๓ สป.

อาคารซี ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐

วันที่ 13 ส.ค. ๕๙

เวลา 09.55 น.

๗ สิงหาคม ๒๕๖๙

- เรื่อง ขอให้พิจารณาสั่งการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล
- เรียน รายชื่อแนบ
- อ้างอิง ๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
๒. พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
๓. พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๐
๔. มติคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการประชุมครั้งที่ ๑/๒๕๖๙ เมื่อวันที่ ๒๕ พฤษภาคม ๒๕๖๙

สิ่งที่ส่งมาด้วย มาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล

ด้วยเหตุการณภัยคุกคามทางไซเบอร์และข้อมูลรั่วไหลที่เกิดขึ้นกับหน่วยงานภาครัฐต่างๆ โดยผู้โจมตีนำข้อมูลบัญชีผู้ใช้งาน (Credential) สำหรับการยืนยันตัวตน และใช้เข้าถึงช่องทางเครือข่ายของระบบภายในของหน่วยงานภาครัฐ เช่น Application Programming Interface (API) การโจมตีโดยใช้รหัสผ่านที่หลุดรั่ว (Compromised Credential Attack) และการโจมตีด้วยมัลแวร์ (Malware) หรือ มัลแวร์เรียกค่าไถ่ (Ransomware) โดยผู้โจมตีสามารถเข้าถึงข้อมูลต่างๆ ของหน่วยงาน รวมถึงข้อมูลส่วนบุคคล และพบว่าถูกนำไปซื้อขายบนแหล่งต่างๆ อาทิ ดาร์กเว็บ (Dark Web) และ เว็บไซต์บรีชฟอรัมส์ (Breach Forum) ส่งผลกระทบให้เกิดความเสียหายต่อหน่วยงานภาครัฐและประชาชน

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมพิจารณาแล้วขอเรียนว่า เพื่อเป็นการยกระดับการป้องกันไม่ใหหน่วยงานภาครัฐถูกโจมตีระบบ ข้อมูลบัญชีผู้ใช้งาน (Credential) ถูกขโมย และป้องกันข้อมูลส่วนบุคคลรั่วไหล จึงขอให้ท่านพิจารณาสั่งการหน่วยงานภายใต้สังกัดของท่าน (ส่วนราชการระดับกรม รัฐวิสาหกิจ องค์การมหาชน และอื่นๆ) ในการดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมาตรการคุ้มครองข้อมูลส่วนบุคคล ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ได้มีมติเห็นชอบแนวทางการป้องกันข้อมูลส่วนบุคคลรั่วไหลจากเหตุบัญชีผู้ใช้งานสำหรับยืนยันตัวตน (Credential) รั่วไหล ด้วยมาตรการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เช่น การใช้ Digital Identity (ThalID) หรือวิธีการยืนยันตัวตนในรูปแบบอื่นที่มีความมั่นคงปลอดภัย เป็นต้น ทั้งนี้ ในส่วนของมาตรการเร่งด่วนขอให้ท่านสั่งการให้ทุกหน่วยงานถือปฏิบัติในการเปลี่ยนรหัสผ่านเป็นประจำ ตลอดจนระงับบัญชีที่ไม่มีความจำเป็น และทบทวนสิทธิ์การเข้าถึงอย่างเคร่งครัด (สิ่งที่ส่งมาด้วย) โดยประสานงาน

กับสำนักงาน ...

ลับมาก

ลับมาก

รายชื่อแนบ

๑. ปลัดสำนักนายกรัฐมนตรี
๒. ปลัดกระทรวงกลาโหม
๓. ปลัดกระทรวงการคลัง
๔. ปลัดกระทรวงการต่างประเทศ
๕. ปลัดกระทรวงการท่องเที่ยวและกีฬา
๖. ปลัดกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
๗. ปลัดกระทรวงเกษตรและสหกรณ์
๘. ปลัดกระทรวงคมนาคม
๙. ปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม
๑๐. ปลัดกระทรวงพลังงาน
๑๑. ปลัดกระทรวงพาณิชย์
๑๒. ปลัดกระทรวงมหาดไทย
๑๓. ปลัดกระทรวงยุติธรรม
๑๔. ปลัดกระทรวงแรงงาน
๑๕. ปลัดกระทรวงวัฒนธรรม
๑๖. ปลัดกระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม
๑๗. ปลัดกระทรวงศึกษาธิการ ✓
๑๘. ปลัดกระทรวงสาธารณสุข
๑๙. ปลัดกระทรวงอุตสาหกรรม
๒๐. ผู้บัญชาการตำรวจแห่งชาติ
๒๑. เลขาธิการคณะกรรมการการเลือกตั้ง
๒๒. เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ
๒๓. ผู้ว่าการตรวจเงินแผ่นดิน
๒๔. เลขาธิการสภาผู้แทนราษฎร
๒๕. เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน
๒๖. ปลัดกรุงเทพมหานคร
๒๗. ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
๒๘. เลขาธิการสำนักงานศาลรัฐธรรมนูญ
๒๙. เลขาธิการสำนักงานศาลปกครอง
๓๐. สำนักงานเลขาธิการศาลยุติธรรม
๓๑. ผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล
๓๒. เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๓๓. สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (กสม.)

ลับมาก