เอกสารการแจ้งเตือนกรณีให้หน่วยงานยกระดับความมั่นคงปลอดภัยไซเบอร์ เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเป็นจำนวนมาก

เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเกี่ยวกับ Account ผู้ใช้งานภายในหน่วยงานรั่วไหล และถูกเผยแพร่ทั้ง User และ Password เป็นจำนวนมากในปัจจุบัน อาจทำให้มีผู้ไม่ประสงค์ดีเข้าโจมตีระบบภายในหน่วยงานหน้าเว็บไซต์ของหน่วยงาน สื่อโซเชียลมีเดีย หรือแพลตฟอร์มที่มีความเกี่ยวข้องกับหน่วยงาน นั้น

สกมช. จึงขอให้หน่วยงานในประเทศไทย ยกระดับการเฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์อย่างใกล้ชิด เนื่องจากขณะนี้มีกลุ่มผู้ไม่ประสงค์ดี ได้มีการเคลื่อนไหวและเริ่มโจมตีไปที่ระบบภายในหน่วยงาน และหน้าเว็บไซต์แล้ว

ทั้งนี้ สกมช. แนะนำให้หน่วยงานควรเตรียมแผนสำรองการรับมือเหตุการณ์ให้สามารถทำงานได้อย่างต่อเนื่อง หากระบบเกิดการ Offline หรือระบบหยุดชะงัก ให้รีบตรวจสอบและปิดช่องโหว่ที่ถูกโจมตีและเฝ้าระวัง ติดตามข่าวสาร การรายงานเหตุการณ์จาก สกมช. เพื่อรับการแจ้งเตือนได้ทันท่วงที อย่างไรก็ตาม เพื่อเป็นการป้องกันการโจมตีทางไซเบอร์ที่อาจจะเกิดขึ้น หน่วยงานควรตรวจสอบระบบสารสนเทศภายในองค์กรให้มีความมั่นคงปลอดภัยเพื่อป้องกันตนเองจากภัยคุกคามที่อาจจะเกิดขึ้น โดยสามารถดำเนินการได้ทันที ดังนี้

1. ดำเนินการตรวจสอบและปิดช่องโหว่จากข้อมูลที่คาดว่าเป็นช่องโหว่ที่ใช้ในการโจมตีดังกล่าว
2. สำรองข้อมูลอย่างน้อย 3 ชุด โดยต้องมีการ Backup แบบ Offline และควรให้สำเนาข้อมูลอยู่ในอุปกรณ์จัดเก็บข้อมูล หรือ Cloud ที่แยกออกจากระบบงาน และไม่สามารถเข้าถึงได้จากระบบงานปกติ
3. ตรวจสอบระบบการเข้าถึงเครือข่ายจากระยะไกล เช่น Remote Desktop Protocol, Virtual Private Network ว่ามีการเข้าถึงที่ผิดปกติหรือไม่ และควรหมั่นตรวจสอบสิทธิ์ การเข้าถึงระบบอย่างสม่ำเสมอ
4. User และ Password ควรใช้การยืนยันตัวตนแบบ Multi-factor Authentication(MFA) และตั้งรหัสผ่านให้ซับซ้อนคาดเดาได้ยาก
5. ควรอัปเดตคอมพิวเตอร์ ระบบปฏิบัติการ อุปกรณ์ต่าง ๆ รวมถึง Applications ให้ทันสมัยอยู่เสมอ โดยเฉพาะช่องโหว่ที่มีการแจ้งเตือนล่าสุด หรือช่องโหว่ประเภท 0-day ต่าง ๆ เช่น log4j, SolarWinds Supply Chain, Exchange Server และ Win32 Elevation Vulnerability เป็นต้น
6. ติดตั้งโปรแกรมป้องกันมัลแวร์ และอัปเดตให้ทันสมัยอยู่เสมอ
7. ตรวจสอบระบบของพนักงานที่มีการ Work from home โดยเฉพาะระบบที่ System Admin ใช้งาน
8. เพิ่ม Indicators of Compromise (IOCs) ลงในอุปกรณ์รักษาความมั่นคงปลอดภัยของระบบเพื่อเป็นการป้องกันการโจมตีอีกทาง
9. ไม่ควรใช้รหัสผ่านที่คาดเดาได้ง่าย ควรตั้งรหัสผ่านให้มีความซับซ้อน มีอักขระพิเศษ อักษรตัวเล็ก ตัวใหญ่ มีตัวเลขผสมผสานกัน และใช้การยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) เป็นอย่างน้อย ตัวอย่าง เช่น การสแกนลายนิ้วมือ คำถามเฉพาะเพื่อกู้รหัสผ่าน การส่งรหัสผ่านแบบครั้งเดียวที่ส่งผ่านข้อความสั้นเข้าโทรศัพท์มือถือ (SMS OTP) การใช้กุญแจรักษาความปลอดภัย เป็นต้น

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ขอแนะนำการยืนยันตัวตนแบบ Multi-Factor Authentication (MFA)[1] หรือระบบพิสูจน์ตัวบุคคลผ่านแอปพลิเคชัน ThaID (ไทยดี)[2] มีขั้นตอน ดังนี้

1. การลงทะเบียน ผู้ใช้งานสร้างบัญชีด้วยชื่อผู้ใช้และรหัสผ่าน จากนั้นผู้ใช้จะเชื่อมโยงรายการอื่น ๆ เช่น หมายเลขโทรศัพท์มือถือหรือกุญแจรีโมท เข้ากับบัญชีของผู้ใช้งาน รายการเหล่านี้ช่วยระบุผู้ใช้งานที่ไม่เหมือนกันและไม่ควรแบ่งปันกับผู้อื่น

2. การยืนยันตัวตน เมื่อผู้ใช้งานที่มีการเปิดใช้งานยืนยันตัวตนแบบ Multi-Factor Authentication (MFA) ได้ลงชื่อเข้าใช้เว็บไซต์ระบบจะแจ้งขอชื่อผู้ใช้และรหัสผ่านและการตอบสนอง เพื่อยืนยันตัวตนจากอุปกรณ์ผู้ใช้งาน หากยืนยันความถูกต้อง ระบบจะเชื่อมโยงไปยังรายการอื่น ๆ ตัวอย่างเช่น ระบบอาจออกรหัสตัวเลขให้กับอุปกรณ์ฮาร์ดแวร์หรือส่งโค้ดทาง SMS ไปยังอุปกรณ์เคลื่อนที่ของผู้ใช้งาน

3. การโต้ตอบ ผู้ใช้งานสามารถยืนยันตัวตนด้วยการยืนยันความถูกต้องของรายการอื่นๆ ตัวอย่างเช่น ผู้ใช้งานอาจป้อนรหัสที่ได้รับ หรือกดปุ่มบนอุปกรณ์ฮาร์ดแวร์ ผู้ใช้จะสามารถเข้าถึงระบบได้ต่อเมื่อข้อมูลทั้งหมดได้รับการยืนยันความถูกต้อง

4. การนำกระบวนการมาใช้ คือการยืนยันตัวตนโดยใช้หลายปัจจัยอาจนำมาใช้ได้ในหลายวิธีระบบขอเพียงรหัสผ่าน เรียกว่าการยืนยันตัวตนโดยใช้สองปัจจัย จะใช้แอปพลิเคชันของบุคคลภายนอกที่เรียกว่าเครื่องมือยืนยันตัวตนจะยืนยันความถูกต้องของตัวตนของผู้ใช้งาน ซึ่งผู้ใช้งานสามารถป้อนรหัสผ่านเข้าในเครื่องมือยืนยันตัวตน ในระหว่างการยืนยันความถูกต้องผู้ใช้งานจะป้อนข้อมูลไบโอเมตริกด้วยการสแกนลายนิ้วมือ หรือส่วนอื่น ๆ ของร่างกาย โดยระบบอาจขอให้มีการยืนยันตัวตนหลายครั้งต่อเมื่อผู้ใช้งานเข้าถึงระบบเป็นครั้งแรกบนอุปกรณ์ใหม่ หลังจากนั้นระบบจะจดจำเครื่อง และถามเพียงรหัสผ่านเท่านั้น

5.แอปพลิเคชัน ThaID จะแสดงภาพบัตรประจำตัวประชาชนในรูปแบบดิจิทัล ทั้งด้านหน้าบัตรและหลังบัตร เพื่อใช้ในการพิสูจน์และยืนยันตัวตน (Digital ID) รวมถึงการเปรียบเทียบภาพใบหน้า(Face Verification System) ทางดิจิทัล เมื่อประชาชนเข้าไปใช้บริการจากทางภาครัฐหรือภาคเอกชนที่จำเป็นต้องมีการยืนยันตัวตนก็สามารถเข้าสู่ระบบแอปพลิเคชัน ThaID เพื่อยืนยันตัวตนได้ โดยไม่ต้องกรอกข้อมูลหรือใช้เอกสารยืนยันตัวตัว

ทั้งนี้ ผู้ใช้งานหรือผู้ดูแลควรตรวจสอบและปฏิบัติตามคำแนะนำข้างต้น เพื่อลดความเสี่ยงที่อาจเกิดขึ้น สามารถติดตามข้อมูลเพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

อ้างอิง

1. https://aws.amazon.com/th/what-is/mfa
2. https://www.bora.dopa.go.th/app-thaid/