บรรยาย เรื่อง “ความมั่นคงปลอดภัยทางไซเบอร์ของระบบบริการสุขภาพ”

วันที่ 21 สิงหาคม 2566

เวลา 13.00 – 14.30 น.

ห้องประชุม ❍ Grand Ballroom

❍ ห้องประชุม 1 ⊘ ห้องประชุม 2 ❍ ห้องประชุม 3

โดย พ.ต.อ.ณัทกฤช พรหมจันทร์ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ปัจจุบันประเทศไทย ถือเป็นหนึ่งในประเทศที่พบปัญหาภัยคุกคามบนโลกออนไลน์ อ้างอิงจากสถิติการโจมตีข้อมูลพบว่า มีการถูกแฮคข้อมูล 31% การโจมตีทาง Cyber 62% และภัยคุกคามด้านอื่น ๆ อีก 7 % นอกจากนี้ยังพบว่ามีการฝังเว็บพนันออนไลน์ไว้ในเว็บไซต์ภาครัฐ ยกตัวอย่างเช่น การฝังโฆษณาเว็บพนันออนไลน์ไว้ในเว็บไซต์ของโรงพยาบาล, สำนักงานกฎหมาย, กรมการขนส่งทางบก เป็นต้น

ด้วยเหตุนี้ การเตรียมความพร้อมสำหรับการรับมือต่อภัยคุกคามไซเบอร์ จึงเป็นแนวทางสำคัญที่จะสร้างความปลอดภัยต่อการปกป้องข้อมูลส่วนบุคคลด้วยตนเอง ซึ่งสามารถทำได้ดังนี้ 1) มีการเตรียมตัวหากเกิดเหตุคุกคาม/โจมตี/โจรกรรมข้อมูลในระบบอยู่เสมอ เพื่อให้ผู้มีส่วนเกี่ยวข้องตระหนักถึงความสำคัญของเหตุการณ์ไม่คาดฝันที่อาจเกิดขึ้นได้ 2) ทำความเข้าใจกับสิ่งที่เกิดขึ้นถึงขั้นตอนและสิ่งที่ต้องทำ เช่น หากเกิดเหตุการณ์โจรกรรมข้อมูล มีกฎหมายหรือประกาศใดบ้างที่มีความจำเป็นต้องใช้, การพูดคุยหรือแจ้งเหตุกับหน่วยงานที่เกี่ยวข้อง รวมถึงการดำเนินการเมื่อเกิดเหตุ 3) การใช้ Hardware และ Software ที่ทันสมัย มีการดูแลอยู่สม่ำเสมอ เนื่องจากโปรแกรมรุ่นใหม่จะสามารถป้องกันไวรัสได้อัตโนมัติและสามารถป้องกันการโจรกรรมข้อมูลได้ 4) ผู้ใช้งานมีความเข้าใจต่อการใช้โปรแกรม ไม่ส่งเสริมให้แฮคเกอร์สามารถคาดเดาพฤติกรรมได้โดยง่าย เช่น การใช้รหัส 123456

ท้ายที่สุดแล้ว การรักษาความปลอดภัยไซเบอร์ ถือเป็นประเด็นสำคัญที่ทุกคนจะต้องเรียนรู้และตระหนักถึงความสำคัญในการป้องกัน เพื่อไม่ให้เกิดปัญหาที่อาจนำไปสู่ภัยร้ายแรง

ข้อคิดเห็นในที่ประชุม

1. ทุกหน่วยงานควรส่งเสริมให้มีการใช้ Hardware และ Software ที่ทันสมัยมากที่สุด เพื่อลดการโจมตีทางไซเบอร์รวมถึงป้องกันการโจรกรรมข้อมูลผู้ป่วย

2. การเตรียมตัวในหน่วยงานเพื่อป้องกันความมั่นคงปลอดภัยไซเบอร์

2.1 การเตรียมบุคลากร : บุคลากรที่มีการใช้งานอุปกรณ์ไอทีทุกคนต้องมีความเข้าใจต่อโปรแกรมและสามารถสังเกตสถานการณ์หรือความผิดปกติของโปรแกรมที่ใช้งานได้ เพื่อป้องกันเหตุเบื้องต้นหรือแจ้งระงับเหตุต่อหน่วยงานที่เกี่ยวข้อง

2.2 อุปกรณ์/ระบบ : อุปกรณ์หรือระบบสามารถตรวจจับความผิดปกติได้ รวมถึงการป้องกันไม่ให้แฮคเกอร์เข้าถึงข้อมูลและจดจำพฤติกรรมเจ้าของข้อมูลตัวจริง

2.3 วิธีการ/การจัดการ : มีการกำหนดแนวทางการป้องกันเหตุเบื้องต้นหรือแจ้งระงับเหตุผ่านการสื่อสารและประชาสัมพันธ์ในหน่วยงาน

1. นางสาวณัฐณา ศรีคงแก้ว

2. นางสาวสุดารัตน์ ยมสวัสดิ์

บันทึกการประชุม