กิจกรรมสื่อสารแลกเปลี่ยนเรียนรู้ภายในองค์กร
เรื่อง การป้องกันองค์กรให้ปลอดภัยจากการโดนโจรกรรมข้อมูล
ในการประชุมติดตามความก้าวหน้าผลการปฏิบัติราชการตามคำรับรองปฏิบัติราชการ
สำนักทันตสาธารณสุข ประจำปีงบประมาณ พ.ศ. 2566 (ประจำเดือนมีนาคม)
วันศุกร์ที่ 7 เมษายน 2566 ณ ห้องประชุมกำธร สุวรรณกิจ อาคาร 1 ชั้น 1 กรมอนามัย
****

การป้องกันองค์กรไม่ให้โดนโจรกรรมข้อมูล เป็นเรื่องที่สำคัญอย่างยิ่ง เนื่องจากข้อมูลและสารสนเทศขององค์กรเป็นสิ่งที่มีค่ามาก ซึ่งถูกจัดเก็บไว้ในระบบคอมพิวเตอร์และมีการเชื่อมต่อเครือข่าย การโจรกรรมข้อมูลสามารถทำให้องค์กรเสียหายได้หลายด้านไม่ว่าจะเป็นการสูญเสียข้อมูลลับของผู้มีส่วนได้ส่วนเสียหรือลูกค้า การละเมิดความเป็นส่วนตัวของพนักงานหรือเจ้าหน้าที่ทำให้เกิดความเสียหายต่อทรัพย์สินหรือการเงิน

วิธีการป้องกันองค์กรไม่ให้โดนโจรกรรมข้อมูล ต้องเริ่มจากการสร้างความตระหนักให้กับพนักงานทุกคนเกี่ยวกับความสำคัญของความเป็นส่วนตัวและความมั่นคงของข้อมูล นอกจากนี้องค์กรต้องมีการติดตั้งระบบป้องกันโจรกรรมข้อมูลที่มีประสิทธิภาพ เช่น ระบบ Firewall การเข้ารหัสข้อมูล และการตรวจสอบความปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอ

กรมอนามัย มีการใช้งานระบบคอมพิวเตอร์และมีการเชื่อมต่อเครือข่าย ทั้งภายในและภายนอก โดยติดตั้งระบบต่างๆบน Cloud กรมอนามัย จำนวน 229 ระบบ ซึ่งตั้งอยู่ที่กองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย ซึ่งสำนักทันตสาธารณสุข ภายใต้สังกัดกรมอนามัย เป็นหน่วยงานหนึ่งในการขอใช้งานระบบคอมพิวเตอร์และเชื่อมต่อเครือข่าย ซึ่งมีมากกว่า 20 ระบบงานในปัจจุบัน ดังนั้นทาง กรมอนามัย จึงมีแนวทางการป้องกันองค์กรไม่ให้โดนโจรกรรมข้อมูล ดังนี้

1. ตรวจสอบช่องโหว่อยู่เสมอ กรมอนามัยร่วมกับสำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน) (สพร.) ตรวจสอบและแนะนำการแก้ไข ช่องโหว่ระบบงานของหน่วยงานที่ติดตั้งบน Cloud กรมอนามัย โดยดำเนินการเป็นประจำทุกปี และแจ้งผู้รับผิดชอบระบบงาน ดำเนินการแก้ไขช่องโหว่ที่ตรวจพบในระบบงาน
2. เฝ้าระวังและแจ้งภัยคุกคามทางไซเบอร์ กรมอนามัยใช้ระบบ Thaicert Government Monitoring System ของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) ในการประมวลผลวิเคราะห์ข้อมูลการโจมตีทางไซเบอร์ ดำเนินการประเมินความเสี่ยงระบบงาน/ระบบสารสนเทศ ตลอด 24 ชั่วโมง และรายงาน CIO กรมอนามัย
3. ประเมินความเสี่ยงด้านระบบสารสนเทศ ดำเนินการประเมินความเสี่ยงระบบงาน/ระบบสารสนเทศเป็นประจำทุกปีและรายงาน CIO กรมอนามัย
4. ความปลอดภัยด้านคอมพิวเตอร์และเครือข่าย มีอุปกรณ์ป้องกันและเฝ้าระวังความปลอดภัยทางเครือข่าย

a. อุปกรณ์ป้องกันความปลอดภัยด้านเครือข่าย เช่น Firewall, IPS, DDOS, Web Application firewall เป็นต้น
b. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ โดยการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN เป็นต้น
c. ซอฟต์แวร์เฝ้าระวังภัยคุกคามทางไซเบอร์ เช่น PRTG Network Monitor เป็นต้น

5. ความปลอดภัยด้านคอมพิวเตอร์และเครือข่าย มีระบบสำรองข้อมูลแบบอัตโนมัติ (Veeam Backup) เพื่อสามารถนำข้อมูลกลับมาใช้งานได้อย่างต่อเนื่อง ด้วยการกู้คืนข้อมูล (Restore) รวมทั้งสำรองข้อมูลไปยัง GDCC Cloud Service ภายนอกกรมอนามัย และมีการทดสอบกู้คืนระบบสารสนเทศโดยดำเนินการเป็นประจำทุกปี
6. Blockchain หรือระบบในการเก็บข้อมูลที่มีความน่าเชื่อถือ โปร่งใส และไม่ต้องอาศัยคนกลาง การป้องกันโดยการแบ่งข้อมูล เช่น ข้อมูลสุขภาพ ออกเป็นชุดเล็กๆ ในรูปแบบ Verifiable Credential: VC การจัดเก็บข้อมูลในระบบสมุดสุขภาพที่ใช้ Blockchain ในการเข้ารหัส เพื่อป้องกันการโจรกรรมข้อมูล
7. ติดตั้งซอฟต์แวร์รักษาความปลอดภัย (Anti Virus) มีการติดตั้ง/สแกน/อัพเดทฐานข้อมูล ซอฟต์แวร์ป้องกันไวรัส (Antivirus) อย่างสม่ำเสมอ
8. การรักษาความปลอดภัยด้านกายภาพ สถานที่ และ สภาพแวดล้อมห้องควบคุม ระบบคอมพิวเตอร์และเครือข่าย การควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยในการเข้าใช้งานหรือเข้าถึงพื้นที่ใช้งานในระบบสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยี สารสนเทศข้อมูล ซึ่งมีผลบังคับใช้กับผู้ใช้งานและรวมถึงบุคคล
9. แยกสัญญาณ Wi-Fi จากสาธารณะ มีการแยกสัญญาณ Wi-Fi และแยกกลุ่มผู้ใช้งานภายในองค์กรและผู้ใช้งานภายนอกออกจากกัน
10. ติดตั้งเฉพาะโปรแกรมที่มีความน่าเชื่อถือ ติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์และป้องกันการติดตั้งโปรแกรมโดยใช้ Active Directory บริหารจัดการเครื่องคอมพิวเตอร์และบัญชีชื่อผู้ใช้งานของกรมอนามัย
11. อัพเดทโปรแกรมและระบบปฏิบัติการอยู่เสมอ มีการอัพเดทโปรแกรมและระบบปฏิบัติการล่าสุด
12. การตั้งรหัสผ่านให้มีความปลอดภัย มีการแจ้งบุคลากรของทุกหน่วยงาน ในการกำหนดรหัสผ่านอย่างน้อย 8 ตัวอักษร (พิมพ์เล็ก, พิมพ์ใหญ่, อักขระพิเศษ และตัวเลข) และเปลี่ยนรหัสผ่านทุก 6 เดือน
13. การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Awareness) ให้กับบุคลากร ในองค์กร การสร้างความรู้ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยให้กับบุคลากรในองค์กร โดยมีการจัดประชุม Digital Literacy และ การประชุมภาคีเครือข่ายไอซีที
14. ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบงาน/ระบบสารสนเทศ และกำหนดสิทธิ การเข้าถึงข้อมูลต้องปฏิบัติตามกฎหมาย
    a. กฎหมายด้านเทคโนโลยีสารสนเทศ เช่น พรบ.คุ้มครองข้อมูลส่วนบุคคล และ พรบ.การรักษาความมั่นคงปลอดภัยทางไซเบอร์, พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์,

พรบ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ และประกาศ กรมอนามัย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน สารสนเทศ เป็นต้น

b. เจ้าหน้าที่และผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ใน ประเทศไทยรวมทั้งกฎระเบียบของกรมอนามัย

ถึงจะมีแนวทางในการป้องกันองค์กรไม่ให้โดนโจรกรรมข้อมูล แต่พฤติกรรมของผู้ใช้งาน ที่อาจทำให้องค์กรต้องเสี่ยงกับการถูก Cyber Attack ก็เป็นส่วนหนึ่งด้วยเช่นกัน จึงขอยก 6 พฤติกรรม เพื่อลดความเสี่ยง ดังนี้

1. ควรอัพเดตระบบปฏิบัติการ โปรแกรมหรือซอฟต์แวร์ต่าง ๆ สม่ำเสมอ
2. หลีกเลี่ยงการใช้รหัสผ่านเดิมซ้ำๆ และควรเปิดใช้งานระบบยืนยันตัวตนแบบ two-factor authentication (2FA)
3. หลีกเลี่ยงการใช้ Wi-Fi สาธารณะ
4. ควรดาวน์โหลด Application จาก Official store เท่านั้น
5. ควรเข้าใช้งานเว็บไซต์ที่ปลอดภัย เช่น URL เว็บที่ใช้ต้อง Https เป็นต้น
6. ติดตามข่าวสารการใช้งานเทคโนโลยีเป็นประจำ

นายอรรถพล คงมาก
เจ้าพนักงานทันตสาธารณสุขปฏิบัติงาน
เจ้าหน้าที่ IT สำนักทันตสาธารณสุข