แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สำนักงานพัฒนาที่ดินเขต ๒
รอบการประเมินที่ ๒/๒๕๖๘ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๘ – ๓๐ กันยายน ๒๕๖๘
ประจำปีงบประมาณ พ.ศ. ๒๕๖๘

ชื่อ-นามสกุล นางสาวพัชรนันท์ ทวีพงศ์จิรภาส **ตำแหน่ง** นักวิชาการเงินและบัญชีปฏิบัติการ
หน่วยงาน กลุ่ม/ฝ่าย/สพด./ศูนย์ ฝ่ายบริหารทั่วไป
หัวข้อการพัฒนา การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)
วิธีการพัฒนา อบรมผ่านระบบออนไลน์ e-Learning สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)
วันที่พัฒนา ๑๐ มิถุนายน ๒๕๖๘ **สถานที่** สำนักงานพัฒนาที่ดินเขต ๒
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)
วัตถุประสงค์

๑. เพื่อเรียนรู้และตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ในปัจจุบัน
๒. เพื่อเรียนรู้เกี่ยวกับภัยคุกคามต่างๆทางไซเบอร์ และแนวทางป้องกันแก้ไข
๓. เพื่อสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

สรุปสาระสำคัญ รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

๑. มีความรู้ ความเข้าใจ ในเรื่องภัยคุกคามทางไซเบอร์
๒. มีความรู้และวิธีการรับมือ รวมถึงการป้องกันภัยคุกคามทางอินเตอร์เน็ตอย่างถูกต้อง สามารถนำมาประยุกต์ใช้ในการปฏิบัติงานได้ และป้องกันภัยทางไซเบอร์ให้กับตนเองและหน่วยงาน

(ลงนาม) .....
(นางสาวพัชรนันท์ ทวีพงศ์จิรภาส)
ตำแหน่ง นักวิชาการเงินและบัญชีปฏิบัติการ

(ลงนาม) .....
(นางสาวกิ่งดาว ชลธาร)
ตำแหน่ง หัวหน้าฝ่ายบริหารทั่วไป

การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

CYBER SECURITY

Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้องโดยประกอบไปด้วย ระบบสารสนเทศ (Information System) โปรแกรมประยุกต์ (Application) ข้อมูล (Data) ระบบคอมพิวเตอร์ หรือเครื่องมือที่ใช้ในการเข้าระบบเครือข่าย (Mobile Phone, Tablet, TV) หน่วยบันทึกข้อมูลและอุปกรณ์เครือข่าย (Storage, Network Device) ศูนย์ข้อมูล (Data Center) รวมถึงกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับความปลอดภัยของระบบคอมพิวเตอร์โดยเฉพาะระบบเครือข่ายอินเตอร์เน็ต ซึ่งมีจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม ดังนั้นหลาย ๆ องค์กรจึงให้ความสำคัญเรื่องระบบรักษาความปลอดภัยของข้อมูลไม่แพ้กัน เพราะหากลูกค้าหรือผู้ใช้บริการโดนโจรกรรมข้อมูลทางอิเล็กทรอนิกส์ไป อาจทำให้องค์กรเสียหายหรือเสียชื่อเสียงได้

ความสำคัญของ CYBER SECURITY

1. ความสุ่มเสี่ยงต่อการถูกโจรกรรมทางไซเบอร์จากการศึกษาของ University of Maryland พบว่าระบบคอมพิวเตอร์ทั่วโลกมีแฮกเกอร์พยายามเข้าถึงและโจมตีระบบในระยะเวลาเพียง 39 วินาที โดยประมาณ หรือประมาณ 2,244 ครั้งต่อวัน ดังนั้น องค์กรจะต้องให้ความสำคัญกับการเก็บข้อมูล โดยเฉพาะข้อมูลส่วนบุคคลของลูกค้า ข้อมูลทางการเงิน ทรัพย์สินทางปัญญา และข้อมูลสำคัญระดับประเทศ เป็นต้น หากไม่มีระบบการป้องกันทางไซเบอร์ที่เข้มงวด แฮกเกอร์อาจสามารถเข้าถึง และนำข้อมูลไปใช้งานได้อย่างง่ายดาย

2. การรั่วไหลของข้อมูลหากองค์กรไม่มีระบบการป้องกันและรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพเพียงพอ อาจทำให้เกิดการรั่วไหลของข้อมูลสำคัญ โดยเฉพาะข้อมูลส่วนบุคคล (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) อาจถูกเปิดเผยหรือนำไปใช้งานอย่างไม่เหมาะสมที่อาจก่อให้เกิดความเสียหายมหาศาลตามมาได้

3. องค์กรเสียชื่อเสียงเมื่อเกิดเหตุการณ์ที่องค์กรไม่สามารถรักษาความปลอดภัยของข้อมูลได้ จนทำให้บุคคลภายนอกสามารถเข้าถึงหรือเปิดเผยข้อมูล อาจส่งผลกระทบร้ายแรงต่อองค์กร เช่น สูญเสียค่าใช้จ่ายมหาศาลในการแก้ไขสถานการณ์เฉพาะหน้า และซื้อข้อมูลที่ถูกขโมยไปกลับมา หรือแม้กระทั่งชื่อเสียงเกี่ยวกับความปลอดภัยขององค์กรก็จะเสื่อมถอยลง ทำให้เกิดภาพลักษณ์ไม่ดีต่อองค์กรและยากที่จะกู้คืนความเชื่อมั่นของผู้ใช้บริการให้กลับมาเชื่อมั่นในองค์กรเหมือนเดิม

CYBER SECURITY 5 ประเภท

1. Critical Infrastructure Security เป็นการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐานที่สำคัญ การสร้างระบบความปลอดภัยที่เหมาะสมเป็นสิ่งจำเป็น เนื่องจากหากไม่มีการป้องกันอย่างเหมาะสม อาจเกิดความเสี่ยงที่จะถูกโจมตีมากกว่ารูปแบบอื่น โดยเฉพาะระบบรักษาความปลอดภัยของธนาคาร ตลาดหลักทรัพย์ รัฐบาล ที่มีข้อมูลส่วนบุคคลอยู่เป็นจำนวนมาก หรือแม้กระทั่งข้อมูลทางการเงินก็นับว่าเป็นข้อมูลละเอียดอ่อน ที่การรักษาความปลอดภัย Critical Infrastructure Security จะต้องทำโครงสร้างออกมาให้แข็งแรง เพื่อป้องกันข้อมูลได้ดียิ่งขึ้น

2. Network Security คือ การรักษาความปลอดภัยของระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นการป้องกัน การคุกคามจากบุคคลภายนอกที่พยายามเข้าถึงและใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยไม่ได้รับอนุญาต ร่วมกับการนำเทคโนโลยีและระบบปัญญาประดิษฐ์มาช่วยเพื่อตรวจจับ และแจ้งเตือนเกี่ยวกับความผิดปกติ ที่เกิดขึ้น

3. Cloud Security หากองค์กรตัดสินใจเก็บข้อมูลต่าง ๆ ในเซิร์ฟเวอร์ภายในบริษัทจะมีความเสี่ยงที่ข้อมูลอาจถูกโจมตีได้ การโอนย้ายข้อมูลเพื่อจัดเก็บบน Cloud Security เป็นตัวช่วยที่สามารถเพิ่มความปลอดภัยและประหยัดค่าใช้จ่ายได้มากขึ้น อีกทั้งในปัจจุบันระบบความปลอดภัยของคลาวด์ มีการพัฒนาและปรับปรุงอย่างต่อเนื่อง ทำให้เหมาะสมกับความต้องการ และเป็นทางเลือกที่ดีในการใช้งาน

4. Application Security ในกระบวนการพัฒนาหรือติดตั้งแอปพลิเคชัน อาจเกิดการโจมตีหรือการแฝงตัวเข้ามาได้ ดังนั้นการเลือกใช้ตัวช่วยในการรักษาความปลอดภัยผ่านแอปพลิเคชันเป็นทางเลือกที่ดีเพื่อเพิ่มระดับความปลอดภัยให้กับกระบวนการพัฒนาระบบได้อีกวิธีหนึ่ง

5. Internet of Things Security การรักษาความปลอดภัยบนอุปกรณ์ Internet of Things (IoT) ที่มีการใช้งานตลอดเวลาเป็นเรื่องสำคัญ เนื่องจากระบบ IoT มีการส่งรับข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ดังนั้น จำเป็นต้องมีการกำหนดมาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยบนอุปกรณ์เหล่านี้ให้มีประสิทธิภาพและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

รูปแบบภัยคุกคาม CYBER SECURITY

1. มัลแวร์ (Malware) เป็นช่องโหว่ที่สามารถทะลุการปกป้องเครือข่ายของคุณ เช่น สปายแวร์ (spyware) ไวรัสเรียกค่าไถ่ (ransomware) และไวรัสคอมพิวเตอร์ (viruses)

2. ฟิชชิ่ง (Phishing) ข้อความเหล่านี้เป็นข้อความที่เป็นอันตราย (โดยส่วนมากที่พบคืออีเมล) ที่มีลิงก์ที่เป็นอันตราย ซึ่งเมื่อได้คลิกเข้าไปแล้วจะทำการหลอกล่อให้คุณส่งข้อมูลที่ละเอียดอ่อนไปยังเป้าหมาย

3. การปฏิเสธการให้บริการ (Denial of Service (DoS)) แฮกเกอร์มักทำการโจมตี เพื่อทำให้เครือข่าย หรือระบบของคุณที่มีข้อมูลส่วนเกินจนล้นเครือข่าย และบังคับให้ระบบหยุดทำงาน

4. เทคนิคคนกลาง (Man in the middle (MitM)) อาชญากรไซเบอร์ที่เข้ามาอยู่ระหว่างการเชื่อมต่อของคุณ ซึ่งมักจะกระทำผ่านเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย และขโมยข้อมูลที่ละเอียดอ่อนของคุณไป

5. การโจมตีแบบซีโร่เดย์ (Zero-day attack) พบได้น้อย แต่มากขึ้นเรื่อย ๆ การโจมตีทั่วไปที่เกิดขึ้นระหว่างรอการประกาศการอัปเดตความปลอดภัย หรือโปรแกรมแก้ไข และการติดตั้ง

5 เหตุผลที่องค์กรต้องทำระบบ CYBER SECURITY

1. เพื่อปกป้องข้อมูลขององค์กรและข้อมูลส่วนบุคคลไม่ให้ถูกนำไปใช้ในทางทุจริต การสร้างระบบ Cyber security ที่รัดกุมและครอบคลุมตั้งแต่การป้องกัน ไปจนถึงการวางแผนระยะยาว คือส่วนสำคัญที่จะช่วยให้องค์กรสามารถสกัดกั้นการโจมตีจากแฮกเกอร์ก่อนที่จะเข้ามาขโมยข้อมูลและนำไปใช้ในทางทุจริต ไม่ว่าจะเป็นการเข้าระบบเพื่อโจมตีให้ข้อมูลเสียหาย การขโมยข้อมูลลูกค้าไปขายหรือใช้ในการหลอกลวงเพื่อสร้างความเสียหายต่อบุคคล การนำข้อมูลไปใช้ปลอมแปลงเพื่อการทำธุรกรรม รวมทั้งการโจรกรรมข้อมูลเพื่อเรียกค่าไถ่ (Ransomware) เป็นต้น

2. เพื่อป้องกันไม่ให้เกิดความเสียหาย ทั้งในด้านค่าใช้จ่ายและชื่อเสียงขององค์กรหากองค์กรถูกโจมตีทางไซเบอร์ แน่นอนว่าสิ่งที่ตามมานั้นคือความเสียหายทางด้านค่าใช้จ่ายที่อาจมีมูลค่ามหาศาล อย่างเช่น การโจรกรรมข้อมูลเพื่อเรียกค่าไถ่ด้วยวิธีการแอบลักลอบขนข้อมูลออกไปและติดตั้งมัลแวร์เพื่อเข้ารหัสข้อมูลไม่ให้เจ้าของข้อมูลสามารถใช้งานได้หากไม่ยอมจ่ายเงินที่เรียกว่า Ransomware หรืออาจเกิดค่าใช้จ่ายในการกู้คืนข้อมูลที่สูญหายไป รวมไปถึงความเสียหายในด้านชื่อเสียงขององค์กร ที่ประเมินค่าเป็นตัวเลขชัดเจนไม่ได้

3. เพื่ออุดช่องโหว่การป้องกันด้วยระบบสารสนเทศขั้นพื้นฐานรูปแบบเดิม ๆ ที่ไม่เพียงพอในการป้องกันภัยไซเบอร์สมัยใหม่ มาตรการทางสารสนเทศ (IT Policy) คือมาตรฐานในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งถือเป็นเกราะป้องกันภัยขององค์กรที่มีประสิทธิภาพและประสบความสำเร็จมาโดยตลอด แต่ปัจจุบันภัยคุกคามทางไซเบอร์มีการพัฒนารูปแบบการโจมตีที่มีความหลากหลายและซับซ้อนมากขึ้น ทำให้การป้องกันเพียงระบบสารสนเทศขั้นพื้นฐาน (Infrastructure Protection) อาจดีไม่เพียงพอสำหรับโลกในยุคปัจจุบัน

4. เพื่อสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรที่ร่วมงานกับองค์กรสถิติการเกิดภัยคุกคามทางไซเบอร์ที่ค่อนข้างสูงทั้งในประเทศไทยและทั่วโลก ทำให้องค์กร หน่วยงาน รวมถึงประชาชนเอง ต่างเกิดความกังวล และเกิดคำถามว่าข้อมูลที่หมุนเวียนอยู่ในโลกดิจิทัลนั้นถูกปกป้องอย่างดีแล้วหรือยัง ดังนั้น องค์กรและธุรกิจจึงต้องเร่งสร้างความเชื่อมั่นด้านความปลอดภัยในข้อมูลให้ได้มากที่สุด ผ่านการวางระบบ Cyber security ที่ชัดเจนและได้ประสิทธิภาพ เพื่อเป็นการสร้างความมั่นใจให้กับพันธมิตรทางธุรกิจและลูกค้าผู้ใช้บริการที่ร่วมเดินทางไปพร้อมกับองค์กร

5. ปฏิบัติตามพรบ.คุ้มครองข้อมูลส่วนบุคคล (PDPA) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562 หรือ PDPA คือข้อสำคัญที่ทำให้องค์กรต้องวางระบบความปลอดภัยในข้อมูลเพื่อดูแลและปกป้องข้อมูลของลูกค้า ข้อมูลผู้ใช้งาน หรือข้อมูลพนักงานในองค์กรให้ได้ประสิทธิภาพและปลอดภัยที่สุด เพราะถ้าหากองค์กรหรือหน่วยงานใดไม่ปฏิบัติตามจะทำให้เกิดบทลงโทษกฎหมาย ซึ่งมีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง จึงเป็นเหตุผลให้องค์กรทั้งภาครัฐและเอกชนต้องตระหนักและเพิ่มมาตรการการรักษาข้อมูล เพื่อป้องกันความเสียหายทั้งต่อบุคคล องค์กร และความเสียหายทางด้านโทษทางกฎหมาย

จัดทำโดย นางสาวพัชรนันท์ ทวีพงศ์จิรภาส
นักวิชาการเงินและบัญชีปฏิบัติการ