บันทึกข้อความ

ส่วนราชการ ฝ่ายบริหารทั่วไป สำนักงานพัฒนาที่ดินเขต ๑๑ โทร. ๐๗๗๓๑๑๑๑๐

ที่ กษ ๐๘๑๘/- **วันที่** ๒๙ สิงหาคม ๒๕๖๗

เรื่อง สรุปบทเรียนการพัฒนาทักษะด้านดิจิทัล

เรียน หัวหน้าฝ่ายบริหารทั่วไป

ตามที่ กรมฯ ได้กำหนดให้ข้าราชการ ดำเนินการจัดทำตัวชี้วัดรายบุคคลด้านการพัฒนาบุคลากร “ระดับความสำเร็จของการพัฒนาบุคลากรในหน่วยงาน” รอบการประเมินที่ ๒ (๑ เมษายน ๒๕๖๗ – ๓๐ กันยายน ๒๕๖๗) ของปีงบประมาณ พ.ศ.๒๕๖๗ โดยให้มีการพัฒนาทักษะด้านดิจิทัล ๑ เรื่องครบถ้วนตามเงื่อนไขของหลักสูตร และพัฒนาความรู้ ๑ เรื่อง รวมทั้งมีการสรุปบทเรียน ๑ เรื่อง ส่งให้ผู้บังคับบัญชาทราบภายในวันที่ ๒ กันยายน ๒๕๖๗ เพื่อรวบรวมขึ้นเว็บไซต์ของหน่วยงานต่อไป นั้น

ข้าพเจ้านางสาวอัมพิกา พวงแก้ว ตำแหน่ง นักจัดการงานทั่วไปชำนาญการ สังกัดฝ่ายบริหารทั่วไป สพข.๑๑ ได้ดำเนินการพัฒนาทักษะด้านดิจิทัล ๑ เรื่อง การสร้างความตระหนักรู้ด้านความมั่นคงทางโซเบอร์ (Cybersecurity Awareness) ผ่านเรียบร้อยแล้ว จึงขอส่งสรุปบทเรียน รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรด พิจารณาดำเนินการต่อไป

(นางสาวอัมพิกา พวงแก้ว)
นักจัดการงานทั่วไปชำนาญการ

สรุปบทเรียนการพัฒนาทักษะด้านดิจิทัล

เรื่อง : การสร้างความตระหนักรู้ด้านความมั่นคงทางโซเบอร์ (Cybersecurity Awareness)

****

Cybersecurity คืออะไร

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกัน และรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรมที่อาจจะเกิดความเสียหาย จากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มาในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลาย ความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยพางไซเบอร์ ได้แก่ พ.ร.บ.การรักษาความมันคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล และมาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

ความรู้พื้นฐานของ Cybersecurity พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิ์ในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัทคน

integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง ได้แก่ ข้อมูลของธนาคารด้านการเงิน เช่นข้อมูลบัญชีธนาคาร และข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ได้แก่ ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร และข้อมูลที่อยู่บนระบบคอมพิวเตอร์

รูปแบบภัยคุกคามของ Cybersecurity

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้ง หรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) และโทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

<u>เพิ่มเติม</u> เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลมูลดังกล่าวของเหยื่อใช้ในการทำธุรกรรม

Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น Code ของเว็บไซต์ เช่น CMS Web Server หรือ Database Server วิธีการโจมตีที่นิยมใช้ Cross-Site Scripting, SQL Injection และ Path Traversal สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดนั้นๆ

<u>ผลกระทบ</u> ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่ ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง วิธีการป้อง นำหลักการ Zero Trust มาใช้งานภายในองค์กร

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานใต้อีกครั้ง วิธีการป้องกัน สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมาควรมีความตระหนักก่อนที่จะทำการเปิด

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดี และ ไม่ควรบอก Password แก่ผู้อื่น

Password การใช้ Password ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! ๒ ๕ #)

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password, ๑๒๓๔๕๖, วันเกิด, หมายโทรศัพท์

๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗. ไม่ควรบอก Password แก่ผู้อื่น

E-mail สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

Website สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ

๒. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

๗. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

<u>เพิ่มเติม</u> ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล

Fake News หรือ ข่าวปลอมเป็นภัยคุยคุณใกล้ตัวประประมาทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวสารปลอมที่นำมาเผยแพร่นั้นดูมีความเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตุข่าวปลอม

๑. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ

๒. ระบุที่มาของข่าวไม่ได้

๓. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์

๔. สำนวนการเขียนออกแนวการโฆษณา

Conference สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์เอกสารต่างๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

<u>เพิ่มเติม</u> ควรมีการขออนุญาตผู้เข้าร่วมประชุม conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

Free WIFI สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Mobile สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓. กำหนด Application permission ให้เหมาะสม

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

Internet Connection สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒. เปลี่ยน ๕๕ID และรหัสผ่านของ VIFI ที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

ผู้สรุปบทเรียน
นางสาวอัมพิกา พวงแก้ว
นักจัดการงานทั่วไปชำนาญการ

DIGITAL GOVERNMENT DEVELOPMENT AGENCY

สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
TDGA
THAILAND DIGITAL GOVERNMENT ACADEMY

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

อัมพิกา พวงแก้ว

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 29 ส.ค. 2567

(นางไอรดา เหลืองวิไล)

รองผู้อำนวยการสำนักงานพัฒนารัฐบาลดิจิทัล

รักษาการแทนผู้อำนวยการสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

7888d2b4

Signed by สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)
Date: 2024-08-29T18:14:31.530+07:00
Reason: Confirm Certificate