แบบรายงานสรุปผลการเข้ารับการฝึกอบรม
เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ สังกัด สำนักงานพัฒนาที่ดินเขต ๘

เรียน หัวหน้าฝ่ายบริหารทั่วไป

ด้วย นางสาวชิดชนก แจ่มดี ตำแหน่ง เจ้าพนักงานธุรการชำนาญงาน สังกัดฝ่ายบริหารทั่วไป สำนักงานพัฒนาที่ดินเขต ๘ กรมพัฒนาที่ดิน ได้เข้ารับการฝึกอบรมหลักสูตร การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness) ผ่านระบบ E-LEARNING ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy หรือ TDGA เมื่อวันที่ ๒๘ มกราคม ๒๕๖๙ เป็นเวลารวมทั้งสิ้น ๑.๓๐ ชั่วโมง ซึ่งหลักสูตรดังกล่าวจัดโดยสำนักงานพัฒนารัฐบาลดิจิทัล

จึงขอรายงานสรุปผลการพัฒนาความรู้เพื่อเพิ่มประสิทธิภาพการปฏิบัติงานของข้าราชการ ดังนี้

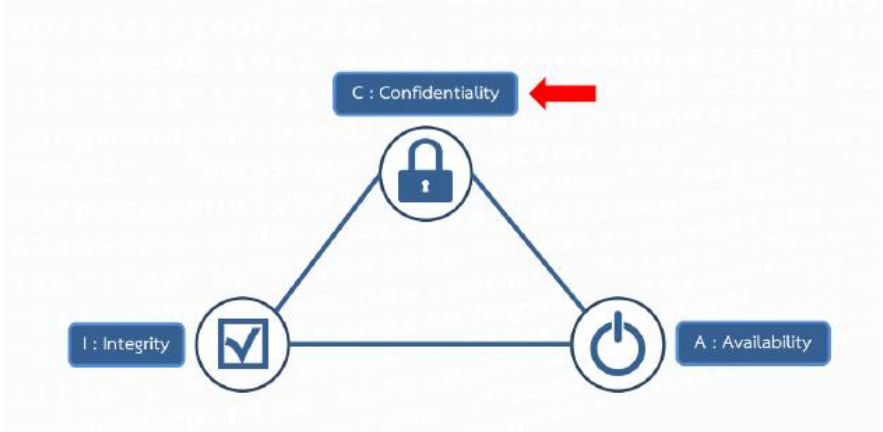
๑. วัตถุประสงค์

๑.๑ เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๑.๒ เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ และแนวทางป้องกันแก้ไข
๑.๓ เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

๒. เนื้อหาและหัวข้อวิชา

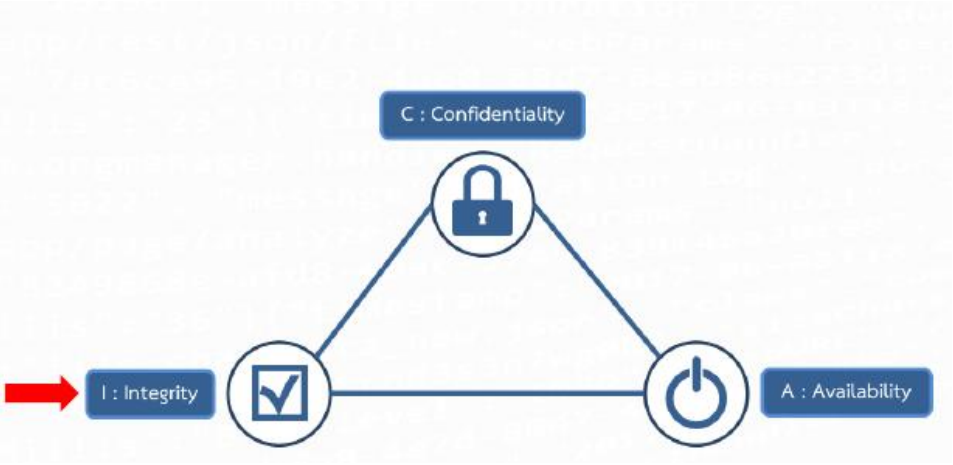
CyberSecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย,โครงสร้างพื้นฐานทางสารสนเทศ,ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาตในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อย ๆ

ความรู้พื้นฐานของ CyberSecurity
พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์



๒.๑ Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

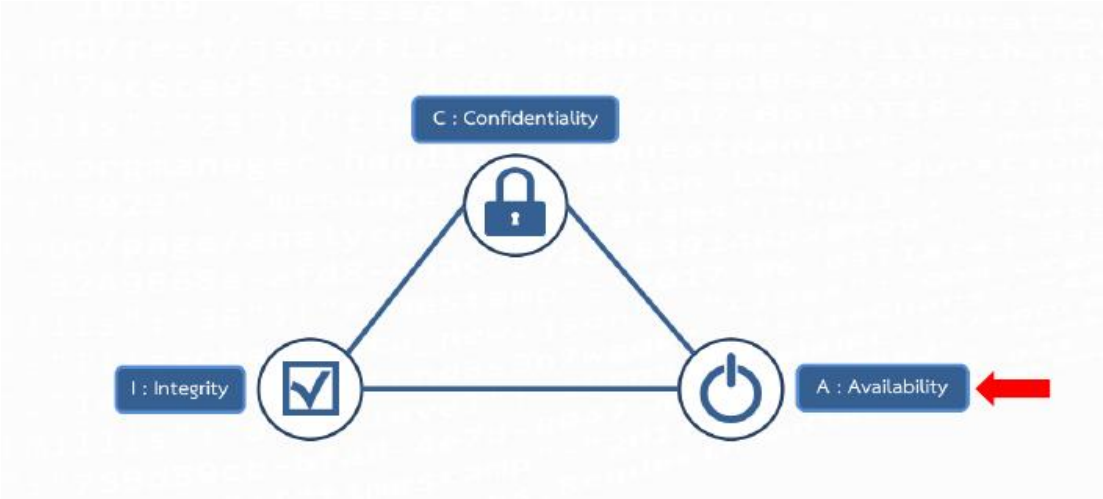
๑) ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็นความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น



๒.๒ Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

๑) ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

๒) ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



๒.๓ Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

๑) ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

๒) ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

๒.๔ รูปแบบภัยคุกคามของ CyberSecurity

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่ายรวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

๑) ไวรัส (Virus)

๒) เวิร์ม (Worms)

๓) โทรจัน (Trojans)

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

๒.๖ Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๒.๗ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น

๑) Code ของเว็บไซต์เช่น CMS

๒) Web Server หรือ Database Server

๒.๗.๑) วิธีการโจมตีที่นิยมใช้

๑) Cross-Site Scripting

๒) SQL Injection

๓) Path Traversal

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

๒.๘ DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๒.๙ Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๒.๙.๑ ผลกระทบ

๑) ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนไปเผยแพร่

๒) ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล

๓) สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๒.๑๐ Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๒.๑๑ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๒.๑๒ Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๒.๑๒.๑ วิธีการป้องกัน

๑) สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

๒) ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๓) ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

๒.๑๓ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวณผลเพื่อสร้างรายได้กลับไปที่ Hacker

๒.๑๔ ความตระหนักรู้ด้าน CyberSecurity ในชีวิตประจำวัน

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

๒.๑๕ การใช้ Password ที่ดี คือ

๑) มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)

๒) มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓) ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่ายเช่น password, ๑๒๓๔๕๖, วันเกิด หมายเลขโทรศัพท์

๔) มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕) ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖) ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗) ไม่ควรบอก Password แก่ผู้อื่น

๒.๑๖ สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑) ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๒) ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๓) ไม่คลิก Link ใน E-Mail โดยไม่มีการตรวจเช็ค

๔) เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

๓. ประโยชน์ที่ได้รับ

ได้รับความรู้และความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ เช่น การโจมตีทางฟิชชิ่ง มัลแวร์ และการหลอกลวงผ่านสื่อออนไลน์ สามารถนำความรู้ไปประยุกต์ใช้ในการป้องกันตนเองจากความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในชีวิตประจำวันและการทำงาน สามารถเป็นส่วนหนึ่งในการช่วยเฝ้าระวัง แจ้งเตือน และลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

๔. แนวทางการนำความรู้ไปปรับใช้ให้เกิดประโยชน์แก่หน่วยงาน นำความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ไปปรับใช้ในการปฏิบัติงานและการใช้งานระบบสารสนเทศอย่างถูกต้อง และสามารถเผยแพร่หรือแลกเปลี่ยนความรู้กับเพื่อนร่วมงาน เพื่อสร้างความตระหนักรู้ร่วมกันภายในหน่วยงาน

๕. ความต้องการการสนับสนุนจากผู้บังคับบัญชา (ถ้ามี) ส่งเสริมให้มีการเข้ารับการฝึกอบรมเพื่อเพิ่มทักษะความรู้ และสามารถนำมาประยุกต์ใช้ในองค์กรเพื่อให้เกิดประสิทธิภาพมากยิ่งขึ้น

(นางสาวชิดชนก แจ่มดี)
เจ้าพนักงานธุรการชำนาญงาน

(นางพรรทิภา น้อมนิล)
หัวหน้าฝ่ายบริหารทั่วไป