แบบฟอร์มสำหรับรายงานต่อ
ผู้บังคับบัญชา

แบบรายงานผลการพัฒนาความรู้ของข้าราชการ
สถานีพัฒนาที่ดินสมุทรปราการ สำนักงานพัฒนาที่ดินเขต ๑
รอบการประเมินที่.....๑/๒๕๖๙.....ตั้งแต่วันที่...๑ ต.ค. ๒๕๖๘ – ๓๑ มี.ค. ๒๕๖๙.....
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ-นามสกุล นางสาวสุรัชนา พิชญานนท์ **ตำแหน่ง** นักวิชาการเกษตรชำนาญการ
กลุ่ม/ฝ่าย สถานีพัฒนาที่ดินสมุทรปราการ สำนักงานพัฒนาที่ดินเขต ๑
หัวข้อการพัฒนา การสร้างความตระหนักรู้ด้านความมั่นคงทางไซต์เบอร์ (Cybersecurity Awareness)
.....
สถานที่ ระบบทางไกลอิเล็กทรอนิกส์ **วันที่** ๙ กุมภาพันธ์ ๒๕๖๙
วิทยากร/ผู้ให้ความรู้ วิทยากรจาก "TDGA" **หน่วยงานที่จัดอบรม** สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล

สรุปสาระสำคัญ

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซต์เบอร์ (Cybersecurity Awareness)

รายละเอียดบทเรียน

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงาน และชีวิตประจำวัน

วัตถุประสงค์

๑. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
๒. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆและแนวทางป้องกันแก้ไข
๓. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

หัวข้อในบทเรียน

- แนะนำบทเรียน
- Cybersecurity คืออะไร
- ความรู้พื้นฐานของ Cybersecurity
- รูปแบบภัยคุกคามของ Cybersecurity
- ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

Cybersecurity คืออะไร Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและ กระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึง จากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่อง ของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กร เพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ. ศ. ๒๕๖๒
- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ. ศ. ๒๕๖๐
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO ๒๗๐๐๑ (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

<u>ความรู้พื้นฐานของ Cybersecurity</u>

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัวซี(C) ตัวไอ(I) และตัวเอ(A)

C:Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรักษาความลับของข้อมูล คือ การที่ ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น - ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการ ส่วนทรัพยากรบุคคลเท่านั้น - เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงาน บริษัททุกคน

I: Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบบสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

A:Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

สรุปคือ CIA Model สามารถนำมาปรับใช้ให้เข้ากับส่วนของข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้

<u>รูปแบบภัยคุกคามของ Cybersecurity</u>

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบ ต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากร ของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆในเครือข่าย รวมถึงเซิร์ฟเวอร์ ต่างๆได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้น ครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไป ที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เพิ่มเติม : เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆเช่น E-Mail,SMS,เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆเช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL injection
- Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ แอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Inside threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น
ซึ่ง Inside threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้ภายในองค์กร Zero Trust เป็นคอนเซปต์การจัดการซิเคียวริตี้ สมัยใหม่ ที่หลายองค์กรได้นำมาปรับใช้ ตั้งแต่การตรวจสอบผู้เข้าระบบทุกครั้ง การให้สิทธิ์ที่น้อยที่สุดหรือ เท่าที่จำเป็นกับผู้ใช้งาน

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้ง โปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือ ดำเนินการ

บางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบ ว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

-สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

-ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

-ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

<u>ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน</u>

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล

๒. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

๔. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด password และติด password ไว้ที่หน้าจอ

๗. มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

สรุปเรื่องการสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ในส่วนของความปลอดภัยกับความ สะดวกสบาย ตัวอย่างในรูปจะให้เห็นว่าสิ่งที่เราต้องทำคือเราต้องพยายามถ่วงน้ำหนักให้เท่ากันในส่วนของ เรื่องความปลอดภัยทางด้านไซเบอร์ซีเคียวริตี้และความสะดวกสบาย หลักสูตรนี้น่าจะสร้างความตระหนักรู้ ความมั่นคงทางไซเบอร์ให้ทุกท่านได้เห็นภาพมากยิ่งขึ้นและในหลายๆส่วนอยากจะให้ทุกท่านนำไปปฏิบัติตาม เพื่อความปลอดภัยในชีวิตประจำวัน

(ลงนาม).....

(นางสาวสุรัชนา พิชญานนท์)

ตำแหน่ง นักวิชาการเกษตรชำนาญการ

(ลงนาม).....

(นางสาวสุดารัตน์ สุรินทร์)

ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินสมุทรปราการ