สรุปการพัฒนาความรู้

หลักสูตร การสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์

Cybersecurity Awareness

โดย สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (TDGA)

บรรยายโดย คุณพลากร ลาภอลงกรณ์
ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)

Cybersecurity คืออะไร ?

Cybersecurity หรือ ความมั่นคงปลอดภัยทางไซเบอร์ เป็นการนำเครื่องมือทางเทคโนโลยี รวมถึงกระบวนการต่าง ๆ มาป้องกันและรับมือจากการถูกโจมตีทางอินเทอร์เน็ต ปกป้องข้อมูลจากการโจรกรรมของพวกแฮกเกอร์ ป้องกันการรั่วไหลของข้อมูลจนก่อให้เกิดความเสียหายแก่องค์กร ในปัจจุบันนั้นหลายองค์กร จึงเลือกที่จะให้ความสำคัญกับการปกป้องข้อมูล ป้องกันการเข้าถึงการแก้ไขเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ไม่เหมาะสม

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562
- พ.ร.บ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2562
- พ.ร.บ.คุ้มครองส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

พื้นฐานของ Cybersecurity

C-I-A

Confidentiality

การรักษาความลับของข้อมูล คือ การระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

Integrity

การรักษาความถูกต้องของข้อมูล คือ การระบุสิทธิของการแก้ไขข้อมูลและการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง

Availability

ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล



รูปแบบภัยคุกคามของ Cybersecurity

Malware

สิ่งที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์แล้ว สามารถแชร์ข้อมูลไปยังเครื่องอื่นๆในเครือข่าย โดยมีพฤติกรรมต่างกันไปตามวัตถุประสงค์ของผู้ไม่หวังดี

Web-based attracks

วิธีโจมตีเหยื่อผ่านช่องทางเว็บไซต์ โจมตีเว็บไซต์ที่มีช่องโหว่ เมื่อเหยื่อเข้าสู่เว็บไซต์ดังกล่าว จะถูกนำไปสู่ปลายทางที่ถูกวาง Malware ไว้เพื่อทำให้อุปกรณ์ของเหยื่อติด Malware

Phishing

การโจมตีเหยื่อผ่านช่องทาง Social โดยวิธีหลอกล่อให้หลงเชื่อและยอมให้ข้อมูลส่วนตัว หรือข้อมูลสำคัญ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attracks

วิธีการโจมเว็บไซต์เป้าหมาย โดยอาศัยช่องโหวต่างๆ เช่น Code ของเว็บไซต์ Web Server หรือ Database Server วิธีโจมตีที่นิยม เช่น SQL injection หรือ Path Traversal

Spam

วิธีการที่ผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่างๆไปยังผู้รับ โดยการส่งเป็นจำนวนมากทั้งที่ไม่ได้รับอนุญาต เพื่อสร้างความรำคาญหรือก่อกวน

Distributed Denial of Service

วิธีการโจมเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่ต้นทางเป็นจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน ทำให้ระบบล่ม

Data Breach

การรั่วไหลของข้อมูล หรือการโจมตีเพื่อขโมยข้อมูลโดยที่เจ้าของไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลนั้นไปขาย หรือเพื่อเป็นการเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

Inside threat

เป็นภัยที่เกิดจากบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านอุปกรณ์ของตนเอง ที่มักจะมีการป้องกันอุปกรณ์ในระดับที่ต่ำ ทำให้เกิดการโจมตีได้ง่าย

Botnets หรือ Robot Network

โปรแกรมที่เขียนโดยผู้ไม่ประสงค์ดี ติดตั้งแฝงตัวไว้ในเครื่องคอมพิวเตอร์ เพื่อรอรับคำสั่งโจมตีเป้าหมายโดยจะทำงานเมื่อถูกสั่ง ทำให้เหยื่อไม่ทราบว่าติดตั้งเอาไว้

Ransomware

เป็นโปรแกรมที่เมื่อถูกติดตั้งแล้วจะทำการล็อคไฟล์ โดยวิธีเข้ารหัสไฟล์ข้อมูลในเครื่อง ทำให้ไม่สามารถเปิดใช้งานได้ จุดประสงค์นั้นก็เพื่อเป็นการเรียกค่าไถ่ในการปลดล็อคไฟล์

Cryptocurrency

เป็นเหรียญดิจิทัล ซึ่งจะมีการประมวลผลอยู่ตลอดเวลา การประมวลผลดังกล่าว ใช้พื้นที่บนเครื่องคอมพิวเตอร์เป็นจำนวนมาก ทำให้เสียพื้นที่ทั้งที่ไม่ได้ใช้งานอะไรเลย

ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

Computer

1. แยก User ที่ใช้งานของแต่ละบุคคลไม่ใช้ร่วมกัน
2. Log out เมื่อไม่อยู่ที่หน้าจอเครื่องคอมพิวเตอร์
3. ติดตั้ง Anti-Malware และมีการ update เสมอ
4. Update Patch ระบบปฏิบัติการของ OS เสมอ
5. Update Version โปรแกรมภายในเครื่องเสมอ
6. ไม่จด Password และติด Password ไว้หน้าจอ
7. ใช้ Password ที่ดี และไม่ควรบอกให้ผู้อื่นทราบ

E-mail

1. ไม่ควรเปิด E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจากผู้ที่น่าสงสัย หรือที่ไม่ชัดเจน
3. ไม่คลิก Link ใน E-mail ที่ไม่ได้มีการตรวจสอบ
4. ก่อนทำธุรกรรมต่างๆ ควรตรวจสอบก่อนทุกครั้ง

Messaging

1. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
2. หากไม่ใช่เครื่องส่วนตัวไม่ควรบันทึกไฟล์ต่างๆไว้
3. มีความตระหนักรู้ก่อนเปิด Link หรือ ไฟล์ต่างๆ
4. Update Version ของโปรแกรมอย่างสม่ำเสมอ

Conference

1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้เกี่ยวข้อง
3. แชร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ Update Program อย่างสม่ำเสมอ

Password

1. มีความซับซ้อน มีทั้งตัวเลข ตัวอักษร อักขระพิเศษ
2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร
3. หลีกเลี่ยง Password ที่สามารถคาดเดาได้โดยง่าย
4. มีการเปลี่ยน Password อยู่เรื่อยๆ อย่างสม่ำเสมอ
5. ใช้ Multi Factor Authentication หากใช้งานได้
6. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบที่ใช้งาน

Website

1. ไม่กดเข้าไปในเว็บไซต์ ที่ได้รับจากแหล่งที่ไม่แน่ชัด
2. ไม่ทำการบันทึก Password ต่างๆ ไว้บน Browser
3. เว็บไซต์ธุรกรรมสำคัญ ต้องเข้าผ่าน HTTPS เท่านั้น
4. ควรใช้ Browser ที่น่าเชื่อถือ เป็นที่นิยมใช้กันทั่วไป
5. ควรมีการ Update Version ของ Browser เสมอ
6. ถ้าไม่ใช่เครื่องส่วนตัวควรใช้ Safe Web browsing
7. ควรติดตั้ง Anti-Malware และ update สม่ำเสมอ

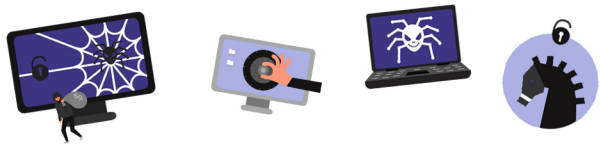
Fake News

Fake News คือ ข่าวปลอมที่เป็นภัยคุกคามใกล้ตัวเรา

1. มีการพาดหัวข่าว ข้อความเกินจริงเรียกความสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาเกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา

Cloud Store

1. แยก User ใช้งานแต่ละบุคคล
2. กำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็น
3. ปิดการเข้าถึงไฟล์เมื่อไม่จำเป็น
4. ติดตั้ง Anti-Malware และคอย update อยู่เสมอ
5. มีการ Update Program อย่างสม่ำเสมอ
6. ตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น



ประโยชน์ที่ได้จากการพัฒนาความรู้

ความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
ช่วยให้เราสามารถเปลี่ยนจาก "จุดอ่อน" กลายเป็น "ด่านหน้า" ความปลอดภัย
โดยทำให้สามารถรู้เท่าทันกลโกงทางไซเบอร์ ที่เทคโนโลยีป้องกันไม่ได้ 100%
นอกจากนี้ยังช่วยสร้างนิสัยการป้องกันเชิงรุก เช่น การตั้งรหัสผ่านที่ซับซ้อน
เพื่อรักษาความเป็นส่วนตัว และปกป้องข้อมูลสำคัญขององค์กร
ท้ายที่สุดคือการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์
ที่อาจสร้างความเสียหายทั้งต่อทรัพย์สินและชื่อเสียงได้อย่างยั่งยืน

จัดทำโดย

นางสาวฐานิตา กุญแจทอง
ตำแหน่งเจ้าหน้าที่ระบบงานคอมพิวเตอร์
กลุ่มทะเบียนประวัติและบำเหน็จความชอบ
กองการเจ้าหน้าที่

กุมภาพันธ์ 2569