การสร้างความตระหนักรู้ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Awareness)

นางสาวอุบลวรรณ วรรณใหญ่ เจ้าพนักงานธุรการปฏิบัติงาน กองเทคโนโลยีชีวภาพทางดิน
ที่มา : วันที่ 12 กุมภาพันธ์ 2569 อบรมออนไลน์ผ่าน TDGA (TDGA e-Learning) ชื่อวิทยากร คุณพลากร ลาภอลงกรณ์ สังกัด : TDGA

Cybersecurity หรือความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึง จากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่อง ของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้นเนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น

1. Cyber Security มี 5 ประเภทดังนี้

1.1 Critical Infrastructure Security คือเป็นการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐานที่สำคัญ การสร้างระบบความปลอดภัยที่เหมาะสมเป็นสิ่งจำเป็น เนื่องจากหากไม่มีการป้องกันอย่างเหมาะสม อาจเกิดความเสี่ยงที่จะถูกโจมตีมากกว่ารูปแบบอื่น โดยเฉพาะระบบรักษาความปลอดภัยของธนาคาร ตลาดหลักทรัพย์ รัฐบาล ที่มีข้อมูลส่วนบุคคลอยู่เป็นจำนวนมาก หรือแม้กระทั่งข้อมูลทางการเงินก็นับว่าเป็นข้อมูลละเอียดอ่อน ที่การรักษาความปลอดภัย Critical Infrastructure Security จะต้องทำโครงสร้างออกมาให้แข็งแรง เพื่อป้องกันข้อมูลได้ดียิ่งขึ้น

1.2 Network Security คือ การรักษาความปลอดภัยของระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นการป้องกันการคุกคามจากบุคคลภายนอกที่พยายามเข้าถึงและใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยไม่ได้รับอนุญาต ร่วมกับการนำเทคโนโลยีและระบบปัญญาประดิษฐ์มาช่วยเพื่อตรวจจับและแจ้งเตือนเกี่ยวกับความผิดปกติที่เกิดขึ้นในส่วนนี้

1.3 Cloud Security หากองค์กรตัดสินใจเก็บข้อมูลต่าง ๆ ในเซิร์ฟเวอร์ภายในบริษัท จะมีความเสี่ยงที่ข้อมูลอาจถูกโจมตีได้ การโอนย้ายข้อมูลเพื่อจัดเก็บบน Cloud Security เป็นตัวช่วยที่สามารถเพิ่มความปลอดภัยและประหยัดค่าใช้จ่ายได้มากขึ้น อีกทั้งในปัจจุบันระบบความปลอดภัยของคลาวด์ก็มีการพัฒนาและปรับปรุงอย่างต่อเนื่อง ทำให้เหมาะสมกับความต้องการและเป็นทางเลือกที่ดีในการใช้งาน

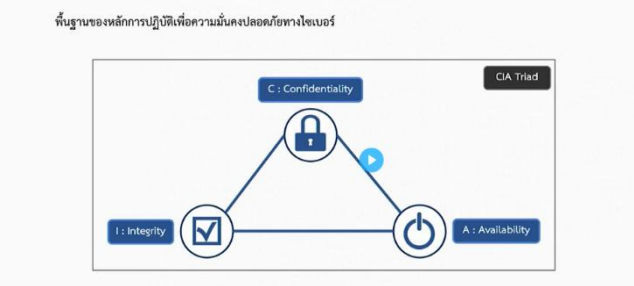
1.4 Application Security ในกระบวนการพัฒนาหรือติดตั้งแอปพลิเคชัน อาจเกิดการโจมตีหรือการแฝงตัวเข้ามาได้ ดังนั้นการเลือกใช้ตัวช่วยในการรักษาความปลอดภัยผ่านแอปพลิเคชันเป็นทางเลือกที่ดีเพื่อเพิ่มระดับความปลอดภัยให้กับกระบวนการพัฒนาระบบได้อีกวิธีหนึ่ง

1.5 Internet of Things Security การรักษาความปลอดภัยบนอุปกรณ์ Internet of Things (IoT) ที่มีการใช้งานตลอดเวลาเป็นเรื่องสำคัญ เนื่องจากระบบมีการส่งรับข้อมูลผ่านเครือข่ายอินเทอร์เน็ต

ดังนั้นจำเป็นต้องมีการกำหนดมาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยบนอุปกรณ์เหล่านี้ให้มีประสิทธิภาพและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

2. ความรู้พื้นฐานของ Cybersecurity

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



ภาพ CIA model

C : Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้

I : Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบบสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง

A : Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล

สรุปคือ CIA Model สามารถนำมาปรับใช้ให้เข้ากับส่วนของข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้

3. รูปแบบภัยคุกคามของ Cybersecurity

ภาพ Cybersecurity

ในภาพคือตัวอย่างจาก ENISA คือ องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ สรุป 15 ภัยคุกคามที่ เกิดขึ้นในปี 2020

3.1 Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบ ต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้

สามารถเข้าถึงทรัพยากร ของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆใน เครือข่าย รวมถึงเซิร์ฟเวอร์ ต่างๆได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้น ครอบคลุมถึง

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

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

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

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

4. ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน มีดั้งนี้

4.1 Computer สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

4.1.1 ควรมีการแยก user ใช้งานกันของแต่ละบุคคล

4.1.2 ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

4.1.3 ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

4.1.4 มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

4.1.5 มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

4.2 Password สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

4.2.1 มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

4.2.2 มีความยาวของ Password อย่างน้อย 8 ตัวอักษร

4.2.3 ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดา ได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์

4.2.4 มีการเปลี่ยน Password อย่างสม่ำเสมอ

4.3 Messaging สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

4.3.1 ไม่ควรบันทึก password ไว้ที่โปรแกรม

4.3.2 กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง

4.3.3 มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา