

Hakka.
ハッカー

C R E A T I V E

CYBERSECURITY

BEGINNING

SUPACHAI POOPAINGAM

2022

.....

TABLE OF CONTENTS

.....

Our content today is divided into six parts. Each part will be described with examples.

01

Module Objectives

02

Module Description

03

Key Topics

04

Key Terminologies

05

Module Contents

06

Module Summary

MODULE OBJECTIVES

1.1

อธิบายนิยามและแนวคิดเกี่ยวกับหลักการด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยใชเบอร์

1.2

อภิปรายคุณสมบัติและองค์ประกอบต่าง ๆ ที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ

1.3

เรียนรู้เกี่ยวกับแนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย การทำงานและการใช้งาน

1.4

อภิปรายประเภท รูปแบบของภัยคุกคามและการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ

1.5

อภิปรายแนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

1.6

ทำความเข้าใจความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ



MODULE DESCRIPTION

ความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูล สารสนเทศ และระบบสารสนเทศ องค์ประกอบคุณสมบัติหลักด้านความมั่นคงปลอดภัยสารสนเทศ 3 ด้าน (การรักษาความลับ ความถูกต้อง และความพร้อมใช้) และองค์ประกอบสำคัญอื่นที่เกี่ยวข้อง แนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย พังก์ชันการทำงาน และการใช้งาน

(the Security, Functionality and Usability Triangle) สำหรับการกำหนดระดับความมั่นคงปลอดภัยสารสนเทศ รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ ประเภทภัยคุกคามและช่องโหว่ ลักษณะภัยคุกคามทางไซเบอร์ แนวโน้มด้านความมั่นคงปลอดภัย การบริหารความเสี่ยงและมาตรการจัดการความเสี่ยง



KEY TOPICS

กลุ่มสาระเนื้อหาที่เราจะได้รับจาก
บทเรียนต่อไปนี้

1

แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ/ไซเบอร์

2

องค์ประกอบและคุณสมบัติด้านความมั่นคงปลอดภัยสารสนเทศ

3

ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

4

ประเภทการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ

5

แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

6

ความเสี่ยงด้านความมั่นคงปลอดภัยและมาตรการจัดการ

KEY TERMINOLOGIES

นิยามความสำคัญในแต่ละบท
เรียน



Information
Security



Confidentiality



Integrity



Availability



Cybersecurity



Cyber



CyberThreats

THE
**INFORMATION
SECURITY**



“ความมั่นคงปลอดภัยด้านสารสนเทศ”

(1) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การรำรงไว้ซึ่ง

- ความลับ (Confidentiality)
- ความถูกต้องครบถ้วน (Integrity)
- สภาพพร้อมใช้งาน (Availability)

รวมทั้งคุณสมบัติอื่น ได้แก่

- ความถูกต้องแท้จริง (Authenticity)
- ความรับผิด (Accountability)
- การห้ามปฏิเสธความรับผิด (Non-repudiation)
- ความน่าเชื่อถือ (Reliability)

(2) “ความมั่นคงปลอดภัยของระบบสารสนเทศ” หมายความว่า

การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึงใช้เปิดเผยขัดขวางเปลี่ยนแปลงแก้ไขทำให้สูญหายทำให้เสียหายถูกทำลายหรือล่วงรู้โดยไม่ชอบ

THE
CONFIDENTIALITY



“การรักษาความลับ”

“การรักษาความลับ”

หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึงใช้หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

THE
INTEGRITY



.....

“การรักษาความครบถ้วน”

“การรักษาความครบถ้วน”

หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งานประจำผลโอบหรือเก็บรักษาเพื่อมิให้มีการเปลี่ยนแปลงแก้ไขทำให้สูญเสียทำให้เสียหายหรือถูกกำล่ายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

THE
AVAILABILITY



“การรักษาสภาพร้อนใช้งาน”

“การรักษาสภาพร้อนใช้งาน”

หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงานเข้าถึงหรือใช้งานได้ในเวลาที่ต้องการ

THE
CYBERSECURITY



“การรักษาความมั่นคงปลอดภัยไซเบอร์”

“การรักษาความมั่นคงปลอดภัยไซเบอร์”

หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

THE
CYBER



.....

“ไซเบอร์”

“ไซเบอร์”

หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรศัพท์ รวมถึงการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

THE
CYBERTHREATS



“กัยคุกความทางไซเบอร์”

“กัยคุกความทางไซเบอร์”

หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยต่อรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

ลักษณะของกัยคุกความทางไซเบอร์ แบ่งออกเป็น 3 ระดับ ได้แก่ กัยคุกความทางไซเบอร์ในระดับไม่ร้ายแรงกัยคุกความทางไซเบอร์ในระดับร้ายแรง กัยคุกความทางไซเบอร์ในระดับวิกฤติ

MODULE CONTENTS

- แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ
- หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ
- คุณสมบัติและองค์ประกอบหลักด้านความมั่นคงปลอดภัยฯ
- คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงฯ
- ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัยฯ
- การรักษาความมั่นคงปลอดภัยไซเบอร์
- การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล
- ความท้าทายด้านความมั่นคงปลอดภัยสารสนเทศ
- กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ
- ลักษณะของภัยคุกคามทางไซเบอร์
- รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ
- ประเภทการโจมตีระบบสารสนเทศ
- แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ
- การบริหารความเสี่ยงและมาตรการจัดการ

แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศ

คือ การสร้างความมั่นใจในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ของสารสนเทศ ตลอดจนข้อมูล ระบบสารสนเทศ และทรัพย์สินสารสนเทศ ซึ่งครอบคลุมถึงข้อมูลที่จัดเก็บ ประมวลผล และรับส่งผ่านเครือข่าย จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยไม่ได้รับอนุญาต การใช้ในการที่ผิด การทำลายหรือการเปลี่ยนแปลง โดยมีการบริหารจัดการความเสี่ยง และนำมาตรการต่าง ๆ ด้านบริหารจัดการ ด้านเทคโนโลยีด้านกายภาพที่เหมาะสมมาใช้จัดการภัยคุกคามต่าง ๆ

แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ

การรักษาความมั่นคงปลอดภัยสารสนเทศและการบริหารความเสี่ยง

จุดมุ่งหมายเพื่อสร้างความมั่นใจต่อการดำเนินธุรกิจได้อย่างต่อเนื่องและยั่งยืน ลดผลกระทบที่เกิดขึ้นจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการปฏิบัติตามข้อกำหนดของกฎหมายและกฎเกณฑ์ที่มีผลใช้บังคับ ภายใต้สภาพความเสี่ยงที่ยอมรับได้ขององค์กร

หลักการสำคัญของการรักษาความมั่นคง ปลอดภัยสารสนเทศ

หลักการพื้นฐานสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

คือ การปกป้องทรัพย์สินสารสนเทศตามสภาพความเสี่ยงขององค์กร การสร้างความตระหนักรู้เกี่ยวกับความจำเป็นและความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ การกำหนดความรับผิดชอบและนโยบายสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ความต่อเนื่องในการให้บริการข้อมูลสารสนเทศระบบ และทรัพย์สินสารสนเทศ

โดยดำเนินการในเชิงกระบวนการอย่างเป็นระบบและต่อเนื่องพร้อมกับประสิทธิผลของมาตรการควบคุมทั้งมาตรการด้านบริหารจัดการ (Administrative) มาตรการด้านเทคนิค (Technical) และมาตรการทางกายภาพ (Physical security) ตอบสนองความต้องการทางธุรกิจและกลุ่มผู้มีส่วนได้เสีย และภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ขององค์กร

คุณสมบัติและองค์ประกอบหลักด้านความ มั่นคงปลอดภัยสารสนเทศ

C

การรักษาความลับ (Confidentiality)

ข้อมูล สารสนเทศ เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้น จะต้องไม่มีการเปิดเผยโดยบังเอิญ หรือโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต

I

การรักษาความถูกต้องครบถ้วน (Integrity)

ข้อมูล สารสนเทศ มีความถูกต้อง จะมีการแก้ไข เปลี่ยนแปลง ได้เฉพาะผู้ที่มีสิทธิ์ หรือได้รับอนุญาตเท่านั้น

A

สภาพความพร้อมใช้ (Availability)

ข้อมูล สารสนเทศ มีความพร้อมในการใช้งานอยู่เสมอผู้มีสิทธิ์หรือได้รับอนุญาตสามารถเข้าถึงได้เมื่อต้องการ

คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้อง ด้านความมั่นคงปลอดภัยสารสนเทศ

A

ความถูกต้องแท้จริง
(Authenticity)

คุณลักษณะเฉพาะเพื่อยืนยัน
ความถูกต้องแท้จริงถึงตัว
ตนผู้ใช้งาน

A

ความรับผิด
(Accountability)

ความรับผิดชอบที่สามารถ
ตรวจสอบได้

N

การห้ามปฏิเสธความรับผิด
(Non-repudiation)

วิธีการที่ผู้ส่งและผู้รับ
ข้อความจะไม่สามารถปฏิเสธ
การส่งหรือการรับข้อความ
นั้นได้ หากได้ดำเนินการนั้นไป
แล้ว

A

ความน่าเชื่อถือ
(Reliability)

ความสามารถในการให้บริการ
ได้ตามที่กำหนดไว้

ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคง ปลอดภัย การทำงาน และการใช้งาน

การกำหนด “ระดับความมั่นคงปลอดภัยของสารสนเทศ” ต้องพิจารณาการรักษาความสมดุลขององค์ประกอบ 3 ด้าน ที่เรียกว่า “ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย ด้านฟังก์ชันการทำงาน และด้านการใช้งาน” ซึ่งจะต้องยึดหยุ่น หรือปรับไปตามจุดประสงค์ที่ต้องการ จากข้อกำหนดด้านความมั่นคงปลอดภัย (Requirements) คุณลักษณะ (Features) และความต้องการใช้งาน (GUI) ตัวอย่างเช่น ในบางครั้งเพื่อตอบสนองความสะดวกในการใช้งาน ก็อาจจำเป็นต้องลดระดับมาตรการด้านความมั่นคงปลอดภัย

การรักษาความมั่นคงปลอดภัยไซเบอร์

การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการปกป้องด้านความมั่นคงปลอดภัยจากภัยคุกคามต่าง ๆ ตามเป้าหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ ในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ สำหรับข้อมูลสารสนเทศ และระบบสารสนเทศ ในสภาพแวดล้อมไซเบอร์ที่มีการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรศัพท์เคลื่อนที่ รวมถึงการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อ กันเป็นการทั่วไป ทั้งนี้ เพื่อดำเนินการมาตราการจัดการภัยคุกคามทางไซเบอร์

การรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure: CII) จะต้องมีการประเมินและตรวจสอบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือคาดว่าจะเกิดขึ้นหรือไม่ โดยให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตาม ประมวลแนวทางปฏิบัติและกรอบ มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลคือ การตรวจสอบความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคลทั้งนี้ เพื่อป้องกัน การสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยไม่ชอบ โดยต้องมีมาตรการป้องกันด้านการบริหารจัดการด้านเทคนิคและด้านกฎหมาย น้อยครอบคลุมในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล (AccessControl)

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

DataBreach: การรั่วไหลของข้อมูล และเหตุละเมิดที่เกี่ยวข้องกับข้อมูล ซึ่งมีสิทธิสูงเพิ่มขึ้นเรื่อย ๆ ได้กลายเป็นภัยคุกคามร้ายแรงต่อองค์กร ทั้งกรณีข้อมูลเสียหายสูญหาย รวมถึงประเด็นด้านชื่อเสียงและภาพลักษณ์ขององค์กร อันเนื่องมาจากการละเมิดหรือเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์

ความท้าทายด้านความมั่นคงปลอดภัยสารสนเทศ และความมั่นคงปลอดภัยไซเบอร์

- ความก้าวหน้าและการเปลี่ยนแปลงด้านเทคโนโลยี
- การเพิ่มมากขึ้นของระบบงานผ่านเครือข่าย
- ความซับซ้อนของการบริหารจัดการเทคโนโลยีระบบคอมพิวเตอร์ และโครงสร้างพื้นฐาน
- ความยุ่งยากในการจัดการสภาพแวดล้อมระบบที่กระจายภายใต้การจัดการแบบรวมศูนย์
- เหตุละเมิดด้านความมั่นคงปลอดภัยและการรั่วไหลของข้อมูลที่ส่งผลกระทบต่อองค์กร
- ความสามารถในการปฏิบัติตามกฎหมายและข้อกำหนดของหน่วยงานกำกับดูแล
- การรักษาความต่อเนื่องและความพร้อมรับมือต่อภัยคุกคามในการให้บริการระบบและข้อมูล

กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัย สารสนเทศ

(1) ภัยคุกคามระบบเครือข่าย (Network Threats)

ภัยคุกคามที่มีต่อชุดระบบคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เชื่อมต่อกันด้วยช่องทางเครือข่ายสื่อสารเพื่อแบ่งปันทรัพยากรและข้อมูล โดยที่ผู้ไม่ประสงค์ดีอาจเจาะเข้าไปในช่องทางเครือข่ายสื่อสาร เพื่อขโมยข้อมูล ที่ส่งผ่านเครือข่าย หรือกระทำได้ ฯ ที่ส่งผลต่อข้อมูล สารสนเทศ และระบบสารสนเทศ

NETWORK THREATS

Information Gathering	การล่าดตามะเวน หรือเก็บรวบรวมข้อมูลของเป้าหมาย
Sniffing and Eavesdropping	การดักจับข้อมูลและการลักลอบดักฟัง
Spoofing	การปลอมตัวเพื่อโจมตีระบบหรือควบคุมระบบ
Session Hijacking, Man-in-the-Middle Attack	การขโมยเชสชั่นและปลอมแทรกระหว่างกลาง
DNS and ARP Poisoning	การเปลี่ยนข้อมูลโดเมนเว็บไปยังปลายทางอื่น
Password-based Attacks	การโจมตีรหัสผ่าน
Denial-of-Service Attack	การโจมตีระบบให้บริการหยุดชะงัก
Compromised-key Attack	การโจมตีเจาะกุญแจรหัส
Firewall and IDS Attacks	การโจมตีอุปกรณ์ความปลอดภัยเครือข่าย

กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัย สารสนเทศ

(2) ภัยคุกคามระบบโฮสต์ (Host Threats)

ภัยคุกคามที่มุ่งเป้าระบบโฮสต์เฉพาะที่มีข้อมูลที่มีค่าหรือความสำคัญ ผู้ไม่ประสงค์ดีพยายามละเมิดความปลอดภัยของกริพยากรระบบข้อมูล ซึ่งส่งผลต่อการใช้งาน

NETWORK THREATS

Malware Attacks

การโจมตีด้วยมัลแวร์

Footprinting

การสำรวจร่องรอยและรวบรวมข้อมูลระบบ

Password Attacks

การโจมตีรหัสผ่าน

Denial-of-Service Attack

การโจมตีระบบให้บริการหยุดชะงัก

Arbitrary Code Execution

การสั่งดำเนินการด้วยคำสั่งแปลกปлом

Unauthorized Access

การเข้าถึงโดยไม่ได้รับอนุญาต

Privilege Escalation

การยกระดับสิทธิ์ของผู้ไม่ประสงค์ดีเพื่อควบคุมระบบ

Backdoor Attacks

การโจมตีผ่านเส้นทางลับที่เป็นรูร่วงของระบบ

Physical Security Threats

ภัยคุกคามด้านความมั่นคงปลอดภัยทางกายภาพ

กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัย สารสนเทศ

(3) ภัยคุกคามระบบงาน (Application Threats)

ภัยคุกคามที่มีต่อช่องโหว่ของระบบงานหรือระบบสารสนเทศ อันเนื่องมาจากการด้านความมั่นคงปลอดภัยที่ไม่เหมาะสมในระหว่างการพัฒนาหรือการบำรุงรักษาระบบ

NETWORK THREATS

Improper Data/Input Validation

การตรวจสอบข้อมูลหรือการนำเข้าสู่ระบบที่ไม่เหมาะสม

Authentication and Authorization Attacks

การโจมตีต่อการยืนยันตัวตนและการพิสูจน์ตัวตน

Security Misconfiguration

การตั้งค่าผิดพลาดด้านความมั่นคงปลอดภัย

Information Disclosure

การเปิดเผยข้อมูล

Broken Session Management

การจัดการเซสชันที่บกพร่อง

Buffer Overflow Issues

ปัญหาจากข้อมูลไม่ประسঙค์ได้ที่เกินขนาดความจุหน่วยความจำชั่วคราว

Cryptography Attacks

การโจมตีด้านการเข้ารหัสลับ

SQL Injection

การใช้คำสั่ง SQL เพื่อทำความเสียหายต่อระบบฐานข้อมูล

Improper Error Handling and Exception Management)

ความบกพร่องในการจัดการข้อผิดพลาด

ลักษณะของภัยคุกคามทางไซเบอร์

ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์หรือ **ภัยคุกคามทางไซเบอร์** หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมีช่องโถด้วยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยันตรายที่ใกล้จะถึง

ลักษณะของภัยคุกคามทางไซเบอร์

ลักษณะของภัยคุกคามทางไซเบอร์แบ่งออกเป็น 3 ระดับ

- ภัยคุกคามทางไซเบอร์ในระดับวิกฤต
- ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
- ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ລັກສະນະຂອງກັຍຄຸກຄາມກາງໄຊເບ່ອຮ

(1) ກັຍຄຸກຄາມກາງໄຊເບ່ອຮໃນຮະດັບໄມ່ຮ້າຍແຮງ

ກັຍຄຸກຄາມກາງໄຊເບ່ອຮທີ່ມີຄວາມເສື່ອງອຍ່າງມີນັຍສໍາຄັນກຶ່ງຮະດັບທີ່ກຳໃຫ້ຮະບບຄອມພິວເຕອົບຂອງໜ່ວຍ
ງານໂຄຮງສ້າງພື້ນຖານສໍາຄັນຂອງປະເທດ (CII) ຮີ່ອການໃຫ້ບໍລິການຂອງຮັຈ ດ້ວຍປະສິກີກາພລົງ

ລັກຜະບອນກໍາຕຸກຄາມທາງໄຊເບອຣ

(2) ກໍາຕຸກຄາມທາງໄຊເບອຣໃນຮະດັບຮ້າຍແຮງ

ກໍາຕຸກຄາມທີ່ມີລັກຜະບອນພົມເປັນຂຶ້ນຍ່ອຍຢ່າງນິບ້າຍສໍາຄັນຂອງການໂຈມຕີຮະບບຄອມພິວເຕອຣ ຄອມພິວເຕອຣ ທີ່ຮູ້ອໜ້າມູລຄອມພິວເຕອຣ ໂດຍມຸ່ງໝາຍເພື່ອໂຈມຕີໂຄຮງສ້າງພື້ນຫຼານສໍາຄັນຂອງປະເທດແລະການໂຈມຕີ ດັ່ງກ່າວມີຜລກຳໃຫ້ຮະບບຄອມພິວເຕອຣທີ່ໂຄຮງສ້າງສໍາຄັນການສາຮສນເຖິກທີ່ເກີ່ຽວຂ້ອງກັບການໃຫ້ ບຣິກາຮອງໂຄຮງສ້າງພື້ນຫຼານສໍາຄັນຂອງປະເທດ ຄວາມມື້ນຄົງຂອງຮັບຮັບ ຄວາມສັນພັນຮະຫວ່າງປະເທດ ກາຮປ້ອງກັນປະເທດ ເຄຮ່ອງກົງ ກາຮສາຮາຮນສຸຂ ຄວາມປລອດກໍາຕຸກຄາມທາງໄຊເບອຣ ທີ່ຮູ້ອໜ້າມູລຄອມພິວເຕອຣ ຂອງປະຊາບເສີ່ຍ້າຍ ຈົນໄມ່ສາມາດກຳດັບກຳດັກໄດ້

ລັກສະນະຂອງກໍາຄຸກຄາມທາງໄຊເບອຣ

(3) ភាយគុកការពារនៃបច្ចេកទេស

- เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศไทยลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศไทยที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

ลักษณะของกัยคุกความทางไซเบอร์

(3) กัยคุกความทางไซเบอร์ในระดับวิกฤต

- เป็นกัยคุกความทางไซเบอร์อันกระแทบ หรืออาจกระแทบต่อความสงบเรียบร้อยของประชาชน หรือ เป็นกัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำการใดๆ ที่มีผลต่อการดำเนินการตามกฎหมายอาญา การระบุ หรือการสังหาร ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกคล้องระบบ ประชาธิปไตยอันมีพระบรมราชูปถัมภ์เป็นประบุขตามรัฐธรรมบัญญัติแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความ ปลอดภัยของประชาชน การดำเนินชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย หรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหาย จากภัยพิบัติสาธารณสุขอันมีมาอย่างจุกเจ็บและร้ายแรง

រូបແບບការໂຈມពីដោយគ្មានម៉ែនគង់ផ្តល់កាយ សារសហពេទ្យនិងគ្មានម៉ែនគង់ផ្តល់កាយឱចបេវេរ

- កាយគ្មានការការងារឱចបេវេរបានបានបាន (Advanced Persistent Threats: APT)
- កាយគ្មានការពេញចិត្តនិងការប្រើប្រាស់ការពេញចិត្ត (Mobile Threats)
- កាយគ្មានការប្រើប្រាស់បណ្តុះបណ្តាល (Cloud Computing Threats)
- ម៉ាល់វេរ ឲវេសគុមពិវេទេរ និងអនុគមពិវេទេរ (Malware, Virus and Worms)
- បុណ្យលើក (Botnet)
- ការໂຈមពីកីឡើងខ្លួនជាកាយនៃក្រសួង (Insider Attack)

ประเภทการโจมตีระบบสารสนเทศ

ระบบที่มีจุดบกพร่องหรือช่องโหว่ด้านความมั่นคงปลอดภัย อันเนื่องมาจากการพัฒนาและบำรุงรักษาระบบที่ไม่ดีหรือไม่เหมาะสม การทดสอบที่ไม่เพียงพอ รวมถึงการกำหนดค่าความปลอดภัยของระบบอย่างผิดพลาดหรือไม่ถูกต้อง เป็นช่องโหว่ให้ผู้โจมตีสามารถเข้าถึงข้อมูลหรือระบบหรืออาจใช้ประโยชน์โดยมิชอบ

ผู้ดูแลระบบควรต้องตรวจสอบและปรับปรุงแก้ไขช่องโหว่ระบบอย่างสม่ำเสมอ รวมทั้งเปลี่ยนการใช้ค่าเริ่มต้นของอุปกรณ์และระบบ ปิดใช้งานพอร์ตและบริการที่ไม่จำเป็น เพื่อลดความเสี่ยงจากการโจมตีระบบสารสนเทศ โดยจำแนกประเภทการโจมตี เป็น 4 ระดับ

- ระดับระบบปฏิบัติการ Operating System Attacks
- ระดับค่าการติดตั้งระบบ Mis-configuration Attacks
- ระดับระบบงาน Application-Level Attacks
- ระดับชุดคำสั่งระบบ Shrink-Wrap Code Attacks

ประเภทการโจมตีระบบสารสนเทศ

(1) การโจมตีระบบปฏิบัติการ (Operating System Attacks)

ช่องโหว่บางอย่างของระบบปฏิบัติการ ตัวอย่าง ได้แก่

- ช่องโหว่ในพื้นที่หน่วยความจำชั่วคราว (Buffer overflow vulnerabilities)
- จุดบกพร่องในระบบปฏิบัติการ (Bugs in the operating system)
- ระบบปฏิบัติการที่ไม่มีการแก้ไขปรับปรุง (An unpatched operating system)

การโจมตีในระดับระบบปฏิบัติการ ตัวอย่าง ได้แก่

- การใช้ประโยชน์จากการใช้งานโปรโตคอลเครือข่ายที่เฉพาะเจาะจง (Exploiting specific network protocol implementations)
- การโจมตีผ่านระบบพิสูจน์ตัวตนที่ติดตั้งในระบบ (Attacking built-in authentication systems)
- การทำลายความมั่นคงปลอดภัยของระบบแฟ้มข้อมูล (Breaking file-system security)
- การเจาะรหัสผ่านและกลไกการเข้ารหัส (Cracking passwords and encryption mechanisms)

ประเภทการโจมตีระบบสารสนเทศ

(2) การโจมตีที่มีต่อการกำหนดค่าติดตั้งระบบที่ไม่ถูกต้อง (Mis-configuration Attacks)

การตั้งค่าความปลอดภัยของระบบที่ผิดพลาดหรือไม่ถูกต้อง เป็นช่องโหว่ที่มีผลต่อเครื่องแม่ป้ำย ระบบเว็บ แพลตฟอร์มระบบงาน ฐานข้อมูล เครือข่าย หรือกระบวนการทำงาน ซึ่งอาจมีการเข้าถึงโดย มิชอบ ดังนั้น จึงควรต้องมีการตรวจหาช่องโหว่อย่างสม่ำเสมอ และปิดใช้บริการที่ไม่จำเป็น

ประเภทการโจมตีระบบสารสนเทศ

(3) การโจมตีในระดับระบบงาน (Application-Level Attacks)

การพัฒนาและทดสอบที่ไม่สมบูรณ์เพียงพอ หรืออาจมาจากการขาดความตระหนักร้านความมั่นคง ปลอดภัย ทำให้เกิดช่องโหว่และเป็นเป้าหมายการโจมตีระบบ ตัวอย่าง ได้แก่

- การโจมตีช่องโหว่ในพื้นที่หน่วยความจำชั่วคราว (Buffer Overflow Attacks)
- การเปิดเผยข้อมูลที่ละเอียดอ่อน (Sensitive Information Disclosure)
- การผังชุดคำสั่งเพื่อขโมยข้อมูล (Cross-site Scripting)
- การขโมยเชสชั่นการทำงานระบบ (Session Hijacking)
- การโจมตีโดยการปลอมแทรกระหว่างกลาง (Man-in-the-middle Attacks)
- การโจมตีระบบให้บริการหยุดชะงัก (Denial-of-service Attacks)
- การโจมตีโดยการใช้คำสั่ง SQL เพื่อให้เกิดความเสียหายต่อระบบฐานข้อมูล (SQL Injection Attacks)
- การหลอกลวงผ่านอีเมลหรือข้อความอิเล็กทรอนิกส์ (Phishing)
- การแทรกแซงเพื่อควบคุมพารามิเตอร์หรือเปลี่ยนข้อมูล (Parameter / Form Tampering)
- การโจมตีช่องโหว่ที่เข้าถึงระบบไฟล์ (Android)(Directory Traversal Attacks)

ประเภทการโจมตีระบบสารสนเทศ

(4) การโจมตีผ่านชุดคำสั่งสาราระนະ (Shrink-Wrap Code Attacks)

นักพัฒนาซอฟต์แวร์มักจะใช้ชุดคำสั่ง (Libraries and Code) ที่ได้รับอนุญาตจากแหล่งอื่น เพื่อลดเวลาและค่าใช้จ่ายในการพัฒนา ซึ่งเป็นความเสี่ยงหากผู้ไม่ประสงค์ดีค้นพบช่องโหว่ในชุดคำสั่งนั้น ดังนั้น จึงจำเป็นต้องมีการปรับแต่งชุดคำสั่ง หรือเพิ่มค่าความบันคงปลอดภัย

แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

- เทคโนโลยีใหม่ ๆ อาจยังไม่มีความมั่นคงปลอดภัยได้ทันที หรือไม่เพียงพอ
- การโจมตีข้อมูลขององค์กร และข้อมูลส่วนบุคคลในระบบคลาวด์เพิ่มขึ้น
- มัลแวร์ผ่าน SMS แพร่หลายมากขึ้นบนโทรศัพท์มือถือ และอุปกรณ์พกพา
- การยืดบัญชีผู้ใช้งานที่เป็นเหยื่อจากสื่อสังคมออนไลน์ หรือโปรแกรมต่าง ๆ ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงโทรศัพท์มือถือ หรืออุปกรณ์พกพาของเหยื่อ เพื่อเข้าถึงข้อมูลและบัญชีอื่นได้
- ผู้ไม่ประสงค์ดีใช้เทคโนโลยีในการล่อหลวงระดับผู้บริหาร ให้เปิดเผยข้อมูลมากยิ่งขึ้น เพื่อร่วบรวมและเข้าถึงข้อมูลในองค์กร โดยใช้สื่อสังคมออนไลน์ เช่น LinkedIn หรือกระบวนการหลอกลวงทางไซเบอร์/วิศวกรรมสังคม (Social Engineering)
- หน่วยงานของรัฐ/หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) เป็นกลุ่มเป้าหมายการโจมตีจากผู้ไม่ประสงค์ดี/อาชญากรไซเบอร์ที่เพิ่มมากขึ้น
- อาชญากรไซเบอร์มุ่งเป้าหมายไปที่ลิงก์ที่อ่อนแอกลืนหัวใจในห่วงโซ่การแลกเปลี่ยนข้อมูล ได้แก่ การแบ่งปันข้อมูลกับผู้ให้บริการภายนอก ที่ปรึกษา และการแลกเปลี่ยนข้อมูลระหว่างองค์กร
- การเผยแพร่หรือแบ่งปันชุดคำสั่ง (Source Code) สู่สาธารณะ หรือชุดคำสั่งริ่วไหลเป็นการเร่งให้มัลแวร์เพิ่มมากขึ้นอย่างรวดเร็ว ทำให้อาชญากรไซเบอร์ศึกษาและสร้างมัลแวร์รูปแบบใหม่ ๆ ซึ่งอาจมีคุณสมบัติหลบเลี้ยงจากการตรวจพบทั่วไป

ແນວໂນມດ້ານຄວາມມື່ນຄອງປລອດກັຍສາຮສະເທດ

- ມັລແວຣີສໍາເຮົາຈຸດຕາສິ່ງເພື່ອເຈາະຮະບບ ຮາໄດ້ຈ່າຍມາກຂຶ້ນໃນອິນເກອຣເນີຕ ກຳໃຫ້ມີອາຊາກຣໃເບອຣໜ້າໃໝ່ ອີ່ຮູ້ມີອສມັກຮ່າຍເລັ່ນມາກຍຶ່ງຂຶ້ນ ຖໍ່ຈະລອງກົດສອບໂຈມຕີຮະບບຄວາມມື່ນຄອງປລອດກັຍຂອງເປົາໝາຍ
- Exploit kits ຍັງຄອງເປັນກັຍຄຸກຄານຫລັກສໍາຮັບ Windows XP ທີ່ Microsoft ພູດສັບສຸນ ຜູ້ໄມ່ປະສົງຄົດຈຶ່ງສາມາດກຳໜັດເປົາໝາຍໄດ້ ເນື່ອງຈາກຜູ້ໃຊ້ຈຳນວນນາກອາຈໄມ່ໄດ້ຢ້າຍໄປຢັງ Windows ເວັບເປົ້າລ່າສຸດ ທີ່ມີຄຸນຫລັກໜະດ້ານຄວາມປລອດກັຍຂຶ້ນສູງ

การบริหารความเสี่ยงและมาตรการจัดการ

การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป็นการประสานกิจกรรมเพื่อสั่งการและควบคุมองค์กรเกี่ยวกับความเสี่ยง เพื่อดำเนินการจัดการผลของความไม่แน่นอนต่อวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ในการรักษาความลับ ความถูกต้อง สภาพพร้อมใช้ของข้อมูลสารสนเทศ ระบบสารสนเทศ ทรัพย์สินสารสนเทศ โดยมี กรอบการบริหารความเสี่ยง (RiskManagementFramework) และกระบวนการบริหารความเสี่ยง (RiskManagementProcess) เพื่อพิจารณาดำเนินการมาตรการควบคุมที่เหมาะสมสำหรับจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ตามสภาพความเสี่ยงที่ยอมรับได้ขององค์กร

การบริหารความเสี่ยงและมาตรการจัดการ

การจัดการข้อมูลในองค์กรเพื่อตอบสนองตามวัตถุประสงค์และลักษณะของธุรกิจ จำแนกตามสถานะของข้อมูล เป็น 3 รูปแบบ โดยต้องมีการปกป้องข้อมูลและมาตรการควบคุม

- Data at Rest : ข้อมูลที่ถูกจัดเก็บอยู่ในสื้อบันทึกหรือ Storage ขององค์กร (Storage Server, Files Server, Database, Backup Image, ฯลฯ) กึ่งในส่วนกลางและเครื่องผู้ใช้งาน
- Data in Transit : ข้อมูลที่มีการรับส่ง โอนย้ายระหว่างอุปกรณ์หรือระบบคอมพิวเตอร์ การส่งข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง
- Data in Use : ข้อมูลที่ใช้งานอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน (Client/Endpoint)

សុលប៉ែកា



ความมั่นคงปลอดภัยสารสนเทศเกี่ยวกับข้อมูลกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูลสารสนเทศระบบสารสนเทศ ทรัพย์สินสารสนเทศ จากการเข้าถึงโดยมิชอบ การใช้โดยมิชอบ การนำไปใช้ในทางผิด การทำลายทำให้เสียหาย หรือการเปลี่ยนแปลงแก้ไขโดยมิชอบ

คุณสมบัติสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ : องค์ประกอบหลัก 3 ด้าน ได้แก่

- การรักษาความลับ (Confidentiality)
- ความถูกต้องครบถ้วน (Integrity)
- สภาพความพร้อมใช้งาน (Availability)

องค์ประกอบอื่น ได้แก่

- ความถูกต้องแท้จริง (Authenticity)
- ความรับผิดที่ตรวจสอบได้ (Accountability)
- การห้ามปฏิเสธความรับผิด (Non-repudiation)
- ความน่าเชื่อถือ (Reliability)

ระดับความมั่นคงปลอดภัยในระดับใด ๆ จะกำหนดขึ้นได้โดยการรักษาความสมดุลความสัมพันธ์ขององค์ประกอบ 3 ด้าน ได้แก่

- ความมั่นคงปลอดภัย (Security)
- ฟังก์ชันการทำงาน (Functionality)
- และการใช้งาน (Usability)

ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ จำแนกเป็น 3 กลุ่ม ได้แก่

- กลุ่มภัยคุกคามระบบเครือข่าย (Network Threats)
- กลุ่มภัยคุกคามระบบโฮสต์ (Host Threats)
- และกลุ่มภัยคุกคามระบบงาน (Application Threats)
- ความน่าเชื่อถือ (Reliability)

รูปแบบการโจมตีที่สำคัญ ๆ ด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ได้แก่ กัยคุกความระดับสูง (APT) กัยคุกความต่ออุปกรณ์พกพา กัยคุกความจากการประมวลผลแบบคลาวด์ มัลแวร์ บอตเน็ต และการโจมตีที่เกิดขึ้นจากภายในองค์กร

กัยคุกความการทำงานไซเบอร์ หมายถึง การกระทำการทำให้การดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ ลักษณะของกัยคุกความการทำงานไซเบอร์ แบ่งออกเป็น 3 ระดับ ได้แก่

คุณสมบัติสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ : องค์ประกอบหลัก 3 ด้าน ได้แก่

- กัยคุกความการทำงานไซเบอร์ในระดับวิกฤติ
- กัยคุกความการทำงานไซเบอร์ในระดับร้ายแรง
- กัยคุกความการทำงานไซเบอร์ในระดับไม่ร้ายแรง

ประเภทการโจมตีระบบสารสนเทศ จำแนก 4 ระดับ ได้แก่

- ระดับระบบปฏิบัติการ Operating System Attacks
- ระดับค่าการติดตั้งระบบ Mis-configuration Attacks
- ระดับระบบงาน Application-level Attacks
- ระดับชุดคำสั่งระบบ Shrink-Wrap Code Attacks

แนวโน้มด้านความมั่นคงปลอดภัย (Trends in Security) ได้แก่ เทคโนโลยีใหม่ ๆ อาจยังไม่มีความมั่นคงปลอดภัยได้กันที่หรือไม่เพียงพอ การโจมตีข้อมูลขององค์กรและข้อมูลส่วนบุคคลในระบบคลาวด์เพิ่มขึ้นการโจมตีผ่านโทรศัพท์มือถือและอุปกรณ์พกพา วิธีการหลอกลวงทางไซเบอร์ และมัลแวร์ใหม่ ๆ ที่หลบเลี้ยงการตรวจพบโดยโปรแกรมป้องกันไวรัสโดยทั่วไป

THANK YOU

END OF MODULE