สรุปกฎหมาย(part II)

“ระบบคอมพิวเตอร์” คือ อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่งและแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

CIA คือ เป็นคนในองค์กร เป็นฝ่ายตรวจสอบภายใน ก็จะตรวจสอบการปฏิบัติงานของคนในองค์กรทั้งหมด ป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

C = ควบคุมครองความลับ

I = ความถูกต้อง

A = ความพร้อมใช้

Dos (Denial of Service) เป็นการโจมตีโดยมีจุดมุ่งหมายทำให้ระบบไม่สามารถให้บริการได้

การโจมตีด้วยโครงข่าย (Network base Attack) ผู้โจมตีจะส่งข้อมูลที่มีปริมาณมหาศาลเข้าไปที่เป้าหมายเพื่อทำให้การรับ-ส่งข้อมูลเกิดคอขวด จนไม่สามารถติดต่อสื่อสารกับผู้ใช้งานทั่วไปได้

การโจมตีด้วยแอพพลิเคชั่น (Application base Attack) จะส่งข้อมูลที่อยู่ในเลเยอร์ที่เจ็ดของโอเอสไอ เพื่อมุ่งเป้าไปให้แอพพลิเคชั่นหยุดทำงาน ซึ่งการโจมตีชนิดนี้จะอยู่ในระดับที่สูงกว่าการโจมตีด้วย และยังสามารถโจมตีผ่านทางช่องโหว่ของระบบได้ด้วย

DDos (Distributed Denial of Service) เป็นการโจมตีเพื่อให้ระบบหยุดการทำงานไม่สามารถใช้เครื่องคอมพิวเตอร์ได้ทั้งระบบหรือเครื่องเดียวๆ

รูปแบบการโจมตี

1. การโจมตีแบบ SYN Flood โจมตีโดยการส่ง แพ็คเก็ต TCP ที่ตั้งค่า SYN บิตไว้ไปยังเป้าหมาย เสมือนกับการเริ่มต้นร้องขอการติดต่อแบบ TCP ตามปกติ เป้าหมายก็จะตอบสนองโดยการส่ง SYN-ACK กลับมา ผู้โจมตีจะควบคุมเครื่องที่ถูกระบุใน source IP address ไม่ให้ส่งข้อมูลตอบกลับ ทำให้เกิดสภาวะ half-open ทำให้คิวของการให้บริการของเครื่องเป้าหมายเต็ม ทำให้ไม่สามารถให้บริการตามปกติได้

2การโจมตีแบบ ICMP Flood เป็นการส่งแพ็คเก็ต ICMP ขนาดใหญ่จำนวนมากไปยังเป้าหมาย ทำให้เกิดการใช้งานแบนด์วิดธ์เต็มที่

3. การโจมตีแบบ UDP Flood เป็นการส่งแพ็คเก็ต UDP จำนวนมากไปยังเป้าหมาย ซึ่งทำให้เกิดการใช้แบนด์วิดธ์อย่างเต็มที่หรือทำให้ทรัพยากรของเป้าหมายถูกใช้ไปจนหมด

ผู้ให้บริการ = ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเตอร์เน็ตหรือติดต่อถึงกันได้ โดยผ่านระบบคอมพิวเตอร์ไม่ว่าจะเป็นบริการในนามตนเอง หรือ เพื่อประโยชน์บุคคลอื่น

ผู้ใช้บริการ = ผู้ใช้บริการของผู้ให้บริการไม่ว่าจะเสียค่าใช้จ่ายหรือไม่ก็ตาม

ประเภทของผู้ให้บริการ

1 ผู้ให้บริการในการเชื่อมต่อสู่ระบบอินเตอร์เน็ต เช่น ทรู ดีแทค วันทูคลอ 3bb

2 ผู้ให้บริการเกี่ยวกับข้อมูล เช่น Pantip DekD (จำพวกเว็ปบอร์ด)

หน้าที่ของผู้ให้บริการ

1. ดูแลไม่ให้มีข้อมูลที่ขัดต่อกฎหมาย
2. จัดเก็บข้อมูลคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์
3. จัดเก็บข้อมูลของผู้ใช้บริการ
4. ประสานงานและดำเนินการตามคำสั่งของพนักงานและเจ้าหน้าที่

การกำหนดบทลงโทษผู้ให้บริการ

มาตรา 15 ผู้ให้บริการผู้ใดจงใจสนับสนุนหรือยินยอมให้มีการกระทำความผิด ตามมาตรา 14ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิดตามมาตรา 14 เหตุผล ผู้ให้บริการในที่นี้มุ่งประสงค์ถึงเจ้าของเว็บไซต์ ซึ่งมีการพิจารณาว่าควรต้องมีหน้าที่ลบเนื้อหาอันไม่เหมาะสมด้วย

การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

วัตถุประสงค์ ออกภายใต้ มาตรา 26 วรรค 3 ข้อมูลจราจรทางคอมพิวเตอร์เป็นพยานหลักฐานสำคัญต่อการนำผู้กระทำความผิดมาลงโทษ ประเภทผู้ให้บริการแบ่งเป็น 2 ประเภทใหญ่

(1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกัน โดยประการอื่น แบ่งออกเป็น

ก. ผู้ประกอบกิจการโทรคมนาคม (Telecommunication Carrier)

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access ServiceProvider)

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider)

(2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล ตาม (1) บางส่วน เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Content Service Provider)

ข้อมูลที่ต้องเก็บ - ข้อมูลจราจรที่สามารถระบุผู้ใช้บริการเป็นรายบุคคลได้

รูปแบบการเก็บ - ต้องเก็บในสื่อที่รักษา Integrity/Confidentiality/identification

1. การเข้าถึงระบบหรือข้อมูลของผู้อื่นโดยมิชอบ (มาตรา 5-8)

การเข้าถึงระบบหรือข้อมูลของผู้อื่นโดยมิชอบ หมายถึง การที่บุคคลล่วงรู้รหัสผ่านที่เป็นความลับของผู้อื่น และได้ทำการเข้าไปเจาะข้อมูลทางคอมพิวเตอร์ของผู้อื่น โดยที่เจ้าของข้อมูลไม่ได้อนุญาต ซึ่งก่อให้เกิดความเสียหายแก่ผู้อื่น หรือการปล่อยไวรัสมัลแวร์เข้าคอมพิวเตอร์ของผู้อื่น เพื่อทำการเจาะข้อมูลบางอย่าง หรือการ Hack เพื่อเข้าไปขโมยข้อมูลของผู้อื่นจะต้องได้รับโทษตามความผิดตาม พ.ร.บ.คอมพิวเตอร์

2. การแก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย (มาตรา 9-10)

การแก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหาย หมายถึง การทำให้ข้อมูลของผู้อื่นเกิดความเสียหาย การทำลายข้อมูล การเปลี่ยนแปลงและแก้ไขข้อมูล การเพิ่มเติมข้อมูลของผู้อื่นโดยความเห็นชอบจากผู้ที่เป็นเจ้าของ มิได้รับ หรือการทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ จะต้องได้รับโทษตามความผิดทาง พ.ร.บ. ทางคอมพิวเตอร์

3. การส่งข้อมูลหรืออีเมลกวนผู้อื่น หรือส่งอีเมลสแปม (มาตรา 11)

การส่งข้อมูลหรืออีเมลกวนผู้อื่น หรือส่งอีเมลสแปม หมายถึง การส่งข้อความหาผู้อื่นทางออนไลน์ เช่น กรณีที่พ่อค้าและแม่ค้าที่ขายของทางออนไลน์ ที่ส่งอีเมลขายของที่ลูกค้าไม่ยินดีที่จะรับ หรือที่รู้จักกันว่า อีเมลสแปม การฝากร้านตาม Facebook กับ Instagram ก็ถือเป็นสิ่งที่ไม่ควรทำและรวมถึงคนที่ขโมย Database ลูกค้าจากคนอื่น แล้วส่งอีเมลขายของตัวเอง เป็นต้น จากกรณีเหล่านี้จะต้องได้รับผิดตาม พ.ร.บ. ทางคอมพิวเตอร์

5. การจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด (มาตรา 13) *เน้น

การจำหน่ายหรือเผยแพร่ชุดคำสั่งเพื่อนำไปใช้กระทำความผิด หมายถึง การกระทำความผิดทางคอมพิวเตอร์ตามมาตรา 5-11

บทลงโทษ

ต้องจำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

กรณีทำเพื่อเป็นเครื่องมือในการกระทำความผิดทางคอมพิวเตอร์ มาตรา 12 ต้องจำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ หากมีผู้นำไปใช้กระทำความผิด ผู้จำหน่ายหรือผู้เผยแพร่ต้องรับผิดชอบร่วมด้วย

6. การนำข้อมูลที่ผิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ (มาตรา 14) *เน้น

การนำข้อมูลที่ผิดพ.ร.บ.เข้าสู่ระบบคอมพิวเตอร์ หมายถึง การโพสต์ข้อมูลปลอม การทุจริตหลอกลวง (อย่างเช่น ขาวปลอม โฆษณาธุรกิจลูกโซ่ที่หลอกลวงเอาเงินลูกค้า และไม่มีการส่งมอบของให้จริง ๆ เป็นต้น) การโพสต์ข้อมูลความผิดเกี่ยวกับความมั่นคงปลอดภัย การก่อการร้าย การโพสต์ข้อมูลลามก อนาจาร ที่ประชาชนเข้าถึงได้

บทลงโทษ

ในกรณีที่เป็นการกระทำที่ส่งผลถึงประชาชน ต้องได้รับโทษจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ และหากเป็นกรณีที่เป็นการกระทำที่ส่งผลต่อบุคลใดบุคคลหนึ่ง ต้องได้รับโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ (แต่ในกรณีอย่างหลังสามารถยอมความกันได้)

7. การให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด (มาตรา 15) *เน้น

การให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจกับผู้ร่วมกระทำความผิด เช่น การที่เพจต่าง ๆ ที่เปิดให้มีการแสดงความคิดเห็น แล้วมีความคิดเห็นที่มีเนื้อหาผิดกฎหมาย แต่ถ้าหากแอดมินเพจตรวจสอบแล้วพบเจอ และลบออก จะถือว่าเป็นผู้ที่พ้นความผิด

บทลงโทษ

ในกรณีที่แอดมินไม่ยอมลบออก จะต้องได้รับโทษ ถือว่าเป็นผู้กระทำความผิดตามมาตรา 14 ต้องได้รับโทษเช่นเดียวกันผู้โพสต์ หรือแสดงความคิดเห็นทางออนไลน์ แต่ถ้าผู้ดูแลระบบพิสูจน์ได้ว่า ตนได้ปฏิบัติตามขั้นตอนการแจ้งเตือนแล้วไม่ต้องรับโทษ

การทำความผิดตามมาตรา 59

มาตรา 59 คือ องค์ประกอบความผิด มี 2 องค์ประกอบ

1. องค์ประกอบภายนอก เช่น เอามือตบหัวเพื่อน มองเห็นเป็นความผิดภายนอก
2. องค์ประกอบภายใน เช่น เอามือตบหัวเพื่อนเพราะมียุงกำลังกัดหัวเพื่อน เป็นความคิดภายในไม่ได้ตั้งใจทำร้ายเพื่อน

เรื่องโปรเจค

1. packet sniffing

โปรแกรมที่เอาไว้ดักจับข้อมูล บนระบบ Network การดักจับข้อมูลที่ผ่านไปมาระหว่าง เน็ตเวิร์คเรียกว่า sniffing (คล้ายๆ การดักฟังโทรศัพท์ แต่การดักฟังโทรศัพท์จะทำได้ทีละเครื่อง แต่ sniffer ทำได้ทีเดียวทั้ง network เลย)

2. DDos

หลักการทำงานคือใช้ zombie system ใน botnets ที่เตรียมไว้เป็นเครื่องมือโจมตี วิธีที่นิยมคือ Smurf attack หรือการใช้เครื่องส่ง request ไปหา server ต่างๆ แต่ปลอมแปลง IP (spoofing) สำหรับตอบกลับให้เป็น IP ของเป้าหมาย เมื่อ server เหล่านั้นตอบกลับมา ก็จะไปตอบเครื่องเป้าหมาย เป้าหมายก็จะถูกโจมตีด้วย traffic จำนวนมาก

3. Rainbow table

ตารางเก็บข้อมูลส่วนมากนิยมนำมาเก็บข้อมูลรหัสผ่าน โดยเก็บข้อมูลของรหัสผ่านที่แปลงเป็นค่า hash นำมาเก็บในตารางข้อมูล และเมื่อทำการสุ่มรหัสผ่านการใช้วิธีนี่จะทำให้การสุ่มนั้นง่ายและรวดเร็ว โดยการนำค่า hash มาเปรียบเทียบกับรหัสผ่านที่ผ่านการ hash แล้ว หากเหมือนกันแสดงว่าผู้บุกรุกได้ทำการเจาะรหัสผ่านสำเร็จ

4. Bluetooth Vulnerability

ช่องโหว่ ความปลอดภัยระดับบริการ ผู้จัดการความปลอดภัยส่วนกลางจัดการรับรองความถูกต้องการกำหนดค่าและอนุญาต อาจไม่สามารถเปิดใช้งานโดยผู้ใช้ ไม่มีความปลอดภัยระดับอุปกรณ์

ความปลอดภัยระดับอุปกรณ์ การรับรองความถูกต้องและการเข้ารหัสตามความลับ เปิดเสมอ บังคับการรักษาความปลอดภัยสำหรับการเชื่อมต่อระดับต่ำ

5. Pdf Vulnerability

CVE-2018-16018 เป็นช่องโหว่ประเภท Privilege Escalation คือ “ช่องโหว่ยกระดับสิทธิ์” แนวทางแก้ไข

อัปเดต Apache Struts เป็นเวอร์ชั่น 2.3.35 หรือ 2.5.17

CVE-2018-16011 เป็นประเภท Arbitrary Code Execution คือการบ่งบอกถึงความพยายามในการโจมตีเพื่อหาช่องโหว่การใช้งานหลังจากช่องโหว่ฟรีใน Adobe Acrobat และ Reader

แนวทางแก้ไขไม่ควรเปิดไฟล์ และลิงก์ที่ดูไม่น่าปลอดภัยในอีเมล นอกจากนี้ควรเก็บข้อมูลสำรองไว้เสมอ

6. Windows exploitation

7. Linux Exploitation

8. Wireless Network Compromised

Router Wi-Fi หลายยี่ห้อมักใช้ชิพคอมพิวเตอร์ราคาถูกซึ่งแฮคเกอร์แคทีเดียวก็ได้รหัสผ่าน นักวิจัยด้านความปลอดภัยรายงานว่าชิพคอมพิวเตอร์ยอดนิยมที่ใช้ในเราท์เตอร์มักจะใช้วิธีสร้างตัวเลขแบบสุ่ม “random number generator” **โปรแกรมแฮก Wi-Fi Kali Linux** คือ โอเอสลินุกซ์แบบหนึ่ง พัฒนาขึ้นมาเพื่อจุดประสงค์ทางด้านตรวจสอบความปลอดภัยของระบบเครือข่าย **การป้องกัน** พยายามติดตั้งอุปกรณ์ Router ไว้กลางบ้านไกล ๆ ตั้งรหัสสำหรับเข้าใช้ WiFi

9. Malware Trojan

malware ที่แฝงอยู่ในเครื่องเพื่อรอดำเนินการบางอย่าง trojan มักไม่ได้มีวิธีการแพร่กระจายไปเครื่องอื่นโดยอาศัยเราหรือเครื่องเรา แต่อาจใช้วิธีเช่น แฝงมากับโปรแกรมอื่นที่ดูมีเจตนาดี เช่น โปรแกรมฟังเพลง เมื่อ user เปิดโปรแกรมนั้น ก็ติด trojan

10. Ransomware

Ransomware เป็น มัลแวร์ (malware) ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆคือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้งานแต่อย่างใด แต่จะทำการเข้ารหัสหรือล็อกไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

11. MITM

มี Hacker เข้าไปอยู่ตรงกลางระหว่าง user 2 ฝั่ง ทั้ง 2 ฝั่งคิดว่าตนเองส่งข้อมูลหากัน แต่จริงๆ แล้วทุกอย่างผ่าน hacker ตรงกลางหมดเลย

12. PHP Security

13. Session Hijacking

Session Hi Jacking คือ การที่ Hacker ขโมย Session จากเหยื่อโดยที่ Hacker จะใช้ตัวแปรคำนึงเก็บรหัส Session ของเหยื่อเอาไว้เพื่อใช้ในการเข้าเว็บไซต์ในครั้งถัดไปโดยไม่ต้องกรอกรหัสใหม่ วิธีการป้องกัน Session Hi Jacking เพิ่มตัวแปร ตัวแปรนึงไว้ใน Sessionเพื่อตรวจสอบว่ามาจากที่เดียวกัน

14. Javascript Vulnerabilities

ช่องโหว่ความปลอดภัย JavaScript ที่พบบ่อยที่สุดอย่างหนึ่งคือ Cross-Site Scripting (XSS) วิธีรับมือกับภัยรูปแบบนี้จะต้องอัพเดทเวอร์ชันของซอฟต์แวร์ และโปรแกรมให้เป็นเวอร์ชันล่าสุดอยู่เสมอ หรือเพิ่มความปลอดภัยด้วย ชุดโปรแกรมรักษาความปลอดภัย ที่สามารถตรวจจับสคริปท์อันตรายเหล่านี้ได้

15. SQL Injection

เป็นภาษาที่ใช้จัดการ database และ software จำนวนไม่น้อยรันด้วย SQL ประเภทใดประเภทหนึ่ง SQL injection ก็คือการใส่คำสั่ง SQL ลงไปในฟอร์มเพื่อหวังผลให้เกิดความเสียหายต่อ database ของเรา ถ้าโปรแกรมไม่ได้เตรียมป้องกันเรื่องนี้ (เช่น form validation) ก็จะมีปัญหาได้

16. Steganography

17. Windows Server Security

เป็นการเจาะช่องโหว่โดยเรียกช่องโหว่นั้นว่า enternalblue เป็นการเจาะช่องโหว่ของ Microsoft ที่ชื่อว่า MS17-010 โดยแฮกเกอร์สามารถสแกนเพื่อเข้าถึงพอร์ต SMB ผ่านอินเตอร์เน็ต หากพบช่องโหว่แฮกเกอร์จะสามารถโจมตีเป้าหมายได้ สามารถปิดช่องโหว่นั้นโดยการเข้าไปปิดพอร์ต SMB/หมั่นอัปเดท Windows อย่าสม่ำเสมอ

18. Malware Analysis