ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

THAILAND COMPUTER
EMERGENCY
RESPONSE TEAM
[ThaiCERT]

ANNUAL REPORT

CYBERSECURITY IS OUR MISSION

ศูนย์ประสานการรักษา
ความมั่นคงปลอดภัย
ระบบคอมพิวเตอร์ประเทศไทย
(ไทยเซิร์ต)

2012

www.thaicert.or.th

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ELECTRONIC TRANSACTIONS DEVELOPMENT AGENCY
(PUBLIC ORGANIZATION)
www.etda.or.th

ร่วมกับ
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

THAILAND COMPUTER EMERGENCY RESPONSE TEAM [ThaiCERT]

ANNUAL REPORT

ชื่อเรื่อง THAILAND COMPUTER EMERGENCY RESPONSE TEAM ANNUAL REPORT

เรียบเรียงโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เลข ISBN : ISBN 978-974-9765-46-3

พิมพ์ครั้งที่ 2 พฤษภาคม 2556
พิมพ์จำนวน 2,000 เล่ม
ราคา 200 บาท

จัดพิมพ์และเผยแพร่โดย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ.
ร่วมกับ สำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์
สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และ
สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ 0-2142-2483
โทรสาร 0-2143-8071

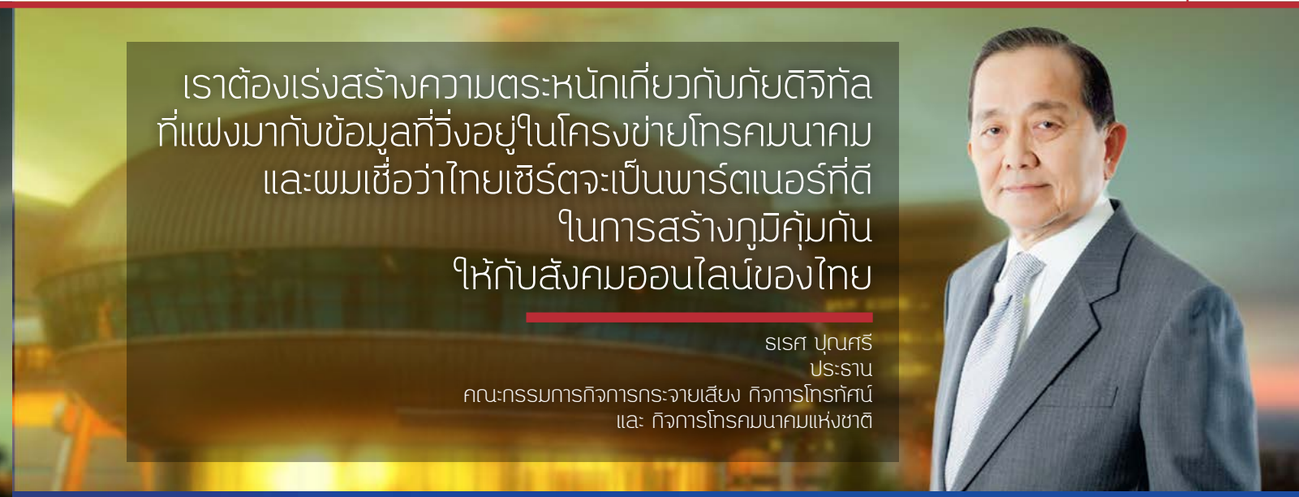
เว็บไซต์ สพธอ. http://www.etda.or.th
เว็บไซต์ ครอ. http://www.etcommission.go.th
เว็บไซต์ไทยเซิร์ต http://www.thaicert.or.th
เว็บไซต์ กสทช. http://www.nbtc.go.th
เว็บไซต์กระทรวงฯ http://www.mict.go.th

“เมื่อประเทศจำเป็นต้องเปลี่ยนผ่านจากระบบ อะนาล็อกเป็นระบบดิจิทัล
ถึงปี 2556 จะมีคอมพิวเตอร์แท็บเล็ตเพื่อยกระดับการศึกษารวม 2.6 ล้านเครื่อง
ปี 2557 ประมาณการว่ามูลค่า e-Commerce จะสูงกว่า 60,800 ล้านบาท
ปี 2558 โครงข่ายบรอดแบนด์ที่มีคุณภาพจะถึงประชาชนไม่น้อยกว่าร้อยละ 80
รัฐบาลจึงให้ความสำคัญอย่างยิ่งกับการรับมือกับภัยคุกคามทางออนไลน์
ที่มาพร้อมกับความก้าวหน้านั้น การบูรณาการการทำงานด้านความมั่นคงปลอดภัย
จึงเกิดขึ้น เป็นที่มาของการตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
และ สพธอ.ซึ่งมี ThaiCERT ก็จะเข้ามาช่วยผลักดันงานสำคัญนี้”

ยิ่งลักษณ์ ชินวัตร
นายกรัฐมนตรี

ไทยเซิร์ตเป็นหนึ่งในกลไกที่สำคัญ
ในด้านความมั่นคงปลอดภัยทางไซเบอร์
และสนับสนุนการพัฒนาประเทศตาม
นโยบาย Smart Thailand ของรัฐบาล

นาวาอากาศเอกอนุดิษฐ์ นาครทรรพ
รมว. เทคโนโลยีสารสนเทศและการสื่อสาร



เราต้องเร่งสร้างความตระหนักเกี่ยวกับภัยดิจิทัล
ที่แฝงมากับข้อมูลที่วิ่งอยู่ในโครงข่ายโทรคมนาคม
และผมเชื่อว่าไทยเซิร์ตจะเป็นพาร์ตเนอร์ที่ดี
ในการสร้างภูมิคุ้มกัน
ให้กับสังคมออนไลน์ของไทย

ธเรศ ปุณศรี
ประธาน
คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และ กิจการโทรคมนาคมแห่งชาติ

ผมหวังจะเห็นไทยเซิร์ตมีการทำงานเชิงรุก
และเป็นกำลังสำคัญในการสร้างความเชื่อมั่น
ในการทำธุรกรรมทางอิเล็กทรอนิกส์
ของประเทศไทย

จรัมพร โชติกเสถียร
ประธานกรรมการบริหาร
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สำนักงาน กสทช. พร้อมสนับสนุน
การทำงานด้าน Security ให้เข้มแข็งมากขึ้น
และพร้อมผนึกกำลังกับไทยเซิร์ต สพธอ.

นายฐากร ตัณฑสิทธิ์
เลขาธิการ
คณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์
และ กิจการโทรคมนาคมแห่งชาติ

ไม่อยากให้นึกถึงกระทรวงไอซีทีเรื่องปิดเว็บไซต์
จนลืมไปว่าเรามีภารกิจสำคัญด้าน Security
ที่ทำงานอยู่หลังบ้านช่วยสนับสนุนหน่วยงานต่างๆ
ตลอดมา และในกระทรวงไอซีที
ก็มีไทยเซิร์ต สพธอ. เป็นกำลังหลัก

นายไชยยันต์ พึ่งเกียรติไพโรจน์
ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

ไทยเซิร์ตมีจุดเริ่มต้นที่เนคเทค สวทช.
และมาสานต่อภารกิจเพื่อดูแลและปกป้อง
ธุรกรรมออนไลน์ที่ สพธอ. จึงเป็นภารกิจ
ที่ สพธอ. ให้ความสำคัญ เพื่อทำให้ประเทศ
มีความพร้อม ในการรับมือกับภัยคุกคาม
ทางออนไลน์ ก่อนเข้าสู่ AEC 2015

สุรางคณา วายุภาพ
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

สารบัญ

สารบัญตาราง

สารบัญรูปภาพ

สารบัญกราฟ

บทนำ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. ร่วมกับสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ หรือ ธอ. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เป็นหน่วยงานหลักที่ทำหน้าที่ดำเนินการพัฒนา ส่งเสริม และสนับสนุนการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ ด้วยเหตุนี้ สพธอ. และ ธอ. จึงทำหน้าที่สนับสนุนคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ที่มีบทบาทเชิงรุกในการสร้างความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อลดความเสี่ยงของภาครัฐและเอกชนในการดำเนินการต่างๆ ทางออนไลน์ อีกทั้งยังมีการประสานการทำงานอย่างใกล้ชิดกับสำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร กลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยี กองบังคับการสนับสนุนทางเทคโนโลยี และกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ รวมทั้งร่วมผนึกกำลังกับสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ ที่ขานรับนโยบายคุ้มครองและปกป้องผู้บริโภคทางออนไลน์ของคณะกรรมการ กสทช. ด้วยเหตุนี้ สพธอ. จึงมีอีกบทบาทในการสนับสนุน คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่มีบทบาทในการดูแลความมั่นคงปลอดภัยจากภัยคุกคามด้านไซเบอร์ (Cybersecurity Threat) ซึ่งมีรูปแบบที่เปลี่ยนแปลงไปจากอดีตและมีความซับซ้อนมากขึ้น อีกทั้งยังเป็นภัยคุกคามที่สามารถโจมตีได้จากทุกทิศทาง ซึ่งส่งผลกระทบและสร้างความเสียหายให้กับผู้ให้บริการและผู้ใช้บริการเป็นจำนวนมาก จึงเป็นเหตุให้การรับมือและจัดการภัยคุกคามระบบคอมพิวเตอร์ จำเป็นต้องมีการประสานงานร่วมกับหน่วยงานทั้งในประเทศและต่างประเทศ เพื่อแก้ปัญหาให้เร็วที่สุด

ดังนั้น สพธอ. จึงได้ผลักดันการทำงานเชิงรุกของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยหรือไทยเซิร์ต (ThaiCERT) ให้ทำหน้าที่เป็นกลไกหลักของประเทศด้านความมั่นคงปลอดภัยของสังคมออนไลน์ และมีการประสานความร่วมมือกับเครือข่าย และหน่วยงานเซิร์ต (CERT/Computer Emergency Response Team) ของต่างประเทศ ซึ่งสอดคล้องกับกรอบปฏิบัติในการเตรียมความพร้อมเข้าร่วมเป็นส่วนหนึ่งของประชาคมเศรษฐกิจอาเซียน (AEC 2015) ตามที่กำหนดใน ASEAN Economic Community Blueprint และ ASEAN ICT Master Plan 2015 เพื่อสร้างความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความเข้มแข็งมากยิ่งขึ้น

ดังนั้น เพื่อรวบรวมกรณีศึกษาจากผลการดำเนินงานของไทยเซิร์ตและสถิติภัยคุกคามด้านสารสนเทศที่ไทยเซิร์ต ได้รับแจ้งหรือที่ตรวจพบในปี 2555 สพธอ. จึงได้จัดทำรายงาน ThaiCERT Annual Report ประจำปี 2555 ที่ได้มีการวิเคราะห์ข้อมูลภัยคุกคามด้านสารสนเทศที่ไทยเซิร์ตได้รับแจ้งในหลายมิติ เช่น แยกตามประเภทภัยคุกคามที่ได้รับแจ้ง แยกตามประเภทหน่วยงานผู้แจ้งเหตุภัยคุกคาม และแยกตามเครือข่ายคอมพิวเตอร์ของหน่วยงานหรือผู้ให้บริการอินเทอร์เน็ต (ISP) ภายในประเทศ เป็นต้น เพื่อนำเสนอภาพรวมของภัยคุกคามด้านสารสนเทศที่เกิดขึ้นในประเทศไทยปี 2555 ในรูปแบบข้อมูลเชิงสถิติ และสะท้อนสถานภาพของภัยคุกคามที่เกิดขึ้นในประเทศไทย เพื่อให้ผู้ที่เกี่ยวข้องใช้ประกอบการตัดสินใจในเชิงนโยบายและผลักดันให้เกิดกลไกในการป้องกันและแก้ไขปัญหาจากภัยคุกคามที่เกิดขึ้นกับระบบสารสนเทศทั้งในภาคประชาชน ภาคธุรกิจและภาครัฐ โดยเฉพาะหน่วยงานที่เป็นโครงสร้างพื้นฐานที่สำคัญของประเทศต่อไป

สุรางคณา วายุภาพ
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

1

“Cybersecurity” ปฐมบทของความเชื่อมั่นในการใช้ไอซีที

ปัจจุบัน เครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์และอุปกรณ์อิเล็กทรอนิกส์ต่างๆ ถูกนำมาใช้เป็นกลไกหลักที่สนับสนุนการประกอบธุรกิจ การดำเนินงานขององค์กร หรือการติดต่อสื่อสารของประชาชนทั่วไป เพื่อเพิ่มประสิทธิภาพและประสิทธิผล ตลอดจนอำนวยความสะดวกในการทำธุรกรรม ด้วยการใช้เอกสารในรูปอิเล็กทรอนิกส์ (Electronic document) การชำระเงินทางอิเล็กทรอนิกส์ (Electronic payment) การใช้สื่อสังคมออนไลน์ (Social media)

การทำธุรกรรมทางอิเล็กทรอนิกส์เหล่านี้มีการใช้งานอย่างแพร่หลายทั่วไป และมีกฎหมายรองรับผลของการทำธุรกรรมทางอิเล็กทรอนิกส์มาตั้งแต่ปี พ.ศ. 2544 ตามพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 แก้ไขเพิ่มเติม พ.ศ. 2551 อย่างไรก็ตามการทำธุรกรรมทางอิเล็กทรอนิกส์มีความเสี่ยงจากภัยคุกคามด้านสารสนเทศ (Threat) และช่องโหว่ของระบบสารสนเทศ (Vulnerability) ที่เกี่ยวข้อง ซึ่งอาจถูกใช้เป็นช่องทางในการก่ออาชญากรรมในหลายรูปแบบ ทั้งที่อยู่ในลักษณะการใช้อินเทอร์เน็ตในการก่ออาชญากรรมโดยตรงซึ่งเรียกว่า “อาชญากรรมคอมพิวเตอร์” หรือในลักษณะที่มีการใช้อินเทอร์เน็ตเป็นสื่อในการก่ออาชญากรรมต่าง ๆ ดั้งนั้นหน่วยงานของรัฐ ภาคเอกชน และประชาชนควรมีความตระหนักถึงความรุนแรงของผลกระทบ และความเสียหายที่อาจจะเกิดขึ้น และมีการรักษาความมั่นคงปลอดภัยที่เหมาะสมเพื่อปกป้องป้องกัน หรือรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Incident) ซึ่งจะทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

กรอบความคิดด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) ได้ถูกกำหนดไว้ในมาตรฐานสากลไอเอสโอ ไออีซี 27001 ปี 2005 (ISO/IEC 27001:2005 Information Security Management System) ซึ่งในปัจจุบันอยู่ในระหว่างการปรับปรุงเนื้อหาและจะประกาศใหม่ในปี 2013 มาตรฐานใหม่ให้ความสำคัญกับการรักษาความลับของข้อมูลสารสนเทศ (Confidentiality) การรักษาความครบถ้วนสมบูรณ์ของข้อมูลสารสนเทศ (Integrity) และการรักษาสภาพพร้อมใช้งานของระบบ (Availability) ซึ่งเป็นปัจจัยพื้นฐานในการพิจารณาความมั่นคงปลอดภัยด้านสารสนเทศ โดยอาศัยการประเมินความเสี่ยง (Risk assessment) ที่สารสนเทศอาจได้รับผลกระทบหรือเกิดความเสียหายจากภัยคุกคามด้านสารสนเทศและช่องโหว่ในระบบสารสนเทศ (Vulnerabilitiy) เช่น ฐานข้อมูลรายชื่อลูกค้าของหน่วยงานซึ่งอยู่ในระบบบริหารทรัพยากรขององค์กร (Enterprise Resource Planning System) เป็นข้อมูลลับของหน่วยงานซึ่งต้องมีความครบถ้วนสมบูรณ์ และอยู่ในสภาพพร้อมใช้งานตลอดเวลา ซึ่งภัยคุกคามต่อระบบสารสนเทศนั้น อาจมาจากทั้งทางอิเล็กทรอนิกส์ (Logical) และทางกายภาพ (Physical) ดังนั้นหน่วยงานจึงควรเตรียมการให้สามารถใช้ฐานข้อมูลรายชื่อลูกค้าได้แม้มีภัยคุกคามด้านสารสนเทศเกิดขึ้น

ตัวอย่างของมาตรการในการจัดการกับความเสี่ยงถูกกำหนดไว้ในมาตรฐานสากล ไอเอสโอ ไออีซี 27002 (ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security management) ซึ่งครอบคลุม 133 มาตรการจัดเป็นกลุ่มได้ 11 กลุ่ม ครอบคลุมตั้งแต่เรื่องนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ การบริหารจัดการองค์กร การบริหารทรัพยากรบุคคล การบริหารจัดการระบบสารสนเทศ และการปฏิบัติตามกฎหมาย เป็นต้น

อย่างไรก็ตาม ถึงแม้หน่วยงานต่าง ๆ และประชาชนจะมีความตระหนักด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แต่ภัยคุกคามด้านสารสนเทศก็ยังมีโอกาสที่จะเกิดความเสี่ยงและอาจเกิดขึ้นได้ตลอดเวลา ดังนั้น จึงจำเป็นต้องมีหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ หรือเซิร์ต (CERT/Computer Emergency Response Team) ซึ่งทำหน้าที่ประสานงานกับหน่วยงานต่าง ๆ ภายในและต่างประเทศ

เพื่อแก้ปัญหาภัยคุกคามด้านสารสนเทศได้อย่างรวดเร็วที่สุด นอกจากนี้เซิร์ต (CERT) ยังเป็นกรอบปฏิบัติที่กำหนดไว้ในพิมพ์เขียวในการจัดตั้งประชาคมเศรษฐกิจอาเซียน (ASEAN Economic Community Blueprint) ในข้อ B4 รายการที่ 51 และ 52

ปัจจุบัน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ได้ดำเนินโครงการศูนย์ประสานการรักษาความมั่นคงระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) มาตั้งแต่เดือนธันวาคม พ.ศ. 2554 โดยในปีแรกให้ความสำคัญกับภัยคุกคามด้านสารสนเทศ 2 ประเภทที่พบมากที่สุด ได้แก่ ประเภทที่ 1 ภัยคุกคามจากเว็บไซต์หลอกลวง (Phishing) ซึ่งในปีที่ผ่านมามีรายงานว่า ในบางกรณี ประชาชนที่ตกเป็นเหยื่อในแต่ละรายสูญเสียเงินในธนาคารไปหลายแสนบาทจากการถูกหลอกลวงนี้โดยแต่ละเดือนไทยเซิร์ตจะได้รับการรายงานเรื่องเกี่ยวกับเว็บไซต์หลอกลวงจากในและต่างประเทศเฉลี่ยประมาณ 50 กรณี หากจะประเมินผลกระทบเบื้องต้นก็สามารถกล่าวได้ว่า การแก้ไขปัญหาเว็บไซต์หลอกลวงอย่างเดียวของไทยเซิร์ตเป็นการลดโอกาสของความสูญเสีย ที่มีมูลค่านับหลายสิบล้านบาทต่อเดือนและ ประเภทที่ 2 ปัญหาบอตเน็ต (BOTNET) เช่น ซูส (Zeus) รูสต๊อก (Rustock) หรือ เคลิฮอส (Kelihos)ที่แพร่ระบาดบนเครื่องคอมพิวเตอร์ในประเทศไทยเป็นจำนวนมากกว่า 100,000 เครื่อง ซึ่งเครื่องที่ติดโปรแกรมไม่พึงประสงค์นี้ถูกใช้เป็นเครื่องมือในการโจมตีผู้อื่นหรือสร้างความเสียหายให้กับเจ้าของเครื่องคอมพิวเตอร์ เช่น การถูกใช้เป็นเครื่องมือในการส่งสแปม (SPAM) มากกว่า 25,000 ฉบับต่อชั่วโมง การถูกใช้เป็นเครื่องมือในการขโมยข้อมูลธุรกรรมออนไลน์ของผู้ใช้งาน และการถูกใช้เป็นเครื่องมือในการร่วมโจมตีสภาพความพร้อมใช้งานของระบบผู้อื่น (DDoS)

ภัยคุกคามด้านสารสนเทศทั้ง 2 ประเภทดังกล่าว เป็นเพียงส่วนหนึ่งของภัยคุกคามด้านสารสนเทศที่ไทยเซิร์ตได้รับแจ้ง ซึ่งจะเห็นได้จากข่าวการแพร่ระบาดของภัยคุกคามด้านสารสนเทศหลายประเภทที่เกิดขึ้นบนอินเทอร์เน็ตอย่างแพร่หลายและมีรูปแบบของภัยคุกคามด้านสารสนเทศซับซ้อนและแปลกใหม่ขึ้นทุกวัน ตามการเปลี่ยนแปลงของเทคโนโลยี ดังนั้นการพัฒนาความมั่นคงปลอดภัยด้านสารสนเทศ ควรมีการเตรียมการรับมือภัยคุกคามด้านสารสนเทศซึ่งไม่สามารถคาดการณ์ล่วงหน้าได้ ทั้งภัยคุกคามด้านสารสนเทศที่รู้จักกันดีและภัยคุกคามด้านสารสนเทศรูปแบบใหม่ ๆ เพื่อรักษาความต่อเนื่องของการดำเนินภารกิจของหน่วยงาน (Business Continuity) และการให้บริการของหน่วยงานต่าง ๆ โดยเฉพาะหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญยิ่งยวดของประเทศ (Critical Infrastructure) เช่น หน่วยงานด้านการสาธารณูปโภคและพลังงาน ด้านการสื่อสาร ด้านการแพทย์ เป็นต้น หน่วยงานโครงสร้างพื้นฐานสำคัญเหล่านี้นำเทคโนโลยีเข้ามาบริหารจัดการมากขึ้น ส่งผลให้ระบบสารสนเทศที่เกี่ยวข้องทวีความซับซ้อนเพิ่มขึ้น เมื่อมีการโจมตีระบบสารสนเทศหรือเครือข่าย ทีมรับมือภัยคุกคามด้านสารสนเทศจึงต้องมีศักยภาพที่จะช่วยกู้คืนระบบและบริการ ตรวจสอบและวิเคราะห์ข้อมูลเพื่อลดความเสี่ยง ปิดช่องโหว่หรือลดความเสียหายและผลกระทบในทันทีได้ถือเป็นโครงสร้างพื้นฐานสำคัญที่ควรเร่งพัฒนาให้มีความพร้อมรับมือกับความเสียหายที่จะเกิดขึ้น

ในด้านบุคลากร ไทยเซิร์ตจึงได้พัฒนาบุคลากรอย่างต่อเนื่อง เพื่อให้มีความรู้ความสามารถในการรับมือภัยคุกคามด้านสารสนเทศรูปแบบใหม่ ๆ เช่น ความรู้ด้านการจัดการสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Handling), การวิเคราะห์กรณีบุกรุกทางสารสนเทศ (Intrusion Analysis) การทดสอบเจาะระบบสารสนเทศ (Penetration Testing) การดูแลจัดการระบบคอมพิวเตอร์ (System Administration) และการดูแลความมั่นคงระบบเครือข่ายคอมพิวเตอร์ (Network Security) โดยมีเป้าหมายให้การดำเนินการของไทยเซิร์ตสามารถให้บริการรับมือและจัดการภัยคุกคามด้านสารสนเทศได้อย่างต่อเนื่อง และเพิ่มความสามารถในการรับมือและจัดการภัยคุกคามด้านสารสนเทศได้ในระดับประเทศ ประกอบด้วย การวิเคราะห์และแก้ไขปัญหาโปรแกรมไม่พึงประสงค์ (Malware) ทั้งแบบเคยตรวจพบก่อนเกิดความเสียหายหรือตรวจพบหลังเกิดความเสียหาย การวิเคราะห์และแก้ไขการหลอกลวงผ่านเว็บไซต์ประเภทฟิชชิ่ง (Phishing) และการวิเคราะห์และแก้ไขช่องโหว่ของบริการธุรกรรมที่สำคัญของประเทศ รวมถึงการจัดเตรียมระบบสำรอง (backup site) ที่พร้อมให้บริการแบบพร้อมใช้ทันที (Hot-Standby)

การดำเนินงานของไทยเซิร์ตยังมุ่งเน้นในการพัฒนาบุคลากรให้มีความสามารถในการวิเคราะห์ภัยคุกคามด้านสารสนเทศและจัดการได้อย่างมีประสิทธิภาพ มีการจัดให้มีการแบ่งความรับผิดชอบของทีมออกเป็นหลายด้านที่ครอบคลุมกับสถานภาพภัยคุกคามด้านสารสนเทศที่เกิดขึ้นในปัจจุบัน โดยมีทั้งทีมวิจัยและวิเคราะห์ภัยคุกคามด้านสารสนเทศทั้งที่มีอยู่ในปัจจุบันและภัยคุกคามด้านสารสนเทศในรูปแบบใหม่ ทีมที่ทำหน้าที่ในการเฝ้าระวังระบบเครือข่ายระบบสารสนเทศ ทีมที่คอยจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security Incident) ที่เกิดขึ้นอย่างทันท่วงที ทีมที่คอยทำหน้าที่ประสานความร่วมมือกับหน่วยงานทั้งภายในและต่างประเทศ เมื่อมีเหตุการณ์เกิดขึ้น พร้อมทั้งมีทีมที่คอยส่งเสริมและสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นอกจากนี้ การดำเนินงานของไทยเซิร์ตจำเป็นต้องอาศัยความร่วมมือของหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับภัยคุกคามด้านสารสนเทศที่เกิดขึ้นภายในประเทศ และจำเป็นต้องสร้างเครือข่ายความร่วมมือเพื่อรับมือภัยคุกคามด้านสารสนเทศกับหน่วยงานประเภทเดียวกันในระดับนานาชาติ เช่น การเข้าร่วมเป็นสมาชิกของเอพีเซิร์ต (APCERT/ - Asia Pacific Computer Emergency Response Team) และเฟิร์ส (FIRST/ - Forum of Incident Response and Security Teams) เป็นต้น ซึ่งองค์กรระดับนานาชาตินี้ เกิดจากการรวมตัวกันของกลุ่มผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและเครือข่ายขององค์กรเซิร์ต (CERTs/- Computer Emergency Response Team) หรือซีเสิร์ต (CSIRTs/ - Computer Security Incident Response Team) ที่มีอยู่ในแต่ละประเทศ เพื่อทำหน้าที่ในการตอบรับประสานความร่วมมือ ตลอดจนการบริหารจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์และเครือข่าย โดยเมื่อได้รับแจ้งเหตุภัยคุกคามด้านสารสนเทศจากหน่วยงาน CERTs หรือ CSIRTs แล้วหน่วยงาน APCERT หรือ FIRST จะทำหน้าที่ประสานความร่วมมือไปยังหน่วยงานในเครือข่ายที่เป็นตัวแทนของแต่ละประเทศสมาชิก เพื่อยับยั้งเหตุการณ์การละเมิดความมั่นคงปลอดภัยด้านสารสนเทศต่อไป

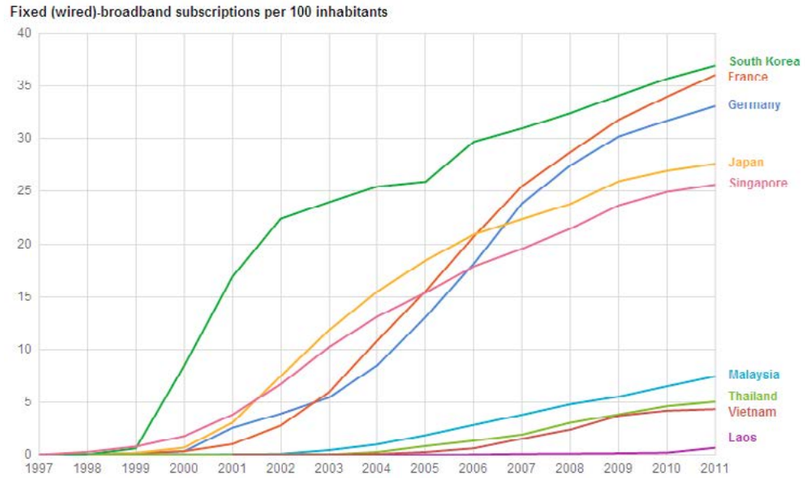
หากระบบที่ให้บริการหลักถูกโจมตี ไทยเซิร์ตจึงจำเป็นต้องจัดเตรียมทรัพยากร บุคลากร และระบบสารสนเทศ เพื่อเป็นศูนย์กลางในการประสานความร่วมมือในการรักษาความมั่นคงปลอดภัยของประเทศให้มีเข้มแข็งทั้งในการจัดการต่อสถานการณ์ความมั่นคงปลอดภัยด้านสารสนเทศทั้งในระดับประเทศและต่างประเทศ ซึ่งจะส่งผลกระทบโดยตรงต่อความเชื่อมั่นของกับประชาชนในการทำธุรกรรมทางอิเล็กทรอนิกส์ อีกทั้งยังเป็นการลดความเสี่ยงที่ก่อให้เกิดความเสียหายจากภัยคุกคามด้านสารสนเทศ ที่อาจจะเกิดขึ้นได้อีกทางหนึ่ง

2

“IT Threats & Risks” กับสถานะและความพร้อมของประเทศไทย

2. “IT Threats & Risks” กับสถานะและความพร้อมของประเทศไทย

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีส่วนเกี่ยวข้องกับชีวิตประจำวันเพิ่มมากขึ้น ผลจากการสำรวจครัวเรือนประจำปี 2554 ที่รวบรวมโดยสำนักงานสถิติแห่งชาติ ได้รายงานว่าประเทศไทยมีผู้ใช้คอมพิวเตอร์ร้อยละ 32.1 ใช้อินเทอร์เน็ตร้อยละ 24.72 และใช้โทรศัพท์มือถือร้อยละ 66.43 และนอกจากนี้ข้อมูลสถิติที่รวบรวมโดย International Telecommunication Union (ITU) ก็แสดงว่าการใช้เทคโนโลยีสารสนเทศมีแนวโน้มที่จะเติบโตอย่างต่อเนื่อง ดังตัวอย่างข้อมูลผู้ใช้งานบรอดแบนด์ ผู้ใช้งานอินเทอร์เน็ต และผู้ใช้โทรศัพท์มือถือในช่วงสิบกว่าปีที่ผ่านมา



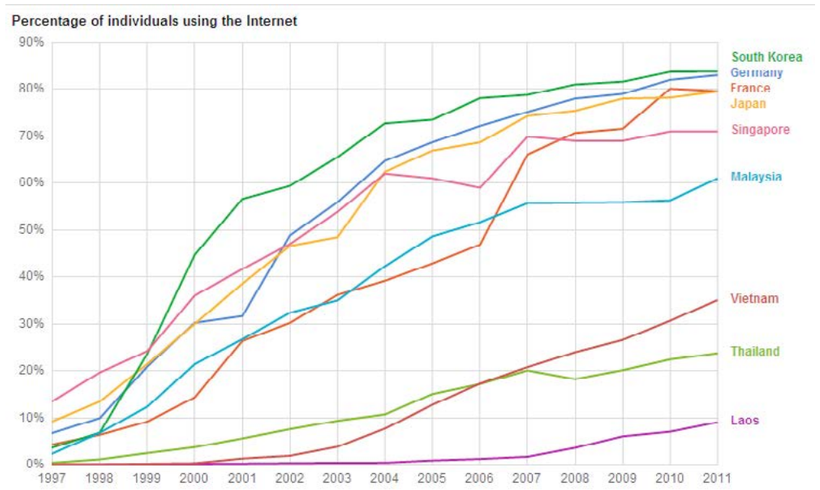
กราฟที่ 1 จำนวนผู้สมัครใช้บริการบรอดแบนด์ (Broadband) แบบใช้สายต่อผู้อยู่อาศัยจำนวน 100 คน ในประเทศไทยเปรียบเทียบกับประเทศอื่น ๆ ในช่วงปี ค.ศ. 1997-2011 (พ.ศ. 2540 – 2554)[4]

1 สรุปผลสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2554 (http://service.nso.go.th/nso/nsopublish/download/files/ict_household54_pocketbook.pdf)

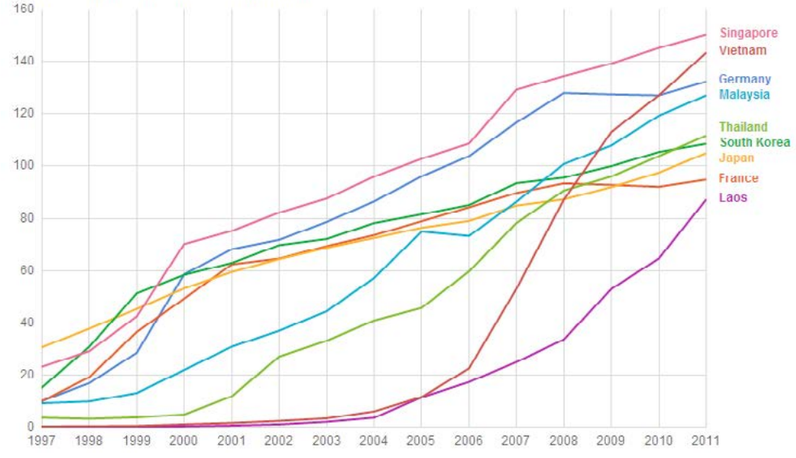
2 สรุปผลสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2554 (http://service.nso.go.th/nso/nsopublish/download/files/ict_household54_pocketbook.pdf)

3 สรุปผลสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2554 (http://service.nso.go.th/nso/nsopublish/download/files/ict_household54_pocketbook.pdf)

4 ICT Data and Statistics (IDS) โดย International Telecommunication Union (http://www.itu.int/ITU-D/ict/statistics/explorer/index.html)



กราฟที่ 2 สัดส่วน (ร้อยละ) ของผู้ใช้งานอินเทอร์เน็ตในประเทศไทยเปรียบเทียบกับประเทศอื่น ๆ ในช่วงปี ค.ศ. 1997-2011 (พ.ศ. 2540 – 2554)[5]



กราฟที่ 3 จำนวนผู้สมัครใช้บริการโทรศัพท์มือถือต่อผู้อยู่อาศัยจำนวน 100 คน ในประเทศไทยเปรียบเทียบกับประเทศอื่น ๆ ในช่วงปี ค.ศ. 1997-2011 (พ.ศ. 2540 – 2554)[6]

ด้วยอัตราการใช้และเข้าถึงเทคโนโลยีสารสนเทศที่เพิ่มมากขึ้นเรื่อย ๆ เช่นนี้ ย่อมมีผลกระทบต่อความสามารถในการป้องกันและรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) ซึ่งแต่ละองค์กรจะต้องควบคุมและบริหารจัดการภัย

5 ICT Data and Statistics (IDS) โดย International Telecommunication Union (http://www.itu.int/ITU-D/ict/statistics/explorer/index.html)

6 ICT Data and Statistics (IDS) โดย International Telecommunication Union (http://www.itu.int/ITU-D/ict/statistics/explorer/index.html)

คุกคาม (Threats) และความเสี่ยง (Risks) ให้หมดสิ้นไปหรืออยู่ในระดับที่สามารถยอมรับได้ ภัยคุกคามด้านสารสนเทศและความเสี่ยงในบริบทของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสามารถพิจารณาได้จากหลายมุมมอง เช่น การแบ่งลักษณะของภัยคุกคามด้านสารสนเทศและความเสี่ยงจากแหล่งต้นกำเนิดเป็นสองประเภท ได้แก่ ภัยคุกคามด้านสารสนเทศและความเสี่ยงที่เกิดขึ้นจากปัจจัยภายในองค์กร (Internal Threat & Risk) และภัยคุกคามด้านสารสนเทศและความเสี่ยงที่เกิดขึ้นเนื่องจากปัจจัยที่มาจากภายนอกองค์กรที่ส่งผลกระทบต่อการดำเนินงานภายในองค์กร (External Threat & Risk)

ภัยคุกคามด้านสารสนเทศที่เกิดขึ้นจากปัจจัยภายในองค์กรเป็นภัยที่เกิดขึ้นเนื่องจากบุคลากรขององค์กรขาดความพร้อมในการบริหารจัดการหรือใช้งานเทคโนโลยี ขาดประสบการณ์ ความรู้ความชำนาญ ความตระหนัก ไม่เข้าใจหรือเพิกเฉย ซึ่งอาจมีสาเหตุจากบุคลากรไม่มีความเข้าใจหรือเห็นความสำคัญกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ไม่ได้รับการฝึกอบรมอย่างเหมาะสม หรือองค์กรไม่ได้กำหนดนโยบายของหน่วยงานที่ชัดเจนว่า สิ่งใดสอดคล้องหรือไม่สอดคล้องกับนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร หรือไม่ได้จัดเตรียมเครื่องมือที่เหมาะสมไว้ให้บุคลากรใช้งาน ในขณะที่ภัยซึ่งเกิดจากปัจจัยภายนอกองค์กร เช่น การโจมตีจากผู้ไม่ประสงค์ดี ภัยธรรมชาติ ความขัดข้องของบริการจากผู้ให้บริการด้านสารสนเทศขององค์กร ช่องโหว่ของซอฟต์แวร์ที่องค์กรใช้งาน เป็นต้น อาจเป็นภัยที่อยู่นอกเหนือการควบคุมและไม่สามารถตรวจพบได้ล่วงหน้า แต่ก็สามารถบริหารจัดการเพื่อปรับใช้มาตรการที่ช่วยลดความเสี่ยงจากภัยคุกคามนั้นลงได้

ในการบริหารจัดการกับภัยคุกคามและความเสี่ยงที่เกิดจากภัยคุกคามนั้น ๆ องค์กรสามารถนำหลักการตามมาตรฐานสากล ไอเอสโอ ไออีซี 27002 (ISO/IEC 27002) มาปฏิบัติ โดยจะต้องคำนึงถึงหัวข้อ (Domain) ทั้ง 11 ด้าน ประกอบกัน ได้แก่

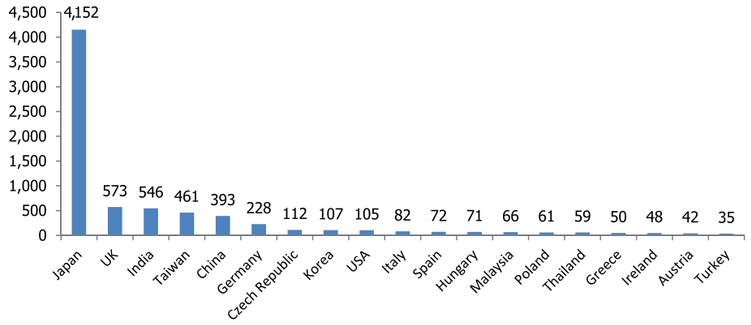
(1) Security Policy
(2) Organizing Information Security
(3) Asset Management
(4) Human Resource Security
(5) Physical & Environmental Security
(6) Communications & Operations Management
(7) Access Control
(8) Information System Acquisition, Development and Maintenance
(9) Information Security Incident Report
(10) Business Continuity Management
(11) Compliance

ก็จะทราบว่าโอกาสและผลกระทบของภัยคุกคามด้านสารสนเทศ ที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศขององค์กรนั้นมีอะไรบ้าง และหากเกิดเหตุการณ์เช่นนั้นแล้วจะมีผลกระทบอะไรบ้าง รวมถึงผลกระทบต่อระบบอื่น ๆ ที่อาจเกิดขึ้นได้อีก ซึ่งข้อมูลเหล่านี้เป็นประโยชน์มากเมื่อนำมาใช้พัฒนาและกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร หรือที่เรียกว่า ICT Security Policy ที่เหมาะสมและสอดคล้องกับลักษณะของการปฏิบัติงานขององค์กร เพื่อใช้เป็นเครื่องมือในการกำหนดนโยบายป้องกันปัญหาและบรรเทาผลกระทบที่เกิดขึ้นจากภัยคุกคามและความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศ และในขั้นตอนต่อไปสามารถนำไปพัฒนาเป็นแผนยุทธศาสตร์ในการบริหารจัดการความเสี่ยงขององค์กร (Risk Management Strategic Plan) ต่อไป

เมื่อวิเคราะห์สถานภาพและความพร้อมในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ในประเทศไทยนั้นสามารถเปรียบเทียบจากจำนวนองค์กรที่ได้รับใบรับรอง ไอเอสโอ ไออีซี 27001:2005 (ISO/IEC 27001:2005) ซึ่งเป็นมาตรฐานสากลในการรับรองระบบจัดการความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Management System - ISMS) จากสถิติล่าสุดซึ่งรวบรวมโดย International Register of ISMS Certificate เมื่อเดือนสิงหาคม พ.ศ. 2555 พบว่าญี่ปุ่นเป็นอันดับหนึ่งมีองค์กรที่ผ่านการรับรองแล้วจำนวน 4,152 แห่ง ในขณะ

ที่ประเทศไทยมีองค์กรที่ได้รับการรับรองแล้วจำนวน 59[7] องค์กร มากเป็นอันดับที่ 2 ในกลุ่มประชาคมอาเซียนรองจากมาเลเซีย และมากเป็นอันดับที่ 15 ของโลก ซึ่งจำนวนองค์กรในประเทศไทยที่ให้ความสำคัญในเรื่องการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ มีเป็นจำนวนสูงกว่าหลายประเทศในภูมิภาคอาเซียน และอยู่ใน 20 ลำดับแรกของโลก ส่วนหนึ่งเป็นผลมาจากการกำหนดและออกประกาศที่เกี่ยวข้องกับกฎหมายธุรกรรมอิเล็กทรอนิกส์ของประเทศในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยอ้างอิงตามข้อกำหนดของมาตรฐาน ไอเอสโอ ไออีซี 27001 นี้ เช่น พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมอิเล็กทรอนิกส์ พ.ศ. 2553 และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 เป็นต้น ทำให้หลายองค์กรได้ให้ความสำคัญในการจัดการความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับข้อกำหนดของกฎหมายนี้

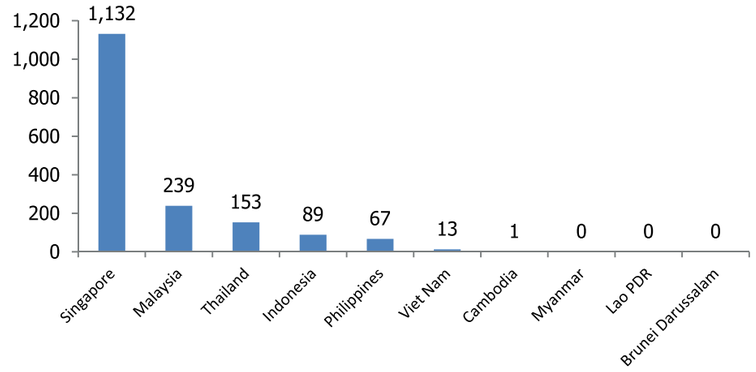
7 International Register of ISMS Certificates (http://www.iso-27001certificates.com/Register%20Search.htm)



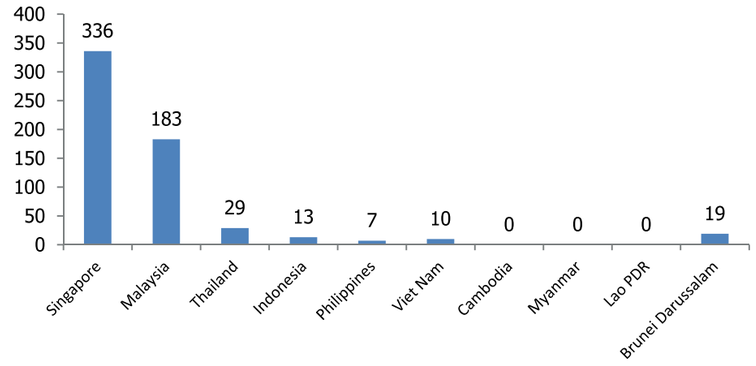
กราฟที่ 4 จำนวนองค์กรที่ได้รับมาตรฐาน ISO/IEC 27001 ของแต่ละประเทศ

นอกจากความพร้อมขององค์กรแล้ว ยังจะต้องพิจารณาถึงความพร้อมด้านบุคลากรภายในองค์กร ซึ่งสามารถวัดได้จากจำนวนบุคลากรที่ได้รับใบรับรองความเชี่ยวชาญในสาขาวิชาชีพด้านความมั่นคงปลอดภัยด้านสารสนเทศที่ได้รับการยอมรับในระดับสากล เช่น ใบรับรอง Certified Information System Security Professional (CISSP) ซึ่งรับรองโดย (ISC)[2] ผลการสำรวจเมื่อเดือนมีนาคม พ.ศ. 2556[8] พบว่าทั่วโลกมีผู้ที่ได้รับใบรับรอง CISSP 85,285 คน จาก 144 ประเทศ ประเทศที่มีผู้เชี่ยวชาญ CISSP สูงสุดคือสหรัฐอเมริกา (55,924 คน) อันดับที่สองคือสหราชอาณาจักร (4,256 คน) อันดับที่สามคือแคนาดา (4,075 คน) อันดับที่สี่คือเกาหลีใต้ ส่วนประเทศไทย (153 คน) อยู่ในอันดับที่ 34 ของโลก และเป็นอันดับที่สามในประชาคมอาเซียน รองจากสิงคโปร์ (1,132 คน) และมาเลเซีย (239 คน)

8 (ISC)², Inc (https://www.isc2.org/member-counts.aspx)



กราฟที่ 5 จำนวนของผู้ได้รับประกาศนียบัตร CISSP ในประเทศไทยเปรียบเทียบกับประเทศอื่น ๆ ในอาเซียน เมื่อเดือนมีนาคม 2556



กราฟที่ 6 จำนวนของผู้ได้รับประกาศนียบัตรของจีแอค (GIAC) ในประเทศไทย เปรียบเทียบกับประเทศในภูมิภาคอาเซียน[9]

กราฟที่ 6 แสดง จำนวนผู้เชี่ยวชาญในประเทศไทยที่ได้รับประกาศนียบัตรของจีแอค (GIAC)[10] จำนวน 29 ใบรับรอง ในขณะที่ประเทศในภูมิภาคอาเซียนซึ่งมีจำนวนผู้เชี่ยวชาญที่ได้รับประกาศนียบัตรของจีแอค (GIAC) มากเป็นลำดับที่หนึ่ง คือ ประเทศสิงคโปร์มีจำนวน 336 ใบรับรอง และประเทศมาเลเซียเป็นลำดับที่สองมีจำนวน 183 ใบรับรอง

สถาบัน EC-Council ซึ่งเป็นองค์กรที่ให้การรับรองวิชาชีพของบุคลากร โดยประกาศนียบัตรของ EC-Council ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศซึ่งเป็นที่รู้จักและได้รับการยอมรับในระดับสากล เช่น ประกาศนียบัตร

9 ข้อมูลจากผู้แทน SANS Asian Pacific เดือนกรกฎาคม 2555

10 Global Information Assurance Certification (GIAC) สถาบันรับรองประกาศนียบัตรในสาขาวิชาชีพด้านความมั่นคงปลอดภัยด้านสารสนเทศที่เน้นเนื้อหาด้านเทคนิคและการนำไปปฏิบัติ ซึ่งได้รับการยอมรับในระดับนานาชาติ

Certified Ethical Hacker (C|EH) และประกาศนียบัตร Certified Hacking Forensic Investigator (CHFI) จำนวนผู้เชี่ยวชาญในภูมิภาคอาเซียนที่ได้ประกาศนียบัตรของ EC-Council มีจำนวน 15,000 ใบรับรอง ซึ่งในจำนวนนี้เกินร้อยละ 90 เป็นผู้ที่ได้รับประกาศนียบัตรในประเทศสิงค์โปร์และประเทศมาเลเซีย สำหรับในประเทศไทยมีจำนวนเฉลี่ยประมาณ 400 ใบรับรอง[11]

จากข้อมูลจำนวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศของประเทศในภูมิภาคอาเซียน ถึงแม้ว่าจำนวนผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศไทยอยู่ในลำดับที่ 3 และมีจำนวนสูงกว่าหลายประเทศในภูมิภาคอยู่ก็ตาม แต่เมื่อเทียบเปรียบกับประเทศในภูมิภาคอาเซียนที่ได้รับการยอมรับว่ามีความก้าวหน้าในด้านเทคโนโลยีสารสนเทศ เช่น ประเทศสิงค์โปร์ และประเทศมาเลเซียแล้ว จำนวนผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของไทยยังมีจำนวนน้อยกว่าอย่างมีนัยสำคัญ สะท้อนให้เห็นถึงความขาดแคลนผู้เชี่ยวชาญที่มีทักษะสูงของไทยและเป็นความท้าทายที่ไทยต้องพัฒนาส่วนของการสร้างคนหรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยให้เป็นที่ยอมรับและได้รับการรับรองในระดับสากล เพื่อยกระดับความน่าเชื่อถือและรักษาระดับความเชื่อมั่นต่อการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและเพื่อให้มีศักยภาพที่พร้อมต่อในการแข่งขันกับประเทศต่าง ๆ ในภูมิภาคนี้

11 ข้อมูลที่ได้รับจากผู้แทนของ EC-Council ประจำภูมิภาคเอเชียแปซิฟิกในเดือนธันวาคม 2555

3

ความเป็นมาของเครือข่าย CERTs และทีม ThaiCERT

3. ความเป็นมาของเครือข่าย CERTs และทีม ThaiCERT

เซิร์ต หรือ CERT ย่อมาจากคำว่า Computer Emergency Response Team เป็นคำที่มหาวิทยาลัยคาเนกี้เมลล่อน (Carnegie Mellon University) ประเทศสหรัฐอเมริกาได้จดทะเบียนการค้าไว้ในฐานะที่จัดตั้งเป็นหน่วยงานเซิร์ตแห่งแรกของโลกซึ่งทำหน้าที่ตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นภายในประเทศ ต่อมาหลายประเทศก็ได้เลียนแบบแนวคิดนี้ และตั้งหน่วยงานภายในประเทศตนเองเพื่อทำหน้าที่เช่นเดียวกันนี้ขึ้นมา ซึ่งในภายหลังมีการรวมตัวกันเพื่อแลกเปลี่ยนข้อมูลและสร้างความร่วมมือเป็นเครือข่ายเซิร์ตที่ครอบคลุมทั่วโลก

ในส่วนของประเทศไทยนั้น ได้มีการจัดตั้งศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (Thailand Computer Emergency Response Team - ThaiCERT) ขึ้นภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) กระทรวงวิทยาศาสตร์และเทคโนโลยี เมื่อปี พ.ศ. 2543 ให้มีภารกิจหลักเพื่อตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) และให้การสนับสนุนที่จำเป็นและคำแนะนำในการแก้ไขภัยคุกคามและการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและเผยแพร่ข่าวสารและสถานการณ์ทางด้านความมั่นคงปลอดภัยคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

ซึ่งต่อมาภารกิจของ ไทยเซิร์ต ได้โอนมาที่ สพธอ. ตามมติคณะรัฐมนตรีมายังสพธอ.ซึ่งเป็นหน่วยงานที่จัดตั้งขึ้นใหม่ภายใต้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อเดือนกุมภาพันธ์ พ.ศ. 2554

ไทยเซิร์ตได้เปิดตัวอย่างเป็นทางการและให้บริการอย่างเต็มรูปแบบภายใต้ สพธอ. มาตั้งแต่เดือนธันวาคม 2554 และได้ปรับเปลี่ยนชื่อทางการของไทยเซิร์ตเป็น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือที่เรียกสั้น ๆ ว่า ไทยเซิร์ต โดยมีวิสัยทัศน์ให้สังคมออนไลน์มีความมั่นคงปลอดภัย เกิดความเชื่อมั่นกับผู้ทำธุรกรรมทางอิเล็กทรอนิกส์ พันธกิจของไทยเซิร์ต มุ่งเน้นการประสานงานกับหน่วยงานในเครือข่าย และหน่วยงานที่เกี่ยวข้องเพื่อดำเนินการแก้ไขเหตุภัยคุกคามด้านสารสนเทศที่ได้รับแจ้งหรือที่ตรวจสอบพบเจอ นอกจากนี้ไทยเซิร์ตยังมีพันธกิจเชิงรุกที่ให้ความสำคัญกับการพัฒนาทรัพยากรบุคคลเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยและเพื่อสร้างคนให้กับประเทศ

เนื่องจากไทยเซิร์ตมิได้เป็นหน่วยงานรักษากฎหมายโดยตรง ดังนั้นการปฏิบัติงานจึงมีลักษณะเป็นการประสานความร่วมมือกับเครือข่ายหน่วยงานต่าง ๆ ทั้งภายในและต่างประเทศที่เกี่ยวข้องเพื่อจัดการปัญหาภัยคุกคามด้านสารสนเทศที่เกิดขึ้น การดำเนินการของไทยเซิร์ตจึงต้องให้เจ้าของหน่วยงานที่เป็นเหยื่อของภัยคุกคามนั้นอนุญาตหรือยินยอมให้ไทยเซิร์ตเข้าไปให้บริการหรือเข้าไปช่วยแก้ไขปัญหาเมื่อเกิด incidents หรือภัยคุกคามต่างๆขึ้น และไทยเซิร์ตก็ได้ทำงานใกล้ชิดกับผู้ให้บริการและหน่วยงานในสายกระบวนการยุติธรรมเพื่อสนับสนุนการตรวจหาร่องรอย ตัวอย่างหน่วยงานภายในประเทศที่ไทยเซิร์ตได้ประสานความร่วมมือ ได้แก่

- ผู้ให้บริการอินเทอร์เน็ต
- สมาคมธนาคารไทย
- สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
- สำนักป้องกันและปราบปรามการกระทำความผิดทางเทคโนโลยีสารสนเทศ สำนักงานปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
- สำนักงานตำรวจแห่งชาติ
- กรมสืบสวนคดีพิเศษ

ในกรณีที่มีความจำเป็นต้องประสานความร่วมมือกับต่างประเทศ ไทยเซิร์ตก็มีเครือข่ายความร่วมมือกับหน่วยงานที่เกี่ยวข้องซึ่งได้ร่วมลงนามบันทึกความเข้าใจในการแลกเปลี่ยนข้อมูลและร่วมมือแก้ไขภัยคุกคามด้านสารสนเทศ ที่เกิดขึ้นกับหน่วยงานในระดับสากล เช่น

- เจพีเซิร์ต/ซีซี หรือ JPCERT/CC (Japan Computer Emergency Response Team Coordination Center) เป็นหน่วยงานเซิร์ตหลักของประเทศญี่ปุ่นที่เข้มแข็งและประสบความสำเร็จในการบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ทั้งในระดับประเทศและต่างประเทศ

- เอพีดับบลิวจี หรือ APWG (Anti-Phishing working group) เป็นหน่วยงานประเภทไม่แสวงหาผลกำไรในประเทศสหรัฐอเมริกา มีภารกิจรับมือและจัดการภัยคุกคามด้านสารสนเทศ ที่เกิดจากการใช้เครือข่ายอินเทอร์เน็ตเป็นเครื่องมือในการฉ้อโกง (Fraud) โดยใช้วิธีลักลอบขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อ รหัสผ่าน ข้อมูลสำคัญของบัตรเครดิต หรือข้อมูลสำคัญสำหรับทำธุรกรรมทางอิเล็กทรอนิกส์

- ทีมคัมรี หรือ Team Cymru เป็นหน่วยงานประเภทไม่แสวงหาผลกำไรในประเทศสหรัฐอเมริกา มีภารกิจวิจัยและพัฒนาเทคโนโลยีด้านความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) เพื่อแก้ไขปัญหาภัยคุกคามใหม่ ๆ ที่เกิดขึ้นในปัจจุบัน และให้บริการข้อมูลสถานการณ์ด้านความมั่นคงปลอดภัย (Incident) ที่ได้รวบรวมและวิเคราะห์ได้จากระบบตรวจจับของหน่วยงาน

นอกจากนี้ ไทยเซิร์ตยังได้เข้าร่วมเป็นสมาชิกเต็มรูปแบบขององค์กรทั้งในระดับภูมิภาคและนานาชาติ ได้แก่ เอพีเซิร์ต หรือ APCERT (Asia Pacific CERT) สำหรับประสานความร่วมมือกับประเทศในภาคพื้นเอเชียแปซิฟิกและ เฟิร์ส หรือ FIRST (Forum of Incident Response and Security Teams) สำหรับประสานความร่วมมือกับประเทศทั่วโลก

- เอพีเซิร์ต (APCERT) เป็นการรวมกลุ่มทีม ซีเสิร์ตส์ (CSIRTs/Computer Security and Incident Response Team) หรือทีมเซิร์ตส์ (CERTs) จากประเทศสมาชิกในแถบภูมิภาคเอเชียแปซิฟิก เพื่อสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยและพัฒนาศักยภาพของประเทศสมาชิก ในการจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ได้ทัดเทียมกับมาตรฐานนานาประเทศและกลุ่มภูมิภาคอื่น

- เฟิร์ส (FIRST) เป็นองค์กรระดับนานาชาติที่เกิดจากการรวมตัวกันของกลุ่มผู้เชี่ยวชาญทางด้านการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์และเครือข่ายของแต่ละประเทศทั่วโลก ทำหน้าที่ตอบรับ ประสานความร่วมมือ ตลอดจนการบริหารจัดการกับเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ ภารกิจส่วนใหญ่ของหน่วยงานนี้จะทำหน้าที่เป็นตัวแทนของแต่ละประเทศและหน่วยงานในการตอบรับเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบคอมพิวเตอร์และเครือข่าย โดยการประสานความร่วมมือไปยังหน่วยงานของเครือข่ายของเฟิร์ส (FIRST) เพื่อยับยั้งเหตุการณ์การละเมิดความมั่นคงปลอดภัยต่อไป

ตลอดสิบกว่าปีที่ผ่านมาไทยเซิร์ตทำหน้าที่เป็นหน่วยงานหลักของประเทศที่ให้คำแนะนำและให้การสนับสนุนที่จำเป็นในการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ แก่หน่วยงานภาครัฐ เอกชน ประชาชน และภาคธุรกิจ ในปัจจุบันไทยเซิร์ตได้รับการยอมรับและเป็นที่รู้จักทั้งในระดับภูมิภาคและนานาชาติจากผลงานที่ได้มีส่วนร่วมเป็นเครือข่ายช่วยป้องกันและยับยั้งปัญหาความมั่นคงปลอดภัยคอมพิวเตอร์ในโลกไซเบอร์ ซึ่งในปี 2556 ไทยเซิร์ต/สพธอ. ได้รับเกียรติให้เป็นเจ้าภาพร่วมจัดงานสัมมนาและประชุมประจำปีของเฟิร์สครั้งที่ 25 ปี 2013 (25th Annual FIRST Conference 2013) ในระหว่างวันที่ 16 – 21 มิถุนายน 2556 ณ โรงแรมคอนราด กรุงเทพมหานคร

งานประชุมครั้งนี้นับเป็นการจัดงานประชุมใหญ่ประจำปีครั้งที่ 2 ของเฟิร์ส (FIRST) ที่มีการจัดขึ้นในภูมิภาคอาเซียน นับจากในปี 2005 ที่จัดขึ้นที่ประเทศสิงค์โปร์ จากการคาดการณ์ของคณะกรรมการกำกับแนวทางการดำเนินงานของเฟิร์ส (FIRST Steering Committee) ได้ประมาณไว้ว่าจะมีผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้านสารสนเทศจากทั่วโลกเข้าร่วมงานไม่น้อยกว่า 500 คน ในจำนวนนี้ประมาณครึ่งหนึ่งจะเป็นบุคลากรจากหน่วยงานประเภทเซิร์ตที่เป็นสมาชิกของเฟิร์ส (FIRST) เข้าร่วมงาน ซึ่งเป็นประสบการณ์ครั้งสำคัญ ที่สร้างโอกาสให้ไทยเซิร์ตเป็นที่รู้จักในเวทีสากลและเป็นการช่วยกระตุ้นให้คนไทยหรือผู้เกี่ยวข้องตระหนักถึงเรื่อง Cybersecurity และได้แลกเปลี่ยนประสบการณ์กับผู้เชี่ยวชาญในระดับนานาชาติ

4

รายงาน “Threats & Cybersecurity ปี 2555” ภายใต้บทบาท ThaiCERT

4. รายงาน “Threats & Cybersecurity ปี 2555” ภายใต้บทบาท ThaiCERT

4.1 บริการของ ThaiCERT

การสนับสนุนให้สังคมออนไลน์มีความมั่นคงปลอดภัยและเกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์ การเตรียมการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Security Event) ซึ่งไม่สามารถคาดการณ์ล่วงหน้าได้ และการจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident) ถือเป็นกลไกที่จำเป็นเพื่อรักษาความต่อเนื่องในการดำเนินภารกิจของหน่วยงาน (Business Continuity) และการให้บริการของหน่วยงานต่าง ๆ โดยเฉพาะหน่วยงานที่ถือเป็นโครงสร้างพื้นฐานสำคัญยิ่งยวดของประเทศ (Critical Infrastructure) เช่น หน่วยงานด้านการสาธารณูปโภคและพลังงาน ด้านการสื่อสาร ด้านการแพทย์ เป็นต้น เนื่องจากหน่วยงานโครงสร้างพื้นฐานสำคัญเหล่านี้นำเทคโนโลยีเข้ามาบริหารจัดการมากขึ้น และเพิ่มความซับซ้อนให้กับระบบสารสนเทศที่เกี่ยวข้อง หากมีการโจมตีระบบสารสนเทศหรือเครือข่าย หน่วยงานที่ทำหน้าที่รับมือและจัดการภัยคุกคามด้านความมั่นคงปลอดภัยคอมพิวเตอร์ (Computer Emergency Response Team: CERT- เซิร์ต) จึงมีบทบาทที่สำคัญในการดำเนินการรับมือและจัดการภัยคุกคามเหล่านี้ รวมถึงการตรวจสอบและวิเคราะห์ข้อมูลโดยเฉพาะการดำเนินการตรวจพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) เพื่อหาตัวผู้กระทำความผิด

ไทยเซิร์ต (ThaiCERT/Thailand Computer Emergency Response Team) ถือเป็นหน่วยงานประเภทเซิร์ตหลักของประเทศ หรือเป็นที่รู้จักในชื่อสากลอีกชื่อหนึ่งว่าซีเสิร์ต (Computer Security Incident Response Team หรือ CSIRT) ที่มีภารกิจในการจัดการต่อสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์สำหรับหน่วยงานในขอบเขตการดำเนินงาน (Constituency) ครอบคลุมระบบเครือข่ายอินเทอร์เน็ตภายในประเทศไทยและระบบคอมพิวเตอร์ภายใต้โดเมนเนมของประเทศไทย (.th) มีเจ้าหน้าที่คอยเฝ้าระวังภัยคุกคามกับระบบสารสนเทศและระบบเครือข่าย และคอยรับมือและจัดการกับสถานการณ์ภัยคุกคามด้านสารสนเทศที่เกิดขึ้นตลอด 24 ชั่วโมง และในกรณีที่ต้องทำหน้าที่ประสานความร่วมมือกับประเทศอื่น ๆ เพื่อแก้ไขหรือระงับเหตุภัยคุกคามด้านสารสนเทศที่เกิดขึ้น รวมถึงการดำเนินการเพื่อส่งเสริมและสร้างความตระหนักในการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ให้กับผู้ใช้งานภายในประเทศ

ในปี 2555 ซึ่งเป็นปีแรกที่ไทยเซิร์ตให้บริการภายใต้ สพธอ. ไทยเซิร์ตได้ดำเนินกิจกรรมในภารกิจของหน่วยงานประเภทเซิร์ตผ่านบริการ 3 ประเภท ประกอบด้วย บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย (Incident Response) บริการข้อมูลข่าวสารความมั่นคงปลอดภัยด้านสารสนเทศ และบริการวิชาการเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และคาดว่าจะพร้อมให้บริการตรวจพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics) ได้เต็มรูปแบบในปี 2556

4.1.1 บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย

ปัจจุบันไทยเซิร์ตให้บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย ทางโทรศัพท์และทางอีเมลแก่บุคคลทั่วไป สถาบันการศึกษาและสถาบันวิจัย หน่วยงานภาครัฐและเอกชนทั่วโลก เมื่อได้รับแจ้งเหตุภัยคุกคาม ผู้เชี่ยวชาญของไทยเซิร์ตตรวจสอบข้อมูลเพื่อยืนยันว่าสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ได้รับแจ้งเกิดขึ้นและมีอยู่จริง แล้ววิเคราะห์ข้อมูลเพื่อหาหน่วยงานที่เป็นต้นเหตุของปัญหา จากนั้นจึงประสานงานไปยังหน่วยงานที่เกี่ยวข้องดังกล่าวเพื่อให้คำแนะนำและดำเนินการแก้ไขปัญหาต่อไป

ไทยเซิร์ตมีระบบการติดตามความคืบหน้าของการจัดการปัญหาที่ได้รับแจ้ง และได้กำหนดมาตรฐานการให้บริการไว้ กล่าวคือ ไทยเซิร์ตจะแจ้งหน่วยงานที่เกี่ยวข้องเพื่อแก้ปัญหาที่ได้รับแจ้งและรายงานสถานะของการจัดการและแก้ไขปัญหาภายใน 2 วันทำการ จากนั้นจะติดตามผลการดำเนินงานในทุก 2 วันทำการ โดยไทยเซิร์ตได้จัดเตรียมช่องทางการติดต่อเพื่อแจ้งเหตุภัยคุกคามด้านสารสนเทศ ไว้ 2 ช่องทาง ประกอบด้วย ทางโทรศัพท์หมายเลข 02-142-2483 เวลา 8.30 – 17.30 น. ทุกวันยกเว้นวันหยุดราชการ และทางอีเมลที่ report@thaicert.or.th และในกรณีที่ผู้แจ้งมีความประสงค์จะรักษาความลับของข้อมูลในอีเมลที่ส่งถึงไทยเซิร์ต ผู้แจ้งสามารถเข้ารหัสลับข้อมูลด้วยเทคโนโลยีพีจีพี (PGP)[12] ด้วยกุญแจสาธารณะของไทยเซิร์ตดังต่อไปนี้

- อีเมล: report@thaicert.or.th
- หมายเลขของกุญแจ (Key ID): 0x F2CB3EE1
- ประเภทของกุญแจ (Key Type): RSA
- วันหมดอายุ (Expires): 2015-06-25
- ขนาดความยาว (Key size): 2048
- Fingerprint: 29B3 2C79 FB4A D4D7 E71A 71ED 5FFE F781 F2CB 3EE1

4.1.2 บริการข้อมูลข่าวสารความมั่นคงปลอดภัย

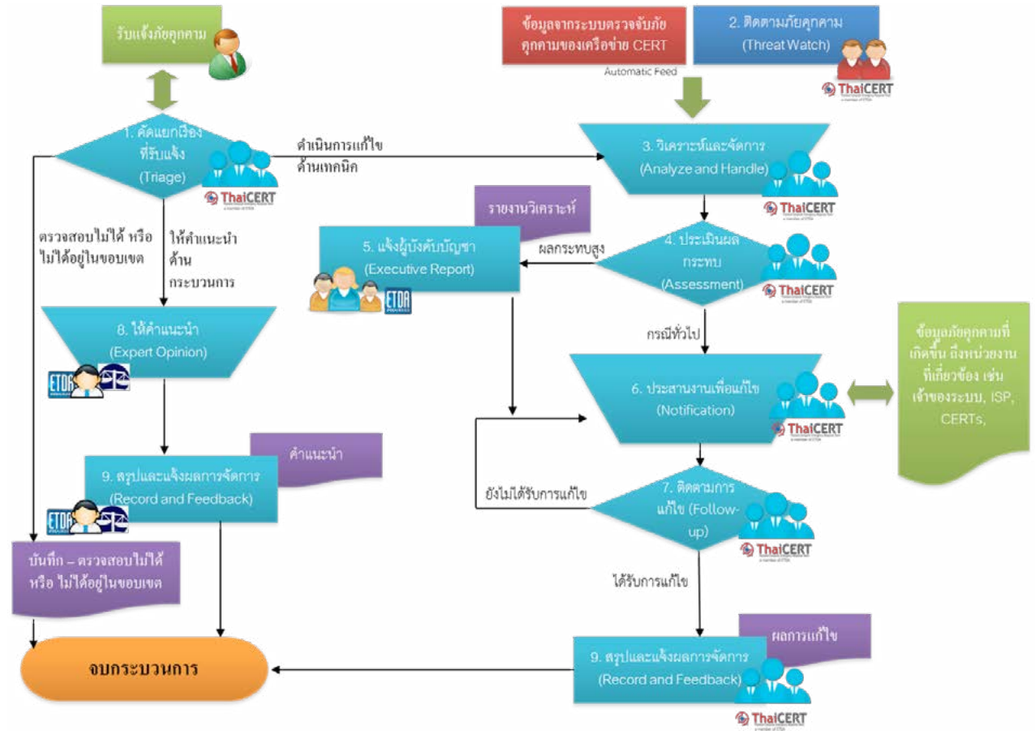
ไทยเซิร์ตมีภารกิจในการแจ้งเตือนภัยคุกคามด้านสารสนเทศ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ได้รับแจ้งจากเครือข่ายของหน่วยงานประเภทเซิร์ต (CERT) หรือ ซีเสิร์ต (CSIRT) และที่ถูกตรวจพบจากการทำงานของไทยเซิร์ตเอง อีกทั้งยังมีภารกิจในการสร้างความตระหนักและความพร้อมในการรับมือต่อภัยคุกคามด้านสารสนเทศ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดขึ้น โดยผู้เชี่ยวชาญของไทยเซิร์ตจะวิเคราะห์ข้อมูลภัยคุกคามด้านสารสนเทศ หรือเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่มีผลกระทบสูงกับผู้ใช้งาน พร้อมเสนอแนะข้อควรปฏิบัติในการรับมือ แก้ไขหรือป้องกัน ในบทความแจ้งเตือนภัยคุกคามด้านสารสนเทศของไทยเซิร์ต นอกจากนั้น ไทยเซิร์ตยังจัดทำข้อมูลเชิงสถิติของเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ได้รับแจ้งและนำมาเผยแพร่บนเว็บไซต์ไทยเซิร์ต (www.thaicert.or.th) เป็นรายเดือน เพื่อนำเสนอสถิติและแนวโน้มสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดภายในประเทศไทย

4.1.3 บริการวิชาการในการรักษาความมั่นคงปลอดภัย

ไทยเซิร์ตมีผู้เชี่ยวชาญที่มีความรู้ ความสามารถ และศักยภาพในการให้บริการวิชาการด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกับหน่วยงานทั้งภายในและต่างประเทศ โดยให้คำปรึกษากับหน่วยงานภายในประเทศในการวิเคราะห์ข้อมูลภัยคุกคามด้านสารสนเทศ การจัดทำแผนและนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้สอดคล้องกับมาตรฐานสากลทางด้านเทคโนโลยีสารสนเทศและสอดคล้องกับข้อกำหนดของกฎหมาย พร้อมให้คำปรึกษาในการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ การจัดอบรมสัมมนา เพื่อสร้างความตระหนักหรือเสริมสร้างศักยภาพของบุคลากรของหน่วยงานให้สามารถป้องกันและแก้ไขภัยคุกคามด้านสารสนเทศ อีกทั้งจัดการซักซ้อมรับมือภัยคุกคามด้านสารสนเทศเพื่อเสริมทักษะและสร้างความพร้อมในการรับมือภัยคุกคามด้านสารสนเทศให้บุคลากรของทั้งภาครัฐและเอกชน รวมถึงการสนับสนุนวิทยากรในการบรรยายเพื่อสร้างความตระหนักและให้ความรู้กับหน่วยงานทั้งในและต่างประเทศ

12 PGP – Pretty Good Privacy เป็นเทคโนโลยีที่ใช้ในการเข้ารหัสลับข้อมูลในรูปแบบเทคโนโลยีกุญแจสาธารณะ (Public Key) สร้างขึ้นโดย Philip R. Zimmermann นิยมใช้เข้ารหัสลับและลงลายมือชื่ออิเล็กทรอนิกส์ในการรับส่งอีเมล

4.2 การประสานเพื่อรับมือและจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย



รูปที่ 1 ขั้นตอนการดำเนินงานเพื่อแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ได้รับแจ้งของไทยเซิร์ต

เพื่อให้การแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ได้รับแจ้งดำเนินการไปอย่างมีประสิทธิภาพ มีมาตรฐานของบริการเทียบเท่ากับการดำเนินงานของหน่วยงานในภาคเอกชน และเป็นไปตามกระบวนการที่ถูกต้อง ไทยเซิร์ตจึงกำหนดขั้นตอนการประสานเพื่อรับมือและจัดการภัยคุกคามด้านสารสนเทศ เป็นขั้นตอน ดังนี้

4.2.1 การคัดแยกเรื่องที่ได้รับแจ้ง (Triage)

เมื่อเจ้าหน้าที่ไทยเซิร์ตได้รับแจ้งเรื่องร้องเรียนภัยคุกคาม หรือสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ จะดำเนินการคัดกรองเรื่องที่ได้รับแจ้งก่อนการดำเนินการ โดยใช้หลักเกณฑ์การพิจารณาคัดแยก ตามเงื่อนไขอย่างน้อย 1 เงื่อนไข ดังนี้

- พบข้อเท็จจริงที่ยืนยันให้เห็นว่าเรื่องร้องเรียนหรือเหตุภัยคุกคามว่าเกิดขึ้นจริง และเป็นสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นกับหน่วยงานในขอบเขตการดำเนินงาน (Constituency) ภายในประเทศไทยของไทยเซิร์ต

- สามารถยืนยันตัวตนผู้เสียหายหรือผู้แจ้งได้จริง
- เป็นสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับรายงานจากแหล่งที่เชื่อถือได้ เช่น เป็นหน่วยงานที่น่าเชื่อถือ เป็นหน่วยงานภายในเครือข่ายที่มีการติดต่อและแจ้งเหตุภัยคุกคามด้านสารสนเทศกับไทยเซิร์ตอยู่ก่อนแล้ว เป็นต้น

หลังการคัดแยกแล้วเสร็จเจ้าหน้าที่ไทยเซิร์ตจะแจ้งให้ผู้แจ้งทราบถึงผลการคัดแยกว่าทางไทยเซิร์ต/สพธอ. จะรับเรื่องที่ได้รับแจ้งไปดำเนินการต่อหรือไม่ ซึ่งมีขั้นตอนการดำเนินการดังนี้

- รับดำเนินการ เมื่อเจ้าหน้าที่ไทยเซิร์ตพิจารณา เรื่องที่ได้รับแจ้งว่าเป็นการขอรับคำแนะนำการแก้ไขปัญหาในเชิงกระบวนการซึ่งเกี่ยวข้องทางกฎหมาย จะส่งเรื่องต่อให้กับเจ้าหน้าที่กฎหมาย สพธอ. เพื่อพิจารณาและให้คำแนะนำต่อผู้แจ้ง สำหรับเรื่องที่เป็นภัยคุกคามและจำเป็นต้องดำเนินการด้านเทคนิค เจ้าหน้าที่ไทยเซิร์ตจะวิเคราะห์และจัดการสถานการณ์ด้านความมั่นคงปลอดภัยในขั้นตอนต่อไปของการดำเนินงาน
- ไม่รับดำเนินการ เจ้าหน้าที่ไทยเซิร์ตจะแจ้งให้ผู้แจ้งทราบถึงเหตุผลในการปฏิเสธการดำเนินการ เช่น เรื่องที่แจ้งเป็นเรื่องอยู่นอกขอบเขตบริการ หรือไม่สามารถตรวจสอบได้ พร้อมทั้งบันทึกข้อมูลในระบบและจบกระบวนการ

4.2.2 การวิเคราะห์และจัดการภัยคุกคาม (Analyze and Handle)

เจ้าหน้าที่ไทยเซิร์ตที่มีหน้าที่โดยตรงในการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย โดยจะดำเนินการทางเทคนิคเพื่อตรวจสอบและแก้ไขภัยคุกคามของสถานการณ์ที่ได้รับแจ้งและผ่านการคัดกรอง รวมถึงสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับแจ้งจากหน่วยงานเครือข่ายของไทยเซิร์ต หรือ ที่ทีมติดตามภัยคุกคามของไทยเซิร์ตตรวจพบ

หลังจากตรวจสอบสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดขึ้น เจ้าหน้าที่ไทยเซิร์ตจะประเมินผลกระทบที่เกิดขึ้นว่า จำเป็นต้องยกระดับการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย และรายงานเหตุการณ์ที่เกิดขึ้นต่อระดับนโยบายรับทราบในทันทีเพื่อพิจารณาสั่งการหรือไม่ โดยเกณฑ์ในการประเมินระดับผลกระทบของภัยคุกคาม แบ่งเป็น 2 ประเภทคือ

ผลกระทบสูง : เป็นสถานการณ์ภัยคุกคามที่มีความสำคัญและมีผลกระทบในระดับกลางขึ้นไป อ้างอิงตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. 2555 หรือเป็นภัยคุกคามที่จะส่งผลกระทบต่อความมั่นคง หรือมีผลกระทบทางสังคมในวงกว้าง ซึ่งเจ้าหน้าที่ไทยเซิร์ตต้องรีบจัดการสถานการณ์ภัยคุกคามที่เกิดขึ้นและรายงานต่อระดับนโยบายในทันที

กรณีทั่วไป : เป็นสถานการณ์ภัยคุกคามที่เกิดขึ้นที่ส่งผลต่อองค์กรหรือหน่วยงานและอาจทำให้เกิดการสูญเสีย ทางทรัพย์สินหรือข้อมูลอันเป็นความลับของผู้ใช้หรือ หน่วยงานได้ โดยเจ้าหน้าที่ไทยเซิร์ตจะรับมือและจัดการภัยคุกคามตามมาตรฐานของบริการ

หมายเหตุ รายละเอียดของเกณฑ์การประเมินผลกระทบ และขั้นตอนการรายงานสถานการณ์ภัยคุกคามต่อระดับนโยบายอยู่ระหว่างการพิจารณาทบทวน

4.2.3 การให้คำแนะนำในการแก้ปัญหา (Expert Opinion)

ในหลายกรณี ผู้แจ้งหรือผู้เสียหายจากสถานการณ์ภัยคุกคาม ต้องการขอรับความเห็นในการดำเนินการต่าง ๆ ที่เกี่ยวข้องทางกฎหมาย เจ้าหน้าไทยเซิร์ตจะประสานกับเจ้าหน้าที่ฝ่ายกฎหมาย สพธอ. เพื่อให้ความเห็นในเรื่องที่ได้รับแจ้ง ในกรณีที่เป็นเรื่องที่มีความละเอียดอ่อนและซับซ้อน เจ้าหน้าที่ฝ่ายกฎหมาย สพธอ. จะติดต่อผู้เชี่ยวชาญด้านกฎหมายภายนอกที่ได้รับความเห็นชอบจาก สพธอ. เพื่อขอรับความเห็นในประเด็นต่าง ๆ ที่เกี่ยวข้องเพื่อสรุปและแจ้งให้ผู้แจ้งรับทราบถึงความเห็นในการดำเนินการต่อไป

4.2.4 การแจ้งเตือนและติดตามผล (Notification and Follow-up)

เจ้าหน้าที่ไทยเซิร์ตที่มีหน้าที่โดยตรงในการรับมือและจัดการสถานการณ์ภัยคุกคาม โดยแจ้งสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นให้กับหน่วยงาน/บุคคลที่เกี่ยวข้องตามข้อมูลการลงทะเบียนที่ผ่านการตรวจสอบและยืนยันความถูกต้องจากเจ้าหน้าที่ไทยเซิร์ตแล้ว เช่น เจ้าของระบบคอมพิวเตอร์ ผู้ให้บริการอินเทอร์เน็ต หน่วยงานประเภทเซิร์ต (CERT) หน่วยงานของรัฐ มหาวิทยาลัย หน่วยงานในสายสืบสวนสอบสวน หน่วยงานสายยุติธรรม เป็นต้น เพื่อดำเนินการแก้ไขภัยคุกคามที่เกิดขึ้นจนได้รับผลลัพธ์เป็นที่น่าพอใจกับผู้เกี่ยวข้องทุกฝ่ายและบันทึกผลการดำเนินการ ส่วนกรณีที่สถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ยังไม่ได้รับการแก้ไขจนเป็นที่น่าพอใจ เจ้าหน้าที่ผู้รับผิดชอบจะติดตามผลการแก้ไขในทุก 2 วันหลังรับแจ้งเหตุจนกว่าสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับแจ้งนั้นจะได้รับการแก้ไขจนเป็นที่น่าพอใจ

4.2.5 สรุปและแจ้งผลการจัดการ (Record and Feedback)

หลังการแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับแจ้งจนได้รับผลเป็นที่น่าพอใจ เจ้าหน้าที่ไทยเซิร์ตจะบันทึกรายละเอียดการดำเนินการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น รวมถึงผลการวิเคราะห์ต้นเหตุของปัญหาที่เกิดขึ้น จากนั้นจึงแจ้งผลการแก้ไขให้กับผู้แจ้งได้รับทราบ

4.3 Threats ที่ไทยเซิร์ตรับแจ้งและดำเนินการ

ในปี 2555 ที่ผ่านมา ไทยเซิร์ตได้รับแจ้งสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกี่ยวข้องกับประเทศไทยจาก 2 ช่องทางคือ ทางอีเมลหรือโทรศัพท์โดยตรงยังไทยเซิร์ต และทางระบบอัตโนมัติ (Automatic Feed) โดยข้อมูลที่ได้รับแจ้งผ่านระบบอัตโนมัตินั้นมาจากหน่วยงานที่มีความร่วมมือกับไทยเซิร์ตด้านการรักษาความมั่นคงปลอดภัยในระดับสากล เช่น เอพีดับบิวจี (Anti-Phishing Working Group, APWG) ทีมคัมรี (Team CYMRU) และ ไมโครซอฟต์ (Microsoft)

จากการรับแจ้งผ่านทั้ง 2 ช่องทางที่กล่าวมานั้น ไทยเซิร์ตได้พัฒนากระบวนการวิเคราะห์ ประสานเพื่อรับมือและจัดการ และให้คำแนะนำเพื่อแก้ไขสถานการณ์ภัยคุกคามที่เกิดขึ้นกับผู้เกี่ยวข้องโดยตรง อีกทั้งยังนำข้อมูลสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับแจ้งทั้งหมดในปี 2555 มาวิเคราะห์ถึงแนวโน้มภัยคุกคามด้านสารสนเทศที่เกิดขึ้น และจัดทำทวิเคราะห์สถิติสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ในภาพรวมของประเทศไทย ซึ่งสามารถนำสรุปประเด็นที่น่าสนใจได้ ดังนี้

- โปรแกรมไม่พึงประสงค์ที่ได้รับรายงานสูงสุด คือโปรแกรมซูส (Zeus) ซึ่งเป็นโปรแกรมไม่พึงประสงค์ประเภทบอตเน็ต (Botnet)[13] ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน รองลงมาเป็น โปรแกรมรูสต๊อค (Rustock) ที่มีความสามารถในการส่งสแปม (Spam)[14] ได้มากกว่า 25,000 ฉบับต่อชั่วโมง

13 บอตเน็ต (Botnet) ภัยคุกคามด้านสารสนเทศที่เกิดกับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ ซึ่งโปรแกรมไม่พึงประสงค์นี้จะทำการรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ต โดยอาจเป็นคำสั่งที่ให้ทำการโจมตีระบบเครือข่าย ส่งสแปม หรือโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อ เป็นต้น

14 สแปม (Spam) ภัยคุกคามด้านสารสนเทศที่เกิดจากผู้ไม่ประสงค์ดีทำการส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมาก ที่ไม่ได้มีความประสงค์ที่จะได้รับข้อมูลนั้นมาก่อน ส่วนมากเป็นการโฆษณาสินค้าและบริการ สร้างความเดือดร้อนรำคาญแก่ผู้รับ

และยังสามารถใช้โจมตีความพร้อมใช้งานของระบบคอมพิวเตอร์อื่นในลักษณะดีดอส (DDoS)[15] ได้เช่นกัน โดยในปี 2555 จำนวนรายการที่ได้รับรายงานที่เป็น Botnet มีจำนวนทั้งสิ้น 4,404,089 รายการ และส่วนใหญ่ระบาดอยู่ในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตในประเทศไทย

- ได้รับรายงานประเภท Spam เป็นจำนวน 1,523,469 รายการ ซึ่งทั้งหมดเป็นการรับแจ้งผ่าน Automatic Feed
- พบว่าเครื่องให้บริการดีเอ็นเอส (DNS) ในเครือข่ายอินเทอร์เน็ตในประเทศไทยจำนวนมากกว่า 143,302 หมายเลขไอพี (IP Address) ไม่ได้รับการตั้งค่าให้เหมาะสมและเสี่ยงต่อการถูกใช้เป็นเครื่องมือในการโจมตีในลักษณะ DDoS ได้
- ได้รับรายงานประเภทพอร์ตสแกนนิ่ง (Port Scanning) จำนวนทั้งสิ้น 30,521 รายการ โดยเป้าหมายส่วนใหญ่จะเป็นพอร์ต (Port) ที่เกี่ยวข้องกับบริการการเข้าถึงและดูแลระบบสารสนเทศจากระยะไกล (Remote Administration) ของระบบปฏิบัติการวินโดวส์ (Windows) คิดเป็นสัดส่วนประมาณร้อยละ 80 สำหรับ พอร์ตและเมื่อแบ่งแยกตามหมายเลขของพอร์ตแล้ว พอร์ตที่เป็นเป้าหมายในการสแกนสูงสุดสองลำดับแรกประกอบด้วย พอร์ต หมายเลข 4899[16] (Port 4899) คิดเป็นร้อยละ 45.40 และพอร์ตหมายเลข 3389[17] (Port 3389) คิดเป็นร้อยละ 34.16
- แม้ว่าจำนวนประเภท DDoS ที่ได้รับรายงานจะมีจำนวนน้อยที่สุดเมื่อเทียบกับภัยคุกคามด้านสารสนเทศประเภทอื่น ๆ แต่ไม่สามารถจะสรุปได้ว่าประเทศไทยแทบไม่มีภัยคุกคามประเภท DDoS เกิดขึ้น เนื่องจากการตรวจจับและวิเคราะห์ประเภท DDoS สามารถดำเนินการได้ยากกว่าการตรวจวิเคราะห์ภัยคุกคามด้านสารสนเทศประเภทอื่น ๆ
- จากการรายงาน การโจมตีเกือบทุกประเภทถูกพบในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตรายใหญ่ของประเทศ และพบว่ามีการระบาดของโปรแกรมไม่พึงประสงค์ประเภท Botnet ในเครือข่ายของผู้ให้บริการโทรศัพท์เคลื่อนที่ด้วย
- การฉ้อโกง (Fraud) จัดเป็นภัยคุกคามที่ได้รับแจ้งผ่านอีเมลสูงสุดโดยมีจำนวน 534 รายการ คิดเป็นสัดส่วนร้อยละ 67.42 จากทั้งหมด 792 รายการที่ได้รับแจ้ง

15 ดีดอส (DDoS) ภัยคุกคามด้านสารสนเทศในลักษณะการโจมตีสภาพความพร้อมใช้งานของระบบ โดยมีลักษณะการโจมตีมาจากหลายแห่งไปยังเป้าหมายเดียวกันภายในช่วงเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

16 พอร์ทหมายเลข 4899 ใช้ในเรื่องของการดูแลระบบจากระยะไกล (TCP Radmin Remote administration)

17 พอร์ทหมายเลข 3389 ใช้ในเรื่องของการดูแลคอมพิวเตอร์จากระยะไกล (Port 3389/TCP Windows Remote Desktop)

4.3.1 สถิติ Incident ที่เกิดภายในประเทศไทยและได้รับแจ้งผ่านระบบอัตโนมัติ (Automatic Feed)

เริ่มตั้งแต่เดือนสิงหาคม 2555 ที่ผ่านมา ในกรณีที่มีการโจมตีจากภายในประเทศไทยไปยังระบบคอมพิวเตอร์ในต่างประเทศ เครือข่ายหน่วยงานด้านความมั่นคงปลอดภัยไซเบอร์ในระดับสากลที่ตรวจจับภัยคุกคามดังกล่าวได้จะแจ้งรายงานข้อมูลมายังไทยเซิร์ต โดยจำแนกสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์แต่ละรายการตามประเภทออกเป็น 9 ประเภท ประกอบด้วย ประเภท Botnet ประเภทบรูทฟอร์ซ (Brute Force)[18] ประเภทดีดอส (DDoS) ประเภทมัลแวร์ ยูอาร์แอล (Malware URL)[19] ประเภทโอเพ่น ดีเอ็นเอส รีโซลเวอร์ (Open DNS Resolver)[20] ประเภทโอเพ่น พร็อกซี่ เซิร์ฟเวอร์ (Open Proxy Server)[21] ประเภทฟิชชิ่ง (Phishing)[22] ประเภทสแกนนิ่ง (Scanning)[23] และประเภท Spam ซึ่งสามารถสรุปเป็นสถิติและบทวิเคราะห์ได้ ดังต่อไปนี้

18 บรูทฟอร์ซ (Brute Force) ภัยคุกคามด้านสารสนเทศในลักษณะการโจมตีหรือเจาะระบบเป้าหมายด้วยวิธีการสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้นเพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น การสุ่มบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าสู่ระบบ

19 มัลแวร์ ยูอาร์แอล (Malware URL) ภัยคุกคามด้านสารสนเทศที่เกิดจากเว็บไซต์ที่ใช้เพื่อเผยแพร่โปรแกรมไม่พึงประสงค์ (Malware) ส่วนมากจะเกิดจากการที่ผู้ไม่ประสงค์ดีบุกรุกเข้าไปยังเว็บไซต์ของผู้อื่นและใช้พื้นที่ของเว็บไซต์นั้นในการเผยแพร่โปรแกรมไม่พึงประสงค์ (Malware) และหลอกลวงให้ผู้อื่นเข้าถึงหรือดาวน์โหลดโปรแกรมไม่พึงประสงค์นี้

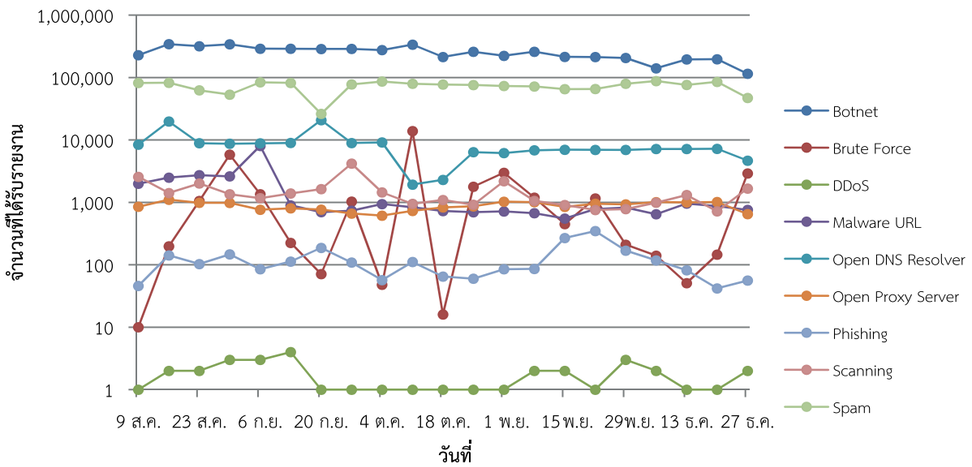
20 โอเพ่น ดีเอ็นเอส รีโซลเวอร์ (Open DNS Resolver) ภัยคุกคามด้านสารสนเทศที่เกิดจากการตั้งค่าของเครื่องให้บริการดีเอ็นเอส (DNS) อย่างไม่เหมาะสม ทำให้อาจถูกใช้เป็นส่วนหนึ่งของการโจมตี ในลักษณะดีดอส (DDOS) ได้

21 โอเพ่น พร็อกซี่ เซิร์ฟเวอร์ (Open Proxy Server) ภัยคุกคามด้านสารสนเทศที่เกิดจากการตั้งค่าเว็บพร็อกซี่ (Web Proxy) ไม่เหมาะสม ทำให้ผู้ใช้งานทั่วไปเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่ผ่านระบบยืนยันตัวตน (Authentication) กลายเป็นช่องทางที่ผู้ไม่ประสงค์ดีสามารถใช้ในการกระทำความผิดหรือใช้โจมตีระบบอื่น ๆ ได้

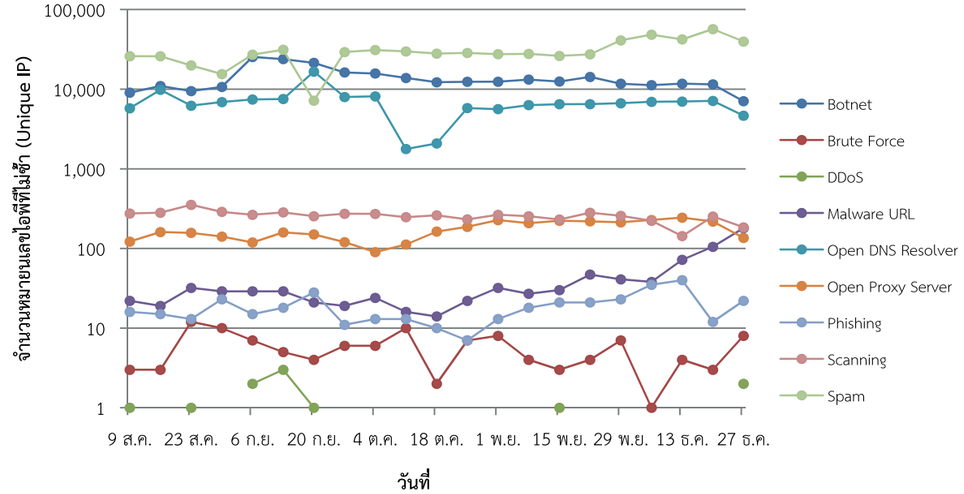
22 ฟิชชิ่ง (Phishing) ภัยคุกคามด้านสารสนเทศในลักษณะการฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ ส่วนใหญ่มีวัตถุประสงค์ในการขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลสำคัญทางธุรกรรมอิเล็กทรอนิกส์ เป็นต้น โดยผู้โจมตีใช้วิธีล่อลวงให้ผู้ใช้งานเข้าถึงบริการที่ถูกปลอมขึ้นและทำให้ผู้ใช้งานเข้าใจผิดว่ากำลังใช้งานกับระบบของผู้ให้บริการจริงอยู่

23 สแกนนิ่ง (Scanning) ภัยคุกคามด้านสารสนเทศที่เกิดจากการที่ผู้ไม่ประสงค์ดี ตรวจสอบข้อมูลเบื้องต้นของระบบปฏิบัติการหรือบริการบนเครื่องแม่ข่ายโดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมายผ่านระบบเครือข่าย แล้วรวบรวมผลลัพธ์จากการตอบสนองจากระบบที่เป็นเป้าหมายนั้น ข้อมูลที่ได้จากการสแกนนิ่ง (Scanning) มักจะถูกใช้เป็นข้อมูลในการเจาะหรือบุกรุกเข้าระบบต่อไป

1.) Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติปี 2555 จำแนกตามประเภทภัยคุกคาม



กราฟที่ 7 จำนวน Incident ที่ได้รับแจ้งจำแนกตามประเภทในเดือนสิงหาคม-ธันวาคม 2555 เป็นรายสัปดาห์



กราฟที่ 8 จำนวน Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัตินับตามจำนวนหมายเลขไอพีที่ไม่ซ้ำกัน และจำแนกตามประเภท ในเดือนสิงหาคม-ธันวาคม 2555 เป็นรายสัปดาห์

ตารางที่ 1 จำนวน Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติจำแนกตามประเภท ในเดือนสิงหาคม-ธันวาคม 2555

ลำดับ	ประเภทภัยคุกคาม	จำนวนที่ได้รับรายงาน
1	Botnet	5,237,832
2	Spam	1,523,469
3	Open DNS Resolver	173,227
4	Brute Force	34,746
5	Scanning	30,521
6	Malware URL	30,193
7	Open Proxy Server	18,418
8	Phishing	2,479
9	DDoS	36

ตารางที่ 2 จำนวน Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัตินับตามจำนวน IP Address ที่ไม่ซ้ำกันและจำแนกตามประเภท ในเดือนสิงหาคม-ธันวาคม 2555

ลำดับ	ประเภทภัยคุกคาม	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)
1	Spam	636,461
2	Botnet	286,919
3	Open DNS Resolver	143,302
4	Scanning	5,375
5	Open Proxy Server	3,597
6	Malware URL	848
7	Phishing	387
8	Brute Force	117
9	DDoS	11

จากรายการสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่ไทยเซิร์ตได้รับแจ้งผ่านระบบอัตโนมัติตั้งแต่เดือนสิงหาคม 2555 เป็นต้นมา ตารางที่ 1 แสดงจำนวนรายการที่ได้รับแจ้งจำแนกตามประเภท รวมรายการทั้งสิ้นที่ได้รับแจ้งเป็นจำนวน 7,050,921 รายการ กราฟที่ 7 แสดงจำนวนรายการที่ได้รับแจ้งจำแนกตามประเภทภัยคุกคามด้านสารสนเทศแสดงตามรายสัปดาห์ พบว่าภัยคุกคามด้านสารสนเทศประเภท Botnet มีจำนวนรายการที่ได้รับรายงานสูงสุด มีค่าเฉลี่ยต่อสัปดาห์ประมาณ 259,000 รายการ ภัยคุกคามด้านสารสนเทศที่ได้รับรายงานสูงสุดต่อสัปดาห์เป็นลำดับที่ 2 คือ Spam เฉลี่ยประมาณ 100,000 รายการต่อสัปดาห์ ส่วนภัยคุกคามด้านสารสนเทศอื่น ๆ ที่เหลือมีจำนวนรายการที่ได้รับแจ้งรวมกันโดยเฉลี่ยน้อยกว่า 12,000 รายการต่อสัปดาห์

เมื่อพิจารณาถึงข้อมูลที่ได้รับรายงานผ่านระบบอัตโนมัติ พบว่ามีการรายงานภัยคุกคามจาก IP Address ที่ใช้ก่อเหตุเดียวกันและเป็นภัยคุกคามด้านสารสนเทศประเภทเดียวกันอยู่เป็นจำนวนมาก ซึ่งความหมายว่าภัยคุกคามด้านสารสนเทศบางประเภท เช่น

Botnet หรือ Spam มีรูปแบบการก่อเหตุด้วยการส่งข้อมูลไปยังเป้าหมายอยู่ตลอดเวลา ทำให้เกิดจำนวนรายงานมากกว่าจำนวน IP Address ที่มีอยู่จริง

ตารางที่ 2 แสดงให้เห็นว่ามี IP Address ทั้งหมดที่ถูกตรวจพบว่าเกี่ยวข้องกับการก่อเหตุภัยคุกคามด้านสารสนเทศมีจำนวน 1,077,017 หมายเลข ซึ่งอาจกล่าวได้ว่านี่คือจำนวน IP Address ในประเทศไทยที่มีปัญหาด้านความมั่นคงปลอดภัยคอมพิวเตอร์ โดยจะเห็นได้ชัดว่า ภัยคุกคามด้านสารสนเทศประเภท Spam เป็นภัยคุกคามที่มีจำนวน IP Address ที่ได้รับแจ้งมากที่สุดถึง 636,461 หมายเลข หรือคิดเป็นสัดส่วนร้อยละ 62.7 จากจำนวนที่ได้รับแจ้งทั้งหมด ส่วนภัยคุกคามด้านสารสนเทศประเภท Botnet มีจำนวน IP Address ที่ได้รับแจ้งสูงสุดเป็นลำดับที่ 2 คือ 286,919 หมายเลข และลำดับที่ 3 คือ Open DNS Resolvers มีจำนวน IP Address ที่ได้รับแจ้งอยู่ 143,302 หมายเลข มีข้อสังเกตที่น่าสนใจ คือ ภัยคุกคามด้านสารสนเทศประเภท Brute Force และ DDoS กลับมีจำนวน IP Address ที่ได้รับรายงานรวมกันน้อยกว่า 100 หมาย ซึ่งข้อมูลของภัยคุกคามด้านสารสนเทศในแต่ละประเภท จะถูกนำมาวิเคราะห์ในเชิงสถิติและนำเสนอในส่วนถัดไป

2.) Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติแยกตามผู้ให้บริการเครือข่ายในประเทศไทย

ตารางที่ 3 จำนวนรายการ Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติ และนับตามจำนวน IP Address ที่ซ้ำกันจำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)	สัดส่วน (ร้อยละ)
1	TOT (Public) Co., Ltd.	568,017	52.75
2	True Internet Co., Ltd.	265,641	24.67
3	Triple T Broadband (Public) Co., Ltd.	123,838	11.50
4	Advanced Info Service (Public) Co., Ltd.	50,188	4.66
5	Total Access Communication (Public) Co., Ltd.	30,174	2.80
6	JasTel Network Co., Ltd.	8,255	0.77
7	Advance Datanetwork Communications Co., Ltd.	4,293	0.40
8	UniNet	3,230	0.30
9	CAT Telecom (Public) Co., Ltd.	3,032	0.28
10	CS Loxinfo (Public) Co., Ltd.	2,838	0.26

ตารางที่ 4 จำนวน IP Address ที่จดทะเบียนโดยหน่วยงานในประเทศไทย 10 ลำดับแรก จำแนกตามผู้ให้บริการเครือข่าย[24]

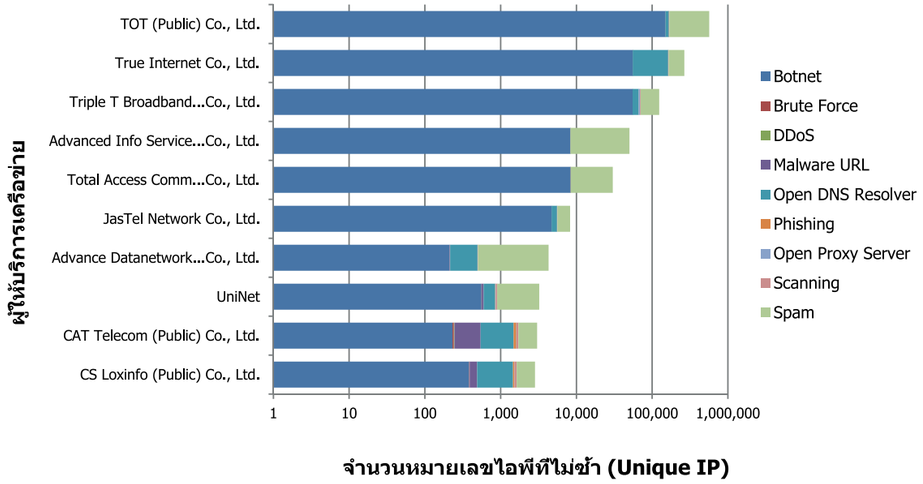
ลำดับ	ผู้ให้บริการเครือข่าย	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)
1	True Internet Co., Ltd.	1,956,864
2	TOT (Public) Co., Ltd.	1,289,984
3	Triple T Broadband (Public) Co., Ltd.	1,048,576
4	CAT Telecom (Public) Co., Ltd.	437,504
5	Advanced Info Service (Public) Co., Ltd.	420,864
6	TT&T (Public) Co., Ltd.	403,456
7	CS Loxinfo (Public) Co., Ltd.	377,088
8	KSC Commercial Internet Co., Ltd.	326,656
9	Total Access Communication (Public) Co., Ltd.	263,168
10	Internet Thailand (Public) Co., Ltd.	221,184

จากข้อมูลสถานการณ์ด้านความมั่นคงปลอดภัยที่ได้รับแจ้งผ่านระบบอัตโนมัติในตารางที่ 3 พบว่า IP Address ที่ได้รับรายงาน ส่วนใหญ่จะอยู่ในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตและผู้ให้บริการโทรศัพท์เคลื่อนที่ทั้งสิ้น เช่น ทีโอที (TOT) ทรู (True) ทริปเปิ้ลที บรอดแบนด์ (Triple T Broadband) เอไอเอส (AIS) และ ดีแทค (DTAC)[25] ซึ่งเป็นทั้งผู้ให้บริการอินเทอร์เน็ตบรอดแบนด์แบบผ่านสาย (Wired Broadband) และผู้ให้บริการอินเทอร์เน็ตบรอดแบนด์แบบไร้สาย (Wireless Broadband) และโดยภัยคุกคามด้านสารสนเทศที่ได้รับรายงานในแต่ละผู้ให้บริการเครือข่ายส่วนใหญ่เป็นประเภท Spam และ Botnet ดังแสดงตามกราฟที่ 9

จากจำนวน IP Address ทั้งหมด 8,559,616 หมายเลขที่จดทะเบียนในประเทศไทย ข้อมูลในตารางที่ 4 แสดงให้เห็นว่าหน่วยงานที่ถือครอง IP Address มากที่สุดใน 10 ลำดับแรกของประเทศไทยเป็นผู้ให้บริการอินเทอร์เน็ต โดยผู้ให้บริการเครือข่ายอินเทอร์เน็ตที่ถือครอง IP Address สูงสุดใน 3 ลำดับแรก ถือครองจำนวน IP Address ประมาณร้อยละ 50 ของจำนวน IP Address ของทั้งประเทศ ในขณะที่ IP Address ที่ถูกตรวจพบว่ามีส่วนเกี่ยวข้องกับภัยคุกคามซึ่งมีจำนวนถึง 872,206 หมายเลข ซึ่งสูงกว่าร้อยละ 10 ของจำนวน IP Address ทั้งหมดของประเทศไทย และเมื่อพิจารณาถึงรูปแบบการใช้งานเครือข่ายอินเทอร์เน็ตในประเทศไทยมักเป็นรูปแบบที่เครื่องคอมพิวเตอร์หลายเครื่องในหน่วยงานเข้าถึงอินเทอร์เน็ตด้วย IP Address หมายเลขเดียวกันแล้ว จึงเป็นไปได้อย่างยิ่งว่า จำนวนเครื่องคอมพิวเตอร์ที่เกี่ยวข้องกับภัยคุกคามที่แท้จริงที่พบสูงกว่าจำนวน IP Address ที่ได้รับรายงานว่าพบปัญหา

24 ข้อมูล Directory Listing เผยแพร่ผ่านบริการ FTP (ftp.apnic.net/stats/apnic/) จาก APNIC ณ วันที่ 16 พฤศจิกายน 2555

25 ดีแทค (DTAC) ใช้ชื่อผู้ให้บริการเครือข่ายที่ลงทะเบียนไว้ ว่า Total Access Communication, Plc



กราฟที่ 9 จำนวนรายการ Incident ที่ได้รับแจ้งผ่านระบบอัตโนมัติ
และนับตามจำนวน IP Address ที่ไม่ซ้ำกัน จำแนกตามประเภทและผู้ให้บริการเครือข่าย

3.) ฟิชชิ่ง (Phishing)

ตารางที่ 5 “10 ลำดับแรกของประเทศที่พบการรายงานประเภทฟิชชิ่ง (Phishing) มากที่สุด”

ลำดับ	ประเทศ	จำนวน Phishing ที่ได้รับรายงาน	สัดส่วน (ร้อยละ)
1	United States	64,064	30.44
2	Hong Kong	32,910	15.64
3	Germany	25,217	11.98
4	China	15,733	7.47
5	Philippines	6,981	3.32
6	United Kingdom	5,740	2.73
7	Moldova, Republic of	5,363	2.55
8	Canada	4,744	2.25
9	Russian Federation	4,506	2.14
10	France	3,802	1.81

ในตารางที่ 5 พบว่า ภัยคุกคามด้านสารเทศประเภท Phishing ในประเทศสหรัฐอเมริกา มากที่สุดถึง 64,064 รายการ คิดเป็นสัดส่วนร้อยละ 30.44 ของจำนวนที่ได้รับรายงานทั้งหมด ลำดับรองลงมาเป็นเขตบริหารพิเศษฮ่องกง และประเทศเยอรมนี ซึ่งมีสัดส่วนของจำนวนภัยคุกคามที่ได้รับรายงาน 32,910 รายการ และ 25,217 รายการ หรือคิดเป็นสัดส่วนร้อยละ 15.64 และร้อยละ 11.98 ตามลำดับ ส่วนประเทศไทยอยู่ในอันดับที่ 14 คิดเป็นสัดส่วนร้อยละ 1.18 หรือเป็นจำนวน 2,474 รายการ

ตารางที่ 6 สถิติภัยคุกคามด้านสารสนเทศประเภท Phishing ที่เกิดขึ้นในประเทศไทย จำแนกตามประเภทของโดเมนเนม

ลำดับ	ประเภทของโดเมน	จำนวนที่ได้รับรายงาน	สัดส่วน (ร้อยละ)
1	.com	1,336	53.89
2	.go.th	329	13.27
3	.co.th	256	10.33
4	.ac.th	173	6.98
5	Unknown (IP address)	130	5.24
6	.net	121	4.88
7	.org	67	2.7
8	.in.th	48	1.94
9	.biz	7	0.28
10	.tv	6	0.24

เมื่อวิเคราะห์ฟิชชิ่ง ยูอาร์แอล (Phishing URL)[26] ที่ได้รับรายงานว่าเกิดขึ้นในประเทศไทยแสดง ในตารางที่ 6 พบสถิติที่น่าสนใจคือเว็บไซต์ในภาคธุรกิจของไทยถูกใช้ในการเผยแพร่หน้า Phishing เป็นจำนวนสูงสุด คิดเป็นร้อยละ 64.50 จากรายการทั้งหมดที่ได้รับรายงาน โดยสามารถแบ่งเป็น .com ร้อยละ 53.89 .co.th ร้อยละ 10.33 และ .biz ร้อยละ 0.28 ส่วนเว็บไซต์ที่จดทะเบียนในลักษณะหน่วยงานของรัฐ (.go.th) และสถาบันการศึกษา (.ac.th) ถูกใช้ในการเผยแพร่หน้า Phishing คิดเป็นสัดส่วนรวมกันร้อยละ 20.25 จากรายการทั้งหมดที่ได้รับแจ้ง นอกจากนั้นยังพบว่ามีการเผยแพร่หน้า Phishing ในเครื่องที่ไม่มีโดเมนเนม (Domain name) หรือเป็นโดเมนเนม Unknown ซึ่งหมายถึง Phishing URL ที่ใช้ IP Address ในการเข้าถึงหน้า Phishing โดยตรง

26 ข้อมูลที่ใช้ระบุที่อยู่ของเว็บไซต์ที่เป็นภัยคุกคามด้านสารสนเทศประเภท Phishing

ตารางที่ 7 สถิติรายการเว็บไซต์ที่ถูกใช้ในการเผยแพร่ฟิชชิ่ง เป็นจำนวนสูงสุด 10 อันดับแรก โดยนับเฉพาะ IP Address ที่ไม่ซ้ำ พร้อมข้อมูลยูอาร์แอล และสัดส่วนจำนวนรายการที่ได้รับรายงาน ต่อ IP Address จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนที่ได้รับรายงาน	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)	จำนวนยูอาร์แอลที่ไม่ซ้ำ (Unique URL)	จำนวนที่ได้รับรายงาน / จำนวน Unique IP
1	CAT Telecom (Public) Co., Ltd.	9931	1,028	130	531	7.9
2	CS Loxinfo (Public) Co., Ltd.	4750 7568 9891	407	62	254	6.6
3	Internet Thailand (Public) Co., Ltd.	4618	175	22	131	8
4	Internet Solution & Service Provider Co., Ltd.	24299 7654	130	19	99	6.8
5	Super Broadband Network Co., Ltd.	45458	110	1	37	110
6	Metrabyte Co., Ltd.	56067	97	27	74	3.6
7	Government Information Technology Services	9835	75	10	43	7.5
8	True Internet Co., Ltd.	7470 9287	64	8	31	8
9	Ministry of Education	23974	45	23	35	2
10	UniNet	4621	44	8	22	5.5

เป็นที่น่าสังเกตว่า รายการที่ได้รับแจ้งส่วนใหญ่จะอยู่ในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ โดยมีเพียงผู้ให้บริการเครือข่ายหน่วยงานของรัฐ (Government Information Technology Services/ GITS) และเครือข่ายภาคการศึกษา (Uninet และกระทรวงศึกษาธิการ) ที่ติดอยู่ใน 10 อันดับแรกของภัยคุกคามด้านสารสนเทศประเภท Phishing ด้วยเช่นกัน และเมื่อพิจารณาจำนวนที่ได้รับรายงาน/จำนวน Unique IP ซึ่งมีค่ามากกว่า 1 นั้น อาจสามารถอธิบายได้เป็นหลายประเด็น เช่น ผู้ให้บริการเครือข่ายส่วนใหญ่ได้ติดตั้งเว็บไซต์ไว้บนเครื่องแม่ข่ายมากกว่า 1 เว็บไซต์และเมื่อเว็บไซต์หนึ่งถูกเจาะระบบได้ เว็บไซต์อื่น ๆ ที่ติดตั้งอยู่บนเครื่องแม่ข่ายเดียวกันก็ถูกเจาะระบบและถูกใช้สำหรับเผยแพร่หน้าฟิชชิ่งด้วย จึงเป็นผลทำให้ค่าเฉลี่ยของจำนวนภัยคุกคามฟิชชิ่งที่พบบนเครื่องแม่ข่ายหนึ่ง ๆ มีค่ามากกว่า 1 หรือในอีกกรณีหนึ่ง อาจเป็นไปได้ว่าเครื่องแม่ข่ายหนึ่ง ๆ ถูกเจาะระบบและถูกใช้เผยแพร่หน้าฟิชชิ่งเป็นจำนวนหลายครั้ง จึงเป็นผลทำให้ค่าเฉลี่ยนี้มีค่ามากกว่า

4.) มัลแวร์ ยูอาร์แอล (Malware URL)

ตารางที่ 8 สถิติประเภท Malware URL ที่ถูกรายงานเป็นจำนวนสูงสุด 10 อันดับแรก จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนที่ได้รับรายงาน	สัดส่วน (ร้อยละ)
1	CAT Telecom (Public) Co., Ltd.	9931	17,087	56.67
2	CS Loxinfo (Public) Co., Ltd.	4750 9891	5,749	19.07
3	Sripatum University	46079	1,784	5.92
4	Internet Solution & Service Provider Co., Ltd.	24299 7654	796	2.64
5	Ministry of Education	23974	796	2.64
6	Internet Thailand (Public) Co., Ltd.	4618	675	2.24
7	i-STT Nation Ltd.	17887	475	1.58
8	Metrabyte Co., Ltd.	56067	424	1.41
9	KSC Commercial Internet Co., Ltd.	7693	309	1.02
10	UniNet	38589 4621	289	0.96

ไทยเซิร์ตได้รับแจ้งภัยคุกคามด้านสารสนเทศ ประเภทมัลแวร์ ยูอาร์แอล (Malware URL) เป็นจำนวนทั้งสิ้น 30,153 รายงาน เมื่อวิเคราะห์ข้อมูลในตารางที่ 8 โดยจำแนกตามผู้ให้บริการเครือข่าย พบว่าส่วนใหญ่อยู่ในเครือข่ายของผู้ให้บริการเครือข่ายแคท เทเลคอม (CAT Telecom) โดยมีสัดส่วนถึงร้อยละ 56.67 ของจำนวนรายงานทั้งหมด รองลงมาเป็นของผู้ให้บริการเครือข่ายซีเอส ล็อกซอินโฟ (CS Loxinfo) คิดเป็นสัดส่วนร้อยละ 19.07 ซึ่งใน 10 อันดับแรกของผู้ให้บริการเครือข่ายนี้ ส่วนใหญ่จะเป็นผู้ให้บริการอินเทอร์เน็ต ที่มีบริการศูนย์ข้อมูลอินเทอร์เน็ต (IDC) ในเชิงพาณิชย์เช่นเดียวกับข้อมูลภัยคุกคามด้านสารสนเทศประเภท Phishing ส่วนผู้ให้บริการเครือข่ายที่เป็นหน่วยงานด้านการศึกษาและสถาบันการศึกษา เช่น กระทรวงศึกษาธิการ มหาวิทยาลัยศรีปทุม และเครือข่ายสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) ก็พบปัญหาประเภท Malware URL มากเป็น 10 อันดับแรกเช่นกัน

ตารางที่ 9 สถิติประเภท Malware URL ที่มีจำนวนยูอาร์แอลที่ไม่ซ้ำกันมากที่สุด 10 อันดับแรก จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนยูอาร์แอลที่ไม่ซ้ำ (Unique URL)	สัดส่วน (ร้อยละ)
1	CAT Telecom (Public) Co., Ltd.	9931	11,793	70.69
2	CS Loxinfo (Public) Co., Ltd.	4750 9891	1,981	11.87
3	Internet Solution & Service Provider Co., Ltd.	24299 7654	435	2.61
4	Ministry of Education	23974	391	2.34
5	i-STT Nation Ltd.	17887	366	2.19
6	Sripatum University	46079	306	1.83
7	Internet Thailand (Public) Co., Ltd.	4618	279	1.67
8	Metrabyte Co., Ltd.	56067	178	1.07
9	Proimage Engineering and Communication Co., Ltd.	23884	124	0.74
10	KSC Commercial Internet Co., Ltd.	7693	115	0.69

ทั้งนี้ข้อมูลสถิติที่ปรากฏ รายการในตารางที่ 9 เป็นรายการของเหตุภัยคุกคามด้านสารสนเทศประเภท Malware URL ที่ได้รับแจ้งมาทั้งหมด ซึ่งในบางครั้งอาจมีการแจ้ง URL ซ้ำเข้ามามากกว่า 1 ครั้ง และเมื่อนำสถิตินี้มาแบ่งข้อมูลตาม IP Address ที่ไม่ซ้ำกันแล้ว พบว่ามีการเปลี่ยนแปลงอันดับอยู่เล็กน้อย ดังแสดงในตารางที่ 10

ตารางที่ 10 สถิติประเภท Malware URL นับที่มีจำนวน IP Address ไม่ซ้ำกันมากที่สุด 10 อันดับแรก จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)	สัดส่วน (ร้อยละ)
1	CAT Telecom (Public) Co., Ltd.	9931	298	35.48
2	CS Loxinfo (Public) Co., Ltd.	4750 9891	100	11.9
3	Ministry of Education	23974	63	7.5
4	Internet Solution & Service Provider Co., Ltd.	24299 7654	43	5.12
5	Internet Thailand (Public) Co., Ltd.	4618	41	4.88
6	Metrabyte Co., Ltd.	56067	37	4.4
7	UniNet	38589 4621	32	3.81
8	Proimage Engineering and Communication Co., Ltd.	23884	21	2.5
9	True Internet Co., Ltd.	7470 9287	20	2.38
10	TOT (Public) Co., Ltd.	9737	18	2.14

จากตารางที่ 10 พบว่ามี IP Address ทั้งหมดที่เกี่ยวข้องอยู่ 840 หมายเลข แบ่งกลุ่มตามผู้ให้บริการเครือข่าย และจัดเรียงลำดับตามจำนวนรายงานที่ได้รับสูงสุด 10 ลำดับแรก โดยในลำดับที่ 1 ยังคงเป็น CAT Telecom มีจำนวน IP Address เพียง 298 หมายเลข เมื่อเทียบกับจำนวน

Malware URL ที่ถูกรายงานถึง 11,793 รายการ ตามข้อมูลในตารางที่ 9 จะเห็นว่าภัยคุกคามประเภท Malware URL เกิดขึ้นโดยเฉลี่ยประมาณ 39.6 รายการต่อ IP Address

ตารางที่ 11 ประเภทของโดเมนเนม 10 ลำดับแรกที่ได้รับรายงานภัยคุกคามด้านสารสนเทศประเภท Malware URL

ลำดับ	ประเภทของโดเมน	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)
1	.com	358
2	.ac.th	189
3	.go.th	72
4	Unknown (IP address)	68
5	.co.th	53
6	.net	43
7	.org	22
8	.in.th	18
9	.or.th	8
10	.mi.th	4

จากตารางที่ 11 พบว่า หน่วยงานที่จดทะเบียนเป็นภาคธุรกิจ (.com และ .co.th) มีรายงานการพบ Malware URL ถึง 411 รายการ ในขณะที่หน่วยงานที่จดทะเบียนโดเมนเนมเป็นสถาบันการศึกษา (.ac.th) และหน่วยงานของรัฐ (.go.th) ต่างถูกรายงานในเรื่องภัยคุกคามประเภทเดียวกันนี้มากเป็นอันดับต้น ๆ เช่นเดียวกัน ซึ่งอาจหมายความว่า ระบบของหน่วยงานดังกล่าวไม่ได้รับการดูแลป้องกันเท่าที่ควร จนทำให้ผู้ไม่หวังดีสามารถบุกรุกเข้าไปใช้ทรัพยากรของระบบเพื่อใช้เผยแพร่ Malware ได้

ตารางที่ 12 รายชื่อโดเมนเนมที่ได้รับรายงาน Malware URL สูงสุด 10 ลำดับแรก

ลำดับ	โดเมนเนม	จำนวนยูอาร์แอลที่ไม่ซ้ำ (Unique URL)
1	phichit.net	8,084
2	www.energyfantasia.com	1,418
3	school.obec.go.th	1,216
4	www.marketatnation.com	356
5	www.thaigoodview.com	290
6	ppdho.com	287
7	www.wearehappy.in.th	224
8	www.winnerwideworld.co.th	165
9	203.172.205.22	128
10	www.msw-101.com	100

ตารางที่ 12 เป็นการวิเคราะห์จำนวน Malware URL โดยจำแนกตามโดเมนเนม พบว่า เว็บไซต์ phichit.net ซึ่งเป็นเว็บไซต์ของสำนักงานพื้นที่การศึกษาพิจิตรเขต 1 มีจำนวน Malware URL อยู่ในเว็บไซต์เป็นอันดับหนึ่งถึง 8,084 รายการ ตามมาด้วยเว็บไซต์ www.energyfantasia.com ซึ่งเป็นเว็บไซต์ของโครงการปฏิบัติการหารสอง กระทรวงพลังงาน ด้วยจำนวน 1,418 รายการ เว็บไซต์ school.obec.go.th ซึ่งเป็นเว็บไซต์ของสำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน ด้วยจำนวน 1,216 รายการ โดย 3 อันดับแรกนี้เป็นเว็บไซต์ของหน่วยงานรัฐทั้งสิ้น

5.) สแปม (Spam)

ตารางที่ 13 สถิติประเภท Spam ที่มากที่สุด 10 อันดับแรก จำแนกตามผู้ให้บริการเครือข่าย

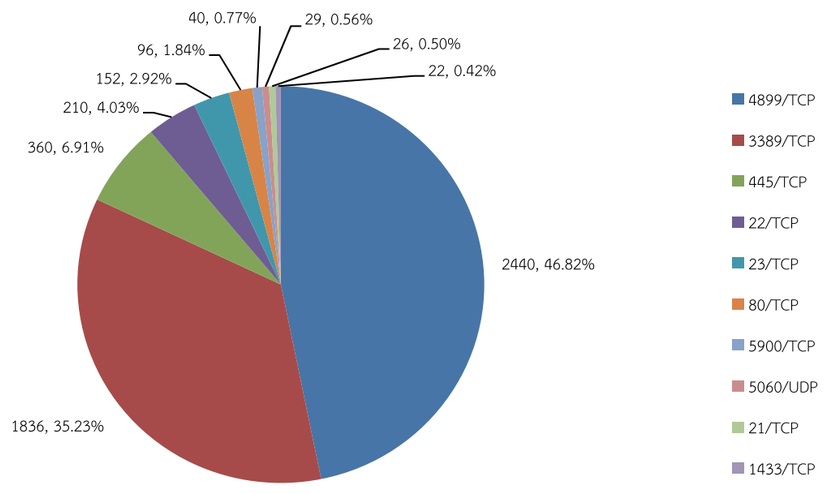
ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนที่ได้รับรายงาน	สัดส่วนรายการ (ร้อยละ)	จำนวน Unique IP	สัดส่วนของ Unique IP (ร้อยละ)	จำนวนที่ได้รับรายงาน / จำนวน Unique IP
1	TOT (Public) Co., Ltd.	23969 56120 9737	680,067	44.68	399,730	62.81	1.7
2	Advanced Info Service (Public)	38444	242,566	15.93	41,821	6.57	5.8
3	Total Access Communication (Public) Co., Ltd.	17724 24378	193,730	12.73	21,743	3.42	8.9
4	True Internet Co., Ltd.	17552 45805 55554 7470 9287	166,146	10.91	100,698	15.82	1.6
5	Triple T Broadband (Public) Co., Ltd.	45758	79,096	5.2	53,176	8.36	1.5
6	UniNet	38589 4621	37,441	2.46	2,330	0.37	16.1
7	CAT Telecom (Public) Co., Ltd.	18252 9931	28,256	1.86	1,312	0.21	21.5
8	CS Loxinfo (Public) Co., Ltd.	45537 4750 9891	14,506	0.95	1,206	0.19	12
9	Super Broadband Network Co., Ltd.	45458	11,009	0.72	1,189	0.19	9.3
10	King Mongkut's University of Technology Thonburi	9551	9,618	0.63	488	0.08	19.7

ในปี 2555 ไทยเซิร์ตได้รับรายงานว่า เครื่องคอมพิวเตอร์ในประเทศไทยได้ถูกใช้เป็นฐานในการส่ง Spam เป็นจำนวนถึง 1,522,224 รายการ โดยส่วนใหญ่จะถูกส่งออก

จากเครือข่ายของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ ได้แก่ เครือข่ายของทีโอที (TOT) คิดเป็นร้อยละ 46.50 เครือข่ายของเอไอเอส (AIS) คิดเป็นร้อยละ 16.59 เครือขายของดีแทค (DTAC) คิดเป็นร้อยละ 13.25 และในเครือข่ายของทรู (True) คิดเป็นร้อยละ 11.36 เป็นต้น ซึ่งเป็นที่น่าสังเกตว่าการที่ผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ถูกใช้เป็นฐานการส่ง Spam ในอันดับต้นๆ เนื่องจากมีลูกค้าเป็นจำนวนมาก จึงทำให้เกิดโอกาสสูงในการใช้เป็นฐานสำหรับการส่ง Spam สิ่งนี้แสดงให้เห็นว่า ผู้ใช้งานอินเทอร์เน็ตมีการใช้บริการอินเทอร์เน็ตผ่านระบบโทรศัพท์เคลื่อนที่มากขึ้นอย่างเห็นได้ชัด และคาดว่าส่วนใหญ่เป็นการกลุ่มใช้งานที่เครื่องคอมพิวเตอร์แบบพกพาที่เชื่อมต่ออินเทอร์เน็ตผ่านเครือข่ายโทรศัพท์เคลื่อนที่ยังขาดความตระหนักและการให้ความสำคัญต่อการรักษาความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์อย่างเหมาะสม หรือมีการใช้งานที่มีความเสี่ยงที่จะตกเป็นเหยื่อของ Malware ประเภทต่างๆ นอกจากนี้ ยังเป็นที่น่าสังเกตว่า สัดส่วนของจำนวน IP Address ที่เกิดปัญหาขึ้นนั้น จะสอดคล้องกับจำนวนผู้ใช้บริการของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ด้วย

เมื่อนำสัดส่วนของจำนวนรายการที่มีการแจ้งต่อ IP Address ของผู้ให้บริการอินเทอร์เน็ตแต่ละรายมาจัดลำดับ พบว่าลำดับที่ไม่มีความสัมพันธกับลำดับของจำนวนรายงานโดยรวม ซึ่งเป็นไปได้ว่าอาจเป็นเพราะเครื่องแม่ข่ายในเครือข่ายของผู้ใช้บริการบางรายถูกเช่าใช้ หรือถูกเจาะระบบโดยผู้ไม่ประสงค์ดี เพื่อใช้สำหรับส่ง Spam โดยเฉพาะหรืออาจจะเกิดจากกรณีอื่นซึ่งต้องตรวจสอบต่อไป

6.) สแกนนิ่ง (Scanning)



กราฟที่ 10 สัดส่วนประเภทและหมายเลขของพอร์ต (Port) ที่ถูกโจมตี ในลักษณะของกราฟรูปวงกลม

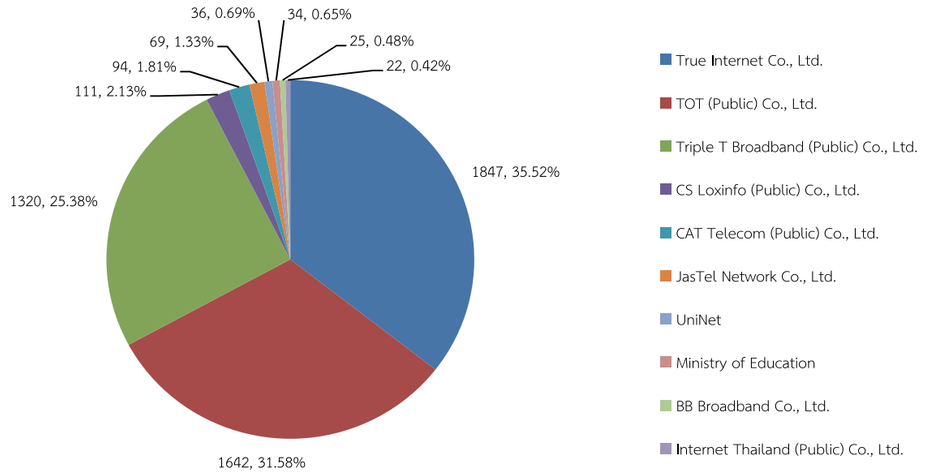
ตารางที่ 14 สถิติประเภท Scanning จำแนกตามประเภทและหมายเลขของพอร์ต (Port) ที่ถูกโจมตีสูงสุด 10 ลำดับแรก

ลำดับ	พอร์ตที่ถูกสแกน	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)	รายละเอียด
1	4899/TCP	2,440	Attacks on Radmin remote administration tool
2	3389/TCP	1,836	Dictionary attacks on RDP (remote desktop) – largely the activity of Morto worm
3	445/TCP	360	Buffer overflow attacks on Windows RPC services
4	22/TCP	210	Dictionary attacks on SSH servers
5	23/TCP	152	Attacks on Telnet service
6	80/TCP	96	Attacks on web applications
7	5900/TCP	40	Attacks on VNC
8	5060/UDP	29	Attacks on SIP
9	21/TCP	26	Attacks on FTP service
10	1433/TCP	22	Attacks on MS SQL

จากรายงานภัยคุกคามด้านสารสนเทศประเภท Scanning ที่มีต้นทางจากเครื่องคอมพิวเตอร์ในประเทศไทย เมื่อแบ่งจาก IP Address ที่ไม่ซ้ำกัน ดังตารางที่ 14 และกราฟที่ 10 พบว่ามี IP Address ที่เป็นต้นทางของการ Scanning ทั้งหมดจำนวน 5,375 หมายเลข และเมื่อแบ่งแยกตาม Port ที่เป็นเป้าหมาย พบว่าส่วนใหญ่เป็น Port ประเภท Remote Administration โดยอันดับแรกคือ 4899/TCP Radmin Remote Administration มีจำนวนถึงร้อยละ 46.82 ลำดับที่ 2 คือ 3389/TCP Windows Remote Desktop มีจำนวนร้อยละ 35.23 ลำดับที่ 3 คือ 445/TCP Windows RPC services มีจำนวนร้อยละ 6.91 และในลำดับที่สี่คือ 22/TCP SSH server มีจำนวนร้อยละ 4.03 สามารถสรุปได้ว่า ผู้โจมตีมีแนวโน้มที่จะรวบรวมข้อมูล และพยายามเจาะระบบเป้าหมายผ่านโปรแกรมประเภท Remote Administration เป็นหลัก ดังนั้นการปิดหรือปิดกั้นการเข้าถึงบริการประเภท Remote Administration บนเครื่องแม่ข่ายที่ติดต่อกับเครือข่ายอินเทอร์เน็ตโดยตรง ถือเป็นการลดความเสี่ยงของการถูกเจาะระบบจากผู้ไม่ประสงค์ดี

ตารางที่ 15 สถิติประเภท Scanning ที่มากที่สุด 10 อันดับแรก พิจารณาจากจำนวน IP Address ไม่ซ้ำกันที่ถูกใช้เพื่อสแกนเครื่องเป้าหมาย จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)
1	True Internet Co., Ltd.	17552 7470 9287	1,847
2	TOT (Public) Co., Ltd.	23969 56120 9737	1,642
3	Triple T Broadband (Public) Co., Ltd.	45758	1,320
4	CS Loxinfo (Public) Co., Ltd.	4750 9891	111
5	CAT Telecom (Public) Co., Ltd.	9931	94
6	JasTel Network Co., Ltd.	45629	69
7	UniNet	38589 4621	36
8	Ministry of Education	23974	34
9	BB Broadband Co., Ltd.	38794	25
10	Internet Thailand (Public) Co., Ltd.	4618	22

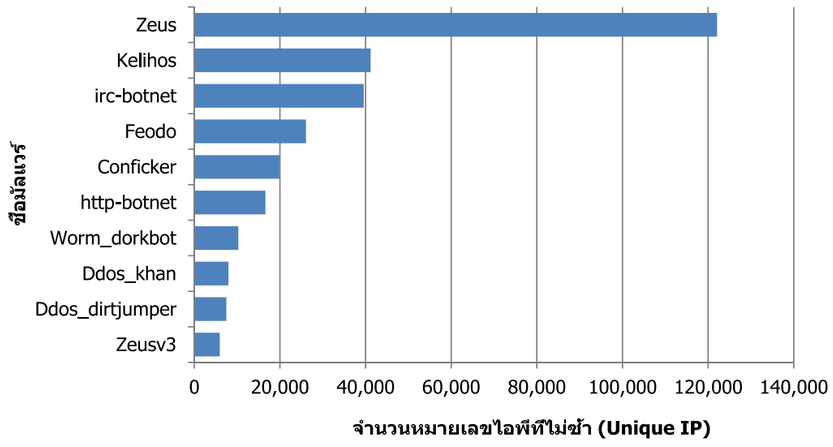


กราฟที่ 11 สถิติประเภท Scanning ที่มากที่สุด 10 อันดับแรก พิจารณาตามจำนวน IP Address ที่ไม่ซ้ำกันที่ถูกใช้เพื่อสแกนเครื่องเป้าหมาย และจำแนกตามผู้ให้บริการเครือข่าย

จากรายการข้อมูลภัยคุกคามด้านสารสนเทศประเภท Scanning โดยจำแนกตามผู้ให้บริการเครือข่าย ดังตารางที่ 15 และกราฟที่ 11 พบว่า IP Address ที่เป็นต้นทางส่วนมากอยู่ในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์รายใหญ่ โดยอันดับหนึ่งได้แก่

ทรู (True) มีจำนวน 1,847 หมายเลข รองลงมาคือ ทีโอที (TOT) จำนวน 1,642 หมายเลข และทริปเปิลที (Triple T) จำนวน 1,320 หมายเลข ซึ่งคิดเป็นสัดส่วนรวมกันประมาณร้อยละ 90 ซึ่งคาดว่าจะเป็นเครื่องคอมพิวเตอร์ในเครือข่ายบรอดแบนด์ของผู้ให้บริการ

7.) บอตเน็ต (Botnet)



กราฟที่ 12 สถิติประเภท Botnet นับตามจำนวนรายงานที่ได้รับแจ้ง และจำแนกตามประเภทของ Botnet

ไทยเซิร์ตได้รับรายงานภัยคุกคามด้านสารสนเทศประเภท Botnet ที่นับเฉพาะ IP Address ที่ไม่ซ้ำกัน พบว่ามีรายงานจำนวนทั้งสิ้น 312,534 รายการ และจัดเรียงลำดับตระกูลของ Botnet ที่ได้รับแจ้งสูงสุด 10 ลำดับแรกได้ดังที่แสดงไว้ในกราฟที่ 12 โดยลำดับที่หนึ่งคือ Botnet ชื่อ ซูส (Zeus) ที่มีจำนวน 122,102 รายการ รองลงมาคือ เคลิฮอส (Kelihos) จำนวน 41,181 รายการและไออาร์ซี-บอตเน็ต (irc-botnet) จำนวน 39,577 รายการ ซึ่งความสามารถของ Botnet เหล่านี้ มีทั้งถูกใช้เป็นฐานในการส่ง Spam การลักลอบขโมยข้อมูลส่วนบุคคลของผู้ใช้งาน การโจมตีในลักษณะ DDoS หรือหลายความสามารถผสมกัน

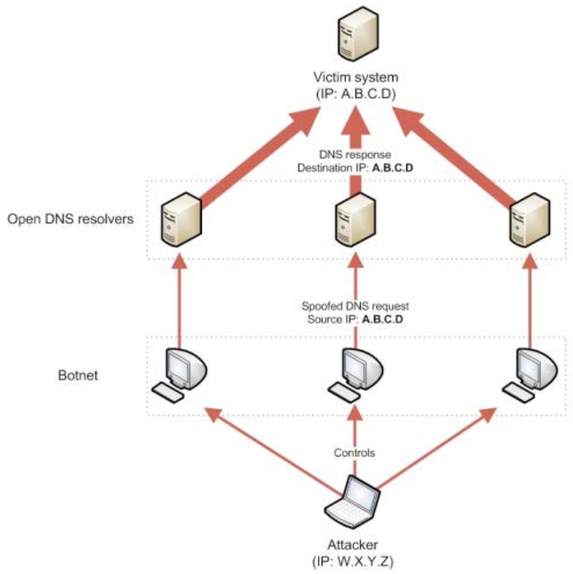
ตารางที่ 16 จำนวนรายงานประเภท Botnet ที่ได้รับแจ้งสูงสุด 10 อันดับแรก จำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	จำนวนที่ได้รับรายงาน
1	TOT (Public) Co., Ltd.	161,402
2	True Internet Co., Ltd.	57,935
3	Triple T Broadband (Public) Co., Ltd.	57,458
4	Advanced Info Service (Public) Co., Ltd.	13,218
5	Total Access Communication (Public) Co., Ltd.	10,899
6	JasTel Network Co., Ltd.	4,904
7	Ministry of Education	2,658
8	UniNet	734
9	CS Loxinfo (Public) Co., Ltd.	407
10	True Move Co., Ltd.	348

จากตารางที่ 16 พบว่า ภัยคุกคามด้านสารสนเทศประเภท Botnet จะพบมากในผู้ให้บริการที่เป็นผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ที่ให้บริการเครือข่ายบรอดแบนด์ เช่น ทีโอที (TOT) ทรู (True) และทริปเปิลที (Triple T) โดยคิดเป็นสัดส่วนรวมกันมากกว่าร้อยละ 88 ของจำนวนรายงานทั้งหมดที่ได้รับ แสดงให้เห็นว่าเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไป เช่น ผู้ใช้งานตามบ้าน ถูกควบคุมด้วย Botnet เป็นจำนวนมาก และเสี่ยงที่จะกลายเป็นเครื่องมือเพื่อใช้ในการโจมตีระบบผู้อื่น หรือถูกขโมยข้อมูลสำคัญของผู้ใช้งานได้

8.) โอเพ่น ดีเอ็นเอส รีโซลเวอร์ (Open DNS Resolver)

ลักษณะของภัยคุกคามด้านสารสนเทศประเภท Open DNS Resolver นี้ จะอาศัยช่องโหว่ของบริการ DNS หรือการตั้งค่าที่ไม่เหมาะสม ที่ยอมให้เกิด Recursive Query จากเครือข่ายอื่น ๆ ได้โดยไม่มีการควบคุม จนกลายเป็นเครื่องมือในการโจมตีบริการสารสนเทศของผู้อื่น ด้วยวิธีการโจมตีแบบ DNS Amplification Attack แสดงตามรูปที่ 2 ซึ่งเป็นการโจมตีด้วยวิธีการส่ง DNS Request ไปยังเครื่อง Open Resolver หลาย ๆ เครื่องพร้อม ๆ กัน โดยปลอมแปลง IP Address ต้นทางใน DNS Request ให้เป็น IP Address ของเครื่องเป้าหมาย ทำให้ DNS Response จาก Open Resolver นั้นถูกตอบกลับไปยังเครื่องเป้าหมาย โดยปกติ DNS Request ประเภท Recursive Query จะมีขนาดเล็ก ในขณะที่ DNS Response จะมีขนาดใหญ่กว่ามาก จุดนี้จึงเป็นช่องทางให้ผู้ไม่ประสงค์ดีใช้ Open Resolver ในการโจมตีผู้อื่นในรูปแบบ DDoS ยิ่งมีการส่ง DNS Request ไปยัง Open Resolver เป็นจำนวนมากเท่าใด เครื่องเป้าหมายก็จะได้รับ DNS Response มากขึ้นเป็นทวีคูณ จนกระทั่งถึงจุดที่ทำให้ช่องสัญญาณของเครือข่ายอินเทอร์เน็ตของเครื่องเป้าหมายเต็มและไม่สามารถสื่อสารข้อมูลได้อีกต่อไป หรือแม้กระทั่งส่งผลให้เครื่องเป้าหมายเกิดความขัดข้อง ส่งผลให้ไม่สามารถให้บริการตามปกติได้



รูปที่ 2 รูปแบบการโจมตีด้วยเทคนิค DNS Amplification

ตารางที่ 17 สถิติประเภท Open DNS Resolver ที่มากที่สุด 10 อันดับแรก นับตามจำนวน IP Address ที่ไม่ซ้ำ และจำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนหมายเลขไอพีที่ไม่ซ้ำ (Unique IP)	สัดส่วน (ร้อยละ)
1	True Internet Co., Ltd.	17552 45805 55554 7470 9287	107,464	75.02
2	TOT (Public) Co., Ltd.	23969 38040 56120 9737	16,413	11.46
3	Triple T Broadband (Public) Co., Ltd.	45758	11,251	7.85
4	CS Loxinfo (Public) Co., Ltd.	45537 4750 7568 9891	966	0.67
5	BB Broadband Co., Ltd.	38794 56085	946	0.66
6	CAT Telecom (Public) Co., Ltd.	9931	940	0.66
7	JasTel Network Co., Ltd.	45629 55423	853	0.6
8	Ministry of Education	23974	752	0.52
9	Jasmine Internet Co., Ltd.	7616	364	0.25
10	Internet Solution & Service Provider Co., Ltd.	24299 7654	356	0.25

จากรายงานภัยคุกคามด้านสารสนเทศประเภท Open DNS Resolver ที่มี IP Address ที่ไม่ซ้ำกัน ตามตารางที่ 17 พบว่ามี IP Address ที่เป็น Open DNS Resolver จำนวนทั้งสิ้น 143,255 หมายเลข ส่วนใหญ่อยู่ในความดูแลของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ขนาดใหญ่ เช่น ทรู (True) ทีโอที (TOT) และทริปเปิลที (Triple T) ซึ่งมีสัดส่วนรวมกันมากถึงร้อยละ 96 และพบว่ามีหน่วยงานของรัฐเพียงหน่วยงานเดียวได้แก่กระทรวงศึกษาธิการที่อยู่ใน 10 ลำดับแรก จากการวิเคราะห์ของไทยเซิร์ตคาดว่าเนื่องจากกระทรวงศึกษาธิการเป็นหน่วยงานรัฐที่มีขนาดใหญ่และมีเครือข่ายคอมพิวเตอร์ที่เชื่อมโยงหน่วยงานภายใต้สังกัดและสถานศึกษาทั่วประเทศ ดังนั้นจึงมีสัดส่วนรายงานภัยคุกคามด้านสารสนเทศประเภท Open DNS Resolver จำนวนมากตามปริมาณการใช้งานบริการสารสนเทศ ซึ่งในส่วนนี้ไทยเซิร์ตได้มีการประสานงานกับทั้งผู้บริหารและผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของกระทรวงศึกษาธิการอย่างใกล้ชิดเพื่อให้ความช่วยเหลือในการตรวจสอบต้นเหตุและหาแนวทางในการลดปัญหาดังกล่าว

9.) โอเพ่น พร็อกซี่ เซิร์ฟเวอร์ (Open Proxy Server)

ลักษณะภัยคุกคามด้านสารสนเทศประเภท Open Proxy Server เป็นการเปิดให้บริการ HTTP Proxy ให้แก่บุคคลทั่วไปโดยไม่มีการควบคุม จนอาจถูกใช้เป็นเครื่องมือของผู้ไม่ประสงค์ดีในการกระทำความผิด โดยอาศัยช่องโหว่จากการตั้งค่าของ HTTP Proxy ที่ไม่เหมาะสม หรือบางครั้งอาจเกิดจากการที่เครื่อง ๆ นั้น ถูกเจาะระบบโดยผู้ไม่ประสงค์ดีก่อนหน้าที่จะถูกตั้งค่าให้เป็น HTTP Proxy และกลายเป็นช่องทางในการกระทำความผิดในภายหลัง

ตารางที่ 18 สถิติประเภท Open Proxy Server ที่มากที่สุด 10 อันดับแรก นับตามจำนวน IP Address ที่ไม่ซ้ำ และจำแนกตามผู้ให้บริการเครือข่าย

ลำดับ	ผู้ให้บริการเครือข่าย	AS Number	จำนวนหมายเลขไอพีทีไม่ซ้ำ (Unique IP)	สัดส่วน (ร้อยละ)
1	Triple T Broadband (Public) Co., Ltd.	45758	2,852	79.31
2	TOT (Public) Co., Ltd.	23969 9737	448	12.46
3	True Internet Co., Ltd.	17552 7470 9287	193	5.37
4	Super Broadband Network Co., Ltd.	45458	21	0.58
5	Ministry of Education	23974	19	0.53
6	CAT Telecom (Public) Co., Ltd.	9931	12	0.33
7	UniNet	4621	9	0.25
8	BB Broadband Co., Ltd.	38794	4	0.11
9	JasTel Network Co., Ltd.	45629	4	0.11
10	CS Loxinfo (Public) Co., Ltd.	4750 9891	3	0.08

จากรายงานประเภท Open Proxy Server ที่มี IP Address ไม่ซ้ำกัน ตามตารางที่ 18 พบว่ามีจำนวน IP Address ที่ได้รับรายงานทั้งสิ้น 3,596 หมายเลข ส่วนใหญ่อยู่ในความดูแลของผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ขนาดใหญ่ เช่น ทริปเปิลที (Triple T) ทีโอที (TOT) และทรู (True) ซึ่งมีสัดส่วนรวมกันมากถึงเกือบร้อยละ 98 และพบว่ามีหน่วยงานของรัฐเพียงหน่วยงานเดียวที่อยู่ใน 10 ลำดับแรก คือ กระทรวงศึกษาธิการ เป็นที่น่าสังเกตว่าภัยคุกคามประเภท Open Proxy เป็นภัยคุกคามที่เกิดขึ้นกับเครื่องแม่ข่าย เมื่อพิจารณาจากข้อมูลข้างต้น พบประเด็นที่น่าสนใจ คือ IP Address ได้รับรายงานส่วนใหญ่อยู่ ในเครือข่ายของผู้ให้บริการบรอดแบนด์ ซึ่งส่วนใหญ่น่าจะเป็นเครื่องคอมพิวเตอร์ของผู้ใช้งานและมีลักษณะการเชื่อมต่อผ่านอุปกรณ์เครือข่าย Boardband Router แทนที่จะเป็นเครื่องแม่ข่ายที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตโดยตรง การตรวจสอบถึงสาเหตุของแหล่งที่มาของภัยคุกคามประเภทนี้ จำเป็นต้องได้รับข้อมูลจากผู้ให้บริการเครือข่ายเพื่อวิเคราะห์หาข้อสรุปต่อไป

4.3.2 สถิติ Incident ที่ได้รับแจ้งโดยตรง

ไทยเซิร์ตมีช่องทางการรับแจ้งสถานการณ์ด้านความมั่นคงปลอดภัย ทางอีเมลและทางโทรศัพท์ โดยจัดเก็บข้อมูลลงในระบบติดตามและบริหารจัดการชื่อ รีเควส แทร็กเกอร์ (Request Tracker) ซึ่งจากข้อมูลรับแจ้งเหตุภัยคุกคามที่เกิดขึ้นในประเทศไทยสามารถสรุปและจัดทำเป็นสถิติ โดยจำแนกประเภทของเหตุออกเป็น 9 ประเภท ตามที่ได้กำหนดโดย

อีซีเซิร์ต (eCSIRT/The European Computer Security Incident Response Team)[27] ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปโดยมีรายละเอียดตามตารางที่ 19

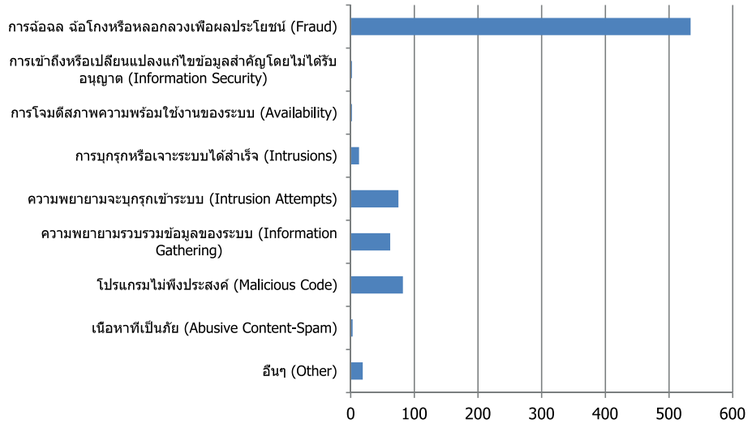
ตารางที่ 19 ประเภทของ Incident

ลำดับ	ประเภท	คำอธิบาย
1	เนื้อหาที่เป็นภัย (Abusive Content)	การใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือ เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (Spam)
2	โปรแกรมไม่พึงประสงค์ (Malicious Code)	โปรแกรมหรือชุดคำสั่งที่ถูกพัฒนาขึ้นด้วยความประสงค์ร้าย (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์นี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ
3	ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกียวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ทีมีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
4	ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusions Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆของระบบ นี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
5	การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	การบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
6	การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	การโจมตีสภาพความพร้อมใช้งานของระบบเพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ อาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่นการโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
8	การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	การฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
9	อื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	ภัยประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุก คามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทนี้ใหม่

27 http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html#HEAD6

ตารางที่ 20 ข้อมูล Incident ที่ไทยเซิร์ตได้รับแจ้งโดยตรงในปี 2555 จำแนกตามประเภท

ประเภท	จำนวน	สัดส่วน
เนื้อหาที่เป็นภัย (Abusive Content-Spam)	3	0.37%
โปรแกรมไม่พึงประสงค์ (Malicious Code)	82	10.35%
ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	62	7.82%
ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	75	9.46%
การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	13	1.64%
การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	2	0.25%
การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	2	0.25%
การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	534	67.42%
อื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	19	2.39%
รวม	792	100%

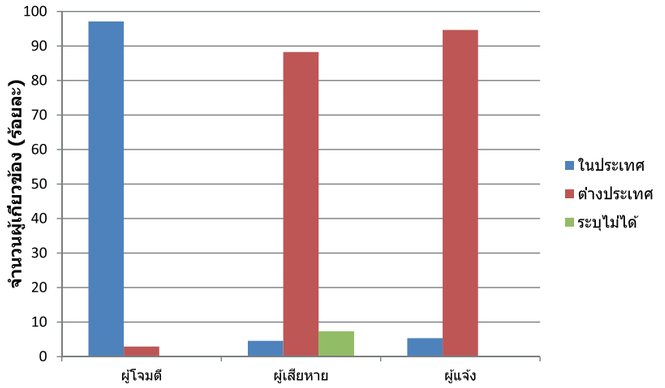


กราฟที่ 13 สถิติ Incident ที่ไทยเซิร์ตได้รับแจ้งโดยตรงในปี 2555

จากรายงานการแจ้งสถานการณ์ภัยคุกคามด้านสารสนเทศ ทางช่องทางอีเมลและโทรศัพท์ ตามตารางที่ 20 พบว่ารายงานที่ได้รับ มีจำนวนทั้งสิ้น 792 รายการ โดยภัยคุกคามด้านสารสนเทศประเภท Fraud ถูกแจ้งมากที่สุดเป็นจำนวนถึง 534 รายการ คิดเป็นร้อยละ 67.42 ของข้อมูลการรับแจ้งเหตุภัยคุกคามด้านสารสนเทศทั้งหมด รองลงมาเป็นประเภท Malicious Code คิดเป็นร้อยละ 10.35 ลำดับถัดไปเป็นประเภทความพยายามบุกรุกเข้าระบบ และประเภทความพยายามรวบรวมข้อมูลของระบบ รวมกันคิดเป็นร้อยละ 17.30

ตารางที่ 21 ข้อมูลการรับแจ้ง Incident จำแนกตามผู้เกี่ยวข้องและแหล่งที่มาของผู้เกี่ยวข้อง

	ผู้แจ้ง	สัดส่วน (ร้อยละ)	ผู้เสียหาย	สัดส่วน (ร้อยละ)	ผู้โจมตี	สัดส่วน (ร้อยละ)
ในประเทศ	51	5.33	40	4.57	761	97.1
ต่างประเทศ	741	94.66	669	88.26	31	2.9
ระบุไม่ได้	0	0	83	7.16	0	0

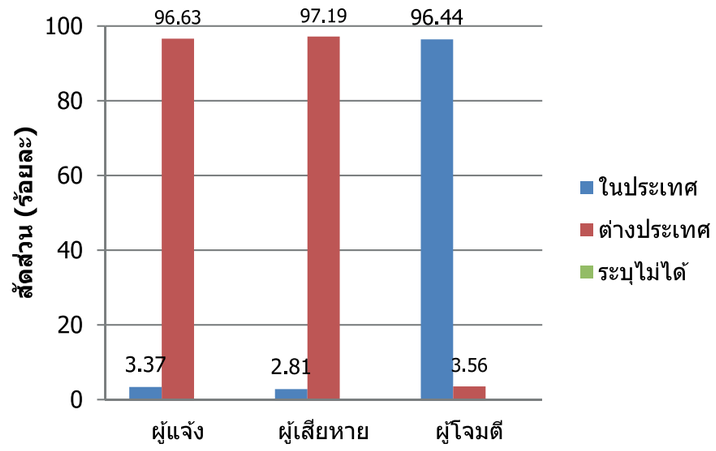


กราฟที่ 14 ข้อมูลการรับแจ้ง Incident จำแนกตามผู้เกี่ยวข้องและแหล่งที่มาของการแจ้ง หน่วยเป็นร้อยละ

ไทยเซิร์ตได้จำแนกลักษณะของผู้เกี่ยวข้องของเหตุออกเป็น 3 ประเภทคือ ผู้แจ้ง (Submitter) ผู้โจมตี (Attacker) และผู้เสียหาย (Victim) และยังแบ่งลักษณะของผู้เกี่ยวข้องตามแหล่งที่มาของการแจ้งได้อีก 3 ลักษณะ คือ ภายในประเทศ (Domestic) ภายนอกประเทศ (Foreign) และไม่ทราบแหล่งที่ตั้ง (Unknown) โดยจากข้อมูลตามตารางที่ 21 และกราฟที่ 14 แสดงให้เห็นว่า ผู้แจ้งส่วนใหญ่มาจากต่างประเทศมากกว่าร้อยละ 90 ซึ่งสอดคล้องกับสัดส่วนของผู้เสียหายในต่างประเทศที่ใกล้เคียงร้อยละ 90 เช่นกัน ส่วนกรณีที่ไม่สามารถระบุประเทศ (Unknown) ได้นั้น เนื่องจากผู้แจ้งไม่ได้ให้ข้อมูลเพียงพอต่อการวิเคราะห์ว่าผู้เสียหายหรือผู้โจมตีมาจากประเทศใด

ตารางที่ 22 ข้อมูลการรับแจ้งประเภทฉ้อโกง (Fraud) จำแนกตามผู้เกี่ยวข้องและแหล่งที่มาของการแจ้ง

	ผู้แจ้ง	สัดส่วน (ร้อยละ)	ผู้เสียหาย	สัดส่วน (ร้อยละ)	ผู้โจมตี	สัดส่วน (ร้อยละ)
ในประเทศ	18	3.37	15	2.81	515	96.44
ต่างประเทศ	516	96.63	519	97.19	19	3.56
ระบุไม่ได้	0	0	0	0	0	0

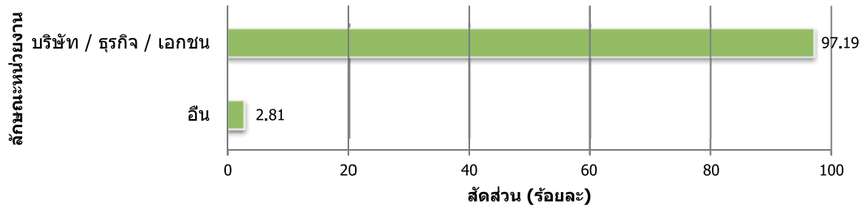


กราฟที่ 15 ข้อมูลผู้เกี่ยวข้องกับเหตุประเภทฉ้อโกง (Fraud) จำแนกตามผู้เกี่ยวข้องและแหล่งที่มาของการแจ้ง

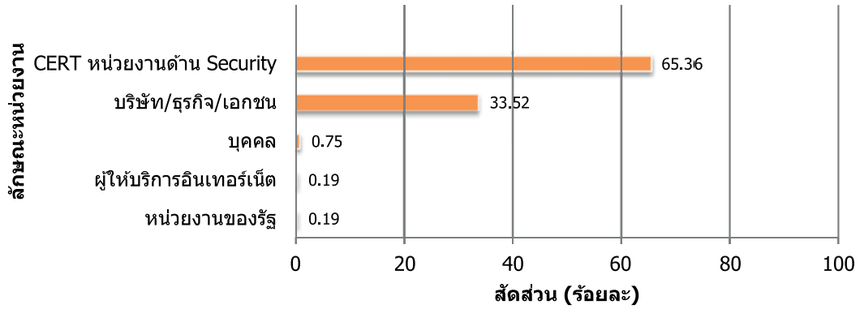
ตารางที่ 23 ข้อมูลการรับแจ้งประเภทฉ้อโกง (Fraud) จำแนกตามผู้เกี่ยวข้องและประเภทหน่วยงาน

	ผู้แจ้ง	สัดส่วน (ร้อยละ)	ผู้เสียหาย	สัดส่วน (ร้อยละ)	ผู้โจมตี	สัดส่วน (ร้อยละ)
บุคคล	4	0.75	0	0	0	0
เซิร์ท (CERT)/หน่วยงานด้านความมั่นคงปลอดภัยคอมพิวเตอร์	349	65.36	0	0	0	0
ผู้ให้บริการอินเทอร์เน็ต	1	0.19	0	0	0	0
บริษัท/ธุรกิจ/เอกชน	179	33.52	519	97.19	345	64.61
สถาบันการศึกษา	0	0	0	0	45	8.43
หน่วยงานของรัฐ	1	0.19	0	0	85	15.92
อื่นๆ	0	0	15	2.81	59	11.05

จากข้อมูลการรับแจ้งประเภท Fraud จำแนกตามลักษณะผู้เกี่ยวข้องกับเหตุดังที่แสดงไว้ในตารางที่ 23 ผู้โจมตี (Attacker) หมายถึงผู้ที่มีส่วนในการเผยแพร่เว็บหลอกลวง อาจเป็นเจ้าของเว็บไซต์ ที่ตั้งใจสร้างหน้า Phishing ขึ้นเอง หรือเว็บไซต์ที่ถูกผู้อื่นเจาะระบบเข้ามาสร้างหน้า Phishing ไว้ก็ได้ ทั้งนี้สังเกตได้ว่าเราสามารถระบุแหล่งที่มาของข้อมูลในกรณีที่เป็นภัยคุกคามด้านสารสนเทศประเภท Fraud ได้ทั้งหมด โดยข้อมูลในตารางที่ 23 ได้จำแนกลักษณะของผู้เกี่ยวข้องได้ออกเป็น 7 ประเภท ได้แก่ บุคคลทั่วไป เซิร์ต (CERT)/หน่วยงานด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ผู้ให้บริการอินเทอร์เน็ต บริษัท/ธุรกิจ/เอกชน สถาบันการศึกษา หน่วยงานของรัฐ, และอื่น ๆ



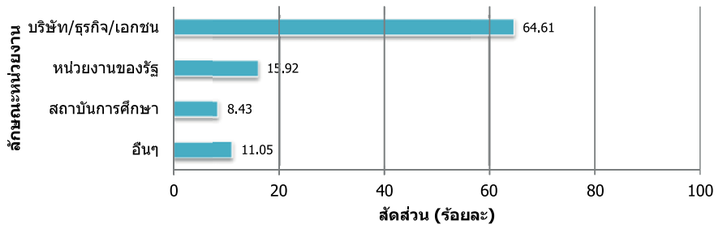
กราฟที่ 16 ข้อมูลผู้เสียหายที่เกิดจากประเภทฉ้อโกง (Fraud)



กราฟที่ 17 ข้อมูลผู้แจ้ง Incident ในประเภทฉ้อโกง (Fraud)

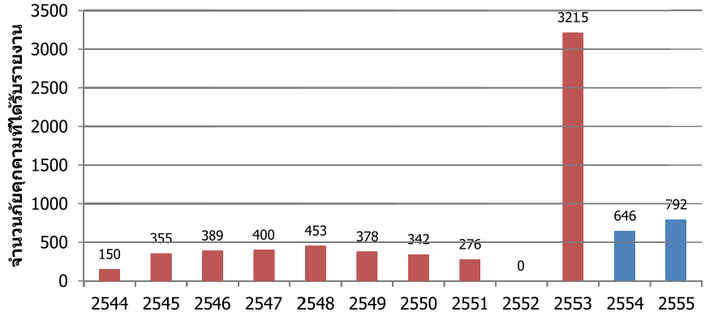
กราฟที่ 16 แสดงให้เห็นว่า จำนวนผู้เสียหายจากการหลอกลวง ส่วนใหญ่อยู่ในกลุ่มประเภทบริษัท/ธุรกิจ/เอกชน คิดเป็นสัดส่วนมากกว่าร้อยละ 90 ของเหตุภัยคุกคามประเภท Fraud ทั้งหมดที่ได้รับแจ้ง นอกนั้นเป็นกรณีอื่น ๆ ซึ่งยังไม่สามารถตรวจสอบยืนยันได้ว่าผู้เสียหายคือใคร เนื่องจากในขณะที่เข้าตรวจสอบนั้น หน้า Phishing ได้ถูกเปลี่ยนแปลงหรือแก้ไขแล้ว และไม่พบข้อมูลเพียงพอที่จะระบุได้ว่า ใครคือเป้าหมายของการโจมตี

จากข้อมูลผู้แจ้งประเภท Fraud ตามกราฟที่ 17 พบว่ามีจำนวนผู้แจ้งกว่าร้อยละ 65 ที่มาจากองค์กรประเภทเซิร์ต (CERT) หรือหน่วยงานด้านความมั่นคงปลอดภัยระบบคอมพิวเตอร์จากทุกภูมิภาคของโลก รองลงมาคือกลุ่มประเภทองค์กรธุรกิจภาคเอกชน เช่น ธนาคาร หรือสถาบันการเงิน ที่มีสัดส่วนร้อยละ 33 ซึ่งทั้งหมดเป็นหน่วยงานหรือองค์กรที่มีบริการออนไลน์ให้กับลูกค้า



กราฟที่ 18 ข้อมูลผู้โจมตีที่เกิดกับประเภทฉ้อโกง (Fraud)

จากข้อมูลผู้โจมตีที่เกี่ยวข้องกับเหตุภัยคุกคามด้านสารสนเทศประเภท Fraud ตามกราฟที่ 18 พบว่าผู้โจมตีส่วนใหญ่อยู่ในกลุ่มประเภทบริษัท/ธุรกิจ/เอกชน มีสัดส่วนประมาณร้อยละ 64 รองลงมาคือหน่วยงานของรัฐและสถาบันการศึกษา มีสัดส่วนรวมกันประมาณร้อยละ 24 โดยจากข้อมูลเพิ่มเติมที่พบในระหว่างการวิเคราะห์และดำเนินการแก้ไขปัญหากับผู้เกี่ยวข้อง พบว่าเว็บไซต์ที่พบหน้า Phishing ทั้งหมดที่ได้รับรายงานไม่ได้เกิดจากหน่วยงานหรือเจ้าของเครื่องแม่ข่ายที่พบหน้า Phishing จงใจสร้างและเผยแพร่หน้า Phishing ในเว็บไซต์ของตนเอง แต่เป็นลักษณะที่หน่วยงานเหล่านั้นตกเป็นเหยื่อของผู้ไม่ประสงค์ดีที่เจาะระบบเข้ามาเพื่อสร้างหน้า Phishing และผู้ดูแลระบบของหน่วยงานเหล่านั้นไม่ทราบมาก่อน ซึ่งแสดงให้เห็นว่าเว็บไซต์ของประเภทบริษัท/ธุรกิจ/เอกชนในประเทศไทยจำนวนไม่น้อย ยังขาดการบำรุงรักษาและการบริหารจัดการรักษาความมั่นคงปลอดภัยที่ดีกับระบบเว็บไซต์ของตน

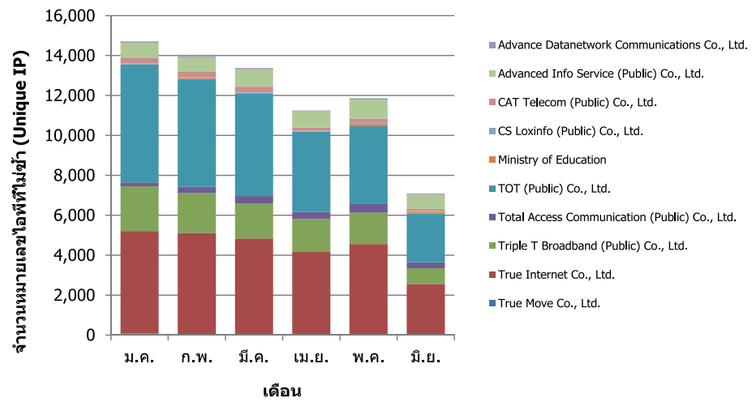


กราฟที่ 19 ข้อมูลจำนวนการรับแจ้ง Incident ในปี 2555 เทียบกับปีก่อนหน้า

ในกราฟที่ 19 ในส่วนกราฟแท่งสีแดงแสดงข้อมูลจำนวนการรับแจ้ง Incident ของไทยเซิร์ตตั้งแต่ปี 2544 – 2553 ซึ่งเป็นช่วงที่ไทยเซิร์ตดำเนินงานอยู่ภายใต้ศูนย์เทคโนโลยีและอิเล็กทรอนิกส์แห่งชาติโดยรวบรวมข้อมูลจากรายงานประจำปีของเอพีเซิร์ต (APCERT/The Asia Pacific Computer Emergency Response Team) ซึ่งเป็นเครือข่ายของหน่วยงานประเภทเซิร์ตในภูมิภาคเอเชียและแปซิฟิก แต่ไม่ได้แสดงข้อมูลของปี 2552 เนื่องจากไทยเซิร์ตไม่ได้รายงานผลการดำเนินงานให้กับ APCERT

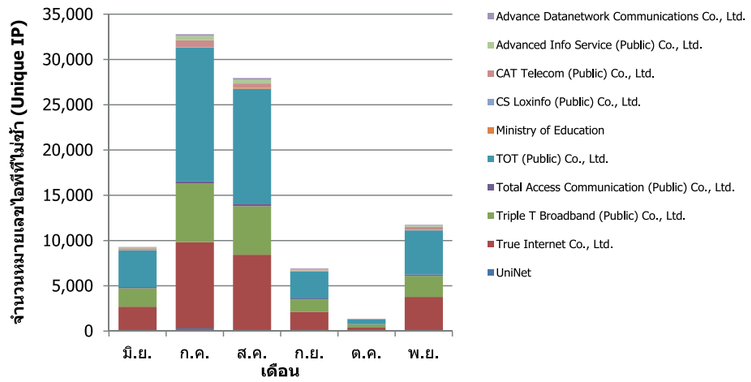
ส่วนแท่งสีน้ำเงินแสดงข้อมูลจำนวนการรับแจ้ง Incident ปี 2555 ซึ่งเป็นช่วงเวลาที่ไทยเซิร์ตได้ดำเนินงานภายใต้ สพธอ. โดยมีจำนวนที่ได้รับแจ้ง 792 รายการ นั้นสูงกว่าจำนวนที่ได้รับแจ้งในปี 2556 (646 รายการ) อยู่ประมาณ 22%

นอกเหนือจากการรับแจ้งผ่านช่องทางระบบอัตโนมัติและทางอีเมลข้างต้น ไทยเซิร์ตยังได้ร่วมมือกับ บริษัทไมโครซอฟต์ ในการเป็นศูนย์กลางการประสานงานกับหน่วยงานต่าง ๆ ในประเทศเพื่อจัดการกับ Malware ชื่อ รูสต๊อค (Rustock) และ ซูส (Zeus) โดยสามารถสรุปสถิติที่น่าสนใจได้ ดังต่อไปนี้



กราฟที่ 20 จำนวน IP Address ที่ไม่ซ้ำกันที่ติดมัลแวร์ รูสต๊อค (Rustock) คิดเป็นรายเดือน และจำแนกตามผู้ให้บริการเครือข่าย

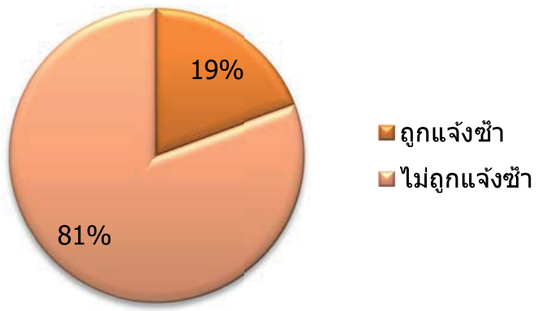
กราฟที่ 20 แสดงข้อมูลของจำนวน IP Address ที่ไม่ซ้ำกันในประเทศไทย ที่บริษัทไมโครซอฟต์ ตรวจพบ Rustock ตั้งแต่วันที่ 13 มกราคม - 20 มิถุนายน 2555 พบว่ามีจำนวน IP Address ที่ติด Malware ชนิดนี้ถึง 71,719 หมายเลข ซึ่งหลังจากที่ได้รับรายงานนี้ไทยเซิร์ตได้วิเคราะห์และประสานงานกับผู้ให้บริการเครือข่ายแต่ละรายเพื่อดำเนินการแก้ไข พบว่าปัญหาจาก Rustock มีแนวโน้มลดลงเป็นลำดับจากในช่วงเดือนมกราคม 2555 ที่มีจำนวน IP Address ที่ได้รับแจ้งประมาณ 4,500 หมายเลข/สัปดาห์ ลดเหลือประมาณน้อยกว่า 3,000 หมายเลข/สัปดาห์ ซึ่งโดยจำนวนที่ลดลงนี้เป็น IP Address ในเครือข่ายของ ทีโอที (TOT) และ ทรู (True)



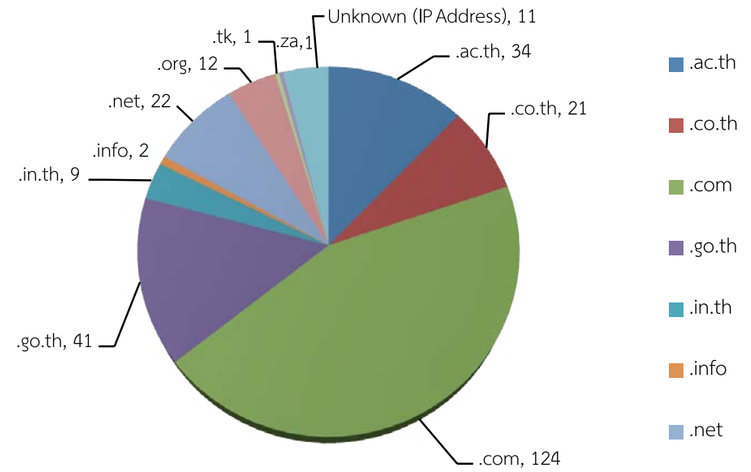
กราฟที่ 21 จำนวนหมายเลขไอพีที่ไม่ซ้ำที่ติดมัลแวร์ Zeus จำแนกตามผู้ให้บริการเครือข่ายเป็นรายเดือน

ต่อมาในเดือนมิถุนายน 2555 บริษัทไมโครซอฟต์ ได้ประกาศยุติการส่งข้อมูล IP Address ที่ติด Rustock ทั้งหมด หลังจากที่สามารถเข้ายึดเครื่องควบคุมและสั่งการ (C&C) ของ Zeus ได้สำเร็จ จนพบว่ามีจำนวนเครื่องที่ติด Zeus ทั่วโลกเป็นจำนวนมากกว่า Rustock อยู่หลายเท่าตัว จึงได้ส่งข้อมูลของ IP Address ที่ติด Zeus ให้กับหน่วยงานในเครือข่ายความร่วมมือแทน โดยในครั้งนี้ไทยเซิร์ตได้รับรายงานจำนวน IP Address จากบริษัทไมโครซอฟต์ ตั้งแต่เดือนมิถุนายนถึงพฤศจิกายน พ.ศ. 2555 แสดงได้ตามกราฟที่ 21

จากกราฟที่ 21 พบว่ามีจำนวน IP Address ที่ได้รับแจ้งทั้งหมด 88,708 หมายเลข โดยในเดือนกรกฎาคมมีสูงถึง 32,217 หมายเลข และเมื่อไทยเซิร์ตได้วิเคราะห์และประสานงานกับผู้ให้บริการเครือข่ายแต่ละรายตามช่องทางที่ไทยเซิร์ตเคยใช้ในกรณี Rustock เพื่อดำเนินการแก้ไข เห็นชัดว่ารายการที่ได้รับแจ้งมีแนวโน้มลดลงตามลำดับ แสดงให้เห็นถึงความร่วมมือของผู้ให้บริการเครือข่ายทั้งหลาย ในการให้ประสานงานแก้ไขปัญหาภัยคุกคามด้านสารสนเทศประเภทนี้



กราฟที่ 22 สัดส่วนร้อยละของ IP Address ที่ถูกแจ้งซ้ำและ IP Address ที่ไม่ถูกแจ้งซ้ำในกรณีภัยคุกคามแบบ Phishing



กราฟที่ 23 สัดส่วนร้อยละของ IP Address ที่ได้ถูกแจ้งซ้ำในกรณีภัยคุกคามแบบ Phishing โดยจำแนกตามโดเมนเนม

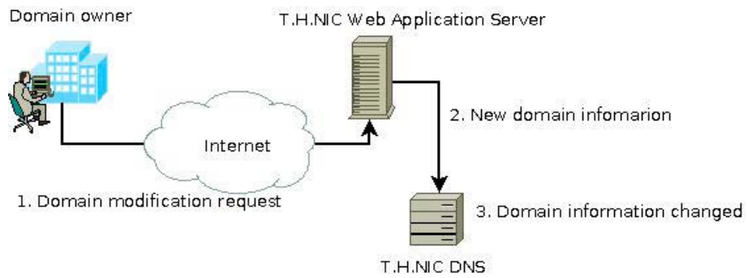
ทั้งนี้ ยังได้วิเคราะห์ภัยคุกคามแบบ Phishing ที่ได้รับแจ้งโดยตรงมาที่ไทยเซิร์ต สามารถแสดงได้ตามกราฟที่ 22 และ 23 ซึ่งจะเห็นว่า IP Address ที่ถูกแจ้งซ้ำในกรณีภัยคุกคามแบบ Phishing มีสัดส่วนถึงร้อยละ 19 และเมื่อจำแนกตามโดนเมนเนมของ IP Address ที่ถูกแจ้งซ้ำนี้ พบว่า โดเมนเนมของหน่วยงานประเภทที่ถูกแจ้งซ้ำมากที่สุด คือ ประเภทที่จดทะเบียนเป็นภาคธุรกิจ (.com) คิดเป็นร้อยละ 44.6 (124 หมายเลข) รองลงไปเป็นหน่วยงานประเภทสถาบันการศึกษา (.ac.th) และหน่วยงานภาครัฐ (.go.th) รวมกันเป็นร้อยละ 26.9 (75 หมายเลข) ซึ่งข้อมูลในส่วนนี้สามารถใช้เป็นตัวชี้วัดถึงประสิทธิภาพในการแก้ไขปัญหาของหน่วยงานเพื่อแก้ไขช่องโหว่ของเว็บไซต์ตนเองหลังได้รับแจ้งปัญหา Phishing

4.4 สถานการณ์ด้านความมั่นคงปลอดภัย (Incident) ที่เป็นกรณีศึกษาที่ไทยเซิร์ตเข้าไปดำเนินการ

ในปี 2555 ไทยเซิร์ตดำเนินการจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัย (Incident) และมีกรณีศึกษาที่น่าสนใจหลายกรณี เช่น การบุกรุกระบบจัดการโดเมนของ ที เอช นิค (T.H. NIC) , โปรแกรมไม่พึงประสงค์ดีเอ็นเอส เชนเจอร์ (DNS Changer), การพบเครื่อง C&C ของ Malware ตระกูลเฟลม (Flame), การขโมยบัญชีผู้ใช้งานอีเมล และปัญหา Phishing ในผู้ให้บริการเว็บโฮสติ้ง (Web Hosting) ของไทย เป็นต้น

4.4.1 การบุกรุกเข้าระบบจัดการโดเมนเนมของ T.H. NIC

ไทยเซิร์ต ได้รับแจ้งจากหน่วยงานด้าน Cybersecurity ในต่างประเทศ ในวันที่ 30 มิถุนายน 2555 ว่ามีการเปลี่ยนแปลงข้อมูล IP Address ของบริษัทต่างชาติสาขาประจำประเทศไทย ในลักษณะที่น่าสงสัยว่าจะเกิดจากผู้ไม่ประสงค์ดี ซึ่งเป็นรูปแบบการโจมตีแบบการโจรกรรมโดมเมนเนม (Domain Hijacking) แต่ยังไม่ทราบว่าเกิดขึ้นที่จุดใด เมื่อตรวจสอบไปยัง T.H.NIC ซึ่งเป็นผู้ให้บริการจดทะเบียนโดเมนเนม ระดับประเทศของไทย (ccTLD/ Country Code - Top Level Domain) ไทยเซิร์ตจึงได้ทราบว่า ระบบฐานข้อมูลผู้จดทะเบียนโดเมนเนมของ T.H.NIC ถูกผู้ไม่ประสงค์ดีลักลอบเข้ามาเปลี่ยนแปลงข้อมูล และมีโดเมนเนมได้รับผลกระทบจำนวนหนึ่งโดยที่เจ้าของโดเมนเนม ยังไม่ทราบว่าเกิดการเปลี่ยนแปลงและถูกโจรกรรมโดเมนเนมแล้ว



รูปที่ 3 โครงสร้างการทำงานของระบบแก้ไขข้อมูลโดเมนเนมของผู้ใช้บริการของที เอช นิค

หลังจากการวิเคราะห์รายงานที่ได้รับแจ้งและดำเนินการติดต่อกับ T.H.NIC เพื่อให้คำแนะนำและความช่วยเหลือ ตั้งแต่วันที่ 31 มิถุนายน จนถึงวันที่ 2 กรกฎาคม 2555 ไทยเซิร์ตได้ตรวจพบว่า ผู้ไม่ประสงค์ดีใช้ IP Address ของประเทศแถบยุโรปตะวันออก เข้าโจมตีช่องโหว่ของระบบจัดการข้อมูล (CMS) ที่ถูกใช้อยู่ในหน้าเผยแพร่ข้อมูลของ T.H.NIC ทำให้สามารถเข้าถึงระบบฐานข้อมูลหลัก รวมถึงคำสั่งในโปรแกรม(Source code) ของระบบแก้ไขข้อมูลผู้จดทะเบียนโดเมนเนมได้ และเนื่องจากระบบทั้งหมดใช้เครื่องแม่ข่ายและฐานข้อมูลร่วมกัน ข้อมูลบันทึก (Log) ของเครื่องแม่ข่ายที่ถูกโจมตียังแสดงให้เห็นว่า ผู้ไม่ประสงค์ดีได้รหัสผ่านของผู้จดทะเบียนโดเมนเนมในระบบไปทั้งหมด รวมถึงรหัสผ่านของผู้ดูแลระบบฐานข้อมูล ส่งผลให้ผู้ไม่ประสงค์ดีสามารถเข้ามาเปลี่ยนแปลงข้อมูลทั้งหมดของผู้จดทะเบียนโดเมนเนมกับ T.H.NIC ได้

ด้วยข้อมูลทั้งหมดที่ได้รับ ทำให้ไทยเซิร์ตสามารถช่วยวิเคราะห์ต้นเหตุของปัญหาในระบบจัดการโดเมนเนมของ T.H.NIC และได้แจ้งข้อเสนอแนะในการปรับปรุงระบบนี้ให้กับ T.H.NIC ทราบ เพื่อให้ดำเนินการปรับปรุงต่อไป

จากกรณีนี้พบว่า ความสามารถในการวิเคราะห์หลักฐานจากระบบที่ถูกบุกรุกได้สำเร็จแล้วเป็นสิ่งที่ไทยเซิร์ตจำเป็นต้องพัฒนาให้สูงขึ้นให้เทียบเท่ากับระดับสากล โดยเฉพาะกับสถานการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นกับระบบสารสนเทศของหน่วยงานที่เป็นโครงสร้างพื้นฐานของระบบเครือข่ายอินเทอร์เน็ตของประเทศ รวมถึงการพัฒนาให้บุคลากรมีความสามารถในด้าน Digital Forensics ที่มิได้มีความสำคัญเฉพาะในการดำเนินงานของหน่วยงานตามที่ถูกบังคับใช้กฎหมาย แต่ยังสามารถใช้เป็นประโยชน์ในการวิเคราะห์ช่องโหว่ของระบบสารสนเทศที่ถูกบุกรุก เพื่อให้สามารถวางแผนการป้องกันได้อย่างมีประสิทธิภาพและทันท่วงที

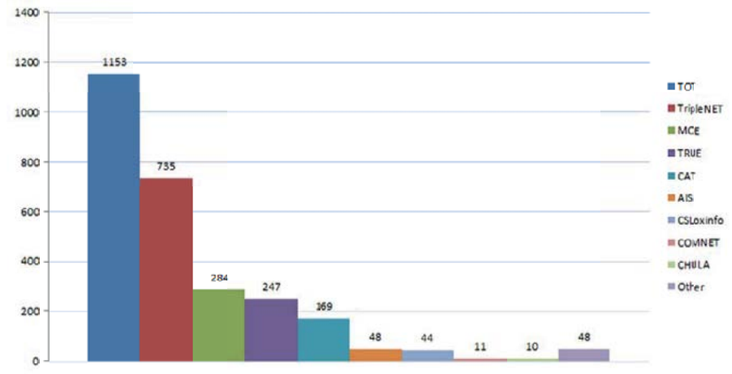
4.4.2 การระบาดของมัลแวร์ดีเอ็นเอส เชนเจอร์ (DNS Changer Malware)

DNS Changer Malware ถูกค้นพบครั้งแรกเมื่อปี 2550 และสามารถทำงานได้ทั้งบนระบบปฏิบัติการวินโดวส์ (Windows) และ แมค โอเอสเท็น (Mac OS X) โดยเครื่องที่ติด DNS Changer Malware จะถูกเปลี่ยนค่า DNS ในเครื่องตนเองให้เป็น IP Address ของ DNS Server ที่ถูกตั้งขึ้นโดยผู้ไม่ประสงค์ดี และเมื่อผู้ใช้พยายามเข้าถึงเว็บไซต์จากเครื่องที่ติด DNS Changer Malware นี้ เขาจะถูกนำพาไปยังเครื่องแม่ข่ายปลอมที่ผู้ไม่ประสงค์ดีเตรียมไว้ เพื่อใช้ในการขโมยข้อมูลสำคัญ หรือเผยแพร่ Malware ตัวอื่น ๆ โดยรายงานจากหน่วยงานเอฟบีไอ (FBI) ของประเทศสหรัฐอเมริกาพบว่ามีเครื่องคอมพิวเตอร์ที่ติด DNS Changer Malware นี้เป็นจำนวนมากกว่า 4 ล้านเครื่องทั่วโลก[28]

28 http://www.fbi.gov/news/stories/2011/november/malware_110911/DNS-changer-malware.pdf

ในเดือนพฤศจิกายน 2554 เอฟบีไอได้จับกุมผู้พัฒนาและเผยแพร่ DNS Changer Malware พร้อมทั้งยึดเครื่องแม่ข่าย DNS ที่เกี่ยวข้องมาใช้ในการวิเคราะห์และสอบสวน ซึ่งแม้ว่าเอฟบีไอจะพยายามปิดบริการเครื่องแม่ข่ายดังกล่าวอยู่หลายครั้ง แต่ไม่สามารถทำได้เนื่องจากจะทำให้เครื่องคอมพิวเตอร์ที่ติด DNS Changer Malware อยู่เป็นจำนวนมากทั่วโลก ไม่สามารถใช้งานเครือข่ายอินเทอร์เน็ตได้ เนื่องจากเครื่องคอมพิวเตอร์เหล่านั้นต้องใช้ DNS ของ DNS Changer ในการทำงาน โดยจากการตรวจสอบในเดือนมีนาคม 2555 พบว่า ยังมีเครื่องคอมพิวเตอร์ที่ติด Malware นี้อยู่ประมาณ 450,000 เครื่องทั่วโลก และในจำนวนนี้มีคอมพิวเตอร์ที่ใช้ในหน่วยงานสำคัญของรัฐบาลอยู่ด้วย

จนกระทั่งวันที่ 23 เมษายน 2555 เอฟบีไอได้แจ้ง IP Address ของผู้ที่ติด DNS Changer Malware ให้กับผู้ให้บริการอินเทอร์เน็ตในแต่ละประเทศ เพื่อให้เร่งดำเนินการประสานงานแก้ไขให้เรียบร้อยก่อนวันที่ 9 กรกฎาคม 2555 ซึ่งเป็นวันที่เอฟบีไอจะปิดเครื่องแม่ข่าย DNS ของ DNS Changer ตัวนี้



กราฟที่ 24 หน่วยงานหรือผู้ให้บริการอินเทอร์เน็ตที่ถูกตรวจสอบพบว่ามีเครื่องที่ติดมัลแวร์ DNS Changer อยู่ในเครือข่าย ข้อมูล ณ วันที่ 8 กรกฎาคม 2555 จาก DCWG.org

ไทยเซิร์ตได้รับข้อมูลจำนวนเครื่องที่ติด DNS Changer Malware จากหน่วยงานดีซีดับบลิวจี (DCWG) 29 เพื่อใช้ในการประสานงานกับผู้ให้บริการอินเทอร์เน็ตในประเทศไทย ซึ่งจากข้อมูลในวันที่ 8 กรกฎาคม 2555 ก่อนกำหนดที่เอฟบีไอจะปิดเครื่องแม่ข่าย DNS ของ DNS Changer เพียง 1 วัน เราพบว่ายังมีเครื่องคอมพิวเตอร์ในประเทศไทยที่ยังไม่ได้รับการแก้ไขปัญหา อยู่ทั้งสิ้น 2,023 รายการ โดยสามารถแบ่งแยกตามผู้ให้บริการเครือข่าย 10 ประเภทได้ดังกราฟที่ 24

จากกราฟจะพบว่า เครื่องคอมพิวเตอร์ที่ติด Malware ส่วนใหญ่อยู่ในเครือข่ายของผู้ให้บริการอินเทอร์เน็ตเชิงพาณิชย์รายใหญ่ เช่น TOT, Triple-T, True และ CAT ได้มีการให้ความร่วมมือกับไทยเซิร์ตมาอย่างต่อเนื่องตามนโยบายที่กำหนดขององค์กร มีบางส่วนอยู่ในหน่วยงานของรัฐด้วย ได้แก่ เว็บไซต์ทางภาคการศึกษา ซึ่งการดำเนินงานที่ผ่านมาไทยเซิร์ตได้มีการประสานงานกับหน่วยงานในสังกัดกระทรวงศึกษาธิการที่เกี่ยวข้อง เพื่อการวางแผนระยะยาวสำหรับการจัดการปัญหาที่เกี่ยวข้องกับภัยคุกคามด้านสารสนเทศ

กรณีนี้นับเป็นกรณีศึกษาที่น่าสนใจ เพราะว่ามีหลายครั้งที่ภัยคุกคามนี้เกี่ยวข้องโดยตรงกับผู้ใช้งานจำนวนมาก แต่ไทยเซิร์ตกลับไม่สามารถทราบว่าข้อมูล IP Address ที่ได้รับรายงานเป็นของผู้ใช้งานรายใด เนื่องจากในประเทศไทยนั้นผู้จดทะเบียน IP Address มักจะเป็นผู้ให้บริการอินเทอร์เน็ต ทำให้ไทยเซิร์ตไม่สามารถติดต่อแจ้งเตือนภัยคุกคามไปถึงผู้ใช้งานที่ได้รับผลกระทบโดยตรงได้ แต่ต้องอาศัยความร่วมมือจากผู้ให้บริการอินเทอร์เน็ตในเชิงพาณิชย์ในการติดต่อประสานงานกับลูกค้าผู้ใช้งานอินเทอร์เน็ตแทน แม้ว่าไทยเซิร์ตจะมีกระบวนการติดตามการแก้ไขปัญหา แต่ประสิทธิภาพของการดำเนินการแก้ไขย่อมแตกต่างกันไป ขึ้นอยู่กับการให้ความร่วมมือ รูปแบบและวิธีการในการดำเนินการของผู้ให้บริการแต่ละราย

4.4.3 การพบเครื่อง C&C ของ Malware ตระกูลเฟลม (Flame)

ไทยเซิร์ตได้รับแจ้งในวันที่ 19 มิถุนายน 2555 จากหน่วยงานเครือข่ายของไทยเซิร์ตในต่างประเทศว่า มีการพบเครื่องแม่ข่าย C&C[29] ของ Malware ประเภท Botnet ที่คาดว่าจะเป็นสายพันธุ์ใหม่ของ Flame ในประเทศไทย ซึ่งในช่วงก่อนหน้านั้น ทั่วโลกกำลังสนใจข่าวการระบาดของ Flame ซึ่งเชื่อกันว่าเป็น Malware ที่มุ่งเป้าหมายไปยังหน่วยงานระดับประเทศในตะวันออกกลาง และจากการตรวจสอบข้อมูลของไทยเซิร์ต พบว่าเครื่อง C&C ดังกล่าวอยู่ในเครือข่ายของผู้ให้บริการ Web Hosting รายหนึ่งในประเทศไทย

ไทยเซิร์ตได้ขอข้อมูลเพิ่มเติมจากหน่วยงานเครือข่ายผู้แจ้ง เพื่อนำมาวิเคราะห์และตรวจสอบความถูกต้อง ซึ่งในที่สุดก็สามารถยืนยันได้ว่า เครื่อง C&C ที่ได้รับแจ้งมีพฤติกรรมเป็นเครื่อง C&C จริง นอกจากนี้แล้ว ทางผู้แจ้งยังระบุด้วยว่า มีความเป็นไปได้ที่เจ้าของเครื่อง C&C นี้ จะมีส่วนรู้เห็นกับการกระทำความผิด และให้คำแนะนำว่า ไทยเซิร์ตไม่ควรประสานงานไปยังผู้ให้บริการ Web Hosting นี้โดยตรง เนื่องจากเกรงว่า เจ้าของเครื่อง C&C อาจลบข้อมูลทั้งหมดในเครื่อง C&C ทิ้งก่อนที่เจ้าหน้าที่จะเข้าดำเนินการ ดังที่เคยมีตัวอย่างมาแล้วในต่างประเทศ โดยผู้แจ้งได้เสนอแนะว่าควรเป็นการดำเนินการทางกฎหมายในลักษณะเข้ายึดเครื่องแม่ข่ายเพื่อตรวจสอบ

ไทยเซิร์ตได้ประชุมหารือกับหน่วยงานด้านกฎหมายทั้งจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร แต่พบว่าในปัจจุบัน ยังไม่มีช่องทางที่จะดำเนินการได้ทางกฎหมาย เนื่องจากไม่สามารถหาผู้เสียหายในประเทศไทยได้ จึงไม่เข้าเกณฑ์ของการใช้กฎหมายอาญา และเนื่องจากไม่เข้าข่าย พ.ร.บ. การกระทำความผิดทางคอมพิวเตอร์ จึงไม่สามารถใช้อำนาจของพนักงานเจ้าหน้าที่ตาม พ.ร.บ. ดังกล่าวเข้าดำเนินการได้เช่นกัน ไทยเซิร์ตจึงได้นำเสนอข้อจำกัดในการดำเนินการ เพื่อใช้เป็นข้อมูลประกอบในการปฏิบัติงานของ เจ้าหน้าที่ซึ่งเกี่ยวข้อง เพื่อใช้ในการปรับปรุงกฎหมายต่อไป แต่อย่างไรก็ดี มาตรการดังกล่าวเป็นมาตรการในระยะยาว แต่ยังขาดมาตรการในระยะสั้น จึงต้องพยายามสร้างมาตรการดังกล่าวขึ้นมา และเพื่อแก้ปัญหาและความเสี่ยงแบบยั่งยืนจึงได้มีการจัดตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) ซึ่งมีนายกรัฐมนตรีทำหน้าที่เป็นประธานกรรมการดังกล่าว

29 Command Control Center (C&C) เครื่องหรือระบบคอมพิวเตอร์ที่ผู้พัฒนาโปรแกรมไม่พึงประสงค์ Malware สร้างไว้สำหรับควบคุมและสั่งการโปรแกรมไม่พึงประสงค์เพื่อให้ทำงานตามที่ต้องการ

4.4.4 การขโมยบัญชีผู้ใช้งานอีเมลของผู้ประกอบการประเภทเอสเอ็มอี

ไทยเซิร์ตได้รับแจ้งจากผู้ประกอบการประเภทเอสเอ็มอี (SME/Small and Medium Enterprise) ที่ใช้อีเมล (Email) เป็นช่องทางในการติดต่อเพื่อซื้อขายสินค้ากับลูกค้าชาวต่างประเทศ โดยที่ผู้ประกอบการใช้บริการอีเมลของผู้ให้บริการจากต่างประเทศ และเกิดการฉ้อโกงระหว่างผู้ไม่ประสงค์ดีกับลูกค้าของผู้ประกอบการ ในลักษณะที่ผู้ไม่ประสงค์ดีได้สร้างอีเมลใหม่ที่มีที่อยู่อีเมล (Email Address) ใกล้เคียงกับของผู้ประกอบการ และใช้อีเมลที่สร้างขึ้นนี้ไปหลอกลวงลูกค้าของผู้ประกอบการว่า ผู้ประกอบการได้เปลี่ยนบัญชีธนาคารสำหรับรับโอนเงินชำระค่าสินค้าแล้ว และในบางรายได้แจ้งรายการส่งเสริมการขายหรือเสนอผลประโยชน์ให้กับลูกค้าของผู้ประกอบการเพื่อหลอกลวงให้ลูกค้าโอนเงินมาที่บัญชีที่แจ้งเปลี่ยนไปใหม่ ส่งผลให้ลูกค้าบางรายหลงเชื่อ และโอนเงินเข้าบัญชีธนาคารดังกล่าว ซึ่งผู้ประกอบการได้นำเรื่องไปแจ้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี และสำนักป้องกันและปราบปรามการกระทำผิดทางเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารแล้ว และได้รับคำแนะนำจากหน่วยงานข้างต้นให้มาปรึกษากับไทยเซิร์ตเพื่อประสานงานไปยังผู้ให้บริการอีเมลในต่างประเทศ เพื่อดำเนินการกับบัญชีผู้ใช้ของผู้ไม่ประสงค์ดี

จากการตรวจสอบข้อมูลหลักฐานที่ผู้เสียหายได้รวบรวมไว้นั้น มีประเด็นที่น่าสนใจ นั่นคือ การที่ผู้ไม่ประสงค์ดี รู้จักที่อยู่อีเมลของลูกค้าของผู้เสียหาย และยังรู้ด้วยว่าผู้เสียหายกับลูกค้าแต่ละรายมีการติดต่อกันอย่างไร ซื้อสินค้าอะไร ราคาเท่าใด จึงสามารถหลอกลวงให้ลูกค้าของผู้ประกอบการหลงเชื่อได้ นอกจากนี้ ยังพบว่าบัญชีธนาคารที่ผู้ไม่ประสงค์ดีได้หลอกลวงให้ลูกค้าโอนเงินมานั้น เป็นบัญชีของธนาคารไทยที่เปิดโดยชาวต่างประเทศ ซึ่งผู้เสียหายได้แจ้งรายละเอียดเหล่านี้ให้แก่กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยีทราบทั้งหมดแล้ว

ไทยเซิร์ตได้พยายามตรวจสอบประวัติการเข้าใช้งานบัญชีผู้ใช้อีเมลของผู้ประกอบการดังกล่าว เนื่องจากคาดว่าผู้ไม่ประสงค์ดีอาจทราบรหัสผ่านของผู้ประกอบการและสามารถเข้าไปลักลอบขโมยข้อมูลต่าง ๆ เช่น รายชื่อลูกค้า ข้อมูลสินค้า รวมถึงข้อมูลการสนทนาทางอีเมลระหว่างผู้ประกอบการกับลูกค้าในอดีต แต่เนื่องจากเหตุการณ์ได้ผ่านมาเป็นระยะเวลาพอสมควรแล้ว จึงไม่สามารถตรวจสอบข้อมูลได้ด้วยเครื่องมือที่ผู้ให้บริการอีเมลเตรียมไว้ให้ ไทยเซิร์ตจึงประสานงานไปยังผู้ให้บริการอีเมลและหน่วยงานเซิร์ต (CERT) ของประเทศของผู้ให้บริการอีเมลเพื่อขอข้อมูลเพิ่มเติม ตลอดจนสอบถามถึงความเป็นไปได้ในการระงับบัญชีผู้ใช้งานของผู้ไม่ประสงค์ดี และได้รับแจ้งว่า จำเป็นต้องใช้เอกสารทางกฎหมายเพื่อดำเนินการในกรณีดังกล่าว ไทยเซิร์ตจึงได้ประสานงานต่อไปยังกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ซึ่งเป็นผู้รับผิดชอบด้านกฎหมายในกรณีนี้โดยตรง และเพื่อให้ความช่วยเหลือกับผู้ประกอบการประเภทเอสเอ็มอีดังกล่าวติดต่อและดำเนินการทางกฎหมายต่อไป

ข้อสังเกตในกรณีนี้คือ ผู้ประกอบการรายดังกล่าวมีการระมัดระวังในการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตค่อนข้างดี เช่นมีการใช้งานซอฟต์แวร์ป้องกัน Malware ที่ถูกลิขสิทธิ์ ไม่เคยเข้าใช้งานระบบอีเมลจากเครื่องคอมพิวเตอร์สาธารณะ อีกทั้งยังใช่รหัสผ่านที่มีความยาว และซับซ้อนในระดับหนึ่ง ซึ่งไม่น่าที่จะมีผู้อื่นเดาได้ถูกต้อง นอกจากนี้แล้ว ผู้ไม่ประสงค์ดียังมีการเตรียมการที่ค่อนข้างเฉพาะเจาะจง ถึงกับมีการเปิดบัญชีธนาคารในประเทศไทยเพื่อรอรับการโอนเงิน และในการติดต่อประสานงานกับผู้ให้บริการอีเมล เสียเวลานานกว่าที่จะได้รับการตอบรับ และไม่สามารถดำเนินการใด ๆ ได้หากไม่มีเอกสารทางกฎหมาย ซึ่งเป็นเรื่องที่ค่อนข้างซับซ้อนและใช้เวลานาน

4.4.5 การแก้ไขปัญหา Phishing ในผู้ให้บริการเว็บโฮสติ้ง (Web Hosting) ของไทย

ในช่วงเวลาตั้งแต่เดือนกรกฎาคม 2554 ถึงเดือนสิงหาคม 2555 ไทยเซิร์ตได้รับคำร้องขอความร่วมมือจากธนาคารบราเดสโก (Bradesco) ในประเทศบราซิล ในการตรวจสอบและประสานงานกับผู้เกี่ยวข้อง เพื่อแก้ไขปัญหา

เว็บหลอกลวงประเภท Phishing ที่เลียนแบบหน้าเว็บไซต์ของ Bradesco ซึ่งถูกพบอยู่เป็นจำนวนมากในเว็บของผู้ให้บริการ Web Hosting รายหนึ่งในประเทศไทย คิดเป็นสัดส่วนถึงร้อยละ 34.7 ของ Incident ประเภท Phishing ทั้งหมดของ Bradesco ที่ไทยเซิร์ตได้รับแจ้ง จากการวิเคราะห์ปัญหา พบว่า ถึงแม้เว็บไซต์ที่ถูกเจาะระบบและใช้เป็นฐานในการเผยแพร่หน้า Phishing จะใช้เทคโนโลยีในการสร้างหน้าเว็บที่แตกต่างกัน แต่กลับมีลักษณะของชุดคำสั่งในหน้า Phishing เหมือนกัน ซึ่งทำให้สามารถตั้งสมมติฐานได้ว่า ผู้ไม่ประสงค์ดีที่โจมตีเว็บไซต์เหล่านี้ อาจเป็นกลุ่มบุคคลเดียวกันก็ได้ ยิ่งไปกว่านั้นผู้ไม่ประสงค์ดีอาจโจมตีเว็บไซต์เหล่านี้ด้วยการเจาะเข้าไปยังระบบบริหารจัดการเว็บไซต์ของผู้ดูแลระบบโดยตรง เนื่องจากง่ายดายกว่าการเข้าไปโจมตีระบบของแต่ละเว็บไซต์ที่ใช้เทคโนโลยีที่แตกต่างกันดังที่กล่าวไว้แล้ว

จากกรณีนี้ ไทยเซิร์ตจึงได้ติดต่อไปยังผู้ดูแลระบบของผู้ให้บริการ Web Hosting รายดังกล่าว พร้อมให้คำแนะนำในการตรวจสอบ และรักษาความมั่นคงปลอดภัย เพื่อป้องกันปัญหาการเจาะระบบที่อาจเกิดขึ้นอีกในอนาคต ทำให้ตั้งแต่เดือนกรกฎาคม 2555 เป็นต้นมา จนถึงเดือนธันวาคม 2555 ยังไม่มีการรายงานว่าพบหน้า Phishing ของ Bradesco ในผู้ให้บริการ Web Hosting รายนี้อีกเลย จึงอาจสรุปได้ว่าผู้ไม่ประสงค์ดีสามารถอาศัยช่องโหว่ในระบบบริหารจัดการเว็บไซต์ ในการบุกรุกเข้าสู่เว็บไซต์พร้อม ๆ กัน แทนที่จะหาช่องโหว่ และโจมตีทีละเว็บไซต์ ซึ่งนับว่าเป็นการโจมตีที่มีผลร้ายแรงมาก เพราะไม่ว่าเว็บไซต์ใดในระบบ จะมีการป้องกันที่ดีขนาดไหน หากมีช่องโหว่ในระบบบริหารจัดการกลาง เว็บไซต์เหล่านั้นก็ยังอาจถูกโจมตีได้เหมือนกับว่าเว็บไซต์ไม่มีการป้องกันใด ๆ เลย อย่างไรก็ตาม การที่ผู้ให้บริการ Web Hosting ตอบสนองต่อการแจ้งสถานการณ์ด้านความมั่นคงปลอดภัยของไทยเซิร์ตอย่างรวดเร็ว มีผลทำให้การดำเนินการแก้ไขภัยคุกคาม เป็นไปอย่างรวดเร็ว และอาจกล่าวได้ว่า ความสำเร็จครั้งนี้ ถือได้ว่า มาจากการทำงานร่วมกันทั้งสองฝ่าย รวมถึงการแจ้งเตือนที่รวดเร็วจากผู้ที่ได้รับผลกระทบด้วย

5

CERTs กับ AEC 2015

5. CERTs กับ AEC 2015

5.1 CERTs พันธกรณีที่กำหนดไว้ในกรอบ AEC 2015

กว่าสิบปีที่ประเทศสมาชิกอาเซียนได้ร่วมกันพัฒนาโครงสร้างพื้นฐานด้านโทรคมนาคมและเทคโนโลยีสารสนเทศของภูมิภาคเพื่อส่งเสริมความเป็นอยู่ที่ดีขึ้นของชาวอาเซียนกว่า 500 ล้านคน ซึ่งรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศได้ยืนยันร่วมกันที่จะส่งเสริมการขับเคลื่อนการพัฒนาเทคโนโลยีสารสนเทศและการสื่อสารในภูมิภาคอาเซียนให้มีความแข็งแกร่ง มีศักยภาพที่จะแข่งขันทางธุรกิจ และดึงดูดการลงทุนจากภูมิภาคอื่น ๆ รวมทั้งการใช้ไอซีทีเพื่อสร้างศักยภาพให้กับประชาชนอาเซียน โดยตั้งเป้าหมายให้ปี พ.ศ. 2558 เป็นปีที่อาเซียนจะรวมตัวกันเป็นหนึ่งเดียวที่เรียกว่าประชาคมอาเซียน (ASEAN Community) ซึ่งเป็นการบูรณาการทั้งในมิติของประชาชน วัฒนธรรม และเศรษฐกิจของอาเซียนเข้าด้วยกัน

เพื่อให้บรรลุเป้าหมายต่าง ๆ ที่ได้วางแผนไว้สมาชิกอาเซียนได้ร่วมกันจัดทำแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน พ.ศ. 2558 (ASEAN ICT Masterplan 2015) ซึ่งได้รับการรับรองในการประชุมรัฐมนตรีอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ ครั้งที่ 10 (The 10th ASEAN Telecommunications and IT Ministers Meeting) ระหว่างวันที่ 13-14 มกราคม พ.ศ. 2554 โดยแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียนนี้กำหนดแผนงาน เป้าหมายและระยะเวลาในการดำเนินการให้สำเร็จภายในระยะเวลา 5 ปี (พ.ศ. 2553-2558) มียุทธศาสตร์หลักจำนวน 6 ข้อ ได้แก่ (1) ใช้ไอซีทีเป็นเครื่องมือในการผลักดันให้อาเซียนเติบโตทางเศรษฐกิจ (2) อาเซียนเป็นศูนย์กลางด้านไอซีทีของโลกแห่งหนึ่ง (3) ประชากรอาเซียนมีคุณภาพชีวิตที่ดีขึ้น และ (4) ไอซีทีมีส่วนช่วยส่งเสริมการรวมกลุ่มของอาเซียน

ซึ่ง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ. กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารเป็นหนึ่งในหน่วยงานหลักของประเทศที่มีหน้าที่ผลักดันให้ประเทศไทยก้าวตามยุทธศาสตร์หลักทั้ง 6 ข้อของแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน พ.ศ. 2558 ที่อาเซียนได้วางไว้ ในส่วนของการดำเนินการที่เกี่ยวข้องกับความมั่นคงปลอดภัยนั้น สพธอ. โดยทีมไทยเซิร์ต (ThaiCERT) มีบทบาทสำคัญในการช่วยสนับสนุนการดำเนินการตามยุทธศาสตร์ที่กำหนดไว้ข้างต้นในหลายด้าน ดังตัวอย่างต่อไปนี้

ยุทธศาสตร์ที่ 2 เพิ่มความสามารถและการมีส่วนร่วมของประชาชน (People empowerment and engagement)

ตารางที่ 24 ยุทธศาสตร์ที่ 2 เพิ่มความสามารถและการมีส่วนร่วมของประชาชน
(People empowerment and engagement)

ความริเริ่มที่ 2.4 เสริมสร้างความเชื่อมั่น	
แผนงาน	**คำอธิบาย**
ส่งเสริมการทำธุรกรรมที่มีความมั่นคงปลอดภัยภายในภูมิภาคอาเซียน	• พัฒนาข้อตกลงยอมรับร่วมกัน (MRA) เพื่อใช้ใบรับรองอิเล็กทรอนิกส์ข้ามประเทศภายในอาเซียน • ส่งเสริมการใช้ระบบความมั่นคงปลอดภัยสองชั้น เพื่อระบุตัวตน (two-factor authentication)
รณรงค์ประชาสัมพันธ์เพื่อส่งเสริมความตระหนักรู้ในเรื่องของความมั่นคงปลอดภัยบนโลกไซเบอร์	• สร้างความตระหนักรู้แก่สาธารณชนในเรื่องความมั่นคงปลอดภัยของระบบออนไลน์ • สร้างความร่วมมือที่ใกล้ชิดระหว่างภาคธุรกิจ และผู้มีส่วนได้ส่วนเสีย • คุ้มครองข้อมูลส่วนบุคคล

ยุทธศาสตร์ที่ 4 การพัฒนาโครงสร้างพื้นฐาน (Infrastructure development)

ตารางที่ 25 ยุทธศาสตร์ที่ 4 การพัฒนาโครงสร้างพื้นฐาน30 (Infrastructure development)

ความริเริ่มที่ 4.2 ส่งเสริม ความเสถียรของโครงข่าย และความมั่นคงปลอดภัยข้อมูลสารสนเทศ การปกป้องข้อมูล และความร่วมมือของศูนย์ประสานงานการรักษาความปลอดภัยทางคอมพิวเตอร์ หรือ เซิร์ต (Computer Emergency Response Team - CERT)	
แผนงาน	**คำอธิบาย**
พัฒนากรอบความมั่นคงปลอดภัยของโครงข่าย	• สร้างมาตรฐานขั้นต่ำที่ใช้ร่วมกันในเรื่องความมั่นคงปลอดภัยของโครงข่ายเพื่อประกันความพร้อมและความเสถียรของโครงข่ายในภูมิภาคอาเซียน • พัฒนาโครงการ “Health Screening” ของอาเซียนเพื่อความมั่นคงปลอดภัยของโครงข่าย โดยให้มีการตรวจสอบความมั่นคงปลอดภัยเป็นระยะ ๆ • สร้างแนวทางปฏิบัติที่ดี (Best Practice Models) เพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง (Business continuity) และการกู้คืนระบบจากภัยพิบัติ (Disaster Recovery) • จัดตั้งสภาด้านความมั่นคงปลอดภัยของโครงข่ายแห่งอาเซียน (ASEAN Network Security Action Council) เพื่อส่งเสริมความร่วมมือเชิร์ต และการแลกเปลี่ยนความเชี่ยวชาญระหว่างกัน
พัฒนากรอบความมั่นคงปลอดภัยทางข้อมูลสารสนเทศ	• แลกเปลี่ยนแนวปฏิบัติที่ดีในเรื่องของการปกป้องข้อมูล และโครงสร้างพื้นฐานทางสารสนเทศในอาเซียน

30 โครงข่ายคือ Network หรือ เน็ตเวิร์ค

จากเนื้อหาของยุทธศาสตร์ที่ 2 และ 4 ของแผนแม่บทเทคโนโลยีสารสนเทศและการสื่อสารอาเซียน 2015 จึงเห็นได้ว่าไทยเซิร์ต (ThaiCERT) มีบทบาททั้งในด้านการเสริมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยในโลกออนไลน์ให้แก่ประชาชน ภาคธุรกิจ และผู้ที่เกี่ยวข้องอื่น ๆ และจัดให้มีมาตรการในการปกป้องและรักษาเสถียรภาพของโครงสร้างพื้นฐานสารสนเทศและความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ซึ่งหนึ่งในตัวอย่างสำคัญคือการมีส่วนร่วมเข้าเป็นสมาชิกสภาด้านความมั่นคงปลอดภัยของโครงข่ายแห่งอาเซียน (ASEAN Network Security Action) ในนามประเทศไทย

5.2 รายงาน CERTS ของประเทศสมาชิกอาเซียน

เนื่องจากภัยคุกคามด้านสารสนเทศ มีลักษณะที่ไร้พรมแดน และมีแนวโน้มที่เกิดกับประเทศต่าง ๆ ในภูมิภาคเดียวกันมีลักษณะใกล้เคียงกัน ในส่วนนี้ จึงนำเสนอข้อมูลภัยคุกคามด้านสารสนเทศ ของ”หน่วยงานเซิร์ต (CERT) ของอาเซียน +3” ซึ่งหน่วยงานเซิร์ต (CERT) จากประเทศในอาเซียน+3 นี้ทั้งหมดเป็นสมาชิกของหน่วยงานเอพีเซิร์ต (APCERT) และได้นำเสนอสถิติภัยคุกคามด้านสารสนเทศที่เกิดขึ้นในประเทศของตนเองในรายงานประจำปี 2011 ของเอพีเซิร์ต (APCERT)

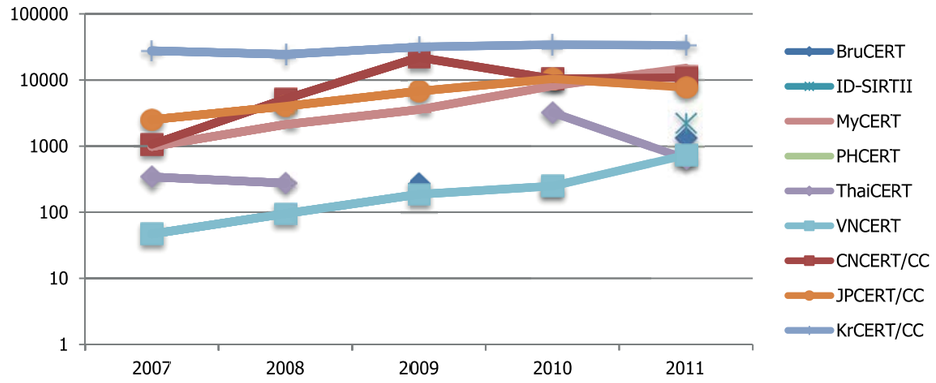
จากรายงานประจำปี 2011 ของเอพีเซิร์ต (APCERT) ได้ระบุจำนวนสมาชิกของกลุ่มประเทศของเครือข่ายความร่วมมือในระดับเอเชียแปซิฟิกว่ามีจำนวนทั้งสิ้น 22 หน่วยงานจาก 19 เขตเศรษฐกิจ โดยในจำนวนนี้เป็นหน่วยงานเซิร์ต (CERT) จากประเทศในอาเซียน+3 จำนวนทั้งสิ้น 17 หน่วยงานจาก 10 ประเทศ ประกอบด้วย

ตารางที่ 26 จำนวนสมาชิกของกลุ่มประเทศเครือข่ายความร่วมมือในระดับเอเชีย-แปซิฟิก

ชื่อหน่วยงาน	ประเทศ
Bach Khoa Internetwork Security Center (BKIS)	เวียดนาม
Brunei Computer Emergency Response Team (BruCERT)	บรูไน
CERNET Computer Emergency Response Team (CCERT)	จีน
National Computer network Emergency Response technical Team / Coordination Center of China People’s Republic of China (CNCERT/CC)	จีน
Indonesia Computer Emergency Response Team (ID-CERT)	อินโดนีเซีย
Indonesia Security Incident Response Team on Internet Infrastructure Coordination Center (ID-SIRTII/CC)	อินโดนีเซีย
Japan Computer Emergency Response Team / Coordination Center (JPCERT / CC)	ญี่ปุ่น
Korea Internet Security Center (KrCERT/CC)	เกาหลี
Malaysian Computer Emergency Response Team (MyCERT)	มาเลเซีย

Philippine Computer Emergency Response Team (PHCERT)	ฟิลิปปินส์
Singapore Computer Emergency Response Team (SingCERT)	สิงคโปร์
Thailand Computer Emergency Response Team (ThaiCERT)	ไทย
Vietnam Computer Emergency Response Team (VNCERT)	เวียดนาม
Government Computer Security and Incident Response Team (GCSIRT)	ฟิลิปปินส์
Myanmar Computer Emergency Response Team (mmCERT)	พม่า
National University of Singapore Computer Emergency Response Team (NUSCERT)	สิงคโปร์

โดยทุกประเทศในอาเซียน+3 มีหน่วยงานเซิร์ต (CERT) ในระดับประเทศและเป็นสมาชิกของหน่วยงา นเอพีเซิร์ต (APCERT) ยกเว้นหน่วยงานลาวเซิร์ต (LaoCERT) จากประเทศลาว และแคมเซิร์ต (CamCERT) จากประเทศกัมพูชา ที่ยังไม่ได้เข้าเป็นสมาชิกของเอพีเซิร์ต (APCERT)



กราฟที่ 25 จำนวนภัยคุกคามด้านสารสนเทศ ที่หน่วยงานเซิร์ต (CERT) ของประเทศในอาเซียน+3 ได้รับรายงานในระหว่างปี 2007 (2550) ถึง 2011 (2554)

จำนวนภัยคุกคามด้านสารสนเทศ ที่หน่วยงานเซิร์ต (CERT) ของประเทศในอาเซียน +3 ได้รวบรวมและนำเสนอไว้ในรายงานประจำปีของหน่วยงานเอพีเซิร์ต (APCERT) ย้อนหลัง 5 ปี แสดงในกราฟที่ 25จำนวนของภัยคุกคามด้านสารสนเทศ ที่แสดงในกราฟนี้แสดงไว้ในแกนลอการิทึม ข้อมูลที่ได้รวบรวมนี้แสดงให้เห็นว่า จำนวนภัยคุกคามด้านสารสนเทศที่หน่วยงานเซิร์ต CERT ในประเทศอาเซียน+3 มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องในช่วงย้อนหลัง 5 ปี โดยสามารถจัดหน่วยงานเซิร์ต CERT ของประเทศที่มีนำเสนอข้อมูลจำนวนภัยคุกคามด้านสารสนเทศ ไว้ในรายงานประจำปีของหน่วยงานเอพีเซิร์ต APCERT อย่างสม่ำเสมอ และมีจำนวนภัยคุกคามด้านสารสนเทศ ที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง หน่วยงานที่รับรายงานเกินจำนวน 10,000 รายการต่อปี ประกอบไปด้วย หน่วยงาน มายเซิร์ต (MyCERT) ซีเอ็นเซิร์ต (CNCERT/CC) เจพีเซิร์ต (JPCERT/CC) และ เคอาร์เซิร์ต (KrCERT/CC) ส่วนจำนวนภัยคุกคามด้านสารสนเทศ รายปีของหน่วยงานเซิร์ต (CERT) ของประเทศนอกเหนือจากกลุ่มข้างต้น บรูเซิร์ต (BruCERT) ไอดีเซอร์ตี้ (ID-SIRTII) พีเอชเซิร์ต (PHCERT) ไทยเซิร์ต (ThaiCERT) และ วีเอ็นเซิร์ต (VNCERT) พบว่ามีแนวโน้มของจำนวนภัยคุกคามด้านสารสนเทศ ที่ได้รับรายงานเพิ่มขึ้นในลักษณะเดียวกับกลุ่มแรก แต่มีจำนวนภัยคุกคามด้านสารสนเทศ ที่ได้รับรายงานน้อยกว่า ซึ่งในปี 2011 มีจำนวนภัยคุกคามด้านสารสนเทศที่ได้รับรายงานอยู่เป็นจำนวนน้อยกว่า 5,000 รายการ

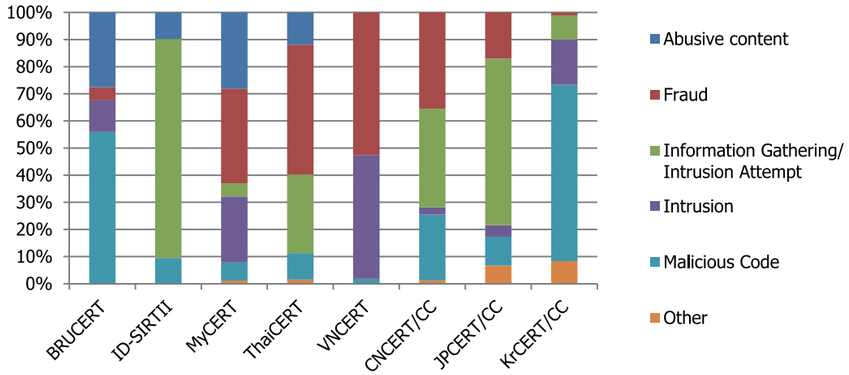
ในตารางที่ 24 แสดงสัดส่วนของภัยคุกคามด้านสารสนเทศ ต่อจำนวนภัยคุกคามด้านสารสนเทศ ทั้งหมดที่ได้รับแจ้งที่หน่วยงานเซิร์ต CERT ระดับประเทศของประเทศอาเซียน+3 ได้สรุปข้อมูลและแสดงไว้ในรายงานประจำปี 2011 ของเอพีเซิร์ต (APCERT) ซึ่งประกอบด้วยข้อมูลจากหน่วยงาน บรูเซิร์ต (BruCERT) ไอดีเซอร์ตี้ (ID-SIRTII) มายเซิร์ต (MyCERT) ไทยเซิร์ต (ThaiCERT) และ วีเอ็นเซิร์ต (VNCERT) ซีเอ็นเซิร์ต/ซีซี (CNCERT/CC) เจพีเซิร์ต/ซีซี (JPCERT/CC) และ เคอาร์เซิร์ต/ซีซี (KrCERT/CC)

ข้อมูลสถิติภัยคุกคามด้านสารสนเทศ ที่หน่วยงานไทยเซิร์ต ได้นำเสนอไว้ในรายงานของเอพีเซิร์ต (APCERT) นี้ เป็นจำนวนภัยคุกคามด้านสารสนเทศ ที่ไทยเซิร์ต ได้รับรายงานเฉพาะในช่วง 6 เดือน ในระหว่างเดือนกรกฎาคม ถึงเดือนธันวาคม 2554 ซึ่งเป็นช่วงของการให้บริการของไทยเซิร์ต ภายใต้การบริหารจัดการของสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ (องค์การมหาชน) นอกจากนั้นข้อมูลภัยคุกคามด้านสารสนเทศ ของหน่วยงาน ซีเอ็นเซิร์ต/ซีซี (CNCERT/CC) และเจพีเซิร์ต/ซีซี (JPCERT/CC) ไม่ได้นำเสนอข้อมูลสถิติของภัยคุกคามด้านสารสนเทศ ประเภทเนื้อหาที่เป็นภัยคุกคามด้านสารสนเทศในส่วนของสแปม (SPAM) ที่ได้รับรายงานผ่านระบบตรวจจับอัตโนมัติในข้อมูลเชิงสถิติของหน่วยงาน

หมายเหตุ หน่วยงานพีเอชเซิร์ต (PHCERT) ไม่ได้นำเสนอรายงานการดำเนินการประจำปี 2011 และ หน่วยงานซิงเซิร์ต (SingCERT) ไม่ได้นำเสนอข้อมูลสถิติภัยคุกคามด้านสารสนเทศ ในรายงานประจำปีที่ 2011 ของเอพีเซิร์ต (APCERT) เพียงแต่ระบุไว้ว่าภัยคุกคามด้านสารสนเทศ ประเภทการฉ้อโกง (Fraud) เป็นประเภทภัยคุกคามด้านสารสนเทศ ที่หน่วยงานซิงเซิร์ต (SingCERT) ได้รับรายงานสูงสุด

ตารางที่ 27 สัดส่วนของภัยคุกคามด้านสารสนเทศ แยกตามประเภทของประเทศในอาเซียน+3 ที่แสดงไว้ในรายงานประจำปีที่ 2011 ของเอพีเซิร์ต (APCERT)

	BRUCERT	ID-SIRTII	MyCERT	ThaiCERT	VNCERT	CNCERT/CC	JPCERT/CC	KrCERT/CC
Abusive content	27.5%	9.8%	28.1%	11.9%	0.0%	0.0%	0.0%	0.0%
Fraud	4.9%	0.0%	35.0%	47.8%	52.6%	35.5%	17.0%	1.1%
Information Gathering/ Intrusion Attempt	0.0%	80.7%	4.8%	28.9%	0.0%	36.3%	61.4%	8.9%
Intrusion	11.7%	0.0%	24.3%	0.0%	45.6%	2.7%	4.3%	16.6%
Malicious Code	55.9%	9.5%	6.7%	9.8%	1.8%	24.3%	10.6%	65.0%
Other	0.0%	0.0%	1.2%	1.5%	0.0%	1.2%	6.7%	8.3%
จำนวนทั้งหมดที่ได้รับรายงาน	**1,345**	**2,248**	**15,218**	**646**	**732**	**15,366**	**7,722**	**33,441**



กราฟที่ 26 สัดส่วนของภัยคุกคามด้านสารสนเทศ แยกตามประเภทของประเทศในอาเซียน+3 ที่แสดงไว้ในรายงานประจำปีที่ 2011 ของเอพีเซิร์ต (APCERT)

จากข้อมูลสถิติภัยคุกคามด้านสารสนเทศ ของหน่วยงานเซิร์ต (CERT) ในประเทศอาเซียน+3 แสดงตามตารางที่ 27 และ กราฟที่ 26 พบว่าภัยคุกคามด้านสารสนเทศ ประเภทโปรแกรมไม่พึงประสงค์เป็นภัยคุกคามด้านสารสนเทศ ที่หน่วยงานเซิร์ต (CERT) ของประเทศบรูไนและประเทศเกาหลีใต้ได้รับแจ้งสูงสุดเป็นอันดับหนึ่งและมีปริมาณมากกว่าร้อยละ 50 ของจำนวนภัยคุกคามด้านสารสนเทศ ทั้งหมดที่ได้รับแจ้ง ส่วนประเทศอินโดนีเซียและประเทศญี่ปุ่น ภัยคุกคามด้านสารสนเทศ ประเภทความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) และ ประเภทความพยายามบุกรุกเข้าระบบ (Intrusion Attempt) มีจำนวนที่ได้รับรายงานสูงสุด และมีปริมาณมากกว่าร้อยละ 80 และร้อยละ 60 ของภัยคุกคามด้านสารสนเทศ ทั้งหมดที่หน่วยงานไอดีเซอร์ตี้ (ID-SIRTII) และ เจพีเซิร์ต (JPCERT/CC) ได้รับรายงานในปี 2554 ตามลำดับ ในส่วนประเทศมาเลเซีย ประเทศไทย ประเทศเวียดนาม และประเทศจีน ภัยคุกคามด้านสารสนเทศ ประเภทฉ้อโกง (Fraud) เป็นประเภทของภัยคุกคาม

ด้านสารสนเทศ ที่หน่วยงานเซิร์ต (CERT) ได้รับแจ้งสูงสุด โดยมีจำนวนในสัดส่วนระหว่างร้อยละ 35 ถึงร้อยละ 52.6 ของจำนวนภัยคุกคามด้านสารสนเทศ ที่ได้รับแจ้งในแต่ละประเทศในกลุ่มนี้

จากข้อมูลภัยคุกคามด้านสารสนเทศ ที่หน่วยงานเซิร์ต (CERT) ในประเทศอาเซียน+3 ได้นำเสนอไว้ในรายงานประจำปีของหน่วยงานเอพีเซิร์ต (APCERT) สามารถสรุปได้ว่า แนวโน้มภัยคุกคามด้านสารสนเทศ ในประเทศต่าง ๆ ในภูมิภาคมีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง และส่วนใหญ่จะเป็นภัยคุกคามด้านสารสนเทศ ในประเภทโปรแกรมไม่พึงประสงค์ ประเภทความพยายามรวบรวมข้อมูลของระบบ ประเภทความพยายามบุกรุกเข้าระบบ และประเภทฉ้อโกง (Fraud)

5.3 ความเข้มแข็งในการทำงานร่วมกันของ CERTs

5.3.1 การสร้างเครือข่ายความร่วมมือ

การดำเนินการแก้ไขภัยคุกคามด้านสารสนเทศ ต้องอาศัยความร่วมมือจากหน่วยงานที่เกี่ยวข้องกับเหตุภัยคุกคามด้านสารสนเทศ โดยเฉพาะอย่างยิ่งกรณีที่หน่วยรับมือภัยคุกคามด้านสารสนเทศ ไม่มีอำนาจทางกฎหมายในการจัดการกับภัยคุกคามด้านสารสนเทศ นั้น ปัจจุบันมีการรวมตัวกันของหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ เป็นเครือข่ายความร่วมมืออยู่หลายเครือข่าย เช่นเฟิร์ส (FIRST), เอพีเซิร์ต (APCERT) และโอไอซีเซิร์ต (OICCERT) เป็นต้น หน่วยงานในเครือข่ายความร่วมมือจะช่วยประสานความร่วมมือในการรับมือภัยคุกคามด้านสารสนเทศ แลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามด้านสารสนเทศ ตลอดจนซักซ้อมการรับมือภัยคุกคามด้านสารสนเทศ ร่วมกัน เพื่อเป็นการสร้างความเข้มแข็งให้กับเครือข่ายความร่วมมือ ปัจจุบันประเทศไทยเป็นสมาชิก เอพีเซิร์ต (APCERT) และเฟิร์ส (FIRST) ซึ่งเป็นเครือข่ายความร่วมมือในระดับเอเชียแปซิฟิกและระดับโลกตามลำดับ

เอพีเซิร์ต (APCERT/Asia Pacific Computer Emergency Response Team) มีหน่วยงานสมาชิก 30 หน่วยงาน จาก 20 ประเทศ ซึ่งมีวิสัยทัศน์ร่วมกันรักษาโลกไซเบอร์ให้มีความมั่นคงปลอดภัย และใช้งานได้โดยอาศัยความร่วมมือระหว่างหน่วยงานทั่วโลก สมาชิกเอพีเซิร์ต (APCERT) พบกันอย่างน้อยปีละหนึ่งครั้งในการประชุมประจำปี ซึ่งมีการแลกเปลี่ยนข้อมูลและประสบการณ์ในการรับมือภัยคุกคามด้านสารสนเทศ นอกจากนี้ยังมีการจัดการซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ ปีละ 1 ครั้ง เพื่อทดสอบแนวทางการรับมือภัยคุกคามด้านสารสนเทศ ว่ายังใช้ได้อย่างมีประสิทธิผลอยู่หรือไม่

เฟิร์ส (FIRST/Forum of Incident Response and Security Teams) มีสมาชิกกว่า 260 หน่วยงาน และมีเป้าหมายสนับสนุนให้หน่วยงานสมาชิกรับมือภัยคุกคามด้านสารสนเทศ ได้อย่างมีประสิทธิภาพมากโดยอาศัยหลักปฏิบัติเครื่องมือ และช่องทางการสื่อสารที่มั่นคงปลอดภัย สมาชิกของเฟิร์ส (FIRST) มีการรวมกลุ่มเพื่อร่วมกันทำงานตามความสนใจ เช่น กลุ่มซีวีเอสเอส (CVSS SIG/CVSS Special Interest Group) จัดทำมาตรฐานการให้คะแนนความรุนแรงของช่องโหว่ระบบสารสนเทศ กลุ่มเมทริกส์เอสไอจี (Metrics SIG) จัดทำแนวทางการประเมินผลการรับมือภัยคุกคามด้านสารสนเทศ ของหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ กลุ่มเน็ตเวิร์ก มอนิเตอริ่ง เอสไอจี (Network Monitoring SIG) ส่งเสริมการเผยแพร่ความรู้เกี่ยวกับวิธีการเก็บและวิเคราะห์ข้อมูล เน็ตเวิร์กเซ็นเซอร์ (network sensor) เพื่อหาเหตุการณ์ผิดปกติในเครือข่ายคอมพิวเตอร์ หรือกลุ่มวิเคราะห์มัลแวร์ เอสไอจี (Malware Analysis SIG) ส่งเสริมการเผยแพร่เครื่องมือและวิธีการวิเคราะห์โปรแกรมไม่พึงประสงค์ (Malware)

กิจกรรมที่หน่วยรับมือภัยคุกคามด้านสารสนเทศ ทำร่วมกันนำไปสู่การกระชับความสัมพันธ์ระหว่างหน่วยงาน เสริมสร้างขีดความสามารถในการรับมือภัยคุกคามด้านสารสนเทศ นำไปสู่การรับมือภัยคุกคามด้านสารสนเทศ ที่มีคุณภาพระดับสากล

5.3.2 การกำหนดผู้ประสานงานหลัก (Point of Contact)

เนื่องจากภัยคุกคามด้านสารสนเทศ มีลักษณะที่ไร้พรมแดน ต้นกำเนิดของภัยคุกคามด้านสารสนเทศ สามารถมาจากทั้งภายในประเทศและต่างประเทศ ซึ่งหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ จำเป็นต้องประสานความร่วมมือกับหน่วยงานเหล่านั้นหรือหน่วยงานในเครือข่ายความร่วมมือให้มีการแก้ไขภัยคุกคามด้านสารสนเทศที่พบ และสิ่งที่สำคัญที่สุดของการประสานความร่วมมือคือ ผู้ประสานงานหลักของหน่วยงานในเครือข่ายความร่วมมือ หรือ พีโอซี (PoC /Point of Contact) ซึ่งควรเป็นผู้ที่มีความเข้าใจในเทคโนโลยีเพียงพอที่จะดำเนินการหรือประสานงานในการแก้ไขปัญหาภัยคุกคามด้านสารสนเทศ นั้นอย่างทันเวลา เพื่อจำกัดความเสียหายที่อาจจะเกิดขึ้น

ปัญหาที่หน่วยงานรับมือภัยคุกคามด้านสารสนเทศพบส่วนใหญ่คือ ข้อมูลพีโอซี (PoC) ไม่มีการปรับปรุงให้เป็นปัจจุบัน เช่น มีการเปลี่ยนตัวผู้ประสานงานความร่วมมือ หรือเปลี่ยนช่องทางการติดต่อผู้ประสานความร่วมมือ เป็นต้น ดังนั้นหน่วยงานต่าง ๆ ควรมีการกำหนดตัวผู้ประสานความร่วมมือในการแก้ไขปัญหาภัยคุกคามด้านสารสนเทศอย่างชัดเจน ปรับปรุงข้อมูลพีโอซี (PoC) ให้ทันสมัยอยู่เสมอ และมีช่องทางประกาศให้หน่วยงานภายนอกทราบข้อมูลที่เป็นปัจจุบัน

ปัจจุบันเครือข่ายความร่วมมือของหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ มีการรวบรวมและประกาศให้สาธารณะทราบเพื่อประโยชน์ในการประสานความร่วมมือในการแก้ไขปัญหา เช่น ข้อมูลพีโอซี (PoC) ของสมาชิกเฟิร์ส (FIRST) สามารถดูได้จาก http://www.first.org/members/teams[31] ซึ่งมีรายการของพีโอซี (PoC) มากกว่า 260 หน่วยงานทั่วโลก สนับสนุนช่องทางการติดต่อแบบโทรศัพท์ โทรสาร หรืออีเมล และยังส่งเสริมให้ใช้เทคโนโลยีกุญแจสาธารณะ (Public Key Technology) ในการยืนยันตัวผู้รับหรือส่งข้อมูล และการเข้ารหัสลับข้อมูลที่รับหรือส่ง

5.3.3 การให้ข้อมูลเกี่ยวกับภัยคุกคามด้านสารสนเทศ

หน่วยงานรับมือภัยคุกคามด้านสารสนเทศ จะทำงานทั้งในเชิงรุกและเชิงรับตามขอบเขตงานและอำนาจตามกฎหมาย หน่วยงานรับมือภัยคุกคามด้านสารสนเทศ บางหน่วยสามารถตรวจจับข้อมูลในเครือข่ายอินเทอร์เน็ตเพื่อเฝ้าระวังภัยคุกคามด้านสารสนเทศได้ แต่บางหน่วยก็ไม่สามารถทำได้ด้วยข้อจำกัดทางกฎหมาย อย่างไรก็ตามมีหน่วยงานอิสระหลายหน่วยพยายามรวบรวมข้อมูลเกี่ยวกับภัยคุกคามด้านสารสนเทศ ขึ้นและสนับสนุนข้อมูลดังกล่าวให้กับหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ เพื่อให้มีการแก้ไขได้อย่างรวดเร็ว เช่น ข้อมูลเกี่ยวกับฟิชชิ่ง (Phishing) มีการรวบรวมไว้โดยกลุ่ม Anti-Phishing Working Group (APWG) หรือโดยฟิชแทงค์ (Phishtank) ซึ่งดำเนินการโดยโอเพนดีเอ็นเอส (OpenDNS) ข้อมูลดังกล่าวประกอบไปด้วยรายการของยูอาร์เอล (URL) ของ เว็บฟิชชิ่ง (Phishing Website) ซึ่งหน่วยงานรับมือภัยคุกคามด้านสารสนเทศ สามารถนำไปใช้ประกอบการดำเนินการแก้ไขปัญหาได้

นอกจากการรับข้อมูลภัยคุกคามด้านสารสนเทศ จากหน่วยงานอิสระแล้ว หน่วยงานรับมือภัยคุกคามด้านสารสนเทศยังมีการแลกเปลี่ยนข้อมูลภัยคุกคามด้านสารสนเทศ ระหว่างกัน ซึ่งรวมถึงต้นกำเนิดและลักษณะของภัยคุกคามด้านสารสนเทศ รวมถึงแนวทางในการป้องกันและแก้ไขภัยคุกคามด้านสารสนเทศ หน่วยงานรับมือภัยคุกคามด้านสารสนเทศสามารถนำข้อมูลลักษณะนี้ไปแจ้งเตือนหน่วยงานที่อาจได้รับผลกระทบจากภัยคุกคามด้านสารสนเทศ ได้ เป็นการสร้างความตระหนัก การให้ความรู้ และส่งเสริมให้เกิดการสร้างภูมิคุ้มกันในระดับหน่วยงาน

31 http://www.first.org/members/teams เข้าถึง ณ วันที่ 31 สิงหาคม 2555

5.3.4 การจัดทำมาตรฐานเกี่ยวกับข้อมูลภัยคุกคามด้านสารสนเทศ

การแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามด้านสารสนเทศในปัจจุบันยังเกิดขึ้นในวงจำกัด โดยที่ส่วนใหญ่ผู้ให้ข้อมูลจะเป็นผู้กำหนดรูปแบบของข้อมูลที่จะให้ ทำให้รูปแบบของข้อมูลมีความหลากหลายเป็นภาระของผู้รับข้อมูลในการแปลงข้อมูลที่ได้รับให้อยู่ในรูปแบบที่สามารถนำไปดำเนินการต่อได้โดยสะดวก หน่วยงานรับมือภัยคุกคามด้านสารสนเทศ ได้ร่วมกันจัดทำมาตรฐานขึ้นเพื่อเพิ่มประสิทธิภาพในการทำงาน เช่น มาตรฐานสำหรับการแลกเปลี่ยนข้อมูลเหตุภัยคุกคามด้านสารสนเทศ หรือ ไอโอดีอีเอฟ (IODEF /The Incident Object Description Exchange Format) เป็นข้อเสนอเพื่อพิจารณาให้ความเห็น RFC 507032 ซึ่งออกภายใต้คณะทำงานไออีทีเอฟ (IETF/Internet Engineering Task Force)

นอกจากนี้ ยังมีการพัฒนามาตรฐานการให้คะแนนความรุนแรงของช่องโหว่ระบบสารสนเทศ หรือ Common Vulnerability Scoring System (CVSS) เพื่อให้การประเมินระดับความรุนแรงของช่องโหว่เป็นมาตรฐานเดียวกัน ทำให้บุคคลทั่วไปเข้าใจตรงกันถึงระดับความรุนแรงหากมีการใช้ช่องโหว่ในทางมิชอบ

5.3.5 การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ

การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ เป็นกิจกรรมที่หน่วยงานรับมือภัยคุกคามด้านสารสนเทศ ดำเนินเป็นประจำเพื่อทดสอบกระบวนการรับมือภัยคุกคามด้านสารสนเทศ ที่กำหนดไว้ล่วงหน้า และทดสอบภาวะการตัดสินใจของบุคลากรที่เกี่ยวข้อง เป็นการสร้างความมั่นใจให้กับหน่วยงาน หากมีเหตุภัยคุกคามด้านสารสนเทศ เกิดขึ้นจริง บุคลากรที่เกี่ยวข้องจะได้ปฏิบัติตนได้อย่างถูกต้อง จำกัดความเสียหายจากเหตุภัยคุกคามด้านสารสนเทศ ให้ได้เร็วที่สุด และอาจติดตามตัวผู้กระทำความผิดมาลงโทษ

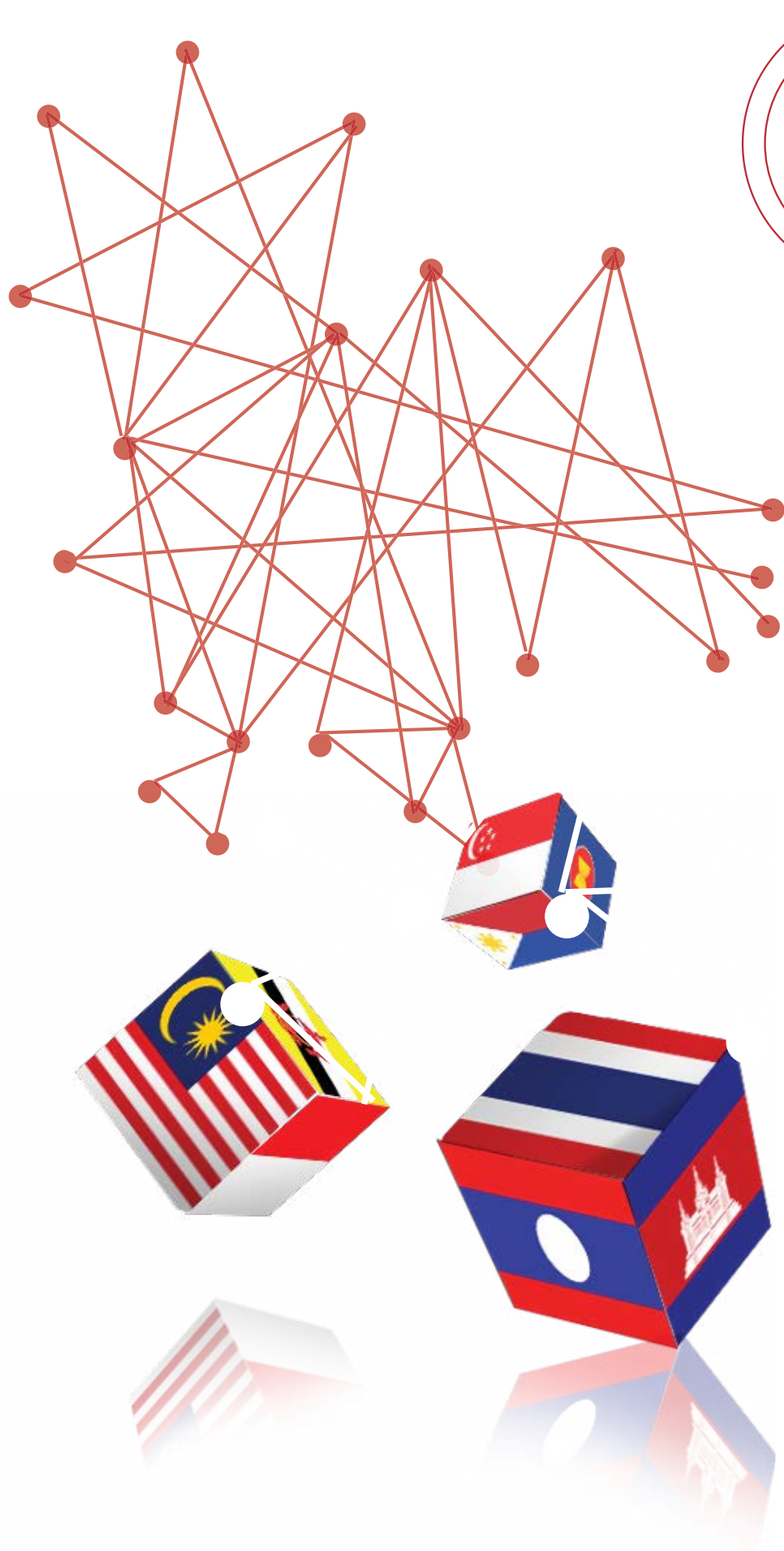
การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ สามารถทำได้หลายระดับ โดยขั้นพื้นฐานที่สุดอาจทำโดยเชิญบุคลากรที่เกี่ยวข้องมาซักซ้อมแนวทางการรับมือภัยคุกคามด้านสารสนเทศ ในห้องประชุม โดยกำหนดเหตุการณ์สมมุติ บทบาทสมมุติสำหรับแต่ละคน และให้แต่ละคนอธิบายการปฏิบัติเพื่อแก้ไขเหตุภัยคุกคามด้านสารสนเทศ ในเหตุการณ์สมมุติตามบทบาทที่เกี่ยวข้อง การซักซ้อมรับมือภัยคุกคามด้านสารสนเทศ อาจทำได้โดยจำลองสถานการณ์จริง และผู้เข้าร่วมสามารถลงมือปฏิบัติได้จริง ก็จะทำให้เห็นข้อผิดพลาดในการปฏิบัติมากขึ้น นำไปปรับปรุงขั้นตอนวิธีการรับมือภัยคุกคามด้านสารสนเทศ อย่างมีประสิทธิภาพและประสิทธิผล

32 http://www.ietf.org/rfc/rfc5070.txt เข้าถึงวันที่ 31 สิงหาคม 2555

5.3.6 การจัดเตรียมระบบเฝ้าระวังภัยคุกคามในเครือข่ายคอมพิวเตอร์ (Sensor Network)

หน่วยงานรับมือภัยคุกคามด้านสารสนเทศ บางหน่วยมีการสร้างระบบเฝ้าระวังความผิดปกติในเครือข่ายคอมพิวเตอร์ โดยการติดตั้งซอฟต์แวร์เก็บข้อมูลจราจรของเครื่องคอมพิวเตอร์ที่ติดตั้ง ระบบคอมพิวเตอร์นี้เรียกว่า เซ็นเซอร์ (Sensors) ในระบบเฝ้าระวังฯ จะมีระบบคอมพิวเตอร์สำหรับประมวลผลข้อมูลจราจรจากเซ็นเซอร์ (Sensors) ที่ได้ติดตั้งทั่วโลก เพื่อใช้วิเคราะห์การไหลของข้อมูลที่มีความผิดปกติ เช่น หากมีการโจมตีแบบดอส (DoS/Denial of Service) จากหลายประเทศ มายังหน่วยงานที่มีเซ็นเซอร์ (Sensors) ติดตั้งระบบเฝ้าระวังสามารถตรวจจับและแจ้งเตือนได้

ระบบซุบาเมะ (Tsubame) ซึ่งดำเนินการโดยเจพีเซิร์ต (JPCERT/CC) หรือหน่วยประสานความร่วมมือหลักในการรับมือภัยคุกคามด้านสารสนเทศ ของประเทศญี่ปุ่น มีเครือข่ายของเซ็นเซอร์ (Sensors) อยู่ทั่วโลก ที่เก็บข้อมูลจราจรและส่งไปยังระบบประมวลผลกลางที่ประเทศญี่ปุ่น ข้อมูลจราจรดังกล่าวประกอบไปด้วย IP Address และ หมายเลขพอร์ต (Port Number) ของต้นกำเนิดของข้อมูล และเวลาที่ได้รับของมูลนั้น ข้อมูลจราจรจากทั่วโลกเหล่านี้ถูกนำไปแสดงเป็นภาพเคลื่อนไหว ทำให้การวิเคราะห์รูปแบบภัยคุกคามด้านสารสนเทศ มีประโยชน์ต่อการคาดการณ์ Incident ที่คาดว่าจะเกิดขึ้น ดังนั้น ระบบดังกล่าว จึงเป็นอีกหนึ่งความพยายามของการพัฒนาระบบกลไกเพื่อลดความเสี่ยงบนโลกไซเบอร์ที่ส่งผลกระทบต่อการให้บริการสารสนเทศที่สำคัญของประเทศ การพัฒนาเครื่องมือที่มีลักษณะเฉพาะเพื่อตรวจจับและติดตามภัยคุกคามนี้ เป็นสิ่งที่แสดงให้เห็นถึงความจำเป็นที่ประเทศไทยต้องให้สำคัญในด้านการวิจัยและพัฒนาความมั่นคงไซเบอร์ในประเทศอย่างเป็นรูปธรรม



6

Threats กับ สิทธิในความเป็นส่วนตัว (Privacy)

6. Threats กับ สิทธิในความเป็นส่วนตัว (Privacy)

เนื่องด้วย Threats มักจะมาพร้อมกับปัญหาการละเมิดความเป็นส่วนตัวและการขโมยข้อมูลส่วนบุคคล เพื่อนำไปใช้ในการฉ้อโกงในรูปแบบต่าง ๆ ซึ่งจากการเก็บรวบรวมสถิติภัยคุกคามลักษณะนี้มีแนวโน้มที่จะทวีความรุนแรงและมีปริมาณสูงขึ้นเรื่อย ๆ โดยประเด็นการคุ้มครองข้อมูลส่วนบุคคลถูกหยิบยกขึ้นมาเป็นประเด็นสำคัญและถูกกล่าวถึงอย่างมากในเวทีระดับนานาชาติ เช่น United Nations APEC ASEAN และ OECD (Organisation for Economic Co-operation and Development) ซึ่งเห็นว่าต้องมีการวางมาตรการป้องกันภัยลักษณะนี้ ทั้งในรูปแบบที่เป็นกฎหมายหรือแนวทางปฏิบัติ (Soft Law) รวมไปถึงการสร้างความตระหนักให้ประชาชนทราบถึงภัยมาตรการป้องกัน และผลกระทบ ที่อาจเกิดจากการขโมยหรือการนำข้อมูลส่วนบุคคลไปใช้อย่างไม่ถูกต้อง เช่น ภัยจาก Spam หรือ Phising โดยการนำข้อมูลส่วนบุคคลที่ได้มาจากการเข้าถึงโดยไม่ชอบไปปลอมแปลงเป็นเจ้าของข้อมูล และอาจนำไปใช้เพื่อให้ได้ประโยชน์ทางการเงิน หรือร้ายแรงกว่านั้นคือการเข้าถึงเข้ามูลส่วนบุคคลและเปลี่ยนแปลงจนอาจทำให้ถึงอันตรายแก่ชีวิต เช่น การเข้าไปเปลี่ยนแปลงข้อมูลการวินิจฉัยของแพทย์หรือใบสั่งยา อย่างไรก็ตาม ภูมิภาคเอเชียและประเทศไทยเองยังคงมีความตระหนักถึงผลกระทบของภัยดังกล่าวอยู่ค่อนข้างน้อยและรู้สึกว่าเป็นเรื่องห่างไกลตัว ทั้งที่การดำเนินกิจวัตรประจำวันต่าง ๆ ถูกทำผ่านระบบคอมพิวเตอร์และ Social Network อยู่ตลอดเวลาและเมื่อกล่าวถึงคำว่า “สิทธิในความเป็นส่วนตัว” (Right of Privacy) หลายคนยังคงเข้าใจว่าเป็นเรื่องข้อมูลส่วนบุคคลเท่านั้น แต่เมื่อพิจารณาจากบทบัญญัติในรัฐธรรมนูญมาตรา 35 ซึ่งบัญญัติไว้ว่า

“สิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงตลอดจนความเป็นอยู่ส่วนตัว ย่อมได้รับความคุ้มครอง การกล่าวหรือไขข่าวแพร่หลายซึ่งข้อความหรือภาพไม่ว่าด้วยวิธีใดไปยังสาธารณชนอันเป็นการละเมิดหรือกระทบถึงสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียงหรือความเป็นอยู่ส่วนตัวจะกระทำมิได้ เว้นแต่เป็นกรณีที่เป็นประโยชน์ต่อสาธารณะ

บุคคลย่อมมีสิทธิได้รับความคุ้มครองจากการแสวงประโยชน์โดยมิชอบจากข้อมูลส่วนบุคคลที่เกี่ยวกับตน ทั้งนี้ตามที่กฎหมายบัญญัติ”

จะเห็นได้ว่าคำนี้มีความหมายกว้างครอบคลุมมากกว่าเรื่องข้อมูลส่วนบุคคล โดยอาจจำแนกออกได้เป็น 4 ด้าน ได้แก่ **ความเป็นส่วนตัวในการติดต่อสื่อสาร (Communication Privacy)** เป็นการให้ความคุ้มครองในความปลอดภัยและความเป็นส่วนตัวในการติดต่อสื่อสารทางจดหมาย โทรศัพท์ ไปรษณีย์อิเล็กทรอนิกส์ หรือวิธีการติดต่อสื่อสารอื่นใดที่ผู้อื่นจะล่วงรู้มิได้ **ความเป็นส่วนตัวในดินแดนหรืออาณาเขต (Territorial Privacy)** เป็นการกำหนดขอบเขตหรือข้อจำกัดที่บุคคลอื่นจะบุกรุกเข้าไปในสถานที่ส่วนตัวมิได้ ซึ่งรวมถึงการติดกล้องวงจรปิด การตรวจสอบรหัสประจำตัวบุคคลเพื่อการเข้าที่พักอาศัย **ความเป็นส่วนตัวในชีวิตร่างกาย (Bodily Privacy)** เป็นการให้ความคุ้มครองในชีวิตร่างกายของบุคคลในทางกายภาพที่จะไม่ถูกดำเนินการใด ๆ อันละเมิดความเป็นส่วนตัว เช่น การทดลองทางพันธุกรรม การทดลองยา เป็นต้น **ความเป็นส่วนตัวในข้อมูลข่าวสาร (Information Privacy)** หรือ “Data Protection” เป็นการให้ความคุ้มครองข้อมูลส่วนบุคคลโดยการวางหลักเกณฑ์เกี่ยวกับการเก็บรวบรวมและการบริหารจัดการข้อมูลส่วนบุคคล

โดยปัญหาการละเมิดสิทธิในความเป็นส่วนตัวนั้นอาจไม่ใช่เรื่องใหม่ โดยหากย้อนกลับไปจะเห็นได้ว่า องค์กรระหว่างประเทศและรัฐบาลในหลายประเทศได้พยายามผลักดันให้ประเทศต่าง ๆ สร้างกลไกการรับรองหรือคุ้มครองป้องกันการละเมิดสิทธิในความเป็นส่วนตัวผ่านการประกาศหรือทำข้อตกลงร่วมกัน ดังเช่น กรณีขององค์การสหประชาชาติที่ได้

มีการกำหนดเรื่องนี้ในมาตรา 12[33] แห่งปฏิญญาสากลว่าด้วยสิทธิมนุษยชน ค.ศ. 1948 (The Universal Declaration of Human Rights 1948) ที่บัญญัติไว้ว่า *"ไม่มีบุคคลใดที่จะถูกแทรกแซงในความเป็นส่วนตัว ครอบครัว บ้าน หรือการติดต่อระหว่างกัน หรือทั้งสิทธิในเกียรติยศ ชื่อเสียงของเขา ทุกคนย่อมมีสิทธิที่จะได้รับการคุ้มครองตามกฎหมายหากมีการถูกแทรกแซงเช่นว่านั้น"* เพื่อให้ประเทศสมาชิกมีการดำเนินมาตรการคุ้มครองสิทธิในความเป็นส่วนตัวของประชาชน

ส่วนของประเทศไทยเองในประเด็นการคุ้มครองข้อมูลส่วนบุคคล แม้ปัจจุบันจะมีกฎหมายหลายฉบับที่มีบทบัญญัติเกี่ยวกับข้อมูลส่วนบุคคล แต่ยังมีการกำหนดนิยามคำว่า "ข้อมูลส่วนบุคคล" ในบริบทที่แตกต่างกันออกไป ทำให้ยังขาดความเข้าใจร่วมกัน ซึ่งโดยทั่วไปแล้วข้อมูลส่วนบุคคลได้แก่ ข้อมูลที่สามารถเชื่อมโยงไปยังบุคคลนั้น ๆ ไม่ว่าทางตรงหรือทางอ้อม เช่น หมายเลขบัตรประจำตัวประชาชน นามสกุล เบอร์โทรศัพท์ ที่อยู่ รูปภาพ อีเมล ฐานะการเงิน ประวัติการศึกษา เป็นต้น ซึ่งข้อมูลเหล่านี้ปัจจุบันถูกนำไปใช้อย่างขาดความตระหนัก ดังนั้น สิ่งที่จำเป็นอย่างยิ่งประการหนึ่งคือการเร่งผลักดันร่างพระราชบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ซึ่งยังอยู่ระหว่างการพิจารณากว่า 10 ปี เพื่อให้มีกฎหมายกลางในการสร้างความสอดคล้องในเรื่องดังกล่าวและเป็นการสร้างความเชื่อมั่นให้แก่ประชาชนในการกำหนดมาตรการดูแลซึ่งต้องมีการเก็บรักษา การนำไปใช้ตามหลักเกณฑ์และมีความมั่นคงปลอดภัย ซึ่งทำให้หลายประเทศ เช่น มาเลเซีย และเกาหลีใต้ กำหนดให้หน่วยงานที่ทำหน้าที่ดูแลเรื่องข้อมูลส่วนบุคคลและดูแลเรื่องความมั่นคงปลอดภัยเป็นหน่วยงานเดียวกัน แต่สำหรับในสถานการณ์ปัจจุบันที่มีการนำระบบเทคโนโลยีสารสนเทศมาประยุกต์ใช้ในการดำเนินชีวิต ซึ่งแม้ว่าจะช่วยอำนวยความสะดวกสบายในหลาย ๆ ด้าน โดยเฉพาะการติดต่อสื่อสารที่สามารถเชื่อมต่อและแลกเปลี่ยนข้อมูลได้อย่างรวดเร็วและไร้พรมแดน ในที่นี้รวมถึงการติดต่อสื่อสารผ่านทางเครือข่ายสังคมออนไลน์ (Social Network) ที่กำลังได้รับความนิยมอย่างสูง ทำให้มีปริมาณข้อมูลมหาศาลซึ่งรวมถึงข้อมูลส่วนบุคคลของผู้ใช้งานต่าง ๆ ทำให้ปัญหาการละเมิดสิทธิในความเป็นส่วนตัวมีความรุนแรงมากกว่าในอดีตมาก เนื่องจากเทคโนโลยีสารสนเทศสามารถทำให้การแทรกแซงหรือการละเมิดสิทธิในความเป็นส่วนตัวทำได้ง่ายขึ้นโดยที่ผู้ที่ถูกละเมิดแทบจะไม่รู้ตัว และมีรูปแบบการกระทำละเมิดที่หลากหลาย ดังเช่นกรณีตัวอย่างตัวอย่างต่อไปนี้

1. กรณีสามบริษัทยักษ์ใหญ่โทรคมนาคมของสหรัฐอเมริกา คือ เบล์เซาธ์ เวอริซอน และเอทีแอนด์ที ถูกฟ้องจากประชาชน 26 ราย ใน 18 รัฐ เรียกค่าเสียหาย 200,000 ล้านดอลลาร์สหรัฐ ข้อหาละเมิดข้อมูลส่วนบุคคลด้วยการทำสัญญามอบข้อมูลการใช้โทรศัพท์ของลูกค้าให้สำนักงานความมั่นคงแห่งชาติ (NSA) ตามโครงการตามรอยทางโทรศัพท์เพื่อแกะรอยการซุ่มวางแผนของเครือข่ายก่อการร้ายโดยไม่ขออนุญาตจากประชาชน ซึ่งภารกิจของ NSA มีการดังฟังทางโทรศัพท์ วิทยุสื่อสาร การดักข้อมูลทางอินเทอร์เน็ตและการสื่อสารรูปแบบอื่น

2. กรณีการติดตามการใช้อินเทอร์เน็ตส่วนบุคคล เช่น โปรแกรม Cookies Web Bug Web Tracking Spy Ware มาตรการสอดส่องทางอินเทอร์เน็ตโดย Packet Sniffer Keystroke Loggers หรือระบบ Carnivore ของ FBI สหรัฐอเมริกา ซึ่งโปรแกรมเหล่านี้มีความสามารถที่ติดตามการใช้คอมพิวเตอร์ของบุคคลและดักข้อมูลทางอินเทอร์เน็ตได้ง่าย

3. กรณีพนักงานประกันสังคมประเทศไทยถูกไล่ออกจากงาน เนื่องจากการขายข้อมูลพนักงานบริษัท พนักงานโรงงานที่เป็นสมาชิกผู้ประกันตนให้บรรดาบริษัทรับจ้างติดตามทวงหนี้หรือบุคคลอื่นเพื่อประโยชน์

4. กรณีการสมัครบัตรเครดิตของสถาบันการเงิน ทั้งแบบ Bank และ Non-bank ซึ่งจะมีใบอนุญาตให้นำข้อมูลของลูกค้าไปเปิดเผยได้มาให้ลูกค้าดังกล่าวลงชื่ออนุญาต เมื่อสถาบันการเงินเหล่านั้นได้ข้อมูลของลูกค้าไปแล้ว จะนำไปขายต่อราคาประมาณ 1-1.5 บาทต่อรายชื่อลูกค้า สถาบันเหล่านั้นจะเป็นผู้คัดรายชื่อที่ตรงกับความต้องการของเจ้าของสินค้าแล้วทำการแนะนำสินค้านั้น ๆ ผ่านจดหมายที่แนบไปพร้อมใบแจ้งหนี้ที่ต้องส่งให้ลูกค้าทุกเดือน

5. กรณีการขายข้อมูลทางเว็บไซต์ ซึ่งเป็นข้อมูลราชการ คือ ทะเบียนประวัติอาชญากร ทะเบียนราษฎร หมายจับ และบริการติดตามพฤติกรรมเชิงชู้สาวที่โฆษณาว่ามีทั้งภาพนิ่งและวีดีโอ เพื่อเป็นหลักฐานในการดำเนินคดี หย่าหรือเรียกค่าเสียหาย การติดตามทวงหนี้ การตรวจสอบหมายเลขโทรศัพท์ย้อนหลังจากบริษัทเครือข่ายมือถือ ในเว็บดังกล่าวนอกจากข้อมูลต่าง ๆ แล้ว เว็บไซต์ดังกล่าวมีระบบตรวจสอบและป้องกันเจ้าหน้าที่ โดยกำหนดให้ผู้ติดต่อกลับของผู้จัดทำเว็บไซต์ซึ่งมีการแจ้งหมายเลขติดต่อที่เปิดบริการไว้ตลอด 24 ชั่วโมง และมีอัตราราคาบริการล้วงข้อมูลลับให้กับผู้ติดต่อขอซื้อบริการด้วย

6. การเฝ้าติดตามคุกคามทางอินเทอร์เน็ต (Cyber Stalking) เป็นการกระทำในลักษณะของการเฝ้าติดตาม ข่มขู่หรือรบกวนผู้อื่นทางอินเทอร์เน็ต เช่น การส่งอีเมล การโพสต์ข้อความหรือรูปภาพทางกระดานสนทนา (Webboard) หรือทางห้องสนทนา (Chat Room) หรือทางเว็บไซต์เครือข่ายสังคมต่าง ๆ เช่น Facebook Instagram Twitter เป็นต้น เพื่อให้ผู้ที่ถูกติดตามหรือบุคคลในครอบครัวเกิดความวิตกกังวล หวาดกลัวทั้งในด้านความปลอดภัยของทรัพย์สินและร่างกาย ซึ่งส่งผลกระทบต่อสภาพจิตใจและไม่สามารถใช้ชีวิตอย่างปกติสุขได้

นอกจากตัวอย่างข้างต้นแล้ว ยังมีรูปแบบการละเมิดสิทธิในความเป็นส่วนตัวอีกหลายรูปแบบ เช่น การโฆษณาหรือประชาสัมพันธ์ในลักษณะที่ก่อให้เกิดความเดือนร้อนรำคาญ การขโมยความเป็นตัวตน (Identity Theft) หรือการใช้สปายแวร์ (Spyware) เพื่อสอดแนมข้อมูลส่วนบุคคล การทำ E-mail Marketing หรือการทำการตลาดในรูปแบบอิเล็กทรอนิกส์ที่เป็นสแปม (Spam) ที่ก่อให้เกิดความเดือนร้อนรำคาญการฉ้อโกง (Fraud) การปลอมแปลงแอบอ้าง (Counterfeit) หรือกลายเป็นเป้าหมายของการทำสงครามข้อมูลข่าวสาร (Information Warfare) หรือการก่อการร้าย (Terrorism) ที่มุ่งกระทำกับฐานข้อมูลขนาดใหญ่ (Big Data) ของประชาชนในรัฐหนึ่งรัฐใด เป็นต้น

ดังนั้น จะเห็นได้ว่าปัญหาการใช้เทคโนโลยีสารสนเทศละเมิดสิทธิในความเป็นส่วนตัวของผู้อื่นมีแนวโน้มที่จะทวีความรุนแรงมากขึ้นและเป็นภัยคุกคามอีกประเภทหนึ่งที่น่าวิตกกังวลไม่ต่างจากภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งความเสียหายที่เกิดขึ้นจากภัยคุกคามนี้สามารถส่งผลต่อความปลอดภัยในชีวิตและทรัพย์สินของประชาชน และส่งผลกระทบต่อการใช้ชีวิตในสังคมอย่างปกติสุขได้ ทำให้ในหลายประเทศมีการกำหนดมาตรการป้องกันต่าง ๆ ที่เข้มข้นมากขึ้น ทั้งในด้านการออกกฎหมาย เช่น การออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล[34] การออกกฎหมายครอบคลุมฐานความผิดเหล่านี้มากขึ้น เป็นต้น หรือการส่งเสริมและสนับสนุนให้เกิดเป็นมาตรการทางสังคมเพื่อให้ประชาชนมีจิตสำนึกในการเคารพสิทธิในความเป็นส่วนตัวของผู้อื่น อย่างไรก็ดี เมื่อ

33 Article 12 of the Universal Declaration of Human Rights 1948 "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondance, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

34 องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา หรือ Organisation for Economic Co-operation and Development (OECD) มีการกำหนดหลักการสากลเป็นกรอบในการคุ้มครองข้อมูลส่วนบุคคลหรือข้อมูลส่วนตัว (Guidelines on the protection of Privacy and Transborder Data Flows of Personal Data) เพื่อให้ประเทศต่าง ๆ กำหนดเป็นมาตรฐานเดียวกัน รายละเอียดดูได้ที่ http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

พิจารณาถึงความตระหนักและการให้ความสำคัญต่อปัญหานี้ในประเทศไทยยังนับว่ามีไม่มากนัก แม้ว่าจะมีการรับรองหรือให้ความคุ้มครองสิทธิในความเป็นส่วนตัวโดยบัญญัติเป็นกฎหมายไว้ในหลายฉบับ เช่น รัฐธรรมนูญ มาตรา 35 พระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ที่กำหนดหลักเกณฑ์การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในการครอบครองของหน่วยงานรัฐ พระราชบัญญัติการประกอบธุรกิจข้อมูลเครดิต พ.ศ. 2545 ที่กำหนดการคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในการครอบครองของสถาบันการเงิน หรือพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 ที่มีประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. 2553 เป็นต้น แต่ในภาพรวมแล้วกฎหมายที่มีอยู่ยังไม่ครอบคลุมหน่วยงานทั้งหมดที่มีการจัดเก็บข้อมูลส่วนบุคคล รวมถึงกลไกการคุ้มครองข้อมูลส่วนบุคคลในกฎหมายหลายฉบับก็ยังไม่ชัดเจนและไม่เป็นไปตามมาตรฐานสากล

สำหรับภาครัฐนั้น เมื่อพิจารณาถึงการดำเนินการของหน่วยงานของรัฐตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง การคุ้มครองข้อมูลส่วนบุคคลก็พบว่ามีหน่วยงานที่ส่งแนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลให้คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตรวจพิจารณาไม่มากนัก ทั้งที่เมื่อประเมินจากปริมาณการครอบครองข้อมูลส่วนบุคคลของภาครัฐจะพบว่าหน่วยงานส่วนใหญ่มีการจัดเก็บข้อมูลของประชาชนไว้ค่อนข้างมาก ซึ่งหากมีภัยคุกคามหรือข้อผิดพลาดเกิดขึ้นแล้วก็อาจส่งผลต่อประเทศในภาพรวมได้

ปัญหาเหล่านี้จึงเป็นปัญหาที่ทุกภาคส่วนต้องหันมาให้ความสำคัญและร่วมมือกันอย่างจริงจัง โดยภาครัฐต้องมีมาตรการที่ให้ความคุ้มครองสิทธิในความเป็นส่วนตัวแก่ประชาชนอย่างทั่วถึง ส่วนภาคเอกชนก็อาจมีการนำนโยบายกำกับดูแลตัวเอง (Self-Regulation) ด้วยการส่งเสริมให้ผู้ใช้เว็บไซต์เครือข่ายสังคมตระหนักถึงความสำคัญของสิทธิในความเป็นส่วนตัว หรือการใช้มาตรการทางเทคนิคต่าง ๆ เช่น การปรับตั้งค่าความเป็นส่วนตัว (Setting Privacy) ในเว็บไซต์เครือข่ายสังคม เพื่อลดปัญหาการละเมิดสิทธิในความเป็นส่วนตัว และสุดท้ายคือภาคประชาชนเองที่ต้องตระหนักรู้และให้ความสำคัญกับสิทธิในความเป็นส่วนตัวของบุคคลอันเป็นสิทธิขั้นพื้นฐานของตนเอง หากได้รับความร่วมมือจากทุกภาคส่วนแล้ว ก็จะช่วยให้มาตรการต่าง ๆ ในการนำมาใช้ป้องกันปัญหาการละเมิดสิทธิในความเป็นส่วนตัวมีประสิทธิภาพมากยิ่งขึ้น และลดความเสียหายที่จะเกิดขึ้นต่อประชาชนและประเทศไทยได้

7

ประเทศไทยพร้อมหรือยัง
กับภัยคุกคามที่เกิดขึ้น

7. ประเทศไทยพร้อมหรือยังกับภัยคุกคามที่เกิดขึ้น

นับจากไทยเซิร์ตได้เริ่มดำเนินการภายใต้ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไทยเซิร์ตได้รับแจ้งเหตุภัยคุกคามผ่านสองช่องทาง คือ การรับข้อมูลภัยคุกคามด้านสารสนเทศอัตโนมัติ จากหน่วยงานเครือข่ายความร่วมมือ และการรับแจ้งจากบุคคลทั่วไปทางอีเมล โดยสถิติข้อมูลได้ชี้ให้เห็นว่า ปัญหาสำคัญด้านความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) เกิดจากการขาดความตระหนักหรือความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยแบ่งเป็นระดับต่าง ๆ ได้แก่

ระดับผู้ดูแลระบบ ปัญหาที่เกิดกับระบบเครื่องแม่ข่ายของหน่วยงานถูกโจมตี และใช้เป็นฐานกระทำความผิด หรือใช้เป็นเครื่องมือในการดำเนินกิจกรรมที่ไม่พึงประสงค์ต่าง ๆ เช่น ส่งสแปมเมล โจมตีระบบคอมพิวเตอร์หรือระบบเครือข่ายอื่นเพื่อวัตถุประสงค์ทำให้บริการผู้อื่นเกิดความขัดข้อง หรือใช้ติดตั้งบริการเพื่อวัตถุประสงค์ในการฉ้อโกงนั้น เป็นต้น มักจะมีสาเหตุมาจากผู้ดูแลระบบคอมพิวเตอร์ไม่ได้บริหารจัดการระบบเครื่องแม่ข่ายให้มีความมั่นคงปลอดภัย ไม่ได้ติดตามและปรับปรุงซอฟต์แวร์ให้ทันสมัยเพื่อแก้ไขปัญหาช่องโหว่ (Vulnerability) เป็นเหตุให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงระบบโดยไม่ได้รับอนุญาต และใช้ระบบเครื่องแม่ข่ายนั้นเป็นฐานในการทำกิจกรรมไม่พึงประสงค์

ระดับผู้ใช้งานทั่วไป ปัญหาที่เกิดกับเครื่องคอมพิวเตอร์สำหรับผู้ใช้งานทั่วไป มีซอฟต์แวร์ไม่พึงประสงค์ติดตั้งอยู่ส่วนใหญ่เป็นผลมาจากผู้ใช้งานใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ ทำให้ไม่สามารถปรับปรุงซอฟต์แวร์ให้ทันสมัยเพื่อแก้ไขปัญหาช่องโหว่ (Vulnerability) ประกอบกับผู้ใช้งานขาดความตระหนักด้านความมั่นคงปลอดภัยและมีพฤติกรรมเสี่ยงต่าง ๆ เช่น เข้าเว็บไซต์โดยไม่ตรวจสอบความน่าเชื่อถือของเว็บไซต์ หรือการเปิดโปรแกรมที่ดาวน์โหลดมาจากเว็บไซต์หรืออีเมลโดยมิได้ตรวจสอบความน่าเชื่อถือของโปรแกรมดังกล่าว เป็นต้น ทำให้ได้รับโปรแกรมไม่พึงประสงค์มาทำงานอยู่ในเครื่อง และในบางกรณีส่งผลต่อเครื่องให้ถูกควบคุมโดยผู้ไม่ประสงค์ดีเพื่อทำกิจกรรมต่าง ๆ เช่น ส่งสแปมเมล หรือถูกดักรับข้อมูลที่พิมพ์บนหน้าจอหรือที่ส่งผ่านเว็บไซต์ เป็นต้น

จะเห็นได้ว่า ปัญหาสถานการณ์ด้านความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ ไม่ว่าจะเป็นระบบเครื่องแม่ข่ายหรือเครื่องคอมพิวเตอร์ที่ใช้งานทั่วไป ถือเป็นตัวนำไปสู่เหตุภัยคุกคามด้านสารสนเทศได้ทุกรูปแบบ ในทุกระดับตั้งแต่ระดับบุคคล ระดับหน่วยงาน ระดับประเทศ หรือระดับโลก เช่น กรณีระบบเครื่องแม่ข่ายในประเทศไทยถูกเจาะระบบและใช้เป็นเครื่องให้บริการเว็บไซต์หลอกลวงเพื่อวัตถุประสงค์ในการฉ้อโกงลูกค้าของสถาบันการเงิน หรือ ฟิชชิ่ง (Phishing) มักเกิดจากผู้ดูแลระบบเครื่องแม่ข่ายไม่ติดตั้งระบบปฏิบัติการหรือซอฟต์แวร์ให้มีความมั่นคงปลอดภัย ปิดพอร์ตบริการที่ไม่จำเป็น ประกอบกับความละเลยที่จะปรับปรุงซอฟต์แวร์ในระบบให้ทันสมัยอยู่เสมอเพื่อแก้ไขปัญหาช่องโหว่ ซึ่งเป็นช่องทางให้ผู้ไม่ประสงค์ดีเจาะเข้ามาใช้เป็นฐานในการสร้างเว็บไซต์หลอกลวงหรือฟิชชิ่ง

ภัยคุกคามด้านสารสนเทศ (Threat) เหล่านี้จะทวีความรุนแรงมากขึ้นหากไม่มีการสร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับบุคลากรในทุกระดับ เนื่องจากเทคโนโลยีที่พัฒนาอย่างต่อเนื่องและรวดเร็วพร้อม ๆ กับแนวโน้มของการใช้อุปกรณ์อิเล็กทรอนิกส์เคลื่อนที่และพกพาอย่างแพร่หลายเสมือนการใช้สินค้าอุปโภคบริโภคทั่วไป (Consumerization) ประกอบกับแนวโน้มของการใช้อุปกรณ์อิเล็กทรอนิกส์ส่วนตัวในสถานที่ทำงาน (Bring Your Own Device: BYOD) และภัยคุกคามด้านสารสนเทศที่มีความซับซ้อนมากขึ้นตามการเปลี่ยนแปลงของเทคโนโลยีที่เกิดขึ้น ไม่เพียงส่งผลกระทบในเชิงความมั่นคงปลอดภัยด้านสารสนเทศ (การรักษาความลับ การรักษาความครบถ้วนสมบูรณ์ และการรักษาสภาพพร้อมใช้) แต่ยังส่งผลกระทบต่อข้อมูลส่วนบุคคลอีกด้วย

ในการสร้างภูมิคุ้มกันด้านความมั่นคงปลอดภัยสารสนเทศของประเทศให้มีความเข้มแข็ง ประเทศไทยจำเป็นต้องเตรียมการในด้านต่าง ๆ ที่สำคัญ ดังนี้

พัฒนาโครงสร้างพื้นฐานที่จำเป็น
■ สร้างและพัฒนาศักยภาพของบุคลากรด้านความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) ให้เป็นผู้เชี่ยวชาญที่ได้รับการยอมรับในระดับสากล และสร้างความตระหนักให้กับผู้ใช้งานเพื่อให้ไม่ตกเป็นเครื่องมือหรือช่องทางในการโจมตีระบบ
■ พัฒนากฎหมายเพื่อเอื้อให้เกิดสภาพแวดล้อมสำหรับเจ้าหน้าที่พนักงานในสายตำรวจ สายยุติธรรม และพนักงานเจ้าหน้าที่ตามกฎหมายที่เกี่ยวข้องกับการกระทำผิดทางคอมพิวเตอร์สามารถดำเนินการป้องปรามและอื่น ๆ ที่จำเป็นต่ออาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นในประเทศได้อย่างมีประสิทธิภาพ
การเตรียมความพร้อม
■ ส่งเสริมให้มีการดำเนินการวิจัยและพัฒนาด้านความมั่นคงปลอดภัยด้านสารสนเทศ (IT Security) เพื่อให้สามารถรับมือกับภัยคุกคามด้านสารสนเทศ ในรูปแบบใหม่ ๆ ที่เกิดขึ้น และลดการพึ่งพาเทคโนโลยีด้านความมั่นคงปลอดภัยไซเบอร์จากต่างประเทศ
■ สร้างความเข้มแข็งของหน่วยงานหรือองค์กรที่มีภารกิจในการรับมือและจัดการสถานการณ์ภัยคุกคามด้านสารสนเทศ
■ การจัดเตรียมหน่วยงานหรือองค์กรเพื่อสนับสนุนหน่วยงานสำคัญภายในประเทศ ในด้านปฏิบัติการรับมือกับภัยคุกคามด้านสารสนเทศ และภัยคุกคามด้านสารสนเทศ อุบัติใหม่ด้านการสื่อสารและโทรคมนาคม เพื่อรองรับ แผนแม่บทความมั่นคงปลอดภัยด้านสารสนเทศของชาติ ในการกำหนดทิศทางและบรูณการในการดำเนินการของหน่วยงานทั้งภาครัฐและเอกชนในการรับมือและตอบสนองต่อภัยคุกคามด้านสารสนเทศที่เกิดขึ้น
■ สร้างความเข้มแข็งในด้านความร่วมมือกับหน่วยงานในต่างประเทศเพื่อตอบสนองและแก้ไขเหตุภัยคุกคามด้านสารสนเทศ ที่พบว่าโจมตีระบบสารสนเทศของหน่วยงานในประเทศ
■ เตรียมความพร้อมสู่การเริ่มต้นประชาคมอาเซียน เพื่อสร้างศักยภาพและความสามารถในการแข่งขันให้กับประเทศ
การบูรณาการ
■ การบูรณาการในการดำเนินการเพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยของระบบสารสนเทศ (IT Security) ให้กับผู้ใช้งานหรือในกลุ่มผู้บริโภคของบริการโทรคมนาคม ของหน่วยงานด้านนโยบาย หน่วยงานผู้ควบคุมกิจการโทรคมนาคม และหน่วยงานอื่น ๆ ที่เกี่ยวข้อง
■ กระบวนการในการรับมือภัยคุกคามด้านสารสนเทศ ที่เกิดจากการบูรณาการทำงานในทุกภาคส่วน เพื่อให้เกิดการประสานงานอย่างมีเอกภาพในการรับมือและจัดการสถานการ์ณภัยคุกคามด้านสารสนเทศ

จากประเด็นที่เสนอให้มีการเตรียมความพร้อมของประเทศข้างต้น การดำเนินงานที่ควบคู่กันไปในปัจจุบัน ได้มีความพยายามในการผลักดันการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อเป็นไปตามมาตรฐานเป็นที่ยอมรับในระดับสากล ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ซึ่งมีหน่วยงานที่ผ่านความเห็นชอบจากคณะกรรมการในการจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ ตั้งแต่ปี 2533 จนถึงปี 2555 จำนวน 56 หน่วยงาน (ข้อมูล ณ วันที่ 26 ธันวาคม 2555) สำหรับการดำเนินงานของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร ในฐานะหน่วยงานสำคัญในการผลักดันให้มีการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ให้เกิดประโยชน์ในทุกภาคส่วนนั้น ภายใต้การผลักดันของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (ซึ่งเป็นสำนักงานที่ทำหน้าที่เป็นหน่วยงานธุรการและเป็นเลขานุการคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยมีสพธอ.ทำหน้าที่สนับสนุนกรรมการธุรกรรมในการดำเนินงาน) จึงได้มีมาตรการผลักดันให้หน่วยงานภาครัฐมีการจัดทำแนวนโยบายและแนวปฏิบัติฯ ทั้งในรูปแบบการเสนอแนะแนวทาง การจัดสัมมนาเพื่อเผยแพร่แนวทางการดำเนินงานดังกล่าว ซึ่งถือเป็นการเริ่มดำเนินงานภายในหน่วยงานให้เกิดมาตรฐานเป็นที่ยอมรับมากขึ้น แต่เพียงการดำเนินงานในเรื่องดังกล่าว อาจจะไม่เพียงพอ จึงนำไปสู่การแต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติขึ้น โดยมีนายกรัฐมนตรีเป็นประธาน เพื่อพิจารณาการยกร่างกรอบนโยบายเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและแผนแม่บทการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตลอดจนการบูรณาการข้อมูลและความร่วมมือระหว่างหน่วยงานในภาคส่วนต่าง ๆ แต่ความท้าทายที่พบในปัจจุบัน คือ คนส่วนใหญ่ยังขาดองค์ความรู้และความตระหนักตั้งแต่ในระดับผู้บริหารเชิงนโยบาย จนถึงระดับปฏิบัติการ เพราะเมื่อใดที่คนขาดความตระหนัก ก็ยากที่จะรับมือกับภัยคุกคามที่อาจจะเกิดขึ้นได้ทุกเวลาอย่างทันท่วงที เนื่องจากทรัพยากรทางด้านบุคคลถือเป็นกลไกสำคัญในการป้องกันและรับมือกับสถานการณ์ที่อาจจะเกิดขึ้น รวมถึงต้องรู้เท่าทัน เพื่อการดูแลเกี่ยวกับปัญหาเฉพาะหน้าที่จะเกิดขึ้น อันจะนำไปสู่การลดความเสี่ยง ซึ่งไม่เพียงแต่หน่วยงานภาครัฐ หรือภาคเอกชนเท่านั้น แต่ยังรวมไปถึงการมีส่วนร่วมกับภาคสังคมมากขึ้น เพื่อผลักดันให้เกิดการดำเนินงานในภาคสาธารณะ และการเผยแพร่ข้อมูลที่เป็นประโยชน์ผ่านช่องทางต่าง ๆ ได้มากขึ้น

สิ่งเหล่านี้ เป็นการแสดงให้เห็นถึงความสำคัญของทรัพยากรทางด้านบุคคล ที่ประเทศไทยต้องเร่งในการสร้างและพัฒนาศักยภาพของคนให้เพิ่มมากขึ้น ทั้งการตั้งรับ ป้องกัน ปราบปราม และการส่งเสริมให้เกิดการทำงานร่วมกับคนในหลายกลุ่ม เพื่อสร้างความเข้าใจในปัญหาเพื่อช่วยเหลือประชาชน

วันนี้ สพธอ. จึงได้ยกระดับการทำงานของ “ไทยเซิร์ต” ให้เป็นการทำงานเชิงรุกและมีเป็นกลไกหนึ่งที่สำคัญในการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ในช่วงระยะเวลา 4 ปี ซึ่งถือเป็นระยะแรกตั้งของ สพธอ. เพื่อเป็นกลไกในการเตรียมความพร้อมของประเทศไทยในการรับมือกับปัญหาสถานการณ์ภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ รวมถึงการสร้างเครือข่ายความร่วมมือให้เกิดขึ้นทั้งในประเทศและต่างประเทศที่ไม่เพียงแต่ในอาเซียน แต่ไทยเซิร์ต สพธอ. ยังขยายเครือข่ายไปยังประเทศต่าง ๆ ทั่วโลก ซึ่งสิ่งเหล่านี้ ถือเป็นแนวทางการดำเนินงานสำคัญที่ ไทยเซิร์ต สพธอ. มุ่งผลักดันเพื่อให้ประเทศไทยมีความพร้อมอย่างจริงจังกับการรับมือภัยคุกคามในทุกรูปแบบอย่างแท้จริง

ทั้งนี้ข้อมูลสถิติที่ปรากฏในตารางต่างๆในบทที่ 4 ข้างต้นนั้น เป็นเพียงจำนวนรายงานมัลแวร์ ยูอาร์แอล 10 อันดับแรกหรือ Malicious Code อันเป็นโปรแกรมไม่พึงประสงค์ที่ไทยเซิร์ตได้รับแจ้ง โดยที่มัลแวร์ หรือ Malicious Code ที่ตรวจพบนั้นอาจปรากฏในเครื่องคอมพิวเตอร์ของลูกค้าที่มาใช้บริการเครือข่าย ดังนั้นจึงมิได้สะท้อนหรือบงชี้ชัดว่าระดับความมั่นคงปลอดภัยของระบบเครือข่ายของผู้ให้บริการนั้นๆ ไม่มั่นคงปลอดภัยแต่อย่างใด

8

ภาคผนวก

8. ภาคผนวก

8.1 ภาคผนวก ก

การจัดประเภทของเหตุภัยคุกคามด้านสารสนเทศ

ตามแนวทางของเครือข่ายความร่วมมือหน่วยงานรับมือภัยคุกคามด้านสารสนเทศในโครงการอีซีเสิร์ตดอทเน็ต (eCSIRT.net) กำหนดให้มีเหตุภัยคุกคามด้านสารสนเทศ 8 ประเภท ในกรณีที่เหตุภัยคุกคามด้านสารสนเทศหนึ่ง ๆ อาจถูกจัดอยู่ได้ในหลายประเภท ให้จัดอยู่ในประเภทภัยคุกคามด้านสารสนเทศ ที่เป็นหลักเพียงอย่างเดียว เช่น ในกรณีที่มีการบุกรุกเข้าระบบ และผู้บุกรุกเข้าถึงระบบได้ในบทบาทผู้ดูแลระบบ (Root Privileges) ทำให้เข้าถึงข้อมูลสำคัญได้หลายชุด นั้น ให้จัดเหตุภัยคุกคามด้านสารสนเทศ นี้อยู่ในประเภทการบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusion) แบบ Privileged Account Compromise รายละเอียดการแบ่งประเภทเหตุภัยคุกคามด้านสารสนเทศของอีซีเสิร์ตดอทเน็ต (eCSIRT.net) ปรากฏในตารางที่ 26

ตารางที่ 28 การแบ่งประเภทเหตุภัยคุกคามด้านสารสนเทศ
ตามอีซีเสิร์ตดอทเน็ต (eCSIRT.net)

Incident Class (mandatory input field)	**Incident Type** (optional but desired input field)	**Description / Examples**
Abusive Content	Spam	or “Unsolicited Bulk Email”, this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having an identical content.
	Harassment	Discreditation or discrimination of somebody (i.e. Cyberstalking)
	Child/Sexual/Violence/	Child Pornography, glorification of violence
Malicious Code	Virus	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code.
	Worm	
	Trojan	
	Spyware	
	Dialer	

Incident Class (mandatory input field)	Incident Type (optional but desired input field)	Description / Examples
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points. This includes also some kind of testing processes to gather information about hosts, services and accounts. Examples: fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT)
	Sniffing	Observing and recording of network traffic (wiretapping).
	Social Engineering	Gathering information from a human being in a non-technical way (e.g. lies, tricks, bribes, or threats).
Intrusion Attempts	Exploiting of known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g. buffer overflow, backdoors, cross side scripting, etc.).
	Login attempts	Multiple login attempts (Guessing / cracking of passwords, brute force).
	new attack signature	An attempt using an unknown exploit.
Intrusions	Privileged Account Compromise	A successful compromise of a system or application (service). This can have been caused remote by a known or new vulnerability, but also by an unauthorized local access.
	Unprivileged Account Compromise	
	Application Compromise	
Availability	DoS	By this kind of an attack a system is bombarded with so many packets that the operations are delayed or the system crashes. Examples of a remote DoS are SYS- a. PING- flooding or E-mail bombing (DDoS: TFN, Trinity, etc.). However, the availability also can be affected by local actions (destruction, disruption of power supply, etc.).
	DDoS	
	Sabotage	
Information Security	Unauthorised access to information	Besides a local abuse of data and systems the information security can be endangered by a successful account or application compromise. Furthermore attacks are possible that intercepts and access information during transmission (wiretapping, spoofing or hijacking).
	Unauthorised modification of information	
Fraud	Unauthorized use of resources	Using resources for unauthorized purposes including profit-making ventures (E.g. the use of e-mail to participate in illegal profit chain letters or pyramid schemes).
	Copyright	Selling or Installing copies of unlicensed commercial software or other copyright protected materials (Warez).
	Masquerade	Type of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it.
Other	All incidents which don't fit in one of the given categories should be put into this class.	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.

หมายเหตุ

(http://www.ecsirt.net/cec/service/documents/wp4-pub-userguide-v10.html ข้อมูล ณ วันที่ 10 กันยายน 2555)

8.2 ภาคผนวก ข

ตารางที่ 29 อภิธานศัพท์และคำย่อ

คำศัพท์	ความหมาย
เนื้อหาที่เป็นภัย (Abusive Content)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือ เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (SPAM)
โปรแกรมไม่พึงประสงค์ (Malicious Code)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากโปรแกรมหรือชุดคำสั่งที่ถูกพัฒนาขึ้นด้วยความประสงค์ร้าย (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์นี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) หรือ สปายแวร์ (Spyware) ต่าง ๆ
ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempt) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ ภัยคุกคามด้านสารสนเทศ นี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามด้านสารสนเทศ ที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามด้านสารสนเทศ อาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่นการโจมตีประเภท DoS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
การฉ้อฉล (Fraud)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากการฉ้อโกง (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
ภัยคุกคามด้านสารสนเทศ อื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	ภัยคุกคามด้านสารสนเทศ ประเภทอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามด้านสารสนเทศ ประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่น ๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามด้านสารสนเทศ นี้ใหม่

คำศัพท์	ความหมาย
ดีดอส(DDoS)	เป็นเทคนิคในการโจมตีสภาพความพร้อมใช้งานของระบบ โดยอาศัยแหล่งโจมตีจากหลายที่ภายในช่วงเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ยกตัวอย่างเช่นการโจมตีเครื่องแม่ข่ายด้วยการส่งคำสั่งขอใช้บริการจากเครื่องคอมพิวเตอร์จำนวนมาก ๆ พร้อม ๆ กัน จนเกิดความสามารถที่เครื่องแม่ข่ายนั้นจะให้บริการได้
บรูทฟอร์ส (Brute Force)	เป็นเทคนิคในการโจมตีด้วยการพยายามสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้น หรือเลือกใช้ เพื่อให้ได้มายังซึ่งข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น การสุ่มชื่อบัญชีผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเข้าสู่ระบบ หรือในบางครั้งผู้โจมตีอาจใช้เพื่อสแกนหาไฟล์สำคัญของเว็บไซต์ ซึ่งการโจมตีในลักษณะนี้จะได้ผลกับระบบที่มีการตั้งค่าความปลอดภัยอย่างไม่เหมาะสม เช่น การตั้งบัญชีผู้ใช้งานและรหัสผ่านที่ง่ายต่อการคาดเดา แนวทางการป้องกันการโจมตีอาจทำได้โดยการใช้งานโมดูลแคปชา (Captcha) บนเว็บไซต์ ซึ่งเป็นเทคนิคที่ช่วยยืนยันว่าการส่งข้อมูลเข้ามายังระบบดังกล่าวเป็นผู้ใช้งานจริง ไม่ใช่โปรแกรมคอมพิวเตอร์ หรือการใช้งานโปรแกรมประเภทแอนตี้บรูทฟอร์ส (Anti Brute Force) บนระบบปฏิบัติการ
ฟิชชิ่ง (Phishing)	เป็นเทคนิคในการโจมตีในลักษณะฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ ส่วนใหญ่มีวัตถุประสงค์ในการขโมยข้อมูลสำคัญของผู้ใช้งานของ เช่น บัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลสำคัญทางธุรกรรมอิเล็กทรอนิกส์ เป็นต้น ผู้โจมตีจะโจมตีด้วยวิธีการล่อลวงให้ผู้ใช้งานใช้บริการของระบบที่ปลอมแปลงขึ้น โดยที่ผู้ใช้งานไม่ทราบว่ากำลังใช้งานระบบปลอมแปลงนั้นอยู่ ช่องทางที่ผู้โจมตีใช้ มีอยู่หลากหลายช่องทางเช่น การส่งอีเมล การส่งข้อความสั้น (Messaging) หรือ การใช้สื่อสังคม (Social Media) เป็นต้น
บอตเน็ต (Botnet)	เป็นมัลแวร์ที่สามารถถูกควบคุมจากผู้โจมตีให้กระทำการต่าง ๆ ในลักษณะที่เป็นอันตรายเช่น โจมตีระบบเครือข่าย หรือการขโมยข้อมูลที่เป็นความลับของเครื่องที่มีมัลแวร์ติดตั้งอยู่ เป็นต้น
รุสต็อค (Rustock)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีความสามารถในการโจมตีในลักษณะดีดอส (DDoS) และเป็นมัลแวร์ที่มีบทบาทสำคัญในการส่งอีเมลสแปม (Spam) ซึ่งจากสถิติพบว่ามัลแวร์ชนิดนี้สามารถส่งอีเมลสแปม (Spam) ได้มากกว่า 25,000 ฉบับต่อชั่วโมง จากข้อมูลของบริษัทไมโครซอฟท์ พบว่ามีผู้ตกเป็นเหยื่อของมัลแวร์รุสต็อค (Rustock) ประมาณ 2.5 ล้านเครื่องทั่วโลก
เคลิฮอส (Kelihos)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีความสามารถในการโจมตีในลักษณะดีดอส (DDoS) และใช้ในการส่งอีเมลสแปม (Spam)
เฟโอโด (Feodo)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
ดีดอสเดิร์ทจัมเปอร์ (Ddos_dirt-jumper)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีความสามารถในการโจมตีในลักษณะดีดอส (DDoS)
ดีดอสข่าน (Ddos_khan)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีความสามารถในการโจมตีในลักษณะดีดอส (DDoS)

คำศัพท์	ความหมาย
คอนฟิกเกอร์ (Conficker)	เป็นมัลแวร์ประเภทเวิร์ม (Worm) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์ในการก่อกวนหรือทำลายความพร้อมในการใช้งานของระบบ เช่น การทำให้ผู้ใช้ไม่สามารถล็อกอินเข้าระบบปฏิบัติการได้ การปิดฟังก์ชันวินโดวส์ อัพเดท (Windows update) อัตโนมัติ การปิดโปรแกรมวินโดว ดีเฟนเดอร์ (Window Defender) และยังทำให้การใช้งานเน็ตเวิร์ก (Network) ตอบสนองช้า เป็นต้น สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในระบบเครือข่ายโดยผ่านระบบเน็ตเวิร์กแชร์ (Network share) และใช้วิธีโจมตีผ่านช่องโหว่ (MS08-067) โดยตรง
ซุส (Zeus)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
วิรัท (Virut)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักเพื่อใช้ดาวน์โหลดและติดตั้งมัลแวร์อื่น ๆ ลงในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์นี้
ทีดีเอสเอส (Tdss)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักเพื่อใช้ดาวน์โหลดและติดตั้งมัลแวร์อื่น ๆ ลงในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์นี้
เวิร์มบอยเบิร์ก(Worm_boinberg)	เป็นมัลแวร์ประเภทเวิร์ม (Worm) ที่ติดในระบบปฏิบัติการวินโดวส์ ถูกควบคุมผ่าน ไออาร์ซี เซิร์ฟเวอร์ (IRC Server โดยทั่วไปจะมีการแพร่กระจายผ่านซอฟต์แวร์ วินโดส์ไลฟ์เมสเซนเจอร์ (Windows Live Messenger) ยูเอสบี ไดรฟ์ (USB drives) และ ฝังตัวผ่านไฟล์ที่มีการบีบอัด เช่น แรร์ (RAR) ซิพ (ZIP) โดยเครื่องที่ติดมัลแวร์จะมีผลกระทบให้เครื่องทำงานช้าลง ถูกขโมยข้อมูลสำคัญไม่ว่าจะเป็นชื่อบัญชีผู้ใช้ รหัสผ่าน เป็นต้น
ทอร์พิก (Torpig)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
คาร์เบิร์บ (Carberp)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
สปายอาย (Spyeye)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
แรมนิท (Ramnit)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ ถูกพบเมื่อปี 2010 ในช่วงแรกเป็นมัลแวร์ที่มีการแพร่กระจายผ่านยูเอสบีไดร์ฟ (USB drive) และยังไม่มีความสามารถที่เป็นอันตรายมากนัก แต่ในปัจจุบันมีการปรับปรุงให้มีความสามารถในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งานด้วย
โกซิ (Gozi)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีจุดประสงค์หลักในการขโมยข้อมูลด้านธุรกรรมออนไลน์ของผู้ใช้งาน
จีบอต (Gbot)	เป็นมัลแวร์ประเภทบอตเน็ต (Botnet) ที่ติดในระบบปฏิบัติการวินโดวส์ มีความสามารถในการโจมตีในลักษณะดีดอส (DDoS) และยังสามารถใช้เพื่อดาวน์โหลดและติดตั้งมัลแวร์อื่น หรือหลอกลวงลักษณะการฉ้อฉล (fraud) แอบโจมตีผู้อื่นทางคอมพิวเตอร์ ที่ติดมัลแวร์นี้ด้วย

คำศัพท์	ความหมาย
ซีแอนด์ซีเซริฟเวอร์ (C&C Server)	ย่อมาจากซีแอนซีเซิร์ฟเวอร์ (Command & Control Server) คือเครื่องที่ใช้ควบคุมเครื่องที่ติดมัลแวร์ประเภทบอตเน็ต (Botnet) ให้กระทำการต่าง ๆ ตามที่ผู้โจมตีต้องการเช่น สั่งให้โจมตีเครื่องอื่น ๆ ในลักษณะดีดอส (DDoS) สั่งให้เครื่องที่ติดบอตเน็ต (Botnet) ส่งข้อมูลสำคัญมาให้กับผู้ควบคุม เช่น บัญชีผู้ใช้ รหัสผ่าน โดยลักษณะการเชื่อมต่อระหว่างแอนซีเซิร์ฟเวอร์ (C&C Server) และบอตเน็ต (Botnet) มีหลากหลายรูปแบบ เช่น การเชื่อมต่อผ่านโพรโตคอลไออาร์ซี (IRC) เอชทีทีพี (HTTP) หรือในลักษณะพีทูพี (P2P) เป็นต้น
โดเมนเนม (Domain Name)	เป็นชื่อที่ตั้งขึ้นเพื่อใช้แทนการเรียกหมายเลขไอพี (IP Address) เพื่อให้เป็นที่รู้จักและจดจำได้ง่ายขึ้น
คอร์ปอเรต (Corporate)	เป็นเครือข่ายที่ให้บริการอินเทอร์เน็ตกับหน่วยงาน หรือองค์กรที่มีหมายเลขไอพี (IP Adrdress) คงที่ โดยทั่วไปจะมีระบบเครือข่ายและสารสนเทศภายในจำนวนมาก และมีผู้ดูแลระบบประจำหน่วยงาน
บรอดแบนด์ (Broadband)	เป็นเครือข่ายที่ให้บริการอินเทอร์เน็ตกับผู้ใช้ทั่วไป มีการระบุหมายเลขไอพี (IP Address) กับเครื่องที่เป็นลักษณะไดนามิกไอพี (Dynamic IP) ซึ่งหมายเลขไอพี (IP Address) จะเปลี่ยนแปลงไปได้ตามเงื่อนไขที่ผู้ให้บริการกำหนด ผู้ใช้เครือข่ายแบบนี้ส่วนมากจะเป็นผู้ใช้บริการตามบ้าน หรือสำนักงานขนาดเล็กที่มีผู้ใช้บริการจำนวนน้อย
สตอร์มเวิร์ม (Storm Worm)	ภัยคุกคามด้านสารสนเทศ จากโปรแกรมไม่พึงประสงค์ในลักษณะเวิร์ม (Worm) ซึ่งมีความสามารถในการแพร่กระจายได้ด้วยตัวเองด้วยส่งโปรแกรมไม่พึงประสงค์พร้อมกับสแปมเมล (Spam mail) สตอร์มเวิร์ม (Storm Worm) มีลักษณะการทำงานในแบบรูปแบบบอตเน็ต (Botnet) ต่างกันที่บอตเน็ตทั่วไปมีโครงสร้างการทำงานที่มีเครื่องที่ทำหน้าที่ควบคุมและสั่งการ แต่สตอร์มเวิร์มทำงานในลักษณะเป็นเครือข่ายเพียร์-ทู-เพียร์ peer-to-peer

8.3 ภาคผนวก ค

กฎหมายอนุบัญญัติที่มีมาตรการเกี่ยวกับความมั่นคงปลอดภัย

กฎหมาย	กลไกการบังคับใช้กฎหมาย			หลักการ
	กำกับ	ป้องกัน	ปราบปราม	
ประมวลกฎหมายอาญา หมวด ๕ ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์			√	เนื่องจากปัจจุบันการใช้เอกสารวัตถุอื่นใดหรือข้อมูลที่จัดทำขึ้นในลักษณะบัตรอิเล็กทรอนิกส์ เช่น บัตรเครดิต บัตรเดบิต โดยมีวัตถุประสงค์เพื่อ ประโยชน์ในการชำระค่าสินค้า ค่าบริการ หรือหนี้อื่น เพิ่มปริมาณและประเภทการใช้งาน อย่างแพร่หลาย และปรากฏว่ามีการกระทำความผิด เกี่ยวกับบัตรและลักลอบนำข้อมูลอิเล็กทรอนิกส์ของผู้อื่นมาใช้อันส่งผลกระทบต่อเศรษฐกิจและผู้บริโภคในวงกว้าง จึงสมควรกำหนดความผิดอาญาสำหรับการกระทำ ความผิดเกี่ยวกับบัตรและข้อมูลอิเล็กทรอนิกส์เพื่อเพิ่มเติมให้ครอบคลุมการกระทำ ความผิดอาญาในรูปแบบต่างๆ และให้มีอัตราโทษเหมาะสมกับความร้ายแรงของการกระทำความผิด
กฎหมายด้านเทคโนโลยีสารสนเทศ				
พ.ร.บ.ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ แก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๕๑	√			เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือและรับรองให้การทำธุรกรรมทางอิเล็กทรอนิกส์มีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไป
พ.ร.ฎ.กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙	√			กำหนดหลักเกณฑ์ วิธีการการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐในสาระสำคัญ เพื่อการส่งเสริม สนับสนุนให้หน่วยงานของรัฐสามารถพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ได้อย่างมีมาตรฐานและเป็นไปในทิศทางเดียวกัน
พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓	√			ใช้บังคับสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์ซึ่งมีผลกระทบต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน และการทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศ โดยกำหนดระดับของวิธีการแบบปลอดภัยและกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับวิธีการแบบปลอดภัยในแต่ละระดับ
ประกาศ คธอ. เรื่อง ประเภทของธุรกรรมทางอิเล็กทรอนิกส์ และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์ตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕	√			เพื่อกำหนดประเภทของธุรกรรมทางอิเล็กทรอนิกส์และหลักเกณฑ์การประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์เพื่อที่จะได้นำมาตรการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมาปรับใช้ได้อย่างถูกต้องและเหมาะสม
ประกาศ คธอ. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕	√			เพื่อกำหนดมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยในแต่ละระดับที่ได้จากการประเมินระดับผลกระทบของธุรกรรมทางอิเล็กทรอนิกส์
ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓	√			เพื่อเป็นแนวทางเบื้องต้นในการกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับหน่วยงานของรัฐเพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงานของรัฐมีความน่าเชื่อถือและมีมาตรฐานในระดับสากล
ประกาศ คธอ. เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓	√			เพื่อเป็นแนวทางเบื้องต้นในการจัดทำนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลสำหรับการทำธุรกรรมทางอิเล็กทรอนิกส์สำหรับหน่วยงานของรัฐซึ่งรวบรวม จัดเก็บ ใช้ เผยแพร่ หรือดำเนินการอื่นใดเกี่ยวกับข้อมูลส่วนบุคคลของผู้ใช้บริการธุรกรรมทางอิเล็กทรอนิกส์
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐		√	√	กำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์จึงมีบทบัญญัติที่กำหนดโทษความผิดทางอาญา วิธีการสืบสวน สอบสวนและอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ รวมถึงการกำหนดหน้าที่ผู้ให้บริการในการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์
กฎหมายด้านโทรคมนาคม และการสื่อสาร				
พระราชบัญญัติการประกอบกิจการโทรคมนาคม พ.ศ. ๒๕๔๔	√			กำหนดหลักเกณฑ์ในการขออนุญาตประกอบกิจการโทรคมนาคม คุณสมบัติของผู้ขอรับใบอนุญาตประกอบกิจการโทรคมนาคม รวมถึงหลักเกณฑ์ในการให้บริการโครงข่ายโทรคมนาคม
ประกาศ กทช. เรื่อง มาตรการคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม	√			เนื่องจากข้อมูลส่วนบุคคลของผู้ใช้บริการในทางโทรคมนาคมเป็นสิ่งที่สามารถประมวลผล และเผยแพร่ถึงบุคคลจำนวนมากได้โดยง่าย สะดวกและรวดเร็วซึ่งจะเป็นการกระทบกระเทือนถึงสิทธิในความเป็นส่วนตัวและเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม จึงได้กำหนดมาตรการเพื่อคุ้มครองสิทธิของผู้ใช้บริการโทรคมนาคมเกี่ยวกับข้อมูลส่วนบุคคล สิทธิในความเป็นส่วนตัว และเสรีภาพในการสื่อสารถึงกันโดยทางโทรคมนาคม
ระเบียบ กทช. ว่าด้วยมาตรการเปิดเผยข้อมูลสารสนเทศ พ.ศ. ๒๕๔๘	√			เพื่อให้การดำเนินการในการบริหารจัดการข้อมูลสารสนเทศมีหลักเกณฑ์การดำเนินการที่ชัดเจนและสอดคล้องตามกฎหมายว่าด้วยข้อมูลข่าวสารของราชการ
ระเบียบ กทช. ว่าด้วยข้อมูลสารสนเทศเกี่ยวกับกิจการโทรคมนาคม พ.ศ. ๒๕๕๐	√			กำหนดหลักเกณฑ์และวิธีการในการบริหารจัดการข้อมูลสารสนเทศเกี่ยวกับกิจการโทรคมนาคม

กฎหมาย	กลไกการบังคับใช้กฎหมาย			หลักการ
	กำกับ	ป้องกัน	ปราบปราม	
กฎหมายการเงินการธนาคาร				
พระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๑	√			เพื่อกำกับดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์เพื่อประโยชน์ในการรักษาความมั่นคงทางการเงินและการพาณิชย์ โดยการกำหนดรูปแบบในการกำกับดูแลและจัดแบ่งประเภทธุรกิจบริการชำระเงินทางอิเล็กทรอนิกส์ที่เหมาะสม
ประกาศ คธอ. เรื่อง หลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๕	√			เพื่อกำหนดหลักเกณฑ์ วิธีการ และเงื่อนไขในการประกอบธุรกิจการชำระเงินทางอิเล็กทรอนิกส์เพิ่มเติมจากพระราชกฤษฎีกา ซึ่งมีการกำหนดคุณสมบัติผู้ให้บริการเพิ่มเติม รวมถึงการกำหนดรายละเอียดในวิธีปฏิบัติให้ผู้ให้บริการตามที่กำหนดไว้ในบัญชีท้ายพระราชกฤษฎีกาว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ ๒๕๕๑
ประกาศ ธปท. ที่ สรข. ๓/๒๕๕๒ เรื่อง นโยบายและมาตรการการรักษาความปลอดภัยทางระบบสารสนเทศในการประกอบธุรกิจของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์	√			สำหรับเป็นแนวทางในการกำหนดมาตรฐานในการกำหนดนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัย และเป็นแนวทางในการกำหนดวิธีปฏิบัติในการตรวจสอบ และรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์
กฎหมายด้านหลักทรัพย์				
พระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. ๒๕๓๕	√			เพื่อกำหนดโครงสร้างขององค์กรกำกับดูแลตลาดทุน หลักเกณฑ์เกี่ยวกับการกำกับดูแลการเสนอขายหลักทรัพย์เพื่อรองรับพัฒนาการของรูปแบบการจัดตั้งผู้ออกหลักทรัพย์ หลักเกณฑ์ในการกำกับดูแลตลาดหลักทรัพย์ให้เป็นสากล และการกำหนดบทบัญญัติรองรับการทำธุรกรรมในตลาดหลักทรัพย์อันได้แก่การบังคับจำนำหลักทรัพย์จดทะเบียน เพื่อให้ธุรกรรมต่าง ๆ สามารถดำเนินไปได้อย่างคล่องตัวมากยิ่งขึ้น เพื่อยกระดับการใช้ความคุ้มครองผู้ลงทุน
ประกาศสำนักงานคณะกรรมการ ก.ล.ต. ที่ สธ/น. ๓๒/๒๕๕๒ เรื่อง การควบคุมการปฏิบัติงานและการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์	√			เพื่อกำหนดหลักเกณฑ์ในการปฏิบัติงาน และการรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของบริษัทหลักทรัพย์

กฎหมาย	กลไกการบังคับใช้กฎหมาย			หลักการ
	กำกับ	ป้องกัน	ปราบปราม	
กฎหมายด้านการประกอบธุรกิจประกันภัย				
พระราชกำหนดกองทุนส่งเสริมการประกันภัยพิบัติ พ.ศ. ๒๕๕๕	√	√		เพื่อบริหารจัดการความเสี่ยงจากภัยพิบัติโดยการรับประกันภัยและทำประกันภัยต่อ และให้ความช่วยเหลือทางการเงินแก่ผู้ประกอบธุรกิจประกันวินาศภัย
พระราชบัญญัติคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย พ.ศ. ๒๕๕๐	√			เนื่องจากการประกอบธุรกิจประกันภัยมีลักษณะเป็นธุรกรรมทางการเงินประเภทหนึ่งซึ่งมีผลกระทบโดยตรงต่อระบบเศรษฐกิจ และการเงินของประเทศและต่อผู้เอาประกันภัยซึ่งเป็นผู้บริโภค องค์กรกำกับดูแลการประกอบธุรกิจประกันภัยจึงต้องมีความคล่องตัวเพื่อให้ทันต่อพัฒนาการของธุรกิจนี้และต้องมีอิสระในการดำเนินงาน เพื่อให้การกำกับดูแลการประกอบธุรกิจประกันภัยและการคุ้มครองสิทธิของผู้เอาประกันภัยเป็นไปอย่างมีประสิทธิภาพ กรณีจึงสมควรให้มีคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยที่มีความเป็นอิสระ และคล่องตัวในการกำกับดูแลธุรกิจประกันภัยขึ้นเป็นการเฉพาะ

8.4 ภาคผนวก ง

ด้วยปัจจุบันปัญหาภัยคุกคามด้านความมั่นคงปลอดภัยทางไซเบอร์มีแนวโน้มทวีความรุนแรงและขยายวงกว้างมากยิ่งขึ้นอันจะส่งผลกระทบอย่างมีนัยสำคัญต่อเศรษฐกิจและสังคมของประเทศทั้งแก่ภาครัฐและภาคเอกชน ซึ่งความเสียหายจากภัยคุกคามดังกล่าวมิได้ส่งผลกระทบเฉพาะกับหน่วยงานที่เป็นเป้าหมายของการโจมตีเท่านั้น หากแต่ยังส่งผลต่อความเชื่อมั่นและความน่าเชื่อในการดำเนินงานหรือการให้บริการของหน่วยงานอื่นในประเทศไทยอย่างเกี่ยวข้องสัมพันธ์กัน ดังนั้น เพื่อให้การดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ของประเทศไทยเป็นไปโดยมีประสิทธิภาพและครอบคลุมในทุกมิติ จึงจำเป็นที่ประเทศไทยจะต้องมีการกำหนดทิศทาง นโยบาย และมาตรการที่ชัดเจนในการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ในภาพรวมของประเทศ โดยคณะกรรมการระดับชาติที่จะสามารถประสานความร่วมมือระหว่างหน่วยงานที่เกี่ยวข้องได้อย่างบูรณาการและครอบคลุมในทุกมิติ ทั้งมิติการรักษาความมั่นคงปลอดภัยทางการทหาร การรักษาความสงบเรียบร้อยภายในประเทศ และการรักษาความมั่นคงในทางเศรษฐกิจ ซึ่งปัจจุบันได้มีคำสั่งสำนักนายกรัฐมนตรีที่ ๗๖/๒๕๕๕ แต่งตั้งคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) เพื่อทำหน้าที่ดังกล่าวขึ้น

นอกเหนือจากการมีคณะกรรมการระดับชาติดังกล่าวข้างต้นแล้ว เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยไซเบอร์เกิดผลในทางปฏิบัติอย่างเป็นรูปธรรม โดยหน่วยงานที่เกี่ยวข้องทั้งภาครัฐและภาคเอกชนสามารถนำแนวทางและมาตรการที่คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee) กำหนดไปดำเนินการได้อย่างถูกต้องและสอดคล้องกับภารกิจหรือบทบาทหน้าที่ของแต่ละหน่วยงาน จึงจำเป็นที่จะต้องมีกลไกในรูปแบบคณะกรรมการระดับองค์หรือระดับหน่วยงานเพื่อทำหน้าที่กำกับดูแลการดำเนินงานด้านรักษาความมั่นคงปลอดภัยไซเบอร์ในขอบเขตความรับผิดชอบของตนควบคู่กัน ไม่ว่าจะเป็นการกำกับดูแลการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามประเภทธุรกิจโดยหน่วยงานกำกับดูแล เช่น ธุรกิจสถาบันการเงินโดยธนาคารแห่งประเทศไทย ธุรกิจหลักทรัพย์โดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือธุรกิจประกันภัยโดยสำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย เป็นต้น รวมทั้งการกำกับดูแลการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ เพื่อประโยชน์ในการสร้างความเชื่อมั่นและความน่าเชื่อถือในการให้บริการภาครัฐและการประกอบธุรกิจของภาคเอกชน

โดยคณะกรรมการที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย ประกอบด้วย

1. คณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee)

องค์ประกอบ

1.	นายกรัฐมนตรี	ประธานกรรมการ
2.	รองนายกรัฐมนตรีที่นายกรัฐมนตรีมอบหมาย	รองประธานกรรมการ
3.	รัฐมนตรีประจำสำนักนายกรัฐมนตรีที่นายกรัฐมนตรีมอบหมาย	กรรมการ
4.	รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการ
5.	รัฐมนตรีว่าการกระทรวงกลาโหม	กรรมการ
6.	รัฐมนตรีว่าการกระทรวงยุติธรรม	กรรมการ
7.	เลขาธิการนายกรัฐมนตรี	กรรมการ
8.	ปลัดกระทรวงกลาโหม	กรรมการ
9.	ปลัดกระทรวงการคลัง	กรรมการ
10.	ปลัดกระทรวงการต่างประเทศ	กรรมการ
11.	ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร	กรรมการ
12.	ปลัดกระทรวงมหาดไทย	กรรมการ
13.	ปลัดกระทรวงยุติธรรม	กรรมการ
14.	เลขาธิการสภาความมั่นคงแห่งชาติ	กรรมการ
15.	ผู้อำนวยการสำนักข่าวกรองแห่งชาติ	กรรมการ
16.	อัยการสูงสุด	กรรมการ
17.	ผู้บัญชาการตำรวจแห่งชาติ	กรรมการ
18.	อธิบดีกรมสอบสวนคดีพิเศษ	กรรมการ
19.	เลขาธิการคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ	กรรมการ
20.	ผู้ทรงคุณวุฒิที่ประธานกรรมการแต่งตั้งจำนวนไม่เกิน 5 คน	กรรมการ
21.	ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)	กรรมการและเลขานุการ
22.	ผู้อำนวยการรักษาความปลอดภัยคอมพิวเตอร์สำนักงานปลัดกระทรวงกลาโหม	กรรมการและผู้ช่วยเลขานุการ
23.	ผู้กำกับการกลุ่มงานตรวจสอบและวิเคราะห์การกระทำความผิดทางเทคโนโลยีกองบังคับการสนับสนุนทางเทคโนโลยี สำนักงานตำรวจแห่งชาติ	กรรมการและผู้ช่วยเลขานุการ

อำนาจหน้าที่

- จัดทำนโยบาย และแผนแม่บทความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ให้สามารถปกป้อง ป้องกัน รับมือ และลดความเสี่ยงจากสถานการณ์ด้านภัยคุกคามในไซเบอร์ อันกระทบต่อความมั่นคงของชาติทั้งจากภายในและภายนอกประเทศ ครอบคลุมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศและความมั่นคงทางเศรษฐกิจ เพื่อนำเสนอต่อคณะรัฐมนตรี
- กำหนดและจัดทำแนวทาง มาตรการ หรือแผนงานและโครงการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ตามนโยบายและแผนแม่บทความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
- ติดตามและประเมินผลการปฏิบัติการตามแนวทาง มาตรการ หรือแผนงานตามที่กำหนดและจัดทำไว้
- รายงานผลการดำเนินการ สถานการณ์ และวิเคราะห์ความเสี่ยงของภัยคุกคามในไซเบอร์ต่อคณะรัฐมนตรี
- ประสานความร่วมมือด้านความมั่นคงปลอดภัยในไซเบอร์ทั้งภายในและภายนอกประเทศ

2. คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

องค์ประกอบ

1. นาวาอากาศเอกอนุดิษฐ์ นาครทรรพ ประธานกรรมการ
   รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
2. นายไชยยันต์ พึ่งเกียรติไพโรจน์ รองประธานกรรมการ
   ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
3. นายฉิม ตันติยาสวัสดิกุล กรรมการด้านการเงินจากภาครัฐ
4. นายธีระ อภัยวงศ์ กรรมการด้านการเงินจากภาคเอกชน
5. นายชัยณรงค์ โชไชย กรรมการด้านการพาณิชย์อิเล็กทรอนิกส์จากภาครัฐ
6. นางเสาวณี สุวรรณชีพ กรรมการด้านการพาณิชย์อิเล็กทรอนิกส์จากภาคเอกชน
7. นายวิศิษฎ์ วิศิษฎ์สรอรรถ กรรมการด้านนิติศาสตร์จากภาครัฐ
8. นายสุชาติ ธรรมาพิทักษ์กุล กรรมการด้านนิติศาสตร์จากภาคเอกชน
9. นายกำพล ศรธนะรัตน์ กรรมการด้านวิทยาการคอมพิวเตอร์จากภาครัฐ
10. นายสหัส ตรีทิพยบุตร กรรมการด้านวิทยาการคอมพิวเตอร์จากภาคเอกชน
11. นายทวีศักดิ์ กออนันตกูล กรรมการด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์จากภาครัฐ
12. นายสุเทพ อุ่นเมตตาจิต กรรมการด้านวิทยาศาสตร์หรือวิศวกรรมศาสตร์จากภาคเอกชน
13. นายสมศักย์ ภูรีศรีศักดิ์ กรรมการด้านสังคมศาสตร์จากภาครัฐ
14. นางสาววิลาวรรณ วนดุรงค์วรรณ กรรมการด้านสังคมศาสตร์จากภาคเอกชน
15. นางสมใจ ประเสริฐจีรังกุล กรรมการและเลขานุการ
    ผู้อำนวยการสำนักงานคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

อำนาจหน้าที่

บทบาทหน้าที่ของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ คือ การเสนอแนะการตรากฎหมายและการออกระเบียบหรือประกาศต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศที่ใช้ในการทำธุรกรรมทางอิเล็กทรอนิกส์ทั้งแก่ภาครัฐและภาคเอกชน โดยการกำหนดมาตรฐานขั้นต่ำเพื่อให้หน่วยงานต่าง ๆ นำไปปฏิบัติ เพื่อประโยชน์ในการรักษาความถูกต้อง ความครบถ้วนและสภาพพร้อมใช้งานของธุรกรรมทางอิเล็กทรอนิกส์ให้มีความน่าเชื่อถือ ตลอดจนให้ข้อเสนอแนะในการรักษาความมั่นคงปลอดภัยของสารสนเทศของหน่วยงานต่าง ๆ

3. คณะอนุกรรมการความมั่นคงปลอดภัย ในคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

องค์ประกอบ

1. นายปริญญา หอมเอนก ที่ปรึกษา
2. นายทวีศักดิ์ กออนันตกูล ประธานอนุกรรมการ
3. นายกำพล ศรธนะรัตน์ อนุกรรมการ
4. รองศาสตราจารย์ยืน ภู่วรวรรณ อนุกรรมการ
5. นางสุรีรัตน์ ลัคนานิตย์ อนุกรรมการ
6. นายยรรยง เต็งอำนวย อนุกรรมการ

7. นายสมญา พัฒนาวรพันธุ์ อนุกรรมการ
8. นายไชยกร อภิวัฒโนกุล อนุกรรมการ
9. นายชาลี วรกุลพิพัฒน์ นุกรรมการ
10. นางสุรางคณา วายุภาพ อนุกรรมการ
11. นายชัยชนะ มิตรพันธ์ อนุกรรมการและเลขานุการ
12. นางสาวรัตนา จำรูญศักดิ์สิทธิ์ อนุกรรมการและผู้ช่วยเลขานุการ
13. นายทวีสิทธิ์ เพ็ญรัศมีพูนสุข อนุกรรมการและผู้ช่วยเลขานุการ

อำนาจหน้าที่

จัดทำข้อเสนอแนะเชิงนโยบายด้านความมั่นคงปลอดภัยเสนอต่อคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ โดยการวิเคราะห์แนวโน้มภัยคุกคามในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่คาดว่าจะเกิดขึ้น เพื่อเสนอการจัดทำยุทธศาสตร์การบริหารความเสี่ยงในด้านดังกล่าว รวมทั้งช่วยเหลือคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ในด้านการส่งเสริมและติดตามให้หน่วยงานภาครัฐนำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์กำหนดไปปฏิบัติ และส่งเสริมให้หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศนำมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัยที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์นำข้อกำหนดไปปรับใช้

4. คณะกรรมการบริหารสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

องค์ประกอบ

1. นายจรัมพร โชติกเสถียร ประธานกรรมการ
2. นายไชยยันต์ พึ่งเกียรติไพโรจน์ กรรมการโดยตำแหน่ง
   ปลัดกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร
3. นายวรวิทย์ จำปีรัตน์ กรรมการโดยตำแหน่งผู้อำนวยการสำนักงบประมาณ
4. นายทวีศักดิ์ กออนันตกูล กรรมการโดยตำแหน่งผู้อำนวยการสำนักงาน
   พัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
5. นางสาววิลาวรรณ วนดุรงค์วรรณ กรรมการผู้ทรงคุณวุฒิด้านการเงิน
6. นายอภิรมย์ น้อยอ่ำ กรรมการผู้ทรงคุณวุฒิด้านพาณิชย์อิเล็กทรอนิกส์
7. นายธีระ อภัยวงศ์ กรรมการผู้ทรงคุณวุฒิด้านวิศวกรรมศาสตร์
8. นายชวลิต อัตถศาสตร์ กรรมการผู้ทรงคุณวุฒิด้านนิติศาสตร์
9. นายปรีชา ปรมาพจน์ กรรมการผู้ทรงคุณวุฒิด้านการเงิน
10. นายสมพรต สาระโกเศศ กรรมการผู้ทรงคุณวุฒิด้านการสังคมศาสตร์
11. นางสุรางคณา วายุภาพ กรรมการและเลขานุการ
    ผู้อำนวยการสำนักงานพัฒนาธุรกรรม
    ทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อำนาจหน้าที่

บทบาทหน้าที่ของคณะกรรมการบริหารสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ คือการกำกับดูแลและให้ข้อเสนอแนะต่อการดำเนินงานของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือ ThaiCERT เพื่อให้สามารถตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ และสามารถประสานการทำงานร่วมกันกับหน่วยงานที่เกี่ยวข้องทั้งในประเทศและต่างประเทศได้อย่างมีประสิทธิภา

5. สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ

ภารกิจสำคัญ

ของกลุ่มนักวิชาชีพด้านความมั่นคงปลอดภัยสารสนเทศในประเทศไทย พัฒนากระบวนการและบุคลากรด้านความมั่นคงปลอดภัยสารสนเทศให้ได้มาตรฐานเป็นที่ยอมรับในระดับสากล

องค์ประกอบ

1. พ.ต.อ. ญาณพล ยั่งยืน	นายกสมาคม
The Department of Special Investigation (DSI)	
2. คุณสมญา พัฒนวรพันธุ์	อุปนายก
National Intelligence Agency	
3. อาจารย์เมธา สุวรรณสาร	อุปนายก
Thailand Information Security Association (TISA)	
4. ดร.รอม หิรัญพฤกษ์	ที่ปรึกษากิตติมศักดิ์
Thailand Information Security Association (TISA)	
5. อาจารย์ปริญญา หอมเอนก	กรรมการและเลขานุการ
ACIS Professional Center Co., Ltd.	

และคณะกรรมการผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยระบบสารสนเทศ

ทีมงานจัดทำ

ThaiCERT Thailand Computer Emergency Response Team a member of ETDA

ANNUAL REPORT 2012

หัวหน้าทีมจัดทำ

สุรางคณา วายุภาพ
ผู้อำนวยการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ดูแลเนื้อหาและนโยบายภาพรวม

ชัยชนะ มิตรพันธ์
ผู้ช่วยผู้อำนวยการ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
ดูแลด้านข้อมูลความมั่นคงปลอดภัย

สรณันท์ จิวะสุรัตน์
ผู้อำนวยการ สำนักความมั่นคงปลอดภัย
ดูแลด้านข้อมูลความมั่นคงปลอดภัย

คัชชิดา มีท่อธาร
รองผู้อำนวยการ สำนักกฎหมาย
ดูแลประเด็นกฎหมาย

อัจฉราพร หมุดระเด่น
ผู้ช่วยผู้อำนวยการ สำนักนโยบายและส่งเสริม
ดูแลประเด็นยุทธศาสตร์

นายธงชัย แสงศิริ
ผู้จัดการส่วนงานตรวจพิสูจน์พยานหลักฐานดิจิทัล
สำนักความมั่นคงปลอดภัย
ดูแลด้านข้อมูลภัยคุกคาม

ทีมคณะผู้จัดทำ

ฝ่ายจัดทำเนื้อหา
ไพฑูรย์ วิมุกตะนันทน์
พรพรหม ประภากิตติกุล
ศุภกร ฤกษ์ดิถีพร
เสฏฐวุฒิ แสนนาม
เจษฎา ช้างสีสังข์
วิศิลป์ ประสงค์สุข
ธงชัย ศิลปวรางกูร
แสนชัย จูโนทับ
โชติกา สันโน
กรรณิกา ภัทรวิศิษฏ์สันธ์
ณัฐโชติ ดุสิตานนท์
และทีมไทยเซิร์ต

ฝ่ายข้อมูลด้านกฎหมาย
พลอย เจริญสม
พิชญสักษณ์ ค่าทองสุก
ณัฐวรรธน์ สุขวงศ์ตระกูล
พลอยพัชร โชไชย

ฝ่ายศิลป์
ณัฐพงศ์ วรพิวุฒิ
นภดล อุษณบุญศิริ
ณัฐนัย รวดเร็ว

ฝ่ายประสานงาน
รจนา ล้าเลิศ
วิภาภรณ์ บุตรเมฆ
สุฉายพิมพ์ ศิริวัฒน์
เขมมิกา สกุลแพทย์
พรรวดี โควินทเศรษฐ

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

THAILAND COMPUTER
EMERGENCY
RESPONSE TEAM
[ThaiCERT]

ANNUAL REPORT 2012

NATIONAL CYBER SECURITY COMMITTEE

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

THAILAND COMPUTER EMERGENCY RESPONSE TEAM [ThaiCERT]

ANNUAL REPORT 2012

ISBN 978-974-9765-46-3

- ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย
  (THAILAND COMPUTER EMERGENCY RESPONSE TEAM)
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สพธอ.
- กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

เลขที่ 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา 5 ธันวาคม 2550 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
โทรศัพท์ : 0-2142-2483 | โทรสาร : 0-2143-8071
อีเมล : office@thaicert.or.th
เว็บไซต์ไทยเซิร์ต : www.thaicert.or.th | เว็บไซต์ สพธอ. : www.etda.or.th | เว็บไซต์กระทรวงฯ : www.mict.go.th

MINISTRY OF ICT Smart Thailand

ETDA สพธอ

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

Electronic Transactions Commission

สำนักงาน กสทช.
สำนักงานคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์และกิจการโทรคมนาคมแห่งชาติ