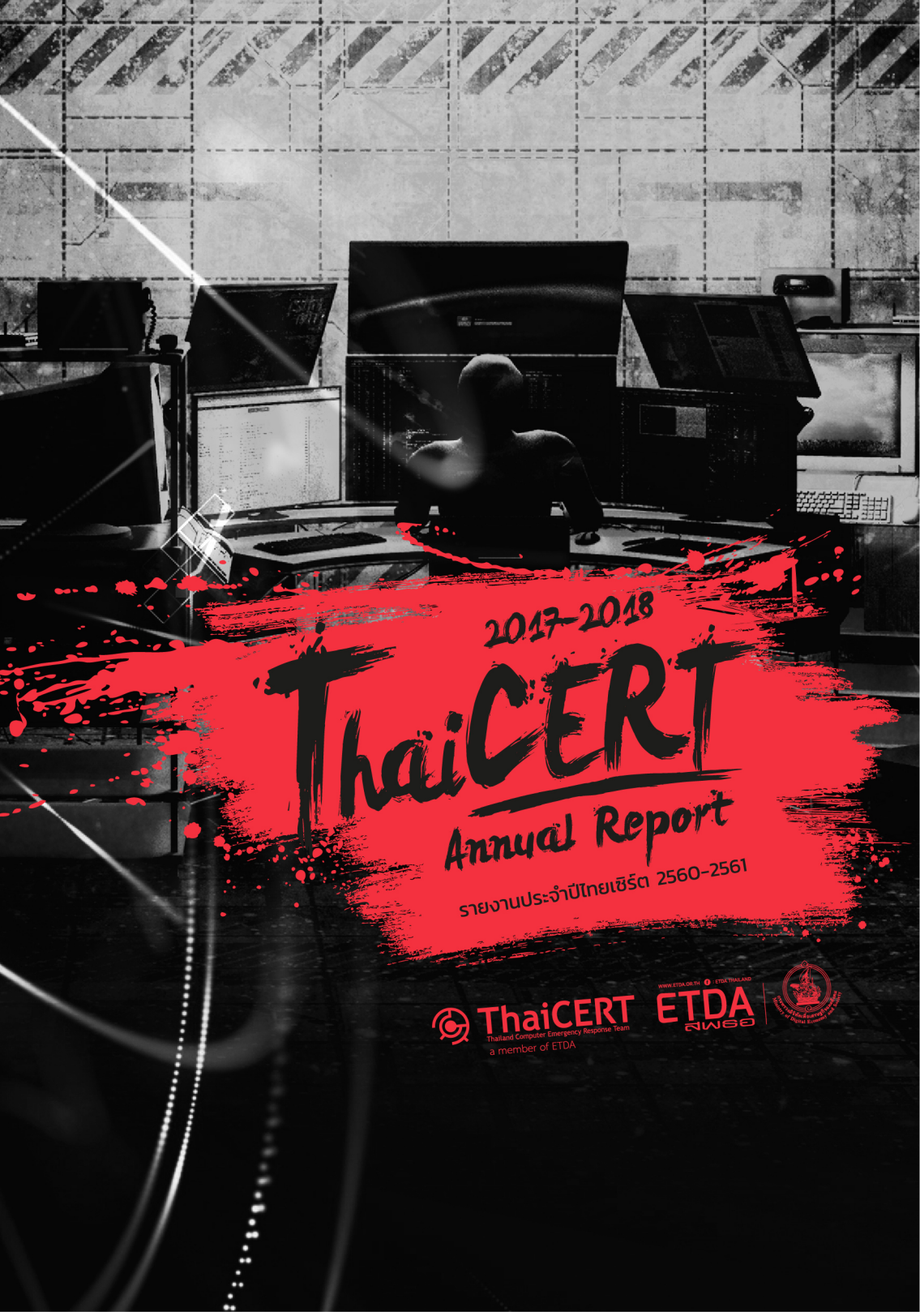


2017-2018

ThaiCERT Annual Report

รายงานประจำปีไทยเซิร์ต 2560-2561

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

WWW.ETDA.OR.TH | ETDA THAILAND

ETDA สพธอ

CYBERSECURITY
@ DIGITAL TRANSFORMATION

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

รายงานประจำปีไทยเซิร์ต 2560-2561
2017-2018 ThaiCERT Annual Report

เรียบเรียงโดย

สุรางคณา วายุภาพ, ชัยชนะ มิตรพันธ์, ศุภโชค จันทรประทิน, อุรัชฎา เกตุพรหม,
พรพรหม ประภากิตติกุล, วีรชัย ประยูรพฤกษ์, Martijn Van Der Heide, สัญญา คล่องในวัย,
อารยะ สวัสดิชัย, กรรณิกา ภัทรวิศิษฏ์สัณธ์, ทรงศักดิ์ ยงยิ่งศักดิ์ถาวร, ณัฐโชติ ดุสิตานนท์,
ฉัตรชัย จันทร์อินทร์, ยุทธนา ชนวัฒน์, เสฏฐวุฒิ แสนนาม, ปวริศ จอมสถาน,
จักรวาล องค์ทองคำ, นันทพงศ์ บุญถนอม, รุ่งวิทย์ จิตรส่องแสง, ธนชัย แสงไพฑูรย์,
สิริณัฐ ตั้งธรรมจิต, ภูรินทร์ หวังกีรติกานต์, วรรณิศา อนุรัตน์, พีร์นิธิ ฐานิวัฒนานนท์

ISBN: 978-616-7956-44-2

พิมพ์ครั้งที่ 2

พิมพ์จำนวน 150 เล่ม
ราคา 300 บาท

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

Thailand Computer Emergency Response Team (ThaiCERT)
Electronic Transactions Development Agency (ETDA)
Ministry of Digital Economy and Society

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า
(อาคารบี) ชั้น 20 เลขที่ 33/4
ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310
โทรศัพท์: 0 2123 1212

สารบัญ

Cybersecurity เป็นเรื่องจำเป็นสำหรับทุกคน และเป็นสิ่งที่ทุกคนต้องช่วยกัน ทั้งภาครัฐ ภาคเอกชน และภาคประชาชน ในการร่วมกันดูแลความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศ

พลอากาศเอก ประจิน จั่นตอง
รองนายกรัฐมนตรี

การปกป้องโครงสร้างพื้นฐานของประเทศ
ถือเรื่องสำคัญ รัฐบาลจึงได้เฝ้าระวังและเตรียมพร้อม
รับมือในกรณีถูกโจมตีทางไซเบอร์ให้ทันท่วงที

พิเชฐ ดุรงคเวโรจน์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

รัฐบาลและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมผลักดันแนวนโยบายต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ไปสู่ **การปฏิบัติอย่างเป็นรูปธรรม** เช่น การผลักดันร่างกฎหมายฉบับต่าง ๆ ซึ่งครอบคลุมการพัฒนาโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์ การพัฒนากำลังคนให้มีความสามารถและเป็นกำลังหลักที่เพียงพอต่อการแข่งขันและพัฒนาประเทศในยุคเศรษฐกิจดิจิทัล

อัจฉรินทร์ พัฒนพันธ์ชัย
ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

วันนี้ ภัยไซเบอร์ได้ขยายขอบเขตและสร้างความเสียหายรุนแรงไปทั่วโลก การสร้าง**กำลังคนด้านไซเบอร์**จำเป็นอย่างยิ่งสำหรับประเทศไทย เพื่อให้ทุกภาคส่วนของไทยพร้อมรับมือกับภัยคุกคามที่อาจจะเกิดขึ้น

จีราวรรณ บุญเพิ่ม
ประธานกรรมการบริหาร
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

"ไทยเซิร์ต" ทำหน้าที่ดูแลความมั่นคงปลอดภัยบนโลกไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็ว ทั้งเชิงรับและเชิงรุก อย่างไรก็ดี ทุกคนก็ต้องร่วมมือและปรับตัวให้รู้เท่าทันต่อการเปลี่ยนแปลงนี้ด้วย หากไม่อยากถูกทิ้งไว้ข้างหลัง ตามคำเปรียบเปรยที่ว่า **"Do or Die?"**

สุรางคณา วายุภาพ
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ก้าวเล็ก
เป็นก้า
เพื่อก้าวต่

ๆ ที่เติบโต
วที่มั่นคง
อไปในอนาคต

ประเทศไทยกำลังยกระดับเศรษฐกิจและสังคมภายใต้นโยบายเศรษฐกิจดิจิทัล กลไกที่สำคัญในการขับเคลื่อนประเทศจึงมีความเกี่ยวข้องกับระบบสารสนเทศที่มีความมั่นคงปลอดภัย เพื่อให้ประชาชนมีความมั่นใจในการใช้งานเทคโนโลยีดิจิทัล อันจะผลักดันให้ประเทศไทยมีการทำธุรกรรมทางอิเล็กทรอนิกส์เพิ่มขึ้น

ผลสำรวจมูลค่าธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทยโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)[1] พบว่าปี 2560 ธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทยมีมูลค่าประมาณ 2.8 ล้านล้านบาท และคาดการณ์ว่าปี 2561 จะมีมูลค่าสูงถึง 3.2 ล้านล้านบาท คิดเป็นอัตราเติบโตร้อยละ 14.04 โดยประเทศไทยมีมูลค่าธุรกรรมทางอิเล็กทรอนิกส์แบบ Business to Consumer (B2C) กว่า 2 แสนล้านบาท และอยู่ในอันดับ 1 ของภูมิภาคอาเซียน ซึ่งแสดงให้เห็นถึงการขยายตัวของการทำธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562 กำหนดให้ สพธอ. ปฏิบัติหน้าที่ฐานะผู้กำกับดูแลด้านการทำธุรกิจบริการด้านธุรกรรมออนไลน์ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์มอบหมาย ซึ่งถือเป็นความท้าทายที่ต้องยกระดับการทำงานของสำนักงานเพื่อรองรับการจัดทำแผนยุทธศาสตร์เกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ จัดทำยุทธศาสตร์การพัฒนาโครงสร้างพื้นฐานด้านมาตรฐาน รวมถึงกำกับดูแลธุรกิจบริการ วิเคราะห์และรับรองมาตรฐานที่เกี่ยวข้อง เพื่อส่งเสริมและเพิ่มขีดความสามารถในการแข่งขันด้านธุรกรรมทางอิเล็กทรอนิกส์ของประเทศไทย

[1] https://www.etda.or.th/publishing-detail/value-of-e-commerce-survey-in-thailand-2018.html

ในขณะที่ประเทศไทยมีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์ ภัยคุกคามไซเบอร์เป็นภัยที่เราต้องเผชิญอย่างหลีกเลี่ยงไม่ได้ การโจมตีระบบ การขโมยข้อมูล การปลอมบัญชีโซเชียลมีเดีย และภัยคุกคามไซเบอร์อื่น ๆ มีปรากฏให้อย่างต่อเนื่อง อาทิ การแพร่ระบาดของ WannaCry ที่เกิดขึ้นทั่วโลก ซึ่งชะลอขัดขวางบริการสารสนเทศของหน่วยงานต่าง ๆ และส่งผลกระทบในการขับเคลื่อนเศรษฐกิจของประเทศ

ร่างรายงาน Global Cybersecurity Index (GCI) ปี 2561[2] ซึ่งเป็นรายงานที่แสดงถึงความเข้มข้นในการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ โดยสหภาพโทรคมนาคมระหว่างประเทศ หรือ International Telecommunications Union (ITU) ประเมินค่าดัชนีความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยคิดเป็น 0.796 และอยู่อันดับ 35 จาก 194 ประเทศ เทียบกับปี 2560 มีค่าดัชนีฯ 0.684 และอยู่ในอันดับที่ 22 แสดงให้เห็นถึงความท้าทายในการปรับปรุงศักยภาพในด้านต่าง ๆ ของประเทศ

[2] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

ภาครัฐเห็นความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงได้ผลักดันร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. .... เพื่อรองรับการเติบโตทางเศรษฐกิจดิจิทัลอย่างมั่นคงและปลอดภัย ซึ่งกำหนดให้มีสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทำหน้าที่เป็นหน่วยงานกลางในการประสานและขับเคลื่อนนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ

รายงานประจำปีไทยเซิร์ตปี 2560-2561 จัดทำสรุปเหตุการณ์ วิเคราะห์แนวโน้ม รวบรวมสถิติภัยคุกคามไซเบอร์ที่เกิดขึ้นในประเทศไทย และกิจกรรมที่สำคัญของไทยเซิร์ต เพื่อสร้างความตระหนักรู้และชี้ให้เห็นถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ในภาครัฐ ภาคเอกชน และภาคประชาสังคม ซึ่งไม่ใช่หน้าที่ของหน่วยงานใดหน่วยงานหนึ่ง แต่เป็นสิ่งที่ทุกภาคส่วนต้องประคับประคองและแก้ไขปัญหาไปพร้อมกัน

แล้วคุณละ... พร้อมหรือยังที่จะเป็นส่วนหนึ่งในการยกระดับความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยอย่างมั่นคงและยั่งยืน

การโจมตีและอีเวนต์ทางไซเบอร์ที่สำคัญในไทย ปี 2560-2561

2560 ก พ

ผลักดันให้มี
คณะทำงาน
จัดการซ้อมรับมือ
APCERT Drill
ภายใต้ APCERT
อย่างเป็นทางการ
โดยมีไทยเซิร์ต
เป็นประธานคณะทำงานฯ

2560 พ.ค.

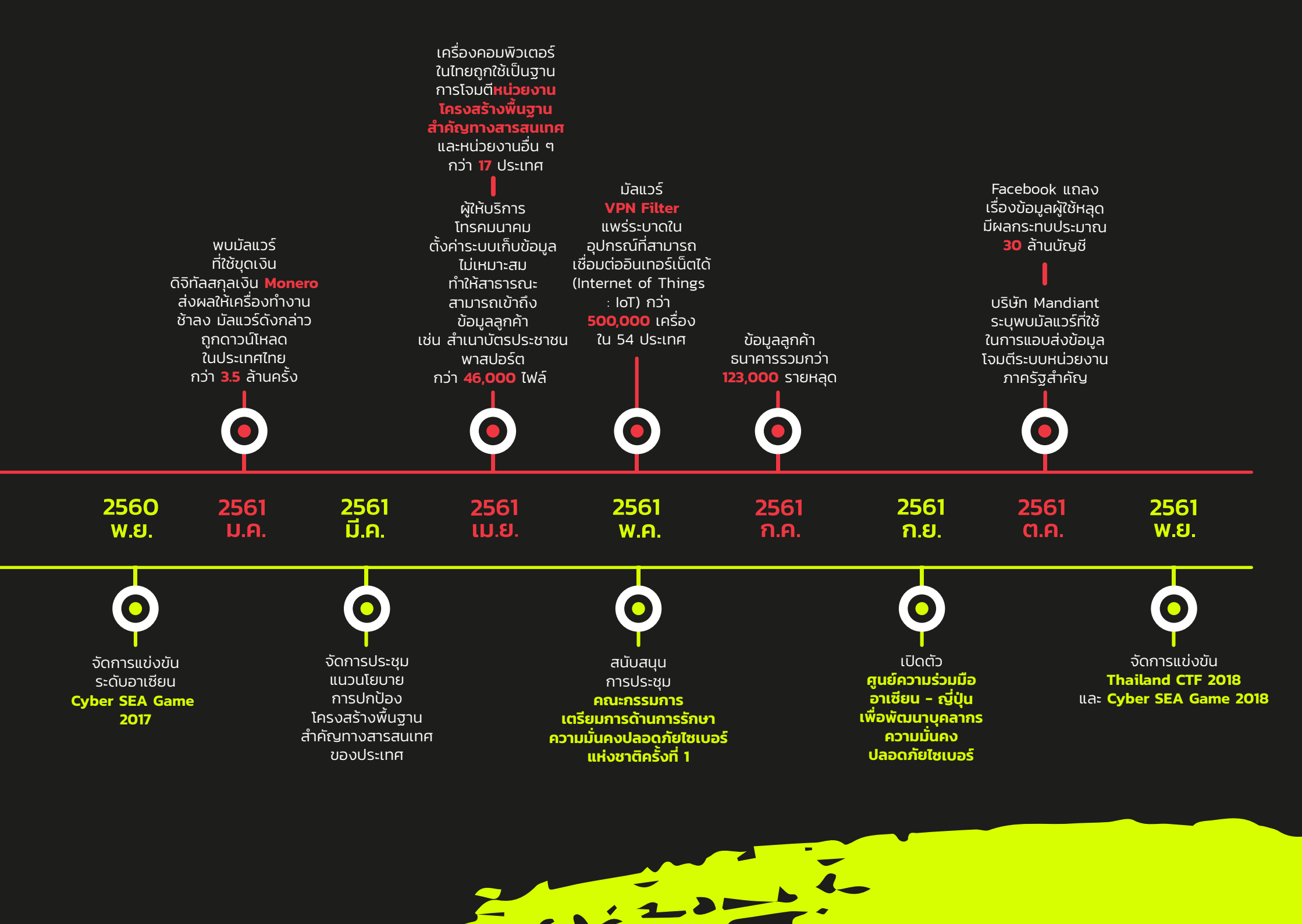
พบการแพร่ระบาดของ
WannaCry
ในเครื่องคอมพิวเตอร์กว่า
200,000 เครื่อง
จาก **112** ประเทศ
ผ่านช่องโหว่ในโพรโทคอล SMB

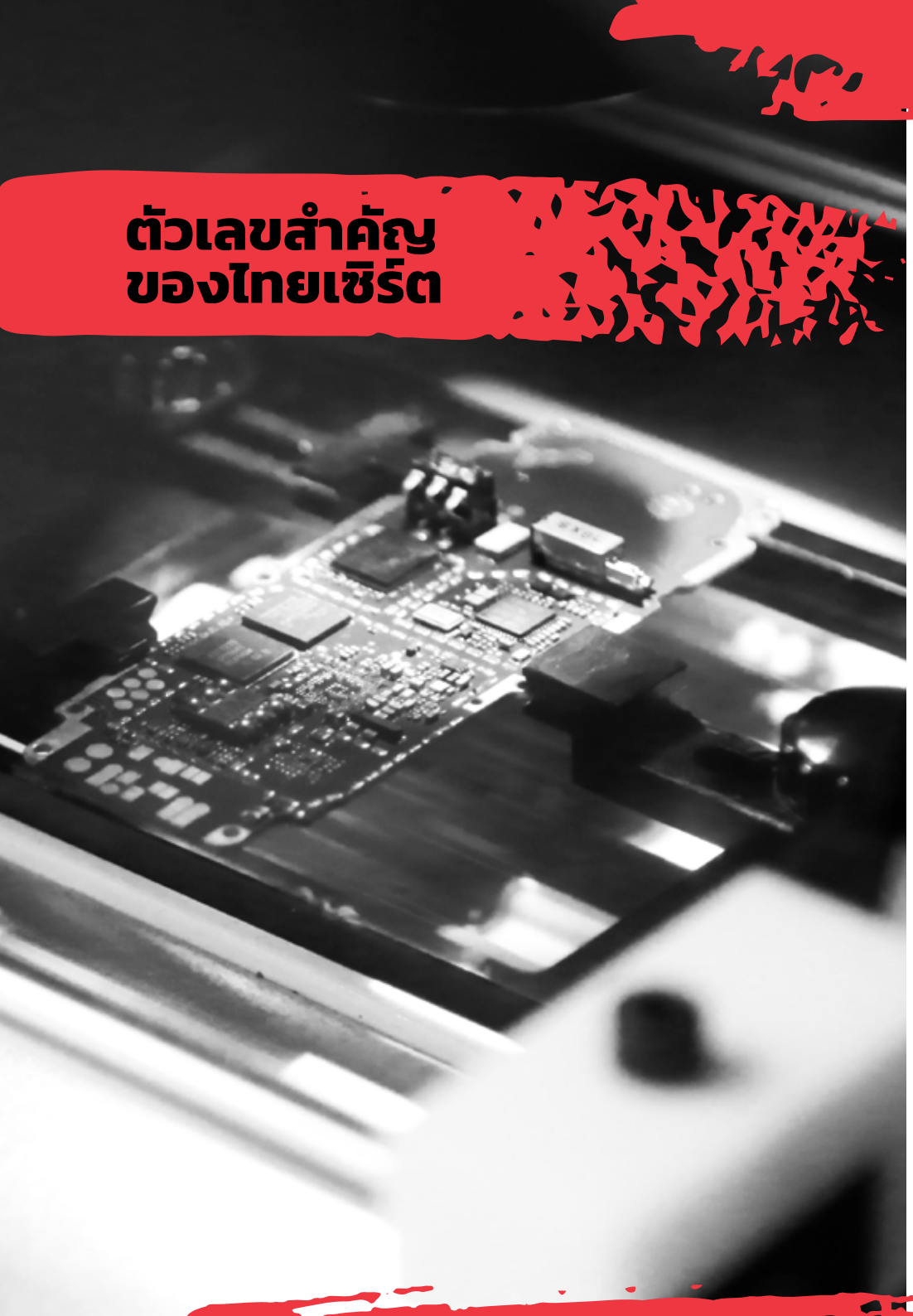
2560 มิ.ย.

จัดสัปดาห์
งานสัมมนาด้านความ
มั่นคงปลอดภัยไซเบอร์
Thailand Cybersecurity Week 2017

2560 ต.ค.

จัดการแข่งขัน
ระดับประเทศ
Thailand CTF 2017


2560 พ.ย.
จัดการแข่งขันระดับอาเซียน Cyber SEA Game 2017
2561 ม.ค.
พบมัลแวร์ที่ใช้ขุดเงินดิจิทัลสกุลเงิน Monero ส่งผลให้เครื่องทำงานช้าลง มัลแวร์ดังกล่าวถูกดาวน์โหลดในประเทศไทยกว่า 3.5 ล้านครั้ง
2561 มี.ค.
จัดการประชุมแนวนโยบายการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
2561 เม.ย.
เครื่องคอมพิวเตอร์ในไทยถูกใช้เป็นฐานการโจมตีหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและหน่วยงานอื่น ๆ กว่า 17 ประเทศ
ผู้ให้บริการโทรคมนาคมตั้งค่าระบบเก็บข้อมูลไม่เหมาะสม ทำให้สาธารณะสามารถเข้าถึงข้อมูลลูกค้า เช่น สำเนาบัตรประชาชน พาสปอร์ต กว่า 46,000 ไฟล์
2561 พ.ค.
มัลแวร์ VPN Filter แพร่ระบาดในอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ (Internet of Things : IoT) กว่า 500,000 เครื่อง ใน 54 ประเทศ
สนับสนุนการประชุมคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติครั้งที่ 1
2561 ก.ค.
ข้อมูลลูกค้าธนาคารรวมกว่า 123,000 รายหลุด
2561 ก.ย.
เปิดตัวศูนย์ความร่วมมืออาเซียน - ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์
2561 ต.ค.
Facebook แถลงเรื่องข้อมูลผู้ใช้หลุดมีผลกระทบประมาณ 30 ล้านบัญชี
บริษัท Mandiant ระบุพบมัลแวร์ที่ใช้ในการแอบส่งข้อมูลโจมตีระบบหน่วยงานภาครัฐสำคัญ
2561 พ.ย.
จัดการแข่งขัน Thailand CTF 2018 และ Cyber SEA Game 2018



ตัวเลขสำคัญของไทยเซิร์ต

Incident Report 2560-2561

3 อันดับสูงสุด

Phishing

699 URLs
2560

692 URLs
2561

กลุ่มบริการที่ตกเป็นเป้า

บริการทางการเงินต่างประเทศ

1

บริการเทคโนโลยี

2

บริการทางการเงินในประเทศ

3

ThaiCERT GMS

240 หน่วยงานรัฐ

983 เว็บไซต์

ที่เข้าร่วมโครงการเพื่อรับการป้องกันและเฝ้าระวัง

Web Defacement

706 URLs

2560

458 URLs

2561

เป้าหมายการโจมตีเป็นเว็บไซต์ภาครัฐ 80%
รองลงมาคือ เว็บไซต์เอกชน 15%
และเว็บไซต์สถาบันการศึกษา 5%

Capacity Building

4,233 คน

2560

4,079 คน

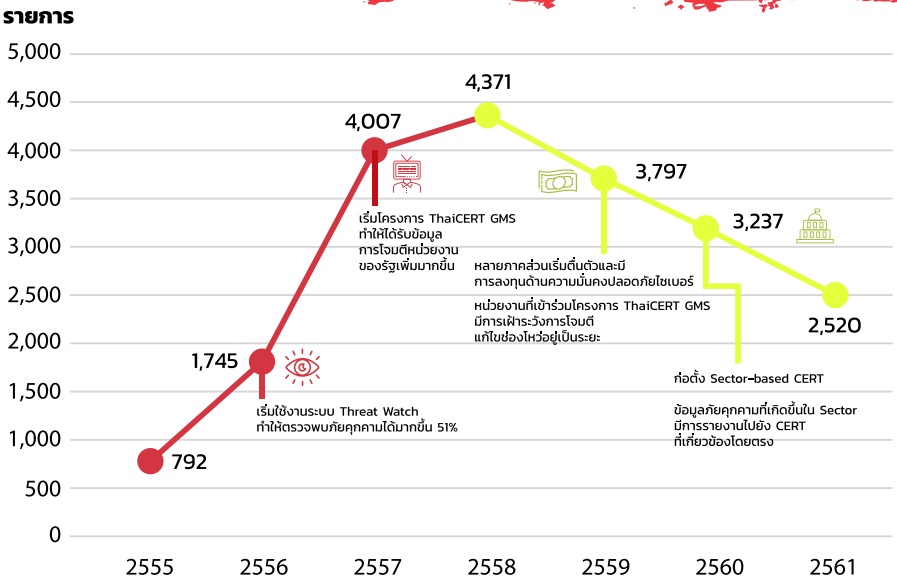
2561

อบรมสร้างความตระหนักรู้ 19 ครั้ง
อบรมให้ความรู้เชิงเทคนิคและการจัดการ 29 ครั้ง
ซ้อมรับมือภัยคุกคาม 6 ครั้ง
จัดการแข่งขัน 5 ครั้ง

ใน 2 ปีที่ผ่านมา ไทยเซิร์ตได้ดำเนินการทั้งในเชิงรุกและเชิงรับเพื่อเสริมสร้างความมั่นคงปลอดภัยให้กับประเทศไทย ทั้งการประสานเพื่อรับมือภัยคุกคามไซเบอร์ในรูปแบบต่าง ๆ เช่น การสร้างหน้าเว็บไซต์ปลอมเพื่อหลอกให้เหยื่อใส่ข้อมูล (Phishing) และการเจาะระบบเพื่อแก้ไขหน้าเว็บไซต์สร้างความเสื่อมเสียให้กับองค์กร (Web Defacement) รวมถึงการดำเนินการปกป้องเว็บไซต์และตรวจจับภัยคุกคามให้กับหน่วยงานภาครัฐในโครงการ ThaiCERT GMS และการพัฒนาบุคลากรในรูปแบบต่าง ๆ เช่น การจัดอบรมให้ความรู้ทั่วไปและเชิงเทคนิค การซ้อมรับมือภัยคุกคามการแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดสถิติที่น่าสนใจดังนี้

สถิติภัยคุกคามที่ได้รับแจ้งและดำเนินการ

สถิติการรับแจ้งเหตุประสานงานภัยคุกคามในแต่ละปี



จำนวนหน่วยงานของรัฐที่เข้าร่วมโครงการกับ ThaiCERT

2558	2559	2560	2561
40 หน่วยงาน	80 หน่วยงาน	80 หน่วยงาน	40 หน่วยงาน

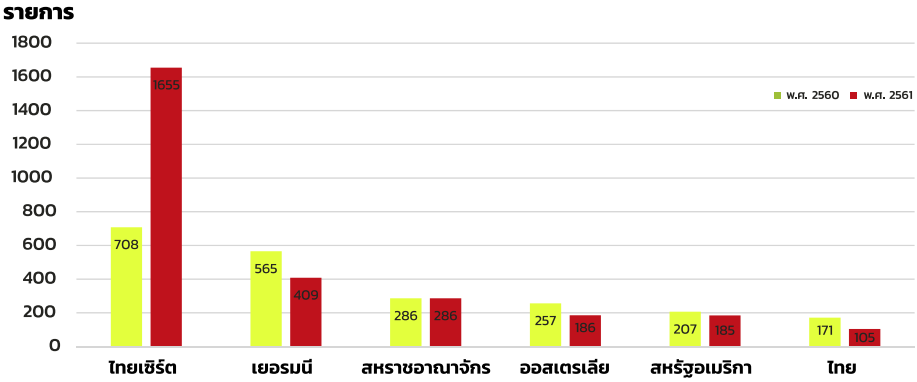
ในปี 2561 ไทยเซิร์ตได้รับแจ้งเหตุและประสานงานภัยคุกคาม 2,520 กรณี ซึ่งลดลงจากปี 2560 ถึงร้อยละ 22 โดยจำนวนเหตุรับแจ้งลดลงอย่างต่อเนื่องตั้งแต่ปี 2558 เนื่องจากหลายภาคส่วนตระหนักและเพิ่มการลงทุนในด้านความมั่นคงปลอดภัยไซเบอร์ ส่งผลให้สามารถก่อตั้ง CERT ประจำภาคส่วนได้สำเร็จในปี 2560 ทำให้ข้อมูลภัยคุกคามต่าง ๆ ที่เกิดขึ้นมีการรายงานไปยัง CERT ที่เกี่ยวข้องโดยตรง รวมถึงการดำเนินการที่มีประสิทธิภาพมากขึ้นของ ThaiCERT GMS ซึ่งประกอบด้วยส่วน Government Threat Monitoring (GTM) และ Government Website Protection (GWP) ที่มีการเฝ้าระวังระบบ ป้องกันการโจมตีเว็บไซต์ รวมทั้งตรวจสอบหาและแก้ไขช่องโหว่ของระบบเพื่อปิดช่องทางการโจมตีของผู้ประสงค์ร้าย

อันดับ	2560	2561
	ประเภทภัยคุกคาม	ประเภทภัยคุกคาม
1	ความพยายาม บุกรุกเข้าระบบ (Intrusion Attempts)	ความพยายาม บุกรุกเข้าระบบ (Intrusion Attempts)
2	การฉ้อโกงหรือหลอกลวง เพื่อผลประโยชน์ (Fraud)	การฉ้อโกงหรือหลอกลวง เพื่อผลประโยชน์ (Fraud)
3	การบุกรุกหรือเจาะระบบ ได้สำเร็จ (Intrusions)	การบุกรุกหรือเจาะระบบ ได้สำเร็จ (Intrusions)
4	การโจมตีสภาพความพร้อม ใช้งานของระบบ (Availability)	โปรแกรมไม่พึงประสงค์ (Malicious Code)
5	โปรแกรมไม่พึงประสงค์ (Malicious Code)	การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูล สำคัญโดยไม่ได้รับอนุญาต (Information Security)

ตารางแสดงภัยคุกคามที่ได้รับแจ้งสูงสุด 5 อันดับแรกในปี 2560 และ 2561[10]

เมื่อพิจารณาภัยคุกคามที่ได้รับแจ้งสูงสุด 5 อันดับแรกในปี 2560 และ 2561 ตามตารางด้านบนพบว่าประเภทภัยคุกคามที่ได้รับแจ้งสูงสุด 3 อันดับแรกของทั้ง 2 ปี คือ 1. ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) 2. การฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ซึ่งส่วนใหญ่คือ Phishing และ 3. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ซึ่งส่วนใหญ่คือ Web Defacement ในขณะที่ภัยคุกคามประเภทการโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) ซึ่งได้รับแจ้งเพิ่มขึ้นอย่างมากในปี 2560 เมื่อเทียบกับปีก่อนหน้า เนื่องจากพบการประกาศการโจมตีให้ส่งผลกระทบต่อการใช้งานเว็บไซต์จากกลุ่มที่ชื่อว่า “พลเมืองต้าน Single Gateway” แต่ในปี 2561 ไม่พบความเคลื่อนไหวจากกลุ่มดังกล่าว จึงได้รับแจ้งภัยคุกคามประเภทนี้ลดลง

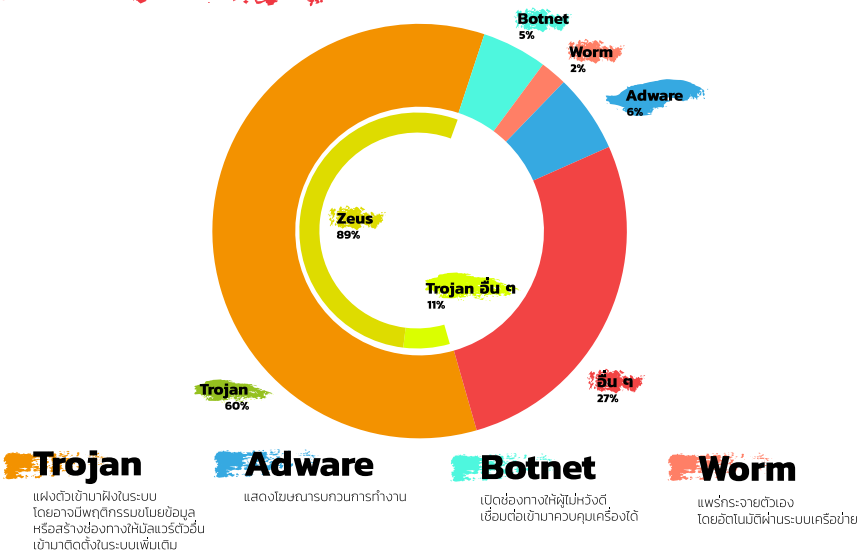
[10] คำอธิบายประเภทภัยคุกคามระบุในภาคผนวก ก ประเภทและตัวอย่างภัยคุกคาม



กราฟแสดง 5 อันดับประเทศที่แจ้งเหตุภัยคุกคามมากที่สุดในปี 2560 และ 2561

เมื่อพิจารณากราฟแสดงอันดับประเทศที่แจ้งเหตุภัยคุกคามมากที่สุดในปี 2560 และ 2561 พบว่าภัยคุกคามส่วนใหญ่ที่ไทยเซิร์ตแก้ไข มาจากการตรวจพบโดยระบบของไทยเซิร์ตที่ที่รวบรวมข้อมูลจากแหล่งต่าง ๆ รวมถึงองค์กรในเครือข่าย ในขณะประเทศที่แจ้งสูงสุดคือประเทศเยอรมนี ซึ่งส่วนใหญ่เป็นภัยคุกคามในลักษณะ Intrusion Attempt ที่ระบบในประเทศไทยโจมตีโดยการสแกนหรือพยายามสุ่มรหัสผ่านเพื่อล็อกอินเข้าระบบเป้าหมายในต่างประเทศ ซึ่งในกรณีนี้สาเหตุส่วนหนึ่งเกิดจากระบบในประเทศถูกผู้ประสงค์ร้ายควบคุมและใช้เป็นเครื่องมือในการโจมตี จึงเป็นเรื่องสำคัญที่ต้องประสานแจ้งและให้คำแนะนำเจ้าของระบบเพื่อแก้ไข

สถิติการให้บริการ ThaiCERT GMS



กราฟแสดงสถิติสัดส่วนการพบมัลแวร์ในปี 2561 โดยจำแนกตามประเภท

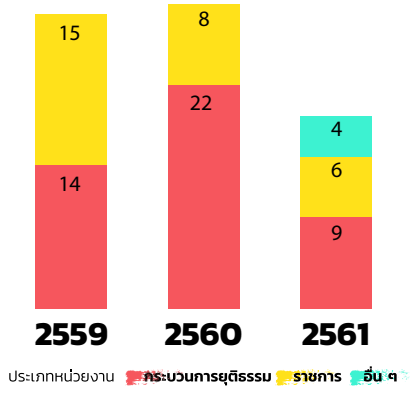
ไทยเซิร์ตได้ให้บริการเฝ้าระวังเครือข่ายให้หน่วยงานภาครัฐในโครงการ ThaiCERT GMS จำนวน 240 หน่วยงาน โดยมัลแวร์ที่ตรวจพบมากที่สุดติดต่อกันตั้งแต่ปี 2558 ถึงปี 2561 เป็นมัลแวร์ประเภท Trojan (ร้อยละ 60) และร้อยละ 89 ของ Trojan ที่พบมาจากสายพันธุ์ Zeus ซึ่งสามารถดักข้อมูลสำคัญของผู้ใช้บริการเพื่อส่งกลับให้ผู้ประสงค์ร้าย เช่น รหัสผ่านและข้อมูลบัตรเครดิต

ในขณะที่บริการส่วนปกป้องเว็บไซต์ (GWP) สามารถป้องกันการโจมตีได้ 6.6 ล้านครั้งในช่วงเดือนตุลาคมถึงธันวาคม 2561 โดยการโจมตีที่พบบ่อยที่สุด คือ Sensitive Data Exposure ซึ่งเป็นความพยายามเข้าถึงข้อมูลสำคัญที่อาจไม่ได้รับการปกปิดเท่าที่ควร เช่น ข้อมูลเกี่ยวกับเว็บเซิร์ฟเวอร์หรือเว็บแอปพลิเคชันที่ผู้ประสงค์ร้ายสามารถนำไปใช้หาช่องโหว่และเจาะระบบ

นอกจากนี้เพื่อเสริมสร้างความมั่นคงปลอดภัยให้กับเว็บไซต์ ในช่วงกลางปี 2561 ไทยเซิร์ตได้ตรวจสอบเว็บไซต์ในโครงการ 119 รายการ และพบ 538 ช่องโหว่ (เฉลี่ยเว็บละ 5 ช่องโหว่) โดยร้อยละ 79 เป็นช่องโหว่ร้ายแรงที่ถูกใช้ในการโจมตีรูปแบบต่าง ๆ เช่น Cross-Site Scripting (ร้อยละ 49) ซึ่งเป็นการแทรกคำสั่งเพื่อดักขโมยข้อมูลจากบุคคลที่สาม และ Injection (ร้อยละ 47) ซึ่งเป็นการแทรกคำสั่งเพื่อเรียกดูหรือแก้ไขฐานข้อมูลโดยมิชอบ หลังจากตรวจสอบ ไทยเซิร์ตได้ประสานหน่วยงานที่เกี่ยวข้องและแนะนำแนวทางแก้ไขเพื่อปิดช่องทางโจมตีจากผู้ประสงค์ร้าย

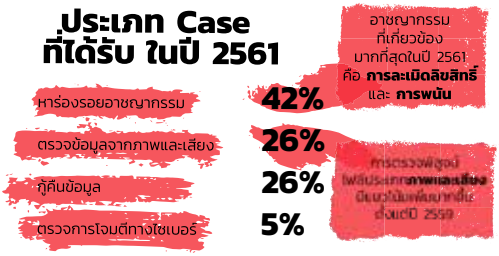
สถิติการให้บริการศูนย์ดิจิทัลฟอเรนสิกส์

ประเภทหน่วยงานที่ขอรับบริการ



ETDA กำลังปรับเพิ่มบทบาทเป็นผู้ให้บริการเก็บพยานหลักฐานกลาง และสนับสนุนเครื่องมือวิเคราะห์ข้อมูลเชิงบูรณาการ

ประเภท Case ที่ได้รับ ในปี 2561



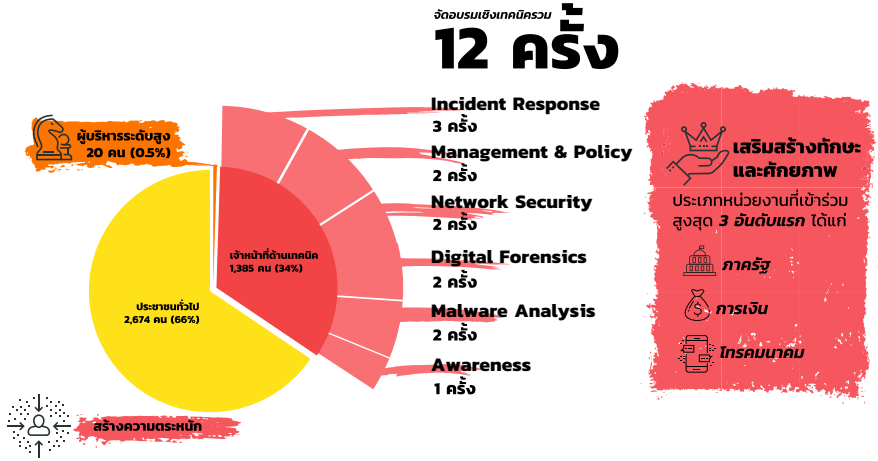
ศูนย์ดิจิทัลฟอเรนสิกส์ได้ให้บริการแก่ประชาชนและหน่วยงานทั้งภาครัฐและเอกชน ซึ่งในปี 2561 ได้ให้บริการทั้งสิ้น 19 รายการ โดยร้อยละ 47 มาจากหน่วยงานกระบวนการยุติธรรม เช่น ตำรวจ ศาล หรืออัยการ และร้อยละ 42 เป็นการหาร่องรอยอาชญากรรม เช่น การละเมิดลิขสิทธิ์และการพนัน

ถึงแม้ว่าจำนวนการร้องขอใช้บริการในปี 2561 จะลดลงเมื่อเทียบกับปีก่อนหน้าที่มีจำนวนถึง 30 รายการ แต่การตรวจพิสูจน์ไฟล์ประเภทภาพและเสียงมีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่องตั้งแต่ปี 2559 เพื่อพัฒนาศักยภาพให้รองรับกับความต้องการที่เพิ่มขึ้นไทยเซิร์ตได้พัฒนาบุคลากร รวมถึงจัดเตรียมเครื่องมือสำหรับวิเคราะห์ในด้านดังกล่าว นอกจากนี้ยังปรับเพิ่มบทบาทเป็นผู้ให้บริการเก็บพยานหลักฐานกลาง และสนับสนุนเครื่องมือวิเคราะห์ข้อมูลเชิงบูรณาการในกรณีที่องค์กรขาดแคลนเครื่องมือ

สถิติการพัฒนาบุคลากร

กิจกรรมพัฒนาบุคลากรปี 2561

จัดทั้งสิ้น **40 กิจกรรม** (อบรม/ซ้อมรับมือ/บรรยาย/แข่งขัน)
มีผู้เข้าร่วม **4,079 คน**

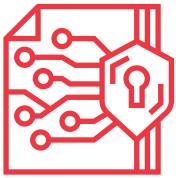


ในปี 2561 ไทยเซิร์ตได้จัดการอบรม การแข่งขัน และการซ้อมรับมือภัยคุกคาม รวมทั้งสิ้น 40 กิจกรรม มีผู้เข้าร่วม 4,079 คน แบ่งเป็น บรรยายให้แก่ผู้บริหารระดับสูง 20 คน (ร้อยละ 0.5) สร้างความตระหนักให้แก่ประชาชนทั่วไป 2,674 คน (ร้อยละ 66) และเสริมสร้างทักษะและศักยภาพให้แก่เจ้าหน้าที่เชิงเทคนิค 1,375 คน (ร้อยละ 34) ทั้งนี้ไทยเซิร์ตได้จัดการอบรมเชิงเทคนิครวม 12 ครั้ง แบ่งตามหัวข้อ ได้แก่ การตอบสนองรับมือภัยคุกคาม การบริหารจัดการและนโยบาย ความมั่นคงปลอดภัยของเครือข่าย การตรวจพิสูจน์พยานหลักฐานดิจิทัล การวิเคราะห์มัลแวร์ และความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ โดยประเภทหน่วยงานที่เข้าร่วมสูงสุด 3 อันดับแรก คือ การเงิน โทรคมนาคม และหน่วยงานภาครัฐ เพื่อเสริมศักยภาพการปกป้องของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ สอดรับกับยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 – 2564

แนวโน้มภัยคุกคามไซเบอร์ปี 2562

แนวโน้มภัยคุกคามไซเบอร์ปี 2562

ทีมไทยเซิร์ตได้วิเคราะห์และสรุปประเด็นสำคัญจากรายงานวิเคราะห์แนวโน้มด้านความมั่นคงปลอดภัยไซเบอร์ปี 2562 ของบริษัทต่าง ๆ เช่น ESET Kaspersky McAfee และ Symantec เป็นต้น ซึ่งความเห็นของแต่ละบริษัทมีลักษณะทั้งที่คล้ายคลึงและแตกต่างกันไป โดยสามารถสรุปเป็นหัวข้อที่น่าสนใจดังต่อไปนี้



กฎหมายและการโจมตีทางไซเบอร์จะส่งผลให้หน่วยงานให้ความสำคัญกับการดูแลข้อมูลส่วนบุคคลมากขึ้น

กฎหมาย General Data Protection Regulation (GDPR) ซึ่งมีผลบังคับใช้เมื่อเดือนพฤษภาคม 2561 ทำให้หน่วยงานต่าง ๆ ตื่นตัวในเรื่องการรักษาข้อมูลส่วนบุคคล เนื่องจากกฎหมายดังกล่าวไม่ได้มีผลบังคับใช้เฉพาะในทวีปยุโรป แต่ยังมีผลต่อทุกหน่วยงานทั่วโลกที่ครอบครองหรือจัดการข้อมูลส่วนบุคคลของประชาชนของยุโรปด้วย นอกจากนี้ยังมีผลกระทบด้านกฎหมายในหลายประเทศ อาทิ สหรัฐอเมริกาได้ผ่านกฎหมาย California Consumer Privacy Act (CCPA) ภายหลังจากมีการบังคับใช้กฎหมาย GDPR 40 วัน

ในขณะเดียวกัน ประเทศไทยก็พยายามผลักดัน (ร่าง) พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล โดยกฎหมายดังกล่าว มีเนื้อหาครอบคลุมการจัดเก็บ รวบรวม และประมวลผลข้อมูลส่วนบุคคลบนพื้นฐานการยินยอมจากเจ้าของข้อมูล ตลอดจนการแจ้งเจ้าของข้อมูลกรณีเกิดข้อมูลรั่วไหล

ในปีที่ผ่านมา ได้พบการรั่วไหลของข้อมูลส่วนบุคคลจำนวนมากจากหน่วยงานต่าง ๆ ทั่วโลก ทั้งที่เกิดจากความผิดพลาดในการตั้งค่าทำให้ถูกเข้าถึงจากสาธารณะ และการถูกโจมตีทางไซเบอร์เพื่อขโมยข้อมูล ตลอดจนมีการเผยแพร่ข้อมูลโดยผู้ประสงค์ร้ายที่ส่งผลต่อชื่อเสียงของหน่วยงานที่เกี่ยวข้อง หน่วยงานที่ต้องดูแลข้อมูลส่วนบุคคลจึงมีความจำเป็นต้องให้ความสำคัญในการรักษาข้อมูลดังกล่าวมากขึ้นพร้อมทั้งเตรียมมาตรการต่าง ๆ ในการป้องกันการถูกโจมตีทางไซเบอร์

การใช้เทคโนโลยี AI มีบทบาทในการป้องกันและโจมตีทางไซเบอร์

บทบาทของ AI ในการป้องกัน

- เฝ้าระวังภัยคุกคามไซเบอร์ของหน่วยงาน โดยให้เรียนรู้พฤติกรรมของผู้ใช้งานเพื่อหาเหตุการณ์ที่ผิดปกติ
- จำลองการโจมตีทางไซเบอร์เพื่อหาช่องโหว่ของระบบ

บทบาทของ AI ในการโจมตี

- ค้นหาช่องโหว่ของระบบเพื่อเลือกเป้าหมายในการโจมตี
- ติดตามพฤติกรรมบนโซเชียลมีเดียเพื่อนำไปหลอกลวง

พบการโจมตีอุปกรณ์ IoT แทนการโจมตีเราเตอร์

หลายปีที่ผ่านมาเราเตอร์ซึ่งถือเป็นอุปกรณ์ประเภท Internet of Thing (IoT) เป็นเป้าหมายหลักในการโจมตีทางไซเบอร์ เช่น ปี 2558 มัลแวร์ Mirai เข้าควบคุมเราเตอร์กว่า 493,000 เครื่อง เพื่อใช้เป็นฐานในการโจมตีบริษัทผู้ให้บริการเว็บโฮสติงในประเทศฝรั่งเศส โดยมีปริมาณการโจมตีสูงถึง 1.1 เทระบิตต่อวินาที[3] ถือเป็นหนึ่งในการโจมตีประเภท DDoS (Distributed-Denial-of-Service) ที่รุนแรงที่สุด

ในปี 2561 การโจมตีอุปกรณ์ IoT มีลักษณะเปลี่ยนแปลงไป โดยเปลี่ยนเป้าการโจมตีจากเราเตอร์เป็นอุปกรณ์อื่น ๆ ตัวอย่างเช่น ผู้ประสงค์ร้ายใช้นามแฝง TheHackerGiraffe เข้าควบคุมเครื่องพิมพ์ (Printer) กว่า 50,000 เครื่องเพื่อสั่งการให้พิมพ์กระดาษที่มีข้อความเชิญชวนให้ติดตามช่อง PewDiePie บนเว็บไซต์ YouTube[4] นอกจากนี้ยังได้เข้าควบคุมอุปกรณ์ Google Chromecast หลายพันเครื่องที่เชื่อมต่อกับโทรทัศน์ให้แสดงเนื้อหาเชิญชวนให้ติดตามช่อง PewDiePie อีกด้วย ทั้งนี้ผู้ประสงค์ร้ายอ้างว่าการกระทำดังกล่าวมีวัตถุประสงค์เพื่อสร้างความตระหนักให้กับประชาชนเกี่ยวกับช่องโหว่ของอุปกรณ์ IoT

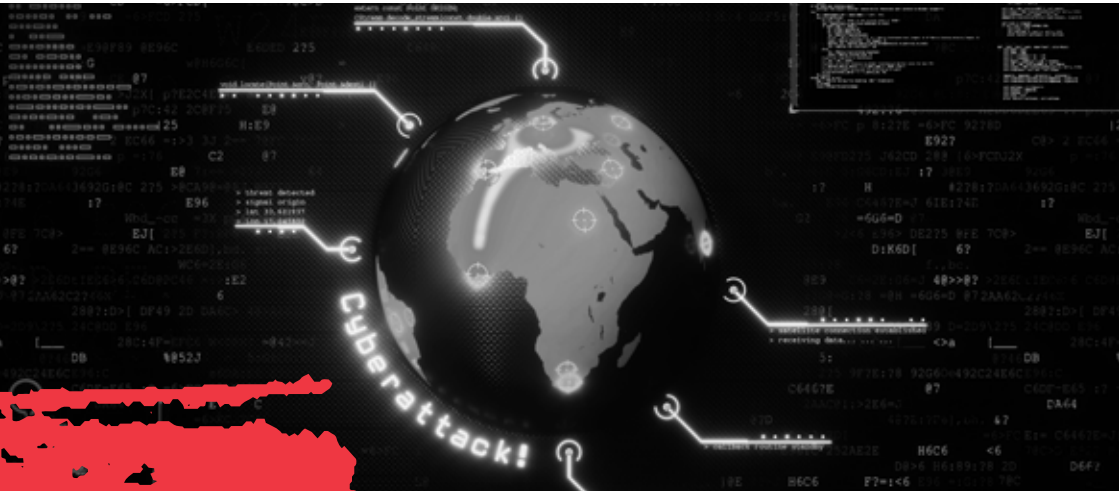
รายงานของบริษัท Symantec[5] และบริษัท McAfee[6] ยังได้ระบุเกี่ยวกับแนวโน้มการโจมตีอุปกรณ์ IoT ในรูปแบบต่าง ๆ ว่าจะเพิ่มมากขึ้นในอนาคต ผู้ใช้งานจึงควรเลือกใช้อุปกรณ์ IoT ที่น่าเชื่อถือ และมีกลไกในการอัปเดตแก้ไขช่องโหว่อย่างสม่ำเสมอ

[3] https://www.thaicert.or.th/papers/general/2016/pa2016ge001.html
[4] https://thehackernews.com/2018/11/pewdiepie-printer-hack.html
[5] https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond
[6] https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/mcafee-labs-2019-threats-predictions/

การโจมตีผ่านผู้ผลิตซอฟต์แวร์ยังคงเป็นการโจมตีแบบวงกว้างที่มีประสิทธิภาพและยังคงถูกใช้ในการโจมตี

ในหลายปีที่ผ่านมาเราได้พบการโจมตีผ่านผู้ผลิตซอฟต์แวร์หลายครั้ง ซึ่งเป็นการโจมตีผู้ผลิตซอฟต์แวร์เพื่อแอบฝังโค้ดอันตรายในซอฟต์แวร์หรือตัวอัปเดตที่เผยแพร่จากเจ้าของผลิตภัณฑ์เช่น ในปี 2559 พบการฝังมัลแวร์เรียกค่าไถ่สายพันธุ์ Notpety ในแพตช์ซอฟต์แวร์ CCleaner เวอร์ชัน 5.33 ซึ่งมีผู้ใช้มากกว่า 2 ล้านรายดาวน์โหลดแพตช์ดังกล่าวจากเซิร์ฟเวอร์ของผู้ผลิตซอฟต์แวร์ อย่างไรก็ตามการโจมตีในรูปแบบนี้ไม่เหมาะกับการโจมตีแบบเฉพาะเจาะจงเนื่องจากถูกตรวจจับได้ง่าย แต่เป็นการโจมตีแบบวงกว้างที่มีประสิทธิภาพและในหลายรายงานเห็นตรงกันว่ายังคงพบเห็นในปี 2562 หน่วยงานจึงควรมีกระบวนการติดตามข่าวสารการแจ้งเตือนเกี่ยวกับซอฟต์แวร์ที่ใช้งาน นอกจากนี้ในรายงาน Symantec[7] ได้คาดการณ์ว่าจะพบการโจมตีผู้ผลิตฮาร์ดแวร์ เช่น การฝังโค้ดอันตรายใน Chip หรือเฟิร์มแวร์ของ BIOS แต่รายงานของ Kaspersky[8] คาดว่ามีโอกาสได้น้อยมาก

[7] https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond
[8] https://securelist.com/kaspersky-security-bulletin-threat-predictions-for-2019/88878/



มีการปลอมบัญชีผู้ใช้งานมากขึ้น

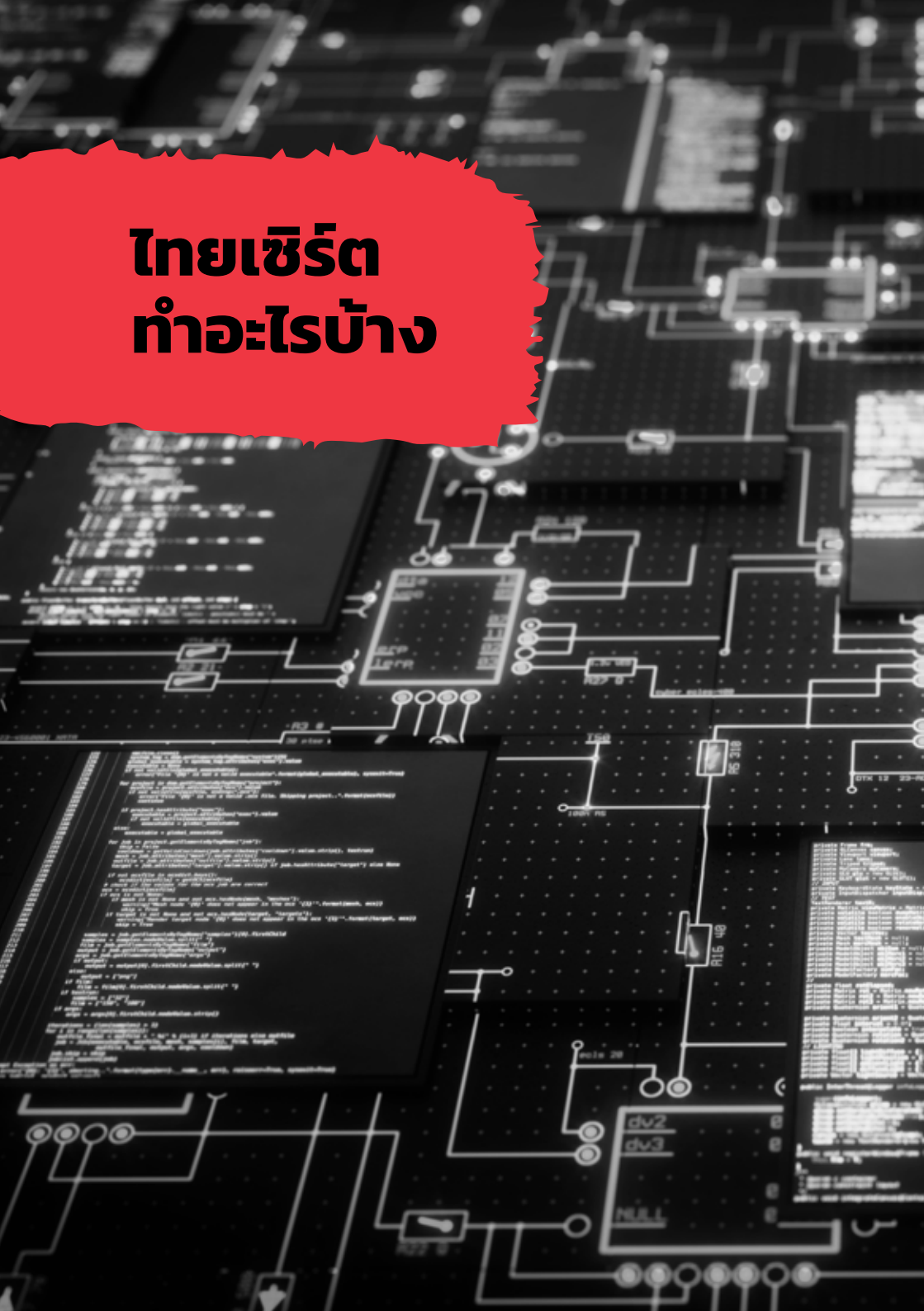
ปัจจุบันนี้ การปลอมบัญชีโซเชียลมีเดียสามารถพบเห็นได้ทั่วไป เช่น การสวมรอยปลอมบัญชีบน Facebook หรือ LINE แล้วอ้างเป็นคนรู้จัก การปลอมอีเมลเป็นบริษัทคู่ค้าเพื่อหลอกลวงให้โอนเงิน อันจะส่งผลต่อความเชื่อมั่นในการทำธุรกรรมออนไลน์

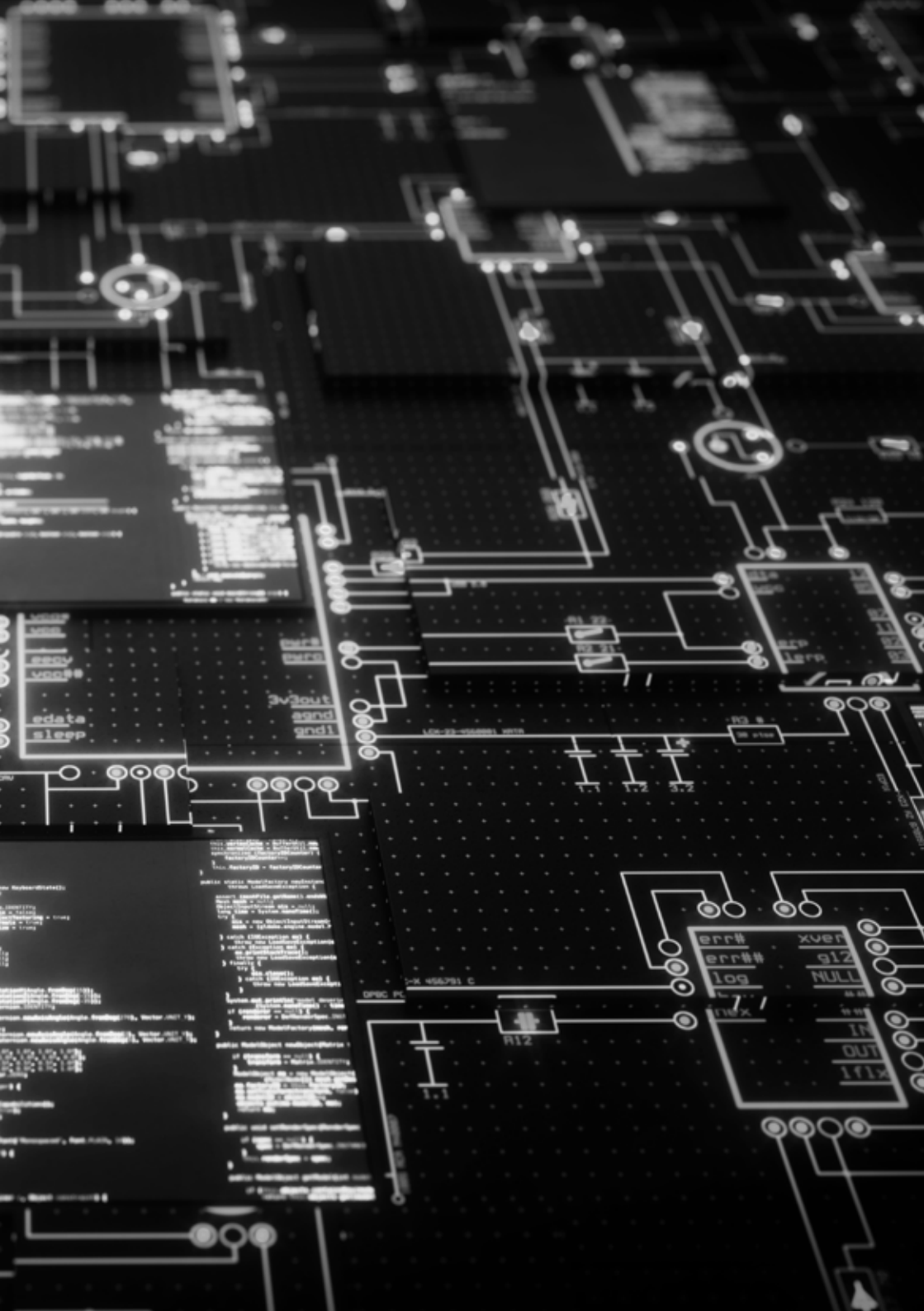
ในปี 2562 ประเทศไทยผลักดันเศรษฐกิจดิจิทัลโดยส่งเสริมให้มีบริการออนไลน์ในรูปแบบต่าง ๆ เช่น บริการธนาคารออนไลน์ บริการ e-wallet ทำให้การทำธุรกรรมออนไลน์เป็นไปอย่างสะดวกรวดเร็ว แต่ในขณะเดียวกันผู้ใช้งานประสบปัญหาในการดูแลบัญชีบริการออนไลน์หลากหลายที่ใช้งานให้มีความมั่นคงปลอดภัย โครงการ National Digital ID[9] ออกแบบให้เชื่อมต่อกับระบบของหน่วยงานต่าง ๆ ทำให้สามารถใช้บัญชีเดียวในการยืนยันตัวตน และสามารถแลกเปลี่ยนข้อมูลระหว่างระบบได้ ซึ่งเป็นการอำนวยความสะดวกในการทำธุรกรรมออนไลน์และง่ายต่อผู้ใช้งานในการดูแลบัญชี

อย่างไรก็ตามในการใช้งานบัญชีเดียวเชื่อมโยงระบบต่าง ๆ หากผู้ประสงค์ร้ายเข้าควบคุมบัญชีดังกล่าว ก็จะสามารถเข้าถึงบริการต่าง ๆ ที่ใช้งานอยู่ รวมถึงบริการทางการเงินที่มักตกเป็นเป้าหมาย ซึ่งจากสถิติการดำเนินการรับมือภัยคุกคามของไทยเซิร์ตพบว่าภัยคุกคามที่ไทยเซิร์ตได้รับแจ้งสูงสุดคือการสร้างเว็บไซต์หลอกลวง (Phishing) เพื่อขโมยข้อมูล และกลุ่มบริการหลักที่ตกเป็นเป้าคือกลุ่มบริการทางการเงิน

ดังนั้น ผู้ใช้งานจึงควรมีความรู้ความเข้าใจเกี่ยวกับภัยไซเบอร์และ Cyber Hygiene ที่เป็นแนวปฏิบัติการใช้งานเทคโนโลยีอย่างมั่นคงปลอดภัย รวมถึงการดูแลบัญชีที่ใช้งานอย่างเหมาะสม เช่น การตั้งรหัสผ่านที่คาดเดาได้ยาก ไม่เปิดเผยรหัสผ่านให้ผู้อื่น การใช้งานการยืนยันตัวตนแบบ 2 ขั้นตอน เพื่อยกระดับความรู้ตัวเองให้เท่าทันการหลอกลวงของผู้ประสงค์ร้าย ทั้งนี้ หน่วยงานกำกับและผู้ให้บริการที่เกี่ยวข้องจำเป็นต้องร่วมช่วยกันดูแลอย่างใกล้ชิดและแจ้งเตือนผู้รับบริการให้หลีกเลี่ยงการตกเป็นเหยื่อตามสถานการณ์ดังกล่าว

[9] https://brandinside.asia/thai-digitalid-nationaldigitalid-electronicpaper-banking


ไทยเซิร์ต
ทำอะไรบ้าง



พันธกิจของไทยเซิร์ต

“ไทยเซิร์ต” ภายใต้การกำกับดูแลของ **สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.)** หรือ **สพธอ.** มีชื่ออย่างเป็นทางการว่า**“ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย”** หรือ **“Thailand Computer Emergency Response Team” (ThaiCERT)** มีพันธกิจในการแก้ไขสถานการณ์ด้านความมั่นคงปลอดภัยทั้งที่ได้รับแจ้งและตรวจพบเองในขอบเขตครอบคลุมระบบเครือข่ายอินเทอร์เน็ตและเว็บไซต์ภายใต้โดเมนเนม (Domain Name) ของประเทศไทย โดยทำงานร่วมกับหน่วยงานในเครือข่ายและหน่วยงานที่เกี่ยวข้อง อีกทั้งให้ความสำคัญกับการพัฒนาบุคลากรเพื่อเพิ่มขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยภายในประเทศไทย และให้คำปรึกษาแก่หน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) ในเรื่องของการป้องกันและแก้ไขปัญหาภัยคุกคามไซเบอร์ เพื่อรักษาความต่อเนื่องในการดำเนินภารกิจของหน่วยงานนั้น ๆ

ไทยเซิร์ตมีภารกิจหลักในการรับมือกับสถานการณ์ภัยคุกคามไซเบอร์ของประเทศไทย ด้วยการประสานระหว่างบุคลากรผู้เชี่ยวชาญ กระบวนการทำงานที่ได้รับมาตรฐาน เทคโนโลยีทันสมัยที่นำมาประยุกต์ใช้ในงาน และเครือข่ายความร่วมมือจากทั่วโลก เพื่อเชื่อมโยงการทำงานให้มีประสิทธิภาพสูงสุดและสามารถรับมือภารกิจที่สำคัญได้อย่างต่อเนื่อง

บริการของไทยเซิร์ต

ปัจจุบันไทยเซิร์ตให้บริการสำคัญเพื่อจัดการรับมือและป้องกันภัยคุกคามไซเบอร์ เช่น บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย บริการเฝ้าระวังและป้องกันภัยคุกคาม บริการตรวจพิสูจน์พยานหลักฐานดิจิทัล บริการ Threat Intelligence ซึ่งรวบรวมข้อมูลแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร รวมถึงบริการพัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อยกระดับความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์และสนับสนุนการพัฒนาเศรษฐกิจดิจิทัลของประเทศไทย โดยดำเนินการใน 3 รูปแบบคือ

• **บริการเชิงรุก**เพื่อป้องกันภัยคุกคาม (Proactive Services) เช่น การตรวจสอบและให้คำแนะนำในการปิดช่องโหว่ของระบบ

• **บริการเชิงรับ**เพื่อตอบสนองภัยคุกคาม (Reactive Services) เพื่อจำกัดความเสียหายจากภัยคุกคามให้เหลือน้อยที่สุดและดำเนินการป้องกันไม่ให้เกิดขึ้นอีก

• **บริการบริหารคุณภาพ**ทางด้านความมั่นคงปลอดภัย (Security Quality Management Services) ซึ่งเป็นการให้บริการวิชาการเพื่อพัฒนาความสามารถและสร้างความตระหนักแก่บุคลากรให้รู้เท่าทันและรับมือภัยคุกคามได้อย่างทันท่วงที

PROACTIVE SERVICES

- CYBER PRACTICE RECOMMENDATION
- TECHNOLOGY WATCH
- SECURITY AUDITS OR ASSESSMENTS
- CONFIGURATION AND MAINTAINANCE OF SECURITY TOOLS, APPLICATIONS, AND INFRASTRUCTURES
- INTRUSION DETECTION SERVICES
- SECURITY-RELATED INFORMATION DISSEMINATION

REACTIVE SERVICES

- ALERTS AND WARNINGS
- INCIDENT HANDLING
- VULNERABILITY HANDLING
- ARTIFACT HANDLING

SECURITY QUALITY MANAGEMENT SERVICES

- BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING
- SECURITY CONSULTING
- AWARENESS BUILDING
- EDUCATION/TRAINING

บริการเชิงรุกเพื่อป้องกันภัยคุกคาม (Proactive Services)

ไทยเซิร์ตได้ปฏิบัติงานในเชิงรุกด้วยมุ่งหวังว่าจะช่วยลดความเสี่ยงในการเกิดภัยคุกคาม และให้บริการที่มุ่งเน้นการสนับสนุนหน่วยงานต่าง ๆ ในการเตรียมพร้อม หลีกเลี่ยง และป้องกันระบบจากการถูกโจมตี ซึ่งจะนำไปสู่การลดลงของสถิติภัยคุกคามร้ายแรงที่เกิดขึ้นได้อย่างมีนัยสำคัญ โดยการบริการเชิงรุกหลักประกอบด้วย บริการแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร บริการเฝ้าติดตามภัยคุกคาม บริการตรวจสอบและประเมินความมั่นคงปลอดภัย

• บริการแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร (Threat Intelligence)

เนื่องจากในปัจจุบันมีภัยคุกคามรูปแบบใหม่เกิดขึ้นอยู่เสมอ ไทยเซิร์ตติดตามข่าวสารด้านความมั่นคงปลอดภัยไซเบอร์จากเครือข่าย CERT และแหล่งข้อมูลที่น่าเชื่อถือทั่วโลก โดยนำมาประเมินและวิเคราะห์ผลกระทบกับระบบสารสนเทศในประเทศไทยก่อนที่จะแจ้งเตือน พร้อมทั้งเสนอข้อแนะนำในการป้องกันและแก้ไขให้สาธารณะได้ทราบในรูปแบบข่าวสั้น (News-Bite) บทความแจ้งเตือน บทความเชิงเทคนิค Infographic และคลิปวิดีโอ รวมถึงเผยแพร่ข้อมูลสถิติภัยคุกคามที่ไทยเซิร์ตประสานงานรับมือและจัดการภัยคุกคามในแต่ละเดือนทางเว็บไซต์ของไทยเซิร์ต (www.thaicert.or.th) โดยจะมีการรวบรวมและวิเคราะห์สถิติภัยคุกคามในแต่ละเดือนและเหตุการณ์สำคัญที่เกิดขึ้นในรอบปี เพื่อกำหนดนโยบายด้านความมั่นคงปลอดภัยไซเบอร์ และวางแผนป้องภัยคุกคามให้แก่ประชาชนและองค์กรต่าง ๆ

• บริการเฝ้าติดตามภัยคุกคาม (Threat Watch)

ไทยเซิร์ตได้พัฒนาระบบ Threat Watch เพื่อเฝ้าติดตามข้อมูลภัยคุกคามตั้งแต่ปี 2557 โดยเป็นระบบที่สามารถรวบรวมและเฝ้าติดตามภัยคุกคามจากแหล่งข้อมูลบนอินเทอร์เน็ต เช่น เว็บไซต์ที่มีการเผยแพร่มัลแวร์ หรือข้อมูลรั่วไหลจากการเจาะระบบเว็บไซต์ นอกจากนี้ไทยเซิร์ตได้เฝ้าติดตามการข่าวจากแหล่งข้อมูลต่าง ๆ เช่น หน่วยงานที่เกี่ยวข้องซึ่งเป็นพันธมิตรกับไทยเซิร์ต แหล่งข้อมูลออนไลน์ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง เพื่อนำมาใช้วิเคราะห์ประเมินผล และตีความให้ได้แหล่งข้อมูลออนไลน์เกี่ยวกับภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น และนำไปใช้ในการวางแผนป้องกันหรือจัดการภัยนั้น ๆ ให้ทันท่วงทีหรือส่งผลกระทบน้อยที่สุด อีกทั้งสามารถนำไปใช้เป็นแนวทางในการวางแผนรับมือภัยคุกคามที่อาจขึ้นในอนาคตได้อีกด้วย

• บริการตรวจสอบและประเมินความมั่นคงปลอดภัย (Security Assessment)

เป็นบริการที่จะช่วยให้หน่วยงานทราบถึงช่องโหว่ของระบบสารสนเทศของตนเอง และสามารถนำไปวิเคราะห์เพื่อจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management Plan: RMP) และแผนบริหารจัดการความต่อเนื่องทางธุรกิจ (Business Continuity Management: BCM) ของหน่วยงานได้

บริการเชิงรับเพื่อตอบสนองภัยคุกคาม (Reactive Services)

ในกรณีที่เกิดเหตุการณ์โจมตีทางไซเบอร์ ไทยเซิร์ตให้การสนับสนุนแก่หน่วยงานทั้งด้านข้อมูลและด้านเทคนิค เพื่อให้สามารถรับมือต่อภัยคุกคามที่ส่งผลกระทบต่อระบบสารสนเทศของตนได้ การบริการเชิงรับหลักประกอบด้วย บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย (Incident Handling) และบริการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics)

• บริการรับมือและจัดการสถานการณ์ด้านความมั่นคงปลอดภัย (Incident Handling)

ไทยเซิร์ตเป็นหน่วยงานประเภท CERT ในระดับประเทศ ทำหน้าที่ให้บริการ 24x7 ในการรับแจ้งเหตุภัยคุกคาม ตรวจสอบและวิเคราะห์หาสาเหตุ และประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อระงับเหตุและแก้ไขกรณีภัยคุกคามนั้น ๆ เพื่อจำกัดความเสียหายที่อาจเกิดขึ้น พร้อมฟื้นฟูระบบและการให้บริการโดยเร็วที่สุด ไทยเซิร์ตได้รับการยอมรับในฐานะเป็นตัวแทนประเทศไทยในเครือข่าย CERT ระหว่างประเทศ เช่น เครือข่าย Asia Pacific CERT (APCERT) และ Forum of Incident Response and Security Teams (FIRST) นอกจากนี้ยังมีการเฝ้าระวังภัยคุกคามให้กับหน่วยงานภาครัฐภายใต้โครงการ ThaiCERT Government Monitoring System (ThaiCERT GMS)

• บริการตรวจพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics)

ศูนย์ดิจิทัลฟอเรนสิกส์ทำหน้าที่ตรวจพิสูจน์พยานหลักฐานดิจิทัลและออกรายงานผลการตรวจวิเคราะห์ตามคำร้องขอของหน่วยงานรักษากฎหมาย รวมทั้งให้คำปรึกษาและคำแนะนำทางเทคนิคแก่เจ้าหน้าที่ซึ่งอาจไม่คุ้นเคยกับเทคโนโลยีและพยานหลักฐานดิจิทัลสมัยใหม่ที่มีรูปแบบต่าง ๆ กันทั้งนี้ ศูนย์ดิจิทัลฟอเรนสิกส์บริหารจัดการกระบวนการตรวจพิสูจน์อย่างเป็นระบบภายใต้กรอบมาตรฐานสากล เพื่อรักษาความต่อเนื่องของการครอบครองพยานหลักฐาน หรือ Chain of Custody ที่ได้มาตรฐานเพื่อให้ผลการตรวจพิสูจน์มีความน่าเชื่อถือและสามารถนำไปใช้ในชั้นศาลได้

บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย (Security Quality Management Services)

หมายถึงบริการสนับสนุนการบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร ซึ่งบริการหลักประกอบด้วยบริการพัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัย (Cybersecurity Skills Development) และการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย (Awareness Building)

• บริการพัฒนาทักษะบุคลากรด้านความมั่นคงปลอดภัย (Cybersecurity Skills Development)

ไทยเซิร์ตเล็งเห็นว่าการยกระดับความรู้ในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้แก่บุคลากร ตลอดจนผู้บริหาร มีความสำคัญต่อการยกระดับความเข้มแข็งของการรักษาความมั่นคงปลอดภัยในองค์กร ไทยเซิร์ตจึงได้เป็นเจ้าภาพจัดอบรมแลกเปลี่ยนข้อมูลเพื่อให้ความรู้เรื่องความมั่นคงปลอดภัย ซึ่งมีการเชิญวิทยากรและผู้ทรงคุณวุฒิจากทั้งในและต่างประเทศมาบรรยายและแลกเปลี่ยนความรู้ นอกจากนี้ ไทยเซิร์ตยังได้จัดตั้งศูนย์ความร่วมมืออาเซียน - ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ จัดการซ้อมรับมือภัยคุกคาม รวมทั้งเตรียมความพร้อมให้กับบุคลกรทั้งในและนอกองค์กรที่มีความสนใจด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเข้าสอบประกาศนียบัตรสำหรับผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยที่ได้รับการยอมรับในระดับสากล

• การสร้างความตระหนักเรื่องความมั่นคงปลอดภัย (Awareness Building)

ไทยเซิร์ตเผยแพร่ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานต่าง ๆ ทั้งภาครัฐ ภาคเอกชน และบุคคลทั่วไป โดยเป็นการเผยแพร่ความรู้ทั้งในลักษณะการบรรยาย และการจัดกิจกรรมภาคปฏิบัติ เช่น โครงการสร้างความตระหนักในการใช้อินเทอร์เน็ตให้เสริมสร้างรายได้และรู้เท่าทันภัยคุกคามไซเบอร์ (Internet for Better Life) เพื่อช่วยให้ความรู้และความตระหนักในการใช้อินเทอร์เน็ตอย่างมั่นคงปลอดภัยแก่นักเรียนระดับชั้นประถมศึกษาและมัธยมศึกษา

เจาะลึกเคสรับมือภัยไซเบอร์ของไทยเซิร์ต

การแพร่ระบาดของ WannaCry

ในช่วงเดือนกลางปี 2560 มีรายงานการแพร่ระบาดของมัลแวร์เรียกค่าไถ่ชื่อ WannaCry อย่างหนักทั่วโลก โดยมัลแวร์ดังกล่าวมีจุดประสงค์หลักคือการเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้

สิ่งที่น่ากังวลเป็นพิเศษสำหรับมัลแวร์นี้คือความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ระบบ SMB (Server Message Block) ของ Windows ผู้ใช้งานที่ไม่อัปเดตระบบปฏิบัติการดังกล่าวมีความเสี่ยงที่จะติดมัลแวร์นี้

ช่องโหว่ที่ถูกใช้ในการแพร่กระจายมัลแวร์เป็นช่องโหว่ที่ถูกเปิดเผยสู่สาธารณะตั้งแต่ช่วงเดือนเมษายน 2560 และถึงแม้ทาง Microsoft จะเผยแพร่อัปเดตแก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แล้วแต่ยังพบว่ามีเครื่องคอมพิวเตอร์ที่ยังไม่ได้อัปเดตแพตช์ดังกล่าวและถูกโจมตีจากมัลแวร์นี้มากกว่า 200,000 เครื่อง จาก 112 ประเทศ ซึ่งเกิดผลกระทบสูงต่อหน่วยงานสาธารณสุขของประเทศอังกฤษ

ในประเทศไทย ไทยเซิร์ตได้ตรวจสอบพบผู้ติดมัลแวร์ตัวนี้อยู่บ้างเป็นจำนวน 258 เครื่อง แต่ยังไม่พบการแพร่กระจายในวงกว้าง อย่างไรก็ตามไทยเซิร์ตได้เฝ้าระวังหน่วยงานสำคัญ รวมถึงให้ความช่วยเหลือและให้คำแนะนำผู้ที่ได้รับผลกระทบ

SSD กับการตรวจพิสูจน์พยานหลักฐานดิจิทัล

ในปี 2560 ศูนย์ดิจิทัลฟอเรนสิกส์ ได้รับพยานหลักฐานประเภท SSD (Solid State Drive) เข้ามาให้ตรวจพิสูจน์มากขึ้น เนื่องมาจากความนิยมใช้ SSD ที่เพิ่มสูงขึ้น ถึงแม้ว่าจะมีราคาสูงกว่าและมีขนาดความจุที่น้อยกว่าฮาร์ดดิสก์แบบจานหมุน HDD (Hard Disk Drive) ก็ตาม แต่ SSD มีข้อดีและมีความสามารถอื่น ๆ ที่เหนือกว่า HDD หลายประการ เช่น ใช้ไฟฟ้าน้อยกว่า มีขนาดเล็กกว่าและน้ำหนักเบากว่า มีความร้อนน้อยกว่า เสียงเบากว่า ไม่มีเสียงดังของจานหมุน และข้อดีที่สำคัญคือ ทำงานเร็วกว่า HDD โดยสามารถเข้าถึงข้อมูลในตำแหน่งที่ต้องการอ่านหรือเขียนได้ทันที ในขณะที่ HDD ต้องรอให้หัวอ่านเลื่อนไปหาตำแหน่งข้อมูลที่ต้องการก่อน

เนื่องด้วย SSD ใช้หน่วยเก็บข้อมูลประเภท NAND Flash ซึ่งมีข้อจำกัดของจำนวนครั้งที่สามารถเขียนข้อมูลลงในหน่วยความจำได้ หากมีการเขียนข้อมูลลงในหน่วยเก็บข้อมูลพื้นที่เดิมบ่อย ๆ จะทำให้พื้นที่นั้นใช้งานไม่ได้อีกต่อไป ดังนั้น เพื่อแก้ปัญหาเรื่องอายุการใช้งานของ SSD จึงได้มีการใช้ 2 เทคนิค ดังนี้

1. Ware Leveling: เมื่อมีการเปลี่ยนแปลงเนื้อหาของไฟล์ใด ๆ เนื้อหาของไฟล์นั้นจะถูกย้ายไปแล้วบันทึกเป็นไฟล์ใหม่ลงในพื้นที่อื่นใน SSD ส่วนพื้นที่เดิมที่เก็บเนื้อหาของไฟล์เก่าจะไปเข้าคิวรอการเคลียร์ข้อมูล

2. Drive Trimming: หรือ Trimming เป็นการเคลียร์ข้อมูลที่อยู่ในตำแหน่งเก่า อาจเป็นข้อมูลที่เกิดจากการเปลี่ยนแปลงเนื้อหาไฟล์ การลบไฟล์หรือการฟอร์แมต เพื่อให้พื้นที่นั้นพร้อมรับการเขียนข้อมูลใหม่ ในระบบปฏิบัติการ Windows 7/8/10 กระบวนการ Trimming ได้ตั้งค่าเริ่มต้น (Default) ให้ทำงานอัตโนมัติตามการตั้งค่าของระบบปฏิบัติการ (Scheduler) โดยทั่วไปมักทำเป็นรายสัปดาห์

แม้ว่าเทคนิค Ware Leveling และ Trimming จะช่วยเรื่องอายุการใช้งานของ SSD และทำให้ SSD ทำงานได้เร็วขึ้น แต่ส่งผลกระทบต่อการตรวจพิสูจน์ด้วยอุปสรรคที่เกิด ได้แก่

1. การเก็บรวบรวมพยานหลักฐานไม่สามารถใช้วิธีดั้งเดิมอีกต่อไป

วิธีดั้งเดิมในข้างต้นหมายถึง กรณีเมื่อผู้เก็บรวบรวมพยานหลักฐาน ณ ที่เกิดเหตุพบเครื่องคอมพิวเตอร์ที่เปิดทิ้งไว้ หลังจากทำสำเนา Volatile Data แล้ว (โดยทั่วไป Volatile Data หมายถึงข้อมูลที่อยู่ใน RAM ซึ่งจะหายไปเมื่อปิดคอมพิวเตอร์) ก็จะดึงปลั๊กที่เชื่อมต่อกับเครื่องคอมพิวเตอร์ออกเพื่อรักษาสภาพของข้อมูล (หากปิดเครื่องด้วยวิธีปกติ จะทำให้มีการเขียนไฟล์และข้อมูลอื่น ๆ เพิ่มเติมก่อนเครื่องถูกปิดลง) จากนั้นจึงนำเครื่องคอมพิวเตอร์เพื่อกลับมาวิเคราะห์ต่อไป

หากคอมพิวเตอร์ที่กำลังทำงานอยู่ใช้ SSD การดึงปลั๊กออกอย่างกะทันหันอาจทำให้ SSD เสียหาย (Brick) อย่างไรก็ตาม เมื่อมีการจ่ายไฟเข้าไปอีกครั้ง SSD ส่วนมากจะสามารถซ่อมแซมข้อมูลในตัวเองได้ ซึ่งในกระบวนการซ่อมแซมข้อมูลนั้นรวมไปถึงการทำ Ware Leveling และ

Trimming ซึ่งจะเป็นปัญหา เนื่องจากสภาพหลักฐาน (ข้อมูลใน SSD) จะถูกเปลี่ยนแปลงไปแล้วเมื่อเทียบกับข้อมูลในสถานที่เกิดเหตุ

ดังนั้น แนวทางปฏิบัติที่นิยมกันสำหรับ SSD จึงเป็นการทำสำเนาข้อมูลในเครื่องคอมพิวเตอร์ในที่เกิดเหตุ ขณะที่เครื่องกำลังเปิดอยู่

2. การใช้เครื่องมือป้องกันการเขียน (Write Blocker) ไม่สามารถป้องกันการเปลี่ยนแปลงข้อมูลได้

โดยปกติ Write Blocker จะใช้เชื่อมต่อกับสื่อบันทึกข้อมูล เพื่อป้องกันการเขียนข้อมูลลงไปในสื่อบันทึกข้อมูลนั้น เช่น การเชื่อมต่อกับพยานหลักฐานต้นฉบับในขั้นตอนการทำเนาข้อมูล เป็นต้น

ในกรณีของ SSD เมื่อเชื่อมต่อกับ Write Blocker จะมีการจ่ายไฟเข้าไป Controller ของ SSD และ Controller อาจเริ่มกระบวนการ Ware Leveling และ Trimming โดยอัตโนมัติ ทำให้ข้อมูลในพยานหลักฐานถูกเปลี่ยนแปลง ดังนั้น หากมีการนำ SSD เดิมมาทำสำเนาข้อมูลซ้ำอีกครั้ง อาจจะได้ค่าแฮชไม่เหมือนเดิม (ค่าแฮชเป็นค่าที่ได้มาจากการใช้อัลกอริทึมคำนวณเนื้อหาของข้อมูล โดยหากข้อมูล 2 ชุดมีค่าแฮชตรงกัน สามารถเชื่อได้ว่าข้อมูลทั้ง 2 ชุดมีเนื้อหาเหมือนกันทุกประการ รูปแบบค่าแฮชที่นิยม เช่น MD5, SHA1 และ SHA256)

3. อาจไม่สามารถกู้คืนข้อมูลที่ถูกลบไปแล้วได้

ในกรณีของ HDD ข้อมูลที่ลบหรือฟอร์แมตไปแล้วจะยังสามารถกู้คืนกลับมาได้ ตราบเท่าที่พื้นเก็บข้อมูลตำแหน่งนั้นยังไม่มีการเขียนทับ เนื่องจากระบบไฟล์ (เช่น NTFS หรือ FAT32) และระบบปฏิบัติการเพียงแค่บันทึกข้อมูลไว้ว่าพื้นที่ตำแหน่งนี้ว่าง สามารถเขียนทับได้ ทำให้ผู้ใช้งานมองไม่เห็นข้อมูลนั้นอีก แต่ข้อมูลยังมีอยู่ที่ตำแหน่งเดิม

ในกรณีของ SSD หากเกิดกระบวนการ Trimming แล้ว ข้อมูลเก่าจะถูกลบออกไปโดยไม่สามารถกู้คืนได้อีก ซึ่งนับเป็นอุปสรรคสำคัญต่อการตรวจพิสูจน์

การตรวจพิสูจน์แอปพลิเคชันให้บริการดูภาพยนตร์ออนไลน์ละเมิดลิขสิทธิ์บน Android TV Box

ปี 2557 บริษัทกูเกิลเปิดตัวผลิตภัณฑ์ใหม่ในชื่อ แอนดรอยด์ทีวี ซึ่งเป็นอุปกรณ์ที่ทำให้เราสามารถรับชมรายการโทรทัศน์ ภาพยนตร์ เล่นเกมส์ รวมทั้งเข้าใช้งานเว็บไซต์ผ่านแอปพลิเคชันบนระบบปฏิบัติการแอนดรอยด์ โดยมีรูปแบบการใช้งาน 2 รูปแบบ คือ แบบติดตั้งระบบปฏิบัติการไว้ในโทรทัศน์ และแบบกล่องเซ็ตท็อปบอกซ์ที่เรียกว่า Android TV Box

เนื่องจากแต่ละครัวเรือนมีโทรทัศน์อยู่แล้ว ดังนั้น Android TV Box จึงเป็นที่นิยมมากกว่า อีกทั้งมีให้เลือกหลายยี่ห้อหลายราคา วิธีใช้งานค่อนข้างง่าย เพียงแค่นำ Android TV Box มาเชื่อมต่อกับโทรทัศน์และอินเทอร์เน็ตก็สามารถใช้งานได้ ส่วนวิธีการดาวน์โหลดและใช้งานแอปพลิเคชันเหมือนการใช้งานสมาร์ตโฟนระบบปฏิบัติการแอนดรอยด์ทั่วไป ซึ่งหลายคนใช้เป็นอยู่แล้ว

ด้วยการใช้งานอย่างแพร่หลายของ Android TV Box ส่งผลให้ผู้ประสงค์ร้ายใช้เป็นช่องทางในการแสวงหาผลประโยชน์ ซึ่งรูปแบบที่มักจะพบบ่อยคือ การเผยแพร่แอปพลิเคชันสำหรับรับชมภาพยนตร์ออนไลน์ที่ละเมิดลิขสิทธิ์ที่มีค่าบริการถูกกว่าการซื้อหรือดาวน์โหลดภาพยนตร์จากแหล่งที่ถูกลิขสิทธิ์

ในปี 2560 ศูนย์ดิจิทัลฟอเรนสิกส์ได้รับพยานหลักฐานที่เป็น Android TV Box โดยหน่วยงานผู้ขอรับบริการขอให้ศูนย์ฯ ตรวจพิสูจน์แอปพลิเคชันที่ติดตั้งไว้ในพยานหลักฐาน ว่าเป็นแอปพลิเคชันที่ให้บริการดูภาพยนตร์และถ่ายทอดสดกีฬาหรือไม่ และถ่ายทอดสัญญาณมาจากหมายเลขไอพีใด

ในการตรวจพิสูจน์ ผู้ตรวจพิสูจน์ได้ใช้เครื่องมือทำสำเนาแอปพลิเคชันที่น่าสงสัยออกมาจากพยานหลักฐานเป็นไฟล์นามสกุล APK (Android Package Kit) ซึ่งเป็นแพ็กเกจสำหรับใช้ติดตั้งโปรแกรมต่าง ๆ บนระบบปฏิบัติการแอนดรอยด์ จากนั้นวิเคราะห์ไฟล์ดังกล่าวเพื่อหากลไกการทำงาน (Reverse Engineering) พบว่าแอปพลิเคชันเรียกหน้าเว็บไซต์หนึ่งมาแสดงผล ผู้ตรวจพิสูจน์จึงได้ตรวจสอบเพิ่มเติมโดยการติดตั้งและเปิดแอปพลิเคชันนั้นใน

แท็บเล็ตที่เป็นระบบปฏิบัติการแอนดรอยด์ของศูนย์ฯ ซึ่งจัดเตรียมไว้สำหรับการวิเคราะห์ข้อมูลโดยเฉพาะ หลังจากเปิดแอปพลิเคชันแล้ว พบหน้าเว็บไซต์แสดงส่วนที่ให้กรอกชื่อบัญชีผู้ใช้และรหัสผ่าน ผู้ตรวจพิสูจน์จึงกรอกชื่อบัญชีผู้ใช้และรหัสผ่านที่ทางผู้ขอรับบริการจัดเตรียมไว้ให้ พบว่าสามารถรับชมภาพยนตร์และถ่ายทอดสดกีฬาได้

จากนั้น ผู้ตรวจพิสูจน์จึงใช้เครื่องมือวิเคราะห์การทำงานของเครือข่าย พบว่ามีสัญญาณถ่ายทอด (Streaming) มาจากหมายเลขไอพีทั้งในและต่างประเทศ

ศูนย์ฯ ได้ส่งรายงานผลการตรวจพิสูจน์ให้หน่วยงานผู้ขอรับบริการ เพื่อนำหมายเลขไอพีประสานไปยังผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) เป็นข้อมูลประกอบการสืบสวนสอบสวนต่อไป

รู้ไว้ใช่ว่า

การตรวจพิสูจน์พยานหลักฐานดิจิทัลประเภทวิดีโอ

ปัจจุบัน ไฟล์ประเภทวิดีโอมีปริมาณสูงขึ้นจากในอดีตอย่างเห็นได้ชัด อันเป็นผลเนื่องมาจากความก้าวหน้าทางเทคโนโลยีและความแพร่หลายของสมาร์ตโฟน และในขณะเดียวกัน ประชาชนยังนิยมติดกล้องวงจรปิดและกล้องหน้ารถมากขึ้น เพื่อบันทึกสถานการณ์ที่ไม่คาดคิด เช่น อุบัติเหตุ หรืออาชญากรรม ซึ่งในส่วนนี้เองที่ไฟล์วิดีโออาจถูกนำมาใช้เป็นพยานหลักฐานประกอบการพิจารณาคดีความ

อย่างไรก็ตาม ไฟล์วิดีโอจากอุปกรณ์ข้างต้นมักมีข้อจำกัดหลายประการ โดยเฉพาะอย่างยิ่งในแง่ความคมชัดของภาพ เป็นต้นว่า หากวิดีโอมีความละเอียดไม่เพียงพอ จะทำให้ไม่สามารถอ่านข้อมูลตัวอักษรขนาดเล็ก เช่น ป้ายทะเบียนรถได้ แต่ทั้งนี้วิดีโอดังกล่าวอาจไม่ไร้ประโยชน์เสียทีเดียว ด้วยการใช้เทคนิคปรับปรุงรูปภาพและวิดีโอ (Image/Video Enhancement) เข้ามาช่วย อาจสามารถดึงข้อมูลที่ตามนุษย์มองไม่เห็นออกมาได้บ้าง

รูปภาพและวิดีโอมีวิธีปรับปรุงทางดิจิทัลอยู่หลายแบบ ที่คนทั่วไปรู้จักดีคือการปรับความสว่าง (Brightness) เฉดสี (Hue) ระดับสี (Levels) หรือมุมมอง (Perspective) นอกจากนี้ ยังมีเทคนิคขั้นสูงอื่นอีก เช่น การตัดสัญญาณภาพรบกวน (Denoising) ขจัดความเลือนจากการเคลื่อนไหว (Motion Deblurring) ปรับเสถียรภาพของวัตถุในวิดีโอ (Stabilization) เฉลี่ยภาพแต่ละฉาก (Frame Averaging) หรือปรับสมดุลฮิสโทแกรม (Histogram Equalization) ซึ่งล้วนเป็นผลจากการพัฒนาองค์ความรู้ทางคณิตศาสตร์ทั้งสิ้น ผู้ตรวจพิสูจน์ต้องอาศัยทักษะและประสบการณ์ในการเลือกใช้วิธีที่เหมาะสมกับปัญหาที่พบในรูปภาพหรือวิดีโอและเป้าหมายในการปรับปรุง

นอกเหนือจากการปรับปรุงให้คมชัดแล้วยังมีรูปแบบการตรวจพิสูจน์อื่นอีก ตัวอย่าง เช่น การประมาณส่วนสูงของผู้ต้องสงสัยที่ปรากฏในรูปหรือวิดีโอ ซึ่งการที่จะคำนวณค่าส่วนสูงได้อย่างแม่นยำได้นั้น จำเป็นต้องกลับไปสำรวจที่เกิดเหตุเพื่อหาวัตถุในระนาบที่จะใช้อ้างอิง ซึ่งต้องเป็นระนาบที่ตั้งฉากกันในทั้งสามมิติและอยู่ในระนาบเดียวกันกับที่ผู้ต้องสงสัยยืนอยู่ แล้ววัดความยาววัตถุนั้น เพื่อนำไปใช้

คำนวณส่วนสูงด้วยหลักการทางเรขาคณิต และมาตรวิทยา

อุปสรรคที่มักพบในการปรับปรุงรูปภาพและวิดีโอ คือ ความละเอียดตั้งต้นไม่เพียงพอ เช่น อักขระละตินพื้นฐาน (อักษร A-Z และตัวเลขอารบิก 0-9) บนป้ายทะเบียนรถควรมีความสูงไม่ต่ำกว่า 8 พิกเซล ส่วนพยัญชนะไทย ก-ฮ ซึ่งมีลักษณะซับซ้อนสูง จะต้องมีความละเอียดมากยิ่งขึ้น โดยเฉพาะเมื่อมีรูปอักษรคล้ายกัน อย่าง ก/ถ/ภ เป็นต้น ส่วนการคำนวณส่วนสูงมีความแม่นยำจำกัด หากบุคคลนั้นไม่ได้อยู่ในท่ายืนตรง หรือไม่ได้อยู่ในระนาบเดียวกับเส้นขนานสามคู่นั้น

เทคนิคยุคใหม่มีการประยุกต์ใช้ปัญญาประดิษฐ์ (Artificial Intelligence) มากขึ้น เช่น การจดจำอัตลักษณ์ของคน หรือติดตามวัตถุ เพื่อย่นระยะเวลาที่ใช้ในการตรวจพิสูจน์ และวิเคราะห์ได้อย่างแม่นยำ

การจัดตั้ง Sector-based CERT

ภัยคุกคามไซเบอร์ที่เปลี่ยนแปลงไปอย่างรวดเร็วและทวีความรุนแรงมากยิ่งขึ้น ทำให้หลายหน่วยงานเกิดความตระหนักถึงความสำคัญในการมีทีมงานด้านความมั่นคงปลอดภัย เพื่อรับมือกับภัยคุกคามไซเบอร์ได้อย่างทันท่วงที รวมถึงการแลกเปลี่ยนข้อมูลกับทีมหรือหน่วยงานอื่น ๆ เพื่อควบคุมและระงับการแพร่ขยายของเหตุภัยคุกคามให้เร็วที่สุด

สพธอ. เล็งเห็นถึงความสำคัญในเรื่องนี้และเดินหน้าสนับสนุนการจัดตั้ง CERT/CSIRT มาโดยตลอด เห็นได้จากการจัดบรรยายและสัมมนาหลาย ๆ ครั้ง ตลอดจนการจัดทำหนังสือคู่มือการจัดตั้ง CSIRT ด้วย อย่างไรก็ตามการที่มีทีมเฉพาะทางด้านความมั่นคงปลอดภัยภายในหน่วยงานอาจยังไม่เพียงพอต่อการรับมือภัยคุกคามขนาดใหญ่ที่ส่งผลข้ามหน่วยงานหรือในระดับภาคธุรกิจ จึงนำมาสู่การผลักดันให้มีการจัดตั้ง CERT/CSIRT ในระดับภาคธุรกิจ (Sector-based CERT) ซึ่งเป็นทีมรับมือภัยคุกคามที่ช่วยประสาน แลกเปลี่ยนข้อมูล และช่วยเหลือเมื่อเกิดเหตุภัยคุกคามในหน่วยงาน CERT ขององค์กรในภาคธุรกิจเดียวกัน

ในปี 2559 สพธอ. ได้ร่วมกับหน่วยงานต่าง ๆ ทำบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ที่ส่งผลกระทบต่อภาคการเงิน การลงทุน การประกันภัย ภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานสำคัญของประเทศ โดยหนึ่งในนั้นเป็นการทำบันทึกข้อตกลงความร่วมมือของกลุ่มภาคธุรกิจการเงิน การลงทุน การประกันภัย ประกอบด้วย 5 หน่วยงาน ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สมาคมธนาคารไทย และ สพธอ.

กลุ่มภาคธุรกิจการเงิน การลงทุน การประกันภัยจัดได้ว่าพร้อมในหลาย ๆ ด้านมากกว่ากลุ่มธุรกิจอื่น อีกทั้งมีความสำคัญอย่างยิ่งต่อประเทศ จึงกลายมาเป็นกลุ่มแรกที่เดินหน้าจัดตั้ง CERT/CSIRT ในระดับกลุ่มธุรกิจขึ้น ภายใต้ข้อตกลงความร่วมมือดังกล่าว สพธอ. ได้ให้การสนับสนุนทั้งการเป็นวิทยากร การจัดซ้อมรับมือภัยคุกคามไซเบอร์แบบ Table Top Exercise ตลอดจนการแลกเปลี่ยนข้อมูลและการสนับสนุนอื่น ๆ เพื่อให้กลุ่มธุรกิจและผู้ประกอบการ

ต่าง ๆ มีความรู้ความเข้าใจ และสามารถจัดตั้ง CERT/CSIRT หรือทีมที่ทำหน้าที่ในลักษณะใกล้เคียงได้

ต่อมาเมื่อวันพุธที่ 21 มิถุนายน 2560 สำนักงานคณะกรรมการกำกับหลัก ทรัพย์และตลาดหลักทรัพย์ ร่วมกับตลาดหลักทรัพย์แห่งประเทศไทย สมาคมบริษัทหลักทรัพย์ไทย และสมาคมบริษัทจัดการการลงทุน เปิดตัวกลุ่มความร่วมมือ Thai Capital Market CERT หรือ TCM-CERT เพื่อร่วมกันยกระดับความพร้อมในการรับมือภัยคุกคามไซเบอร์ในภาคธุรกิจตลาดทุนไทย นับเป็นครั้งแรกของประเทศไทยที่มี CERT ในระดับกลุ่มธุรกิจเกิดขึ้น

จากนั้นเมื่อวันที่ 2 ตุลาคม 2560 ธนาคารแห่งประเทศไทย ร่วมมือกับ สมาคมธนาคารไทย แถลงข่าวการจัดตั้งศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT (TB-CERT) เพื่อเสริมสร้างให้ภาคสถาบันการเงินยกระดับความร่วมมือในการดูแลความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและเตรียมความพร้อมรับมือกับภัยคุกคามไซเบอร์ ให้สอดรับกับการนำเทคโนโลยีมาใช้ในการให้บริการทางการเงินอย่างกว้างขวาง

และในวันที่ 7 กันยายน 2561 สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัยได้ร่วมกับสมาคมประกันชีวิตไทย และสมาคมประกันวินาศภัยไทย จัดตั้ง TiCERT (Thai insurance Computer Emergency Response Team) เพื่อเป็นศูนย์กลางในการประสานงานกับบริษัทประกันภัย โดยมีหน้าที่หลักเพื่อตอบสนองและจัดการกับเหตุการณ์ความปลอดภัยคอมพิวเตอร์ที่เกิดขึ้นกับธุรกิจประกันภัยได้อย่างทันท่วงที รวมถึงสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในภาคการเงินเพื่อแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านไซเบอร์

ประเทศไทยจึงมี Sector-based CERT เกิดขึ้นถึง 3 แห่ง นำไปสู่ความร่วมมือระหว่าง TCM-CERT, TB-CERT, TiCERT และ ThaiCERT เพื่อรับมือภัยคุกคามไซเบอร์ในกลุ่มภาคธุรกิจการเงิน การลงทุน การประกันภัย ในขณะที่หน่วยงานกำกับดูแล ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ก็ทำงานอย่างใกล้ชิดร่วมกับสมาคมธนาคารไทยและ สพธอ. เพื่อยกระดับความมั่นคงปลอดภัยไซเบอร์ของกลุ่มภาคธุรกิจการเงิน การลงทุน การประกันภัยขึ้นไปอีก ตลอดจนร่วมกันพัฒนาบุคลากร สร้างความตระหนักรู้ ฯลฯ ให้ประชาชนชาวไทยสามารถใช้ทำธุรกรรมทางการเงินได้อย่างมั่นใจ

การสนับสนุนคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นคณะกรรมการระดับชาติซึ่งได้รับการแต่งตั้งตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. 2560 โดยมีนายกรัฐมนตรีเป็นประธานกรรมการ และมีองค์ประกอบรวม 32 รายจากภาคส่วนต่าง ๆ

จุดประสงค์ก็เพื่อกำหนดทิศทางการพัฒนาด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ เพื่อให้ประเทศไทยมีความพร้อม สามารถปกป้อง ป้องกัน และรับมือกับสถานการณ์ด้านภัยคุกคามไซเบอร์ในสถานการณ์ปกติ สถานการณ์อันเป็นภัยต่อความมั่นคง และสถานการณ์อันเป็นภัยต่อความมั่นคงอย่างร้ายแรง ตลอดจนเตรียมแผนปฏิบัติการและมาตรการตอบสนองด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นกลไกควบคุมการใช้อำนาจเป็นการเฉพาะตามระดับความรุนแรงของสถานการณ์ เพื่อให้สามารถแก้ไขสถานการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพและเป็นเอกภาพ รวมทั้งมีการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

ในการประชุมคณะกรรมการเตรียมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ครั้งที่ 1/2561 เมื่อวันที่ 9 พ.ค. 2561 ซึ่งมีนายกรัฐมนตรีพลเอก ประยุทธ์ จันทร์โอชา เป็นประธาน ได้มีการรายงานเพื่อทราบภาพรวมสถานการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ปัจจุบันทั้งในและต่างประเทศ สถานะร่างกฎหมายการรักษาความมั่นคงปลอดภัยไซเบอร์ ยุทธศาสตร์ด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศที่สภาความมั่นคงแห่งชาติ (สมช.) จัดทำ รวมถึงความสำเร็จของไทยที่ได้รับคัดเลือกโดยอาเซียนให้จัดตั้งศูนย์พัฒนาบุคลากรทางไซเบอร์ที่ประเทศไทยภายใต้ความร่วมมืออาเซียน-ญี่ปุ่น เพื่อพัฒนาบุคลากรไซเบอร์ให้แก่อาเซียน ในการนี้ คณะกรรมการฯ ได้ร่วมกันพิจารณาวาระที่สำคัญ จำนวน 4 วาระ ได้แก่

1. กรอบแนวคิดนโยบายและแผนระดับชาติเพื่อปกป้อง ป้องกัน รับมือ และลดความเสี่ยง และให้มีความสอดคล้องไปในทิศทางเดียวกัน

2. แนวทางการกำหนดโครงสร้างพื้นฐานสารสนเทศของประเทศและแนวปฏิบัติเพื่อตอบสนองต่อสถานการณ์ฉุกเฉินทางไซเบอร์

3. แนวทางการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ระยะเร่งด่วนและการจัดสรรงบประมาณสนับสนุน

4. การจัดตั้ง Cybersecurity Agency (CSA) ทำหน้าที่หน่วยประสานงานกลางและหน่วยงานเผชิญเหตุด้านความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการฯ ได้มอบหมายให้กระทรวงดิจิทัลฯ โดย สพธอ. ทำหน้าที่หน่วยงานเผชิญเหตุและหน่วยงานประสานงานกลางที่ทำงานร่วมกับหน่วยงานที่เกี่ยวข้องทั้งในระดับนโยบายและระดับปฏิบัติ ซึ่งไทยเซิร์ตช่วยสนับสนุน สพธอ. ผลักดันการดำเนินการในฐานะหน่วยงานเผชิญเหตุและหน่วยงานประสานงานกลาง ใน 4 เรื่อง ได้แก่

1. การตรวจสุขภาพทางไซเบอร์ประจำปี (Cybersecurity Health Check Day 2018) ของหน่วยงาน

2. การกำหนดรายการบริการสำคัญยิ่งยวด (Critical Services) และกำหนดรายชื่อผู้ที่ให้บริการสำคัญยิ่งยวดเหล่านั้น หรือที่เรียกว่าหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Operators)

3. โครงการเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ (Intensive Cybersecurity Capacity Building Program) เพื่อพัฒนาบุคลากรไซเบอร์จำนวน 1,000 คน

4. การจัดงานซ้อมรับมือภัยคุกคามไซเบอร์ภาคธุรกิจการเงิน การลงทุน และการประกันภัย

ไทยเซิร์ตกับการสร้างกำลังคนไซเบอร์

ไทยเซิร์ตในเวทีโลก

ในทุก ๆ ปี สพธอ. สร้างความร่วมมือด้านการพัฒนาบุคลากรในระดับนานาชาติ ผ่านการประชุมและสัมมนาระหว่างประเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งทีมไทยเซิร์ตได้เข้าไปสนับสนุนข้อมูลและการดำเนินงาน

จากการประชุมต่าง ๆ มีเวทีการประชุมสำคัญที่กลุ่มประเทศสมาชิกอาเซียนให้ความสนใจคือ การประชุมเจ้าหน้าที่อาวุโสอาเซียนด้านโทรคมนาคมและเทคโนโลยีสารสนเทศ (The ASEAN Telecommunications and IT Senior Officials Meeting: TELSOM) ซึ่งที่ประชุมได้มีมติอนุมัติให้จัดตั้งศูนย์ความร่วมมืออาเซียน - ญี่ปุ่นเพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ (ASEAN-Japan Cybersecurity Capacity Building Centre: AJCCBC) ในประเทศไทย โดยได้รับการสนับสนุนงบประมาณจากกองทุน Japan - ASEAN Integration Fund (JAIF) แสดงให้เห็นถึงการให้ความสำคัญต่อการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ของอาเซียนและความไว้วางใจที่แต่ละประเทศสมาชิกมีต่อประเทศไทย อีกทั้งยังสอดคล้องกับนโยบายและยุทธศาสตร์ของประเทศไทยในการสร้างความพร้อมรับมือภัยคุกคามไซเบอร์และส่งเสริมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ด้วย ซึ่งประเทศไทยโดย สพธอ. ได้รับมอบหมายในการจัดตั้งศูนย์ความร่วมมือแห่งนี้มาตั้งแต่แรก โดยได้ร่วมมือกับประเทศญี่ปุ่นในการจัดตั้งและจัดการฝึกอบรม ฯลฯ ให้แก่ข้าราชการและเจ้าหน้าที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในอาเซียนทั้ง 10 ประเทศ

อีกหนึ่งในเวทีความร่วมมือที่น่าสนใจคือความร่วมมือระหว่างภูมิภาคอาเซียนและญี่ปุ่นผ่านการประชุมอาเซียน-ญี่ปุ่นด้านความมั่นคงปลอดภัยสารสนเทศ (ASEAN Japan Information Security) ที่ผลักดันในเรื่องต่าง ๆ ที่เกี่ยวข้องในระดับอาเซียนร่วมกับประเทศญี่ปุ่น เช่น การซ้อมรับมือภัยคุกคามไซเบอร์ซึ่งจัดเป็นประจำทุกปี การป้องกันโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การพัฒนาบุคลากร ฯลฯ ซึ่ง สพธอ. เป็นผู้แทนประเทศไทยในการเข้าร่วมประชุมและประเทศไทยได้รับความไว้วางใจให้เป็นผู้นำเรื่องการพัฒนาบุคลากร (Capacity Building) ของการประชุมนี้ตั้งแต่ปี 2562 ด้วย


ASEAN-Japan
Cybersecurity Capacity
Building Centre
JETDA


JETDA
Government of Japan

การฝึกอบรม (Training)

การอบรมและสอบประกาศนียบัตรรับรอง iSEC

ที่ผ่านมา สพธอ. และสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association: TISA) ได้จัดการอบรมหลักสูตร “การฝึกอบรมและสอบวัดสมรรถนะเพื่อพัฒนามาตรฐานการรับรองบุคลากรด้านความมั่นคงปลอดภัยระบบสารสนเทศของประเทศไทย (iSEC)” อย่างต่อเนื่อง จนมารุ่นที่ 5 ในปี 2560 และยังเป็นครั้งแรกที่มีการทดสอบ 5 ครั้ง ครอบคลุม 5 ภูมิภาค ประกอบด้วย กรุงเทพฯ ชลบุรี เชียงใหม่ ภูเก็ต และขอนแก่น ในช่วงเดือนธันวาคม 2559 ถึงกุมภาพันธ์ 2560 เพื่อส่งเสริมให้ภูมิภาคต่าง ๆ เริ่มพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ผลิตกำลังคนเพื่อตอบสนองต่อความต้องการที่เพิ่มขึ้นของบุคลากรในอาชีพสายนี้ โดยใน 5 รุ่นที่ผ่านมา มีผู้ฝึกอบรมและเข้าร่วมสอบ 492 คน

ปัจจุบันมีหลายหน่วยงานที่เกี่ยวข้องกับการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ได้ประกาศการแบ่งความรู้เป็นรูปแบบต่าง ๆ เช่น การแบ่งความรู้เป็น 8 ด้านภายใต้ชื่อ CBK (Common Body of Knowledge) โดยหน่วยงาน (ISC)² ซึ่งการสอบประกาศนียบัตรรับรอง CISSP ก็เป็นการทดสอบความรู้ที่อ้างอิง CBK แต่หลักสูตร iSEC อ้างอิงกรอบความรู้ที่ชื่อ IT Security Essential Body of Knowledge: A Competency and Functional Framework for IT Security Workforce Development หรือ EBK โดยหน่วยงาน Department of Homeland Security ของสหรัฐอเมริกา โดยแบ่งเป็น 14 ด้าน คือ

1. ความมั่นคงปลอดภัยของข้อมูล (Data Security)

2. การพิสูจน์พยานหลักฐานดิจิทัล (Digital Forensics)

3. การสร้างความต่อเนื่องในการดำเนินงาน (Enterprise Continuity)

4. การจัดการภัยคุกคาม (Incident Management)

5. การฝึกอบรมและการสร้างความตระหนักด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security Training and Awareness)

6. การดำเนินงานและการบำรุงรักษาระบบเทคโนโลยีสารสนเทศ (IT Systems Operations and Maintenance)

7. ความมั่นคงปลอดภัยด้านเครือข่ายและโทรคมนาคม (Network and Telecommunications Security)

8. ความมั่นคงปลอดภัยด้านบุคลากร (Personnel Security)

9. ความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม (Physical and Environmental Security)

10. การจัดซื้อจัดจ้างและบริหารงานสัญญา (Procurement)

11. การปฏิบัติตามกฎระเบียบและมาตรฐาน (Regulatory and Standards Compliance)

12. การบริหารความเสี่ยงด้านความมั่นคงปลอดภัย (Security Risk Management)

13. การบริหารความมั่นคงปลอดภัยเชิงกลยุทธ์ (Strategic Security Management)

14. ความมั่นคงปลอดภัยของระบบและแอปพลิเคชัน (System and Application Security)

ในปี 2560 สพธอ. ได้เริ่มเปิดหลักสูตรผ่านระบบ e-Learning ให้แก่ผู้ที่สนใจ โดยสามารถศึกษาเนื้อหา iSEC ได้ที่ isec.tisa.or.th

โครงการ iSEC เป็นหนึ่งความพยายามของ สพธอ. ที่จะผลักดันการพัฒนาบุคลากรในระดับประเทศ นอกจากนี้ สพธอ. กำลังร่างแผนพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ระดับประเทศ โดยจะมีการสำรวจความต้องการตลาดแรงงาน ทักษะที่หน่วยงานเอกชนต้องการ และหาแนวทางพัฒนาคนในระยะสั้น กลาง และยาวให้สอดคล้องกับความต้องการของภาคเอกชน

การอบรม SEC504 โดยสถาบัน SANS

สพธอ. จัดการอบรมร่วมกับสถาบัน SANS สถาบันฝึกอบรมและวิจัยด้านความมั่นคงปลอดภัยไซเบอร์ที่มีชื่อเสียงในระดับนานาชาติ ซึ่งเป็นการอบรมต่อเนื่องของโครงการพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานภาครัฐ โดยจัดอบรมหลักสูตร SEC504 ระหว่าง วันที่ 20-25 กุมภาพันธ์ 2560

การอบรมหลักสูตร SEC504 โดยสถาบัน SANS (SANS Security 504) ครั้งนี้เป็นผลมาจากบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจ การค้า อุตสาหกรรม และโครงสร้างพื้นฐานของประเทศ ปี 2559 ที่ผ่านมา โดยผู้ที่ได้รับคัดเลือกให้เข้าร่วมอบรมหลักสูตรนี้ ต้องผ่านการทดสอบประเมิน Cyber Talent Assessment ซึ่งออกโดยสถาบัน SANS ก่อน โดยมีผู้ผ่านการทดสอบรวม 22 คนเข้าร่วมอบรม

หลักสูตร SEC504 เป็นหลักสูตรสร้างผู้เชี่ยวชาญที่มีหน้าที่รับมือเหตุภัยคุกคามด้านความมั่นคงปลอดภัย (Incident Response) ซึ่งกระทรวงกลาโหม สหรัฐฯ ได้นำมาใช้เป็นแนวทางพัฒนาบุคลากรของหน่วยงาน มีเนื้อหาครอบคลุมการประเมินสถานการณ์ การควบคุมความเสียหาย และประสานงานไปยังผู้ที่เกี่ยวข้องด้วยรูปแบบและวิธีการที่เหมาะสม รวมถึงการแก้ไขเพื่อป้องกันการโจมตีในอนาคต โดยครั้งนี้ได้รับเกียรติจากคุณ Bryce Galbraith จากสถาบัน SANS เป็นผู้ถ่ายทอดความรู้ตลอดทั้ง 6 วัน

Financial Cybersecurity Boot Camp

เริ่มจัดครั้งแรกในปี 2560 มีผู้เข้าร่วมจำนวน 60 คน นับเป็นครั้งแรกที่จัดขึ้นภายใต้ความร่วมมือ 5 หน่วยงาน ได้แก่ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สมาคมธนาคารไทย และ สพธอ. โดยจัดขึ้น ณ มหาวิทยาลัยเกษตรศาสตร์ วิทยาเขตบางเขน ระหว่างวันที่ 6 - 8 ตุลาคม 2560 มีนิสิตนักศึกษาที่สนใจสมัครเข้าร่วมโครงการจากทั่วประเทศ เช่น มหาวิทยาลัยเกษตรศาสตร์ มหาวิทยาลัยมหิดล จุฬาลงกรณ์มหาวิทยาลัย มหาวิทยาลัยขอนแก่น สถาบันเทคโนโลยีไทย-ญี่ปุ่น ฯลฯ และได้วิทยากรที่เชี่ยวชาญจากภาคการเงิน องค์กรของรัฐ และผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ชั้นนำของโลกมาแชร์ความรู้และประสบการณ์แก่ผู้เข้าอบรม โดยผู้เข้าอบรมยังได้ร่วมออกแบบโซลูชันทางการเงินในรูปแบบ Financial Business Cases โดยใช้ความคิดเชิงวิเคราะห์ออกแบบ (Design Thinking) และนำเสนอผลงานต่อคณะกรรมการผู้ทรงคุณวุฒิ พร้อมแมวมองจากบริษัทชั้นนำ

ครั้งที่ 2 จัดขึ้นระหว่างวันที่ 26 - 28 ตุลาคม 2561 โดยเปลี่ยนเป็นการแข่งขันทักษะด้านความมั่นคงปลอดภัยไซเบอร์แบบ Capture The Flag (CTF) อย่างเต็มรูปแบบ เพื่อคัดสรรนิสิตนักศึกษาที่มีความรู้ความสามารถด้านความมั่นคงปลอดภัยไซเบอร์เข้าสู่ธุรกิจการเงิน การลงทุน และการประกันภัย การแข่งขันจัดขึ้น 2 รอบ โดยรอบคัดเลือกเป็นการแข่งออนไลน์ 24 ชั่วโมงและรอบสองเป็นการเข้าค่ายเพื่อเรียนรู้และแข่งขันไปด้วยกันเป็นเวลา 3 วัน 2 คืน ซึ่ง สพธอ. ได้สนับสนุนทุนสำหรับสอบใบรับรองสากลด้านความมั่นคงปลอดภัยไซเบอร์ให้แก่ทีมผู้ชนะด้วย

กิจกรรมดังกล่าวได้รับการตอบรับเป็นอย่างดีและทั้ง 5 หน่วยงานได้ตกลงที่จะจัดอีกในปีต่อ ๆ ไป ซึ่งอาจปรับเนื้อหาให้ตอบโจทย์ความต้องการบุคลากรของภาคธุรกิจในปีนั้น ๆ ให้มากขึ้น

อบรมหลักสูตร Advanced Computer Forensics Investigation

สพธอ. ได้จัดอบรมให้แก่เจ้าพนักงานภาครัฐจำนวน 25 คนจาก 7 หน่วยงานที่ให้บริการด้านการตรวจพิสูจน์หลักฐานดิจิทัล เช่น สำนักงานตำรวจแห่งชาติ สถาบันนิติวิทยาศาสตร์โดยมีเนื้อหามุ่งเน้นการวิเคราะห์หลักฐานเชิงลึกที่มีความซับซ้อนต่าง ๆ เช่น Advanced Windows Forensics, Memory and Virtual Memory Analysis, Internet Activity and Cloud App Analysis, Computer Intrusion Analysis ตลอดจนการฝึกปฏิบัติตามสถานการณ์ที่ได้จำลองขึ้น (Scenario) ที่เกี่ยวข้องกับการติดมัลแวร์ภายในองค์กร เพื่อให้ผู้เข้าร่วมอบรมได้มีส่วนร่วมในการวิเคราะห์และแสดงความคิดเห็นถึงแนวทางในการวิเคราะห์ข้อมูลที่เกี่ยวข้อง

การอบรมครั้งนี้ จัดขึ้นตั้งแต่วันที่ 6-10 พฤศจิกายน 2560 และ 13 พฤศจิกายน 2560 รวม 6 วัน โดยแบ่งเป็นการเรียนและการฝึกทักษะ จำนวน 4 วัน และการฝึกสถานการณ์ที่ได้จำลองขึ้น (Scenario) จำนวน 2 วัน ซึ่งนอกจากเป็นการยกระดับทักษะด้านวิชาชีพให้แก่เจ้าพนักงานด้านการตรวจพิสูจน์หลักฐานดิจิทัลแล้ว ยังช่วยสร้างเครือข่ายระหว่างหน่วยงานภาครัฐที่ให้บริการตรวจพิสูจน์พยานหลักฐาน เพื่อแลกเปลี่ยนข้อมูลและพัฒนาทักษะต่อไป

Thailand CTF Competition/ Cyber SEA Game

ในปี 2560 และ 2561 ประเทศไทย โดย สพธอ. ได้รับเกียรติให้เป็นเจ้าภาพจัดงาน Cyber SEA Game ขึ้นที่ประเทศไทย ซึ่งเป็นอีกหนึ่งในกิจกรรมภายใต้ความร่วมมือระหว่างอาเซียนและประเทศญี่ปุ่น ซึ่งเป็นการแข่งขันรูปแบบ CTF หรือ Capture The Flag โดยผู้เข้าแข่งขันเป็นตัวแทนจาก 10 ประเทศอาเซียน ประเทศละ 4 คน แต่ละทีมต้องแข่งกันตอบโจทย์เฉพาะทางที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และตัดสินผู้ชนะจากทีมที่สามารถทำคะแนนได้สูงสุดภายในเวลาที่กำหนด ทีมที่ชนะเลิศจะได้รับโอกาสเข้าร่วมแข่งขันในเวทีระดับสากลในงาน SECCON ที่ประเทศญี่ปุ่น

ในเดือนตุลาคม 2560 ส่วนของประเทศไทย สพธอ. ได้จัดการแข่งขัน Thailand CTF Competition 2017 เพื่อคัดเลือกตัวแทนประเทศไทยไปแข่งขันต่อในงาน Cyber SEA Game 2017 โดยเป็นการแข่งออนไลน์ที่มีระยะเวลาแข่งขันถึง 24 ชั่วโมงตั้งแต่เช้าวันเสาร์ถึงเช้าวันอาทิตย์ ซึ่งได้รับความสนใจและมีผู้สมัครเข้ามาจำนวนมาก ทีมชนะเลิศที่ได้เป็นทีมตัวแทนประเทศไทยได้แก่ทีม h0ldth3d00r จากจุฬาลงกรณ์มหาวิทยาลัยที่สามารถตอบได้ครบทุกข้อ ส่วนผลการแข่งขัน Cyber SEA Game 2017 ทีมจากประเทศอินโดนีเซียเป็นทีมที่ได้คะแนนสูงสุด ตามมาด้วยประเทศสิงคโปร์และประเทศเวียดนามได้อันดับที่ 2 และ 3 ตามลำดับ ส่วนทีมจากประเทศไทยคว้าอันดับที่ 4

ในเดือนตุลาคม 2561 สพธอ. ได้จัดการแข่งขัน Thailand CTF Competition 2018 มีทีมสมัครทั้งสิ้น 65 ทีม รวมผู้เล่นจำนวน 260 คน โดยทีม Pattara_Knight ด้วยคะแนน 3,290 คะแนน และส่งทีมเข้าแข่งขันแข่งขัน Cyber SEA Game 2018 โดยอันดับที่ 1 - 3 คือประเทศอินโดนีเซีย ประเทศไทย และประเทศเวียดนามตามลำดับ

การแข่งขันทั้งในระดับประเทศไทยและระดับอาเซียน ตลอดจนการประชาสัมพันธ์ที่เกี่ยวข้อง ช่วยกระตุ้นให้คนรุ่นใหม่รู้จักและพัฒนาทักษะด้านความมั่นคงปลอดภัยไซเบอร์ เป็นการพัฒนาบุคลากรเพื่อรับมือภัยคุกคามไซเบอร์ของประเทศ อีกทั้งยังแสดงถึงศักยภาพของประเทศไทยที่สามารถจัดงานแข่งขันด้านความมั่นคงปลอดภัยไซเบอร์ในระดับอาเซียน

การซ้อมรับมือภัยคุกคามสำหรับหน่วยงานของรัฐ (Incident Drill)

ในวันที่ 21 ธันวาคม 2560 ไทยเซิร์ตได้จัดการซ้อมรับมือภัยคุกคามไซเบอร์เพื่อเตรียมความพร้อมให้กับหน่วยงานที่เข้าร่วมโครงการ ThaiCERT GMS ให้สามารถรับมือกับภัยคุกคามรูปแบบใหม่ได้อย่างมีประสิทธิภาพ ณ ห้อง Platinum Hall ชั้น 3 โรงแรมแกรนด์ เมอร์เคียว ฟอร์จูน ซึ่งมีหน่วยงานเข้าร่วมจำนวนทั้งสิ้น 58 หน่วยงาน 105 คน

ผู้เข้าร่วมการซ้อมรับมือภัยคุกคามไซเบอร์จะได้แสดงบทบาทสมมุติในเหตุการณ์จำลองในฐานะผู้ดูแลระบบเว็บไซต์ (Player) โดยจะมีเจ้าหน้าที่ผู้ควบคุมการซ้อม (Excon) คอยควบคุมการซ้อมฯ สนับสนุน รวมถึงช่วยเหลือทั่วไป ในกรณีที่มีปัญหาเกิดขึ้นในระหว่างการซ้อมรับมือภัยคุกคาม โดยผู้เข้าร่วมจะได้รับ Log จำลองที่ไทยเซิร์ตจัดเตรียมไว้ให้ และใช้ระบบวิเคราะห์ภัยคุกคามและเครื่องมือต่าง ๆ ที่ได้เรียนรู้จากการอบรมมาประยุกต์ใช้วิเคราะห์การโจมตี ซึ่งช่วยเสริมสร้างความมั่นใจว่าจะสามารถนำความรู้และเครื่องมือที่ได้รับไปใช้ปกป้องหน่วยงานของตนได้จริง

การประชุมสัมมนาและกิจกรรมอื่น ๆ (Seminars, Conferences and Activities)

Thailand Cybersecurity Week 2017

ในการสร้างความตระหนักรู้สู่ทุกภาคส่วนอย่างต่อเนื่อง ไทยเซิร์ตภายใต้ สพธอ. ได้ผสานความร่วมมือกับทุกภาคส่วนจัดงาน Thailand Cybersecurity Week 2017 ภายใต้แนวคิด“Cybersecurity for All: ความมั่นคงปลอดภัยไซเบอร์เพื่อทุกคน” ขึ้นเพื่อจุดประกายให้ทุกคนและทุกภาคส่วนสร้างความตระหนักรู้ ว่าไม่ว่าจะเป็นคนดูแลระบบ คนทำอีคอมเมิร์ซ ผู้บริหาร และผู้สนใจทั่วไป ให้สามารถลดความเสี่ยงจากภัยคุกคามไซเบอร์ ซึ่งเริ่มต้นได้จากตัวเอง

Thailand Cybersecurity Week 2017 จัดขึ้นระหว่างวันที่ 26–30 มิถุนายน 2560 ณ Space Convention Center ชั้น 12 อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระราม 9 และพิธีเปิดจัดขึ้นในวันที่ 28 มิถุนายน 2560 ณ สโมสรทหารบก วิภาวดี

นับเป็นปรากฏการณ์ครั้งสำคัญในด้านความมั่นคงปลอดไซเบอร์ของประเทศไทย ที่จะเป็นหนึ่งในกลไกสำคัญเพื่อร่วมขับเคลื่อนประเทศไทยสู่เป้าหมายยุค 4.0

ตลอดการจัดงาน 5 วัน มีผู้เข้าร่วมงานกว่า 2,000 คน และมีการมอบรางวัล Thailand Cybersecurity Excellence Awards เพื่อสนับสนุนองค์กรและบุคคลที่เป็นผู้มีส่วนสำคัญในการผลักดันความมั่นคงปลอดภัยไซเบอร์ให้กับสังคม นอกจากจะได้รับความรู้ในระดับต่าง ๆ จากการสัมมนาแล้ว ผู้เข้าร่วมยังมีโอกาสได้พูดคุยกับผู้เชี่ยวชาญในด้านต่าง ๆ เพื่อแลกเปลี่ยนประสบการณ์และความร่วมมืออีกด้วย

งานเสวนา Open Forum

Open Forum เป็นงานเสวนาโดย สพธอ. เพื่อเปิดโอกาสให้ผู้เชี่ยวชาญได้ถกประเด็นหัวข้อที่น่าสนใจ ในปี 2560 ไทยเซิร์ตได้สนับสนุนการจัดหัวข้อที่เกี่ยวกับความมั่นคงปลอดภัย 6 ครั้งเพื่อจุดประสงค์ต่าง ๆ เช่น เพื่อสร้างความตื่นตัวให้กับประชาชนรับทราบถึงการระบาดของมัลแวร์เรียกค่าไถ่สายพันธุ์ WannaCry ให้ระวังและป้องกันก่อนตกเป็นเหยื่อ หรือใช้เป็นโอกาสในรับฟังความคิดเห็นจากทั้งภาครัฐ เอกชน และประชาชน ในเรื่องแผนการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งทำให้เข้าใจความต้องการด้านกำลังคนของภาคเอกชน และเข้าใจความจำเป็นในการร่วมมือกับภาคส่วนต่าง ๆ รวมถึงสถาบันด้านวิชาการ อย่างมหาวิทยาลัย เพื่อผลิตคนให้มีจำนวนและทักษะได้ตรงความต้องการในระยะยาว

ในปี 2561 ไทยเซิร์ตได้สร้างเครือข่ายและร่วมมือกับบริษัทด้านความมั่นคงปลอดภัยร่วมกันจัดสัมมนาเพื่อให้ความรู้กับประชาชนและองค์กรต่าง ๆ ภายใต้ชื่องาน Open Forum: Cybersecurity Knowledge Sharing Series โดยจัดทั้งหมด 7 ครั้ง ซึ่งทางบริษัทได้สนับสนุนวิทยากรผู้เชี่ยวชาญทั้งในประเทศและต่างประเทศ รวมถึงจัดอบรมเฉพาะให้กับหน่วยงานสำคัญ เช่น หน่วยงานที่รับผิดชอบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยมีตัวอย่างการจัดอบรมที่น่าสนใจ เช่น Cisco IoT Security Workshop For Healthcare and Energy Sector, RSA Cybersecurity Workshop For CIO

โครงการสร้างความตระหนักในการใช้อินเทอร์เน็ต ให้เสริมสร้างรายได้และรู้เท่าทันภัยคุกคามไซเบอร์ (Internet for Better Life)

ในปี 2561 ไทยเซิร์ตได้สนับสนุน สพธอ. ดำเนินการโครงการสร้างความตระหนักในการใช้อินเทอร์เน็ต ให้เสริมสร้างรายได้และรู้เท่าทันภัยคุกคามไซเบอร์ (Internet for Better Life) หรือ IFBL โดยได้จัดการอบรมให้กับกลุ่มเป้าหมาย 4,116 คน ได้แก่ เด็กและเยาวชน (ระดับชั้นมัธยมศึกษาตอนต้น) 2,511 คน และกลุ่มผู้สูงอายุ (อายุ 50 ปีขึ้นไป) 1,605 คนในทุกภาคของประเทศไทย ให้มีความตระหนักรู้ ความเข้าใจ เกี่ยวกับการใช้เทคโนโลยีสารสนเทศและอินเทอร์เน็ตอย่างมั่นคงปลอดภัย เพื่อสามารถเป็นแบบอย่างต่อสังคม ซึ่งจะช่วยลดปัญหาความเสี่ยงจากการใช้อินเทอร์เน็ตและการตกเป็นเหยื่อในโลกออนไลน์ โดยการอบรมแต่ละครั้งได้มีการประเมินความรู้ของผู้เข้าอบรมก่อนและหลังการอบรม ซึ่งพบว่าผู้เข้าอบรมมีความรู้เพิ่มขึ้น 93.56%

สำหรับปี 2562 โครงการนี้จะมีการขยายผล นำบทเรียนที่ไปอบรมตลอดทั้งปี มาปรับปรุงและบรรจุไว้เป็นบทเรียนออนไลน์ในรูปแบบ e-Learning ที่ทุกคนสามารถเรียนรู้ได้ด้วยตนเองผ่านทางเว็บไซต์ https://ifbl.etda.or.th และสถานศึกษาที่สนใจร่วมโครงการสามารถติดต่อเพื่อขอรายละเอียดได้ที่ifbl@etda.or.th

ThaiCERT ETDA สพธอ www.etda.or.th

รู้ทันภัยไซเบอร์... ทำธุรกรรมออนไลน์ อย่างไรให้หายห่วง

24 ชม. ในชีวิตออนไลน์
1,440 นาที อาจตกเป็นเหยื่อวายร้ายในโลกไซเบอร์
86,400 วินาที ที่สามารถป้องกันได้ถ้ารู้วิธี

จำกัดวงเงิน ทำธุรกรรมออนไลน์

- ไม่ว่าจะเป็นการโอน หรือจ่ายค่าสินค้า/บริการให้อยู่ในงบประมาณที่เหมาะสม เพื่อจำกัดความเสี่ยงของเงินในกระเป๋าเรา

ระวังเว็บไซต์ประเภทฟิชชิ่ง

- อีเมลปลอม เหมือนส่งมาจากสถาบันการเงินที่มีชื่อเสียง
- เว็บไซต์เลียนแบบโดยเฉพาะธนาคารออนไลน์
- โทรศัพท์แอบอ้างเป็นเจ้าหน้าที่ราชการ ธนาคาร เพื่อลวงข้อมูลส่วนตัวของเรา

เว็บไซต์ที่ใช้บริการ ต้องมีการเข้ารหัสเสมอ

- สองสังเกตสัญลักษณ์กุญแจล็อกที่อยู่บนเบราว์เซอร์ เมื่อคลิกที่สัญลักษณ์ก็จะเห็นใบรับรองอิเล็กทรอนิกส์ หรือ SSL Certificate นั่นเอง

ตั้ง Password ให้ยุ่งยากไว้ก่อน

- ไม่เลือกฟังก์ชันจำ Password อัตโนมัติ

- ไม่ควรใช้ Password เดียวทั้งเข้าอีเมลและทำธุรกรรมออนไลน์

- หมั่นเปลี่ยน Password ทุก 30 – 45 วัน

- ถ้าจำเป็นต้องทำธุรกรรมออนไลน์ผ่านคอมพิวเตอร์สาธารณะให้เปลี่ยน Password ทันที

UPLOW 174!@#$

- ใช้ตัวอักษรผสมทั้งตัวพิมพ์เล็กและใหญ่ มีตัวเลขและอักขระเป็นส่วนประกอบ

ภาคผนวก ก.
ประเภทและตัวอย่าง
ภัยคุกคาม

ชื่อประเภทภัยคุกคาม	ตัวอย่างภัยคุกคาม	คำอธิบาย
Abusive Content (เนื้อหาที่เป็นภัย)	Spam	ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริง หรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือ ก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามกอนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (Spam)
	Child / Sexual / Violence / Contents	
Malicious Code (โปรแกรมไม่พึงประสงค์)	Virus	ภัยคุกคามที่เกี่ยวข้องกับโปรแกรมหรือชุดคำสั่งที่ถูกพัฒนาขึ้นด้วยความประสงค์ร้ายที่เรียกว่ามัลแวร์ (Malware) เพื่อทำให้เกิดความขัดข้องหรือความเสียหายกับระบบ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ เช่น Virus, Worm, Trojan หรือ Spyware อาจอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อนจึงจะสามารถติดตั้งตัวเองหรือทำงานได้ หรืออาจเผยแพร่เข้ามายังเครื่องของผู้ใช้และเริ่มทำงานโดยอัตโนมัติ ซึ่งอาจมาจากหน้าเว็บไซต์ที่มีโค้ดอันตรายที่เผยแพร่มัลแวร์ (Malware URL) แก่ผู้เข้าเยี่ยมชม
	Worm	
	Trojan	
	Spyware	
	Dialer	
	Rootkit	
	Website Spreading Malware	

ชื่อประเภทภัยคุกคาม	ตัวอย่างภัยคุกคาม	คำอธิบาย
Information Gathering (ความพยายามรวบรวมข้อมูลของระบบ)	Scanning	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบโดยผู้ประสงค์ร้าย ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ (Scanning) เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบ ฯลฯ รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
	Sniffing	
	Social Engineering	

ชื่อประเภทภัยคุกคาม	ตัวอย่างภัยคุกคาม	คำอธิบาย
Intrusion Attempts (ความพยายามบุกรุกเข้าระบบ)	Exploiting of Known Vulnerabilities	ภัยคุกคามที่เกิดจากความพยายามเจาะเข้าระบบ ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE-Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อนเพื่อจะได้เข้าควบคุมหรือเข้าถึงข้อมูลของระบบนี้ รวมถึงความพยายามจะเจาะระบบผ่านช่องทางการล็อกอินด้วยวิธีการสุ่ม/เดาบัญชีชื่อผู้ใช้งานและรหัสผ่าน หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
	Login Attempts	
	New Attack Signature	
Intrusions (การบุกรุกหรือเจาะระบบได้สำเร็จ)	Privileged Account Compromise	ภัยคุกคามที่เกิดจากการเจาะระบบสำเร็จทำให้ผู้ประสงค์ร้ายสามารถควบคุมระบบและกระทำการต่าง ๆ เช่น การปรับเปลี่ยนหน้าเว็บไซต์เพื่อทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ (Web Defacement) หรือเข้าถึงและเปลี่ยนแปลงข้อมูลสำคัญในระบบได้
	Unprivileged Account Compromise	
	Defacement	

ชื่อประเภทภัยคุกคาม	ตัวอย่างภัยคุกคาม	คำอธิบาย
Availability (การโจมตีสภาพความพร้อมใช้งานของระบบ)	DoS	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ สาเหตุอาจเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DDoS (Distributed Denial of Service) โดยใช้บริการ DNS ที่ตั้งค่าอย่างไม่เหมาะสม (Open DNS Resolver) หรือบริการอื่น ๆ เป็นเครื่องมือโจมตี นอกจากนี้ยังรวมถึงการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า
	DDoS	
	Outage (No Malice)	
Information Content Security (การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต)	Unauthorised Access to Information	ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorised Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorised Modification) ได้ รวมไปถึงเผยแพร่ข้อมูลที่รั่วไหล (Data Leakage)
	Unauthorised Modification of Information	

ชื่อประเภทภัยคุกคาม	ตัวอย่างภัยคุกคาม	คำอธิบาย
Fraud (การฉ้อฉลฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์)	Unauthorised Use of Resources	ภัยคุกคามที่เกิดจากการฉ้อฉลฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ เช่น การสร้างหน้าเว็บไซต์ปลอม (Web Phishing) ที่หลอกขโมยรหัสผ่านสำหรับล็อกอินจากผู้ใช้ การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง
	Masquerade	
	Phishing	
Vulnerability (ช่องโหว่)	Open for Abuse	ภัยคุกคามที่เกิดจากการพบช่องโหว่ในฮาร์ดแวร์หรือซอฟต์แวร์ที่ส่งผลให้ถูกโจมตีหรือเจาะระบบ
Other (ภัยคุกคามด้านสารสนเทศ อื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น)	-	vภัยคุกคามประเภทอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงประเภทใหม่ หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่น ๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทนี้ใหม่

ภาคผนวก ข.
ลำดับเหตุการณ์สำคัญของไทยเซิร์ต (ThaiCERT Timeline)

เดือน/ปี	กิจกรรม
ต.ค. 43	จัดตั้ง โดยศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC)
ก.พ. 46	เข้าเป็นหนึ่งในสมาชิกรุ่นแรกในการก่อตั้ง APCERT
พ.ค. 48	เข้าเป็นหนึ่งในสมาชิก FIRST
ก.พ. 54	โอนถ่ายภารกิจมายัง สพธอ.
ก.ค. 54	ปรับเปลี่ยนโครงสร้าง รูปแบบการทำงาน เปิดให้บริการเต็มตัว
ม.ค. 55	เริ่มให้บริการพิสูจน์พยานหลักฐานดิจิทัล
ต.ค. 55	เริ่มร่วมกับ JPCERT สนับสนุน LaoCERT พัฒนาบุคลากรในทีม
ม.ค. 56	เริ่มให้บริการตรวจสอบช่องโหว่ให้กับหน่วยงานภาครัฐ
พ.ค. 56	เริ่มให้บริการทดสอบและรับรองความสามารถด้านไซเบอร์ด้วยใบรับรอง iSEC
มิ.ย. 56	เจ้าภาพจัดงานประชุมวิชาการระดับนานาชาติ 25th Annual FIRST Conference โดยมีนายกรัฐมนตรีเป็นประธานเปิดงาน
ก.พ. 57	เริ่มมีบทบาทในฐานะ คณะทำงานจัดงานซ้อมรับมือภัยคุกคามสำหรับสมาชิก APCERT (APCERT Drill) เป็นประจำทุกปี

เดือน/ปี	กิจกรรม
ก.ย. 57	จัดทำและเผยแพร่มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard)
ต.ค. 57	ย้ายที่ตั้งมายังตึก The 9th Tower Grand Rama 9 เพื่อความคล่องตัวในการติดต่อสื่อสารและร่วมมือกับหน่วยงานภาคเอกชน
ก.พ. 58	มีศูนย์ CSoC เฝ้าระวังภัยแบบ 24 ชั่วโมง
ก.ย. 58	เริ่มให้บริการเฝ้าระวังภัยคุกคามให้หน่วยงานภาครัฐ (ThaiCERT Government Monitoring System - ThaiCERT GMS)
ก.ย. 58	จัดการแข่งขันระดับประเทศ Thailand CTF 2015
ต.ค. 58	ได้รับการรับรองจากองค์กร Trusted Introducer
พ.ย. 58	สนับสนุน สพธอ. สำรวจด้านความมั่นคงปลอดภัยไซเบอร์ ของหน่วยงานโครงสร้างพื้นฐาน
ก.ย. 59	ลงนามข้อตกลงความร่วมมือ (MoU) กับ 19 หน่วยงานโครงสร้างพื้นฐานสำคัญ ยกระดับความพร้อม CERT Readiness รับมือภัยคุกคามไซเบอร์
ก.พ. 60	ผลักดันให้มีคณะทำงานจัดการซ้อมรับมือ APCERT Drill ภายใต้ APCERT อย่างเป็นทางการ โดยมีไทยเซิร์ตเป็นประธานคณะทำงานฯ

เดือน/ปี	กิจกรรม
เม.ย. 60	ได้รับการรับรองอย่างเป็นทางการในการใช้คำว่า CERT ใน ThaiCERT จาก Carnegie Mellon University
มิ.ย. 60	สนับสนุนการจัดตั้งหน่วยงานรับมือภัยคุกคามสำหรับภาคธุรกิจตลาดทุน TCM-CERT (Thai Capital Market CERT)
มิ.ย. 60	จัดงานสัมมนาด้านความมั่นคงปลอดภัยไซเบอร์เป็นครั้งแรกของประเทศไทย Thailand Cybersecurity Week 2017
ต.ค. 60	จัดการแข่งขันระดับประเทศ Thailand CTF 2017
ต.ค. 60	สนับสนุนการจัดตั้งศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาคการธนาคาร TB-CERT (Thailand Banking Sector Computer Emergency Response Team)
พ.ย. 60	จัดการแข่งขันระดับอาเซียน Cyber SEA Game 2017
พ.ค. 61	สนับสนุนการประชุมคณะกรรมการเตรียมการไซเบอร์แห่งชาติครั้งที่ 1
ก.ย. 61	เปิดตัวศูนย์ความร่วมมืออาเซียน - ญี่ปุ่น เพื่อพัฒนาบุคลากรความมั่นคงปลอดภัยไซเบอร์ AJCCBC (ASEAN-Japan Cybersecurity Capacity Building Centre)

เดือน/ปี	กิจกรรม
ก.ย. 61	สนับสนุนการจัดตั้งหน่วยงานรับมือภัยคุกคามสำหรับภาคประกันภัย TiCERT (Thai Insurance Computer Emergency Response Team)
พ.ย. 61	จัดการแข่งขัน Thailand CTF 2018
พ.ย. 61	จัดการแข่งขัน Cyber SEA Game 2018


PASSWORD
พาสเวิร์ด
รหัสผ่าน
ตั้งให้ยาก
จำให้ได้
ไม่แชร์กับใคร
อย่าใช้ซ้ำทุกบัญชี
อย่างน้อย
ควรมี 8 ตัวอักษร
เดายาก
ไม่เป็นคำจากพจนานุกรม
ไม่เป็นตัวเลข
หรือตัวอักษรเรียงกัน
หรือซ้ำกัน เช่น abcd1111
112233
ไม่ใช้พาสเวิร์ดหรือ
default password
ที่ตั้งค่ามาตั้งแต่แรก
ไม่ใช้ข้อมูลส่วนตัว
เช่น วันเดือนปีเกิด
เบอร์โทร.
ไม่ใช้ซ้ำกัน
ในบัญชีต่าง ๆ
ใช้การยืนยัน 2 ขั้นตอน
หรือหลายขั้นตอน
ระวังอีเมลฟิชชิง
หลอกให้เปลี่ยนพาสเวิร์ด
โดยให้คลิกลิงก์
พิจารณาใช้งาน
ซอฟต์แวร์ช่วยจัดการ
พาสเวิร์ด
ThaiCERT
ETDA


แบ็กอัปข้อมูลไว้ก่อน
เพราะถ้าหายไป เสียเงินเท่าไร...
ก็อาจไม่ได้คืนมา
รู้มั้ย? 34%
ของคนทั่วโลกเคยสูญเสียข้อมูล
ในปี 2560
กว่าล้านคนถูกโจมตี ด้วยมัลแวร์เรียกค่าไถ่
ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้ปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้วก็ไม่ได้รับประกันว่าจะได้ข้อมูลนั้นคืนมา
แบ็กอัปแบบไหน...ถามใจเธอดู?
วิธีเก็บ
ข้อดี
ข้อเสีย
บริการ Cloud เช่น Google Drive, Dropbox, OneDrive
อุปกรณ์เก็บข้อมูลแบบพกพา เช่น DVD, ฮาร์ดดิสก์, Flash Drive
พิมพ์เป็นกระดาษ
NAS (Network Attach Storage)
ศูนย์ประสานการรักษาความมั่นคงของอินเทอร์เน็ตไทย (ThaiCERT)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
ThaiCERT
ETDA
ThaiCERT
ThaiCERT
thaicert.or.th


JAISA
NEC
ThaiCERT
ETDA
CYBER
SEA GAME
2017

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 20 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพฯ 10310

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th
เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ www.etda.or.th
เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม www.mdes.go.th

ISBN 978-616-7956-44-2