ความมั่นคงปลอดภัยทางไซเบอร์
(Cyber Security)

การพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสารส่งผลให้เกิดการพัฒนาทั้งทางเศรษฐกิจและสังคมอย่างก้าวกระโดด เนื่องจากปัจจุบันมีการพัฒนาแอพพลิเคชั่นและซอฟแวร์ที่มีประสิทธิภาพสูง ทำให้ผู้ใช้งานทั่วไปสามารถเข้าถึงข้อมูลได้สะดวก รวดเร็ว และประหยัดค่าใช้จ่ายได้มากขึ้น หากผู้ใช้งานนำข้อมูลไปใช้ในทางที่สร้างสรรค์ ก็สามารถใช้ให้เป็นประโยชน์ต่อการพัฒนาและยกระดับเศรษฐกิจ สังคม และสิ่งแวดล้อมในมิติต่างๆ ได้ ในทางกลับกัน เทคโนโลยีก็สามารถสร้างความเสียหายได้มากเช่นกัน หากผู้ประสงค์ร้ายได้พัฒนาเครื่องมืออันทันสมัยเพื่อโจมตีระบบขโมย ทำลาย บิดเบือนข้อมูล หรือหลอกลวง ก็จะส่งผลให้เกิดการแทรกแซงและทำลายความมั่นคงได้ในทุกระดับ ไม่ว่าจะเป็นในระดับบุคคล ระดับหน่วยงาน ระดับประเทศ และระดับโลก

อย่างไรก็ตาม การรักษาความมั่นคงปลอดภัยทางไซเบอร์จำเป็นต้องคำนึงถึงการคุ้มครองความเป็นส่วนตัวและความสะดวกสบายในการเข้าถึงระบบของแต่ละบุคคลด้วยเช่นกัน การมุ่งเน้นรักษาความมั่นคงของชาติอาจเกิดการลุกล้ำความเป็นส่วนตัว ในขณะที่การมุ่งให้เกิดความสะดวกสบายในการเข้าถึงระบบอาจทำให้ความมั่นคงปลอดภัยทางไซเบอร์เกิดความหละหลวมเช่นกัน ดังนั้น หน่วยงานที่รับผิดชอบจำเป็นต้องรักษาสมดุลระหว่างการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การคุ้มครองความเป็นส่วนตัว และการอำนวยความสะดวกในการเข้าถึงระบบให้เหมาะสม เพราะเป็นกลไกสำคัญในการสร้างความไว้วางใจ และการส่งเสริมเกิดการใช้เทคโนโลยีดิจิทัลในการทำงานทุกภาคส่วน

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) คืออะไร

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union: ITU) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ว่าคือภาพรวมของเครื่องมือ (tools), นโยบาย (policies), แนวคิดการรักษาความปลอดภัย (security concepts), การรักษาความปลอดภัย (security safeguards), แนวทาง (guidelines), วิธีการบริหารความเสี่ยง (risk management approaches), การปฏิบัติ (actions), การอบรม (training), วิธีปฏิบัติที่เป็นเลิศ (best practices), การรับประกัน (assurance) และเทคโนโลยี (technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์ องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อ

คอมพิวเตอร์, ข้อมูลส่วนตัว, โครงสร้างพื้นฐาน, แอปพลิเคชัน, บริการ, ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์[1]

สำหรับประเทศไทย ยังไม่มีนิยามของคำว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศ ได้ให้นิยามคำว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผดพลาดต่างๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)[2]

ทั้งนี้ มาตรา 3 ใน “ร่างพระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์” ได้ให้ความหมายของ “ความมั่นคงปลอดภัยไซเบอร์” ว่า มาตรการและการดำเนินการที่กำหนดขึ้นเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศให้สามารถปกป้อง ป้องกัน หรือรับมือกับสถานการณ์ด้านภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบหรืออาจก่อให้เกิดความเสี่ยงต่อการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการโดยปกติของดาวเทียม อันกระทบต่อความมั่นคงของชาติซึ่งรวมถึงความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ

หน่วยงานที่มีบทบาทในการเฝ้าระวังการโจมตีทางไซเบอร์ของประเทศไทย

ประเทศไทยมีหน่วยงานภาครัฐที่ดูแลเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) 2 แห่ง คือ

1) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Thailand Computer Emergency Response Team : ThaiCERT) ในการกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ซึ่งมีภาระหน้าที่หลักในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้การสนับสนุนที่จำเป็น และให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทาง

[1] ที่มา http://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

[2] ที่มา https://www.tci-thaijo.org/index.php/ndsijournal/article/viewFile/39369/32571

ด้านคอมพิวเตอร์ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่างๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์เน็ต

2) ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต) (Government Computer Emergency and Readiness Team : G-CERT) ในการกำกับดูแลของ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ รวมทั้งการสร้างเครือข่ายพันธมิตรเพื่อให้เกิดความมั่นคงปลอดภัยและช่วยลดความเสี่ยงต่อการเกิดอาชญากรรมทางคอมพิวเตอร์

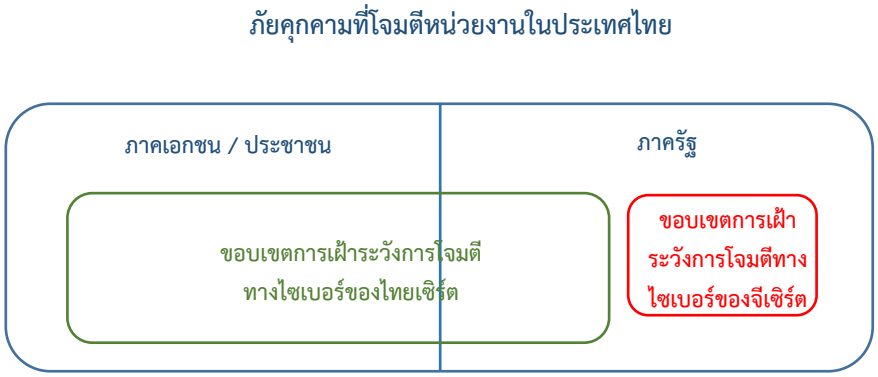
การทำงานของไทยเซิร์ตและจีเซิร์ตจะติดตามการโจมตีทางไซเบอร์ผ่าน 2 ช่องทาง คือ

1) การตรวจจับการโจมตีทางไซเบอร์ด้วยเทคโนโลยีเซ็นเซอร์ที่ติดตั้งอยู่ที่ระบบ

2) การรับแจ้งเหตุการโจมตีทางไซเบอร์จากเครือข่ายเฝ้าระวัง ซึ่งเป็นเสมือนกลุ่มพันธมิตรในการดำเนินงาน

ขอบเขตการทำงานของไทยเซิร์ตจะทำหน้าที่เฝ้าระวังการโจมตีทางไซเบอร์ให้ทั้งหน่วยงานภาครัฐและภาคเอกชน ส่วนภารกิจของจีเซิร์ตจะเฝ้าระวังการโจมตีทางไซเบอร์ให้เฉพาะหน่วยงานภาครัฐเท่านั้น อย่างไรก็ตาม การตรวจจับการโจมตีด้วยเซ็นเซอร์จะใช้การติดตั้งเซ็นเซอร์อยู่ที่ระบบของหน่วยงานที่ใช้บริการของไทยเซิร์ตหรือจีเซิร์ตอย่างใดอย่างหนึ่งเท่านั้น และการรับแจ้งเหตุการโจมตีทางไซเบอร์จากเครือข่ายเฝ้าระวังยังไม่สามารถครอบคลุมทุกเหตุการณ์การโจมตีที่เกิดจริงได้ จึงทำให้การเก็บข้อมูลสถิติการโจมตีทางไซเบอร์ของประเทศไทยยังไม่สามารถเก็บรวบรวมเหตุการณ์การโจมตีที่เกิดขึ้นจริงได้ทั้งหมด และเป็นข้อมูลที่แยกกันชัดเจนระหว่างข้อมูลทางสถิติจากไทยเซิร์ตและข้อมูลทางสถิติจากจีเซิร์ต ดังแสดงในแผนภาพที่ 1

แผนภาพที่ 1 ขอบเขตการเฝ้าระวังการโจมตีทางไซเบอร์ของไทยเซิร์ตและจีเซิร์ต



ที่มา: ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์ ฝ่ายนโยบายและยุทธสาสตร์ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

ตารางที่ 1 10 อันดับประเทศที่เกิดภัยคุกคามทางไซเบอร์มากที่สุด (ระยะเวลา พ.ศ. 2554 – 2559)

ประเทศ	จำนวนการเกิดภัยคุกคามทางไซเบอร์ (ครั้ง)					
	2554	2555	2556	2557	2558	2559
เยอรมัน	23	-	-	587	1410	811
บราซิล	136	137	102	172	173	191
สหรัฐอเมริกา	287	283	392	482	310	160
จอร์เจีย	-	-	-	-	-	89
ออสเตรเลีย	13	32	84	238	97	57
โปรตุเกส	-	-	-	40	-	34
ลิทัวเนีย	-	-	-	-	-	33
ไทย	28	43	82	112	69	29
สิงคโปร์	24		-	-	-	22
สเปน	12	23	12	-	93	-

หมายเหตุ พ.ศ. 2554 เป็นการเก็บข้อมูลในช่วง 31 กรกฎาคม – 31 ธันวาคม 2554
พ.ศ. 2559 เป็นการเก็บข้อมูลในช่วง 1 มกราคม – 31 กรกฎาคม 2559

ที่มา: https://www.thaicert.or.th/statistics/statistics.html

จากข้อมูล 10 อันดับประเทศที่เกิดภัยคุกคามทางไซเบอร์มากที่สุด (ระยะเวลา พ.ศ. 2554 – 2559) ซึ่งเก็บรวบรวมโดยไทยเซิร์ต พบว่าในช่วง 1 ม.ค. 58 – 31 ก.ค. 59 ประเทศเยอรมันเป็นประเทศที่มีการโจมตีทางไซเบอร์มากที่สุด (2,221 ครั้ง) รองลงมาคือประเทศสหรัฐอเมริกา (470 ครั้ง) และประเทศบราซิล (364 ครั้ง) สำหรับประเทศไทย แม้การโจมตีทางไซเบอร์ในแต่ละปีจะไม่สูงเท่าสามประเทศดังกล่าว แต่ยังเป็นประเทศที่ติดอันดับ 1 ใน 10 ของประเทศที่มีการโจมตีทางไซเบอร์มากที่สุด ตั้งแต่ พ.ศ. 2554 ถึงปัจจุบัน

ประเภทภัยคุกคามทางไซเบอร์ของประเทศไทย

ไทยเซิร์ตได้แบ่งประเภทภัยคุกคามทางไซเบอร์เป็น 9 ประเภทตามที่ได้กำหนดโดย The European Computer Security Incident Response Team (eCSIRT) ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน Computer Security Incident Response Team (CSIRT)[3] ในสหภาพยุโรป ซึ่งมีรายละเอียดดังตารางที่ 2

ตารางที่ 2 ประเภทภัยคุกคามทางไซเบอร์ โดย eCSIRT

ประเภทภัยคุกคาม	คำอธิบาย
1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content)	ภัยคุกคามที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่างๆ ทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้นๆ (SPAM)
2. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability)	ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่างๆของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่างๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคารสถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

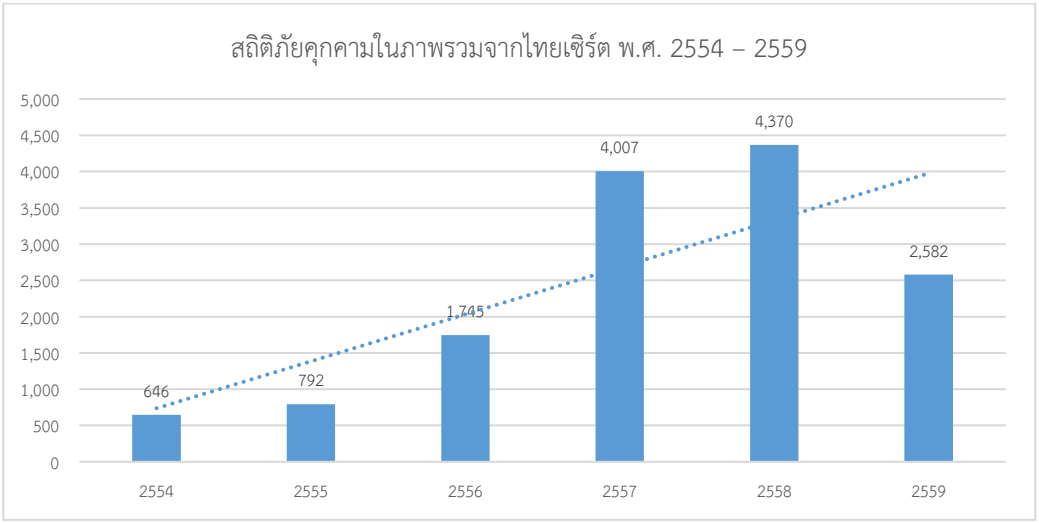
[3] CSIRT ย่อมาจาก Computer Security Incident Response Team หรือ ทีมจัดการปัญหาด้านความปลอดภัยคอมพิวเตอร์ หรือ ทีมสำหรับรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ซึ่งหมายถึง กลุ่มหรือคณะบุคคลที่ ทำการ, ประสานงาน, และสนับสนุน การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย (เหตุการณ์) ที่เกิดขึ้นภายใน sites ของผู้ใช้บริการของ CSIRT นั้น เช่น การแจ้งเตือน การให้คำแนะนำ การอบรม และการบริหารจัดการ (แหล่งที่มา: http://www.moe.go.th/moe/upload/news14/htmlfiles/10428-3189.html)

ประเภทภัยคุกคาม	คำอธิบาย
3. การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
4. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่างๆที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
5. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security)	ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้
6. ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE-Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่างๆของระบบ ภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force)
7. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
8. โปรแกรมไม่พึงประสงค์ (Malicious Code)	ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ประสงค์ร้ายประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟต์แวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ
9. ภัยคุกคามอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other)	ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่นๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่

ที่มา: บทความ Cyber Threats 2012 โดยไทยเซิร์ต

https://www.thaicert.or.th/papers/general/2012/pa2012ge001.html

แผนภาพที่ 2 สถิติภัยคุกคามในภาพรวมจากไทยเซิร์ต พ.ศ. 2554 – 2559



หมายเหตุ พ.ศ. 2554 เป็นการเก็บข้อมูลในช่วง 31 กรกฎาคม – 31 ธันวาคม 2554
พ.ศ. 2559 เป็นการเก็บข้อมูลในช่วง 1 มกราคม – 31 กรกฎาคม 2559

ที่มา: https://www.thaicert.or.th/statistics/statistics.html

ตารางที่ 3 สถิติภัยคุกคามทางไซเบอร์ รายงานโดยไทยเซิร์ต (จำแนกตามประเภทของภัยคุกคาม) ตั้งแต่ปี พ.ศ. 2554 – 2559

ประเภทภัยคุกคาม	จำนวนการเกิดภัยคุกคามทางไซเบอร์ (ครั้ง)					
	2554	2555	2556	2557	2558	2559
Abusive content	77	3	13	8	8	0
Availability	6	2	10	8	6	0
Fraud	309	534	694	1,007	1,141	725
Information gathering	93	62	8	29	0	0
Information security	0	2	0	4	0	0
Intrusion Attempts	94	75	316	504	664	370
Intrusions	0	13	631	709	1,005	699
Malicious code	63	82	73	1,738	1,546	788
Other	4	19	0	0	0	0
Total	**646**	**792**	**1,745**	**4,007**	**4,370**	**2,582**

หมายเหตุ พ.ศ. 2554 เป็นการเก็บข้อมูลในช่วง 31 กรกฎาคม – 31 ธันวาคม 2554
พ.ศ. 2559 เป็นการเก็บข้อมูลในช่วง 1 มกราคม – 31 กรกฎาคม 2559

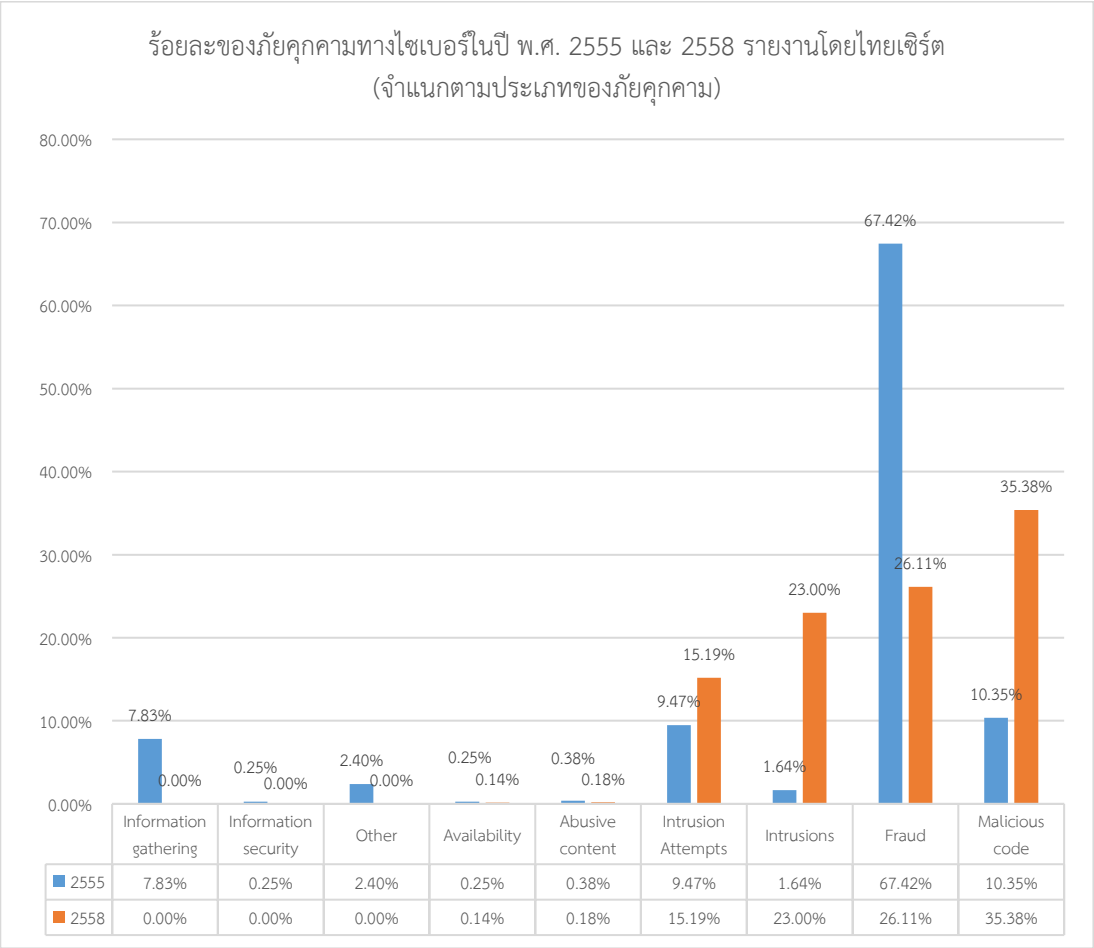
ที่มา: https://www.thaicert.or.th/statistics/statistics.html

สำหรับภัยคุกคามของประเทศไทยที่ติดตามจากข้อมูลที่ไทยเซิร์ตรายงาน (ดังแผนภาพที่ 2 และตารางที่ 3) นั้น พบว่า

1. ภัยคุกคามมีการเพิ่มขึ้นอย่างต่อเนื่อง โดยเฉพาะปี พ.ศ. 2555 – 2558 ที่มีอัตราเพิ่มขึ้นของภัยคุกคามโดยเฉลี่ยร้อยละ 86.34 ต่อปี

2. ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) ยังคงเป็นภัยคุมคามที่เกิดมากกว่าภัยคุกคามประเภทอื่น โดยมีอัตราเพิ่มขึ้นเฉลี่ยร้อยละ 29.46 ต่อปี ตามมาด้วยภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้สำเร็จ (Intrusions) ที่มีอัตราเพิ่มขึ้นเฉลี่ยร้อยละ 1,602.65 ต่อปี ตามมาด้วยภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ที่มีอัตราเพิ่มขึ้นเฉลี่ยร้อยละ 137.52 ต่อปี และพบว่าในช่วงปี พ.ศ. 2557 – 2558 ภัยคุกคามจากโปรแกรมไม่พึงประสงค์ (Malicious Code) เช่น Virus, Worm, Trojan หรือ Spyware ต่างๆ เริ่มเป็นภัยคุกคามที่เกิดมากขึ้นเป็นอันดับ 2 จากภัยคุกคามทั้ง 9 ประเภท โดยมีอัตราเพิ่มขึ้นเฉลี่ยร้อยละ 1,134.89 ต่อปี ซึ่งสวนทางกับภัยคุกคามประเภทอื่นๆ ที่มีแนวโน้มลดลง

แผนภาพที่ 3 ร้อยละของภัยคุกคามทางไซเบอร์ในปี พ.ศ. 2555 และ 2558 รายงานโดยไทยเซิร์ต (จำแนกตามประเภทของภัยคุกคาม)



ที่มา: https://www.thaicert.or.th/statistics/statistics.html

เมื่อพิจารณาจากสัดส่วนภัยคุกคามตามรายงานของไทยเซิร์ต พ.ศ. 2555 และ 2558 (ดังแผนภาพที่ 3) จะเห็นการเปลี่ยนแปลงของภัยคุกคามประเภทความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) ที่มีสัดส่วนเพิ่มขึ้นจาก 9.47% ในปี 2555 เพิ่มขึ้นเป็น 15.19% ในปี 2558 คุกคามประเภทการบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ที่มีสัดส่วนเพิ่มขึ้นจาก 1.64% ในปี 2555 เพิ่มขึ้นเป็น 23.00% ในปี 2558 และคุกคามประเภทโปรแกรมไม่พึงประสงค์ (Malicious Code) ที่มีสัดส่วนเพิ่มขึ้นจาก 10.35% ในปี 2555 เพิ่มขึ้นเป็น 35.38% ในปี 2558 ในทางกลับกัน

ภัยคุกคามประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) แม้จะมีการโจมตีที่สูงและสูงขึ้นทุกปี กลับมีสัดส่วนที่ลดลงจาก 67.42% ในปี 2555 เหลือเพียง 26.11% ในปี 2558

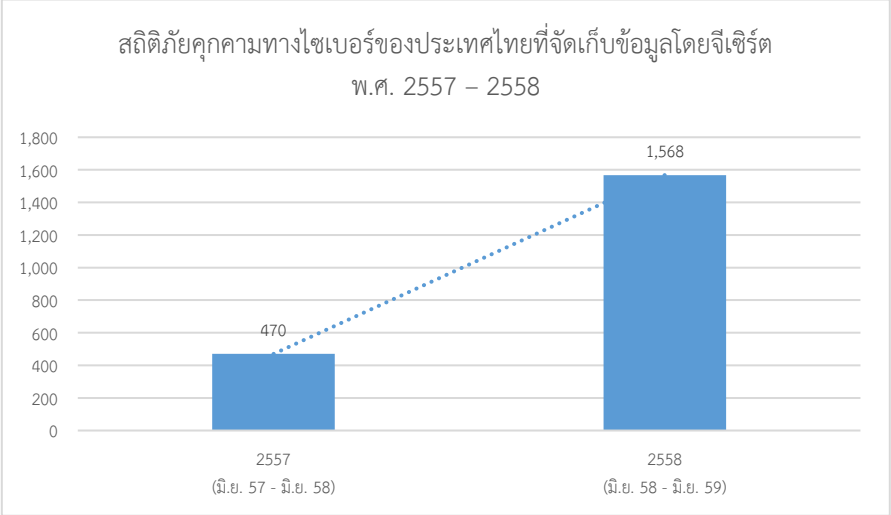
ในขณะที่ศูนย์ประสานงานความมั่นคงปลอดภัยสารสนเทศภาครัฐ (จีเซิร์ต) ซึ่งทำหน้าที่จัดการและตอบสนองเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยทางคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานภาครัฐ ได้แบ่งประเภทภัยคุกคามทางไซเบอร์เป็น 10 ประเภท ซึ่งมีรายละเอียดดังตารางที่ 4

ตารางที่ 4 การแบ่งประเภทภัยคุกคามทางไซเบอร์ โดยจีเซิร์ต

ประเภทภัยคุกคาม	คำอธิบาย
1. Application/Service/ OS configuration problem	เหตุการณ์ที่เกิดจากการ Configuration แอปพลิเคชัน/การให้บริการ/ระบบปฏิบัติการ ที่ผิดพลาด
2. Denial of Service (DoS)	เหตุการณ์ที่ผู้บุกรุกส่งข้อมูล และ packet จำนวนมากไปยังเครือข่ายหรือเครื่องของหน่วยงาน เพื่อให้เครื่องให้บริการหยุดชะงัก
3. Fraud	เหตุการณ์ที่เกิดจากการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์
4. Information Gathering	เหตุการณ์ที่ตรวจพบความพยายามของผู้บุกรุกในการค้นหาข้อมูลสำคัญเพื่อใช้สำหรับการโจมตีเข้าสู่ระบบ
5. Information Leak	เหตุการณ์ที่ตรวจพบการรั่วไหลของข้อมูลสำคัญจากช่องทางต่างๆ เช่น Social Media ที่อาจจะส่งผลกระทบต่อความมั่นคงปลอดภัย
6. Malware Detected	การบุกรุกที่เกิดจากการโจมตีของมัลแวร์ไปยังเครือข่าย และเครื่องให้บริการของหน่วยงาน ได้แก่ Backdoor, Trojan, Virus, Worm และ Botnet
7. Server Compromise	เหตุการณ์ที่ตรวจพบว่าเครื่องให้บริการ (Server) ของหน่วยงานถูกบุกรุกและเข้าถึงโดยไม่ได้รับอนุญาต โดยผู้บุกรุกเป็นที่เรียบร้อย
8. Service Unavaliable	การทำให้บริการมีปัญหาหรือเกิดเหตุขัดข้อง จนไม่สามารถให้บริการได้
9. Suspicious Activity	การเชื่อมต่อข้อมูล และ Traffic ที่ผิดปรกติ และมีความเชื่อมโยงที่จะเป็นการบุกรุกระบบ
10. Web Compromise	Web Application หรือเว็บไซต์ ถูกยึดครองโดยไม่ได้รับอนุญาต

ที่มา: ส่วนความมั่นคงปลอดภัยสารสนเทศ ฝ่ายวิศวกรรมและปฏิบัติการ สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)

แผนภาพที่ 4 สถิติภัยคุกคามทางไซเบอร์ของประเทศไทยที่จัดเก็บข้อมูลโดยจีเซิร์ต พ.ศ. 2557 – 2558



หมายเหตุ รายงานสถิติของจีเซิร์ตจะเก็บข้อมูลเป็นรายปี โดยเริ่มเก็บข้อมูลตั้งแต่เดือนมิถุนายน พ.ศ. 2558
ที่มา: รายงานสรุปการตรวจสอบและเฝ้าระวังระบบบริหารจัดการภัยคุกคามทางสารสนเทศภาครัฐ ประจำปี 2557 และ 2558

ตารางที่ 5 สถิติภัยคุกคามทางไซเบอร์ รายงานโดยจีเซิร์ต (จำแนกตามประเภทของภัยคุกคาม) พ.ศ. 2557 – 2558

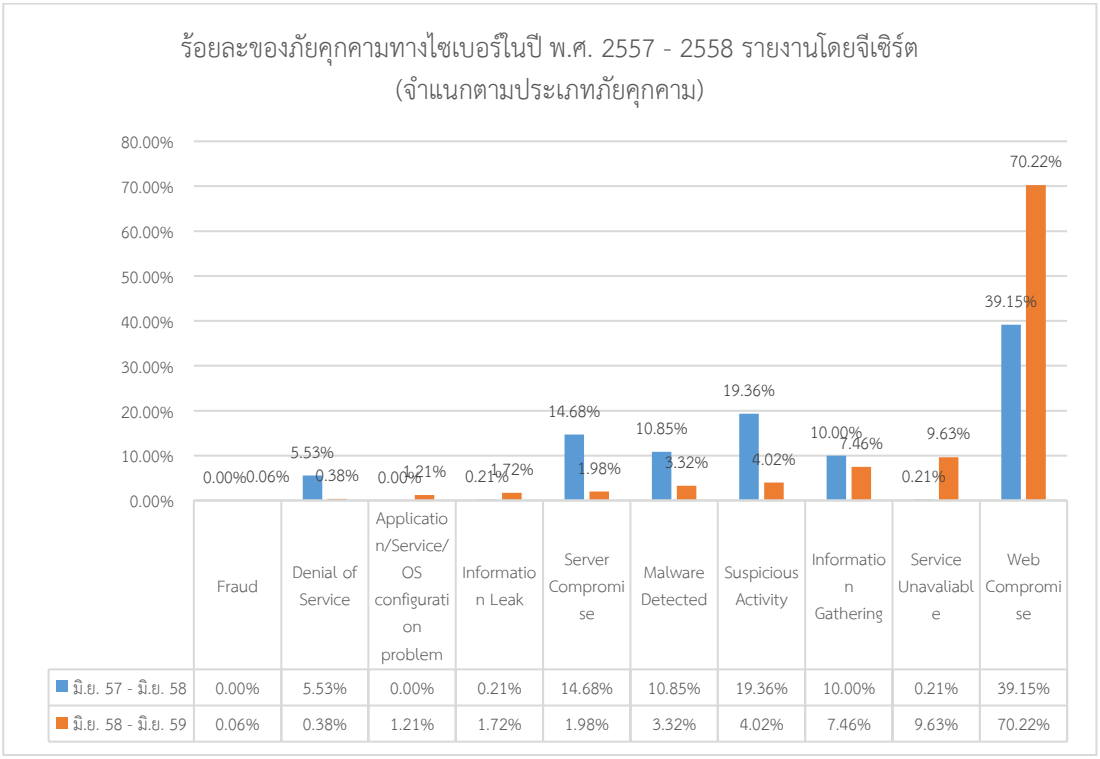
ประเภทภัยคุกคาม	จำนวนการเกิดภัยคุกคามทางไซเบอร์ (ครั้ง)	
	มิ.ย. 57 - มิ.ย. 58	มิ.ย. 58 - มิ.ย. 59
Fraud	0	1
Denial of Service	26	6
Application/Service/OS configuration problem	0	19
Information Leak	1	27
Server Compromise	69	31
Malware Detected	51	52
Suspicious Activity	91	63
Information Gathering	47	117
Service Unavailable	1	151
Web Compromise	184	1,101
Total	**470**	**1,568**

หมายเหตุ รายงานสถิติของจีเซิร์ตจะเก็บข้อมูลเป็นรายปี โดยเริ่มเก็บข้อมูลตั้งแต่เดือนมิถุนายน พ.ศ. 2558
ที่มา: รายงานสรุปการตรวจสอบและเฝ้าระวังระบบบริหารจัดการภัยคุกคามทางสารสนเทศภาครัฐ ประจำปี 2557 และ 2558

จากสถิติภัยคุกคามทางไซเบอร์ที่จัดเก็บโดยจีเซิร์ตพบว่า การโจมตีทางไซเบอร์ที่เกิดขึ้นกับหน่วยงานภาครัฐมีจำนวนเพิ่มขึ้นจาก 470 ครั้งในปี 2557 (มิ.ย. 57 - มิ.ย. 58) เพิ่มเป็น 1,568 ครั้ง ในปี 2558 (มิ.ย. 58 - มิ.ย. 59) หรือคิดเป็นร้อยละ 233.62 โดยเหตุการณ์โจมตีที่เกิดขึ้นสูงที่สุด คือการโจมตีประเภทการโจมตีแบบยึดครองหรือควบคุมเว็บไซต์ (Web Compromise) มีจำนวนทั้งสิ้น 1,101 ครั้ง ในปี 2558 โดยมีอัตราเพิ่มขึ้นถึงร้อยละ 498.37 โดยวิธีการโจมตีวิธีหนึ่งของภัยคุกคามประเภท Web Compromise คือการมุ่งโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บ (Website Defacement) ซึ่งการโจมตีนั้นอาจปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ โดยอาจไม่ได้ก่อความเสียหายที่รุนแรง แต่สามารถทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ โดยเฉพาะอย่างยิ่งเว็บไซต์ของหน่วยงานภาครัฐที่ต้องการความน่าเชื่อถือเป็นอย่างสูง โดยเว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะปรากฏรูปภาพหรือข้อความที่บ่งบอกถึงว่าเว็บไซต์ได้ถูกโจมตีได้สำเร็จ หากผู้ดูแลระบบไม่สามารถปิดช่องโหว่ในกรโจมตีได้สำเร็จ อาจทำให้เว็บไซต์เกิดความเสียหายในรูปแบบเดิมซ้ำๆ จนสุดท้ายอาจทำให้ถูกแจ้งเตือนบนหน้าเว็บไซต์ของผู้ให้บริการ Search engine ต่างๆ เช่น Google, Yahoo เป็นต้น ซึ่งจะยิ่งทำลายความน่าเชื่อถือของเว็บไซต์และหน่วยงานให้ลดลงไปอีก การที่สถิติการเกิดภัยคุกคามประเภทนี้สูงขึ้นมากส่วนหนึ่งมาจากเหตุการณ์การต่อต้านนโยบาย Single Gateway ของรัฐบาล จึงมี “พลเมืองต่อต้าน Single Gateway” เข้ามาก่อกวนและขัดขวางระบบเพื่อทำลายความน่าเชื่อถือของรัฐบาล

เหตุการณ์โจมตีที่เกิดขึ้นสูงอันดับสองคือ การทำให้บริการเกิดเหตุขัดข้องจนไม่สามารถให้บริการได้ (Service Unavaliable) จำนวน 151 ครั้ง และอันดับสาม Information Gathering การตรวจพบว่าผู้บุกรุกพยายามค้นหาข้อมูลสำคัญเพื่อใช้สำหรับการโจมตีเข้าสู่ระบบ จำนวน 117 ครั้ง

แผนภาพที่ 5 ร้อยละของภัยคุกคามทางไซเบอร์ในปี พ.ศ. 2557 - 2558 รายงานโดยจีเซิร์ต (จำแนกตามประเภทภัยคุกคาม)



ที่มา: รายงานสรุปการตรวจสอบและเฝ้าระวังระบบบริหารจัดการภัยคุกคามทางสารสนเทศภาครัฐ ประจำปี 2557 และ 2558

เมื่อพิจารณาจากสัดส่วนภัยคุกคามตามรายงานสรุปการตรวจสอบและเฝ้าระวังระบบบริหารจัดการภัยคุกคามทางสารสนเทศภาครัฐ ประจำปี 2557 และ 2558 ของจีเซิร์ต (ดังแผนภาพที่ 5) จะเห็นได้ว่าการโจมตีประเภทการยึดครองหรือควบคุมเว็บไซต์ของหน่วยงานภาครัฐ (Web Compromise) ยังคงมีสัดส่วนที่มากที่สุด (ร้อยละ 39.15 ในปี 2557 และ ร้อยละ 70.22 ในปี 2558) และเพิ่มขึ้นอย่างก้าวกระโดด ในทางกลับกันการโจมตีประเภทการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สำหรับหน่วยงานภาครัฐมีการเกิดขึ้นเพียงครั้งเดียว และมีสัดส่วนในการเกิดต่ำที่สุด (ร้อยละ 0.00 ในปี 2557 และ ร้อยละ 0.06 ในปี 2558) ในช่วง 2 ปีที่ผ่านมา

อย่างไรก็ตาม ข้อมูลทางสถิติที่นำเสนอมาข้างต้น เป็นการรายงานในมิติของจำนวนครั้งที่เกิดการโจมตีทางไซเบอร์ ซึ่งข้อมูลดังกล่าวยังมีข้อจำกัดในการนำเสนอในมิติเรื่องระดับความรุนแรง ซึ่งเป็นอีกมิติซึ่งมีความสำคัญในด้านผลกระทบและความเสียหายที่เกิดขึ้นทั้งในระดับบุคคล องค์กร และประเทศ ดังเช่นกรณีเมื่อวันที่ 11 กุมภาพันธ์ พ.ศ. 2558 ได้เกิดการโจมตีทางไซเบอร์โดยใช้อีเมลหลอกลวงเพื่อขโมยข้อมูลส่วนตัวของผู้ใช้งาน (Phishing) ซึ่งเป็นวิธีการโจมตีอย่างหนึ่งในภัยคุกคามประเภทการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) โดยผู้ใช้งานอีเมลจะได้รับอีเมลซึ่งมีเนื้อหาชักจูงให้คลิกไปยังลิงค์ที่เชื่อมต่อไปยังหน้าเว็บ Phishing ที่ถูกสร้างขึ้นเพื่อหลอกให้กรอกข้อมูลส่วนบุคคล รวมถึงชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) หากผู้ใช้งานหลงเชื่อกรอกข้อมูลดังกล่าว ผู้ไม่หวังดีก็จะได้ข้อมูลส่วนตัวไปทันที

จากการตรวจสอบทางสถิติโดยใช้เครื่องมือของ Google เฉพาะในวันที่ 13 กุมภาพันธ์ พ.ศ.2558 พบว่ามีผู้ใช้งานอีเมลในประเทศไทยหลงคลิกลิงค์นี้แล้วประมาณ 600 ครั้ง และที่สำคัญยังพบว่าหน่วยงานภาครัฐหลายแห่งตกเป็นเป้าหมายการโจมตีครั้งนี้ ซึ่งอาจจะเป็นความตั้งใจของผู้โจมตีที่มุ่งเจาะข้อมูลของบุคลากรในหน่วยงานรัฐ ใช้เป็นเครื่องมือในการแพร่กระจายอีเมลหลอกลวงไปยังประชาชน ซึ่งอาจส่งผลให้ประชาชนเชื่อและถูกหลอกให้กรอกข้อมูลต่อๆ กันไป จากเหตุการณ์ดังกล่าว ทำให้หน่วยงานภาครัฐต้องเร่งออกประกาศเตือนไปยังประชาชนให้ระมัดระวังการใช้งานอีเมล[4]

หากพิจารณาจากตารางที่ 5 และแผนภาพที่ 5 สถิติการเกิดภัยคุกคามทางไซเบอร์ประเภทการฉ้อฉล ฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) ในปี 2558 นั้น มีการรายงานการเกิดเหตุเพียง 1 ครั้ง และมีสัดส่วนการเกิดภัยคุกคามประเภทนี้ต่ำที่สุด ซึ่งจะเห็นได้ว่าหากพิจารณาเพียงจำนวนครั้งที่เกิดภัยคุกคามทางไซเบอร์อาจทำให้มองข้ามความรุนแรงของผลกระทบจากภัยคุกคามแต่ละประเภทได้

ปัญหาเรื่องภัยคุกคามทางไซเบอร์ (Cyber Security) จะยังคงเติบโตอย่างต่อเนื่องตามเทคโนโลยีที่ทันสมัยมากขึ้น หน่วยงานภาครัฐจะยังคงเป็นเป้าหมายสำคัญในการโจมตีทางไซเบอร์จากผู้ไม่หวังดี ทั้งจากการโจมตีเพื่ออาศัยความน่าเชื่อถือของหน่วยงานภาครัฐมาใช้หลอกลวงประชาชนอีกต่อหนึ่ง และการโจมตีเพื่อทำลายความน่าเชื่อถือของหน่วยงาน อันเกิดจากสาเหตุต่างๆ ไม่ว่าจะเป็นการต้องการแสดงพลังของกลุ่มบุคคลที่ต่อต้านนโยบายของรัฐบาล การมุ่งทำลายชื่อเสียง การก่อกวน หรือแม้กระทั่งการโจมตีเพื่อทดสอบความสามารถของตนเองเพื่อแสดงให้

[4] ที่มา https://www.etda.or.th/content/etda-hackers-alarm-2015-02-17.html

กลุ่มแฮคเกอร์ด้วยกันได้รับรู้ ในอนาคตการโจมตีทางไซเบอร์จะมีการปรับเปลี่ยนวิธีการหรือมีความรุนแรงเพิ่มมากขึ้น เนื่องจากสามารถหาเครื่องมือในการโจมตีได้ง่ายจากอินเตอร์เน็ทและเว็บไซต์ใต้ดิน ซึ่งจะทำให้มีแฮคเกอร์หน้าใหม่เกิดขึ้นได้ง่าย รัฐบาลจะต้องให้ความสำคัญเรื่องความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) อย่างเป็นรูปธรรม โดยมีการประกาศใช้พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ผ่านการทำประชาพิจารณ์เพื่อรับฟังมุมมองที่เป็นประโยชน์และการได้รับการยอมรับจากภาคเอกชนและภาคประชาชน แต่สิ่งที่สำคัญยิ่งกว่านั้น ประชาชนโดยเฉพาะอย่างยิ่งบุคลากรของหน่วยงานภาครัฐในทุกระดับ จะต้องตระหนักถึงความสำคัญ การเฝ้าระวัง และการปฏิบัติให้ถูกต้องตามมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของหน่วยงานเพื่อป้องกันตนเองและหน่วยงานให้ปลอดภัยจากการถูกโจมตี นอกจากนี้การติดตามสถานการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ก็มีความสำคัญที่จะช่วยให้สามารถพร้อมรับมือกับภัยคุกคามใหม่ๆ ที่เกิดขึ้นได้อย่างทันท่วงที

- เอกสารอ้างอิง –

สถิติภัยคุกคาม ประจำปี. (พ.ศ. 2554-2559). Thailand Computer Emergency Response Team (ThaiCERT). สืบค้นข้อมูลจาก https://www.thaicert.or.th/statistics/statistics.html

ความเป็นมาของไทยเซิร์ต จากกระทรวงวิทย์ฯ สู่กระทรวงไอซีที. (6 ก.พ. 2555). Thailand Computer Emergency Response Team (ThaiCERT). สืบค้นข้อมูลจาก http://www.moe.go.th/moe/upload/news14/htmlfiles/10428-3189.html

รายงานสรุปการตรวจสอบและเฝ้าระวังระบบบริหารจัดการภัยคุกคามทางสารสนเทศภาครัฐ ประจำปี (พ.ศ. 2557-2558). สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)(สรอ.)

คณะผู้จัดทำ

อรฉัตร เลียงพิบูลย์	ผู้จัดการส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์
ทิพสุดา โชติชื่น	นักวิเคราะห์นโยบายอาวุโส
ธรรณพ ศิริธรรมวิไล	นักวิเคราะห์นโยบายอาวุโส

ส่วนนโยบายรัฐบาลอิเล็กทรอนิกส์

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน)(สรอ.)

PSP_DIVISION@EGA.OR.TH