TB-CERT

Thailand Banking Sector CERT

ANNUAL REPORT 2020

Incident Response Strategy

Containment

Collaboration

Research and Development

Professional skills development

4th Fl., 5/13 Moo 3, Chaengwattana Rd., Pakkret, Nonthaburi 11120

025587500

https://www.tba.or.th/tb-cert/

contact@tb-cert.or.th

รายงานประจำปี

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร

Thailand Banking Sector CERT: TB-CERT

Annual Report 2020

จัดทำโดย

กิตติ โฆษะวิสุทธิ์

ธาวินี วงศ์วิศว์

กิติศักดิ์ จิรวรรณกูล

ปิลัญญา เชิญถนอมวงศ์

ชญานิน แก้วหาญ

ที่ปรึกษา

กิตติ โฆษะวิสุทธิ์

บรรณาธิการ

ธาวินี วงศ์วิศว์

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร

สมาคมธนาคารไทย

5/13 หมู่ 3 ถนนแจ้งวัฒนะ ตำบลคลองเกลือ

อาเภอปากเกร็ด จังหวัดนนทบุรี 11120

0 2558 7500

contact@tb-cert.or.th

เผยแพร่เมื่อ

กุมภาพันธ์ 2021

TLP: WHITE

Content

เกี่ยวกับ TB-CERT

ความเป็นมา

Thailand Banking Sector Computer Emergency Response Team หรือ TB-CERT จัดตั้งขึ้นโดยความเห็นชอบของผู้บริหารระดับสูงของธนาคารพาณิชย์ในประเทศไทย เพื่อสนับสนุนให้สมาชิกกลุ่มซึ่งเป็นพนักงานของธนาคารได้มีการแลกเปลี่ยนข้อมูลและประสบการณ์เพื่อประโยชน์โดยรวมของสถาบันการเงินในประเทศไทย โดยเฉพาะเพื่อการนำไปใช้ในการป้องกันเหตุภัยคุกคามทางไซเบอร์ที่อาจจะมีผลกระทบกับการบริการ ทรัพยากร หรือบุคลากรขององค์กร โดยจะไม่เสนอความเห็นต่อผลิตภัณฑ์ทางการเงิน (Product) หรือให้ข้อมูลเชิงลบต่อหน่วยงานหรือบุคคลที่สาม อันจะทำให้เกิดความเสื่อมเสียและเป็นอุปสรรคต่อกิจกรรมการแลกเปลี่ยนความคิดเห็นหรือความสัมพันธ์อันดีของสมาชิกในกลุ่ม

ค่านิยมหลัก

TB-CERT เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลในด้านความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์รวมของบุคลากรที่มีความชำนาญด้านไซเบอร์ และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อ ไม่ว่าจะเกิดกับบุคลากร ลูกค้า หรือธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและต่างประเทศเพื่อให้สามารถรับรู้ข่าวสารและช่วยเหลือในการแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การดำเนินงาน

การดำเนินงานของ TB-CERT จะครอบคลุม 4 ด้านที่สำคัญคือ

1. **เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล** ทั้งภัยคุกคามด้านไซเบอร์และแนวทางการแก้ไข
2. **สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัย** ของการใช้เทคโนโลยีใหม่
3. **กำหนดกระบวนการในการรับมือภัยไซเบอร์ภาคการธนาคาร** และจัดให้มีการซ้อมรับมือร่วมกันอย่างสม่ำเสมอ
4. **ส่งเสริมการพัฒนาบุคลากรด้าน Cybersecurity** โดยครอบคลุมทั้งการสร้างบุคลากรใหม่เข้าสู่ภาคการเงินและพัฒนาบุคลากรของสถาบันการเงินให้มีความรู้ความเข้าใจ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

ทิศทาง วิสัยทัศน์ ของภาคการธนาคาร ในมุม Digital Banking & Cybersecurity

คุณรณดล นุ่มนนท์
รองผู้ว่าการ ด้านเสถียรภาพสถาบันการเงิน
ธนาคารแห่งประเทศไทย

ปี 2020 นับเป็นปีที่มีความผันผวน เปลี่ยนแปลงมาก จากสถานการณ์แพร่ระบาดของไวรัส COVID-19 สะท้อนโลกของ VUCA ได้เป็นอย่างดี คือ มีทั้งความผันผวน ไม่แน่นอน และมีความซับซ้อนไม่ชัดเจนเพิ่มขึ้น COVID-19 จึงเป็นปัจจัยสำคัญที่เร่งให้เกิดการปรับตัวในทุกภาคส่วน สำหรับภาคการเงินนั้นต้องปรับตัวในหลายด้าน ทั้งด้านการดูแลช่วยเหลือลูกค้าที่ได้รับผลกระทบจากสถานการณ์ดังกล่าวและภาวะเศรษฐกิจ ขณะเดียวกันต้องปรับรูปแบบการทำงานให้มีความปลอดภัยทั้งกับพนักงานและลูกค้า รวมทั้งต้องสามารถรองรับการให้บริการผ่านช่องทาง online ได้อย่างต่อเนื่อง จึงต้องดำเนินการหลายประการทั้งการปรับรูปแบบธุรกิจ การปรับปรุงระบบ และกฎระเบียบต่าง ๆ รวมทั้งกระบวนการทำงานติดต่อสื่อสาร ขณะที่ภาครัฐได้ใช้ประโยชน์จากบริการการเงิน digital ต่าง ๆ ได้ให้ความช่วยเหลือประชาชนอย่างตรงจุด ดังนั้น ในช่วงนี้เราจึงได้เห็นสถิติการทำธุรกรรมการเงินต่าง ๆ โดยเฉพาะธุรกรรมที่ผ่านระบบพร้อมเพย์สูงขึ้นแบบก้าวกระโดด

ในช่วงการเปลี่ยนผ่าน digital transformation ที่เกิดขึ้นเร็วโดยมี COVID-19 เป็นปัจจัยเร่ง โดยเฉพาะในภาคการธนาคารนี้ ถือว่าเป็นการเปลี่ยนผ่านที่มีความท้าทายเป็นอย่างมาก โดยเฉพาะอย่างยิ่งกับกลุ่มผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ที่เป็นกำลังสำคัญที่จะช่วยระวังป้องกันภัย เพื่อรักษาระดับการบริหารจัดการความเสี่ยง IT และ Cybersecurity ให้อยู่ในระดับมาตรฐานที่ดี พร้อมตอบโจทย์การฟื้นตัวต่อระบบเศรษฐกิจ และความต้องการของลูกค้าประชาชน ท่ามกลางสภาวะการเร่งพัฒนาผลิตภัณฑ์ บริการ และนวัตกรรมใหม่ ดังนั้น การจัดการความเสี่ยงด้านไซเบอร์ จึงเป็นหัวใจสำคัญต่อความเชื่อมั่นของผู้ใช้บริการและระบบการเงิน

ผลงานของ TB-CERT ที่ผ่านมา ได้เห็นประจักษ์มาอย่างต่อเนื่องนับตั้งแต่เริ่มก่อตั้งในปี 2017 ช่วยยกระดับความปลอดภัยของภาคการเงินให้มีมาตรฐานเทียบเคียงสากล และที่สำคัญคือการช่วยติดตาม สอดส่องดูแล และประสานงานในด้านภัยคุกคามไซเบอร์ให้ภาคการธนาคารของประเทศไทยในช่วงวิกฤตในปี 2020 ผมขอชื่นชมและเป็นกำลังใจให้คณะทำงานปฏิบัติหน้าที่ด้วยความเข้มแข็งอย่างต่อเนื่อง

ในก้าวต่อไป TB-CERT ยังมีภารกิจที่สำคัญในการยกระดับความมั่นคงปลอดภัยของโครงสร้างพื้นฐานสำคัญของประเทศตาม พ.ร.บ. ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในมิติด้านการเพิ่มความแข็งแกร่งภายในของภาคการเงินอย่างต่อเนื่อง โดยเฉพาะการพัฒนาศักยภาพของบุคลากรทางเทคนิคเชิงลึกที่ต้องอาศัยการฝึกฝนทักษะความเชี่ยวชาญเพื่อให้มีศักยภาพในการป้องกัน ติดตาม และรับมือภัยไซเบอร์รูปแบบใหม่ ๆ ที่นับวันจะทวีความรุนแรงและซับซ้อนมากยิ่งขึ้น ตลอดจนมิติในด้านการสร้างพันธมิตรกับภาคอุตสาหกรรมอื่นที่มีความเชื่อมโยงกัน อาทิ ภาคสื่อสารและโทรคมนาคม ที่เป็นโครงข่ายสำคัญของการให้บริการ digital banking และ payment ภาคสาธารณูปโภค โดยธนาคารแห่งประเทศไทยยินดีผลักดันและให้การสนับสนุน TB-CERT เพื่อสร้างความเข้มแข็งด้านไซเบอร์ให้กับสถาบันการเงิน ระบบการเงิน และเศรษฐกิจโดยรวมของประเทศไทยต่อไป

คำนิยม

คุณผยง ศรีวณิช
ประธานสมาคมธนาคารไทย

ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์เป็นหนึ่งในภัยคุกคามที่ส่งผลกระทบต่อภาคธุรกิจอย่างหลีกเลี่ยงไม่ได้ในยุคดิจิทัลนี้ ธนาคารจึงต้องปรับตัวให้ทันต่อการเปลี่ยนแปลงและเตรียมพร้อมรับมือกับภัยคุกคามทางไซเบอร์ที่นับวันจะมีความซับซ้อนและทวีความรุนแรงมากยิ่งขึ้น การมีระบบป้องกันที่รัดกุมเข้มแข็ง ระบบการตรวจจับที่แม่นยำน่าเชื่อถือ การตอบสนองต่อเหตุการณ์ที่ทันท่วงที สามารถฟื้นฟูระบบให้กลับมาทำงานได้อย่างรวดเร็ว เป็นสิ่งที่ธนาคารได้ให้ความสำคัญมาโดยตลอด เพื่อลดความเสี่ยง ผลกระทบและความเสียหายต่อธนาคารและลูกค้าของธนาคารได้ รวมทั้งการสร้างความรู้ทักษะของคนในองค์กรและสร้างความตระหนักรู้ให้กับลูกค้าให้มีทักษะความรู้ความเข้าใจถึงภัยไซเบอร์ให้รู้เท่าทันต่อเหตุการณ์ ซึ่งหากไม่มีความตระหนักรู้และเข้าใจว่าภัยไซเบอร์สามารถมาในรูปแบบไหนได้บ้างอาจเป็นจุดอ่อนสำคัญที่จะทำให้เหล่าแฮกเกอร์โจมตีได้ง่าย นอกจากนี้ ระบบการเงินมีการทำงานที่เชื่อมโยงกัน การสร้างความร่วมมือจึงเป็นปัจจัยสำคัญในการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ในทุกภาคส่วน

ผมเล็งเห็นว่า TB-CERT เป็นกลไกสำคัญในการสร้างความเชื่อมั่นและความเข้มแข็งร่วมกันของระบบสถาบันการเงิน ทั้งการศึกษาแลกเปลี่ยนข่าวสาร เหตุการณ์ภัยคุกคามและข้อมูลเชิงลึกร่วมกับพันธมิตรทั้งในและต่างประเทศ การสร้างความรู้ความเข้าใจและการเตรียมความพร้อมของทีมงานและคณะผู้บริหารผ่านการซักซ้อมทดสอบรับมือภัยไซเบอร์อยู่เป็นประจำ ตลอดจนร่วมกันยกระดับมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สถาบันการเงินซึ่งถือเป็นหน่วยงานโครงสร้างพื้นฐานสารสนเทศที่สำคัญของประเทศมีความพร้อม อันจะก่อให้เกิดการบูรณาการของการสร้างความเข้มแข็งอย่างยั่งยืนในระดับประเทศต่อไปและเป็นที่ยอมรับในระดับสากล

NEUTRAL • TRUSTED ADVISOR • EXPERTISE HUB

In cybersecurity for Thailand Banking Sector

สารจากคณะกรรมการ TB-CERT

" การศึกษา สร้างความรู้
การปรับเปลี่ยน สร้างความคิด
การปฏิบัติ สร้างทักษะ
การร่วมมือ สร้างความยั่งยืน "

ดร.กิตติ โฆษะวิสุทธิ์
Senior Vice President, Security Management
ธนาคารกรุงเทพ

คุณชัชวัฒน์ อัศวรักวงศ์
Chief Information Security Officer (Acting)
บริษัทกสิกร บิซิเนส-เทคโนโลยี กรุ๊ป

" วิกฤตและความท้าทายทำให้เราแกร่งขึ้น เก่งขึ้นด้วยสปีดที่เร็วกว่า ปกติ จงเรียนรู้จากวิกฤตและมองให้เป็นโอกาส ผลักดันตัวเราให้วิ่งไปข้างหน้า ก้าวข้ามไปให้ได้ และพวกเราจะประสบความสำเร็จแบบก้าวกระโดด "

" ในปี 2020 รูปแบบของ Cyber Threat มีปรับเปลี่ยนทั้งเพิ่มความซับซ้อนทางด้านเทคนิค มีผลรุนแรงมากขึ้นทั้งกระทบกับธุรกิจ และผู้ใช้บริการ ดังที่เห็นในหลายกรณีศึกษาเช่น Source Code Leak ที่เกิดบนการพัฒนาระบบบน Cloud, Ransomware Attack องค์กรใหญ่ ๆ , Customer Data Leak ที่เกิดจากการโจมตี Critical Vulnerability, และ SMS Phishing Attack ที่เกิดกับหลายธนาคารช่วงปลายปี ทั้งหมดเป็นข้อมูลยืนยันบทบาทของเจ้าหน้าที่ด้านความปลอดภัยไซเบอร์ที่ต้องทำงานเชิงรุกมากขึ้นเพื่อพร้อมรับความท้าทายที่จะเกิด
TB-CERT ยังคงต้องรับบทบาทสำคัญ ในการทำงานเชิงรุกร วมกับธนาคารสมาชิกให้พร้อมในการรับความท้าทายที่เกิด ทั้งนี้ส่งผลให้เกิดความเชื่อมั่นของประชาชนต่อบริการธนาคารในภาพรวม "

คุณภคพงศ์ จุลวงศาศิลป์
Senior Vice President,
Head of Cyber Security Department
ธนาคารกรุงศรีอยุธยา

สารจากคณะกรรมการ TB-CERT

" Cyber Security needs to be the culture.
It is not only IT responsibility,
but it is everyone's. "

คุณสมบูรณ์ หิรัญภัทรศิลป์
Head Country, Technology Management
ธนาคารสแตนดาร์ดชาร์เตอร์ด

คุณนฤดม รุ่งศิริวงศ์
Senior Vice President, IT Security Head
ธนาคารเกียรตินาคินภัทร

" การใช้แนวปฏิบัติที่ดี (Best Practice) เพื่อดำเนินการทางด้าน Cyber Security อาจไม่เพียงพอหรือเกินความจำเป็นก็แล้วแต่บริบทของการใช้งาน สิ่งที่ดีที่สุดในการบริหารจัดการทางด้าน Cyber Security ก็คือการบริหารความเสี่ยงโดยใช้แบบจำลองภัยคุกคาม (Threat Modelling) เพื่อช่วยประเมินและหาทางลดความเสี่ยงได้อย่างเหมาะสม "

" สิ่งที่ท้าทายในการรักษาความปลอดภัยด้านไซเบอร์ คือ การมีความรู้เท่าทันภัยคุกคามในปัจจุบัน รวมถึงการตระหนักรู้ถึงผลกระทบที่จะตามมา ซึ่งสิ่งเหล่านี้เป็นองค์ประกอบสำคัญที่ต้องมีในผู้ดูแลรักษาความปลอดภัยด้านไซเบอร์ให้กับสถาบันการเงิน จึงเป็นสิ่งที่ TB-CERT เห็นถึงความสำคัญนี้ ซึ่งเป็น 1 ในภารกิจสำคัญของ TB-CERT ตลอดมา "

คุณประกลกฤษ แสงชูวงศ์
Team Head of Information,
Security Detection and Response
ธนาคารทหารไทย

คุณยศ กิมสวัสดิ์
Head of Payment System Office
สมาคมธนาคารไทย

" อัตราการเติบโตของการใช้งาน Mobile Banking ได้เพิ่มสูงขึ้นอย่างมีนัยสำคัญในปี 2020 และมีการคาดการณ์ว่าปี 2021 จะเพิ่มสูงขึ้นเช่นกัน ส่วนหนึ่งมาจากการกระตุ้นการใช้งานในสังคมไร้เงินสดผนวกกับสถานการณ์โควิด ทำให้การใช้ Mobile Banking ยิ่งเพิ่มมากขึ้น ความมั่นคงปลอดภัยของบริการจะสร้างความเชื่อมั่นให้กับผู้บริโภคและมีส่วนสำคัญในการกระตุ้นและส่งเสริมให้มีปริมาณการทำธุรกรรมมากขึ้น "

บทนำ

ตลอดระยะเวลา 4 ปีที่ผ่านมาศูนย์ประสานงานความร่วมมือความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคารหรือทีบีเซิร์ต (Thailand Banking Sector CERT: TB-CERT) สมาคมธนาคารไทยได้ดำเนินการหลายอย่างนับตั้งแต่ก่อตั้ง TB-CERT ขึ้นภายใต้ความร่วมมือของธนาคารสมาชิกสมาคมธนาคารไทย 15 แห่ง ซึ่งแนวคิดที่จะจัดตั้ง CERT ขึ้นมาเนื่องจากว่า เมื่อปี 2016 ธนาคารใหญ่หลายแห่งในประเทศไทยถูกขู่จากเหล่า Hacker ว่าจะทำการโจมตีธนาคารด้วยวิธีการทำ DDOS (Distributed Denial of Service) ซึ่งเป็นการขู่โจมเว็บไซต์เป้าหมายโดยอาศัยการขู่โจมจากหลากหลายที่พร้อม ๆ กัน ทำให้เว็บไซต์ไม่สามารถใช้งานได้ หรือที่เราเรียกว่า เว็บล่ม หลังจากเกิดเหตุการณ์นี้ขึ้นผู้บริหารของภาคการธนาคารในสมาคมธนาคารไทยเล็งเห็นว่า ธนาคารจะต้องร่วมมือกันป้องกันภัยไซเบอร์นี้ จึงได้จัดตั้งกลุ่มเหล่าผู้เชี่ยวชาญด้านไซเบอร์จากหลากหลายธนาคารที่มีชื่อว่า ISG ย่อมาจาก Information Sharing Group โดยมีวัตถุประสงค์เพื่อแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ร่วมกันเพื่อเป็นการเตือนภัยและป้องกันให้ธนาคารได้มีการเตรียมพร้อมที่จะรับมือกับภัยไซเบอร์ได้ทันท่วงที ผู้บริหารยังเล็งเห็นว่าการแลกเปลี่ยนข้อมูลระหว่างธนาคารนั้นยังไม่เพียงพอต่อการรับมือกับภัยไซเบอร์ จำเป็นต้องปรับเปลี่ยนบทบาทหน้าที่ของกลุ่ม ISG ให้มีความเป็นบทบาทของ CERT (Computer Emergency Response Team) เพราะนั่นไม่เพียงแต่แลกเปลี่ยนข้อมูลกันยังเองแต่ต้องแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอกอื่น ๆ ด้วย เพื่อสร้างเครือข่ายการแลกเปลี่ยนข้อมูลให้มีข้อมูลมากขึ้นและรวดเร็วขึ้น อีกทั้งการพัฒนาส่งเสริมบุคลากรของภาคการธนาคารให้มีศักยภาพเท่าทันกับภัยไซเบอร์ที่ทวีความซับซ้อนรุนแรงมากขึ้น ก็เป็นส่วนหนึ่งของบทบาทที่จะต้องขับเคลื่อนไปพร้อม ๆ กัน จึงได้จัดตั้ง CERT ของภาคการธนาคารขึ้นในประเทศไทย จึงเป็นจุดกำเนิดของการจัดตั้ง TB-CERT ในเดือนตุลาคม 2017 อย่างเป็นทางการ ซึ่งในสมัยนั้นท่านผู้ว่าการธนาคารแห่งประเทศไทย ดร.วิรไท สันติประภพ คุณปรีดี ดาวฉาย ประธานสมาคมธนาคารไทย คุณสุรางคณา วายุภาพ ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และ ดร.กิตติ โฆษะวิสุทธิ์ ผู้จัดการอาวุโส จัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศสายเทคโนโลยี ธนาคารกรุงเทพ ให้เกียรติเป็นประธานร่วมงานจัดตั้ง TB-CERT อย่างเป็นทางการที่ธนาคารแห่งประเทศไทย

จากวันนั้นถึงวันนี้ TB-CERT ได้ทำภารกิจหลายอย่างซึ่งมุ่งเน้นที่ 5 ส่วนหลัก ๆ อันได้แก่ 1. พัฒนาบุคลากรด้าน Cybersecurity ของ ภาคการธนาคาร 2. ช่วยกำหนดมาตรฐานด้าน Cybersecurity ให้กับภาคการธนาคาร 3. สร้างความตระหนักถึงภัยคุกคามด้าน Cybersecurity สำหรับสมาชิกและประชาชน 4. วิจัยและพัฒนาด้าน Cybersecurity ให้กับภาคการธนาคาร 5. ให้บริการแก่ธนาคารสมาชิกในการวิเคราะห์และแจ้งเตือนเพื่อบรรเทาจากเหตุภัยไซเบอร์ ตลอดระยะเวลา 4 ปีที่ผ่านมาเราพัฒนาอย่างต่อเนื่อง หากแต่ในแต่ละปีสิ่งที่เราเน้นให้ความสำคัญจะมีความแตกต่างไปบ้างตามสถานการณ์ที่เกิดขึ้น อย่างเช่นในปี 2020 ที่ผ่านมานี้ เราได้ให้ความสำคัญกับการสร้างความร่วมมือระหว่างสมาชิกผ่านกิจกรรมต่าง ๆ แม้ว่าจะเจอช่วง

สถานการณ์ COVID-19 ทำให้หลาย ๆ กิจกรรมต้องปรับแผนกันใหม่ก็ตาม แต่ยังคงรักษาความสัมพันธ์ระหว่างเพื่อนสมาชิกไว้มาโดยตลอด นอกจากจะสร้างความสัมพันธ์ภายในสมาชิกแล้วเรายังสร้างความร่วมมือกับหน่วยงานภายนอกสมาชิก อันได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และที่สำคัญอีกหน่วยงานหนึ่งที่ช่วยผลักดันการทำงานด้านไซเบอร์ของประเทศ คือ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) เพื่อร่วมกันส่งเสริมการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ของภาคการเงิน การธนาคาร นอกจากการสร้างความร่วมมือแล้ว หนึ่งในแผนการนดำเนินงานเพื่อสร้างความพร้อมในการรับมือกับภัยไซเบอร์คือ การฝึกซ้อมการรับมือภัยไซเบอร์ (Banking Cyber Drill) ซึ่งมีการซ้อมเป็นประจำทุกปี โดยตลอดระยะเวลาตั้งแต่ต้นปีจนถึงไตรมาสที่ 3 ของปีนี้เราเล็งเห็นว่า ภัยคุกคามทางไซเบอร์นั้นเปลี่ยนแปลงวิถีทางการโจมตีจากทางตรงเป็นการโจมตีทางอ้อม เพราะสถานการณ์ COVID ทำให้ธุรกิจมุ่งเน้นการทำงานออนไลน์มากขึ้นรวมถึงการวางระบบต่าง ๆ ไว้บนคลาวด์ เพื่อให้สามารถเข้าถึงการทำงานจากระยะไกลได้อย่างคล่องตัว และหลาย ๆ ระบบงานไม่เพียงแต่จะเชื่อมโยงกันเองภายในองค์กร แต่ยังเชื่อมโยงไปยังคู่ค้าทางธุรกิจขององค์กรด้วย ทำให้ TB-CERT วิเคราะห์ว่าอาจจะเกิดการโจมตีทางไซเบอร์กับคู่ค้าขององค์กรและส่งผลกระทบไม่ทางตรงก็ทางอ้อมต่อสมาชิกได้ จึงจัดการซ้อมรับมือภัยไซเบอร์ภาคการธนาคารขึ้นภายใต้หัวข้อ "เหตุการณ์ข้อมูลรั่วไหลจากหน่วยงานภายนอกที่เกี่ยวข้องกับการให้บริการของอุตสาหกรรมภาคการธนาคาร (The Banking Service Supply chain is impacted by Cybersecurity breach of 3rd party") ซึ่งก็สอดคล้องกับเหตุการณ์ภัยคุกคามที่เพิ่งเกิดขึ้นกับบริษัท SolarWinds และ FireEye เมื่อต้นเดือนธันวาคม

จากการคาดการณ์อื่น ๆ ของ TB-CERT ได้เล็งเห็นถึงเทคโนโลยีที่ในอนาคตจะมาปรับเปลี่ยนวิธีการทำงานของคนในยุคดิจิทัลนี้ นั่นคือ Artificial Intelligence (AI) ที่ไม่เพียงแต่จะต้องใช้เพื่อทำงานทั่วไปแต่ยังต้องนำมาปรับและคิดวิเคราะห์เพิ่มเติมในมุมของการรับมือกับภัยไซเบอร์ที่เหล่า Hacker อาจจะนำ AI มาใช้ในการโจมตีเราได้เช่นกัน จึงได้จัดงานสัมมนาเกี่ยวกับการนำเทคโนโลยี AI มาปรับใช้ในงานของภาคธุรกิจธนาคารกับภัยไซเบอร์นั้นมีความเกี่ยวข้องกันอย่างไร เพื่อสร้างความตระหนักรู้ให้กับสมาชิกได้นำความรู้ไปประยุกต์ใช้กับองค์กรของตนเองได้

บทความ: สถานการณ์ผันผวนคนปั่นป่วน การเตรียมการกับสิ่งที่เปลี่ยนแปลงตลอดเวลา

ในช่วงปี 2020 มีการเปลี่ยนแปลงทางธุรกิจที่เข้มข้นรวดเร็ว ผนวกกับสถานการณ์ที่ไม่ทันได้เตรียมความพร้อมจากการแพร่ระบาดของโคโรน่าไวรัสสายพันธุ์ใหม่หรือ COVID-19 ทำให้เกิดการเปลี่ยนแปลงด้านการลงทุน สินค้า การให้บริการ กิจกรรมต่าง ๆ รวมไปถึง สภาพชีวิตความเป็นอยู่และการทำงาน ซึ่งทำให้การเตรียมการป้องกันด้านความมั่นคงปลอดภัยของธนาคารสมาชิก ต้องมาปรับลำดับความสำคัญของแนวป้องกันกันใหม่ หลายคนอาจจะเปรียบเทียบสถานการณ์ของการแพร่ระบาดของ COVID-19 ที่เกิดขึ้นอย่างไม่คาดคิดนี้กับปรากฏการณ์ที่เรียกว่า Black Swan หรือ Black Swan Phenomena ซึ่งนาย Nassim Nicholas Taleb ได้เขียนเกี่ยวกับปรากฏการณ์ Black Swan ไว้ในหนังสือชื่อ The Black Swan ว่าหมายถึงเหตุการณ์ที่มีผลกระทบสูงแต่มีโอกาสเกิดขึ้นน้อยมาก ๆ และไม่มีใครคาดคิดว่าจะเกิดขึ้น เหมือนอย่างเช่นความเชื่อที่ว่าหงส์มีสีขาวมีมากว่า 200 ปี จนกระทั่งมาพบหงส์ดำในทวีปออสเตรเลียจึงทำให้ความเชื่อดังกล่าวผิดไปทันที แต่หากมาวิเคราะห์กันให้ดีจะพบว่าในประวัติศาสตร์ของมนุษย์ชาติโรคระบาดไม่ได้เกิดขึ้นครั้งแรก และการระบาดของโคโรน่าไวรัสก็ไม่ได้เกิดขึ้นครั้งแรกเช่นกัน การระบาดของ SARS ในปี 2002 รวมทั้งการระบาดของ MERS ในปี 2012 ล้วนแล้วแต่เป็นโคโรน่าไวรัสทั้งสิ้น แต่เนื่องจากการแพร่ระบาดของ COVID-19 มีการแพร่ระบาดในวงกว้างและที่สำคัญคือสามารถแพร่จากคนสู่คนได้ขณะที่ยังไม่แสดงอาการจึงทำให้มีการพูดถึงมาตรการ ทำงานจากที่บ้าน หรือ Work From Home เพื่อเป็นการลดกิจกรรมที่จะมาพบปะกัน ซึ่งการทำงานทางไกลไม่จำเพาะว่าต้องทำงานจากที่บ้านเท่านั้นมีมานานโข แต่หลายองค์กรยังไม่ได้เริ่มนำมาปฏิบัติอย่างจริงจังจนกระทั่งมีการพูดว่า COVID-19 เป็นผู้ผลักดันการเปลี่ยนแปลงเข้าสู่ยุคดิจิทัล (Digital Transformation) กันเลยทีเดียว การเร่งปรับตัวให้พนักงานทำงานจากที่บ้าน ปรับเปลี่ยนกิจกรรมต่าง ๆ มาเป็นแบบออนไลน์จากสถานการณ์ COVID-19 นั้นก็หมายความว่าสถานการณ์ในปี 200 นั้นแท้จริงแล้วไม่ใช่ปรากฏการณ์ Black Swan เพียงแต่การปรับตัวเข้าสู่ยุคดิจิทัลนั้นไม่อยู่ในลำดับความสำคัญต้น ๆ

ด้วยสถานการณ์ที่บังคับให้เกิดการเปลี่ยนแปลงโดยที่องค์กร บุคลากรในองค์กร หรือผู้ใช้งานอินเทอร์เน็ตยังไม่มีความพร้อม ความเข้าใจในการใช้งานอย่างปลอดภัยก็มักจะมาพร้อมกับโอกาสของผู้ไม่หวังดีที่จะอาศัยช่องว่างของความไม่พร้อมนี้ในการแสวงหาผลประโยชน์ บนโลกไซเบอร์ก็เช่นเดียวกัน ในช่วงการแพร่ระบาดของ COVID-19 พบว่ามีการส่งอีเมลหลอกลวงเพิ่มขึ้นกว่า 600% ทั่วโลก โดยมีเนื้อหาที่เกี่ยวกับ COVID-19 โดยเบี่ยงเบนให้ผู้ที่ได้รับอีเมลมีความอยากรู้อยากติดตามสถานการณ์ สร้างความกังวลหรือเร่งรัดให้ตัดสินใจ โดยมีความมุ่งหมายที่จะหลอกขอข้อมูลส่วนบุคคล

ในด้านของการใช้บริการคลาวด์ในช่วง COVID-19 ในทุกอุตสาหกรรมก็มีปริมาณสูงขึ้นเช่นเดียวกัน เนื่องจากความจำเป็นต้องขยายบริการหรือระบบงานให้รองรับการทำงานออนไลน์ที่เพิ่มสูงขึ้นให้ได้ทัน จากสถิติพบว่าในทุกอุตสาหกรรมมีภัยคุกคามไปที่ระบบคลาวด์เพิ่มขึ้นทั่วโลกอย่างมาก โดยภาคการเงินมีภัยคุกคามไปที่บริการคลาวด์โตขึ้นกว่า 571% ในขณะที่การขนส่งพบว่ามีภัยคุกคามไปที่บริการคลาวด์เพิ่มขึ้นสูงสุดกว่า 1,350% รองลงมาคือภาคการศึกษามีภัยคุกคามเพิ่มขึ้นถึง 1,114% ซึ่งเป็นสิ่งที่สะท้อนถึงพฤติกรรมการใช้งานที่เปลี่ยนแปลงไปในช่วง COVID-19 และโอกาสในการหาประโยชน์ของผู้ไม่หวังดีที่จะโตไปในทิศทางเดียวกัน ในสภาพการณ์เช่นนี้นอกจากองค์กรจะต้องปรับตัวในการสนับสนุนให้พนักงานเปลี่ยนรูปแบบในการทำงานแล้วยังจะต้องให้ความรู้กับพนักงานในการป้องกันตนเองต่อภัยทางไซเบอร์ที่อาจจะสร้างผลกระทบกลับมาที่องค์กรได้

การปรับตัวขององค์กรเพื่อตอบสนองต่อความเปลี่ยนแปลงเพื่อให้การดำเนินธุรกิจมีความต่อเนื่องหรือ Organizational Resilience ที่ทาง TB-CERT ได้เน้นให้กับสมาชิกในปี 2019 นั้นเป็นการปรับเปลี่ยนวัฒนธรรมและกลไกภายในองค์กรที่จะต้องสอดประสานกันเพื่อให้องค์กรมีความสามารถในการตอบสนองต่อผลกระทบที่เกิดขึ้นโดยจะต้องมีการสื่อความและมีความสามารถในการจัดการผลกระทบที่เกิดขึ้นเป็นหัวใจสำคัญ ในปี 2020 นี้จึงตั้ง Theme ในการพัฒนายกระดับความสามารถในการจัดการภัยคุกคามโดยมีเทคนิคการจำกัดผลกระทบหรือ Containment ซึ่งเป็นขั้นตอนสำคัญขั้นตอนหนึ่งในกระบวนการรับมือภัยไซเบอร์

การทำธุรกิจในปัจจุบันมีการเชื่อมโยงระบบและข้อมูลกับหน่วยงานอื่นหรือ Business Supply Chain หากเกิดปัญหาภัยไซเบอร์ในหน่วยงานใดหน่วยงานหนึ่งในห่วงโซ่ จะทำให้เกิดผลกระทบกับบริการได้ยิ่งไปกว่านั้นหากเกิดเหตุการณ์ข้อมูลรั่วไหลโดยเฉพาะข้อมูลส่วนบุคคลก็อาจจะสร้างผลกระทบกับองค์กรอื่นๆ ได้อีกด้วย ในปี 2020 มีการพบเหตุการณ์ข้อมูลรั่วไหลโดยเฉพาะในกลุ่มของบริการซื้อขายออนไลน์ ซึ่งตกเป็นเป้าเนื่องจากมีการใช้งานสูงขึ้นมากจากสถานการณ์ COVID-19 ระบาด ในปี 2020 TB-CERT จึงได้ออกแบบการซักซ้อม Banking Cyber Drill โดยเลือกสถานการณ์จำลองที่เกี่ยวข้องกับการโจมตีของหน่วยงานบุคคลที่ 3 (3rd. Party) และส่งผลกระทบกับภาคการธนาคาร ซึ่งแนวทางการทำ Containment ก็จะมีความซับซ้อนขึ้นเนื่องจากมีปัจจัยที่ไม่สามารถควบคุมความเสี่ยงได้โดยตรงเนื่องจากเป็นระบบของคู่ค้าทางธุรกิจที่เชื่อมต่อกับระบบธนาคาร จากการซักซ้อมหน่วยงานที่เข้าร่วมซ้อมก็จะได้ประเมินความพร้อมขององค์กรตนเองและนำไปเตรียมความพร้อมในสถานการณ์ดังกล่าวซึ่งมีแนวโน้มจะเกิดขึ้นจริง

ก่อนปิดปี มีเหตุการณ์ส่งท้ายปีโดยเกิดเหตุการณ์ Supply Chain Attack ขึ้นจากการที่ Threat Actor[1] ได้ทำการเจาะระบบของบริษัท SolarWinds และฝังมัลแวร์ในซอฟต์แวร์ แล้วอาศัยกลไกการอัปเดตซอฟต์แวร์เพื่อส่งมัลแวร์ไปยังบริษัทลูกค้าของบริษัท SolarWinds โดยบริษัทชั้นนำด้านความปลอดภัยของโลกชื่อบริษัท FireEye ก็ได้รับผลกระทบจาก Supply Chain Attack ในครั้งนี้ด้วยและส่งผลให้ Software ที่ใช้เป็นเครื่องมือในการทำ Red Team หรือเครื่องมือที่ใช้เจาะระบบถูกขโมยออกไปด้วย ซึ่งรูปแบบการโจมตีในลักษณะนี้เป็นรูปแบบที่เคยเกิดขึ้นแล้วใน ประเทศยูเครน เมื่อปี 2017 โดยที่บริษัทพัฒนาซอฟต์แวร์ด้านระบบบัญชีและภาษี MeDoc ซึ่งกว่า 80% ของบริษัทในยูเครนให้ซอฟต์แวร์นี้ โดย Threat Actor ได้เจาะระบบของบริษัท MeDoc Software และแอบฝังมัลแวร์และส่งผ่านการอัปเดตไปยังลูกค้าที่ใช้ซอฟต์แวร์นี้ เช่นเดียวกับ SolarWinds นอกจากนั้นยังมีกรณีศึกษาที่หน่วยงาน NSA-National Security Agency ของรัฐบาลถูกเจาะระบบและข้อมูลช่องโหว่ที่เรียกว่า Ethernal Blue รั่วจากหน่วยงาน NSA เป็นผลให้ถูกนำไปใช้สร้าง Ransomware ที่สร้างผลกระทบไปทั่วโลกนั้นก็คือ Wannacry และ NotPetya ทำให้เราเห็นผลกระทบและความเสี่ยงที่มาในหลากหลายรูปแบบซึ่งเป็นโจทย์ใหญ่ของการป้องกันและการเตรียมการรับมือในช่วงที่จะเปลี่ยนผ่านเข้าสู่ยุคดิจิทัลอย่างเต็มรูปแบบ

ด้วยสภาพเหตุการณ์และเทคนิคการโจมตีที่มีการเปลี่ยนแปลงไป ไม่ว่าจะมีความคล้ายคลึงกับเหตุการณ์ที่เคยเกิดขึ้นหรือจะเป็นวิธีใหม่บนเทคโนโลยีใหม่ที่ภาคการธนาคารนำมาใช้ไม่ว่าจะเป็น Biometric หรือ Artificial Intelligence ก็ตาม การเน้นย้ำถึงความร่วมมือกันระหว่างสมาชิก ความร่วมมือกับภาคอุตสาหกรรมอื่นๆ รวมไปถึงความร่วมมือกับหน่วยงานต่าง ๆ ในต่างประเทศก็จะช่วยบรรเทาหรือช่วยให้มีการเตรียมตัวทั้งสำหรับกลุ่มธนาคาร ลูกค้า คู่ค้าทางธุรกิจ และจะเป็นการปรับเปลี่ยน Life Style ของคนไทยให้มีความมั่นคงปลอดภัยจากภายใน เพื่อสร้างภูมิคุ้มกันภัยไซเบอร์ ภัย COVID-19 หรือภัยในรูปแบบอื่น ๆ ที่จะเกิดขึ้นได้อย่างยั่งยืน

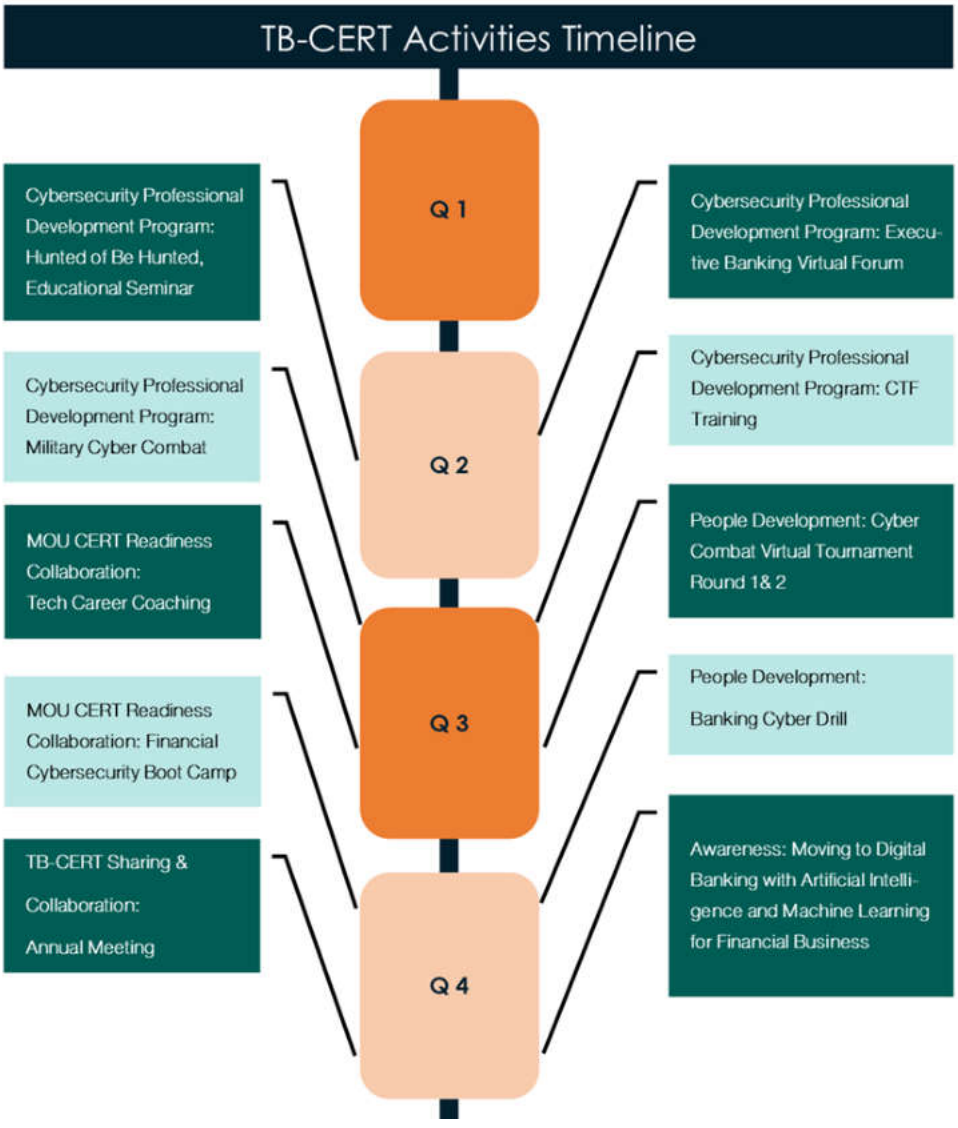
.....Stay Safe.....

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT

[1] มิจฉาชีพไซเบอร์

กิจกรรมในปี 2020

ในปี 2020 TB-CERT ได้พยายามมุ่งเน้นการจัดกิจกรรมเพื่อพัฒนาบุคลากรของหน่วยงานสมาชิก รวมทั้งการยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับหน่วยงานสมาชิก ภายใต้ข้อจำกัดของสถานการณ์โรคระบาดที่ต้องเว้นระยะห่างทำให้หลายกิจกรรมต้องปรับเปลี่ยนรูปแบบเป็นออนไลน์ อย่างไรก็ดี การจัดสัมมนาออนไลน์เป็นการขยายจำนวนผู้เข้าร่วมกิจกรรมให้ออกไปสู่วงกว้างมากขึ้น และยังเป็นการขยายแนวทางการจัดกิจกรรมรูปแบบใหม่โดยที่ยังคงวัตถุประสงค์ของการพัฒนาบุคลากรด้าน Cybersecurity ของภาคการธนาคาร ผ่านการแลกเปลี่ยนความรู้และฝึกฝนทางเทคนิค รวมทั้งการสร้างเครือข่ายระหว่างผู้ปฏิบัติงานด้าน Cybersecurity ของภาคการธนาคารและหน่วยงานที่เกี่ยวข้อง ผ่านกิจกรรมต่าง ๆ ดังนี้



กิจกรรมการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

Executive Banking Virtual Forum

TB-CERT ร่วมกับ FireEye ในการจัดสัมมนาออนไลน์ Executive Banking Virtual Forum โดยผู้เชี่ยวชาญจาก FireEye ได้นำเสนอเกี่ยวกับ Ransomware Trends แนวทางการรับมือ และ Lesson Learned

Hunt or Be Hunted Educational Seminar

TB-CERT ร่วมกับ Group-IB ในการจัดสัมมนาออนไลน์เชิงปฏิบัติการเกี่ยวกับการทำ Threat Hunting ซึ่งผู้เรียนจะได้เรียนรู้วิธีการค้นหาข้อมูลจาก Log ซึ่งเป็นข้อมูลที่บ่งบอกถึงร่องรอยของการใช้งานของบริการ และการเข้าถึงอุปกรณ์ต่าง ๆ โดยจะใช้เครื่องมือเช่น Security Information and Event Management (SIEM) หรืออื่น ๆ เพื่อค้นหาร่องรอยการโจมตี รวบรวมข้อมูลที่เกี่ยวข้องกับเหตุการณ์ผิดปกติ วิเคราะห์พฤติกรรมผิดปกติในระบบ

การเข้าร่วมแข่งขันทักษะทางไซเบอร์ของกองทัพไทย

ตัวแทนทีม TB-CERT จำนวน 2 ทีม ได้มีโอกาสเข้าร่วมกิจกรรมการแข่งขันทักษะทางไซเบอร์ของกองทัพไทย ในวันที่ 6 สิงหาคม เพื่อเป็นการฝึกซ้อมทักษะทางไซเบอร์ร่วมกับผู้เข้าแข่งขันจากภาคส่วนอื่น ๆ ได้แก่ หน่วยงานความมั่นคงของไทยและสหรัฐอเมริกา รวมทั้งสิ้น 30 ทีม

CTF Training

การฝึกอบรม CTF (Capture The Flag) เป็นกิจกรรมที่เชื่อมโยงกับการแข่งขัน Cyber Combat ซึ่งเป็นการอบรมถึงทักษะที่จำเป็นต้องใช้ในการแข่งขันและฝึกคิดวิเคราะห์ในการทำโจทย์ซึ่งแบ่งกลุ่มผู้เรียนออกเป็น 2 กลุ่มคือ Basic และ Intermediate & Advance เพื่อเป็นการเตรียมความพร้อมสำหรับการแข่งขันและที่สำคัญผู้เรียนได้ฝึกฝนทักษะจากการฝึกอบรมแบบเชิงปฏิบัตินี้และนำไปปรับใช้กับการแข่งขันและการทำงานจริงได้

Cyber Combat Virtual Tournament

การแข่งขัน Cyber Combat จัดขึ้นต่อเนื่องเป็นครั้งที่ 3 เพื่อฝึกฝนและพัฒนาทักษะของผู้ปฏิบัติงานด้านการป้องกันภัยไซเบอร์ โดยปีนี้ TB-CERT ร่วมกับ Cisco และ Splunk ในการสนับสนุนระบบการแข่งขัน และมีการปรับรูปแบบเป็นการแข่งขันออนไลน์จำนวน 2 วัน ได้แก่ วันที่ 19 สิงหาคม และ 17 กันยายน 2020 มีผู้เข้าร่วมกิจกรรมรวม 38 ทีม จากหน่วยงานภาคการธนาคาร โทรคมนาคม หน่วยงานความมั่นคง และพลังงาน

Webinar: Moving to Digital Banking with Artificial Intelligence and Machine Learning for Financial Business

TB-CERT ร่วมกับ SAP Thailand จัด Webinar หัวข้อ Moving to Digital Banking with Artificial Intelligence and Machine Learning for Financial Business ว่าด้วยการนำเทคโนโลยี AI มาใช้ใน Digital Banking รวมทั้งมุมมองการนำ AI มาใช้ใน Cybersecurity ในปัจจุบันและอนาคต จากผู้เชี่ยวชาญทั้งจาก SAP Thailand ภาควิชาการและภาคการธนาคาร

การสร้างความร่วมมือเพื่อสร้างความเชื่อมั่นระหว่างหน่วยงานสมาชิก และสร้างเครือข่ายระหว่างผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ภาคการธนาคาร

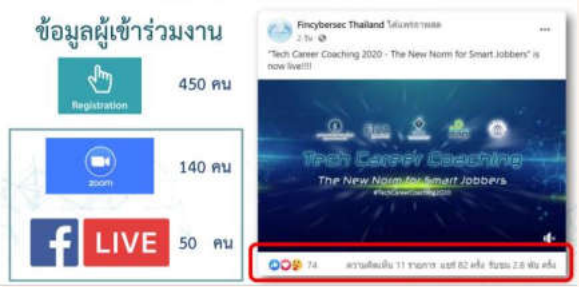
TB-CERT Annual Meeting

นอกจากการจัดประชุมสมาชิกประจำเดือน เพื่อสื่อสารและแลกเปลี่ยนข้อมูลด้านเทคนิคระหว่างกันแล้ว TB-CERT มีการจัดงานประชุมสมาชิกประจำปี ซึ่งเป็นกิจกรรมกลุ่มสัมพันธ์เชิงวิชาการด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นการระดมสมองและวางแผนงานประจำปีของ TB-CERT การแชร์ความรู้ทางเทคนิค ให้สมาชิกได้มีโอกาสพบปะ สร้างเครือข่ายระหว่างผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยไซเบอร์ และเสริมสร้างความร่วมมือกับหน่วยงานกำกับดูแล ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ธนาคารแห่งประเทศไทย โดยจัดขึ้นเมื่อวันที่ 14 ธันวาคม 2020

งานความร่วมมือกับหน่วยงานภายใต้บันทึกความร่วมมือข้อตกลงด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย ด้านการสร้างบุคลากรรุ่นใหม่ (New Hire) และโอกาสทำงานในภาคการเงิน

Tech Career Coaching

โครงการ Tech Career Coaching ในปี 2020 จัดขึ้นเป็นครั้งที่ 2 โดยร่วมกับฝ่ายบุคลากรของหน่วยงานภายใต้การกำกับดูแลในภาคการเงิน ในปีนี้ได้ปรับรูปแบบเป็นออนไลน์ โดยยังคงเนื้อหาหลักในการให้ความรู้ด้านเทคโนโลยีสารสนเทศ การทำงานในสายอาชีพดังกล่าวโดยเฉพาะในภาคการเงิน อีกทั้งเพื่อให้องค์กรภาคการเงินได้มีโอกาสให้ข้อมูลด้านวิชาชีพ การฝึกงาน และทุนการศึกษาด้าน IT และเป็นการสร้างเครือข่ายระหว่างฝ่ายบุคลากรขององค์กรภาคการเงินในการสร้างบุคลากรใหม่ด้าน IT เข้าสู่ภาคการเงินร่วมกัน ผ่านเวทีเสวนาและการให้คำปรึกษาจากองค์กรภาคการเงินผ่านระบบห้องประชุมออนไลน์ และกว่า 30% ของผู้เข้าร่วมกิจกรรมได้เข้าสู่กระบวนการรับสมัครงานและฝึกงานของสถาบันการเงิน



Financial Cybersecurity Boot Camp #4

โครงการ Financial Cybersecurity Boot Camp ครั้งที่ 4 มีวัตถุประสงค์เพื่อเพิ่มโอกาสในการพัฒนาทักษะด้าน Cybersecurity และเป็นการสร้างเครือข่ายบุคลากรรุ่นใหม่ที่มีความสนใจงานด้าน Cybersecurity ในภาคการเงิน รวมทั้งฝึกทักษะผ่านการแข่งขันทั้งในด้านการโจมตีและป้องกันระบบ ปีนี้มีการปรับรูปแบบเป็นกิจกรรมออนไลน์ 2 วัน มีผู้สมัครเข้าร่วมโครงการจำนวน 104 ทีม ส่วนใหญ่กำลังศึกษาระดับปริญญาตรีชั้นปีที่ 3 และปีที่ 4 และคัดเลือกเข้าสู่กิจกรรมรอบชิงชนะเลิศ ณ ศูนย์การเรียนรู้ ธปท.จำนวน 10 ทีม ทั้งหมด 30 คน

Cybersecurity Proficiency Development Program

จากผลสำรวจความต้องการบุคลากรทางด้าน Cybersecurity ของภาคการธนาคาร พบว่าภาคการธนาคารมีความต้องการบุคลากรในด้าน Cybersecurity เป็นจำนวนมาก อ้างอิงจากการสำรวจความต้องการบุคลากรด้าน IT และ Cybersecurity จากธนาคารสมาชิก TB-CERT จำนวน 22 ธนาคาร พบว่าอัตราความต้องการบุคลากรเทียบกับที่มีในปัจจุบันเพิ่มขึ้นคิดเป็น 12% โดยได้แบ่งหมวดหมู่ของกลุ่มฟังก์ชันงานตาม NIST Special Publication 800-181 เป็น 7 ประเภท และผลสำรวจ 3 ลำดับแรกที่มีความต้องการมากที่สุด ได้แก่ (1) ฟังก์ชันงานเกี่ยวกับการพัฒนาและออกแบบระบบ Securely Provision (SP) 26% (2) ฟังก์ชันงานเกี่ยวกับการรับมือภัยคุกคาม Protect and Defend (PR) 23% และ (3) ฟังก์ชันงานเกี่ยวกับการเก็บข้อมูลหลักฐาน Collect and Operate (OC) 18% ตามลำดับ[2] ในขณะที่ภัยคุกคามและการโจมตีทางไซเบอร์ยังคงเพิ่มขึ้นอย่างต่อเนื่อง ดังนั้นความต้องการมืออาชีพในการปกป้องข้อมูลและทรัพย์สินดิจิทัลอื่น ๆ สำหรับภาคการธนาคารยังคงเติบโตต่อเนื่องเช่นกัน นอกจากนี้หลักสูตรการเรียนการสอนในมหาวิทยาลัยยังขาดการพัฒนาทักษะด้านไซเบอร์ที่ทำให้ผู้เรียนสามารถเข้าใจและปฏิบัติงานได้จริงตามที่ทางภาคการธนาคารต้องการ ดังนั้น TB-CERT เล็งเห็นความสำคัญทางด้านการพัฒนาบุคลากรทั้งที่ทำงานแล้วและจบใหม่ ให้มีความรู้ความสามารถและมีทักษะความเชี่ยวชาญตรงกับสายงานที่รับผิดชอบ มุ่งเน้นพัฒนาบุคลากรทางด้าน Cybersecurity ให้มีศักยภาพและสามารถทำงานได้ตรงตามสายอาชีพตามความต้องการของตลาดในปัจจุบันและอนาคต

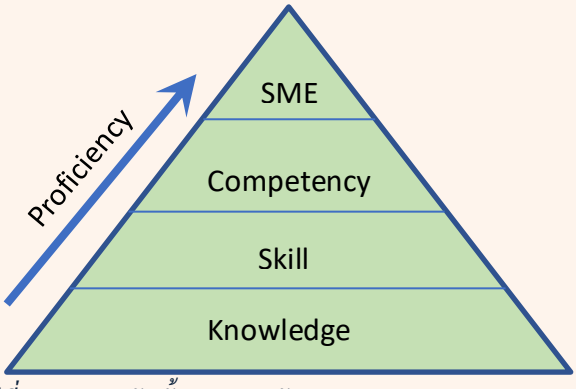
ในปี 2020 TB-CERT ได้วางแผนจัดทำโครงการเพื่อพัฒนาหลักสูตรการเรียนรู้ด้าน Cybersecurity แบบออนไลน์ เรียกว่า Cyber Brain ซึ่งเป็นโครงการที่จัดทำหลักสูตรที่ออกแบบมาให้มีการเรียนการสอนเชิงทฤษฎีและเชิงปฏิบัติเพื่อใช้ฝึกฝนทักษะที่ได้เรียนรู้และผ่านประสบการณ์มา หลักสูตรจะออกแบบให้สมาชิก TB-CERT ได้มีความรู้และทักษะด้าน Cybersecurity เฉพาะด้านและมีการวัดผลเป็นรายบุคคล โครงการ Cyber Brain จะช่วยตอบโจทย์ภายใต้ภารกิจหลักของ TB-CERT และ Mission ที่เราได้กำหนดไว้ คือ TB-CERT จะเป็นศูนย์รวมของกลุ่ม Professional ด้าน Cybersecurity โดยมีวัตถุประสงค์หลักของการจัดทำหลักสูตรโครงการ Cyber Brain ดังต่อไปนี้

- เพื่อเสริมสร้างทักษะและความรู้ด้าน Cybersecurity ให้แก่บุคลากรของหน่วยงานสมาชิก ผ่านระบบ E-learning Platform ตอบโจทย์การทำงานแบบ Work From Home ตามสถานการณ์โลกในปัจจุบัน
- เพื่อพัฒนาหลักสูตรการเรียนด้าน Cybersecurity ให้แก่บุคลากรของหน่วยงาน ตามมาตรฐานสากล
- เพื่อจัดให้มีระบบการเรียนรู้ทางภาคทฤษฎีควบคู่กับการฝึกภาคปฏิบัติ เน้นทักษะประสบการณ์ในโลกแห่งความเป็นจริง
- เพื่อแนะแนวสายอาชีพ Cybersecurity และให้คำปรึกษาการเรียนรู้ตามบทบาทของผู้เรียนที่นำไปใช้สำหรับทำงานจริง

[2] TB-CERT Annual Report 2019 หน้า 11

ลำดับขั้นของการพัฒนาความสามารถ (Proficiency) ในกระบวนการเรียนรู้สามารถแบ่งได้เป็น 4 ระดับ (รูปที่ 1) คือ

1. Knowledge หมายถึงการสร้างองค์ความรู้เพื่อให้เกิดความรู้ความเข้าใจซึ่งถือเป็นขั้นเบื้องต้นของการพัฒนาความสามารถ
2. Skill หมายถึงการนำความรู้ไปฝึกปฏิบัติอย่างต่อเนื่องเพื่อให้เกิดความเข้าใจเชิงลึกขององค์ความรู้และการนำไปปฏิบัติจนเกิดความชำนาญในการใช้งานองค์ความรู้
3. Competency หมายถึงการประยุกต์ทักษะความชำนาญเพื่อนำไปสู่ความสำเร็จตามเป้าหมายที่วางไว้ ซึ่งมักจะต้องอาศัย Soft Skill ด้วยเป็นองค์ประกอบที่สำคัญ
4. SME (Subject Matter Expert) เป็นความชำนิชำนาญในการประยุกต์ ความรู้ ความเข้าใจ และทักษะในเฉพาะด้าน



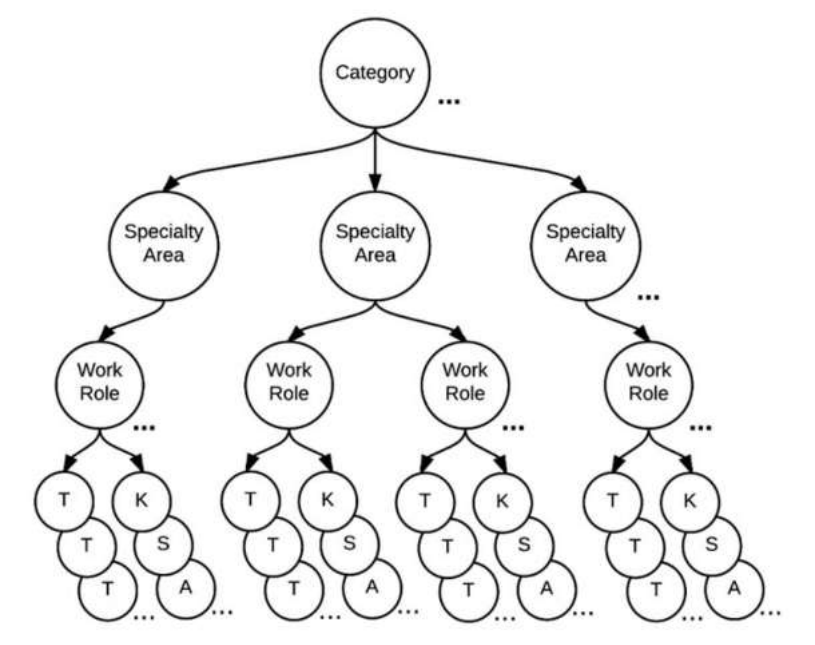
รูปที่ 1 แสดงลำดับขั้นของการพัฒนาความสามารถ (Proficiency)

ทั้งนี้ TB-CERT ได้ศึกษาแนวทางการทำหลักสูตรของโครงการ Cybersecurity Proficiency Development Program จากเอกสาร National Initiative for Cybersecurity Education (NICE) Framework ของสถาบัน National Institute of Standards and Technology (NIST 800-181 Rev1) ที่ใช้เป็นกรอบการพัฒนาความรู้และความสามารถของบุคลากรด้าน Cybersecurity และเป็นพื้นฐานในการกำหนดความรู้ ทักษะความเชี่ยวชาญ และความสามารถของบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ที่จำเป็นต้องมีในแต่ละบทบาทหน้าที่การปฏิบัติงานต่าง ๆ

กรอบกำหนดของ NICE Framework ถือเป็นข้อมูลอ้างอิงพื้นฐานสำหรับการอธิบายบทบาทหน้าที่ความรับผิดชอบที่เกี่ยวข้องกับงานด้านความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงการให้ข้อมูลความสัมพันธ์ระหว่างองค์ความรู้ ทักษะ และความสามารถทางด้านต่าง ๆ ที่จำเป็นกับบทบาทหน้าที่ในสายงานความมั่นคงปลอดภัยไซเบอร์ ตามรูปที่ 2 โครงสร้างการกำหนดองค์ประกอบตาม NICE Framework ประกอบด้วย Category, Specialty Area, Work Role, KSA และ T ซึ่งอธิบายความหมายได้ตามนี้

- **หมวดหมู่ หรือ Category** อธิบายถึงกลุ่มฟังก์ชันงานทางด้านต่าง ๆ ที่เกี่ยวกับสายอาชีพความมั่นคงปลอดภัยทางไซเบอร์ โดยสามารถจัดกลุ่มฟังก์ชันงานได้ทั้งหมด 7 ประเภท ซึ่งจะอธิบายในลำดับถัดไป

- **ความชำนาญเฉพาะทาง หรือ Specialty Area** จากการจัดแบ่งประเภทของกลุ่มฟังก์ชันงานด้านความมั่นคงปลอดภัยทางไซเบอร์ออกเป็น 7 ประเภท ในกลุ่มฟังก์ชันงานแต่ละประเภทจะประกอบด้วยความชำนาญเฉพาะทางด้านต่าง ๆ ที่แตกต่างกันตามแต่ละประเภทของกลุ่มงาน จากเอกสาร National Cybersecurity Workforce Framework (NICE Framework) ระบุความชำนาญเฉพาะทางทั้งหมด 33 ด้าน ซึ่งจากความชำนาญเฉพาะทางแต่ละด้านจะสัมพันธ์กันกับหน้าที่ความรับผิดชอบของบทบาทต่าง ๆ ทางด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการเชื่อมโยงระหว่างความชำนาญเฉพาะทางกับการพัฒนาความรู้ ฝึกฝนทักษะ และรวบรวมความสามารถการทำงานที่เกี่ยวข้องกับความเชี่ยวชาญเฉพาะทางนั้น ๆ รวมเรียกว่า KSA (Knowledge, Skills and Abilities)
- **บทบาทการปฏิบัติงาน หรือ Work Role** อธิบายถึงบทบาทหน้าที่ในการปฏิบัติงานตามสายงานความมั่นคงปลอดภัยทางไซเบอร์ โดยแสดงรายละเอียดคุณลักษณะสำคัญที่เกี่ยวข้องกับการทำงานภายใต้บทบาทนั้น ๆ ในรูปแบบของความรู้ ทักษะ ความสามารถในการดำเนินงานและงานที่ต้องดำเนินการในบทบาทนั้น โดยทั่วไปแต่ละองค์กรจะระบุตำแหน่งงาน และตามด้วยการเลือกบทบาทการปฏิบัติงานอย่างน้อยหนึ่งบทบาทที่เกี่ยวข้องกับตำแหน่งงานนั้น
- **ความรู้ ทักษะ และความสามารถ ที่เกี่ยวข้อง หรือ KSA** ความรู้ ทักษะและความสามารถ (KSA) คือคุณลักษณะสำคัญที่จำเป็นในการปฏิบัติงานตามบทบาทหน้าที่ต่าง ๆ
- **งานที่ต้องดำเนินการ หรือ Task (T)** คือรายละเอียดชิ้นงานที่ต้องดำเนินการตามที่กำหนดไว้ตามแต่ละบทบาทการปฏิบัติงาน



รูปที่ 2 แสดงความสัมพันธ์ขององค์ประกอบ NICE Framework

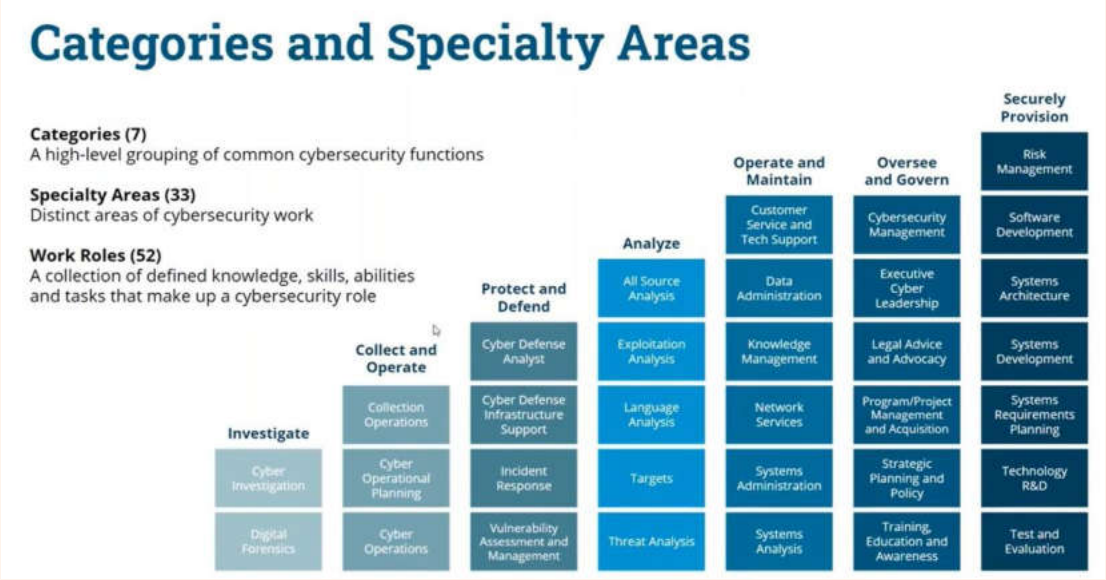
(ที่มา https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf)

การนำ NICE Framework มาเป็นต้นแบบในการออกแบบหลักสูตรการเรียนออนไลน์ เพื่อทำความเข้าใจความต้องการขององค์กร สามารถช่วยองค์กรในการวางแผนการพัฒนาบุคลากรและติดตามผลของการพัฒนาบุคลากรทางด้านความมั่นคงเปลอดภัยทางไซเบอร์ นอกจากนี้ด้วยการกำหนด KSA และ Tasks ช่วยให้ผู้เรียนสามารถเรียนรู้ ฝึกฝนทักษะและความสามารถที่เกี่ยวข้องกับบทบาทหน้าที่ในการปฏิบัติงานจริง เป็นส่วนสำคัญในการเตรียมความพร้อมและให้ความรู้แก่บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์อย่างมีประสิทธิภาพ

ทั้งนี้ NICE Framework ได้จัดประเภทฟังก์ชันงานด้านความมั่นคงปลอดภัย (Category) ออกเป็น 7 ประเภท ประกอบด้วยกลุ่มฟังก์ชันงานดังต่อไปนี้

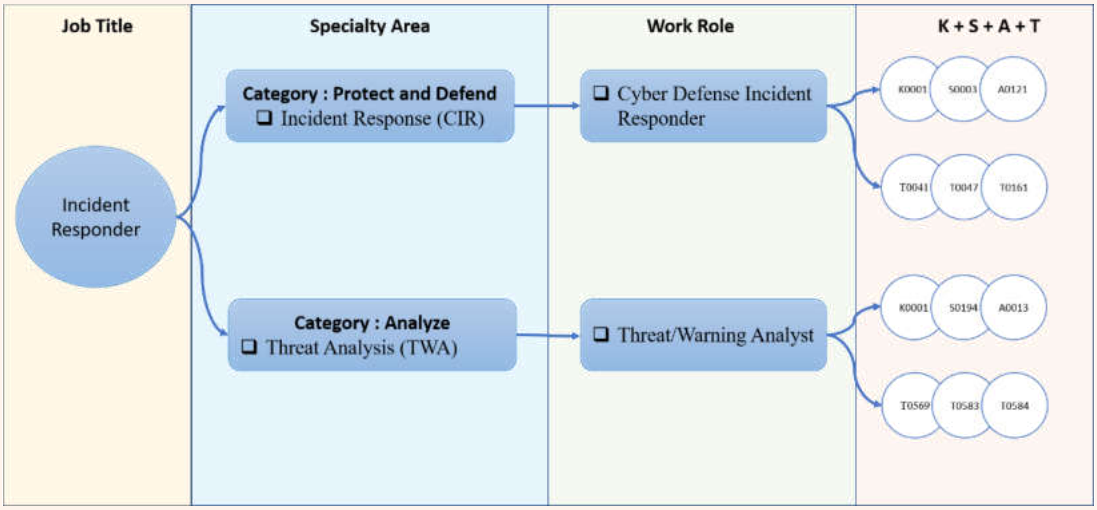
 Securely Provision	1. **SECURELY PROVISION** คือกลุ่มฟังก์ชันงานเกี่ยวกับการกำหนดแนวคิด การออกแบบ และการจัดสร้างพัฒนาระบบความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
 Operate and Maintain	2. **OPERATE AND MAINTAIN** คือกลุ่มฟังก์ชันงานด้านการบริหารจัดการระบบ การดูแลระบบ และการบำรุงรักษาระบบเทคโนโลยีสารสนเทศเพื่อให้การทำงานเป็นไปอย่างมีประสิทธิภาพและมีความปลอดภัย
 Protect and Defend	3. **PROTECT AND DEFEND** คือกลุ่มฟังก์ชันงานเกี่ยวกับการป้องกันและรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อข้อมูลและระบบเทคโนโลยีสารสนเทศ
 Analyse	4. **ANALYZE** คือกลุ่มฟังก์ชันงานด้านการระบุ วิเคราะห์ ตรวจสอบ และประเมินผลกระทบที่เกิดขึ้นจากเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์
 Collect and Operate	5. **COLLECT AND OPERATE** คือกลุ่มฟังก์ชันงานด้านการวิเคราะห์การทำงานที่ผิดปกติ และการเก็บรวบรวมข้อมูลที่เกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อเป็นข้อมูลสำคัญในการพัฒนาระบบ Threat Intelligent
 Investigate	6. **INVESTIGATE** คือกลุ่มฟังก์ชันงานด้านการตรวจสอบเหตุการณ์ความปลอดภัยทางไซเบอร์หรืออาชญากรรมที่เกี่ยวข้องกับข้อมูลระบบเทคโนโลยีสารสนเทศ
 Oversee and Govern	7. **OVERSEE AND GOVERN** คือกลุ่มฟังก์ชันงานด้านการบริหาร กำหนดทิศทาง การพัฒนา และการสนับสนุนเพื่อให้องค์กรสามารถดำเนินงานด้านความปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ภายใต้ Categories ทั้ง 7 ด้าน NICE Framework มีการกำหนด Work Role ไว้ทั้งหมด 52 work roles ภายใต้ 33 Specialty Areas โดย Work Role จะเป็นจุดเริ่มต้นที่สำคัญในการนำ NICE Framework ไปใช้ แม้ว่าโครงสร้างองค์กร ตำแหน่งงานของแต่ละองค์กรจะแตกต่างกัน แต่การนำ 52 work roles นี้ไปเชื่อมโยงเข้ากับบทบาทหน้าที่ความรับผิดชอบที่องค์กรได้กำหนดไว้สำหรับบุคลากรที่ทำงานเกี่ยวข้องกับความมั่นคงปลอดภัยตั้งแต่ระดับบริหารลงมาจนถึงระดับปฏิบัติการ



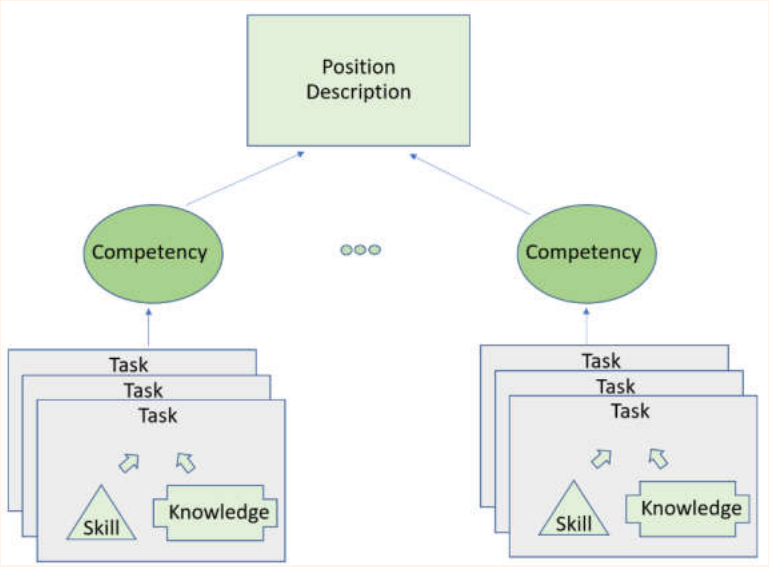
รูปที่ 3 แสดงโครงสร้างและความสัมพันธ์ของ Categories, Specialty Areas

จากโครงสร้างข้อมูลของ NICE Framework ที่ได้กล่าวมาข้างต้น สามารถนำมาประยุกต์ใช้ในการออกแบบหลักสูตรเพื่อพัฒนาบุคลากรและเป็นแนวทางการวางแผนเส้นทางความก้าวหน้าในสายอาชีพ Cybersecurity ต่อไป ในที่นี้ขอยกตัวอย่างตำแหน่งงาน เจ้าหน้าที่รับมือภัยคุกคาม หรือ Incident Responder เพื่อให้เห็นภาพชัดเจนขึ้น ตามรูปที่ 4 ตำแหน่ง Incident Responder ซึ่งเป็นตำแหน่งงานที่สำคัญในการจัดการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ และเป็นอีกบทบาทหน้าที่ที่จำเป็นต้องมีสำหรับการรับมือภัยไซเบอร์ โดยมีบทบาทหน้าที่ (Work Role) ซึ่ง NICE ได้กำหนด Work Role ดังกล่าวไว้ภายใต้ Specialty Area คือ Incident Responder (CIR) และ Threat Analysis (TWA) ตามลำดับ โดย NICE ได้ทำการเชื่อมโยงกับชุดข้อมูลทักษะความรู้ความสามารถ (KSA) พร้อมทั้งรายละเอียดงาน (Task) สำหรับ Specialty Area ทั้งสองเอาไว้แล้ว เพื่อให้สามารถนำไปวางแผนพัฒนาบุคลากรตามความต้องการซึ่งจะแตกต่างกันไปตามโครงสร้างและบทบาทหน้าที่ของแต่ละองค์กร



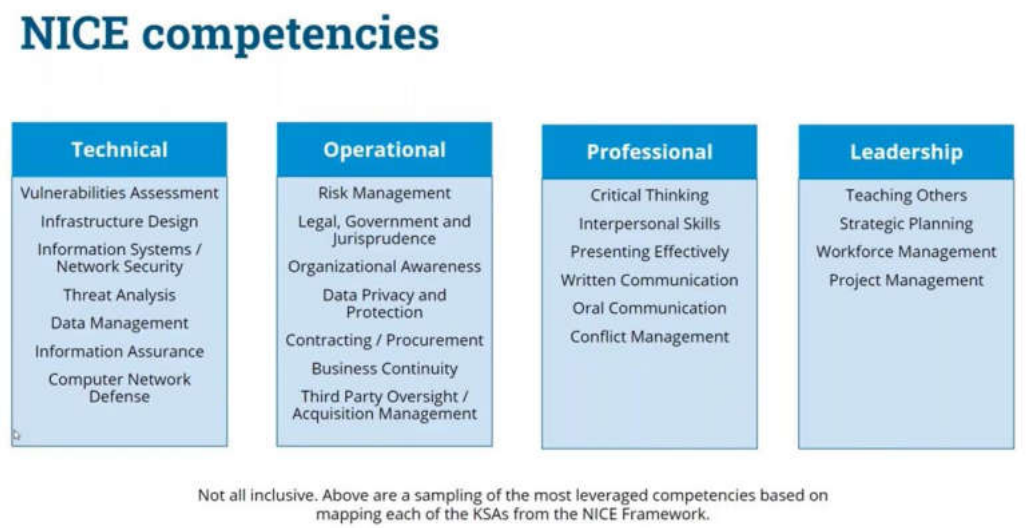
รูปที่ 4 ตัวอย่างตำแหน่งงาน Incident Responder และบทบาทหน้าที่ปฏิบัติงาน

อย่างไรก็ตามในปีที่แล้ว NICE Framework ได้มีการอัปเดตเป็น Revision 1 เพื่อให้ Framework มีความง่ายขึ้น โดยจะเน้นไปที่ Knowledge และ Skill ซึ่งจะนำไปใช้ในการกำหนดเนื้อหาการพัฒนาความรู้ความสามารถ ในขณะเดียวกันก็จะเชื่อมโยงKnowledge และ Skill ไปที่ Task ซึ่งเป็นสิ่งที่หน่วยงานสามารถนำไปผูกกับ Position Description ได้ ทั้งนี้ใน Revision 1 นี้ได้มีการนำเอา Competency เข้ามาเพื่อใช้ในการช่วยในการประเมินความพร้อมในการทำหน้าที่ตาม Task งาน หรือ Work Role ที่ได้รับเมื่อเทียบกับ Position Description ที่องค์กรกำหนดไว้ ตามรูปที่ 5

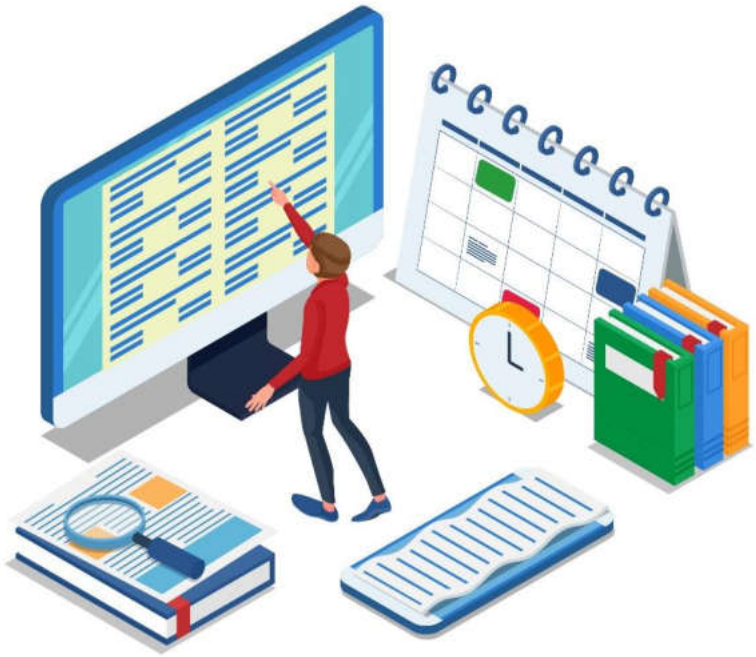


รูปที่ 5 แสดงการนำเอา Competency มาเพื่อให้องค์กรสามารถนำไปเชื่อมโยง กับ Position Description ได้ง่ายขึ้น

นอกจากนั้นได้มีการกำหนด Competency ไว้เป็นแนวทางใน Revision 1 เพื่อให้สามารถนำไปปรับใช้ในการวางแผนพัฒนาบุคลากรให้ได้เหมาะสมกับสภาพการเปลี่ยนแปลงของความรู้ความสามารถและการพัฒนาของเทคโนโลยีและภัยคุกคามได้มีประสิทธิภาพมากยิ่งขึ้น



รูปที่ 6 แสดงสรุป Competencies ในด้านต่างๆ ใน NICE Framework Revision 1



งานด้านการรับมือภัยคุกคามไซเบอร์

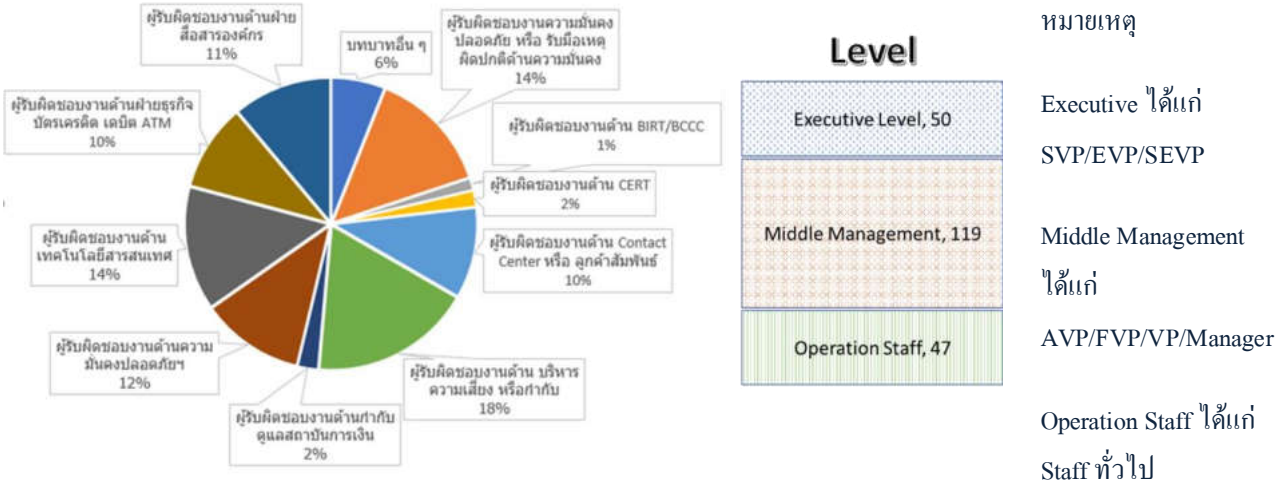
Banking Cyber Drill

เนื่องด้วยสถานการณ์ COVID-19 ทำให้การซ้อมรับมือภัยคุกคามทางไซเบอร์ในปีนี้ปรับรูปแบบมาเป็นการซ้อม Table Top Exercise แบบ Online ผ่าน Microsoft Teams ซึ่งเป็นการจำลองสถานการณ์ภัยคุกคามให้ผู้เข้าร่วมซ้อมได้วิเคราะห์และอธิบายแนวทางการดำเนินการตอบสนองต่อเหตุการณ์จำลองนั้น รวมถึงได้ตัดสินใจเลือกหัวข้อการตอบสนองต่อภัยคุกคามทางไซเบอร์ในบทบาทการทำงานจริงของตนเอง ตามสถานการณ์ที่ดำเนินไปในแต่ละช่วงเวลา ซึ่งเป็นการปลดล็อคข้อจำกัดที่เกี่ยวกับจำนวนผู้เข้าร่วมซ้อมและจะต้องร่วมซ้อมแบบ role play ซึ่งอาจจะมีการตัดสินใจหรือการสื่อความที่ไม่สมจริงเท่าที่ควร อย่างไรก็ตามทางทีมงานตระหนักดีว่าการขยายจำนวนผู้เข้าร่วมซ้อม จะมีผู้ที่ยังไม่คุ้นเคยการซักซ้อมในลักษณะนี้ จึงเสริมกลไกการเรียนรู้ถึงสถานการณ์และทางเลือกเพื่อให้เกิดการเรียนรู้และเข้าใจต่อสถานการณ์ภัยคุกคามทางไซเบอร์ ซึ่งถือเป็นจุดประสงค์สำคัญของการซ้อมในครั้งนี้ด้วย หัวข้อในการซักซ้อมครั้งนี้คือ "เหตุการณ์ข้อมูลรั่วไหลจากหน่วยงานภายนอกที่เกี่ยวข้องกับการให้บริการของอุตสาหกรรมภาคการธนาคาร (The Banking Service Supply chain is impacted by Cybersecurity breach of 3rd party") มีวัตถุประสงค์หลักคือต้องการให้ผู้เข้าร่วมได้ทราบถึงวิธีการรับมือกับภัยไซเบอร์ตามสถานการณ์จำลองที่ตั้งไว้ ได้ฝึกปฏิบัติคิดวิเคราะห์กรณีที่ต้องควบคุมผลกระทบที่เกิดขึ้นต่อเหตุการณ์ที่ซักซ้อมไม่ให้ขยายผลกระทบออกไปในวงกว้าง (containment) และนำไปปรับใช้หรือปรับปรุงพัฒนาแผนรับมือภัยคุกคามไซเบอร์ของหน่วยงานตนเอง รวมถึงเข้าใจบทบาทของผู้อื่นทั้งภายในและภายนอกของตนเอง

การซ้อมในวันที่ 17 พฤศจิกายน 2020 ที่ผ่านมา มีผู้เข้าร่วมงานทั้งสิ้น 216 คน มาจากหน่วยงานสมาชิกของ TB-CERT 26 หน่วยงาน หน่วยงานกำกับดูแลสถาบันการเงิน และคณะ Crisis Management Team ของ Banking Sector (BIRT, BCCC)[1]

[1]BIRT ย่อมาจาก Banking Incident Response Team, BCCC ย่อมาจาก Banking Crisis Command Center

ผู้เข้าร่วมซักซ้อมแบ่งตามบทบาทต่าง ๆ จำนวน 11 บทบาท และมีการแบ่งระดับตำแหน่งงานของผู้เข้าร่วมซ้อมออกเป็น 3 ระดับ ได้แก่ ระดับ Executive, Middle Management และ Operation Staff ตามรายละเอียดในรูปที่ 7



หมายเหตุ

Executive ได้แก่ SVP/EVP/SEVP

Middle Management ได้แก่ AVP/FVP/VP/Manager

Operation Staff ได้แก่ Staff ทั่วไป

รูปที่ 7 จำนวนผู้เข้าร่วมซักซ้อมแบ่งตามบทบาทและระดับตำแหน่งงาน

จากการสำรวจพบว่า ผู้ที่เข้าร่วมซ้อมรับมือภัยคุกคามทางไซเบอร์ส่วนใหญ่มีส่วนร่วมกับการตัดสินใจในการรับมือกับภัยไซเบอร์และพัฒนาแผนการรับมือกับภัยไซเบอร์ขององค์กร ตามรายละเอียดดังรูปที่ 8

ร้อยละของผู้เข้าร่วมซ้อมที่มีส่วนในการตัดสินใจต่อสถานการณ์ไซเบอร์

ร้อยละของผู้เข้าร่วมซ้อมที่มีส่วนร่วมในการพัฒนาแผนการรับมือภัยไซเบอร์

รูปที่ 8 แสดงผลร้อยละของผู้เข้าร่วมซ้อมถึงการมีส่วนร่วมในการตัดสินใจและพัฒนาแผนการรับมือกับภัยไซเบอร์

ผู้เข้าร่วมส่วนใหญ่มีความเห็นว่า การจัดกิจกรรมครั้งนี้ให้ประโยชน์แก่ผู้เข้าร่วมซ้อมเป็นอย่างดี ทั้งการนำไปประยุกต์ใช้และการเตรียมการที่เป็นรูปแบบมากขึ้น รวมทั้งเห็นภาพกระบวนการรับมือภัยไซเบอร์ได้อย่างชัดเจนและเห็นได้ชัดคือ การตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์มีความคิดไปในทิศทางเดียวกันอย่างมีประสิทธิภาพ

ในบทบาทหน้าที่ของผู้เข้าร่วมซ้อม ผู้เข้าร่วมซ้อมมีความเข้าใจหน้าที่ที่รับผิดชอบและบทบาทของตนเองเมื่อต้องรับมือกับภัยไซเบอร์ซึ่งถือเป็นเรื่องสำคัญในช่วงของการเผชิญเหตุ นอกจากนั้นธนาคารให้ความสำคัญในการติดต่อสื่อสาร ตามข่าวสาร รวมถึงแชร์ข้อมูล ระหว่างธนาคารสมาชิกและ TB-CERT

จากการประเมินความพร้อมพบว่า องค์กรส่วนใหญ่มีความพร้อมในการรับมือกับภัยไซเบอร์ได้ในหลาย ๆ ด้าน มีการจัดเตรียมแผนเพื่อใช้ประกอบการซักซ้อม อย่างไรก็ตามพบว่า ธนาคารสมาชิกและผู้เข้าร่วมซ้อมยังต้องมีการพัฒนาแนวทางการประสานงานภายในองค์กรให้มากยิ่งขึ้นโดยเฉพาะหน่วยงาน IT กับ Business Unit เพื่อให้เห็นภาพของสถานการณ์ที่เกิดขึ้นและสามารถประเมินผลกระทบทางการเงินได้อย่างมีประสิทธิภาพ ซึ่งจะเห็นได้ว่าภัยไซเบอร์ไม่ใช่หน้าที่ความรับผิดชอบของ IT ฝ่ายเดียวแต่ทุกหน่วยงานมีส่วนร่วมในการรับผิดชอบเพื่อประเมินและตอบสนองสถานการณ์ร่วมกันในบทบาทของตนเอง สมาคมธนาคารไทยจะต้องปรับปรุงกระบวนการสื่อสารทั้งภายในและภายนอกหน่วยงานให้เห็นเป็นรูปธรรมมากขึ้น รวมทั้งการสร้างกลไก การรายงานสถานการณ์ต่าง ๆ ผลกระทบที่เกิดขึ้น รวมถึงการสื่อความสู่สาธารณะ ทั้งนี้ เล็งเห็นว่าหน่วยงานสมาชิกมีการสื่อสารมายัง TB-CERT เพื่อขอคำแนะนำและแจ้งเตือนธนาคารสมาชิกอื่น ๆ เพื่อเป็นการลดความเสี่ยงต่อภาพรวมของอุตสาหกรรมธนาคารมากขึ้นกว่าทุกปีที่ผ่านมา อีกประเด็นที่สำคัญของการซักซ้อมในครั้งนี้เป็นสถานกการณ์ทางไซเบอร์ที่ไม่ได้เกิดขึ้นในหน่วยงานสมาชิกแต่เกิดขึ้นที่หน่วยงานภายนอกหรือ 3rd party ซึ่งถือว่าเป็นสถานการณ์ในรูปแบบที่ยังไม่คุ้นชินในการจัดการ รวมถึงการต้องตอบสนองต่อสถานการณ์ที่เหตุการณ์นั้นไม่ได้มีผลกระทบโดยตรงต่อระบบของธนาคารจึงทำให้หน่วยงานสมาชิกTB-CERT รวมถึงธนาคารแห่งประเทศไทยได้คิดวิเคราะห์และประเมินถึงสิ่งที่จะต้องดำเนินการและนำไปปรับปรุงแผนการรับมือกับภัยไซเบอร์ของตนเอง รวมถึง TB-CERT เองก็ยังต้องปรับกระบวนการรับแจ้งเหตุและวิเคราะห์เหตุการณ์ให้กับสมาชิก TB-CERT เช่นกัน

ภาพบรรยากาศการซักซ้อมรับมือภัยไซเบอร์

ขอขอบคุณภาพบางส่วนจากผู้เข้าร่วมกิจกรรม

งานด้าน API Standard

ในยุคดิจิทัล 4.0 หรือเรียกว่ายุค Machine-to-Machine เป็นยุคที่เทคโนโลยีเข้ามามีบทบาทในชีวิตประจำวันของเราอย่างมาก เป็นยุคที่อุปกรณ์ต่าง ๆ สามารถสื่อสารและทำงานกันเองได้อย่างอัตโนมัติ เช่น เราสามารถเปิด-ปิด หรือสั่งงานกับเครื่องใช้ไฟฟ้าผ่านแอปพลิเคชันได้โดยไม่ต้องเดินไปกดสวิตช์ เป็นต้น ทำให้มีการรับส่งข้อมูลกันอย่างแพร่หลายและกว้างขวาง ดังนั้นคงปฏิเสธไม่ได้ว่าทุกวันนี้ข้อมูลเข้ามามีบทบาทสำคัญในการทำงานและในชีวิตประจำวันของทุกคนเป็นอย่างมาก และ API (Application Programming Interface) นั้นถือเป็นเบื้องหลังที่สำคัญอย่างหนึ่งในการทำให้การนำข้อมูลมาใช้งานนั้นเกิดขึ้นอย่างมากมาย กล่าวคือ API คือช่องทางการเชื่อมต่อระหว่างระบบหนึ่งไปยังอีกระบบหนึ่ง โดยอาจเป็นการเชื่อมต่อระหว่างผู้ใช้งานกับระบบ หรือจากระบบเชื่อมต่อไปหาอีกระบบหนึ่ง เพื่อให้แอปพลิเคชันสามารถเข้าถึงและเปลี่ยนแปลงข้อมูลบนระบบต่าง ๆ ได้ ในบทความนี้จะกล่าวถึงหลักเกณฑ์ที่ควรพิจารณาในการพัฒนา API ให้มีความปลอดภัยและการจัดอันดับ 10 ช่องโหว่ที่เกิดขึ้นเกี่ยวกับการใช้งาน API เพื่อเป็นแนวทางปฏิบัติให้แก่ผู้พัฒนาระบบนำไปพัฒนาประยุกต์ใช้เข้ากับระบบของตนเองให้มีความปลอดภัยต่อไป

มาตรฐานที่ควรพิจารณาทางด้านความปลอดภัยสำหรับการพัฒนา API มีดังต่อไปนี้

1. **กระบวนการพิสูจน์ตัวตน (Authentication)** ในที่นี้หมายรวมถึงการพิสูจน์ตัวตนทั้งจากด้านผู้ใช้งาน และจากด้านระบบผู้ให้บริการ
   - **1.1 กระบวนการพิสูจน์ตัวตนทางด้านผู้ใช้งาน หรือ Client and App Authentication** คือการพิสูจน์ตัวตนทางฝั่งผู้ใช้งานหรือระบบต้นทางที่ต้องการเชื่อมต่อไปยังอีกระบบนึงเพื่อขอใช้บริการต่าง ๆ แนวทางที่พัฒนาใช้กันส่วนใหญ่มีวิธีดังนี้
     - การพิสูจน์ตัวตนโดยใช้ Username และ Password คือรูปแบบการพิสูจน์ตัวตนที่ง่ายที่สุด อย่างไรก็ตามการใช้ Username และ Password มีจุดอ่อนคือ วิธีการตั้งรหัสผ่านที่คาดเดายาก และการเปลี่ยนรหัสผ่านทำได้ยาก เนื่องจากการกำหนดรหัสผ่านจะถูกใช้ร่วมกันในหลายระบบงาน และการแก้ไขรหัสผ่านจำเป็นต้องแก้ไขข้อมูลในส่วนของการติดตั้งระบบ โดยระหว่างการเปลี่ยนแปลงรหัสผ่านนี้จะต้องปิดการเชื่อมต่อทั้งหมด ทำให้ส่งผลกระทบเกิดขึ้นในวงกว้างและอาจจะเกิดข้อผิดพลาดได้สูง
     - การพิสูจน์ตัวตนโดยใช้ Token-Based คือรูปแบบการพิสูจน์ตัวตนที่ใช้รหัส Token แทนการส่งด้วยข้อมูล Username และ Password โดยตรง ข้อดีของวิธีนี้คือ การพิสูจน์ตัวตนมีความปลอดภัยมากขึ้น เนื่องจากระบบจะมีการสร้างค่า Token สำหรับใช้งานแต่ละครั้ง และสามารถใช้งานในเวลาที่จำกัด ดังนั้นทำให้โอกาสที่ข้อมูล Username และ Password จะถูกดักจับจึงมีโอกาสเกิดขึ้นน้อยมาก และผลกระทบจากการที่ต้องเปลี่ยนแปลงแก้ไขระบบเกิดขึ้นน้อยตามไปด้วย

1.2. กระบวนการพิสูจน์ตัวตนทางด้านผู้ให้บริการ หรือ API and Server Authentication คือกระบวนการที่ผู้ใช้บริการควรตรวจสอบใบรับรองอิเล็กทรอนิกส์ (Certificate) ของเซิร์ฟเวอร์หรือผู้ให้บริการ ซึ่งมีขั้นตอนการตรวจสอบใบรับรองอิเล็กทรอนิกส์ดังต่อไปนี้

- การตรวจสอบว่าใบรับรองอิเล็กทรอนิกส์ถูกออกโดยผู้ให้บริการ CA (Certification Authority) ที่น่าเชื่อถือ
- การตรวจสอบว่าใบรับรองอิเล็กทรอนิกส์ไม่หมดอายุ
- การตรวจสอบว่าใบรับรองอิเล็กทรอนิกส์ไม่ถูกเพิกถอน
- การตรวจสอบว่าใบรับรองอิเล็กทรอนิกส์มีชื่อตรงกับชื่อโดเมนของบริการและเซิร์ฟเวอร์

2. กระบวนการตรวจสอบสิทธิ์การใช้งาน (Authorization) คือกระบวนการตรวจสอบเพื่อกำหนดทรัพยากรที่ผู้ใช้งานสามารถเข้าถึงได้ เพื่อป้องกันไม่ให้ผู้ใช้งานเข้าถึงฟังก์ชัน API หรือการดำเนินการนอกบทบาทที่กำหนดไว้ได้ เช่น API ฝั่งผู้ใช้งานที่มีสิทธิ์แบบอ่านอย่างเดียวไม่ควรได้รับอนุญาตให้เข้าถึงปลายทางที่มีฟังก์ชันการทำงานของ API ฝั่งผู้ดูแลระบบ

3. กระบวนการดูแลและควบคุมความปลอดภัยของข้อมูล (Data Security Management)

3.1. การตรวจสอบความถูกต้องของข้อมูล หรือ Message Integrity คือการตรวจสอบข้อความที่รับส่งระหว่าง API ผู้ใช้งานและผู้ให้บริการว่าข้อความมีความถูกต้องและสมบูรณ์ ไม่ถูกเปลี่ยนแปลงแก้ไขจากบุคคลภายนอกหรือบุคคลที่ไม่ได้รับอนุญาต

3.2. การรักษาความลับของข้อมูล หรือ Message Confidentiality คือการเก็บข้อมูลเป็นความลับและอนุญาตให้เฉพาะผู้ได้รับอนุญาตสามารถอ่านและเข้าถึงข้อมูลได้เท่านั้น กล่าวคือหากข้อความที่รับส่งระหว่าง API ผู้ใช้งานและผู้ให้บริการนั้นประกอบด้วยข้อมูลที่มีความสำคัญ หรือ Sensitive Information ข้อมูลในส่วนนี้ควรจะต้องถูกเก็บเป็นความลับโดยใช้การเข้ารหัสที่รัดกุมและมีความยาวคีย์ที่เพียงพอเพื่อป้องกันการเข้าถึงจากบุคคลที่ไม่ได้รับอนุญาต

3.3. การรับส่งข้อมูลผ่านช่องทางเข้ารหัส หรือ Transport Encoding คือการรับส่งข้อความผ่านทางช่องทางที่เชื่อมต่อระบบด้วยโปรโตคอลที่เข้ารหัสเท่านั้น (HTTPS) เพื่อป้องกันการถูกดักจับข้อมูลสำคัญระหว่างทางและอนุญาตการเชื่อมต่อเฉพาะเทคโนโลยีความปลอดภัยที่ได้มาตรฐานล่าสุดปัจจุบันคือ TLS1.2

3.4. การเปิดเผยข้อมูลเท่าที่จำเป็น คือการควบคุมข้อมูลที่เกิดจากการประมวลผล API ให้แสดงข้อมูลเท่าที่จำเป็นต้องใช้งาน รวมถึงการแสดงข้อความที่เกิดจากข้อผิดพลาดจากการประมวลผล เพื่อให้แสดงเฉพาะข้อความมาตรฐาน โดยไม่ได้แสดงถึงข้อมูลโครงสร้างระบบภายใน

4. **กระบวนการตรวจสอบข้อมูลก่อนนำไปประมวลผล หรือ Data Validation** คือการตรวจสอบข้อมูลที่ส่งมาจากผู้ใช้งาน เพื่อให้แน่ใจว่าข้อมูลเข้ากันได้กับระบบงานและระบบสามารถประมวลผลได้ตรงตามที่คาดหวัง ยกตัวอย่างวิธีการตรวจสอบข้อมูล เช่น การตรวจสอบประเภทของข้อมูลว่าตรงตามที่ต้องการหรือไม่ หรือการตรวจสอบความยาวของข้อมูลว่าอยู่ในขอบเขตที่ระบบรับไปเพื่อประมวลผลได้หรือไม่ ซึ่งวิธีการเหล่านี้จะช่วยคัดกรองข้อมูลที่ผิดปกติหรือข้อมูลไม่เข้ากับการทำงานของระบบออก เพื่อลดความเสี่ยงที่ระบบอาจจะเกิดข้อผิดพลาดต่าง ๆ รวมถึงลดความเสี่ยงของการถูกโจมตีประเภท Injection
5. **การควบคุมปริมาณและการจำกัดโควต้าการใช้งาน API หรือ Throttling and Rate Limits** คือการควบคุมการใช้งานทรัพยากรบนเซิร์ฟเวอร์อย่างมีประสิทธิภาพ การจำกัดจำนวนข้อความ API ต่อวินาที การกำหนดขนาดของข้อความ API ที่สามารถรับและนำไปประมวลผลทำงานต่อได้ เพื่อป้องกันไม่ให้เกิดการใช้งานทรัพยากรของเซิร์ฟเวอร์ที่เกินความสามารถที่ระบบจะรองรับได้และป้องกันการโจมตีประเภท DDoS
6. **การเก็บบันทึกข้อมูล และการเฝ้าระวัง หรือ Logging and Monitoring** คือการเก็บบันทึกข้อมูล Log ที่เกี่ยวข้องกับการทำงานของ API และการเฝ้าระวังตรวจสอบการทำงาน API ที่ผิดปกติ โดยข้อมูลจาก Log file ถือเป็นข้อมูลส่วนสำคัญของการวิเคราะห์การทำงานหรือเหตุการณ์ผิดปกติที่เกิดขึ้น โดยข้อมูลที่ถูกบันทึกนี้จะประกอบด้วยข้อมูลเหตุการณ์ เช่น ใคร ทำอะไร ที่ไหน อย่างไร และเมื่อไหร่ และการเก็บรักษาข้อมูลเหล่านี้ต้องมีการดูแลชุดข้อมูลให้ครบถ้วนและควบคุมการเข้าถึงไม่ให้ใครสามารถเข้าไปเปลี่ยนแปลงข้อมูลชุดนี้ได้ เพื่อกรณีจำเป็นต้องใช้เป็นหลักฐานสำคัญในการพิสูจน์และในการดำเนินคดีต่อไป
7. **การสร้างความแข็งแรงให้กับระบบหรือเซิร์ฟเวอร์ หรือ Server Hardening** คือกระบวนการของการกำหนดค่าพารามิเตอร์ทั้งบนระบบปฏิบัติการและของแอพพลิเคชัน เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต ป้องกันผู้บุกรุก และปิดช่องโหว่ด้านความปลอดภัยอื่นๆ นอกจากนี้การทำ Hardening ใช้หลักการ "ลดสิ่งที่ไม่ได้ใช้ออกไปจากระบบ" ทำให้ระบบมีความน่าเชื่อถือ มีความปลอดภัย และช่วยเพิ่มประสิทธิภาพการทำงานให้ดีขึ้น

นอกจากนี้ทาง OWASP ยังได้จัดอันดับ TOP 10 ความเสี่ยงที่เกิดจากการพัฒนาระบบด้วย API ปี 2019 (OWASP API Security Top 10 – 2019) ดังตารางต่อไปนี้

ความเสี่ยง	คำอธิบาย
1. **Broken Object Level Authorization**	ความเสี่ยงที่เกิดจากระบบหรือผู้ให้บริการขาดการการตรวจสอบสิทธิ์ผู้ใช้งาน API ทำให้ข้อมูลถูกเข้าถึงและใช้งานโดยผู้ไม่ได้รับอนุญาตได้
2. **Broken User Authentication**	ความเสี่ยงที่เกิดจากกระบวนการพิสูจน์ตัวตนผิดพลาด เช่น การตั้งรหัสผ่านที่คาดเดาได้ง่าย หรือการส่งค่า Token บน URL ทำให้ง่ายต่อการถูกดักจับและนำไปใช้งานโดยผู้ที่ไม่ได้รับอนุญาตได้
3. **Excessive Data Exposure**	ความเสี่ยงที่เกิดจากการเปิดเผยข้อมูลที่ไม่จำเป็นมากเกินไป หรือการที่ API ตอบกลับข้อมูลมามากเกินกว่าที่จะต้องนำไปใช้งานจริง
4. **Lack of Resources & Rate Limiting**	ความเสี่ยงที่เกิดจากขาดการกำหนดหรือจำกัดการใช้งานทรัพยากรบนระบบ อาจนำไปสู่การโจมตีประเภท DDOS
5. **Broken Function Level Authorization**	ความเสี่ยงที่เกิดจากระบบหรือผู้ให้บริการขาดการการตรวจสอบสิทธิ์ฟังก์ชันผู้ใช้งาน API ทำให้ผู้ใช้งานสามารถเข้าถึงฟังก์ชันอื่นๆ เช่นเข้าถึงฟังก์ชันข้อมูลถูกเข้าถึงและใช้งานโดยผู้ไม่ได้รับอนุญาตได้
6. **Mass Assignment**	ความเสี่ยงที่เกิดจาก API ยอมรับค่าพารามิเตอร์เกินกว่าที่ควรจะเป็น
7. **Security Misconfiguration**	ความเสี่ยงของ API ที่เกิดจากการตั้งค่าอย่างไม่ปลอดภัย หรือไม่ได้เปิดใช้งานฟังก์ชันด้านความปลอดภัย
8. **Injection**	ความเสี่ยงที่เกิดจากความบกพร่องของการตรวจสอบข้อมูลก่อนนำไปประมวลผล ทำให้ระบบนำข้อมูลไปประมวลผลผิดพลาด
9. **Improper Assets Management**	ความเสี่ยงที่เกี่ยวข้องกับการบริหารจัดการดูแล API ไม่ดี เช่น อนุญาตให้มีการสร้าง API สำหรับทดสอบค้างไว้บนระบบการใช้งานจริง
10. **Insufficient Logging & Monitoring**	ความเสี่ยงที่เกิดจากขาดการเก็บบันทึกข้อมูลและการเฝ้าระวังตรวจสอบข้อมูล

จากมาตรฐานการพัฒนา API และการจัดอันดับความเสี่ยงที่กล่าวมาทั้งหมดข้างต้น สามารถนำมาจัดกลุ่ม Attack and Defense เพื่อให้เห็นมาตรฐานแต่ละข้อที่จะใช้สำหรับการพัฒนา API ให้มีความมั่นคงปลอดภัยได้ตามตาราง ได้ดังต่อไปนี้

มาตรฐานการพัฒนา API	OWASP API Security Top 10 – 2019
กระบวนการพิสูจน์ตัวตน (Authentication)	A2 - Broken User Authentication
กระบวนการตรวจสอบสิทธิ์การใช้งาน (Authorization)	A1- Broken Object Level Authorization A5 - Broken Function Level Authorization
กระบวนการดูแลและควบคุมความปลอดภัยของข้อมูล (Data Security Management)	A3 - Excessive Data Exposure
กระบวนการตรวจสอบข้อมูลก่อนนำไปประมวลผล (Data Validation)	A6 - Mass Assignment A8 - Injection
การควบคุมปริมาณและการจำกัดโควตาการใช้งาน API (Throttling and Rate Limits)	A4 - Lack of Resources & Rate Limiting
การเก็บบันทึกข้อมูล และการเฝ้าระวัง (Logging and Monitoring)	A10 - Insufficient Logging & Monitoring
การสร้างความแข็งแรงให้กับระบบหรือเซิร์ฟเวอร์ (Server Hardening)	A7 - Security Misconfiguration A9 - Improper Assets Management

งานความร่วมมือกับหน่วยงานภายนอก

สมาคมธนาคารไทยได้ลงนามในบันทึกข้อตกลงความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคธุรกิจการเงิน การลงทุน และการประกันภัย เมื่อวันที่ 22 กันยายน 2016 กับหน่วยงานภาคการเงิน ได้แก่ ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย (สำนักงาน คปภ.) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) โดยมีวัตถุประสงค์ในการส่งเสริมและสนับสนุนความร่วมมือระหว่างในการรับมือภัยคุกคามไซเบอร์ ได้แก่ การร่วมกันกำหนดมาตรฐานและกรอบบริหารจัดการภัยคุกคามไซเบอร์ ร่วมกันกำหนดข้อตกลง กลไก กระบวนการ ขั้นตอนการแลกเปลี่ยนข้อมูลของการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมให้หน่วยงานมีแผนรับมือภัยคุกคามไซเบอร์ พัฒนาและยกระดับความพร้อมของบุคลากรในภาคการเงินให้มีความรู้ความเชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ รวมถึงการสร้างเครือข่ายและสรรหาบุคลากรใหม่ด้านความมั่นคงปลอดภัยไซเบอร์เข้าสู่ภาคการเงิน ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร (TB-CERT) ได้จัดทำแผนและกิจกรรมร่วมกับองค์กรภาคการเงินภายใต้บันทึกข้อตกลงดังกล่าวอย่างต่อเนื่อง

นอกจากนี้ ยังมีความร่วมมือกับหน่วยงานในภาคอุตสาหกรรมอื่น เช่น ในปีนี้ได้ร่วมมือกับ LINE ในการแจ้งเหตุการณ์ด้านภัยไซเบอร์อย่างกรณีเกิดการปลอมแปลง LINE official เป็นต้น

สารจากผู้แทนคณะทำงานความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคการเงิน การลงทุน และการประกันภัย

ดร.กำพล ศรธนะรัตน์
ผู้ช่วยเลขาธิการ
สายเทคโนโลยีดิจิทัลและประสิทธิภาพองค์กร
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

" มีโอกาสได้ทำงานร่วมกันกับสมาคมธนาคารไทยมาระยะหนึ่ง รู้สึกประทับใจกับการมองไปข้างหน้าใช้เป้าหมายเป็นที่ตั้ง แล้วขับเคลื่อนไปด้วยกันแบบมืออาชีพ สามารถไว้วางใจได้ในทุกภารกิจที่ลงมือทำว่าจะได้รับผลลัพธ์เกินความคาดหวังเสมอ โดยเฉพาะการสร้าง Cyber Resilience ให้กับภาคตลาดทุนผ่านโปรแกรมต่าง ๆ เช่น การสร้างความตระหนักด้านไซเบอร์ให้กับคณะกรรมการบริษัท การแจ้งเตือนเหตุภัยไซเบอร์ การจัดงาน Financial Cybersecurity Boot Camp เพื่อเปิดโอกาสให้น้อง ๆ นักศึกษาได้มีโอกาสแสดงความสามารถและทำความรู้จักตลาดเงินตลาดทุน การจัดงาน Tech Career Coaching เพื่อเปิดตลาดแรงงานใหม่ ๆ ที่เห็นความสำคัญของคนทำงานด้านเทคโนโลยี การเสริมสร้าง Cyber Capabilities ให้กับบุคลากรในตลาดทุน รวมไปถึงการจัดการฝึกซ้อมด้าน Cyber Drill ทุกครั้งที่เข้าร่วมกิจกรรม ทำให้เราได้เรียนรู้และพัฒนาตลอดเวลา ขอบคุณอีกครั้งสำหรับการให้บริการแบบมืออาชีพครับ "

คุณมยุรินทร์ สุทธิรัตนพันธ์
ผู้ช่วยเลขาธิการ
สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย

" ขณะที่ระบบเทคโนโลยีสารสนเทศทันสมัยยิ่งขึ้น ความเสี่ยงและภัยคุกคามทางไซเบอร์ก็มีแนวโน้มเพิ่มสูงขึ้นอย่างต่อเนื่องเช่นกัน ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ (CERT) จึงเป็นศูนย์กลางในการประสานงานกับบริษัท เพื่อเฝ้าระวัง วางมาตรการรับมือ ตอบสนอง และแนะนำในการจัดการกับเหตุการณ์ความปลอดภัยคอมพิวเตอร์ (Incident Response) ที่เกิดขึ้นกับธุรกิจได้อย่างทันท่วงที รวมถึงสร้างความร่วมมือกับหน่วยงานที่เกี่ยวข้องในภาคการเงินเพื่อแลกเปลี่ยนข้อมูลที่เกี่ยวข้องกับการรักษาความปลอดภัยด้านไซเบอร์ ในปัจจุบันภัยไซเบอร์ที่เกิดขึ้นไม่ได้ส่งผลจำกัดแค่องค์กรใดองค์กรหนึ่ง แต่ส่งผลกระทบในวงกว้าง การร่วมมือกันระหว่างองค์กรจะทำให้สามารถรับมือกับภัยไซเบอร์เหล่านั้นได้ ซึ่งก็จะเป็นประโยชน์สำหรับภาคการเงินอย่างยิ่ง "

ดร. ชัยชนะ มิตรพันธ์
ผู้อำนวยการ
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(องค์การมหาชน)

" TB-CERT เป็นตัวอย่างของความสำเร็จที่หน่วยงานภาคเอกชนมาร่วมกันทำงานเพื่อส่วนรวม ช่วยปกป้องภาคการเงินของประเทศไทยจากภัยไซเบอร์ ด้วยความเป็นมืออาชีพ "

สารจากผู้แทนคณะทำงานความร่วมมือด้านการยกระดับความพร้อมรับมือภัยคุกคามไซเบอร์ (CERT Readiness) ต่อภาคการเงิน การลงทุน และการประกันภัย

คุณนุษกร ธีระปัญญาชัย
ผู้อำนวยการอาวุโส
ฝ่ายนโยบายระบบการชำระเงิน
ธนาคารแห่งประเทศไทย

" การก้าวเข้าสู่สังคมดิจิทัลที่ใช้ชีวิตประจำวันบนโลกเทคโนโลยี "ความร่วมมือ" เป็นกลไกสำคัญในการขับเคลื่อนให้การใช้ชีวิตในยุคดิจิทัลเป็นไปอย่างราบรื่นและปลอดภัย และในปี 2017 เกิดการประสานความร่วมมือครั้งสำคัญของภาคธนาคารไทย เมื่อมีการจัดตั้ง "TB-CERT" โดยมีจุดประสงค์ให้ธนาคารพาณิชย์ร่วมมือกันสร้างความเข้มแข็งและความพร้อมในการรับมือภัยคุกคามไซเบอร์ที่นับวันมีความซับซ้อนและส่งผลกระทบในวงกว้างมากขึ้น การจัดตั้ง TB-CERT ให้เกิดการรวมตัวของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ในภาคธนาคารที่เข้ามาร่วมกันทำงานด้วยความเสียสละและตั้งใจอย่างยิ่ง ทำให้ TB-CERT มีพัฒนาการที่ก้าวหน้าอย่างรวดเร็ว มีการทำงานอย่างเป็นระบบและมีประสิทธิภาพตามมาตรฐานสากล สามารถยกระดับความพร้อม (Maturity) ได้ดีขึ้นต่อเนื่อง จนเป็นแบบอย่างที่ดีให้กับการจัดตั้ง CERT ในภาคธุรกิจอื่น

ในฐานะผู้แทน ธปท. ที่ได้มีโอกาสร่วมทำงานกับ TB-CERT อย่างใกล้ชิด ขอชื่นชมและขอบคุณทีมงาน TB-CERT สมาชิก และทุกท่านที่ได้ร่วมจัดตั้ง ขับเคลื่อน และสนับสนุนให้ TB-CERT เป็นองค์กรที่เข้มแข็ง เชื่อมั่นว่า TB-CERT จะยังคงมีพัฒนาการที่ดีขึ้นต่อเนื่องและจะเป็นกลไกหลักในการสร้างภูมิคุ้มกันให้กับระบบสถาบันการเงินไทย "

คุณภิญโญ ศรีเพชราภรณ์
ผู้อำนวยการ ฝ่ายกำกับและตรวจสอบ
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย

" โลกทุกวันนี้เปลี่ยนแปลงอย่างรวดเร็ว ทุกภาคส่วน ทั้งภาครัฐ เอกชนและประชาชน ต้องปรับตัวเพื่อไม่ให้ถูก disrupt ด้วยเทคโนโลยี และมีภูมิคุ้มกันภัยไซเบอร์ที่เข้มแข็ง ผู้กำกับดูแลภาคธนาคารก็ต้องปรับการกำกับดูแลให้เป็น proactive โดยร่วมมือทำงานหน่วยงานที่เกี่ยวข้องทุกภาคส่วนใกล้ชิดขึ้น ในส่วนของผู้ให้บริการก็จำเป็นต้องเร่งพัฒนาการรับมือภัยคุกคามไซเบอร์แบบเชิงรุก เพื่อป้องกันการลุกลามและเกิดความเสียหายเป็นวงกว้าง "

" ระบบ IT ที่มีเสถียรภาพคือหัวใจสำคัญของการให้บริการของสถาบันการเงิน เสถียรภาพหมายถึงระบบ IT ที่มีความทนทาน ซึ่งมี 2 มิติหลัก มิติแรกคือระบบเพียงพอรองรับปริมาณธุรกรรมที่เพิ่มมากขึ้นแบบก้าวกระโดด และมิติที่สองคือ สถาบันการเงินมีความพร้อมรับมือกับความท้าทายจากภัยไซเบอร์ ซึ่งมิติที่สองนี้มีความท้าทายอย่างมาก ต้องเตรียมตัวให้พร้อมอยู่เสมอ บุคลากรต้องมีความเชี่ยวชาญและชำนาญ มีเครื่องมือที่ทันสมัย และมีกระบวนการทำงานที่สามารถประสานทั้งภายในภายนอกได้อย่างคล่องตัวเมื่อเกิดเหตุ "

คุณวาสนา นิมิตยงสกุล
ผู้อำนวยการอาวุโส
ฝ่ายกำกับและตรวจสอบความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ
ธนาคารแห่งประเทศไทย

" การแข่งขันทางธุรกิจแบ่งแยกบริษัทผม และบริษัทคุณ แต่ในโลกของเทคโนโลยีที่เชื่อมโยงบริษัทผมและบริษัทคุณเข้าด้วยกัน ทำให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์มีแค่คำว่า "เรา" เราจึงต้องร่วมมือและช่วยเหลือซึ่งกันและกัน การแลกเปลี่ยนข้อมูลภัยคุกคามเป็นหนทางหนึ่งที่จะช่วยเราทุกคนให้ปลอดภัยจากภัยไซเบอร์มากยิ่งขึ้น "

คุณเจษฎา ปรมาภรณ์พิลาส
ผู้อำนวยการ ฝ่ายกำกับและตรวจสอบ
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับ
หลักทรัพย์และตลาดหลักทรัพย์

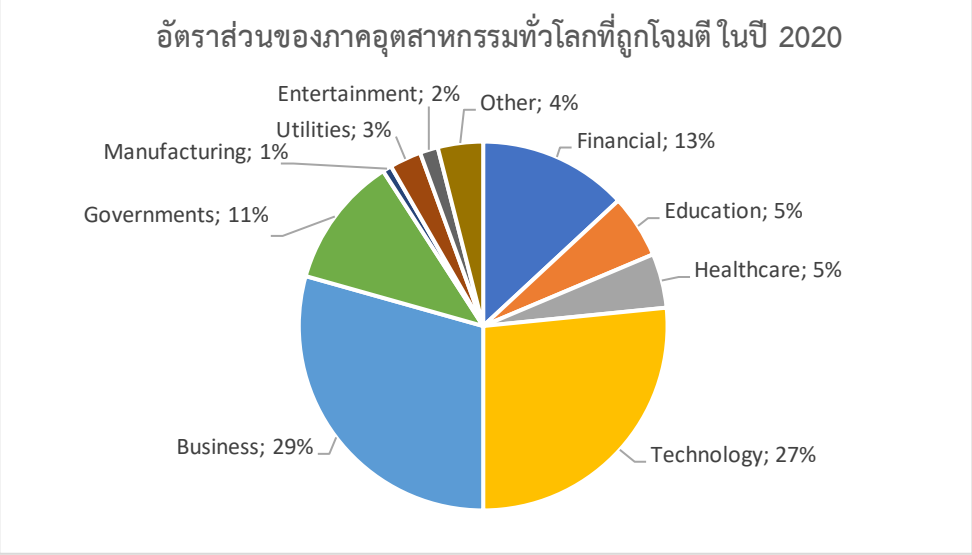
บทวิเคราะห์เหตุการณ์โจมตีในปี 2020

ในปี 2020 ทีมงาน TB-CERT ได้รวบรวมและวิเคราะห์ข่าวเหตุการณ์การโจมตีสำคัญทางไซเบอร์ทั่วโลก กว่า 250 เหตุการณ์ พบว่าภาคอุตสาหกรรม (Sector) ที่เป็นเป้าหมายหลักของการโจมตีในปี 2020 นี้ คือ 29% เป็นภาคธุรกิจ ทั้งบริษัท ห้างร้าน E-commerce และโรงแรม ที่ใช้ระบบเทคโนโลยีสารสนเทศในการขับเคลื่อนธุรกิจหรือให้บริการลูกค้าภายนอก อาจจะด้วยองค์กรเหล่านี้ไม่ได้ให้ความสำคัญกับการรักษาความมั่นคงปลอดภัยมากนัก ขาดบุคลากรและองค์ความรู้ในการรักษาความมั่นคงปลอดภัยก็เป็นได้

รองลงมาเป็นภาคเทคโนโลยี ซึ่งคิดเป็นสัดส่วนถึง 27% รวมตั้งแต่บริษัทที่ให้บริการและผู้พัฒนาผลิตภัณฑ์ด้านเทคโนโลยีสารสนเทศต่าง ๆ ผู้ให้บริการระบบคลาวด์ และระบบอินเทอร์เน็ต เป็นต้น ถึงแม้ว่าองค์กรเหล่านี้จะมีบุคลากรและทักษะในการรักษาความปลอดภัยสูงกว่าภาคอุตสาหกรรมอื่น ๆ แต่บริษัทเหล่านี้มีข้อมูลที่เกี่ยวข้องกับผลิตภัณฑ์และสิทธิบัตรต่าง ๆ [1] เป็นเป้าด้านความท้าทายในการโจมตีบริษัทที่เป็นผู้นำด้านเทคโนโลยี รวมถึงการทำให้บริษัทเจ้าของผลิตภัณฑ์เหล่านี้เป็นฐานที่ใช้ในการโจมตีหน่วยงานอื่น ๆ ต่อไป เช่น ในกรณีที่ฝังมัลแวร์ไว้ในโค้ดอัปเดตของระบบ เป็นต้น ซึ่งจะได้กล่าวถึงรายละเอียดในบทวิเคราะห์ตอนท้ายสุด ว่าด้วยการโจมตีไปยังหน่วยงานบุคคลที่สาม (3rd party)

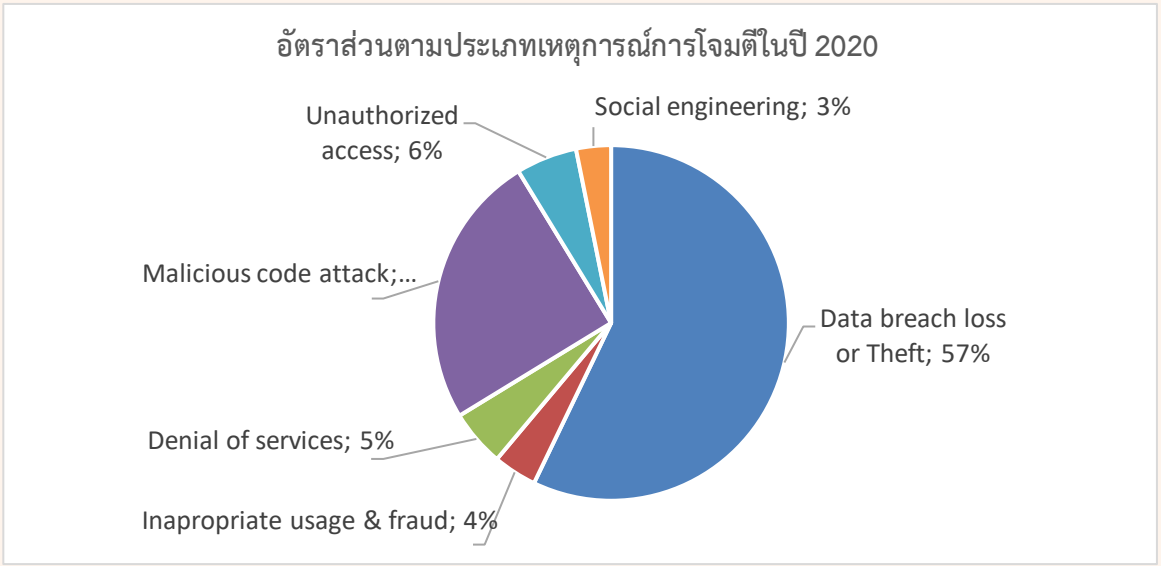
ส่วนภาคการเงินนั้นพบเหตุการณ์การโจมตีมากเป็นอันดับ 3 คิดเป็นสัดส่วน 13% ดังรูปที่ 9 แม้ว่าองค์กรในภาคการเงินนั้นมีบุคลากร ทักษะ และการลงทุนด้านการรักษาความมั่นคงปลอดภัย แต่แรงจูงใจที่ Threat Actor มักจะโจมตีองค์กรในภาคการเงินคือ เงิน และข้อมูลทางด้านการเงิน เนื่องจากองค์กรเหล่านี้มีความสำคัญอย่างมาก และมีโอกาสที่ Threat Actor จะได้รับเงินจากองค์กรเหล่านี้มากกว่าภาคอุตสาหกรรมอื่น ๆ อีกด้วย

อย่างไรก็ตามในปี 2020 นี้เป้าหมายการโจมตีทางไซเบอร์ที่มีความน่าสนใจจะอยู่ที่ภาคสาธารณสุข (Healthcare) โดยเฉพาะการโจมตีและใช้มัลแวร์เรียกค่าไถ่ (Ransomware) ด้วยองค์กรในภาคสาธารณสุขนั้นมีการเก็บข้อมูลส่วนบุคคลเชิงลึกเป็นจำนวนมาก รวมถึงข้อมูลประวัติการรักษาพยาบาล ซึ่งนอกจากการที่ข้อมูลส่วนบุคคลเชิงลึกนั้นจะถูกขโมยไปได้แล้ว จะยังสามารถสร้างผลกระทบในด้านชื่อเสียง ด้านสิทธิความเป็นมนุษย์ของเจ้าของข้อมูลได้อีกด้วย แต่ยังมีเหตุการณ์ที่สร้างความเศร้าโศกที่เกิดจากการที่ผู้ป่วยในโรงพยาบาลต้องมาเสียชีวิตในช่วงที่มัลแวร์เรียกค่าไถ่ทำการปิดระบบของโรงพยาบาลทำให้ผู้ป่วยดังกล่าวต้องถูกนำไปยังโรงพยาบาลที่อยู่ไกลขึ้นและได้เสียชีวิตในระหว่างทาง เป็นเหตุการณ์ที่สะท้อนความเชื่อมโยงอย่างใกล้ชิดยิ่งขึ้นของผลกระทบจากโลกไซเบอร์มายังโลกที่มนุษย์อยู่อย่างที่เรียกได้ว่าไม่สามารถหลีกเลี่ยงได้เลยในปัจจุบัน



รูปที่ 9 แสดงอัตราส่วนของภาคอุตสาหกรรมทั่วโลกที่ถูกโจมตี ในปี 2020 จากการรวบรวมข้อมูลของ TB-CERT

เมื่อวิเคราะห์ประเภทของเหตุการณ์แล้วพบว่า มีเหตุการณ์เกี่ยวกับข้อมูลรั่วไหล ข้อมูลสูญหาย หรือขโมยข้อมูล (Data Breach Loss or Theft) สูงที่สุด ถึง 57% รองลงมาเป็นเหตุการณ์เกี่ยวกับการโจมตีของมัลแวร์ในรูปแบบอื่น ๆ ที่ไม่มุ่งเป้าไปที่ข้อมูล (Malicious Code Attack) 25% ส่วนการเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) การใช้งานไม่เหมาะสม การฉ้อโกง (Inappropriate Usage & Fraud) รวมไปถึงการใช้เทคนิคการหลอกลวง (Social Engineering) ก็ยังคงใช้ได้ผล เนื่องจากในปัจจุบันจุดมุ่งหมายของ Threat Actor นั้นมีความต้องการเงินหรือข้อมูลที่จะสามารถนำไปขายต่อ จะไม่ใช่เป็นเพียง Threat Actor ที่จะมุ่งโจมตีเพื่อศึกษาหรือความสนุกเหมือนกับ Threat Actor ในอดีต จึงจะยังคงพบเห็นการใช้วิธีการต่าง ๆ หรือผสมผสานเพื่อให้เป็นผล



รูปที่ 10 แสดงอัตราส่วนตามประเภทของเหตุการณ์การโจมตีในปี 2020 จากการรวบรวมข้อมูลของ TB-CERT

แรงจูงใจของ Threat Actor

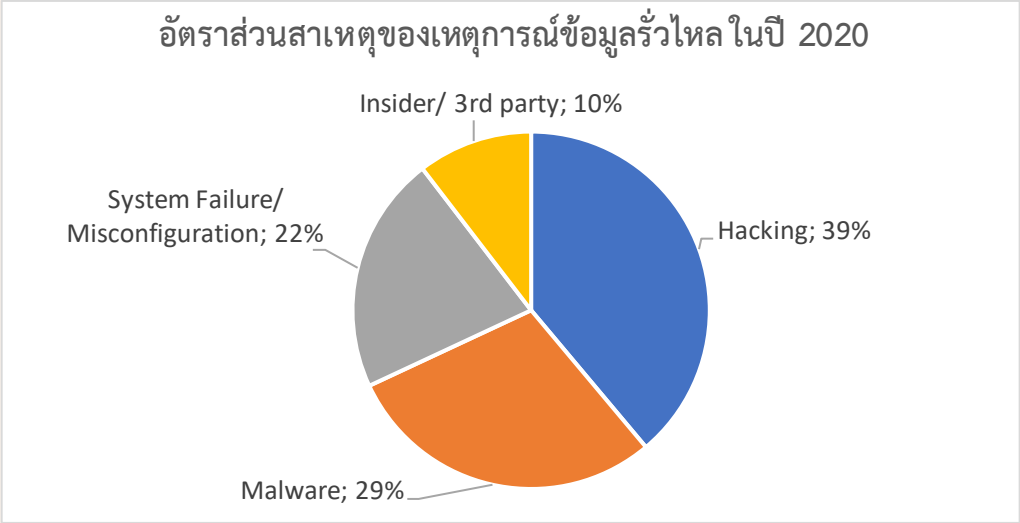
จากรายงานของ Verizon [2] พบว่าแรงจูงใจหลักของ Threat Actor ที่เจาะระบบนั้นคือความต้องการทางด้านการเงินถึง 86% ซึ่งขั้นตอนแรกของ Threat Actor คือการหาทางที่จะหลอกขโมยข้อมูลที่จะใช้ในการเข้าถึงบริการทางการเงินออนไลน์ของเหยื่อบุคคลโดยใช้ฟิชชิง เป็นต้น หรือหากสามารถเจาะระบบและเข้าถึงข้อมูลขององค์กรได้ Threat Actor ก็มักจะปล่อยมัลแวร์และเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ (Ransomed) หรือการข่มขู่ (Blackmail) ที่จะเปิดเผยข้อมูล ซึ่งจะทำให้เหยื่อต้องจ่ายค่าไถ่ตามที่เรียกร้องหรือ Threat Actor ก็จะนำข้อมูลไปขายต่อในตลาดมืด Threat Actor

นอกจากนี้เหตุการณ์ที่เกี่ยวกับการจารกรรมข้อมูล หรือ Cyber Espionage นั้นน่าสนใจ พบว่าในปีที่ผ่านมาทาง Verizon พบเหตุการณ์ที่เกี่ยวข้องกับแคมเปญดังกล่าวถึง 10% ถึงแม้ว่าจะเป็นตัวเลขที่ไม่สูงเมื่อเทียบกับความต้องการทางด้านการเงิน แต่มีผลกระทบในแง่ของความอ่อนไหว ความลับของข้อมูล และความสำคัญทางธุรกิจ ด้วยเหตุนี้จึงเป็นแรงจูงใจที่ไม่ควรละเลย

อย่างไรก็ตามจากรายละเอียดของข่าวในปีที่ผ่านมาพบว่า ลักษณะข้อมูลที่หลุดรั่วจากเหตุการณ์ข้อมูลรั่วไหลต่าง ๆ นั้นประกอบด้วย ข้อมูลส่วนบุคคลของลูกค้าและพนักงาน ข้อมูลที่ใช้ในการเข้าถึงระบบ (บัญชีผู้ใช้และ Credentials) รวมถึงข้อมูลทางด้านการเงิน (เช่น เลขที่บัตรเครดิต หรือเลขที่บัญชีธนาคาร เป็นต้น) ซึ่งจากรายงานของ Verizon ก็ยังพบว่ามี 58% ของเหตุการณ์ข้อมูลรั่วไหลนั้นเกี่ยวข้องกับข้อมูลส่วนบุคคล ที่ประกอบไปด้วย อีเมล ชื่อ หมายเลขโทรศัพท์ และที่อยู่ เป็นต้น รองลงมาเป็นข้อมูล Credentials 39% แสดงให้เห็นว่า Threat Actor นั้นมีเป้าหมายไปที่ข้อมูลส่วนบุคคลและ Credentials ซึ่งอีเมลนั้นมีความสำคัญในการระบุตัวตนทางดิจิทัล และเมื่อ Threat Actor สามารถเข้าถึงอีเมลนี้ก็จะสามารถขโมยและแอบอ้างเป็นบุคคลนั้นได้ อีกทั้งในบางเหตุการณ์ที่ Threat Actor สามารถเข้าถึงบัญชีผู้ใช้งานภายในองค์กรและยังสามารถทำ Lateral Movement หรือการโยกย้ายภายในระบบเครือข่ายขององค์กรเพื่อค้นหาข้อมูลที่อ่อนไหวและสำคัญอื่น ๆ เพื่อนำไปขายต่อได้อีกด้วย

สาเหตุของข้อมูลรั่วไหล

จากเหตุการณ์ข้อมูลรั่วไหลทั่วโลก ได้มีการวิเคราะห์ถึงสาเหตุของการรั่วไหลของข้อมูล พบว่าสาเหตุหลักเกิดจากเจาะระบบถึงกว่า 80% ซึ่งแบ่งประเภทของการ Threat Actor เจาะระบบออกเป็นการเจาะระบบโดยตรงเพื่อขโมยข้อมูล 39% การเจาะระบบขโมยข้อมูลโดยใช้มัลแวร์ 29% ความผิดพลาดของระบบและการปรับแต่งระบบที่ผิดพลาดมีผลให้เป็นช่องทางเข้าถึงข้อมูลได้ 22% และข้อมูลรั่วไหนจากบุคลากรภายในและองค์กรที่เป็น 3rd party เป็นสาเหตุให้ข้อมูลรั่วไหล 10% ซึ่งจะกล่าวถึงรายละเอียดต่อไป



รูปที่ 11 แสดงอัตราส่วนสาเหตุของเหตุการณ์ข้อมูลรั่วไหลในปี 2020 อ้างอิง รายงานของ บ.Verizon

1. **การเจาะระบบ (Hacking)** ซึ่ง Threat ActorThreat Actor ใช้รหัสผ่านที่ถูกขโมยหรือเดารหัสผ่านด้วยวิธีการ Bruteforce รวมทั้งการเจาะระบบผ่านช่องโหว่ (Vulnerability) ที่ยังไม่ได้ patch

2. **มัลแวร์เรียกค่าไถ่ (Malware)** ในปีที่ผ่านมามีเหตุการณ์ข้อมูลรั่วไหลจากมัลแวร์เรียกค่าไถ่หลายเหตุการณ์ เช่น มัลแวร์เรียกค่าไถ่ Maze หรือ Sodinokibi เป็นต้น อาจจะเพราะด้วยผู้ใช้งานไม่ได้เข้าไปทำงานในองค์กร ทำให้มาตรการการป้องกันเครื่องคอมพิวเตอร์ลดลง อีกทั้งผู้ใช้งานอาจขาดความตระหนักและทักษะในการป้องกันตัวเองจากภัยคุกคามต่าง ๆ ทำให้อาจถูกมัลแวร์ต่าง ๆ โดยเฉพาะมัลแวร์เรียกค่าไถ่คุกคามได้

3. **ความผิดพลาดของระบบและการปรับแต่งระบบที่ผิดพลาด (System Failure/Misconfiguration)** จากเหตุการณ์ข้อมูลรั่วไหลในปีที่ผ่านมาพบว่ายังพบเหตุการณ์ที่ระบบการรักษาความปลอดภัยทำงานผิดพลาดส่งผลทำให้ผู้ไม่หวังดีสามารถเข้าถึงฐานข้อมูลที่เป็นความลับได้ นอกจากนี้ยังมีเหตุการณ์ที่ผู้ดูแลระบบปรับแต่งระบบผิดพลาด เช่น มีการอนุญาตให้บุคคลภายนอกสามารถเข้าถึงได้โดยฐานข้อมูลหรือ storage ที่อยู่บนคลาวด์ได้โดยไม่ต้องยืนยันตัวตน ซึ่งถึงแม้ว่าเคยมีเหตุการณ์ในลักษณะนี้เกิดขึ้นก่อนหน้านี้บ่อยครั้ง แสดงเห็นว่าผู้ดูแลระบบขององค์กรอาจจะมีความตระหนักไม่มากเพียงพอก็เป็นได้ หรือผู้ให้บริการควรตั้งค่า default ให้ปิดการเข้าถึงไว้ตลอดเวลา เพื่อเป็นการช่วยเหลือผู้ดูแลระบบที่ใช้บริการ

4. **บุคลากรภายในและหน่วยงานบุคคลที่สาม (Insider/3rd Party)** หน่วยงานบุคคลที่สามนั้นมีหน้าที่ทำงานแทนองค์กรที่เก็บข้อมูลหรือเป็นเจ้าของข้อมูลในการจัดการ จัดเก็บ หรือประมวณผลข้อมูลขององค์กร ซึ่งในปีที่ผ่านมาถึงแม้ว่าจะมีจำนวนเหตุการณ์ไม่มาก แต่เหตุการณ์ที่เกิดขึ้นนั้นส่งผลกระทบด้านความเชื่อมั่นกับองค์กรที่เป็นเจ้าของข้อมูล ซึ่งควรกำหนดมาตรการให้หน่วยงานบุคคลที่สามเข้าถึงข้อมูลเท่าที่จำเป็น หรือกำหนดมาตรฐานการรักษาความปลอดภัยข้อมูลให้กับหน่วยงานบุคคลที่สามปฏิบัติตามอย่างเคร่งครัด

คำแนะนำในการป้องกันเหตุการณ์ข้อมูลรั่วไหล

1. อบรมให้ความรู้แก่ทุกคนในองค์กร ให้ทราบถึงความสำคัญของการป้องกันข้อมูลสำคัญ ทั้งข้อมูลส่วนบุคคลและข้อมูลขององค์กร
2. สร้างทะเบียนข้อมูลและกำหนดความสำคัญของข้อมูล
3. กำหนดสิทธิ์การเข้าถึงข้อมูลเท่าที่จำเป็นเท่านั้น
4. หากใช้คลาวด์ในการเก็บรักษาข้อมูลสำคัญ จะต้องศึกษา ทำความเข้าใจ และออกแบบการใช้งานให้เหมาะสม การกำหนดค่าพารามิเตอร์ควบคุมข้อมูล และมีความมั่นคงปลอดภัยเพียงพอที่จะเก็บรักษาข้อมูลสำคัญได้
5. ห้ามใช้บัญชีและรหัสผ่านร่วมกับผู้อื่นในการเข้าถึงข้อมูลต่าง ๆ ของส่วนตัวและองค์กร
6. พิจารณาการใช้ระบบการยืนยันตัวตนด้วยหลายปัจจัยสำหรับระบบสำคัญ
7. สำรองข้อมูลอยู่เสมอ จัดเก็บไฟล์สำรองออกจากระบบเครือข่าย production และกำหนดแผนในการทดสอบการกู้คืน
8. จำกัดการเข้าถึงจากภายนอกโดยอุปกรณ์ที่มีความปลอดภัย ด้วยสิทธิของบุคคลที่ได้รับอนุญาตและมีการเฝ้าระวังเสมอ
9. เลือกใช้เทคโนโลยีที่เหมาะสม และหมั่นอัปเดตอยู่สม่ำเสมอ

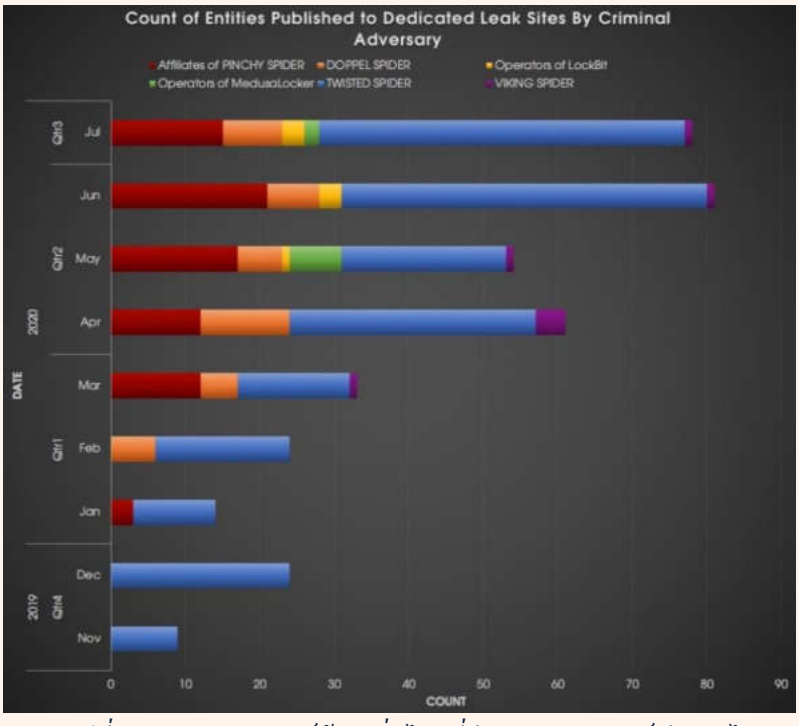
เอกสารอ้างอิง

1. https://www2.deloitte.com/ba/en/pages/risk/articles/High-Technology-Sector.html
2. https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
3. https://www.cybintsolutions.com/cyber-security-facts-stats/
4. https://www.cdnetworks.com/cloud-security-blog/the-5-industries-most-vulnerable-to-cyber-attacks/
5. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/threat-landscape-mapping-infographic-2020
6. https://content.fireeye.com/predictions/rpt-security-predictions-2021

มัลแวร์เรียกค่าไถ่ (Ransomware)

ปี 2020 ถือได้ว่าเป็นปีแห่งมัลแวร์เรียกค่าไถ่ ด้วยมีมัลแวร์เรียกค่าไถ่หลากหลายสายพันธุ์สร้างความเสียหายแก่องค์กร บริษัทมากมายทั่วโลก รวมถึงประเทศไทยด้วย ซึ่งแนวโน้มของมัลแวร์เรียกค่าไถ่ในปีนี้เปลี่ยนแปลงไปอย่างมากจากปีก่อน ๆ ดังนี้

1. **มัลแวร์เรียกค่าไถ่เปิดเผยข้อมูลของเหยื่อเพิ่มขึ้น** จากรายงานประจำปีของ TB-CERT ปี 2019 หน้าที่ 34 [1] ได้คาดการณ์ไว้ว่าปี 2020 นี้มัลแวร์เรียกค่าไถ่นั้น นอกจากจะเข้ารหัสข้อมูลแล้ว ยังจะเปิดเผยข้อมูลของเครื่องที่ถูกมัลแวร์เรียกค่าไถ่คุกคามสู่สาธารณะด้วย จากรายงานของ Crowdstrike [16] เหตุการณ์ข้อมูลรั่วไหลที่เกิดจากมัลแวร์เรียกค่าไถ่ในช่วงปีที่ผ่านมาเป็นจำนวนมาก ดังรูปที่ 12 ซึ่งพบว่าในช่วงพฤศจิกายน 2019 ถึง กรกฎาคม 2020 มัลแวร์เรียกค่าไถ่ TWISTE SPIDER (หรือมัลแวร์เรียกค่าไถ่ Maze) โพสต์ข้อมูลของผู้เสียมากกว่า 230 ราย รองลงมาคือ PINCHY SPIDER (หรือ Sodinokibi) พบว่ามีการโพสต์ข้อมูลของผู้เสียหายมากกว่า 80 รายในช่วงเวลาดังกล่าว แสดงให้เห็นว่าวัตถุประสงค์ของกลุ่มมัลแวร์เรียกค่าไถ่มีแนวโน้มในการโพสต์ข้อมูลของผู้เสียหายมากขึ้น ทำให้ผู้เสียหายถูกข่มขู่ด้วยสาเหตุจากการถูกเข้ารหัสข้อมูล อีกทั้งยังอาจถูกข่มขู่ที่จะเปิดเผยข้อมูลได้อีกด้วย



รูปที่ 12 จำนวนเหตุการณ์ข้อมูลรั่วไหลที่มีสาเหตุจากมัลแวร์เรียกค่าไถ่ตั้งแต่พฤศจิกายน 2019 ถึง กรกฎาคม 2020 [2]

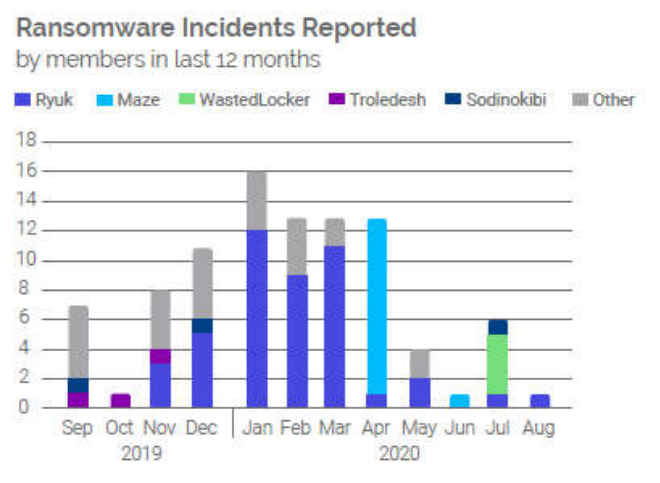
2. **Ransomware-As-A-Service (RaaS) หรือบริการให้เช่าใช้มัลแวร์เรียกค่าไถ่** กล่าวคือ Threat Actor จะสร้างมัลแวร์เรียกค่าไถ่รวมถึงระบบที่เกี่ยวข้องและสร้างเป็นบริการ จากนั้นจะเผยแพร่ต่อไปยังThreat Actor กลุ่มอื่นๆ สามารถนำไปใช้ และนำค่าไถ่ที่ได้มาแบ่งกัน จากรายงานของมหาวิทยาลัยคาร์เนกี้เมลลอน (Carnegie Mellon University) [3] และ Coveware [4] มัลแวร์เรียกค่าไถ่ที่พบในไตรมาสที่ 4 ของปี 2562 จนถึงไตรมาสที่ 1 ของปี 2020 ในตารางที่ 1 พบว่ามีมัลแวร์เรียกค่าไถ่ 4 สายพันธุ์จาก 10 สายพันธุ์ที่พบมากที่สุด ได้แก่ มัลแวร์เรียกค่าไถ่ Sodinokibi Phobos Dharma และ GlobeImposter ต่างก็ให้บริการ Ransomware-As-A-Service ทั้งสิ้น แสดงให้เห็นว่าแนวโน้มที่Threat Actorจะสร้างมัลแวร์เรียกค่าไถ่และเปิดให้บริการ Ransomware-As-A-Service มีเพิ่มขึ้น และในอนาคตมัลแวร์เรียกค่าไถ่ใหม่จะใช้เวลาในการพัฒนาลดลง ใช้ต้นทุนต่ำลง โดยใช้ระบบโครงสร้างของมัลแวร์เรียกค่าไถ่ในกลุ่มนี้

ตารางที่ 1 แสดงรายชื่อสายพันธุ์ของมัลแวร์เรียกค่าไถ่ 10 อันดับแรกที่ยังมีการโจมตีในไตรมาสที่ 1 ของปี 2020 [3][4]

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2019
1	Sodinokibi	26.7%	-
2	Ryuk	19.6%	-
3	Phobos	7.8%	-
3	Dharma	7.8%	+1
5	Mamba	4.8%	+4
6	GlobeImposter	4.4%	+5
7	Snatch	2.6%	+1
8	IEncrypt	2.2%	+2
8	777	2.2%	+8
8	MedusaLocker	2.2%	+8

3. **องค์กรด้านสาธารณสุขกลายเป็นเป้าหมายอันดับต้นในการโจมตีในปีนี้** อาจจะด้วยสาเหตุที่ปีนี้มีการแพร่ระบาดของไวรัส COVID-19 จึงทำให้ Threat Actor อาศัยเหตุการณ์ดังกล่าวส่งมัลแวร์เรียกค่าไถ่ไปพร้อมกับคำเชิญชวนต่าง ๆ เพื่อหลอกล่อให้เปิดมัลแวร์ดังกล่าว ซึ่งในปีนี้ทาง CISA FBI และ HHS ประเทศสหรัฐอเมริกาได้ออกประกาศแจ้งเตือนไปยังองค์กรด้านสาธารณสุขเกี่ยวกับการพบมัลแวร์ Trickbot และ Bazarloader ที่สามารถเรียกค่าไถ่ ขโมยข้อมูล และทำให้บริการด้านสาธารณสุขหยุดชะงัก [9]

4. **มัลแวร์เรียกค่าไถ่สามารถแพร่กระจายผ่านมัลแวร์ในตระกูล Trickbot และ Emotet** มัลแวร์ที่แพร่กระจายผ่านทางอีเมลมากที่สุดในโลก [5] เช่น มัลแวร์เรียกค่าไถ่ Ryuk ซึ่งเมื่อวิเคราะห์จากรายงานของ FS-ISAC [6] ที่ได้รับการแจ้งเหตุการณ์จากสมาชิกพบว่าในช่วงปลายปี 2019 จนถึงต้นปี 2020 พบการโจมตีจากมัลแวร์เรียกค่าไถ่ชนิดนี้เป็นจำนวนมากที่สุดเมื่อเทียบกับมัลแวร์เรียกค่าไถ่อื่น ดังรูปที่ 13 เนื่องจากความสามารถในการแพร่กระจายผ่านทางอีเมลของ Trickbot และ Emotet ทำให้มัลแวร์เรียกค่าไถ่ Ryuk สามารถแพร่กระจายเป็นวงกว้าง และสร้างความเสียหายอย่างมากมาย โดยเฉพาะองค์กรภาครัฐและองค์กรด้านสาธารณสุขในประเทศสหรัฐอเมริกา จนทำให้องค์กรด้านความมั่นคงออกมาประกาศแจ้งเตือนด้วย [5]

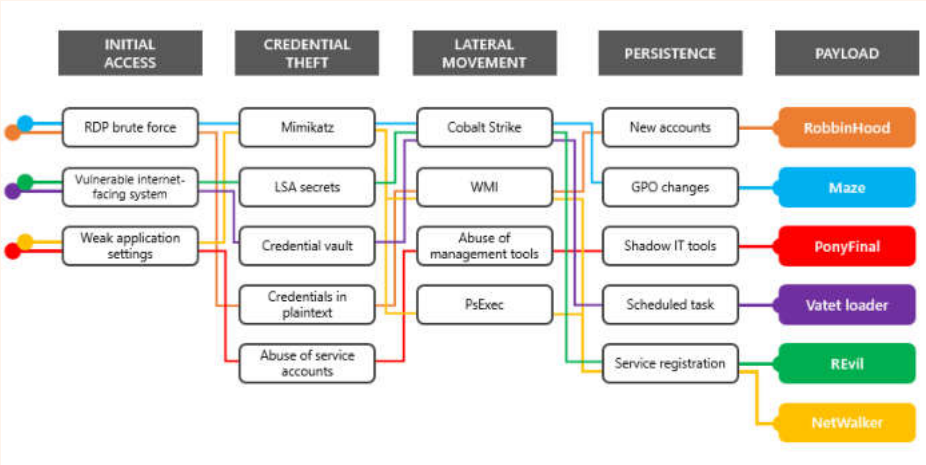


รูปที่ 13 แสดงกราฟเหตุการณ์มัลแวร์เรียกค่าไถ่ที่สมาชิกของ FS-ISAC แจ้งเหตุการณ์ [6]

เหตุการณ์มัลแวร์เรียกค่าไถ่ที่น่าสนใจ

ในช่วงต้นปี 2020 มัลแวร์ **Ryuk** มีการโจมตีอย่างรุนแรงในประเทศสหรัฐอเมริกา หนึ่งในเหตุการณ์สำคัญของปีนี้คือการโจมตีระบบคอมพิวเตอร์ขององค์กรที่จัดการเกี่ยวกับการเดินเรือแห่งหนึ่งภายใต้ Maritime Transportation Security Act (MTSA) จนศูนย์ป้องกันชายฝั่งสหรัฐ ฯ หรือ U.S. Coast Guard (USCG) ประกาศแจ้งเตือนเกี่ยวกับมัลแวร์เรียกค่าไถ่ Ryuk นี้ ซึ่งจากการตรวจสอบพบอีเมลหลอกลวงที่แนบลิงก์อันตรายส่งเข้ามายังบุคลากรขององค์กร ส่งผลให้มัลแวร์ดังกล่าวแพร่ไปยังระบบคอมพิวเตอร์และเข้ารหัสไฟล์ต่าง ๆ บนระบบ ทำให้ต้องปิดระบบนานถึง 30 ชั่วโมง นอกจากนี้เป้าหมายของมัลแวร์เรียกค่าไถ่นี้ยังมีองค์กรในกลุ่มภาคสาธารณสุขในประเทศสหรัฐอเมริกา จน CIA, FBI, และ the Department of Health and Human Services ประกาศแจ้งเตือนในช่วงปลายปีด้วย อย่างไรก็ตามในช่วงปลายปีพบการพัฒนารูปแบบการโจมตีของ Ryuk คือได้นำช่องโหว่ Zerologon ซึ่งเป็นช่องโหว่ใหม่ระดับ critical ของระบบปฏิบัติการ Microsoft Windows ทุกรุ่น มาใช้ในการแพร่กระจายด้วย

ส่วนในช่วงกลางปีมัลแวร์เรียกค่าไถ่ **Maze** โจมตีองค์กรต่าง ๆ พร้อมทั้งเปิดเผยข้อมูลผ่านทางเว็บไซต์ Microsoft [7] ยังมีการระบุว่าเป้าหมายหลักของ Maze คือการโจมตีกลุ่มผู้ให้บริการ (Managed Service Provider) เพื่อใช้เป็นช่องทางในการเข้าถึงผู้ใช้บริการในกลุ่มธุรกิจนี้ด้วย จากรูปที่ 14 มัลแวร์เรียกค่าไถ่ Maze มีลักษณะการโจมตีโดยการเข้าถึงระบบที่มีความเสี่ยงด้วยการโจมตีผ่านเซอร์วิส Remote Desktop (RPD) ซึ่งตั้งค่าไว้อย่างไม่ปลอดภัย หรืออาจใช้วิธีการเดารหัสผ่าน (Bruteforce) จากนั้นใช้โปรแกรม Mimikatz ในการระบุหาข้อมูลสำหรับยืนยันตัวตนในระบบ และจะถูกใช้เพื่อเข้าถึงระบบอื่นๆ อีกทั้งยังสามารถเคลื่อนย้ายตัวเองในระบบภายในขององค์กรด้วย Cobalt Strike ซึ่งประกอบด้วยเทคนิคการโจมตีแบบ Pass-the-Hash, WinRM หรือการใช้เซอร์วิส PsExec ในการเข้าถึงด้วยข้อมูลสำหรับยืนยันตัวตนที่ได้มา นอกจากนี้ Maze ยังสามารถแก้ไขการตั้งค่าใน Group Policy หลายรายการเพื่อช่วยอำนวยความสะดวกในการโจมตีอีกด้วย



รูปที่ 14 แสดงลักษณะวิธีการโจมตีของมัลแวร์เรียกค่าไถ่ต่าง ๆ [7]

มัลแวร์เรียกค่าไถ่ **WastedLocker** ซึ่งเหตุการณ์สำคัญในปีนี้คือการโจมตีบริษัท Garmin ส่งผลให้ต้องปิดบริการเป็นการชั่วคราวเพื่อแก้ไขสถานการณ์ดังกล่าว โดยมีข่าวว่าการเรียกค่าไถ่ข้อมูลครั้งนี้มีมูลค่าถึง 10 ล้านเหรียญสหรัฐ และหลังจากนั้น 4 วันทางบริษัท Garmin ก็ประกาศว่าบริษัทได้เริ่มกู้คืนบริการต่าง ๆ กลับสู่ภาวะปกติ อีกทั้ง WastedLocker เป็นมัลแวร์เรียกค่าไถ่ที่มุ่งโจมตีระดับองค์กรขนาดใหญ่ (Enterprise-Targeting Ransomware) ซึ่งเชื่อกันว่าบริษัท Garmin ยินยอมจ่ายค่าไถ่เพื่อให้ได้เครื่องมือในการถอดรหัส โดยที่ทางบริษัทไม่ได้มีการเปิดเผยใด ๆ เกี่ยวกับเรื่องนี้ เมื่อศึกษาถึงวิธีการแพร่กระจายของมัลแวร์เรียกค่าไถ่ชนิดนี้พบว่าใช้เทคนิคการโจมตีไปยังเว็บไซต์ด้วย SocGholish ซึ่งเป็น Framework ในการโจมตีที่ถูกพัฒนาด้วย JavaScript เมื่อเหยื่อหลงเชื่อและเข้าไปยังเว็บไซต์ดังกล่าว มัลแวร์จะแสดงข้อความให้ดาวน์โหลดอัปเดตเว็บเบราว์เซอร์เมื่อเหยื่อหลงเชื่อจะถูกดาวน์โหลดและติดตั้งมัลแวร์เรียกค่าไถ่อย่างง่ายดาย

มัลแวร์เรียกค่าไถ่ Sodinokibi หรือ REvil เป็นมัลแวร์เรียกค่าไถ่ที่ดำเนินการในลักษณะของการให้เช่ามัลแวร์เพื่อโจมตี (Ransomware-As-A-Service หรือ RaaS) โดยเงินที่ได้จากการเรียกค่าไถ่จะถูกแบ่งกันระหว่างผู้เช่าและผู้ให้เช่ามัลแวร์ โดยเน้นโจมตีองค์กรและยังไม่มีตัวถอดรหัสที่สามารถถอดรหัสได้ฟรีโดยไม่เสียเงินค่าไถ่ ในช่วงที่ผ่านมากลุ่มเบื้องหลัง Sodinokibi มีการพัฒนาไปอีกขั้นด้วยการสนับสนุนให้ผู้เช่ามัลแวร์ขโมยข้อมูลออกมาก่อนจะทำการปล่อยมัลแวร์ให้เข้ารหัส เพื่อในกรณีที่องค์กรตัดสินใจไม่ยอมจ่ายค่าไถ่กู้คืนไฟล์จะข่มขู่เพื่อปล่อยข้อมูลเพิ่มเติม ทำให้กลายเป็นเหตุการณ์ข้อมูลหลุดซึ่งอาจจะนำไปสู่การผิดกฎหมายคุ้มครองข้อมูลส่วนบุคคลอย่าง GDPR หรือกฎหมายในลักษณะเดียวกัน อาจนำไปสู่การปรับเงินที่สูงกว่าค่าไถ่มาก กดดันให้องค์กรตัดสินใจจ่ายค่าไถ่แทน จากข้อมูลการวิจัยจากผู้ให้บริการด้านความมั่นคงปลอดภัยพบการโจมตีจาก Sodinokibi ถึง 29.4% จากการโจมตีทั้งหมด และการติดมัลแวร์เรียกค่าไถ่ส่วนใหญ่ (57.4%) เกิดจากการโจมตีผ่าน RDP [8]

สาเหตุที่องค์กรมักได้รับผลกระทบจากการถูกมัลแวร์เรียกค่าไถ่โจมตี

1. **Awareness** ผู้ใช้งานขาดความตระหนักถึงการเปิดอ่านอีเมลฟิชชิง และเปิดอีเมลที่มีมัลแวร์แนบมา นอกจากนี้ยังมีการใช้รหัสผ่านเดียวกันในหลายแอปพลิเคชัน ทำให้เมื่อ Threat Actor ล่วงรู้รหัสผ่าน ก็สามารถยึดครองบัญชีในระบบอื่น ๆ ได้
2. **Protection** ทางองค์กรขาดการรักษาความปลอดภัยทางอีเมล เช่นระบบกรองสแปมเมล หรือกรองมัลแวร์ผ่านทางอีเมลเป็นต้น เมื่อมัลแวร์เรียกค่าไถ่ถูกส่งมาทางอีเมล ทำให้มัลแวร์ถูกส่งผ่านทางอีเมลมายังเจ้าหน้าที่ในองค์กรได้ รวมถึงโปรแกรมป้องกันมัลแวร์ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์นั้นหมดอายุ จึงไม่สามารถอัปเดตให้ตรวจจับมัลแวร์ใหม่ ๆ ได้
3. **Privilege** ผู้ใช้งานหลายคนมีสิทธิ์ของ Local admin หลังจากที่มัลแวร์ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานที่มีสิทธิ์ที่สามารถเข้าถึงระบบสำคัญ ทำให้มัลแวร์มีสามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์และเซิร์ฟเวอร์อื่นๆที่สำคัญด้วยสิทธิ์ที่มีระดับสูง เช่น ในเซิร์ฟเวอร์ที่ให้บริการ Active Directory หรือฐานข้อมูล เป็นต้น อีกทั้งบางองค์กรอนุญาตให้บุคลากรใช้งาน VPN ไปยังระบบสำคัญได้ และหากไม่มีการป้องกันที่ดีพอ ทำให้มัลแวร์เรียกค่าไถ่อาจสามารถเดาสุ่มรหัสผ่านของบัญชี VPN และเข้าถึงระบบงานสำคัญได้
4. **Backup** องค์กรขาดการสำรองข้อมูลที่เหมาะสม เช่น นโยบาย รวมถึงสื่อที่ใช้ในการสำรอง การรักษาความปลอดภัยข้อมูลในระบบสำรอง และระยะเวลาการเก็บข้อมูล รอบการเก็บข้อมูล เทคโนโลยีที่ใช้ นอกจากนี้ในหลายองค์กรยังขาดการทดสอบกู้คืนข้อมูลที่ถูกสำรองไว้อีกด้วย
5. **Resource** การใช้ฮาร์ดแวร์ และซอฟต์แวร์ที่เก่าเกินไป คอมพิวเตอร์ที่ใช้ในองค์กรบางครั้งอาจมีบางเครื่องที่ติดตั้งระบบปฏิบัติการวินโดวส์ที่ล้าสมัย เช่น XP หรือ เก่ากว่านั้น และไม่สามารถอัพเกรดได้เนื่องจากฮาร์ดแวร์ที่เก่าเกินไป รวมทั้งมีการเปิดใช้งานบริการที่ไม่จำเป็น เช่น Remote Desktop Protocol ทำให้Threat Actorสามารถใช้ช่องทางดังกล่าวในการแพร่กระจายมัลแวร์ได้

วิธีการป้องกันมัลแวร์เรียกค่าไถ่

1. สร้างความตระหนักด้านความมั่นคงปลอดภัยให้แก่ผู้ใช้งานในองค์กรเรื่องความเสี่ยงที่อาจเกิดขึ้นจากมัลแวร์เรียกค่าไถ่
2. หากประสบปัญหาภัยคุกคามมัลแวร์เรียกค่าไถ่ในองค์กร ไม่ควรจ่ายเงินค่าไถ่ เนื่องจากการจ่ายเงินเป็นการกระตุ้นให้Threat Actorกลับมาโจมตีองค์กรได้ อีกทั้งอาจจะไม่สามารถแก้ไขได้
3. ตรวจสอบการสำรองข้อมูล (Backup) โดยเฉพาะระบบที่มีข้อมูลสำคัญว่ายังคงทำงานอย่างปกติ เนื่องจากเพื่อให้สามารถกู้คืนระบบได้หากถูกมัลแวร์เรียกค่าไถ่คุกคาม
4. ตรวจสอบและติดตั้งโปรแกรมป้องกันมัลแวร์ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องภายในองค์กร ทั้งเครื่องเซิร์ฟเวอร์และคอมพิวเตอร์ของพนักงาน รวมถึงการอัปเดตล่าสุดด้วย

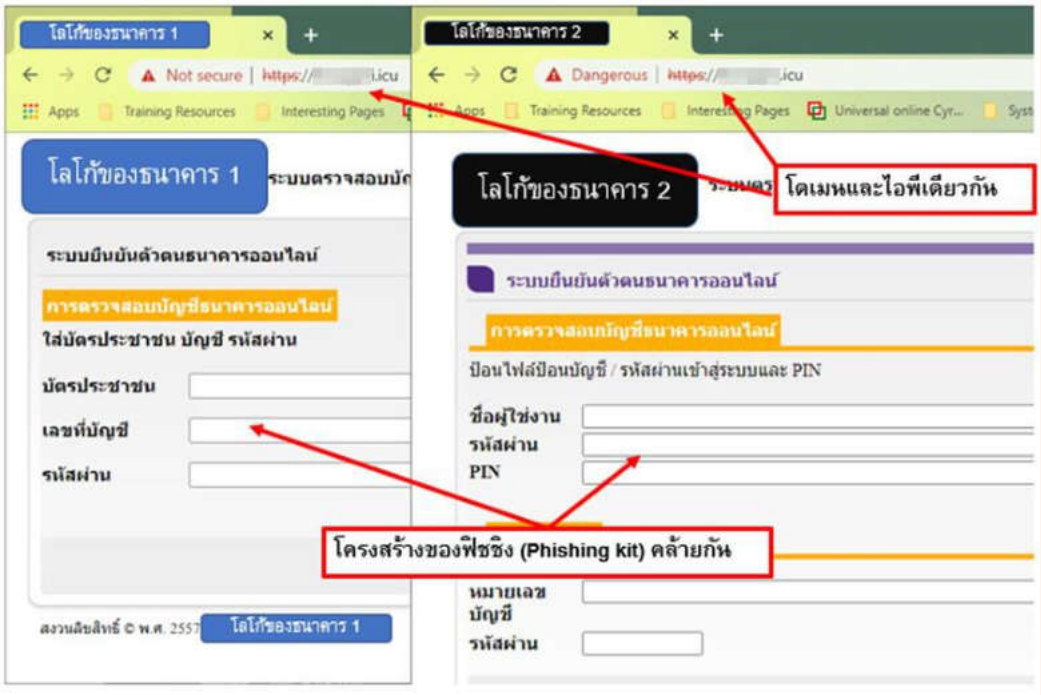
5. เฝ้าระวังและปิดกั้นอีเมลที่น่าสงสัย โดยเพิ่มข้อมูลอีเมลที่น่าสงสัยให้กับระบบกรองอีเมลขององค์กร หรือการใช้โปรแกรมป้องกันมัลแวร์ที่ระบบ E-mail gateway เป็นต้น เช่นลักษณะของไฟล์แนบ หรือลิงก์ที่อยู่ในเนื้อความของอีเมล เป็นต้น เพื่อป้องกันอีเมลที่แนบมัลแวร์เรียกค่าไถ่นี้ถูกส่งเข้ามายังองค์กร
6. ตรวจสอบประวัติการเรียกโพรเซส หรือประวัติการเรียกใช้งานสคริปต์ (เช่น PowerShell เป็นต้น) หากมีการเก็บล็อกเหล่านี้ไว้ ว่าพบสคริปต์ในการเชื่อมต่อหรืออัพโหลดไปยังเซิร์ฟเวอร์ FTP เพื่อให้แน่ใจว่าไม่มีข้อมูลรั่วไหลจากองค์กร
7. พิจารณาปิดกั้นการใช้งาน Remote Desktop Protocol และ Critix Web Portal จากภายนอก หากจำเป็นต้องใช้งานควรจะมีมาตรการควบคุมเพิ่มเติม เช่น Whitelist หรือระบบการยืนยันตัวตนด้วยหลายปัจจัย (Multi Factor Authentication)
8. เฝ้าระวังการเชื่อมต่อไปยังเครื่อง C2 และพิจารณาปิดกั้นหากพบว่ามีเครือข่ายภายในองค์กรพยายามติดต่อออกไปยังเครื่อง C2 โดยตรวจสอบที่ไฟร์วอลล์ (Firewall) และพร็อกซี่ (Proxy) ขององค์กร เป็นต้น
9. อัปเดตแพทช์ (Patch) ของซอฟต์แวร์และระบบปฏิบัติการที่ใช้ ให้เป็นเวอร์ชันล่าสุดอยู่เสมอ โดยเฉพาะช่องโหว่บน Citrix Application Delivery Controller (CVE-2019-19781) และช่องโหว่บน Pulse Secure VPN (CVE-2019-11510) รวมถึงระบบต่าง ๆ ภายในองค์กร ทั้งเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่าย
10. กำหนดให้มีการเปลี่ยนรหัสผ่านของบัญชีผู้ใช้งานและผู้ดูแลระบบให้ยากต่อการคาดเดาอยู่สม่ำเสมอ รวมถึงพิจารณาการใช้ระบบการยืนยันตัวตนด้วยหลายปัจจัย (Multi factor authentication)
11. ตรวจสอบบัญชีผู้ใช้งานที่มีพฤติกรรมการล็อกอินที่ผิดปกติ เช่น ล็อกอินนอกเวลางาน หรือล็อกอินจากต่างประเทศ (หากผู้ใช้ไม่ได้เดินทางไปต่างประเทศ) ซึ่งเหตุการณ์เหล่านี้อาจเกิดจาก Threat Actor สามารถเข้าควบคุมบัญชีได้ เป็นต้น
12. ตรวจสอบและยกเลิกบัญชีผู้ใช้งานที่เป็น Default ของระบบ บัญชีผู้ใช้งานที่น่าสงสัย และบัญชีผู้ใช้งานที่ไม่ได้ใช้งานแล้ว เพื่อลดความเสี่ยงที่Threat Actorจะอาศัยบัญชีเหล่านั้นในการล็อกอินเพื่อโจมตีระบบ

เอกสารอ้างอิง

1. https://www.tba.or.th/wp-content/uploads/2020/02/tb-cert-Annual-Report-2019.1.pdf
2. https://www.crowdstrike.com/blog/double-trouble-ransomware-data-leak-extortion-part-1/
3. https://insights.sei.cmu.edu/sei_blog/2020/10/ransomware-as-a-service-raas-threats.html
4. https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
5. https://us-cert.cisa.gov/ncas/alerts/aa20-302a
6. https://www.fsisac.com/hubfs/Campaigns/RansomwareReport-2020/FS-ISAC_Ransomware2020.pdf
7. https://www.microsoft.com/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk/
8. https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate

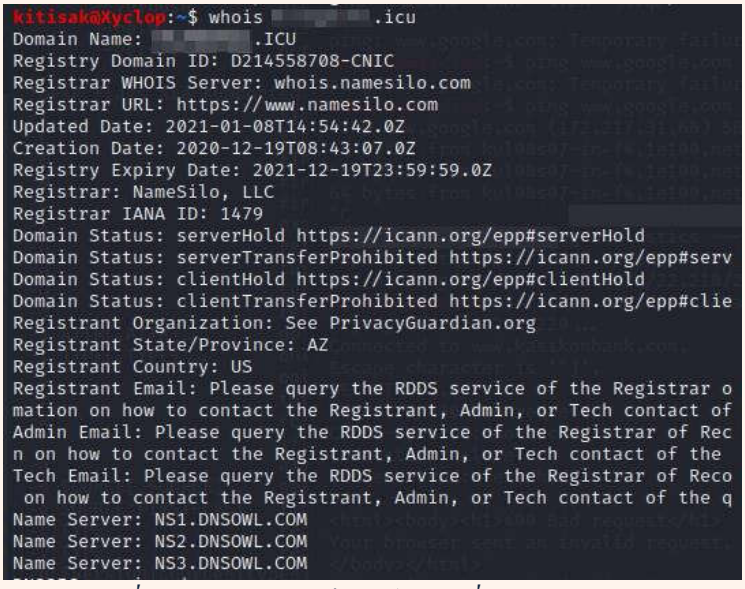
การเปลี่ยนแปลงเทคนิคของการโจมตีด้วยฟิชชิง

จากเหตุการณ์ฟิชชิงที่ TB-CERT ได้รับแจ้งเหตุการณ์ในปี 2020 มีจำนวนทั้งสิ้น 25 เหตุการณ์ ซึ่งพบว่ามีจำนวนเว็บไซต์ฟิชชิง 40 เว็บไซต์ (ในเหตุการณ์การณ์หนึ่งๆ อาจจะมีเว็บไซต์ฟิชชิงมากกว่า 1 เว็บไซต์) ในช่วงเดือนพฤศจิกายนถึงธันวาคมเป็นช่วงที่ได้รับแจ้งเหตุการณ์มากที่สุด และพบว่าในช่วงดังกล่าว Threat Actor ใช้เทคนิคการส่งลิงก์ฟิชชิงผ่านทางข้อความ SMS หรือบางครั้งจะเรียกว่า (SMS-Phishing หรือ Smishing) ที่มีผลกระทบต่อลูกค้าของธนาคารหลายแห่ง จากการวิเคราะห์ข้อมูลสันนิษฐานได้ว่าเป็น Threat Actor กลุ่มเดียวกัน เนื่องจากมีการใช้ชุดโปรแกรมฟิชชิง (Phishing Kit) ที่มีลักษณะคล้ายกัน อีกทั้งยังมีการใช้บริการจากผู้ให้บริการและหมายเลขไอพีของเว็บเซิร์ฟเวอร์เดียวกันอีกด้วย ดังรูปที่ 15 (ภาพประกอบในเอกสารนี้เป็นภาพเว็บไซต์ที่ Threat Actor สร้างขึ้นเพื่อหลอกเหยื่อ มิได้เกี่ยวข้องกับบริการของธนาคารใด ๆ)



รูปที่ 15 แสดงเว็บฟิชชิงที่สันนิษฐานว่าน่าจะเป็นฝีมือของ Threat Actor กลุ่มเดียวกัน

จากรูปที่ 16 เมื่อวิเคราะห์โดเมนของเว็บไซต์ฟิชชิงพบกว่าถูกจดทะเบียนโดย Namesilo และถูกจดเมื่อวันที่ 19 ธันวาคม 2020 ซึ่งเป็นช่วงเวลาที่พบฟิชชิงดังกล่าว เนื่องจาก Namesilo นั้นมีค่าใช้จ่ายในการจดทะเบียนโดเมนถูกและมีนโยบายรักษาความลับของลูกค้าที่จะไม่เปิดเผยข้อมูลของผู้จดทะเบียน ทำให้ Threat Actor สามารถปิดบังตัวตนได้ จึงจูงใจให้ Threat Actor ไปจดทะเบียนโดเมนที่ Namesilo



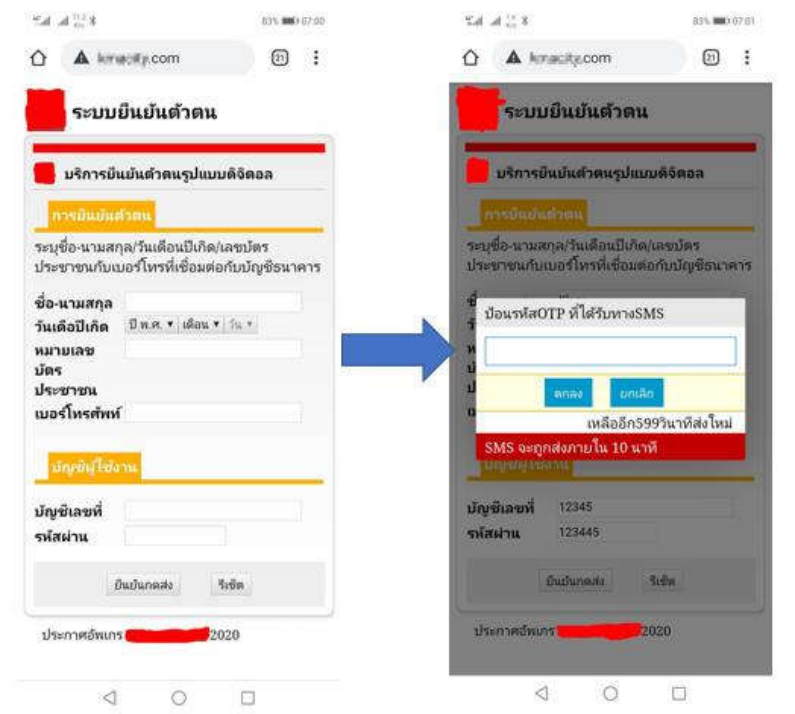
รูปที่ 16 แสดงข้อมูลที่ได้จาก whois ของเว็บไซต์ฟิชชิง ที่ถูกจดทะเบียนโดเมนโดย Namesilo

จุดมุ่งหมายหลักของ Threat Actor นั้นต้องการที่จะขโมยเงินจากบัญชีของเหยื่อผ่านทาง Mobile Banking โดยหลอกขโมยข้อมูลของเหยื่อและเพื่อที่จะนำไปใช้เปลี่ยนแปลงอุปกรณ์ในการเข้าถึงบัญชีใน Mobile Banking อีกทั้งรูปแบบการหลอกลวงนั้นเปลี่ยนแปลงจากการส่งผ่านทางอีเมล มาใช้ข้อความ SMS เนื่องจากบนโทรศัพท์มือถือจะไม่มีกลไกการตรวจสอบลิงก์ฟิชชิงบนข้อความ SMS อีกทั้งชื่อผู้ส่งข้อความ (SMS Sender Name) นั้นยังใช้ชื่อที่ใกล้เคียงกับชื่อผู้ส่ง SMS ที่ธนาคารใช้จึงทำให้เหยื่อหลงเชื่อได้ง่ายอีกด้วย

ดังตัวอย่างข้อความฟิชชิงในรูปที่ 17 ซึ่งเมื่อเหยื่อกดลิงก์ฟิชชิงจะเข้าถึงเว็บไซต์ที่แอบอ้างว่าเป็นเว็บของธนาคารเพื่อหลอกลวงข้อมูลส่วนบุคคล เช่น ชื่อนามสกุล วันเดือนปีเกิด เลขที่บัตรประชาชน หมายเลขโทรศัพท์สำหรับส่ง SMS OTP ชื่อบัญชี Mobile Banking และรหัสผ่าน จากนั้นเมื่อผู้ใช้งานกรอกข้อมูลทั้งหมดแล้ว จะมี SMS OTP ส่งมาให้ยังโทรศัพท์มือถือของเหยื่อ และในเว็บไซต์ฟิชชิงจะทำการขอรหัส OTP ดังกล่าวด้วย ทำให้สามารถรวบรวมข้อมูลของผู้ใช้งานเพียงพอที่จะนำไปใช้เปลี่ยนแปลงอุปกรณ์เพื่อเข้าถึงบัญชี Mobile Banking และทำธุรกรรมด้านการเงินแทนได้

รูปที่ 17 แสดงข้อความฟิชชิงผ่านทาง SMS

เมื่อเข้าไปยังเว็บไซต์ฟิชชิงดังกล่าว (ควรระวังในการเข้าหน้าเว็บไซต์ฟิชชิงด้วยตนเอง) พบว่าหน้าฟิชชิงนั้นมีการขอข้อมูลส่วนบุคคล รวมถึงชื่อบัญชี Mobile banking และรหัสผ่าน จากนั้นจะทำการส่ง Request ไปขอ SMS OTP จากเว็บไซต์ของธนาคารจริง เพื่อส่งให้เหยื่อกรอก SMS OTP ที่ได้รับมาบนหน้าเว็บฟิชชิงต่อไป ดังรูปที่ 18 จากนั้น Threat Actor จะทำการเปิดใช้งานบัญชี Mobile Banking ของเหยื่อบนเครื่องโทรศัพท์ของ Threat Actor โดยใช้ข้อมูลทั้งหมดที่รวบรวมได้ แล้วจึงทำการโอนเงินของเหยื่อต่อไป

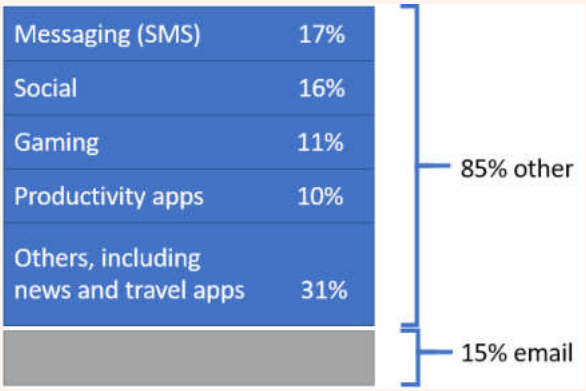


รูปที่ 18 แสดงหน้าจอของเว็บไซต์ฟิชชิง

วิเคราะห์เทคนิคและแรงจูงใจของการโจมตีด้วยฟิชชิง

1. วิธีการเข้าถึงลูกค้า

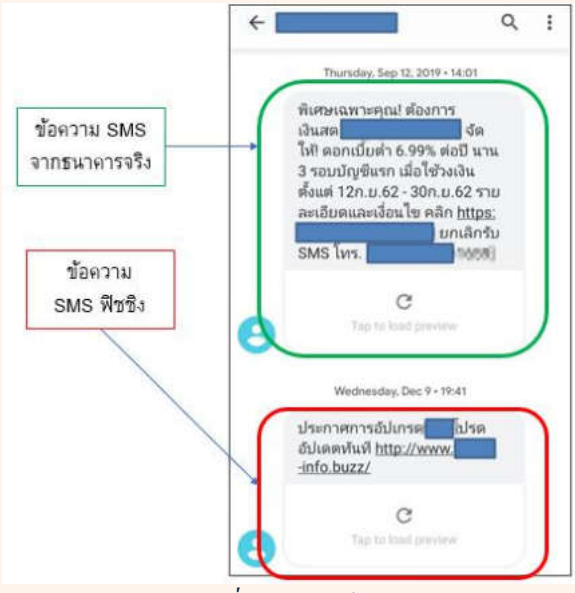
ปัจจุบันThreat Actor เปลี่ยนพุ่งเป้าหมายไปยังผู้ใช้งานโทรศัพท์มือถือเพิ่มมากขึ้น โดยจากรายงานของ Verizon [1] พบว่า 85% ของฟิชชิงทั้งหมด เป็นฟิชชิงที่ถูกส่งมายังบนโทรศัพท์มือถือทางข้อความ SMS นั้นมีถึง 17% เครือข่ายสังคมออนไลน์ (Social Media) 16% และเกมส์ 11% ดังรูปที่ 19 ผู้ใช้งานโทรศัพท์มือถือมีโอกาสถูกหลอกให้กรอกข้อมูลผ่านเว็บฟิชชิงมากขึ้น ส่งผลทำให้แนวโน้มที่ Threat Actor นั้นอาศัยการส่งฟิชชิงมายังโทรศัพท์มือถือมีเพิ่มขึ้น การส่งผ่านช่องทาง SMS เป็นช่องทางหลักนั้น เนื่องจากโทรศัพท์มือถือทุกเครื่องมีบริการดังกล่าวอยู่แล้ว อย่างไรก็ตามบริการของเครือข่ายสังคมออนไลน์ก็ไม่ควรละเลยในการให้ความสำคัญและมีโอกาสที่ Threat Actor จะพยายามส่งข้อความฟิชชิงมายังช่องทางดังกล่าวได้อีกด้วย แต่ด้วยบริการเครือข่ายสังคมออนไลน์นั้นมีหลากหลายผู้ให้บริการและสามารถเข้าถึงผู้ใช้งานได้มาก ทำให้การส่งฟิชชิงด้วยช่องทางนี้มีสัดส่วนที่ใกล้เคียงกับ SMS ซึ่งควรที่จะต้องเฝ้าระวังติดตามเทคนิคที่กลุ่ม Threat Actor จะทำการหลอกลวงในช่องทางสังคมออนไลน์อีกด้วย



รูปที่ 19 แสดงสัดส่วนของฟิชชิงที่ถูกส่งมาตามช่องทางต่าง ๆ [1]

สาเหตุที่ Threat Actor ใช้ SMS เพื่อส่งฟิชชิงแทนการส่งอีเมล เนื่องจาก

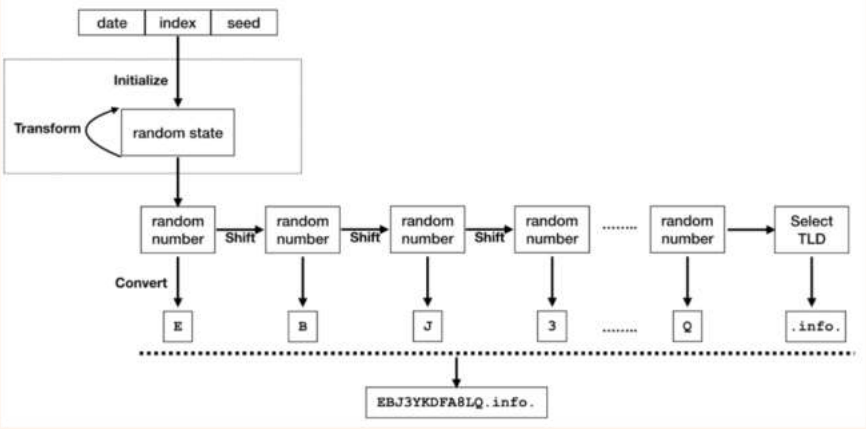
- สามารถเข้าถึงลูกค้าโดยตรงและเป็นช่องทางเดียวกับธนาคารที่ใช้ในการสื่อสารกับลูกค้าเพื่อแจ้งข้อมูลเกี่ยวกับการทำธุรกรรมและการประชาสัมพันธ์ และลักษณะการใช้งานที่เร่งรีบในการอ่านข้อความต่าง ๆ บนโทรศัพท์มือถือ ดังรูปที่ 20 แสดงตัวอย่างข้อความฟิชชิงที่เลียนแบบข้อความของธนาคารและส่งผ่านทาง SMS
- สามารถใช้บริการส่ง Bulk text message ซึ่งเป็นบริการส่งข้อความประชาสัมพันธ์ผ่านทาง SMS โดยใช้ชื่อที่ใกล้เคียงกับชื่อผู้ส่ง SMS ที่ธนาคารใช้
- สามารถหลบเลี่ยงการตรวจจับผ่านทางระบบคัดกรองฟิชชิง เนื่องจากการส่ง SMS ไม่มีระบบคัดกรองฟิชชิงเหมือนระบบอีเมล
- เหยื่อสามารถเข้าถึงเว็บไซต์ได้ง่ายเมื่อกดคลิกลิงก์ และสังเกตชื่อเว็บไซต์บนหน้าจอโทรศัพท์ได้ยากกว่าบนเว็บเบราว์เซอร์ในเครื่องคอมพิวเตอร์



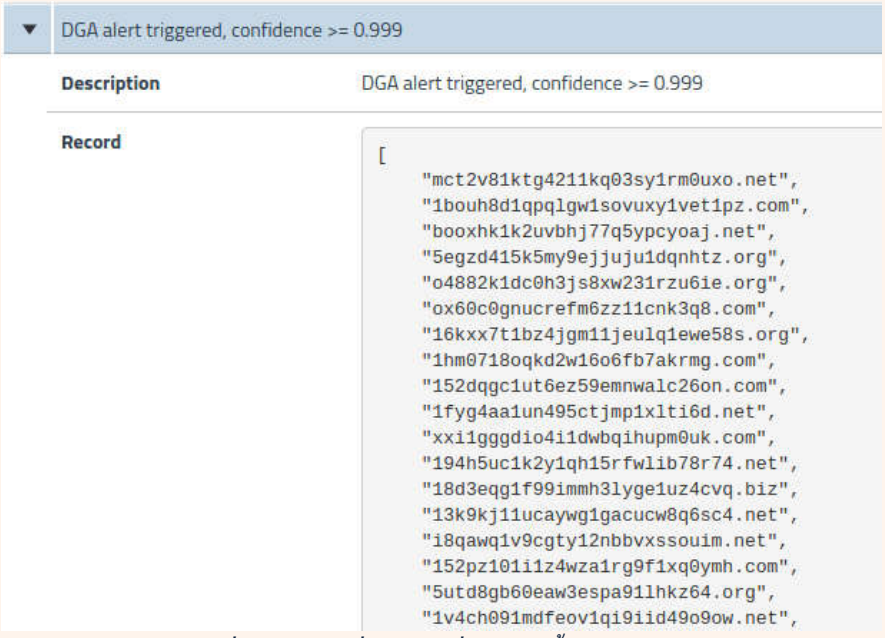
รูปที่ 20 แสดงข้อความฟิชชิงผ่าน SMS ที่เลียนแบบข้อความของธนาคารและส่งผ่านทาง SMS

2. เทคนิควิธีการสร้างชื่อโดเมนด้วย DGA

Threat Actor ใช้วิธี Domain Generation Algorithm (DGA) ในการสร้างชื่อโดเมน ซึ่งเทคนิคนี้เป็นการสร้างโดเมนเนมจำนวนหนึ่งขึ้นมาเพื่อให้ยากต่อการตรวจจับ และปิด (Takedown) ทั้งหมดได้ เทคนิคนี้มักจะถูกนำมาใช้ในการแพร่กระจายมัลแวร์ หรือเว็บไซต์อันตรายต่าง ๆ อีกด้วย จากรูปที่ 21 แสดงให้เห็นถึงกระบวนการสร้างชื่อโดเมน ทั้งนี้ขึ้นอยู่กับอัลกอริทึมที่ผู้เขียนโปรแกรมใช้ มีด้วยกันหลากหลายวิธี เช่น การอ้างอิงคำในพจนานุกรม การสุ่มใหม่ทั้งหมด หรือการกำหนดแพทเทิร์น เป็นต้น [3] และมีตัวอย่างโดเมนที่ถูกสร้างขึ้นดังรูปที่ 22



รูปที่ 21 แสดงกระบวนการของสร้างชื่อโดเมนด้วย Domain Generation Algorithm



รูปที่ 22 ตัวอย่างชื่อโดเมนที่ถูกสร้างขึ้นด้วย DGA [4]

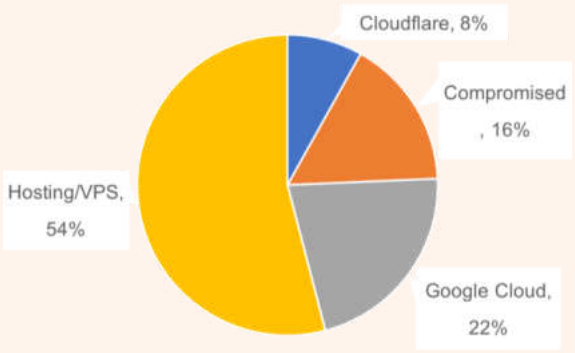
จากเหตุการณ์ฟิชชิงในช่วงเดือนพฤศจิกายนและธันวาคม พบว่า Threat Actor ใช้เทคนิคนี้ในการสร้างชื่อโดเมน โดยกำหนดให้มีตัวอักษรที่เป็นชื่อแอปพลิเคชันของธนาคาร หรือมีชื่อธนาคารอยู่ในโดเมน แล้วตามด้วยอักษร หรือตัวเลขที่ได้จากการสุ่มขึ้นมา

แรงจูงใจในการใช้ Domain Generator Algorithm ในการสร้างชื่อโดเมน

- สามารถหลบเลี่ยงการป้องกันการเข้าถึงจากการกำหนดชื่อโดเมนได้ง่าย
- ทำการปิด (Takedown) ได้ยากกว่า เนื่องจาก Threat Actor สามารถสร้างโดเมนใหม่ได้เรื่อย ๆ
- สามารถซ่อนหรือปิดบังรายชื่อโดเมนที่จะฝังอยู่ในโค้ดของมัลแวร์ได้ ทำให้นักวิเคราะห์ไม่สามารถคาดการณ์เกี่ยวกับชื่อของโดเมนได้

3. เทคนิคการสร้างเว็บไซต์ฟิชชิง

ในอดีต Threat Actor มักจะสร้างเว็บไซต์ฟิชชิงโดยการเจาะระบบอื่นและวางหน้าฟิชชิงไว้ ต่อมามีการใช้บริการของเว็บโฮสติ้งหรือ VPS (virtual private server) แต่ด้วยมีข้อจำกัดหลายด้าน เช่น ระยะเวลาที่ใช้ในการเจาะระบบ หรือการขอใช้บริการเว็บโฮสติ้งนั้นมีกระบวนการที่ยุ่งยากและอาจจะมีค่าใช้จ่าย ดังนั้นการใช้บริการคลาวด์สาธารณะจึงเป็นอีกวิธีที่ Threat Actor เลือกใช้ โดยประเมินจากเหตุการณ์ฟิชชิงที่ได้รับแจ้งพบว่ามีการใช้บริการคลาวด์สาธารณะ อย่าง Cloudflare หรือ Google Cloud ในการเปิดเว็บไซต์ฟิชชิง ดังรูปที่ 23



รูปที่ 23 แสดงสัดส่วนของประเภทการโฮสต์เว็บฟิชชิงในปี 2563

(ที่มา: ข้อมูลสถิติจากเหตุการณ์ฟิชชิงที่ TB-CERT ได้รับแจ้งในปี 2020 จำนวน 25 เหตุการณ์ ซึ่งพบเว็บไซต์ฟิชชิง จำนวน 40 เว็บไซต์)

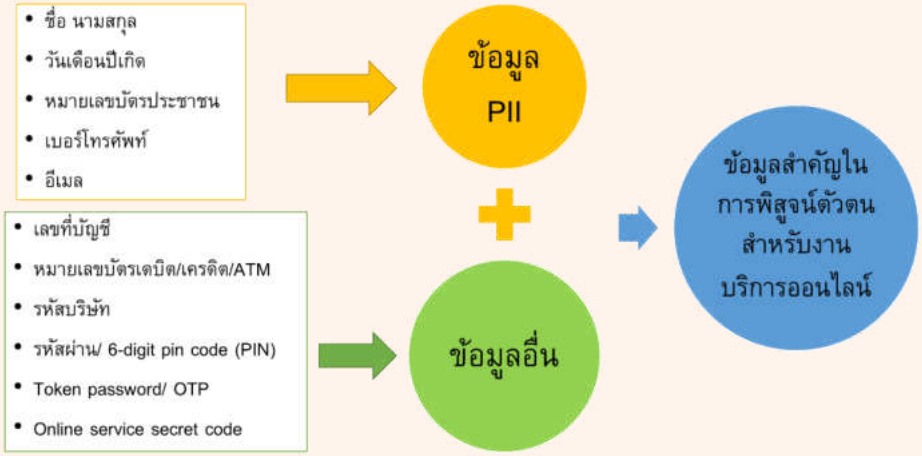
แรงจูงใจในการสร้างเว็บไซต์ฟิชชิงบนบริการคลาวด์สาธารณะเพิ่มขึ้น เนื่องจาก

- สามารถสร้างเว็บไซต์ฟิชชิงง่าย ประหยัดเวลา ต้นทุนที่ถูกบนบริการคลาวด์ด้วย VPS (Virtual Private Server) เมื่อเทียบกับการเจาะระบบอื่นเพื่อวางเว็บไซต์ฟิชชิง
- มีความน่าเชื่อถือมากกว่าโดเมนโฮสติ้งอื่นทั่วไป (ในอดีตฟิชชิงถูกโฮสต์อยู่ในประเทศรัสเซียเป็นต้น) และยังจะถูกปิดกั้นการเข้าถึง (Block) ได้ยาก เนื่องจากใช้หมายเลขไอพี (IP address) ร่วมกับบริการคลาวด์อื่น ๆ อีกด้วย
- ถึงแม้ว่าเว็บไซต์ฟิชชิงอาจจะถูกปิด (Takedown) ได้เร็ว เพราะสามารถติดต่อผู้ให้บริการในการยุติการเข้าถึงเว็บไซต์ฟิชชิงนั้นได้ อย่างไรก็ตาม Threat Actor สามารถสร้างเครื่องใหม่ได้ง่ายและรวดเร็วเช่นกัน

4. แรงจูงใจของการโจมตีด้วยฟิชชิง (Phishing)

แรงจูงใจของ Threat Actor ที่พยายามเก็บข้อมูลที่ต้องการเพื่อใช้ในการพิสูจน์ตัวตนสำหรับการใช้บริการออนไลน์ของธนาคาร ขึ้นอยู่วัตถุประสงค์ของ Threat Actor ซึ่งโดยส่วนใหญ่แล้ว Threat Actor จะพยายามขโมยเงินของเหยื่อผ่านช่องทางที่ Threat Actor สามารถใช้เพื่อเข้าถึงบัญชีของเหยื่อโดยที่ไม่ต้องพบกับเจ้าหน้าที่ของธนาคาร เช่นการติดตั้ง Mobile banking ด้วยบัญชีของเหยื่อบนโทรศัพท์มือถือของ Threat Actor ซึ่งในกระบวนการนี้ทางธนาคารจะขอข้อมูลส่วนบุคคล เช่น เลขที่บัตรประชาชน หรือวันเดือนปีเกิด จากนั้นจะแจ้งขอเปลี่ยนแปลงเครื่องโทรศัพท์ที่ใช้ติดตั้งผ่านการร้องขอผ่าน Mobile Banking เพื่อให้ Threat Actor สามารถได้รับ SMS OTP จากธนาคารเองโดยตรง จากนั้นทำการโอนเงินออกไปยังบัญชีภายนอก เป็นต้น ดังนั้นข้อมูลที่ Threat Actor มักจะให้เหยื่อกรอกในเว็บไซต์ฟิชชิงนั้นจะประกอบด้วย 2 ส่วน คือ

- ข้อมูลส่วนบุคคล (PII) ได้แก่ ชื่อ นามสกุล วันเดือนปีเกิด หมายเลขบัตรประชาชน หมายเลขโทรศัพท์ และอีเมล เป็นต้น
- ข้อมูลอื่น ๆ ได้แก่ เลขที่บัญชีธนาคาร หมายเลขบัตรเดบิต/เครดิต/ATM รหัสบริษัท (สำหรับฟิชชิงที่มีเป้าหมายหลอกลูกค้ากลุ่มนิติบุคคล) รหัสผ่าน PIN รหัสผ่านโทเคน OTP และ Online service secret code เป็นต้น



รูปที่ 24 แสดงลักษณะข้อมูลที่Threat Actor ต้องการเก็บจากเหยื่อ

เพื่อเป็นข้อมูลให้เห็นว่าเป้าหมายของ Threat Actorในการหลอกลวงข้อมูลส่วนบุคคล และเพื่อที่จะให้เกิดความตระหนักเพื่อให้ตรวจสอบก่อนที่จะให้ข้อมูลในกลุ่มดังกล่าว และจะไม่ตกเป็นเหยื่อของฟิชชิง

คำแนะนำในการป้องกันตัวเองจากฟิชชิง

1. ระลึกไว้เสมอว่า **ธนาคารไม่มีนโยบายร้องขอข้อมูลส่วนบุคคลของลูกค้าผ่านช่องทาง SMS หรือเว็บไซต์**
2. **ตรวจสอบลิงก์**ที่มาพร้อมกับอีเมล SMS หรือ โปรแกรมสนทนา (เช่น Line หรือ FB messenger เป็นต้น) หากไม่แน่ใจแหล่งที่มา ห้ามเปิดลิงก์แนบอย่างเด็ดขาด
3. **ห้ามเปิดเผยข้อมูลส่วนบุคคลใด ๆ** ผ่านการร้องขอที่ไม่แน่ใจ หากไม่แน่ใจให้ทำการติดต่อกลับไปยังธนาคารโดยตรง
4. หากพบข้อความ หรือเว็บไซต์ที่สงสัยว่าจะเป็นฟิชชิงที่เกี่ยวข้องกับธนาคาร **กรุณาติดต่อธนาคารทันที**
5. ในกรณีหลงเชื่อและเปิดเผยรหัสผ่านแล้ว ให้ติดต่อไปยังธนาคารเพื่อขอคำแนะนำและทำการ**เปลี่ยนรหัสผ่านทันที**

เอกสารอ้างอิง

1. https://enterprise.verizon.com/resources/reports/2020-msi-report.pdf
2. https://www.welivesecurity.com/2021/01/22/why-do-we-fall-sms-phishing-scams-so-easily/
3. https://zvelo.com/domain-generation-algorithms-dgas/
4. https://www.tigera.io/blog/detecting-domain-generation-algorithms-dga-in-kubernetes/

เหตุการณ์ภัยคุกคามไซเบอร์ที่หน่วยงานบุคคลที่สาม (3rd Party)

ในการประกอบธุรกิจในยุคดิจิทัล ธุรกิจต่างมีการเชื่อมโยงกันในรูปแบบต่าง ๆ ตามโมเดลธุรกิจ ซึ่งนอกจากจะมีการเชื่อมโยงกันทางระบบ แล้วยังมีการรับส่งข้อมูลระหว่างกันเป็นห่วงโซ่ธุรกิจ หรือ Business Supply Chain ในปี 2020 มีเหตุการณ์การโจมตีบริษัทในประเทศไทยและบริษัทที่คนไทยใช้บริการจำนวนมาก โดยเฉพาะในช่วง COVID-19 ไม่ว่าจะเป็นเหตุการณ์ข้อมูลรั่วไหลของบริษัท Wongnai ถูกขโมยข้อมูลหลุดกว่า 4 ล้านรายการ ประกอบด้วยข้อมูล อีเมล, รหัสผ่าน (ที่ถูกเข้ารหัสอีกชั้นแล้ว), ชื่อจริง, ชื่อบัญชีผู้ใช้งาน Facebook และ Twitter, วันเกิด, หมายเลขโทรศัพท์, รหัสไปรษณีย์ [1] หรือ ระบบฐานข้อมูลของ Lazada ในสิงคโปร์ที่ถูกแฮก กว่า 1.1 ล้านบัญชี ซึ่งหากดูเผิน ๆ อาจจะเป็นสิ่งที่บริษัทดังกล่าวต้องจัดการปัญหาเหล่านั้นแต่ด้วยความเชื่อมโยงทางระบบงาน และการที่ธนาคารจะต้องใช้ชุดข้อมูลส่วนบุคคลของบุคคลเดียวกัน เหตุการณ์ดังกล่าวจึงถือเป็นความเสี่ยงมาที่ธนาคารได้ด้วย

เหตุการณ์ข้อมูลรั่วไหลไม่จำกัดความรับผิดชอบแค่ตาม พรบ.คุ้มครองข้อมูลส่วนบุคคล แม้ว่าจะเลื่อนการบังคับใช้ไปถึง 1 มิถุนายน 2021 ก็ตาม การควบคุมดูแลข้อมูลให้กับเจ้าของข้อมูลให้มีความมั่นคงปลอดภัยก็ยังคงเป็นเรื่องสำคัญ ตราบใดที่ข้อมูลเหล่านั้นยังคงจะสร้างผลกระทบให้กับเจ้าของข้อมูล ด้วยความเชื่อมโยงของข้อมูลและด้วยการที่ใช้ข้อมูลส่วนบุคคลชุดเดียวกันในการพิสูจน์ตัวตน การวิเคราะห์ผลกระทบของกลไกการตรวจสอบตัวตนจากเหตุการณ์ข้อมูลรั่วไหลของหน่วยงานอื่น จึงมีความสำคัญและควรจะต้องได้รับความร่วมมือในภาพกว้าง โดยจะต้องคำนึงถึงการแพร่กระจายของข่าวอันจะเป็นผล Viral Effect ไปที่หน่วยงานที่ประสบกับเหตุการณ์ข้อมูลรั่วไหล ตัวอย่างเหตุการณ์ที่โรงพยาบาลสระบุรีซึ่งถูกคุกคามโดยมัลแวร์เรียกค่าไถ่ (Ransomware) มีผลให้ระบบทะเบียนของโรงพยาบาลใช้งานไม่ได้ เกิดผลกระทบกับการรับผู้ป่วยที่เข้ารักษาที่โรงพยาบาล นอกจากนั้นโรงพยาบาลก็ไม่สามารถจ่ายเงินค่าไถ่ตามที่ Threat Actor เรียกร้องได้ ซึ่งอาจจะมีผลให้กลุ่ม Threat Actor อาจจะนำข้อมูลบางส่วนออกขายในตลาดมืด อันอาจจะมีผลให้การนำข้อมูลเหล่านั้นประกอบกับข้อมูลที่เคยรั่วไหลในเหตุการณ์อื่น ๆ ของหน่วยงานอื่น ๆ เมื่อรวมแล้ว อาจจะสามารถใช้ในการแสดงตัวกับธนาคารในช่องทางดิจิทัลของธนาคารได้ เป็นโจทย์ที่ท้าทายในการทำธุรกิจในยุคดิจิทัลอย่างมาก

เมื่อต้นธันวาคม ยังเกิดเหตุการณ์ที่เกี่ยวข้องกับบุคคลที่สามในอีกรูปแบบหนึ่ง คือเหตุการณ์ที่ Threat Actor ทำการเจาะระบบของบริษัท Solarwinds ซึ่งเป็นบริษัทที่พัฒนาระบบการบริหารจัดการอุปกรณ์ในองค์กร จากนั้น Threat Actor ได้ทำการฝังมัลแวร์ลงในซอฟต์แวร์โมดูล Orion ที่บริษัทลูกค้าของ Solarwinds จะต้องดาวน์โหลดจากช่องทางที่ได้เตรียมไว้สำหรับอัปเดต Solarwinds Orion ซึ่งปรากฏว่าบริษัทต่าง ๆ ติดมัลแวร์ที่ฝังตัวไปนั้นผ่านช่องทางการอัปเดต ซึ่งมักจะไม่ได้ตรวจความมั่นคงปลอดภัยของ Software Distribution Package นั้น ๆ จึงเป็นวิธีการเข้าถึงองค์กรในช่องทางที่มีการสร้างความเชื่อถือระหว่างกันไว้ก่อน แม้ว่าการเจาะระบบต้นน้ำจะไม่ง่ายก็ตาม แต่สามารถหวังผลที่ได้สูงขึ้นหลายเท่าตัวทีเดียว วิธีการเช่นนี้เรียกว่าการโจมตีแบบ Supply Chain Attack โดยในกรณีของ Solarwinds เรียกกันว่า Sunburst ซึ่งสามารถอ้างอิงรายละเอียดการวิเคราะห์กรณีของ Sunburst ได้ที่เอกสาร TR20-014 (เรื่อง คำแนะนำเกี่ยวกับเหตุการณ์การโจมตี Software Supply Chain) ของ TB-CERT จากเทคนิคการโจมตีนี้ คาดการว่าจะมีการเลียนแบบและใช้โจมตีไปที่ Supply Chain มากขึ้น

การจัดการความเสี่ยงที่มาจากบุคคลที่สามหรือภัยคุกคามที่มาในรูปแบบของ Supply Chain Attack นั้น แม้ว่าจะมีหลายส่วนที่อยู่นอกเหนือจากการควบคุมโดยตรงขององค์กร แต่มีความจำเป็นจะต้องนำเหตุการณ์ดังกล่าวมาปรับเพิ่มเติมในกระบวนการบริหารจัดการบุคคลที่สาม หรือ 3rd Party โดยสามารถสรุปได้ดังต่อไปนี้

1. กำหนดบทบาทหน้าที่และความรับผิดชอบของหน่วยงานบุคคลที่สามอย่างชัดเจน ในสัญญาในด้านการบริหารจัดการความมั่นคงปลอดภัยในการเชื่อมต่อระบบ ข้อมูลและการดูแลความมั่นคงปลอดภัยของระบบที่ใช้เชื่อมต่อ ให้ครอบคลุมตามระดับความเสี่ยงและความสำคัญของบริการที่เชื่อมต่อนั้น
2. สร้างความสัมพันธ์ที่ดีกับหน่วยงานบุคคลที่สามที่สำคัญ (Strategic Partnership) โดยเฉพาะสำหรับบริการที่สำคัญ รวมถึงความสามารถที่จะรับทราบถึงการเปลี่ยนแปลงสำคัญต่างๆ ของหน่วยงานบุคคลที่สามที่มีความเกี่ยวข้องการเชื่อมต่อของบริการ
3. มีการเฝ้าระวังและตรวจสอบการส่งผ่านข้อมูล ปริมาณข้อมูล พฤติกรรมที่ผิดแปลกไปจากปกติ และกำหนดให้หน่วยงานบุคคลที่สามแจ้งและให้ข้อมูลในรายละเอียดหากพบสิ่งผิดปกติเกี่ยวกับภัยไซเบอร์
4. เทคโนโลยีที่ใช้ในการเชื่อมต่อจะต้องได้มาตรฐานสากลที่ยอมรับได้ทั่วไป
5. ช่องทางในการเชื่อมต่อจะต้องจำกัดเท่าที่ใช้งานเพื่อจำกัด Attack Surface
6. เตรียมแผนรับมือผลกระทบที่อาจจะเกิดขึ้นจากหน่วยงานบุคคลที่สามในกรณีของเหตุการณ์ภัยไซเบอร์ที่เกิดขึ้นที่หน่วยงานบุคคลที่สาม
7. กำหนดกระบวนการวิเคราะห์ผลกระทบจากการใช้ข้อมูลที่รั่วไหลในช่องทางต่าง ๆ ขององค์กร
8. ติดตามข่าวสารจาก TB-CERT และแหล่งข้อมูลอื่น ๆ เพื่อที่จะได้เตรียมการหรือตรวจสอบได้รวดเร็วขึ้น
9. พิจารณาทำประกันภัยไซเบอร์ (Cyber Insurance) เพื่อลดผลภาระให้กับองค์กรจากภัยทางไซเบอร์

เอกสารอ้างอิง

1. https://www.wongnai.com/pages/wongnai-security-incident?ref=ct
2. TR Document ของ TB-CERT หมายเลข TR20-014 เรื่อง คำแนะนำเกี่ยวกับเหตุการณ์การโจมตี Software Supply Chain
3. ประกาศธนาคารแห่งประเทศไทย สนส. 21/2562 เรื่องหลักเกณฑ์การกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศของสถาบันการเงิน
4. ISO27001 Annex A.15 Supplier Relationships

คาดการณ์แนวโน้มภัยไซเบอร์ในปี 2021

จากการรวบรวมข้อมูลเหตุการณ์ที่เกิดขึ้นในปีที่ผ่านมาประกอบกับการวิเคราะห์สถานการณ์และแนวโน้มจากรายงานหลายแหล่ง TB-CERT จึงได้ทำการคาดการณ์แนวโน้มรูปแบบการโจมตีทางไซเบอร์สำหรับปี 2021 นี้ดังนี้

1. การโจมตีสิ่งแวดล้อมการทำงานในยุค New Normal

จากสถานการณ์การแพร่ระบาดของไวรัส COVID-19 ในช่วงปีที่ผ่านมาตลอดจนต้นปีนี้ ส่งผลกระทบต่อการเปลี่ยนแปลงในการใช้งานเทคโนโลยีสารสนเทศอย่างมาก จนอาจเกิดความเสี่ยงจากหลายด้านดังนี้

1) คอมพิวเตอร์จากที่บ้านอาจกลายเป็นช่องทางโจมตีองค์กร เนื่องด้วยหลายองค์กรอนุญาตให้พนักงานทำงานจากที่บ้าน (Work From Home) แล้วพนักงานทำการเชื่อมต่อกลับเข้ามายังระบบเครือข่ายขององค์กรผ่านอินเทอร์เน็ต อีกทั้งการใช้งานคอมพิวเตอร์จากที่บ้านนั้นไม่มีระบบรักษาความปลอดภัยเฉกเช่นเดียวกับในองค์กร ดังนั้นจึงมีโอกาสที่ Threat Actor จะโจมตีคอมพิวเตอร์ของพนักงานที่ใช้อยู่ที่บ้านเพื่อกลับเข้ามาโจมตีระบบเครือข่ายขององค์กรได้
2) อุปกรณ์โทรศัพท์มือถือและแท็บเล็ตซึ่งนิยมใช้กันมากขึ้น ประกอบกับพฤติกรรมการใช้งานอุปกรณ์เคลื่อนที่ต่าง ๆ ที่ผู้ใช้งานอาจจะมีความเร่งรีบใช้งาน การแสดงผลมีข้อจำกัด ขาดความระมัดระวัง ซึ่งจะเป็นเป้าในการโจมตีและนำไปสู่การขโมยเงินจากระบบ Mobile Banking และ Mobile Payment ต่าง ๆ โดยอาจจะมีมัลแวร์บนโทรศัพท์มือถือเพิ่มมากขึ้นด้วย
3) การพิสูจน์ยืนยันตัวตนข้ามองค์กร (Federated Authentication) จะมีการขยายการใช้งานมากขึ้นเพื่อเสริมความมั่นคงปลอดภัยของการพิสูจน์ยืนยันตัวตนด้วยข้อมูลขององค์กรเดียว แต่ด้วยการยกระดับความมั่นคงปลอดภัยของทุกองค์กรในระบบนิเวศน์ดิจิทัลยังไม่สามารถทำได้เต็มที่ ซึ่งจะทำให้เกิดการโจมตีไปที่จุดอ่อนในระบบนิเวศน์ดิจิทัลได้

2. การละเมิดความเป็นส่วนตัวจากระบบ IoT

จากความเร็วของการพัฒนาและการเร่งรีบนำไปใช้ ปัจจุบันอุปกรณ์ IoT มีจำนวนเพิ่มขึ้นอย่างมาก ทั้งสำหรับส่วนบุคคลและภาคอุตสาหกรรม นอกจากนี้การจัดเก็บข้อมูลจากอุปกรณ์ต่าง ๆ บนคลาวด์ และแอปพลิเคชันอาจจะไม่ได้รับการดูแลเรื่องความปลอดภัยที่ดีเพียงพอ ประกอบกับการพัฒนาด้านฟังก์ชันการใช้งานเป็นไปอย่างรวดเร็วจนอาจมีช่องโหว่หรือข้อผิดพลาด นำไปสู่การเข้าถึงอุปกรณ์ IoT และข้อมูลความเป็นส่วนตัวจากระบบ IoT ของผู้ใช้งานได้ ซึ่งผลกระทบที่อาจพบได้ อย่างเช่นการเผยแพร่ข้อมูลส่วนบุคคล เช่นภาพจากกล้องวงจรปิดในบ้าน หรือแม้กระทั่งการข่มขู่กรรโชกเพื่อเรียกร้องเงินและทรัพย์สินของเหยื่อ ดังนั้น การใช้เทคโนโลยี IoT จึงควรคำนึงถึงความปลอดภัยและความเป็นส่วนตัวของผู้ใช้งาน รวมถึงการศึกษาคุณสมบัติและวิธีการรักษาความปลอดภัยข้อมูลที่เก็บบนอุปกรณ์ที่เลือกใช้ด้วย

3. การโจมตีในลักษณะ Supply Chain Attack มากขึ้น

จากเหตุการณ์ที่ Threat Actor เจาะระบบของบริษัท Solarwinds แล้วฝัง backdoor ไว้นั้น ทำให้เกิดการตื่นตัวในการดูแลและป้องกันไม่ให้เหตุการณ์ลักษณะเดียวกันนี้เกิดขึ้นกับบริษัทผู้ผลิตอุปกรณ์ด้านเทคโนโลยีสารสนเทศทั่วโลก แต่หากมองอีกมุมหนึ่ง Threat Actor ก็มีแรงจูงในในการโจมตีระบบของบริษัทเหล่านี้ ที่ต้องการแทรกซึมเพื่อเข้าไปยังระบบเครือข่ายของเป้าหมายและขโมยข้อมูล หรือต้องการแพร่กระจายมัลแวร์ให้กับผู้ใช้งานจำนวนมากเพื่อขโมยข้อมูลหรือใช้เป็นฐานในการโจมตีระบบเครือข่ายเป้าหมายต่อไปได้ ซึ่งนอกจากพฤติกรรมเลียนแบบของการโจมตีแบบ Supply Chain Attack ที่อาจจะเกิดขึ้นแล้ว ส่วนหนึ่งอาจจะเกิดจากข้อมูลที่รั่วไหลหรือผลพวงจาก Supply Chain Attack ที่จะเกิดต่อไปโดยการใช้ข้อมูลจากเหตุการณ์ที่เกิดขึ้นไปแล้ว ดังนั้นในปี 2021 นี้เหตุการณ์ลักษณะใกล้เคียงกันนี้จะเกิดขึ้นกับบริษัทอื่น ๆ ในภาคอุตสาหกรรมด้านเทคโนโลยีต่าง ๆ ไม่ว่าจะผู้พัฒนาซอฟต์แวร์ต่าง ๆ บนเครื่องคอมพิวเตอร์และโทรศัพท์มือถือ ผู้ผลิตฮาร์ดแวร์ เป็นต้น

บทสรุป

ตลอดระยะเวลา 1 ปีเต็มที่ TB-CERT ได้ดำเนินงานในสถานการณ์ที่ผันผวน เหตุการณ์ภัยคุกคามเกิดขึ้นมากมาย ผนวกกับสถานการณ์ COVID -19 ที่ทำให้ต้องมีการปรับกระบวนการทำงานค่อนข้างมาก โดยเฉพาะการทำงานแบบออนไลน์ ไม่ว่าจะเป็น ประชุมออนไลน์ สัมมนาออนไลน์ เรียนออนไลน์ ฝึกซ้อมรับมือกับภัยไซเบอร์ออนไลน์ การปรับตัวการทำงานในช่วงเหตุการณ์นี้ของ TB-CERT ถือว่าเป็นเรื่องที่ท้าทายการทำงานของทีมงานและเพื่อนสมาชิกทุกคน เพื่อยังคงให้เป้าหมายหลักของ TB-CERT ดำเนินการไปได้อย่างต่อเนื่องและมีประสิทธิภาพสูงสุด ธนาคารต้องเตรียมความพร้อมในการรับมือกับภัยไซเบอร์ให้ได้อย่างทันท่วงที สร้างความเชื่อมั่นให้กับลูกค้าประชาชนในสภาวะเช่นนี้ได้ โดยผ่านกิจกรรมต่าง ๆ ที่จัดทำขึ้นในรูปแบบออนไลน์เพื่อจะช่วยตอบโจทย์ให้กับสมาชิกของ TB-CERT กิจกกรรมหนึ่งที่เป็นหัวใจสำคัญของ TB-CERT และสำเร็จลุล่วงไปได้ด้วยดีในสถานการณ์ที่ทุกคนต้องทำงานจากที่บ้าน คือการซักซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ในระดับภาคการธนาคาร Banking Cyber Drill และการแข่งขันทักษะทางไซเบอร์ TB-CERT Cyber Combat ซึ่งนอกเหนือจากสมาชิกจะได้รับการพัฒนาทักษะความรู้ใหม่ ๆ ให้เท่าทันกับภัยใหม่ ๆ จากการทำกิจกรรมแล้ว สมาชิกยังได้ฝึกประสานงาน สื่อสารกันแบบออนไลน์ ฝึกใช้อุปกรณ์ที่สนับสนุนการทำงานแบบออนไลน์ให้คุ้นชิน ฝึกทักษะการลงมือปฏิบัติในลักษณะออนไลน์ การจัดเตรียมสภาพแวดล้อมให้สามารถทำงานแบบออนไลน์ โดยเฉพาะอย่างยิ่งการได้วิเคราะห์แนวทางการ ทำ Containment สำหรับสถานการณ์จำลองในการซ้อม Cyber Drill สิ่งเหล่านี้ล้วนแต่จะทำให้สมาชิกได้ทดสอบและนำมาประยุกต์ใช้กับองค์กรของสมาชิกเอง และต่อยอดเพื่อนำไปใช้เป็นแนวทางการทำงานเพื่อป้องกันภัยไซเบอร์ให้กับลูกค้าประชาชนได้

แม้ว่าการสถานการณ์ COVID-19 จะดูเหมือนว่ามาปรับเปลี่ยนการทำงานในชีวิตประจำวัน แต่จริง ๆ แล้วเป็นเพียงส่วนหนึ่งที่กระตุ้นให้เกิดการทำงานในลักษณะนี้เร็วขึ้น จึงถือว่าเป็นก้าวสำคัญก้าวหนึ่งของ TB-CERT ในการเตรียมความพร้อมเพื่อรับมือกับภัยไซเบอร์ในยุคดิจิทัล

เป้าหมายการดำเนินงานในปี 2021

แม้ว่าจะเจอสถานการณ์ COVID-19 ที่ทำให้การทำงานในหลาย ๆ ภาคธุรกิจเป็นไปอย่างยากลำบาก TB-CERT ที่ได้ดำเนินการตามภารกิจหลักอย่างต่อเนื่องเพื่อยกระดับความมั่นคงปลอดภัยของภาคการธนาคารก็ได้ปรับเปลี่ยนรูปแบบการทำงานให้ตอบรับต่อสถานการณ์เช่นนี้เช่นกัน ไม่ว่าจะเป็นการประชุมออนไลน์ การจัดสัมมนาออนไลน์ เรายังคงดำเนินการตามภารกิจเช่นเดิมแม้อาจจะต้องปรับเปลี่ยนรูปแบบไปบ้างก็ตาม หัวใจหลักของการเป็น CERT (Computer Emergency Response Team) คือ การมีทีมที่ดีที่สามารถรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงทีและมีประสิทธิภาพ เพื่อประโยชน์ต่อองค์กรและสาธารณะ แต่การสร้าง CERT ที่มีประสิทธิภาพนั้น ประกอบไปด้วยปัจจัยหลายอย่าง ไม่ว่าจะเป็นความร่วมมือกันในการแชร์ข้อมูลของบุคลากรใน Community นั้น ๆ กระบวนการต่าง ๆ ที่ใช้ตอบสนองต่อเหตุการณ์ในการรับมือกับภัยไซเบอร์ รวมถึงเทคโนโลยีที่ใช้ในการวิเคราะห์ข้อมูลด้วย และที่สำคัญคือทักษะความรู้ของบุคลากรด้านไซเบอร์ที่ต้องอาศัยประสบการณ์ในการทำงาน ซึ่งต้องพัฒนาอยู่ตลอดเวลา

TB-CERT มีเป้าหมายการดำเนินงานในปี 2021 อยู่ 4 แกนหลัก ได้แก่

1. TB-CERT ต้องการวิเคราะห์ Threat เชิงลึกให้กับสมาชิกซึ่งเป็นแนวทางการนำ CERT ไปสู่ CERT Maturity ที่ Level 4 และเป็นหัวใจสำคัญของการพัฒนา CERT ให้มีประสิทธิภาพและเกิดประโยชน์สูงสุดต่อสมาชิก
2. การขยายเครือข่ายความร่วมมือเพื่อให้เกิดการแชร์ข้อมูลที่หลากหลายและมากขึ้นทำให้เรามีข้อมูลเพื่อใช้ในการวิเคราะห์ได้ดีขึ้น เป็นประโยชน์ต่อการรับรู้ข่าวสารที่รวดเร็วทันต่อเหตุการณ์ที่อาจจะเกิดขึ้นและช่วยให้สมาชิกสามารถป้องกันภัยได้ทันท่วงที
3. กำหนดมาตรฐานสำหรับเทคโนโลยีใหม่ที่ใช้ในธุรกิจธนาคาร
4. พัฒนาบุคลากรที่มีอยู่ให้มีศักยภาพเพิ่มขึ้น โดยเน้นการฝึกอบรมแบบเน้นไปที่การลงมือปฏิบัติหลังจากมีการอบรมเชิงทฤษฎีแล้ว ซึ่งกลยุทธ์นี้จะช่วยให้สมาชิกสามารถนำไปปรับใช้งานได้จริง

ภาคผนวก

เอกสารเผยแพร่

ในช่วง 1 ปีที่ผ่านมา TB-CERT ได้นำเสนอบทความด้านเทคนิคเกี่ยวกับข่าวสาร และแนวทางการป้องกันเพื่อไม่ให้ตกเป็นเหยื่อของภัยไซเบอร์ให้กับหน่วยงานสมาชิก หน่วยงานภาคการเงิน รวมทั้งประชาชนรับทราบและตระหนักถึงความเสี่ยงด้านภัยไซเบอร์ที่อาจเกิดขึ้น อาทิ คำแนะนำเกี่ยวกับการใช้งาน Mobile Banking อย่างปลอดภัย ภัยไซเบอร์ที่อาจเกิดขึ้นในช่วงสถานการณ์ COVID-19 รวมถึงข้อมูลปฏิบัติการโจมตีจากกลุ่ม Threat Actor ต่าง ๆ เป็นต้น โดยได้ทำการเผยแพร่ผ่านเว็บไซต์สมาคมธนาคารไทย และโซเชียลมีเดียของ TB-CERT (Facebook page) ดังนี้

https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/

https://www.facebook.com/TBCERT.Official

เอกสารเผยแพร่

5 ขั้นตอน เตรียมพร้อมใช้งาน Mobile banking อย่างปลอดภัย

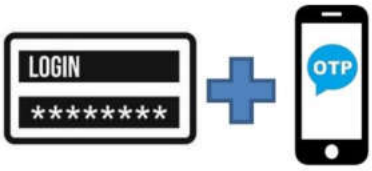
TLP: WHITE

เผยแพร่วันที่ 7 กุมภาพันธ์ 2563

Mobile Banking Application เป็นแอปพลิเคชันบนโทรศัพท์มือถือและแท็บเล็ตที่ธนาคารพัฒนาเพื่ออำนวยความสะดวกในการทำธุรกรรมด้านการเงินต่างๆ เช่น แสดงยอดเงินในบัญชี โอนเงิน หรือ ชำระสินค้า เป็นต้น ด้วยเหตุนี้ผู้ใช้งานต้องคำนึงถึงความปลอดภัยในการใช้งานโทรศัพท์และแท็บเล็ต ดังนั้นก่อนจะติดตั้ง Mobile Banking Application จึงควรปฏิบัติตามคำแนะนำต่อไปนี้

1. ล็อกหน้าจออยู่เสมอ

ล็อกหน้าจอด้วยรหัสผ่าน ลายนิ้วมือ หรือการจดจำใบหน้า และปรับแต่งให้ล็อกหน้าจออัตโนมัติเมื่อไม่ได้ใช้งานเกิน 30 วินาที – 1 นาที เพื่อป้องกันไม่ให้ผู้ไม่หวังดีที่สามารถเข้าถึงโทรศัพท์สามารถเรียกแอปพลิเคชัน Mobile Banking ขึ้นมาทำงานได้

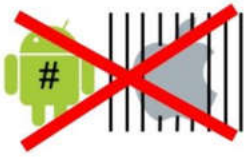


2. ตั้งรหัสผ่านอย่างปลอดภัย ควบคู่กับระบบยืนยันตัวตนด้วยหลายปัจจัย (Multi Factor Authentication)

ตั้งรหัสผ่านที่ผู้อื่นคาดเดาได้ยาก โดยไม่ควรตั้งรหัสผ่านด้วยวันเดือนปีเกิด หรือใช้เลขเรียงลำดับ เช่น 123456 และใช้ควบคู่กับระบบยืนยันตัวตนด้วยหลายปัจจัย เช่น One Time Password (OTP) เป็นต้น รวมถึงควรหมั่นเปลี่ยนรหัสผ่านบ่อยๆ และควรแยกรหัสผ่านระหว่างแอปพลิเคชันทั่วไปกับแอปพลิเคชันด้านการเงิน

3. ติดตั้งแอปพลิเคชันอย่างระมัดระวัง

เลือกติดตั้งแอปพลิเคชันจาก App Store (สำหรับผู้ใช้ระบบปฏิบัติการ iOS) หรือ Play Store (สำหรับผู้ใช้ระบบปฏิบัติการ Android) เท่านั้น รวมถึงเลือกโดย ตรวจสอบรีวิวว่ามีความน่าเชื่อถือ การอัพเดตล่าสุด และข้อมูลติดต่อผู้พัฒนา ในกรณีที่มีปัญหา



4. ห้ามปลดการควบคุมด้านความมั่นคงปลอดภัยด้วยวิธี Jailbreak หรือ Root

เนื่องจากการ Jailbreak หรือ Root จะทำให้การควบคุมด้านความมั่นคงปลอดภัย (Security Measure) ลดลง ส่งผลทำให้ถูกแฮกหรือฝังมัลแวร์ได้ง่าย

5. อัพเดตระบบปฏิบัติการให้เป็นเวอร์ชั่นล่าสุดอยู่เสมอ

เพื่อให้โทรศัพท์มือถือทำงานได้อย่างมีประสิทธิภาพ เพิ่มฟีเจอร์ด้านความปลอดภัย รวมถึงแก้ปัญหาต่างๆ ที่ตรวจสอบพบในเวอร์ชั่นก่อนหน้า

TR20-001

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

5 เหตุผลที่ไม่ควร Jailbreak หรือ Root

TLP: WHITE

เผยแพร่วันที่ 13 มีนาคม 2563

การ Jailbreak บนระบบปฏิบัติการ Apple IOS หรือการ Root บนระบบปฏิบัติการ Android เป็นกระบวนการดัดแปลงระบบปฏิบัติการบนโทรศัพท์มือถือ หรือแท็บเล็ต เพื่อให้ผู้ใช้สามารถแก้ไขระบบหรือติดตั้งโปรแกรมบางชนิดที่ปกติไม่สามารถติดตั้งได้ ซึ่งจะทำให้การทำงานของทุกแอปพลิเคชันสามารถเข้าถึงข้อมูล และไฟล์ต่างๆ ในเครื่องได้

5 เหตุผลที่ไม่ควร Jailbreak หรือ Root

1. ระบบปฏิบัติการทำงานไม่เสถียร

เนื่องจากการปรับแต่งค่าการทำงานโดยไม่ได้ผ่านการทดสอบจากผู้พัฒนา

2. ระดับการรักษาความปลอดภัยลดลง

Jailbreak หรือ Root คือการแก้ไขสิทธิ์ให้ทำงานด้วยสิทธิ์ผู้ดูแลระบบ ทำให้สามารถควบคุมเครื่องได้ทุกอย่าง ซึ่งก็ทำให้มัลแวร์ที่อาจจะติดเข้ามาในเครื่องก็จะสามารถทำงานด้วยสิทธิสูงและสามารถแก้ไขแอปพลิเคชันและการปรับแต่งค่าพารามิเตอร์ต่างๆในเครื่อง และส่งผลกระทบต่อความปลอดภัยที่ผู้ผลิตเตรียมไว้ได้

3. อาจถูกติดตั้งมัลแวร์จากแฮกเกอร์

เครื่องสามารถติดตั้งแอปพลิเคชั่นนอก App Store ได้ จึงมีโอกาสที่จะสามารถถูกติดตั้งมัลแวร์ได้

4. ถูกละเมิดความเป็นส่วนตัวได้

แฮกเกอร์สามารถติดตั้งมัลแวร์ และมัลแวร์อาจจะสามารถขโมยข้อมูลสำคัญภายในโทรศัพท์ ได้แก่ รหัสผ่าน ข้อมูลส่วนตัว รายละเอียดการทำธุรกรรมทางการเงินต่างๆ เป็นต้น

5. บอกลาการปรับปรุงระบบอย่างถาวร

เพื่อป้องกันไม่ให้กระทบกับการทำงานของเครื่องที่ Root หรือ Jailbreak แล้ว จึงไม่ยอมให้ปรับปรุงระบบปฏิบัติการ ทำให้มีความเสี่ยงที่จะถูกโจมตีด้วยวิธีการอื่นๆ ได้ เพราะเครื่องไม่ได้รับการปรับปรุงแก้ไขความปลอดภัยที่ส่งมาอัปเดต

TR20-003

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

เอกสารเผยแพร่

ระวังมัลแวร์แพร่กระจายผ่านเว็บหลอกลวงติดตามสถานการณ์ COVID-19

TLP: WHITE

เผยแพร่วันที่ 19 มีนาคม 2563

สถานการณ์ระบาดของไวรัส Corona หรือ COVID-19 ที่ขยายตัวไปในเกือบทุกประเทศทั่วโลก ทำให้มีนักวิชาการต่างๆ สร้างเว็บไซต์ที่รวบรวมข้อมูลที่เกี่ยวกับ COVID-19 เพื่อให้ผู้สนใจสามารถติดตามสถานการณ์ รวมถึงข้อมูลที่เป็นประโยชน์ในการเตรียมตัวป้องกัน ภายใต้สถานการณ์เช่นนี้แฮกเกอร์มักจะฉวยโอกาสที่ผู้ใช้งานมุ่งความสนใจไปที่ข้อมูลที่เกี่ยวข้องกับสถานการณ์โรคระบาด จนหลายๆ ครั้งทำให้ขาดความระวังในการป้องกันตนเองในโลกไซเบอร์เมื่อเปิดอีเมลแปลกๆ ดาวน์โหลดโปรแกรมหรือเผลอให้ข้อมูลไปอย่างง่ายๆ ตัวอย่าง เช่น มีการสร้างเว็บไซต์ปลอม (www.Corona-Virus-Map[.]com) ที่แสดงแผนที่อัปเดตการแพร่กระจายของไวรัส Corona พร้อมข้อมูลต่างๆ เช่น สถิติการเสียชีวิต จำนวนผู้ที่รักษาหาย และจำนวนผู้ติดเชื้อ เป็นต้น ซึ่งใช้ข้อมูลจากเว็บของมหาวิทยาลัย John Hopkins และหลอกให้เหยื่อดาวน์โหลดและติดตั้งไฟล์มัลแวร์ลงบนเครื่องของเหยื่อ

ลักษณะของมัลแวร์

มัลแวร์นี้ถูกจัดอยู่ในตระกูล AZORult โดยเมื่อเหยื่อเยี่ยมชมเว็บไซต์ปลอมจะถูกบังคับให้ดาวน์โหลดและติดตั้งไฟล์มัลแวร์ชื่อ Corona-virus-Map.com.exe จากนั้นจะมัลแวร์นี้จะสร้างไฟล์อื่นเพิ่มเติม เช่น CoronaMap.exe, Corona.exe และ Corona.sfx.exe เป็นต้น อีกทั้งยังเชื่อมต่อไปยังเซิร์ฟเวอร์ที่แฮกเกอร์เตรียมไว้เพื่อเก็บข้อมูลด้วย

ผลกระทบ

มัลแวร์นี้จะขโมยข้อมูลสำคัญ เช่น ชื่อบัญชี รหัสผ่าน เลขที่บัตรเครดิต เงินในกระเป๋าเงินดิจิทัล ภาพหน้าจอ และข้อมูลอื่นๆ ที่ถูกเก็บอยู่ในเว็บเบราเซอร์ เป็นต้น

วิธีการแก้ไข

1. ติดตั้งโปรแกรมป้องกันมัลแวร์ที่เชื่อถือได้ และอัพเดตให้มีข้อมูลมัลแวร์ใหม่ล่าสุด
2. สแกนค้นหามัลแวร์ในเครื่อง หากพบให้ทำการลบทันที

วิธีการป้องกัน

1. ติดตามข่าวสารสถานการณ์ COVID-19 จากเว็บไซต์และช่องทางสื่อสารที่เป็นทางการจากกระทรวงสาธารณสุข เช่น
   - Web: https://ddc.moph.go.th/viralpneumonia/index.php
   - LINE : https://lin.ee/dAEig3e
   - Twitter : https://twitter.com/thaimoph
   - Facebook : https://www.facebook.com/thaimoph
   - TikTok : https://vt.tiktok.com/jcvfwN/
2. ไม่ดาวน์โหลดและติดตั้งโปรแกรมใดๆ ที่เกี่ยวกับการติดตามสถานการณ์ไวรัส รวมถึงโปรแกรมที่ไม่ทราบหรือไม่แน่ใจว่ามาจากแหล่งที่น่าเชื่อถือ

TR20-005

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT
Thailand Banking Sector CERT

เอกสารเผยแพร่

5 เหตุผลที่ควรอัพเดตระบบปฏิบัติการบนโทรศัพท์มือถือ

TLP: WHITE

เอกสารเวอร์ชัน 1.0
เผยแพร่วันที่ 27 เมษายน 2563

ระบบปฏิบัติการบนโทรศัพท์มือถือ (Mobile Operating System) หมายถึงโปรแกรม หรือซอฟต์แวร์ระบบ มีหน้าที่ควบคุมการทำงานของฮาร์ดแวร์ (Hardware) ของโทรศัพท์มือถือ และแอปพลิเคชั่นต่างๆ (Application) ที่ถูกติดตั้ง ทำให้ประสิทธิภาพโทรศัพท์มือถือเพิ่มขึ้นสามารถทำงานได้มากกว่าการโทรออกหรือรับสาย ซึ่งโทรศัพท์มือถือในปัจจุบันติดตั้งระบบปฏิบัติการหลากหลายประเภท แต่ที่ได้รับความนิยมมากที่สุดคือ ระบบปฏิบัติการ iOS และ Android

5 เหตุผลที่ควรอัพเดตระบบปฏิบัติการ

1. เพิ่มความปลอดภัย

การอัพเดตระบบปฏิบัติการจะช่วยอุดช่องโหว่ ป้องกันไม่ให้แฮกเกอร์เจาะระบบปฏิบัติการเพื่อทำการควบคุมและขโมยข้อมูลสำคัญบนโทรศัพท์มือถือไป

2. เพิ่มความเสถียร

การอัพเดตระบบปฏิบัติการจะช่วยเพิ่มความเสถียร เพิ่มประสิทธิภาพในการทำงาน และรองรับกับการทำงานของแอปพลิเคชั่นใหม่ๆ ได้

3. แก้ไขข้อผิดพลาดของระบบ

เมื่อระบบปฏิบัติการมีข้อผิดพลาดที่ส่งผลทำให้โทรศัพท์มือถือมีปัญหาในการใช้งาน ผู้ผลิตจะพัฒนาโปรแกรมอัพเดตเพื่อช่วยแก้ไขให้โทรศัพท์มือถือทำงานถูกต้อง

4. ปรับปรุงการทำงานกับฮาร์ดแวร์

การอัพเดตช่วยให้การทำงานของฮาร์ดแวร์มีประสิทธิภาพมากขึ้น เช่น สามารถใช้แบตเตอร์รี่ได้นานขึ้น หรือสามารถรับส่งข้อมูลได้ดีขึ้นในสภาพแวดล้อมที่มีคลื่นรบกวนสูง เป็นต้น

5. เพิ่มฟีเจอร์ใหม่

การอัพเดตระบบปฏิบัติการนั้นสามารถเพิ่มฟีเจอร์หรือลูกเล่นใหม่ๆ ให้กับโทรศัพท์มือถือได้ เช่น การถ่ายภาพสามมิติเสมือน เป็นต้น

สามารถตรวจสอบเวอร์ชั่นล่าสุดได้ที่

https://www.apple.com/th/ios/ https://www.android.com/

สามารถติดตามเอกสารเผยแพร่อื่นๆ ของ TB-CERT ได้ที่
https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/

TR20-006

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

วิธีการตรวจสอบและอัพเดตระบบปฏิบัติการบนโทรศัพท์มือถือ

TLP: WHITE

เอกสารเวอร์ชั่น 1.0
เผยแพร่วันที่ 29 เมษายน 2563

วิธีการตรวจสอบเวอร์ชั่นของระบบปฏิบัติการบนโทรศัพท์มือถือ

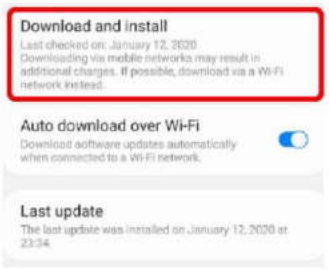
สำหรับผู้ใช้งาน iOS	สำหรับผู้ใช้งาน Android
	
1. ไปที่เมนู "การตั้งค่า" (Settings) เลือกที่เมนู "ทั่วไป" (General) 2. เลือก "เกี่ยวกับ" (About) 3. ดูที่ "เวอร์ชั่นซอฟต์แวร์" (Software Version)	1. ไปที่เมนู "การตั้งค่า" (Settings) เลือกที่เมนู "เกี่ยวกับโทรศัพท์" (About phone) 2. เลือก "ข้อมูลซอฟต์แวร์" (Software information) 3. ดูที่ "เวอร์ชั่น Android" (Android version)

วิธีการอัพเดตระบบปฏิบัติการบนโทรศัพท์มือถือ

อุปกรณ์ที่ใช้ระบบปฏิบัติการ iOS

1. ไปที่เมนู "การตั้งค่า" (Settings)
2. เลือกที่เมนู "ทั่วไป" (General)
3. เลือก "รายการอัพเดตซอฟต์แวร์" (Software Update)
4. เลือก "เลือกดาวน์โหลดและติดตั้ง" (Download and Install)

อุปกรณ์ที่ใช้ระบบปฏิบัติการ Android



1. ไปที่เมนู "การตั้งค่า" (Settings)
2. เลือกที่เมนู "อัพเดตซอฟต์แวร์" (Software Update)
3. เลือก "เลือกดาวน์โหลดและติดตั้ง" (Download and Install)

สามารถติดตามเอกสารเผยแพร่อื่นๆ ของ TB-CERT ได้ที่
https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/

TR20-007

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

ระวัง!!! การหลอกลวงที่อาจเกิดขึ้นหลังจากการลงทะเบียนรับสิทธิประโยชน์ต่างๆ

TLP: WHITE

เผยแพร่วันที่ 15 เมษายน 2563

หลังจากที่รัฐบาลมีมาตรการเยียวยา รวมถึงมอบสิทธิประโยชน์ต่างๆ แก่ประชาชน ไม่ว่าจะเป็น การรับเงินชดเชยรายได้ 5,000 บาทต่อเดือน (ระยะเวลา 3 เดือน) รับเงินประกันการใช้ไฟฟ้าและน้ำประปา โดยผู้ใช้งานจะต้องลงทะเบียนด้วยข้อมูลส่วนบุคคลผ่านแอปพลิเคชั่นบนโทรศัพท์มือถือ หรือทางเว็บไซต์ที่หน่วยงานเตรียมไว้ ซึ่งหลายคนคงลงทะเบียนไปเรียบร้อยและบางคนอาจได้รับเงินแล้ว อย่างไรก็ตามจากสถานการณ์ดังกล่าวอาจเกิดการหลอกลวงในรูปแบบต่างๆ ได้

รูปแบบการหลอกลวงที่อาจเกิดขึ้น

เว็บไซต์หลอกลวง (Phishing)
แฮกเกอร์อาจสร้างเว็บไซต์ปลอม โดยเลียนแบบเว็บไซต์รับลงทะเบียนหรือติดตามผลการรับเงิน จากนั้นแฮกเกอร์จะส่งลิงค์มายังผู้ใช้งาน ผ่านทางอีเมล SMS หรือโปรแกรมสนทนาต่าง ๆ เพื่อหลอกให้ผู้ใช้งานกรอกข้อมูลส่วนตัวได้

การหลอกลวงทางโทรศัพท์ (Voice phishing)
แฮกเกอร์อาจต่อสายโทรศัพท์มาโดยแอบอ้างว่าเป็นเจ้าหน้าที่จากหน่วยงานราชการเพื่อขอข้อมูลส่วนตัวยืนยัน หรือหลอกให้โอนเงิน

การหลอกลวงผ่านข้อความ SMS (SMS phishing)
แฮกเกอร์อาจส่งข้อความเชิญชวนให้ดาวน์โหลดและติดตั้งแอปพลิเคชั่นที่เป็นมัลแวร์ เพื่อแอบขโมยข้อมูลในเครื่องโทรศัพท์ได้ หรือหลอกให้เข้าเว็บไซต์ปลอม เพื่อลวงให้ผู้ใช้งานกรอกข้อมูลส่วนตัวได้

วิธีการป้องกันตนเอง

1. **พึงระลึกเสมอว่าข้อมูลส่วนบุคคลมีค่ามาก** หากสูญเสียไปให้แฮกเกอร์แล้ว จะเกิดความเสียหายแก่เจ้าของข้อมูลได้ อีกทั้งข้อมูลบางอย่างไม่สามารถแก้ไขหรือเปลี่ยนแปลง เพื่อปกปิดให้เป็นความลับต่อไปได้
2. **ติดตามความคืบหน้าผ่านช่องทางการสื่อสารที่หน่วยงานกำหนด** เช่น เว็บไซต์ อีเมล หรือ SMS ของหน่วยงาน เป็นต้น
3. **อย่าหลงเชื่อสายที่ได้รับทางโทรศัพท์หรือข้อความ SMS ที่น่าสงสัย** หากไม่แน่ใจในสายที่โทรมาหรือข้อความที่ได้รับว่ามาจากแหล่งนั้นจริง ให้ติดต่อกลับไปสอบถามตามหมายเลขโทรศัพท์ของหน่วยงานที่รับผิดชอบโดยตรง
4. **ควรใช้บริการแจ้งเตือนความเคลื่อนไหวของบัญชีผ่านช่องทางที่ธนาคารกำหนด** เช่น SMS หรือ LINE เป็นต้น เพื่อติดตามและสอบถามเคลื่อนไหวของบัญชี หากพบรายการธุรกรรมที่ผิดปกติหรือข้อมูลบัญชีไม่ถูกต้อง ให้ติดต่อธนาคารเจ้าของบัญชีโดยทันที

สามารถติดตามเอกสารเผยแพร่อื่นๆ ของ TB-CERT ได้ที่
https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/

TR20-008

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT
Thailand Banking Sector CERT

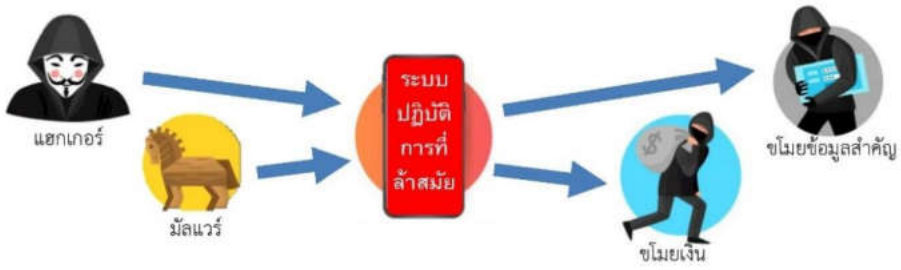
เอกสารเผยแพร่

คำแนะนำเกี่ยวกับเวอร์ชั่นขั้นต่ำของระบบปฏิบัติการที่ควรใช้กับ Mobile Banking Application

TLP: WHITE

เผยแพร่วันที่ 25 เมษายน 2563

ปัจจุบันโทรศัพท์มือถือกลายเป็นอุปกรณ์ที่สำคัญอย่างมากในชีวิตประจำวัน ไม่ว่าจะใช้ในการทำธุรกรรมโอนเงิน ชำระเงินผ่าน Mobile Banking Application ใช้ในการติดต่อสื่อสารผ่านโปรแกรมสนทนาและเครือข่ายสังคมออนไลน์ รวมถึงการใช้เพื่อความบันเทิงต่างๆ เป็นต้น โทรศัพท์มือถือดังกล่าวจะมีระบบปฏิบัติการไม่ว่าจะเป็น iOS หรือ Android เพื่อใช้ควบคุมการทำงานของเครื่อง ระบบปฏิบัติการดังกล่าวจะมีการพัฒนาปรับปรุงและออกเวอร์ชั่นใหม่อยู่เสมอ เพื่อที่จะปรับปรุงประสิทธิภาพการทำงานและที่สำคัญคือเพื่อที่จะแก้ไขช่องโหว่ด้านความปลอดภัยไม่ให้แฮกเกอร์เข้ามาขโมยข้อมูลหรือควบคุมการทำงานของเครื่อง ซึ่งจะส่งผลทำให้เกิดความสูญเสียทางการเงินได้อีกด้วย



เวอร์ชั่นขั้นต่ำของระบบปฏิบัติการที่ควรใช้กับ Mobile Banking Application

Mobile Banking Application เป็นแอปพลิเคชั่นที่ใช้ทำธุรกรรมด้านการเงิน ดังนั้นเพื่อความปลอดภัยสูงสุดของบัญชีและข้อมูลผู้ใช้งาน จึงควรติดตั้งบนระบบปฏิบัติการ iOS หรือ Android เวอร์ชั่นใหม่ล่าสุด หรือเวอร์ชั่นที่ยังมีการอัพเดตจากผู้พัฒนาอยู่เสมอ อย่างไรก็ตามในกรณีที่ไม่สามารถอัพเดตเวอร์ชั่นของระบบปฏิบัติการได้ ควรจะต้องใช้ระบบปฏิบัติการบนโทรศัพท์มือถือตั้งแต่ "iOS เวอร์ชั่น 8" ขึ้นไป หรือ "Android เวอร์ชั่น 5" ขึ้นไป เนื่องจากระบบปฏิบัติการที่ต่ำกว่าเวอร์ชั่นดังกล่าวมีช่องโหว่ระดับร้ายแรงจำนวนมากที่อาจทำให้ผู้ใช้ถูกเจาะระบบปฏิบัติการได้

นอกจากนี้ทางภาคการธนาคารจะมีการพิจารณาและแนะนำเวอร์ชั่นที่เหมาะสมและควรใช้กับ Mobile Banking Application อย่างสม่ำเสมอ เพื่อให้ผู้ใช้งานสามารถใช้งานได้อย่างปลอดภัยสูงที่สุด ดังนั้นหากผู้ใช้งานที่จำเป็นต้องใช้ Mobile Banking Application จึงควรพิจารณาเปลี่ยนโทรศัพท์มือถือให้สามารถใช้ระบบปฏิบัติการที่ยังคงมีการพัฒนาและยังได้รับการสนับสนุนจากผู้ผลิต

แนวทางปฏิบัติเกี่ยวกับการอัพเดตระบบปฏิบัติการ

1. ติดตามข่าวสารเกี่ยวกับระบบปฏิบัติการบนโทรศัพท์มือถือเวอร์ชั่นใหม่ๆ
2. ติดตามประกาศเวอร์ชั่นของระบบปฏิบัติการที่รองรับ Mobile Banking Application จากธนาคารที่ใช้บริการ
3. หมั่นตรวจสอบและอัพเดตระบบปฏิบัติการอยู่เสมอ
4. หากไม่สามารถอัพเดตระบบปฏิบัติการได้ และยังอยู่ในเงื่อนไขที่ธนาคารอนุญาตให้ใช้ Mobile Banking Application ได้ ควรพิจารณาจำกัดวงเงินในการทำธุรกรรมผ่านแอปพลิเคชั่น หรือสมัครใช้บริการแจ้งเตือนความเคลื่อนไหวของบัญชีอัตโนมัติ
5. หากสามารถทำได้ ให้พิจารณาเปลี่ยนมาใช้โทรศัพท์มือถือที่รองรับระบบปฏิบัติการเวอร์ชั่นใหม่ หรือยังได้รับการสนับสนุนการพัฒนาจากผู้ผลิตอยู่

สามารถติดตามเอกสารเผยแพร่อื่นๆ ของ TB-CERT ได้ที่
https://www.tba.or.th/tb-cert-document-report/tb-cert-public-awareness/

TR20-013

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

รายนามคณะกรรมการ TB-CERT (วาระ 2562-2564)

ประธานกรรมการ	**ดร. กิตติ โฆษะวิสุทธิ์** Senior Vice President, Head of Security Management ธนาคารกรุงเทพ
รองประธานกรรมการ	**คุณชัชวัฒน์ อัศวรักวงศ์** Chief Information Security Officer (Acting) บริษัท กสิกร บิซิเนส-เทคโนโลยี กรุ๊ป
กรรมการ	**คุณภคพงศ์ จุลวงศาศิลป์** Senior Vice President, Head of Cyber Security Department ธนาคารกรุงศรีอยุธยา
กรรมการ	**คุณนฤดม รุ่งศิริวงศ์** Senior Vice President, IT Security Head ธนาคารเกียรตินาคินภัทร
กรรมการ	**คุณสมบูรณ์ หิรัญภัทรศิลป์** Head Country, Technology Management ธนาคารสแตนดาร์ด ชาร์เตอร์ด
กรรมการ	**คุณประกลกฤษ แสงชูวงศ์** Team Head of Information, Security Detection and Response ธนาคารทหารไทย
กรรมการ	**คุณยศ กิมสวัสดิ์** Head of Payment System Office สมาคมธนาคารไทย
คณะเลขานุการ	**คุณกิติศักดิ์ จิรวรรณกูล** CERT Manager
	คุณปิลันญา เชิญถนอมวงศ์ CERT Manager
	คุณธาวินี วงศ์วิศว์ CERT Relations Manager

หน่วยงานสมาชิก TB-CERT

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร Bank of Agriculture and Agricultural Cooperatives	ธนาคารกรุงไทย จำกัด (มหาชน) Krung Thai Bank Public Company Limited
ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน) Bank of Ayudhya Public Company Limited (Krungsri)	ธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน) Land and Houses Bank Public Company Limited
ธนาคารกรุงเทพ จำกัด (มหาชน) Bangkok Bank Public Company Limited	ธนาคารมิซูโฮ จำกัด สาขากรุงเทพฯ Mizuho Bank Bangkok Branch
ธนาคารแห่งประเทศไทย Bank of Thailand	บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด National Credit Bureau Company Limited
ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน) CIMB Thai Bank Public Company Limited	บริษัท ศูนย์ประมวลผล จำกัด Processing Center Company Limited
ธนาคารซิตี้แบงก์ Citibank N.A.	ธนาคารไทยพาณิชย์ จำกัด (มหาชน) The Siam Commercial Bank Public Company Limited
ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย Export-Import Bank of Thailand	ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน) Standard Chartered Bank (Thai) Public Company Limited
ธนาคารอาคารสงเคราะห์ Government Housing Bank	ธนาคารธนชาต จำกัด (มหาชน) Thanachart Bank Public Company Limited
ธนาคารออมสิน Government Savings Bank	ธนาคาร ไทยเครดิต เพื่อรายย่อย จำกัด (มหาชน) The Thai Credit Retail Bank Public Company Limited
ธนาคาร ไอซีบีซี (ไทย) จำกัด (มหาชน) Industrial and Commercial Bank of China (Thai) Public Company Limited (ICBC Thai)	ธนาคารทิสโก้ จำกัด (มหาชน) TISCO Bank Public Company Limited
ธนาคารอิสลามแห่งประเทศไทย Islamic Bank of Thailand	ธนาคารทหารไทย จำกัด (มหาชน) TMB Bank Public Company Limited
บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด National ITMX Company Limited	ธนาคารยูโอบี จำกัด (มหาชน) United Overseas Bank (Thai) Public Company Limited
ธนาคารกสิกรไทย จำกัด (มหาชน) KASIKORNBANK Public Company Limited	บริษัท วีซ่า อินเตอร์เนชั่นแนล ประเทศไทย จำกัด Visa International (Thailand) Ltd.
ธนาคารเกียรตินาคินภัทร จำกัด (มหาชน) Kiatnakin Phatra Bank Plc.	

Cybersecurity is not IT alone,
It is for everyone's responsibility

TB-CERT
Thailand Banking Sector CERT

4th Fl., 5/13 Moo 3, Chaengwattana Rd.,
Pakkret, Nonthaburi 11120