Thailand Banking Sector CERT

TB-CERT
Thailand Banking Sector CERT

ANNUAL REPORT 2018

The Thai Bankers' Association
4th Fl., 5/13 Moo 3, Chaengwattana Rd.,
Pakkret, Nonthaburi 11120
Phone: 025587500
Website: www.tba.or.th

รายงานผลการดำเนินงาน
ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
(Thailand Banking Sector CERT: TB-CERT)
ปี 2561

จัดทำโดย
กิตติ โฆษะวิสุทธิ์
ศลิษา แซ่เล้า
กิติศักดิ์ จิรวรรณกูล
ธาวินี วงศ์วิศว์
ชญานิน แก้วหาญ

ที่ปรึกษา
กิตติ โฆษะวิสุทธิ์

บรรณาธิการ
ธาวินี วงศ์วิศว์

ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
(Thailand Banking Sector CERT: TB-CERT)
สมาคมธนาคารไทย
5/13 หมู่ 3 ตำบลคลองเกลือ อำเภอปากเกร็ด จังหวัดนนทบุรี 11120
0 2558 7500
contact@tb-cert.or.th

เผยแพร่เมื่อ
กุมภาพันธ์ 2562

TB-CERT ANNUAL REPORT 2018

สารบัญ

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 และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อไม่ว่าจะเกิดกับบุคลากร ลูกค้า หรือธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและต่างประเทศ เพื่อให้สามารถรับรู้ข่าวสารและช่วยเหลือในการแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์และพร้อมรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การดำเนินงาน

การดำเนินงานของ TB-CERT จะครอบคลุม 4 ด้านที่สำคัญคือ

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

คำนิยม

โดย

ดร. พิเชฐ ดุรงคเวโรจน์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

"บทบาทของ TB-CERT ในการแลกเปลี่ยนข้อมูล สร้างเครือข่ายของผู้เชี่ยวชาญ และสร้างความตระหนักให้กับภาคประชาชน ในด้านความมั่นคงปลอดภัยทางไซเบอร์ ถือเป็นบทบาทที่สำคัญ โดยเฉพาะสำหรับภาคการเงินเองซึ่งถือเป็นโครงสร้างพื้นฐานสารสนเทศที่สำคัญของประเทศ ในการที่จะเตรียมการรับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามที่เปลี่ยนรูปแบบตลอดเวลาได้อย่างรวดเร็วและมีประสิทธิภาพ ซึ่งถือเป็นแนวทางในนโยบายของภาครัฐที่กำลังขับเคลื่อนประเทศในปัจจุบันและอนาคต"

คำนิยม

โดย

คุณปรีดี ดาวฉาย
ประธานสมาคมธนาคารไทย

"นับจากวันที่ธนาคารสมาชิกของสมาคมธนาคารไทย ได้ริเริ่มจัดตั้ง ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ Thailand Banking Sector CERT: TB-CERT ขึ้นเมื่อวันที่ 2 ตุลาคม 2560 TB-CERT ได้มีกิจกรรมต่าง ๆ อย่างต่อเนื่องตามเป้าหมายและแผนงาน (Roadmap) และได้ขยายสมาชิกให้ครอบคลุมสถาบันการเงินของรัฐ ธนาคาร และสาขาธนาคารต่างประเทศ และผู้กำกับดูแลภาคการธนาคาร จนครบถ้วน ทำให้ TB- CERT เป็นองค์กรที่มีบทบาทสำคัญของภาคธนาคารในยุคดิจิทัล

ความสำเร็จที่ผ่านมาของ TB-CERT เกิดจากทีมงาน คณะกรรมการ และสมาชิกของ TB-CERT ที่ได้ร่วมมือกันในกิจกรรมต่าง ๆ ซึ่งผม ในฐานะประธานสมาคมธนาคารไทย ขอขอบคุณ และชมเชย ในความทุ่มเทของผู้เกี่ยวข้องที่ได้กล่าวถึงข้างต้น

เมื่อมองไปข้างหน้า ภายใต้การเปลี่ยนแปลงการทำธุรกิจการธนาคารที่เป็นดิจิทัล TB-CERT จะต้องเผชิญกับความท้าทายที่จะต้องยกระดับขีดความสามารถให้สูงขึ้นตาม Roadmap ที่กำหนดไว้ เพื่อให้รองรับภัยไซเบอร์ที่นับวันจะมีพัฒนาการและความรุนแรงที่เพิ่มขึ้น สมาคมธนาคารไทยพร้อมที่จะให้การสนับสนุนกิจกรรมต่าง ๆ ของ TB-CERT เพื่อให้ TB-CERT มีความเข้มแข็ง พร้อมที่จะเป็นกลไกที่ช่วยให้ลูกค้าและภาคธนาคารดำเนินธุรกรรมต่าง ๆ ได้อย่างปลอดภัย ซึ่งจะเป็นพื้นฐานที่สำคัญของการพัฒนาเศรษฐกิจดิจิทัลของประเทศต่อไป"

สารจากคณะกรรมการ

“กระบวนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ จำเป็นอย่างยิ่งที่องค์กรจะต้องนำมาทบทวน ปรับเปลี่ยน และฝึกซ้อมอย่างสม่ำเสมอ เพื่อให้ทันกับภัยไซเบอร์ใหม่ ๆ ที่นับวันยิ่งเพิ่มมากขึ้นอย่างมีนัยสำคัญ”

ยศ กิมสวัสดิ์

“Decisive response grows organizational resiliency but reactive response does not”

ดร.กิตติ โฆษะวิสุทธิ์

“จากกลุ่มเล็ก ๆ ของ TB-CERT วันนี้เราเป็นชุมชนที่มีพัฒนาการแบบก้าวกระโดด จนได้รับการยอมรับจากสังคมรอบข้าง นับว่าเป็นปีที่ดีของเรา”

สมหมาย ฟองน้ำทิพย์

“Security ไม่ใช่เรื่องของ Do & Don't แต่เป็นเรื่องการจัดการความเสี่ยง ซึ่ง เลือกได้ ...”

นฤดม รุ่งศิริวงศ์

สารจากคณะกรรมการ

"พันธกิจของ TB-CERT ในปีที่ผ่านมา ไม่เพียงแค่การรับมือและประสานงานให้ความช่วยเหลือธนาคารสมาชิก เรายังมุ่งเน้นไปในเชิงรุกในการแชร์ข้อมูลข่าวสาร การซ้อมรับมือ และการพัฒนาความรู้ให้กับสมาชิก และบุคลากรที่เกี่ยวข้องของธนาคาร ซึ่งเราจะพัฒนาให้ดียิ่ง ๆ ขึ้นต่อไป รวมถึงการบริการวิจัยพัฒนาด้าน Cybersecurity ให้กับภาคธนาคาร เพื่อให้สมาชิกได้ประโยชน์สูงสุดในปีนี้และต่อ ๆ ไป"

ศลิษา แซ่เล้า

"เกิด Dynamic จากการพบปะแลกเปลี่ยนข้อมูล ความรู้ ความคิดเห็น และประสบการณ์จากสมาชิกแต่ละคน ซึ่งสิ่งนี้จะขับเคลื่อนให้สมาชิกมี Cyber Defense ที่แข็งแกร่งยิ่งขึ้น"

อารยาภา พานิชปรีชา

"ดีใจครับ ที่เห็นความร่วมมือกันของสมาชิก TB-CERT ทุกคน ทุกธนาคาร เต็มใจแชร์ความรู้และช่วยกันทำเพื่อความมั่นคงและปลอดภัยของระบบการเงินการธนาคารของประเทศเราครับ"

สมบูรณ์ หิรัญภัทรศิลป์

การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยกับความอยู่รอดขององค์กรจากภัยไซเบอร์ (1/2)

บทความประจำปี

ในช่วงเวลาที่เทคโนโลยีดิจิทัลกำลังเข้ามาเปลี่ยนแปลงสภาพการใช้ชีวิตประจำวัน ความเป็นอยู่ สภาพแวดล้อมในการทำงานอย่างรวดเร็ว จนทำให้ต้องมีการปรับเปลี่ยนกระบวนการทำงาน ปรับตัวให้เข้ากับเทคโนโลยีใหม่ๆ หรือแม้กระทั่งจะต้องปรับมุมมองที่มีต่อความเปลี่ยนแปลงซึ่งหน้า เพื่อให้สามารถช่วยผลักดันองค์กรผ่านช่วงการเปลี่ยนแปลงที่สำคัญนี้ไปให้ได้ การเปลี่ยนแปลงนี้ไม่ได้มาลำพัง แต่มาพร้อมกับภัยคุกคามที่ใช้เทคโนโลยีดิจิทัล ผ่านเครือข่ายการเชื่อมต่อที่ไปได้ถึงทุกมุมโลก หรือที่เรียกกันว่าภัยทางโลกไซเบอร์ซึ่งมีความซับซ้อนมากขึ้น โดยการโจมตีจากภัยดังกล่าว จะอาศัยช่องว่างของความเข้าใจในเทคโนโลยีที่เกิดจากการเปลี่ยนแปลงไปอย่างรวดเร็ว จนทำให้ผู้ใช้งานเรียนรู้หรือสร้างความเข้าใจในการใช้งานไม่ทัน และทำให้เกิดช่องโหว่ที่ผู้ไม่ประสงค์ดีอาจจะหยิบมาใช้ประโยชน์ เช่น การหลอกให้หลงเชื่อโดยซ่อนซอฟท์แวร์ในการขโมยข้อมูลมาด้วย ซึ่งผู้ใช้ไม่สามารถแยกแยะความแตกต่างได้ เป็นต้น

วิธีการลดความเสี่ยงจากภัยไซเบอร์ที่คุ้นเคยและมักจะเป็นเรื่องแรกที่คิดถึงคือการป้องกัน (Protection) ไม่ให้ภัยคุกคามนั้นเข้ามาในองค์กรหรือเข้ามาถึงสินทรัพย์ที่สำคัญขององค์กร วิธีลดความเสี่ยงดังกล่าวด้วยการสร้างแนวป้องกันนี้ ก็ยังคงเป็นวิธีที่ต้องคงอยู่ แต่จากเหตุการณ์ด้านความปลอดภัยที่เกิดขึ้นและเป็นข่าว หากสังเกตกันให้ดีแล้ว จะเห็นว่าการบุกรุกดังกล่าวหลุดรอดแนวป้องกันไปได้ ผู้บุกรุกย่อมหาแนวทางในการหลบหลีกแนวป้องกันที่วางไว้แม้ว่าองค์กรจะทุ่มงบลงทุนสักเท่าไร แม้ว่าจะทุ่มเทพลังงานให้การที่จะป้องกันหรือติดตามข้อมูลเกี่ยวกับภัยคุกคามสักเท่าไร ก็ยังจะมีความเป็นไปได้ที่ผู้บุกรุกจะเข้าถึงองค์กรไม่ว่าจะเป็นทางช่องโหว่ของเทคโนโลยี หรือช่องโหว่ที่เกิดจากคนด้วยเทคนิค Social Engineering

การลงทุนเพื่อเสริมสร้างความมั่นคงปลอดภัยให้มีความสามารถในการสร้างการรับรู้สภาพการณ์ (Visibility) ที่ดีขึ้น หรือก็คือเทคโนโลยีจำพวกที่มีความสามารถการตรวจจับสิ่งผิดปกติ ไม่ว่าจะเป็นแบบที่ตรวจจับด้วย signature หรือจะเป็นการตรวจจับพฤติกรรมโดยมีการวิเคราะห์แยกแยะพฤติกรรมของการใช้งานของผู้ใช้งาน ออกจากพฤติกรรมที่มุ่งขโมยข้อมูลเปลี่ยนแปลงสิทธิ หรือเพื่อเข้าควบคุมระบบงาน ข้อมูลที่ได้จากการตรวจจับด้วย Signature แสดงถึงภัยคุกคามที่มีผู้ค้นพบและเทคโนโลยีที่องค์กรใช้มีความสามารถในการตรวจจับ ซึ่งถือว่าเป็น Known Problem หรือคือปัญหาที่องค์กรรับรู้ ปัญหาที่ถูกประกาศให้รับทราบกันไว้ก่อนและจะเชื่อมต่อไปถึงการมีแนวทางในการจัดการกับปัญหานั้น ในบางครั้งอาจจะมาใช้เป็นสถิติในการประเมินแนวโน้มหรือตัวบ่งบอกถึงแนวโน้มของภัยคุกคามได้ แต่หากเป็นพฤติกรรมที่ผิดปกติใหม่ที่ยังไม่มีองค์กรใดเคยพบเจอ ซึ่งรูปแบบการโจมตีนั้นอาจจะถูกสร้างมาเพื่อโจมตีเป้าหมายเฉพาะเจาะจง (Targeted Zero-Day Attack) ซึ่งถือว่ากำลังเผชิญกับ Unknown Problem หรือปัญหาที่ยังไม่เคยรู้มาก่อน ปัญหาในลักษณะนี้นอกจากจะมีความยากเป็นอย่างยิ่งในการรับมือแล้ว การโจมตีลักษณะเช่นนี้จะพยายามที่จะหลบหลีกแนวการป้องกัน (Protection) และกลไกในการตรวจจับ (Detection) สิ่งที่จะเป็นสัญญาณของการบุกรุกคงจะเหลือแต่ร่องรอยของพฤติกรรมบางอย่างที่บ่งบอกถึงความพยายามในการเปลี่ยนแปลงสิทธิ การเคลื่อนตัวไปยังเป้าที่น่าสนใจ (Lateral Movement) การที่องค์กรตรวจพบพฤติกรรมที่น่าสงสัยดังกล่าว กระบวนการตอบสนองต่อสิ่งที่พบหรือสิ่งที่เกิดขึ้นในองค์กร (Incident Response) โดยเฉพาะเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์เป็นสิ่งที่สำคัญ ทั้งนี้เพื่อเป้าหมายที่จะจำกัดความเสียหายให้ได้เร็วที่สุด ลดระยะเวลาที่จะกู้คืนบริการก่อนที่จะลุกลามกว้างไกล และก็ยังช่วยจำกัดค่าใช้จ่ายที่สูงที่อาจจะตามมาจากสถานการณ์ที่ขยายวงและสร้างผลกระทบกว้างขึ้น

การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย กับความอยู่รอดขององค์กรจากภัยไซเบอร์ (2/2)

Incident Response จึงเป็นกลไกสำคัญในการเตรียมความพร้อมให้กับองค์กรสำหรับภัยคุกคามที่ไม่มีข้อมูลหรือไม่สามารถระบุถึงภัยคุกคามได้ (Unknown Threat) องค์กรจำเป็นต้องเตรียมโครงสร้างทีมที่มีความสามารถในการวิเคราะห์สัญญาณเตือนภัยต่าง ๆ ไม่ว่าจะมาจากอุปกรณ์ใด ๆ ในองค์กรที่สามารถบ่งชี้ถึงกิจกรรมที่อาจจะเป็นร่องรอยของการสอดส่อง สืบค้น คืบคลานไปเพื่อที่จะหาเป้าหมายที่ต้องการของผู้บุกรุก การนำข้อมูลดังกล่าวมาวิเคราะห์ร่วมกับข้อมูลจาก Cyber Threat Intelligence (CTI) หรือคือข้อมูลบ่งชี้ถึงการโจมตี (Indicator of Compromise) โดยจะต้องมีการวางเป้าหมายหรือพฤติกรรมของการโจมตีที่องค์กรสนใจ เพื่อที่จะนำมาซักซ้อมแผนเตรียมความพร้อมให้กับผู้ที่เกี่ยวข้องทุกฝ่าย โดยเฉพาะวิธีการสื่อสารกันภายในองค์กร เพื่อให้เกิดการประเมินสถานการณ์และผลกระทบกับองค์กรได้ถูกต้องที่สุดตามสภาพการณ์ที่เกิดขึ้น การสื่อสารกับหน่วยงานภายนอกองค์กรเพื่อที่จะสร้างความเข้าใจกับสาธารณะต่อสถานการณ์ได้อย่างถูกต้อง อันจะเป็นการควบคุมมิให้ตื่นตระหนกต่อเหตุการณ์จนเกินไป

เมื่อมีเหตุการณ์การคุกคามทางไซเบอร์เกิดขึ้น การเก็บข้อมูลเพื่อการวิเคราะห์สถานการณ์เป็นขั้นตอน จะช่วยให้เข้าใจขอบเขตของความเสียหายและสามารถประเมินแนวทางการรับมือ แนวทางการแก้ไขสถานการณ์ ควบคุมสถานการณ์ ไปจนถึงแนวทางในการกู้คืนบริการจากความเสียหาย โดยในทางปฏิบัติแล้ว ข้อมูลที่จะนำมาใช้เพื่อการวิเคราะห์สภาพการณ์ของเหตุการณ์มักจะต้องพัฒนาขึ้นไปตามเวลา ตามประสบการณ์ และความสามารถของบุคลากรในองค์กร เมื่อควบคุมและแก้ไขเหตุการณ์ให้สงบลงได้แล้ว จะต้องมีการรวบรวมข้อมูลการดำเนินการแก้ไขสถานการณ์ที่ได้ดำเนินการไปเพื่อที่จะนำมาวิเคราะห์หาจุดบกพร่อง เพื่อเพิ่มประสิทธิภาพในการจัดการกับเหตุการณ์ และเกิดการเรียนรู้ของผู้ที่เกี่ยวข้องในองค์กร (Learning Organization)

การพัฒนาความรู้ความสามารถ การเสริมสร้างประสบการณ์ เพื่อให้เกิดทักษะพร้อมในการรับมือจึงเป็นเป้าหมายหนึ่งของ TB-CERT ในการที่จะช่วยให้ธนาคารสมาชิกรวมทั้งหน่วยงานที่เกี่ยวข้องกับการให้บริการสำคัญของภาคการธนาคาร ได้มีความรู้ความสามารถในการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย มีการซักซ้อมแผนรับมือภัยคุกคามทางไซเบอร์ร่วมกัน เพื่อเป็นการสร้างเครือข่ายในการเฝ้าระวัง ช่วยกันวิเคราะห์สถานะการณ์และยกระดับการเตรียมความพร้อมในการรับมือภัยไซเบอร์ และสร้างความแข็งแกร่งให้กับภาคการธนาคารของประเทศไทยด้านความมั่นคงปลอดภัย ซึ่งจะเป็นพื้นฐานที่สำคัญสำหรับธุรกิจในการก้าวสู่ยุคดิจิทัลได้อย่างมั่นคง

ดร.กิตติ โฆษะวิสุทธิ์
ประธานกรรมการ TB-CERT

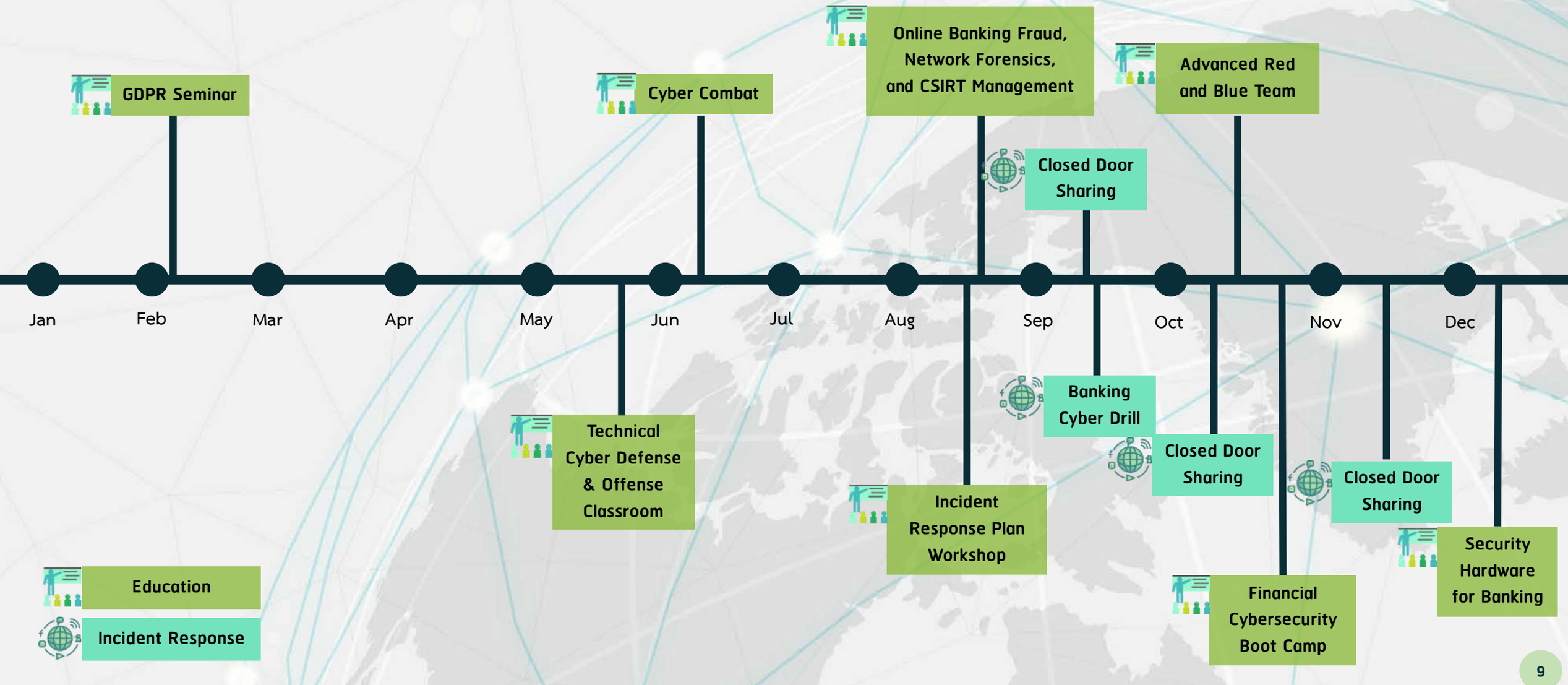



กิจกรรมในปี 2561

Timeline กิจกรรมในปี 2561

พันธกิจของ TB-CERT ที่ทำอย่างต่อเนื่องตลอด 2 ปี ที่ผ่านมา เราได้เน้นการสร้างรากฐานของ TB-CERT ให้มีความมั่นคงแข็งแรงเพื่อให้สมาชิกมีกรอบในการแลกเปลี่ยนข้อมูลอย่างไว้วางใจซึ่งกันและกัน รวมถึงการยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับทุกภาคส่วนของหน่วยงานสมาชิก โดยการพัฒนาบุคลากร สร้างความตระหนักรู้ให้กับสาธารณะ และสร้างมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์เพื่อให้ทุกธนาคารมีหลักการและหลักปฏิบัติร่วมกัน

จากการที่นายกรัฐมนตรี พลเอก ประยุทธ์ จันทร์โอชากล่าวในงาน Thailand Digital Big Bang 2017 ว่าต้องการบุคลากรในด้านนี้เป็นจำนวนมาก จึงเห็นว่าแนวโน้มในปี 2561 นี้รัฐบาลจะดำเนินการผลิตบุคลากรด้านนี้เข้าสู่ตลาด ทำให้เรา TB-CERT ในฐานะที่เป็นส่วนหนึ่งของประเทศที่สามารถส่งเสริมนโยบายนี้เพื่อเพิ่มศักยภาพของประเทศดำเนินแผนการพัฒนาบุคลากรด้าน Cybersecurity ของภาคการเงินการธนาคารให้มีศักยภาพทัดเทียมกับระดับสากล จึงเล็งเห็นถึงการพัฒนาบุคลากรซึ่งเป็นทรัพยากรที่สำคัญที่สุดขององค์กรและเป็นที่ขาดแคลนอย่างมากในอุตสาหกรรมการเงินการธนาคาร ได้จัดให้มีการให้ความรู้กับบุคลากรของหน่วยงานสมาชิกในทุกระดับ ตั้งแต่ระดับเจ้าหน้าที่ผู้ปฏิบัติการ จนถึงผู้บริหารระดับสูง ทั้งในแง่ของการเรียนรู้เชิงเทคนิคและเชิงบริหาร การสร้าง Awareness และมากไปกว่านั้น เราได้เรียนรู้กับการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์เพื่อรับมือกับภัยไซเบอร์ที่อาจเกิดขึ้นอยู่ตลอดเวลาอย่างทันท่วงที โดยจะเห็นจากกิจกรรมตลอดทั้งปี 2561 นี้



สรุปกิจกรรมในปี 2561

GDPR Seminar

TB-CERT ร่วมกับชมรม Compliance สมาคมธนาคารไทยและบริษัท ไมโครซอฟท์ ประเทศไทย ในการจัดงานสัมมนา หัวข้อ “Are you ready for GDPR in May 2018” เพื่อเผยแพร่ความรู้ความเข้าใจและเตรียมความพร้อมสำหรับการบังคับใช้กฎหมายให้ความคุ้มครองข้อมูลส่วนบุคคลของผู้บริโภคฉบับใหม่ของ EU หรือ General Data Protection Regulation (GDPR) และให้ธนาคารไทยเข้าใจถึงผลกระทบของ GDPR ต่อการดำเนินธุรกิจในประเทศไทย

Technical Cyber Defense & Offense Classroom

“หลักสูตรพัฒนาและฝึกทักษะการโจมตีและป้องกันภัยไซเบอร์” มีวัตถุประสงค์เพื่อฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์แบบ Technical Simulation ซึ่งลักษณะของการฝึกจะแบ่งออกเป็น 2 ทีม ได้แก่ Red Team (การโจมตี) และ Blue Team (การป้องกัน) เพื่อเสริมสร้างทักษะให้กับบุคลากรของหน่วยงานสมาชิก โดยฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นซึ่งเป็นการจำลองสถานการณ์จริง

Cyber Combat

การแข่งขัน“TB-CERT Cyber Combat” ได้จัดต่อเนื่องจากการอบรมหลักสูตรพัฒนาและฝึกทักษะการโจมตีและป้องกันภัยไซเบอร์ ผ่านการฝึกซ้อมรับมือภัยคุกคามแบบ Technical Simulation และยังได้จัดควบคู่กับงานสัมมนา “Know Your Enemy, Know Yourself” ซึ่งได้มีการเผยแพร่ความรู้และประสบการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้กับบุคลากรในอุตสาหกรรมภาคการเงินการธนาคาร และหน่วยงานที่เกี่ยวข้อง

Incident Response Plan Workshop

TB-CERT ร่วมกับธนาคารแห่งประเทศไทยจัดการอบรมเชิงปฏิบัติการ เรื่อง “Cyber Security Incident Response: Policy, Plan and Playbook” เพื่อเสริมสร้างความรู้และฝึกปฏิบัติในการจัดทำแผนรับมือภัยไซเบอร์ และยังได้จัด Clinic Session เพื่อให้ผู้เข้าร่วมอบรมได้นำความรู้ที่ได้ไปจัดทำแผนรับมือภัยไซเบอร์นำมาแลกเปลี่ยนและปรึกษาหารือเพิ่มเติมอีกด้วย

Online Banking Fraud, Network Forensics, and CSIRT Management

Cybersecurity Professional Development Program เป็นการจัดงานสัมมนาหรืออบรมเชิงปฏิบัติการในด้านเทคนิคเพื่อเสริมสร้างและพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ โดยเชิญวิทยากรที่น่าสนใจจากทั้งในและต่างประเทศ กิจกรรมในครั้งนี้จัดขึ้นต่อเนื่อง 2 วันผ่านการอบรม 3 หัวข้อ ได้แก่ Online Banking Fraud, Network Forensics และ CSIRT Management โดยวิทยากรจากบริษัท Group-IB

สรุปกิจกรรมในปี 2561

Banking Cyber Drill

การซ้อมรับมือภัยไซเบอร์ภาคการธนาคารแบบ Table Top Exercise จัดขึ้นต่อเนื่องเป็นครั้งที่ 3 ซึ่งในปีนี้มีผู้เข้าร่วมซักซ้อมถึง 110 คนจาก 22 หน่วยงานสมาชิก ในการซักซ้อมคณะทำงานได้กำหนดเหตุการณ์จำลองเพื่อให้แต่ละหน่วยงานประเมินว่าจะมีแผนในการรับมือกับภัยคุกคามอย่างไร มีกระบวนการแก้ปัญหาอย่างไร ทั้งในเชิงเทคนิคและบริหาร รวมถึงการตัดสินใจในการดำเนินการตามสถานการณ์ที่เกิดขึ้น ช่วยพัฒนาและปรับปรุงกระบวนการรับมือเหตุการณ์ให้มีประสิทธิภาพและเหมาะสมกับภาคการเงินการธนาคารมากขึ้น

Advanced Red and Blue Team

Cybersecurity Professional Development Program ในครั้งนี้ จัดขึ้นในลักษณะของ Cybersecurity Talk ร่วมกับธนาคารแห่งประเทศไทย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โดยเรียนเชิญวิทยากร Mr. Stephen Sims จาก SANS Institute มาบรรยายเรื่อง “Advanced Red and Blue Team: Tactics & Coordination” ณ ธนาคารทิสโก้ อาคารทิสโก้ทาวเวอร์

Financial Cybersecurity Boot Camp

Financial Cybersecurity Boot Camp จัดขึ้นเป็นครั้งที่ 2 ร่วมกับธนาคารแห่งประเทศไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) สำนักงานคณะกรรมการกำกับและส่งเสริมผู้ประกอบธุรกิจประกันภัย และสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ โดยในปีนี้ได้ปรับรูปแบบการจัดงานเป็นเชิงเทคนิคมากขึ้น ผ่านการแข่งขัน Capture The Flag (CTF) รวมทั้งการศึกษาดูงาน ณ Security Operation Center และ Digital Forensics Center มีผู้สนใจเข้าร่วมโครงการถึง 55 ทีม และได้คัดเลือกเข้าร่วมโครงการเพียง 15 ทีม 45 คนเท่านั้น ซึ่งโครงการได้สร้างเครือข่ายระหว่างนิสิตนักศึกษาในสาขาวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ และโอกาสทางอาชีพในสถาบันการเงิน องค์กรกำกับดูแล รวมทั้งหน่วยงานที่เกี่ยวข้อง

Security Hardware for Banking

Cybersecurity Professional Development Program ในครั้งนี้ ได้ร่วมกับคณะวิศวกรรมศาสตร์ มหาวิทยาลัยธรรมศาสตร์ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล และธนาคารแห่งประเทศไทย ในการจัดงานสัมมนาเชิงวิชาการ หัวข้อ “International Workshop in Banking Security with Trusted Hardware” ต่อเนื่อง 2 วัน โดยได้รับเกียรติจากผู้เชี่ยวชาญและอาจารย์ด้านความมั่นคงปลอดภัยไซเบอร์ทั้งในและต่างประเทศ และได้รับความสนใจจากผู้เข้าร่วมอบรมทั้งจากภาคการเงินการธนาคารและอุตสาหกรรมอื่น ๆ อีกด้วย

เหตุการณ์ด้านภัยไซเบอร์ในปี 2561

Timeline เหตุการณ์สำคัญในปี 2561

มกราคม

- Meldown และ Spectre เป็นช่องโหว่ของสถาปัตยกรรมของโพรเซสเซอร์ที่ใช้เทคนิค speculative execution ในการเพิ่มความเร็วในการทำงานซึ่งมีผลให้สามารถขโมยข้อมูลจาก Cache ได้ ซึ่งการแก้ไขด้วย Patch จะทำให้การทำงานของโพรเซสเซอร์ช้าลง

กุมภาพันธ์

- หน่วยงานภาคการเงินของตุรกีตกเป็นเป้าหมายการโจมตีของกลุ่มแฮกเกอร์เกาหลีเหนือ ชื่อ Lazarus (Hidden Cobra) ไม่มีการระบุความเสียหาย

มีนาคม

- ธนาคารกลางมาเลเซีย หรือ Bank Negara Malaysia ตรวจพบความพยายามในการปลอมข้อความร้องขอโอนเงินผ่าน SWIFT แต่ทางธนาคารสามารถยุติการโอนเงินเหล่านั้นได้ทัน
- ข้อมูลประชาชนอินเดียกว่า 1,100 ล้านคนรั่วไหล เหตุเกิดจากบริษัทที่ดูแลระบบอนุญาตให้บุคคลภายนอกเข้ามาดาวน์โหลดข้อมูลทางการเงินและข้อมูลส่วนบุคคลจากฐานข้อมูลที่เก็บข้อมูลประชาชนในประเทศอินเดีย (Aadhaar)

เมษายน

- ผู้ให้บริการโทรศัพท์มือถือในประเทศไทย ตั้งค่าการเข้าถึงข้อมูลลูกค้าของบริษัทที่ถูกเก็บไว้บน AWS S3 Bucket ไม่ปลอดภัยเพียงพอ ส่งผลให้ข้อมูลรูปบัตรประชาชนของลูกค้ากว่า 46,000 รายรั่วไหลสู่สาธารณะ
- หน่วยงานภาคการเงินใน 17 ประเทศทั่วโลก ถูกกลุ่มแฮกเกอร์ Lazarus (Hidden Cobra) โจมตีภายใต้ชื่อปฏิบัติการ GhostSecret มีเชิร์ฟเวอร์จากสถาบันการศึกษาของประเทศไทยถูกเจาะระบบและใช้เป็นฐานในการโจมตีในปฏิบัติการนี้ด้วย

พฤษภาคม

- ธนาคารหลายแห่งในเม็กซิโกถูกแฮกเกอร์โจมตีผ่านระบบโอนเงินมูลค่าสูงระหว่างธนาคารของเม็กซิโกที่ชื่อว่า Interbanking Electronic Payment System (SPEI) โดยพยายามขโมยเงินจำนวน 110 ล้านเหรียญสหรัฐ แต่เหตุการณ์นี้ไม่ได้รับการยืนยันความเสียหายและชื่อธนาคารที่ได้รับผลกระทบ

มิถุนายน

- ธนาคาร Banco de Chile ประเทศชิลี ถูกโจมตีโดยกลุ่มแฮกเกอร์ APT38 จากประเทศเกาหลีเหนือ โดยทำธุรกรรมโอนเงินผ่านระบบ SWIFT 10 ล้านเหรียญสหรัฐ แล้วปล่อยมัลแวร์เพื่อลบข้อมูล (Wiper) ไปยัง 9,000 workstations และ 500 servers

กรกฎาคม

- ธนาคารในประเทศไทยสองแห่งถูกเปิดเผยข้อมูลของลูกค้า อย่างไรก็ตาม ไม่พบความเสียหายทางการเงินใดๆ ในบัญชีของลูกค้า
- ศูนย์การแพทย์สิงคโปร์ (SingHealth) ถูกขโมยข้อมูลส่วนบุคคลของผู้ป่วย 1.5 ล้านบัญชี รวมถึงข้อมูลของนายกรัฐมนตรี Lee Hsien Loong โดยโจมตีที่เครื่องคอมพิวเตอร์ของพนักงานที่มีบัญชีผู้ใช้ที่มีสิทธิ์เข้าถึงฐานข้อมูล
- ธนาคาร PIR ในรัสเซียถูกกลุ่มแฮกเกอร์ MoneyTaker ขโมยเงินเกือบ 1 ล้านเหรียญสหรัฐ โดยเริ่มต้นโจมตีที่เร้าเตอร์ (Router) รุ่นเก่าและไม่มีการสนับสนุนแล้วของธนาคาร

สิงหาคม

- เว็บไซต์ของ Bank of Spain ถูกโจมตีด้วย DDoS (Distributed Denial-of-Service) ส่งผลให้เว็บไซต์ไม่สามารถเข้าใช้งานได้ ภายหลังมีกลุ่มแฮกเกอร์ Anonymous Catalonia อ้างว่าเป็นผู้โจมตีภายใต้ปฏิบัติการที่ชื่อว่า #OpCatalonia
- ธนาคาร Cosmos ประเทศอินเดียสูญเสีย 13.5 ล้านเหรียญสหรัฐ โดยถูกขโมยข้อมูลของบัตรลูกค้า เพื่อปลอมบัตร ATM และใช้ถอนเงินจำนวน 11.5 ล้านเหรียญออกไปผ่านตู้ ATM 14,849 ครั้งจาก 28 ประเทศทั่วโลก นอกจากนี้ ผู้โจมตียังโอนเงินผ่านระบบ SWIFT ไปยังบัญชีที่ประเทศฮ่องกง สร้างความเสียหายอีกเป็นมูลค่า 2 ล้านเหรียญ
- ธนาคาร NS Bank ในประเทศรัสเซีย และธนาคาร Carpatica/Patria ในประเทศโรมาเนีย ถูกโจมตีโดยฝีมือกลุ่มแฮกเกอร์ชื่อ Cobalt โดยใช้มัลแวร์ Coblnt ไม่มีการเปิดเผยมูลค่าความเสียหาย
- บริษัทสายการบิน British Airways ถูกกลุ่มแฮกเกอร์ Magecart เจาะระบบและขโมยข้อมูลส่วนตัวและข้อมูลทางการเงินของลูกค้าไปกว่า 380,000 ราย

พฤศจิกายน

- ธนาคารในประเทศปากีสถานถูกเปิดเผยข้อมูลบัตรเดบิตของลูกค้าชาวปากีสถานเกือบ 200,000 รายการบนดาร์คเว็บ (Dark web) ซึ่งเกี่ยวข้องกับเหตุการณ์ที่ธนาคารอิสลามถูกโจมตีในเดือนตุลาคม และ Pakistan CERT อธิบายว่าข้อมูลน่าจะถูกขโมยด้วยวิธีการ Skimming
- ผู้ให้บริการอินเทอร์เน็ตในประเทศกัมพูชาถูกโจมตีด้วย DDoS ที่รุนแรงที่สุดในประวัติศาสตร์
- ธนาคารในรัสเซียถูกกลุ่มแฮกเกอร์ Silence โจมตีโดยส่งอีเมลแอบอ้างว่าส่งโดยธนาคารกลางรัสเซีย (Central Bank of Russia) และแนบไฟล์เอกสารเพื่อดาวน์โหลดมัลแวร์ Silence.Downloader

ธันวาคม

- บริษัท Marriott International เครือโรงแรมที่ใหญ่ที่สุดในโลก ถูกแฮกเกอร์เจาะระบบฐานข้อมูลการจองที่พัก ทำให้ข้อมูลลูกค้ากว่า 500 ล้านบัญชีรั่วไหล

กันยายน

- เฟสบุ๊ค (Facebook) ถูกเปิดเผยข้อมูลผู้ใช้งานจำนวน 50 ล้านราย และอีก 40 ล้านรายอาจได้รับผลกระทบจากช่องโหว่ในฟีเจอร์ View As ทำให้เฟสบุ๊คต้องรีเซ็ต token ของผู้ใช้ที่ได้รับผลกระทบ
- นักวิจัยเปิดเผยเครื่องมือและเทคนิคที่จะใช้ของกลุ่มแฮกเกอร์รัสเซียชื่อ Silence ที่มีเป้าหมายโจมตีธนาคารในประเทศรัสเซียและยุโรปตะวันออก

ตุลาคม

- ธนาคารอิสลาม (BankIslami) ที่ประเทศปากีสถานถูกโจมตีระบบบัตรของธนาคาร และโอนเงินไปยังบัญชีในประเทศต่าง ๆ ส่งผลให้ธนาคารสูญเสียเงินจำนวนกว่า 6.5 ล้านเหรียญสหรัฐ โดยต้นทางที่มีการใช้งานมาจากประเทศบราซิลและสหรัฐอเมริกา
- สายการบิน Cathay Pacific พบการเข้าถึงข้อมูลผู้โดยสารโดยไม่ได้รับอนุญาตตั้งแต่เดือนมีนาคม 2561 รวมผู้โดยสารที่อาจได้รับผลกระทบ 9.4 ล้านคน
- ธนาคารในรัสเซียถูกกลุ่มแฮกเกอร์ชื่อ MoneyTaker โจมตี ด้วยการปลอมแปลงอีเมล์โดยใช้ชื่อผู้ส่งมาจาก FinCERT ซึ่งแนบไฟล์อันตรายและมีรูปแบบของเอกสารแนบนั้นเหมือนถูกส่งมาจากธนาคารกลางรัสเซีย (Central Bank of Russia)

บทวิเคราะห์เหตุการณ์การโจมตีสถาบันการเงินในปี 2561 (1/2)

ในปี 2561 จากเหตุการณ์การโจมตีของกลุ่มแฮกเกอร์ต่างๆ ทั่วโลก การโจมตีระบบโอนเงินระหว่างประเทศ (SWIFT) ยังเป็นเป้าหมายอันดับแรกของกลุ่มแฮกเกอร์ เนื่องจากระบบนี้เป็นช่องทางหนึ่งที่ทำให้กลุ่มแฮกเกอร์สามารถได้เงินจำนวนมหาศาล โดยจะเห็นว่าเกิดเหตุการณ์การโจมตีระบบ SWIFT ในธนาคารต่าง ๆ ได้สำเร็จในเกือบทุกไตรมาส อย่างไรก็ตามไม่ได้หมายความว่าระบบดังกล่าวมีจุดอ่อนหรือช่องโหว่ แต่ขึ้นอยู่กับวิธีการติดตั้งระบบ วิธีการดูแลรักษาความมั่นคงปลอดภัยของธนาคารที่ติดตั้งระบบนี้ นอกจากนี้ พนักงานธนาคารที่ไม่มีความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเพียงพอก็เป็นจุดอ่อนแรกที่กลุ่มแฮกเกอร์มักจะใช้เป็นช่องทางเริ่มต้นเพื่อก่อเหตุ โดยใช้วิธีการส่งอีเมลประเภทสเปียร์ฟิชชิง (Spear Phishing) ที่เลือกส่งเฉพาะกลุ่มเป้าหมายและหลอกให้เปิดไฟล์มัลแวร์ที่แนบมา ซึ่งไฟล์นี้จะอยู่ในรูปแบบของไฟล์เอกสาร Microsoft Word อีกทั้งไฟล์มัลแวร์นี้ยังมีองค์ประกอบของโปรแกรมเจาะระบบผ่านช่องโหว่ต่าง ๆ ของโปรแกรมพื้นฐานที่ผู้ใช้งานมักจะติดตั้ง เช่น Adobe Flash Player และ Microsoft Office เป็นต้น ซึ่งวิธีการโจมตีลักษณะนี้มีแนวโน้มเพิ่มขึ้นและต่อเนื่องมาจนถึงปี 2562

นอกจากการขโมยเงินจากสถาบันการเงินแล้ว การขโมยข้อมูลสำคัญจากบริษัทต่าง ๆ ยังคงเป็นอีกหนึ่งเป้าหมายของกลุ่มแฮกเกอร์ ซึ่งเกิดได้ทุกภาคอุตสาหกรรม อาจจะเพื่อนำไปสร้างความเสียหายต่อชื่อเสียงของบริษัทนั้น หรือนำไปจำหน่ายในดาร์กเว็บ อย่างไรก็ตามเมื่อวิเคราะห์ถึงผลกระทบที่เกิดขึ้นต่อลูกค้าผู้เป็นเจ้าของข้อมูล บริษัทที่เก็บข้อมูลของลูกค้า รวมถึงความน่าเชื่อถือของบริษัท ทำให้ในบางเหตุการณ์ไม่อาจประเมินมูลค่าความเสียหายได้ ทั้งมูลค่าของข้อมูล ค่าใช้จ่ายในการแก้ไขและปรับปรุงหลังจากเกิดเหตุการณ์ หรือในบางครั้งอาจจะมีค่าปรับที่เกิดขึ้นได้ตามระเบียบการคุ้มครองข้อมูลทั่วไป (General Data Protection Regulation – GDPR)

ไม่เพียงแต่การโจมตีผ่านช่องโหว่ของระบบเพื่อขโมยข้อมูลเท่านั้น ยังมีอีกช่องโหว่หนึ่งที่ทำให้กลุ่มแฮกเกอร์สามารถขโมยข้อมูลได้ คือผู้ดูแลระบบ ไม่ว่าจะเป็นการปรับแต่งค่าการรักษาชั้นความลับของข้อมูลที่ไม่เหมาะสมในการใช้คลาวด์ Amazon S3 Bucket การเปิดสิทธิ์อนุญาตให้บุคคลภายนอกสามารถดาวน์โหลดข้อมูลจากเซิร์ฟเวอร์ ยังคงเป็นเรื่องที่ผู้ดูแลระบบควรระมัดระวังในการดูแลรักษาความมั่นคงปลอดภัย รวมถึงการป้องกันการโจมตีแบบ DDoS ที่ยังคงเกิดขึ้นในช่วงปี 2561 ที่ผ่านมา

สำหรับกลุ่มแฮกเกอร์หลากหลายกลุ่มที่อยู่เบื้องหลังเหตุการณ์การโจมตีต่าง ๆ ทั่วโลกนั้น มีกลุ่มแฮกเกอร์ 5 กลุ่มที่มีความเคลื่อนไหวในการโจมตีสถาบันการเงินอย่างต่อเนื่อง และทำให้ต้องเฝ้าระวังอย่างใกล้ชิด ได้แก่ กลุ่ม Lazarus และ APT38 จากประเทศเกาหลีเหนือ รวมทั้ง Cobalt MoneyTaker และ Silence จากประเทศรัสเซีย

Lazarus

ชื่ออื่น: Lazarus Group, HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY
จากประเทศ: เกาหลีเหนือ
ประเทศเป้าหมาย: ทั่วโลก (ไม่ระบุ)

กลุ่มแฮกเกอร์ Lazarus จากประเทศเกาหลีเหนือ ถูกจัดว่าเป็นกลุ่มแฮกเกอร์ที่มีระดับความสามารถสูง เนื่องจากแฮกเกอร์กลุ่มนี้พัฒนาเครื่องมือโดยเฉพาะ โดยหลาย ๆ เหตุการณ์จะใช้อีเมลส่งไฟล์แนบที่เป็นเอกสาร Microsoft Word ที่มีโค้ดอันตรายเพื่อโจมตีช่องโหว่ของโปรแกรม Adobe Flash Player (CVE-2018-4878) และฝังมัลแวร์ตระกูล Bankshot เพื่อขโมยข้อมูลส่งไปยังเครื่องเซิร์ฟเวอร์ที่อยู่ในระบบเครือข่ายของ C&C ที่แบ่งเป็น 3 ชั้น และมีการเข้ารหัสในการเชื่อมต่อด้วย ซึ่งเป็นรูปแบบเฉพาะของกลุ่มแฮกเกอร์นี้ นอกจากนี้ยังมีการตรวจสอบพบว่ามีเครื่องเซิร์ฟเวอร์ของสถาบันการศึกษาในประเทศไทยถูกเจาะระบบและถูกใช้เป็น C&C ในเครือข่ายของกลุ่มแฮกเกอร์อีกด้วย

บทวิเคราะห์เหตุการณ์การโจมตีสถาบันการเงินในปี 2561 (2/2)

Cobalt

ชื่ออื่น: Cobalt Group Cobalt Gang Cobalt Spider
จากประเทศ: รัสเซีย
ประเทศเป้าหมาย: ประเทศในยุโรปตะวันออก เอเชียกลาง และเอเชียตะวันออกเฉียงใต้

รองลงมาคือกลุ่มแฮกเกอร์ Cobalt ที่มีเทคนิคการเริ่มต้นโจมตีคล้ายกับกลุ่ม Lazarus แม้ว่าเทคนิคจะไม่ได้ซับซ้อนเหมือนกับกลุ่ม Lazarus อย่างไรก็ตามด้วยกลุ่มแฮกเกอร์นี้มีเป้าหมายในประเทศในเอเชียตะวันออกเฉียงใต้และใช้เครื่องมือเฉพาะกลุ่ม จึงทำให้ควรยกระดับการเฝ้าระวังให้สูงขึ้น ซึ่งการโจมตีเริ่มต้นใช้ Spear Phishing โดยปลอมเป็นสถาบันการเงินหรือ Supplier/Partner ของสถาบันการเงินนั้น พร้อมทั้งแนบไฟล์เอกสาร Microsoft Word ที่สามารถโจมตีผ่านช่องโหว่ของโปรแกรม Microsoft Office หมายเลข CVE-2017-8570, CVE-2017-11882, และ CVE-2018-0802 และดาวน์โหลดมัลแวร์ชื่อ CobInt รวมถึงส่วนประกอบอื่น ๆ ของมัลแวร์นี้ ซึ่งเป็นเครื่องมือเฉพาะของกลุ่มแฮกเกอร์นี้

MoneyTaker

ชื่ออื่น: -
จากประเทศ: รัสเซีย
ประเทศเป้าหมาย: ทั่วโลก

อันดับสามเป็นของกลุ่มแฮกเกอร์ MoneyTaker ที่มีเทคนิคค่อนข้างหลากหลายและแตกต่างจากกลุ่มแฮกเกอร์อื่น ๆ เช่น ในเหตุการณ์ของธนาคาร PIR ประเทศรัสเซีย กลุ่มแฮกเกอร์ใช้วิธีการเข้าถึงระบบเครือข่ายของธนาคารผ่านเร้าเตอร์รุ่นเก่าและฝังมัลแวร์ด้วย PowerShell จากนั้น กลุ่มแฮกเกอร์เห็นระบบเครือข่ายทั้งหมดของธนาคารและเข้าถึงบัญชีของ AWS CBR (Automated Work Station Client of the Russian Central Bank) ที่ต้องใช้ควบคุมธุรกรรมทางการเงินของธนาคารกลางรัสเซีย แล้วจึงทำการโอนเงินไปยัง 17 บัญชีที่ถูกสร้างไว้ล่วงหน้าแล้วถอนเงินด้วย ATM อย่างรวดเร็ว นอกจากนี้ยังพบการใช้เทคนิคการโจมตีโดยการส่งอีเมลหลอก โดยปลอมว่าส่งมาจากหน่วยงานด้านการรักษาความปลอดภัย พร้อมทั้งแนบไฟล์จำนวน 5 ไฟล์ ซึ่ง 3 ใน 5 ไฟล์ เป็นไฟล์ปกติไม่มีอันตราย ส่วนอีก 2 ไฟล์ทมีมัลแวร์ที่จะถูกติดตั้งและเชื่อมต่อไปยังเซิร์ฟเวอร์ของกลุ่ม

APT38

ชื่ออื่น: -
จากประเทศ: เกาหลีเหนือ
ประเทศเป้าหมาย: ทั่วโลก

ถัดมาอันดับที่สี่ APT38 เป็นกลุ่มแฮกเกอร์จากเกาหลีเหนือ ที่มีความเกี่ยวข้องกับกลุ่มแฮกเกอร์ Lazarus เทคนิคการโจมตีที่ APT38 ใช้ จะเริ่มต้นจากการหลอกล่อเหยื่อเข้าถึงเว็บไซต์ที่มีมัลแวร์ที่เตรียมไว้ จากนั้นจะทำการค้นหาเครื่องเซิร์ฟเวอร์ที่ติดตั้งระบบปฏิบัติการลินุกซ์ที่มีช่องโหว่ของโปรแกรม Apache Struts2 แล้วจึงเริ่มติดตั้งมัลแวร์ต่าง ๆ เพื่อค้นหาการเชื่อมต่อไปยังระบบ SWIFT และทำธุรกรรมโอนเงิน สุดท้ายเมื่อขโมยเงินได้สำเร็จ จะทำการลบข้อมูลบันทึกการเข้าถึงต่าง ๆ โดยการติดตั้งมัลแวร์ลบข้อมูลเพื่อทำลายข้อมูลบันทึกการเข้าถึงต่าง ๆ ด้วย

Silence

ชื่ออื่น: -
จากประเทศ: รัสเซีย
ประเทศเป้าหมาย: รัสเซีย

อันดับสุดท้ายกลุ่มแฮกเกอร์ Silence ถึงแม้ว่าเป็นกลุ่มเล็กกว่าทั้ง 4 กลุ่มที่ได้กล่าวมา เทคนิคที่ใช้ก็คล้ายกับแฮกเกอร์กลุ่มอื่น ๆ แต่มีเป้าหมายที่ธนาคารในประเทศรัสเซีย จึงทำให้อีเมลที่ส่งนั้นแอบอ้างว่าส่งมาจากธนาคารกลางรัสเซีย (Central Bank of Russia) ให้ผู้รับเปิดไฟล์เอกสารที่มีไฟล์บีบอัดเพื่อดาวน์โหลดมัลแวร์ Silence.Downloader ซึ่งเป็นเครื่องมือเฉพาะของแฮกเกอร์กลุ่มนี้ อย่างไรก็ตามตรวจสอบพบว่าลักษณะอีเมลหลอกนี้ มีลักษณะเหมือนกับอีเมลที่ถูกส่งโดยธนาคารกลางรัสเซียจริง ทำให้สันนิษฐานเพิ่มเติมได้ว่าสมาชิกของแฮกเกอร์กลุ่มนี้น่าจะเคยมีความเกี่ยวข้องกับธนาคารกลางรัสเซีย บางแหล่งข้อมูลบอกว่าแฮกเกอร์กลุ่มนี้น่าจะรับจ้างเจาะระบบให้ธนาคารดังกล่าว

เพื่อลดความเสี่ยงที่อาจเกิดจากเกิดเหตุการณ์การโจมตีสถาบันการเงินในประเทศไทย ในการนี้ ทางศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร หรือ TB-CERT และสมาชิกทั้งหมด ให้ความสำคัญในการเฝ้าระวังและติดตามสถานการณ์ต่าง ๆ รวมทั้งเครื่องมือและเทคนิคที่กลุ่มแฮกเกอร์เหล่านี้ใช้อย่างใกล้ชิด พร้อมทั้งให้ความช่วยเหลือกันในการแจ้งเตือนและหาแนวทางป้องกันร่วมกัน ทั้งนี้เพื่อช่วยให้สมาชิกทั้งหมดมีความมั่นคงปลอดภัย พร้อมเป็นการยกระดับความมั่นคงปลอดภัยให้กับภาคการธนาคารของประเทศไทยอีกด้วย

แนวโน้มภัยคุกคามด้านไซเบอร์ 2562 (1/2)

1. อีเมลฟิชชิงที่เหมือนอีเมลจริงมากขึ้น

จากการวิเคราะห์เหตุการณ์การโจมตีในปี 2561 พบว่ากลุ่มแฮกเกอร์ต่าง ๆ มักจะใช้อีเมลฟิชชิงเป็นจุดเริ่มต้นในการโจมตี โดยในช่วงปลายปีพบว่ากลุ่มแฮกเกอร์หลายกลุ่มมักจะเลือกปลอมอีเมลให้เหมือนกับองค์กรที่มีหน้าที่กำกับดูแลธนาคารในประเทศนั้นๆ อีกทั้งไฟล์เอกสารแนบก็ยังเลียนแบบรูปแบบของเอกสารนั้นได้เหมือนกับเอกสารจากหน่วยงานนั้นจริง ๆ ถึงแม้ว่าแนวโน้มของอีเมลฟิชชิงในปี 2562 นี้ยังคงรูปแบบเดิม แต่เพิ่มลักษณะอีเมลและไฟล์แนบจะเหมือนกับอีเมลจริงจากองค์กรที่ถูกแอบอ้างมากยิ่งขึ้น

2. มัลแวร์ไร้ไฟล์ (Fileless malware) ถูกใช้มากขึ้น

มัลแวร์ที่แนบมาพร้อมกับอีเมลฟิชชิง จากเดิมที่กลุ่มแฮกเกอร์ใช้ไฟล์แนบที่ฝังโค้ดอันตรายในรูปแบบของไฟล์ Microsoft Word และสามารถโจมตีช่องโหว่ของแอปพลิเคชันพื้นฐานต่าง ๆ เช่น Microsoft Office หรือ Adobe Flash Player ฯลฯ โดยจะเปลี่ยนไปเป็นรูปแบบของมัลแวร์ไร้ไฟล์ (Fileless Malware) หรือ Script-based Malware ซึ่งเป็นรูปแบบของมัลแวร์ที่พัฒนาเพื่อหลบหลีกระบบตรวจจับแบบเดิม โดยจะอาศัยการส่งสคริปต์ที่เป็น Payload ของมัลแวร์เข้าไปทำงานในหน่วยความจำโดยตรง โดยไม่จำเป็นต้องมีการสร้างไฟล์ใด ๆ ลงบนฮาร์ดดิสก์ ส่งผลทำให้การตรวจจับของระบบป้องกันต่าง ๆ ก็จะทำได้ยากขึ้น รวมถึงเมื่อต้องการพิสูจน์พยานหลักฐานทางดิจิทัล (Digital Forensics) ก็จะยิ่งทำได้ยาก เนื่องจากการค้นหาร่องรอยของมัลแวร์ที่อยู่ในหน่วยความจำที่มีโอกาสเสียหายได้เมื่อมีการรีสตาร์ทเครื่อง

รูปแบบการโจมตีของมัลแวร์ไร้ไฟล์จะถูกพบในหลากหลายลักษณะ เริ่มต้นด้วยมัลแวร์จะถูกส่งมาในรูปแบบของสคริปต์ PowerShell (.ps1) ซึ่งเป็นเครื่องมือที่มีไว้ให้ผู้ดูแลระบบสามารถใช้ช่วยในการบริหารจัดการระบบ ซึ่งไม่จำเป็นต่อผู้ใช้งานวินโดวส์ส่วนใหญ่ ด้วยเหตุนี้เองกลุ่มแฮกเกอร์จึงเลือกรูปแบบของไฟล์ประเภทนี้ในการทำงาน อีกทั้งมัลแวร์ไร้ไฟล์ที่ใช้รูปแบบ Javascript (.js) ซึ่งเป็นการพัฒนาด้วยภาษาจาวาสคริปต์ เป็นอีกหนึ่งรูปแบบไฟล์ที่กลุ่มแฮกเกอร์จะใช้ในการส่งมัลแวร์ นอกจากนี้ยังมีไฟล์อีกหลายประเภทที่สามารถนำมาสร้างมัลแวร์ไร้ไฟล์ได้ ดังตารางที่ 1

ตารางที่ 1 แสดงรูปแบบของไฟล์ที่ใช้สร้างมัลแวร์ไร้ไฟล์

รูปแบบของไฟล์	รายละเอียดประเภทของไฟล์	องค์ประกอบของวินโดวส์ที่ใช้รัน
.CHM	Compiled HTML help	HTML Help Executable (hh.exe)
.CMD	Microsoft command file	Shell
.CPL	Control Panel	Shell
.DOTM	Macro-enabled document template	Word.exe
.HTA	HTML application	Windows Script Host (wscript.exe)
.JAR	Java application	java.exe
.JS	Javascript	Windows Script Host (wscript.exe)
.LNK	Windows shortcut	Shell
.PIF	Program Information File	Shell
.PS1	PowerShell script	powershell.exe
.SCF	Shell Command File	Shell
.VBS	Visual Basic Script	Windows Script Host (wscript.exe)
.WSF	Windows Script File	Windows Script Host (wscript.exe)

แนวโน้มภัยคุกคามด้านไซเบอร์ 2562 (2/2)

3. มัลแวร์ที่ผสมผสานความสามารถในการโจมตี

ปี 2561 ที่ผ่านมาจำนวนมัลแวร์ประเภท Crypto Miner ใหม่ ๆ เพิ่มขึ้นอย่างมาก ทั้งนี้อาจเป็นเพราะ Crypto Miner สามารถทำรายได้ให้กับแฮกเกอร์ได้ง่ายกว่า Ransomware และ Banking Trojan อย่างไรก็ตามรูปแบบของมัลแวร์เหล่านี้ในปี 2562 จะเป็นลักษณะการผสมผสานการทำงานกันของมัลแวร์ทั้ง 3 ชนิด (Ransomware, Crypto Miner และ Banking Trojans) เพื่อทำให้มัลแวร์มีความสามารถที่ซับซ้อนมากยิ่งขึ้น มีความรุนแรงสูงขึ้น ถูกตรวจจับได้ยากขึ้น อีกทั้งยังอาจเพิ่มโอกาสได้เงินจากเหยื่อมากขึ้นอีกด้วย

4. การขโมยข้อมูลขององค์กรในคลาวด์

ปัจจุบันหลายองค์กรใช้บริการคลาวด์เพิ่มขึ้น โดยมีวัตถุประสงค์เพื่อเก็บข้อมูลสำคัญ ให้บริการแก่บุคคลทั่วไป หรือประมวลผลข้อมูลเพื่อการประชาสัมพันธ์ เป็นต้น ดังนั้นในปี 2562 นี้ องค์กรที่ใช้งานคลาวด์อาจจะต้องให้ความระมัดระวังในการใช้งาน เนื่องจากอาจจะถูกขโมยข้อมูลที่สำคัญขององค์กรได้ ซึ่งจากเหตุการณ์ที่บุคคลภายนอกสามารถเข้าถึงข้อมูลที่ถูกจัดเก็บไว้ในคลาวด์ Amazon S3 Bucket แสดงให้เห็นว่ามีคนบางกลุ่มพยายามค้นหาข้อมูลที่ถูกจัดเก็บไว้ในคลาวด์ที่อนุญาตให้เข้าถึงได้จากสาธารณะ หรือข้อมูลสำคัญที่ไม่มีการเข้ารหัส รวมถึงความพยายามหาช่องโหว่ของระบบคลาวด์เพื่อให้แฮกเกอร์สามารถเจาะระบบและเข้าถึงข้อมูลต่าง ๆ ที่ถูกจัดเก็บไว้ในคลาวด์แล้วนำไปเปิดเผยต่อไป

5. การฉ้อโกงผ่านบริการธนาคารดิจิทัล

การเปิดบัญชีโดยไม่มีสมุดบัญชีคู่ฝาก บริการธนาคารดิจิทัล (Digital Banking) รวมไปถึงบริการทางการเงินอื่น ๆ โดยใช้เทคโนโลยีเพื่ออำนวยความสะดวกในการทำธุรกรรมที่เกี่ยวข้องกับการเงินแก่ผู้ใช้งาน แต่ก็อาจทำให้แฮกเกอร์สามารถขโมยเงินจากบัญชีผู้ใช้ได้ง่ายขึ้นด้วย ไม่ว่าจะเป็นการขโมยข้อมูลที่ใช้ยืนยันตัวตน และลักลอบนำไปใช้งานในทางที่ผิด ดังนั้นการแนวโน้มการฉ้อโกงทางดิจิทัลในปี 2562 จึงมีโอกาสเพิ่มสูงขึ้น และมูลค่าความเสียหายก็สูงขึ้นเช่นกัน

6. การปลอมแปลงข้อมูลทางชีวมิติ (Biometric)

เพื่อใช้ยืนยันตัวตน ซึ่งอาจจะมีเหตุการณ์การโจมตีเกิดขึ้นจริงกับระบบรักษาความปลอดภัยต่าง ๆ เนื่องจากในช่วงที่ผ่านมามีข่าวการทดลองปลอมข้อมูลทางชีวมิติโดยใช้เครื่องพิมพ์ 3 มิติ (3D Printer) จำลองใบหน้า หรือสร้างลายนิ้วมือปลอมด้วยกาวทาไม้ เป็นต้น เพื่อใช้ยืนยันตัวตนบนโทรศัพท์สมาร์ทโฟนรุ่นต่าง ๆ นอกจากนี้ ยังมีความพยายามในการหลีกเลี่ยงในการยืนยันตัวตนก่อนเข้าใช้งานสมาร์ทโฟน ซึ่งในปัจจุบันมีการใช้สมาร์ทโฟนในการทำธุรกรรมทางการเงิน ดังนั้นอาจจะเกิดเหตุการณ์ที่แฮกเกอร์ขโมยเงินโดยใช้วิธีการปลอมแปลงข้อมูลทางชีวมิติได้

สถานะของภาคการธนาคารในประเทศไทย

ในปี 2561 ที่ผ่านมา ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร หรือ TB-CERT และสมาชิกทั้งหมดได้ช่วยกันเสริมสร้างความแข็งแกร่งด้านการรักษาความมั่นคงปลอดภัยสารสนเทศในภาคการธนาคารในประเทศไทยในหลาย ๆ ด้าน เริ่มจากด้านความพร้อมในการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งเมื่อเปรียบเทียบกับปีที่แล้ว พบว่าปี 2561 ธนาคารและหน่วยงานสมาชิกมีความพร้อมของแผนการรับมือภัยคุกคามทางไซเบอร์มากขึ้น โดยปรับปรุงแผนการรับมือเหตุการณ์ให้มีการเชื่อมโยงการรับมือระหว่างธนาคาร และยกระดับการรับมือเหตุการณ์โดยซักซ้อมความพร้อมของแผนดังกล่าวร่วมกับหน่วยงานอื่นในภาคอุตสาหกรรมการเงิน อาทิ ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานคณะกรรมการกำกับและส่งเสริมการประกอบธุรกิจประกันภัย และบริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ เป็นต้น

ด้านการแลกเปลี่ยนข้อมูลข่าวสาร เมื่อหน่วยงานสมาชิกตรวจสอบพบเหตุการณ์การโจมตีหรือเหตุการณ์ที่น่าสงสัยที่เกิดภายในหน่วยงานตนเอง นอกจากการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น จะมีการแลกเปลี่ยนข้อมูลเชิงเทคนิคระหว่างสมาชิก เพื่อให้ TB-CERT Incident Response Team (TB-CERT IR Team) หาความสัมพันธ์ของเหตุการณ์และนำไปวิเคราะห์ ก่อนส่งต่อให้สมาชิกอื่นสามารถนำข้อมูลเหตุการณ์เหล่านั้นไปตรวจสอบและเตรียมการป้องกันก่อนที่จะเกิดเหตุการณ์เดียวกันกับสมาชิกที่เกิดเหตุ โดยมีการใช้ระบบ Sharing Portal กลาง ซึ่งดูแลโดย TB-CERT IR Team ในการเก็บข้อมูล เพื่อให้สมาชิกสามารถเข้าถึง และค้นหาข้อมูลได้อย่างสะดวกรวดเร็ว รวมถึงข้อมูลที่จัดเก็บก็มีการรักษาความปลอดภัยอย่างเข้มงวด นอกจากนี้ระบบดังกล่าว ยังรองรับการนำข้อมูลออกไปป้อนให้กับระบบ Sharing Portal ภายในของหน่วยงานสมาชิกได้อีกด้วย

ในการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในหน่วยงานสมาชิก จำเป็นต้องอาศัยข้อมูลจากแหล่งต่าง ๆ ซึ่งทาง TB-CERT เองได้รับข้อมูลจากแหล่งข้อมูลจากการเข้าร่วมเป็นสมาชิกในเครือข่ายหน่วยงานด้านความมั่นคงปลอดภัยสารสนเทศระดับโลก อาทิเช่น Forum of Incident Response and Security Teams (FIRST) เป็นต้น นอกเหนือจากการใช้ข้อมูลในการวิเคราะห์เหตุการณ์ภัยคุกคามแล้ว ยังนำไปใช้เป็นแหล่งข้อมูลข่าวสารด้านความมั่นคงปลอดภัยที่เกิดขึ้นในประเทศต่าง ๆ ให้กับสมาชิกอีกด้วย อีกทั้งมีการสรุปวิเคราะห์ข่าวสารที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นทั่วโลกอยู่เป็นประจำมาแลกเปลี่ยนระหว่างสมาชิกด้วยกัน

นอกจากนี้ การพัฒนาบุคลากรด้านการรักษาความมั่นคงปลอดภัยสารสนเทศสำหรับภาคการธนาคารนั้น ทุกธนาคารต่างก็ให้ความสำคัญ โดยส่งบุคลากรเข้าร่วมอบรมเชิงปฏิบัติการในการรับมือภัยไซเบอร์อย่างสม่ำเสมอ ในปี 2561 ที่ผ่านมา มุ่งเน้นการอบรมเพื่อพัฒนากระบวนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ โดยเริ่มตั้งแต่การสร้างกระบวนการรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ วิธีการเฝ้าระวังภัยไซเบอร์ ไปจนถึงการวิเคราะห์พยานหลักฐานทางดิจิทัล เป็นต้น ทำให้บุคลากรที่ดูแลเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศของธนาคารมีขีดความสามารถที่สูงขึ้น

บทสรุป

จากเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับภาคการเงินการธนาคารต่าง ๆ ทั่วโลก ที่มีการพัฒนารูปแบบวิธีการใหม่ตามยุคดิจิทัลแบงก์กิ้ง สิ่งที่จะช่วยให้การรับมือภัยไซเบอร์ของภาคธนาคาร ได้อย่างรวดเร็ว มีประสิทธิภาพ จำเป็นที่จะต้องอาศัยการเตรียมความพร้อมในการรับมือภัยคุกคามไซเบอร์หลัก 3 ด้าน ได้แก่ ด้านการพัฒนาบุคลากร ด้านการพัฒนากระบวนการ และด้านการพัฒนาเทคโนโลยี

ในด้านการพัฒนาประสิทธิภาพบุคลากรของหน่วยงานสมาชิก โดยผ่านกิจกรรมการจัดฝึกอบรมทั้งภาคทฤษฎี และปฏิบัติอย่างต่อเนื่อง เพื่อเพิ่มความรู้ความเชี่ยวชาญให้กับบุคลากรที่เกี่ยวข้องกับการรับมือภัยไซเบอร์ การสรรหานิสิตนักศึกษาที่มีความรู้ความสามารถทางด้าน Cyber Security ผ่านกิจกรรม Financial Cybersecurity Boot Camp ประจำปี เพื่อให้หน่วยงานสมาชิกสามารถคัดเลือกบุคลากรที่มีประสิทธิภาพเข้าร่วมทำงานในหน่วยงานสมาชิก

ด้านการพัฒนากระบวนการรับมือภัยคุกคามไซเบอร์ โดยการจัดทำแนวทางกระบวนการรับมือภัยคุกคามไซเบอร์สำหรับหน่วยงานสมาชิก ผ่านกิจกรรม Incident Response Plan Workshop เพื่อให้สมาชิกนำไปพิจารณาปรับใช้ให้เหมาะสมกับหน่วยงานของตนเอง การซักซ้อมกระบวนการรับมือภัยคุกคามอย่างสม่ำเสมอ ผ่านกิจกรรม Banking Cyber Drill ประจำปี เพื่อทดสอบประสิทธิภาพของกระบวนการรับมือภัยคุกคาม ตลอดจนการพัฒนากระบวนการแลกเปลี่ยนข้อมูลเหตุการณ์การโจมตีในรูปแบบต่าง ๆ ของแฮกเกอร์ ระหว่างหน่วยงานสมาชิกหน่วยงาน CERT ทั้งในและนอกประเทศภายใต้พันธะสัญญาแลกเปลี่ยนข้อมูล ที่จะช่วยให้สมาชิกได้ทราบข้อมูลเหตุการณ์ภัยไซเบอร์ เพื่อนำไปเตรียมการป้องกันได้อย่างรวดเร็วยิ่งขึ้น

สุดท้าย ด้านการพัฒนาเทคโนโลยีสร้างเครื่องมือในการแลกเปลี่ยนข้อมูลระหว่างหน่วยงานสมาชิก เพื่อให้สมาชิกสามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว แม่นยำ และสามารถส่งต่อข้อมูลนั้นไปยังระบบป้องกันต่าง ๆ ของหน่วยงานสมาชิก เพื่อให้การป้องกันการโจมตีระบบสารสนเทศขององค์กรตนเองมีประสิทธิภาพมากขึ้น

ทั้งนี้ การพัฒนาบุคลากร กระบวนการ และเทคโนโลยี ของภาคการธนาคาร เพื่อรับมือภัยคุกคามไซเบอร์ จำเป็นต้องอาศัยศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร หรือ TB-CERT ภายใต้สมาคมธนาคารไทย เป็นกลไกหลักในการขับเคลื่อนพันธกิจการยกระดับความพร้อมที่จะรับมือกับภัยคุกคามด้านไซเบอร์ เพื่อสร้างความเชื่อมั่นให้กับลูกค้าและประชาคมโลก ที่ใช้ระบบและบริการทางการเงินของภาคการธนาคารในประเทศไทย

ภาคผนวก

รู้จักกับ Meltdown และ Spectre ช่องโหว่บนเครื่องคอมพิวเตอร์รุ่นใหม่ (1/2)

TLP WHITE

เผยแพร่วันที่ 6 มกราคม 2561

เปิดฉากปีใหม่ ในวันที่ 3 มกราคม 2561 มีการรายงานช่องโหว่ด้านความปลอดภัยที่มีผลกระทบกับ ซีพียู รุ่นใหม่เกือบทุกรุ่น ด้วยการอาศัยช่องโหว่นี้ผู้ประสงค์ร้ายจะสามารถสร้างโปรแกรมเพื่อขโมยข้อมูลของโปรแกรมอื่นที่กำลังประมวลผลอยู่ในขณะนั้น ไม่ว่าจะเป็นข้อมูลรหัสผ่าน ข้อมูลกุญแจลับ โทเค็น อีเมล หรือแม้กระทั่งข้อมูลสำคัญทางธุรกิจ ซึ่งโดยปกติแล้วระบบปฏิบัติการจะไม่อนุญาตให้เข้าถึงข้อมูลของโปรแกรมอื่นได้

เทคนิคการโจมตี

การเพิ่มความเร็วในการประมวลผลของคอมพิวเตอร์ในยุคที่ซีพียูรุ่นใหม่มีประสิทธิภาพในการทำงานที่สูงนั้น เทคนิคหนึ่งที่ใช้กันคือการทำ speculative execution หรือ การคาดเดาและโหลดชุดคำสั่งที่จะใช้งานล่วงหน้า ซึ่งหากการคาดเดาทำได้อย่างถูกต้องแม่นยำจะเป็นการเพิ่มประสิทธิภาพการทำงานอย่างมาก แต่หากการคาดเดาไม่ถูกต้องก็จะทำการโหลดชุดคำสั่งตามลำดับที่ควรจะเป็นเหมือนเช่นเดิม อย่างไรก็ตามเทคนิคนี้จะสร้างปัญหาด้านความปลอดภัย กล่าวคือการโหลดชุดคำสั่งล่วงหน้ารวมถึงข้อมูลที่ต้องใช้ในการทำงานของชุดคำสั่งก่อนช่วงเวลาที่จำเป็นต้องใช้งานมาไว้ในหน่วยความจำ จะทำให้สามารถเขียนโปรแกรมเข้าไปขโมยข้อมูลดังกล่าวได้ ซึ่งเป็นเทคนิคของการโจมตีช่องโหว่ Meltdown และ Spectre **จุดแตกต่างของช่องโหว่ Meltdown และ Spectre คือระดับที่จะขโมยข้อมูลได้ ซึ่ง Meltdown ลงลึกได้ถึงระบบปฏิบัติการ ส่วน Spectre จะเป็นแอปพลิเคชันที่ทำงานอยู่ในขณะนั้น**

ทั้งนี้การจะโจมตีช่องโหว่นี้ผู้ประสงค์ร้ายจำเป็นต้องหาวิธีลงโปรแกรมบนเครื่องเป้าหมายให้ได้ก่อน จึงจะสามารถรันโปรแกรมและใช้ช่องโหว่ Meltdown หรือ Spectre ในการขโมยข้อมูล ซึ่งอาจจะใช้วิธีการฝังโปรแกรมบนเว็บไซต์ ส่งมัลแวร์ทางอีเมล หรือ Thumb Drive ปัจจุบันยังไม่มีข้อมูลชัดเจนว่ามีการใช้เทคนิคใดบ้าง เพียงแค่พบรูปแบบของการเขียนโค้ดเป็น JavaScript ฝังอยู่ในเว็บไซต์ นอกจากนั้นยังไม่ได้รับรายงานงานว่ามีการส่งโปรแกรมแบบรีโมทและยังไม่พบข้อมูลที่ระบุวิธีการส่งข้อมูลที่ขโมยได้ออกไป

อุปกรณ์ที่ได้รับผลกระทบ

TR18-001

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง TB-CERT

รู้จักกับ Meltdown และ Spectre ช่องโหว่บนเครื่องคอมพิวเตอร์รุ่นใหม่ (2/2)

TLP WHITE

เผยแพร่วันที่ 6 มกราคม 2561

ข้อแนะนำ

1. ประเมินความเสี่ยงของระบบงานเพื่อจัดลำดับความสำคัญในการทดสอบและติดตั้งแพตช์บนเครื่องเซิร์ฟเวอร์ โดยต้องพิจารณาการควบคุมการเชื่อมต่อของเซิร์ฟเวอร์ประกอบด้วย ควรจะให้ลำดับการติดตั้งแพตช์สำหรับเซิรฟ์เวอร์ที่มีการเชื่อมต่ออินเตอร์เน็ตหรือควบคุมการเชื่อมต่ออินเตอร์เน็ตให้รัดกุมมากขึ้น
2. ทดสอบและติดตั้งแพตช์ (Patch) ปัจจุบันเจ้าของผลิตภัณฑ์ทยอยประกาศแจ้งเตือนให้ติดตั้งแพตช์เพื่อควบคุมความเสี่ยงนี้ อย่างไรก็ตามแพตช์ดังกล่าวอาจจะมีผลกระทบต่อประสิทธิภาพการทำงานของเครื่อง หรืออาจทำให้ทำงานขัดกับซอฟต์แวร์ Anti-virus ดังนั้นจำเป็นต้องทดสอบการติดตั้งแพตช์ ก่อนนำไปลงใน Production เพื่อไม่ให้ส่งผลกระทบกับบริการ
3. ป้องกันเครื่องคอมพิวเตอร์ที่เชื่อมต่อในองค์กร โดยใช้ proxy ในการควบคุมการเข้าถึงเว็บไซต์ที่มีความเสี่ยง ผู้ดูแลจะต้องยกระดับการเฝ้าระวังให้สูงขึ้นสำหรับเว็บไซต์ที่มีความเสี่ยงสูงโดยเฉพาะเว็บไซต์ที่ถูกพัฒนาด้วย Java Script หากเครื่องที่เข้าถึงอินเตอร์เน็ตจากในองค์กรยังไม่สามารถติดตั้งแพตช์ได้ครบถ้วน
4. ป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่เชื่อมอินเตอร์เน็ตโดยตรง **สำหรับผู้ใช้งานทั่วไป** ให้พิจารณาปิดการใช้งาน Java Script หรือจำกัดให้เข้าถึงเฉพาะเว็บไซต์ที่น่าเชื่อถือได้เป็นพิเศษ (Trusted site) ในช่วงที่ยังไม่ได้ติดตั้งแพตช์
5. ติดตามข้อมูลการประกาศแพตช์จากเจ้าของผลิตภัณฑ์ที่ใช้งานอยู่ รวมถึงติดตามข้อมูลความคืบหน้าของการโจมตีนี้
6. ติดตามสอบถามข้อมูลเรื่องการลงแพตช์หรือมาตรการป้องกันสำหรับผู้ใช้บริการคลาวด์จากผู้ให้บริการ

ข้อควรระวัง

1. ปัจจุบันซอฟต์แวร์ Anti-virus ยังไม่สามารถตรวจจับได้หรือป้องกันช่องโหว่นี้ได้
2. การจะติดตั้งแพตช์อาจจะส่งผลกระทบต่อประสิทธิภาพของเครื่อง หรือขัดกับซอฟต์แวร์ Anti-virus ดังนั้นจำเป็นต้องสอบถามข้อมูลกับบริษัทซอฟต์แวร์ Anti-virus ด้วย

เอกสารอ้างอิง

1. https://meltdownattack.com/
2. https://www.us-cert.gov/ncas/alerts/TA18-004A

TR18-001

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง TB-CERT

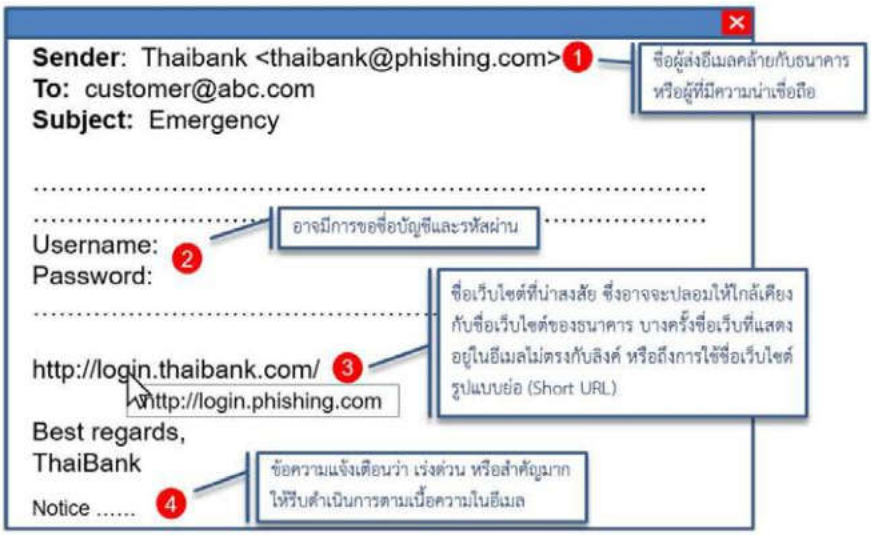
TLP: WHITE

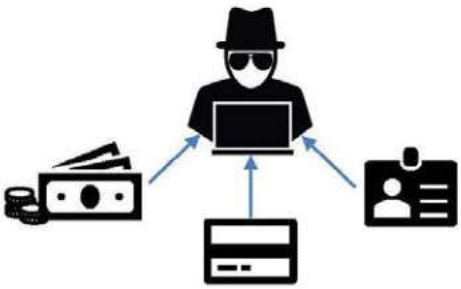
ฟิชชิง (PHISHING)

ฟิชชิง (Phishing) เป็นเทคนิคการหลอกลวงทางอินเทอร์เน็ตประเภทหนึ่ง ซึ่งมักจะมาในรูปแบบของการปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้น เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต และหมายเลขบัตรประจำตัวประชาชน เป็นต้น

ผู้ประสงค์ร้ายจะส่งอีเมลหลอกลวงโดยใช้ชื่อผู้ส่งและเนื้อความที่น่าเชื่อถือ โดยเป็นข้อความในลักษณะแจ้งเตือน และเร่งให้ดำเนินการหากไม่ต้องการให้เกิดผลเสีย เมื่อเหยื่อหลงเชื่อ ก็จะดำเนินการตามความต้องการของผู้ประสงค์ร้าย เช่น เข้าเว็บไซต์เพื่อกรอกข้อมูลส่วนตัว รหัสผ่าน หรือตอบกลับอีเมลด้วยข้อมูลส่วนตัว เป็นต้น

วิธีการสังเกตอีเมลหลอกลวง





ผลกระทบที่อาจเกิดขึ้น

- สูญเสียทรัพย์สินหรือเงินในบัญชีธนาคาร
- สูญเสียข้อมูลสำคัญ เช่น รหัสผ่าน เลขที่บัตรเครดิต และข้อมูลส่วนตัวต่าง ๆ เป็นต้น
- สูญเสียชื่อเสียงจากการส่งข้อมูลต่อไปให้ยังรายชื่อผู้ติดต่อหรือการแอบอ้างชื่อของเหยื่อในการกระทำความผิดอื่นต่อไป

วิธีการป้องกัน

1. อย่าหลงเชื่อลิงค์ที่มาพร้อมกับอีเมลที่ไม่แน่ใจแหล่งที่มา โดยห้ามเปิดลิงค์แนบอย่างเด็ดขาด
2. ห้ามเปิดเผยข้อมูลส่วนตัวใด ๆ ผ่านการร้องขอผ่านทางอีเมล หากไม่แน่ใจให้ทำการติดต่อกลับไปยังธนาคารโดยตรง
3. หากพบอีเมลที่สงสัยว่าจะเป็นฟิชชิงที่เกี่ยวข้องกับธนาคาร กรุณาติดต่อธนาคารทันที
4. ในกรณีหลงเชื่อและเปิดเผยรหัสผ่านแล้ว ให้ติดต่อไปยังธนาคารเพื่อทำการเปลี่ยนรหัสผ่านทันที

TR18-002

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

TLP: WHITE

ข้อมูลส่วนบุคคล (Personal Data)
ตอนที่ 1/4 นิยามและความสำคัญ

ในยุคดิจิทัล ทรัพย์สินมีค่านั้นไม่ได้มีเพียงแค่เงินในบัญชีออนไลน์ แต่ยังรวมถึงข้อมูลส่วนบุคคลด้วย ซึ่งข้อมูลส่วนบุคคล หรือ Personal Data คือข้อมูลที่สามารถระบุหรือยืนยันความเป็นตัวบุคคลได้ หรือ ข้อมูลที่บอกถึงลักษณะเฉพาะตัวของบุคคล ซึ่งแต่ละข้อมูลมีความละเอียดอ่อน (Sensitive) แตกต่างกันไป

ตัวอย่างข้อมูลส่วนบุคคล

	ชื่อ-นามสกุล
	ที่อยู่ อีเมล หมายเลขโทรศัพท์
	หมายเลขประจำตัวต่าง ๆ เช่น เลขประจำตัวประชาชน เลขหนังสือเดินทาง
	ข้อมูลที่สามารถเชื่อมโยงไปยังข้อมูลอื่นได้ เช่น วันเกิด ข้อมูลการแพทย์ ข้อมูลทางการเงิน
	ข้อมูลทางชีวมิติ (Biometric) เช่น ลายนิ้วมือ ข้อมูลสแกนม่านตา ข้อมูลอัตลักษณ์เสียง

ข้อมูลส่วนบุคคลใช้เพื่ออะไรบ้าง

เจ้าของข้อมูลส่วนบุคคลสามารถใช้ข้อมูลในการยืนยันตัวตนกับหน่วยงานต่าง ๆ ทั้งภาครัฐและเอกชน เพื่อทำธุรกรรมหรืออ้างอิงในการเข้าถึงสิทธิประโยชน์ของบุคคลนั้น ๆ อีกทั้งยังใช้เพื่อบอกความเป็นตัวเองให้คนอื่นได้ทราบผ่านช่องทางต่าง ๆ ได้อีกด้วย

ความสำคัญของข้อมูลส่วนบุคคล

ด้วยข้อมูลส่วนบุคคลเป็นข้อมูลที่บ่งบอกถึงลักษณะเฉพาะของบุคคลนั้น หน่วยงานต่าง ๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน โดยเฉพาะอย่างยิ่งสถาบันการเงิน มักจะใช้ข้อมูลนี้เพื่อยืนยันตัวตน ดังนั้นข้อมูลส่วนบุคคลจึงมีความสำคัญ เพราะหากมีผู้ไม่หวังดีล่วงรู้ก็อาจจะใช้สวมรอยในการทำธุรกรรมแทนและสร้างความเสียหายให้แก่เจ้าของข้อมูลได้

TR18-007

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

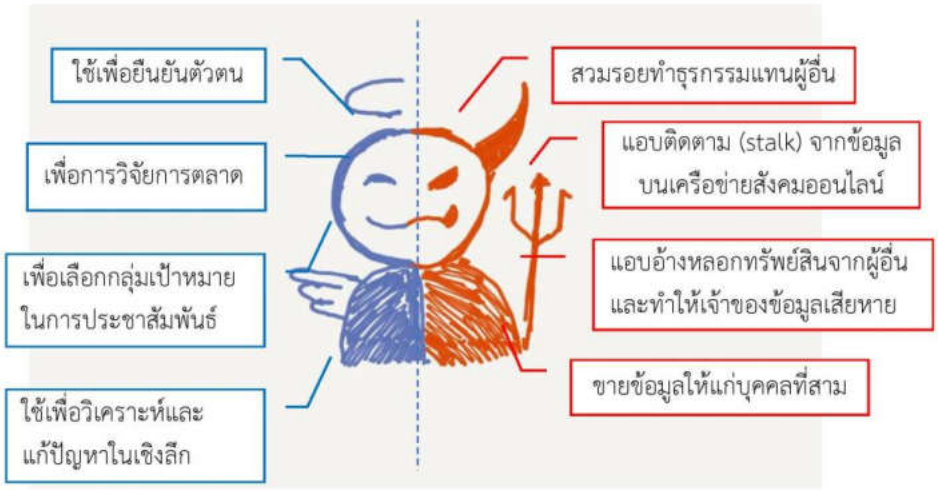
TB-CERT

TLP: WHITE

ข้อมูลส่วนบุคคล (Personal Data)
ตอนที่ 2/4 ประโยชน์ของข้อมูลส่วนบุคคล

ตัวอย่างการใช้งานข้อมูลส่วนบุคคล

โดยปกติแล้วข้อมูลส่วนบุคคลนั้นสามารถถูกนำไปใช้ได้หลากหลายวิธี ขึ้นอยู่กับวัตถุประสงค์ของผู้นำไปใช้ ซึ่งหากนำไปใช้ในทางที่ดี จะเกิดคุณอนันต์ แต่หากนำไปใช้ในทางที่ไม่ดี อาจจะเกิดโทษมหันต์กับเจ้าของข้อมูลได้



ข้อคิดก่อนให้ข้อมูลส่วนบุคคลแก่ผู้อื่น

ข้อมูลส่วนบุคคล ถือเป็นสิ่งสำคัญเฉพาะตัวบุคคลนั้น ๆ เจ้าของข้อมูลจำเป็นจะต้องจัดเก็บ ดูแลรักษาข้อมูลเหล่านี้ให้ดีที่สุด ดังนั้นก่อนจะให้ข้อมูลส่วนบุคคลใด ๆ กับใครควรคำนึงดังต่อไปนี้

- ตระหนักรู้ว่ากำลังจะให้ข้อมูลส่วนบุคคลที่มีความสำคัญ
- พิจารณาความน่าเชื่อถือของผู้ขอข้อมูล และต้องรู้ว่าข้อมูลนั้นเปิดเผยกับใคร
- ต้องให้ความยินยอมในการให้ข้อมูลก่อนทุกครั้ง
- พิจารณาวัตถุประสงค์ของหน่วยงานที่ร้องขอข้อมูล ต้องรู้ว่าข้อมูลที่ให้นั้น นำไปใช้เพื่อวัตถุประสงค์ตรงกับวัตถุประสงค์ในการให้ข้อมูล
- ตระหนักรู้ถึงผลกระทบหากข้อมูลนั้นมีรั่วไหล
- ให้ข้อมูลเท่าที่จำเป็น

TR18-008

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

เอกสารเผยแพร่

TLP: WHITE

ข้อมูลส่วนบุคคล (Personal Data)
ตอนที่ 3/4 การคุ้มครองดูแลข้อมูลส่วนบุคคลของผู้อื่น

ผู้ที่ขอใช้ข้อมูลส่วนบุคคลของผู้อื่นต้องคำนึงถึงสิ่งใด

ผู้ที่ร้องขอข้อมูลส่วนบุคคลของผู้อื่นนั้นจำเป็นต้องมีมาตรการหรือนโยบายในการคุ้มครองข้อมูลส่วนบุคคลของผู้อื่น เพื่อป้องกันมิให้ข้อมูลส่วนบุคคลของผู้อื่นนั้นถูกขโมย แอบอ้าง หรือลักลอบนำไปใช้งานอื่น อันจะทำให้เกิดผลกระทบโดยตรงกับเจ้าของข้อมูล ซึ่งจะต้องปฏิบัติดังนี้

- ปฏิบัติตามกฎหมายและกฎข้อบังคับ
- เก็บรวบรวมข้อมูลส่วนบุคคลอย่างจำกัด
- รักษาคงคุณภาพของข้อมูลส่วนบุคคล
- ระบุวัตถุประสงค์ในการเก็บรวบรวม
- นำข้อมูลส่วนบุคคลไปใช้ตามขอบเขตของวัตถุประสงค์ที่แจ้งขณะขอความยินยอมจากเจ้าของข้อมูล
- ดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การสูญหาย ความเสียหาย การรั่วไหลของข้อมูล
- เปิดเผยข้อมูลเกี่ยวกับมาตรการและการดำเนินการแนวปฏิบัติและนโยบายที่เกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล
- เปิดเผยรายละเอียดข้อมูลส่วนบุคคลต่อเมื่อได้รับการร้องขอจากเจ้าของข้อมูล หรือผู้แทนตามกฎหมาย
- มีความรับผิดชอบต่อข้อมูลส่วนบุคคลของผู้อื่น

หากดูแลข้อมูลของผู้อื่นไม่ดีพอ ข้อมูลอาจถูกขโมย

มีหลายเหตุการณ์ที่มีหน่วยงานหรือบริษัทถูกขโมยข้อมูลส่วนบุคคลที่รวบรวมไว้ และเผยแพร่สู่สาธารณะ ส่งผลทำให้เจ้าของข้อมูลนั้นเสียหาย อาจถูกนำไปใช้ทำธุรกรรมแทน อาจถูกนำไปแอบอ้างเพื่อจุดประสงค์ไม่ดีบางอย่าง นอกจากนี้ยังทำให้หน่วยงานหรือบริษัทที่เก็บข้อมูลส่วนบุคคลของผู้อื่นไว้เสียหาย ทั้งเสียชื่อเสียง ความไว้วางใจ ตลอดจนต้องเสียค่าใช้จ่ายในการแก้ไขปัญหา หรือแม้กระทั่งข้อมูลเหล่านั้นเสียหายทั้งหมดได้

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลนั้น กำหนดให้ผู้ที่ขอใช้ข้อมูลส่วนบุคคลของผู้อื่นนั้นจะต้องดูแลข้อมูลนั้น หากมีความเสียหายเกิดขึ้นกับเจ้าของข้อมูล ถือว่ามีความผิด นอกจากนี้ยังมีวัตถุประสงค์เพื่อให้เจ้าของข้อมูลมั่นใจได้ว่าข้อมูลส่วนบุคคลนั้นจะถูกดูแล สิทธิของเจ้าของข้อมูลส่วนบุคคล รวมถึงการร้องเรียน การตรวจสอบ และการอุทธรณ์อีกด้วย

TR18-009

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

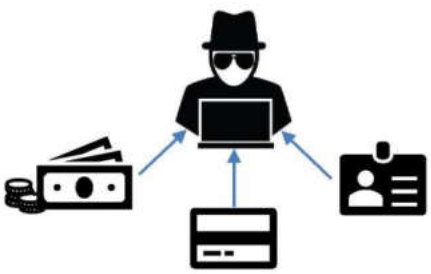
TLP: WHITE

ข้อมูลส่วนบุคคล (Personal Data)
ตอนที่ 4/4 ข้อมูลส่วนบุคคลบนเครือข่ายสังคมออนไลน์ (1/2)

ปัจจุบันมีการเปิดเผยข้อมูลส่วนบุคคลผ่านทางเครือข่ายสังคมออนไลน์ที่ได้รับความนิยมและใช้งานกันอย่างแพร่หลาย ไม่ว่าจะเป็น Facebook Twitter Instagram และ Line เป็นต้น ทำให้ข้อมูลไปอยู่บนโลกออนไลน์มากขึ้น และมีโอกาสที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลเหล่านี้ได้โดยง่าย

ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลส่วนบุคคลได้อย่างไร

- **ผู้ใช้งานเปิดเผยข้อมูลเอง** เช่น การโพสต์ รูปบัตรประชาชน วันเดือนปีเกิด บนเครือข่ายสังคมออนไลน์ เป็นต้น
- **ผู้ใช้งานถูกหลอกให้บอกข้อมูล** ผู้ไม่หวังดีใช้เล่ห์เหลี่ยมในการหลอกลวงให้เหยื่อเปิดเผยข้อมูลส่วนตัว
- **แอปพลิเคชันที่ขอเข้าถึงข้อมูลส่วนบุคคล** ผู้ใช้งานติดตั้งแอปพลิเคชันเพิ่มเติมในเครือข่ายสังคมออนไลน์ได้ เช่น เกมส์ และแบบทดสอบออนไลน์ โดยที่แอปพลิเคชันเหล่านั้นจะขอสิทธิ์ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งาน



สัญญาณบ่งบอกว่าถูกผู้ไม่หวังดีนำข้อมูลส่วนบุคคลไปใช้งาน

- ไม่สามารถล็อกอินได้ เนื่องจากรหัสผ่านถูกเปลี่ยนไป
- พบบันทึกการล็อกอินที่ผิดปกติ จากอุปกรณ์ที่ใช้ ช่วงเวลา และสถานที่ ซึ่งผู้ใช้งานไม่ได้เป็นผู้ดำเนินการ เช่น พบการล็อกอินจากต่างประเทศ โดยที่ผู้ใช้งานอยู่ในประเทศไทย เป็นต้น
- มีการโพสต์ข้อความโดยที่ผู้ใช้งานไม่ได้ดำเนินการ
- พบธุรกรรมทางการเงินที่ผิดปกติ เช่น มีการใช้จ่ายโดยที่ผู้ใช้งานไม่ได้ซื้อสินค้า เป็นต้น

TR18-010

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT

TLP: WHITE

ข้อมูลส่วนบุคคล (Personal Data)
ตอนที่ 4/4 ข้อมูลส่วนบุคคลบนเครือข่ายสังคมออนไลน์ (2/2)

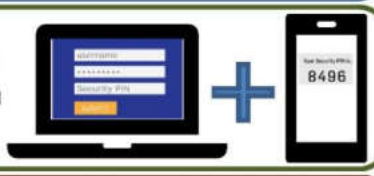
คำแนะนำในการป้องกันข้อมูลส่วนบุคคลบนเครือข่ายสังคมออนไลน์

1

ไม่โพสต์ข้อมูลส่วนบุคคลที่สำคัญ
เช่น วันเดือนปีเกิด เลขที่บัตรประชาชน และ ข้อมูลทางการเงิน เป็นต้น

2

ใช้รหัสผ่านที่ไม่สามารถเดาได้และใช้การยืนยันตัวตนหลายปัจจัย
ใช้รหัสผ่านที่ยากควบคู่กับ OTP (One Time Password) รวมถึงการเปลี่ยนรหัสผ่านบ่อย ๆ



3

ไม่รับเพิ่มบัญชีรายชื่อคนที่ไม่รู้จัก
รับเพิ่มบัญชีรายชื่อเพื่อนเฉพาะคนที่รู้จักเท่านั้น เพื่อจำกัดให้เพื่อนหรือคนที่รู้จักสามารถเข้าถึงข้อมูล

4

พิจารณาตั้งค่าความเป็นส่วนตัวตามความจำเป็นของข้อมูลที่โพสต์และผลกระทบที่อาจจะเกิดขึ้นหากข้อมูลรั่วไหลออกไป
ตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับข้อมูลที่โพสต์ เพื่อจำกัดผู้ที่สามารถเข้าถึงข้อมูลที่โพสต์ได้

5

ปิดบัญชีเครือข่ายสังคมออนไลน์ที่ไม่ได้ใช้แล้ว
เพื่อป้องกันไม่ให้ผู้ไม่หวังดีลักลอบใช้งาน และอาจจะถูกนำไปใช้สร้างข้อมูลที่เป็นเท็จ

6

ไม่ควรติดตั้งแอปพลิเคชันที่น่าสงสัยบนเครือข่ายสังคมออนไลน์
โดยอาจพิจารณาจากคอมเม้นท์รีวิวที่มีต่อแอปพลิเคชัน หรือข่าวการแจ้งเตือนเกี่ยวกับแอปพลิเคชันหลอกลวงต่าง ๆ

7

ล็อกเอาท์ทุกครั้งหลังใช้งานผ่านคอมพิวเตอร์ของผู้อื่น
เพื่อป้องกันไม่ให้ผู้ไม่หวังดีลักลอบนำบัญชีเครือข่ายสังคมออนไลน์ไปใช้งานในทางไม่ดี

การนำข้อมูลส่วนบุคคลของผู้อื่นไปใช้ จนทำให้ผู้นั้นได้รับความเสียหาย ถือว่ามีความผิดตาม พรบ.ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ รวมถึงอาจจะมีความผิดตามพรบ.คุ้มครองข้อมูลส่วนบุคคลที่จะประกาศใช้ในอนาคตด้วย

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT Thailand Banking Sector CERT

TR18-010

รายชื่อคณะกรรมการ

กิตติ โฆษะวิสุทธิ์ ประธานกรรมการ	**ธนาคารกรุงเทพ** ผู้จัดการอาวุโส ฝ่ายความมั่นคงปลอดภัย เทคโนโลยีสารสนเทศ
นฤดม รุ่งศิริวงศ์ กรรมการ	**ธนาคารเกียรตินาคิน** ผู้อำนวยการ หัวหน้าทีม IT Security and Solution Architecture
ศลิษา แซ่เล้า กรรมการ	**ธนาคารธนชาต** ผู้อำนวยการ ฝ่ายความปลอดภัยระบบ สารสนเทศและเทคโนโลยี
สมบูรณ์ หิรัญภัทรศิลป์ กรรมการ	**ธนาคารสแตนดาร์ด ชาร์เตอร์ด** Head Country Technology Management
สมหมาย ฟองน้ำทิพย์ กรรมการ	**ธนาคารกรุงศรี** Vice President Cyber Security Operation and IT Security Solution Management Department
อารยาภา พานิชปรีชา กรรมการ	**ธนาคารทิสโก้** Head of Technology Governance
ยศ กิมสวัสดิ์ เลขานุการ	**สมาคมธนาคารไทย** ประธานสำนักงาน ระบบการชำระเงิน
กิติศักดิ์ จิรวรรณกูล ผู้ช่วยเลขานุการ	**สมาคมธนาคารไทย** ผู้จัดการเซิร์ต
ธาวินี วงศ์วิศว์ ผู้ช่วยเลขานุการ	**สมาคมธนาคารไทย** ผู้จัดการเซิร์ตสัมพันธ์

รายชื่อหน่วยงานสมาชิก TB-CERT ปี 2561

ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร
Bank of Agriculture and Agricultural Cooperatives

ธนาคารกรุงศรีอยุธยา จำกัด (มหาชน)
Bank of Ayudhya Public Company Limited (Krungsri)

ธนาคารกรุงเทพ จำกัด (มหาชน)
Bangkok Bank Public Company Limited

ธนาคารแห่งประเทศไทย
Bank of Thailand

ธนาคาร ซีไอเอ็มบี ไทย จำกัด (มหาชน)
CIMB Thai Bank Public Company Limited

ธนาคารอาคารสงเคราะห์
Government Housing Bank

ธนาคารออมสิน
Government Savings Bank

ธนาคารไอซีบีซี (ไทย) จำกัด (มหาชน)
Industrial and Commercial Bank of China (Thai) Public Company Limited (ICBC Thai)

บริษัท เนชั่นแนล ไอทีเอ็มเอ็กซ์ จำกัด
National ITMX Company Limited

ธนาคารกสิกรไทย จำกัด (มหาชน)
(KASIKORNBANK Public Company Limited)

ธนาคารเกียรตินาคิน จำกัด (มหาชน)
Kiatnakin Bank Public Company Limited

ธนาคารกรุงไทย จำกัด (มหาชน)
Krung Thai Bank Public Company Limited

ธนาคารแลนด์ แอนด์ เฮ้าส์ จำกัด (มหาชน)
Land and Houses Bank Public Company Limited

บริษัท ข้อมูลเครดิตแห่งชาติ จำกัด
National Credit Bureau Company Limited

บริษัท ศูนย์ประมวลผล จำกัด
Processing Center Company Limited

ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
The Siam Commercial Bank Public Company Limited

ธนาคารสแตนดาร์ดชาร์เตอร์ด (ไทย) จำกัด (มหาชน)
Standard Chartered Bank (Thai) Public Company Limited

ธนาคารธนชาต จำกัด (มหาชน)
Thanachart Bank Public Company Limited

ธนาคารไทยเครดิต เพื่อรายย่อยจำกัด (มหาชน)
The Thai Credit Retail Bank Public Company Limited

ธนาคารทิสโก้ จำกัด (มหาชน)
TISCO Bank Public Company Limited

ธนาคารทหารไทย จำกัด (มหาชน)
TMB Bank Public Company Limited

ธนาคารยูโอบี จำกัด (มหาชน)
United Overseas Bank (Thai) Public Company Limited

Preparation

Detection & Analysis

Containment Eradiction&Recovery

Post-Incident Activity

Incident Response Process

Preparation

Incident response methodologies typically emphasize preparation—not only establishing an incident response capability so that the organization is ready to respond to incidents, but also preventing incidents by ensuring that systems, networks, and applications are sufficiently secure. Although the incident response team is not typically responsible for incident prevention, it is fundamental to the success of incident response programs

Detection & Analysis

Incident can occur in countless ways. Organization must constantly monitor their systems, networks, security protection and detection systems and look for sign of attacks. Incidents may be detected through many different means with varying level of details.
Determining whether a particular event is actually an incident requires collaboration with other technical and information security practitioners to make judgement. The initial analysis should provide enough information for the team to prioritize subsequent activities such as containment, hunting and recovery.

Containment Eradication & Recovery

Containment is important before an incident increase damage, so it is crucial to make a consideration at the early stage to handle each incident. Organization should define acceptable risks in dealing with incidents and develop strategies and procedures for containing the incident.
After incident has been contained, eradication may be necessary to eliminate components of incidents. During eradication, it is important to identify all affected hosts within organization so that they can be remediated. The systems and operation will be restored to normal operation subsequently.

Post-Incident Activitiy

Learning and improving are the most important part of incident response. Organization should improve their handling process and learn from the past. They should focus on collecting the information of incident activities that happened. Organization should be able to answer what was happened? when? how? How long? what tools? etc. and keep data to help themselves gain the value together for future use.

Ref. NIST 800-61 Revision 2