TB-CERT

Thailand Banking Sector CERT

ANNUAL REPORT 2017

Be a Neutral and Trusted Adviser,
An Expertise hub in Cybersecurity for Thailand banking sector

รายงานผลการดำเนินงานของ Thailand Banking Sector CERT ปี 2560

TB-CERT Annual Report 2017

กิตติ โฆษะวิสุทธิ์
กิติศักดิ์ จิรวรรณกูล
ธาวินี วงศ์วิศว์

ที่ปรึกษา
กิตติ โฆษะวิสุทธิ์
บรรณาธิการ
ธาวินี วงศ์วิศว์

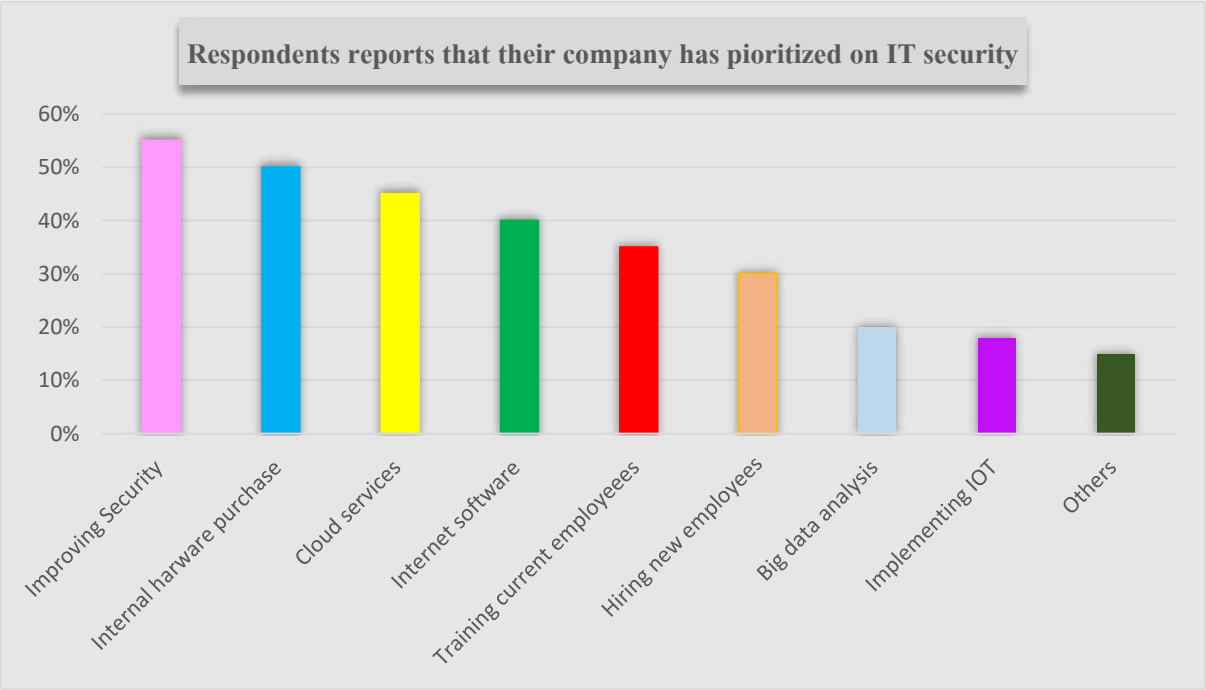
สำนักพิมพ์: ศูนย์ประสานงานความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคการธนาคาร
(Thailand Banking Sector CERT: TB-CERT)
ปีที่พิมพ์: 2561
สถานที่พิมพ์: กรุงเทพฯ

คำนำ

สถาบันการเงินในยุคดิจิทัลได้นำเทคโนโลยีมาประยุกต์ใช้ในการให้บริการทางการเงินและการชำระเงินอย่างกว้างขวาง ซึ่งช่วยให้ลูกค้าสามารถเข้าถึงบริการได้สะดวก รวดเร็ว ทุกที่ ทุกเวลา และทุกอุปกรณ์ และมีค่าใช้จ่ายโดยรวมถูกลง อย่างไรก็ตาม เป็นปกติของการใช้เทคโนโลยีที่ย่อมจะต้องเผชิญกับความเสี่ยงใหม่ๆ ที่เกิดขึ้นและหนึ่งในความเสี่ยงที่ทั่วโลกจัดให้เป็นความเสี่ยงสำคัญ คือ ความเสี่ยงจากภัยไซเบอร์ ที่นับวันเพิ่มขึ้นอย่างรวดเร็ว มีรูปแบบที่หลากหลายและซับซ้อน และส่งผลกระทบในวงกว้างมากขึ้น เห็นได้ ว่า World Economic Forum ได้เล็งเห็นถึงความสำคัญนี้จึงจัดตั้งหน่วยงานภายใต้ World Economic Forum ที่มีชื่อว่า Global Center for Cybersecurity [1] โดยมีวัตถุประสงค์หลักเพื่อช่วยสร้างความมั่นคงปลอดภัยให้กับทุกคนในโลกของไซเบอร์โดยสร้างความร่วมมือจากทุกภาคส่วน เช่น รัฐ เอกชน รัฐวิสาหกิจ และอื่นๆ ให้ร่วมมือกันรับมือกับภัยคุกคามใหม่ๆ ที่เกิดขึ้นทั่วโลกได้ ทั้งนี้ได้จัดอันดับให้ภัยไซเบอร์เป็น 1 ใน ความเสี่ยงที่สำคัญมากและสร้างผลกระทบให้เกิดความเสียหายทั่วโลกโดยคิดเป็นเงิน 500 พันล้านเหรียญสหรัฐ โดยองค์กรนี้เน้นถึงเรื่องความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์จากการสร้างความร่วมมือ การแลกเปลี่ยนข้อมูล และการสร้างความไว้วางใจ ระดับโลก

หากกลับมาดูสถานการณ์ภัยไซเบอร์ที่เกิดขึ้นกับภาคการเงินในเอเชีย พบว่าเป็นไปในทางที่เพิ่มมากขึ้น สถาบันการเงินในเอเชียซึ่งรวมทั้งในประเทศไทยเผชิญกับภัยในหลากหลายรูปแบบ ทั้ง DDoS attack Malware E-mail Phishing และล่าสุดเมื่อกลางปีที่ผ่านมาเกิดผลกระทบทั่วโลกรวมทั้งในเอเชีย และในประเทศไทย คือ กรณี Ransomware Wannacry ซึ่งจะเห็นได้ว่าภัยคุกคามต่างๆอาจเกิดขึ้นได้ทุกเมื่อทุกเวลาและไม่จำกัดองค์กร

หลายองค์กรมุ่งเน้นในการนำเทคโนโลยีมาใช้ในบริการ เพื่อปรับปรุงการปฏิบัติงานในด้านต่างๆ ให้มีประสิทธิภาพ คุณภาพ และมาตรฐาน พร้อมทั้งการเพิ่มความสะดวกรวดเร็ว เพื่อเป็นการยกระดับการบริการของตนเองให้ทัดเทียมคู่แข่งทั้งในระดับประเทศและสากล จึงเห็นได้จากรายงานข่าวจาก ZDNET กล่าวถึง การใช้งบประมาณขององค์กรด้านไอทีโดยเฉลี่ยคิดเป็น 10% ของงบประมาณการใช้จ่ายขององค์กร และได้แบ่งสัดส่วนมาเน้นด้าน Cybersecurity เฉพาะทางดังนี้



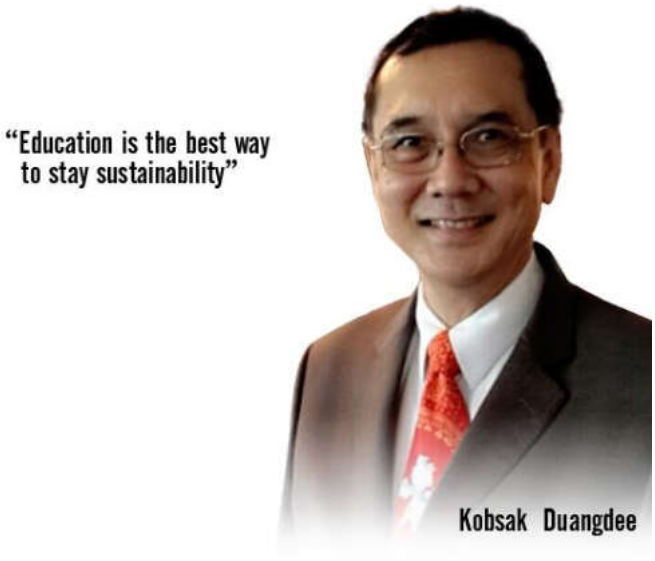
รูปที่ 1 กราฟแสดงเปอร์เซ็นการจัดลำดับการให้ความสำคัญการใช้จ่ายด้าน Cybersecurity เฉพาะทาง[2]

Improving Security 55%, Internal harware purchase 50%, Cloud services 45%, Internet software 40%, Training current employeees 35%, Hiring new employees 30%, Big data analysis 20%, Implementing IOT 18%, และ Others 15%

การปรับปรุงบริการให้มีความทันสมัย ตอบสนองการแข่งขันของภาคธุรกิจ รองรับความต้องการของประชาชนที่มีความต้อการใช้เทคโนโลยีเข้ามาเพื่ออำนวยความสะดวกในชีวิตประจำวัน ซึ่งจะเห็นได้จากข้อมูลสถิติปีที่2560 (ณ.เดือนธันวาคม) บริการการโอนเงิน(*รายย่อย*) [3] ข้ามธนาคารผ่านอินเตอร์เน็ตและโทรศัพท์เคลื่อนที่มีจำนวนมากถึง 43,967,000 รายการ โดยเมื่อเทียบกับปีก่อนหน้า ธันวาคม 2559 มีบริการการโอนเงิน(*รายย่อย*)ข้ามธนาคารผ่านอินเตอร์เน็ตและโทรศัพท์เคลื่อนที่เป็นจำนวน 16,422,000 รายการ โดยคิดเป็นอัตราการเติบโตที่เพิ่มขึ้นถึง 167.7% ดังนั้นจะเห็นว่าผู้คนสนใจการทำธุรกรรมผ่านทางอินเตอ์เน็ตและโทรศัพท์มากขึ้นจึงทำให้ธนาคารพาณิชย์จึงตกเป็นเป้าของการโจรกรรมทางไซเบอร์ที่เหล่าแฮกเกอร์ให้ความสนใจมากโดยหลีกเลี่ยงไม่ได้ ธนาคารจึงต้องคำนึงเป็นพิเศษถึงความปลอดภัยและการรักษาข้อมูลของผู้ใช้บริการและธนาคารซึ่งเป็นผู้ให้บริการควบคู่ไปด้วยกัน

สารจากผู้บริหาร

"ผมเชื่อว่า หากเราส่งเสริมและผลักดันการศึกษาให้กับเยาวชนรุ่นใหม่ให้มีความรู้ความเข้าใจในด้านความมั่นคงปลอดภัยไซเบอร์มากขึ้น พวกเขาเหล่านั้นจะเติบโตขึ้นมาเป็นส่วนหนึ่งของสังคมในยุคดิจิทัลนี้และจะช่วยยกระดับความมั่นคงปลอดภัยไซเบอร์ให้กับประเทศชาติอย่างมั่นคงแข็งแรงและยั่งยืน"



คุณกอบศักดิ์ ดวงดี

เลขาธิการสมาคมธนาคารไทย

"การที่องค์กรจะก้าวไปเป็นผู้นำในด้านใดๆ ก็ตาม เราจะต้องปรับตัวให้เข้ากับทุกสถานการณ์เท่าทันปัจจุบัน และที่ขาดไม่ได้เลยก็คือ ความร่วมมือร่วมใจทำงานกันเป็นทีม เพื่อตอบสนองต่อเหตุการณ์ภัยคุกคามได้อย่างทันท่วงที"

คุณยศ กิมสวัสดิ์
ประธานสำนักงานระบบการชำระเงิน
สมาคมธนาคารไทย

“สิ่งสำคัญยิ่งในการสร้างความร่วมมือระหว่างองค์กรคือความไว้วางใจ เมื่อใดที่เรามีความไว้วางใจระหว่างสมาชิกด้วยกันเมื่อนั้นเราจะเกิดการร่วมมือกันแลกเปลี่ยนข้อมูลที่เป็นประโยชน์ต่อสาธารณะและองค์กรของสมาชิกเพื่อช่วยกันเตรียมพร้อมรับมือกับภัยไซเบอร์และช่วยยกระดับความมั่นคงปลอดภัยให้กับภาคการเงินการธนาคารอย่างมีประสิทธิภาพ”

Dr. Kitti Kosavisutte

ดร. กิตติ โฆษะวิสุทธิ์

ประธานกรรมการ TB-CERT

สารบัญ

ที่มาของTB-CERT

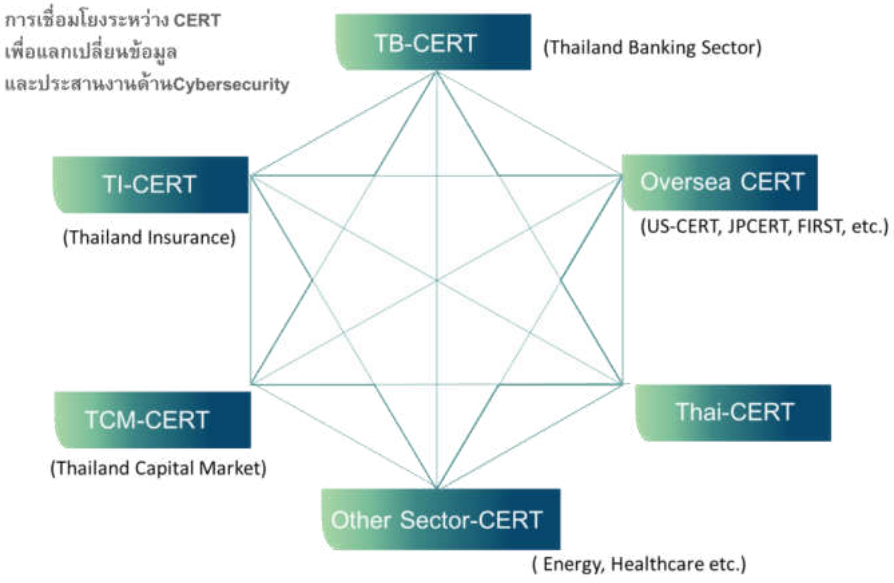
เนื่องจากภัยคุกคามทางไซเบอร์มีความซับซ้อนและรุนแรงมากขึ้นเรื่อย ๆ การที่แต่ละธนาคารต้องเผชิญกับการแก้ปัญหาเองนั้นทำให้ไม่สามารถระงับเหตุและรับมือกับภัยคุกคามได้อย่างมีประสิทธิภาพ การรวมกลุ่มกันเพื่อแลกเปลี่ยนข้อมูลและแนวทางในการแก้ไขปัญหาจึงช่วยเพิ่มประสิทธิภาพในการป้องกันภัยไซเบอร์ให้กับภาคการเงินการธนาคาร ทางสมาคมธนาคารไทยได้เล็งเห็นความจำเป็นดังกล่าวจึงมีการตั้งกลุ่ม Information Sharing Group หรือ ISG ขึ้นเพื่อสร้างเครือข่ายของผู้ที่ทำงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของธนาคารสมาชิกและเพื่อแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งนอกจากจะเป็นการระงับเหตุที่เกิดขึ้นกับภาคการเงินการธนาคารแล้วยังเป็นการยกระดับความเชี่ยวชาญของบุคคลากรในภาคการเงินการธนาคารด้วย จากความตั้งใจที่จะแก้ไขปัญหาดังกล่าวของผู้บริหารธนาคารสมาชิกภายใต้สมาคมธนาคารไทย จึงได้ยกระดับ ISG ให้เป็นหน่วยงาน CERT หรือ Computer Emergency Response Team เพื่อขยายความร่วมมือไปยังหน่วยงาน CERT อื่น ๆ ทั้งในและนอกประเทศ โดยนอกจากการเชื่อมข้อมูลที่กว้างขึ้นแล้ว ยังจะช่วยสร้างองค์ความรู้และพัฒนาความเชี่ยวชาญในการแก้ไขปัญหาภาพรวมที่รวดเร็วขึ้นและยังเป็นการใช้ทรัพยากรที่มีอยู่ อย่างมีประสิทธิภาพ จึงได้เปลี่ยนชื่อจาก ISG เป็น Thailand Banking Sector CERT หรือ TB-CERT

ค่านิยมหลัก

TB-CERT เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลในด้านความมั่นคงปลอดภัยไซเบอร์ เป็นศูนย์รวมของบุคลากรที่มีความชำนาญด้านไซเบอร์ และเป็นแหล่งให้ความรู้และสร้างความตระหนักในการระวังภัยที่อาจเกิดขึ้นได้ทุกเมื่อกับบุคคลากรของธนาคาร ลูกค้าของธนาคารและธุรกิจของธนาคาร รวมถึงเป็นศูนย์กลางในการติดต่อสื่อสารกับองค์กรที่เกี่ยวข้องทั้งในและนอกประเทศเพื่อให้สามารถรับรู้ข่าวสารและช่วยแก้ปัญหาภัยไซเบอร์ที่เกิดขึ้นกับสมาชิก ทั้งนี้เพื่อให้ทุกภาคส่วนมีความรู้และเข้าใจเรื่องภัยไซเบอร์ที่มีเพิ่มขึ้นทุกวันและพร้อมที่จะรับมือกับภัยเหล่านี้ได้อย่างมีประสิทธิภาพ

การสร้างความเข้มแข็งให้กับTB-CERT

การสร้างความร่วมมือกับหน่วยงานหรือองค์กรอื่นโดยเฉพาะหน่วยงานที่เป็น CERT ด้วยกันจะช่วยให้ TB-CERT สามารถรับรู้ข้อมูลข่าวสาร ภัยไซเบอร์ เทคนิคการโจมตีในรูปแบบต่างๆ กรณีศึกษาจากผู้ที่พบเจอเหตุการณ์คุกคามทางไซเบอร์จากภายนอกได้อย่างรวดเร็วเท่าทันกับภัยที่เกิดขึ้นอย่างมาก และการเชื่อมโยง ประสานงานของกลุ่ม CERT เหล่านี้ยังช่วยสร้างความสัมพันธ์ที่ดีเพื่อในกรณีเกิดเหตุและจำเป็นต้องขอความร่วมมือกับหน่วยงานที่เกี่ยวข้องสามารถทำได้อย่างทันท่วงที



ประโยชน์ที่ได้รับ

ประโยชน์ที่ผู้มีส่วนได้ส่วนเสียของธนาคารพึงจะได้รับ

ภาคการธนาคาร	ธนาคารสมาชิก	ลูกค้า
• มาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์ • ประสิทธิภาพการรับมือภัยไซเบอร์	• การแจ้งเตือนภัยไซเบอร์ • ข้อแนะนำด้านความปลอดภัยไซเบอร์	• ความรู้ความเข้าใจด้านความมั่นคงปลอดภัยไซเบอร์ • ความมั่นใจในบริการออนไลน์ของธนาคาร

สมาชิก

สมาชิกประกอบไปด้วย 4 กลุ่มหลัก ได้แก่

กลุ่มที่ 1: สมาชิกที่มาจากธนาคารพาณิชย์ซึ่งเป็นสมาชิกของสมาคมธนาคารไทย

กลุ่มที่ 2: สมาชิกที่มาจากธนาคารเฉพาะกิจของรัฐ

กลุ่มที่ 3: สมาชิกที่มาจากธนาคารพาณิชย์ซึ่งเป็นสมาชิกของสมาคมธนาคารนานาชาติ

กลุ่มที่ 4: สมาชิกที่มาจากองค์กรที่สนับสนุนธุรกิจและกำกับดูแลธนาคารในประเทศไทย

พันธกิจของTB-CERT

Thailand Banking Sector CERT หรือ TB-CERT มีบทบาทที่สำคัญในการเป็นศูนย์กลางของกลุ่มการเงินการธนาคารเพื่อแลกเปลี่ยนข้อมูลและประสานงานแก้ไขปัญหาภัยคุกคามไซเบอร์ โดยมีผู้ที่มีความรู้ความสามารถและความเข้าใจผลกระทบกับการบริการของภาคการเงินการธนาคารมาช่วยวิเคราะห์และหาแนวทางในการรับมือกับภัยไซเบอร์ นอกจากนั้น TB-CERT ยังมีส่วนช่วยยกระดับความเข้าใจด้านความมั่นคงปลอดภัยให้กับธนาคารสมาชิก รวมถึงลูกค้าของธนาคารอีกด้วย การที่ TB-CERT มีความเชื่อมโยงกับหน่วยงาน CERT และ แหล่งข้อมูล ทั้งในประเทศและต่างประเทศทำให้เราสามารถรับข้อมูลข่าวสารจากทั่วทุกมุมโลกได้อย่างรวดเร็วเราจึงได้กำหนดกรอบการดำเนินงานโดยจะครอบคลุม 4 ด้านที่สำคัญคือ

ด้านที่ 1 เป็นศูนย์กลางในการแลกเปลี่ยนข้อมูล ทั้งภัยคุกคามทางด้านไซเบอร์และแนวทางการแก้ไข

ด้านที่ 2 สร้างมาตรฐานกลางด้านความมั่นคงปลอดภัยของการใช้เทคโนโลยีใหม่

ด้านที่ 3 กำหนดกระบวนการในการรับมือภัยไซเบอร์ในภาคการธนาคาร และจัดให้มีการซ้อมรับมือร่วมกันสม่ำเสมอ

ด้านที่ 4 ส่งเสริมการพัฒนาบุคลากรด้าน Cybersecurity โดยครอบคลุมทั้งการสร้างบุคลากรใหม่เข้าสู่ภาคการเงิน และพัฒนาบุคลากรของสถาบันการเงินให้มีความรู้ความเข้าใจ และสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์

กิจกรรมและเหตุการณ์สำคัญปี 2560

25 มีนาคม 2560 จัดอบรมเรื่อง Digital Evident Preservation Workshop ให้กับสมาชิก ณ ห้องประชุม สมาคมธนาคารไทย

17-21 สิงหาคม 2560 จัดอบรมเรื่อง ISO 27001 Boot Camp for implementer and Auditor ณ อาคารทิสโก้ ทาวเวอร์

2 ตุลาคม 2560 จัดงานแถลงข่าวการจัดตั้ง TB-CERT ร่วมกับธนาคารแห่งประเทศไทย และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

2 พฤศจิกายน 2560 จัดการฝึกซ้อมรับมือภัยคุกคามไซเบอร์ภาคการธนาคาร (Banking Cyber Drill 2017: Table Top Exercise) ณ ธนาคารกสิกรไทย

24 พฤศจิกายน 2560 จัดอบรมให้แก่สมาชิก TB-CERT ในหัวข้อ IoT and SCADA security; Hacker view ณ ธนาคารกรุงเทพ ถนนพระราม 3

27 มิถุนายน 2560 จัดอบรมเรื่อง APT Analysis ให้กับสมาชิก ณ ธนาคารกรุงเทพ ถนนพระราม 3

5 กันยายน 2560 ได้บรรลุข้อตกลงในการจัดตั้ง Thailand Banking Sector CERT (TB-CERT) จาก CERT/CC อย่างเป็นทางการ

6-8 ตุลาคม 2560 จัดกิจกรรมโครงการ Financial Sector Cybersecurity Boot Camp ให้แก่นิสิต นักศึกษาในสาขาวิชาที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ณ สำนักบริการคอมพิวเตอร์ มหาวิทยาลัยเกษตรศาสตร์

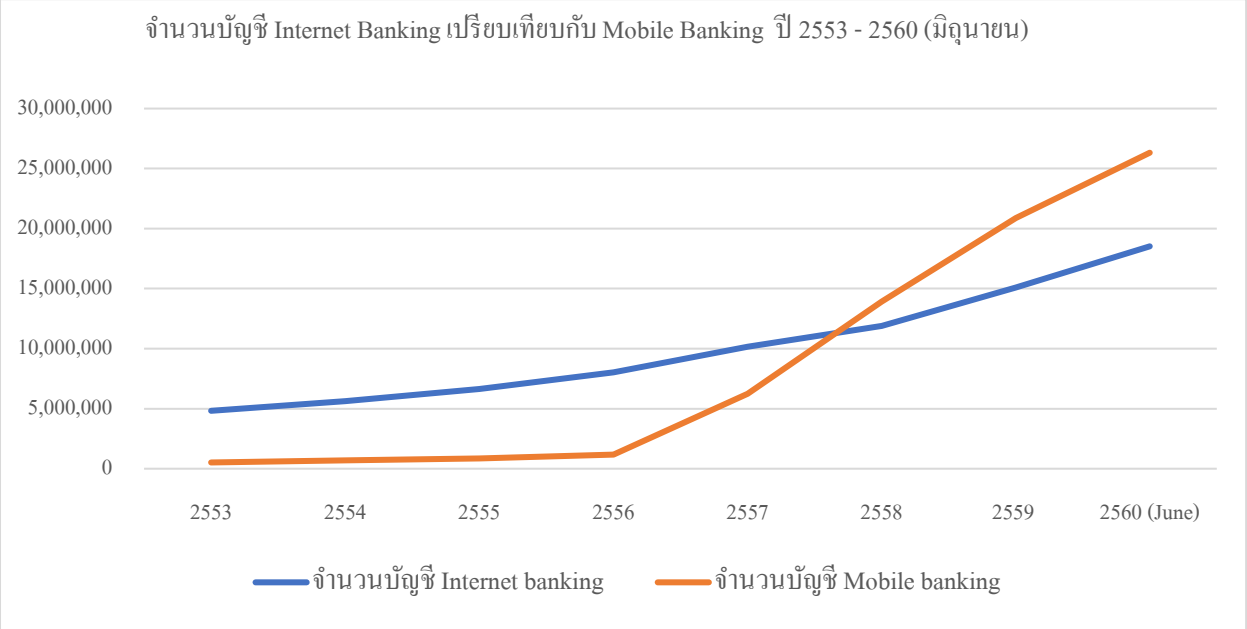
23 พฤศจิกายน 2560 ร่วมจัดงานสัมมนาเพื่อเสริมสร้างความรู้และความตระหนักด้านความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Resilience) ให้แก่คณะกรรมการและผู้บริหารระดับสูงของสถาบันการเงิน ณ ห้องภัทรรวมใจ ธนาคารแห่งประเทศไทย

บทวิเคราะห์ภัยคุกคามทางไซเบอร์

ปัจจุบันเทคโนโลยีสารสนเทศทั้งอินเทอร์เน็ตและโทรศัพท์มือถือเข้ามามีบทบาทอย่างมากในชีวิตประจำวัน จากผลสำรวจการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2559 ของสำนักงานสถิติแห่งชาติพบว่า ในจำนวนประชากรที่มีอายุ 6 ปีขึ้นไปประมาณ 62.8 ล้านคน มีจำนวนผู้ใช้โทรศัพท์มือถือประเภทสมาร์ทโฟนมากถึง 31.7 ล้านคน (ร้อยละ 50.5) โดยมีอัตราการใช้เพิ่มขึ้นอย่างต่อเนื่องนับตั้งแต่ ปี 2555 ที่มีผู้ใช้สมาร์ทโฟนเพียง 5 ล้านคน หรือ (ร้อยละ 8.0) ส่วนกิจกรรมที่ทำส่วนใหญ่ใช้งานสมาร์ทโฟนเพื่อใช้งานเครือข่ายสังคมออนไลน์ (Social Media) ร้อยละ 91.5 ใช้เพื่อดาวน์โหลด หนัง เพลง ร้อยละ 88.0 ใช้อัพโหลดข้อมูล ร้อยละ 55.9 และใช้ติดตามข่าวสาร ร้อยละ 46.5

เทคโนโลยีการชำระเงินก็เช่นกัน จากในอดีตที่นิยมใช้จ่ายด้วยเงินสด ปัจจุบันมีการนำเทคโนโลยีมาช่วยอำนวยความสะดวกทำให้การชำระเงินง่ายดาย สะดวกสบายและมีความรวดเร็วมากยิ่งขึ้น ยกตัวอย่าง เช่น พร้อมเพย์ การชำระเงินด้วยคิวอาร์โค้ด หรือการโอนเงินผ่านอินเทอร์เน็ต เป็นต้น จากสถิติธุรกรรมการชำระเงินผ่านบริการ Mobile Banking และ Internet Banking ของธนาคารแห่งประเทศไทย [4] พบว่า จำนวนบัญชีผู้ใช้งาน Internet Banking และ Mobile Banking เพิ่มขึ้นอย่างต่อเนื่องตั้งแต่ปี 2553 ที่มีจำนวนบัญชี 4,822,947 และ 519,450 บัญชีตามลำดับ จนในปี 2560 เดือนมิถุนายน มีจำนวนบัญชีผู้ใช้งาน Internet Banking 18,523,590 บัญชี และ Mobile Banking 26,322,671 บัญชี ซึ่งเมื่อวิเคราะห์เพิ่มเติมจากกราฟรูปที่ 1

จะเห็นว่าจำนวนบัญชีผู้ใช้งาน Internet Banking จะเพิ่มขึ้นค่อนข้างคงที่ แต่จำนวนบัญชีผู้ใช้งาน Mobile Banking เพิ่มขึ้นอย่างรวดเร็วตั้งแต่ปี 2556 มีอัตราการเติบโตถึงประมาณร้อยละ 50 ของทุกปี



รูปที่ 2 กราฟแสดงความสัมพันธ์ของจำนวนบัญชี Internet Banking เปรียบเทียบกับ Mobile Banking ตั้งแต่ปี 2553 – 2560 (มิถุนายน)

เมื่อจำนวนผู้ใช้งานอินเตอร์เน็ตเพิ่มมากขึ้น ไม่เพียงแต่การใช้เพื่อค้นหาข้อมูลความรู้ต่างๆ หรือเพื่อความบันเทิงแต่ยังมีแนวโน้มที่จะใช้เพื่อความสะดวกในชีวิตประจำวันไม่ว่าจะเป็นด้านการเงิน การลงทุน ด้านสุขภาพ ซึ่งล้วนแล้วแต่เป็นการใช้งานที่ต้องใช้ข้อมูลสำคัญและเชื่อมโยงกับข้อมูลส่วนบุคคลทั้งสิ้น จึงไม่น่าแปลกใจที่จะเป็นแรงจูงใจให้ผู้ประสงค์ร้ายจะมุ่งฉกฉวยโอกาสที่จะขโมยทรัพย์สินมีค่า ไม่ว่าจะเป็นเงินในบัญชี หรือข้อมูลสำคัญต่างๆ ดังนั้นผู้ใช้งานที่ขาดความระมัดระวังและความตระหนักด้านการรักษาความมั่นคงปลอดภัยสารสนเทศจึงอาจตกเป็นเหยื่อของผู้ประสงค์ร้ายเหล่านี้ได้อย่างง่ายดาย ด้านของผู้ให้บริการก็มีแนวโน้มที่จะย้ายบริการต่างๆ ไปอยู่ที่ผู้ให้บริการคราวส์ แม้ว่าความมั่นคงปลอดภัยระบบของผู้ให้บริการคราวส์โดยส่วนใหญ่จะมีความเข้มแข็งกว่าอีกหลายหน่วยงานโดยเฉพาะสำหรับหน่วยงานขนาดเล็กก็ไม่สามารถลงทุนเทคโนโลยีด้านความมั่นคงปลอดภัยได้เท่าเทียมกัน ส่วนด้านการพัฒนาด้าน

บุคคลากรก็ยังคงเป็นโจทย์ที่ต้องร่วมกันในทุกภาคส่วน จากสถานการณ์การใช้งานของผู้ใช้งานและการให้บริการบนโลกไซเบอร์ที่มีการเปลี่ยนแปลงสูงในระยะนี้ทาง TB-CERT ได้มีการรวบรวมข้อมูลเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ของภาคการธนาคารได้ดังนี้

1) ภัยคุกคามเกี่ยวกับการหลอกขโมยข้อมูล ภัยคุกคามประเภทนี้ไม่ใช่ภัยคุกคามรูปแบบใหม่แต่ยังคงเป็นภัยคุกคามที่ยังใช้ได้อย่างมีประสิทธิภาพเนื่องจากปัจจัยสำคัญ 2 ประการคือ ประการแรก การพัฒนาของเทคโนโลยีในปัจจุบันเป็นไปอย่างรวดเร็วโดยผู้ใช้งานไม่สามารถติดตามการเปลี่ยนแปลงเทคโนโลยีหรือมีความเข้าใจเพียงพอเพื่อที่จะสามารถแยกแยะระหว่างสิ่งที่ถูกต้องและสิ่งที่ทำเลียนแบบเพื่อขโมยข้อมูล ประการที่สอง เทคนิคการชวนเชื่อของผู้ประสงค์ร้ายมีการพัฒนาไปตามสถานการณ์และมีความซับซ้อนแนบเนียนมากขึ้น แต่การแจ้งเตือนถึงวิธีเหล่านั้นให้กับผู้ใช้อินเตอร์เน็ตที่มีจำนวนมากเป็นไปได้ช้ากว่ามาก จึงทำให้เทคนิคการหลอกขโมยยังใช้ได้อย่างมีประสิทธิภาพ ไม่ว่าจะเป็น phishing (การหลอกขโมยข้อมูลทางเมล), vishing(Voice Over IP Phishing การหลอกขโมยข้อมูลทางโทรศัพท์) เป็นต้น

“เทคนิคการหลอกขโมยข้อมูลยังใช้ได้มีประสิทธิภาพเนื่องจากผู้ใช้ไม่สามารถติดตามการเปลี่ยนแปลงเทคโนโลยีได้ทัน”

นอกจากนั้นในปีที่ผ่านมามีการพบการสร้างฟิชชิงด้วย Punycode ซึ่ง Punycode โดยการใช้อักษรในภาษาอื่นที่มีลักษณะใกล้เคียงกับตัวอักษรภาษาอังกฤษบนชื่อเว็บไซต์ ทำให้เมื่อผู้ใช้งานเปิดใช้เว็บเบราเซอร์บางเวอร์ชั่นที่ไม่แสดงชื่อเว็บไซต์เป็น Punycode ก็ไม่มีทางทราบอย่างแน่นอนว่าเว็บไซต์ดังกล่าวเป็นเว็บหลอกลวงนอกจากจะต้องพิมพ์ URL ของ Website ที่สำคัญด้วยตัวเอง

สำหรับการหลอกลวงผ่านทางโทรศัพท์ (วิชชิง หรือ Vishing) ซึ่งในประเทศไทยรู้จักกันในชื่อของ “แก๊งคอลล์เซ็นเตอร์” ยังคงถูกใช้กันอย่างแพร่หลาย ลักษณะรูปแบบการหลอกลวง

ประเภทนี้ ผู้ประสงค์ร้ายจะแอบอ้างตัวเป็นธนาคารหรือหน่วยงานราชการต่าง ๆ แล้วทำการติดต่อเหยื่อทางโทรศัพท์ เพื่อหลอกถามข้อมูลส่วนตัวของเหยื่อหรืออาจหลอกล่อให้เหยื่อดำเนินการตามความต้องการของตน เช่น การหลอกให้โอนเงินผ่านตู้เอทีเอ็ม หรือเติมเงินในโทรศัพท์มือถือ เป็นต้น ตัวอย่างเหตุการณ์ที่ผู้ประสงค์ร้ายนิยมใช้เพื่อการหลอกลวง ได้แก่ โทรศัพท์ไปแจ้งว่าเหยื่อเป็นหนี้บัตรเครดิต เป็นผู้โชคดีได้รับรางวัล หรือมีพัสดุค้างที่ไปรษณีย์ เป็นต้น แม้ว่าจะไม่มีหน่วยงานใดยืนยันข้อมูลความเสียหายรายปีของผู้ที่ถูกแก๊งคอลล์เซ็นเตอร์หลอกลวงในประเทศไทย แต่ข่าวจากหน้าหนังสือพิมพ์ พบว่าในช่วง 7 เดือนของปี 2560 เจ้าหน้าที่ตำรวจสามารถยึดของกลางจากแก๊งคอลล์เซ็นเตอร์ได้กว่า 120 ล้านบาท ซึ่งผู้เสียหายบางคนสามารถอายัดบัญชีได้ทันก่อนที่คนร้ายจะโอนเงินออกไป และผู้เสียหายบางคนถูกหลอกลวงเงินไปมากกว่า 1.5 ล้านบาท ดังนั้น ผู้ใช้งานจึงต้องใช้ความระมัดระวังในการตอบคำถามผ่านทางโทรศัพท์ โดยเฉพาะอย่างยิ่งเมื่อมีคนที่ไม่รู้จักคุ้นเคยพยายามโน้มน้าวให้ต้องรีบโอนเงินให้ ยิ่งต้องใช้ความระมัดระวังให้มากขึ้นอีกด้วย

ผลกระทบของภัยคุกคามประเภทนี้คงไม่ได้หยุดอยู่ที่การที่ข้อมูลถูกขโมย แต่เนื่องจากในปัจจุบันข้อมูลเป็นสิ่งที่สำคัญโดยเฉพาะข้อมูลส่วนบุคคล ซึ่งมักจะเป็นเป้าหมายแรงจูงใจให้ผู้ประสงค์ร้ายหาวิธีที่จะหลอกขโมยข้อมูลไปเพื่อนำไปสร้างผลกระทบกับเจ้าของข้อมูลต่อไป ไม่ว่าจะเป็นการเข้าใช้ Internet Banking, เปิดบัญชีในนามของเจ้าของบัญชีหรือแม้กระทั้งนำข้อมูลไปขาย ซึ่งล้วนแล้วแต่จะเป็นผลกระทบที่ไม่สามารถคาดการได้

2) ภัยคุกคามต่อเมลที่ใช้ในกระบวนการทำธุรกิจ (BEC – Business Email Compromise) ในปีที่ผ่านมากระแสเทคนิคการส่งข้อความเลียนแบบข้อความที่ใช้ในธุรกิจเริ่มตั้งแต่การส่งเมลเพื่อติดต่อธุรกิจ แจ้งความจำนงค์ในการร่วมทำธุรกรรม จนถึงการปลอมเมลเพื่ออนุมัติการจ่ายเงินหรือโอนเงิน ซึ่งกระบวนการดังกล่าวอาจจะดำเนินไปอย่างช้าๆ แต่ผู้ประสงค์ร้ายจะต้องทำการศึกษาขั้นตอนและกระบวนการทำธุรกิจเป็นอย่างดีรวมถึงรูปแบบข้อความการรับส่งเมลโต้ตอบ และที่สำคัญคือผู้ประสงค์ร้ายต้องมีความเข้าใจกลไกการรับส่งเมลรวมถึงจุดอ่อนของ

“ระบบเมลถูกพัฒนามาในช่วงที่ไม่ได้ให้ความสำคัญด้านความมั่นคงปลอดภัย องค์กรจะต้องให้ความเข้าใจถึงข้อสังเกตกับเจ้าหน้าที่ที่ปฏิบัติงาน”

การรับส่งเมลเนื่องจากระบบเมลถูกพัฒนามาในช่วงที่ไม่ได้ให้ความสำคัญด้านความมั่นคงปลอดภัย กล่าวคือ สามารถปลอมเมลผู้ส่งหรือควบคุมการส่งเมลกลับได้อย่างไม่ยาก ความเสียหายจากภัยคุกคามประเภทนี้ สร้างความเสียหายทางธุรกิจเป็นจำนวนมาก โดยองค์กรจะต้องให้ความเข้าใจถึงข้อสังเกตให้กับเจ้าหน้าที่ที่ปฏิบัติงานเพื่อให้สามารถแยกแยะความแตกต่างระหว่างเมลจริงและเมลปลอมหรืออาจจะเพิ่มเครื่องมือหรือกระบวนการตรวจสอบความผิดปกติก่อนอนุมัติธุรกรรมการเงิน ถึงแม้ว่ายังไม่เคยมีประกาศความเสียหายที่เกิดจากเทคนิคดังกล่าวในประเทศไทย แต่ภัยคุกคามประเภทนี้ได้ถูกใช้อย่างแพร่หลายทั่วโลก FBI มีรายงานความเสียหายที่เกิดจากภัยคุกคาม BEC ทั่วโลกนับตั้งแต่เดือนตุลาคมปี 2556 จนถึงสิ้นปี 2559 พบว่ามีความเสียหายราว 5.3 พันล้านเหรียญสหรัฐ นับว่าเป็นตัวเลขที่สูงมาก

3) ภัยคุกคามที่เกิดจากมัลแวร์เรียกค่าไถ่ (Ransomware) การเรียกค่าไถ่ถือเป็นเทคนิคที่ถูกนำมาใช้มากขึ้นในระยะ 2-3 ปีนี้ โดยทั่วไปมัลแวร์เรียกค่าไถ่จะแพร่กระจายตัวเองผ่านใช้อีเมลหรือฝังตัวเองในเว็บไซต์ต่างๆ เมื่อผู้ใช้งานเปิดไฟล์แนบในอีเมลหรือเข้าเว็บไซต์ที่มัลแวร์เรียกค่าไถ่นี้ฝังตัวอยู่ ไฟล์ในเครื่องของผู้ใช้งานจะถูกเข้ารหัส ทำให้ไม่สามารถเปิดใช้งานไฟล์เหล่านี้ได้ จากนั้นจะมีข้อความแสดงขึ้นบนหน้าจอคอมพิวเตอร์ของผู้ใช้งาน แจ้งผู้ใช้งานให้จ่ายเงินค่าไถ่เพื่อที่จะได้กุญแจเพื่อถอดรหัสกู้ข้อมูลกลับคืนมา แต่กลไกการจ่ายเงินเรียกค่าไถ่นั้นมักจะเกี่ยวข้องกับ cyptocurrency เพื่อมิให้สามารถติดตามได้ว่าผู้รับประโยชน์เป็นใคร ในอีกด้านหนึ่งก็หมายความว่าผู้ที่ตกเป็นเหยื่อแม้ว่าจะจ่ายเงินตามที่ถูกร้องขอมาก็ไม่ได้มีอะไรเป็น

หลักประกันที่จะได้กุญแจในการถอดรหัส อีกทั้งอาจจะเป็นการส่งเสริมธุรกิจของผู้ประสงค์ร้ายให้แพร่หลายมากขึ้นอีกด้วย

"การจ่ายเงินค่าไถ่ไม่ได้มีอะไรเป็นหลักประกันที่จะได้กุญแจในการถอดรหัส"

จนกระทั่งปี 2560 ได้มีการค้นพบ Wannacry ซึ่งเป็นมัลแวร์เรียกค่าไถ่ชนิดแรกที่สามารถแพร่กระจายด้วยเทคนิคโจมตีผ่านช่องโหว่ของระบบปฏิบัติการไมโครซอฟท์วินโดวส์ หมายเลข MS17-010 (เป็นช่องโหว่ของ Microsoft Server Message Block 1.0 (SMBv1) server) ซึ่งคล้ายกับเทคนิคการแพร่กระจายตัวของหนอนอินเทอร์เน็ต ด้วยเทคนิคการแพร่กระจายนี้เองทำให้มัลแวร์เรียกค่าไถ่ Wannacry สามารถแพร่กระจายได้อย่างรวดเร็ว ต่อมาไม่นานก็มีมัลแวร์เรียกค่าไถ่ชื่อ Petya ถูกค้นพบ และใช้เทคนิคในการแพร่กระจายเหมือนกับ Wannacryข้อมูลสถิติความเสียหายทั่วโลกในช่วงที่มัลแวร์เรียกค่าไถ่ทั้ง 2 ชนิดนี้แพร่กระจายพบว่า มีจำนวนเครื่องคอมพิวเตอร์ที่ถูก Wannacry คุกคามมากกว่า 200,000 เครื่อง จาก 112 ประเทศ โดยเกิดผลกระทบสูงต่อหน่วยงานสาธารณสุขของประเทศอังกฤษ ในประเทศไทยพบผู้ติดมัลแวร์ตัวนี้บ้าง แต่ไม่พบการแพร่กระจายในวงกว้าง ส่วนการแพร่กระจายตัวของ Petya นั้นพบว่ามีประเทศที่ได้รับแจ้งว่าถูกโจมตี ได้แก่ รัสเซีย ยูเครน อินเดีย และประเทศในแถบยุโรป โดยมีหน่วยงานที่ได้รับผลกระทบ เช่น ธนาคารกลาง บริษัทพลังงานไฟฟ้า และสนามบิน เป็นต้น

ฉะนั้นแนวทางปฏิบัติที่เหมาะสมคือการสำรองข้อมูลอย่างสม่ำเสมอ ซึ่งถึงแม้ว่าไม่มีการเรียกค่าไถ่ แต่การสำรองข้อมูลอย่างสม่ำเสมอก็ยังช่วยให้ธุรกิจมีความมั่นคงมีเสถียรภาพและยังเป็นการเตรียมความพร้อมรับมือไม่ว่าจะเป็นภัยไซเบอร์หรือเหตุการณ์วิกฤติต่อระบบงานเทคโนโลยีสารสนเทศได้ดีอีกด้วย

4) ภัยคุกคามที่มุ่งไปที่กระบวนการบริหารจัดการ Patch อย่างที่ทราบกันว่าช่องโหว่ของซอฟท์แวร์ไม่ว่าจะเป็น OS ของค่ายใด application software ของบริษัทไหน firmware ของ

อุปกรณ์เน็ตเวอร์คไฟลวอล หรือแม้กระทั้งซีพียู ก็ยังมีช่องโหว่ด้านความมั่นคงปลอดภัย แต่การปิดช่องโหว่เป็นกระบวนการที่ใช้ระยะเวลาและมีผลกระทบสูงเนื่องจากทางเจ้าของสินค้าต้องสร้าง Patch และกระจายให้ผู้ใช้งานนำไปทดสอบเพื่อให้มั่นใจว่าไม่มีผลกระทบกับบริการนั้นๆ ก่อนที่จะนำไปลงในระบบงานจริง ในบางครั้งข้อมูลช่องโหว่ก็ไม่ถูกเปิดเผยออกสู่สาธารณะแต่ข้อมูลดังกล่าวกลับถูกรู้โดยกลุ่มมิจฉาชีพ และ ถูกนำไปใช้ในการสร้างมัลแวร์เรียกค่าไถ่เช่น Ransomware Wannacry ในปีที่ผ่านมาซึ่งมีอัตราการแพร่กระจายอย่างรวดเร็วมากจนทำให้เกิดผลกระทบในวงกว้างทั่วโลก ส่วนช่องโหว่ที่น่าจับตามองอีกช่องโหว่หนึ่งคงหนีไม่พ้นช่องโหว่ของ CPU ที่เรียกกันว่า Meldown and Spectre ซึ่งเรียกได้ว่าเป็นช่องโหว่ที่ทราบกันก่อนปี 2018 แต่ช่องโหว่นี้เป็นช่องโหว่ของการออกแบบซีพียูเพื่อให้มีประสิทธิภาพในการทำงานสูงขึ้นเนื่องจากซีพียูมีความสามารถในการประมวลผลที่สูงมาก ในการออกแบบการทำงานของซีพียูจึงสร้างกลไกที่

“การปิดช่องโหว่เป็นกระบวนการที่ใช้ระยะเวลาและมีผลกระทบสูง”

เรียกว่า Speculative execution เพื่อให้ซีพียูสามารถคาดเดาและประมวลผลในขั้นตอนล่วงหน้าหากอัลกอริทึมในการคาดเดาเป็นไปได้อย่างมีประสิทธิภาพจะทำให้การทำงานโดยรวมมีประสิทธิภาพที่สูงขึ้น แต่การทำเช่นนี้จะทำให้เกิดช่องโหว่ที่ application อื่นจะสามารถเข้าถึงข้อมูลของ application อื่นโดยที่ Speculative execution ไม่ได้ออกแบบมาเพื่อป้องกันด้านการเข้าถึงข้อมูลโดย application อื่นจึงสร้างปัญหาช่องโหว่ด้านความมั่นคงปลอดภัยซึ่งการป้องกันปัญหาช่องโหว่นี้จะทำให้เกิดผลกระทบกับ performance ของเครื่องโดยตรงเนื่องจากเป็น feature ที่ช่วยด้านประสิทธิภาพการทำงานของซีพียู โดยในหลายองค์กรยังต้องการให้มีการแก้ปัญหาช่องโหว่นี้ร่วมกับแนวทางที่ไม่มีผลกระทบกับ performance อย่างไรก็ตามปัญหาช่องโหว่นี้ยังคงเป็นข้อถกเถียงกันในวงกว้างและยังมีอีกหลายองค์กรที่ยังไม่ได้แก้ไขช่องโหว่นี้

โดยตรง ในปี 2018 นี้จึงจะเป็นประเด็นที่น่าจับตามองเนื่องจากมิจฉาชีพจะยังคงสามารถใช้ใช้ช่องโหว่นี้ก่อกวนไม่ว่าจะเป็นการสร้าง Ransomware หรืออาจจะใช้ในการเรียกค่าไถ่ขโมยข้อมูลได้อีกด้วย

5) ภัยคุกคามที่มุ่งจะขโมยข้อมูลองค์กร (Data Breach attack) ซึ่งอย่างที่ทราบกันว่าการศึกษาวิจัยหรือการทำธุรกิจในปัจจุบัน ข้อมูลเป็นสิ่งที่สำคัญเป็นอย่างมากเนื่องจากข้อมูลจะสร้างความได้เปรียบ จะสร้างความก้าวหน้า จะสร้างความสะดวกสบายให้กับผู้ใช้งาน แล้ว ในอีกด้านหนึ่งการที่ข้อมูลถูกขโมยไปจะทำให้เกิดผลกระทบในด้านความมั่นใจ ความเชื่อมั่นหรือสูญเสียสภาพการแข่งขันอีกด้วย ข้อมูลที่มักจะเป็นเป้าหมายในการขโมยนั้นเป็นได้ทั้งข้อมูลบริษัทบริษัทคู่ค้าและข้อมูลส่วนบุคคลที่เก็บอยู่ในระบบงาน โดยไม่จำกัดว่าจะเป็นระบบงานในดาต้าเซ็นเตอร์หรือเป็นระบบงานบนคราวส์ซึ่งเป็นแนวทางที่หลายๆ หน่วยงานมีแผนที่จะทยอยเริ่มใช้บริการของผู้ให้บริการคราวส์ซึ่งข้อมูลที่สำคัญในการทำธุรกิจก็จะเริ่มไปอยู่บนคราวส์มากขึ้นในขณะเดียวกันวิธีบริหารจัดการในการใช้บริการคราวส์ก็จำเป็นต้องมีขั้นตอนและกรอบการบริหารจัดการที่เหมาะสม

“ข้อมูลถูกขโมยไปจะทำให้เกิดผลกระทบในด้านความมั่นใจ ความเชื่อมั่นหรือสูญเสียสภาพการแข่งขันอีกด้วย”

วิธีโจมตีเพื่อเข้าถึงข้อมูลขององค์กรนั้นมีได้หลากหลายซึ่งรวมทั้งการเริ่มต้นใช้ phishing หรือบางครั้งคือ Spear phishing สำหรับการระบุเป้าหมายบุคคลชัดเจน การใช้เทคนิค BEC การใช้มัลแวร์ฝังตัวในองค์กร เฝ้าเก็บข้อมูลกิจกรรมต่างๆ ภายในองค์กรจนสามารถเข้าถึงข้อมูลที่ต้องการ หรือแม้กระทั้งการใช้เทคนิคร่วมกับ social engineering

เพื่อให้สามารถเข้าถึงระบบภายในองค์กรซึ่งก็ล้วนแล้วแต่มีแรงจูงใจเพื่อ gain access ให้สามารถเข้าถึงข้อมูลสำคัญ ทั้งนี้การเตรียมการป้องกันการรั่วไหลของข้อมูลนั้นนอกจากจะต้องมีการเฝ้าติดตามกิจกรรมการเข้าถึงข้อมูลองค์กร การเฝ้าระวังกิจกรรมของมัลแวร์ในองค์กร

การกำหนดสิทธิการเข้าถึงข้อมูลให้อยู่ในระดับเข้มงวดตามความจำเป็น (Need to Know basis) และที่สำคัญอย่างยิ่งคงจะหนีไม่พ้นการอบรมให้ความรู้สร้างความตระหนักให้กับพนักงาน ผู้บริหารและผู้ที่เกี่ยวข้องทุกคนในองค์กร

ส่วนในรอบปีที่ผ่านมามีเหตุการณ์ภัยคุกคามด้านไซเบอร์ที่เกิดขึ้นกับธนาคารในหลายประเทศทั่วโลกที่น่าสนใจ อาทิเช่น

- วันที่ 30 มิถุนายน 2560 มีเหตุการณ์การโจมตีแบบการปฏิเสธการให้บริการ (Distributed Denial of Services หรือ DDoS) ของกลุ่มผู้โจมตีชื่อ Armada Collective ที่มีการส่งอีเมล์ข่มขู่เพื่อเรียกค่าไถ่จากหน่วยงานในกลุ่มธนาคารและกลุ่มหลักทรัพย์ในประเทศ ญี่ปุ่น เกาหลีใต้ และจีน โดยการโจมตีด้วย DDoS เกิดขึ้นจริงตามคำขู่ด้วย
- วันที่ 29 กรกฎาคม 2560 บริษัท Equifax ถูกเจาะระบบขโมยเพื่อข้อมูลบัตรเครดิตของลูกค้าในประเทศสหรัฐอเมริกาจำนวน 143 ล้านราย
- วันที่ 8 ตุลาคม 2560 เหตุการณ์การโจมตีระบบ SWIFT ของธนาคาร Far Eastern International Bank ประเทศไต้หวัน ส่งผลทำให้ธนาคารถูกขโมยเงินกว่า 60 ล้านเหรียญสหรัฐ

จากบทวิเคราะห์ที่กล่าวมาจะเห็นว่า ภัยคุกคามที่เกิดขึ้นแบ่งได้เป็นภัยคุกคามที่เกิดกับผู้ใช้งานและธนาคารผู้ให้บริการ ซึ่งทุกเหตุการณ์ล้วนสร้างความเสียหายมหาศาล ส่งผลให้ผู้ใช้งานสูญเสียทรัพย์สินและข้อมูล และธนาคารผู้ให้บริการนอกจากอาจจะสูญเสียทรัพย์สินหรือข้อมูลแล้ว ยังอาจสูญเสียชื่อเสียงและความเชื่อมั่นต่อผู้ใช้งาน ส่งผลกระทบต่อผลประกอบการของธนาคารอีกด้วย ดังนั้น แนวทางการป้องกันภัยคุกคามจึงต้องเกิดขึ้นจากทั้ง 2 ฝ่ายคือ ผู้ใช้งานควรต้องความระมัดระวังและความตระหนักด้านความปลอดภัยสารสนเทศ ส่วนทางด้านธนาคารผู้ให้บริการต้องป้องกันภัยคุกคามด้านไซเบอร์อย่างรัดกุม

แนวโน้มเทคโนโลยีและภัยไซเบอร์ในปี 2018 ของภาคการเงินการธนาคารในประเทศไทย

ปัจจุบันเทคโนโลยีสารสนเทศมีการพัฒนาอย่างรวดเร็ว และมีบทบาทสำคัญในด้านการลดต้นทุนและเพิ่มประสิทธิภาพในการทำงานให้แก่ภาคการธนาคารอย่างมีนัยสำคัญ ในขณะเดียวกันการพัฒนาทางด้านเทคโนโลยีก็เป็นช่องทางให้เกิดการโจมตีทางด้านไซเบอร์ที่มีปริมาณความถี่และความรุนแรงสูงขึ้น อันก่อให้เกิดความเสียหายทางเศรษฐกิจ สูญเสียประสิทธิภาพในการทำงาน รวมทั้งส่งผลกระทบต่อความเชื่อมั่นของผู้ใช้บริการ มีรายงานและผลสำรวจจำนวนมากยืนยันถึงความสำคัญในการป้องกันอันตรายที่มาจากการโจมตีทางไซเบอร์ เช่น

- จากผลการสำรวจองค์กรที่ใช้หุ่นยนต์และระบบอัตโนมัติของ 2018 Global State of Information Security Survey (GSISS) [5] พบว่า 40% ขององค์กรที่ถูกสำรวจ เห็นว่าการโจมตีทางไซเบอร์เป็นปัจจัยหลักที่ทำให้การดำเนินงานทางธุรกิจหยุดชะงัก และในปัจจุบันก็ยังไม่มีการเตรียมตัวรับมือการโจมตีอย่างจริงจัง
- Global Risks Report 2018 [6] จากหน่วยงาน World Economic Forum ระบุว่าการโจมตีทางไซเบอร์เป็นความเสี่ยงอันดับ 3 ของความเสี่ยงทั้งหมดทั่วโลก รองจากภัยพิบัติธรรมชาติและภัยลมฟ้าอากาศสุดโต่ง (extreme weather) อีกทั้งยังมีการใช้จ่ายด้านการตอบสนองต่อภัยคุกคามทางไซเบอร์เพิ่มขึ้นถึง 27.4% จากปี 2560 ที่มีการใช้จ่ายประมาณ 11.7 ล้านปอนด์ต่อบริษัท

- บริษัท Gartner [7] กล่าวว่ามีการใช้จ่ายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั่วโลกในปี 2560 ประมาณ 86.4 พันล้านเหรียญสหรัฐ และคาดการณ์ว่าในปี 2561 จะมีการใช้จ่ายด้านการรักษาความมมั่นคงปลอดภัยไซเบอร์ทั่วโลกรวมประมาณ 93 พันล้านเหรียญสหรัฐ
- Financial Stability Oversight Council (FSOC) ซึ่งเป็นหน่วยงานกำกับดูแลด้านการเงินของสหรัฐอเมริกาได้ประกาศรายงานประจำปี 2560 ว่าการคุกคามด้านไซเบอร์เป็นหนึ่งในความเสี่ยงสูงสุด

จะเห็นได้ว่า ปัจจุบันการโจมตีทางไซเบอร์ได้กลายเป็นความเสี่ยงอันดับต้นๆ ของทุกภาคส่วน โดยเฉพาะหน่วยงานธนาคารซึ่งกลายเป็นเป้าหมายหลักในการถูกโจมตี โดยแนวโน้มเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่น่าสนใจในปี 2561 มี 7 ด้าน ดังต่อไปนี้

1. **การชำระเงินผ่านอินเทอร์เน็ต** ในช่วงไม่กี่ปีที่ผ่านมาเทคโนโลยีที่เกี่ยวข้องกับการชำระเงินถูกพัฒนาไปอย่างรวดเร็ว ธนาคารต่างๆ ในประเทศไทยเปิดให้บริการโอนเงินด้วยระบบพร้อมเพย์ (Promptpay) การชำระเงินด้วยคิวอาร์โค้ด รวมทั้งจะมีบริการใหม่ๆ ซึ่งถูกนำมาใช้ในอนาคตอันใกล้ตามนโยบาย National e-payment ความสะดวกรวดเร็วในการทำธุรกรรมก็มาพร้อมกับ*ความเสี่ยง* ทั้งในเรื่องของความถูกต้องของข้อมูล ความผิดพลาดในการทำธุรกรรมอันเกิดจากความไม่ชำนาญหรือคุ้นชินกับเทคโนโลยี และอาจเป็นการเปิดโอกาสให้ผู้ประสงค์ร้ายหาประโยชน์จากความผิดพลาดต่างๆ เหล่านั้น ดังนั้น ผู้ใช้งานจึงจำเป็นต้องศึกษาเทคโนโลยีใหม่ๆ และฝึกหัดใช้งานให้เกิดความชำนาญหรือคุ้นเคย เพื่อจะได้ไม่ตกเป็นเหยื่อของเหล่าผู้ประสงค์ร้ายที่มักฉกฉวยโอกาสในการหลอกลวงทรัพย์สินผ่านทางระบบเทคโนโลยีการชำระเงินได้ ส่วนผู้ให้บริการเอง ทั้งในด้านของธนาคารและผู้ที่เกี่ยวข้องกับระบบการชำระเงินก็ต้องทำการติดตั้งระบบที่มีความปลอดภัยสูง การเฝ้าระวัง รวมถึงการวิเคราะห์เหตุการณ์ความเสี่ยงต่างๆ เพื่อช่วยเหลือให้ผู้ใช้สามารถใช้บริการได้อย่างปลอดภัย
2. **Social Engineering** เป็นเทคนิคที่ผู้ประสงค์ร้ายปลอมตัว เลียนแบบ และกล่าวอ้างว่าเป็นบุคคลหรือหน่วยงานที่น่าเชื่อถือเพื่อหลอกลวงผู้ใช้งาน อาจจะเพื่อต้องการเงินหรือข้อมูลส่วนตัวสำคัญของเหยื่อได้ ตัวอย่างเทคนิคการหลอกลวงนี้ได้แก่ การสร้างเว็บไซต์หลอกลวง หรือฟิชชิง (Phishing) การโทรศัพท์หลอกลวง (Vishing) หรือการส่งอีเมลหลอกให้โอนเงิน (Business Email Compromise – BEC) เป็นต้น เนื่องจากการโจมตีด้วยเทคนิคเหล่านี้ทำได้ง่าย ได้ผลค่อนข้างเร็ว และ

อาศัยพื้นฐานการโจมตีไปที่ตัวบุคคล ด้วยการอ้างถึงผลประโยชน์ให้เหยื่อดีใจ หรือการข่มขู่ให้กลัว หรือตกใจจนขาดสติตรึกตรองใช้เหตุผล ดังนั้น ผู้ใช้งานจึงควรต้องมีสติและใช้ความตระหนักในการเปิดอ่านอีเมล รับโทรศัพท์ และเข้าถึงเว็บไซต์ต่างๆ ว่าอาจจะถูกหลอกลวงได้ตลอดเวลา หากไม่มั่นใจว่าผู้ที่ติดต่อมานั้นเป็นธนาคารหรือสถาบันการเงินจริงหรือไม่ ให้ทำการติดต่อสอบถามไปยังธนาคารหรือสถาบันการเงินแห่งนั้นโดยตรงแทน

3. **ระบบคลาวด์ (Cloud)** คือระบบที่ผู้ให้บริการจะแบ่งปันทรัพยากรให้แก่ผู้ต้องการใช้งานผ่านทางอินเทอร์เน็ต ซึ่งปัจจุบันองค์กรส่วนใหญ่เปลี่ยนมาใช้งานระบบคลาวด์มากขึ้น เนื่องจากความสะดวกสบายในการขอใช้บริการและสามารถลดค่าใช้จ่ายขององค์กรในการจัดซื้ออุปกรณ์ด้านคอมพิวเตอร์และระบบเครือข่าย หลายองค์กรใช้งานระบบคลาวด์เพื่อเก็บรักษาข้อมูลขององค์กร หรือนำข้อมูลไปประมวลผลเพื่อวัตถุประสงค์บางอย่าง ด้วยเหตุนี้เองทำให้ผู้ประสงค์ร้ายพยายามโจมตีระบบคลาวด์ต่างๆ เพื่อขโมยข้อมูลสำคัญ ดังนั้นผู้ให้บริการคลาวด์ควรใช้มาตรฐาน หรือหลักเกณฑ์ด้านความปลอดภัย และกลยุทธ์ในการลดความเสี่ยงต่อการถูกคุกคามจากโลกไซเบอร์ อีกทั้งองค์กรเองก็ต้องตรวจสอบและเฝ้าระวังการโจมตี นอกจากนี้ การดูแลด้านความปลอดภัยขององค์กรขึ้นอยู่กับบริการที่เลือกด้วย เช่น หากองค์กรใช้บริการ Software as a Service (SaaS) องค์กรต้องระมัดระวังข้อมูลที่เก็บในคลาวด์ และต้องติดตามข่าวสารด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบคลาวด์ที่รับบริการ เป็นต้น

4. **การขยายตัวของการใช้ Internet of Things (IoT)** ปัจจุบันหลายภาคส่วนจำนวนมากได้นำอุปกรณ์ IoT มาใช้ ด้วยความสามารถของอุปกรณ์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ ทำให้ผู้ใช้สามารถควบคุมอุปกรณ์เหล่านี้จากระยะไกล อย่างไรก็ตามระบบส่วนใหญ่ยังการขาดการออกแบบอย่างปลอดภัย ซึ่งเป็นสาเหตุหลักที่อุปกรณ์ IoT เหล่านี้มักถูกโจมตีได้ง่าย [8] จากรายงาน Global Risks Report 2018 ของ World Economic Forum กล่าวว่าในปี 2560 มีการใช้งานอุปกรณ์ IoT ประมาณ 8.4 พันล้านชิ้น (จำนวนประชากรทั้งโลก 7.6 พันล้านคน) และคาดการณ์ว่าจะมีการใช้อุปกรณ์ประมาณ 20.4 พันล้านชิ้นในปี 2563 ดังนั้นเมื่อมีการใช้งานอุปกรณ์จำนวนมากขึ้น สามารถก่อให้เกิดการโจมตีแบบ Distributed Denial of Service (DDoS) ได้อย่างง่ายดาย จากในอดีตก็เคยมีเหตุการณ์บ็อตเน็ต (Botnet) ชื่อ Mirai ซึ่งเป็นมัลแวร์ประเภทหนึ่งฝังตัวอยู่ในอุปกรณ์ IoT จากนั้นร่วมกันที่ส่งแพ็กเก็ตปริมาณมหาศาลจากอุปกรณ์เหล่านี้พร้อมกันเพื่อโจมตีแบบ DDoS และในอนาคตการโจมตีคล้ายกันนี้สามารถเกิดขึ้นได้อีก นอกจากนี้ หากมีการใช้งาน IoT บ่อยขึ้น ข้อมูลที่

ถูกเก็บในอุปกรณ์เองหรือระบบคลาวด์ที่เก็บข้อมูลก็อาจตกเป็นเป้าหมายของผู้ประสงค์ร้ายได้ อย่างไรก็ตามการป้องกันนั้นต้องเริ่มตั้งแต่กระบวนการผลิตอุปกรณ์ IoT จากโรงงาน ที่จำเป็นต้องเพิ่มความระมัดระวังในเรื่องของความปลอดภัยตั้งแต่เริ่มกระบวนการออกแบบ แทนที่จะเพิ่มในตอนหลัง รวมถึงผู้ใช้งานเองก็ควรศึกษาวิธีการติดตั้งและใช้งานอย่างปลอดภัย ตลอดจนการเฝ้าระวังภัยและติดตามข่าวสารเกี่ยวกับช่องโหว่ที่อาจเกิดจากอุปกรณ์เหล่านี้ด้วย

5. **ภัยคุกคามบนโทรศัพท์มือถือ (Mobile threats)** การใช้งานโทรศัพท์มือถือของคนไทยมีแนวโน้มเพิ่มสูงขึ้นทุกปี ทั้งในแง่ของการใช้เพื่อติดต่อสื่อสาร เพื่อความบันเทิง หรือเพื่อทำธุรกรรมทางการเงินผ่านอินเทอร์เน็ต จึงไม่น่าแปลกใจที่ในปัจจุบันผู้ประสงค์ร้ายใช้ช่องทางโทรศัพท์เป็นเป้าหมายสำคัญในการโจมตี จะเห็นได้จากมัลแวร์ในรูปแบบใหม่ๆ มีการพัฒนามาอย่างต่อเนื่อง โดยมุ่งเป้าหมายไปที่โทรศัพท์มือถือจำนวนหลายล้านเครื่องทั่วโลก เช่น การสร้างมัลแวร์ในลักษณะของแอปพลิเคชันและเผยแพร่บน Google Play Store นอกจากนี้ มัลแวร์บางตัวยังถูกสร้างมาเพื่อมุ่งหวังในการขโมยข้อมูลความลับทางการเงิน เช่น การขโมยรหัสผ่านในการเข้าใช้งาน mobile banking เป็นต้น ดังนั้น หากผู้ใช้งานขาดทักษะหรือความระมัดระวังด้านความปลอดภัยสารสนเทศ ก็อาจตกเป็นเหยื่อของผู้ประสงค์ร้ายได้ ผู้ใช้งานจึงควรมีความตระหนักถึงความปลอดภัยในการใช้โทรศัพท์มือถือ เช่น การตรวจสอบแอปพลิเคชันก่อนติดตั้งบนโทรศัพท์มือถือ และเลือกติดตั้งแอปพลิเคชันที่น่าเชื่อถือได้เท่านั้น เพื่อช่วยลดความเสี่ยงที่อาจเกิดจากภัยคุกคามประเภทนี้ได้

6. **ยุคทองของ Cryptocurrency** ในยุคที่มูลค่าของ cryptocurrency (อาทิเช่น บิตคอยน์) เพิ่มสูงขึ้นอย่างมาก นอกจากจะดึงดูดให้นักลงทุนมากมายเข้ามาทำการซื้อขายแล้ว ก็ยังจูงใจต่อผู้ประสงค์ร้ายในการขโมยเงินจากนักลงทุนด้วย โดยอาจผ่านการใช้วิธีขโมยเงินจากกระเป๋าเงินออนไลน์ (Wallet) หรือฝังมัลแวร์เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อเป็นเครื่องมือขุดเหมือง (Mining) ได้ ซึ่งผู้ประสงค์ร้ายจะทำการเจาะระบบเว็บไซต์และฝังสคริปส์เพื่อขุดเหมือง เมื่อเหยื่อเข้าถึงเว็บไซต์ดังกล่าวจะถูกติดตั้งสคริปส์ในการขุดเหมืองเพื่อหา cryptocurrency โดยอัตโนมัติ หรือในบางกรณีเหยื่อถูกผู้ประสงค์ร้ายพยายามโจมตีเพื่อขโมยเงินจากกระเป๋าเงินออนไลน์ (Wallet) รวมถึงโดนหลอกลวงให้ร่วมลงทุนในสกุลเงินที่ไม่มีอยู่จริง ดังนั้น ผู้ใช้ต้องทำการศึกษาการลงทุนและการใช้งานกระเป๋าเงินออนไลน์ให้ละเอียด ตั้งค่ารหัสผ่านที่ยากต่อการเข้าถึง เพื่อ

ป้องกันไม่ให้ถูกขโมยเงินจากกระเป๋าเงินออนไลน์ รวมถึงการป้องกันไม่ให้ผู้ประสงค์ร้ายฝังมัลแวร์ในเครื่องคอมพิวเตอร์ได้

7. **การใช้ปัญญาประดิษฐ์ (Artificial Intelligence - AI)** ท่ามกลางกระแสการโจมตีที่เปลี่ยนแปลงรูปแบบ วิธีการ อย่างรวดเร็ว ซับซ้อน และยากต่อการตรวจจับ ทำให้การตรวจสอบค้นหารูปแบบการโจมตีแบบเดิมๆ ไม่สามารถค้นหาการโจมตีรูปแบบใหม่ได้อย่างทันท่วงที หรือบางครั้งกว่าจะทราบก็เกิดความเสียหายเรียบร้อยแล้ว ทั้งนี้อาจจะด้วยสาเหตุการขาดเครื่องมือที่ทันสมัย ขาดบุคลากรที่มีทักษะเพียงพอ หรือเกิดการโจมตีที่ซับซ้อนมากก็เป็นได้ ดังนั้น การนำเทคโนโลยีปัญญาประดิษฐ์มาช่วยในการค้นหาและตรวจสอบการโจมตี ทำให้สามารถค้นหาตรวจสอบ หรือคาดการณ์การโจมตีที่อาจจะเกิดขึ้นในระบบเครือข่ายได้อย่างมีประสิทธิภาพ อีกทั้งยังเป็นการช่วยลดขั้นตอนกระบวนการทำงานและเพิ่มประสิทธิภาพในการทำงานอีกด้วย ถึงแม้ว่าการนำเทคโนโลยีนี้มาใช้จะยังไม่สามารถทดแทนเทคโนโลยีเดิมได้ในระยะเวลาอันสั้น แต่ในปี 2561 นี้น่าจะได้เห็นอุปกรณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่มาพร้อมกับปัญญาประดิษฐ์มากขึ้น

บทสรุป

จากแนวโน้มเทคโนโลยีและภัยคุกคามที่มีการพัฒนาอย่างรวดเร็ว เมื่อเทคโนโลยีมีความก้าวหน้ามากก็ยิ่งทำให้ความซับซ้อนของภัยคุกคามสูงขึ้นเป็นเงาตามตัว ดังนั้น จึงไม่รอให้เทคโนโลยีในการป้องกันถูกพัฒนาให้ทันกับแนวโน้มภัยคุกคามใหม่ๆ เท่านั้น แต่ผู้ให้บริการเองก็ต้องเตรียมการป้องกันด้วยวิธีอื่นๆ ให้ครอบคลุมและรัดกุมมากที่สุด ทางฝ่ายผู้ใช้เองนั้นก็ควรต้องทำการศึกษาให้เกิดความเข้าใจวิธีการใช้เทคโนโลยีสารสนเทศและประเมินความเสี่ยงที่จะอาจเกิดจากการนำเทคโนโลยีเหล่านั้นมาใช้งาน เทคนิคการโจมตีแม้ว่าอาจจะใช้วิธีเดิมๆ แต่มีแนวโน้มที่จะใช้หลากหลายเทคนิคร่วมกัน (multi-vector attack) ซึ่งจะยิ่งสร้างความซับซ้อนและป้องกันยากขึ้น การสร้างความร่วมมือและแบ่งปันข้อมูลเป็นแนวทางที่มีประสิทธิภาพที่นอกจากจะลดผลกระทบในวงกว้างแล้วยังเหมาะกับสถานการณ์ที่ทุกองค์กรขาดแคลนบุคคลากรด้านความมั่นคงปลอดภัยแต่การสร้างความร่วมมือกันนี้จะเป็นการสร้างความแข็งแกร่งในภาพรวมของภาคธุรกิจการธนาคารซึ่งก็จะเป็นส่วนที่สร้างเสริมความแข็งแกร่งด้านความมั่นคงปลอดภัยให้กับประเทศได้อีกด้วย

เอกสารอ้างอิง

1. Georg Schmitt, 24 Jan 2018, To Prevent a Digital Dark Age: World Economic Forum Launches Global Centre for Cybersecurity. World Economic Forum 2018, Retrieved from: https://www.weforum.org/press/2018/01/to-prevent-a-digital-dark-age-world-economic-forum-launches-global-centre-for-cybersecurity/
2. Amy Talbott, October 2, 2017, Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud. ZDNet 2018, Retrieved from: https://www.zdnet.com/article/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud/
3. สุชนนี, พรชัย, 3 เม.ย. 2561, PS_PT_002 ปริมาณการชำระเงินผ่านระบบการชำระเงินและช่องทางต่าง ๆ. ธนาคารแห่งประเทศไทย 2561. Retrieved from: http://www2.bot.or.th/statistics/BOTWEBSTAT.aspx?reportID=681&language=TH
4. ธนาคารแห่งประเทศไทย (2017) ธุรกรรมการชำระเงินผ่านบริการ Mobile banking และ Internet banking 1, Retrieved from: http://www2.bot.or.th/statistics/ReportPage.aspx?reportID=688
5. PwC. (2017). The Global State of Information Security® Survey 2018, Retrieved from: https://www.pwc.com/us/en/cybersecurity/information-security-survey.html

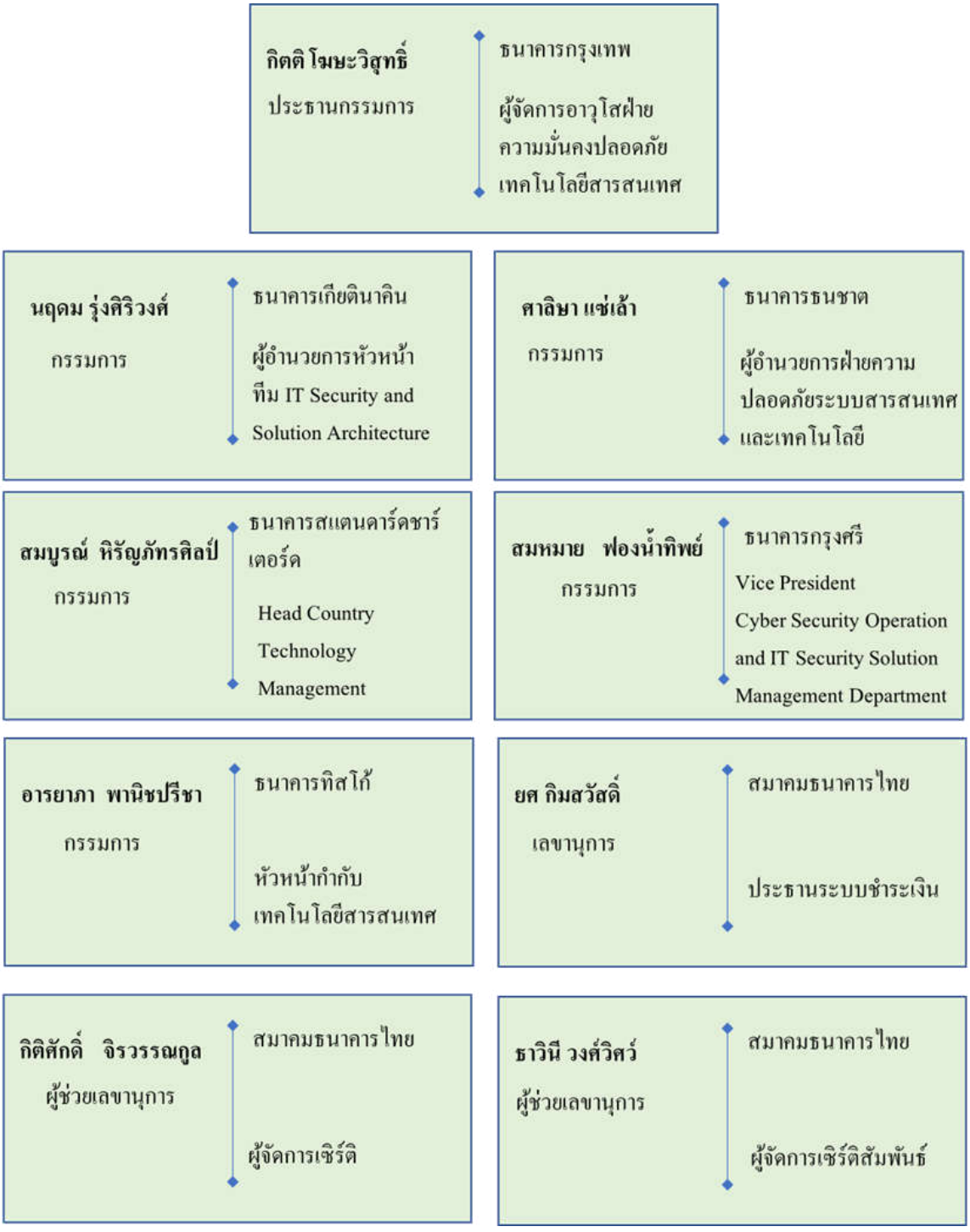
6. World Economic Forum. (2017). The Global Risks Report 2018, Retrieved from: https://www.weforum.org/reports/the-global-risks-report-2018
7. Gartner. (2017). Business Impact of Security Incidents and Evolving Regulations Driving Market Growth, , Retrieved from: https://www.gartner.com/newsroom/id/3784965
8. NTT Security. (2017). NTT Security 2018 Security Trends & Predictions, Retrieved from: https://www.nttsecurity.com/docs/librariesprovider3/default-document-library/gbl_trends_predictions_uea_v1.pdf
9. Nadeau M. (2017). Our top 7 cyber security predictions for 2018. *CSOOnline*, Retrieved from: https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

ภาคผนวก

รายชื่อคณะกรรมการTB-CERT

เอกสารเผยแพร่

รายชื่อคณะกรรมการ



TLP:WHITE

เผยแพร่วันที่ 6 ตุลาคม 2560

Business Email Compromise (BEC)

Business Email Compromise หรือ BEC คือภัยคุกคามที่มิจฉาชีพใช้การโจมตีด้วยอีเมลที่มีเนื้อหาในการหลอกลวงเชิงธุรกิจ โดยทำการยึดครองบัญชีอีเมลของผู้ใช้อีเมลบริษัท หรือสร้างอีเมลเลียนแบบ เพื่อใช้ปลอมตัวเป็นผู้ติดต่อธุรกิจ บุคคลที่มีตำแหน่งสูงของบริษัท หรือบุคคลที่เกี่ยวข้องกับการดำเนินการทางธุรกิจ และหลอกลวงเหยื่อที่ติดต่อธุรกิจให้หลงเชื่อและโอนเงินให้ในที่สุด

รูปแบบของ BEC

ใบแจ้งหนี้ปลอม (The Bogus Invoice Scheme)
มิจฉาชีพยึดบัญชีอีเมลและใช้อีเมลของพนักงานบริษัทเพื่อส่งใบแจ้งการชำระเงินหลอกลวงลูกค้าของบริษัทให้ชำระเงินไปยังบัญชีของมิจฉาชีพ

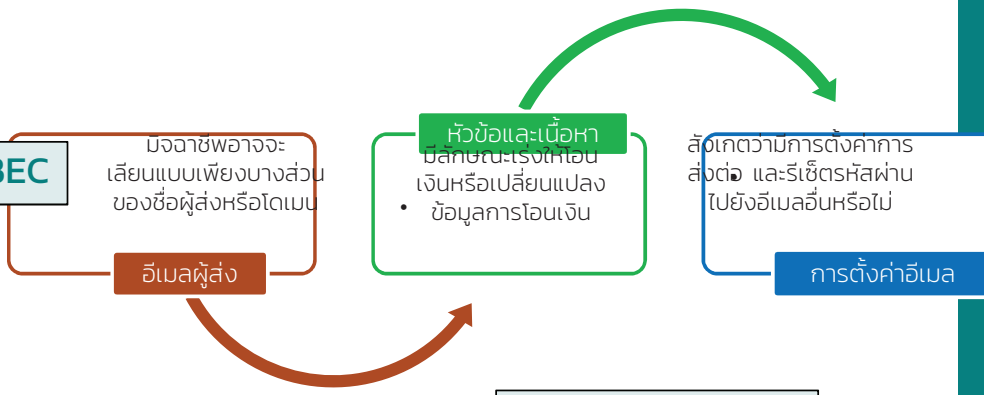
การฉ้อโกงด้วยชื่อผู้บริหาร (CEO Fraud)
มิจฉาชีพจะปลอมอีเมลเป็นผู้บริหาร หรือบุคคลที่มีหน้าที่สั่งชำระเงิน จากนั้นส่งอีเมลไปยังฝ่ายการเงินเพื่อแจ้งให้โอนเงินไปยังบัญชีของมิจฉาชีพ

การขโมยข้อมูล (Data theft)
มิจฉาชีพยึดครองบัญชีอีเมลและปลอมเป็นเจ้าหน้าที่ฝ่ายบุคคลส่งอีเมลเพื่อขอให้พนักงานแจ้งข้อมูลส่วนตัว จากนั้นมิจฉาชีพจะนำข้อมูลเหล่าไปทำธุรกรรมอื่นต่อไป

การยึดครองบัญชี (Account Compromise)
มิจฉาชีพยึดครองบัญชีอีเมลของพนักงานและส่งอีเมลไปยังบริษัทผู้ขาย (vendors) จำนวนมากเพื่อขอใบแจ้งชำระเงิน จากนั้นมิจฉาชีพก็นำใบแจ้งชำระเงินนี้ไปเรียกเก็บเงินจากบริษัท โดยให้โอนเงินผ่านบัญชีของมิจฉาชีพ

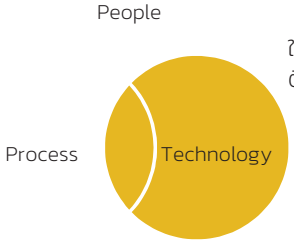
การปลอมเป็นอัยการ (Attorney Impersonation)
มิจฉาชีพจะส่งอีเมลไปยังพนักงานหรือผู้บริหารของบริษัท โดยหลอกลวงว่าเป็นทนายความและอ้างว่าต้องจัดการกับเรื่องที่มีความสำคัญสูงมากและใช้เรื่องของเวลามากดดันให้เหยื่อต้องรีบโอนเงินให้

วิธีการสังเกต BEC



วิธีการป้องกัน

จัดอบรมสร้างความตระหนักด้านการรักษาความปลอดภัยสารสนเทศให้พนักงาน



ใช้อีเมลที่เป็น**โดเมนของบริษัท**ในการติดต่อธุรกิจ แทนการใช้อีเมลฟรีทั่วไป

ก่อนโอนเงินทุกครั้ง ต้อง**ยืนยันตัวตน**ของผู้รับเงินผ่านช่องทางอื่นด้วย

ตั้ง**รหัสผ่าน**ที่มีความปลอดภัยเพียงพอ และควรใช้**ระบบการยืนยันตัวหลายปัจจัย** (multi-factors authentication)

ถ้าสงสัยว่าตัวเองตกเป็นเหยื่อมิจฉาชีพให้รีบ**แจ้งตำรวจ**หรือหน่วยงานที่เกี่ยวข้อง

ใช้**ลายมือชื่อดิจิทัล** (Digital Signature) ในอีเมลเพื่อให้ผู้รับอีเมลสามารถตรวจสอบได้ว่าเป็นอีเมลของผู้ส่งอีเมลจริง

หากได้รับอีเมลที่มีลักษณะขอเปลี่ยนแปลงข้อมูลผู้รับโอนเงิน ให้ตรวจสอบข้อมูลผ่าน**ช่องทางอื่น**อย่างเร่งด่วน

นึกถึง Cyber Security ด้านการธนาคาร นึกถึง TB-CERT Thailand Banking Sector CERT

ช่องโหว่ WPA/WPA2 KEY REINSTALLATION ATTACK

TLP:WHITE

เผยแพร่วันที่ 29 ตุลาคม 2560

KRACK ย่อมาจาก **Key Reinstallation AttaCK** เป็นการโจมตีที่ช่องโหว่บนโปรโตคอล WiFi Protected Access (WPA และ WPA2) โดยผู้โจมตีใช้ช่องโหว่ของ WPA และ WPA2 ในช่วงที่เครื่องของเหยื่อกำลังเชื่อมต่อไปยัง Access Point (AP) ซึ่งจะมีการส่งกุญแจในการเชื่อมต่อไปให้ AP การโจมตีนี้จะส่งผลให้เครื่องของเหยื่อทำการส่งกุญแจในการเชื่อมต่อออกมาซ้ำ จากนั้นผู้โจมตีจะนำไปคำนวณหากุญแจเข้ารหัสที่ใช้ระหว่างเครื่องของเหยื่อกับ AP และทำให้สามารถขโมยเซสชั่น (Session) ของการเชื่อมต่อนั้นและส่งมัลแวร์เข้าไปที่เครื่องของเหยื่อหรือขโมยข้อมูลที่เหยื่อส่งผ่าน WiFi ได้

แนวทางการป้องกันการโจมตีนี้คือการติดตั้งแพทช์ (Patch) แต่ในปัจจุบัน Patch ที่สามารถปิดช่องโหว่โดยไม่ให้มีการส่งกุญแจในการเชื่อมต่อออกมาซ้ำนั้น ในบางอุปกรณ์ยังออกมาไม่ครบ จึงต้องติดตามและต้องติดตั้ง Patch ทันทีที่มีประกาศ Patch ออกมา

อุปกรณ์ที่ได้รับผลกระทบ

อุปกรณ์ที่สามารถเชื่อมต่อเครือข่ายไร้สายทุกชนิดที่ใช้ WPA และ WPA2 ไม่ว่าจะเป็นระบบปฏิบัติการ Android Linux Apple Windows OpenBSD และอุปกรณ์ IoT อื่น ๆ รวมทั้ง Access Point ที่เปิดใช้ IEEE802.11r สำหรับการขยายขอบเขตของสัญญาณ WiFi ระหว่าง AP ด้วยกัน ผู้ใช้งานจะสามารถตรวจสอบข้อมูลอุปกรณ์ที่ได้รับผลกระทบได้จากฐานข้อมูลของ CERT/CC (เอกสารอ้างอิง 3)

ข้อสังเกต

- การโจมตีนี้ไม่ได้เป็นการขโมยรหัส WiFi
- อัลกอลิทึมการเข้ารหัสของ WPA และ WPA2 ไม่ได้มีช่องโหว่
- คนร้ายต้องอยู่ภายในระยะของสัญญาณระหว่างเหยื่อและ AP จึงจะสามารถแทรกสัญญาณ WiFi เพื่อการโจมตีช่องโหว่ของ WPA และ WPA2 ดังกล่าว
- วิธีการโจมตีนี้สามารถทำได้กับการเชื่อมต่อระหว่าง AP กับ AP ผ่านโปรโตคอล IEEE802.11r ที่ใช้ในการขยายขอบเขตของสัญญาณ WiFi ระหว่าง AP

ข้อแนะนำ

ผู้ดูแลโครงสร้างพื้นฐาน WiFi ขององค์กร

- ตรวจสอบ Patch ของอุปกรณ์ AP ที่ใช้งานและติดตั้ง Patch ทันทีที่มีประกาศแจ้ง Patch
- หากยังไม่มี patch เพื่อปิดช่องโหว่นี้ ให้พิจารณาปิด IEEE802.11r หากไม่ได้ใช้งาน หรือ เฝ้าระวัง Rogue AP อย่างเข้มงวดเพื่อพื้นที่การใช้งาน WiFi ขององค์กรมีความปลอดภัยจากช่องโหว่ดังกล่าว
- ให้คำแนะนำกับผู้ใช้งานขององค์กรเรื่องช่องโหว่และการลง patch

ผู้ใช้งาน WiFi

- ตรวจสอบ Patch ของอุปกรณ์ที่ใช้งาน และต้องติดตั้ง Patch ทันทีที่มีประกาศแจ้ง
- ไม่ควรใช้ WiFi สาธารณะให้การทำธุรกรรมออนไลน์ หากยังไม่ได้ลง Patch ป้องกันช่องโหว่ KRACK
- ปิดการใช้งาน WiFi เมื่อไม่ได้ใช้งาน
- ติดตามข่าวสารเรื่อง WPA2 KRACK

คำถามที่มักพบบ่อย

1. การเปลี่ยนรหัสผ่าน WiFi ที่ AP จะช่วยลดความเสี่ยงได้หรือไม่
ตอบ การเปลี่ยนรหัสผ่าน WiFi ไม่ได้ช่วยปิดความเสี่ยงนี้ เนื่องจากการโจมตี KRACK ไม่ได้ขโมยรหัสผ่าน

2. หากอุปกรณ์ที่ใช้งานยังไม่ได้มีการติดตั้ง Patch ควรจะทำธุรกรรมออนไลน์ผ่านเครือข่าย WiFi หรือไม่
ตอบ หลีกเลี่ยงการทำธุรกรรมออนไลน์การผ่านเครือข่าย WiFi ในที่สาธารณะ หรือพิจารณาใช้เครือข่าย 3G/4G แทน

3. จะรู้ได้อย่างไรว่ากำลังเป็นเหยื่อ
ตอบ การโจมตีช่องโหว่นี้ทำที่ระดับโปรโตคอล ผู้ใช้งานจะไม่สามารถทราบได้เลยว่ากำลังถูกโจมตี แต่หากใช้งานผ่าน VPN หรือ บริการออนไลน์ที่ใช้ https:// โดยต้องสังเกตว่าจะไม่เปลี่ยนลดลงมาเป็น http:// จะปลอดภัยจากการโจมตีด้วยวิธีนี้

4. เราควรจะยังใช้ WPA2 ต่อไปหรือไม่
ตอบ หากลง Patch สำหรับช่องโหว่นี้แล้ว WPA2 ยังคงเป็นโปรโตคอลที่ปลอดภัยในการใช้งาน

เอกสารอ้างอิง

1. https://www.krackattacks.com/
2. http://www.securityfocus.com/bid/101274
3. https://www.kb.cert.org/vuls/byvendor?searchview&Query=FIELD+Reference=228519
4. https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-13077
5. https://thehackernews.com/2017/10/wpa2-krack-wifi-hacking.html
6. http://www.kb.cert.org/vuls/id/228519
7. http://www.revolutionwifi.net/revolutionwifi/2017/10/wpa2-krack-vulnerability-getting-information
8. http://www.idownloadblog.com/2017/10/18/krack-attack-faq/

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

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT
Thailand Banking Sector 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

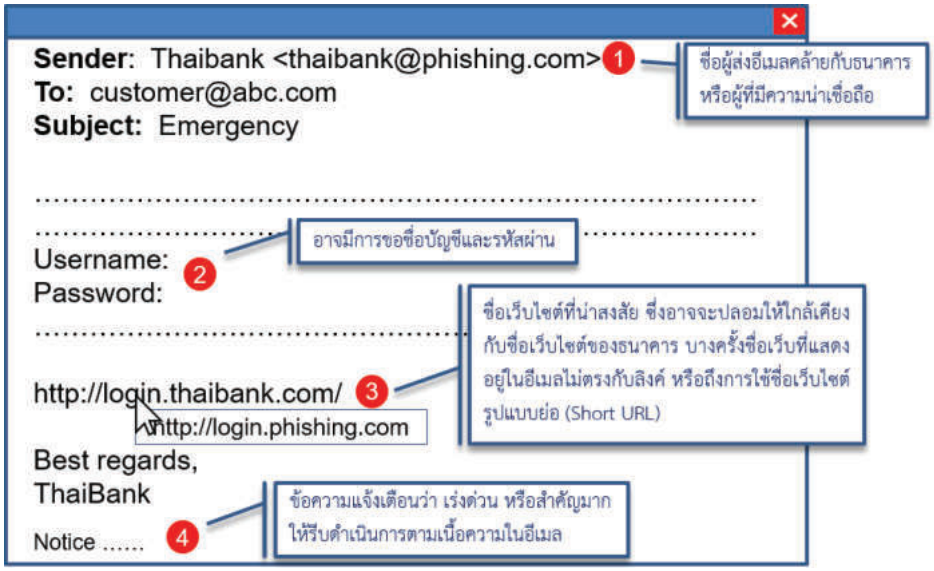
TLP: WHITE

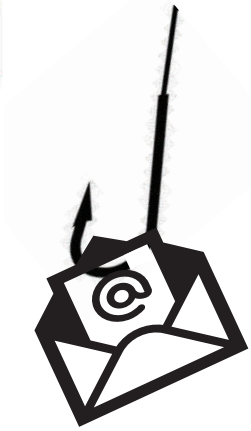
ฟิชชิง (PHISHING)

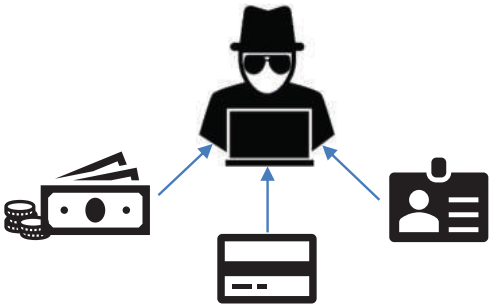
ฟิชชิง (Phishing) เป็นเทคนิคการหลอกลวงทางอินเทอร์เน็ตประเภทหนึ่ง ซึ่งมักจะมาในรูปแบบของการปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้น เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต และหมายเลขบัตรประจำตัวประชาชน เป็นต้น

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

"THE EFFECTIVENESS OF CYBER RESILIENCE DEPENDS ON THE PREPARATION"

The Thai Bankers' Association

5/13 Chaeng Watthana Rd, Pak Kret District, Nonthaburi 11120