InterRisk Thai Report <2022 No.01>

อาชญากรรมทางไซเบอร์ในประเทศไทย

[สรุป]

- ในปีพ.ศ. 2564 มีผู้ใช้งานภายในประเทศไทยถูกโจมตีทางไซเบอร์ 21% ซึ่งต่ำกว่าค่าเฉลี่ยทั่วโลกที่อยู่ที่ 29%
- มูลค่าความเสียหายเฉลี่ยของอาชญากรรมทางไซเบอร์ในปีพ.ศ. 2564 เพิ่มขึ้นถึง 144% หรือ 2.2 ล้านดอลลาร์สหรัฐ หรือประมาณ 72.6 ล้านบาท
- บริษัทสาขาย่อยถูกใช้เป็นสื่อกลางในการบุกรุกไปยังระบบของบริษัทสำนักงานใหญ่
- การฝึกอบรมอย่างสม่ำเสมอโดยผู้เชี่ยวชาญเพื่อเสริมสร้างทักษะการสื่อสารที่รวดเร็วสำหรับการเตรียมพร้อมรับมือกรณีเกิดเหตุฉุกเฉินนั้นเป็นสิ่งที่สำคัญ

อาชญากรรมทางไซเบอร์เป็นอาชญากรรมที่เกี่ยวข้องกับคอมพิวเตอร์และเครือข่ายโดยมีจุดประสงค์ที่ผิดกฎหมาย เช่น การฉ้อโกง การขโมยข้อมูลยืนยันตัวตน หรือการละเมิดความเป็นส่วนตัว ไวรัสคอมพิวเตอร์เองก็เป็นหนึ่งในอาชญากรรมทางไซเบอร์ และอาจเป็นอาชญากรรมประเภทแรกผู้ใช้งานคอมพิวเตอร์หรืออินเทอร์เน็ตรู้จัก ไวรัสนั้นแพร่ระบาดในระบบคอมพิวเตอร์ สร้างความเสียหายให้กับไฟล์ ทำให้ระบบการทำงานโดยรวมของคอมพิวเตอร์ผิดปกติ และสามารถจำลองตัวเองไปยังอุปกรณ์และระบบอื่น ๆ ได้ ไวรัสจัดเป็นมัลแวร์รูปแบบหนึ่ง ซึ่งครอบคลุมซอฟต์แวร์ที่เป็นอันตรายทุกประเภท รวมถึงรหัสหรือโปรแกรมต่าง ๆ ที่ถูกสร้างขึ้นมาด้วยจุดประสงค์เพื่อกระจายและสร้างความเสียหาย ขโมยข้อมูล และสร้างรายได้ให้กับเจ้าของไวรัส นอกจากนี้ยังมีแรนซัมแวร์ซึ่งสามารถล็อคไฟล์ของเป้าหมายได้ จนกว่าเป้าหมายจะจ่ายค่าไถ่เพื่อแลกกับการปลดล็อคไฟล์ดังกล่าว

อาชญากรรมทางไซเบอร์เป็นปัญหาที่พบได้ในสังคมปัจจุบันเนื่องจากเทคโนโลยีมีการก้าวหน้าอยู่ตลอดเวลา ทว่ามาตรการด้านความปลอดภัยสำหรับการปกป้องเทคโนโลยีและผู้ใช้งานไม่สามารถพัฒนาตามความก้าวหน้าดังกล่าวได้ทัน จึงส่งผลให้อาชญากรรมทางไซเบอร์เกิดขึ้นอยู่บ่อยครั้ง

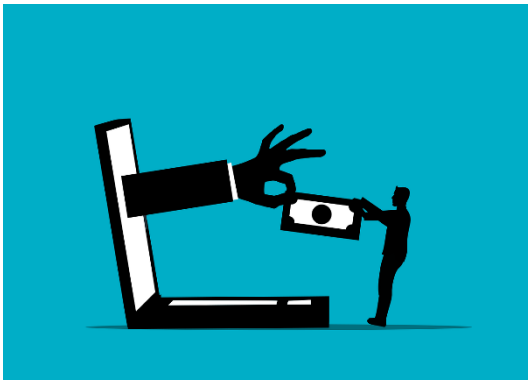
หน่วยงาน Cybersecurity Ventures ที่รวบรวมนักวิจัยชั้นนำของโลกคาดการณ์ว่าอาชญากรรมทางไซเบอร์จะเพิ่มขึ้น 15% ต่อปีในช่วง 5 ปีข้างหน้า และมีมูลค่าความเสียหายสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐต่อปี ภายในปีพ.ศ. 2568 เพิ่มขึ้นจาก 3 ล้านล้านดอลลาร์สหรัฐในปีพ.ศ. 2558 ซึ่งจัดว่าเป็นการเปลี่ยนแปลงทางเศรษฐกิจครั้งใหญ่ที่สุดในประวัติศาสตร์ที่มีมูลค่ามากกว่าความเสียหายที่เกิดจากภัยธรรมชาติในหนึ่งปีเป็นทวีคูณ

สถานการณ์อาชญากรรมทางไซเบอร์ในประเทศไทยเป็นอย่างไร ขอเชิญท่านมาหาข้อมูลที่น่าสนใจในจดหมายข่าวฉบับนี้

โดยในประเทศไทย เหตุอาชญากรรมทางไซเบอร์แบ่งออกเป็น 9 ประเภท ดังตารางด้านล่าง

ตารางที่ 1 ประเภทของอาชญากรรมทางไซเบอร์ในประเทศไทย

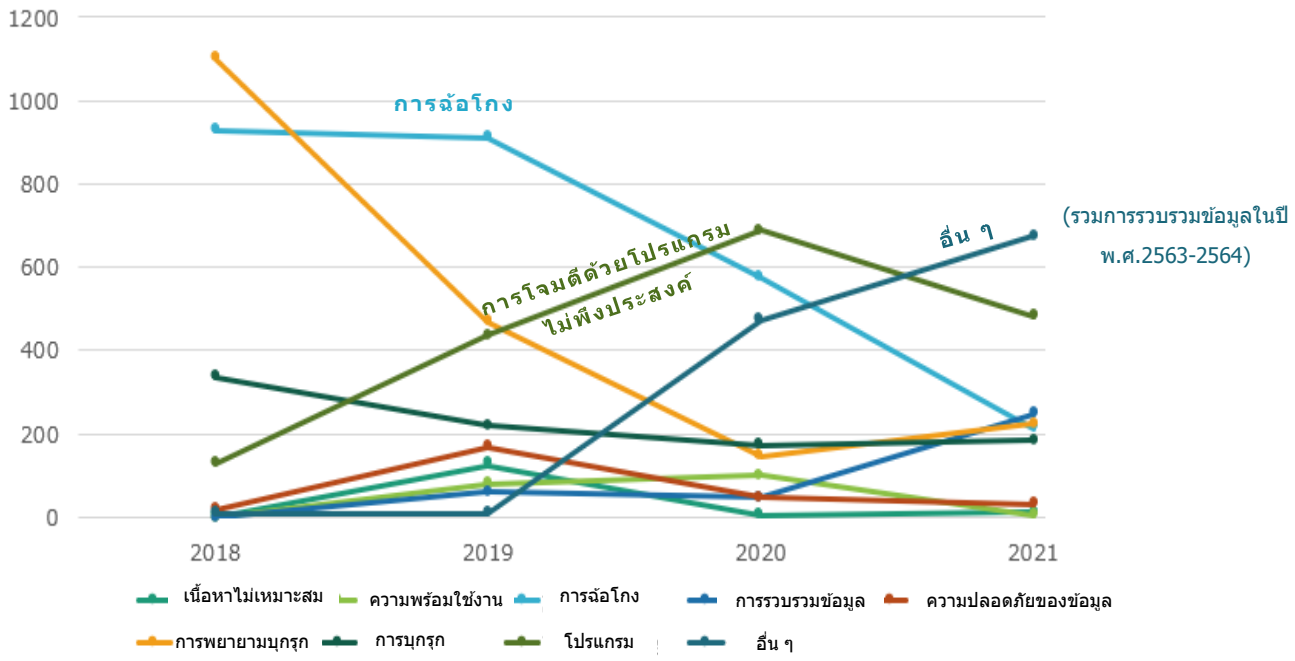
ประเภท	คำอธิบาย
1. เนื้อหาที่ไม่เหมาะสม	ภัยคุกคามที่เกิดจากการใช้และเผยแพร่เนื้อหาที่ไม่เหมาะสมเพื่อสร้างความเสียหายต่อความน่าเชื่อถือของบุคคลหรือองค์กรโดยมีจุดประสงค์เพื่อก่อให้เกิดความขัดแย้ง หรือข้อมูลที่ผิดกฎหมาย เช่น ภาพลามกอนาจาร การหมิ่นประมาท และการโฆษณาผลิตภัณฑ์ต่าง ๆ ทางอีเมลโดยที่ไม่คำนึงถึงความต้องการ เจตนาของผู้รับ (SPAM)
2. ความพร้อมใช้งานของระบบ	ภัยคุกคามที่เกิดจากการโจมตีระบบ ทำให้ระบบไม่สามารถใช้งานได้ตามปกติ ส่งผลต่อการตอบสนองการบริการ หรือนำไปสู่ความล้มเหลวของระบบ ภัยคุกคามดังกล่าวนี้อาจเกิดขึ้นจากการโจมตีระบบบริการโดยตรง เช่น การโจมตี DOS (Denial of Service) การโจมตีโครงสร้างพื้นฐานที่สนับสนุนระบบบริการ เช่น อาคาร ระบบไฟฟ้า และระบบปรับอากาศ เป็นต้น
3. การฉ้อโกง	ภัยคุกคามที่เกิดจากการหลอกลวง ฉ้อโกงที่พบเห็นได้ในหลายกรณี ไม่ว่าจะเป็น การใช้ข้อมูลหรือระบบเพื่อผลประโยชน์ส่วนตนโดยไม่ได้รับอนุญาต การปลอมแปลงหน้าเว็บไซต์ (Phishing) ที่สามารถขโมยรหัสผ่านของผู้ใช้งานได้ หรือใช้ในการจำหน่ายผลิตภัณฑ์ ซอฟต์แวร์ที่ขัดต่อกฎหมายลิขสิทธิ์
4. การรวบรวมข้อมูล	ภัยคุกคามที่เกิดจากการพยายามรวบรวมข้อมูลเกี่ยวกับช่องโหว่โดยฝ่ายผู้โจมตี (Scanning) ผ่านการบริการที่มีการใช้งานอยู่ภายในระบบ เช่น ข้อมูลระบบปฏิบัติการ ข้อมูลซอฟต์แวร์ที่มีการติดตั้ง ข้อมูลบัญชี ฯลฯ นอกจากนี้ยังรวมถึงการรวบรวมตรวจสอบการส่งผ่านข้อมูลภายในเครือข่าย (Sniffing) เพื่อล่อลวงผู้ใช้งานให้เปิดเผยข้อมูลภายในระบบ
5. ความปลอดภัยของข้อมูล	ภัยคุกคามที่เกิดจากการเข้าถึงข้อมูลละเอียดอ่อน หรือการแก้ไข ดัดแปลงข้อมูลโดยไม่ได้รับอนุญาต
6. การพยายามบุกรุก	ภัยคุกคามที่เกิดจากการพยายามบุกรุก ทั้งผ่านข้อมูลช่องโหว่ทั่วไป (Common Vulnerabilities and Exposures : CVE) หรือผ่านข้อมูลช่องโหว่พิเศษ ภัยคุกคามดังกล่าวนี้ยังรวมถึงการพยายามแฮ็คระบบ การคาดเดาวิธีการยืนยันตัวตนเพื่อเขาถึงบัญชีผู้ใช้ ชื่อผู้ใช้และรหัสผ่าน หรือการทดลองรหัสผ่านทุกรูปแบบเพื่อเข้าถึงระบบโดยที่ไม่ได้รับอนุญาต (Brute Force)
7. การบุกรุก	ภัยคุกคามอันเนื่องมาจากการที่ระบบถูกบุกรุกได้สำเร็จ ส่งผลให้ระบบถูกควบคุมโดยบุคคลที่ไม่ได้รับอนุญาต
8. การโจมตีด้วยโปรแกรมไม่พึงประสงค์	ภัยคุกคามที่เกิดจากโปรแกรม หรือซอฟต์แวร์ที่นำไปสู่ผลลัพธ์ที่ไม่พึงประสงค์ต่อผู้ใช้งานหรือระบบ (Malicious Code) เช่น ทำให้ระบบทำงานผิดปกติ สร้างความเสียหายต่อระบบ เป็นต้น โดยทั่วไปแล้วผู้ใช้งานจำเป็นต้องเปิดใช้งานโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์เหล่านี้ก่อน จากนั้นตัวโปรแกรมจึงจะทำการติดตั้งตัวเอง และทำงานในลักษณะคล้ายคลึงกับไวรัส เวิร์ม ม้าโทรจัน หรือสปายแวร์
9. อื่น ๆ	ภัยคุกคามนอกเหนือจากประเภทที่ได้กล่าวมา เป็นภัยคุกคามที่ถูกจัดว่าเป็นภัยคุกคามรูปแบบใหม่ หรือไม่สามารถระบุประเภทได้ โดยหากจำนวนกรณีของภัยคุกคามทางไซเบอร์ประเภทนี้มีจำนวนมากกว่าภัยคุกคามที่ได้กล่าวไว้ข้างต้น อาจจำเป็นต้องทำการแก้ไขตารางประเภทภัยคุกคามนี้อีกครั้งเพื่อความทันสมัยของข้อมูล



ข้อมูลสถิติประวัติศาสตร์อาชญากรรมทางไซเบอร์ในประเทศไทยตั้งแต่ปีพ.ศ. 2561 มีแนวโน้มลดลง ทว่าจำนวนกรณียังคงสูง โดยมูลค่าความเสียหายเฉลี่ยของอาชญากรรมทางไซเบอร์ในปีพ.ศ. 2564 เพิ่มขึ้นถึง 144% หรือ 2.2 ล้านดอลลาร์สหรัฐ (ประมาณ 72.6 ล้านบาท) อุตสาหกรรมที่ได้รับผลกระทบมากที่สุด ได้แก่ บริการด้านกฎหมาย การก่อสร้าง การขายส่งและขายปลีก ระบบสาธารณสุข และนิคมอุตสาหกรรม นอกจากนี้ประเทศไทยยังอยู่ในอันดับที่ 6 ของประเทศแถบเอเชียแปซิฟิก โดยมีประเทศญี่ปุ่นที่ได้รับผลกระทบจากแรนซัมแวร์มากที่สุด

จากแบบสอบถามของบริษัทไซเบอร์ในหลายประเทศ พบว่าผู้ใช้งานในประเทศไทยถูกโจมตีโดยอาชญากรทางไซเบอร์ประมาณ 21% ในปี 2564 ต่ำกว่าค่าเฉลี่ยทั่วโลกซึ่งอยู่ที่ 29%

ในช่วง 4 ปีที่ผ่านมา มีจำนวนเหตุอาชญากรรมทางไซเบอร์อยู่ที่ 2,250 กรณี (ปีพ.ศ. 2561) 2,470 กรณี (ปีพ.ศ. 2562) 2,250 กรณี (ปีพ.ศ. 2563) และ 2,069 กรณี (ปีพ.ศ. 2564) ซึ่งจัดว่าไม่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ อย่างไรก็ตาม เหตุอาชญากรรมทางไซเบอร์ประเภทการบุกรุกลดลงในขณะที่การโจมตีด้วยโปรแกรมไม่พึงประสงค์และภัยคุกคามอื่น ๆ (เช่น การรวบรวมข้อมูล) เพิ่มมากขึ้นดังแผนภาพดังต่อไปนี้



แผนภาพที่ 1 จำนวนกรณีของเหตุอาชญากรรมทางไซเบอร์ในประเทศไทย

ตารางที่ 2 ตัวอย่างอาชญากรรมทางไซเบอร์ครั้งใหญ่ในประเทศไทย

วันที่เกิดเหตุ	ประเภทธุรกิจ	รายละเอียด
ส.ค. 2559	ธนาคาร	ตู้ ATM ติดมัลแวร์และถูกขโมยเงินรวมมูลค่ากว่า 12 ล้านบาท โดยอาชญากรได้ทำการถอนเงินครั้งละ 40,000 บาท จากตู้ ATM 21 ตู้ กว่า 300 ครั้ง
ก.ค. 2560	ธนาคาร	ชื่อของบริษัทที่ใช้บริการออกหนังสือค้ำประกันแบบออนไลน์ได้รั่วไหลออกไปเป็นจำนวน 3,000 ราย นอกจากนี้ยังมีกรณีของธนาคารรายอื่น คือ ข้อมูลบัญชี 120,000 รายได้รั่วไหลออกไปผ่านการยื่นเรื่องออนไลน์สำหรับสินเชื่อขนาดเล็ก เช่น สินเชื่อที่อยู่อาศัย และสินเชื่อส่วนบุคคล
มี.ค. 2561	บริษัทโทรคมนาคม	ข้อมูลลูกค้า 11,400 รายรั่วไหลจากบริษัทโทรคมนาคมรายใหญ่
พ.ค. 2563	บริษัทโทรคมนาคม	บันทึกการใช้อินเทอร์เน็ตมากกว่า 8 พันล้านรายการรั่วไหลจากบริษัทโทรคมนาคมรายใหญ่ที่สุดของประเทศไทย ทางบริษัทอธิบายว่า "รายการบันทึกที่รั่วไหลมีไว้เพื่อแสดงภาพรวมการใช้อินเทอร์เน็ตเพียงเท่านั้น ไม่ได้มีการแสดงข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับของลูกค้าแต่อย่างใด"
ก.ย. 2563	โรงพยาบาล	แฮคเกอร์โจมตีระบบของโรงพยาบาลด้วยแรนซัมแวร์ ส่งผลให้ระบบทั้งหมดใช้งานไม่ได้ สร้างความเสียหายแก่บริการทางการแพทย์ โดยฝั่งอาชญากรได้เรียกร้องเงินเป็นจำนวน 200,000 Bitcoins (ประมาณ 63 พันล้านบาท)
พ.ค. 2564	บริษัทประกัน	กลุ่มประกันภัยรายใหญ่ได้รับความเสียหายจากการโจมตีทางไซเบอร์โดยกลุ่มแฮ็กเกอร์ "Avaddon" ข้อมูลขนาด 3TB ได้แก่ รายงานทางการแพทย์ของลูกค้า (ข้อมูลละเอียดอ่อน) เอกสารสแกนบัญชีธนาคาร และบัตรประจำตัวประชาชนได้รั่วไหลออกไป

หลักการของมาตรการความปลอดภัยทางไซเบอร์

เนื่องจากในบริษัทสาขาต่างประเทศ รวมถึงประเทศไทยนั้นเมื่อเปรียบเทียบกับสำนักงานใหญ่แล้วมีทรัพยากร (บุคลากร, เวลา และงบประมาณ) ที่ค่อนข้างจำกัด ทำให้ระดับความปลอดภัยของบริษัทสาขาต่างประเทศมีแนวโน้มที่จะต่ำกว่าสำนักงานใหญ่ ซึ่งฝั่งผู้โจมตีทราบถึงสถานการณ์ดังกล่าวนี้อยู่แล้ว จึงส่งผลให้เกิดกรณีที่มีการบุกรุกมายังระบบของบริษัทสาขาต่างประเทศ เพื่อใช้เป็นขั้นบันไดสำหรับบุกรุกไปยังระบบของสำนักงานใหญ่

การโจมตีทางไซเบอร์นั้นมีวิธีการที่หลากหลายมากขึ้นในช่วงหลายปีที่ผ่านมา ทำให้จำเป็นต้องมีความยืดหยุ่นเป็นอย่างมากในการรับมือ และแม้ว่าจะทราบรายละเอียดของมาตรการรับมืออยู่ก่อนแล้วก็ไม่สามารถรับรองได้ว่าจะสามารถรับมือได้อย่างเหมาะสม จึงส่งผลให้การรับมือหลังเกิดเหตุโดยไม่พึ่งองค์กรหรือผู้เชี่ยวชาญจากภายนอกนั้นเป็นไปได้ยาก ดังนั้นการแบ่งหน้าที่ความรับผิดชอบกับสำนักงานใหญ่และผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จากภายนอกให้ชัดเจนจึงมีความสำคัญเป็นอย่างมาก ซึ่งในบทความนี้จะขอแนะนำให้ท่านทำการฝึกซ้อมรับมืออย่างสม่ำเสมอ โดยจัดเตรียมมาตรการรับมือที่เริ่มตั้งแต่กระบวนการ “การตรวจพบความผิดปกติ” จนถึง “การรับมือขั้นต้น” ผ่านสถานการณ์จำลองที่ชัดเจนดังตัวอย่างด้านล่าง

ตั้งแต่การตรวจพบจนถึงการรับมือขั้นต้น

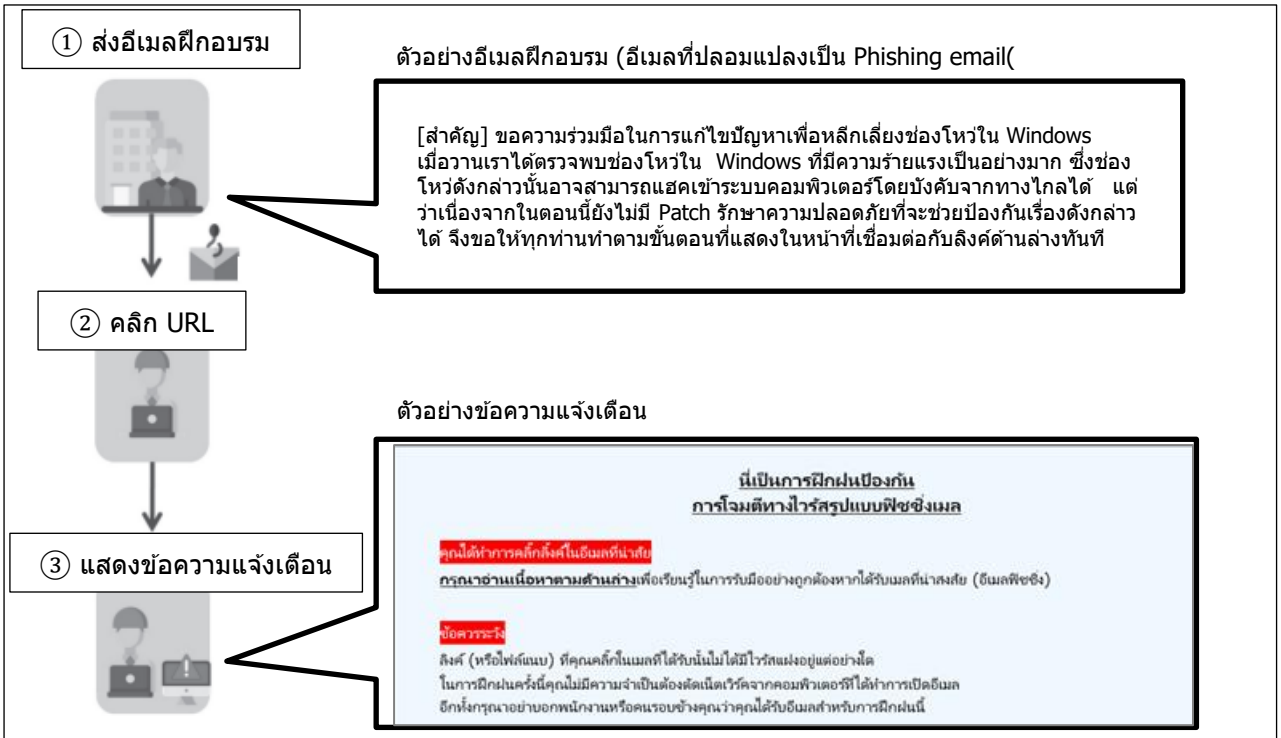
“ท่านสังเกตเห็นหรือไม่” (การตรวจพบความผิดปกติ)	ท่านสามารถสังเกตและทราบถึงการโจมตีทางไซเบอร์ได้อย่างรวดเร็ว และลดความเสียหายให้เหลือน้อยที่สุดได้หรือไม่ (มีการจัดการฝึกอบรมและให้ข้อมูลแก่พนักงานตั้งแต่ในช่วงเวลาปกติ และบันทึกผลในรูปแบบเอกสารให้ชัดเจน)
“ท่านสามารถรายงานและเริ่มเคลื่อนไหวได้ด้วยตัวเองหรือไม่” (การรับมือขั้นต้น)	การแบ่งปันข้อมูลทั้งหมด • ผู้พบเหตุคนแรกจำเป็นต้องปรึกษา หรือรายงานแก่ใคร *กำหนดการรับมือพื้นฐานโดยอ้างอิงจากอะไร • ใครเป็นผู้ตัดสินว่าสถานการณ์ดังกล่าวเป็นเหตุโจมตีทางไซเบอร์ (หรือมีความเป็นไปได้ว่าจะเป็นเหตุโจมตีทางไซเบอร์) และหลังจากนั้นได้รับผิดชอบในการจัดเตรียมมาตรการรับมือหรือไม่

	• จำเป็นต้องรายการแก่ผู้กำกับดูแลหรือไม่ *มีบทลงโทษหรือไม่ หากไม่มีการรายงาน การรายงานไปยังสำนักงานใหญ่ • กระบวนการรายงานไปยังสำนักงานใหญ่และข้อมูลติดต่อในการรายงานมีความชัดเจนหรือไม่ *หากได้รับการยืนยันว่าติดมัลแวร์ ข้อมูลรั่วไหล ให้ทำการรายงานไปยังสำนักงานใหญ่อย่างรวดเร็ว (โดยเฉพาะกรณีที่ระบบเครือข่ายเชื่อมต่อกับสำนักงานใหญ่ ความเสียหายอาจเพิ่มมากขึ้น และแพร่กระจายไปยังสำนักงานใหญ่ได้) การยับยั้ง การตรวจสอบหาสาเหตุ และการวิเคราะห์ • ข้อมูลติดต่อของผู้รับผิดชอบแผนก ผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จากภายนอก ระบบการประสานงาน และการแบ่งหน้าที่ความรับผิดชอบมีความชัดเจนหรือไม่ *เนื่องจากบริษัททท่านหรือสำนักงานใหญ่อาจตัดสินใจ หรือดำเนินการรับมือได้ยากในหลาย ๆ ด้าน การติดต่อประสานงานกับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จากภายนอกจึงมีความสำคัญเป็นอย่างยิ่ง โดยเฉพาะอย่างยิ่งในกระบวนการรับมือขั้นต้น

การสนับสนุนด้านการฟื้นฟูระบบผ่านประกันภัยและบริการเสริม

ในส่วนนี้จะกล่าวถึงการประกันความเสี่ยงภัยด้านความปลอดภัยไซเบอร์ ในกรณีที่เกิดเหตุทางไซเบอร์ ดังที่กล่าวข้างต้น การรับมือขั้นต้นของบริษัททท่านมีความสำคัญเป็นอย่างมากในการลดความเสียหาย ทว่าในการรับมือนั้นนอกจากความรวดเร็วแล้ว มาตรการการรับมือทางเทคนิคขั้นสูงเองก็มีความจำเป็นเช่นเดียวกัน บริษัทสาขาต่างประเทศที่ทรัพยากรมีจำกัดและสามารถรับมือต่อเหตุทางไซเบอร์ได้โดยไม่พึ่งองค์กรจากภายนอกนั้นมีไม่มาก เพราะฉะนั้นการฝึกอบรมอย่างสม่ำเสมอ และเตรียมความพร้อมในการประสานงานเพื่อที่หากเกิดเหตุจะได้สามารถประสานงานกับผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์จากภายนอกได้อย่างรวดเร็วจึงมีความสำคัญเป็นอย่างมาก

ในกรณีที่ใช้บริการประกันภัยอยู่แล้ว บริษัทประกันภัยจะทำการประสานงานกับผู้เชี่ยวชาญด้านเหตุไซเบอร์ และทำการแก้ไขปัญหาโดยเร็วเพื่อให้สามารถฟื้นฟูได้เร็วที่สุดเท่าที่จะทำได้ รวมทั้งหากมีการว่าจ้างบริษัท IT อยู่แล้วก็จะช่วยให้สามารถแก้ไขปัญหาได้รวดเร็วขึ้นด้วยเช่นกัน นอกจากนี้ยังมีบริษัทประกันภัยที่ให้บริการด้านการฝึกอบรม Phishing email ดังตัวอย่างด้านล่างซึ่งจะช่วยเพิ่มประสิทธิภาพในการรับมือต่อเหตุทางไซเบอร์ได้อีกด้วย



แผนภาพที่ 2 ตัวอย่างการฝึกอบรมรับมือ Phishing email

ความเสี่ยงทางไซเบอร์ เช่น ภาระทางการเงินมหาศาลอันเนื่องมากจากความเสียหายจากแรนซัมแวร์กำลังเพิ่มขึ้นและมีความซับซ้อนมากขึ้นทุกปี และนอกจากความเสียหายโดยตรงแล้ว จำนวนของความเสียหายที่เป็นผลสืบเนื่องและเหตุการณ์เล็กน้อยก็เพิ่มขึ้นด้วยเช่นเดียวกัน ซึ่งเหตุดังกล่าวนั้นไม่เพียงส่งผลกระทบต่อบริษัทของท่านเพียงอย่างเดียว แต่ยังส่งผลกระทบต่อคู่ค้าทางธุรกิจ ลูกค้า ผู้ถือหุ้น และในบางกรณีอาจส่งผลกระทบต่อตลาดและสังคมด้วยเช่นกัน เพราะฉะนั้นจึงอยากให้ท่านทราบว่า แม้ว่าจะเป็นสภาวะที่มีทรัพยากรจำกัดก็สามารถแก้ไขสถานการณ์ด้วยความความเร่งด่วนและการรับมือทางเทคนิคขั้นสูงได้เช่นกันหากมีการใช้บริการประกันภัยอย่างมีประสิทธิภาพ

ผลประโยชน์ของการใช้บริการประกันภัยมีดังนี้

1. การสนับสนุนการฝึกอบรมรับมือการโจมตีทางไซเบอร์ และการจัดหาเครื่องมือสำหรับการฝึกอบรม Phishing email สำหรับพนักงาน ฯลฯ
2. การสนับสนุนมาตรการฉุกเฉินสำหรับกรณีเกิดเหตุทางไซเบอร์และการฟื้นฟูระบบผ่านการประสานงานกับผู้เชี่ยวชาญ
3. ชดเชยค่าใช้จ่ายในการฟื้นฟูหลังเกิดเหตุทางไซเบอร์และค่าใช้จ่ายสำหรับผู้มีส่วนได้ส่วนเสีย (คู่ค้าทางธุรกิจ ฯลฯ) รวมถึงชดเชยค่าใช้จ่ายที่เกิดขึ้นจากการดำเนินการตามมาตรการฉุกเฉิน ค่าชดเชยสำหรับผู้ได้รับความเสียหายอันเนื่องมาจากการรั่วไหลของข้อมูลส่วนบุคคล และค่าชดเชยสำหรับคู่ค้าทางธุรกิจกรณีข้อมูลความลับรั่วไหล ฯลฯ

อ้างอิง

- https://www.avast.com/c-cybercrime
- https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx
- Kaspersky Security Bulletin Overall Statistics for 2020
- https://www.itday.in.th/kaspersky-reveals-a-30-45-percent-increase-in-web-threats-targeting-thai-users-in-q1-64/
- https://www.newsdirectory3.com/top-5-cyber-threats-to-attack-asean-thai-big-target-and-ransomware-that-hopes-more-than-money/
- https://www.terranovasecurity.com/what-is-ransomware/
- https://www.thairath.co.th/news/tech/2375175
- https://www.trendmicro.com/vinfo/us/security/definition/ransomware

รูปภาพ

- https://www.pixabay.com/photos/hacker-silhouette-hack-anonymous-3342696/
- https://www.pixabay.com/photos/regulation-gdpr-data-protection-3246979/
- https://www.pixabay.com/illustrations/question-mark-think-question-2318030/
- https://www.pixabay.com/vectors/scam-phishing-fraud-money-6922102/

MS&AD InterRisk Research & Consulting, Inc. is a MS&AD Insurance Group company specialized in risk management survey research and consulting services. For inquiry about consultation and seminar etc. for companies expanding business in Thailand, please feel free to contact the nearest Mitsui Sumitomo Insurance or Aioi Nissay Dowa Insurance sales representatives.

MS&AD InterRisk Research & Consulting, Inc.
International Section, Corporate Planning Department
TEL.03-5296-8920
http://www.irric.co.jp

InterRisk Asia (Thailand) is a MS&AD Insurance Group company which was established in Thailand to provide risk management services, such as fire safety, flood risk management, electrical safety and risk consulting services, such as automotive risk assessment, occupational safety and burglary risk survey to our clients in Thailand. For inquiry, please feel free to contact us.

InterRisk Asia (Thailand) Co., Ltd.
175 Sathorn City Tower, South Sathorn Road, Thungmahamek, Sathorn, Bangkok, 10120, Thailand
TEL: +66-(0)-2679-5276
FAX: +66-(0)-2679-5278
http://www.interriskthai.co.th/

The purpose of this report is to provide our customers with the useful information for the occupational safety and health management. There is no intention to criticize any individuals and parties etc.