ความปลอดภัยทางไซเบอร์

ภาคอุตสาหกรรมโลจิสติกส์ ประเทศเนเธอร์แลนด์

สำนักงานส่งเสริมการค้าในต่างประเทศ กรุงเฮก ประเทศเนเธอร์แลนด์

สารบัญ

คำนำ

ในยุคปัจจุบันเทคโนโลยีสารสนเทศได้ก้าวหน้าและพัฒนาไปอย่างมาก สามารถสร้างความสะดวกสบายและตอบสนองความต้องการให้กับผู้บริโภคจนกลายเป็นบริการที่สำคัญและจำเป็นอย่างสูง โดยเห็นได้จากการซื้อสินค้าและบริการต่างๆ และรูปแบบการทำธุรกรรมผ่านระบบออนไลน์มากขึ้น อาทิ แบบฟอร์มใบสมัคร อินเตอร์เน็ตแบงค์กิ้ง อี-คอมเมิร์ส ฐานข้อมูลออนไลน์ โซเชียลมิเดีย ฯลฯ ซึ่งการพัฒนารูปแบบเทคโนโลยีสารสนเทศเหล่านี้ส่งผลให้เศรษฐกิจของประเทศเติบโตได้อย่างรวดเร็ว แต่ในขณะเดียวกันความก้าวหน้าทางเทคโนโลยีสารสนเทศก็ทำให้ผู้ประกอบการต้องเจอกับปัญหาภัยคุกคามทางไซเบอร์ที่มีความก้าวหน้า รุนแรงและมากขึ้นอย่างต่อเนื่อง รวมทั้งยังสร้างความเสียหายให้กับทั้งผู้ใช้งานและผู้ประกอบการเช่นกัน

ในรายงานฉบับนี้จะกล่าวถึงภัยคุกคามทางไซเบอร์ ผลกระทบที่เกิดขึ้นและตัวอย่างผลกระทบที่เกิดขึ้นในภาคอุตสาหกรรมโลจิสติกส์ในประเทศเนเธอร์แลนด์ รวมถึงวิธีทางการป้องกันของภาครัฐและภาคเอกชนในเนเธอร์แลนด์ ทั้งนี้เพื่อให้ผู้อ่านได้เข้าใจในรายงานฉบับนี้มากยิ่งขึ้น ทางสำนักงานฯขออธิบายถึงคำกำจัดความต่างๆเพิ่มเติม ดังนี้

มัลแวร์ (Malware) : ย่อมาจาก Malicious Software เป็นโปรแกรมที่มีจุดประสงค์ไปในทางที่ทำให้คอมพิวเตอร์ได้รับความเสียหายหรือใช้การไม่ได้ รวมไปถึงการโจรกรรมข้อมูล แบ่งออกได้หลากหลายประเภท เช่น ไวรัส (Virus) เวิร์มหรือหนอนอินเทอร์เน็ต (Worm) ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger) บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน ตลอดจนโปรแกรมประเภทขโมยข้อมูล (Cookie)

แรนซัมแวร์ (Ransomware) : มัลแวร์ประเภทหนึ่งที่จะเข้าทำการตั้งรหัสลับหรือล็อคไฟล์ต่างๆในเครื่องคอมพิวเตอร์ ทั้งประเภทไฟล์เอกสาร รูปภาพ และวีดีโอ โดยหากไฟล์ใดถูกตั้งรหัสหรือถูกล็อค จะมีข้อความแสดงบนหน้าจอให้ผู้ใช้งานจ่ายเงินเพื่อกู้ไฟล์หรือปลดล็อกไฟล์นั้นๆ หรือเรียกว่า“ เงินเค่าไถ่“

สแปม (Spam) : คือการส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมาก โดยผู้ที่ได้รับจดหมายเหล่านั้นไม่ได้มีความประสงค์ที่จะรับ ส่วนมากเป็นการโฆษณาสินค้าและบริการ

ฟิชชิ่ง (Phishing) : การหลอกลวงหรือกลลวงทางอินเตอร์เนตเพื่อเข้ามาหาข้อมูลที่สำคัญ เช่น บัญชีผู้ใช้งานหรือรหัสผ่าน เป็นต้น โดยส่วนใหญ่จะใช้วิธีส่งผ่านอีเมล์และระบุถึงความสำคัญและความเสียหายที่จะเกิดขึ้นหากผู้รับอีเมล์ไม่กดลิงค์ที่แนบมาเพื่อเข้าไปแก้ไขหรืออัพเดทข้อมูล และ/หรืออาจใช้วิธีสร้างเว็บไซต์ปลอมให้คล้ายกับเว็บไซต์ของธนาคารหรือบัตรเครดิตเพื่อให้เข้าสู่ระบบและใส่ข้อมูลที่สำคัญ นอกจากนี้ฟิชชิ่งอาจมาในรูปแบบของโทรศัพท์ด้วยเช่นกัน

Spear Phishing: ฟิชชิ่งประเภทหนึ่ง เป็นการโจมตีขั้นสูง แต่มีเป้าหมายเฉพาะเจาะจง

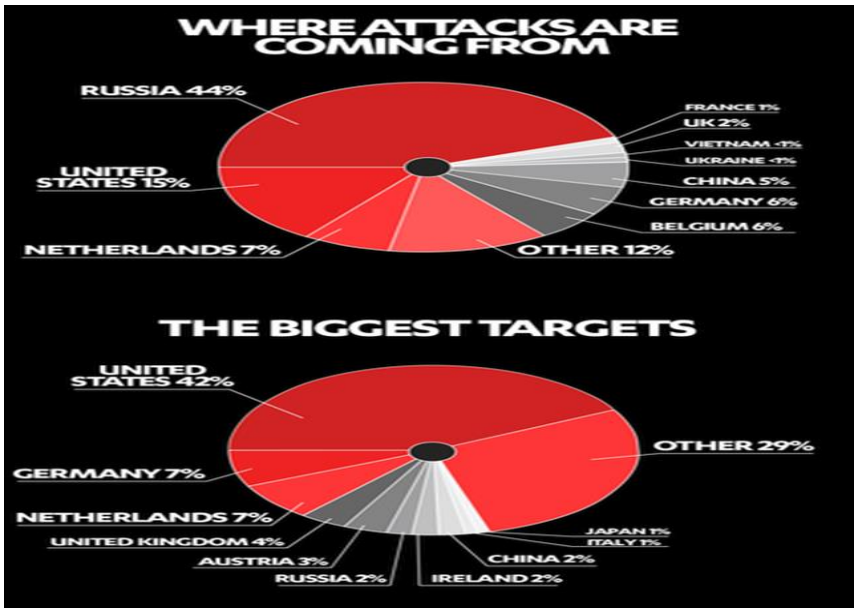
อาชญากรรมคอมพิวเตอร์ : หรือ อาชญากรรมไซเบอร์ เป็นอาชญากรรมที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ โดยการเปลี่ยนแปลง ทำลาย หรือขโมยข้อมูลของบุคคลอื่นเพื่อใช้แสวงหาผลประโยชน์อย่างผิดกฎหมาย

บล็อคเชน (Blockchain) : เทคโนโลยีการจัดเก็บข้อมูลชนิดหนึ่ง (Database) ที่ไม่มีศูนย์กลางแต่มีลักษณะเป็นบล็อกเรียงต่อกันเป็นสาย แต่ละบล็อกมีชุดข้อมูลที่สามารถเชื่อมโยงไปยังบล็อกก่อนหน้าได้ แต่ยังคงความสามารถในการตรวจสอบเต็ม 100% เหมือนเดิม และสามารถนำไปประยุกต์ใช้กับระบบอื่นๆ ในแต่ละภาคอุตสาหกรรมได้

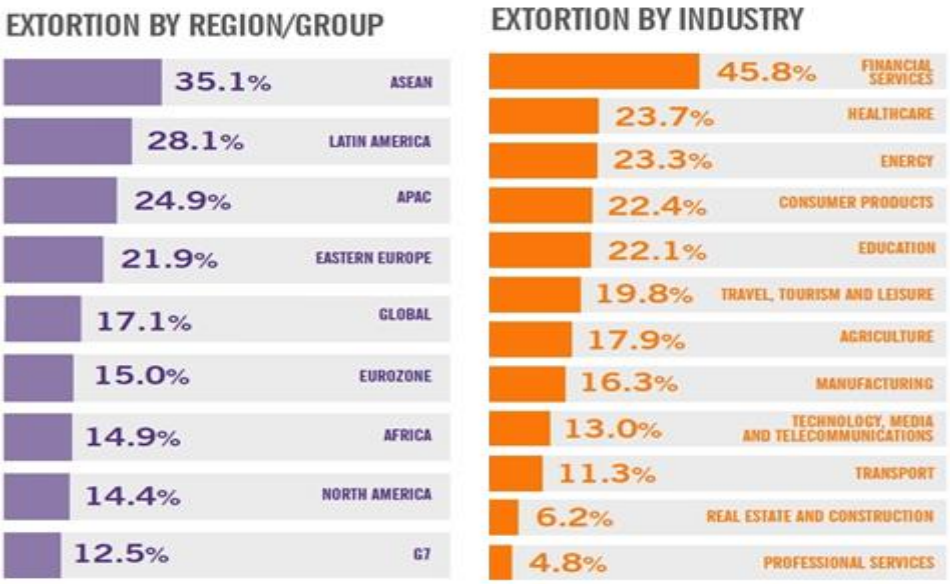
1) ภัยคุกคามทางไซเบอร์และอุปสรรคในการจัดการ

ในปัจจุบันอาญชากรรมหรือภัยคุมคามทางไซเบอร์นับว่าเป็น 1 ใน 10 ความเสี่ยงสำคัญของบริษัทหรือองค์กร โดยภัยคุกคามทางไซเบอร์จะมาในรูปแบบต่างๆ ทั้งต้องการก่อกวนหรือทำลายระบบ (มัลแวร์ต่างๆ หนอน ไวรัส ม้าโทรจัน) การขโมยข้อมูล หรือดักฟังข้อมูล (แฮกกิ้ง หรือ ฟิชชิ่ง) ต้องการเข้าระบบโดยไม่ได้รับอนุญาต การปลอมแปลงหรือสวมรอยเป็นบุคคลอื่น การโฆษณาชวนเชื่อและอีเมล์หลอกลวง (สแปม) หรือแม้แต่การก่อการร้าย โดยสาเหตุที่เกิดขึ้น ได้แก่ การเข้าเว็บไซต์ที่ไม่น่าเชื่อถือ การเข้าอีเมล์หรือลิงค์ที่แปลกปลอม การเข้าเครือข่ายไร้สายที่ไม่ปลอดภัย และการดาวโหลดหรือลงโปรแกรมที่แฝงด้วยมัลแวร์ชนิดต่างๆ เป็นต้น

ประเทศเนเธอร์แลนด์เป็นประเทศหนึ่งที่มีอาชญากรไซเบอร์แฝงตัวเพื่อใช้เครือข่ายในการสร้างภัยคุมคามทั่วโลก รวมทั้งเป็นแหล่งเป้าหมายของอาชญากรไซเบอร์ถึงร้อยละ 7 โดยรัสเซียและสหรัฐอเมริการเป็นแหล่งที่มาของภัยคุกคามร้อยละ 44 และ 15 ตามลำดับ และสหรัฐอเมริกาเป็นประเทศเป้าหมายสูงสุดร้อยละ 42



แหล่งที่มา : www.beveilignieuws.nl



แหล่งที่มา : www.consultancy.nl

ปัญหาภัยคุกคามไซเบอร์ได้แพร่ไปยังทั่วโลกที่มีการใช้คอมพิวเตอร์และเครือข่ายอินเตอร์เน็ต โดยเกิดขึ้นมากสุดในแถบภูมิภาคเอเชีย (ร้อยละ 35.1) ลาตินอเมริกา (ร้อยละ 28.1) และเอเปค (ร้อยละ 24.9) มีเป้าหมายหลักคืออุตสาหกรรมการเงินการธนาคาร (ร้อยละ 45.8) ตามด้วยอุตสาหกรรมสาธารณสุข (ร้อยละ 23.7) และพลังงาน (23.3) โดยภัยคุกคามทั่วโลกนี้สร้างความเสียหายให้แก่บริษัททั่วโลกโดยรวมกว่า 280 พันล้านดอลล่าห์สหรัฐในปี 2016

1.1) <u>ปัญหาและอุปสรรคในการจัดการภัยคุกคามทางไซเบอร์</u>

จากการสำรวจ พบว่า สาเหตุที่ภัยคุกคามไซเบอร์ยังสามารถเกิดได้อย่างต่อเนื่องนั้น ได้แก่

- ผู้บริหารและพนักงานยังไม่ให้ความสำคัญหรือไม่เห็นความจำเป็น ทั้งนี้อาจเนื่องจากยังเห็นเป็นเรื่องใหม่หรือยังไม่เคยได้รับผลกระทบจากเหตุการณ์ถูกโจมตีทางไซเบอร์ จึงทำให้บริษัทยังไม่เห็นความสำคัญในจุดนี้
- ขาดความรู้และทักษะ หรือขาดระบบรักษาความปลอดภัยไซเบอร์ที่มีประสิทธิภาพ โดยพนักงานหรือผู้บริหารเองยังขาดความรู้หรือทักษะเกี่ยวกับภัยคุกคามทางไซเบอร์ รวมทั้งบริษัทยังขาดแคลนระบบรักษาความปลอดภัยที่มีประสิทธิภาพ หรือไม่มีบุคลากรผู้รับผิดชอบและดูแลในส่วนนี้อย่างจริงจัง
- ขาดงบประมาณสำหรับระบบรักษาความปลอดภัยทางไซเบอร์ ทั้งนี้งบประมาณจัดว่าเป็นปัจจัยหนึ่งที่สำคัญหากบริษัทไม่มีงบประมาณในส่วนนี้แล้วก็จะทำให้เกิดความเสี่ยงต่อความเสียหายที่อาจจะเกิดขึ้นได้
- การใช้งานเทคโนโลยีเพิ่มมากขึ้นทำให้เกิดความเสี่ยงจากภัยคุกคามเพิ่มมากขึ้นเช่นกัน
- บริษัทและองค์กรปกปิดข้อมูลข่าวสารเหตุการณ์การโจมตีทางไซเบอร์ เนื่องจากกลัวกระทบต่อชื่อเสียง สินค้าและผลิตภัณฑ์ของบริษัท ที่จะทำให้ยอดขายหรือรายได้บริษัทลดลงได้
- กฎหมายยังไม่สามารถจัดการกับผู้กระทำผิดทางไซเบอร์ได้อย่างครอบคลุม หรือยังมีช่องโหว่งทางกฎหมาย

2) ภัยคุกคามทางไซเบอร์กับภาคอุตสาหกรรมโลจิสติกส์เนเธอร์แลนด์

ภาคอุตสาหกรรมโลจิสติกส์เป็นอีกเป้าหมายหนึ่งของอาชญากรไซเบอร์ โดยรูปแบบของภัยคุกคามนั้น ได้แก่ การพยายามเปลี่ยนแปลงหมายเลขบัญชีธนาคารในระบบ (รวมทั้งอาจมีการแฮ็กข้อมูลในระบบของซัพพลายเออร์ด้วย) การโยกย้าย แก้ไข หรือขโมยข้อมูลในฐานข้อมูลการขนส่ง การขโมยข้อมูลพนักงานในบริษัทขนส่งเพื่อใช้ทำการโอนเงิน/โอนสินค้าอย่างผิดกฎหมาย รวมทั้งการล็อคไฟล์เพื่อเรียกค่าปลดล็อค เป็นต้น ทั้งนี้การคุกคามทางไซเบอร์ในอุตสาหกรรมโลจิสติกส์เนเธอร์แลนด์ได้เพิ่มขึ้นอย่างมากในช่วง 2-3 ปีที่ผ่านมา โดยเฉพาะการโจมตีจากฟิชชิ่งที่เกิดจากข้อมูลที่รั่วไหลของบริษัทและ Ransomware โดยในเดือนมิถุนายนที่ผ่านมา ได้มีเหตุการณ์การถูกโจมตีทางไซเบอร์ของบริษัทโลจิสติกส์ขนาดใหญ่ในเนเธอร์แลนด์ 2 แห่ง และได้รับความเสียหายอย่างมาก ดังนี้

- บริษัท Maersk (บริษัทขนส่งโลจิสติกส์และพลังงานจากประเทศเดนมาร์ก)

ถูกโจมตีจากมัลแวร์ “NotPetya-ransomware” ในระหว่างการลงซอฟแวร์ด้านบัญชี ในบริเวณท่าเรือ Rotterdam จนทำให้ระบบปฏิบัติการและเครือข่ายทั้งหมดของบริษัท Maersk Line และบริษัทในเครืออย่าง APM Terminals และ Damco ไม่สามารถทำงานได้และหยุดการขนส่งในทันที ทางบริษัทฯใช้เวลากว่า 2 สัปดาห์ในการกู้ระบบและบริหารจัดการใหม่เพื่อสามารถให้บริการได้ โดยได้ประเมินค่าความเสียหายที่เกิดขึ้นประมาณ 255 ล้านดอลล่าห์สหรัฐ

- บริษัท TNT Express (บริษัทขนส่งและโลจิสติกส์ ประเทศเนเธอร์แลนด์)

ถูกโจมตีจากมัลแวร์ “Not Petya-ransomware” และเรียกร้องค่าปลดล็อค หรือ “เงินเรียกค่าไถ่” จำนวน 300 ล้านดอลล่าห์สหรัฐ จากการโจมตีนี้ทำให้ระบบปฏิบัติการไม่สามารถใช้งานได้ รถบรรทุกและเครื่องบินขนส่งหยุดทำการทั้งหมด ส่งผลให้จดหมายและกล่องพัสดุจำนวนมากติดค้างและไม่สามารถนำส่งผู้รับได้ตามกำหนด ทั้งนี้บริษัท TNT Express ไม่มีประกันภัยความเสียหายทางไซเบอร์ และคาดการณ์ความเสียหายอย่างต่ำที่ 300 ล้านดอลล่าห์สหรัฐ

ทั้งนี้อุตสาหกรรมโลจิสติกส์จัดว่าเป็นหนึ่งในอุตสาหกรรมที่มีความสำคัญอย่างมากของเนเธอร์แลนด์ เนื่องด้วยการค้าส่วนใหญ่ของประเทศเป็นลักษณะนำเข้าเพื่อส่งออก รวมทั้งเนเธอร์แลนด์มีทำเลที่ตั้งเหมาะสมและมีศักยภาพในการขนส่งและระบายสินค้าได้อย่างรวดเร็ว จึงทำให้เนเธอร์แลนด์กลายเป็นแหล่งศูนย์กลางกระจายสินค้าในภูมิภาคยุโรป นอกจากนี้เนเธอร์แลนด์ยังมีท่าเรือ (Port of Rotterdam) ที่ใหญ่ที่สุดในยุโรปและเป็น gateway สินค้าผ่านเข้า-ออกสู่ยุโรป ดังนั้นการโจมตีทางไซเบอร์กับบริษัทโลจิสติกส์ที่ไม่มีการเตรียมการหรือไม่มีระบบบริหารความปลอดภัยที่มีประสิทธิภาพเพียงพอนั้นสามารถสร้างความเสียหายให้กับบริษัทและผู้ที่เกี่ยวข้องได้อย่างมหาศาล

3) มาตรการกฎหมายและแนวทางการปฏิบัติในประเทศเนเธอร์แลนด์

ประเทศเนเธอร์แลนด์นั้นมีกฎหมายบัญญัติเกี่ยวกับเรื่องความปลอดภัยของข้อมูล (Information security) และ การรั่วไหลของข้อมูล (Data leaking) ดังนั้นเหตุการณ์ใดที่เกิดขึ้นและบ่งชี้ว่าเป็นอาชญากรรมทางไซเบอร์จะต้องมีการรายงานต่อเจ้าหน้าที่ตำรวจในทันที ทั้งนี้เพื่อเพิ่มความกดดันและความตระหนักต่อความปลอดภัยด้านไซเบอร์ในกลุ่มผู้ประกอบการมากยิ่งขึ้น โดยผู้ประกอบการนั้นจะต้องรายงานข้อมูลของบริษัท ลักษณะธุรกิจที่ดำเนินการและบริษัทคู่ค้าที่ทำการติดต่อด้วยทั้งหมดเพื่อเป็นประโยชน์ต่อการจับกุม นอกจากนี้ทางสหภาพยุโรปยังมีกฎหมายที่เกี่ยวกับข้อมูลส่วนบุคคล (Privacy law) ซึ่งจะต้องนำมาพิจารณาหากต้องการทำธุรกิจที่นี่ ทั้งนี้ผู้บริโภคและบริษัทผู้ประกอบการในประเทศเนเธอร์แลนด์มีแนวทางปฏิบัติเพื่อความปลอดภัยทางไซเบอร์ ดังนี้

3.1) กลุ่มบุคคลทั่วไป

ในประเทศเนเธอร์แลนด์นั้นได้มีการเตือนผู้บริโภคเกี่ยวกับภัยคุกคามทางไซเบอร์ผ่านสื่อโทรทัศน์เป็นครั้งคราว ซึ่งจัดทำโดยองค์กรภาครัฐและเอกชน เพื่อให้ประชาชนได้รับรู้และระมัดระวังถึงกลลวงต่างๆที่แฝงตัวจากการใช้งานอินเตอร์เนต เช่น การไม่เข้าลิงค์ในอีเมล์ที่ผิดปกติ การไม่เข้าเว็บไซต์ที่ไม่คุ้นเคยหรือไม่มีความน่าเชื่อถือ รวมถึงการไม่ให้ข้อมูลส่วนตัวของตนกับเว็บไซต์หรือบุคคลอื่น เป็นต้น หากกรณีพลาดพลั้งถูกภัยคุกคามจนได้รับผลกระทบและความเสียหายนั้น สามารถแจ้งความผ่านเบอร์โทรศัพท์ 0900-8844 หรือผ่านเว็บไซต์ของสำนักงานตำรวจแห่งชาติดัชต์

3.2) กลุ่มบริษัทและผู้ประกอบการ

- เลือกใช้ระบบหรือเทคโนโลยีที่มีความก้าวหน้าและมีประสิทธิภาพสูง

กลุ่มบริษัทและผู้ประกอบการพยายามมองหาแนวทางป้องกันภัยคุกคามที่อาจเกิดขึ้น โดยหลายบริษัทในเนเธอร์แลนด์เลือกใช้เทคโนโลยี Block chain เป็นตัวช่วยด้านการจัดเก็บฐานข้อมูลอย่างมีประสิทธิภาพและเชื่อถือได้ เช่น กลุ่มธนาคารและสถาบันการเงิน (ABN Amro, ING, SociétéGénérale), บริษัท พลังงาน (BP, Gunvor, Koch Supply & Trading, Mercuria, Shell, Statoil) เทคโนโลยีนี้สามารถปรับใช้ได้กับทุกภาคอุตสาหกรรม โดยขณะนี้เทคโนโลยี Block chain กำลังถูกพัฒนาอย่างต่อเนื่องเพื่อลดความเสี่ยงและค่าใช้จ่ายในการบริหาร รวมทั้งเพิ่มประสิทธิภาพในการทำธุรกรรมที่ปลอดภัยและโปร่งใสมากขึ้น ซึ่งคาดว่าจะสามารถพร้อมใช้งานได้เต็มรูปแบบภายในสิ้นปี 2018 นี้

นอกจากนี้ภาคอุตสาหกรรมโลจิสติกส์ยังมีระบบบันทึกพิเศษเพื่อช่วยเพิ่มรักษาความปลอดภัยและลดปัญหาอาชญากรรมที่เรียกว่า 'Warning Register Logistics Sector หรือ WLS' เป็นการร่วมจัดทำโดยองค์กรต่างๆในภาคอุตสาหกรรมโลจิสติกส์ ที่มุ่งเน้นด้านการตรวจสอบพนักงานและบันทึกข้อมูลทางอาญา โดยจะจัดเก็บรายชื่อผู้ต้องคดีความ (Black list) เป็นเวลาอย่างน้อย ปี 4 หรือจนกว่าจะพ้นคดีความ ทั้งนี้ระบบ WLS สามารถช่วยผู้ประกอบการคัดกรองพนักงานได้อย่างรวดเร็วและสามารถลดความเสี่ยงจากปัญหาอาชญากรรม(ไซเบอร์)ได้ระดับหนึ่ง

- การจัดสัมมนาหรืออบรมเกี่ยวกับเรื่องความปลอดภัยทางไซเบอร์

หลายบริษัทได้มีการจัดสัมมนาหรืออบรมสำหรับพนักงานในองค์กรเพื่อให้รู้ถึงประเภทภัยคุกคามที่อาจจะเกิดขึ้นและวิธีปฏิบัติเมื่อประสบเหตุการณ์ ซึ่งนับว่าเป็นอีกวิธีหนึ่งที่สามารถช่วยป้องกันและลดความเสี่ยงจากการคุมคามทางไซเบอร์ได้

- การทำประกันภัยความเสียหาย

การมีประกันภัยความเสียหายด้านไซเบอร์สามารถช่วยชดเชยความเสียหายที่เกิดขึ้นจากอาชญากรรมไซเบอร์ได้บางส่วน เช่น การสูญเสียรายได้ในช่วงระหว่างการถูกโจมตี (โดยเฉพาะร้านค้าออนไลน์) ทั้งนี้จากงานวิจัยของ TNL พบว่าบริษัทในเนเธอร์แลนด์ส่วนใหญ่ (มากกว่าร้อยละ 80) ยังไม่สนใจทำประกันประเภทนี้

ส่วนการแจ้งความในรูปแบบบริษัทนั้นจะต้องเป็นผู้ที่มีอำนาจหน้าที่หรือได้รับเป็นตัวแทนในการดำเนินการแจ้งความ โดยสามารถแจ้งความผ่านเว็บไซต์ของสำนักงานตำรวจแห่งชาติดัชต์เท่านั้น ซึ่งการแจ้งความในรูปแบบบริษัทจำเป็นจะต้องลงทะเบียนเพื่อขอรับบัญชีผู้ใช้งานและรหัสผ่าน

3.3) <u>ภาครัฐ</u>

จากรายงานเหตุการณ์อาชญากรรมไซเบอร์ที่เกิดขึ้นบ่อยครั้งและสร้างความเสียหายอย่างมหาศาลทำให้รัฐบาลเนเธอร์แลนด์ตระหนักและเห็นความสำคัญเรื่องความมั่นคงและปลอดภัยทางไซเบอร์(แห่งชาติ)มากขึ้น โดยในปีนี้ทางรัฐบาลได้ตั้งงบประมาณจัดสรรไว้ถึง 26 ล้านยูโร รวมทั้งยังได้ผลักดันกฎหมายใหม่ “Sleepwet” ที่มีจุดประสงค์เพื่อสร้างความมั่นคงและปลอดภัยของประเทศ โดยสามารถเข้าถึงเครือข่ายและข้อมูลทุกอย่างและมีหน่วยข่าวกรอง MIVD และ AIVD ของภาครัฐเป็นผู้ควบคุมดูแล ทั้งนี้เนื้อหาของกฎหมายใหม่ที่เปลี่ยนแปลงไปจากเดิมอย่างเห็นได้ชัด มี 4 ข้อหลักดังต่อไปนี้

- Sleepwet สามารถดักฟังการสนทนาออนไลน์ของบุคคลทั้งหมด ทั้งผู้ต้องสงสัยและบุคคลทั่วไป ตัวอย่างเช่น เพื่อนบ้านโดยรอบในเขตพื้นที่ที่ผู้ต้องสงสัยอาศัยอยู่
- อุปกรณ์และเครื่องมือสื่อสารทุกชนิดสามารถถูกแฮ็กได้ทั้งหมด เช่น คอมพิวเตอร์ โทรศัพท์มือถือ สมาร์ททีวี ฯลฯ
- ประชาชนทุกคนสามารถเข้าดูฐานข้อมูลลับ DNA ได้
- อาจมีการแบ่งปันข้อมูลให้กับหน่วยข่าวกรองต่างประเทศ โดยไม่ต้องมีการวิเคราะห์ข้อมูลก่อน

การต้องการพยายามเข้าควบคุมและรับรู้ทุกการสื่อสารของภาครัฐนั้น ส่งผลให้ประชาชนในประเทศบางกลุ่มรู้สึกถึงความไม่เป็นส่วนตัว รวมทั้งรู้สึกขัดต่อข้อบัญญัติเกี่ยวกับเรื่องเสรีภาพ และได้มีการต่อต้านด้วยการจัดทำประชามติ (referendum) โดยมีประชาชนบางส่วนร่วมลงคะแนนประชามติต่อต้านจำนวน 417.000 คน ทั้งนี้ กฎหมาย Sleepwet ได้ถูกนำเสนอแก่วุฒิสภาเมื่อวันที่ 11 กรกฎาคม 2017 และจะได้ข้อสรุปอย่างเป็นทางการในเดือนมีนาคม 2018

4) องค์กรและหน่วยงานที่เกี่ยวข้อง

AIVD (Algemene Inlichtingen- en Veiligheidsdienst)
หน่วยข่าวกรองและความปลอดภัยของประเทศเนเธอร์แลนด์ (เรียกได้ว่าเป็น “Secret Service” on the internet) สังกัดกระทรวงมหาดไทย ก่อตั้งเมื่อปี 2002 มีสำนักงานใหญ่ที่เมือง Zoetermeer ประเทศเนเธอร์แลนด์ (www.aivd.nl)

MIVD (Militaire Inlichtingen- en Veiligheidsdienst)
หน่วยข่าวกรองทางทหารของประเทศเนเธอร์แลนด์ สังกัดกระทรวงกลาโหม ก่อตั้งขึ้นปี 2002
มีสำนักงานใหญ่อยู่ที่กรุงเฮก ประเทศเนเธอร์แลนด์ (www.mivd.nl)

Tno (Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek)
องค์กรอิสระไม่แสวงหากำไรที่นับว่าเป็นสถาบันเพื่อการวิจัยและพัฒนาที่ใหญ่ที่สุดในเนเธอร์แลนด์ ให้บริการในด้านงานวิจัย บริการคำปรึกษาพิเศษ และออกใบรับรองสำหรับผู้ปกครอง รวมทั้งบริการซอฟแวร์ชนิดพิเศษ นอกจากนี้ TNO ยังทำหน้าที่ทดสอบและออกใบรับรองให้กับสินค้าและบริการ รวมถึงประเมินผลคุณภาพอย่างอิสระ และยังช่วยก่อตั้งบริษัทรายใหม่สู่ตลาดนวัตกรรม ก่อตั้งเมื่อปี 1932 มีสำนักงานใหญ่ที่กรุงเฮก ประเทศเนเธอร์แลนด์ (www.tno.nl)

TLN (Transport and Logistics Netherlands)
สมาคมเพื่อการขนส่งและโลจิสติกส์ ประเทศเนเธอร์แลนด์ ให้ความช่วยเหลือต่างๆแก่สมาชิก เช่น การเจรจาและจัดการเกี่ยวกับข้อตกลงการขนส่ง และเงินบำนาญที่เหมาะสมแก่สมาชิก เป็นต้น มีสำนักงานใหญ่ที่เมือง Zoetermeer ประเทศเนเธอร์แลนด์

NCSC (Nationaal Cyber Security Centrum)
องค์กรภาครัฐ อยู่ภายใต้สังกัดกระทรวงยุติธรรมและความมั่นคง เป็นจุดศูนย์กลางข้อมูลและความชำนาญสำหรับความมั่นคงปลอดภัยทางไซเบอร์ในประเทศเนเธอร์แลนด์ นอกจากนี้ NCSC ยังเป็นแกนหลักในการประสานงานด้านปฏิบัติการในภาวะวิกฤติด้านไอซีทีและทีมงานดูแลและรับผิดชอบเครือข่ายคอมพิวเตอร์เร่งด่วน (CERT) ของรัฐบาล (www.ncsc.nl)

CERT-EU (Computer emergency response team – EU)
เป็นการรวมกลุ่มจัดตั้งของสมาชิกสหภาพยุโรปในปี 2012 เพื่อประสานงานและกระตุ้นให้กับ CSIRT/CERT ของแต่ละประเทศร่วมดำเนินการด้านการรักษาความปลอดภัยไซเบอร์และแจ้งเตือนภัยให้แก่สมาชิกอย่างต่อเนื่องตลอด 24 ชั่วโมง นอกจากนี้ยังมี EGC (European Government CERT) ซึ่งเกิดจากการรวมตัวของประเทศสมาชิกและให้ความช่วยเหลือกันทางด้านเทคนิคแบบไม่เป็นทางการ เพื่อเฝ้าระวังและตอบโต้กับภัยคุกคามทางไซเบอร์ให้กับประเทศสมาชิกสหภาพยุโรป โดยมีภารกิจหลัก ได้แก่ การสนับสนุนประเทศสมาชิกและองค์กรต่างๆ ของสหภาพยุโรปให้สามารถป้องกันตนเองจากการโจมตีทางไซเบอร์ (cert.europa.eu)

สำนักงานตำรวจแห่งชาติดัชตต์ (Team High Tech Crime)
อยู่ภายใต้สังกัดกระทรวงยุติธรรมและความมั่งคง ให้บริการประชาชน 24 ชั่วโมง (www.politie.nl)

NBIP (Nationale Beheersorganisatie Internet Providers)
เป็นผู้บริการให้ความช่วยเหลือแก่ผู้ให้บริการเครือข่ายอินเตอร์เน็ตเพื่อจุดประสงค์ด้านความปลอดภัยในเครือข่ายอินเตอร์เน็ต ก่อตั้งขึ้นในปี 2002 (www.nbip.nl)

บทสรุปและข้อเสนอแนะ

ภาคอุตสาหกรรมขนส่งและโลจิสติกส์เป็นภาคอุตสาหกรรมหนึ่งที่มีความสำคัญและจำเป็นสำหรับการพัฒนาและขับเคลื่อนเศรษฐกิจของประเทศ ในส่วนของผู้ประกอบการนั้น การบริหารและจัดการโลจิสติกส์อย่างมีประสิทธิภาพนอกจากจะสามารถช่วยลดต้นทุนให้กับบริษัทแล้วยังสามารถสร้างความน่าเชื่อถือและไว้วางใจให้กับผู้ร่วมการค้าและผู้รับบริการได้อย่างมาก ทั้งนี้จากข้อมูลและตัวอย่างความเสียหายที่เกิดขึ้นในรายงานฉบับนี้จะเห็นได้ว่าการไม่เตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ อาจสร้างความเสียหายให้แก่บริษัทได้อย่างมหาศาล ดังนั้นการป้องกันและจัดการกับปัญหาภัยคุกคามหรืออาชญากรรมไซเบอร์ที่มีมากขึ้นอย่างต่อเนื่องนั้น จึงเป็นอีกหนึ่งหัวข้อหลักที่ผู้ประกอบการควรให้ความสนใจและให้ความความสำคัญเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นในอนาคต

สำนักงานส่งเสริมการค้าในต่างประเทศ ณ กรุงเฮก ประเทศเนเธอร์แลนด์

พฤศจิกายน 2017