รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ

จัดทำโดย นายชูเกียรติ ประเสริฐสุข
รหัส 12019

รายงานนี้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูต รุ่นที่ 12 ปี 2563
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ

รายงานการศึกษาส่วนบุคคล
(Individual Study)

เรื่อง มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับสำนักงานในต่างประเทศ

จัดทำโดย นายชูเกียรติ ประเสริฐสุข
รหัส 12019

หลักสูตรนักบริหารการทูต รุ่นที่ 12 ปี 2563
สถาบันการต่างประเทศเทวะวงศ์วโรปการ กระทรวงการต่างประเทศ
รายงานนี้เป็นความคิดเห็นเฉพาะบุคคลของผู้ศึกษา

เอกสารรายงานการศึกษาส่วนบุคคลนี้ อนุมัติให้เป็นส่วนหนึ่งของการฝึกอบรม
หลักสูตรนักบริหารการทูตของกระทรวงการต่างประเทศ

ลงชื่อ.....

(เอกอัครราชทูตกิตติพงษ์ ณ ระนอง)
อาจารย์ที่ปรึกษา

ลงชื่อ.....

(ศาสตราจารย์ ดร.พลภัทร บุราคม)
อาจารย์ที่ปรึกษา

ลงชื่อ.....

(รองศาสตราจารย์ ดร.รุ่งพงษ์ ชัยนาม)
อาจารย์ที่ปรึกษา

บทสรุปสำหรับผู้บริหาร

สถานเอกอัครราชทูตและสถานกงสุลใหญ่ (สอท./สกญ.) แต่ละแห่งนั้น มีความพร้อมด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และระบบเทคโนโลยีสารสนเทศที่แตกต่างกัน และมีความต่างด้านความอ่อนไหวของข้อมูลหรือมีความเสี่ยงต่อการรั่วไหลของข้อมูลด้วยเช่นกัน และในช่วง 2–3 ปีที่ผ่านมา สอท./สกญ. บางแห่งประสบปัญหาการละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (security breach) จนทำให้เกิดความเสียหายและไม่สามารถใช้งานในบางระบบได้ ดังนั้น เพื่อเป็นการป้องกันและรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่สำคัญให้กับ สอท./สกญ. ผู้เขียนจึงได้จัดทำรายงานการศึกษาส่วนบุคคลนี้ในหัวข้อเรื่อง มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ ภายใต้แนวคิดการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ สอท./สกญ. ให้มีมาตรฐานเดียวกันทั่วโลก โดยอาศัยหลักการทฤษฎีประกอบการจัดทำมาตรฐาน ดังนี้ (1) หลักการพื้นฐาน 3 ประการของการรักษาความมั่นคงปลอดภัยของข้อมูล CIA Triad คือ การรักษาความลับของข้อมูล Confidentiality), ความครบถ้วนถูกต้อง (Integrity) และความพร้อมใช้ (Availability) (2) หลักการสำคัญของการดำเนินการรักษาความมั่นคงปลอดภัยอันประกอบด้วย การป้องกัน (protection) การตรวจจับ (detection) และการฟื้นสภาพ (recovery) (3) การแบ่งแยกเครือข่าย (segregation in networks) ซึ่งจะเกี่ยวกับการแบ่งส่วนเครือข่าย (network segmentations) ออกเป็นโซนต่าง ๆ ให้เกิดความมั่นคงปลอดภัยและสะดวกในการบริหารจัดการ

สำหรับวัตถุประสงค์ของการศึกษาก็เพื่อศึกษาถึงสถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ทั่วโลก ความเสี่ยงต่อการรั่วไหลของข้อมูลและความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ และเพื่อกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานระบบฯ, หมายเลข IP Address ภายในระบบเครือข่ายของ สอท./สกญ. แต่ละแห่ง และคุณลักษณะเฉพาะของอุปกรณ์/ระบบป้องกันภัยคุกคามไซเบอร์ที่จะจัดซื้อจัดจ้าง นอกจากนี้ก็เพื่อกำหนดเกณฑ์การใช้มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เกิดความเหมาะสมของแต่ละ สอท./สกญ. ต่อไป

ในการศึกษานี้ ผู้เขียนได้ทำการรวบรวมข้อมูลปฐมภูมิ (Primary Data) ซึ่งได้จากการสำรวจ การสัมภาษณ์เจ้าหน้าที่ที่เคยออกประจำการบางท่าน จากการรายงานปัญหาภัยคุกคามทางไซเบอร์ของ สอท./สกญ. บางแห่ง และจากการสังเกตการณ์ด้วยตนเอง สำหรับข้อมูลทุติยภูมิ (Secondary Data) นั้น ได้ทำการรวบรวมสถิติภัยคุกคามทางไซเบอร์ที่เกิดขึ้นทั้งในระดับองค์กร ระดับประเทศ และระดับโลก แล้วจึงนำข้อมูลดังกล่าวมาทำการวิเคราะห์ศึกษา ซึ่งสามารถสรุปผล

การศึกษาได้ว่า สถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. หลายแห่ง (มากกว่าร้อยละ 55) ยังขาดความพร้อมในการจัดการภัยคุกคามที่อาจเกิดขึ้น เนื่องจากแต่ละแห่งมีความพร้อมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับต่ำ และมีช่องโหว่ในระบบสูง พร้อมกันนั้นยังไม่มีมาตรฐานระบบรักษาความมั่นคงปลอดภัยที่เหมาะสม

เพื่อให้ สอท./สกญ. แต่ละแห่งมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ผู้เขียนจึงได้กำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ ออกเป็น 2 ระดับ คือ มาตรฐานขั้นพื้นฐาน และมาตรฐานขั้นสูง โดยมาตรฐานขั้นพื้นฐานจะเป็นมาตรฐานที่ สอท./สกญ. ทุกแห่งต้องนำไปปฏิบัติให้เกิดความมั่นคงปลอดภัย สำหรับมาตรฐานขั้นสูงจะเป็นมาตรฐานที่มีความซับซ้อนของระบบและมีอุปกรณ์รักษาความปลอดภัยที่มีประสิทธิภาพมากกว่ามาตรฐานขั้นพื้นฐาน โดยมาตรฐานขั้นสูงนี้จะมีความเหมาะสมกับ สอท./สกญ. ขนาดใหญ่ที่มีความพร้อมหรือมีโอกาสหรือความเสี่ยงต่อการถูกโจมตี หรือมีการรั่วไหลของข้อมูลสูง

เมื่อดำเนินการจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศเป็นที่เรียบร้อยแล้ว จะได้มาตรฐานที่มีองค์ประกอบหลัก 3 ส่วน คือ (1) มาตรฐานโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน และขั้นสูง ซึ่งอยู่ในรูปของแผนผัง (diagram) (2) มาตรฐานหมายเลข IP Address สำหรับเครือข่ายภายในของ สอท./สกญ. ทุกแห่ง (3) คุณลักษณะเฉพาะของอุปกรณ์หรือระบบรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับอุปกรณ์ไฟร์วอลล์ อุปกรณ์ IPS และโปรแกรมป้องกันไวรัส เป็นต้น

ดังนั้น การสร้างมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ สอท./สกญ. ให้สำเร็จได้นั้น จำเป็นต้องได้รับการสนับสนุนทางด้านนโยบายจากผู้บริหารของกระทรวงฯ เป็นอย่างยิ่ง เพื่อให้เกิดการดำเนินการอย่างเป็นรูปธรรมโดยเร็ว อีกทั้งต้องได้รับความร่วมมือจาก สอท./สกญ. ทุกแห่งและผู้เกี่ยวข้องเช่นกัน นอกจากนี้จะต้องดำเนินการฝึกอบรมให้ความรู้เกี่ยวกับมาตรฐานดังกล่าวให้แก่ข้าราชการที่จะออกประจำการให้เกิดความรู้ความเข้าใจ เพื่อจักได้นำไปเป็นแนวทางในการพัฒนาปรับปรุงและดูแลระบบได้อย่างมีประสิทธิภาพ สิ่งสำคัญอีกอย่างของการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศก็เพื่อเตรียมความพร้อมด้านโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้รองรับกับการพัฒนาไปสู่การเป็นรัฐบาลดิจิทัลต่อไป

กิตติกรรมประกาศ

รายงานการศึกษาส่วนบุคคลฉบับนี้ สำเร็จลงด้วยดีจากการที่ผู้เขียนได้รับโอกาสและได้รับการสนับสนุน อีกทั้งได้รับคำปรึกษาแนะนำจากผู้ทรงคุณวุฒิทั้งหลาย โอกาสนี้ ผู้เขียนขอขอบพระคุณท่านอาจารย์ที่ปรึกษารายงานส่วนบุคคลทั้ง 3 ท่าน คือ ท่านเอกอัครราชทูตกิตติพงษ์ ณ ระนอง ศ.ดร. พลภัทร บุราคม และ รศ.ดร. รุ่งพงษ์ ชัยนาม ที่กรุณาให้คำปรึกษา ชี้แนะแนวทาง ให้ข้อคิดเห็นในประเด็นต่าง ๆ ซึ่งเป็นประโยชน์ต่อการจัดทำรายงานให้สำเร็จลุล่วงสมบูรณ์เป็นอย่างยิ่ง

ผู้เขียนขอขอบพระคุณผู้บังคับบัญชา คือ นายนิกรเดช พลางกูร เอกอัครราชทูตประจำกระทรวง และนางสาวสุรีย์ ไตรรัตนนุกูล ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการต่างประเทศ ที่ได้ให้โอกาสผู้เขียนในการเข้ารับการฝึกอบรมหลักสูตรนักบริหารการทูต (นบท.) รุ่นที่ 12 และขอขอบพระคุณผู้บริหารกระทรวงฯ เป็นอย่างสูง ที่เปิดโอกาสให้ผู้เขียนได้รับการพิจารณาเข้ารับการฝึกอบรมในหลักสูตรนี้ และขอขอบคุณเพื่อนข้าราชการนายช่างไฟฟ้าทุกท่านเป็นอย่างยิ่งสำหรับข้อมูลที่ได้จากการสัมภาษณ์ และขอบคุณทีมงานส่วนความมั่นคงปลอดภัยไซเบอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่ช่วยกันปฏิบัติงานของส่วนฯ ตามที่ได้รับมอบหมายเป็นไปด้วยความเรียบร้อยตลอดระยะเวลาที่ผู้เขียนรับการฝึกอบรมนี้

ทั้งนี้ ผู้เขียนขอขอบคุณสถาบันเทวะวงศ์วโรปการที่จัดฝึกอบรมหลักสูตร นบท. นี้ ซึ่งถือว่าเป็นประโยชน์อย่างยิ่งต่อการนำไปใช้ปฏิบัติงานให้เกิดประสิทธิภาพและเกิดผลสัมฤทธิ์ต่อกระทรวงการต่างประเทศต่อไป และขอขอบคุณผู้เข้าร่วมการฝึกอบรมหลักสูตร นบท. รุ่นที่ 12 ทุกท่านที่มอบมิตรไมตรีจิตและกำลังใจให้กันและกันตลอดมา

ชูเกียรติ ประเสริฐสุข
กันยายน 2563

สารบัญ

สารบัญตาราง

สารบัญภาพ

บทที่ 1
บทนำ

1.1 ภูมิหลังและความสำคัญของปัญหา

ปัจจุบันโครงสร้างพื้นฐานทางด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถานเอกอัครราชทูตและสถานกงสุลใหญ่ (สอท./สกญ.) แต่ละแห่งนั้น มีความหลากหลายและความพร้อมที่แตกต่างกัน ไม่ว่าจะเป็นจำนวนเครื่องคอมพิวเตอร์และอุปกรณ์ ความเร็วของอินเทอร์เน็ต ระบบรักษาความปลอดภัยทางกายภาพ และอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ นอกจากนี้ แต่ละ สอท./สกญ. ยังมีระดับความสำคัญและความอ่อนไหวของข้อมูล รวมถึงระบบการให้บริการที่แตกต่างกัน

ความหลากหลายเหล่านี้ ส่งผลให้เกิดข้อจำกัดในการควบคุมดูแลระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีประสิทธิภาพ และนำไปสู่การเกิดช่องโหว่งในระบบ ทำให้ สอท./สกญ. บางแห่งประสบปัญหาจากการละเมิดความมั่นคงปลอดภัยทางไซเบอร์ (security breach) ในช่วง 2–3 ปีที่ผ่านมา ภัยคุกคามดังกล่าวได้ก่อให้เกิดความเสียหายอย่างมาก โดยส่งผลกระทบต่อข้อมูลซึ่งถือเป็นสินทรัพย์ที่สำคัญที่สุดขององค์กร รวมถึงความไม่พร้อมใช้งานของระบบเว็บไซต์ และระบบสารสนเทศอื่น ๆ เป็นต้น

กระทรวงการต่างประเทศมีมาตรการให้ความสำคัญกับการรักษาความปลอดภัยของข้อมูลเพื่อป้องกันการรั่วไหลของข้อมูลราชการและการถูกบุกรุกโจมตีจากภัยคุกคามทางไซเบอร์ ดังนั้นจึงมีแนวคิดที่จะจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ สอท./สกญ. อันเป็นหลักสำคัญในการวางรากฐานการพัฒนาและการบูรณาการระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ทั่วโลก ให้มีมาตรฐานและมีประสิทธิภาพ

สำหรับการจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสถานเอกอัครราชทูตและสถานกงสุลใหญ่ นั้น ได้มีแนวคิดจัดทำมาตรฐานใน 2 ระดับ ได้แก่ มาตรฐานขั้นพื้นฐาน และมาตรฐานขั้นสูง

มาตรฐานขั้นพื้นฐานเป็นมาตรฐานความมั่นคงปลอดภัยไซเบอร์ที่ทุก สอท./สกญ. ทั่วโลกจำเป็นต้องปฏิบัติตาม เพื่อเป็นการเสริมสร้างความเข้มแข็งทางด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในภาพรวมให้เกิดความปลอดภัย (Security) มีความยั่งยืน (Sustainability) และมีมาตรฐานสากล (Standard) ส่วนมาตรฐานขั้นสูงเป็นมาตรฐานที่แนะนำให้ สอท./สกญ. บางแห่งที่มีระบบและข้อมูลที่มีความสำคัญและมีความอ่อนไหวสูงนำไปใช้ป้องกันให้มีความมั่นคงปลอดภัย

ที่สูงขึ้น อย่างไรก็ตามด้วยเหตุแห่งปัจจัยอื่นอย่างเช่น งบประมาณ การดูแลรักษา ความซับซ้อนของโครงสร้างพื้นฐานทางเทคโนโลยีภายใน การให้บริการ และปัญหาทางเทคนิค เป็นต้น ซึ่งสิ่งเหล่านี้ถือเป็นข้อจำกัดและอุปสรรคในการดำเนินการตามมาตรฐานขั้นสูง ในขณะที่มาตรฐานขั้นพื้นฐานก็เพียงพอต่อความจำเป็นด้านความมั่นคงปลอดภัยทางไซเบอร์ในระดับหนึ่ง

1.2 วัตถุประสงค์ของการศึกษา

1.2.1 เพื่อศึกษาสถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ทั่วโลก

1.2.2 เพื่อกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ทางด้านโครงสร้างพื้นฐานระบบฯ, หมายเลข IP Address ภายใน และคุณลักษณะเฉพาะของอุปกรณ์/ระบบป้องกันภัยคุกคามไซเบอร์

1.2.3 เพื่อกำหนดเกณฑ์การใช้มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์

1.3 ขอบเขตการศึกษา วิธีการดำเนินการศึกษา และระเบียบวิธีการศึกษา

1.3.1 ขอบเขตการศึกษา

รวบรวมข้อมูลสถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งได้สำรวจจาก สอท./สกญ. ก่อนหน้านี้ จากการสัมภาษณ์ และศึกษาค้นหาข้อมูลเพิ่มเติมเพื่อมาประมวลวิเคราะห์ พร้อมกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน และขั้นสูง โดยดำเนินการออกแบบโครงสร้างพื้นฐานของระบบในรูปแบบ Network Security Diagram[1] อีกทั้งมีการจัดทำตารางหมายเลข IP Address เพื่อเป็นมาตรฐานระบบเครือข่ายของแต่ละสำนักงาน พร้อมจัดทำคุณลักษณะเฉพาะของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ โดยการศึกษานี้จะใช้ระยะเวลาระหว่างเดือนกรกฎาคม–กันยายน พ.ศ. 2563

1.3.2 วิธีการดำเนินการศึกษา และระเบียบวิธีการศึกษา

1.3.2.1 จัดเก็บรวบรวมข้อมูลปฐมภูมิ (Primary Data) จากการสำรวจ การสัมภาษณ์เจ้าหน้าที่ที่เคยออกประจำการบางท่าน ข้อมูลจากโทรเลขที่ สอท./สกญ. บางแห่งรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้น และจากการสังเกตการณ์ด้วยตนเอง

1) ข้อมูลการสำรวจระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ทุกแห่งทั่วโลก

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการสำรวจความพร้อมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. แต่ละแห่ง โดยทำการสำรวจว่า

[1] Network Security Diagram หมายถึง แผนผังการเชื่อมต่อระบบเครือข่ายที่มีอุปกรณ์หรือระบบป้องกันภัยคุกคามทางไซเบอร์สำหรับควบคุมการเข้าถึงและป้องกันการบุกรุกโจมตีเครือข่ายและสารสนเทศของหน่วยงาน

สอท./สกญ. แต่ละแห่งมีอุปกรณ์ไฟร์วอลล์, ระบบ IPS, โปรแกรมป้องกันไวรัส และระบบป้องกันอื่นหรือไม่อย่างไรตามโทรเลข[2] ที่ 0203/ว.475/2562 ลว. 6 มิถุนายน 2562 ก็เพื่อศึกษาดูความพร้อมและความต้องการแต่ละแห่ง ซึ่งการสำรวจที่ผ่านมาพบว่ามี สอท./สกญ. แจ้งผลสำรวจเข้ามาเพียง 34 แห่ง จาก 97 แห่งทั่วโลก คิดเป็นร้อยละ 35.05 ของกลุ่มเป้าหมาย ซึ่งเป็นกลุ่มตัวอย่างค่อนข้างน้อยและให้ข้อมูลบางอย่างไม่ถูกต้อง จึงส่งผลต่อคุณภาพของข้อมูลที่อาจไม่สะท้อนความเป็นจริงในภาพรวมได้ และถือเป็นข้อจำกัดหรืออุปสรรคในการเก็บรวบรวมข้อมูลให้มีความครบถ้วนถูกต้องได้

2) ข้อมูลจากการสัมภาษณ์เจ้าหน้าที่นายช่างไฟฟ้าชำนาญงาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการต่างประเทศ เมื่อวันที่ 13 กรกฎาคม 2563

เป็นข้อมูลที่ได้จากการสัมภาษณ์ข้าราชการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารในตำแหน่ง นายช่างไฟฟ้าชำนาญงาน จำนวน 6 ท่าน ซึ่งเคยออกประจำการในหลายประเทศและหลายภูมิภาค อีกทั้งมีความรู้ทางด้านไอทีและทราบรายละเอียดในด้านต่าง ๆ ของ สอท./สกญ. เป็นอย่างดี จึงทำให้ข้อมูลที่ได้รับมีคุณภาพและความน่าเชื่อถือสูงอันจะเป็นประโยชน์ต่อการกำหนดมาตรฐาน และออกแบบโครงสร้างระบบได้อย่างถูกต้องและเหมาะสมเป็นอย่างมาก

3) ข้อมูลจากการรายงานภัยคุกคามไซเบอร์ที่เกิดกับ สอท./สกญ. บางแห่ง

เป็นข้อมูลที่ได้รับจาก สอท./สกญ. โดยตรง ซึ่งบางแห่งจะรายงานเหตุการณ์การถูกโจมตีทางไซเบอร์มายังกระทรวงฯ โดยข้อมูลดังกล่าวจะมีประโยชน์ต่อการศึกษาแนวทาง และลักษณะการโจมตีทางไซเบอร์ที่เคยเกิดขึ้น เพื่อนำไปเป็นกรณีศึกษาสำหรับจัดทำมาตรฐาน และออกแบบโครงสร้างพื้นฐานของระบบต่อไป

4) ข้อมูลจากการสังเกตและจากการศึกษา

ข้อมูลปฐมภูมิอีกแหล่งหนึ่งก็คือจากการที่ผู้เขียนรายงานได้เคยไปศึกษาดูงานและไปให้การสนับสนุนงานของ สอท./สกญ. ในบางโอกาสนั้น ก็สังเกตเห็นสภาพแวดล้อมเครื่องคอมพิวเตอร์และอุปกรณ์ที่ใช้ ระบบงานสนับสนุนภายใน การให้บริษัทท้องถิ่นเข้ามาดูแลระบบและโดยเฉพาะอย่างยิ่งระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละแห่ง ปัญหาการรั่วไหลของข้อมูล ปัญหาการใช้งานอินเทอร์เน็ตและ Wi–Fi และปัญหาไวรัส เป็นต้น ซึ่งข้อมูลเหล่านี้ก็จะได้นำมาประกอบการพิจารณากำหนดเกณฑ์มาตรฐานด้วยเช่นกัน

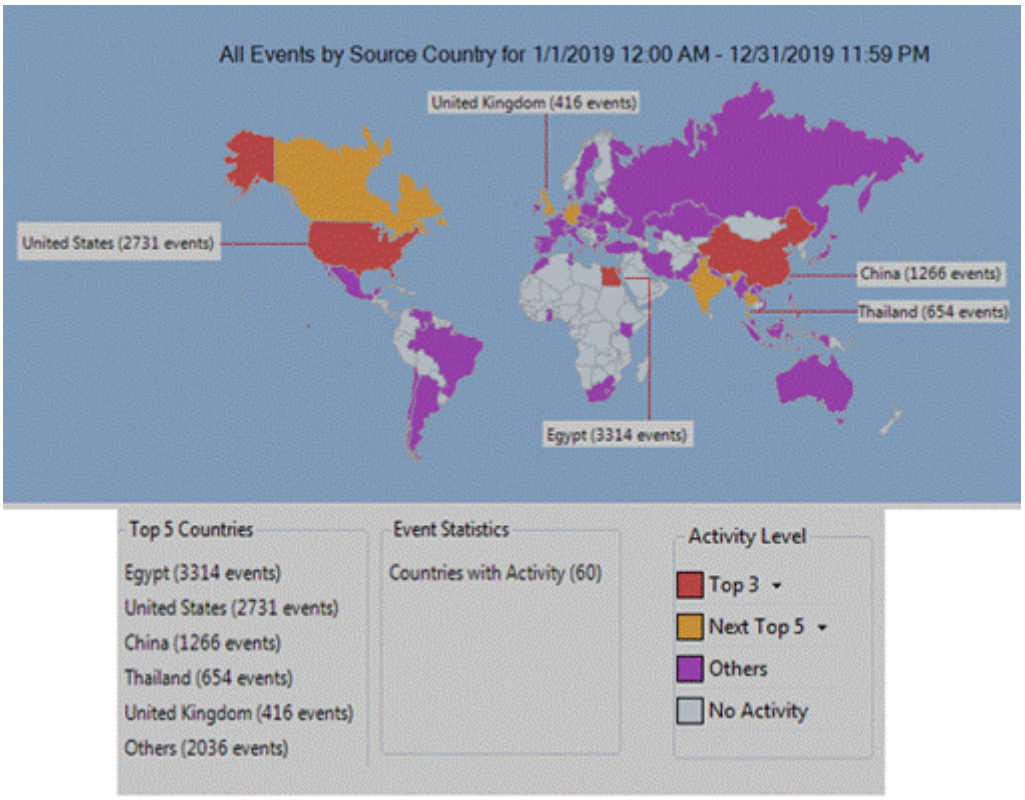
1.3.2.2 เนื่องด้วยข้อจำกัดในการรวบรวมข้อมูลภัยคุกคามที่เกิดขึ้นกับ สอท./สกญ. ทั่วโลกในภาพรวม ดังนั้น การเก็บรวบรวมข้อมูลทุติยภูมิ (Secondary Data) จากสถิติภัยคุกคามที่เกิดขึ้นทั้งในระดับองค์กร ระดับประเทศ และระดับโลก จึงมีความสำคัญในการวิเคราะห์แนวโน้มของ

---

[2] โทรเลข คือ หนังสือประสานงานประเภทหนึ่งนอกจากบันทึกข้อความที่กระทรวงฯ ใช้ติดต่อประสานงานเป็นการภายในระหว่าง กระทรวงฯ กับ สอท./สกญ. ทั่วโลก

ภัยคุกคามที่อาจเกิดขึ้น เพื่อกำหนดมาตรฐานและออกแบบโครงสร้างพื้นฐานของระบบให้มีความสอดคล้องกับสถานการณ์อย่างมีประสิทธิผล ดังสถิติภัยคุกคามที่เกิดขึ้นต่อไปนี้

1) สถิติภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงการต่างประเทศ ในปี พ.ศ. 2562 ซึ่งระบบไฟร์วอลล์ได้ตรวจพบการโจมตีทั้งหมด 475,056 ครั้ง โดยเป็นภัยคุกคามในระดับ critical จำนวน 149,715 ครั้ง ระดับสูง จำนวน 128,715 ครั้ง เป็นต้น สำหรับประเทศต้นทาง 5 อันดับสูงสุดที่โจมตีเข้ามาที่ระบบเครือข่ายสารสนเทศของกระทรวงฯ คือ จากประเทศอียิปต์ (3,314 เหตุการณ์) สหรัฐอเมริกา (2,731 เหตุการณ์) จีน (1,266 เหตุการณ์) ประเทศไทย (654 เหตุการณ์) และอังกฤษ (416 เหตุการณ์) ดังแสดงในภาพที่ 1



ภาพที่ 1 ประเทศต้นทางที่โจมตีเข้ามาที่กระทรวงฯ มากที่สุด 5 อันดับแรก

2) สถิติภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารในประเทศไทย ประจำปี พ.ศ. 2562 ตามที่หน่วยงานไทยเซิร์ตได้รับแจ้งโดย eCSIRT[3] ดังภาพต่อไปนี้

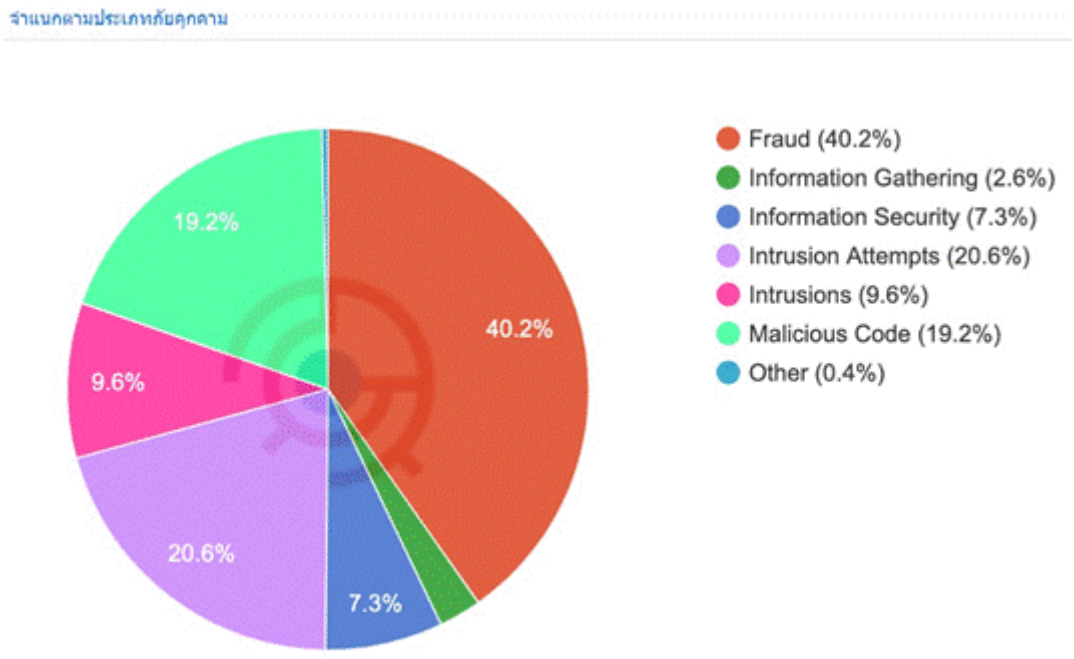
[3] eCSIRT หรือ The European Computer Security Incident Response Team ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรป

สถิติภัยคุกคาม ประจำปี พ.ศ. 2562

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive content	0	0	1	6	98	7	5	2	2	1	1	1	**124**
Availability	0	0	0	0	0	0	0	21	29	8	17	4	**79**
Fraud	87	46	59	60	84	53	128	69	86	93	88	59	**912**
Information gathering	0	0	0	0	0	0	0	40	4	3	10	3	**60**
Information security	39	0	0	3	40	1	45	22	11	0	1	3	**165**
Intrusion Attempts	78	90	62	33	24	43	84	22	9	4	11	7	**467**
Intrusions	12	10	24	13	34	12	6	46	39	9	5	8	**218**
Malicious code	20	8	13	7	6	7	16	88	51	46	84	90	**436**
Other	0	0	0	3	0	0	0	0	5	1	0	0	**9**
รวม	**236**	**154**	**159**	**125**	**286**	**123**	**284**	**310**	**236**	**165**	**217**	**175**	**2470**

ภาพที่ 2 สถิติภัยคุกคามประจำปี พ.ศ. 2562

ที่มา: https://www.thaicert.or.th/statistics/statistics2019.html



ภาพที่ 3 สถิติภัยคุกคามประจำปี พ.ศ. 2562 แยกตามประเภทภัยคุกคาม

ที่มา: https://www.thaicert.or.th/statistics/statistics2019.html

จากกราฟจะเห็นได้ว่าภัยคุกคามที่ทางไทยเซิร์ตได้รับแจ้งนั้น ส่วนใหญ่จะเป็นภัยคุกคามด้านการฉ้อฉล จำนวน 40.2% ด้านพยายามจะบุกรุกเข้าสู่ระบบ จำนวน 20.6% ด้านโปรแกรมไม่พึงประสงค์ จำนวน 19.2% และด้านบุกรุกระบบ จำนวน 9.6%

3) สถิติภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารทั่วโลก

จากรายงาน Check Point Software Security Report 2020[4] ในปี พ.ศ. 2562 ได้รายงานสถิติภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารทั่วโลก ดังนี้

	Cryto Miners	Botnet	Mobile	Banking	Infostealer	Ransomware
Global	38%	28%	27%	18%	18%	7%
APAC	47%	30%	34%	20%	18%	8%
Americas	33%	22%	24%	14%	13%	5%
Europe, Middle East, and Africa	38%	23%	26%	15%	15%	7%

ภาพที่ 4 สถิติภัยคุกคามทางด้านเทคโนโลยีสารสนเทศและการสื่อสารทั่วโลก ปี พ.ศ. 2562

ภัยคุกคามทางไซเบอร์รูปแบบดังกล่าวโจมตีผ่านทางช่องทางต่าง ๆ โดยเฉพาะอีเมล และเว็บไซต์ หากนำทั้งสองช่องทางมาเปรียบเทียบแล้ว Check Point ได้สรุปว่ามีการโจมตีผ่านทาง email มากถึง 68% ขณะที่มีการโจมตีทางเว็บไซต์อยู่ที่ 32% ตามข้อมูลการโจมตีทางไซเบอร์ที่ได้รับการรวบรวมโดย Check Point Software พบว่ามีบัญชีชื่ออีเมล จำนวน 770 ล้านบัญชี และรหัสเข้าใช้งานอีเมลถูกเปิดเผยถึง 21 ล้านบัญชี ในเดือนมกราคม ปี พ.ศ. 2562

สอดคล้องกับ แดน วิลลี่ย์ ผู้เชี่ยวชาญ และหัวหน้าการตอบสนองสถานการณ์ภัยคุกคามทางไซเบอร์ของ บริษัท Check Point Software กล่าวว่าอีเมล์เป็นช่องทางที่ถูกโจมตีทางไซเบอร์มากที่สุดเป็นอันดับหนึ่ง การโจมตีจะมุ่งเป้าหมายที่โจรกรรมข้อมูลส่วนบุคคล ข้อมูลการเข้ารหัส และธุรกรรมทางการเงิน

1.3.2.3 ทำการวิเคราะห์ข้อมูลดังกล่าวข้างต้นเพื่อมาใช้ออกแบบโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานและขั้นสูงสำหรับ สอท./สกญ.

[4] รายงานด้านภัยคุกคามประจำปีพ.ศ. 2563 ของบริษัท Check Point Software Technologies Ltd. หนึ่งในผู้ให้บริการระบบรักษาความปลอดภัยรายใหญ่ระดับโลก

1.3.2.4 จัดทำตารางหมายเลข IP Address มาตรฐานสำหรับ สอท./สกญ. ทั้ง 97 แห่งทั่วโลก

1.3.2.5 กำหนดคุณลักษณะเฉพาะของระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามมาตรฐานที่กำหนด

1.3.2.6 นำผลการดำเนินการข้างต้นมาจัดทำเป็นมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานและขั้นสูงสำหรับ สอท./สกญ.

1.3.2.7 เผยแพร่มาตรฐานดังกล่าวเมื่อได้รับความเห็นชอบจากกระทรวงฯ เพื่อใช้เป็นแนวทางปฏิบัติในการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้ดียิ่งขึ้นที่มีมาตรฐานต่อไป

1.3.2.8 ติดตามผลการดำเนินการของ สอท./สกญ. ว่าได้ดำเนินการตามมาตรฐานที่กำหนดไว้หรือไม่อย่างไร โดยทำเป็น checklist ให้ตรวจสอบแล้วแจ้งผลกลับมายังกระทรวงฯ ทราบ สำหรับกรณีที่ไม่สามารถดำเนินการให้เป็นไปตามมาตรฐานที่กำหนดได้ ทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะหาแนวทางให้การสนับสนุนหรือความช่วยเหลือต่อไป

1.4 คำถามการศึกษา

จะสร้างมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับสถานเอกอัครราชทูตและสถานกงสุลใหญ่อย่างไร

1.5 สมมติฐานการศึกษา

การออกแบบมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ สอท./สกญ. จะทำให้เกิดความมั่นคงปลอดภัยไซเบอร์มากยิ่งขึ้น

1.6 ประโยชน์ของการศึกษา

1.6.1 กระทรวงฯ กำหนดเป็นนโยบายให้ สอท./สกญ. ทุกแห่งนำมาตรฐานดังกล่าวไปพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นแนวทางเดียวกัน

1.6.2 สอท./สกญ. มีแนวทางในการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปตามกรอบมาตรฐานเดียวกันทั่วโลก

1.6.3 มีการแบ่งแยกระบบเครือข่ายของ สอท./สกญ. ให้เกิดความมั่นคงปลอดภัยมากยิ่งขึ้น

1.6.4 สอท./สกญ. จะนำมาตรฐานดังกล่าวนี้ไปใช้ในการพัฒนาปรับปรุงได้อย่างมีประสิทธิภาพ

1.6.5 สอท./สกญ. สามารถกำหนดคุณลักษณะเฉพาะสำหรับกระบวนการจัดซื้อจัดจ้างได้สอดคล้องตามมาตรฐานที่กำหนดได้

1.6.6 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สามารถให้การสนับสนุน ให้คำปรึกษา แนะนำ และแก้ปัญหาทางเทคนิคได้อย่างมีประสิทธิภาพมากขึ้น เมื่อสำนักงานแต่ละแห่งได้ดำเนินการตามมาตรฐานที่กำหนด

1.7 นิยามศัพท์

กระทรวงฯ หมายถึง กระทรวงการต่างประเทศ

สำนักงานในต่างประเทศ หมายถึง สถานเอกอัครราชทูต/สถานกงสุลใหญ่/สำนักงานการค้าและเศรษฐกิจไทย (ไทเป) ซึ่งรวมถึงหน่วยงานทีมไทยแลนด์ที่อยู่ภายใต้อาคารเดียวกัน และมีการใช้ทรัพยาการทางเทคโนโลยีสารสนเทศและการสื่อสารภายใต้ระบบเครือข่ายร่วมกัน

เจ้าหน้าที่ หมายถึง ข้าราชการและพนักงานของสถานเอกอัครราชทูต/ สถานกงสุลใหญ่และสำนักงานการค้าและเศรษฐกิจไทย (ไทเป)

โครงสร้างพื้นฐานสำคัญของประเทศ หมายความว่า บรรดาหน่วยงานหรือองค์กรหรือส่วนงานหนึ่งส่วนงานใดของหน่วยงานหรือองค์กร ซึ่งธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานหรือองค์กรหรือส่วนงานของหน่วยงานหรือองค์กรนั้น มีผลเกี่ยวเนื่องสำคัญต่อความมั่นคงหรือความสงบเรียบร้อยของประเทศหรือต่อสาธารณชน

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายความว่า คอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

ภัยคุกคามทางไซเบอร์ หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ระบบเครือข่าย หมายถึง การนำเครื่องคอมพิวเตอร์มาเชื่อมต่อกันโดยใช้สื่อกลางเพื่อให้เกิดการติดต่อสื่อสารแลกเปลี่ยนข้อมูล และใช้อุปกรณ์ในเครือข่ายร่วมกันได้อย่างมีประสิทธิภาพ

โครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ รวมถึงการออกแบบโครงสร้างระบบเครือข่ายภายในของหน่วยงาน และกระบวนการดำเนินการในวิธีการที่ปลอดภัย

บทที่ 2
แนวคิดทฤษฎีและวรรณกรรมที่เกี่ยวข้อง

กระทรวงการต่างประเทศถือเป็นส่วนราชการที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) ตามประกาศคณะกรรมการธุรกรรมอิเล็กทรอนิกส์เรื่องรายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็นโครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559 ดังนั้นสำนักงานในต่างประเทศทุกแห่งที่เป็นหน่วยงานของกระทรวงฯ จึงจำเป็นต้องปกป้องรับมือกับภัยคุกคามทางไซเบอร์ที่นับวันจะทวีความรุนแรงและส่งผลกระทบจนอาจสร้างความเสียหายอย่างมากได้

การจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศหรือสถานเอกอัครราชทูตและสถานกงสุลใหญ่ นั้น จำเป็นต้องศึกษาค้นหาข้อมูลในประเด็นที่เกี่ยวข้องเพื่อใช้เป็นกรอบแนวทางในการดำเนินการจัดทำมาตรฐานดังกล่าว โดยมีรายละเอียดการศึกษาดังต่อไปนี้

2.1 แนวคิดทฤษฎี

2.1.1 หลักการพื้นฐาน 3 ประการสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูล (CIA Triad)

วัตถุประสงค์หลักในการสร้างศักยภาพในการป้องกันภัยคุกคามทางไซเบอร์ คือ เพื่อป้องกัน รักษาสภาพ และคงความพร้อมใช้งานของข้อมูลและระบบในองค์กร หากระบบรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพดังกล่าวแล้ว องค์กรนั้น ๆ ก็จะมีความมั่นคงปลอดภัย ลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นกับข้อมูลสารสนเทศขององค์กรได้

หลักการพื้นฐาน 3 ประการในการรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) ประกอบด้วย Confidentiality, Integrity และ Availability หรือที่เรียกว่า CIA Triad โดยหลักการพื้นฐานนี้บางครั้งก็เรียกว่า Information Security Requirement ซึ่งการจะทำให้บรรลุวัตถุประสงค์ทางด้านนี้นั้น อาจต้องใช้ security mechanism ต่าง ๆ อย่างเช่น การควบคุมการเข้าถึง (access control) การเข้ารหัส (encryption) การมีระบบ backup site เป็นต้น สำหรับรายละเอียดของหลักการพื้นฐาน 3 ประการ ดังภาพที่ 5

ภาพที่ 5 CIA Triad

ที่มา : https://www.dga.or.th/upload/download/

1) การรักษาความลับ (Confidentiality) เพื่อเป็นการป้องกันข้อมูลสารสนเทศมิให้ถูกเปิดเผย หรือเข้าถึงโดยมิได้รับอนุญาต ซึ่งจะมีการนำมาตรการควบคุมการเข้าถึง (access control) มาใช้ป้องกัน

2) การรักษาความครบถ้วนถูกต้อง (Integrity) เพื่อเป็นการรักษาสภาพของข้อมูลสารสนเทศให้มีความครบถ้วน ถูกต้อง มิทำให้สูญหาย เสียหาย เปลี่ยนแปลงแก้ไขหรือถูกทำลายโดยมิชอบ ซึ่งสามารถนำเรื่องการเข้ารหัสข้อมูล (encryption) มาสนับสนุนการป้องกันในเรื่องนี้

3) การรักษาสภาพความพร้อมใช้ (Availability) เพื่อให้สามารถเข้าถึงหรือเรียกใช้งานข้อมูลสารสนเทศได้อยู่เสมอ เช่น การมีระบบ Disaster Recovery Site เพื่อพร้อมทำงานทันทีหากระบบหลักไม่พร้อมให้บริการ อีกทั้งต้องมีการดูแลบำรุงรักษาระบบอยู่เป็นประจำ มีมาตรการในการป้องกันและแก้ไขปัญหาได้อย่างรวดเร็ว มีแผนสำรองเพื่อมิให้ระบบล่มเป็นระยะเวลานานเกินไป เป็นต้น

2.1.2 หลักดำเนินการที่สำคัญของการรักษาความมั่นคงปลอดภัย

การป้องกันถือเป็นกระบวนการรักษาความปลอดภัยขององค์กรเชิงรุกเพื่อบริหารความเสี่ยง ลดผลกระทบและความเสียหายที่อาจเกิดขึ้นได้ เพื่อเป็นการผ่อนหนักให้เป็นเบาเมื่อได้รับผลกระทบ โดยหลักการสำคัญของการดำเนินการรักษาความมั่นคงปลอดภัย มีอยู่ด้วยกัน 3 ประการ คือ การป้องกัน (protection) การตรวจจับ (detection) และการฟื้นสภาพ (recovery)

2.1.2.1 การป้องกัน (protection)

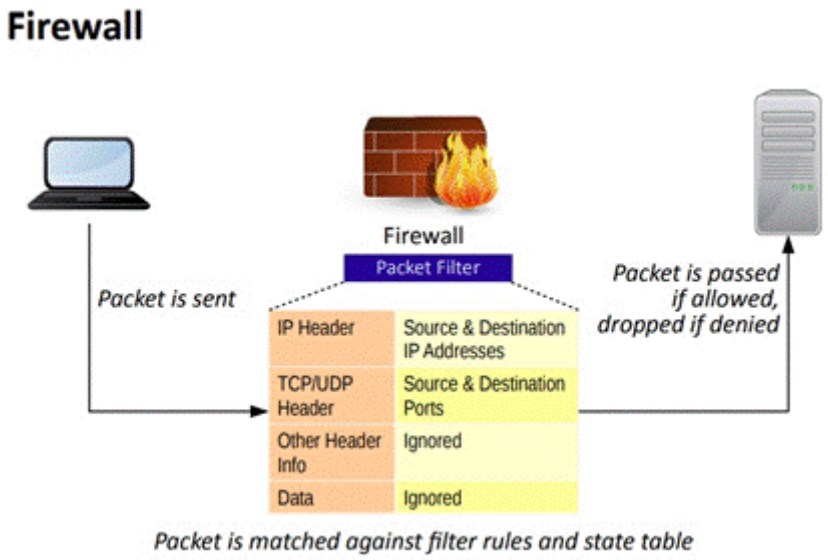
อุปกรณ์ระบบรักษาความมั่นคงปลอดภัยหลักที่ใช้ในการปกป้ององค์กรเพื่อป้องกันการบุกรุกโจมตีจากภัยคุกคามทางไซเบอร์นั้น ได้แก่ ไฟร์วอลล์ (Firewall) ระบบ IPS (Intrusion Prevention System) และระบบป้องกันไวรัส เป็นต้น

1) ไฟร์วอลล์ (Firewall)

ไฟร์วอลล์เป็นอุปกรณ์หรือระบบเพื่อควบคุมการเข้า–ออกระบบเครือข่าย ที่ควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศต่าง ๆ ขององค์กรให้มีความปลอดภัย ซึ่งใช้ป้องกันภัยคุกคามเข้าสู่ระบบเครือข่ายและสารสนเทศได้อย่างมีประสิทธิภาพ ไฟร์วอลล์สามารถแบ่งออกเป็นหลายประเภทตามลักษณะการทำงาน แต่สำหรับรายงานการศึกษาฉบับนี้จะมุ่งเน้นที่ระบบไฟล์วอลล์ที่ใช้กันอยู่ในยุคปัจจุบัน ซึ่งก็คือ Next Generation Firewall หรือที่เรียกว่า แอพพลิเคชั่นไฟร์วอลล์ (Application Firewall)

Application Firewall เป็นไฟร์วอลล์ที่ทำงานได้ในระดับ application ดังนั้นจึงมีความสามารถในการควบคุมการเข้าถึง การกำหนดกฎการใช้งาน (Rule Base Policy) เพื่อที่จะอนุญาตหรือไม่อนุญาตใครเข้าใช้ระบบเครือข่าย ระบบสารสนเทศ โปรแกรมหรือแอพพลิเคชั่นใดได้บ้างอย่างไร อีกทั้งสามารถตรวจสอบภัยคุกคามที่มาในรูปแบบของโปรแกรมหรือ application ได้ ดังนั้นจึงทำให้อุปกรณ์ไฟร์วอลล์ประเภทนี้มีความเข้มแข็งในการควบคุมการเข้าถึงที่มีการกรองการเชื่อมต่อทั้งขาเข้าและขาออกให้มีความปลอดภัย ซึ่งสามารถป้องกันการโจมตีระบบเครือข่ายและสารสนเทศได้ถึงระดับ application ได้อย่างมีประสิทธิภาพ ขณะเดียวกันภัยคุกคามไซเบอร์ส่วนใหญ่ที่พบในปัจจุบันนี้จะมีการบุกรุกโจมตีในระดับ application เป็นส่วนใหญ่ ดังนั้นการพิจารณาเลือกใช้ไฟร์วอลล์ประเภทนี้ให้กับองค์กรจึงเป็นสิ่งสำคัญต่อการรักษาความมั่นคงปลอดภัยเครือข่ายและสารสนเทศขององค์กรในปัจจุบันได้อย่างมีประสิทธิผล

สำหรับรูปแบบการทำงานของระบบไฟร์วอลล์โดยทั่วไป สามารถอธิบายได้ดังภาพที่ 6 ต่อไปนี้



ภาพที่ 6 การทำงานของไฟร์วอลล์

ที่มา : https://www.dga.or.th/upload/download/

จากภาพที่ 6 เมื่อต้องการติดต่อสื่อสารข้อมูลจากเครื่องคอมพิวเตอร์ต้นทาง (source IP address) มายังปลายทาง (destination IP address) เพื่อเข้ามาใช้บริการที่เครื่องเซิร์ฟเวอร์ อย่างเช่น เว็บไซต์ อีเมล VPN (Virtual Private Network) และ VoIP (Voice over IP) เป็นต้น โดยเครื่องคอมพิวเตอร์ต้นทางจะผ่านการตรวจสอบและคัดกรองจากระบบไฟร์วอลล์ก่อน โดยไฟร์วอลล์จะทำการตรวจสอบว่าการสื่อสารข้อมูลที่เข้ามานั้นเป็นไปตามกฎหรือ rule base firewall หรือ firewall policy หรือไม่ หากเข้ามาและเป็นไปตามกฎหรือ policy ที่กำหนดแล้ว ไฟร์วอลล์ก็จะอนุญาตให้เข้าใช้บริการเครื่องเซิร์ฟเวอร์ปลายทางนั้นได้ แต่หากไม่ตรงตามกฎหรือ policy ที่กำหนดไว้ ไฟร์วอลล์ก็จะไม่อนุญาตหรือทำการปฏิเสธการเข้าถึงนั้น ๆ ทันที เพื่อเป็นการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต หรือการเข้าใช้งานนอกเหนือจากที่ได้กำหนดไว้

2) โปรแกรมป้องกันไวรัสและมัลแวร์ (Antivirus and Malware)

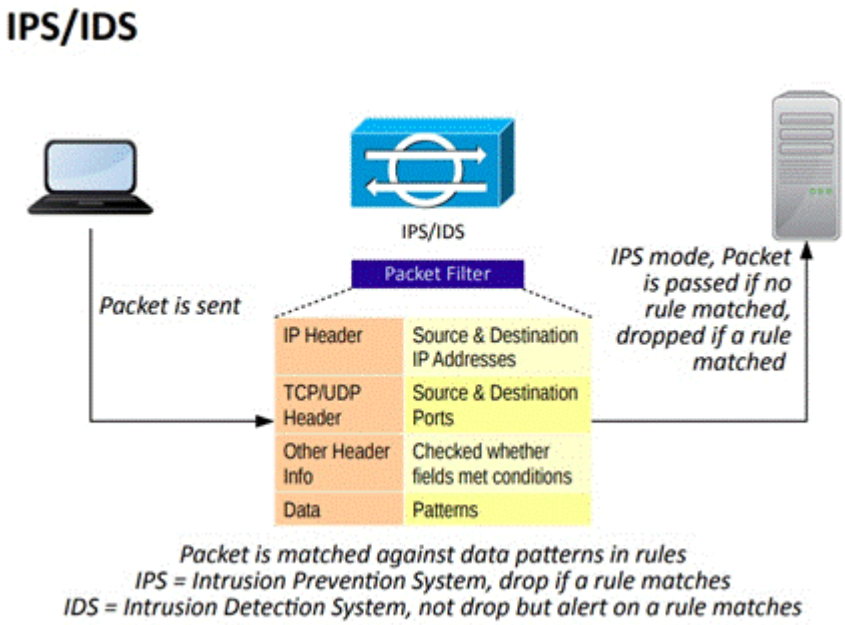
เครื่องคอมพิวเตอร์ลูกข่าย (clients) และเครื่องคอมพิวเตอร์เซิร์ฟเวอร์ (server) จำเป็นต้องมีโปรแกรมป้องกันไวรัสและมัลแวร์ที่มีประสิทธิภาพอย่างมาก เนื่องจากการโจมตีส่วนใหญ่จะเน้นการนำโปรแกรมประสงค์ร้ายเข้าสู่ระบบ หรือมีการฝัง backdoor ไว้ที่เครื่องเซิร์ฟเวอร์หรือเครื่อง clients เพื่อโจมตีหรือทำการบุกรุกต่อไปยังเครื่องอื่น และอาจสร้างความเสียหายจากการแพร่กระจายในวงกว้างได้ ดังนั้นโปรแกรมป้องกันภัยคุกคามที่เป็น endpoint security ที่มีความสามารถในลักษณะป้องกันภัยคุกคามเชิงลึกประเภท Zero Day Attack, APT (Advance Persistence Threat) และที่มีลักษณะการป้องกันแบบ Behavior–Based Protection

หรือใช้เทคโนโลยี Artificial Intelligence Antivirus (AI) ที่ทันสมัย ก็จะช่วยเสริมสร้างความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ลูกข่ายและเครื่องเซิร์ฟเวอร์ได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

2.1.2.2 การตรวจจับ (detection)

อุปกรณ์ระบบรักษาความมั่นคงปลอดภัยหลักที่ทำหน้าที่ตรวจจับและป้องกันการบุกรุกโจมตีจากภัยคุกคามทางไซเบอร์ที่สำคัญมากอีกระบบคือ ระบบ IPS และ IDS (Intrusion Prevention System)/ IDS (Intrusion Detection System)

IDS เป็นระบบที่ใช้ตรวจจับ เฝ้าระวังและแจ้งเตือนภัยคุกคามที่จะบุกรุก ซึ่งจะทำการแจ้งเตือนเหตุการณ์การเข้าใช้งานที่ผิดปกติ และส่วนใหญ่ไม่สามารถที่จะป้องกันการบุกรุกได้ ดังนั้นจึงได้มีระบบ IPS มาใช้ป้องกันการบุกรุกโจมตีจากภัยคุกคามเชิงลึกได้อย่างทันท่วงที ซึ่งระบบ IPS ในปัจจุบันนั้นมีประสิทธิภาพในการทำงานเป็นอย่างมากและสำคัญยิ่งต่อองค์กร นอกเหนือจากอุปกรณ์ไฟร์วอลล์ โดยอุปกรณ์ IPS ในปัจจุบันได้มีฟังก์ชั่นการทำงานของ IDS รวมอยู่ด้วยภายใต้ระบบเดียวกัน

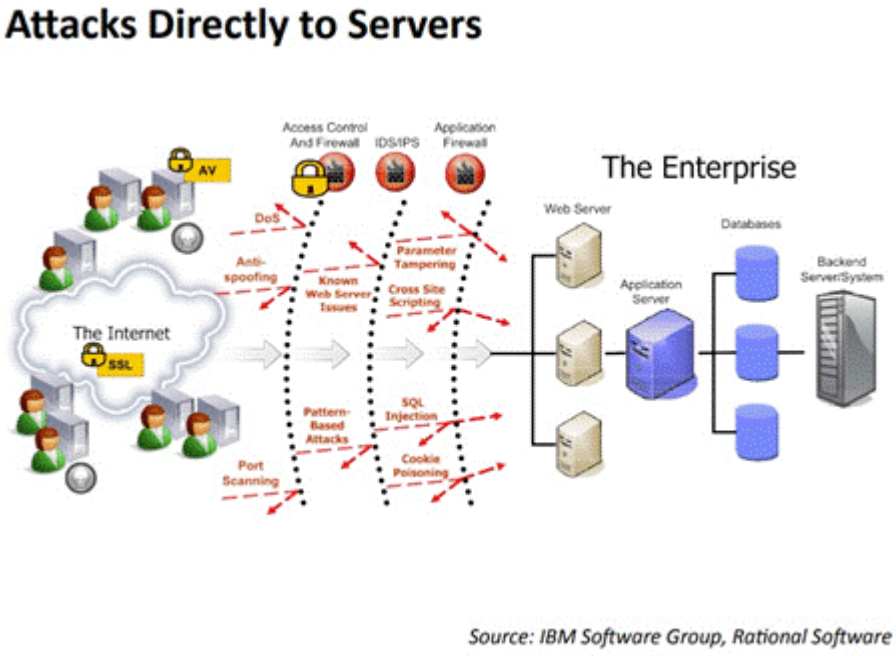


ภาพที่ 7 การทำงานของ IPS/IDS

ที่มา: https://www.dga.or.th/upload/download/

จากภาพที่ 7 เมื่อมีการติดต่อสื่อสารข้อมูลจากต้นทาง (source IP address) มายังเครื่องเซิร์ฟเวอร์ปลายทาง (destination IP address) เพื่อขอใช้บริการ อาทิ เว็บไซต์

อีเมล VPN (Virtual Private Network) หรือระบบอินทราเน็ตภายใน ก็จะต้องผ่านการคัดกรองจากระบบไฟร์วอลล์ก่อน จากนั้นก็จะผ่านการตรวจจับจาก IDS หากพบว่าเป็นภัยคุกคามก็จะทำการแจ้งเตือนและทำการป้องกันการบุกรุกโจมตีและหยุดยั้งด้วย IPS ทันที ซึ่งกระบวนการวิเคราะห์ การตรวจสอบภัยคุกคามและการโจมตีต่าง ๆ นั้น จะตรวจสอบจากฐานข้อมูลของระบบและจากพฤติกรรมของภัยคุกคามที่เกิดขึ้น หากเข้าข่ายเป็นภัยคุกคามต่อระบบเครือข่ายหรือสารสนเทศ ระบบ IPS ก็จะทำการหยุดหรือปฏิเสธการเข้าถึงเครื่องเซิร์ฟเวอร์ปลายทางทันที



ภาพที่ 8 การโจมตีผ่านระบบรักษาความมั่นคงปลอดภัย
ที่มา: https://www.dga.or.th/upload/download/

จากภาพที่ 8 เมื่อมีการเข้าใช้งานจากอินเทอร์เน็ตมาที่ web server ก็จะถูกระบบไฟร์วอลล์ในชั้นแรกควบคุมการเข้าถึงก่อน หากได้รับอนุญาตก็จะผ่านเข้ามาและถูกตรวจจับจากระบบ IDS/IPS อีกที ว่าเป็นลักษณะการใช้งานปกติหรือไม่อย่างไร หากมีการเข้าใช้งานผิดปกติหรือมีลักษณะการโจมตีระบบ IPS ก็จะทำการหยุดการเข้าถึงทันที แต่เมื่อตรวจสอบแล้วว่าเป็นปกติก็จะผ่านเข้ามาตรวจสอบที่ไฟร์วอลล์อีกชั้นหนึ่งซึ่งเป็น application firewall เมื่อตรวจสอบการเข้าถึงและการใช้งานในระดับ application แล้วปรากฏว่าไม่ใช่ภัยคุกคามและมีการเรียกใช้งานที่เป็นปกติตามที่กำหนดใน policy ของไฟร์วอลล์ ก็จะอนุญาตเข้าใช้งาน web server นั้นได้

2.1.2.3 การฟื้นสภาพ (recovery)

การฟื้นสภาพหรือการ recovery ระบบ ซึ่งเป็นสิ่งสำคัญต่อการกลับสู่สถานภาพการทำงานเดิมของระบบให้เป็นปกติและสามารถกลับมาทำงานหรือให้บริการได้ ดังนั้น การฟื้นสภาพจึงเป็นกระบวนการอย่างหนึ่งที่ต้องมีการวางแผนเพื่อลดผลกระทบความเสียหายที่อาจเกิดขึ้น และถือเป็นการบริหารความเสี่ยงอย่างหนึ่ง การฟื้นสภาพให้กับระบบรักษาความมั่นคงปลอดภัยไซเบอร์จะเกี่ยวข้องกับการ recovery ทั้งฮาร์ดแวร์ซอฟต์แวร์และการให้บริการที่เกี่ยวข้อง ทั้งในเรื่อง data recovery, network recovery, system recovery และอื่น ๆ เป็นต้น

2.1.3 การแบ่งแยกเครือข่าย (Segregation in Networks)

การแบ่งส่วนเครือข่าย (Network Segmentation) นับเป็นกลยุทธ์เชิงลึกเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กร เพื่อเป็นการปฏิบัติตามกฎระเบียบและวิธีการที่ปลอดภัย ลดพื้นที่การถูกโจมตี เป็นการแบ่งระบบเพื่อเพิ่มความพร้อมใช้งานของระบบต่าง ๆ และสามารถจำกัดการให้บริการของระบบได้ นอกจากนี้ก็สามารถควบคุมการเข้าถึงระบบเครือข่ายและสารสนเทศได้อย่างมีประสิทธิภาพ

สำหรับการทำ network segmentation โดยทั่วไปนั้น สามารถกำหนดเป็นโซน (zone) ได้หลากหลายโซน ทั้งนี้ก็ขึ้นอยู่กับโครงสร้างองค์กร และบริบทในการดำเนินงานขององค์กรนั้น ๆ ซึ่งโซนหลักทั่วไป ประกอบด้วย

1) External Zone

หมายถึงระบบเครือข่ายภายนอกซึ่งถือว่ามีความปลอดภัยต่ำอย่างเช่น เครือข่าย Internet

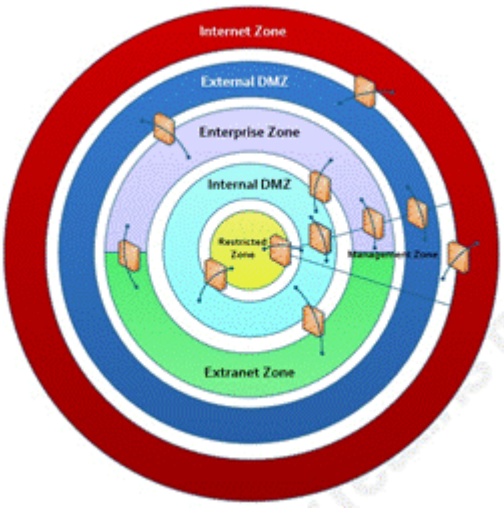
2) DMZ (Demilitarized Zone)

หมายถึงโซนสำหรับให้บริการสาธารณะ หรือที่เรียกว่า Public Zone เป็นโซนให้บริการเว็บไซต์ขององค์กรทั่วไป ซึ่งจะถูกควบคุมการเข้าถึงโดยไฟร์วอลล์ให้เป็นไปอย่างปลอดภัย

3) Internal Zone

หมายถึงโซนของระบบเครือข่ายภายใน ซึ่งถือว่ามีความน่าเชื่อถือและปลอดภัยสูงสุด และเป็นโซนสำหรับฐานข้อมูล, แอพพลิเคชั่นระบบ และเครื่องคอมพิวเตอร์ผู้ใช้งาน เป็นต้น

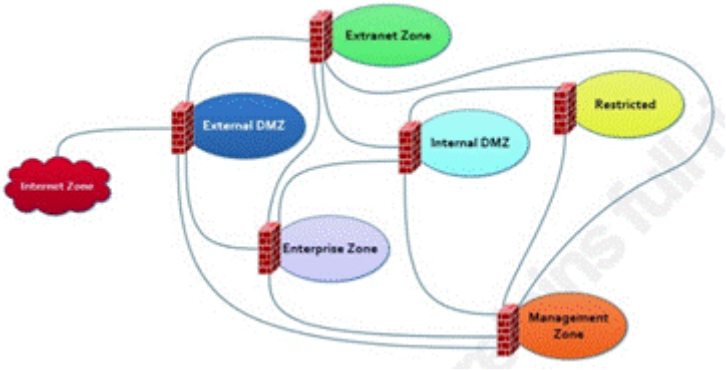
สำหรับหลักการในการแบ่งโซนที่ปลอดภัยนั้น จะมีการจัดแบ่งและมีการควบคุมการเข้าถึงระหว่างโซนด้วยอุปกรณ์ไฟร์วอลล์อย่างเข้มข้น เพื่อป้องกันข้อมูลสารสนเทศขององค์กรให้ปลอดภัยจากภัยคุกคามและความเสี่ยงที่อาจเกิดขึ้นได้ ดังสถาบัน SANS Institute ได้กำหนดหลักการแบ่งโซน ดังภาพที่ 9



ภาพที่ 9 Conceptual Zone Pattern

ที่มา : SANS Institute

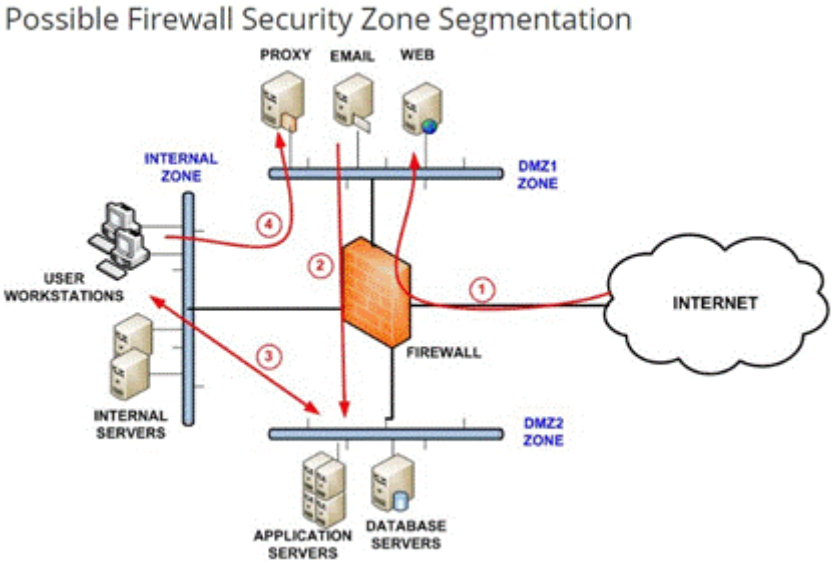
สำหรับการติดต่อสื่อสารระหว่างโซนต่าง ๆ นั้น สามารถแสดงได้ดังภาพที่ 10



ภาพที่ 10 Rules of Communication among Zone

ที่มา : SANS Institute

ท้ายที่สุดเมื่อได้ดำเนินการออกแบบโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์เรียบร้อยแล้ว จะมีรูปแบบการแบ่งส่วนเครือข่ายออกเป็นโซนต่าง ๆ ที่แต่ละโซนต้องผ่านการควบคุมการเข้าถึงจากไฟร์วอลล์ตามหลักการและทฤษฎี ดังภาพข้างล่างนี้



ภาพที่ 11 Security Zone Segmentation

ที่มา : https://www.arctitan.com/blog/best-practices-to-improve-security-network-segmentation/

2.2 วรรณกรรมที่เกี่ยวข้อง

2.2.1 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้มีการประกาศในราชกิจจานุเบกษา เมื่อวันที่ 27 พฤษภาคม 2562 และมีผลบังคับใช้ตั้งแต่วันที่ 28 พฤษภาคม 2562 โดยที่การจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ นั้น มีแนวความคิดการดำเนินงานให้สอดคล้องตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยเฉพาะหมวด 3 การรักษาความมั่นคงปลอดภัยไซเบอร์ ส่วนที่ 1 นโยบายและแผน มาตรา 41 และ 44 ที่มีหลักใจความสำคัญ ดังนี้

การรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความเป็นเอกภาพและการบูรณาการในการดำเนินงาน เพื่อสร้างศักยภาพในการป้องกันภัยคุกคามทางไซเบอร์ โดยหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

2.2.2 ภัยคุกคามทางไซเบอร์ (Cyber Threat)

ภัยคุกคามไซเบอร์มีหลายรูปแบบด้วยกันที่สามารถสร้างความเสียหายให้กับองค์กรได้ ซึ่งภัยคุกคามแต่ละประเภทก็จะมีการโจมตีในลักษณะที่แตกต่างกันไป หรือคล้าย ๆ กันก็มี อย่างไรก็ตาม ภัยคุกคามหลัก ๆ ที่พบส่วนใหญ่ อาทิเช่น

1) Malware เป็นซอฟต์แวร์อันตรายที่สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์เครื่องอื่นหรือไปยังระบบเครือข่ายอื่นได้อย่างรวดเร็ว โดยทำการแฝงตัวเข้ามาแล้วโจมตีจนอาจสร้างความเสียหายต่อระบบคอมพิวเตอร์ขององค์กร การรั่วไหลของข้อมูลทั้งส่วนบุคคลและขององค์กรได้

2) Phishing พบมากผ่านทางอีเมล หรือจากการใช้งานอินเทอร์เน็ต โดยจะทำการหลอกลวงให้เหยื่อหลงเชื่อแล้วทำการคลิกลิงค์ หรือหลอกให้ดาวน์โหลดไฟล์อันตรายประเภทมัลแวร์มาฝังไว้ที่เครื่องคอมพิวเตอร์ของเหยื่อเพื่อจารกรรมข้อมูล หรือใช้เป็นช่องทางโจมตีระบบอื่นต่อไป

3) SQL Injection เป็นการโจมตีไปยังฐานข้อมูลผ่านช่องโหว่ของระบบ และอาจสร้างความเสียหายได้อย่างมากหากเป็นข้อมูลที่สำคัญโดยเฉพาะอย่างยิ่งข้อมูลส่วนบุคคล และข้อมูลที่มีชั้นความลับ เป็นต้น

4) Cross–site Scripting (XSS) เป็นการโจมตีผ่านการเขียนโค้ดหรือฝังสคริปต์ไว้บนเว็บไซต์ที่มีช่องโหว่ โดยจะโจมตีเมื่อผู้ใช้เรียกใช้เว็บไซต์ นอกจากนี้แฮกเกอร์อาจทำการฝังมัลแวร์โทรจัน (Trojan) เพื่อจารกรรมข้อมูลออกไปในภายหลังได้

5) Denial of Service (DoS) เป็นการโจมตีในลักษณะที่ต้องการให้เครื่องเซิร์ฟเวอร์ไม่พร้อมให้บริการ โดยเป็นการโจมตีในลักษณะเสมือนมีการเข้าใช้บริการเว็บไซต์มากผิดปกติจนเกินกว่าเครื่องเซิร์ฟเวอร์จะรองรับได้ และในที่สุดเครื่องเซิร์ฟเวอร์ก็ไม่สามารถให้บริการได้

6) Man–in–the–Middle Attacks เป็นการโจมตีเพื่อสกัดดักจับข้อมูลระหว่างทางของการติดต่อสื่อสารกันระหว่างเครื่องคอมพิวเตอร์โดยที่เหยื่อไม่รู้ตัว

7) Brute Force Attack เป็นการโจมตีแบบสุ่มเดารหัสผ่าน โดยเฉพาะของผู้ดูแลระบบ ดังนั้นหากกำหนดรหัสผ่านที่คาดเดาได้ง่าย ก็อาจทำให้ผู้ไม่ประสงค์ดีเข้าทำการยึดครอง (Compromise) เครื่องเซิร์ฟเวอร์ หรือระบบที่ใช้งานได้

2.2.3 ประเภทของการโจมตี

การโจมตีทางไซเบอร์สามารถแบ่งออกได้เป็น 4 ประเภท คือ

1) การเปิดเผย (Disclosure) มีการเปิดเผยหรือเข้าถึงข้อมูลโดยมิได้รับอนุญาตหรือไม่มีสิทธิ์ในการเข้าถึง เช่นการ Sniffing แอบดูข้อมูล

2) การหลอกลวง (Deception) เป็นการปลอมแปลงหรือการให้ข้อมูลอันเป็นเท็จ

3) การขัดขวาง (Disruption) มีลักษณะขัดขวางไม่ให้กระทำต่อข้อมูลอย่างถูกต้อง

4) การควบคุมระบบ (Usurpation) เป็นการกระทำเพื่อควบคุมระบบบางส่วนหรือทั้งระบบโดยไม่ได้รับอนุญาต

2.2.4 แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 โดยมีสาระสำคัญที่เกี่ยวข้องกับการออกแบบโครงสร้างระบบเครือข่าย และการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนั้น หน่วยงานจำเป็นต้องมีแนวปฏิบัติ ดังนี้

1) การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

2) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (user authentication for external connection) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

3) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

4) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

5) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

6) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึง

7) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

2.2.5 การกำหนดมาตรฐาน

การประเมิน (evaluation) หมายถึง กระบวนการศึกษา วิเคราะห์ กำหนดเกณฑ์ วางแผน และดำเนินการอย่างเป็นระบบ ซึ่งผู้ประเมินจะต้องกำหนดเกณฑ์ (criterion) และมาตรฐาน (standard) ที่เหมาะสม ขณะที่มาตรฐานหมายถึงเป้าหมายที่เป็นรูปธรรม ซึ่งใช้เป็นเกณฑ์การประเมิน

ที่เราพิจารณา โดยมาตรฐานจะมีความแตกต่างกันระหว่างหน้าที่งานแต่ละชนิดและประเภทขององค์การหรืออุตสาหกรรม โดยที่การกำหนดมาตรฐานสำหรับควบคุมกลยุทธ์จะต้องสามารถวัดมิติเชิงกลยุทธ์ (strategic dimensions) ของการดำเนินงานอย่างเป็นรูปธรรม

2.3 สรุปกรอบแนวคิด

ในช่วงเวลามีผ่านมาองค์กรและหน่วยงานต่าง ๆ ซึ่งรวมถึงกระทรวงการต่างประเทศได้เผชิญปัญหาด้านความมั่นคงปลอดภัยทางไซเบอร์จำนวนไม่น้อย ภัยคุกคามที่ส่งผลกระทบต่อระบบและข้อมูลภายในมีด้วยกันหลากหลายรูปแบบ โดยประเภทภัยคุกคามที่พบเห็นมากที่สุดคือ Malware สำหรับวัตถุประสงค์ในการโจมตีทางไซเบอร์อาจทำได้หลายลักษณะ ได้แก่ เพื่อเปิดเผยข้อมูล เพื่อหลอกลวง เพื่อขัดขวางการปฏิบัติการในระบบ หรือเพื่อควบคุมระบบ เป็นต้น

ภัยคุกคามเหล่านี้ส่งผลให้มีการกำหนดให้แต่ละหน่วยงานกำหนดมาตรฐานโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีศักยภาพในการป้องกัน และรับมือภัยคุกคามที่อาจเกิดขึ้น โดยแนวความคิดการรักษาความมั่นคงปลอดภัยที่น่าสนใจที่ได้หยิบยกมาได้แก่ (1) หลักการพื้นฐาน 3 ประการสำหรับการรักษาความมั่นคงปลอดภัยของข้อมูล (CIA Triad) (2) หลักดำเนินการที่สำคัญของการรักษาความมั่นคงปลอดภัย และ (3) การแบ่งแยกเครือข่าย (segregation in networks)

ด้วยแนวคิดเหล่านี้ประกอบกับข้อมูลปฐมภูมิและทุติยภูมิที่ได้ทำการศึกษารวบรวมจะนำไปวิเคราะห์ศึกษาเพื่อกำหนดมาตรฐานและออกแบบโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยสำหรับมาตรฐานขั้นพื้นฐานและขั้นสูงให้กับ สอท./สกญ. ทั่วโลก ให้มีความเหมาะสม และสอดคล้องกับสถานการณ์ภัยคุกคามที่เกิดขึ้นอย่างมีประสิทธิภาพ

ด้วยมาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยขั้นพื้นฐาน และขั้นสูงสำหรับ สอท./สกญ. จะสามารถอุดช่องโหว่และความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายและระบบสารสนเทศของ สอท./สกญ. ได้ พร้อมกันนั้นจะเอื้ออำนวยให้เจ้าหน้าที่ที่รับผิดชอบสามารถควบคุมดูแลระบบได้อย่างมีประสิทธิภาพมากยิ่งขึ้น

บทที่ 3
ผลการศึกษา

จากข้อมูลทุติยภูมิเกี่ยวกับสถิติภัยคุกคามทางไซเบอร์ในระดับองค์กร ระดับประเทศ และระดับโลก จะพบว่ามีความพยายามโจมตีทางไซเบอร์ในทุกระดับ ดังเช่นในระดับองค์กรอย่างกรณีของกระทรวงการต่างประเทศ ซึ่งระบบไฟร์วอลล์ได้ตรวจพบความพยายามคุกคามทางไซเบอร์มากถึง 475,056 ครั้ง เมื่อปีที่ผ่านมา โดยพบว่าเป็นภัยคุกคามในระดับวิกฤตสูงถึงร้อยละ 31 และในระดับสูงร้อยละ 27 โดยภัยคุกคามส่วนใหญ่ที่รุนแรงระดับวิกฤติ (critical) จะเป็นความพยายามบุกรุกระบบและเว็บไซต์ และการโจมตีอีเมลผ่านทางไฟล์แนบ (attachment) เป็นต้น ซึ่งที่ผ่านมา กระทรวงฯ พบว่า มีความพยายามในการส่งอีเมลหลองลวงจำนวนมากเข้ามายังหน่วยงานภายในและมายังเจ้าหน้าที่ของกระทรวงฯ ในลักษณะที่เรียกว่า phishing email ซึ่งจะเห็นได้ว่าสอดคล้องกับผลการศึกษาภัยคุกคามในประเทศไทยในปี พ.ศ. 2562 โดยหน่วยงานไทยเซิร์ต ที่พบภัยคุกคามทางไซเบอร์ประเภทความพยายามบุกรุกระบบ และประเภทฉ้อฉลหลอกลวงเป็นจำนวนมาก จากแนวโน้มดังกล่าวนับเป็นภาพสะท้อนเหตุการณ์โจมตีที่เกิดขึ้นทั่วโลก โดยการโจมตีหลักจะผ่านช่องทางอีเมลและเว็บไซต์เป็นส่วนใหญ่

ภัยคุกคามที่เกิดขึ้นต่างมีลักษณะเฉพาะและรูปแบบการโจมตีที่แตกต่างกันไป จึงเป็นการตอกย้ำความจำเป็นที่แต่ละหน่วยงานต้องมีระบบรักษาความมั่นคงปลอดภัยที่มีศักยภาพ และมีมาตรฐานเดียวกันเพื่อการดูแลระบบอย่างมีประสิทธิภาพ

ดังนั้น การศึกษาเพื่อจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ นั้น ได้เริ่มจากการค้นคว้าหาข้อมูล การสำรวจระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่ได้รับแจ้งจาก สอท./สกญ. บางแห่ง การสัมภาษณ์ ข้อมูลโทรเลขรายงานภัยคุกคามที่เกิดขึ้น และข้อมูลงานวิจัยและสถิติภัยคุกคาม เพื่อมาวิเคราะห์สถานะระบบรักษาความมั่นคงปลอดภัยทางไซเบอร์ล่าสุดของแต่ละ สอท./สกญ.

3.1 ผลการศึกษาสถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ทั่วโลก

3.1.1 การสำรวจความพร้อมของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ตามโทรเลขกระทรวงการต่างประเทศ ที่ 0203/ว.475/2562 ลงวันที่ 6 มิถุนายน 2562

วัตถุประสงค์ของการสำรวจก็เพื่อสำรวจสถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. ถึงความพร้อมของการมีระบบไฟร์วอลล์ (Firewall), ระบบ IPS (intrusion prevention system) และโปรแกรมป้องกันไวรัส

วิธีการสำรวจคือศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการต่างประเทศได้ทำโทรเลขสอบถามไปยัง สอท./สกญ. ถึงการมีระบบหรืออุปกรณ์ไฟร์วอลล์, อุปกรณ์ IPS (Intrusion Prevention System) และโปรแกรมป้องกันไวรัส หรือไม่อย่างไร พร้อมแจ้งข้อมูลตอบกลับให้กระทรวงฯ ทราบ และพบว่ามี สอท./สกญ. ส่งผลสำรวจเข้ามาเพียง 34 แห่ง จากทั้งหมด 97 แห่งทั่วโลก หรือคิดเป็นร้อยละ 35.05 ของกลุ่มเป้าหมาย ขณะที่บางแห่งที่แจ้งข้อมูลเข้ามานั้นมีบางรายการที่เข้าใจผิดพลาด ซึ่งสิ่งเหล่านี้นับว่าเป็นข้อจำกัดของการสำรวจต่อความครบถ้วนถูกต้องและคุณภาพของข้อมูลอย่างมาก

จากผลการสำรวจและการวิเคราะห์พบว่า สอท./สกญ. ที่มีระบบและอุปกรณ์ป้องกันพื้นฐานครบทั้งอุปกรณ์ไฟร์วอลล์, ระบบ IPS (ใช้โมดูลที่มากับไฟร์วอลล์ด้วยได้) และระบบป้องกันไวรัส มีเพียง 6 แห่งเท่านั้น หรือคิดเป็นร้อยละ 17.6 จากผลสำรวจที่ได้ 34 แห่ง ดังตารางที่ 1

ตารางที่ 1 สอท./สกญ. ที่มีระบบรักษาความมั่นคงปลอดภัยฯ พื้นฐานครบทั้ง 3 ระบบ

ลำดับ	หน่วยงาน	ระบบ		
		Firewall	IPS	Antivirus
1	สอท. ณ กรุงกัวลาลัมเปอร์	WatchGuard รุ่น XTM 25		Kaspersky
2	สอท. ณ กรุงโรม	รุ่น ZYXEL - ZYWALL USG 100 - UNIFIED SECURITYGATEWAY		มีแต่ไม่ได้ระบุยี่ห้อ
3	สอท. ณ กรุงบรัสเซลส์	Fortinet รุ่น Fortigate 60D		Endpoint Security
4	สอท. ณ กรุงวอชิงตัน	Dell SonicWal รุ่น NSA 2600		Kaspersky
5	สกญ. ณ นครเชียงใฮ้	มีแต่ไม่ได้ระบุยี่ห้อ	มีแต่ไม่ได้ระบุยี่ห้อ	มีแต่ไม่ได้ระบุยี่ห้อ
6	สกญ. ณ นครลอสแอนเจลิส	Fortigate รุ่น 60D		Kaspersky
รวมหน่วยงานที่มีทั้ง 3 ระบบ จำนวน 6 หน่วยงาน				

สำหรับ สอท./สกญ. ที่มีระบบป้องกันพื้นฐานเพียง 2 ระบบ คือ มีอุปกรณ์ไฟร์วอลล์และระบบป้องกันไวรัส จำนวน 9 แห่ง หรือคิดเป็นร้อยละ 26.4 จากทั้ง 34 แห่ง ดังตารางที่ 2

ตารางที่ 2 สอท./สกญ. ที่มีระบบรักษาความมั่นคงปลอดภัยฯ พื้นฐาน จำนวน 2 ระบบ

ลำดับ	หน่วยงาน	ระบบ	
		Firewall	Antivirus
1	สอท. ณ กรุงโคลัมโบ	มีแต่ไม่ได้ระบุ	ESET Internet Security
2	สอท. ณ กรุงโซล	CISCO รุ่น RV042G	McAfee
3	สอท. ณ กรุงโตเกียว	Fortinet รุ่น Fortigate 90D	Avast
4	สอท. ณ กรุงนิวเดลี	Cisco รุ่น RV042 / Mikrotik รุ่น CCR-1036	Windows Defender
5	สอท. ณ กรุงมานามา	มีแต่ไม่ได้ระบุ	Nod32
6	สอท. ณ กรุงลิสบอน	Draytek Vigor 2960	Kaspersky
7	สอท. ณ กรุงเฮลซิงกิ	มีแต่ไม่ได้ระบุ	มีแต่ไม่ได้ระบุ
8	สกญ. ณ เมืองฟูกูโอกะ	Clavistere80	Kaspersky
9	คณะทูตถาวรฯ ณ นครเจนีวา	Sonicwall TZ300	Sophos Endpoint
รวมหน่วยงานที่มีทั้ง 2 ระบบ จำนวน 9 หน่วยงาน			

นอกจากนี้จะเห็นได้ว่า สอท./สกญ. ส่วนใหญ่จะมีเพียงระบบป้องกันไวรัสเพียงอย่างเดียว จำนวน 19 แห่ง หรือคิดเป็นร้อยละ 55.8 ซึ่งถือว่าส่วนใหญ่ไม่มีความพร้อมทางด้านนี้ ดังตารางที่ 3

ตารางที่ 3 สอท./สกญ. ที่มีระบบรักษาความมั่นคงปลอดภัยฯ พื้นฐานเพียง 1 ระบบ

ลำดับ	หน่วยงาน	ระบบ	
		Firewall	Antivirus
1	สอท. ณ กรุงโคเปนเฮเกน	ไม่มี	Microsoft Defender
2	สอท. ณ กรุงไคโร	ไม่มี	McAfee
3	สอท. ณ กรุงซันติอาโก	ไม่มี	Kaspersky/ESET NOD32
4	สอท. ณ กรุงดิลี	ไม่มี	SMADAV 2019
5	สอท. ณ กรุงไนโรบี	ไม่มี	Kaspersky
6	สอท. ณ กรุงมาดริด	ไม่มี	McAfee
7	สอท. ณ กรุงเม็กซิโก	ไม่มี	ESET NOD32

ตารางที่ 3 (ต่อ)

ลำดับ	หน่วยงาน	ระบบ	
		Firewall	Antivirus
8	สอท. ณ บันดาร์เสรีเบกาวัน	ไม่มี	Avast
9	สอท. ณ กรุงวอ์ซอ	ไม่มี	ESET NOD32
10	สอท. ณ กรุงเวลลิงตัน	ไม่มี	Trend Micro Maximum Security
11	สอท. ณ กรุงออตตาวา	ไม่มี	Avast Antivirus / Symamtec
12	สอท. ณ กรุงอัมมาน	ไม่มี	Kaspersky
13	สอท. ณ กรุงเอเธนส์	ไม่มี	Endpoint Security
14	สกญ. ณ นครกวางโจว	ไม่มี	ESET NOD32
15	สกญ. ณ เมืองชิงต่าว	ยี่ห้อ H3C รุ่น ER2100	ไม่มี
16	สกญ. ณ เมืองเจดดาห์	ไม่มี	Norton Security
17	สกญ. ณ นครหนานหนิง	ไม่มี	Kingsoft
18	สกญ. ณ เมืองปีนัง	ไม่มี	Endpoint Security
19	สกญ. ณ แขวงสะหวันนะเขต	ไม่มี	Kaspersky
รวมหน่วยงานที่มีเพียง 1 ระบบ จำนวน 19 หน่วยงาน			

เมื่อพิจารณาในภาพรวมพอจะอนุมานผลการสำรวจ สอท./สกญ. ทั้ง 34 แห่ง จาก 97 แห่งทั่วโลกได้ ซึ่งคิดเป็นกลุ่มตัวอย่างประมาณ 35% (ขนาดกลุ่มตัวอย่างที่เหมาะสมส่วนใหญ่จะใช้กลุ่มตัวอย่าง 20%, 25% และ 30% แต่นิยมกันมากที่สุดที่ 20%)[5] ดังนั้น โดยภาพรวมจะเห็นได้ว่า สอท./สกญ. ส่วนใหญ่ยังขาดความพร้อมด้านการป้องกันภัยคุกคามทางไซเบอร์เป็นอย่างมาก ทั้งนี้ไม่นับรวมกับบางแห่งที่มีระบบแต่ขาดการบำรุงรักษา ไม่ได้ต่ออายุ software subscriptions อย่างต่อเนื่อง จึงส่งผลให้ระบบป้องกันฯ เกิดช่องโหว่และความไม่พร้อมรับมือกับภัยคุกคามทางไซเบอร์ในรูปแบบต่าง ๆ อย่างมีประสิทธิภาพได้ ดังนั้น สอท./สกญ. จำเป็นต้องพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นส่วนสำคัญด้านโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศให้มีความพร้อมและรองรับการเติบโตและการขับเคลื่อนของภาครัฐไปสู่รัฐบาลดิจิทัลในอนาคตต่อไป

[5] ที่มา: https://sites.google.com/site/bb24690p/khnad-khxng-klum-tawxyang-thi-hemaa-sm ขนาดกลุ่มตัวอย่างที่เหมาะสม จากสูตรคำนวณ วิธีที่ 3 กำหนดเป็นเปอร์เซ็นต์ ซึ่งโดยมากจะกำหนด 20%, 25% หรือ 30% ของประชากรทั้งหมด ถ้าประชากรมีขนาดเป็นร้อย อาจกำหนดขนาดตัวอย่าง 25% หรือ 30%

3.1.2 การสัมภาษณ์ข้าราชการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เมื่อวันที่ 13 กรกฎาคม 2563 ดังภาคผนวก ก

สรุปประเด็นสำคัญของการสัมภาษณ์เจ้าหน้าที่นายช่างไฟฟ้าชำนาญงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการต่างประเทศ จำนวน 6 ท่าน ที่เคยออกประจำการ โดยข้อมูลที่ได้รับจากการสัมภาษณ์นั้นถือว่ามีความถูกต้องและน่าเชื่อถือสูง เนื่องจากแต่ละท่านจะมีความรู้และประสบการณ์ด้าน ICT กอปรกับทราบรายละเอียดของ สอท./สกญ. แต่ละแห่งที่ได้ไปประจำการเป็นอย่างดี

สำหรับข้อมูลที่จะนำมาใช้พิจารณาเพื่อกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์จะประกอบด้วย ระบบเครือข่ายภายในของ สอท./สกญ. การใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของ สอท./สกญ. ไม่ว่าจะเป็นจำนวนเครื่องคอมพิวเตอร์และอุปกรณ์การใช้งานอินเทอร์เน็ต และรวมถึงการรั่วไหลของข้อมูล เป็นต้น โดยพอสรุปรายละเอียดได้ดังนี้

ตารางที่ 4 สรุปจำนวนเครื่องคอมพิวเตอร์และอุปกรณ์ของ สอท./สกญ. จากการสัมภาษณ์

สอท./สกญ.	**จำนวนเครื่องคอมพิวเตอร์และอุปกรณ์**					**รวม**
	PC	Server	Access Point (Wi-Fi)	VoIP	CCTV	
สอท. ณ กรุงกัวลาลัมเปอร์	30	2	9	10	52	94
สอท. ณ กรุงย่างกุ้ง	32	3	12	N/A	39	86
สอท. ณ เวียงจันทน์	50	2	3	N/A	22	77
สอท. ณ กรุงเดลี	30	3	10	30	N/A	73
สอท. ณ กรุงเบอร์ลิน	30	5	7	12	16	70
สอท. ณ กรุงวอชิงตัน ดีซี	50	5	10	20	10	95
สกญ. ณ นครนิวยอร์ก	30	N/A	N/A	10	N/A	40

หากมองในเรื่องการให้ความสำคัญของข้อมูลสารสนเทศหรือการจัดเก็บข้อมูลที่มีชั้นความลับซึ่งสำคัญต่อกระทรวงฯ หรือประเทศชาติแล้ว จะพบว่ามี สอท. ณ กรุงกัวลาลัมเปอร์ สอท. ณ กรุงย่างกุ้ง สอท. ณ เวียงจันทน์ และสกญ. ณ นครนิวยอร์ก

สำหรับ สอท./สกญ. ที่มีหน่วยงานภายนอกซึ่งหมายถึงทีมไทยแลนด์อยู่ด้วย ก็จะมีการใช้ facility ร่วมกัน โดยเฉพาะอย่างยิ่งการใช้งานอินเทอร์เน็ตหรือบริการทางด้านเทคโนโลยีสารสนเทศอื่น จึงเป็นปัจจัยทำให้มีโอกาสเกิดช่องโหว่และความเสี่ยงเพิ่มขึ้น ดังนั้นจึงจำเป็นต้องมีมาตรการ การบริหารจัดการและการควบคุมดูแลให้เกิดการใช้งานเป็นไปอย่างมั่นคงปลอดภัยด้วย

เช่นกัน และเป็นเหตุผลที่จะต้องนำประเด็นนี้มาวิเคราะห์เพื่อออกแบบโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยด้วยเช่นกัน

จากผลการศึกษาข้างต้น จะเห็นได้ว่าสถานะระบบรักษาความมั่นคงปลอดภัยของ สอท./สกญ. แต่ละแห่งยังมีข้อจำกัดในการป้องกันภัยคุกคามทางไซเบอร์อยู่มาก โดยมีระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่ไม่เพียงพอที่จะต่อกรรับมือกับภัยคุกคามในปัจจุบันได้ อีกทั้งไม่มีมาตรฐานที่เป็นไปในทิศทางเดียวกัน ซึ่งจะเป็นอุปสรรคต่อการรักษาความมั่นคงปลอดภัยและการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของ สอท./สกญ. ให้เป็นไปอย่างมีประสิทธิภาพและมีประสิทธิผลได้ อีกทั้งเพื่อพัฒนาทางเทคโนโลยีดิจิทัลของ สอท./สกญ. ต่อไปในอนาคตด้วย

จากสถานการณ์ภัยคุกคามที่เกิดขึ้นในทุกระดับ และสถานะล่าสุดของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยังขาดศักยภาพในการป้องกันการบุกรุกโจมตีที่เพิ่มสูงขึ้น ดังนั้น รายงานศึกษาฉบับนี้จึงมุ่งเน้นที่จะกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับ สอท./สกญ. ทั่วโลก เพื่อให้มั่นใจได้ว่า สอท./สกญ. แต่ละแห่งจะมีความพร้อมในการป้องภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ และมีมาตรฐานของระบบฯ เป็นไปในแนวทางเดียวกัน ซึ่งเอื้ออำนวยต่อการบริหารจัดการ การกำหนดมาตรการ การให้การสนับสนุนและให้ความช่วยเหลือจากส่วนกลางได้เพื่อให้การแก้ปัญหาที่เกิดขึ้นเป็นไปอย่างมีประสิทธิภาพ

3.2 การกำหนดมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์

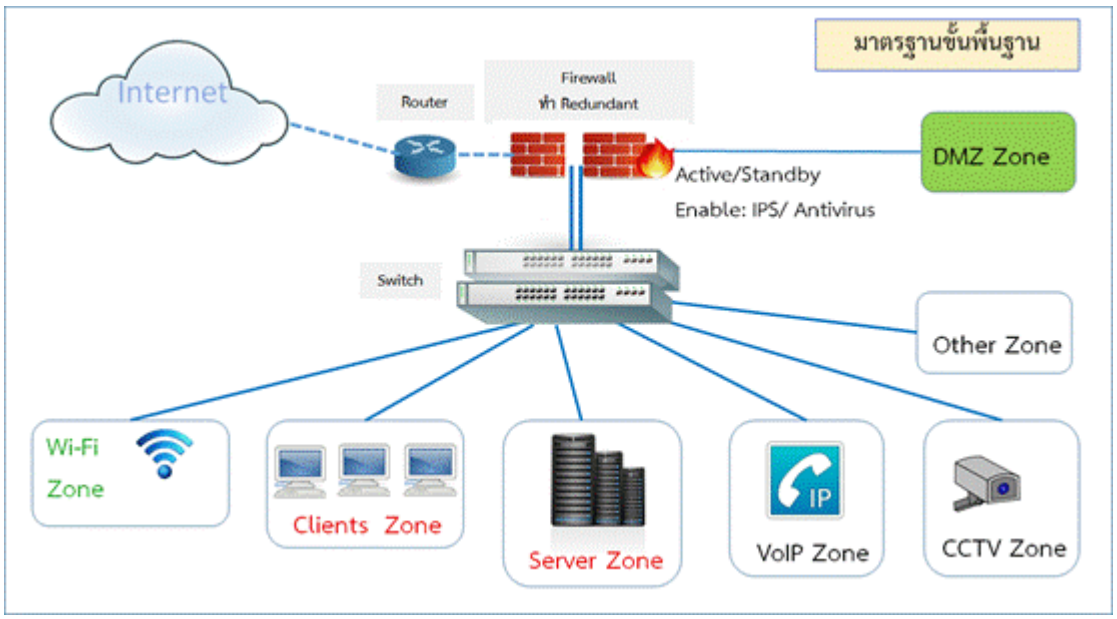
มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย 3 ส่วนหลัก ได้แก่ (1) มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ (2) มาตรฐานหมายเลข IP Address ภายใน (3) มาตรฐานคุณลักษณะเฉพาะของอุปกรณ์/ระบบป้องกันภัยคุกคามไซเบอร์

3.2.1 มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับการจัดทำมาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสถานเอกอัครราชทูตและสถานกงสุลใหญ่ นั้น ได้มีแนวคิดจัดทำมาตรฐานใน 2 ระดับ ได้แก่ มาตรฐานขั้นพื้นฐาน และมาตรฐานขั้นสูง โดยมาตรฐานแต่ละประเภทจะมีการแบ่งแยกระบบเครือข่ายภายใน (network segmentations) ตามความจำเป็นและเหมาะสมต่อการใช้งาน และมีความซับซ้อนของระบบเครือข่ายที่มีอุปกรณ์หรือระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่แตกต่างกันทั้งทางด้านคุณลักษณะเฉพาะและจำนวนเครื่องคอมพิวเตอร์ เทคโนโลยีหรือระบบที่จำเป็นต้องใช้งาน ดังรายละเอียดต่อไปนี้

3.2.1.1 มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานสำหรับ สอท./สกญ.

มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานนี้ หรือมาตรฐานขั้นต่ำที่ทุก สอท./สกญ. ทั่วโลกจำเป็นต้องดำเนินการให้เป็นไปตามมาตรฐานนี้ โดยมีการออกแบบโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้มีความพร้อมในการรับมือสามารถปกป้องและป้องกันการบุกรุกโจมตีระบบเครือข่ายสารสนเทศ จึงทำการแบ่งแยกระบบเครือข่าย (network segmentation) ออกเป็นโซนต่าง ๆ ตามความจำเป็นและการใช้งานพื้นฐานให้เกิดความปลอดภัยมากยิ่งขึ้น โดยออกแบบผังโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ดัง Diagram ตามภาพที่ 12 นี้



ภาพที่ 12 Diagram โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน

จากภาพ diagram โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานข้างต้น จะเห็นได้ว่ามีการออกแบบโดยใช้หลักการแบ่งแยกเครือข่าย (segregation in networks) ตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มงานระบบต่าง ๆ ตามที่จำเป็น โดยเป็นการแบ่งส่วนระบบเครือข่าย หรือ network segmentation ซึ่งการแบ่งส่วนระบบเครือข่ายนับเป็นกลยุทธ์เชิงลึกเพื่อสร้างความมั่นคงปลอดภัยให้กับองค์กรที่จะช่วยลดความเสี่ยงและความเสียหายที่จะช่วยให้การบริหารจัดการกับปัญหาภัยคุกคามหรือดำเนินมาตรการควบคุมต่าง ๆ ได้มากขึ้น อีกทั้งเป็นการลดพื้นที่จากการถูกโจมตีเพื่อไม่ให้เกิดความเสียหายในวงกว้างได้ อันเป็นแนวทางปฏิบัติตามระเบียบและวิธีการที่ปลอดภัยต่อองค์กร

สำหรับการแบ่งโซนของโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานนี้ จะขอแบ่งออกเป็น 5 โซน ซึ่งเป็นโซนพื้นฐานเบื้องต้นที่สำคัญต่อการใช้งานของ สอท./สกญ. แต่ละแห่ง อันประกอบด้วย

1) โซน DMZ (ถ้ามีระบบให้บริการสาธารณะ) ในกรณีที่ สอท./สกญ. มีระบบสารสนเทศหรือเว็บไซต์ให้บริการแก่สาธารณะ หรือคนทั่วไป อย่างเช่น เว็บไซต์สำหรับบริการประชาชน การประชาสัมพันธ์ เป็นต้น

2) โซน Server สำหรับเครื่องเซิร์ฟเวอร์ที่ใช้เป็นการภายใน เช่น File Server, เครื่องเซิร์ฟเวอร์ระบบโทรเลข เป็นต้น

3) โซน Clients เป็นโซนสำหรับเครื่องคอมพิวเตอร์ Clients และอุปกรณ์ต่อพ่วงเช่น เครื่องพิมพ์ (printer) สแกนเนอร์ (scanner) เป็นต้น

4) โซน Wi–Fi เป็นโซนเพื่อให้บริการอินเทอร์เน็ตผ่าน Wi–Fi เท่านั้น และไม่อนุญาตให้เข้าถึงระบบภายในใด ๆ ได้

5) โซน CCTV เป็นโซนใช้กับอุปกรณ์ของระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัย

6) โซน VoIP (Voice over IP) เป็นโซนที่ใช้กับอุปกรณ์ระบบ VoIP หรือเครื่องโทรศัพท์ VoIP

7) โซนอื่น (หากมี) กรณีที่ต้องการเพิ่มโซนเพื่อความปลอดภัยมากยิ่งขึ้น หรือสำหรับการใช้งานระบบอื่นนอกเหนือจากข้างต้น ก็สามารถแบ่งส่วนระบบเครือข่ายเพิ่มขึ้นได้

จากการแบ่ง network segmentation ออกเป็นโซนต่าง ๆ นั้น จะเห็นว่ามีโซนพื้นฐานหลักทั่วไปที่ทุก สอท./สกญ. จำเป็นต้องมีเป็นอย่างน้อย ประกอบด้วย 5 โซนด้วยกัน คือ โซนที่ 2–6 โดยการแบ่งโซนนั้น จะเกิดที่ไฟร์วอลล์ นั่นหมายถึง ไฟร์วอลล์จะทำหน้าที่ควบคุมการเข้าถึงระบบเครือข่ายสารสนเทศ การติดต่อสื่อสารระหว่างโซน หรือแม้แต่การออกอินเทอร์เน็ตของเครื่อง clients และ Wi–Fi ก็จำเป็นต้องถูกกำหนด Policy หรือกฎ (Rule Base Policy) บนอุปกรณ์ไฟร์วอลล์ให้มีการเข้าถึงและการใช้งานระบบสารสนเทศต่าง ๆ ขององค์กรให้มีความมั่นคงปลอดภัยจากการบุกรุกโจมตีจากผู้ไม่หวังดี หรือจากมัลแวร์ต่าง ๆ ได้อย่างมีประสิทธิภาพ

สำหรับอุปกรณ์ไฟร์วอลล์ที่พิจารณานำมาใช้นั้น จะเป็นอุปกรณ์ Application Firewall หรือบางผลิตภัณฑ์เรียกว่า Next Generation Firewall เป็นไฟร์วอลล์ที่ทำงานได้ถึงระดับ Application ดังนั้นไฟร์วอลล์ประเภทนี้จึงมีความสามารถในการควบคุมการเข้าถึง ตรวจสอบภัยคุกคาม และป้องกันการโจมตีที่เข้ามาในระดับแอพพลิเคชั่นได้ ดังนั้นการพิจารณาเลือกใช้ไฟร์วอลล์ประเภทนี้ให้กับองค์กรจึงเป็นสิ่งสำคัญต่อการรักษาความมั่นคงปลอดภัยเครือข่ายและสารสนเทศขององค์กรในปัจจุบันได้อย่างมีประสิทธิผล นอกจากนี้ เพื่อให้อุปกรณ์ไฟร์วอลล์มี

ความพร้อมใช้อยู่เสมอ อันส่งผลต่อการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารภายใน จึงออกแบบให้มีไฟร์วอลล์จำนวน 2 เครื่อง เพื่อช่วยกันทำงาน (Redundant) เพื่อป้องกันหากเครื่องใดเครื่องหนึ่งไม่สามารถทำงานได้ หรือที่เรียกว่า การทำ HA (High Availability)[6] ของอุปกรณ์ไฟร์วอลล์ให้เกิดความพร้อมใช้งานอยู่เสมอ

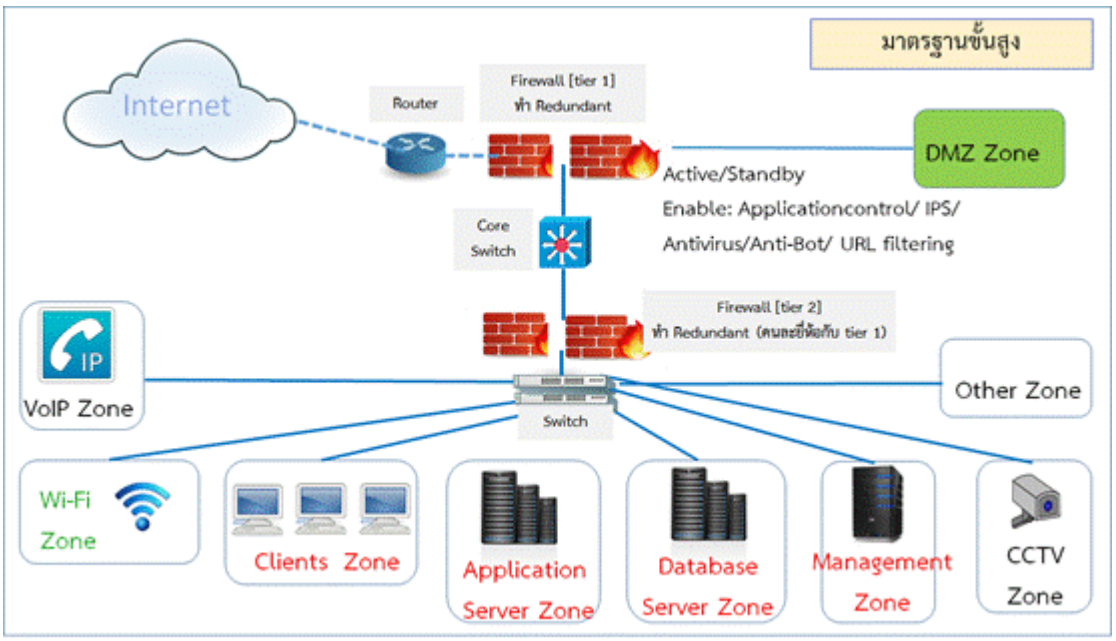
เพื่อเป็นการป้องกันการบุกรุกโจมตีระบบจึงจำเป็นต้องมีระบบที่มีความสามารถในการป้องกันการโจมตีเป็นการเฉพาะอย่างระบบ IPS (Intrusion Prevention System) ซึ่งจะมีฟังก์ชั่น IDS (Intrusion Detection System) มาในตัวเพื่อให้สามารถเฝ้าระวังตรวจจับการบุกรุก และป้องกันการบุกรุกโจมตีได้ ดังนั้นระบบ IPS จึงถูกนำมาใช้ป้องกันการบุกรุกโจมตีจากภัยคุกคามไซเบอร์เชิงลึกได้อย่างทันท่วงที

อย่างไรก็ตาม เพื่อให้เครื่องคอมพิวเตอร์ทุกเครื่องภายใต้ระบบเครือข่ายมีความปลอดภัยจากไวรัสและมัลแวร์ต่าง ๆ และป้องกันการรั่วไหลของข้อมูลทั้งส่วนบุคคลและองค์กร จึงจำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ทุกเครื่อง โดยเลือกใช้โปรแกรมป้องกันไวรัสที่มีคุณสมบัติในการป้องกันมัลแวร์ขั้นสูงได้ อย่างเช่น โปรแกรมป้องกันไวรัสและมัลแวร์ประเภท Endpoint Security หรือที่เรียกว่า EDR (Endpoint Detection and Response) ก็จะช่วยรับมือกับภัยคุกคามและมัลแวร์ขั้นสูงได้ปลอดภัยมากยิ่งขึ้น

3.2.1.2 มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูงสำหรับ สอท./สกญ.

มาตรฐานขั้นสูงเป็นมาตรฐานที่แนะนำสำหรับ สอท./สกญ. ที่มีความอ่อนไหวของข้อมูลสูง มีที่ตั้งอยู่ในประเทศยุทธศาสตร์อย่างประเทศมหาอำนาจ ประเทศเพื่อนบ้าน มีการใช้งานเทคโนโลยีสารสนเทศในปริมาณสูง เป็น สอท./สกญ. ที่ประกอบด้วยทีมไทยแลนด์ หรือมีความเสี่ยงต่อการถูกคุกคามทางไซเบอร์สูง อีกทั้งยังเป็นทางเลือกสำหรับ สอท./สกญ. ที่ต้องการเพิ่มศักยภาพในการป้องกันที่เข้มข้นมากยิ่งขึ้น โดยมีการออกแบบภายใต้แนวคิดเดียวกันกับมาตรฐานขั้นพื้นฐาน แต่ต่างกันที่มาตรฐานขั้นสูงจะมีระบบไฟร์วอลล์คอยป้องกันถึง 2 ชั้น (2 tiers) และมีการแบ่งโซนที่หลากหลายและซับซ้อนขึ้น จึงทำให้เกิดความปลอดภัยเป็นอย่างมาก ดัง Diagram ข้างล่างนี้

[6] การทำให้ระบบพร้อมใช้งานอยู่เสมอ แม้มีเหตุการณ์ไม่ปรกติเกิดขึ้นกับระบบ



ภาพที่ 13 Diagram โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูง

จาก Diagram โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูง จะมีการออกแบบโดยใช้หลักการเดียวกันกับมาตรฐานขั้นพื้นฐาน แต่เพิ่มแนวป้องกันการควบคุมการเข้าถึงระบบเครือข่ายและสารสนเทศด้วยไฟร์วอลล์ คือ จากไฟร์วอลล์ 1 tier เป็นไฟร์วอลล์ 2 tiers ซึ่งจะช่วยให้โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์มาตรฐานนี้มีความปลอดภัยเป็นอย่างมาก อย่างไรก็ตามไฟร์วอลล์ชั้นที่ 1 กับชั้นที่ 2 ควรเลือกใช้ต่างยี่ห้อกัน เนื่องจากถ้าเป็นยี่ห้อเดียวกันแล้วหากเกิดมีช่องโหว่ก็เท่ากับว่าไฟร์วอลล์ทั้งสองชั้นนั้นสามารถถูกโจมตีผ่านช่องโหว่เดียวกันได้ นั่นเท่ากับว่าการมีไฟร์วอลล์ 2 ชั้น ไม่ค่อยเกิดประโยชน์เท่าที่ควร

สำหรับการแบ่งโซนของโครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูงนี้ จะมีการแบ่งโซนอย่างน้อย 8 โซน ดังเช่น

1) โซน DMZ เป็นโซนสำหรับที่อยู่ของเครื่องเซิร์ฟเวอร์ที่ให้บริการสาธารณะอย่างเช่นเว็บไซต์ของ สอท./สกญ. เพื่อให้บริการประชาชน เป็นต้น

2) โซน Application Server สำหรับเครื่องเซิร์ฟเวอร์สำหรับการทำงานของแอพพลิเคชั่นซึ่งไม่ได้จัดเก็บข้อมูลหรือฐานข้อมูลใด ๆ สำคัญของระบบ

3) โซน Database Server เครื่องเซิร์ฟเวอร์สำหรับจัดเก็บข้อมูล หรือฐานข้อมูลของระบบสารสนเทศต่าง ๆ ซึ่งจะถูกติดตั้งภายใต้โซนนี้ โดยฐานข้อมูลในโซนนี้จะถูกเรียกใช้จากเครื่องเซิร์ฟเวอร์ของระบบที่อยู่ในโซน application server ต่อไป

4) โซน Management Server ส่วนใหญ่จะเป็นที่อยู่ของเครื่องเซิร์ฟเวอร์ที่ใช้บริหารจัดการระบบจากส่วนกลาง อย่างเช่น เครื่องเซิร์ฟเวอร์บริหารจัดการระบบไฟร์วอลล์ เครื่องเซิร์ฟเวอร์บริหารจัดการ antivirus และระบบบริหารจัดการเว็บไซต์ เป็นต้น

5) โซน Clients เป็นโซนสำหรับเครื่องคอมพิวเตอร์ Clients และอุปกรณ์ต่อพ่วงเช่น เครื่องพิมพ์ (printer) สแกนเนอร์ (scanner) เป็นต้น

6) โซน Wi–Fi เป็นโซนเพื่อให้บริการอินเทอร์เน็ตผ่าน Wi–Fi เท่านั้น และไม่อนุญาตให้เข้าถึงระบบอินทราเน็ตหรือภายในใด ๆ

7) โซน CCTV เป็นโซนสำหรับอุปกรณ์ระบบกล้องวงจรปิดในการรักษาความปลอดภัย

8) โซน VoIP (Voice over IP) เป็นโซนที่ใช้กับอุปกรณ์ระบบ VoIP ที่รวมถึงอุปกรณ์ IPPBX และเครื่องโทรศัพท์ VoIP เป็นต้น

9) โซนอื่น ๆ (หากมี) กรณีที่ต้องการเพิ่มโซนเพื่อความปลอดภัยมากยิ่งขึ้น หรือสำหรับการใช้งานระบบอื่นนอกเหนือจากข้างต้น ก็สามารถแบ่งส่วนระบบเครือข่ายเพิ่มได้

จากการแบ่งส่วนระบบเครือข่าย หรือ network segmentation สำหรับมาตรฐานขั้นสูงนี้ จะมีการแบ่งโซนพื้นฐานจำนวนโซนมากกว่ามาตรฐานขั้นพื้นฐาน เนื่องด้วยเป็นระบบเครือข่ายที่ใหญ่กว่า มีการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่หลากหลาย และเพื่อความปลอดภัยที่มากขึ้น จึงจำเป็นต้องมีการแบ่งส่วนระบบเครือข่ายที่มีจำนวนโซนมากขึ้น ดังเช่น application zone, database zone และ management zone เป็นต้น ซึ่งการแบ่งส่วนระบบเครือข่ายที่หลากหลายมากขึ้นนี้ ก็จะช่วยให้การบริหารจัดการระบบเครือข่ายที่มีความซับซ้อนทำได้สะดวกและเกิดประสิทธิผลมากยิ่งขึ้น

สำหรับอุปกรณ์ไฟร์วอลล์ที่พิจารณานำมาใช้นั้น จะเป็นอุปกรณ์ application firewall เช่นเดียวกันกับมาตรฐานขั้นต่ำ เพื่อให้มีความสามารถในการควบคุมการเข้าถึง ตรวจสอบภัยคุกคาม และป้องกันการโจมตีในระดับแอพพลิเคชั่นได้อย่างมีประสิทธิผล อย่างไรก็ตาม ยังได้มีการออกแบบให้มีระบบไฟร์วอลล์ 2 ชั้น ที่ทำงานในลักษณะ 2 tiers ซึ่งแต่ละชั้นหรือแต่ละ tier นั้นจะมีไฟร์วอลล์จำนวน 2 เครื่อง เพื่อช่วยกันทำงาน (Redundant) ซึ่งก็คือมีการทำ HA (High Availability) ของอุปกรณ์ไฟร์วอลล์เช่นกัน นอกจากนี้ได้มีการป้องกันการบุกรุกโจมตีระบบด้วยโมดูล IPS (Intrusion Prevention System) และ IDS (Intrusion Detection System) ที่มาพร้อมกับอุปกรณ์ไฟร์วอลล์หรือแยกเฉพาะ เพื่อให้สามารถเฝ้าระวัง ตรวจจับการบุกรุก และป้องกันการบุกรุกโจมตีได้

อย่างไรก็ตาม เครื่องคอมพิวเตอร์ทุกเครื่องภายใต้ระบบเครือข่ายของ สอท./สกญ. ควรได้รับการปกป้องจากโปรแกรมป้องกันไวรัสและมัลแวร์ประเภท Endpoint

Security หรือที่เรียกว่า EDR (Endpoint Detection and Response) เพื่อความปลอดภัยมากขึ้นด้วยเช่นกัน

จะเห็นได้ว่ามาตรฐานขั้นสูงนี้จะมีระดับการป้องกันที่เข้มแข็งมากกว่ามาตรฐานขั้นพื้นฐานมาก ด้วยการมีระบบไฟร์วอลล์ไว้ป้องกันเครือข่ายและสารสนเทศของ สอท./สกญ. ถึง 2 ชั้น ซึ่งเป็นลักษณะการออกแบบใกล้เคียงกับระบบเครือข่ายขององค์กรระดับ enterprise system สำหรับการแบ่งโซนตามหลักการของ network segmentation นั้น ก็ได้มีการแบ่งโซนตามแนวทางอย่างปลอดภัยที่มีการแยกเครื่องเซิร์ฟเวอร์หรือระบบตามภารกิจเพื่อการควบคุมและบริหารจัดการ ลดความเสี่ยงและผลกระทบต่อระบบเครือข่ายในภาพรวมได้ในกรณีเกิดปัญหาด้านภัยคุกคามทางไซเบอร์

3.2.2 มาตรฐานหมายเลข IP Address ภายใน สำหรับ สอท./สกญ.

มาตรฐานหมายเลข IP Address ภายใน สำหรับ สอท./สกญ. ได้จัดทำขึ้นเพื่อใช้กำหนดหมายเลข IP Address ให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ของแต่ละ สอท./สกญ. ทุกแห่งให้มีมาตรฐาน โดยไม่คำนึงถึงว่าจะเป็นมาตรฐานขั้นพื้นฐานหรือขั้นสูง การกำหนด IP Address จะเอื้ออำนวยให้เจ้าหน้าที่ให้สามารถจัดการดูแลระบบได้สะดวกยิ่งขึ้น เนื่องจากหมายเลข IP Address จะถูกนำไปใช้ในโซนต่าง ๆ และกำหนดหมายเลข IP Address ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องภายใต้โซนนั้น ๆ ตามที่ได้ทำการแบ่งส่วนระบบเครือข่าย (network segmentation) ซึ่งการกำหนด IP Address ดังกล่าว จะช่วยอำนวยความสะดวกในการบริหารจัดการ และที่สำคัญคือสามารถอ้างอิงหรือวิเคราะห์ตรวจสอบแหล่งที่มาหรือเส้นทางการบุกรุกโจมตีต่อไปได้ ซึ่งนับว่าเป็นสิ่งสำคัญที่จะช่วยสนับสนุนด้านการรักษาความมั่นคงปลอดภัยอีกทางหนึ่ง

สำหรับรูปแบบของหมายเลข IP Address ภายในของ สอท./สกญ. แต่ละแห่งจะใช้หมายเลขไอพีของเน็ตเวิร์ควง 172.16.x.x–172.31.x.x ซึ่งเป็นช่วงหมายเลขไอพีที่อนุญาตให้ใช้ในเน็ตเวิร์คภายใน (private ip address) โดยกำหนดหมายเลข IP Address ให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ภายใต้ระบบเครือข่ายตามโซนต่าง ๆ ต่อไป ดังตัวอย่างเช่น

สอท. ณ กรุงโรม ถูกกำหนดหมายเลข IP Address ของเครือข่ายเป็น 172.X.124.X ซึ่งสามารถอธิบายได้ ดังนี้

X หมายถึง เน็ตเวิร์คโซนภารกิจใด ๆ

124 หมายถึง สอท. ณ กรุงโรม

X หมายถึง หมายเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์ ซึ่งจะเริ่มจากเครื่องหมายเลข 1–254

ดังนั้น หมายเลข IP Address : 172.20.124.3 จึงหมายถึง หมายเลข IP Address ของเครื่องคอมพิวเตอร์วง clients ซึ่งเป็น IP Address ของระบบเครือข่ายของ สอท. ณ กรุงโรม ที่มี

หมายเลขเครื่องคอมพิวเตอร์เป็นหมายเลข 3 หากตำแหน่งหมายเลข 20 เป็นหมายเลข 22 แสดงว่าเป็นเน็ตเวิร์คของวง CCTV ของ สอท. ณ กรุงโรม เป็นต้น

โซนของเน็ตเวิร์ค	
172.17.x.x	วง VoIP
172.18.x.x	วง DMZ
172.19.x.x	วง Wi-Fi
172.20.x.x	วง Clients
172.21.x.x	วง Server
172.22.x.x	วง CCTV
.	.
.	.
.	.
172.30.x.x	วง Management

ภาพที่ 14 โซนของเน็ตเวิร์คแยกตามหมายเลข IP Address

สำหรับตารางหมายเลข IP Address ของ สอท./สกญ. ทั้ง 97 แห่ง และคณะทูตถาวร อีก 3 แห่ง ดังมีรายละเอียดในภาคผนวก ข

3.2.3 มาตรฐานคุณลักษณะเฉพาะของอุปกรณ์/ระบบป้องกันภัยคุกคามไซเบอร์ (Specifications)

จาก Diagram มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูง และขั้นพื้นฐาน นั้น จะประกอบด้วยอุปกรณ์หรือระบบป้องกันภัยคุกคามทางไซเบอร์ที่เป็นพื้นฐานหลักสำคัญ คือ อุปกรณ์ไฟร์วอลล์ อุปกรณ์ IPS และโปรแกรมป้องกันไวรัสและมัลแวร์ เป็นต้น โดยที่อุปกรณ์ไฟร์วอลล์ในปัจจุบันหลายยี่ห้อที่เป็น application firewall หรือ next generation firewall จะเป็นอุปกรณ์ที่มีโมดูลทำหน้าที่ IPS (Intrusion prevention system) มาด้วย หรือไม่ก็เป็นอุปกรณ์ทำหน้าที่ IPS เป็นการเฉพาะ ซึ่งอุปกรณ์ IPS ประเภทนี้จะมีประสิทธิภาพการทำงานที่สูงกว่าและส่วนใหญ่นำไปใช้กับระบบเครือข่ายที่เป็น enterprise network ขนาดใหญ่ที่มีระบบสารสนเทศที่ต้องการปกป้องเป็นจำนวนมาก

อย่างไรก็ตาม ไฟร์วอลล์ที่จะนำมาใช้กับมาตรฐานทั้งสอง อาจมีสเปคเดียวกันก็เป็นไปได้ เนื่องจากผลิตภัณฑ์ไฟร์วอลล์บางยี่ห้อจะมีสเปคที่ครอบคลุมทั้ง 2 มาตรฐานของโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ เว้นแต่บางยี่ห้อจะมีสเปคค่อนข้างจำกัด สำหรับระบบป้องกันภัยคุกคามที่เครื่อง clients และเครื่อง server ซึ่งมีความจำเป็นที่ขาดไม่ได้ก็คือโปรแกรมป้องกันไวรัสและมัลแวร์ ซึ่งปัจจุบันนี้โปรแกรมป้องกันไวรัสที่มีคุณสมบัติทั่วไปไม่สามารถป้องกันภัยคุกคามที่เกิดขึ้นในปัจจุบันได้เท่าที่ควร จึงจำเป็นต้องพิจารณาเลือกโปรแกรมประเภท Endpoint Security ซึ่งเป็นเทคโนโลยีสมัยใหม่มาใช้ป้องกัน จึงจะสามารถสร้างความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ clients และเครื่อง servers ได้

สำหรับรายละเอียดของสเปคหรือคุณลักษณะเฉพาะของอุปกรณ์ไฟร์วอลล์ (พร้อมโมดูล IPS) และโปรแกรมป้องกันไวรัสหรือโปรแกรม Endpoint security เพื่อประโยชน์ในการนำไปใช้เป็นแนวทางประกอบกระบวนการจัดซื้อจัดจ้าง อย่างไรก็ตามก็ต้องมีการปรับปรุงรายละเอียดคุณลักษณะเฉพาะให้ทันสมัยอยู่เป็นประจำ สำหรับตัวอย่างรายละเอียดคุณลักษณะเฉพาะของระบบดังภาคผนวก ค

3.3 เกณฑ์การใช้มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์

มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ทั้ง 2 มาตรฐานนั้น ได้รับการออกแบบอยู่บนหลักแนวคิดและทฤษฎีเดียวกัน เพียงแต่แตกต่างทางด้านจำนวนชั้น (tier) ของไฟร์วอลล์ที่ใช้ในการควบคุมการเข้าถึง โดยจะมีการออกแบบให้ใช้ไฟร์วอลล์แบบ 1 tier หรือจะเป็นแบบ 2 tiers ตามแต่ละมาตรฐาน อีกทั้งจำนวนโซนที่จำเป็นตามการแบ่งส่วนระบบเครือข่ายหรือ network segmentation โดยเมื่อเปรียบเทียบศักยภาพในการป้องกัน การจัดการภัยคุกคามที่เกิดขึ้น มาตรฐานขั้นสูงจะมีศักยภาพในการจัดการภัยคุกคามได้มีประสิทธิภาพสูงกว่าอย่างเห็นได้ชัด ซึ่งจะเป็นการดีหากทุก สอท./สกญ. สามารถนำมาตรฐานขั้นสูงไปประยุกต์ใช้กับองค์กรของตน

อย่างไรก็ตาม ด้วยสภาวการณ์ของแต่ละ สอท./สกญ.ที่มีงบประมาณ จำนวนเครื่องคอมพิวเตอร์ clients และ servers ผู้ดูแลระบบ และความเสี่ยงการถูกโจมตีที่แตกต่างกัน ดังนั้น มาตรฐานขั้นพื้นฐานจึงได้รับการออกแบบให้มีศักยภาพการจัดการภัยคุกคามที่เพียงพอต่อข้อจำกัดต่าง ๆ ให้มีความเหมาะสมต่อการนำไปปฏิบัติใช้ได้จริง (practical) อย่างเป็นรูปธรรม

สำหรับด้านการลงทุนในการจัดซื้อฮาร์ดแวร์และซอฟต์แวร์สำหรับระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐานภายใต้รายงานการศึกษานี้ จะประกอบด้วย อุปกรณ์ไฟร์วอลล์ อุปกรณ์หรือระบบ IPS และโปรแกรมป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์ Clients และ Servers ซึ่งพอจะประมาณการค่าใช้จ่ายเป็นสังเขปได้ ดังนี้

3.3.1 ค่าใช้จ่ายอุปกรณ์ไฟร์วอลล์

สำหรับอุปกรณ์ไฟร์วอลล์ที่จะใช้เป็นมาตรฐานนี้จะพิจารณาเลือกใช้ไฟร์วอลล์ที่มีคุณสมบัติครบครันแบบเบ็ดเสร็จในเครื่องเดียว หรือที่เรียกว่า UTM (Unified Threat Management) เป็นอุปกรณ์ไฟร์วอลล์ซึ่งมีโมดูลของ IPS และฟังก์ชั่นการป้องกันอื่นรวมอยู่ด้วย เพื่อการบริหารจัดการที่สะดวก มีค่าใช้จ่ายไม่มาก ซึ่งเหมาะกับระบบเครือข่ายขนาดเล็ก โดยประมาณการค่าใช้จ่ายในการจัดซื้อประมาณ 3 แสนบาท สำหรับไฟร์วอลล์ 1 tier และค่าใช้จ่ายในการต่ออายุ software subscriptions ในปีถัดไปปีละประมาณไม่เกิน 40% จากราคาซื้อครั้งแรก

อย่างไรก็ตาม อุปกรณ์ไฟร์วอลล์ประเภท UTM ของแต่ละผลิตภัณฑ์ก็มีสเปคและความต่างทางด้านราคาอย่างมากเช่นกัน บางผลิตภัณฑ์อาจมีราคาต่ำกว่าหรือสูงกว่านี้มากก็เป็นไปได้

3.3.2 ค่าใช้จ่ายโปรแกรมป้องกันไวรัส หรือระบบป้องกันไวรัส

โปรแกรมป้องกันไวรัสสำหรับติดตั้งบนเครื่อง clients และ servers มีหลายผลิตภัณฑ์และหลากหลายราคาอย่างมากเช่นกัน ซึ่งขึ้นอยู่กับฟังก์ชั่นการใช้งาน โดยโปรแกรมป้องกันไวรัสทั่วไปจะมีค่า Licenses ปีละประมาณ 500–1,000 บาท ต่อ1 license และถ้าต้องการโปรแกรมป้องกันไวรัสและมัลแวร์ประเภท endpoint security หรือประเภท EDR (Endpoint Detection and Response) ที่มีความสามารถสูงและรองรับการตรวจจับและป้องกันภัยคุกคามประเภทมัลแวร์ร้ายแรงได้มีประสิทธิผลกว่า ก็จะมีค่าใช้จ่ายประมาณ 2,000–3,000 บาทต่อ 1 license

ทั้งนี้ ค่าใช้จ่ายของแต่ละผลิตภัณฑ์ และรวมถึงคุณสมบัติเทคโนโลยีในการป้องกันที่แตกต่างกันก็ทำให้มีค่าใช้จ่ายที่แตกต่างกันไป และไม่นับถึงเรื่องระบบบริหารจัดการที่ต้องใช้ ก็เป็นอีกปัจจัยหนึ่งที่สำคัญต่อค่าใช้จ่ายที่แตกต่างกันด้วย

สำหรับประมาณการค่าใช้จ่ายโดยการเปรียบเทียบระหว่างมาตรฐานขั้นพื้นฐานกับมาตรฐานขั้นสูง ดังแสดงในตารางที่ 5

ตารางที่ 5 เปรียบเทียบประมาณการค่าใช้จ่ายอุปกรณ์รักษาความมั่นคงปลอดภัยแต่ละมาตรฐาน

รายการ	มาตรฐานขั้นพื้นฐาน จำนวนเงิน (บาท)	มาตรฐานขั้นสูง จำนวนเงิน (บาท)
อุปกรณ์ Firewall ประเภท UTM (พร้อม IPS) จำนวน 2 เครื่องต่อ 1 tier	300,000.- (1 tier)	800,000.- (2 tiers)
โปรแกรม Antivirus (ต่อ license)	500 -1,000 (antivirus ทั่วไป)	2,000 -3,000 (ประเภท EDR)

หมายเหตุ: อุปกรณ์ Firewall ที่มี 2 tiers จะมีราคาสูงกว่าแบบ 1 Tier

3.4 สรุปผลการศึกษา

จากการศึกษาข้างต้นพบว่า ขณะที่มีภัยคุกคามทางไซเบอร์ที่เกิดขึ้นเป็นจำนวนมาก ทั้งในระดับองค์กร ระดับประเทศ และทั่วโลก สถานะระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ. หลายแห่งทั่วโลกนั้น ยังขาดความพร้อมในการจัดการภัยคุกคามที่อาจเกิดขึ้น เนื่องจากแต่ละแห่งมีระบบรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับต่ำ และมีช่องโหว่ในระบบสูง พร้อมกันนั้นยังไม่มีมาตรฐานระบบรักษาความมั่นคงปลอดภัยที่เหมาะสมสำหรับการป้องกันและรับมือกับปัญหาภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้

ด้วยเหตุนี้ ผู้เขียนจึงได้กำหนดและออกแบบมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมกับ สอท./สกญ. แต่ละแห่ง เพื่อให้มีความพร้อมในการรับมือกับภัยคุกคามที่อาจเกิดขึ้น และเอื้ออำนวยให้เจ้าหน้าที่สามารถปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพ

มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ สามารถแบ่งออกเป็น 2 ระดับ ได้แก่ มาตรฐานขั้นพื้นฐาน และมาตรฐานขั้นสูง โดยมาตรฐานขั้นพื้นฐานจะเป็นมาตรฐานที่ สอท./สกญ. ทุกแห่งต้องนำไปปฏิบัติให้เกิดความมั่นคงปลอดภัย สำหรับมาตรฐานขั้นสูงจะเป็นมาตรฐานที่มีความซับซ้อนของระบบมาก และมีอุปกรณ์รักษาความปลอดภัยที่มีประสิทธิภาพมากกว่ามาตรฐานขั้นพื้นฐาน แต่หากนำมาเปรียบเทียบกันแล้ว มาตรฐานขั้นสูงจะมีความเหมาะสมกับ สอท./สกญ. ขนาดใหญ่หรือที่ประสบปัญหาและมีโอกาสต่อการรั่วไหลของข้อมูลสูง หรือมีความเสี่ยงต่อการถูกโจมตี หรือเป็น สอท./สกญ. ที่มีความพร้อมและต้องการไปสู่มาตรฐานขั้นสูง

เนื่องจากการพัฒนาระบบตามมาตรฐานขั้นสูงนั้น จำเป็นต้องใช้งบประมาณที่สูงกว่าการพัฒนาระบบตามมาตรฐานขั้นพื้นฐานอย่างมีนัยสำคัญ ดังนั้นการพัฒนาระบบตามมาตรฐานขั้นสูงจึงเป็นข้อแนะนำหากสามารถนำไปดำเนินการได้โดยไม่มีข้อจำกัดดังกล่าว หากแต่ สอท./สกญ.จะใช้มาตรฐานขั้นพื้นฐานก็เพียงพอต่อการจัดการภัยคุกคามที่อาจเกิดขึ้นได้ในระดับหนึ่ง เนื่องจากทั้งสองมาตรฐานได้รับการออกแบบจากแนวคิดเดียวกัน ที่มีการป้องกัน การตรวจจับภัยคุกคามและง่ายต่อการฟื้นฟู โดยมีการกำหนดคุณสมบัติของอุปกรณ์ระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสม เพื่อที่ระบบจะสามารถทำหน้าที่ตามวัตถุประสงค์ที่วางไว้คือ การรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อรักษาไว้ซึ่งความลับ ความครบถ้วนถูกต้อง และความพร้อมใช้ของระบบอยู่เสมอ

อย่างไรก็ตามระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่ไดรับการออกแบบมาอย่างรอบคอบนี้ ก็ไม่สามารถรับประกันถึงความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างสมบูรณ์

บทที่ 4
บทสรุปและข้อเสนอแนะ

4.1 สรุปผลการศึกษา

มาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ จะถูกแบ่งออกเป็น 2 ระดับ คือ มาตรฐานขั้นพื้นฐาน และมาตรฐานขั้นสูง โดยมาตรฐานขั้นพื้นฐานจะเป็นมาตรฐานหลักที่ สอท./สกญ. ทุกแห่งต้องนำไปพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นมาตรฐานเดียวกันทั่วโลกที่เป็นไปในทิศทางเดียวกัน ขณะที่มาตรฐานขั้นสูงจะเป็นมาตรฐานที่มีความเข้มข้นทางด้านการป้องกันและมีความซับซ้อนของระบบมากกว่า กล่าวคือ

4.1.1 มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นสูง

หมายถึง มาตรฐานระดับเข้มข้นที่แนะนำ หาก สอท./สกญ. มีความพร้อมและสามารถดำเนินการได้ โดยเฉพาะอย่างยิ่งกับ สอท./สกญ. ที่มีความเสี่ยงต่อการรั่วไหลของข้อมูลสูง หรือมีความเสี่ยงต่อการถูกบุกรุกโจมตี หรือเป็น สอท./สกญ. ขนาดใหญ่และมีการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารเป็นจำนวนมาก ซึ่งตามมาตรฐานนี้ ได้ทำการออกแบบโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีการวางอุปกรณ์ไฟร์วอลล์ 2 ชั้น (2 tiers) เพื่อควบคุมการเข้าถึงที่มีประสิทธิภาพมากยิ่งขึ้น อีกทั้งรองรับให้เกิดความพร้อมในการใช้งานอยู่เสมอ จึงได้ออกแบบให้มีอุปกรณ์ไฟร์วอลล์ จำนวน 2 อุปกรณ์ในแต่ละ tier เพื่อเป็นการทำ Redundant ไฟร์วอลล์ และมีระบบ IPS เพื่อใช้ในการตรวจจับการบุกรุกโจมตีอย่างมีประสิทธิภาพอีกด้วย นอกจากนี้ได้มีการแบ่งโซนออกเป็นจำนวนอย่างน้อย 8 โซน เพื่อให้เกิดความมั่นคงปลอดภัยมากยิ่งขึ้น โดยที่ไฟร์วอลล์แต่ละชั้นควรจะเป็นคนละยี่ห้อกันและมีการกำหนดการเข้าถึงเฉพาะเท่าที่จำเป็นเท่านั้นเพื่อให้เกิดความปลอดภัยและป้องกันการบุกรุกโจมตีจากแฮกเกอร์ (hacker) ได้อย่างมีประสิทธิภาพ

4.1.2 มาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน

หมายถึง มาตรฐานขั้นต่ำที่ทุก สอท./สกญ. ต้องนำไปดำเนินการให้เป็นไปตามมาตรฐาน ซึ่งถือว่าเพียงพอต่อการป้องกันภัยคุกคามทางไซเบอร์ได้ในระดับหนึ่ง โดยมีการออกแบบโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอุปกรณ์ไฟร์วอลล์ชั้นเดียว (1 tiers) โดยมีไฟร์วอลล์ จำนวน 2 อุปกรณ์ที่ทำ Redundant กัน เพื่อให้เกิดความพร้อมใช้งานของอุปกรณ์ไฟร์วอลล์อยู่เสมอ นอกจากนี้ ยังได้แบ่งโซนพื้นฐานภายในระบบเครือข่ายออกเป็น 5 โซน เพื่อให้เกิด

ความมั่นคงปลอดภัยมากยิ่งขึ้น นอกจากไฟร์วอลล์แล้ว ยังมีการป้องกันการบุกรุกโจมตีจากระบบ IPS ที่มีมาพร้อมกับอุปกรณ์ไฟร์วอลล์เพื่อใช้ตรวจจับและหยุดการโจมตีที่อาจเกิดขึ้นได้

อย่างไรก็ตาม สิ่งที่สำคัญต่อความปลอดภัยของเครื่องคอมพิวเตอร์ clients และเครื่อง server คือทุกเครื่องจำเป็นต้องติดตั้งโปรแกรมป้องกันไวรัส โดยเฉพาะการเลือกใช้โปรแกรมป้องกันไวรัสและมัลแวร์ที่มีศักยภาพการป้องกันสูงอย่าง endpoint security ก็จะเสริมสร้างความมั่นคงปลอดภัยให้กับเครื่องคอมพิวเตอร์ทุกเครื่องมากยิ่งขึ้น และลดการแพร่กระจายของมัลแวร์ได้อย่างมาก สำหรับข้อมูลที่มีชั้นความลับและที่สำคัญต่อประเทศชาตินั้น จำเป็นต้องมีการเข้ารหัส (encryptions) และมีการควบคุมการเข้าถึงให้เฉพาะผู้ที่มีสิทธิ์ใช้งานเท่านั้น และมีการจัดเก็บด้วยวิธีการอย่างปลอดภัยก็จะลดความเสี่ยงจากการรั่วไหลของข้อมูลสำคัญได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ทุกระบบจำเป็นต้องได้รับการดูแลบำรุงรักษาอยู่เสมออย่างต่อเนื่องและมีการต่ออายุสิทธิการใช้งาน subscriptions เป็นประจำทุกปีด้วยเช่นกัน

เมื่อดำเนินการจัดทำมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศเป็นที่เรียบร้อยแล้ว สอท./สกญ. ก็จะสามารถนำมาตรฐานดังกล่าวไปใช้เป็นเครื่องมือในการพัฒนาปรับปรุงระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐาน อันประกอบด้วย

1) แผนผัง (Diagram) โครงสร้างระบบรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นพื้นฐาน และขั้นสูง

2) มาตรฐานตารางหมายเลข IP Address สำหรับระบบเครือข่ายภายในของ สอท./สกญ. ทั้ง 97 แห่งทั่วโลก ที่มีรูปแบบเป็นมาตรฐานเดียวกัน

3) คุณลักษณะเฉพาะของอุปกรณ์หรือระบบรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ อย่างเช่น อุปกรณ์ไฟร์วอลล์ ระบบ IPS และโปรแกรมหรือระบบป้องกันไวรัส เป็นต้น เพื่อให้ สอท./สกญ. ใช้ประกอบการจัดซื้อระบบฯ เป็นไปในทิศทางเดียวกันอย่างมีมาตรฐาน

4.2 ข้อเสนอแนะ

4.2.1 ข้อเสนอแนะเชิงนโยบาย

1) การได้รับการสนับสนุนจากกระทรวงฯ และการได้รับความร่วมมือจาก สอท./สกญ. ทุกแห่ง

การสร้างมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสถานเอกอัครราชทูตและสถานกงสุลใหญ่ ถือเป็นกลยุทธ์องค์กรที่สำคัญเพื่อกำหนดมาตรฐานระบบเครือข่าย ระบบรักษาความมั่นคงปลอดภัยเครือข่าย และมีการควบคุมการเข้าถึงอย่างมีประสิทธิภาพ อันนำไปสู่องค์กรแห่งความปลอดภัย ดังนั้น การเชิญชวนให้ สอท./สกญ. มาพัฒนาปรับปรุงโครงสร้าง

พื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามมาตรฐานที่กำหนดนั้นอาจไม่ได้รับความสนใจหรือให้ความสำคัญเท่าที่ควร โดยเฉพาะบางแห่งที่ยังไม่เคยประสบปัญหาด้าน security breach ก็อาจไม่ได้รับความร่วมมือในการขับเคลื่อนได้ จึงมีความจำเป็นต้องได้รับการสนับสนุนจากผู้บริหารกระทรวงฯ ทั้งในเชิงนโยบายและด้านงบประมาณ เพื่อให้ สอท./สกญ. สามารถนำไปดำเนินการต่อไปได้

เนื่องจากการผลักดันในระดับนโยบายเพื่อให้ สอท./สกญ. ทุกแห่งดำเนินการตามมาตรฐานนั้น จึงเป็นปัจจัยสู่ความสำเร็จที่สำคัญยิ่งต่อการขับเคลื่อนในภาพรวมได้โดยเร็ว ซึ่งจะนำไปสู่ความมั่นคงปลอดภัยอย่างมีเสถียรภาพและเกิดความยั่งยืนต่อไป อีกทั้งเป็นการรองรับเพื่อนำไปสู่การเปลี่ยนแปลงทางดิจิทัล (Digital Transformation) ของกระทรวงฯ และภาครัฐในอนาคต

2) การจัดทำแผนพัฒนาไปสู่การเป็นมาตรฐาน

เพื่อให้การดำเนินการขับเคลื่อนเป็นไปอย่างมีประสิทธิภาพ จึงจำเป็นต้องมีการจัดทำแผนพัฒนาหรือปรับปรุงสำหรับ สอท./สกญ. นั้น ๆ กับกระทรวงฯ โดยต้องได้รับความเห็นชอบในระดับนโยบายระหว่าง สอท./สกญ. กับศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

3) การทำโครงการ ICT เยือน สอท./สกญ.

การให้การสนับสนุนจากส่วนกลางทั้งในการแก้ไขปัญหา การให้คำปรึกษาและการดำเนินการ การสำรวจตรวจสอบให้เป็นไปตามมาตรฐานนี้ และรวมถึงด้านการใช้งานด้าน ICT ให้แก่ สอท./สกญ. ในลักษณะเดินทางไปเยี่ยมเยียนเป็นประจำทุกปี จะเป็นแรงผลักดันให้เกิดการเปลี่ยนแปลงที่เร็วขึ้นเพื่อให้เกิดการพัฒนาบนพื้นฐานแห่งมาตรฐานเดียวกัน ดังนั้น การนำเสนอโครงการในลักษณะนี้ จักต้องได้รับความเห็นชอบและได้รับการสนับสนุนจากผู้บริหารและที่เกี่ยวข้องด้วยเช่นกัน เนื่องจากจำเป็นต้องมีงบประมาณในการเดินทางและการดำเนินการ

4.2.2 ข้อเสนอแนะในการดำเนินการ

1) สร้างความรู้ความเข้าใจให้กับ สอท./สกญ. และเจ้าหน้าที่ที่เกี่ยวข้อง

การสื่อสารประชาสัมพันธ์ให้เกิดความเข้าใจในนโยบายและแนวทางการดำเนินการจึงเป็นสิ่งสำคัญยิ่งต่อการนำเอามาตรฐานนี้ไปปฏิบัติให้เกิดเป็นรูปธรรม อีกทั้งจำเป็นต้องจัดหลักสูตรฝึกอบรมให้ความรู้ในเรื่องมาตรฐานโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์ การดูแลบำรุงรักษาระบบ และการดำเนินการต่าง ๆ ให้แก่ข้าราชการที่จะออกประจำการ เนื่องจากเป็นเรื่องเกี่ยวข้องกับทางเทคนิคค่อนข้างมาก และบางเรื่องจำเป็นต้องสร้างความเข้าใจที่ตรงกันเพื่อให้เกิดการพัฒนาเป็นไปในแนวทางที่ถูกต้อง และที่สำคัญคือการให้ความร่วมมือกันอย่างเต็มที่ให้ประสบผลสำเร็จ

2) เตรียมทีมงานสนับสนุนทางเทคนิคแก่ สอท./สกญ.

การที่ สอท./สกญ. จะนำเอามาตรฐานดังกล่าวไปดำเนินการได้อย่างถูกต้องและเป็นไปตามเป้าหมายอย่างมีประสิทธิภาพได้นั้น ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจำเป็นต้องให้การสนับสนุนเสมือนพี่เลี้ยง ในการให้คำปรึกษาแนะนำ การสนับสนุนทางด้านเทคนิคและช่วยแก้ปัญหา โดยจัดตั้งทีมงานให้รองรับกับภารกิจดังกล่าว ซึ่งอาจมอบหมายเจ้าหน้าที่รับผิดชอบเป็นรายภูมิภาคก็จะเกิดประสิทธิผลมากขึ้น

3) จัดทำคู่มือมาตรฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับสำนักงานในต่างประเทศ เพื่อให้สถานเอกอัครราชทูตและสถานกงสุลใหญ่ทุกแห่งนำไปใช้เป็นแนวทางปฏิบัติต่อไป

สิ่งสำคัญที่เสมือนเป็นเข็มทิศชี้แนวทางในการพัฒนาปรับปรุงโครงสร้างพื้นฐานระบบรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ สอท./สกญ. ก็คือการจัดทำคู่มือหรือ Guideline ที่อยู่ในรูปไฟล์อิเล็กทรอนิกส์เพื่อประกอบการศึกษาและดำเนินการให้ตรงตามมาตรฐานต่อไป

4) การควบคุมการเข้าถึง

การเข้าใช้งานระบบเครือข่าย ระบบสารสนเทศ หรือเครื่องคอมพิวเตอร์และอุปกรณ์ใดก็ตาม ทั้งในสถานะของผู้ใช้งานทั่วไปหรือแม้แต่ผู้ดูแลระบบ จึงจำเป็นต้องมีการควบคุมการเข้าถึงหรือเข้าใช้งานตามสิทธิ์เท่าที่จำเป็นหรือที่ได้รับเท่านั้น สำหรับระบบไฟร์วอลล์ที่ใช้ป้องกันและควบคุมการเข้าถึงระบบเครือข่ายก็จำเป็นต้องกำหนดกฎหรือนโยบาย (policy) ในการควบคุมการเข้าถึงระบบเครือข่ายหรือสารสนเทศอย่างจำกัดเท่าที่จำเป็นเท่านั้น เนื่องจากการควบคุมการเข้าถึงเป็นสิ่งสำคัญที่สุดอันดับแรกที่ต้องกำหนดให้เหมาะสมและมีความมั่นคงปลอดภัยอย่างที่สุด มิฉะนั้นจะกลายเป็นช่องทางในการนำไปสู่ปัญหาทางด้าน security breach ได้

บรรณานุกรม

ทิฆัมพร วาสิทธิ์. การจัดการเชิงกลยุทธ์. [ออนไลน์]. 2561. แหล่งที่มา: https://sites.google.com/site/krutikamporn/home/bth-thi-9/9-3-kar-kahnd-matrthan. [27 กรกฎาคม 2563]

ไทยเซิร์ต. สถิติภัยคุกคามปี 2562. [ออนไลน์]. 2562. แหล่งที่มา: https://www.thaicert.or.th/statistics/statistics2019.html. [26 กรกฎาคม 2563]

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง รายชื่อหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงานหรือองค์กรที่ถือเป็น โครงสร้างพื้นฐานสำคัญของประเทศซึ่งต้องกระทำตามวิธีการแบบปลอดภัยในระดับเคร่งครัด พ.ศ. 2559. [ออนไลน์]. 2559. แหล่งที่มา: https://ictlawcenter.etda.or.th/laws/detail/noti-criti-infra-2559 [25 กรกฎาคม 2563]

ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553. [ออนไลน์]. 2553. แหล่งที่มา: https://www.etda.or.th/app/webroot/files/1/files/16.pdf. [27 กรกฎาคม 2563]

ปริญญา หอมอเนก. 360 IT Management. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร: บริษัท เออาร์ไอพี จำกัด (มหาชน), 2554.

ภส จันทรศิริ. ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่าย และคอมพิวเตอร์. พิมพ์ครั้งที่ 1. กรุงเทพมหานคร. สำนักงานส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศและการสื่อสาร. 2553.

Cyber Security report. [Online]. 2020. Available from: https://resources.checkpoint.com/cyber-security-resources/cyber-security-report-2020. [2020, August 30]

Gordon, Adam. Guide to the CISSP CBK. 4th edition. New York: CRC Press, 2015.

Narudom Roongsiriwong. Digital Cyber Security. [Online]. 2017. Available from: https://www.dga.or.th/upload/download/. [2020, July 26]

NIST ออกเอกสาร SP 800-184 คู่มือแนะนำวิธีการกู้คืนระบบหลังเกิดเหตุการณ์การโจมตีไซเบอร์. [ออนไลน์]. 2559. แหล่งที่มา: https://www.techtalkthai.com/nist-sp-800-184-guide-for-cybersecurity-event-recovery/ [5 กันยายน 2563]

Retains Full Rights. Infrastructure Security Architecture for Effective Security Monitoring. [PDF]. 2015. Available from: SANS Institute InfoSec Reading Room. [2020, July 26].

Slay, Jill., and Koronios, Andy. Information Technology Security and Risk Management. 3rd edition. Sydney and Melbourne: John Wiley & Sons Australia, Ltd, 2006.

ภาคผนวก

ภาคผนวก ก
การสัมภาษณ์เพื่อแสวงหาข้อมูล

การสัมภาษณ์ข้าราชการของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กระทรวงการต่างประเทศ เมื่อวันที่ 13 กรกฎาคม 2563 ดังมีรายนามต่อไปนี้

1. นายวีระเดช นิ่มเวชอารมณ์ชื่น ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ กรุงเบอร์ลิน
2. นายคำทอง เหลืองเจริญพงศ์ ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ เวียงจันทน์
3. นายพงศกร เถาว์หิรัญ ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ กรุงนิวเดลี
4. นายไกสอน สุวรรณไกษร ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ กรุงย่างกุ้ง
5. นายประหยัด ดิษฐเนตร ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ กรุงกัวลาลัมเปอร์
6. นายโอภาส ฉวีรักษ์ ตำแหน่ง นายช่างไฟฟ้าชำนาญงาน
   ให้ข้อมูลสัมภาษณ์เกี่ยวกับ สอท. ณ กรุงวอชิงตัน ดีซี และ สกญ. ณ นครนิวยอร์ก

วัตถุประสงค์ของการสัมภาษณ์

1. เพื่อทราบเกี่ยวกับโครงสร้างพื้นฐานทางด้านอินเทอร์เน็ต เครื่องคอมพิวเตอร์ Clients และ Servers
2. เพื่อทราบเกี่ยวกับระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของ สอท./สกญ.
3. เพื่อทราบถึงระดับการให้ความสำคัญของข้อมูลชั้นความลับ

คำถามที่ใช้ในการสัมภาษณ์

เป็นลักษณะคำถามให้อธิบายถึงระบบนั้น ๆ ยี่ห้อ รุ่น สเปคหรือขนาด และจำนวน เป็นต้น โดยประเด็นคำถาม ประกอบด้วย

<u>ด้านโครงสร้างพื้นฐานของ สอท./สกญ. ในประเทศนั้น ๆ</u>

1. ความเร็วอินเทอร์เน็ตที่ใช้ และความมีเสถียรภาพ
2. สาธารณูปโภค

3. จำนวนเครื่องคอมพิวเตอร์ Clients และระบบปฏิบัติการที่ใช้
4. กล้อง CCTV
5. โปรแกรม Antivirus ที่ใช้
6. จำนวน VoIP
7. มีการใช้ VPN หรือไม่

<u>ด้านเทคโนโลยีที่ใช้</u>

8. มีไฟร์วอลล์, IPS หรือไม่ ใช้ยี่ห้อใด
9. ระบบเครือข่าย มีการแบ่งแยกหรือไม่ จำนวนโซน
10. จำนวน Access Point สำหรับ Wi–Fi
11. จำนวนเครื่อง Server และสำหรับระบบใด
12. Web Server ใช้ที่กระทรวงฯ หรือพัฒนาเอง
13. ห้องเซิร์ฟเวอร์

<u>ด้านข้อมูลและอื่น ๆ</u>

14. มีข้อมูลลับหรือให้ความสำคัญระดับใด
15. มีทีมไทยแลนด์ที่ใช้งานเทคโนโลยีสารสนเทศภายใต้ระบบเครือข่ายเดียวกับ สอท./สกญ. หรือไม่

ภาคผนวก ข.

ตารางหมายเลข IP Address ภายใน สำหรับสถานเอกอัครราชทูตและสถานกงสุลใหญ่

ตารางกำหนดหมายเลข IP Address ภายใน สำหรับสถานเอกอัครราชทูต

No.	รายชื่อ	IP Address
1	สถานเอกอัครราชทูต ณ กรุงบัวโนสไอเรส	172.x.100.x
2	สถานเอกอัครราชทูต ณ กรุงแคนเบอร์รา	172.x.101.x
3	สถานเอกอัครราชทูต ณ กรุงเวียนนา	172.x.102.x
4	สถานเอกอัครราชทูต ณ กรุงธากา	172.x.103.x
5	สถานเอกอัครราชทูต ณ กรุงบรัสเซลส์	172.x.104.x
6	สถานเอกอัครราชทูต ณ กรุงบราซิเลีย	172.x.105.x
7	สถานเอกอัครราชทูต ณ บันดาร์เสรีเบกาวัน	172.x.106.x
8	สถานเอกอัครราชทูต ณ กรุงพนมเปญ	172.x.107.x
9	สถานเอกอัครราชทูต ณ กรุงออตตาวา	172.x.108.x
10	สถานเอกอัครราชทูต ณ กรุงซันติอาโก	172.x.109.x
11	สถานเอกอัครราชทูต ณ กรุงปักกิ่ง	172.x.110.x
12	สถานเอกอัครราชทูต ณ กรุงปราก	172.x.111.x
13	สถานเอกอัครราชทูต ณ กรุงโคเปนเฮเกน	172.x.112.x
14	สถานเอกอัครราชทูต ณ กรุงไคโร	172.x.113.x
15	สถานเอกอัครราชทูต ณ กรุงปารีส	172.x.114.x
16	สถานเอกอัครราชทูต ณ กรุงเบอร์ลิน	172.x.115.x
17	สถานเอกอัครราชทูต ณ กรุงเอเธนส์	172.x.116.x
18	สถานเอกอัครราชทูต ณ กรุงบูดาเปสต์	172.x.117.x
19	สถานเอกอัครราชทูต ณ กรุงนิวเดลี	172.x.118.x
20	สถานเอกอัครราชทูต ณ กรุงจาการ์ตา	172.x.119.x
21	สถานเอกอัครราชทูต ณ กรุงเตหะราน	172.x.120.x
22	สถานเอกอัครราชทูต ณ กรุงอัมมาน	172.x.121.x
23	สถานเอกอัครราชทูต ณ กรุงแบกแดด	172.x.122.x
24	สถานเอกอัครราชทูต ณ กรุงเทลอาวีฟ	172.x.123.x

No.	รายชื่อ	IP Address
25	สถานเอกอัครราชทูต ณ กรุงโรม	172.x.124.x
26	สถานเอกอัครราชทูต ณ กรุงโตเกียว	172.x.125.x
27	สถานเอกอัครราชทูต ณ กรุงไนโรบี	172.x.126.x
28	สถานเอกอัครราชทูต ณ กรุงโซล	172.x.127.x
29	สถานเอกอัครราชทูต ณ คูเวต	172.x.128.x
30	สถานเอกอัครราชทูต ณ เวียงจันทน์	172.x.129.x
31	สถานเอกอัครราชทูต ณ กรุงกัวลาลัมเปอร์	172.x.130.x
32	สถานเอกอัครราชทูต ณ กรุงเม็กซิโก	172.x.131.x
33	สถานเอกอัครราชทูต ณ กรุงราบัต	172.x.132.x
34	สถานเอกอัครราชทูต ณ กรุงย่างกุ้ง	172.x.133.x
35	สถานเอกอัครราชทูต ณ กรุงกาฐมาณฑุ	172.x.134.x
36	สถานเอกอัครราชทูต ณ กรุงเฮก	172.x.135.x
37	สถานเอกอัครราชทูต ณ กรุงเวลลิงตัน	172.x.136.x
38	สถานเอกอัครราชทูต ณ กรุงออสโล	172.x.137.x
39	สถานเอกอัครราชทูต ณ กรุงมัสกัต	172.x.138.x
40	สถานเอกอัครราชทูต ณ กรุงอิสลามาบัด	172.x.139.x
41	สถานเอกอัครราชทูต ณ กรุงมะนิลา	172.x.140.x
42	สถานเอกอัครราชทูต ณ กรุงวอร์ซอ	172.x.141.x
43	สถานเอกอัครราชทูต ณ กรุงลิสบอน	172.x.142.x
44	สถานเอกอัครราชทูต ณ กรุงบูคาเรสต์	172.x.143.x
45	สถานเอกอัครราชทูต ณ กรุงมอสโก	172.x.144.x
46	สถานเอกอัครราชทูต ณ กรุงริยาด	172.x.145.x
47	สถานเอกอัครราชทูต ณ กรุงดาการ์	172.x.146.x
48	สถานเอกอัครราชทูต ณ สิงคโปร์	172.x.147.x
49	สถานเอกอัครราชทูต ณ กรุงพริทอเรีย	172.x.148.x
50	สถานเอกอัครราชทูต ณ กรุงมาดริด	172.x.149.x
51	สถานเอกอัครราชทูต ณ กรุงโคลัมโบ	172.x.150.x
52	สถานเอกอัครราชทูต ณ กรุงสตอกโฮล์ม	172.x.151.x
53	สถานเอกอัครราชทูต ณ กรุงเบิร์น	172.x.152.x

No.	รายชื่อ	IP Address
54	สถานเอกอัครราชทูต ณ กรุงอังการา	172.x.153.x
55	สถานเอกอัครราชทูต ณ กรุงอาบูดาบี	172.x.154.x
56	สถานเอกอัครราชทูต ณ กรุงลอนดอน	172.x.155.x
57	สถานเอกอัครราชทูต ณ กรุงวอชิงตัน	172.x.156.x
58	สถานเอกอัครราชทูต ณ กรุงฮานอย	172.x.157.x
59	สถานเอกอัครราชทูต ณ กรุงมานามา	172.x.158.x
60	สถานเอกอัครราชทูต ณ กรุงโดฮา	172.x.159.x
61	สถานเอกอัครราชทูต ณ กรุงดิลี	172.x.160.x
62	สถานเอกอัครราชทูต ณ กรุงเฮลซิงกิ	172.x.161.x
63	สถานเอกอัครราชทูต ณ กรุงอาบูจา	172.x.162.x
64	สถานเอกอัครราชทูต ณ กรุงอัสตานา	172.x.163.x
65	สถานเอกอัครราชทูต ณ กรุงตริโปลี	172.x.164.x
66	สถานเอกอัครราชทูต ณ กรุงลิมา	172.x.165.x
67	สถานเอกอัครราชทูต ณ กรุงมาปูโต	172.x.166.x

ตารางกำหนดหมายเลข IP Address ภายในของสถานกงสุลใหญ่

No.	รายชื่อ	IP Address
1	สถานกงสุลใหญ่ ณ นครซิดนีย์	172.x.200.x
2	สถานกงสุลใหญ่ ณ นครแวนคูเวอร์	172.x.201.x
3	สถานกงสุลใหญ่ ณ นครเฉิงตู	172.x.202.x
4	สถานกงสุลใหญ่ ณ เมืองเซี่ยเหมิน	172.x.203.x
5	สถานกงสุลใหญ่ ณ เมืองซีอาน	172.x.204.x
6	สถานกงสุลใหญ่ ณ นครหนานหนิง	172.x.205.x
7	สถานกงสุลใหญ่ ณ นครกวางโจว	172.x.206.x
8	สถานกงสุลใหญ่ ณ เมืองชิงต่าว	172.x.207.x
9	สถานกงสุลใหญ่ ณ เมืองฮ่องกง	172.x.208.x
10	สถานกงสุลใหญ่ ณ นครคุนหมิง	172.x.209.x
11	สถานกงสุลใหญ่ ณ นครเซียงไฮ้	172.x.210.x
12	สำนักงานการค้าและเศรษฐกิจไทย	172.x.211.x
13	สถานกงสุลใหญ่ ณ นครแฟรงเฟิร์ต	172.x.212.x
14	สถานกงสุลใหญ่ ณ เมืองกัลกัตตา	172.x.213.x
15	สถานกงสุลใหญ่ ณ เมืองมุมไบ	172.x.214.x
16	สถานกงสุลใหญ่ ณ เมืองเจนไน	172.x.215.x
17	สถานกงสุลใหญ่ ณ นครโอซากา	172.x.216.x
18	สถานกงสุลใหญ่ ณ แขวงสะหวันนะเขต	172.x.217.x
19	สถานกงสุลใหญ่ ณ เมืองโกตาบารู	172.x.218.x
20	สถานกงสุลใหญ่ ณ เมืองปีนัง	172.x.219.x
21	สถานกงสุลใหญ่ ณ เมืองการาจี	172.x.220.x
22	สถานกงสุลใหญ่ ณ เมืองเจดดาห์	172.x.221.x
23	สถานกงสุลใหญ่ ณ เมืองดูไบ	172.x.222.x
24	สถานกงสุลใหญ่ ณ นครชิคาโก	172.x.223.x
25	สถานกงสุลใหญ่ ณ นครลอสแอนเจลิส	172.x.224.x
26	สถานกงสุลใหญ่ ณ นครนิวยอร์ก	172.x.225.x
27	สถานกงสุลใหญ่ ณ นครโฮจิมินห์	172.x.226.x

No.	รายชื่อ	IP Address
28	สถานกงสุลใหญ่ ณ กรุงอันตานานาริโว	172.x.227.x
29	สถานกงสุลใหญ่ ณ นครมิวนิก	172.x.228.x
30	สถานกงสุลใหญ่ ณ เมืองฟูกูโอกะ	172.x.229.x

ตารางกำหนดหมายเลข IP Address ภายใน สำหรับคณะผู้แทนถาวรไทย

No.	รายชื่อ	IP Address
1	คณะผู้แทนถาวรไทยประจำอาเซียน ณ กรุงจาการ์ตา	172.x.250.x
2	คณะทูตถาวรฯ ณ นครเจนีวา	172.x.251.x
3	คณะทูตถาวรฯ ณ นครนิวยอร์ก	172.x.252.x

ภาคผนวก ค.
มาตรฐานคุณลักษณะเฉพาะของระบบรักษาความมั่นคงปลอดภัยไซเบอร์

คุณลักษณะเฉพาะของระบบรักษาความมั่นคงปลอดภัยไซเบอร์

1. คุณลักษณะเฉพาะอุปกรณ์ไฟร์วอลล์ (Firewall)

1.1 เป็นอุปกรณ์ไฟร์วอลล์ แบบ Appliance ที่สร้างขึ้นเพื่อทำหน้าที่ตรวจจับและควบคุม Application, User, Content เป็นอย่างน้อย

1.2 มี Network Interface แบบ 10/100/1000 Copper ไม่น้อยกว่า 8 พอร์ท

1.3 มี Interface แบบ 10/100/1000 สำหรับบริหารจัดการโดยเฉพาะ (Out of Band Management) ไม่น้อยกว่า 1 พอร์ท โดยทั้งหมดไม่นับรวมกับ interface จากข้อที่ 2

1.4 มี Application Firewall Throughput หรือ NGFW Throughput ไม่น้อยกว่า 500 Mbps ในแบบ Appmix หรือ Enterprise testing condition หรือ Enterprise traffic mix

1.5 มี Threat prevention Throughput ไม่น้อยกว่า 250 Mbps และจำนวน Max Sessions ได้ไม่น้อยกว่า 60,000 sessions และ New Sessions ไม่น้อยกว่า 4,000 ต่อวินาที

1.6 สามารถติดตั้งในรูปแบบ Transparent Inline, Non–Inline Monitoring (Tap), L2 และ L3 ได้โดยสามารถติดตั้งรูปแบบดังกล่าวได้พร้อมกันบนตัวอุปกรณ์โดยไม่ต้องแบ่ง Virtual System หรือ Virtual Domain

1.7 สามารถสร้าง VLAN ตามมาตรฐาน 802.1Q VLAN tags ได้ไม่น้อยกว่า 4094 VLANs ต่ออุปกรณ์

1.8 สามารถทำการตรวจสอบทราฟฟิคที่เข้ารหัส SSL ด้วยการทำ SSL decryption (ทั้งแบบ Inbound และ Outbound)

1.9 สามารถทำงานร่วมกับระบบการพิสูจน์ตัวตน (Authentication Systems) ได้แก่ Active Directory, LDAP, Radius เพื่อทำการติดตามผู้ใช้ได้เป็นอย่างน้อย

1.10 สามารถป้องกันภัยคุกคามประเภท Vulnerability และ Spyware ได้โดยสามารถมีการอัพเดท Signature ใหม่แบบอัตโนมัติได้

1.11 สามารถกำหนดนโยบายการเข้าถึง website (URL Filtering) สามารถติดตามและควบคุมการเข้าถึงเว็บได้ตาม Category, Block list, Allow list ที่กำหนดได้ และสามารถจัด category ให้กับแต่ละ website ไม่น้อยกว่า 2 category (Multi–Category)

1.12 มีระบบตรวจจับ Advanced Malware แบบ Cloud–Based ที่ใช้เทคโนโลยีแบบ Sandbox เพื่อใช้ระบุ Malware ประเภทใหม่ (Zero–day Malware) ซึ่งไม่มีใน Signature มา

ก่อน โดยสามารถแสดงรายละเอียดการทำงานของ Malware ในรูปแบบ Report และสามารถสร้าง Signature ขึ้นมาเพื่อใช้ป้องกันระบบเครือข่ายได้โดยอัตโนมัติ

1.13 สามารถทำรายงานรวมถึงปรับแต่งรายงานตามความต้องการ ในรูปแบบ PDF ได้เป็นอย่างน้อย พร้อมทั้งตั้งเวลาส่งรายงานผ่านทาง Email แบบอัตโนมัติได้

1.14 สามารถจัดเก็บบันทึกข้อมูลโดยส่ง Syslog, Netflow และ SNMP ไปยังระบบจัดการเครือข่ายที่รองรับคุณสมบัติดังกล่าวได้

1.15 สามารถบริหารจัดการผ่านทาง GUI Software หรือ Web User Interface และ Command Line Interface ได้

1.16 รองรับการติดตั้งเพื่อทำ High Availability แบบ Active–Active และ Active–Passive ได้

1.17 มีแหล่งจ่ายไฟฟ้า (Power Supply) แบบ redundant

1.18 ต้องได้รับการรับรองมาตรฐานดังนี้ FCC และ VCCI เป็นอย่างน้อย

1.19 รับประกันอุปกรณ์เป็นเวลาอย่างน้อย x ปี

2. คุณลักษณะอุปกรณ์ป้องกันและตรวจจับการบุกรุก IPS (Intrusion Prevention System) ** กรณีที่ระบบเครือข่ายขนาดเล็กและไม่ซับซ้อน สามารถใช้ IPS ที่เป็นโมดูลมาพร้อมกับ ไฟร์วอลล์ได้ **

2.1 เป็นอุปกรณ์ IPS ที่เป็นแบบAppliance ทำหน้าที่ป้องกันการบุกรุกเครือข่าย

2.2 มี IPS Throughput ไม่น้อยกว่า 600 Mbps

2.3 สามารถตรวจจับการบุกรุกและป้องกันเครือข่ายได้อย่างน้อย ดังนี้ Signature matching, Protocol, Anomalies, Overflow, Worm, Virus, Backdoor, Program, Trojan Horse, Port Scanning, Spyware, Packet Analysis,DOS, DDOS

2.4 สามารถทำงานได้อย่างน้อย ..... segments ภายใต้ IPS mode

2.5 สามารถบริหารจัดการผ่านมาตรฐาน HTTPS หรือ SSH ได้เป็นอย่างน้อย

2.6 สามารถเก็บและส่ง Log ในรูปแบบ Syslog ได้

2.7 สามารถใช้งานตามมาตรฐาน IPV4 และ IPV6 ได้

3. คุณลักษณะโปรแกรมป้องกันไวรัส

3.1 มี Agent ที่สามารถติดตั้งลงบนระบบปฏิบัติการ ดังต่อไปนี้ได้ Windows 8, Windows 8.1, Window 10, Windows Server 2008 R2, Windows Server 2012, Windows Server 2016 ได้เป็นอย่างน้อย

3.2 สามารถติดตั้ง Agent บนเครื่องลูกข่าย (Clients) ได้อย่างน้อยดังนี้

3.3 สามารถตรวจจับมัลแวร์ (Malware Detection) ดังต่อไปนี้ virus, trojan, worm, spyware, adware, rootkit และ potentially unwanted program บนเครื่องลูกข่ายได้

3.4 สามารถตรวจจับ, ป้องกันและแจ้งเตือน อันตรายจากภัยต่างๆ จากโปรแกรมไม่พึงประสงค์ (Malware) โดยใช้เทคนิคดังต่อไปนี้

1) Signature Base

2) Cloud Reputation

3) Behavior base

3.5 สามารถทำการตรวจจับ (Detect) การโจมตีผ่านช่องโหว่ทางความปลอดภัย (Exploit) แบบ Zero–day ได้

3.6 สามารถควบคุมการใช้งานอุปกรณ์จำพวก Removable drive ,CD/DVD, Bluetooth device เพื่อจำกัดการให้ใช้หรือไม่ให้ใช้งานได้ ในระดับผู้ใช้งาน พร้อมทั้งสามารถกำหนดไม่ให้อ่านหรือเขียนไฟล์ลงไปในอุปกรณ์ดังกล่าวได้

3.7 รองรับการส่งไฟล์ที่ต้องสงสัย (Unknown File) จากเครื่องคอมพิวเตอร์ลูกข่ายได้ไปวิเคราะห์ผ่านระบบป้องกัน APT หรือ Sandbox ในอนาคตได้

3.8 สามารถเชื่อมต่อกับระบบฐานข้อมูลของภัยคุกคามขั้นสูง (Threat Intelligence) จากเจ้าของผลิตภัณฑ์เพื่อรับข้อมูลชื่อเสียงของไฟล์ที่ต้องสงสัย (Reputation) เพื่อใช้ในการตรวจสอบภัยคุกคามที่ตรวจพบในระบบได้

3.9 มีระบบตรวจสอบอุปกรณ์ที่ติดตั้ง Agent ในระบบและอุปกรณ์ที่ไม่มี Agent ได้

3.10 สามารถบริหารจัดการนโยบายของระบบที่เสนอได้จากจุดเดียว (Centralized Management) และสามารถส่งคำสั่งลบโปรแกรมป้องกันความปลอดภัยและ Agent ได้

ประวัติผู้เขียน

ชื่อ–สกุล ชูเกียรติ ประเสริฐสุข

ประวัติการศึกษา
– วิทยาศาสตรบัณฑิต สาขา สถิติ มหาวิทยาลัยรามคำแหง
– วิทยาศาสตรมหาบัณฑิต สาขาการจัดการเทคโนโลยีสารสนเทศ มหาวิทยาลัยวลัยลักษณ์

ประวัติการทำงาน

พ.ศ. 2536	เจ้าหน้าที่ระบบงานคอมพิวเตอร์ 3 กองคำนวณและประมวลผล กรมที่ดิน
พ.ศ. 2538	เจ้าหน้าที่ระบบงานคอมพิวเตอร์ 4 กองคำนวณและประมวลผล กรมที่ดิน
พ.ศ. 2540	นักวิชาการคอมพิวเตอร์ 5 กองคำนวณและประมวลผล กรมที่ดิน
พ.ศ. 2541	นักวิชาการคอมพิวเตอร์ 5 ศูนย์ข้อมูล สำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ
พ.ศ. 2545	นักวิชาการคอมพิวเตอร์ 6ว ศูนย์ข้อมูล สำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ
พ.ศ. 2547	นักวิชาการคอมพิวเตอร์ 7วช ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสารสำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ
พ.ศ. 2551	นักวิชาการคอมพิวเตอร์ชำนาญการ ศูนย์เทคโนโลยีสารสนเทศ และการ สื่อสารสำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ

ตำแหน่งปัจจุบัน นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวง กระทรวงการต่างประเทศ