แผนรับมือภัยคุกคามระบบสารสนเทศ
ศูนย์สารสนเทศ กรมควบคุมโรค

หลักการและเหตุผล

ระบบเครือข่ายคอมพิวเตอร์ รวมถึงระบบข้อมูลสารสนเทศ ถือเป็นทรัพยากรที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาให้มีความถูกต้องและปลอดภัย เพื่อให้มั่นใจว่าระบบเครือข่ายคอมพิวเตอร์ และระบบข้อมูลสารสนเทศสามารถใช้ได้งานได้ตามปกติ ส่งเสริมสนับสนุนการปฏิบัติตามภารกิจของกรมควบคุมโรคได้

ศูนย์สารสนเทศได้ตระหนักถึงภัยคุกคามระบบสารสนเทศ ทั้งในรูปแบบไวรัสคอมพิวเตอร์ การโจมตีระบบ ศูนย์สารสนเทศจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยคุกคามระบบสารสนเทศ ของกรมควบคุมโรค (IT Contingency Plan) เพื่อเป็นกรอบ แนวทางในการแก้ไขปัญหาเมื่อเกิดภัยคุกคามระบบสารสนเทศ ให้ระบบสารสนเทศสามารถใช้งานได้ตามปกติหรือจำกัดความเสียหายให้น้อยที่สุด ตลอดจนการดูแลรักษาระบบสารสนเทศให้มีเสถียรภาพ พร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

วัตถุประสงค์

1. เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ
2. เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้การปฏิบัติราชการ ดำเนินไปได้อย่างมีเสถียรภาพ
4. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยด้านเทคโนโลยีสารสนเทศของกรมควบคุมโรค

1. การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางระบบสารสนเทศ

1.1 การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการ ศูนย์สารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

1.2 กระบวนการดำเนินงาน (Procedure)

ศูนย์สารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมข้อมูลหลักฐานเพื่อหาช่องโหว่ วิธีการที่ถูกโจมตีหรือระบุตัวผู้โจมตี เพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างถูกต้อง ทันเวลา และสามารถป้องกันการโจมตีในลักษณะเดิม ระบบงานต่างๆ ที่มีความสำคัญต้องมีการสำรองข้อมูล เพื่อความพร้อมในการกู้คือข้อมูลหากข้อมูลความเสียหายจากการถูกโจมตี

1.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข, สำนักบริหารเทคโนโลยีสารสนเทศภาครัฐ, ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCert) เป็นต้น

1.4 การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยคุกคามที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์สารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม antivirus/spyware
- แผ่น driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

1.5 การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับข้อมูลหรือระบบงาน จากภัยคุกคามระบบสารสนเทศ ให้สามารถกู้คืนข้อมูลที่เสียหายหรือถูกทำลายกลับมาได้ให้มากที่สุด ให้การดำเนินงานขององค์กรมีความต่อเนื่อง โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

1.6 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

1) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากกรณีจำเป็นให้มีเจ้าหน้าที่ของศูนย์สารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องสแกนลายนิ้วมือ เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย

2) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลาและมีการ Monitor เป็นประจำ

3) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

4) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

5) มีการทำระบบ Authentication โดยมีการ Login ชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

6) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

7) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

2. การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่แผนกต่างๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

1) ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

2) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

3) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

3. กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

3.1 เจ้าหน้าที่ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้ความเสียหายแพร่กระจายในวงกว้าง โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบประกอบด้วย

นางสาวสุพจนา คุ้มวงษ์ เบอร์โทรศัพท์ติดต่อ 085-994-3328
นายจักรพันธ์ ยมวาน เบอร์โทรศัพท์ติดต่อ 094-487-7313
นายวรรณวิทย์ คล้ายบุญส่ง เบอร์โทรศัพท์ติดต่อ 089-033-0660
นายศุภเสกย์ ทิพยาวงษ์ เบอร์โทรศัพท์ติดต่อ 087-104-6440
นายชันรัฐ เอมะรุจิ เบอร์โทรศัพท์ติดต่อ 082-989-0067

3.2 แจ้งหัวหน้ากลุ่มสนับสนุนระบบบริการ นายสมชาย เวียงพิทักษ์ ทางโทรศัพท์ 084-164-2568 เพื่อทราบ และดำเนินการสั่งการให้ทีมที่ได้รับมอบหมายเข้าควบคุมสถานการณ์ ให้ระบบงานหรือเครือข่ายได้รับความเสียหายน้อยที่สุด และสามารถกลับมาใช้งานได้ตามปกติโดยเร็วที่สุด

4. ขั้นตอนการปฏิบัติการและกู้คืนระบบ กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

4.1 ตรวจสอบภัยคุกคาม

1) ตรวจสอบภัยคุกคามระบุสาเหตุ เพื่อแก้ไขปัญหาเบื้องต้นในทันที
2) รายงานหัวหน้ากลุ่ม และเรียกประชุมทีมงานที่เกี่ยวข้องเพื่อติดตามสถานการณ์
3) วิเคราะห์ข้อมูลถึงความร้ายแรงของผลกระทบที่เกิดขึ้น

4.2 ควบคุมภัยคุกคาม

1) ควบคุมภัยคุกคามเพื่อบรรเทาความเสียหายที่เกิดขึ้นให้ส่งผลกระทบน้อยที่สุด
2) ระบุช่องว่างหรือแหล่งที่มาของภัยคุกคามในระบบเพื่อปิดช่องทางโจมตีเบื้องต้น

4.3 แก้ไขปัญหา

1) วิเคราะห์และหาสาเหตุของภัยคุกคามฯที่เกิดขึ้น และพร้อมดำเนินการแก้ไขเพื่อกำจัดเหตุ
2) หากไม่สามารถแก้ไขได้ให้ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert) เพื่อขอคำแนะนำหรือความช่วยเหลือ
3) กำจัดข้อมูล โปรแกรม หรือสิ่งแปลกปลอมทั้งหลายออกจากระบบ
4) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่นๆ
5) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

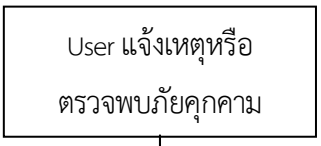
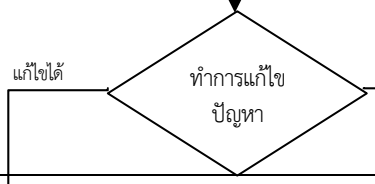
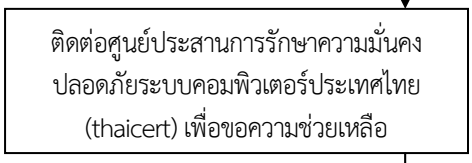
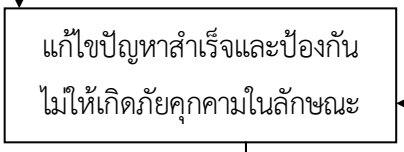
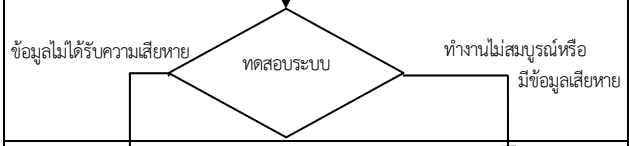
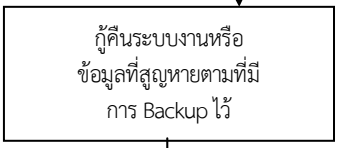
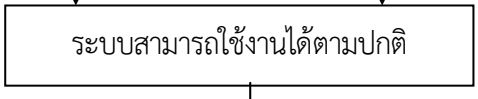
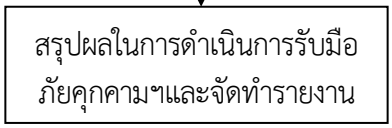
4.4 กู้คืนระบบคอมพิวเตอร์

1) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่
2) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)
3) อุดช่องโหว่ในระบบเครือข่าย
4) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

4.5 สรุปรายงานผลการดำเนินงาน

1) สรุปผลการดำเนินการในการรับมือภัยคุมคามฯ รายงานต่อผู้บังคับบัญชา
2) แจ้งผลการดำเนินงานให้ผู้เกี่ยวข้องทราบ

Flowchart แสดงขั้นตอนการปฏิบัติ กรณีภัยคุกคามระบบสารสนเทศ

เหตุการณ์	รายละเอียด
	จากการเฝ้าระวังตรวจสอบ Log จะช่วยให้ตรวจพบภัยคุกคามก่อนที่จะสร้างเสียหายในวงกว้าง
	ตรวจสอบถึงชนิดประเภท ความรุนแรงและกระทบที่คาดว่าจะเกิดกับระบบ
	ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ เช่น ปิดระบบ, ตัดการเชื่อมต่อ เป็นต้น
	แก้ไขหรือสามารถกำจัดภัยคุกคามได้ในเบื้องต้นให้ทำการแก้ไขในทันที
	หากไม่สามารถแก้ไขได้ให้ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert) เพื่อขอคำแนะนำหรือความช่วยเหลือ
	เมื่อแก้ไขภัยคุกคามได้สำเร็จให้ตรวจหาช่องโหว่และทำการป้องกันเพื่อไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำ
	ตรวจสอบการใช้งานระบบว่าทำงานได้ปกติหรือมีข้อมูลสูญหายหรือไม่
	หากพบว่ามีความเสียหายให้กู้คืนข้อมูลหรือระบบตามที่มีการ Backup ไว้
	ระบบอยู่ในสภาพการให้บริการตามปกติ
	สรุปผลในการดำเนินการรับมือภัยคุกคามฯ รวมทั้ง แจ้งผลการดำเนินการให้ผู้ที่เกี่ยวข้องรับทราบ และบันทึกรายงานการดำเนินงานเพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง

กำหนดหน้าที่ความรับผิดชอบบุคลากรในองค์กร

ข้อมูลขององค์กร

รายละเอียด	
ชื่อองค์กร	ศูนย์สารสนเทศ กรมควบคุมโรค
ที่อยู่	88/21 ถนนติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี 11000
สถานที่ตั้ง	ตึกกรมควบคุมโรค อาคาร 2 ชั้น 3 กระทรวงสาธารณสุข
เบอร์โทรศัพท์	02-590-3093
เบอร์โทรศัพท์สำรอง	02-965-9576
อีเมล์	thaiddc.ict@ddc.mail.go.th

คณะทำงานหลัก – การติดต่อและบทบาทหน้าที่

ชื่อ สกุล	**โทรศัพท์ที่ทำงาน**	**โทรศัพท์นอกสถานที่ทำงาน**	**บทบาทหน้าที่ต่อเตรียมความพร้อมสำหรับภัยคุกคามระบบสารสนเทศ**	**ผู้รับผิดชอบรอง**
นายแพทย์สมศักดิ์ ไชยวัฒน์	0-2590-3093	-	- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ให้คำปรึกษา ตัดสินใจ สั่งการและควบคุมการดำเนินงาน - รับรายงานให้สรุปผลการดำเนินงานให้ข้อเสนอแนะหลังการดำเนินงาน	
นายสมชาย เวียงพิทักษ์	0-2590-3093	089-667-6109	- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นางสาวสุพจนา คุ้มวงษ์	0-2590-3093	085-994-3328	- Monitor ระบบ ลิงค์, AD, Firewall - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ	

			ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายจักรพันธ์ ยมวนา	0-2590-3093	094-487-7313	- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายชัยรัฐ เอมะรุจิ	0-2590-3093	082-989-0067	- ประสานงานผู้ติดต่อภายนอก - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	

นายวรรณวิทย์ คล้ายบุญส่ง	0-2590-3093	089-033-0660	- Monitor ระบบ ลิงค์, AD, Firewall - Backup ฐานข้อมูล - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายศุภเสกย์ ทิพยยาวงษ์	0-2590-3093	087-104-6440	- Monitor ระบบ ลิงค์, AD, Firewall - Backup ฐานข้อมูล - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายสัตวแพทย์ พรพิทักษ์ พันธุ์หล้า			- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ให้การสนับสนุนและตัดสินใจ	
นายวรวิทย์ พยุงเกียรติบวร	0-2590-3093	081-755-8080	- Backup ฐานข้อมูล - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ	

			- ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายชัยรัตน์ ปรีชากร	0-2590-3093	086-520-6276	- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นางจันทร์เพ็ญ เอกมอญ	0-2590-3093	086-570-9368	- เผยแพร่ข้อมูลลง Social - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายชาญวิทย์ อมรสุรินทวงศ์	0-2590-3093	086-553-8372	- Backup ฐานข้อมูล - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อ	

			ตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุดอื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นางสาวชนนี ขันวงษ์	0-2590-3093	081-390-9266	- ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ - ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน - ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลามหรือขยายวงไปยังจุด อื่นๆ - การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น - ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	
นายปรีชา ภูมิพื้นผล	0-2590-3093	089-492-5704	- รับเรื่องภัยคุกคาม - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ	
นางฐิติยา ภูริศรี	0-2590-3093	089-825-2362	- รับเรื่องภัยคุกคาม - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ	
นางพรรณี รัตนวงศ์วิจิตร	0-2590-3093	087-804-2531	- รับเรื่องภัยคุกคาม - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ	
นางเกตน์สิรี พุ่มระย้า	0-2590-3093	086-905-8497	- รับเรื่องภัยคุกคาม - ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ	

รายละเอียดผู้ที่ติดต่อภายนอก

องค์กร	ชื่อ สกุล	โทรศัพท์ที่ทำงาน	โทรศัพท์นอกสถานที่ทำงาน
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข	คุณชวลิต คุณราชิ	0-2590-1201 0-2590-1169	
สำนักบริหารเทคโนโลยีสารสนเทศภาครัฐ	คุณปรัสตยุ เทียมทอง	0-2612-6060	089-722-3731
บริษัท สมาร์ท เทคโนโลยี โซลูชั่น จำกัด	คุณเทอรดพัน สหตรงจิตร คุณศุภโชค ณ ระนอง	0-2383-8931-3	089-444-8554 086-311-0422
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (thaicert)	-	0-2590-3033	084-529-7712 081-855-1400
บริษัท ดีเอ็กซ์พี (ไทยแลนด์) จำกัด	นายพงศ์อมร พัฒนพงศ์โสภณ	0-2590-3093	081-904-4669

ขั้นตอนการปฏิบัติของทีมงาน

ทีม : กลุ่มบริหารจัดการเทคโนโลยีสารสนเทศ		ผู้จัดการ : นายปรีชา ภูมิพื้นผล		
		ผู้จัดการสำรอง : นางฐิติยา ภูริศรี		
ขั้นตอนการปฏิบัติ	**กิจกรรม**			
	ก่อนการถูกโจมตี -	**ผู้รับผิดชอบ** -		**เอกสาร/ทรัพยากร** -
	ระหว่างการถูกโจมตี 1. รับเรื่องภัยคุกคามและแจ้งไปผู้รับผิดชอบ	**ผู้รับผิดชอบ** กลุ่มบริหารจัดการเทคโนโลยีสารสนเทศ	**เวลาที่ใช้ (นาที)** 1-5	**เอกสาร/ทรัพยากร** - โทรศัพท์,คอมพิวเตอร์
	หลังการถูกโจมตี -	**ผู้รับผิดชอบ**	**เวลาที่ใช้ (นาที)**	**เอกสาร/ทรัพยากร**
ทีม : กลุ่มสนับสนุนระบบบริการ		ผู้จัดการ : นายสมชาย เวียงพิทักษ์		
		ผู้จัดการสำรอง : นายศุภเสกย์ ทิพยยาวงษ์		
ขั้นตอนการปฏิบัติ	**กิจกรรม**			
1. ประชุมกลุ่มสนับสนุนระบบบริการ เพื่อพิจารณาแนวทาง วิธีการดำเนินงาน รวมทั้งการมอบหมายงานภายในกลุ่ม 2. พิจารณามอบหมายงานเจ้าหน้าที่ภายในกลุ่ม และหรือเจ้าหน้าที่ในทีมอื่น ให้ปฏิบัติงานแทนกรณีเหตุ	**ก่อนการถูกโจมตี** 1. เฝ้าระวังตรวจสอบความผิดปกติของระบบ 2. ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ 3. มีกระบวนการ Backup ข้อมูลตามแผน 4. จัดทำคู่มือการกู้คืนระบบและแก้ไขปัญหาเบื้องต้น	**ผู้รับผิดชอบ** นายวรรณวิทย์ คล้ายบุญส่ง, นายศุภเสกย์ ทิพยยาวงษ์, นายจักรพันธ์ ยมวนา, นางสาวสุพจนา คุ้มวงษ์ กลุ่มสนับสนุนระบบบริการ นายวรรณวิทย์ คล้ายบุญส่ง, นายศุภเสกย์ ทิพยยาวงษ์ กลุ่มสนับสนุนระบบบริการ		**เอกสาร/ทรัพยากร** - ระบบ Monitor, คอมพิวเตอร์ - คอมพิวเตอร์ - คอมพิวเตอร์ - คู่มือการกู้คืนระบบ,แก้ไข

	5. จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งการซ้อมปฏิบัติ	กลุ่มสนับสนุนระบบบริการ		ปัญหาเบื้องต้น,เอกสารข่าวสาร - คอมพิวเตอร์
	ระหว่างการถูกโจมตี	**ผู้รับผิดชอบ**	**เวลาที่ใช้ (นาที)**	**เอกสาร/ทรัพยากร**
	1. รับแจ้งเหตุภัยคุกคาม	กลุ่มสนับสนุนระบบบริการ	5	- โทรศัพท์,คอมพิวเตอร์
	2. ตรวจพบภัยคุกคามจากระบบ Monitor	นายวรรณวิทย์ คล้ายบุญส่ง, นายศุภเสกย์ ทิพยยาวงษ์, นายจักรพันธ์ ยมวนา, นางสาวสุพจนา คุ้มวงษ์	5	- คอมพิวเตอร์
	3. ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ และระบุถึงหน่วยงาน	กลุ่มสนับสนุนระบบบริการ	15	- คอมพิวเตอร์
	4. ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ	กลุ่มสนับสนุนระบบบริการ	5-10	- คอมพิวเตอร์
	5. การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น	กลุ่มสนับสนุนระบบบริการ	5-60	- คอมพิวเตอร์
	6. ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	กลุ่มสนับสนุนระบบบริการ	30	- คอมพิวเตอร์
	7. ประสานงานผู้ติดต่อภายนอก	นายสมชาย เวียงพิทักษ์, นายชัยรัฐ เอมะรุจิ	5-10	- โทรศัพท์,คอมพิวเตอร์
	หลังการถูกโจมตี	**ผู้รับผิดชอบ**	**เวลาที่ใช้ (นาที)**	**เอกสาร/ทรัพยากร**
	1. ตรวจสอบการทำงานของระบบและข้อมูลว่าถูกกระทบจากการโจมตีแค่ไหน	กลุ่มสนับสนุนระบบบริการ	30	- คอมพิวเตอร์

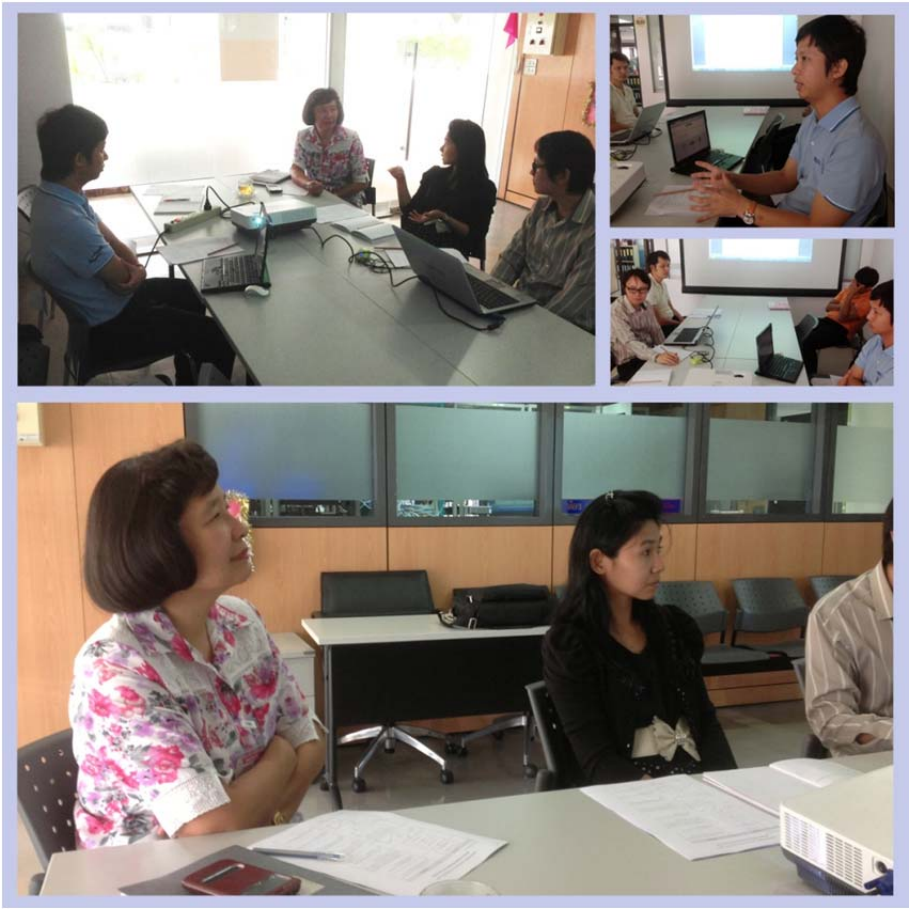
	2. การกู้คืนระบบหรือข้อมูล ให้อยู่ในสภาพพร้อมบริการ 3. ประเมินผลในการดำเนินการรับมือ 4. บันทึกรายงานการดำเนินงาน เพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง	นายวรรณวิทย์ คล้ายบุญส่ง, นายศุภเสกย์ ทิพยยาวงษ์ กลุ่มสนับสนุนระบบบริการ นางสาวสุพจนา คุ้มวงษ์, นายศุภเสกย์ ทิพยยาวงษ์	60 30 60-120	- คอมพิวเตอร์ - คอมพิวเตอร์ - คอมพิวเตอร์
ทีม : กลุ่มพัฒนาระบบบริการ		ผู้จัดการ : นายสัตวแพทย์พรพิทักษ์ พันธุ์หล้า ผู้จัดการสำรอง :นายวรวิทย์ พยุงเกียรติบวร		
ขั้นตอนการปฏิบัติ	**กิจกรรม**			
	ก่อนการถูกโจมตี	**ผู้รับผิดชอบ**		**เอกสาร/ทรัพยากร**
1. ประชุมกลุ่มพัฒนาระบบบริการ เพื่อพิจารณาแนวทาง วิธีการดำเนินงาน รวมทั้งการมอบหมายงานภายในกลุ่ม 2. พิจารณามอบหมายงานเจ้าหน้าที่ภายในกลุ่ม และหรือเจ้าหน้าที่ในทีมอื่น ให้ปฏิบัติงานแทนกรณีเหตุ	1. ติดตามข่าวสารการแจ้งเตือนการโจมตีจากสื่อต่างๆ 2. มีกระบวนการ Backup ข้อมูลตามแผน 3. จัดทำคู่มือการกู้คืนระบบและแก้ไขปัญหาเบื้องต้น 4. จัดอบรมเจ้าหน้าที่ที่เกี่ยวข้อง รวมทั้งการซ้อมปฏิบัติ	กลุ่มพัฒนาระบบบริการ นายวรวิทย์ พยุงเกียรติบวร, นายชาญวิทย์ อมรสุรินทวงศ์ กลุ่มพัฒนาระบบบริการ กลุ่มพัฒนาระบบบริการ		- คอมพิวเตอร์ - คอมพิวเตอร์ - คู่มือการกู้คืนระบบ,แก้ไขปัญหาเบื้องต้น,เอกสารข่าวสาร - คอมพิวเตอร์
	ระหว่างการถูกโจมตี	**ผู้รับผิดชอบ**	**เวลาที่ใช้ (นาที)**	**เอกสาร/ทรัพยากร**
	1. รับแจ้งเหตุภัยคุกคาม 2. ระบุเหตุและรายงานภัยคุกคามฯ เพื่อตรวจสอบและบันทึกภัยคุกคามฯ ประเมินผลกระทบ 3. ควบคุมภัยคุกคามฯ เพื่อบรรเทาความเสียหายที่	กลุ่มพัฒนาระบบบริการ กลุ่มพัฒนาระบบบริการ กลุ่มพัฒนาระบบบริการ	5 15 5-10	- โทรศัพท์,คอมพิวเตอร์ - คอมพิวเตอร์ - คอมพิวเตอร์

	เกิดจากภัยคุกคามฯ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้ลุกลาม หรือ ขยายวงไปยังจุด อื่นๆ			
	4. การแก้ไขเหตุและกำจัดเหตุของภัยคุกคามฯ ที่เกิดขึ้น	กลุ่มพัฒนาระบบบริการ	5-60	- คอมพิวเตอร์
	5. ป้องกันไม่ให้เกิดภัยคุกคามในลักษณะเดิมซ้ำอีก	กลุ่มพัฒนาระบบบริการ	30	- คอมพิวเตอร์
	6. ประสานงานผู้ติดต่อภายนอก	นางจันทร์เพ็ญ เอกมอญ, นายชัยรัตน์ ปรีชากร	5-10	- โทรศัพท์,คอมพิวเตอร์
	หลังการถูกโจมตี	**ผู้รับผิดชอบ**	**เวลาที่ใช้ (นาที)**	**เอกสาร/ทรัพยากร**
	1. ตรวจสอบการทำงานของระบบและข้อมูลว่าถูกกระทบจากการโจมตีแค่ไหน	กลุ่มพัฒนาระบบบริการ	30	- คอมพิวเตอร์
	2. การกู้คืนระบบหรือข้อมูล ให้อยู่ในสภาพพร้อมบริการ	นายวรวิทย์ พยุงเกียรติบวร, นายชาญวิทย์ อมรสุรินทวงศ์	60	- คอมพิวเตอร์
	3. ประเมินผลในการดำเนินการรับมือ	กลุ่มพัฒนาระบบบริการ	30	- คอมพิวเตอร์
	4. บันทึกรายงานการดำเนินงาน เพื่อให้บุคคลที่เกี่ยวข้องได้ทราบ และใช้เป็นกรณีศึกษาในภายหลัง	นายวรวิทย์ พยุงเกียรติบวร, นายชัยรัตน์ ปรีชากร	60-120	- คอมพิวเตอร์

ซ้อมแผนรับมือภัยคุกคามระบบสารสนเทศ

ศูนย์สารสนเทศ กรมควบคุมโรค

วันจันทร์ที่ 30 มิถุนายน พ.ศ.2557 ศูนย์สารสนเทศ กรมควบคุมโรคได้จัดประชุมเพื่อเตรียมความพร้อมในการซ้อมแผนรับมือภัยคุกคามระบบสารสนเทศ โดยมีท่านบุษบง เจาฑานนท์ ผู้ทรงคุณวุฒิกรมควบคุมโรคเป็นประธานและร่วมให้คำปรึกษาในการประชุมครั้งนี้



รูปที่ 1.1 ประชุมเพื่อเตรียมความพร้อมในการซ้อมแผนรับมือภัยคุกคามระบบสารสนเทศ

ศูนย์สารสนเทศ กรมควบคุมโรคได้ซ้อมแผนรับมือภัยคุกคามระบบสารสนเทศ โดยจำลองเหตุการณ์เครื่อง Server หรือ Personal Computer (PC) ภายในกรมควบคุมโรคติด Virus พยายามต่อ Internet ภายนอกเพื่อแพร่กระจายหรือส่งข้อมูลออกไป

โดยการใช้งาน Internet ของกรมควบคุมโรคได้มีการวางระบบรักษาความปลอดภัยทั้ง Firewall และระบบ Authentication ทำให้ Virus ไม่สามารถต่อ Internet เพื่อแพร่กระจายหรือส่งข้อมูลออกไปได้ เนื่องจากต้องผ่านระบบ Authentication และเมื่อ Virus พยายามต่อ Internet หลายๆครั้งถือว่าเป็นการโจมตีระบบ Authentication ด้วยวิธี Denial-of Service (DoS) คือ เป็นการโจมตีโดยการส่งข้อมูลแพ็กเกตจำนวนมหาศาลไปยังเครื่องเป้าหมาย ทำให้เครื่องเป้าหมายทำงานหนัก และไม่สามารถทำงานได้ตามปกติ

วันอังคารที่ 1 กรกฎาคม พ.ศ.2557 กลุ่มบริหารจัดการเทคโนโลยีสารสนเทศ ได้รับโทรศัพท์แจ้งจากทางผู้ใช้ว่าไม่สามารถ Login ระบบ Authentication เพื่อใช้งาน Internet ได้ โดยได้สอบถามอาการเบื้องต้น พบว่า เข้ามาหน้า Login แต่ Login ไม่ผ่าน และบางเครื่องใกล้เคียงกันสามารถ Login ได้ปกติ

รูปที่ 1.2 ได้รับแจ้งปัญหาการใช้งานระบบ Authentication

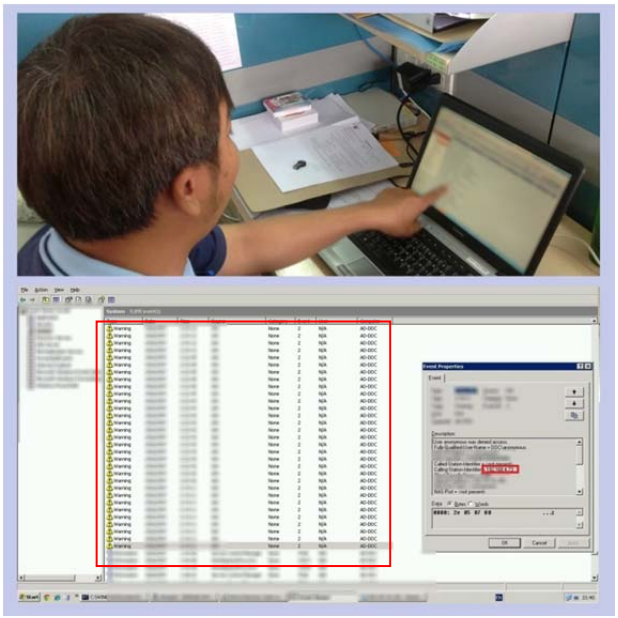
กลุ่มสนับสนุนระบบบริการ ได้เช็คระบบ Authentication และ Firewall เพื่อดูผลกระทบ ความรุนแรง หรือความผิดปกติของระบบเบื้องต้น พบว่าระบบยังสามารถทำงานได้ แต่มีผู้ใช้งานระบบ Authentication น้อยผิดปกติ และยังมีผู้โทรมาแจ้งปัญหาเดียวกันอย่างต่อเนื่อง

รูปที่ 1.3 ตรวจสอบระบบ Authentication และ Firewall

กลุ่มสนับสนุนระบบบริการ ได้พูดคุยเพื่อหาทางแก้ไข พร้อมทั้งประสานงานกับหน่วยงานภายนอก เพื่อสอบถามความผิดปกติในการเชื่อมโยง Internet และเตรียมความพร้อมระบบ Authentication สำรอง หากมีความจำเป็นต้องใช้งานระบบสำรอง

รูปที่ 1.4 ร่วมกันหาทางแก้ไข พร้อมทั้งประสานงานกับหน่วยงานภายนอก

หลังจากการตรวจสอบระบบโดยละเอียด พบว่าใน Log ของระบบ Authentication มีการแจ้งเตือน ว่ามีการพยายามต่อ Internet หลายครั้งใน IP Address เดียวกัน ทำให้ใช้ทรัพยากรของระบบจำนวนมาก ระบบจึงทำงานได้ไม่ปกติ



รูปที่ 1.5 พบว่ามีการพยายามต่อ Internet หลายครั้งใน IP Address เดียวกัน

ทางศูนย์สารสนเทศได้ประสานไปยังผู้ใช้งานเครื่อง IP Address เพื่อแจ้งในเบื้องต้น พร้อมทั้ง Block IP Address เพื่อเป็นการแก้ไขเบื้องต้นในทันที ก่อนทำการ รีสตาร์ทระบบ Authentication เพื่อให้ระบบสามารถกลับมาทำงานได้ตามปกติ หลังจากนั้น กลุ่มสนับสนุนระบบบริการ ได้ประชุมเพื่อสรุปผลการดำเนินงานรวมถึงหาวิธีป้องกันไม่ให้เกิดภัยคุกคามในลักษณะนี้ซ้ำ โดยจะทำหนังสือแจ้งไปยังผู้ใช้งานเครื่อง IP Address นั้นเพื่อให้ติดตั้งโปรแกรม Antivirus หรือ อัพเดต Patch ให้เป็นปัจจุบัน และแจ้งเตือนไปยังหน่วยงานต่างๆ สำหรับเป็นกรณีศึกษาในภายหลัง

รูปที่ 1.6 ประชุมเพื่อสรุปผลในการดำเนินการรับมือภัยคุกคามฯ รวมทั้ง แจ้งผลการดำเนินการให้ผู้ที่เกี่ยวข้องรับทราบ และบันทึกรายงานการดำเนินงาน