ระบบปรับปรุงและป้องกันภัยคุกคามบนอุปกรณ์รักษาความปลอดภัยแบบอัตโนมัติ

Automatic threat and security policy update on security devices systems

วิชญ์พงศ์ เกื้ออรุณ(Wichapong Kua-Arun)[1] อนุรักษ์ เชยชุ่ม (Anurak Choeichum)[2]
และชัยพร เขมะภาตะพันธ์ (Chaiyaporn Khemapatapan)[3]

[1]สาขาวิชาวิศวกรรมคอมพิวเตอร์และโทรคมนาคม คณะวิศวกรรมศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์
Email: wichapong.k@gmail.com

บทคัดย่อ

งานวิจัยนี้ได้นำเสนอระบบที่จะช่วยปรับปรุงและพัฒนาระบบรักษาความปลอดภัยภายในระบบเครือข่ายคอมพิวเตอร์แบบอัตโนมัติ ซึ่งมีจุดประสงค์เพื่อช่วยแก้ปัญหาของผู้ดูแลระบบ ที่ต้องตอบสนองต่อภัยคุกคาม จากการโจมตีและเครือข่าย แพร่กระจายภายใต้ระบบที่ตนเองดูแลอยู่ ภายในระยะเวลาที่จำกัด แต่กลับมีปริมาณข้อมูลเป็นจำนวนมาก ซึ่งต้องอาศัยระยะเวลา และความเชี่ยวชาญของผู้ดูแลในวิเคราะห์ข้อมูล ทำให้ ระยะเวลาที่ต้องใช้ในการค้นหา และแก้ไข ภัยคุกคามต่างๆ ไม่สามารถกำหนดระยะเวลาที่แน่นอนได้ ทำให้เกิดผลกระทบร้ายแรงต่อข้อมูล และระบบเครือข่ายคอมพิวเตอร์นั้นๆ

จึงได้เกิดแนวคิดให้มีระบบสำหรับรับข้อมูลที่เกิดขึ้นจากอุปกรณ์รักษาความปลอดภัยประเภทต่างๆ แล้วนำมาวิเคราะห์หาภัยคุกคามต่างๆที่กำลังเกิดขึ้น หลังจากนั้นทำการกำหนดนโยบายรักษาความปลอดภัย ส่งกลับไปยังอุปกรณ์รักษาความปลอดภัยชนิดต่างๆ แบบอัตโนมัติ เพื่อให้สามารถตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้ภายใต้ระยะเวลาที่เหมาะสม

ซึ่งจากการทดลองพบว่า หลังจากที่ระบบได้รับข้อมูลภัยคุกคามจากต้นทาง ก็สามารถส่งข้อมูลการโจมตีไปยังอุปกรณ์รักษาความปลอดภัยชนิดต่างๆ เพื่อป้องกันการแพร่กระจายของมัลแวร์ไปยังเครื่องคอมพิวเตอร์ลูกข่ายเครื่องอื่นๆในระบบได้เร็วกว่าที่ผู้เชี่ยวชาญหรือผู้ดูแลระบบจะสามารถทำการปรับปรุงนโยบายรักษาความปลอดภัยของอุปกรณ์ที่มีอยู่ในระบบได้ครบ ได้อย่างมีประสิทธิภาพมาก

คำสำคัญ—ระบบเครือข่าย; นโยบายรักษาความปลอดภัย; อัตโนมัติ; รักษาความปลอดภัย

ABSTRACT

This paper has proposed the systems to enhanced and automatic improve security within a computer network. The main proposed of this research is to help systems administrator who needs to response to attack in the systems that spread in the networks within limited timeframe but since there are lots of data which require both time and skill from an administrator to identify the problem. Which is unable to predict the exact timeframe and result in damage to data and network systems

The idea of this research is to have the systems to receive all the logs from security devices, analyze the log then automatic create a security policy and push the update to the security devices. In order to response to the incident in the time manner.

As the results show in this research, after the systems received attack information from source that detects attack in the systems can update this attack information to others security devices in the systems to block malware that will spread throughput the network more efficiency than using human or systems administrator to do all the work with security devices

Keyword-- computer network; security policy; automatic; network security, log

1. บทนำ

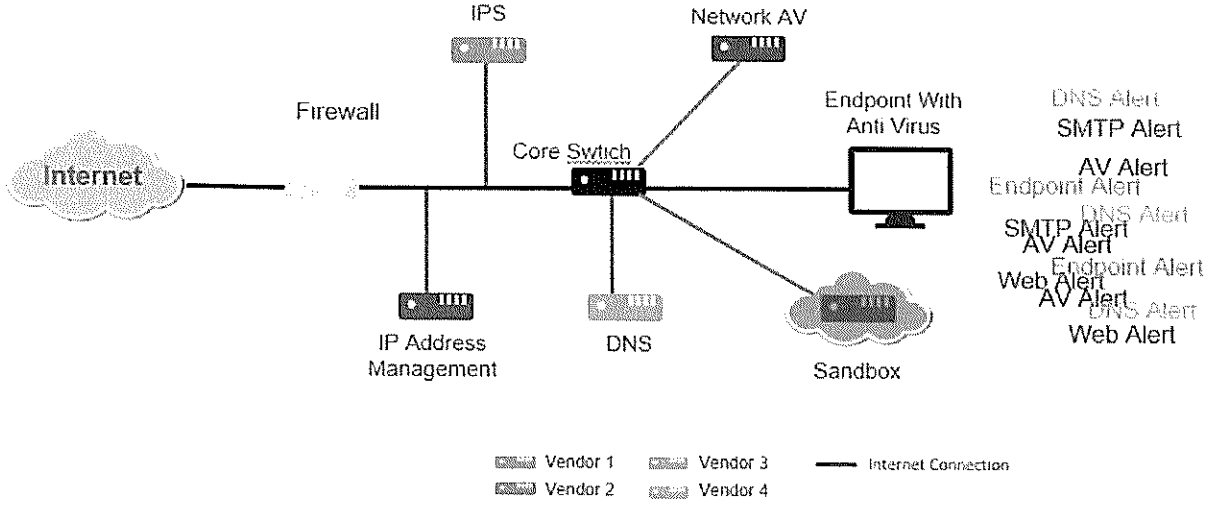
ในปัจจุบัน องค์กรต่างๆ ได้มีการลงทุนกับระบบรักษาความปลอดภัยของระบบเครือข่ายอินเตอร์เน็ตเพิ่มมากยิ่งขึ้น เนื่องจากภัยคุกคามในยุคปัจจุบัน นอกจากความสามารถในการหลบหลีกการตรวจจับที่มีเพิ่ม

มากขึ้นแล้วนั้น ผลกระทบที่เกิดขึ้นจากการโจมตีในแต่ละครั้ง ยังมีความร้ายแรง และส่งผลเสียต่อธุรกิจในรุนแรงมากขึ้นเรื่อยๆ ดังนั้น องค์กรต่างๆจึงได้มีความพยายามที่จะป้องกันภัยคุกคามต่างๆ ที่มีอยู่มากมายในปัจจุบัน โดยเลือกซื้ออุปกรณ์ที่มีความสามารถในการป้องกันระบบเครือข่าย และมีเป้าหมายในการตรวจจับภัยคุกคามที่เกิดขึ้น ให้ได้เร็วที่สุด และทำการแก้ไขระบบเครือข่าย ให้สามารถป้องกันการโจมตีนั้นๆ ได้

แต่ปัญหาที่เกิดขึ้นก็คือ อุปกรณ์รักษาความปลอดภัยระบบเครือข่ายนั้น มีอยู่หลากหลาย อาทิเช่น ระบบป้องกันการบุกรุก (Firewall), ระบบป้องกันผู้บุกรุก (Intrusion Prevention Systems) และอื่นๆ ซึ่งอุปกรณ์แต่ละชนิด ก็มีความสามารถ และมีรูปแบบการทำงานที่แตกต่างกันออกไป ดังนั้น ผู้ดูแลระบบ จึงต้องมีความเชี่ยวชาญ ในการทำความเข้าใจ กับข้อมูลหรือเหตุการณ์ที่เกิดขึ้นในระบบของตนเอง เพื่อนำมาวิเคราะห์ และนำไปปรับปรุงระบบรักษาความปลอดภัยของตนเอง ให้มีความปลอดภัยมากยิ่งขึ้น ทั้งนี้ ยังต้องดำเนินการ ภายใต้ระยะเวลาที่จำกัด

จึงเป็นที่มาของแนวความคิด ในการศึกษาค้นคว้าวิจัย ระบบปรับปรุงความปลอดภัยของระบบเครือข่ายแบบ อัตโนมัติ โดยอาศัยการรับข้อมูลที่เกิดขึ้น จากอุปกรณ์ต่างๆ ที่แต่ละองค์กรมีอยู่ มาวิเคราะห์ และหาความเชื่อมโยงกับข้อมูลที่มีอยู่ในระบบเครือข่ายและทำการส่งข้อมูลที่ได้ ไปยังอุปกรณ์แต่ละชนิด ให้สามารถป้องกันภัยคุกคามได้ในระยะเวลาที่เหมาะสม

จากการศึกษาค้นคว้าวิจัยพบว่า ระบบนี้ สามารถช่วยลดระยะเวลาที่ผู้ดูแล จะต้องนำข้อมูลจากอุปกรณ์แต่ละชนิด มาวิเคราะห์ และมองหาความเชื่อมโยงของข้อมูลแต่ละชนิด และยังเป็นการช่วยลดทั้งระยะเวลา และค่าใช้จ่ายที่จะเกิดขึ้นจากการแก้ปัญหาได้อีกทางหนึ่งด้วย



ภาพที่ 1: ระบบรักษาความปลอดภัยในปัจจุบันมีข้อมูลหลากหลายและมากเกินกว่าที่จะทำความเข้าใจได้ในระยะเวลาอันสั้น

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

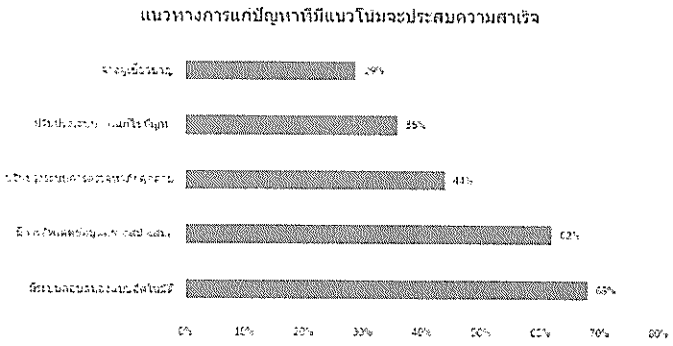
จากงานวิจัย [1] พบว่า ในแต่ละสัปดาห์ องค์กรต่างๆ จะได้รับเหตุการณ์ (Event) จากอุปกรณ์รักษาความปลอดภัยที่มีอยู่ภายในองค์กรประมาณ 17,000 เหตุการณ์ และจากจำนวนการแจ้งเตือนทั้งหมด มีร้อยละ 19 เปอร์เซ็นต์หรือ 3,218 เหตุการณ์ที่ถูกตัดสินว่าเป็นการแจ้งเตือนที่มีความน่าสนใจ หรือมีความน่าจะเป็นที่จะเป็นเหตุการณ์ต้องสงสัย แต่กลับมีเพียงร้อยละ 4 หรือ 705 เหตุการณ์ เท่านั้น ที่ถูกนำมาวิเคราะห์และหาจุดเริ่มต้นของปัญหา

ซึ่งสาเหตุที่จำนวนของเหตุการณ์ที่ถูกนำมาวิเคราะห์ต่อมีจำนวนน้อยนั้น ก็เป็นเพราะว่า ในแต่ละเหตุการณ์ที่จะต้องวิเคราะห์จำเป็นที่จะต้องใช้ระยะเวลานาน ต้องอาศัยความเชี่ยวชาญของผู้วิเคราะห์ เพื่อหาความเชื่อมโยง และหาสาเหตุต้นตอของปัญหา อีกทั้งองค์กรส่วนมาก ก็ไม่ได้มีเครื่องมือที่ใช้ในการตรวจจับภัยคุกคามและวิเคราะห์ความเสี่ยงแบบอัตโนมัติมากนัก

ข้อมูลจากการวิจัย ยังได้เปิดเผยข้อมูลอีกส่วนหนึ่ง ที่พบว่าองค์กรต่างๆ นั้นจะมีค่าใช้จ่ายโดยเฉลี่ยในการวินิจฉัยปัญหาที่เกิดขึ้นอยู่ที่ประมาณ 25,000 เหรียญดอลล่าสหรัฐต่อสัปดาห์ หรือสูงถึง 1.27 ล้านเหรียญดอลล่าสหรัฐต่อปี

จากงานวิจัยทั้งสองฉบับนั้น จะเห็นได้ว่า ถึงแม้องค์กรต่างๆ ที่ประสบปัญหาในเรื่องของภัยคุกคาม จะมีอุปกรณ์ในระบบเครือข่าย ที่ทำหน้าที่ในการป้องกัน และแจ้งเตือนไปยังผู้ดูแลระบบอย่างสม่ำเสมอ แต่ปัจจัยสำคัญที่ทำให้ระบบยังเกิดปัญหาเกิดขึ้น มีต้นเหตุมาจากข้อมูลที่มีจำนวนมากเกินไป จนผู้ดูแลระบบไม่สามารถที่จะทำความเข้าใจ และไม่สามารถวิเคราะห์ข้อมูลทั้งหมดที่มีอยู่ได้ ภายในช่วงเวลาที่จะตอบสนองต่อภัยคุกคามนั้นได้อย่างทันท่วงที

งานวิจัยอีกฉบับหนึ่ง [2] ซึ่งได้มีการเก็บข้อมูลจากองค์กรทั่วๆไป เพื่อทำการจัดลำดับและระบุรูปแบบที่ผู้ดูแลระบบต่างเห็นตรงกันว่า สามารถนำมาใช้ประโยชน์ในการป้องกันภัยคุกคามได้สูงที่สุด ดังในภาพต่อไปนี้



ภาพที่ 2: แนวทางการแก้ปัญหาที่มีแนวโน้มประสบความสำเร็จ

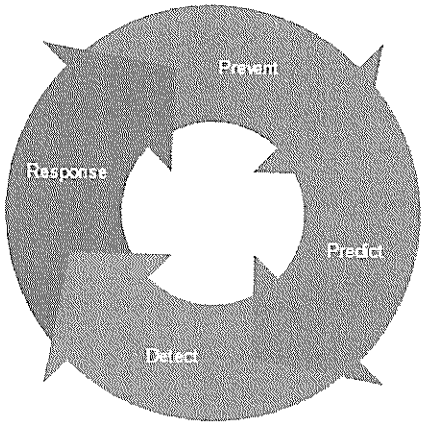
จากข้อมูลดังกล่าว จึงเป็นที่มาของการพัฒนาระบบตอบสนองต่อเหตุการณ์ที่เกิดขึ้นแบบอัตโนมัติ ซึ่งมีแนวโน้มที่จะช่วยให้องค์กร สามารถตอบสนอง หรือแก้ไขปัญหาเบื้องต้น ได้รวดเร็วมากยิ่งขึ้น ซึ่งเมื่อเปรียบเทียบกับข้อมูลจากงานวิจัย [3] อีกงานหนึ่ง ที่พบว่า ระยะเวลาเฉลี่ยที่องค์กรต่างๆ ใช้ในการตรวจพบ ภัยคุกคามที่แอบแฝงเข้ามาในองค์กร คือ 209 วันในปี 2014 ซึ่งถึงแม้จะลดลงจาก 229 วันในปี 2013 ก็ตาม ตัวเลขดังกล่าวยังเป็นตัวเลขที่มากเกินไปในการจัดการกับภัยคุกคามอยู่ดี

งานวิจัยอีกฉบับหนึ่ง [4] ได้มีความพยายามที่จะสร้างระบบตอบสนองแบบอัตโนมัติ เพื่อที่จะทำการวิเคราะห์ถึงการโจมตี และเลือกการตอบสนองที่เหมาะสมต่อภัยคุกคามมากที่สุด เพียงแต่งานวิจัยฉบับนี้ จะมุ่งเน้นไปในการตอบสนองต่อภัยคุกคามทางด้านปริมาณของการร้องขอที่จะเข้ามาสู่ระบบเครือข่าย มากกว่าที่จะเป็นตอบสนองต่อภัยคุกคามที่เกิดขึ้นภายในระบบ

เช่นเดียวกันงานวิจัย [6] [7] ที่ได้มีการนำเสนอ ระบบวิเคราะห์เหตุการณ์และอัพเดตกลับไปยังอุปกรณ์รักษาความปลอดภัยประเภทต่างๆ ในระบบเช่นเดียวกัน เพียงแต่ระบบดังกล่าว จะทำการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นแล้วในระบบเท่านั้น ไม่ได้มุ่งเน้นในเรื่องของการปรับปรุงระบบรักษาความปลอดภัยให้มีความทันสมัย เพื่อป้องกันไม่ให้การโจมตีเกิดขึ้น โดยจะเป็นการใช้ความพยายามที่จะ detect และประมวลผลหาร่องรอยของภัยคุกคาม แล้วถึงจะส่งคำสั่งไปยังอุปกรณ์รักษาความปลอดภัยให้ทำการปรับเปลี่ยนกฎ หรือข้อกำหนด อีกทั้งยังไม่ได้มุ่งเน้นไปในการรักษาความปลอดภัย เมื่อระบบมีอยู่หลายๆ โลเคชั่น

3. การออกแบบและวิธีวิจัย

งานวิจัยฉบับนี้ จะนำเสนอรูปแบบการปรับปรุงระบบรักษาความปลอดภัยของระบบเครือข่าย โดยอ้างอิงตาม โครงสร้าง Adaptive Security Architecture ที่มีส่วนประกอบสี่ส่วนคือ ขั้นตอนการป้องกัน (Prevent) , ขั้นตอนการตรวจจับ (Detect), ขั้นตอนการตอบสนอง (Response) และขั้นตอนในการคาดเดาการโจมตี Predict [5] ดังที่แสดงในภาพที่ 3 ซึ่งจะเป็นการทำงานตามลำดับวนไปเรื่อยๆ เพื่อปรับปรุงระบบรักษาความปลอดภัยขององค์กร ให้เกิดความปลอดภัยสูงที่สุด

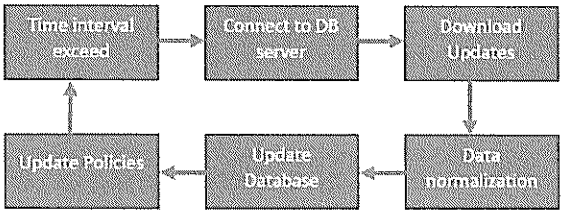


ภาพที่ 3: กระบวนการการปรับปรุงระบบรักษาความปลอดภัย

โดยระบบนี้ จะมุ่งเน้นการทำงานให้อยู่ในส่วนของการตอบสนองต่อปัญหาที่เกิดขึ้น และทำการคาดคะเน หรือคาดเดาแนวโน้มของการโจมตีที่จะเกิดขึ้น และเตรียมข้อมูลสำหรับในส่วนของการป้องกันให้กับอุปกรณ์รักษาความปลอดภัยแต่ละชนิดของแต่ละองค์กร เป็นองค์ประกอบสำคัญในการทำงาน และยกหน้าที่ในการทำงานด้านการป้องกัน และตรวจจับปัญหาที่เกิดขึ้น ให้เป็นหน้าที่ของอุปกรณ์แต่ละชนิดทำงานตามปกติ

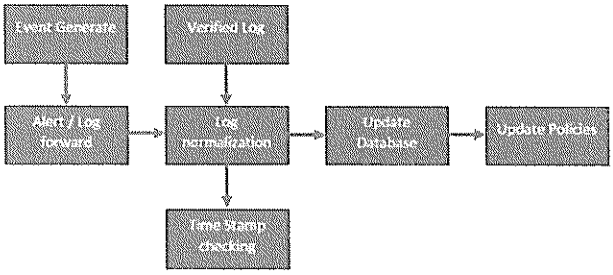
ซึ่งตัวระบบจะมีการทำงานแบ่งออกเป็นดังนี้

1.) ในสภาวะปกติ ระบบจะทำงานในส่วนของการคาดคะเนปัญหา แล้วทำการป้องกันการโจมตีที่อาจจะเกิดขึ้นในระบบ โดยเชื่อมต่อเข้ากับฐานข้อมูลของระบบต่างๆ ที่เปิดให้ระบบสามารถเชื่อมต่อ เพื่อทำการปรับปรุงข้อมูลของการโจมตีใหม่ๆ อาทิเช่น หมายเลขไอพี แอดเดรส ของผู้โจมตี หรือ ที่อยู่ของข้อมูลเว็บไซต์ หรือ URL ใหม่ๆ ที่สามารถระบุได้อย่างแน่ชัด ว่าเป็น URL ที่มีความอันตราย เพื่อทำการดาวโหลดข้อมูลมาเก็บลงไปในฐานข้อมูลที่เตรียมไว้แล้วอัพเดตข้อมูลไปให้อุปกรณ์ชนิดต่างๆ ไม่ว่าจะเป็นการ ส่งคำสั่งไปยังอุปกรณ์ที่ต้องการเพื่อทำการกำหนดเป็นกฎหรือเงื่อนไขการใช้งาน หรือในอุปกรณ์บางชนิด ก็สามารถทำการเชื่อมต่อมายังฐานข้อมูลของระบบ เพื่อดึงข้อมูลที่เก็บอยู่ในฐานข้อมูลไปใช้งาน โดยมีจุดประสงค์เพื่อป้องกันไม่ให้ผู้ใช้งานในระบบ ทำการเชื่อมต่อไปยังปลายทางดังกล่าว โดยสามารถอ้างอิงขั้นตอนการทำงานได้ ดังนี้



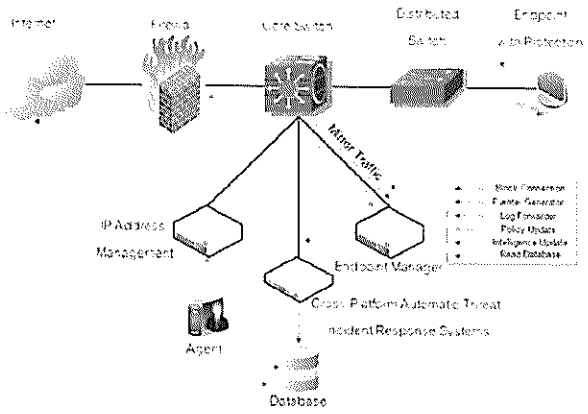
ภาพที่ 4: ขั้นตอนการทำงานของระบบในช่วงสภาวะคาดคะเน

2.) ในสภาวะที่ได้รับข้อมูลเหตุการณ์จากอุปกรณ์อื่นๆ หรือการตอบสนองต่อปัญหา โดยระบบจะรับเหตุการณ์ต่างๆ จากอุปกรณ์ที่อยู่ภายในระบบเครือข่าย แล้วนำข้อมูลที่ได้มาแยกประเภท และตรวจสอบกับฐานข้อมูล เช่น นำค่าเฉพาะของไฟล์ชนิดต่างๆ หรือค่า Hash ไปตรวจสอบกับฐานข้อมูล ว่ามีความน่าจะเป็นที่จะเป็นไฟล์ที่มีความอันตราย มากน้อยเพียงใด ถ้าหากพบว่ามีความสัมพันธ์ กับภัยคุกคามก็จะทำการอัพเดต ค่าของไฟล์ดังกล่าวลงไปเก็บในฐานข้อมูล หรืออีกตัวอย่างหนึ่ง คือในกรณีที่อุปกรณ์คอมพิวเตอร์ลูกข่ายที่มีการติดตั้งโปรแกรมหรือระบบป้องกันภัยคุกคามไว้ หรือระบบตรวจจับภัยคุกคามขององค์กรสามารถตรวจจับภัยคุกคามได้ ระบบดังกล่าวจะทำการส่งข้อมูลไปยังศูนย์ควบคุมส่วนกลาง เพื่อทำหน้าที่ในการส่งต่อข้อมูลไปให้กับระบบ ที่จะทำหน้าที่รับผิดชอบในการแยกแยะข้อมูล แล้วส่งคำสั่งไปให้อุปกรณ์ที่ทำหน้าที่บริหารจัดการไอพี แอดเดรส ทำการปิดการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายดังกล่าว เพื่อป้องไม่ให้เครื่องคอมพิวเตอร์ลูกข่ายดังกล่าว ทำการแพร่ภัยคุกคามไปยังเครื่องคอมพิวเตอร์ลูกข่ายเครื่องอื่นๆ ที่อยู่ภายใต้ระบบเครือข่ายเดียวกัน ทำให้ลดภาระงานของผู้ดูแลระบบที่จะต้องทำการแก้ไขปัญหาของเครื่องคอมพิวเตอร์ลูกข่ายจำนวนมาก เหลือเพียงเครื่องคอมพิวเตอร์ลูกข่ายที่สามารถตรวจจับภัยคุกคามได้เป็นเครื่องแรกเท่านั้น และในกรณีที่มีอุปกรณ์อื่นเข้ามาเกี่ยวข้อง ระบบก็สามารถที่จะส่งข้อมูลไปยังอุปกรณ์อื่นๆ เพื่อให้กำหนดค่าเป็นกฎสำหรับรักษาความปลอดภัยส่งต่อไป ดังแสดงในแผนภาพดังต่อไปนี้



ภาพที่ 5: การทำงานของระบบในสภาวะของการตอบสนอง

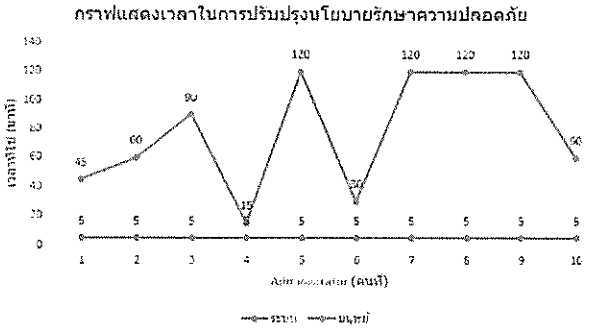
โดยในการเชื่อมต่อเพื่อรับส่งคำสั่ง หรืออัพเดตข้อมูลการรักษาความปลอดภัยนั้น จะเป็นการดำเนินการผ่าน API (Application Program Interfaces) เพื่อให้รองรับการเชื่อมต่อสื่อสารระหว่างอุปกรณ์แต่ละชนิดที่มีความหลากหลายของชุดคำสั่ง โดยมีขั้นตอนและรูปแบบในการดำเนินงาน ดังภาพที่ 5



ภาพที่ 5: แสดงขั้นตอนการทำงานของระบบ

4. ผลการทดสอบ

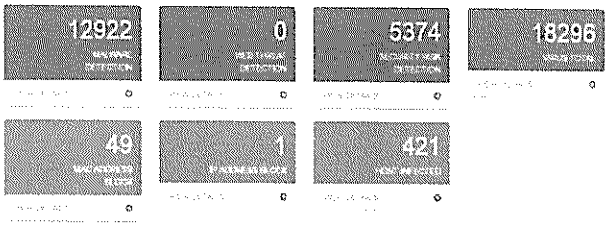
จากการทดลองโดยการรับข้อมูลจากระบบเครือข่าย เพื่อรับข้อมูลการใช้งานจริงจากระบบ เพื่อนำมาเปรียบเทียบโดยการทำแบบสอบถามจากผู้ดูแลระบบที่มีความเชี่ยวชาญ เกี่ยวกับเวลาที่ใช้ในการปรับปรุงระบบนโยบายรักษาความปลอดภัยนั้น พบว่า เมื่อระบบได้รับข้อมูลจากอุปกรณ์ตรวจจับการโจมตี หรือภัยคุกคามที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์นั้น ระบบสามารถปรับปรุงนโยบายรักษาความปลอดภัยของอุปกรณ์รักษาความปลอดภัยได้เร็วกว่าผู้ดูแลระบบ ดังรูปที่ 6



ภาพที่ 6: ระยะเวลาในการปรับปรุงนโยบายรักษาความปลอดภัย

และในส่วนของผู้ดูแลระบบ สามารถตรวจสอบปริมาณเหตุการณ์ที่เกิดขึ้น ในแต่ละช่วงเวลาได้ อาทิเช่น จำนวนเครื่องคอมพิวเตอร์ลูกข่ายที่ถูกควบคุมการใช้งานจากผู้ไม่ประสงค์ดีอยู่ และเครื่องที่ยังรอการแก้ไขจากผู้ดูแลระบบ

DASHBOARD



ภาพที่ 7: หน้าแสดงผลข้อมูลโดยรวมให้กับผู้ดูแลระบบ

5. สรุป

จากงานวิจัยสามารถสรุปได้ว่า ระบบนี้ ช่วยให้ผู้ดูแลระบบสามารถทำการบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพมากยิ่งขึ้น เนื่องจากระบบสามารถรับข้อมูลการตรวจจับภัยคุกคามที่เกิดขึ้นภายในระบบ แล้วเลือกตอบสนองต่อภัยคุกคามนั้นได้แบบอัตโนมัติ ทำให้ช่วยลดระยะเวลาที่ผู้ดูแลระบบจะต้องใช้ในการตรวจสอบข้อมูลต่างๆ จากอุปกรณ์หลายๆชนิดด้วยตนเอง และยังเป็นการยับยั้งการแพร่กระจายของมัลแวร์ และภัยคุกคามต่างๆ ไม่ให้แพร่หลายไปเครื่องคอมพิวเตอร์ลูกข่ายเครื่องอื่นๆ ในระบบ ทำให้ระยะเวลาที่ผู้ดูแลระบบต้องใช้ในการแก้ปัญหาที่เกิดขึ้นลดต่ำลง อีกทั้งยังเป็นการช่วยลดค่าใช้จ่ายในการแก้ปัญหาอีกทางหนึ่งด้วย

เอกสารอ้างอิง

[1] Independently conducted by Ponemon Institute LLC, January 2015. "The Cost of Malware Containment". [Online]. Available: http://www.ponemon.org/local/upload/file/Damballa%20Malware%20Containment%20FINAL%203.pdf

[2] Independently conducted by Ponemon Institute LLC, 2014 "Cyber Security Incident Response: Are we as prepared as we think?" [Online] Available: https://www.lancope.com/sites/default/files/Lancope-Ponemon-Report-Cyber-Security-Incident-Response.pdf

[3] Mandiant a FireEye company. 2015 "M-Trend 2015: A view from the frontlines" [Online]. Available: https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf

[4] Sven Ossenb¨uhl, Jessica Steinberger and Harald Baier "Towards automated incident handling: How to select an appropriate response against a network-based attack?," 2015 Ninth International Conference on IT Security Incident Management & IT Forensics, DOI 10.1109/IMF.2015.13, 2015.

[5] Gartners, 2014 "Designing an Adaptive Security Architecture for Protection From Advanced Attacks", [Online]. Available: https://www.gartner.com/doc/2665515/designing-adaptive-security-architecture-protection

[6] H. Hasegawa, Y. Yamaguchi, H. Shimada, and H. Takakura, "Proposal of a network control system to detect, analyze and mitigate targeted cyber attacks," IEICE technical report (Internet architecture), vol. 113, no. 240, pp. 1–6, 2013.

[7] H. Hasegawa, Y. Yamaguchi, H. Shimada, and H. Takakura, "An Incident Response Support System Based on Seriousness of Infection," ICOIN 2016