

การวิเคราะห์และการตอบสนองต่อภัยคุกคามจากการโจมตีทางไซเบอร์ในระบบ เครือข่ายขององค์กร

Analysis and Response to Cybersecurity Threats in Organizational Network Systems

อมร เจือตี้*

Amorn Juatee*

สาขาวิชาคอมพิวเตอร์ศึกษา คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏกาญจนบุรี

Computer Education Program, Faculty of Science and Technology, Kanchanaburi Rajabhat University

email: amorn@kru.ac.th

Received: November 13, 2024; Revised: April 4, 2024; Accepted: March 8, 2025

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์เพื่อ (1) วิเคราะห์ลักษณะของการโจมตีทางไซเบอร์ที่เกิดขึ้นในระบบเครือข่ายของมหาวิทยาลัยราชภัฏกาญจนบุรี (2) ศึกษาชนิด ลักษณะ และผลกระทบของภัยคุกคามที่มีต่ออุปกรณ์เครือข่าย และ (3) ปรับปรุงมาตรการด้านความปลอดภัยและพัฒนากลยุทธ์การตอบสนองต่อภัยคุกคามที่ส่งผลกระทบต่อระบบเครือข่าย โดยมุ่งเน้นการวิเคราะห์การโจมตีประเภทมัลแวร์ ประตูล้างเว็บเชลล์ และการโจมตีแบบเดรทส์ผ่าน พร้อมทั้งศึกษารูปแบบภัยคุกคาม ผลกระทบ และแนวทางป้องกันที่เหมาะสม การเก็บข้อมูลดำเนินการผ่านระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง และระบบจัดการเหตุการณ์ด้านความปลอดภัย จากเครื่องแม่ข่ายจำนวน 95 เครื่อง โดยเลือกวิเคราะห์เชิงลึกจากเครื่องที่มีความเสี่ยงสูงจำนวน 5 เครื่อง ผลการวิจัยพบว่ามัลแวร์เป็นภัยคุกคามที่พบมากที่สุด รองลงมาคือประตูล้างเว็บเชลล์ และการโจมตีแบบเดรทส์ผ่าน แม้จะพบไม่บ่อยแต่ยังคงเป็นความเสี่ยงที่ต้องเฝ้าระวัง การนำมาตรการด้านความปลอดภัยมาปรับใช้ อาทิ ระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนแบบหลายปัจจัย และการอัปเดตซอฟต์แวร์อย่างต่อเนื่อง ส่งผลให้จำนวนเหตุการณ์ภัยคุกคามลดลงอย่างมีนัยสำคัญ โดยมีมัลแวร์ลดลงร้อยละ 59.53 เว็บเชลล์ลดลงร้อยละ 60.61 และการโจมตีแบบเดรทส์ผ่านลดลงร้อยละ 33.33 จากผลการวิจัยยังเสนอแนะแนวทางการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง เพื่อเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามเชิงรุก เสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย และรองรับการรับมือกับภัยคุกคามที่มีความซับซ้อนในบริบทขององค์กรได้อย่างยั่งยืน

คำสำคัญ: ประตูล้างเว็บเชลล์ มัลแวร์ การโจมตีแบบเดรทส์ผ่าน ความปลอดภัยทางไซเบอร์ ระบบเครือข่าย

Abstract

This research aimed (1) to analyze the characteristics of cyberattacks occurring within the university network of Kanchanaburi Rajabhat University, (2) to examine the types, patterns, and impacts of threats on network devices, and (3) to improve security measures and develop response strategies for mitigating network-related threats. The study focused on analyzing malware attacks, web shell backdoors, and password-guessing attacks, along with investigating their patterns, impacts, and appropriate preventive measures. Data was collected through endpoint detection and response systems

and a security event management system across 95 servers, with in-depth analysis conducted on 5 high-risk machines. The results revealed that malware was the most frequent threat, followed by web shell backdoors and password-guessing attacks, which, although less common, remained significant risks requiring continuous monitoring. The implementation of enhanced security measures — including web application firewalls, multi-factor authentication, and continuous software updates — significantly reduced threat incidents: malware decreased by 59.53%, web shell attacks by 60.61%, and password-guessing attacks by 33.33%. Furthermore, the study recommends integrating artificial intelligence (AI) and machine learning (ML) technologies to strengthen proactive threat detection, improve network security resilience, and sustainably enhance the organization's capacity to respond to increasingly complex cyber threats.

Keywords: Web Shell Backdoor, Malware, Password-Guessing Attack, Cybersecurity, Network System

บทนำ

ในปัจจุบัน ระบบเครือข่ายขององค์กรต้องเผชิญกับภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นทั้งในด้านความถี่และความซับซ้อน เนื่องจากการพึ่งพาเทคโนโลยีสารสนเทศที่สูงขึ้น รูปแบบการโจมตีที่พบบ่อย ได้แก่ มัลแวร์ ประตูลังเว็บเชลล์ และการโจมตีแบบเดรทส์ผ่าน ซึ่งส่งผลกระทบต่อการทำงานของข้อมูล การเข้าควบคุมระบบโดยมิชอบ และการหยุดชะงักของการดำเนินงาน องค์กรที่ให้บริการระบบสารสนเทศจำนวนมาก โดยเฉพาะสถาบันการศึกษา จึงตกเป็นเป้าหมายสำคัญของการโจมตี ทำให้การพัฒนาและเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่ายเป็นสิ่งจำเป็น

สถาบันการศึกษามีระบบเครือข่ายที่เชื่อมโยงข้อมูลสำคัญหลายด้าน ทั้งข้อมูลบุคลากร นักศึกษา งานวิจัย ระบบการเรียนการสอน และความร่วมมือระหว่างประเทศ การโจมตีระบบเหล่านี้ก่อให้เกิดความเสียหายอย่างมีนัยสำคัญ ทั้งด้านข้อมูล ภาพลักษณ์ และความเชื่อมั่นของผู้ใช้งาน มหาวิทยาลัยราชภัฏกาญจนบุรี เป็นหนึ่งในสถาบันที่มีการใช้งานเทคโนโลยีอย่างแพร่หลาย งานวิจัยนี้จึงมุ่งศึกษารูปแบบภัยคุกคามในระบบเครือข่าย โดยอาศัยข้อมูลจากระบบตรวจจับและตอบสนอง รวมถึงระบบจัดการความปลอดภัย เพื่อประเมินประสิทธิภาพของมาตรการที่มีอยู่ และเสนอแนวทางปรับปรุงที่เน้นการใช้ระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนหลายปัจจัย และการใช้เทคโนโลยีปัญญาประดิษฐ์ในการรับมือภัยคุกคามที่ซับซ้อนอย่างยั่งยืน

งานวิจัยที่เกี่ยวข้อง

ในการทบทวนวรรณกรรมครั้งนี้ ผู้วิจัยได้ศึกษาผลงานวิชาการที่เกี่ยวข้องกับแนวทางการบรรเทาและจัดการภัยคุกคามทางไซเบอร์ในโครงสร้างพื้นฐานของเครือข่ายองค์กร โดยมุ่งเน้นการประยุกต์ใช้เทคโนโลยีด้านความปลอดภัย อาทิ ไฟร์วอลล์สำหรับแอปพลิเคชันเว็บ ระบบจัดการข้อมูลความปลอดภัยและเหตุการณ์ อัลกอริทึมการเรียนรู้ของเครื่อง รวมถึงระบบตรวจจับและตอบสนองต่อภัยคุกคาม พร้อมทั้งมีการวิเคราะห์เปรียบเทียบเพื่อออกแบบและปรับใช้กลยุทธ์การป้องกันที่เหมาะสมภายใต้บริบทขององค์กร

การใช้ไฟร์วอลล์เว็บแอปพลิเคชันควบคู่กับการวิเคราะห์ไฟล์บันทึกเพื่อลดการบุกรุกประเภท ประตูลังเว็บเชลล์ภายในโครงสร้างพื้นฐานเครือข่ายวิชาการผลการวิจัยชี้ให้เห็นว่าวิธีการนี้สามารถลดอัตราการบุกรุกลดลง 93 เปอร์เซ็นต์ในขณะเดียวกันก็ลดความถี่ของการแจ้งเตือนที่ผิดพลาดลงอย่างเห็นได้ชัด (Che & Liu, 2024)

การศึกษาจะประเมินอัลกอริทึมการเรียนรู้ของเครื่องต่าง ๆ อย่างเป็นระเบียบโดยเน้นที่ XGBoost โดยเฉพาะเพื่อระบุการบุกรุกแบบแบ็คดอร์อย่างชำนาญ การค้นพบนี้มีจุดมุ่งหมายเพื่อเสริมการป้องกันสภาพแวดล้อมที่พัฒนาขึ้นของภัยคุกคามทางไซเบอร์ โดยให้ข้อมูลเชิงลึกที่สำคัญสำหรับสถาบันในการแก้ไขช่องโหว่ที่เกี่ยวข้องกับการโจมตีแบบแบ็คดอร์ (Sharma & Babbar, 2024)

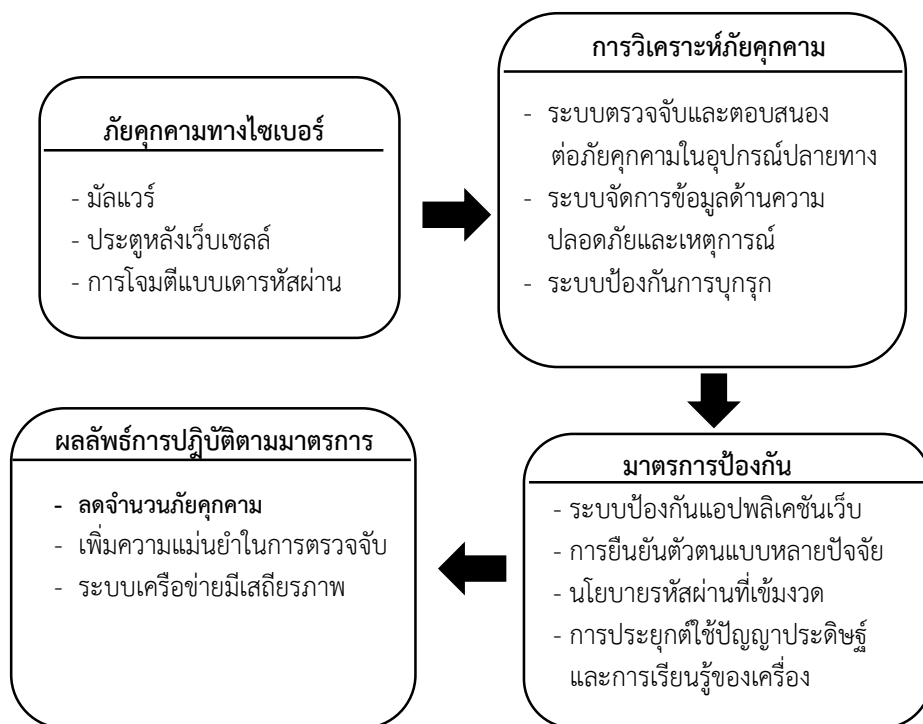
การโจมตีบนเว็บแบ็คดอร์มุ่งเน้นไปที่ TridentShell โดยเฉพาะ ซึ่งฝังแบ็คดอร์ที่มองไม่เห็นได้ในเว็บแอปพลิเคชันอย่างลับ ๆ โดยไม่ทิ้งหลักฐานที่มองเห็นได้ เทคนิคนี้ใช้ประโยชน์จากช่องโหว่ของระบบและข้อบกพร่องในเว็บแอปพลิเคชันทำให้สามารถระบุได้ทำลายผ่านวิธีการตรวจจับคุณสมบัติแบบคงที่ทั่วไป แม้ว่าจะไม่ได้มีส่วนร่วมโดยตรงกับมัลแวร์หรือการโจมตีเชิงรุก แต่ก็ชี้ให้เห็นถึงความสำคัญที่สำคัญของการรักษาความปลอดภัยทางไซเบอร์และความปลอดภัยเครือข่ายในการบรรเทาภัยคุกคามที่เกิดจากเว็บเซลล์ซึ่งอาจส่งผลให้ผู้ดูแลเว็บเป็นอันตรายอย่างมาก (Yu et al., 2023)

การโจมตีแบบแบ็คดอร์ รวมถึงเว็บเซลล์แบ็คดอร์แสดงถึงภัยคุกคามอย่างมีนัยสำคัญต่อความปลอดภัยทางไซเบอร์ โดยใช้ประโยชน์จากข้อบกพร่องด้านความปลอดภัยของเครือข่ายที่มักจะไม่มีใครสังเกตเห็นการวิจัยชี้ให้เห็นถึงความจำเป็นสำหรับองค์กรในการเพิ่มความสามารถในการตรวจจับและสร้างมาตรการป้องกันที่แข็งแกร่งต่อความหลากหลายของเวกเตอร์การโจมตี รวมถึงมัลแวร์และการบุกรุก การวิเคราะห์นี้โดดเด่นด้วยการตรวจสอบภัยคุกคามเหล่านี้อย่างเข้มงวด การศึกษามุ่งมั่นที่จะกำหนดแบบจำลองภัยคุกคามที่อำนวยความสะดวกในการทำนายความเสี่ยงและเสริมสร้างกรอบความปลอดภัยที่ครอบคลุมภายในองค์กร (Nasharuddin & Abubakar, 2024)

วัตถุประสงค์

1. เพื่อวิเคราะห์ลักษณะและรูปแบบของการโจมตีทางไซเบอร์ที่เกิดขึ้นในระบบเครือข่ายของมหาวิทยาลัยราชภัฏกาญจนบุรี โดยเฉพาะการโจมตีประเภทมัลแวร์ ประตูลังเว็บเซลล์ และการโจมตีแบบเดารหัสผ่าน
2. เพื่อศึกษาชนิด ลักษณะ และผลกระทบของภัยคุกคามแต่ละประเภทที่มีต่ออุปกรณ์และระบบเครือข่ายของมหาวิทยาลัยราชภัฏกาญจนบุรี
3. เพื่อพัฒนาและปรับปรุงมาตรการด้านความมั่นคงปลอดภัย รวมถึงกลยุทธ์การตอบสนองต่อการโจมตีทางไซเบอร์ให้มีประสิทธิภาพและเหมาะสมกับบริบทขององค์กร

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวคิดการวิจัย

ภาพที่ 1 กรอบแนวคิดการวิจัย แสดงความสัมพันธ์ระหว่างภัยคุกคามทางไซเบอร์ที่สำคัญ ได้แก่ มัลแวร์ ประสิทธิภาพเว็บไซต์ และการโจมตีแบบเดรทส์ผ่าน กับกระบวนการวิเคราะห์ภัยคุกคามโดยใช้ระบบตรวจจับและตอบสนองต่อภัยคุกคามในอุปกรณ์ปลายทาง ระบบจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ และระบบป้องกันการบุกรุก เพื่อประเมินความถี่และความรุนแรงของเหตุการณ์

จากนั้นนำมามาตรการป้องกัน อาทิ ระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนแบบหลายปัจจัย นโยบายรหัสผ่านที่เข้มงวด และการประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง มาใช้ในการเสริมประสิทธิภาพการตรวจจับและตอบสนอง โดยมุ่งหวังผลลัพธ์ในการลดจำนวนภัยคุกคาม เพิ่มความแม่นยำในการตรวจจับ และเสริมสร้างความมั่นคงของระบบเครือข่ายขององค์กร

วิธีดำเนินการวิจัย

ผู้วิจัยมุ่งเน้นการศึกษารูปแบบการโจมตี โดยดำเนินการตามขั้นตอน ดังนี้

ขั้นตอนที่ 1 ผู้วิจัยรวบรวมข้อมูลการโจมตีทางไซเบอร์จากเครื่องแม่ข่ายจำนวน 95 เครื่องในศูนย์ข้อมูลกลางของมหาวิทยาลัยราชภัฏกาญจนบุรี โดยเลือกเครื่องที่มีความเสี่ยงสูง 5 เครื่องมาวิเคราะห์เชิงลึก ครอบคลุมประเภทภัยคุกคาม ความถี่ และผลกระทบที่เกิดขึ้น ระหว่างวันที่ 12 กรกฎาคม ถึง 28 ธันวาคม พ.ศ. 2567 ข้อมูลได้รับจากระบบป้องกันการบุกรุก พฤติกรรมผู้ใช้ และข้อมูลการเข้าถึงระบบ โดยใช้เครื่องมือ เช่น ระบบป้องกันแอปพลิเคชันเว็บ ระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง และเครื่องมือวิเคราะห์ข้อมูล เพื่อประเมินแนวโน้มการโจมตีและสนับสนุนการพัฒนามาตรการที่เหมาะสม

ขั้นตอนที่ 2 การวิเคราะห์ข้อมูล ผู้วิจัยได้นำระบบที่มีฟังก์ชันการเรียนรู้ของเครื่อง มาประยุกต์ใช้งานผ่านระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง และระบบจัดการเหตุการณ์ด้านความปลอดภัย ซึ่งมีความสามารถในการวิเคราะห์พฤติกรรมการใช้งาน ตรวจจับความผิดปกติ และแจ้งเตือนภัยคุกคามได้โดยอัตโนมัติ ทั้งนี้ ระบบดังกล่าวมีמודูล Machine Learning ฝังอยู่ในตัวเครื่องมือโดยผู้วิจัยไม่ได้พัฒนาโมเดลขึ้นมาเอง แต่ใช้ประโยชน์จากพีเจอร์อัจฉริยะที่มาพร้อมระบบ เพื่อสนับสนุนการวิเคราะห์เชิงรุกและเพิ่มความแม่นยำในการตรวจจับภัยคุกคาม

ขั้นตอนที่ 3 การพัฒนาแนวทางการป้องกันหลายชั้นมาใช้เพื่อเสริมสร้างความมั่นคงปลอดภัยทางไซเบอร์และลดความเสี่ยงจากภัยคุกคาม โดยพัฒนามาตรการหลัก 5 ด้าน ดังนี้

1. เสริมสร้างโครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยของระบบเครือข่าย
2. กำหนดและควบคุมสิทธิ์การเข้าถึง พร้อมบังคับใช้นโยบายความปลอดภัยอย่างเคร่งครัด
3. เฝ้าระวังและตรวจจับภัยคุกคามเชิงรุกจากแหล่งข้อมูลที่หลากหลาย
4. พัฒนาและทดสอบระบบรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อประเมินประสิทธิภาพของมาตรการ
5. ส่งเสริมความรู้และการบริหารความเสี่ยงทางไซเบอร์ให้แก่บุคลากรทุกระดับ เพื่อเป็นองค์ประกอบ

สำคัญในการรักษาความมั่นคงปลอดภัยขององค์กร

ขั้นตอนที่ 4 ดำเนินการทดลองมาตรการป้องกันภัยคุกคามในสภาพแวดล้อมจริง โดยเก็บข้อมูลจากระบบรักษาความปลอดภัยหลัก 3 ประเภท ได้แก่ ระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง ระบบจัดการข้อมูลด้านความปลอดภัยและเหตุการณ์ และระบบป้องกันการบุกรุก ข้อมูลที่ได้จะนำมาวิเคราะห์แนวโน้มภัยคุกคาม ความถี่การโจมตี ประสิทธิภาพในการตอบสนอง และผลกระทบต่อระบบเครือข่าย เพื่อนำไปปรับปรุงมาตรการรักษาความปลอดภัยให้มีประสิทธิภาพมากยิ่งขึ้น

ขั้นตอนที่ 5 เปรียบเทียบผลการทดลองมาตรการป้องกันภัยคุกคามทางไซเบอร์ โดยเก็บข้อมูลจากระบบตรวจจับและวิเคราะห์ ทั้งในสภาวะปกติและภายใต้การโจมตี เพื่อประเมินแนวโน้มภัยคุกคาม ประสิทธิภาพการตอบสนอง และผลกระทบต่อระบบเครือข่าย เพื่อนำข้อมูลมาเปรียบเทียบกับมาตรการเดิม พร้อมวิเคราะห์ความสัมพันธ์ของเหตุการณ์และประยุกต์ใช้การเรียนรู้ของเครื่อง เพื่อเพิ่มความแม่นยำในการตรวจจับและเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย

ผลการวิจัย

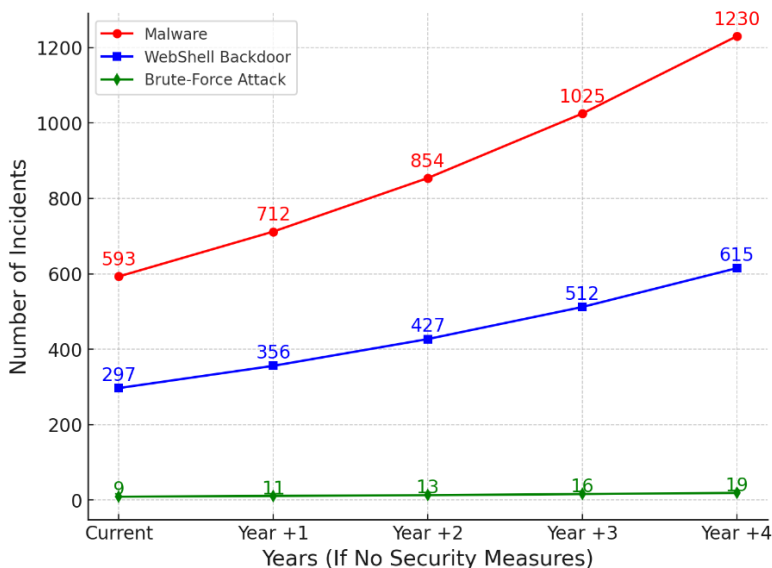
การวิจัยนี้วิเคราะห์ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อระบบเครือข่าย โดยศึกษารูปแบบการโจมตี ผลกระทบ และแนวทางป้องกัน พร้อมประเมินประสิทธิภาพของมาตรการผ่านการเปรียบเทียบก่อนและหลังการใช้งานจริง โดยนำเสนอผลลัพธ์ในรูปแบบภาพประกอบและตาราง ดังต่อไปนี้

ตารางที่ 1

การจำแนกประเภทภัยคุกคามทางไซเบอร์ในระบบเครือข่ายขององค์กร

ประเภทภัยคุกคาม	คำจำกัดความ	จำนวนเหตุการณ์	ผลกระทบ	มาตรการป้องกัน
มัลแวร์	ซอฟต์แวร์ที่ทำลายหรือควบคุมระบบ	593 ครั้ง	- สูญเสียข้อมูล - ระบบหยุดทำงาน	- การใช้โปรแกรมป้องกันมัลแวร์
ประตูลังเว็บเซลล์	มัลแวร์ที่ฝังในเซิร์ฟเวอร์เพื่อควบคุมจากระยะไกล	297 ครั้ง	- ขโมยข้อมูล - ระบบถูกควบคุม	- ระบบป้องกันแอปพลิเคชันเว็บ - อัปเดตซอฟต์แวร์
การโจมตีแบบเดารหัสผ่าน	การพยายามเดารหัสผ่านโดยการทดสอบความเป็นไปได้ทั้งหมด	9 ครั้ง	- เข้าถึงข้อมูลที่เป็น ความลับ	- รหัสผ่านซับซ้อน - การยืนยันตัวตนหลายปัจจัย

ตารางที่ 1 พบว่า มัลแวร์เป็นภัยคุกคามที่พบมากที่สุด 593 ครั้ง ส่งผลให้เกิดการสูญเสียข้อมูลและระบบหยุดชะงัก แนวทางป้องกันที่แนะนำ ได้แก่ การติดตั้งโปรแกรมป้องกันมัลแวร์ที่ทันสมัย การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ และใช้ระบบตรวจจับพฤติกรรมผิดปกติ (Buriro et al., 2024) สำหรับประตูลังเว็บเซลล์ตรวจพบ 297 ครั้ง เพิ่มความเสี่ยงต่อการควบคุมระบบจากระยะไกล ควรใช้ระบบป้องกันแอปพลิเคชันเว็บ ระบบเฝ้าระวังแบบเรียลไทม์ และตรวจสอบไฟล์บันทึกต่อเนื่อง (Santos et al., 2018) ส่วนการโจมตีแบบเดารหัสผ่านแม้พบเพียง 9 ครั้ง แต่ยังคงเฝ้าระวัง โดยควรใช้นโยบายรหัสผ่านที่ซับซ้อน การยืนยันตัวตนหลายปัจจัย และตรวจสอบพฤติกรรม การเข้าถึงอย่างรอบคอบ (Premesai, 2024) ทั้งนี้ ควรพัฒนาแนวทางป้องกันที่เป็นระบบ ปรับปรุงนโยบายความปลอดภัย และประยุกต์ใช้เทคโนโลยีปัญญาประดิษฐ์และระบบเรียนรู้ของเครื่อง เพื่อเพิ่มประสิทธิภาพในการตรวจจับและตอบสนอง ลดความเสี่ยง และเสริมสร้างความมั่นคงปลอดภัยของระบบเครือข่าย



ภาพที่ 2 แนวโน้มเหตุการณ์ภัยคุกคามทางไซเบอร์ในกรณีไม่มีมาตรการป้องกัน

ภาพที่ 2 แสดงแนวโน้มของภัยคุกคามทางไซเบอร์ที่มีแนวโน้มเพิ่มขึ้นอย่างต่อเนื่อง หากไม่มีมาตรการป้องกัน โดยมีมัลแวร์เพิ่มจาก 593 เป็น 1,230 ครั้งในระยะเวลา 4 ปี ประตูลังเว็บเชลล์จาก 297 เป็น 615 ครั้ง และการโจมตีแบบเดรทส์ผ่านจาก 9 เป็น 19 ครั้ง ซึ่งสะท้อนถึงความจำเป็นในการใช้มาตรการรักษาความปลอดภัยที่มีประสิทธิภาพ เช่น ระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนหลายปัจจัย การเข้ารหัสแบบเรียลไทม์ รวมถึงการประยุกต์ใช้ข่าวกรองภัยคุกคามและการเรียนรู้ของเครื่อง เพื่อเพิ่มความแม่นยำในการตรวจจับและตอบสนองต่อเหตุการณ์ ทั้งนี้ แนวโน้มดังกล่าวอิงจากแนวคิดการวิเคราะห์แนวโน้ม (Trend Analysis) และการพยากรณ์ด้วยข้อมูลอนุกรมเวลา (Time Series Forecasting) ซึ่งเป็นแนวทางที่ใช้กันอย่างแพร่หลายในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อแสดงให้เห็นถึงความเสี่ยงที่อาจเกิดขึ้นหากไม่มีการดำเนินการป้องกันอย่างเพียงพอ

ตารางที่ 2

การวิเคราะห์คอมพิวเตอร์แม่ข่ายที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์

อุปกรณ์	หมายเลขไอพี	การโจมตี	จำนวนโจมตี	ผลกระทบ
WIN-B7SQ2UVP2VA	10.0.0.217	ประตูลังเว็บเชลล์ - PHP.MLVirus	143 ครั้ง	- ควบคุมระบบจากระยะไกลและขโมยข้อมูล
WIN-BAGUHNNBMTL	10.0.0.164	ประตูลังเว็บเชลล์ - ASP.MLVirus	106 ครั้ง	- ขโมยข้อมูลสำคัญและลดประสิทธิภาพของระบบ

ตารางที่ 2 (ต่อ)

อุปกรณ์	หมายเลข ไอพี	การโจมตี	จำนวน โจมตี	ผลกระทบ
WIN TBE115CCQ02	10.0.0.206	การโจมตีแบบฉีดคำสั่ง SQL ผ่านเว็บเซลล์	48 ครั้ง	- ระบบหยุดชะงักชั่วคราว และเกิดความเสี่ยงต่อ ฐานข้อมูล
WIN ILSUPK5420F	10.0.0.132	- เครื่องมือโจมตีระบบ ระยะไกล - PsExec	1 ครั้ง	- เครื่องมือสำหรับโจมตี ระบบระยะไกล
WIN-SERVER01	10.0.0.157	การโจมตีแบบเดรทส์ ผ่านบน SMB	1,555 ครั้ง	- พยายามเดรทส์ผ่านซ้ำ ๆ แต่ไม่สำเร็จ
WIN-SERVER02	10.0.0.198	การโจมตีแบบเดรทส์ผ่าน	9 ครั้ง	- พยายามเข้าถึงระบบไม่ สำเร็จ แต่ยังคงเสี่ยงต่อ การโจมตีในอนาคต

ตารางที่ 2 พบว่า เครื่องแม่ข่ายขององค์กรเผชิญกับภัยคุกคามหลายรูปแบบ โดย WIN-B7SQ2UVP2VA และ WIN-BAGUHNBNBMTL ถูกโจมตีด้วยประตูลังเว็บเซลล์รวม 249 ครั้ง ซึ่งมีสาเหตุมาจากช่องโหว่ของแอปพลิเคชันเว็บและการตั้งค่าความปลอดภัยที่ไม่เหมาะสม ส่งผลให้ระบบเสี่ยงต่อการถูกควบคุมและข้อมูลรั่วไหล ส่วน WIN-TBE115CCQ02 ถูกโจมตีแบบฉีดคำสั่ง SQL ผ่านเว็บเซลล์ 48 ครั้ง อันเนื่องมาจากการป้องกันคำสั่งในฟอร์มอินพุตไม่เพียงพอ ส่งผลต่อเสถียรภาพและความปลอดภัยของฐานข้อมูล ขณะที่ WIN-ILSUPK5420F พบเครื่องมือโจมตีระบบระยะไกล (PsExec) จำนวน 1 ครั้ง ซึ่งมักเกิดจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต ด้าน WIN-SERVER01 และ WIN-SERVER02 เผชิญการโจมตีแบบเดรทส์ผ่านรวม 1,564 ครั้ง โดยเกิดจากการเปิดให้บริการ SMB โดยไม่มีมาตรการควบคุมการเข้าถึงที่เหมาะสม แม้ยังไม่สำเร็จ แต่ยังคงเป็นความเสี่ยงที่ต้องเฝ้าระวัง โดยควรใช้มาตรการป้องกันแบบหลายชั้นร่วมกับการยืนยันตัวตน นโยบายรหัสผ่านที่รัดกุม ระบบตรวจจับพฤติกรรมที่ผิดปกติ และการเฝ้าระวังความปลอดภัยแบบเรียลไทม์

ตารางที่ 3

การวิเคราะห์เหตุการณ์ด้านความปลอดภัยทางไซเบอร์

เหตุการณ์ความปลอดภัย	จำนวน ครั้ง	สถานะการ โจมตี	ผลจากการโจมตีสำเร็จ	ผลกระทบ
WebShell- Backdoor.PHP.MIVirus	256 ครั้ง	สำเร็จ	ข้อมูลสำคัญถูกขโมยและ ระบบถูกควบคุมจาก ระยะไกล	ควบคุมระบบ ระยะไกลและขโมย ข้อมูล
Brute-Force บน SMB	5 ครั้ง	ไม่สำเร็จ	ไม่มีผลกระทบ	พยายามเดา รหัสผ่าน

ตารางที่ 3 (ต่อ)

เหตุการณ์ความปลอดภัย	จำนวน ครั้ง	สถานะการ โจมตี	ผลจากการโจมตีสำเร็จ	ผลกระทบ
WebShell.ASP.MlVirus	17 ครั้ง	สำเร็จ	ข้อมูลถูกขโมยและส่งผลกระทบต่อประสิทธิภาพของระบบ	ขโมยข้อมูลสำคัญ
SQL Injection ผ่าน WebShell	12 ครั้ง	สำเร็จ	ฐานข้อมูลเสี่ยงต่อการโจมตีเพิ่มเติม	ความเสี่ยงต่อฐานข้อมูล
การพยายามเข้าถึงระบบแบบ Brute-Force	4 ครั้ง	ไม่สำเร็จ	ไม่มีผลกระทบสำคัญ	ความพยายามในการเข้าถึงล้มเหลว

ตารางที่ 3 แสดงให้เห็นว่า WebShell-Backdoor.PHP.MlVirus เป็นภัยคุกคามที่ตรวจพบบ่อยที่สุดจำนวน 256 ครั้ง ซึ่งมีความเสี่ยงสูงต่อการถูกควบคุมระบบจากระยะไกลและการเข้าถึงข้อมูลสำคัญโดยมิชอบตามด้วย WebShell.ASP.MlVirus จำนวน 17 ครั้ง และ SQL Injection ผ่าน WebShell อีก 12 ครั้ง ซึ่งแม้บางรายการจะไม่สำเร็จในการเจาะระบบ แต่ยังแสดงให้เห็นถึงความพยายามเข้าถึงช่องโหว่ที่เกี่ยวข้องกับการจัดการคำสั่งในระดับแอปพลิเคชัน อีกทั้งยังพบการโจมตีแบบ Brute-Force บน SMB จำนวน 5 ครั้ง และอื่น ๆ อีก 4 ครั้ง ซึ่งสะท้อนถึงความเสี่ยงจากช่องทางการเข้าสู่ระบบที่ไม่ได้รับการควบคุมอย่างรัดกุม องค์ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ชี้ว่า WebShell เป็นหนึ่งในภัยคุกคามที่ตรวจจับได้ยาก เนื่องจากมักถูกฝังอยู่ในโค้ดของเว็บแอปพลิเคชันที่ถูกเผยแพร่หรือไม่มีการตรวจสอบอย่างสม่ำเสมอ ข้อสังเกตจากผลการวิเคราะห์นี้คือภัยคุกคามที่พบนั้นส่วนใหญ่เกี่ยวข้องกับการละเมิดระดับแอปพลิเคชันและสิทธิ์การเข้าถึง จึงจำเป็นต้องเสริมมาตรการรักษาความปลอดภัยในหลายระดับ โดยเฉพาะระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนหลายปัจจัย ระบบป้องกันการบุกรุก และการใช้ข่าวกรองภัยคุกคาม ร่วมกับการวิเคราะห์พฤติกรรมผู้ใช้เพื่อเพิ่มประสิทธิภาพในการตรวจจับล่วงหน้าและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

ตารางที่ 4

การประเมินความเสี่ยงและมาตรการจัดการจากเหตุการณ์ด้านความปลอดภัยในระบบเครือข่าย

เหตุการณ์ความปลอดภัย	ความถี่ของการโจมตี	ผลกระทบต่อการปฏิบัติงาน	ผลกระทบต่องานองค์กร	ระดับความเสี่ยง	มาตรการเพิ่มเติม
WebShell-Backdoor.PHP.MlVirus	สูง	สูง	สูง	สูง	- ใช้ระบบป้องกันแอปพลิเคชันเว็บ - ตรวจสอบการเข้าถึงเครือข่าย

ตารางที่ 4 (ต่อ)

เหตุการณ์ ความปลอดภัย	ความถี่ ของการ โจมตี	ผลกระทบ ต่อการ ปฏิบัติงาน	ผลกระทบต่อ ภาพลักษณ์ องค์กร	ระดับ ความเสี่ยง	มาตรการเพิ่มเติม
Brute-Force บน SMB	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	- ใช้การยืนยันตัวตน หลายปัจจัย - กำหนดนโยบาย รหัสผ่านที่เข้มงวด
WebShell- Backdoor.PHP.MlVirus	สูง	สูง	สูง	สูง	- ใช้ระบบป้องกัน แอปพลิเคชันเว็บ - ตรวจสอบการ เข้าถึงเครือข่าย
Brute-Force บน SMB	ต่ำ	ต่ำ	ปานกลาง	ปานกลาง	- ใช้การยืนยันตัวตน หลายปัจจัย - กำหนดนโยบาย รหัสผ่านที่เข้มงวด
WebShell- Backdoor.ASP.MlVirus	ปานกลาง	ปานกลาง	ปานกลาง	ปานกลาง	- ใช้ระบบป้องกัน แอปพลิเคชันเว็บ - อัปเดตซอฟต์แวร์ อย่างสม่ำเสมอ
SQL Injection ผ่าน WebShell	ปานกลาง	สูง	ปานกลาง	สูง	- ติดตั้งระบบป้องกัน ฐานข้อมูล
การพยายามเข้าถึงระบบ แบบ Brute-Force	ต่ำ	ต่ำ	ต่ำ	ต่ำ	- ใช้การยืนยันตัวตน หลายปัจจัย - ตรวจสอบการเข้า สู่ระบบ

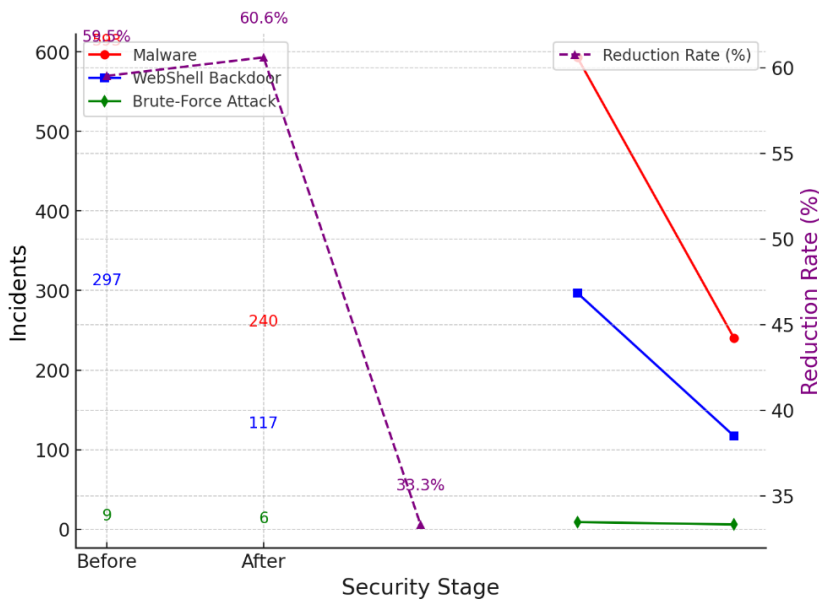
จากตารางที่ 4 พบว่า WebShell-Backdoor.PHP.MlVirus เป็นภัยคุกคามที่มีความเสี่ยงสูงสุด ทั้งด้านความถี่และผลกระทบ ควรใช้ระบบป้องกันแอปพลิเคชันเว็บและตรวจสอบการเข้าถึงอย่างใกล้ชิด ส่วน SQL Injection แม้พบไม่บ่อยแต่กระทบฐานข้อมูลโดยตรงจึงต้องมีมาตรการเฉพาะ ด้าน Brute-Force บน SMB และ WebShell.ASP มีความเสี่ยงปานกลาง ควรใช้การยืนยันตัวตนหลายปัจจัยและอัปเดตระบบสม่ำเสมอ ขณะที่การเดารหัสผ่านทั่วไปแม้มีความเสี่ยงต่ำแต่ยังต้องเฝ้าระวัง ผลการประเมินสะท้อนความจำเป็นในการจัดการความเสี่ยงอย่างเป็นระบบและจัดสรรทรัพยากรอย่างเหมาะสม

ตารางที่ 5

เปรียบเทียบแนวโน้มภัยคุกคามทางไซเบอร์ก่อนและหลังการใช้มาตรการรักษาความปลอดภัย

ประเภทภัยคุกคาม	จำนวนเหตุการณ์ ก่อนปรับปรุง	จำนวนเหตุการณ์ หลังปรับปรุง	อัตราการลดลง (%)	ระดับความเสี่ยง คงเหลือ
มัลแวร์	593 ครั้ง	240 ครั้ง	-59.53%	ปานกลาง
ประตูหลังเว็บเซิร์ฟเวอร์	297 ครั้ง	117 ครั้ง	-60.61%	ปานกลาง
การโจมตีแบบเดารหัสผ่าน	9 ครั้ง	6 ครั้ง	-33.33%	ต่ำ

ตารางที่ 5 แสดงให้เห็นว่ามาตรการด้านความปลอดภัยที่นำมาใช้สามารถลดการโจมตีทางไซเบอร์ได้อย่างมีนัยสำคัญ โดยมัลแวร์ลดลง 59.53% เว็บเซิร์ฟเวอร์ลดลง 60.61% และการเดารหัสผ่านลดลง 33.33% ซึ่งเป็นผลจากการใช้ซอฟต์แวร์ป้องกัน การอัปเดตแพตช์ ระบบตรวจจับภัยคุกคาม และการยืนยันตัวตนหลายปัจจัย อย่างไรก็ตาม ภัยคุกคามบางประเภทยังคงมีความเสี่ยง จึงจำเป็นต้องเฝ้าระวังและปรับปรุงมาตรการอย่างต่อเนื่อง โดยเฉพาะการใช้ข่าวกรองภัยคุกคามและการเรียนรู้ของเครื่องเพื่อเพิ่มความแม่นยำในการคาดการณ์และตอบสนองอย่างมีประสิทธิภาพ



ภาพที่ 3 เปรียบเทียบแนวโน้มภัยคุกคามทางไซเบอร์ก่อนและหลังการใช้มาตรการรักษาความปลอดภัย

ภาพที่ 3 แสดงการเปรียบเทียบแนวโน้มภัยคุกคามทางไซเบอร์ก่อนและหลังการใช้มาตรการรักษาความปลอดภัย โดยพบว่าจำนวนเหตุการณ์ลดลงอย่างชัดเจนในทุกประเภท ได้แก่ มัลแวร์ลดจาก 593 เหลือ 240 ครั้ง เว็บเซิร์ฟเวอร์จาก 297 เหลือ 117 ครั้ง และการโจมตีแบบเดารหัสผ่านจาก 9 เหลือ 6 ครั้ง สะท้อนให้เห็นถึง

ประสิทธิภาพของมาตรการที่นำมาใช้ ทั้งในด้านระบบตรวจจับภัยคุกคาม การป้องกันแอปพลิเคชันเว็บ และการยืนยันตัวตนหลายปัจจัย (Tong et al., 2023) ซึ่งชี้ให้เห็นถึงความสำคัญของการประยุกต์ใช้เทคโนโลยีด้านความมั่นคงปลอดภัยเพื่อรับมือกับภัยคุกคามที่ซับซ้อนในระบบเครือข่าย

สรุปผลการวิจัย

การวิจัยนี้มีเป้าหมายเพื่อวิเคราะห์และประเมินภัยคุกคามทางไซเบอร์ในระบบเครือข่ายขององค์กร โดยมุ่งเน้นภัยคุกคามหลัก 3 ประเภท ได้แก่ มัลแวร์ ประตูลังเว็บเซลล์ และการโจมตีแบบเดรทส์ผ่าน พร้อมนำเสนอแนวทางป้องกันและตอบสนองที่มีประสิทธิภาพ ผลการศึกษาแสดงให้เห็นว่า ประตูลังเว็บเซลล์เป็นภัยคุกคามที่มีความรุนแรงสูงสุด ตรวจพบจำนวน 297 ครั้ง และมีอัตราการโจมตีสำเร็จสูง ส่งผลให้ผู้ไม่ประสงค์ดีสามารถควบคุมอุปกรณ์จากระยะไกลและเข้าถึงข้อมูลสำคัญโดยไม่ชอบ ซึ่งก่อให้เกิดความเสี่ยงต่อการละเมิดข้อมูล แนวทางป้องกันที่มีประสิทธิภาพ ได้แก่ การใช้ระบบป้องกันแอปพลิเคชันเว็บ การจำกัดการเข้าถึงจากหมายเลขไอพีที่ไม่น่าเชื่อถือ และการตรวจสอบบันทึกกิจกรรมอย่างต่อเนื่อง (Bansal & Mahajan, 2023)

นอกจากนี้ มัลแวร์เป็นภัยคุกคามที่ตรวจพบมากที่สุด จำนวน 593 ครั้ง โดยร้อยละ 20 ของเหตุการณ์มีความรุนแรงสูง ส่งผลให้เกิดการสูญเสียข้อมูลและระบบหยุดชะงัก แนวทางป้องกันที่มีประสิทธิภาพ ได้แก่ การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันมัลแวร์ การวิเคราะห์พฤติกรรมภัยคุกคาม และการใช้ระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง (Jeyshri & Sasirekha, 2023) สำหรับการโจมตีแบบเดรทส์ผ่าน แม้จะพบเพียง 9 ครั้ง แต่มีถึง 5 กรณีที่พยายามเข้าถึงระบบผ่านโปรโตคอล SMB ซึ่งเป็นช่องโหว่ของระบบที่ขาดมาตรการป้องกันเพียงพอ ดังนั้น การตั้งรหัสผ่านที่ซับซ้อน การยืนยันตัวตนหลายปัจจัย และการตรวจสอบพฤติกรรมการณ์การเข้าถึงระบบ จึงเป็นมาตรการสำคัญในการลดความเสี่ยง

ผลการประเมินความเสี่ยงของภัยคุกคามพบว่า WebShell-Backdoor.PHP.MLVirus และการโจมตีแบบ SQL Injection ซึ่งดำเนินการผ่านสคริปต์หรือโค้ดที่เป็นอันตราย จัดอยู่ในระดับความเสี่ยงสูง และส่งผลกระทบต่อระบบและภาพลักษณ์ขององค์กร จึงควรมีการติดตั้งระบบป้องกันแอปพลิเคชันเว็บและระบบป้องกันฐานข้อมูลที่มีประสิทธิภาพ สำหรับ Brute-Force บน SMB และ WebShell-Backdoor.ASP.MLVirus ซึ่งมีระดับความเสี่ยงปานกลาง ควรเสริมด้วยการยืนยันตัวตนแบบหลายปัจจัย การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ และการเฝ้าระวังการเข้าสู่ระบบอย่างต่อเนื่อง ขณะที่การโจมตีแบบเดรทส์ผ่านแม้จะมีระดับความเสี่ยงต่ำ แต่ควรมีการตรวจสอบบันทึกกิจกรรมและวิเคราะห์พฤติกรรมการณ์การเข้าถึงที่ผิดปกติเพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้น

ผลการวิจัยสรุปได้ว่า ระบบเครือข่ายขององค์กรเผชิญกับภัยคุกคามหลัก 3 ประเภท ได้แก่ มัลแวร์ ประตูลังเว็บเซลล์ และการโจมตีแบบเดรทส์ผ่าน ซึ่งส่งผลกระทบต่อความมั่นคงของข้อมูลและระบบ การนำมาตรการป้องกัน เช่น ระบบป้องกันแอปพลิเคชันเว็บ การยืนยันตัวตนหลายปัจจัย และการอัปเดตซอฟต์แวร์มาใช้งาน ส่งผลให้ภัยคุกคามลดลงอย่างมีนัยสำคัญ โดยมัลแวร์ลดลง 59.53% เว็บเซลล์ 60.61% และการเดรทส์ผ่าน 33.33% อย่างไรก็ตาม ยังจำเป็นต้องเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง และควรประยุกต์ใช้ข่าวกรองภัยคุกคาม ร่วมกับการเรียนรู้ของเครื่อง เพื่อเพิ่มความแม่นยำในการตรวจจับและพัฒนามาตรการป้องกันให้สอดคล้องกับสภาวะการณ์ที่เปลี่ยนแปลง (Jamnik et al., 2024)

การอภิปรายผล

ผลการวิจัยพบว่า มัลแวร์ ประตูล้างเว็บเซลล์ และการโจมตีแบบเดรทส์ผ่าน เป็นภัยคุกคามหลักที่ส่งผลกระทบต่อระบบเครือข่ายขององค์กร โดยเฉพาะประตูล้างเว็บเซลล์ที่ตรวจพบสูงถึง 297 ครั้ง และมีอัตราการโจมตีสำเร็จในระดับสูง ทำให้ผู้ไม่หวังดีสามารถควบคุมระบบและเข้าถึงข้อมูลจากระยะไกลได้โดยไม่ถูกตรวจจับ ซึ่งสอดคล้องกับข้อค้นพบของ (Liu & Cheng, 2024) ที่แนะนำให้ใช้ระบบป้องกันแอปพลิเคชันเว็บและจำกัดการเข้าถึงจากไอพีที่ไม่น่าเชื่อถือเพื่อลดความเสี่ยง มัลแวร์พบมากที่สุด 593 ครั้ง โดยร้อยละ 20 มีความรุนแรงสูง ส่งผลให้เกิดการสูญเสียข้อมูลและระบบหยุดชะงัก (Mehta & Gadhavi, 2024) ส่วนการโจมตีแบบเดรทส์ผ่าน แม้พบน้อยเพียง 9 ครั้ง แต่มีถึง 5 กรณีที่พยายามเข้าถึงระบบโดยมิชอบ จึงจำเป็นต้องใช้รหัสผ่านที่ซับซ้อน ร่วมกับการยืนยันตัวตนหลายปัจจัยและการตรวจสอบพฤติกรรมผู้ใช้ (Dheeswar et al., 2024)

จากการดำเนินการวิจัย พบข้อค้นพบสำคัญว่า การนำระบบตรวจจับและตอบสนองในอุปกรณ์ปลายทาง ระบบจัดการเหตุการณ์ด้านความปลอดภัย และระบบป้องกันการบุกรุก มาใช้ร่วมกัน สามารถเพิ่มความแม่นยำในการตรวจจับภัยคุกคามและลดเวลาในการตอบสนองได้อย่างมีนัยสำคัญ โดยเฉพาะเครื่องมือช่วยที่มีความเสี่ยงสูง เมื่อใช้แนวทางการวิเคราะห์เชิงรุกและการเฝ้าระวังแบบเรียลไทม์ สามารถลดผลกระทบจากการโจมตีได้อย่างชัดเจน นอกจากนี้ การพัฒนานโยบายการรักษาความปลอดภัยแบบหลายชั้นและการส่งเสริมความรู้ด้านความมั่นคงปลอดภัยให้แก่บุคลากรยังเป็นปัจจัยสำคัญในการยกระดับความสามารถในการรับมือกับภัยคุกคามที่ซับซ้อน

ผลการเปรียบเทียบก่อนและหลังการใช้มาตรการป้องกัน พบว่ามัลแวร์ลดลง 59.53% เว็บเซลล์ลดลง 60.61% และการเดรทส์ผ่านลดลง 33.33% สะท้อนถึงประสิทธิภาพของการใช้ระบบไฟร์วอลล์สำหรับแอปพลิเคชันเว็บ การยืนยันตัวตนแบบหลายปัจจัย และการอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ อย่างไรก็ตาม ภัยคุกคามบางประเภทยังคงมีความซับซ้อนและต้องเฝ้าระวังอย่างต่อเนื่อง ข้อค้นพบที่สำคัญอีกประการคือ การใช้ข่าวกรองภัยคุกคาม และเทคโนโลยีการเรียนรู้ของเครื่อง สามารถช่วยพยากรณ์แนวโน้มภัยคุกคามปรับปรุงมาตรการตอบสนอง และพัฒนากลยุทธ์ความมั่นคงปลอดภัยให้สอดคล้องกับสภาพแวดล้อมของแต่ละองค์กร (Kalra & Tanwar, 2023; Tong et al., 2023)

ข้อเสนอแนะ

จากการวิจัยผู้วิจัยมีข้อเสนอแนะที่ได้จากงานวิจัยดังนี้

1. ควรศึกษาการประยุกต์ใช้ปัญญาประดิษฐ์และการเรียนรู้ของเครื่อง ในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ โดยเฉพาะการตรวจจับพฤติกรรมผิดปกติ และการพัฒนาแบบจำลองที่สามารถเรียนรู้และปรับปรุงความแม่นยำได้อย่างต่อเนื่อง
2. ควรพัฒนาระบบรักษาความปลอดภัยที่มีต้นทุนต่ำ เหมาะสมกับองค์กรที่มีงบประมาณจำกัด โดยใช้ซอฟต์แวร์โอเพนซอร์ส ระบบแจ้งเตือนที่เข้าใจง่าย และมาตรการป้องกันที่สามารถนำไปปฏิบัติได้จริง พร้อมทั้งประเมินประสิทธิภาพและความคุ้มค่าในการใช้งาน

เอกสารอ้างอิง

- Bansal, Y., & Mahajan, S. (2023). Network security breaches: Comprehension and its implications. In K. Kaushik, & A. Bhardwaj (Eds.), *Perspectives on ethical hacking and penetration testing* (pp. 239-254). IGI Global Scientific Publishing. <https://doi.org/10.4018/978-1-6684-8218-6.ch010>

- Buriro, A., Rafi, A., Yaqub, M. A., & Luccio, F. (2024). Malware detection using anomaly detection algorithms. In *Proceedings of the 15th International Conference on Ubiquitous and Future Networks* (pp. 330–335). IEEE Xplore. <https://doi.org/10.1109/icufn61752.2024.10624871>
- Che, L., & Liu, X. (2024). Research on WebShell encrypted communication detection based on machine learning. In *Proceedings of the 3rd International Conference on Algorithms, Microchips, and Network Applications*. SPIE Digital Library. <https://doi.org/10.1117/12.3032051>
- Dheeswar, K., Babu, K. K., & Vidya, M. Q. M. (2024). Multifactor authentication system. *International Scientific Journal of Engineering and Management*, 3(3), 1-7. <https://doi.org/10.55041/isjem01343>
- Jamnik, K. R., Dhake, N. S., Rani, S., Mishra, R. R., Ukey, V. L., & Patil, J. P. (2024). Mathematical frameworks for threat intelligence analysis: Leveraging graph theory and machine learning for cyber threat assessment. *International Scientific Journal of Engineering and Management*, 31(3s), 503–519. <https://doi.org/10.52783/cana.v31.804>
- Jeyshri, J., & Sasirekha, R. (2023). Malware mitigation tools. In S. S. Darshan, M. M. Kumar, B. Prashanth, & Y. V. S. Murthy (Eds.), *Malware analysis and intrusion detection in cyber-physical systems* (pp. 331-347). IGI Global Scientific Publishing. <https://doi.org/10.4018/978-1-6684-8666-5.ch015>
- Kalra, K., & Tanwar, B. (2023). Cyber security policy in India: Examining the issues, challenges, and framework. In S. Verma, V. Vyas, & K. Kaushik (Eds.), *Cybersecurity issues, challenges, and solutions in the business world* (pp. 120-137). IGI Global Scientific Publishing. <https://doi.org/10.4018/978-1-6684-5827-3.ch009>
- Liu, J., & Cheng, W. (2024). Design and implementation of a web application firewall system based on OpenResty. In *Proceedings of the 9th International Symposium on Computer and Information Processing Technology* (pp. 6–9). IEEE Xplore. <https://doi.org/10.1109/iscipt61983.2024.10673202>
- Mehta, S., & Gadhavi, L. J. (2024). Anticipating threats through malware detection approaches to safeguard data privacy and security: An in-depth study. In *Proceedings of the 3rd International Conference for Innovation in Technology* (pp. 1–8). IEEE Xplore. <https://doi.org/10.1109/inocon60754.2024.10511971>
- Nasharuddin, M. Z. S. M., & Abubakar, A. (2024). Analyzing threat level of the backdoor attack method for an organization's operation. *International Journal on Perceptive and Cognitive Computing*, 10(2), 51-59. <https://doi.org/10.31436/ijpcc.v10i2.484>
- Premasai, R. (2024). Evaluating the impact of multi factor authentication on cybersecurity effectiveness. *International Scientific Journal of Engineering and Management*, 3(7), 1-9. <https://doi.org/10.55041/isjem02098>

- Santos, A. P. F. F., Ribeiro, R. M. S., & Silva, F. M. G. (2018, October 11). Web application protection. Google Patents. <https://patents.google.com/patent/US10489561B2/en>
- Sharma, A., & Babbar, H. (2024). Unveiling backdoor attacks in networking with machine learning approaches. In *Proceedings of the 2nd International Conference on Intelligent Cyber Physical Systems and Internet of Things* (pp. 1327–1331). IEEE Xplore. <https://doi.org/10.1109/icoici62503.2024.10696089>
- Tong, X., Tan, X., & Sun, X. (2023). Abnormal behavior detection based on GCN-BiLSTM. In *Proceedings of the 3rd International Conference on Machine Learning and Computer Application*. SPIE Digital Library. <https://doi.org/10.1117/12.2675168>
- Yu, X., Meng, W., Liu, Y., & Zhou, F. (2023). TridentShell: An enhanced covert and scalable backdoor injection attack on web applications. *Journal of Network and Computer Applications*, 223, 1-12. <https://doi.org/10.1016/j.jnca.2023.103823>