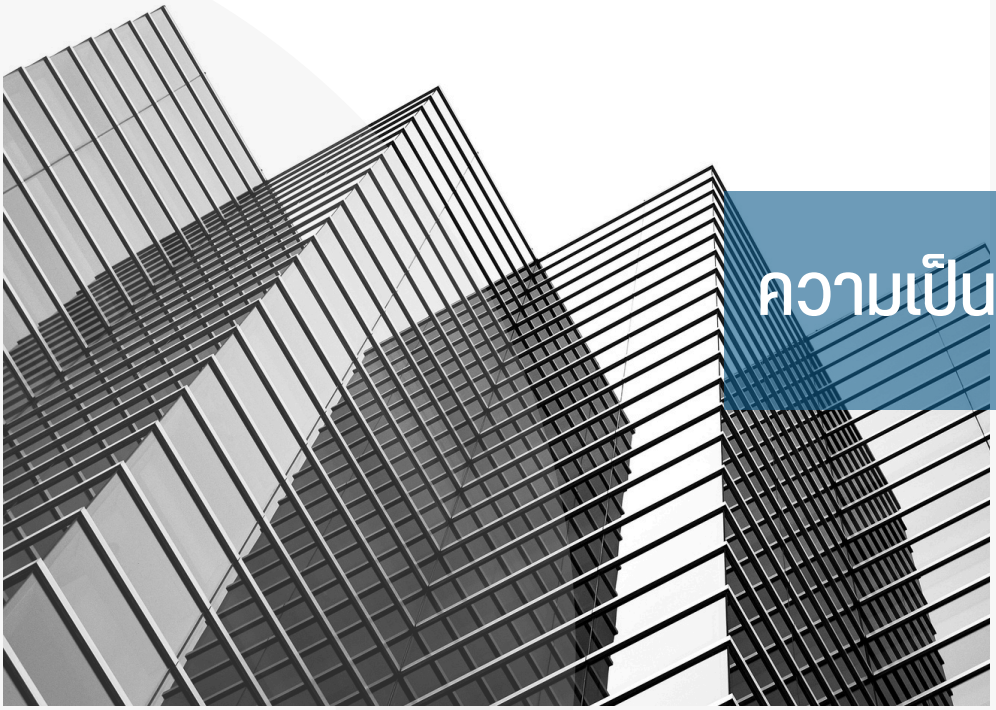
โครงการ
Cyber Security

กรมสนับสนุนบริการสุขภาพ
กระทรวงสาธารณสุข

บริษัท เทคโนวเลจ คอนซัลติ้ง จำกัด

TECH KNOWLEDGE

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support



ความเป็นมาของโครงการ

กรมสนับสนุนบริการสุขภาพ เป็นหน่วยงานที่มีบทบาทสำคัญในการบริหารจัดการระบบบริการสุขภาพในประเทศไทย โดยมีภารกิจหลักสำคัญในการดูแลและยกระดับคุณภาพระบบสุขภาพในภาคประชาชน เพื่อคุ้มครองผู้บริโภคและส่งเสริมความสามารถในการพึ่งพาตนเองด้านสุขภาพอย่างยั่งยืน ซึ่งการบรรลุภารกิจนี้มีความจำเป็นต้องอาศัยการมีส่วนร่วมจากทุกภาคส่วนรวมถึงการนำเทคโนโลยีสารสนเทศเข้ามาประยุกต์ใช้ในการบริหารจัดการระบบบริการสุขภาพ เพื่อให้เพิ่มประสิทธิภาพในการให้บริการดียิ่งขึ้นและรองรับความต้องการที่หลากหลายและการเปลี่ยนแปลงอย่างรวดเร็วของสังคมในยุคสมัยใหม่

สถานการณ์ปัจจุบัน

ในปัจจุบัน การพัฒนาเทคโนโลยีดิจิทัลได้มีความก้าวหน้าอย่างรวดเร็ว และการใช้ระบบสารสนเทศในการบริหารจัดการข้อมูลสุขภาพโดยมีความสำคัญมากขึ้น เช่น ข้อมูลสุขภาพที่สำคัญของผู้ป่วย ข้อมูลส่วนบุคคลของประชาชน และข้อมูลทางการแพทย์ ซึ่งข้อมูลเหล่านี้มีความสำคัญอย่างยิ่งในการวางแผนและให้บริการสุขภาพที่เหมาะสมและมีประสิทธิภาพเพิ่มขึ้น

อย่างไรก็ตาม การจัดเก็บและการจัดการข้อมูลในปัจจุบันยังคงเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นเรื่อย ๆ ไม่ว่าจะเป็นการโจมตีในทางระบบเครือข่าย (Network Attacks), มัลแวร์ (Malware), แรนซัมแวร์ (Ransomware) รวมถึงการโจมตีเว็บไซต์และระบบข้อมูลสารสนเทศขององค์กร การที่ข้อมูลเหล่านี้ถูกโจมตีหรือเข้าถึงโดยไม่ได้รับอนุญาตอาจก่อให้เกิดความเสียหายต่อความมั่นคงขององค์กรและความไว้วางใจจากประชาชนได้

ความจำเป็นในการจัดทำโครงการ

ปกป้องธุรกิจจาก
การโจมตีทาง Cyber

ป้องกันการ
โจมกรรมทางข้อมูล

สร้างความน่าเชื่อถือ
ของข้อมูล

มั่นใจในความปลอดภัย
ของข้อมูล

กรมสนับสนุนบริการสุขภาพจึงมีความจำเป็นต้องยกระดับระบบรักษาความปลอดภัยทางไซเบอร์ โดยจัดทำโครงการ Cyber Security เพื่อพัฒนาและนำระบบปกป้องข้อมูลที่ทันสมัยและมีประสิทธิภาพมาใช้ในการจัดการและปกป้องข้อมูลที่มีความสำคัญ

โครงการมุ่งเน้นไปที่การเพิ่มความปลอดภัยและความมั่นคงของข้อมูล โดยมีการนำระบบเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยที่ทันสมัยเข้ามาใช้ ไม่ว่าจะเป็นระบบป้องกันการบุกรุกเครือข่าย ระบบตรวจจับและตอบสนองภัยคุกคามและระบบวิเคราะห์ข้อมูลแบบเรียลไทม์ได้ เพื่อให้กรมสนับสนุนบริการสุขภาพสามารถมีการเฝ้าระวังและมีการป้องกัน การตอบสนองต่อการโจมตีทางไซเบอร์ได้อย่างมีประสิทธิภาพเพิ่มมากยิ่งขึ้น

วัตถุประสงค์ของโครงการ

โครงการ Cyber Security ของกรมสนับสนุนบริการสุขภาพมีเป้าหมายหลักในการเพิ่มความมั่นคงปลอดภัยในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคลของผู้ใช้บริการและหน่วยงานที่เกี่ยวข้องโดยวัตถุประสงค์ของโครงการสามารถแบ่งออกเป็นหลายด้าน ดังนี้

1.การปกป้องข้อมูลสำคัญและข้อมูลส่วนบุคคล

ข้อมูลของผู้ป่วย ข้อมูลส่วนบุคคลของประชาชนและข้อมูลภายในหน่วยงานจะได้รับการปกป้องจากการเข้าถึงโดยไม่ได้รับอนุญาตและการโจมตีทางไซเบอร์ การรักษาความลับของข้อมูลเป็นปัจจัยที่จำเป็นในการสร้างความเชื่อมั่นแก่ผู้ใช้บริการและสังคม

2.การเฝ้าระวังและติดตามภัยคุกคามแบบเรียลไทม์

การสร้างระบบสามารถเฝ้าระวังและตรวจจับภัยคุกคามไซเบอร์ที่เกิดขึ้นได้แบบเรียลไทม์ ที่ระบบแจ้งเตือนหากมีการโจมตีหรือพบความผิดปกติในเครือข่าย ทำให้ทางทีมรักษาความปลอดภัยสามารถตอบสนองและดำเนินการแก้ไขได้ทัน เพื่อลดความเสี่ยงที่จะเกิดความเสียหายต่อข้อมูลและระบบขององค์กร

3.การป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์

มีการลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์ที่มีในการพัฒนา อยู่ตลอดเวลา เช่น มัลแวร์, แรนซัมแวร์, การโจมตี DDoS และการโจมตีผ่านเว็บแอปพลิเคชันการปกป้องจากภัยคุกคามนี้ทำให้ระบบบริการสุขภาพสามารถดำเนินไปได้อย่างต่อเนื่องและเพื่อให้มีประสิทธิภาพ

4.การสร้างความมั่นใจในความปลอดภัยให้กับผู้ใช้บริการ

ข้อมูลส่วนบุคคลและข้อมูลสุขภาพที่เกี่ยวข้องจะได้รับการจัดเก็บและบริหารจัดการด้วยมาตรการความปลอดภัยที่ทันสมัยและเชื่อถือได้ การสร้างความมั่นใจนี้เป็นสิ่งสำคัญที่ทำให้ผู้ใช้บริการมีความไว้วางใจในระบบการให้บริการของกรมสนับสนุนบริการสุขภาพ

5.การสนับสนุนการดำเนินงานขององค์กรด้วยเทคโนโลยีที่ทันสมัย

เพื่อยกระดับการทำงานของกรมสนับสนุนบริการสุขภาพโดยนำในด้านเทคโนโลยีรักษาความปลอดภัยที่ทันสมัยมาใช้ระบบดังกล่าวจะช่วยให้การปฏิบัติงานด้านการบริหารจัดการของข้อมูลและการให้บริการสุขภาพเป็นไปอย่างมีประสิทธิภาพยิ่งขึ้นเพื่อทำให้องค์กรสามารถปรับตัวและพัฒนาระบบรักษาความปลอดภัยให้รองรับกับภัยคุกคามใหม่ๆได้ตลอดเวลา

6. การปฏิบัติตามมาตรฐานและข้อกำหนดด้านความปลอดภัย

การสร้างระบบที่ปฏิบัติตามมาตรฐานสากลและข้อกำหนดด้านความปลอดภัยไซเบอร์ เช่น การปฏิบัติตามระเบียบทางกฎหมายการปกป้องข้อมูลส่วนบุคคลและการรับรองความปลอดภัยโดยในโครงการนี้จะช่วยให้กรมสนับสนุนบริการสุขภาพสามารถดำเนินงานตามข้อกำหนดที่จำเป็นและลดความเสี่ยงในการละเมิดกฎหมายด้านความปลอดภัยของข้อมูล

ระบบที่นำมาใช้ในปัจจุบัน

การดำเนินโครงการ Cyber Security เพื่อยกระดับความปลอดภัยของข้อมูล กรมสนับสนุนบริการสุขภาพ ระบบเดิมที่ใช้อยู่ในปัจจุบันยังมีข้อจำกัดและไม่สามารถรับมือกับภัยคุกคามที่ซับซ้อนและพัฒนาอย่างรวดเร็วได้ โดยระบบที่ใช้งานในปัจจุบันมีลักษณะ ดังนี้

1.ระบบเดิมที่ใช้งานในปัจจุบันมีการติดตั้งอุปกรณ์ Firewall
การป้องกัน การบุกรุกจากภายนอกระบบนี้สามารถตรวจจับการโจมตีทั่วไปได้ เช่น การโจมตีแบบ Distributed Denial of Service (DDoS) ผ่านช่องโหว่ของเครือข่าย ที่เกี่ยวข้องกับโปรโตคอลพื้นฐานของเครือข่าย

2.ระบบเฝ้าระวังและติดตามการใช้งานเครือข่าย
เครือข่ายที่ถูกออกแบบเพื่อดูแลการใช้งานทรัพยากรเครือข่ายขององค์กร แต่ไม่สามารถตรวจสอบหรือติดตามการเข้าถึงข้อมูลสำคัญ ทำให้การปกป้องข้อมูลสำคัญบางครั้งยังไม่ครอบคลุมและไมาสามารถป้องกันภัยคุกคามที่ซับซ้อนเต็มที่

3.การตรวจจับความผิดปกติในระดับพื้นฐาน
ในปัจจุบันระบบที่ใช้งานอยู่มุ่งเน้นที่การตรวจจับภัยคุกคามที่เกิดจากพฤติกรรมเครือข่ายที่ผิดปกติเท่านั้น แต่ไม่สามารถวิเคราะห์ข้อมูลได้ในเชิงลึกเพื่อระบุปัญหาและแก้ไขได้อย่างรวดเร็ว

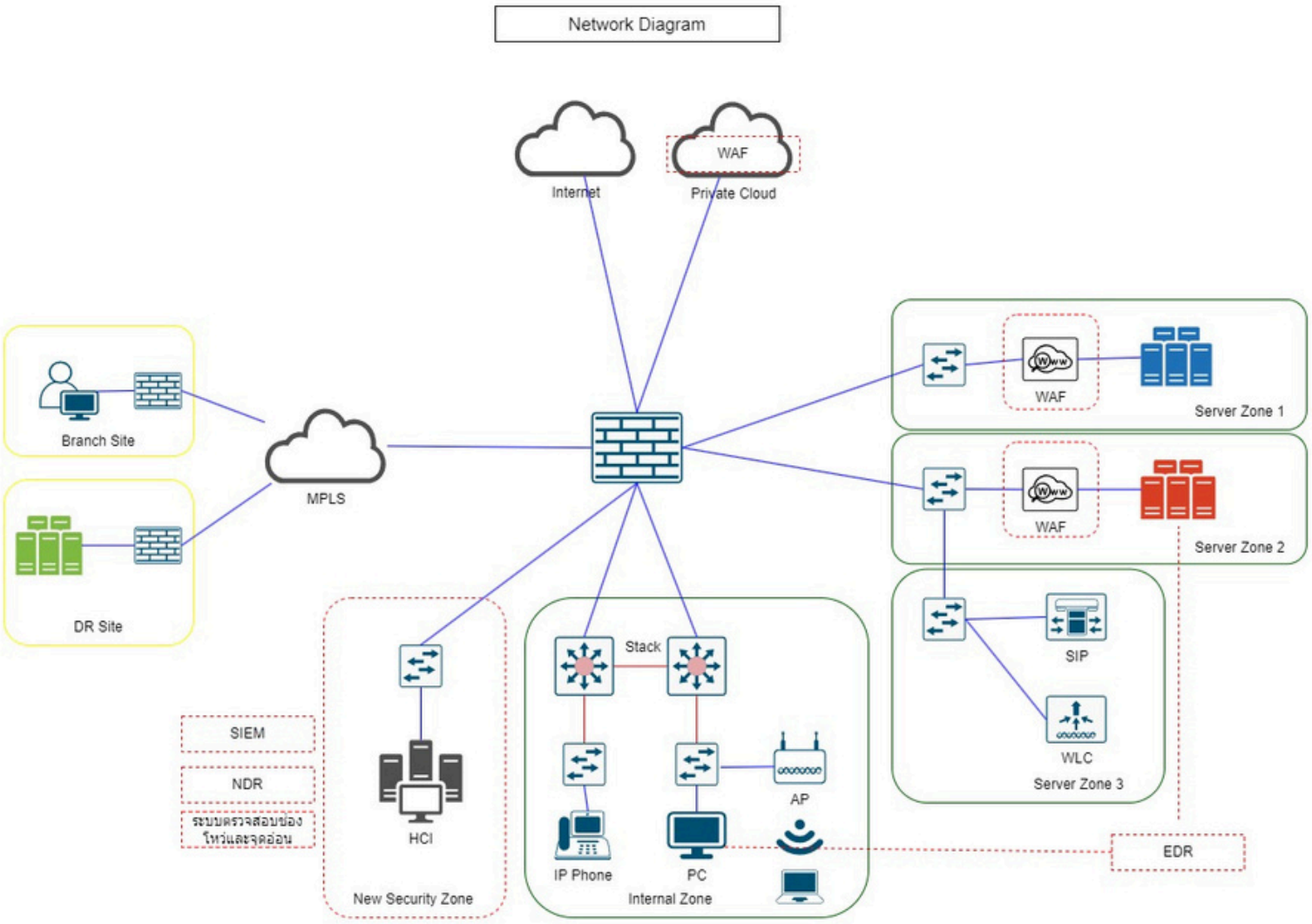
4.ข้อจำกัดในการป้องกันภัยคุกคามใหม่
ระบบเดิมมีการติดตั้งอุปกรณ์รักษาความปลอดภัยพื้นฐานอยู่แล้ว แต่ความสามารถในการป้องกันภัยคุกคามแบบใหม่ เช่น มัลแวร์ที่มีการพัฒนาอย่างรวดเร็ว แรนซัมแวร์และการโจมตีผ่านเว็บ ยังไม่เพียงพอ ทำให้การป้องกันในปัจจุบันมีช่องโหว่และไม่สามารถตอบสนองต่อการโจมตีอย่างมีประสิทธิภาพ

5.การขาดการบูรณาการระหว่างระบบต่าง ๆ
การจัดการข้อมูลด้านความปลอดภัยขาดความเป็นระบบและทำให้เกิดความล่าช้าในการตอบสนองความปลอดภัย การขาดการเชื่อมโยงติดตามการใช้กรัพยากรของระบบเครือข่ายในองค์ ทำให้การวิเคราะห์ตอบสนองต่อภัยคุกคามทำได้ยาก

6.ความท้าทายของระบบที่ใช้งานในปัจจุบัน
ในระบบเดิมไม่สามารถตอบสนองต่อความต้องที่เพิ่มขึ้นในการป้องกันข้อมูลที่ซับซ้อนในยุคดิจิทัล และไม่สามารถจัดการกับภัยคุกคามในรูปแบบที่ทันสมัยอย่างเต็มที่ เช่น การโจมตีที่เกิดขึ้นกับข้อมูลส่วนบุคคลหรือข้อมูลสำคัญที่มีความละเอียดอ่อน

กรมสนับสนุนบริการสุขภาพ

กรมสนับสนุนบริการสุขภาพ
Department of Health Service Support



Network Diagram

แผนผังระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ในโครงการ

ระบบที่ใช้งานในโครงการ

ระบบที่ได้มีการออกแบบเพื่อนำมาใช้ในด้านของการปกป้อง ติดตามและเฝ้าระวัง ข้อมูลสำคัญ รวมถึงข้อมูลส่วนบุคคล ของกรมสนับสนุนบริการสุขภาพ ประกอบด้วยอุปกรณ์ และระบบหลายระบบมาใช้ในการวิเคราะห์ แจ้งเตือน ในส่วนของความผิดปกติในระบบ Network ไปยังระบบ Monitor หลัก เพื่อที่ผู้ดูแลระบบจะใช้ในการวิเคราะห์ข้อมูลเหล่านั้นได้อย่างรวดเร็วเมื่อพบความผิดปกติ ซึ่งประกอบไปด้วยระบบดังนี้

1.อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall)

ทำหน้าที่ป้องกันการโจมตีจากภายนอกและภายในที่พยายามเข้าถึงเว็บไซต์ของกรมสนับสนุนบริการสุขภาพ โดยตรวจจับและป้องกันการโจมตีที่พุ่งเป้าไปที่ช่องโหว่ เช่น การโจมตีแบบ SQL Injection, Cross-Site Scripting (XSS) และการโจมตีอื่น ๆ ที่มีความเสี่ยง

2.อุปกรณ์ตรวจจับและตอบสนองภัยคุกคามเครือข่าย (NDR)

ทำหน้าที่ตรวจสอบการสื่อสารภายในเครือข่าย เพื่อค้นหาและตอบสนองต่อภัยคุกคามที่ อาจเกิดขึ้น เช่น การเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต การเคลื่อนย้ายข้อมูลที่ผิดปกติ ซึ่งอาจบ่งชี้ถึงการบุกรุกเครือข่ายที่ไม่ปลอดภัย

3.ระบบตรวจจับการโจมตีและตอบสนองภัยคุกคามเครื่องแม่ข่าย (EDR)

ทำหน้าที่ในการตรวจสอบสถานะเครื่องแม่ข่ายและเครื่องลูกข่ายในองค์กร เพื่อป้องกันและตอบสนองต่อการโจมตีที่มุ่งเป้าไปยังอุปกรณ์ปลายทาง เช่น มัลแวร์, แรนซัมแวร์ หรือการ โจมตีรูปแบบอื่นที่มุ่งเข้าถึงข้อมูลในเครื่อง

4.ระบบตรวจสอบจุดอ่อนและช่องโหว่ในระบบเครือข่าย

ทำหน้าที่ตรวจสอบจุดอ่อนที่อาจเกิดขึ้นจากการตั้งค่าระบบเครือข่าย หรือการใช้งานอุปกรณ์ที่มี ช่องโหว่สูง ทำให้สามารถแจ้งเตือนและดำเนินการป้องกันก่อนที่ภัยคุกคามจะเข้ามาโจมตีผ่านช่องโหว่

5.ระบบตรวจสอบจุดอ่อนและช่องโหว่ในระบบ Web Application Server

ทำหน้าที่ป้องกันเว็บไซต์ที่มีปริมาณมากในการเข้าถึงข้อมูลจากการโจมตี เช่น DDoS และการโจมตีผ่านช่องโหว่ต่าง ๆ โดยการป้องกันนี้มีความสามารถทำงานแบบ Real-Time ทำให้การตอบสนองรวดเร็วและแม่นยำ

6.ระบบเพิ่มประสิทธิภาพการตรวจจับและตอบสนองต่อภัยคุกคาม (SIEM)

ทำหน้าที่รวมรวมข้อมูลภายในเครือข่าย เช่น การแจ้งเตือนจากอุปกรณ์ป้องกันการบุกรุก และระบบอื่นๆ เพื่อวิเคราะห์ความผิดปกติของข้อมูล นอกจากนี้ยังมีการแจ้งเตือนแบบ Real-Time เพื่อเพิ่มประสิทธิภาพยิ่งขึ้น

ปัญหาและอุปสรรคในโครงการ

1. การเฝ้าระวังและติดตามภัยคุกคามแบบเรียลไทม์

เนื่องจากกรมสนับสนุนบริการสุขภาพมีการใช้งานระบบรักษาความปลอดภัยเดิมมาก่อน การผสานระบบใหม่เข้ากับระบบเดิมอาจเกิดปัญหาใช้งานได้บางส่วน การตั้งค่าของ Config หรือการบริหารจัดการระหว่างอุปกรณ์และซอฟต์แวร์จากผู้ผลิตต่าง ๆ ทำให้ต้องใช้เวลาในการปรับปรุงและตรวจสอบเพื่อให้ทุกระบบทำงานได้อย่างสอดคล้องกัน

2. การขาดแคลนบุคลากรที่เชี่ยวชาญเฉพาะด้าน

การดำเนินงานโครงการ Cyber Security ที่ต้องการการตั้งค่าและการตรวจสอบในระบบที่ซับซ้อนจำเป็นต้องอาศัยบุคลากรที่มีความรู้ความเชี่ยวชาญเฉพาะด้านของการรักษาความปลอดภัยไซเบอร์ ซึ่งบางครั้งการขาดแคลนบุคลากรที่มีทักษะสูงอาจส่งผลให้การติดตั้งและการใช้งานระบบไม่เป็นไปตามแผน หรืออาจต้องใช้เวลานานขึ้นในการแก้ไขปัญหาที่เกิดขึ้นระหว่างการดำเนินงาน

3. งบประมาณและการจัดการทรัพยากรที่จำกัด

ระบบรักษาความปลอดภัยไซเบอร์ที่ทันสมัยจำเป็นต้องใช้งบประมาณสูงในการจัดซื้อหาอุปกรณ์และตัวซอฟต์แวร์ ที่รวมถึงการบำรุงรักษาอย่างต่อเนื่อง ซึ่งอาจเกิดความท้าทายด้านการจัดสรรงบประมาณในระยะยาว และทรัพยากรที่จำเป็น เช่น อุปกรณ์เพิ่มเติมหรือการอัปเกรดระบบ อาจต้องมีการพิจารณาและจัดการให้สอดคล้องกับงบประมาณ

4. ความยุ่งยากในการจัดการข้อมูลจำนวนมาก

การติดตั้งระบบสามารถตรวจสอบและแจ้งเตือนจากภัยคุกคามแบบเรียลไทม์จากข้อมูลที่หลากหลาย ทำให้ปริมาณข้อมูลต้องประมวลผลจำนวนมากหากไม่มีการจัดการที่ดีอาจส่งผลทำให้ทางทีมที่ดูแลการรักษาความปลอดภัยต้องเผชิญกับข้อมูลที่ล้นหลาม (Information Overload) จนไม่สามารถแยกแยะภัยคุกคามที่แท้จริงจากสัญญาณที่ไม่สำคัญได้

5. การรับมือกับภัยคุกคามที่ซับซ้อนและไม่คาดคิด

ภัยคุกคามทางไซเบอร์มีการพัฒนาอย่างรวดเร็วและบางครั้งอาจเกิดการโจมตีรูปแบบใหม่ ที่ยังไม่มีการบันทึกไว้ในฐานของตัวข้อมูลหรือระบบแจ้งเตือน ทำให้ระบบรักษาความปลอดภัยไซเบอร์ที่มีอยู่อาจไม่สามารถตรวจจับหรือตอบสนองต่อการโจมตีเหล่านี้ได้ทันท่วงเวลา ซึ่งอาจส่งผลต่อความปลอดภัยของข้อมูลและระบบขององค์กร

6. การฝึกอบรมและการสร้างความตระหนักรู้แก่พนักงาน

การติดตั้งระบบรักษาความปลอดภัยที่มีประสิทธิภาพสูงแต่หากบุคลากรในองค์กรไม่มีความรู้เพียงพอในการใช้งานระบบหรือไม่มีการตระหนักถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ ก็อาจทำให้เกิดช่องโหว่ในการรักษาความปลอดภัย เช่น การเปิดเผยข้อมูลโดยไม่ตั้งใจ หรือการตกเป็นเป้าหมายของการ โจมตีผ่านฟิชชิง (Phishing)

ผลสัมฤทธิ์ของโครงการ

โครงการ Cyber Security ที่ดำเนินการโดยกรมสนับสนุนบริการสุขภาพได้ประสบความสำเร็จอย่างมีนัยสำคัญในหลายด้านหลังจากการติดตั้งและทดสอบระบบใหม่ทั้งหมดแล้วโครงการได้ส่งผลให้เกิดประโยชน์สำคัญดังนี้

1. การเพิ่มความปลอดภัยของข้อมูลสำคัญและข้อมูลส่วนบุคคล

ระบบใหม่ที่ติดตั้งสามารถปกป้องข้อมูลที่สำคัญทางการแพทย์และข้อมูลระบบบริการสุขภาพอื่น ๆ โดยเฉพาะยุคดิจิทัลที่ข้อมูลมีความสำคัญอย่างมาก ทำให้เกิดความน่าเชื่อถือและความมั่นใจจากผู้ใช้บริการและหน่วยงานที่เกี่ยวข้อง

2. การตรวจสอบและตอบสนองต่อภัยคุกคามได้รวดเร็ว

การติดตั้งระบบทำให้กรมสนับสนุนบริการสุขภาพตรวจจับและตอบสนองภัยคุกคามหลายรูปแบบทางไซเบอร์อย่างรวดเร็ว เช่น NDR, EDR, SIEM และ Web Application Firewall และลดความเสี่ยงจากภัยคุกคามการให้บริการทางสุขภาพขององค์กร

3. การวิเคราะห์ข้อมูลเชิงลึกเพื่อเพิ่มประสิทธิภาพการป้องกัน

ระบบ SIEM และระบบตรวจจับอื่น ๆ ทำให้กรมสนับสนุนบริการสุขภาพสามารถรวบรวมข้อมูลและวิเคราะห์กิจกรรมต่าง ๆ ภายในเครือข่ายระบุจุดอ่อนและช่องโหว่ได้อย่างชัดเจน รวมถึงการพัฒนากระบวนการป้องกันที่ตรงจุดมากยิ่งขึ้น และการใช้ข้อมูลจากการแจ้งเตือนช่วยในด้านความปลอดภัยอย่างต่อเนื่อง

4. การเพิ่มความน่าเชื่อถือและสร้างความมั่นใจให้กับผู้ใช้บริการ

การมีระบบรักษาความปลอดภัยที่ทันสมัยมีประสิทธิภาพในการปกป้องข้อมูลส่วนบุคคลและข้อมูลที่เป็นความลับ ทำให้ผู้ใช้บริการมีความเชื่อมั่นขององค์กร ในมาตรฐานความปลอดภัยที่เข้มงวดยังเสริมสร้างภาพลักษณ์ขององค์กรในฐานะผู้นำในด้านการบริหารจัดการข้อมูลสุขภาพยิ่งขึ้น

5. การปฏิบัติตามข้อกำหนดด้านกฎหมายและมาตรฐานสากล

กรมสนับสนุนบริการสุขภาพสามารถปฏิบัติตามระบบรักษาความปลอดภัยที่นำมาใช้ให้สอดคล้องกับข้อกำหนดทางกฎหมาย และมาตรฐานสากลด้านความปลอดภัยไซเบอร์ ซึ่งช่วยลดความเสี่ยงจากการละเมิดกฎหมายและการถูกคุกคามทางกฎหมายที่เกี่ยวข้องกับการปกป้องข้อมูล

6. การลดความเสี่ยงต่อการหยุดชะงักของบริการ

การตรวจจับภัยคุกคามและตอบสนองได้อย่างรวดเร็วช่วยลดความเสี่ยงที่ระบบหรือบริการสำคัญ จะถูกขัดขวางหรือหยุดชะงัก เช่น การโจมตีแบบ DDoS หรือการโจมตีอื่น ๆ ที่มุ่งหวังทำให้ระบบไม่ สามารถ ให้บริการได้