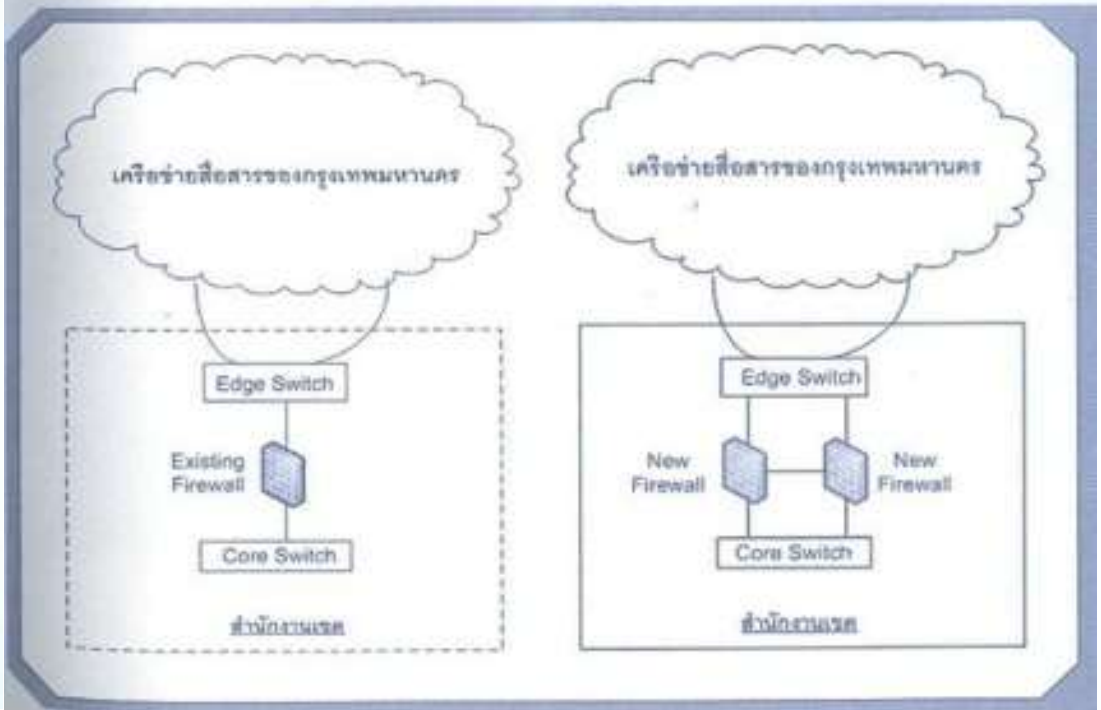
การเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามให้กับระบบสารสนเทศของกรุงเทพมหานคร

กองพัฒนาระบบงานคอมพิวเตอร์

ปัจจุบันระบบสารสนเทศของกรุงเทพมหานคร มีความสำคัญต่อการทำงานเพื่อให้บริการประชาชนในพื้นที่กรุงเทพมหานครอย่างมาก เช่น ระบบบริการจุดเดียวเบ็ดเสร็จ ระบบ MIS และระบบบริการออนไลน์ต่างๆ ซึ่งระบบงานสารสนเทศเหล่านี้ ทำงานผ่านระบบเครือข่ายสื่อสารโดยติดต่อกับเครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์ข้อมูลส่วนกลางทั้งหมด ดังนั้นนโยบายการป้องกันภัยระบบสารสนเทศ จึงต้องมีความรอบคอบและทรงประสิทธิภาพสูงสุด โดยที่ผ่านมากรุงเทพมหานครได้จัดทำโครงการระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์แล้ว โดยมีการติดตั้งอุปกรณ์ป้องกันผู้บุกรุก (Firewall) ณ สำนักงานเขต 50 เขต แต่ด้วยระยะเวลาการใช้งานที่มากกว่า 4 ปีทำให้อุปกรณ์ดังกล่าวเริ่มมีการเสื่อมสภาพ และคุณสมบัติต่ำลงเมื่อเทียบกับเทคโนโลยีรุ่นใหม่ที่อยู่ในท้องตลาดปัจจุบัน และประกอบกับเมื่อภัยคุกคามต่างๆ ได้มีการพัฒนารูปแบบการโจมตีอย่างรวดเร็วและซับซ้อน ทำให้ระบบรักษาความปลอดภัยเดิมที่มีอยู่ทำงานไม่ทันต่อภัยคุกคามทำให้เกิดความเสี่ยงและความเสียหายจากการโจมตีระบบสารสนเทศของกรุงเทพมหานคร ดังนั้น จึงต้องมีการปรับปรุงประสิทธิภาพการป้องกันภัยระบบสารสนเทศ ของกรุงเทพมหานคร เพื่อป้องกันความเสียหายจากภัยคุกคาม และผู้ไม่หวังดีต่อระบบการทำงานของกรุงเทพมหานคร

ดังนั้น แนวทางในการเพิ่มประสิทธิภาพระบบป้องกันภัยคุกคามในครั้งนี้จึงได้มีการจัดหาอุปกรณ์อันได้แก่

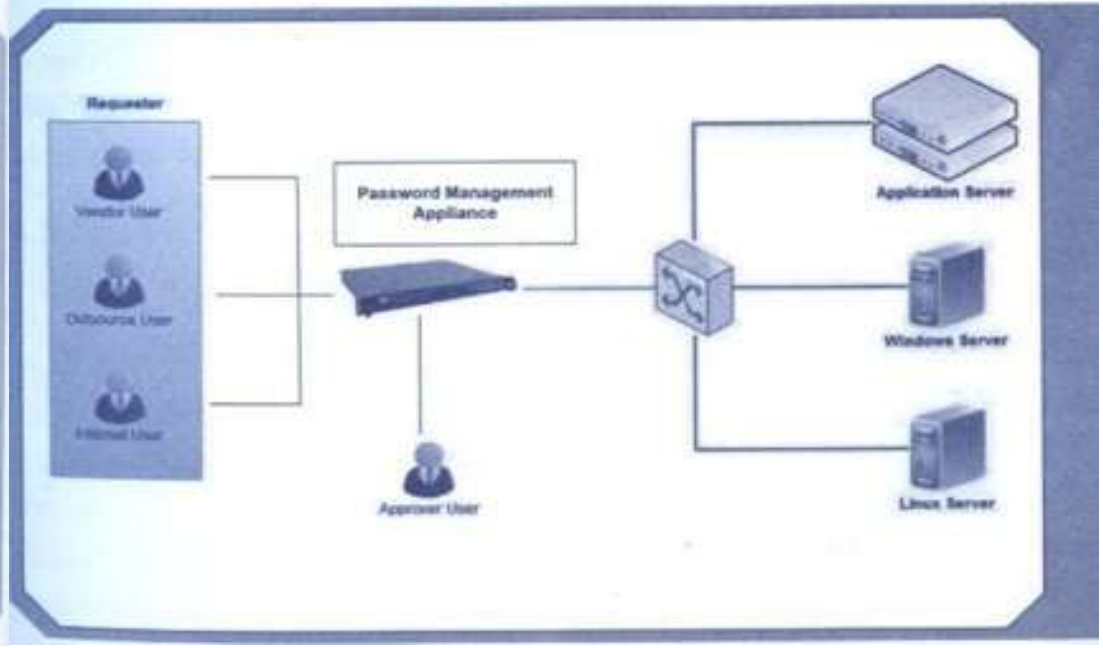
1. การมีอุปกรณ์รักษาความปลอดภัยทางเครือข่ายสื่อสาร (IPS Firewall) ที่มีคุณสมบัติด้านความสามารถในการคัดกรองผู้รับและส่งข้อมูล (Firewall) ความสามารถในการตรวจจับและป้องกันการสื่อสารที่มีลักษณะเป็นภัยคุกคาม (Intrusion Prevention System) ความสามารถในการตรวจจับไวรัส (Anti-Virus) และประสิทธิภาพในส่วนของ Firewall Throughput และ IPS Throughput ที่เพิ่มมากขึ้น เพื่อให้เครือข่ายสื่อสารระหว่างสำนักงานเขตกับส่วนกลางมีการป้องกันและรักษาความปลอดภัยที่มีประสิทธิภาพมากยิ่งขึ้น โดยมีการติดตั้งอุปกรณ์ดังกล่าวจำนวน 2 ชุดต่อสำนักงานเขต เพื่อทำงานทดแทนกันในลักษณะ Active-Standby โดยมีอุปกรณ์ทำหน้าที่หลักหนึ่งตัวและอีกตัวจะทำหน้าที่เป็นตัวสำรอง ในกรณีที่อุปกรณ์ตัวหลักเสียหายอุปกรณ์ตัวสำรองจะทราบสถานะการเสียหายของอุปกรณ์ตัวหลักทันที เนื่องจากมีการตรวจสอบสถานะกันอยู่ตลอดเวลาผ่านการเชื่อมต่อตรงกัน ทำให้อุปกรณ์ตัวสำรองสามารถทำหน้าที่แทนอุปกรณ์ได้อย่างทันที โดยมีการกำหนดนโยบายการรักษาความปลอดภัยของทั้งสองอุปกรณ์มีประสิทธิภาพเหมือนกันทุกประการ



2. การมีอุปกรณ์ป้องกันภัยคุกคามผ่านเว็บไซต์แอพพลิเคชั่น (Web Application Firewall) เพื่อป้องกันภัยคุกคามในระดับ Source Code หรือ Applications ให้กับระบบสารสนเทศของกรุงเทพมหานคร

ทั้งนี้เนื่องจากระบบงานสารสนเทศต่างๆ ของกรุงเทพมหานคร เช่น ระบบ MIS ระบบงาน 50 เขต เป็นลักษณะการทำงานผ่านระบบ Web Application ซึ่งการสื่อสารระหว่างเครื่องลูกข่ายกับเครื่องแม่ข่ายจะติดต่อกันผ่านช่องทางสื่อสาร (Port) ที่เรียกว่า TCP Port 80 (HTTP) หรือ 443 ซึ่งช่องทางสื่อสารดังกล่าวจะได้รับการยกเว้นการตรวจสอบจากอุปกรณ์ป้องกันผู้บุกรุกทางเครือข่าย (Firewall/IPS) ทำให้เป็นช่องโหว่ของการโจมตี โดยลักษณะอาการความผิดปกติของระบบที่ถูกโจมตีระดับ source code ระบบการทำงานหรือการตอบสนองจะช้า และใช้เวลาการสั่งการนานผิดปกติ จึงมีการติดตั้งอุปกรณ์ดังกล่าวจำนวน 2 เครื่อง ที่ส่วนกลางของศูนย์ข้อมูลระบบคอมพิวเตอร์ในลักษณะการทำงานแบบควบคู่กัน ซึ่ง WAF จะทำหน้าที่เรียนรู้พฤติกรรมการใช้งานปกติของ Web Application ที่ต้องการจะป้องกันก่อน แล้วเก็บรูปแบบการใช้งานปกติไว้ ซึ่งเมื่อเกิดใช้งานที่ผิดปกติหรือเกิดการพยามโจมตีระบบ อุปกรณ์จะปิดกันสื่อสารนั้นๆ เพื่อป้องกันเครื่องคอมพิวเตอร์แม่ข่ายทันที และแจ้งให้ผู้ดูแลระบบทราบเพื่อดำเนินการจัดการทางด้านนโยบายต่างๆ เพื่อความปลอดภัยของระบบ

3. การมีระบบจัดการรหัสลับ (Password Management) เพื่อให้การดูแลรักษาความปลอดภัยในการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์คอมพิวเตอร์ มีระบบบริหารจัดการผู้ใช้ที่มีการรักษาความปลอดภัยมากยิ่งขึ้น โดยระบบดังกล่าวจะทำหน้าที่ให้บริการระบบงานรวมถึงจัดเก็บข้อมูลสำคัญต่างๆ ดังนั้นผู้ที่เข้าถึงและควบคุมเครื่องแม่ข่ายได้จะต้องเป็นผู้ที่ได้รับอนุญาตอย่างถูกต้อง โดยทั่วไปการเข้าถึงและควบคุมเครื่องแม่ข่ายจะอาศัยรหัสลับเพียงชุดเดียวและไม่ค่อยเปลี่ยนแปลง ทำให้มีความเสี่ยงที่ผู้ใช้งานชั่วคราว เช่น ผู้รับจ้าง ที่ได้รับสิทธิการเข้าถึงเครื่องแม่ข่ายนั้นๆ เพียงชั่วคราว จะสามารถเข้าถึงเครื่องแม่ข่ายในภายหลังและก่อให้เกิดความเสียหายแก่เครื่องแม่ข่ายหรือข้อมูลต่างๆ ซึ่งระบบบริหารจัดการรหัสลับจะทำการเปลี่ยนรหัสลับทุกครั้งหรือเป็นกำหนดเป็นช่วงเวลาตามที่ดูแลกำหนด ทำให้รหัสลับสำหรับเข้าใช้งานเครื่องแม่ข่าย ยังคงเป็นรหัสลับที่ไม่มีผู้ใดล่วงรู้ได้ เพื่อความปลอดภัยเครื่องแม่ข่ายและความปลอดภัยของข้อมูลบนเครื่องแม่ข่าย อีกทั้งยังช่วยให้ผู้ดูแลไม่ต้องจัดเก็บรหัสลับเอง ซึ่งเสี่ยงต่อการที่รหัสลับจะสูญหายหรือรั่วไหลอีกด้วย การติดตั้งอุปกรณ์ระบบจัดการรหัสลับ ที่ศูนย์กลางระบบเครื่องแม่ข่ายเพื่อดำเนินการจัดการรหัสลับของระบบงานต่างๆ ให้มีความปลอดภัย ครบถ้วน



ปัจจุบันระบบสารสนเทศของกรุงเทพมหานคร มีความสำคัญต่อการทำงานเพื่อให้บริการประชาชนในพื้นที่กรุงเทพมหานครอย่างมาก ดังนั้นนโยบายการป้องกันภัยระบบสารสนเทศจึงต้องมีความรอบคอบและทรงประสิทธิภาพสูงสุด

ซึ่งในปีงบประมาณ 2556-255
สำนักยุทธศาสตร์และประเมินผลจะดำเนิน
การปรับปรุงและเพิ่มประสิทธิภาพระบบ
ป้องกันภัยคุกคามให้กับระบบสารสนเทศของ
กรุงเทพมหานครให้มีประสิทธิภาพในด้าน
ต่างๆ ดังนี้

1. ระบบรักษาความปลอดภัยทาง
เครือข่ายสื่อสารที่ทำงานได้โดยไม่มีช่องโหว่
ตลอดเวลา

2. ระบบรักษาความปลอดภัยระบบ
งานภายในที่ทำงานในระดับ โปรแกรม
ประยุกต์บนเครือข่ายสื่อสารมีความปลอดภัย
อย่างสูงสุด

3. สามารถลดการถูกโจมตีทาง
เครือข่ายจากผู้บุกรุกหรือภัยคุกคามประเภท
ต่างๆ และเพิ่มเสถียรภาพการทำงานของ
ระบบเครือข่ายสื่อสาร

4. สามารถช่วยให้เจ้าหน้าที่ของ
สำนักและสำนักงานเขตต่างๆ สามารถปฏิบัติ
งานได้สะดวกและรวดเร็วขึ้นจากการทำงาน
ผ่านเครือข่ายสื่อสารที่มีความปลอดภัย