นนทวรรธนะ สาระมาน
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

มาตรการสร้างศูนย์เตือนภัยทางอินเทอร์เน็ตเชิงรูปธรรม

หน้าที่ในการตรวจตราและเฝ้าระวังระบบเครือข่าย เป็นเรื่องที่ทุก ๆ องค์กรพึงเอาใส่ใจให้ความสำคัญ ด้วยมาตรการรักษาความปลอดภัยที่จริงจังและชัดเจน

เราได้กล่าวถึงการสร้างความเข้าใจถึงการสร้างศูนย์เตือนภัยทางระบบเครือข่ายมาเป็นระยะเวลาหนึ่ง เพื่อต้องการสร้างความตระหนักถึงภัยคุกคามบนระบบอินเทอร์เน็ต เราจำเป็นต้องมีศูนย์เตือนภัยทางอินเทอร์เน็ตที่สร้างขึ้นเองได้ภายในหน่วยงาน หรือสร้างเป็นงานบริการระดับผู้ให้บริการอินเทอร์เน็ต (ISP) ดังนั้นบทความต่อไปนี้จะเสนอในเชิงรูปธรรมเพื่อให้ทราบถึงขั้นตอนการสร้างศูนย์เตือนภัยและวิธีการนำไปใช้อย่างถูกต้องต่อไป

เป้าหมายในการสร้างศูนย์เตือนภัย

1. เพื่อเฝ้าระวังสิ่งผิดปกติที่เกิดขึ้นบนระบบเครือข่าย
2. เพื่อแก้ไขสถานการณ์ เพื่อลดความเสี่ยงที่เกิดจากการบุกรุกบนระบบเครือข่ายได้อย่างทันเหตุการณ์
3. เป็นการเก็บสถิติเหตุการณ์ต่าง ๆ ที่เกิดขึ้นบนระบบเครือข่าย เพื่อทำรายงานผลประจำวัน/เดือน/ปี
4. เพื่อสร้างความแข็งแรงและการปรับปรุงให้กับระบบเครือข่ายอยู่อย่างสม่ำเสมอ
5. ควบคุมและจัดการด้านการรักษาความปลอดภัยเครือข่ายได้อย่างเป็นระบบ

ส่วนประกอบของศูนย์เตือนภัย

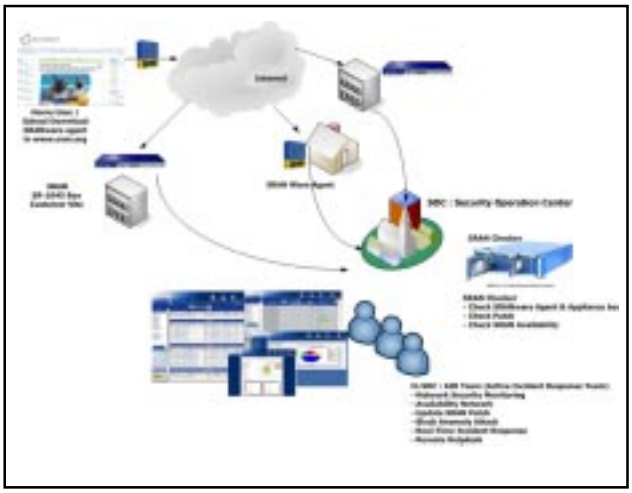
1. การออกแบบศูนย์เตือนภัยทางอินเทอร์เน็ต (Design Security Operation Center)

1.1 อุปกรณ์เพื่อการจัดการข้อมูลบนศูนย์เตือนภัย ประกอบด้วยระบบที่ใช้ในการตรวจสอบและรวบรวม log ที่เกิดขึ้นบนระบบเครือข่ายที่เรียกว่า SIM

1.2 ผู้ปฏิบัติงานในศูนย์เตือนภัย ประกอบด้วย 4 หน้าที่คือ

- นักเฝ้าระวังเครือข่าย (Network Security Monitoring Operation) ตำแหน่งวิศวกร เพื่อดูแลความเป็นระเบียบเรียบร้อยในระบบเครือข่าย หน้าที่ประจำคือประเมินความเสี่ยงระบบเครือข่าย (Security Assessment) ออกผลรายงานประจำวัน ทั้งผลการประเมินความเสี่ยงและผลการเฝ้าตรวจตราความผิดปกติระบบเครือข่าย รวมถึงการแจ้งเตือนเมื่อมีเหตุฉุกเฉิน จำนวนผู้ปฏิบัติงาน 6 คน เวลาในการปฏิบัติงาน ช่วงเช้า 8 ชั่วโมง กลางวัน 8 ชั่วโมง กลางคืนอีก 8 ชั่วโมง (เท่ากับ 24x7 ชั่วโมง)
- นักวิเคราะห์ความผิดปกติระบบเครือข่าย (Network Forensics Analysis Packets) ตำแหน่งผู้เชี่ยวชาญในการวิเคราะห์หาความผิดปกติระบบเครือข่าย รับหน้าที่ต่อจากวิศวกร เมื่อเกิดเหตุการณ์น่าสงสัยว่าจะเป็นภัยต่อระบบเครือข่าย จำนวนผู้ปฏิบัติงาน 2 คนเป็นอย่างน้อย จำเป็นต้องมีประสบการณ์ในงานด้านความปลอดภัยไม่น้อยกว่า 3 ปี
- นักกู้ระบบฉุกเฉินเมื่อเกิดเหตุผิดปกติบนระบบเครือข่าย (Incident Response Team) ตำแหน่งทีมกู้ระบบฉุกเฉิน หน้าที่ประจำคือ onsite เพื่อทำการแก้ไขปัญหาฉุกเฉินเมื่อนักวิเคราะห์ความผิดปกติระบบเครือข่ายได้แจ้งมา จำนวนผู้ปฏิบัติ 2 คนเป็นอย่างน้อย

รูปที่ 1 The Heart of The Network ของ Military Information Technology, USA



รูปที่ 2 การให้บริการในศูนย์เตือนภัยทางอินเทอร์เน็ต

● ผู้บัญชาการศูนย์เตือนภัยทางอินเทอร์เน็ต (Head Security Operation Services) หน้าที่ประจำเป็นผู้ดูแลศูนย์ รับผิดชอบและออกคำสั่งในการปฏิบัติงาน โดยดูแลเรื่อง SLA (Services Level Agreement) ที่กำหนดในการให้บริการ จำเป็นต้องเป็นผู้ที่มีประสบการณ์งานระบบเครือข่ายอย่างน้อย 7-8 ปี และควรมีประสบการณ์ด้านความปลอดภัยเครือข่ายเป็นอย่างดี

1.3 วิธีการปฏิบัติงาน

● เรียนรู้และเข้าใจถึงอุปกรณ์ในการใช้งานบนศูนย์เตือนภัยทางอินเทอร์เน็ต

● เรียนรู้ขั้นตอนการทำงานจากผู้บังคับบัญชา เพื่อกำหนดบทบาทและหน้าที่ในการปฏิบัติงาน

● ประชุมสรุปถึงปัญหาที่เกิดขึ้นเป็นระยะ ๆ

● ดูแลบำรุงรักษาอุปกรณ์ที่ใช้เฝ้าระวังภัยทางอินเทอร์เน็ต

2. การจัดหาอุปกรณ์เพื่อจัดการในศูนย์เตือนภัย

จุดที่ควรพิจารณาแบ่งเป็น 3 ส่วนคือ

2.1 อุปกรณ์บนระบบเครือข่าย

● ส่วนที่เป็นชายแดนของระบบเครือข่าย : เมื่อนับจากการให้สัญญาณอินเทอร์เน็ตเข้าสู่ระบบเครือข่ายของเรา

❑ อุปกรณ์ที่พิจารณาคืออุปกรณ์ Router

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log ที่เกิดจากอุปกรณ์ Router

● ส่วนที่เป็นการควบคุมทางออกทางเข้าของระบบเครือข่าย (Network Gateway) : คืออุปกรณ์ที่ใช้เป็นตัวกลางในการแบ่งโซนระบบเครือข่าย และทำตัวเป็นตัวกลางในการเชื่อมโยงระบบเครือข่าย

❑ อุปกรณ์ที่พิจารณาคือ Firewall หรือ Proxy

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log Firewall หรือ Proxy

● ส่วนที่เป็นระบบตรวจจับผู้บุกรุก (Intrusion Detection System) : คืออุปกรณ์ที่ใช้ในการตรวจจับสิ่งผิดปกติที่เกิดขึ้นบนระบบเครือข่าย

❑ อุปกรณ์ที่พิจารณาคือ NIDS sensor (Network Intrusion Detection System sensor)/NIPS (Network Intrusion Prevention System)

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log NIDS หรือ NIPS

2.2 บนเครื่องแม่ข่าย

● ส่วนที่เครื่องแม่ข่าย

❑ อุปกรณ์ที่พิจารณาคือ Web Server, Mail Server, Database Server เป็นต้น

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log ทั้งหมดที่เกิดขึ้นบนเครื่องแม่ข่าย

● ส่วนที่เป็นเครื่องป้องกันภัยที่เป็นคอมพิวเตอร์แม่ข่าย

❑ อุปกรณ์ที่พิจารณาคือ Anti-virus Server, Domain Controller Server และ PC Management เป็นต้น

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log ทั้งหมดที่เกิดขึ้นบนเครื่องแม่ข่าย

● เครื่องแม่ข่ายที่ใช้สำหรับประเมินความเสี่ยง (Vulnerability Server Scan)

❑ อุปกรณ์ที่พิจารณาคือโปรแกรมที่ใช้ทำการประเมินความเสี่ยงระบบ

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ ผลรายงานการประเมินความเสี่ยงระบบเครื่องแม่ข่าย/เครื่องลูกข่าย

2.3 บนเครื่องลูกข่าย

● ส่วนที่เป็นเครื่องลูกข่าย

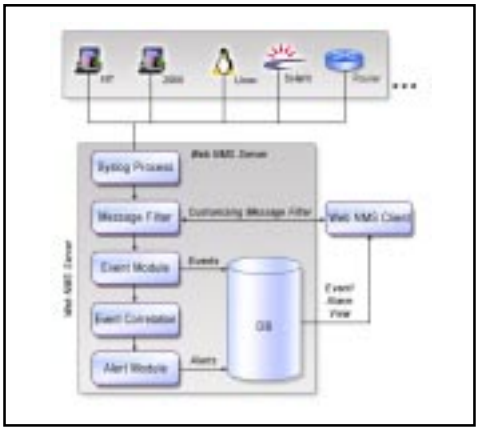
❑ อุปกรณ์ที่พิจารณาคือ HIDS (Host Base Intrusion Detection System)

❑ สิ่งที่ใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ตคือ log ที่เกิดขึ้นบน HIDS และเครื่องลูกข่าย

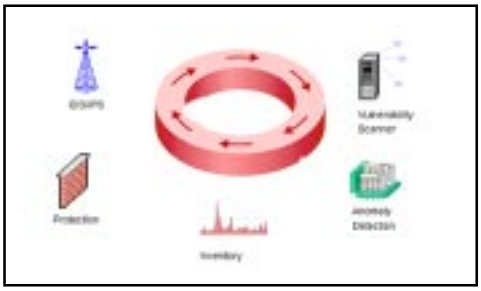
การนำ log ของอุปกรณ์เครือข่าย เครื่องแม่ข่ายและเครื่องลูกข่าย มาทำการวิเคราะห์หาสิ่งผิดปกติที่เกิดขึ้นบนระบบทั้งหมดที่เกิดขึ้นจากการใช้งานข้อมูลสารสนเทศหรือ Security Information Management เรียกง่าย ๆ ว่า SIM เป็นอุปกรณ์ที่สร้างมาเพื่อวิเคราะห์ log ที่เกิดขึ้นบนระบบเครือข่าย โดยจุดประสงค์เพื่อให้ผู้ดูแลระบบสามารถจัดการรายงานผลที่เกิดขึ้นได้จากจุดศูนย์กลาง

SIM จะจัดการรวบรวมข้อมูลที่เป็นการโจมตีที่รู้จักและไม่รู้จัก (Centralization) โดยคำนึงถึงการซ้ำกันของข้อมูลรวมเป็นข้อมูลเดียว (Normalization) และทำการแยกแยะข้อมูล (Aggregation) โดยมีค่าที่กำหนดไว้ให้เป็นชนิดใด และมีความเสี่ยงเท่าใด (Correlation)

ในรูปที่ 4 แสดงลำดับเหตุการณ์ในการทำงานของ SIM = Centralization log => Normalization => Aggregation => Correlation



รูปที่ 3 การรวบรวมข้อมูลจากเหตุการณ์ที่เกิดขึ้นบนระบบต่าง ๆ



รูปที่ 4 วัฏจักรการใช้เทคโนโลยีด้านความปลอดภัยเพื่อใช้ในศูนย์เตือนภัยทางอินเทอร์เน็ต

3. วิธีแก้ปัญหาบริการเฝ้าระวังและจัดการบนศูนย์เตือนภัยทางอินเทอร์เน็ต

ระบบความปลอดภัยทางอินเทอร์เน็ตที่จัดให้จะมีบริการเฝ้าระวังและการจัดการสำหรับระบบเครือข่ายและผู้ให้บริการ ซึ่งออกแบบโดยเฉพาะสำหรับป้องกันองค์กรจากการโจมตีทั้งจากภายในและภายนอกระบบเครือข่ายของท่าน ซึ่งเป็นส่วนแก้ปัญหาความเสียหายที่เกิดขึ้นในองค์กร บริการที่จัดให้ครอบคลุมบริการแบบ 24/7 ผู้เชี่ยวชาญการเฝ้าระวัง การจัดการ และการวิเคราะห์ระบบตามเหตุการณ์โต้ตอบปัจจุบัน และการเพิ่มของกิจกรรมที่ไม่เหมาะสมที่อาจเกิดขึ้นทำให้บริษัทมีความเสี่ยง ในการเพิ่มบริการเฝ้าระวังและแจ้งเตือนที่ศูนย์เตือนภัยรวมถึงการเข้าถึงความชำนาญด้านความปลอดภัยที่ทำได้ ช่วยฟื้นฟูระบบและทำให้ความเสี่ยงลดลงอย่างได้ผล

4. ลักษณะของบริการเฝ้าระวังและจัดการศูนย์เตือนภัยทางอินเทอร์เน็ต

ระบบความปลอดภัยทางอินเทอร์เน็ต บริการจัดการ IDS สำหรับระบบเครือข่ายและผู้ให้บริการ ครอบคลุมการแก้ไขปัญหา ออกแบบ การบำรุงรักษา และทำให้องค์กรของท่านและสภาพแวดล้อมปลอดภัย ควรประกอบด้วย

- **คืนงบประมาณ การประกันจากบุกรุก โดยใช้พื้นฐาน SLAs (Service Level Agreement)**

จัดรับประกันเวลาตอบกลับและการโต้ตอบสำหรับเหตุการณ์ความปลอดภัย พบเป้าหมายขององค์กรหรือบริการฟรี เหล่านี้เป็นการปรับปรุง SLAs การตลาดที่แตกต่างและทำให้แน่ใจทันที การแสดงและการแจ้งเมื่อมีเหตุการณ์ตรวจจับความปลอดภัยตามความเหมาะสมสำหรับแสดงตัวบุคคลและการโต้ตอบ การบำรุงรักษาความปลอดภัยที่มีประสิทธิภาพ

- **การดูแลรักษาความปลอดภัยเครือข่าย**

มีประสิทธิภาพและราคาที่ให้ประสิทธิผล กระบวนการที่พร้อมสำหรับ patch ที่ปลอดภัย ซึ่งเป็นเรื่องกว้าง ๆ ในระบบเครือข่าย โดยจะเข้าไปควบคุมสถานการณ์ ระบุชื่อความอ่อนแอและแจ้งเตือน สามารถอัพเดตโดยอัตโนมัติ ประยุกต์นโยบายการป้องกันความอ่อนแอของระบบก่อนการโจมตี ดังนั้นการตรวจจับความอ่อนแอเป็นการป้องกันที่ดีที่สุด เทคโนโลยีการแก้ปัญหาและทำการติดตั้งด้วยราคาที่คุ้มค่า ควบคุมกระบวนการที่เกิดขึ้นในระบบเครือข่ายตลอดเวลา

สนใจติดต่อสอบถามข้อมูลเพิ่มเติมได้ที่

หน่วยพัฒนาและออกแบบผลิตภัณฑ์ด้านความปลอดภัยข้อมูลสารสนเทศ
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด (มหาชน)
โทรศัพท์ 0 2982 3338-9
www.gbtech.co.th