ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

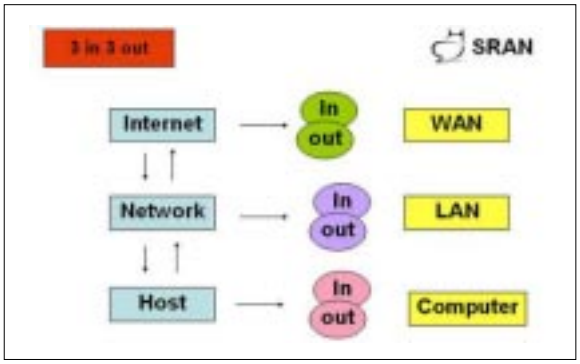
SRAN Security Center ทุกความปลอดภัย ต้องอยู่บนฐานของความถูกต้อง

นอกจากจะเป็นระบบเฝ้าระวังเครือข่ายภายในองค์กรแล้ว SRAN Security Center ยังช่วยประเมินความเสี่ยงที่เกิดขึ้น พร้อมทั้งเก็บบันทึกข้อมูล (Log Compliance Management) สรุปเป็นรายงานที่ไม่ซับซ้อน (Network Security Appliance) ทำให้องค์กรสามารถประเมินสถานการณ์ได้ถูกต้องทันท่วงที

SRAN กับการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในระบบ SRAN ได้ถูกออกแบบมาเพื่อวิเคราะห์และประเมินความเสี่ยงที่พบในระบบเครือข่าย SRAN เป็นระบบอัตโนมัติ ทุ่นแรงงานและการใช้คนมาเพื่อนั่งวิเคราะห์หาปัญหาระบบเครือข่าย อีกทั้งระบบ SRAN ได้ทำรายงานผลการเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้อีกด้วย

ลักษณะการตรวจจับข้อมูลบนระบบเครือข่าย SRAN แบ่งตามหลักการ 3 in 3 out

นั่นคือการพิจารณาถึงการเข้าและออกของข้อมูลในระบบเครือข่าย โดยระบบ SRAN จะสนใจระดับชั้น Network ที่เป็นทั้ง Core Network (ระบบเครือข่ายหลัก) ไปจนถึง Border Network (ขอบเขตการใช้ระบบเครือข่าย)



รูปที่ 1 หลักการ 3 in 3 out

คุณสมบัติของ SRAN Security Center

1. ระบบวิเคราะห์ข้อมูลบนระบบเครือข่าย (Network Analysis) โดยพิจารณาระบบการใช้ข้อมูล แบนด์วิดธ์ (Bandwidth) ที่ใช้งานทั้งที่เป็นข้อมูลขาเข้าและขาออก จากนั้นวิเคราะห์ตามโปรโตคอล (Protocol) ที่ใช้งาน ได้แก่ การตรวจสอบการใช้ HTTP (Web), SMTP (Mail), FTP, P2P และอื่น ๆ

2. ระบบตรวจจับผู้บุกรุกและป้องกันภัยคุกคามทางเครือข่ายคอมพิวเตอร์ (Intrusion Detection and Prevention) ได้แก่ การตรวจจับสิ่งผิดปกติที่เกิดขึ้นบนระบบเครือข่าย ทั้งที่เป็นภัยคุกคามจากภายนอกอินเทอร์เน็ตเข้าสู่ภายในองค์กร เรียกว่า Intrusion และภัยคุกคามจากภายในองค์กรออกสู่อินเทอร์เน็ต เรียกว่า Extrusion

3. ระบบประเมินความเสี่ยง (Network Vulnerability Assessment)

4. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Compliance) ทำการออกรายงานผลเปรียบเทียบตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์และ Log ISO 17799 โดยมีหัวข้อดังนี้

- การเก็บข้อมูลจราจรบนระบบเครือข่ายตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ เราจะสามารถมองเห็นความเคลื่อนไหวของข้อมูลบนระบบเครือข่ายได้โดยใช้ระบบ SRAN Security Center

และทำการเลือกหน้า LAW (กฎหมาย) จะปรากฏหน้าจอพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ที่แสดงถึง Log ต่าง ๆ ที่พบบนระบบเครือข่ายที่ติดตั้งระบบ SRAN

ในโครงสร้างหน้าจอนี้ประกอบด้วย 2 ส่วน คือส่วนพระราชบัญญัติและหมวดข้อมูลจราจรทางคอมพิวเตอร์ การเก็บข้อมูลจราจรทางคอมพิวเตอร์แบ่งเป็น 4 ส่วน ได้แก่

หมวด ก. คือข้อมูลที่สามารถระบุและติดตามถึงแหล่งกำเนิดต้นทางของการติดต่อสื่อสารของระบบคอมพิวเตอร์

รูปที่ 2 ภาพรวมความเสี่ยงที่เกิดขึ้นบนระบบเครือข่าย

รูปที่ 3 โครงสร้างหน้าจอ Log Compliance

รูปที่ 4 กราฟสรุปเหตุการณ์ผิดปกติในระบบเครือข่าย

รูปที่ 5 จัดจำนวนเหตุการณ์และความหมายของมาตราที่ระบบ SRAN ตรวจจับได้

หมวด ข. คือข้อมูลที่สามารถระบุปลายทางของการติดต่อสื่อสารของระบบคอมพิวเตอร์

หมวด ค. คือข้อมูลที่สามารถระบุวันที่ เวลาและระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์

และหมวดสุดท้ายคือการเก็บบันทึกข้อมูลการใช้งานอินเทอร์เน็ตภายในองค์กร

รูปที่ 4 เป็นกราฟสรุปเหตุการณ์ผิดปกติในระบบเครือข่ายที่อาจจะส่งผลกระทบตามมาตราต่าง ๆ ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จากรูปที่ 4 จะเห็นว่ามีเหตุการณ์ที่อาจจะเข้าข่ายการกระทำผิดตามมาตรา 5 อยู่ 78 %

ในรูปที่ 5 กล่าวถึงการเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือนหรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ คิดเป็น 184 เหตุการณ์ ประกอบด้วย

- การพยายามเข้าถึงระดับ User Account Admin จำนวน 1 ครั้ง
- การพยายามเข้าถึงระดับผู้ใช้ทั่วไปอยู่ 183 ครั้ง ดังแสดงในรูปที่ 6

ในหน้าการเก็บข้อมูลจราจรตามหมวดต่าง ๆ (รูปที่ 7) ระบบ SRAN ได้ประมวลผลโดยใช้เทคโนโลยี Ajax จะเป็นการประมวลผลข้อมูลจราจรที่เกิดขึ้นบนระบบเครือข่ายที่ทำการติดตั้ง SRAN แบบ Real-Time ไม่ต้องทำการ Refresh หน้าจอจากบราวเซอร์

- การเก็บ Log ของ User Authentication (รูปที่ 8) ได้แก่การระบุ IP ที่ทำการเปิดใช้งานเว็บไซต์ (www) เมื่อทำการล็อกอินเพื่อเข้าสู่ระบบ SRAN

ในรูปที่ 9 เป็นการเปิดหรือเรียกดูการใช้งานของผู้ใช้ตาม IP ที่ทำการเปิดเว็บ (www) หากเครื่องใดที่ได้มีการระบุชื่อจะปรากฏชื่อเครื่องคอมพิวเตอร์ที่ Real Name เช่น IP 192.168.1.8 ชื่อเครื่อง rokoman เป็นต้น

ในรูปที่ 10 เราสามารถตรวจดูการเปิดเว็บตามรายชื่อผู้ใช้ที่ทำการล็อกอินได้ โดยจัดอันดับของการเปิดเว็บจากการใช้ข้อมูลมากไปหาน้อย ในรูปที่ 10 จะเห็นว่า IP 192.168.1.47 เปิดเว็บ http://map.sran.net จากอัตราของการใช้งาน 6.8 M คิดเป็น 79.8% ของการเปิดเว็บไซต์ทั้งหมดของผู้ใช้ที่ใช้ IP 192.168.1.47

- การเก็บ Log เหตุการณ์ที่ผิดปกติบนระบบเครือข่ายตาม ISO 17799 นอกจาก SRAN จะเก็บข้อมูลตามพระราชบัญญัติแล้ว ยังสามารถที่จะ Compliance Log ที่เกิดขึ้นให้สอดคล้องกับ ISO 17799 ได้อีกด้วยเพื่อเป็นประโยชน์ให้กับนักตรวจสอบระบบสารสนเทศ (IT Auditor) มีความสะดวกในการทำงาน

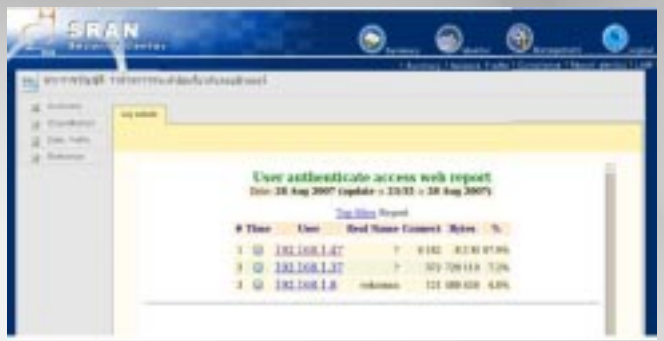
ระบบ SRAN จะทำการตรวจสอบตามหัวข้อดังต่อไปนี้

- เรื่อง Access Control Enforcement หมายถึง Log การเข้าถึงระบบต่าง ๆ

รูปที่ 6 แสดงถึงระดับการเข้าถึงระบบ

รูปที่ 7 แสดงเหตุการณ์ตามเวลาและทำการบันทึกเหตุการณ์ที่เกิดขึ้น (Data Traffic) บนตัวระบบ SRAN

รูปที่ 8 การบันทึกการเยี่ยมชมเว็บรายวันตามการใช้งานของผู้ใช้



รูปที่ 9 เรียกดูการใช้งานของผู้ใช้ตาม IP ที่ทำการเปิดเว็บ (www)

รูปที่ 10 ตรวจดูการเปิดเว็บตามรายผู้ใช้ที่ทำการล็อกอิน

รูปที่ 11 กราฟที่เกิดขึ้นจาก Log Compliance ISO 17799

รูปที่ 12 การเก็บข้อมูล (Files Archiving) ตามวัน เดือน ปี

• เรื่อง Configuration Control หมายถึง Log ที่เกิดขึ้นจากการปรับแต่งระบบ ทั้งอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ที่เกิดขึ้นบนระบบเครือข่าย

• Malicious Code Detection หมายถึง Log ที่เกิดขึ้นจากซอฟต์แวร์ไม่พึงประสงค์ ซึ่งอาจเกิดจากการใช้งานผิดปกติหรือมีการยิงข้อมูลไวรัส/หนอนคอมพิวเตอร์ รวมถึงสแปม หรือ bonnet จากภายในองค์กรไปสู่อินเทอร์เน็ต

• เรื่อง User Monitoring & Management หมายถึง Log ที่เกิดจากผู้ใช้ที่มีพฤติกรรมผิดปกติในการใช้งานหรือการกระทำการใด ๆ ที่ไม่เหมาะสม ได้แก่ การเล่นเว็บไซต์ที่ไม่เหมาะสม การเล่นแชต (Chat) รวมไปถึงการดาวน์โหลดข้อมูลที่ผิดปกติ เป็นต้น

เหตุการณ์จาก Log Compliance จะถูกเก็บเอาไว้ในตัวระบบ พร้อมที่จะสามารถเรียกดูย้อนหลังได้ตามวัน เดือน ปีที่ระบุและบันทึกไว้ (Log Archiving)

จะเห็นได้ว่าระบบ SRAN Security Center นอกจากจะเป็นระบบที่คอยเฝ้าระวังเครือข่ายภายในองค์กรและการประเมินความเสี่ยงต่าง ๆ ที่อาจเกิดขึ้นแล้ว ยังสามารถทำการเก็บบันทึกข้อมูลจราจรตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ได้อีกด้วย โดยสรุปออกมาเป็นรายงานผลในรูปแบบที่ไม่ซับซ้อนและเข้าใจง่าย ทำให้องค์กรที่ใช้ระบบ SRAN สามารถประเมินสถานการณ์ได้ว่าองค์กรของตนขาดตกบกพร่องหรือมีความเสี่ยงในมาตราใดตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์

สนใจสอบถามข้อมูลเพื่อรับบริการได้ที่

ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

โทรศัพท์ 02-982-3339
อีเมล์ info@gbtech.co.th
เว็บไซต์ www.gbtech.co.th