☐ Advertorial ทีมงาน SRAN-Dev บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

บริหารจัดการความมั่นคงข้อมูลโดยใช้ SRAN Security Center

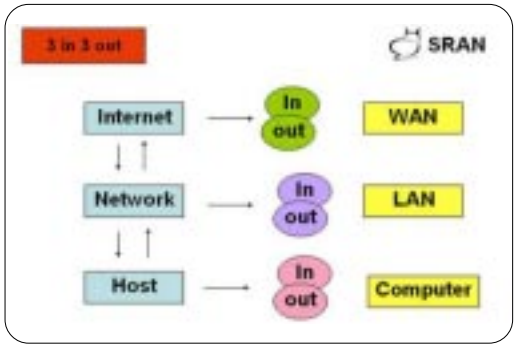
ภายใต้บริการ MSSP โดยใช้ SRAN Security Center ซึ่งคอยทำหน้าที่ออกรายงานที่มีแบบฟอร์มพร้อมใช้งาน ด้วยแผนปฏิบัติงานเพื่อบริหารจัดการข้อมูลที่ปลอดภัย วิเคราะห์ปัญหาเครือข่ายให้พร้อมที่จะปฏิบัติงานต่อไป

GLOBAL TECH
Lower Cost, More Secure

SRAN Security Center คือระบบเก็บข้อมูลจราจรทางเครือข่ายคอมพิวเตอร์ พร้อมทั้งออกรายงานการป้องกันภัยเครือข่าย การตรวจจับข้อมูลที่ผิดปกติ พร้อมทั้งประเมินความเสี่ยงระบบเครือข่ายได้ในหนึ่งเดียว หรืออาจเรียกได้ว่า SRAN Security Center คือกล่องดำ (รูปที่ 1) เพื่อบันทึกเหตุการณ์ที่เกิดขึ้นบนระบบเครือข่าย พร้อมออกรายงานผลที่เกิดขึ้นให้มีความสอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550

หลักการทำงาน SRAN Security Center เกิดจากการวิเคราะห์ระบบเครือข่ายตาม 3 in 3 out (รูปที่ 2) สามารถอ่านรายละเอียดหลักการ 3 in 3 out ได้ที่ http://blog.sran.org/archives/85 ซึ่งออกแบบมาเพื่อประหยัดการเก็บข้อมูล เป็นพื้นที่ความจุที่จำกัดได้ 4 ระบบในหนึ่งเดียว

รูปที่ 1
SRAN Security Center เป็นเสมือนกล่องดำบนเครื่องบิน



รูปที่ 2
การวิเคราะห์ระบบเครือข่ายตามแบบ 3 in 3 out

1. ระบบวิเคราะห์ระบบเครือข่าย

ระบบวิเคราะห์ระบบเครือข่าย (Network Analysis) เป็นการวิเคราะห์ขนาดการใช้งานข้อมูลจราจรบนระบบเครือข่าย (Bandwidth) ทั้งขาเข้า-ขาออก การวิเคราะห์การใช้งานตามโปรโตคอล (Protocol) ได้แก่ Web, Mail, POP3, DNS, IM, P2P และอื่น ๆ พร้อมออกรายงานแบนด์วิดธ์เป็นรายปี รายเดือน รายสัปดาห์ และรายชั่วโมงได้ (รูปที่ 3)

รูปที่ 3 ระบบวิเคราะห์ระบบเครือข่าย

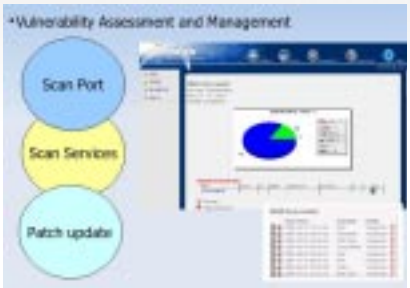
2. ระบบตรวจจับและป้องกันภัยคุกคามทางเครือข่าย

ระบบตรวจจับและป้องกันภัยคุกคามทางเครือข่าย (Intrusion Detection & Prevention System) เป็นระบบตรวจจับหรือป้องกันภัยระบบเครือข่าย ทั้งภัยคุกคามจากภายนอกเข้าสู่ระบบภายในองค์กร (Intrusion) และภัยจากภายในองค์กรเครือข่าย (Extrusion) และประมวลผลผ่านเว็บบราวเซอร์ พร้อมออกรายงานผลเป็นรายวันได้ (รูปที่ 4)

รูปที่ 4 ระบบตรวจจับและป้องกันภัยคุกคามทางเครือข่าย

3. ระบบประเมินความเสี่ยงและออกรายงานช่องโหว่ที่ค้นพบ

ระบบประเมินความเสี่ยงและออกรายงานช่องโหว่ที่ค้นพบ (Vulnerability Assessment/ Management) ระบบนี้จะทำการตรวจสอบและวิเคราะห์ความเสี่ยง โดยเริ่มจากการสแกน Port Services ทำการประเมินความเสี่ยงจากการสแกน พร้อมออกรายงาน โดยพิจารณาตามอุปกรณ์เครือข่าย (Devices) อุปกรณ์แม่ข่าย (Server) และ Application Services (รูปที่ 5)



รูปที่ 5 ระบบประเมินความเสี่ยงและออกรายงาน

4. ระบบเก็บบันทึกข้อมูลจราจรเครือข่ายเพื่อเปรียบเทียบตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550

ระบบเก็บบันทึกข้อมูลจราจรเครือข่ายเพื่อทำการเปรียบเทียบตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550 (Log Compliance) การบันทึกข้อมูลจราจรเครือข่าย (Data Traffic) ที่สามารถบันทึกได้ไม่น้อยกว่า 2 ปี โดยใช้เทคโนโลยีการบีบอัดข้อมูลแบบพิเศษ สามารถทำให้ Log files ที่เกิดขึ้นมีขนาดเล็กโดยไม่ต้องใช้สตอเรจ (Storage) ขนาดใหญ่ พร้อมทั้งทำรายงานผล Log Compliance (รูปที่ 6) ให้สอดคล้องตาม

รูปที่ 6 ระบบเก็บบันทึกข้อมูลจราจรเครือข่ายเพื่อเปรียบเทียบตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550

ISO 177999 และพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550

คุณสมบัติอุปกรณ์ SRAN Security Center โดยสรุป

1. สามารถแสดงลักษณะการใช้งานของเครือข่ายในจุดต่าง ๆ โดยมีระบบที่สามารถตรวจสอบและรวบรวมข้อมูลของสถานการณ์ต่าง ๆ ที่เกิดขึ้นในเครือข่ายแบบ Real Time
2. สามารถตรวจจับเนื้อหา รูปแบบของภัยคุกคามทางระบบเครือข่าย และแจ้งเตือนการโจมตีจากไวรัสคอมพิวเตอร์ชนิดต่าง ๆ ทางระบบเครือข่ายได้
3. สามารถตรวจจับการโจมตีจากผู้ไม่หวังดีในรูปแบบต่าง ๆ เช่น การโจมตีผ่านเครือข่ายในรูปแบบที่เรียกว่า DDoS/DoS, Spyware, Trojan และ Backdoor ได้เป็นอย่างน้อย
4. สามารถแสดงลักษณะการใช้งานระบบเครือข่ายในจุดต่าง ๆ สามารถวัดและตรวจจับ Network Performance ของระบบเครือข่ายได้ โดยสามารถแสดงผลถึงระดับข้อมูลจราจร (Data Traffic)
5. สามารถจัดลำดับความเสี่ยงที่เกิดขึ้นบนระบบเครือข่ายได้เป็นระดับสูง กลางและต่ำ พร้อมแสดงผลผ่านเว็บบราวเซอร์ (SSL)
6. สามารถออกรายงานผลย้อนหลังและสรุปความเสี่ยง ลักษณะการโจมตีระบบ รวมถึงวิธีป้องกันได้ โดยสามารถดูย้อนหลังเป็นรายวันเป็นอย่างน้อย
7. สามารถทำการแจ้งเตือนความผิดปกติของระบบผ่านอีเมล์เมื่อตรวจพบว่ามีการแพร่กระจายของไวรัสหรือหนอนคอมพิวเตอร์ (worm) ที่เกิดขึ้น
8. สามารถทำการตรวจความจุของเนื้อที่ในการประมวลผลและควบคุมด้วย (ได้) เว็บบราวเซอร์ พร้อมระบบรายงาน (Report) ในลักษณะไฟล์เอกสารหรือรูปแบบ HTML/ PDF
9. มีระบบประเมินความเสี่ยงของระบบเครือข่ายคอมพิวเตอร์ (Vulnerability Assessment) ในตัวอุปกรณ์
10. สามารถนำ Log จากการบุกรุกระบบเครือข่ายมาประมวลผลให้สอดคล้องตาม ISO17799 ได้ และออกรายงานผลที่สามารถดูย้อนหลังเป็นรายวัน

11. สามารถออกรายงานผลการตรวจจับภัยคุกคามทั้งภายในและภายนอกเครือข่ายขององค์กรให้สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ได้

บริการการจัดการความมั่นคงทางข้อมูลแบบรวมศูนย์

นอกจากนี้ยังมีบริการจัดการความมั่นคงทางข้อมูลแบบรวมศูนย์โดยใช้ SRAN Security Center (Management Security Services) หมายถึงการออกแบบ SRAN Security Center เพื่อใช้เป็นอุปกรณ์หนึ่งในศูนย์เตือนภัยทางระบบเครือข่ายหรือที่เรียกว่า SOC (Security Operation Center) เพื่อให้บริการ MSSP (Management Security Services Provider)

จุดประสงค์

การบริการจัดการความมั่นคงทางข้อมูลแบบรวมศูนย์มีจุดประสงค์เพื่อ

- ลดความซับซ้อนในการลงทุนและติดตั้งระบบเฝ้าระวังภัยทางระบบเครือข่าย
- รายงานผลสำรวจ ตรวจสอบ วิเคราะห์และประเมินความเสี่ยงอย่างเป็นระบบตามมาตรฐาน ISO 17799 และพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์
- จัดเก็บบันทึกข้อมูลจราจรบนเครือข่าย 2 ปีเป็นอย่างน้อย สามารถตรวจสอบได้จากลูกค้าที่ใช้บริการ

หลักการทำงาน

หลักการทำงานของการบริการจัดการความมั่นคงทางข้อมูลแบบรวมศูนย์ (รูปที่ 7)

- เฝ้าวิเคราะห์การใช้งานระบบเครือข่าย (Network Analysis) พร้อมออกรายงานผลรายวัน รายเดือนและรายปีตามที่ต้องการ
- เฝ้าระวังภัยคุกคามที่อาจจะเกิดขึ้นจากภายนอกระบบเครือข่าย (Intrusion Detection/Prevention) และภัยคุกคามจากภายในระบบเครือข่าย (Extrusion Detection/Prevention) พร้อมออกรายงานรายวัน
- ประเมินความเสี่ยงของระบบเครือข่ายทั้งอุปกรณ์เครือข่าย เครื่องแม่ข่าย พร้อมออกรายงาน (Vulnerability Assessment/Management) เพื่อสร้างความแข็งแรงให้ระบบเครือข่ายอย่างต่อเนื่อง
- การออกรายงานผลเพื่อให้สอดคล้องกับ ISO 17799 และพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี 2550 (Log Compliance)

วิธีปฏิบัติ Step by Step ในไซต์ลูกค้า

1. กำหนดจุดติดตั้ง SRAN Security Center โดยสังเกตจุดเชื่อมโยงระบบเครือข่าย ได้แก่ จุดเชื่อมต่อระหว่างเราเตอร์หรือสวิตช์

2. ทำการติดตั้ง SRAN Security Center ให้เหมาะสมกับรุ่น (SR110, SR 1045, SR L, SR X และ SR X2) แนะนำให้พิจารณาจากปริมาณข้อมูลที่อยู่ในเครือข่าย (Throughput) และปริมาณเครื่องคอมพิวเตอร์ภายในระบบ รูปแบบการติดตั้ง ได้แก่

- Inline วางขวางระบบ (แนะนำว่าวิธีนี้เหมาะสำหรับเครือข่ายขนาดเล็กและกลางที่มีเครือข่ายไม่เกิน 200 เครื่อง)
- Passive ติดตั้งตามอุปกรณ์สวิตช์โดยการทำ Mirror Port

3. เฝ้าระวังภัยผ่านเครือข่ายโดยใช้ SSL (HTTPS) Protocol ผ่านทางเว็บบราวเซอร์ (https://) กำหนดระดับการเข้าถึง (Login) และสิทธิการใช้งาน (แนะนำว่าควรสอบผ่านใบประกาศนียบัตรการปฏิบัติงานจากทีมงาน SRAN เสียก่อน)

เพียง 3 ขั้นตอนก็สามารถบริหารจัดการความมั่นคงทางข้อมูล (Management Security Services) ได้อย่างสะดวก ปลอดภัยและคุ้มค่าการลงทุน (รูปที่ 8)

ผลลัพธ์จากการบริหารจัดการแบบรวมศูนย์

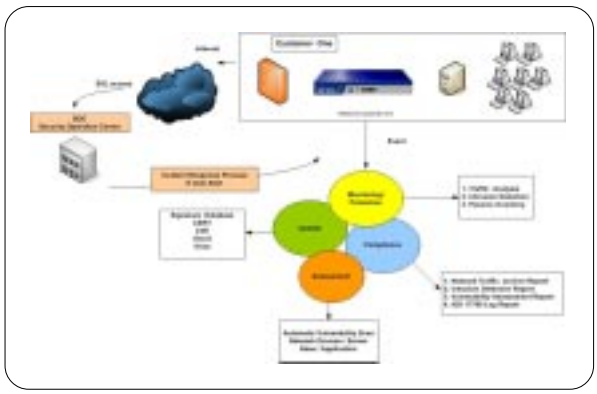
ผลลัพธ์จากการบริหารจัดการแบบรวมศูนย์โดยใช้ SRAN Security Center

1. เฝ้าติดตามและรายงานผล (รูปที่ 9)

1.1 วิเคราะห์การตรวจวัดข้อมูลการใช้งานบนระบบเครือข่ายคอมพิวเตอร์ โดยแบ่งประเภทรายงานผลดังนี้

- รายงานภาพรวมขนาดการใช้งานข้อมูลทั้งหมด (Bandwidth Report)
- รายงานผลชนิดการใช้งานตามโปรโตคอลที่มีการใช้งานภายในองค์กร (Protocol Report)
- รายงานผลลักษณะการใช้งานตามชนิดของแอพพลิเคชั่น โดยเรียงลำดับเครื่องที่ใช้ข้อมูลจากมากไปหาน้อยจำนวน 10 อันดับ (Network Traffic Report)

1.2 เฝ้าระวังภัยคุกคามที่อาจจะเกิดขึ้นบนระบบเครือข่ายคอมพิวเตอร์ (Intrusion Detection/Prevention Report) โดยแบ่งประเภทของผลการรายงานได้ดังนี้



รูปที่ 7
หลักการทำงานของบริการจัดการความมั่นคงทางข้อมูลแบบรวมศูนย์

รูปที่ 8
บริหารจัดการความมั่นคงทางข้อมูลใน 3 ขั้นตอน

• รายงานช่วงเวลาที่พบว่ามีความเสี่ยงสูงกลางหรือต่ำในแต่ละวัน

• รายงานระบบตรวจจับผู้บุกรุก ลักษณะภัยคุกคามในแต่ละวัน (อันประกอบด้วยชนิดภัยคุกคามที่เกิดจาก Virus/worm, Spyware, Trojan และ Backdoor เป็นอย่างน้อย ลักษณะการใช้งานที่ไม่เหมาะสม ได้แก่ การเปิดเว็บไม่เหมาะสม การดาวน์โหลดชนิด P2P การเล่น IM (Instant Messaging) ที่มีผลต่อภัยคุกคามภายในองค์กร การเฝ้าระวังการส่งไปรษณีย์อิเล็กทรอนิกส์ขยะ (Spam) ที่เกิดขึ้นภายในองค์กร ทั้งหมดจะเป็นการอธิบายความเสี่ยงที่เกิดเหตุการณ์จากมากไปหาน้อย 10 อันดับในแต่ละวัน

• รายงานผลของการประเมินความเสี่ยงอุปกรณ์ระบบเครือข่าย (Devices Vulnerability Assessment/Management) จากอุปกรณ์ระบบเครือข่าย ได้แก่ IDS/IPS ไม่เกิน 5 IP อุปกรณ์เราเตอร์ ไฟร์วอลล์ โดยให้มีการจัดทำรายงานผลเป็นรายเดือน

• รายงานผลการประเมินความเสี่ยงของเครื่องแม่ข่ายที่สำคัญ (Server Vulnerability Assessment/Management) เครื่องแม่ข่ายเหล่านั้นได้แก่เว็บเซิร์ฟเวอร์ เมล์เซิร์ฟเวอร์ ดาต้าเบสเซิร์ฟเวอร์ไม่เกิน 5 IP โดยจัดทำรายงานผลเป็นรายเดือน

• รายงานผลการเก็บบันทึกข้อมูลกิจกรรม (Logs) ที่เกิดขึ้นในแต่ละวัน ทำการเปรียบเทียบให้สอดคล้องกับมาตรฐาน ISO 17799 และพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์

2. การแจ้งเตือนเมื่อเกิดเหตุฉุกเฉิน (รูปที่ 10)

• ผู้ใช้บริการ SRAN MSSP จะได้รับการแจ้งเตือนโดยผ่านระบบโทรศัพท์มือถือในการติดต่อผู้ที่เกี่ยวข้องเพื่ออธิบายเหตุการณ์หากพบปัญหาที่อาจจะเกิดขึ้นในองค์กรได้ตลอด 24 ชั่วโมง

• ผู้ใช้ SRAN MSSP จะได้รับบริการสำรวจ ตรวจสอบ วิเคราะห์ และประเมินความเสี่ยงระบบเครือข่ายจากผู้เชี่ยวชาญแบบ In-House เดือนละ 1 ครั้งเพื่อประเมินสุขภาพเครือข่ายเป็นประจำทุกเดือน

รูปที่ 9 เฝ้าติดตามและรายงานผล

รูปที่ 10 การแจ้งเตือนภัยเมื่อเกิดเหตุฉุกเฉิน

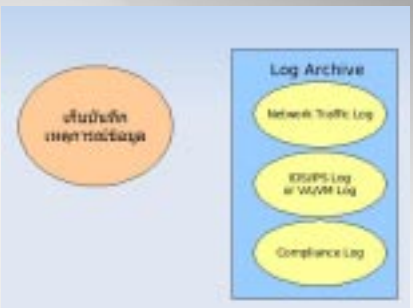
• กรณีพบเหตุการณ์ฉุกเฉินที่ไม่สามารถแก้ไขได้ทันเวลา สามารถเรียก SRAN MSSP ทำการแก้ไขและวิเคราะห์ปัญหาที่เกิดขึ้นได้แบบ On-site Services ตั้งแต่ช่วงเวลา 10:00 - 18:00 น. ในแต่ละวัน ยกเว้นวันหยุดราชการ

3. การสำรองข้อมูลบันทึกกิจกรรมเครือข่าย (Log Archive)

SRAN MSSP จะดำเนินการสำรองข้อมูล (Log Files) ดังรูปที่ 11 ประกอบด้วย

• การสำรองข้อมูลบันทึกกิจกรรมตรวจวัดลักษณะการใช้ข้อมูลเครือข่ายคอมพิวเตอร์ (Network Traffic Log Archive)

• การสำรองข้อมูลบันทึกกิจกรรมตรวจจับสิ่งผิดปกติที่เกิดขึ้นบนระบบเครือข่าย อีกทั้งผลของภัยคุกคามที่เกิดจากภายในและภายนอกองค์กร (Intrusion/Extrusion Log Archive)



รูปที่ 11 การสำรองข้อมูลบันทึกกิจกรรมเครือข่าย (Log Archive)

***** สำหรับผู้ประกอบการ ISP หรือผู้ประกอบการอื่น ๆ ที่สนใจให้บริการ MSSP โดยใช้ SRAN Security Center สามารถติดต่อได้ที่ sales@gbtech.co.th โดยทีมงาน SRAN จะอบรมการใช้งาน การออกรายงานที่มีแบบฟอร์มพร้อมใช้ แผนปฏิบัติงาน (Operation) และวิธีวิเคราะห์ปัญหาระบบเครือข่ายให้พร้อมที่จะปฏิบัติงานต่อไป**

• การสำรองข้อมูลบันทึกกิจกรรมประเมินความเสี่ยงอุปกรณ์เครือข่ายและเครื่องแม่ข่ายที่สำคัญ (Vulnerability Assessment Log Archive)

• การสำรองข้อมูลบันทึกกิจกรรมตรงตามมาตรฐาน ISO 17799 และพระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ (Compliance Log Archive) ทั้งหมดในรูปแบบซีดีรอม เป็นรายวัน รายเดือน และรายปี เพื่อสะดวกในการค้นหาข้อมูล ซึ่งหน่วยงานสามารถนำไปใช้ประโยชน์ได้อย่างครบถ้วน นอกจากนี้ยังจัดส่งให้หน่วยงานที่ใช้บริการ SRN MSSP ทุกวันที่ 10 ของทุกเดือนอีกด้วย

สนใจสอบถามข้อมูลเพื่อรับบริการได้ที่

ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด
โทรศัพท์ 02-982-3339
อีเมล์ info@gbtech.co.th
เว็บไซต์ www.gbtech.co.th

The End