SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 4 ประจำเดือน พฤษภาคม 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

หลบข่าวการเมืองร้อนๆ มาผ่อนคลายกับเนื้อหาแนวสืบสวน กับการแกะรอยหาหลักฐานออนไลน์ ตอบรับประเด็นด้าน IT Forensics ที่เริ่มเป็นที่สนใจมากขึ้นในบ้านเรา พร้อมแผนพัฒนาผลิตภัณฑ์ SRAN Security Center จากความต้องการของลูกค้าและตัวแทนจำหน่าย

ทั้งนี้ ขอขอบคุณทุกความคิดเห็นที่ส่งเข้ามา บริษัทฯ จะนำไปพัฒนาผลิตภัณฑ์และบริการให้ดียิ่งขึ้นต่อไปค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- โกลบอลเทคฯ ผนึก เน็ต ออพติคส์ เดินหน้าพัฒนาผลิตภัณฑ์ IT Security หน้า 1
- แกะรอยออนไลน์...สืบจาก LOG หน้า 2
- Message from SRAN หน้า 3
- FAQ for SRAN Secrity Center หน้า 3

โกลบอลเทคฯ ผนึก เน็ต ออพติคส์ เดินหน้าพัฒนาผลิตภัณฑ์ IT Security

นายนรัตถ์ สาระมาน (ที่ 2 จากขวา) กรรมการผู้จัดการ บริษัท โกลบอลเทคโนโลยี อินทิเกรเทด จำกัด ผู้คิดค้นและพัฒนาผลิตภัณฑ์ระบบเฝ้า ระวังภัยคุกคามเครือข่ายสารสนเทศ "SRAN" ผนึกกำลัง นายโรเบิร์ต อี ชอว์ (ที่ 2 จากซ้าย) ประธานและ ประธานเจ้าหน้าที่บริหาร บริษัท เน็ต ออฟติคส์ อิงค์ หรือ NetOptics ผู้นำระดับโลกด้านอุปกรณ์เชื่อมต่อ เครือข่ายเพื่อการมอนิเตอร์ (Network TAP and Switch Aggregation Solution) เพื่อร่วมกันวิจัยพัฒนาและจำหน่ายผลิตภัณฑ์ด้าน IT Security พร้อมกันนี้ยัง ไว้วางใจแต่งตั้ง โกลบอลเทคฯ เป็น ตัวแทนจำหน่ายผลิตภัณฑ์ NetOptics และดูแลตัวแทนจำหน่ายทั่วทั้ง ภูมิภาคเอเชียตะวันออกเฉียงใต้

Message from SRAN

จะมีอะไรใน SRAN Security Center ไตรมาส 3 ของปี 2552 ?

- Customize จำนวนวันในการเก็บ Log และ signature ได้
- ออกรายงานผลในรูปแบบ CVS file ได้
- ระบบแจ้งเตือนก่อน Partition ใน Harddisk เต็ม
- แจ้งเตือนทางอีเมล์ ก่อน MA หมดอายุ...

FAQ for SRAN Security Center

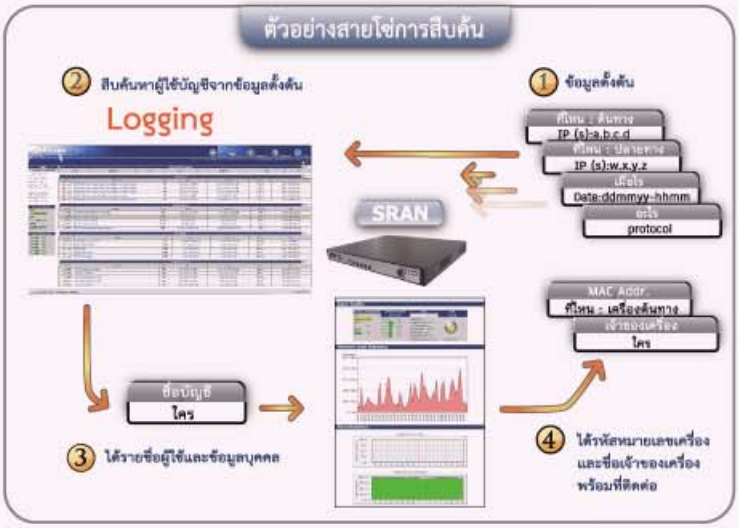
- อุปกรณ์ SRAN Security Center ไม่ทำงาน ควรทำอย่างไร ?
- ติดตั้ง SRAN แบบ Inline แล้ว ทุกเครื่องออก Internet ไม่ได้ ?

แกะรอยออนไลน์... สืบจาก LOG!

หากเครือข่ายคอมพิวเตอร์ถูกบุกรุก ข้อมูลถูกเปลี่ยนแปลงหรือสูญหาย ไม่ว่าจะเกิดจากฝีมือคนในองค์กร หรือนอกองค์กร ไม่ว่าจะทำด้วยเจตนา หรือด้วยความรู้เท่าไม่ถึงการณ์ หลักฐานสำคัญสำหรับการสืบสวนสอบสวนคือ "Log File" องค์ประกอบหนึ่งของ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งเป็นเพียงเครื่องมือช่วยในการสืบสวนสอบสวน และเป็นหลักฐานประกอบคดี ขณะที่สาระสำคัญอยู่ที่ "การสืบสวนหาตัวผู้กระทำความผิด" ...

ก่อนแกะรอยหาหลักฐานออนไลน์ เรามาทำความเข้าใจถึงที่มาของ Log กันก่อนค่ะ

แกะรอยออนไลน์...สืบจาก LOG



Log File หรือข้อมูลจราจร เกิดขึ้นจากการสื่อสารส่ง-รับ และลำเลียงข้อมูล เช่น ระหว่างคอมพิวเตอร์เครื่องหนึ่งกับเว็บไซต์หนึ่ง เมื่อกดปุ่ม Enter เรียกดูเว็บไซต์ ข้อมูลคำสั่งจากเครื่องคอมพิวเตอร์จะถูกลำเลียงผ่านอุปกรณ์เครือข่าย ไปยังผู้ให้บริการ ISP, Internet Gateway (หากเว็บนั้นอยู่ต่างประเทศ) ต่อไปยังเว็บไซต์ปลายทางประมวลผล แล้วลำเลียงข้อมูลกลับสู่ต้นทาง ระยะทางแสนไกล แต่ใช้เวลาสั้นกระชับ...และทุกที่ที่มีการลำเลียงข้อมูล จะทิ้งร่องรอยไว้เสมอ หากมีการเก็บบันทึก Log ตลอดเส้นทางลำเลียงข้อมูล และมีแฮกเกอร์ประมาทเลินเล่อ คิดเพียงลบ Log ที่ตนทำและรับรู้ อาจไม่สามารถลบได้หมดจด จึงไม่ยากนักกับการหาร่องรอยผู้กระทำความผิดในโลกดิจิตอล

ข้อมูลที่ไหลเวียนบนระบบเครือข่าย อยู่ในรูปแบบ Real-Time ไม่สามารถเรียกดูย้อนหลังได้ ทำได้เพียงวิธีเดียว คือ ดูจาก Log File ซึ่งหากให้ง่ายต่องานสืบสวนสอบสวน Log ที่บันทึกควรระบุใคร, ทำอะไร, ที่ไหน, เวลาใด และอย่างไร ตามหลักห่วงโซ่ของเหตุการณ์ (Chain of Event) สิ่งบันทึกเหล่านี้เรียกว่า "Data Archive" ซึ่งหากมีการแก้ไขข้อมูลบนห่วงโซ่ใดห่วงโซ่หนึ่ง ร่องรอยหลักฐานยังคงปรากฏอยู่บนห่วงโซ่ที่เหลือ แต่อาจส่งผลให้ข้อมูลบนห่วงโซ่คลาดเคลื่อนผิดเพี้ยน ไม่อาจสืบหาสาเหตุต้นตอ หรือเกิดกรณี "หลักฐานไม่เพียงพอ" ได้เช่นกัน ดังนั้น เพื่อให้หลักฐานเกิดความน่าเชื่อถือ จึงต้องมีการยืนยันความถูกต้องของข้อมูลที่บันทึก ว่าไม่ถูกเปลี่ยนแปลงแก้ไข เรียกว่า ทำ "Data Hashing" เป็นการยืนยันความถูกต้องของหลักฐาน นำไปประกอบคดีได้ในชั้นศาล

คดีความออนไลน์ส่วนใหญ่มักเกิดจากกรณีหมิ่นประมาท, หลอกลวงให้ผู้อื่นเสียหาย, การขโมย/ปลอมแปลงข้อมูล ซึ่งหนีไม่พ้นการใช้ Web, Mail, Chat, VoIP, Upload/Download ไฟล์ ฯลฯ มีสาเหตุจากการใช้งานด้วยพฤติกรรมไม่เหมาะสม ขาดจริยธรรม ก่อเกิดเป็นคดีความที่มีแนวโน้มเพิ่มขึ้นตามความเจริญทางเทคโนโลยีและวัตถุ ซึ่งผู้ที่เสี่ยงต่อการก่อเหตุไม่พึงประสงค์ล้วนแล้วแต่เป็น **"ผู้ใช้งาน" (User)** และส่วนใหญ่เป็นคนในองค์กร การควบคุมผู้ใช้งานอินเตอร์เน็ตทำได้หลากวิธี ไม่ยุ่งยาก แต่การควบคุมผู้ใช้งานภายในองค์กรไม่ใช่เรื่องง่ายนัก ต้องอาศัยโครงสร้างพื้นฐาน ประกอบด้วย คน เทคโนโลยี และนโยบายที่เหมาะสม ประสานการทำงานให้สอดคล้องกัน

ฉบับต่อไปจะนำเสนอหลักการวิเคราะห์หาผู้กระทำความผิดบนระบบเครือข่ายคอมพิวเตอร์ ด้วยทฤษฎี 3-in-3-out ของ SRAN โปรดติดตามค่ะ

จากความต้องการของลูกค้าและตัวแทนจำหน่าย ให้พัฒนาคุณสมบัติของ SRAN Security Center เพิ่มเติม บริษัทฯ ได้กำหนดแผนพัฒนาระยะสั้น ซึ่งคาดว่าจะแล้วเสร็จในไตรมาส 3 ของปี 2552 รายละเอียดดังนี้

Message from SRAN

- พัฒนาระบบให้ผู้ใช้งานสามารถ customize จำนวนวันในการเก็บ Log และ signature บางอย่างได้เอง เช่น การ กำหนด port proxy
- พัฒนาคุณสมบัติให้สามารถออกรายงานผลในรูปแบบ CVS file ได้
- เพิ่มระบบแจ้งเตือนก่อน Partition ใน Harddisk เต็ม
- เพิ่มระบบแจ้งเตือนทางอีเมล์ ก่อน MA หมดอายุ

นอกจากนี้ บริษัทฯ ยังมีแผนพัฒนาในไตรมาสที่ 4 อีกจำนวนหนึ่ง ซึ่งจะได้นำเสนอให้ทราบในฉบับต่อไป หากท่านใดต้องการให้ SRAN มีคุณสมบัติเพิ่มเติมด้านใด สามารถส่งอีเมล์แจ้งได้ที่ info@gbtech.co.th บริษัทฯ จะได้นำไปวางแผนพัฒนาเพื่อสนองความต้องการสูงสุดของลูกค้าต่อไป

FAQ for SRAN Security Center

Q: อุปกรณ์ SRAN Security Center ไม่ทำงาน ควรทำอย่างไร ?

A: มีแนวทางการตรวจสอบดังนี้

- **กรณีติดตั้งแบบ Inline หรือ Transparent** ให้ตรวจสอบชนิดของสายแลนที่ใช้ว่าถูกต้องหรือไม่ เช่น การต่อจากอุปกรณ์ firewall มาที่เครื่อง SRAN โดยส่วนมากควรใช้สายแลนแบบต่อไขว้ (Crossover Ethernet Cable) ไม่ใช่แบบต่อตรง (Straight-Through Ethernet Cable)
- **กรณีติดตั้งแบบ Passive** อาจเกิดจากการติดตั้งสาย LAN ไม่ถูกต้อง เช่น Mirroring หรือ SPAN Port ผิด ทำให้ดึงข้อมูลผิด Port ให้ดูวิธีการติดตั้งจากคู่มือให้ถูกต้อง หรือการส่งค่าของข้อมูลออกเพียง TX หรือ RX มาอย่างใดอย่างหนึ่งไม่ได้ หาก Proxy เป็น ISA เนื่องจากเครื่อง SRAN จะติดว่าใส่รูปแบบไม่ได้ เช่น \domain\user@pass ซึ่งยังไม่ Support การ Authen แบบนี้ แนะนำให้ Config ที่ ISA ว่าอนุญาตให้ IP เครื่อง SRAN ออกข้างนอกได้เลย หรือกรณีไม่อยากให้ออกทุก Protocol ก็แจ้งให้อนุญาต ออกไปข้างนอก Port 21, 80, 443 เป็นต้น

Q: ติดตั้ง SRAN แบบ Inline แล้ว ทุกเครื่องออก Internet ไม่ได้ ?

A: มีแนวทางการตรวจสอบดังนี้

- ให้ทำการตรวจสอบในหน้า Management -> Services -> Start/Stop Service ดูว่า Service ของ IDP ทำงานหรือไม่ ถ้าไม่ทำงานให้สั่ง Start Service
- ให้ทำการตรวจสอบหน้า Management -> Protect ว่าได้ Set ให้ block 0.0.0.0/0 จาก SourceIP หรือไม่ หากใช่ก็จะทำให้ออก Internet ไม่ได้ ให้ลบ Rule นี้ออก

ดูข้อมูล FAQ เพิ่มเติมได้ที่
http://www.gbtech.co.th/th/contacts/faq