SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 5 ประจำเดือน มิถุนายน 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จดหมายข่าวฉบับนี้ เสนอบทความเกี่ยวกับแนวคิด 3-in-3-out ของ SRAN กับการสร้างระบบความปลอดภัยข้อมูลสารสนเทศ พร้อมนำเสนอบริการ IT Security Consulting ซึ่งลูกค้า SRAN และผู้แทนจำหน่ายสามารถขอรับคำปรึกษาด้านการออกแบบและจัดทำระบบเครือข่ายสารสนเทศให้ปลอดภัยได้ฟรี ดูรายละเอียดที่ Message from SRAN ค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- แนวคิด 3-in-3-out กับความปลอดภัยข้อมูลสารสนเทศ หน้า 2-3
- Message from SRAN หน้า 1
- FAQ for SRAN Secrity Center หน้า 3

แนวคิด 3-in-3-out กับความปลอดภัยข้อมูลสารสนเทศ

การสร้างระบบรักษาความปลอดภัยบนเครือข่ายสารสนเทศอาจดูเป็นเรื่องไกลตัว ยากแก่การเข้าใจ แต่สามารถอธิบายให้เห็นภาพชัด เปรียบเทียบกับการสร้างระบบรักษาความปลอดภัยทางกายภาพสำหรับองค์กรหนึ่งๆ โดยแบ่งองค์ประกอบทางกายภาพขององค์กร และสิ่งที่จำเป็นต้องมีเพื่อรักษาความปลอดภัย

การสร้างระบบรักษาความปลอดภัยบนเครือข่ายสารสนเทศก็เช่นเดียวกัน สามารถแบ่งออกได้เป็น 3 ส่วน โดยองค์กรควรจัดหาระบบเฝ้าระวังและป้องกันภัยทั้ง 3 ส่วน...

Message from SRAN

บริษัทฯ ได้เปิดให้บริการ IT Security Consulting ครอบคลุมเนื้องานดังนี้

Network Security Design & Implementation :

ให้คำปรึกษาด้านการออกแบบและจัดทำระบบเครือข่ายองค์กรให้มีความมั่นคงปลอดภัย

Network Security Monitoring :

ให้คำปรึกษาเกี่ยวกับเทคนิค วิธีการ และนโยบายเพื่อปฏิบัติงานเฝ้าระวังภัยคุกคามทางระบบเครือข่ายคอมพิวเตอร์

Log Forensic & Analysis :

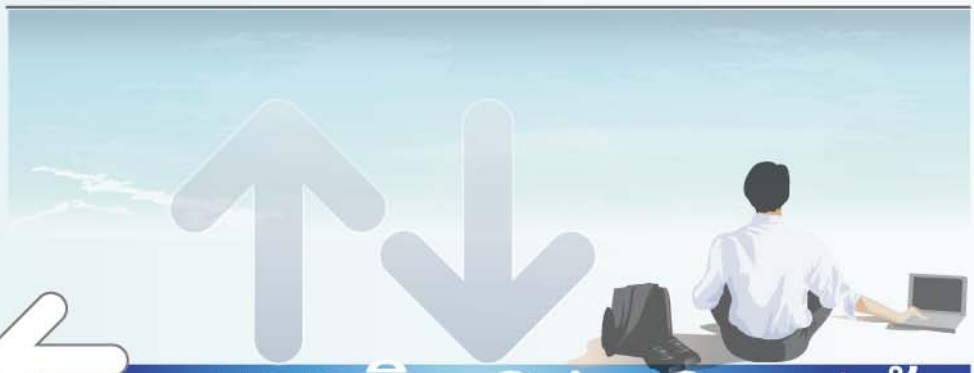
ให้คำปรึกษาเกี่ยวกับการพิสูจน์หาหลักฐานเพื่อหาผู้กระทำความผิดจาก Log ตลอดจนการวิเคราะห์ข้อมูลจาก Log File

ทั้งนี้ สำหรับลูกค้า SRAN และผู้แทนจำหน่ายทุกราย สามารถติดต่อขอรับคำปรึกษาแนะนำในเรื่องการออกแบบและจัดทำระบบเครือข่ายสารสนเทศให้ปลอดภัย **ได้ฟรี** จนถึงวันที่ 31 ธันวาคม 2552

ติดต่อที่ 02-982-5445 หรือ info@gbtech.co.th

FAQ for SRAN Security Center

- หน้าจอ LCD ไม่แสดงผล เกิดจากสาเหตุใด ?
- Hard Disk ในส่วนของ Backup Log เต็ม ส่งผลให้ SRAN หยุดเก็บ Log ทุกอย่าง ?



แนวคิด 3-in-3-out กับ ความปลอดภัยข้อมูลสารสนเทศ

องค์ประกอบทางกายภาพและสิ่งที่จำเป็นต้องมีเพื่อรักษาความปลอดภัยขององค์กร แบ่งออกเป็น 3 ส่วน คือ

	องค์ประกอบทางกายภาพขององค์กร	สิ่งที่จำเป็นต้องมีเพื่อรักษาความปลอดภัย
1	ด้านนอกอาคาร ก่อนเข้าสู่ตัวอาคาร	รั้วและประตูรั้ว ป้องกันการบุกรุกเข้าสู่ตัวอาคาร
2	ประตูเข้า-ออก ของอาคาร	ระบบ Access Control เช่น เครื่องอ่านบัตร, เครื่องสแกนลายนิ้วมือ
3	ตู้เซฟเก็บเงินสดและเอกสารสำคัญขององค์กร	รหัสตู้เซฟ เพื่อให้ผู้มีรหัสเท่านั้นที่มีสิทธิเปิดเซฟได้

หากอยากให้ระบบรักษาความปลอดภัยข้างต้นมีความปลอดภัยขึ้นอีก จะทำอย่างไร? คำตอบคือ ทำได้โดยติดตั้งกล้องทีวีวงจรปิดบริเวณรั้วหรือภายในตัวอาคาร, ติดตั้งสัญญาณกันขโมยในอาคาร, จ้างพนักงานรักษาความปลอดภัยคอยเฝ้าระวังทั้งภายในและภายนอกอาคาร ส่วนตู้เซฟอาจติดตั้งในห้องนิรภัย กำหนดให้ผู้มีอำนาจ เข้าถึงเท่านั้นที่สามารถเข้าไปในห้องดังกล่าวได้

การสร้างระบบรักษาความปลอดภัยบนเครือข่ายสารสนเทศก็เช่นเดียวกัน สามารถแบ่งออกได้เป็น 3 ส่วน โดยองค์กรควรจัดหาระบบเฝ้าระวังและป้องกันภัยทั้ง 3 ส่วน ดังนี้

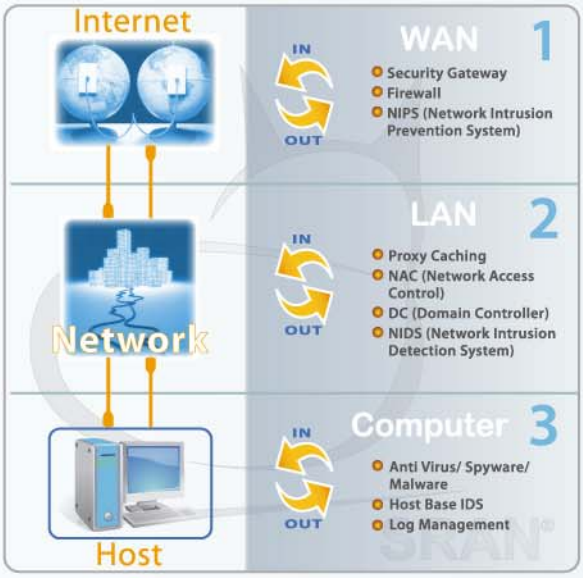
	องค์ประกอบของระบบเครือข่ายสารสนเทศ	สิ่งที่จำเป็นต้องมีเพื่อสร้างเครือข่ายให้ปลอดภัย	เป้าหมาย
1	ด่านหน้าของระบบเครือข่ายที่เชื่อมต่อกับโลกอินเตอร์เน็ต	Router ฝั่ง ISP และ Router ฝั่งองค์กรที่จะทำการใช้งานอินเตอร์เน็ต Security Gateway หรือ Firewall Network Intrusion Prevention System (NIPS)	ติดตั้งที่ระบบเครือข่าย เพื่อป้องกันผู้บุกรุกจากภายนอกองค์กร เพื่อกำหนดทิศทางการไหลเวียนข้อมูลจากฝั่งภายในองค์กรเพื่อออกสู่อินเตอร์เน็ต
2	ระบบเครือข่ายสารสนเทศขององค์กร (Local Area Network)	Proxy Caching NAC (Network Access Control) หรือ DC (Domain Controller) NIDS (Network Intrusion Detection System)	เพื่อระบุตัวตนผู้ใช้งานในองค์กร เพื่อกำหนดสิทธิในการใช้งานเครือข่าย เพื่อเฝ้าระวังการกระทำผิดหรือการกระทำที่ไม่เหมาะสมในองค์กร*
3	เครื่องคอมพิวเตอร์ (Host base)	ติดตั้ง Anti Virus/ Spyware/ Malware Host Base IDS Patch Management Log Management	เพื่อป้องกันเครื่องผู้ใช้งานให้มีความปลอดภัยในการใช้ระบบงานไอที ปรับปรุงและปิดช่องโหว่ให้ทันสมัย

* เนื่องจากการโจมตี หรือการบุกรุกระบบในปัจจุบัน มักเข้ามาทางช่องทางปกติ เช่นทาง mail, การเข้าเยี่ยมชม website ที่เป็นอันตราย ซึ่งอุปกรณ์ Firewall/ UTM อาจไม่สามารถตรวจสอบหรือปิดกั้นได้

ข้อมูลจราจรทางระบบเครือข่าย (Traffic Data) ที่วิ่งผ่านเข้า-ออก ในระบบเครือข่ายขององค์กรนั้นจะไหลเวียนอยู่ 3 ระดับ ดังแจกแจงข้างต้น สรุปเป็นแนวคิด 3-in-3-out ตามภาพ ซึ่งการเก็บบันทึกข้อมูลจราจรครบทั้ง 3 ส่วน จะช่วยให้งานสืบสวนสอบสวนง่ายขึ้น แต่หากเก็บไม่ครบถ้วนอาจได้หลักฐานไม่เพียงพอ จนไม่สามารถมัดตัวผู้กระทำความผิดได้

ในด้านการรักษาความปลอดภัยข้อมูลสารสนเทศภายในองค์กรนั้น องค์กรในที่นี้หมายรวมถึงบริษัท, สถาบัน การศึกษา, โรงแรม, โรงพยาบาล, ร้านอินเตอร์เน็ตคาเฟ่ ฯลฯ ที่มีการเชื่อมต่ออินเตอร์เน็ตหรือเชื่อมข้อมูลสู่ภายนอกองค์กร (Extranet) ต้องมีการเก็บบันทึกข้อมูลจราจร (Log File) ส่วนสถานที่ให้บริการเครือข่ายไร้สาย เช่น ร้านกาแฟ, อพาร์ตเมนท์ ฯลฯ ซึ่งเป็นสถานที่สาธารณะที่สามารถใช้ ระบบอินเตอร์เน็ตเชื่อมต่อข้อมูลได้ ก็จำเป็นต้องเก็บบันทึกข้อมูลจราจรเพื่อเป็นประโยชน์ในการสืบหา ผู้กระทำความผิด เมื่อเกิดเรื่องราวฟ้องร้องขึ้น จะได้สืบหาผู้กระทำความผิดได้สะดวกยิ่งขึ้น

แนวคิด 3-in-3-out กับ ความปลอดภัยข้อมูลสารสนเทศ



เนื่องจากปัญหาส่วนใหญ่เกิด จากผู้ใช้งาน (User) ดังนั้นการควบคุมการใช้งานของผู้ใช้งานในระบบไอทีนั้น สามารถควบคุมได้โดย

1. **ใช้เทคโนโลยีควบคุมคน** กำหนดการใช้งานผ่านระบบเครือข่าย ได้แก่

- ควบคุมการใช้งานอินเตอร์เน็ต โดยใช้ Firewall เป็นอุปกรณ์กำหนดทิศทางการใช้งาน เช่น กำหนดให้ออกเพียง port 80 การเล่นเว็บไซต์ เท่านั้น เป็นต้น
- ควบคุมสิทธิการใช้งานระบบ โดยใช้ NAC เพื่อระบุตัวตนก่อนเข้าสู่ระบบเครือข่ายในองค์กรและระบุสิทธิในการเข้าถึงข้อมูลทั้งระบบงานภายใน และการใช้งานอินเตอร์เน็ต เป็นต้น
- เฝ้าระวังภัยคุกคามและเก็บบันทึกหลักฐานการใช้งาน โดยใช้ NIDS/NIPS ในการติดตามเฝ้าระวังภัยคุกคามทั้งที่เกิดจากการใช้งานภายในองค์กรและภายนอกองค์กร พร้อมทั้งเก็บบันทึกหลักฐาน (Log File) ผ่านอุปกรณ์ Log management เพื่อให้สอดคล้องกับกฎหมาย ซึ่งกำหนดให้เก็บบันทึก Log File เพื่อประโยชน์ในการสืบหาผู้กระทำผิดไว้ไม่ น้อยกว่า 90 วัน เป็นต้น

2. **ใช้นโยบายควบคุมคน** โดยกำหนดพันธกิจ ของ องค์กรในด้านระบบรักษาความมั่นคง ปลอดภัยข้อมูลและออกกฎระเบียบเพื่อให้พนักงาน, ผู้ใช้งานระบบไอที, ต้องปฏิบัติตามกฎระเบียบนั้น ซึ่งสามารถนำมาตรฐานที่เกี่ยวข้อง มาใช้ได้ เช่น มาตรฐาน ISO27001 เป็นต้น

3. **สร้างภูมิคุ้มกันที่คน** โดยการฝึกอบรม เพื่อสร้างความตระหนักในการใช้ข้อมูลสารสนเทศอย่างถูกต้องและมีความระมัดระวังมากขึ้น

FAQ for SRAN Security Center

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

Q: หน้าจอ LCD ไม่แสดงผล เกิดจากสาเหตุใด ?

A: พิจารณาดังนี้

- หน้าจอ LCD เป็นส่วนที่แสดงผลเป็นตัวสุดท้าย ต้องใช้เวลาระยะหนึ่ง แต่หากพบว่าหน้าจอไม่แสดงผลจริงๆ ให้ทำการ restart เครื่องใหม่ หน้าจอจะกลับมาแสดงผลตามปกติ
- หน้าจอ LCD เสีย ให้สังเกตว่าไฟเข้าอุปกรณ์ตามปกติ แต่หน้าจอไม่ทำงานแม้ได้ restart เครื่องแล้ว

Q: Hard Disk ในส่วนของ Backup Log เต็มส่งผลให้ SRAN หยุดเก็บ Log ทุกอย่าง ?

A: ใน Firmware Version ใหม่ จะมีการแจ้งเตือนเมื่อมีการใช้งาน Harddisk ไป 80% แล้ว ส่งไปที่อีเมล์ของ Admin ซึ่ง Admin ควร Backup Log ไว้ก่อนทำการลบทิ้ง อย่างไรก็ตามอีเมล์ที่ส่งไปอาจเข้าไปอยู่ใน Folder Junk Mail ผู้ดูแลระบบควรหมั่นตรวจสอบ Folder นี้ และกำหนดค่าอีเมล์ที่มาจาก SRAN เป็นอีเมล์ปกติ (Not Junk) เพื่อให้อีเมล์แจ้งเตือนครั้งต่อๆ ไปส่งถึง Inbox ของผู้ดูแลระบบโดยตรง