ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

เทคโนโลยีเพื่อรองรับพ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ครบในหนึ่งเดียว "All in One Thai Cyber Law Solution"

สำหรับผู้มองหาเทคโนโลยีเพื่อรองรับพ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ปี 2550 นี่คือทางออกที่สะดวกและประหยัดงบที่ชื่อเรียกว่า "All in One Thai Cyber Law Solution" เพื่อแก้ปัญหาการติดตั้งที่ยุ่งยาก การจัดหาอุปกรณ์เก็บบันทึก และค่าซอฟต์แวร์ License

สาระสำคัญของพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ต้องการเพื่อบันทึกเหตุการณ์ที่สามารถระบุได้ว่าใครทำอะไร ที่ไหน เวลาใด อย่างไรเพื่อประโยชน์ในการสืบสวน ซึ่งเป็นไปตามหลักการที่เรียกว่า Chain of event หรือเส้นทางการลำเลียงข้อมูลตามเหตุการณ์ที่เกิดขึ้น ซึ่งเราควรจะต้องมีการรักษาหลักฐานตามเส้นทางการลำเลียงข้อมูลหรือที่เรียกว่า Chain of Custody จึงเป็นที่มาของเนื้อหาพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ในส่วนพนักงานเจ้าหน้าที่ ในส่วนผู้ให้บริการในการเก็บรักษาข้อมูลที่ว่าด้วย "มีให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ สามารถทำได้โดยการเก็บไว้ใน Centralized log server การทำ Data Archive หรือการทำ Data Hashing เป็นต้น" ก็เพื่อเป็นการรักษาหลักฐานทางข้อมูลตาม Chain of Custody ที่กล่าวมา

ในมาตราที่ 3 จึงมีการพูดถึง "ข้อมูลจราจรทางคอมพิวเตอร์ซึ่งหมายถึงข้อมูลต่าง ๆ เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ต้องสามารถระบุถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น ๆ"

ในมาตราที่ 3 นี้เองจึงจำเป็นต้องเก็บบันทึกข้อมูลจราจรที่เกิดขึ้นเพื่อใช้ในการสืบสวนสอบสวนหากเกิดเหตุการณ์ที่ไม่พึงประสงค์ และเพื่อเป็นประโยชน์สำหรับเจ้าหน้าที่พนักงานและตำรวจเพื่อใช้ในการทำคดีต่อไป

การเก็บบันทึกข้อมูลปกติ (Normal Data Traffic) และข้อมูลไม่ปกติ (Threat Data Traffic) บนระบบ SRAN สามารถเก็บบันทึกข้อมูลได้ทั้งที่เป็นแบบ Network Evidence Base และ Remote Syslog Server โดยเหตุการณ์ที่เป็นข้อมูลไม่ปกติ (Threat Data Traffic) ตัวระบบเองสามารถ

ที่จะจับเปรียบเทียบเหตุการณ์ (Correlation) ให้สอดคล้องตามมาตรฐานต่าง ๆ ได้ โดยนำ Log ที่เกิดขึ้นจากเทคโนโลยี Network Analysis ที่พิจารณาแบนด์วิดธ์ โปรโตคอล และลักษณะการบุกรุก ทั้งแบบ Intrusion และ Extrusion พร้อมทั้ง Syslog ที่ส่งมาจากอุปกรณ์เครือข่ายและเครื่องแม่ข่าย มาทำการ Correlation ให้จับเหตุการณ์ที่เกิดขึ้น แล้วทำการเปรียบเทียบให้สอดคล้องตามหมวดความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ในมาตราที่ 5 ถึง 12 ซึ่งจะมีประโยชน์สำหรับผู้ใช้งานที่สามารถประเมินความเสี่ยงจากเครือข่ายของตนเอง (Self Assessment) ว่ามีความเสี่ยงตามมาตราใดบ้าง ด้วยเหตุการณ์อะไร พร้อมทั้งระบุถึงเครื่องที่มีความเสี่ยงที่อาจเข้าข่ายตามมาตราที่ 5 ถึง 12 เพื่อทำการแก้ไขต่อไป

เรามีทางออกที่สะดวกและประหยัดงบประมาณสำหรับผู้ที่กำลังมองหาเทคโนโลยีเพื่อรองรับ พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี พ.ศ. 2550 เรียกว่า “All in One Thai Cyber Law Solution” เพื่อแก้ไขปัญหา

การติดตั้งที่ยุ่งยาก (implementation)

หากใช้ SRAN การติดตั้งให้ผลเชิงรูปธรรมจะทำได้เพียง 5 นาทีก็สามารถพร้อมใช้งานได้

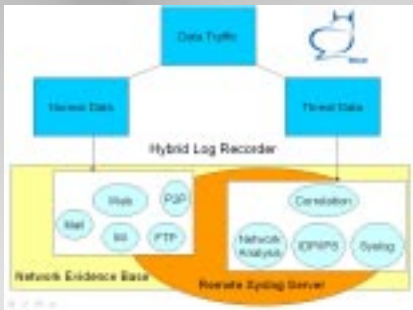
การจัดหาอุปกรณ์เก็บบันทึก (Storage)

หากใช้ SRAN ไม่ต้องใช้สตอเรจขนาดใหญ่ เนื่องจากในระบบ SRAN จะทำการจัดเทียบเหตุการณ์ที่สำคัญและเก็บบันทึกให้อย่างชาญฉลาด จะช่วยในการเก็บบันทึกได้ระดับหนึ่ง

ค่าซอฟต์แวร์ License

หากใช้ SRAN ผู้ใช้ไม่ต้องเสียค่า License ซอฟต์แวร์ในแต่ละอุปกรณ์เก็บบันทึกเหตุการณ์จราจร (Log)

ปัญหาทั้ง 3 จะหมดไปด้วยเทคนิคที่เรียกว่า “Hybrid Log Recorder” บนระบบ SRAN เราจะได้ทั้งระบบที่สามารถระบุภัยคุกคามและจับเปรียบเทียบเหตุการณ์ตามมาตราต่าง ๆ พร้อมออกรายงานผล อีกทั้งเก็บบันทึกข้อมูลจราจรได้โดย



รูปที่ 1 อธิบายถึงการพิจารณาข้อมูลจราจรบนระบบ SRAN

แบบที่ 1

การทำ Network Evidence Base จากเส้นทางลำเลียงข้อมูล ทั้งที่เป็น Full Content Data, Session Data และ Static Data ซึ่งวิธีการทำสามารถทำได้โดยการเก็บบันทึกเหตุการณ์ด้วยการ Mirror Port จากอุปกรณ์ Core Switch หรือใช้ Flow Collector ที่ดูค่า SNMP จากอุปกรณ์ ทั้ง Mirror Port และ Flow Collector เพื่อพิจารณาการรับส่งข้อมูล การจัดทำ Mirror Port โดยใช้เทคโนโลยี Deep Packets Inspection จะสามารถมองเห็นค่า Payload ที่ระบุถึงลักษณะการใช้งาน ส่วน Flow Collector ไม่สามารถระบุถึงลักษะการใช้งานได้ เพียงแค่ทราบถึงความเสถียรภาพของอุปกรณ์

แบบที่ 2

การทำ Remote Syslog จากอุปกรณ์ (Device) เข้าสู่ Syslog Server ที่ติดตั้งเพื่อใช้ในการเก็บบันทึกข้อมูล วิธีการนี้ได้ครบจาก Log แต่ละเครื่อง ทั้งที่เป็น Log OS, System และเหตุการณ์

การทำ SRAN โดยใช้เทคโนโลยี Hybrid Log Recorder คือเป็นการผสมผสานเทคโนโลยี ทั้ง Network Evidence Base และการทำ Syslog Server ในอุปกรณ์เดียวกัน

เพียงอุปกรณ์เดียว สามารถตอบโจทย์เหล่านี้ได้

Data Archive

การจัดเก็บข้อมูลจราจรไม่น้อยกว่า 90 วัน พร้อมมีการทำ Data Hashing เพื่อยืนยันว่าไม่สามารถแก้ไขข้อมูลจราจรนี้ได้

Thai Cyber Law Compliance

เฝ้าระวังภัยที่องค์กรของท่านอาจจะพบความเสี่ยงตามหมวดความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ พร้อมออกรายงานผลให้ทราบถึงเครื่องภายในองค์กรว่าเครื่องใดที่มีความเสี่ยง

ISO Compliance

ออกรายงานผลภัยคุกคามที่เกิดขึ้นภายในเครือข่าย จัดให้สอดคล้องกับ ISO 17799 หรือ ISO 27001

Easy Implementation

สะดวกในการติดตั้ง ใช้เวลาในการติดตั้งอุปกรณ์เพื่อพร้อมใช้งานเพียงไม่เกิน 5 นาที โดยไม่ต้องแก้ไขระบบเครือข่ายเดิม

Automatic Report

ออกรายงานผลได้ในตัวเอง พร้อมสามารถดูย้อนหลังตามวันเวลาที่ต้องการ

SRAN Security Center เป็นอุปกรณ์ที่มีความสามารถออกรายงานผลตาม พ.ร.บ.ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ โดยรองรับมาตราต่าง ๆ ได้ถึง 10 มาตราในอุปกรณ์เดียว นั่นคือ มาตราที่ 3 มาตราที่ 5 มาตราที่ 6 มาตราที่ 7 มาตราที่ 8 มาตราที่ 9 มาตราที่ 10 มาตราที่ 11 มาตราที่ 12 และมาตราที่ 26

ฐานความผิด	โทษจำคุก	โทษปรับ
มาตรา ๕ เข้าถึงคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๖ เดือน	ไม่เกิน ๑๐,๐๐๐ บาท
มาตรา ๖ ล่วงรู้มาตรการป้องกัน	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๗ เข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ	ไม่เกิน ๒ ปี	ไม่เกิน ๔๐,๐๐๐ บาท
มาตรา ๘ การดักข้อมูลคอมพิวเตอร์	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท
มาตรา ๙ การรบกวนข้อมูลคอมพิวเตอร์	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๐ การรบกวนระบบคอมพิวเตอร์	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๑ สแปมเมล์	ไม่มี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๒ การกระทำต่อความมั่นคง (๑) ก่อความเสียหายแก่ข้อมูลคอมพิวเตอร์ (๒) กระทบต่อความมั่นคงปลอดภัยของประเทศ/เศรษฐกิจ วรรคท้าย เป็นเหตุให้ผู้อื่นถึงแก่ชีวิต	 ไม่เกิน ๑๐ ปี ๓ ปี ถึง ๑๕ ปี ๑๐ ปี ถึง ๒๐ ปี	 +ไม่เกิน ๒๐๐,๐๐๐ บาท ๖๐,๐๐๐–๓๐๐,๐๐๐ บาท ไม่มี
มาตรา ๑๓ การจำหน่าย/เผยแพร่ชุดคำสั่ง	ไม่เกิน ๑ ปี	ไม่เกิน ๒๐,๐๐๐ บาท
มาตรา ๑๔ การเผยแพร่เนื้อหาอันไม่เหมาะสม	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๕ ความรับผิดของ ISP	ไม่เกิน ๕ ปี	ไม่เกิน ๑๐๐,๐๐๐ บาท
มาตรา ๑๖ การตัดต่อภาพผู้อื่น ถ้าสุจริต ไม่มีความผิด	ไม่เกิน ๓ ปี	ไม่เกิน ๖๐,๐๐๐ บาท

ตารางแสดงฐานความผิด รวมทั้งโทษจำคุกและโทษปรับ

การออกแบบเพื่อให้ระบบ SRAN ทำงานในส่วนของ Hybrid Log Recorder สามารถออกแบบได้ดังรูปที่ 2

หมายเลขที่ 1 จากรูปที่ 2 จะเห็นได้ว่าตัวระบบจะใช้หลักการเฝ้าสังเกตการเหตุการณ์พร้อมทำการบันทึกข้อมูลจราจรเข้าและออกบนระบบเครือข่ายตามหลัก Network Evidence Base

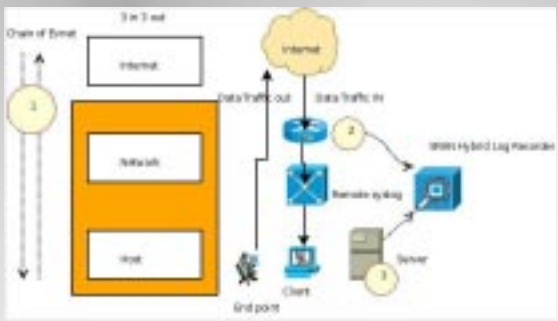
หมายเลขที่ 2 จากรูปที่ 2 จะเห็นว่าอุปกรณ์เครือข่าย Router สามารถที่จะส่งค่า syslog มาให้ตัวระบบ SRAN เพื่อทำการเก็บบันทึกข้อมูลได้

หมายเลขที่ 3 จากรูปที่ 2 จะเห็นได้ว่าเครื่องแม่ข่ายที่สำคัญ (Server) สามารถจัดส่งค่า syslog มาให้ตัวระบบ SRAN เพื่อเก็บบันทึกข้อมูลได้

กล่าวโดยสรุปคือ SRAN สามารถเก็บบันทึกข้อมูลจราจรตามหลักการรักษาเหตุการณ์ลำเลียงข้อมูลจราจร (Chain of Custody) ตามเส้นทางเดินข้อมูลเข้าและออกบนระบบเครือข่ายคอมพิวเตอร์ และสามารถเก็บบันทึกข้อมูลจากอุปกรณ์ที่สำคัญหรือเครื่องแม่ข่ายที่สำคัญเพื่อไม่ให้เก็บข้อมูลเกินความจำเป็น

ความเสี่ยงจากระดับเครื่องคอมพิวเตอร์ผู้ใช้ ซึ่งมีความเสี่ยงตาม พ.ร.บ.คอมพิวเตอร์ได้ส่วนใหญ่เป็นเหตุการณ์ที่เกิดจากการใช้งานอินเทอร์เน็ต หากเทียบกับเครือข่ายในองค์กรความเสี่ยงเหล่านี้มักจะเกิดจากเครื่องไคลเอนต์คือเครื่องที่พนักงานใช้นั่นเอง ได้แก่ การโพสต์เว็บที่มีเนื้อหาไม่เหมาะสม การส่งข้อมูลขยะ (Spam) การโจมตีระบบ (DDoS/DoS) การเข้าถึงระบบโดยมิชอบ (Hacking) ซึ่งสามารถตรวจจับเหตุการณ์ พร้อมการเก็บบันทึกข้อมูลดังกล่าวได้จากเทคนิค Network Evidence Base จะสะดวกที่สุดในการเก็บบันทึกเหตุการณ์

ส่วนข้อมูลจราจรที่เกิดจากเครื่องสำคัญ ๆ ได้แก่ Web Server, Proxy Server หรืออุปกรณ์เครือข่าย ได้แก่ เราเตอร์ ไฟร์วอลล์ หรือระบบ IDS/IPS หากต้องการเก็บให้ครบตามสมควร สามารถส่งมาเก็บบันทึกที่ Syslog Server ภายในเครือข่ายที่ปฏิบัติงานได้เช่นกัน



รูปที่ 2 หลักการทำงานของ SRAN Hybrid Recorder

ดังนั้นการทำ Hybrid Log Recorder จึงสามารถทำได้ทั้ง 2 วิธี ทั้งที่เก็บบนเครือข่ายในการใช้งานอินเทอร์เน็ต และเพื่อทำให้เก็บได้ครบถ้วนจากเครื่องแม่ข่ายซึ่งเป็นอุปกรณ์ที่สำคัญได้อีกด้วย

สรุปเทคโนโลยีที่อยู่ใน SRAN Security Center

ด้วยคุณสมบัติทางเทคโนโลยีที่เป็นมากกว่าระบบป้องกันภัยคุกคาม ยังสามารถทำงานในโหมดที่เป็นประโยชน์ต่อผู้ดูแลระบบได้อีกด้วย โดยประกอบด้วย

เทคโนโลยี Network Analysis

ทำการวิเคราะห์ข้อมูลทั้งที่เป็นข้อมูลปกติและไม่ปกติ โดยแยกส่วนการวิเคราะห์จากแบนด์วิดธ์ โปรโตคอลที่ใช้งาน โดยแยกแยะโปรโตคอลสำคัญ ๆ เช่น การใช้เว็บ การใช้เมล การใช้ FTP, P2P และการสนทนาออนไลน์

เทคโนโลยี Intrusion/Extrusion Detection

เฝ้าระวังภัยคุกคามทั้งภายในและภายนอกองค์กร พร้อมบอกลักษณะวิธีโจมตี โดยการทำ Deep Packet Inspection จึงสามารถทราบถึงลักษณะการโจมตีได้ในระดับลึก

เทคโนโลยีประเมินความเสี่ยง (Vulnerability Assessment & Management)

สามารถทราบความเสี่ยงได้จากอุปกรณ์ในเครือข่าย เครื่องแม่ข่ายที่สำคัญ รวมถึงแอพพลิเคชันเซอร์วิส

มีช่องโหว่ซึ่งพร้อมรายงานผลให้ผู้ดูแลระบบได้รับทราบ

เทคโนโลยีในการเก็บบันทึกข้อมูล (Log Archive) จะจัดเก็บบันทึกข้อมูลที่เป็นข้อมูลปกติและข้อมูลไม่ปกติตามมาตราที่ 26 มีระบบยืนยันการรับค่าข้อมูลจราจรที่ไม่สามารถแก้ไขได้ และสามารถเรียกดูย้อนหลังเหตุการณ์ (Play Back) เพื่อสืบหาผู้กระทำความผิดอันเป็นประโยชน์แก่เจ้าพนักงานในการสืบสวนสอบสวนต่อไป

เทคโนโลยีการบริหารจัดการเปรียบเทียบเหตุการณ์ให้มีความสอดคล้องกับมาตรฐานด้านความมั่นคงปลอดภัยทางข้อมูล (Log Compliance) ทำการเปรียบเทียบเหตุการณ์ตาม ISO 17799 และเปรียบเทียบเหตุการณ์ตามมาตราที่ 5 ถึง 12 พร้อมออกรายงานผลทั้งที่เป็นไฟล์ PDF และ HTML

เทคโนโลยีทั้งหมดนี้อยู่ในอุปกรณ์เดียว ประหยัดงบประมาณการลงทุน ประหยัดเวลา ลดปัญหาการติดตั้งที่ซับซ้อน มีรายงานผลเป็นรูปธรรม

เมื่อเลือก SRAN Security Center ปัญหาต่าง ๆ ที่คิดไว้จะลดลง

สนใจสอบถามข้อมูลเพื่อรับบริการได้ที่

Lower Cost, More Secure

ทีมงาน SRAN-Dev

บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

โทรศัพท์ 0 2982 3339

โทรสาร 0 2982 3338

อีเมล์ info@gbtech.co.th

เว็บไซต์ www.gbtech.co.th