ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

บริหารจัดการความมั่นคงทางข้อมูล โดยใช้ SRAN Security Center

สำนักงานตำรวจแห่งชาติเลือกใช้ SRAN Security Center บันทึกข้อมูลจราจรและเฝ้าระวังภัยคุกคามที่เกิดขึ้นบนเครือข่าย

เมื่อเดือนตุลาคมที่ผ่านมา ทางสำนักงานตำรวจแห่งชาติ โดยศูนย์เทคโนโลยีสารสนเทศกลาง สำนักงานเทคโนโลยีสารสนเทศและการสื่อสารได้ตั้ง "ศูนย์บริการข้อมูลทางอินเตอร์เน็ตสำนักงานตำรวจแห่งชาติ (Police Internet Data Center - PIDC" ขึ้น เพื่อเป็นศูนย์กลางในการแลกเปลี่ยนข้อมูลระหว่างประชาชนกับหน่วยงานในสำนักงานตำรวจแห่งชาติ หรือระหว่างหน่วยงานด้วยกันบนเครือข่ายคอมพิวเตอร์ ด้วยภาระที่สำนักงานตำรวจแห่งชาติมอบหมายให้นี้ ศูนย์เทคโนโลยีสารสนเทศกลางจึงมีความจำเป็นต้องวางแผนการดำเนินการและการป้องกันภัยคุกคามจากผู้มิหวังดี ในการนี้ได้เลือกใช้อุปกรณ์ SRAN ทั้งระบบเพื่อป้องกันภัยคุกคาม โดย Gateway Security ที่ชื่อ SRANwall รุ่น F851 และซอฟต์แวร์เฝ้าระวังภัยคุกคาม พร้อมบันทึกข้อมูลจราจรตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี พ.ศ. 2550 ที่ชื่อ SRAN Security Center รุ่น SR L

หลายคนอาจจะสงสัยว่าเมื่อเปรียบเทียบ SRAN Security Center กับระบบ SIM (Security Information Management) ในการเก็บบันทึกข้อมูลจราจร พร้อมทั้งการเปรียบเทียบเหตุการณ์เพื่อกระทำการให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ว่าเวลาติดตั้งระบบ (Implement) ระบบเก็บบันทึกข้อมูลจราจร (Log) เราต้องทำอย่างไรบ้าง

แน่นอนวิธีนี้ทุกคนต้องคิดถึงไปในทิศทางเดียวกัน คือการเก็บบันทึกข้อมูลผ่านระบบ Syslog Server และพัฒนาการต่อจาก Syslog

Server คือเป็นระบบ SIM เป็นลำดับต่อไป ไม่ว่าจะเป็นระบบ Syslog Server หรือ SIM มีลักษณะการใช้งานเหมือนกัน แต่การทำงานแตกต่างกันคือ

การใช้งาน

ทั้งคู่เป็นระบบรับข้อมูลหรือพูดภาษาง่าย ๆ ว่าเป็น "ตัวรับ" รับอะไร รับข้อมูล Log จากอุปกรณ์ เครื่องแม่ข่าย หรือแอพพลิเคชั่นต่าง ๆ แสดงว่าการรับครั้งนี้จะเกิดขึ้นก็ต่อเมื่อมีการส่งข้อมูลที่ต้องบันทึกมาที่เครื่อง Syslog หรือ SIM นั่นเอง อุปกรณ์เราเตอร์ ไฟร์วอลล์ เครื่องแม่ข่าย เว็บเซิร์ฟเวอร์ เมลเซิร์ฟเวอร์ และ IDS/IPS อื่น ๆ ต้องส่ง Log ไปที่ Syslog Server พูดง่าย ๆ ว่าต้องมี "ตัวส่ง"

ฉะนั้นการส่งนี้จะเกิดขึ้นเองไม่ได้ ต้องอาศัยคนหนึ่งคนไปกำหนดเส้นทางการส่งข้อมูล ให้ส่งข้อมูลผ่านโปรโตคอล (Protocol) Syslog หากเป็นระบบธรรมดา ๆ ก็ไม่ลำบากอะไร คือส่งผ่าน UDP 514 โดยส่งมาเป็นระยะ ๆ

หรือส่งจากการควบคุมของเซิร์ฟเวอร์ฝั่งรับ (Syslog Server) หากรับข้อมูล Log ไม่ปกติ คือส่งนอกเหนือจากแบบฟอร์ม UDP 514 ก็ต้องค้นหาจากคู่มือ (Manual) กันให้วุ่นวายแน่ครับ

สรุปว่าระบบ Syslog Server และระบบ SIM มีการใช้งานเหมือนกัน คือเป็นระบบรับข้อมูล Log จากเครื่องส่ง (อุปกรณ์เครื่องแม่ข่าย เครื่องลูกข่าย แอพพลิเคชั่น) เหมือนกัน

การทำงานและผลลัพธ์

ส่วนการทำงานและผลลัพธ์ที่เกิดขึ้นจาก Syslog Server และระบบ SIM แตกต่างกันตรงที่ว่า Syslog Server เก็บข้อมูลอย่างเดียว ส่วน SIM เก็บข้อมูลแล้วก็จะนำไปวิเคราะห์เปรียบเทียบตามมาตรฐาน (Compliance) ต่าง ๆ โดยมีรูปแบบการรวบรวมข้อมูลที่แตกต่างกันในแต่ละผลิตภัณฑ์เพื่อให้การ Compliance ได้ผลลัพธ์ตรงตามมาตรฐานนั้น ๆ (ส่วนใหญ่ผลิตภัณฑ์ที่วางจำหน่ายกันจะใช้ Compliance ตามมาตรฐาน ISO 27001, HIPAA, SOX, PCI หรืออื่น ๆ ที่เป็นสากล ไม่ได้เกี่ยวกับมาตราต่าง ๆ ในพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ของประเทศไทย (เราต้องจับประเด็นมาประมวลผลเหตุการณ์เอง)

รูปที่ 1 หน้าจอ Data Traffic Recorder

ข้อดี-ข้อเสียของระบบ Syslog Server และ SIM

ต่อไปจะขอกล่าวถึงข้อดี-ข้อเสียของระบบ Syslog Server และ SIM เริ่มจากข้อดีที่เห็นได้ชัดคือการได้รับ Log อย่างครบถ้วนละเอียดและแม่นยำกว่าวิธีอื่น ๆ และเป็นการมองภาพการใช้งานระบบไอทีทั้งองค์กรได้

ส่วนข้อเสียคือมักจะติดปัญหาเรื่องการติดตั้ง (Implement) เนื่องจากต้องคอนฟิก (Config) อุปกรณ์ (Device) ทั้งหมด หรือลงซอฟต์แวร์ในอุปกรณ์เพื่อทำการส่งค่า Log มาที่ตัวรับกลาง คือระบบ Syslog Server/SIM นั่นเอง

คำถาม : ท่านมีความคิดเห็นเกี่ยวกับภัยคุกคามสมัยใหม่ที่มากับระบบข้อมูลสารสนเทศอย่างไรคะ

คำตอบ : *ภัยคุกคามบนระบบเครือข่ายคอมพิวเตอร์นับวันจะทวีความรุนแรงมากขึ้น มีรูปแบบวิธีการซับซ้อนและแยบยลมากขึ้นเรื่อย ๆ ยิ่งกว่าในอดีต รวมไปถึงมูลค่าของความเสียหายที่เกิดจากภัยคุกคามนี้มากขึ้นเป็นทวีคูณ และมีรัศมีความเสียหายกระจายเป็นวงกว้างมากขึ้น ไม่ว่าจะเป็นภัยคุกคามที่ทำให้เกิดความเสียหายเป็นส่วนบุคคล ตัวอย่างเช่น การนำข้อมูลธุรกรรมทางธนาคารของเหยื่อไปเบิกถอนเงิน หรือเข้าไปคุกคามระบบคอมพิวเตอร์เครือข่าย แล้วนำข้อมูลความลับออกจากเครื่องคอมพิวเตอร์ส่วนตัว และที่ร้ายกว่านั้นคือภัยคุกคามที่ทำให้เกิดความเสียหายในส่วนรวม ยกตัวอย่าง*

พันตำรวจโท ดร.ณรงค์ศักดิ์ บวรวงศ์พิทักษ์
ศูนย์บริการข้อมูลทางอินเทอร์เน็ต สำนักงานตำรวจแห่งชาติ

เช่น การเข้าไปคุกคามระบบคอมพิวเตอร์เครือข่ายขององค์กรรัฐบาลหรือองค์กรสำคัญเพื่อนำข้อมูลความลับมาก่อการร้ายหรือกระทำอย่างใดอย่างหนึ่ง ทำให้เกิดความเสียหายทั้งชีวิตและทรัพย์สินเป็นจำนวนมาก ดังนั้นภาครัฐบาลและภาคเอกชนควรเน้นและให้ความสำคัญในการเฝ้าระวังภัยที่เกิดจากการคุกคามระบบข้อมูลสารสนเทศบนเครือข่ายคอมพิวเตอร์ให้มากขึ้น

คำถาม : เหตุผลที่ทางสำนักงานตำรวจแห่งชาติเลือกใช้ระบบ SRAN เพราะอะไรคะ

คำตอบ : *ก่อนอื่นต้องขอบคุณผู้บริหารของศูนย์เทคโนโลยีสารสนเทศกลางที่เห็นความสำคัญกับการให้บริการข้อมูลสารสนเทศบนเครือข่ายคอมพิวเตอร์ จึงได้มอบหมายให้ทีมงานของเราดำเนินการจัดตั้ง "ศูนย์บริการทางอินเทอร์เน็ตสำนักงานตำรวจแห่งชาติ" แน่นอนระบบป้องกันภัยคุกคามข้อมูลสารสนเทศเหล่านี้ต้องถูกออกแบบให้ทำงานคู่กับระบบหลัก เพื่อให้ทราบสาเหตุทันเหตุการณ์ เฝ้าระวังภัยที่มีการแจ้งเตือนภัยได้ พร้อมกับจัดเก็บบันทึกข้อมูล*

สมมติว่ามีอุปกรณ์อยู่ 20 ตัว ก็ต้องส่งคนไปคอนฟิกหรือลงซอฟต์แวร์ทั้ง 20 ตัวนี้ แล้วส่ง Log ออกมาให้แก่ตัวรับกลาง (Syslog Server/SIM) ถ้ามี 200 ตัว ก็ต้องทำเช่นกัน ซึ่งในโลกความเป็นจริงคนที่เข้าไปทำอย่างนั้นได้ต้องมีความรู้ในแต่ละเวอร์ชั่น ยี่ห้อ อุปกรณ์ที่จะทำการส่ง Log

ปัญหาข้อที่ 2 คือเนื้อที่ในการเก็บข้อมูลที่ต้องใช้ระบบสตอเรจ (Storage) มาใช้งานเพื่อรองรับ Log จำนวนมากจากอุปกรณ์ ซึ่งหากพูดถึงระบบสตอเรจก็จะมีค่าใช้จ่ายเพิ่มขึ้นอีก

ปัญหาข้อที่ 3 คือการออกแบบ Syslog Server/SIM หากออกแบบไม่ดีพออาจเกิดการ DDoS/DoS เข้าสู่เครื่อง Syslog Server เสียเอง เนื่องจากการส่ง Log จากอุปกรณ์จำนวนมากในแต่ละช่วงเวลาส่งที่กำหนดมา ถ้ามีการส่งเข้ามามาก ๆ ในเวลาพร้อม ๆ กัน ก็จะเกิด DDoS ขึ้นเองได้ ซึ่งทำให้ Syslog Server/SIM ใช้การไม่ได้

ปัญหาข้อที่ 4 เรื่อง License หากเป็นซอฟต์แวร์ที่ต้องติดตั้งตามเครื่องคอมพิวเตอร์แต่ละเครื่องเพื่อทำการส่ง Log ออกมา จะต้องคิดค่าใช้จ่ายเพิ่มเป็นเงาตามตัว

สรุปว่าการใช้ Syslog Server/SIM เป็นเรื่องดีทางอุดมคติ แต่ในโลกความเป็นจริงยังยากที่จะเป็นไปได้ โดยเฉพาะระบบไอทีในประเทศไทยที่ค่อนข้างมีงบประมาณจำกัดในการลงทุน

ทางทีมพัฒนา SRAN มองเห็นปัญหานี้ จึงได้พัฒนาระบบ SRAN Security Center ที่ได้รับออกแบบมาเพื่อประหยัดงบประมาณ สร้างแนวทางการเก็บ Log บนความพอเพียง ตัดปัญหาต่าง ๆ ที่พบจากการติดตั้งก็ดี การหาสตอเรจเพิ่มก็ดี การถูก DDoS/DoS กันเองก็ดี ตัดปัญหานี้ทิ้งไปได้แบบอยู่หมัดเพียงใช้อุปกรณ์ตัวเดียว

SRAN Security Center ได้ใช้เทคโนโลยี Passive Scan เก็บรวบรวมข้อมูลแบบเงียบ ๆ โดยใช้การ TAP จาก Core Switch และใช้เทคโนโลยี IDS/IPS และ Network Analysis มาใช้ในการเปรียบเทียบเหตุการณ์ภัยคุกคาม (Correlation Log)

ส่วนข้อมูลการใช้งานปกติเราก็ทำการเก็บบันทึกให้ด้วย เช่น การเก็บบันทึกการใช้เว็บ การรับส่งเมล การสนทนาอื่น ๆ อย่างครบถ้วน โดยการทำ Filtering เฉพาะเรื่องที่กฎหมายไทยให้เก็บบันทึก ไม่ได้เอาข้อมูลทั้งหมด จึงทำให้เกิดผลดีดังนี้

รูปที่ 2 หน้าจอ SRAN Security Center ในการเก็บบันทึกข้อมูลจราจร

ที่สามารถสืบหาหลักฐานทางอิเล็กทรอนิกส์ได้ จึงเป็นเหตุผลหนึ่งที่เลือกใช้ SRAN ส่วนอีกเหตุผลหนึ่งคือให้โอกาสผลิตภัณฑ์ที่พัฒนาขึ้นโดยฝีมือคนไทย โดยส่วนตัวแล้วเชื่อว่าคนไทยสามารถพัฒนาให้มีความสามารถใกล้เคียงกับต่างประเทศได้ เราควรส่งเสริมและให้โอกาสเพื่อให้คนรุ่นใหม่ที่มีความกล้าและความคิดสร้างสรรค์กล้าทำสิ่งดี ๆ ได้ในอนาคต และต้องพยายามลดความคิดค่านิยมของคนในชาติที่ยังเชื่อว่าสินค้าจากต่างประเทศดีกว่าของคนไทย เท่าที่ศูนย์บริการข้อมูลทางอินเทอร์เน็ต สำนักงานตำรวจแห่งชาติใช้อยู่ก็ไม่มีปัญหาอะไร อีกทั้งทีมงานเจ้าหน้าที่หลังการขายสามารถแก้ไขปัญหาได้ทันและตรงจุด ทำให้เรามั่นใจว่าการใช้ SRAN สามารถช่วยเหลือทางตำรวจได้

คำถาม : ตอนนี้ที่สำนักงานตำรวจแห่งชาติใช้อยู่คุณสมบัติหนึ่งของ SRAN คือเก็บบันทึกข้อมูลจราจรและรวบรวมเหตุการณ์ที่เป็นภัยคุกคาม แล้วนำมาเปรียบเทียบตามมาตราต่าง ๆ ในพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ทางสำนักงานตำรวจแห่งชาติใช้แล้วมีความคิดเห็นอย่างไรคะ

คำตอบ : *ถือว่าเป็นสิ่งที่ดี ทางศูนย์บริการข้อมูลทางอินเทอร์เน็ตต้องการทราบข้อมูลการติดต่อและรวบรวมที่เป็นภัยคุกคามในระบบของเราอย่างต่อเนื่อง อีกทั้งการจัดเก็บบันทึกข้อมูลระบบนี้ไม่ต้องใช้อุปกรณ์ (Storage) ขนาดใหญ่ แต่มีการจัดเก็บข้อมูลเพียงบางส่วนเท่านั้น เพื่อใช้ในการสืบสวนหาผู้กระทำผิดจริง ๆ ทำให้ไม่เปลืองค่าใช้จ่าย การติดตั้งระบบไม่ซับซ้อน ข้อดีอีกประการหนึ่งคือการจัดเก็บข้อมูลเกี่ยวกับเหตุการณ์ที่เป็นภัยคุกคามซึ่งเปรียบเทียบตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์นั้นถือเป็นการพัฒนาซอฟต์แวร์ให้ทันสถานการณ์สอดคล้องกับความเป็นจริง ตรงกับวัฒนธรรมและกฎหมายในประเทศเอง ซึ่งผลิตภัณฑ์จากต่างประเทศคงทำได้ยาก การพัฒนาของ SRAN จึงตอบสนองได้เร็ว*

ในอนาคตบทบาทและหน้าที่ของศูนย์บริการข้อมูลทางคอมพิวเตอร์ สำนักงานตำรวจแห่งชาติต้องรองรับโครงการต่าง ๆ บนเครือข่ายคอมพิวเตอร์ของหน่วยงานในสำนักงานตำรวจแห่งชาติ ตัวอย่างเช่น โครงการแจ้งเบาะแสของประชาชนหรือโครงการตรวจสอบหมายจับของเจ้าหน้าที่ตำรวจ เป็นต้น ซึ่งล้วนแต่เป็นข้อมูลความลับทั้งสิ้น แต่ผมยังมั่นใจ SRAN ในระบบการป้องกันภัยคุกคาม และต้องการให้ SRAN พัฒนาผลิตภัณฑ์ให้มีประสิทธิภาพและความสามารถมาก ๆ เพื่อจะได้ส่งไปขายยังต่างประเทศ สร้างชื่อเสียงกลับสู่ประเทศไทยของเราให้จงได้...

1. การติดตั้งง่าย เพียงเสียบสาย LAN กับตัว Core Switch ทำการเปิดเครื่อง รอ Passive ข้อมูลเข้าเครื่อง SRAN จึงทำให้การติดตั้งระบบ SRAN ไม่มีความจำเป็นต้องใช้ผู้เชี่ยวชาญที่ต้องรู้จักอุปกรณ์ทุกตัว

2. ตัดปัญหาเรื่องเนื้อที่เก็บข้อมูลและการใช้สตอเรจ เนื่องจากระบบจะกรอง (Filter) เฉพาะส่วนที่ทางกฎหมายบังคับให้เก็บและเพิ่มวิธีการบีบอัดข้อมูลพิเศษ จึงทำให้ไม่ต้องการเนื้อที่ความจำเป็นจำนวนมากอีกต่อไป เพียงใช้ฮาร์ดดิสก์ในการจัดเก็บมากกว่า 80 กิกะไบต์ ก็สามารถเก็บ Log ทั้งหมดที่เกิดขึ้นบนเครือข่ายผ่านตัวระบบนี้ได้ไม่นานกว่า 1 ปีตามกฎหมายบังคับ เนื่องจาก Log ในแต่ละวันที่พบในเครื่อง SRAN เมื่อผ่านการบีบอัดแล้วจะเหลือเพียง 500 กิโลไบต์ - 5 เมกะไบต์ ขึ้นอยู่กับขนาดของไซต์ที่ติดตั้ง (500 กิโลไบต์ - 5 เมกะไบต์ x 365 ก็ตกแค่ปีละไม่ถึง 50 กิกะไบต์อีกด้วย)

3. Log ที่เกิดขึ้นไม่สามารถแก้ไขได้ในตัวระบบ เพราะการสร้างค่า Check SUM เพื่อเป็นการยืนยันความไม่เปลี่ยนแปลงของข้อมูลใน Log นั้น อีกทั้งระบบจัดหน้าควบคุมเป็นแบบปฏิทิน ซึ่งสามารถดู Log ย้อนหลังแบบ Replay ดึงเหตุการณ์ในวันที่กำหนดมาเปิดดูได้โดยไม่ต้องใช้ซอฟต์แวร์อื่นช่วย

รูปที่ 3 เปรียบเทียบความเสี่ยงในมาตราต่าง ๆ ตาม พ.ร.บ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์

4. Log ที่เกิดขึ้นนอกจากบันทึกตามพระราชบัญญัติที่ให้เก็บทั้งการใช้เว็บ เมล การสนทนาอื่น ๆ แล้ว ระบบ SRAN Security Center ยังได้ทำการรวบรวมข้อมูลและนำมาทำการเปรียบเทียบตามมาตราต่าง ๆ เพื่อเป็นการป้องกันตนเองก่อนที่จะเกิดความเสียหาย โดยออกรายงานผลความเสี่ยงเองอัตโนมัติ

รูปที่ 2 เป็นหน้าจอ SRAN Security Center ในการเก็บบันทึกข้อมูลจราจร ประกอบด้วยการเล่นเว็บ เมล การสนทนาออนไลน์ การใช้ FTP และ VoIP ในส่วน P2P

เท่านี้ก็อยู่ครบถ้วนทั้งเทคโนโลยีและลดความซับซ้อน รวมถึงประหยัดงบประมาณในการลงทุน IT Security ให้สอดคล้องตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์อีกด้วย

ในรูปที่ 3 เป็นหน้าจอ SRAN Security Center ในส่วนเปรียบเทียบความเสี่ยงในมาตราต่าง ๆ ตามพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ ปี พ.ศ. 2550

ตัวอย่างนี้เป็นอีกหนึ่งความมั่นใจที่ใช้เทคโนโลยี SRAN ในการเก็บบันทึกข้อมูลจราจรที่สำนักงานตำรวจแห่งชาติเลือกใช้ระบบ SRAN

สนใจสอบถามข้อมูลเพื่อรับบริการได้ที่

GLOBAL TECH
Lower Cost, More Secure

ทีมงาน SRAN-Dev

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

The End