□ ทีมงาน SRAN-Dev
บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด

โกลบอลเทคเปิดตัว ผลิตภัณฑ์และบริการใหม่ เพื่อเครือข่ายที่ปลอดภัยภายใต้การดูแลของมืออาชีพ

ผลิตภัณฑ์ใหม่ –SRAN Light : IT Security New Generation
บริการใหม่ – บริการตรวจประเมินและออกรายงานการผ่านมาตรฐาน PCI DSS และให้คำปรึกษาในการตรวจรับรองมาตรฐาน ISO27001

SRAN Light - IT Security New Generation

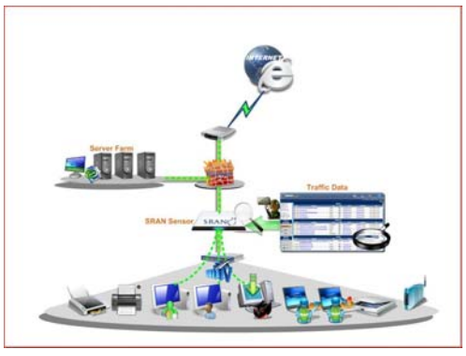
ปัญหาด้านความปลอดภัยข้อมูลสารสนเทศ จากเดิมที่องค์กรเสี่ยงต่อการถูกโจมตีจากภายนอก เช่น ไวรัส มัลแวร์ แฮกเกอร์ ปัจจุบันแนวโน้มเปลี่ยนไป เน้นเรื่องความปลอดภัยของข้อมูลในองค์กรมากขึ้น **เพราะการโจมตีเปลี่ยนรูปแบบไปสู่ภัยคุกคามจากพนักงานภายในองค์กร (Insider Threat) ทั้งตั้งใจและไม่ตั้งใจ โดยมีสถิติเพิ่มสูงขึ้น** ทั้งการโจรกรรมข้อมูล การฉ้อโกงภายในองค์กร การแพร่ไวรัส/มัลแวร์จากเครื่องโน้ตบุ๊กตัวเองไปยังเครื่องอื่นๆ ในองค์กร เป็นต้น

SRAN จึงได้พัฒนา "SRAN Light" ขึ้นเพื่อฉายภาพพฤติกรรมการใช้งานไอทีภายในองค์กร รวมทั้งภัยคุกคามต่างๆ ให้เห็นเด่นชัด เชื่อมงาน IT Security เข้ากับงานบริหารทรัพยากรบุคคล เสมือนมีกล้องวงจรปิดในเครือข่ายสารสนเทศที่บันทึกการใช้งานได้อย่างครบถ้วน และสะดวกต่อการตรวจสอบพฤติกรรมการใช้งานโดยไม่ละเมิดสิทธิส่วนบุคคลตามนโยบายของแต่ละองค์กร

ด้วยเทคโนโลยี "HBW" หรือ Human Behavioral Warning ของ SRAN Light ที่ได้นำเทคนิค Intrusion Detection System ในระดับ Network Base มาผนวกเข้ากับการจัดเก็บคลังข้อมูล (Inventory) จึงสามารถตรวจจับรายชื่อพนักงาน ชื่อหน่วยงาน ค่า MAC Address แล้วนำมาเชื่อมโยงกับ IP Address (ทั้งแบบ Dynamic และ Static IP) ได้

ลักษณะการตรวจวิเคราะห์ Application Protocol ที่ SRAN Light สามารถเก็บบันทึกได้แบ่งเป็น 2 ส่วนคือ (ดูรูปที่ 1)

- ข้อมูลที่เกิดจากการใช้งานปกติ (Normal Traffic) ได้แก่ Web, Email, Messenger, File Transfer, P2P และอื่นๆ เช่น Telnet, Remote Desktop, VNC, Radius เป็นต้น
- ข้อมูลที่เกิดจากการใช้งานที่ไม่ปกติ (Threat Traffic) ได้แก่
  - ลักษณะการแพร่กระจายสิ่งผิดปกติ เช่น Virus/Worm, Backdoor, Trojan, Malware, Botnet
  - ลักษณะการโจมตีชนิดต่างๆ เช่น DDoS/DoS, Brute force password, Buffer overflow
  - ลักษณะความผิดปกติจากการรับ-ส่งข้อมูล เช่น Spam, Phishing อุปกรณ์เครือข่ายที่ปล่อยสัญญาณผิดปกติจากโปรโตคอล ICMP, SNMP เป็นต้น



รูปที่ 1

- ลักษณะการปลอมแปลงข้อมูล เช่น การ Spoof ค่า MAC โดยใช้เทคนิค ARP-spoof, การ Spoof ค่า DNS เป็นต้น

คุณสมบัติเด่นของ SRAN Light

รายละเอียดเกี่ยวกับคุณสมบัติเด่นของ SRAN Light ได้แก่ (ดูรูปที่ 2)

1. ตรวจจับและเฝ้าระวังภัยคุกคามทางเครือข่ายด้วยเทคโนโลยี NIDS/IPS ช่วยปกป้องเครือข่ายจากภัยคุกคามทั้งจากภายนอกสู่องค์กร (Intrusion) และภัยคุกคามจากภายในเครือข่ายออกสู่ภายนอก (Extrusion) การประมวลผลโดยผ่านทางเว็บบราวเซอร์ พร้อมออกรายงานผลเป็นรายวัน โดยจัดลำดับความเสี่ยงเป็นสูง กลาง ต่ำ

2. เก็บบันทึก Log File และเปรียบเทียบให้สอดคล้องกับ พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ดังนี้

- ระบุตัวตนผู้ใช้งาน ช่วยให้ทราบพฤติกรรมการใช้ข้อมูลบนระบบไอทีในองค์กร โดยสามารถพิสูจน์ว่าใคร (who) ทำอะไร (what) ที่ไหน (where) เมื่อใด (when) อย่างไร (why/how) ได้อย่างครบถ้วน
- สามารถแยกแยะภัยคุกคามที่เกิดขึ้นในองค์กร พร้อมทั้งนำเสนอวิธีการแก้ไข
- จัดทำสถิติการใช้ข้อมูลทั่วไป เพื่อเก็บบันทึกตามหลักเกณฑ์การเก็บบันทึกข้อมูลจราจร

3. ช่วยให้สามารถทราบถึงพฤติกรรมการใช้งานไอทีภายในองค์กร โดยเชื่อมโยง IP Address และ MAC Address เข้ากับข้อมูลรายชื่อพนักงาน สามารถเพิ่มรูปพนักงานเข้าไปในระบบได้ พร้อมเก็บประวัติการใช้งาน

4. สามารถจัดเก็บค่า Inventory แบบ Passive ทางระบบเครือข่าย ประกอบด้วยข้อมูลดังนี้

- รายชื่อพนักงานบริษัท (Name)
- ชื่อแผนก (Department)

รูปที่ 2

- ชื่อระบบปฏิบัติการของพนักงาน (Operating System)
- ค่า IP Address และ MAC Address ของแต่ละเครื่องภายในองค์กร

5. รายงานผลการใช้ข้อมูลสารสนเทศเป็นรายแผนก รายบุคคล และภาพรวมของบริษัทได้ในรูปแบบไฟล์ CSV, HTML ทั้งยังสามารถออกรายงานผลเพื่อเชื่อมโยงกับระบบอุปกรณ์ประเภทมือถือได้ผ่านช่องทาง XML

6. เฝ้าระวังพฤติกรรมการใช้งานโดยสามารถกำหนด Rule Policy ตามนโยบายองค์กรเพื่อป้องกันการละเมิดสิทธิส่วนบุคคลของพนักงานในองค์กร

บริการตรวจประเมินและออกรายงานการผ่านมาตรฐาน PCI DSS

มาตรฐาน PCI DSS หรือ Payment Card Industry Data Security Standard เป็นมาตรฐานความปลอดภัยสารสนเทศที่แพร่หลายทั่วโลก รวบรวมโดยคณะกรรมการ Payment Card

ตารางที่ 1 ข้อกำหนด PCI DSS

วัตถุประสงค์ที่ควบคุม	ข้อกำหนด PCI DSS
สร้างเครือข่ายที่ปลอดภัยและบำรุงรักษาไว้	1. ติดตั้งและดูแลรักษาค่าที่ตั้งไว้ของไฟร์วอลล์เพื่อปกป้องข้อมูลของผู้ถือบัตร 2. ไม่ใช้ค่าที่ตั้งมาพร้อมกับผลิตภัณฑ์สำหรับรหัสผ่านและการรักษาความปลอดภัยอื่นๆ ของระบบ
ปกป้องข้อมูลผู้ถือบัตร	3. ปกป้องข้อมูลของผู้ถือบัตรที่ได้เก็บรักษาไว้ 4. เข้ารหัสข้อมูลผู้ถือบัตรก่อนส่งผ่านเครือข่ายสาธารณะแบบเปิด
บำรุงรักษาโปรแกรมที่ใช้จัดการกับช่องโหว่	5. ใช้โปรแกรมแอนตี้ไวรัสและอัพเดตสม่ำเสมอสำหรับทุกระบบที่มักได้รับผลกระทบจากมัลแวร์ 6. พัฒนาและดูแลรักษาระบบและแอพพลิเคชั่นต่างๆ ให้ปลอดภัย
ใช้มาตรการที่รัดกุมในการควบคุมการเข้าถึง	7. จำกัดการเข้าถึงข้อมูลผู้ถือบัตร เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น 8. กำหนดหมายเลขประจำตัวเฉพาะ (Unique ID) ให้กับผู้ที่สามารถเข้าถึงคอมพิวเตอร์ได้ 9. จำกัดการเข้าถึงทางกายภาพสำหรับข้อมูลผู้ถือบัตร
ตรวจตราและทดสอบเครือข่ายต่างๆ อย่างสม่ำเสมอ	10. ติดตามและเฝ้าดูการเข้าถึงทรัพยากรทางเครือข่ายและข้อมูลผู้ถือบัตร 11. ทดสอบระบบและขั้นตอนต่างๆ ในการรักษาความปลอดภัยอย่างสม่ำเสมอ
คงไว้ซึ่งนโยบายความปลอดภัยสารสนเทศ	12. คงไว้ซึ่งนโยบายด้านการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

Industry Security Standards Council (PCI SSC) มาตรฐานดังกล่าวถูกกำหนดขึ้นเพื่อช่วยให้องค์กรต่างๆ ที่มีการรับชำระเงินด้วยบัตรเครดิตสามารถป้องกันการฉ้อโกงบัตรเครดิต โดยควบคุมข้อมูลและช่องโหว่ต่างๆ ให้เข้มงวดมากยิ่งขึ้น และได้นำไปใช้กับทุกองค์กรที่เก็บรักษา ประมวลผล หรือรับส่งข้อมูลของผู้ถือบัตรอิเล็กทรอนิกส์ ทั้งในรูปของบัตรเครดิต บัตรเดบิต บัตรเติมเงิน ตารางที่ 1 เป็นข้อกำหนด PCI DSS ที่ยึดถือปฏิบัติกันทั่วไป

ทั้งนี้ ผู้ที่เข้าข่ายต้องปฏิบัติให้สอดคล้องกับมาตรฐาน PCI DSS มิได้จำกัดแค่เพียงสถาบันการเงินเท่านั้น แต่ยังจำแนกออกเป็น 2 กลุ่มใหญ่ๆ ดังนี้

1. กลุ่มผู้จำหน่ายสินค้า/บริการ (Merchant) ที่รับชำระเงินค่าสินค้าและบริการด้วยบัตรเครดิต เช่น

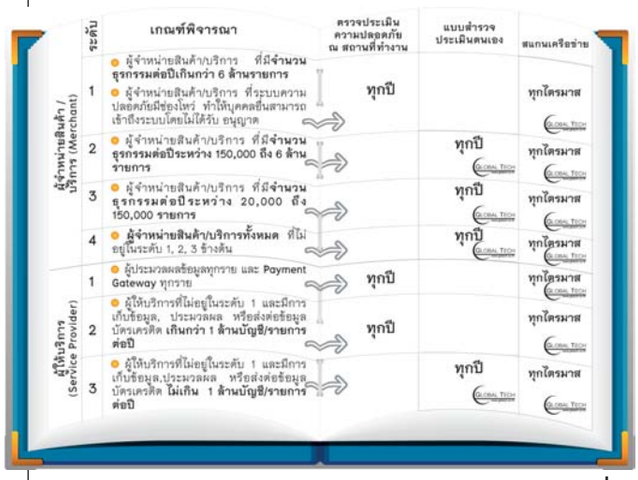
- เว็บไซต์ขายสินค้า เช่น amazon.com
- ร้านค้าปลีก เช่น ห้างสรรพสินค้าต่างๆ บรรดา Discount Store เป็นต้น
- สถาบันการศึกษา
- โรงพยาบาล
- โรงแรม ร้านอาหาร
- ปั๊มน้ำมัน

2. กลุ่มผู้ให้บริการ (Service Provider) คือองค์กรที่ประมวลผล เก็บข้อมูล และส่งต่อข้อมูลของผู้ถือบัตรเครดิตแทนตัวผู้ถือบัตรเอง หรือผู้จำหน่ายสินค้า/บริการ (ตามข้อแรก) รวมทั้งผู้ให้บริการรายอื่นๆ ได้แก่ ธนาคาร พาณิชย์ต่างๆ พวก Payment Gateway, e-Commerce Host Provider, Credit Reporting Agency เป็นต้น

เนื่องจากมาตรฐาน PCI DSS ส่งผลกระทบต่อเครือข่ายและงานด้านสารสนเทศของทุกองค์กรที่เก็บข้อมูล ประมวลผล และส่งต่อข้อมูลของผู้ถือบัตร **การประเมินความเสี่ยงเพื่อตรวจหาช่องโหว่** (Vulnerability Assessment) เพื่อตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายสารสนเทศจึงเป็นสิ่งที่จำเป็นอย่างยิ่งต่อการปกป้องข้อมูลของผู้ถือบัตร ทั้งยังช่วยวัดระดับความปลอดภัยยกระดับความคุ้มครองให้สูงสุด และสอดคล้องตามมาตรฐาน PCI DSS อีกด้วย

การประเมินความเสี่ยงให้สอดคล้องกับ PCI DSS นั้นจะต้องสแกนหาช่องโหว่ทั้งภายในและภายนอกเครือข่ายเป็นประจำอย่างต่อเนื่อง เพื่อการตรวจหาช่องโหว่ใหม่ๆ และปิดช่องโหว่ดังกล่าว โดยเฉพาะเมื่อมีการเปลี่ยนแปลงเครือข่ายครั้งสำคัญ เช่น ติดตั้งระบบใหม่ เปลี่ยนโครงสร้างเครือข่าย ปรับกฎระเบียบ (Rule) ของไฟร์วอลล์ เป็นต้น

ทั้งนี้ ผู้ประกอบการที่เข้าข่ายต้องปฏิบัติงานให้สอดคล้องกับมาตรฐาน PCI DSS จะต้องมีการตรวจสอบระบบเครือข่ายของตนในรูปแบบต่างๆ ดังนี้



	ระดับ	เกณฑ์พิจารณา	ตรวจประเมินความปลอดภัย ณ สถานที่ทำงาน	แบบสำรวจประเมินตนเอง	สแกนเครือข่าย
ผู้จำหน่ายสินค้า/บริการ (Merchant)	1	ผู้จำหน่ายสินค้า/บริการ ที่มีจำนวนธุรกรรมต่อปีเกินกว่า 6 ล้านรายการ ผู้จำหน่ายสินค้า/บริการ ที่ระบบความปลอดภัยมีช่องโหว่ ทำให้บุคคลอื่นสามารถเข้าถึงระบบโดยไม่ได้รับ อนุญาต	ทุกปี		ทุกไตรมาส
	2	ผู้จำหน่ายสินค้า/บริการ ที่มีจำนวนธุรกรรมต่อปีระหว่าง 150,000 ถึง 6 ล้านรายการ		ทุกปี	ทุกไตรมาส
	3	ผู้จำหน่ายสินค้า/บริการ ที่มีจำนวนธุรกรรมต่อปีระหว่าง 20,000 ถึง 150,000 รายการ		ทุกปี	ทุกไตรมาส
	4	ผู้จำหน่ายสินค้า/บริการทั้งหมด ที่ไม่อยู่ในระดับ 1, 2, 3 ข้างต้น		ทุกปี	ทุกไตรมาส
ผู้ให้บริการ (Service Provider)	1	ผู้ประมวลผลข้อมูลทุกราย และ Payment Gateway ทุกราย	ทุกปี		ทุกไตรมาส
	2	ผู้ให้บริการที่ไม่อยู่ในระดับ 1 และมีการเก็บข้อมูล, ประมวลผล หรือส่งต่อข้อมูลบัตรเครดิต เกินกว่า 1 ล้านบัญชี/รายการต่อปี	ทุกปี		ทุกไตรมาส
	3	ผู้ให้บริการที่ไม่อยู่ในระดับ 1 และมีการเก็บข้อมูล,ประมวลผล หรือส่งต่อข้อมูลบัตรเครดิต ไม่เกิน 1 ล้านบัญชี/รายการต่อปี		ทุกปี	ทุกไตรมาส

รูปที่ 3

- **ตรวจประเมินความปลอดภัยประจำปี ณ ที่ทำงาน** (Annual On-Site Security Audit) สำหรับองค์กรใหญ่ ซึ่งต้องดำเนินการโดยผู้ตรวจสอบภายนอกที่ได้รับการรับรอง
- **จัดทำแบบสำรวจเพื่อการประเมินตนเองประจำปี** (Annual Self-Assessment Questionnaire) สำหรับองค์กรขนาดเล็ก
- **สแกนเครือข่ายรายไตรมาส** (Quarterly Network Scan) เป็นสิ่งจำเป็นสำหรับทุกองค์กร ซึ่งต้องดำเนินการโดยองค์กรภายนอกที่ได้รับการรับรอง ไม่ว่าจะเป็น ASV (Approved Scanning Vendor) หรือ QSA (Qualified Security Assessor)

แต่ละองค์กรต้องปฏิบัติอย่างไรบ้างนั้นขึ้นอยู่กับขนาดขององค์กรและปริมาณธุรกรรมในหนึ่งปี ซึ่งขอแจกแจงให้เห็นชัดเจนด้วยรูปแบบตารางในรูปที่ 3

บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด ในฐานะตัวแทนผู้ให้บริการของ Approved Scanning Vendor (ASV) ที่ได้รับการรับรองจาก PCI Security Standard Council ได้เปิดให้บริการตรวจประเมินและออกรายงานการผ่านมาตรฐาน PCI DSS พร้อมบริการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศด้วยทีมงานมืออาชีพ

นอกจากนี้ด้วยขีดความสามารถของบริษัท รวมถึงความเชี่ยวชาญของทีมงาน บริษัทจึงเปิดบริการให้คำปรึกษาและเตรียมความพร้อมในการขอตรวจรับรองมาตรฐาน ISO27001 สำหรับหน่วยงานหรือองค์กรที่ต้องการใบรับรองมาตรฐานดังกล่าวอีกด้วย

สนใจผลิตภัณฑ์และบริการสามารถศึกษารายละเอียดเพิ่มเติมได้ที่ www.gbtech.co.th, www.sran.net หรือสอบถามได้ที่

Reg No. 7426661258

โทรศัพท์ 02-982-5445

อีเมล info@gbtech.co.th