SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 8 ประจำเดือน กันยายน 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จากข้อมูลเกี่ยวกับ PCI DSS ที่ได้นำเสนอไปใน SRAN e-Newsletter ฉบับเดือนสิงหาคมนั้น ได้รับความสนใจมากพอสมควร ฉบับนี้จึงขอเจาะรายละเอียดให้ได้รับทราบกันเพิ่มเติม เพื่อเป็นประโยชน์แก่ภาคธุรกิจที่ต้องการสร้างความปลอดภัยในระบบการชำระเงินทางอิเล็กทรอนิกส์ของตนกันค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- มารู้จักมาตรฐาน PCI DSS (ตอนที่ 2) หน้า 1-3
- Message from SRAN หน้า 1

มารู้จักมาตรฐาน PCI DSS ตอนที่ 2

ข้อมูลทางการเงิน ไม่ว่าจะเป็นหมายเลขบัญชีเงินฝาก, หมายเลขบัตรเครดิต หรือแม้แต่ User-name / Password สำหรับการทำธุรกรรมทางการเงินแบบออนไลน์ ล้วนเป็นข้อมูลส่วนบุคคลที่มีความสำคัญ อีกมุมหนึ่งก็เป็นข้อมูลที่มิจฉาชีพต้องการนำไปแสวงประโยชน์โดยมิชอบเช่นกัน ดังที่เป็นข่าวครึกโครมเมื่อกลางเดือนสิงหาคม 2552 ที่ผ่านมาเกี่ยวกับการขโมยเลขบัตรเครดิตและเดบิตกว่า 130 ล้านใบ ในประเทศสหรัฐอเมริกา ซึ่งถือเป็นคดีโจรกรรมข้อมูลส่วนบุคคลที่ใหญ่ที่สุดในประวัติศาสตร์อเมริกา ...

อ่านต่อหน้า 2

Message from SRAN

โกลบอลเทค เปิดให้บริการตรวจประเมินและออกรายงานการผ่านมาตรฐาน PCI DSS โดย Approved Scanning Vendor (ASV) ของ PCI Security Standard Council พร้อมบริการด้านการรักษาความปลอดภัยข้อมูลสารสนเทศด้วย ***ทีมงานมืออาชีพ***

ติดตามข่าวสารด้านความปลอดภัยเครือข่ายสารสนเทศ และเกาะติดความเคลื่อนไหวด้านการพัฒนาผลิตภัณฑ์และบริการของ SRAN ได้ที่

twitter@SRAN_Light

SRAN เปิดให้บริการปรึกษาปัญหาและรับข้อร้องเรียน ติดต่อ **สายด่วน** (Hotline) หมายเลข

086-445-5366

ได้ทุกวัน ตลอด **24 ชั่วโมง**

กำหนดการฝึกอบรมการใช้งาน SRAN Security Center ฟรี สำหรับลูกค้า (ระยะเวลาอบรม 2 วัน)

ก.ย.	ต.ค.	พ.ย.	ธ.ค.
17-18	15-16	19-20	17-18

SRAN Promotion :

สำหรับลูกค้าและตัวแทนจำหน่าย ตั้งแต่วันนี้ ถึง 31 ธันวาคม 2552

- บริการ SRAN Data Safehouse **ฟรี** เพื่อความปลอดภัยของเว็บไซต์พร้อมเก็บบันทึกข้อมูลจราจร และสถิติการใช้งานเว็บไซต์ สมัครได้ที่ www.datasafehouse.net โดยระบุชื่อบริษัทที่ช่อง Company Name
- บริการให้คำปรึกษาแนะนำ เรื่องการออกแบบและจัดทำระบบเครือข่ายสารสนเทศให้ปลอดภัย

คำถามคือ เราจะป้องกันไม่ให้เกิดเหตุการณ์ที่สร้างความเสียหาย ดังกล่าวได้อย่างไร?

มารู้จักมาตรฐาน PCI DSS ตอนที่ 2

เมื่อเราใช้บัตรเครดิตในการซื้อสินค้าและบริการ ข้อมูลทางการเงินของเราไม่ได้อยู่นิ่งแค่ในร้านค้าที่เราจับจ่ายเท่านั้น หากแต่มีการประมวลผลและส่งต่อไปยังหน่วยงานต่างๆ ที่เกี่ยวข้องมากมาย ด้วยเหตุนี้ผู้ประกอบการที่เกี่ยวข้องกับบริการการชำระเงินทางอิเล็กทรอนิกส์ จึงควรตระหนักถึงความมั่นคงปลอดภัยในระบบการชำระเงินอิเล็กทรอนิกส์ ทั้งในรูปของบัตรเครดิต บัตรเดบิต และบัตรเติมเงิน และให้ความสำคัญต่อการตรวจสอบระบบสารสนเทศของตนให้มีความมั่นคงปลอดภัย

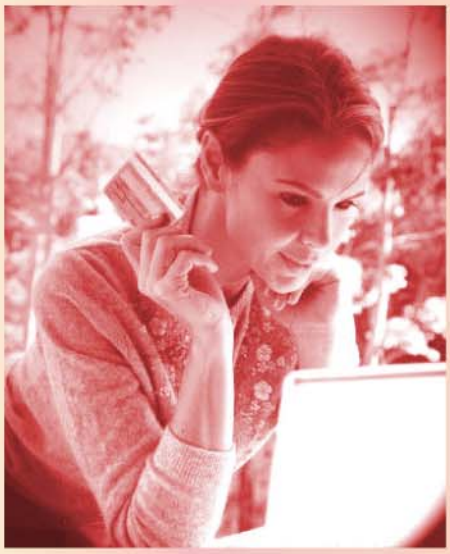
ทั้งนี้ ผู้ที่เข้าข่ายต้องปฏิบัติให้สอดคล้องกับมาตรฐาน **PCI DSS** มิได้จำกัดแค่เพียงสถาบันการเงินเท่านั้น แต่จำแนกออกได้เป็น 2 กลุ่มใหญ่ ดังนี้

1. กลุ่มผู้จำหน่ายสินค้า/บริการ (Merchant) ที่รับชำระเงินค่าสินค้าและบริการด้วยบัตรเครดิต เช่น

- เว็บไซต์ขายสินค้า เช่น amazon.com
- ร้านค้าปลีก เช่น ห้างสรรพสินค้าต่างๆ, Discounted Store เป็นต้น
- สถาบันการศึกษา
- โรงพยาบาล
- โรงแรม, ร้านอาหาร
- ปั๊มน้ำมัน

2. กลุ่มผู้ให้บริการ (Service Provider) คือ องค์กรที่ประมวลผล, เก็บข้อมูล และส่งต่อข้อมูลของผู้ถือบัตรเครดิต แทนตัวผู้ถือบัตรเอง หรือผู้จำหน่ายสินค้า/บริการ (ตามข้อ 1) รวมทั้งผู้ให้บริการรายอื่นๆ ได้แก่ Payment Gateway, ธนาคารต่างๆ, e-commerce host provider, credit reporting agency เป็นต้น

เนื่องจากมาตรฐาน PCI DSS ส่งผลกระทบต่อเครือข่ายและงานด้านสารสนเทศของทุกองค์กรที่เก็บข้อมูล, ประมวลผล และส่งต่อข้อมูลของผู้ถือบัตร การตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายสารสนเทศ จึงเป็นสิ่งจำเป็นต่อการปกป้องข้อมูลของผู้ถือบัตร หากองค์กรใดไม่เคยตรวจสอบระบบของตนเลย ก็ทำได้เพียงตั้งความหวังลมๆ แล้งๆ ว่าข้อมูลของผู้ถือบัตรจะอยู่รอดปลอดภัยเท่านั้น



ทั้งนี้ ผู้ประกอบการที่เข้าข่ายต้องปฏิบัติให้สอดคล้องกับมาตรฐาน PCI DSS จะต้องมีการตรวจสอบระบบเครือข่ายของตนในรูปแบบต่างๆ ดังนี้

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

มารู้จักมาตรฐาน PCI DSS ตอนที่ 2

ด้วยเหตุนี้ การประเมินความเสี่ยงเพื่อตรวจหาช่องโหว่ (Vulnerability Assessment) จึงเป็นวิธีเดียวที่ช่วยวัดระดับความปลอดภัย และยกระดับความคุ้มครองให้สูงสุด ทั้งยังสอดคล้องตามมาตรฐาน PCI DSS อีกด้วย **ซึ่งการประเมินความเสี่ยงให้สอดคล้องกับ PCI DSS นั้น จะต้องสแกนหาช่องโหว่ทั้งภายในและภายนอกเครือข่ายเป็นประจำอย่างต่อเนื่อง** เพื่อตรวจหาช่องโหว่ใหม่ๆ และปิดช่องโหว่ดังกล่าว โดยเฉพาะเมื่อมีการเปลี่ยนแปลงเครือข่ายครั้งสำคัญ เช่น ติดตั้งระบบใหม่, เปลี่ยนโครงสร้างเครือข่าย, ปรับ rule ของไฟร์วอลล์ เป็นต้น

การสแกนเพื่อหาช่องโหว่ภายในเครือข่าย เป็นการประเมินความปลอดภัยในเครือข่ายขององค์กร นับจากขอบนอกสุดของไฟร์วอลล์เข้ามา เพื่อทดสอบทิศทางที่ง่ายต่อการโจมตีจากภายในเครือข่าย ส่วนการสแกนเพื่อหาช่องโหว่ภายนอกเครือข่ายนั้น ก็เพื่อประเมินความปลอดภัยของทุก Host ที่เชื่อมต่อกับอินเทอร์เน็ต ซึ่งอาจเสี่ยงต่อการถูกโจมตีจากภายนอกเครือข่าย การสแกนหาช่องโหว่ภายนอกนี้จะต้องดำเนินการเป็นประจำทุกไตรมาส โดยผู้ให้บริการที่ได้รับการรับรองจาก Payment Card Industry แต่การสแกนภายหลังเครือข่ายมีการเปลี่ยนแปลง สามารถทำได้โดยพนักงานในองค์กรเอง

แต่ละองค์กรต้องปฏิบัติอย่างไรบ้างนั้น ขึ้นอยู่กับขนาดขององค์กรและปริมาณธุรกรรมในหนึ่งปี ซึ่งขอแจกแจงให้เห็นชัดเจนดังตารางต่อไปนี้

	ระดับ	เกณฑ์พิจารณา	ตรวจประเมินความปลอดภัย ณ สถานที่ทำงาน	แบบสำรวจประเมินตนเอง	สแกนเครือข่าย
ผู้จำหน่ายสินค้า / บริการ (Merchant)	1	ผู้จำหน่ายสินค้า/บริการ ที่มีจำนวนธุรกรรมต่อปีเกินกว่า 6 ล้าน รายการ ผู้จำหน่ายสินค้า/บริการ ที่ระบบความปลอดภัยมีช่องโหว่ ทำให้บุคคลอื่นสามารถเข้าถึงระบบโดยไม่ได้รับอนุญาต	ทุกปี		ทุกไตรมาส
	2	ผู้จำหน่ายสินค้า/บริการ ที่มีจำนวนธุรกรรมต่อปีระหว่าง 150,000 ถึง 6 ล้าน รายการ		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/รายการ ต่อปี		ทุกปี	ทุกไตรมาส

หวังเป็นอย่างยิ่งว่าเนื้อหาที่ได้นำเสนอในครั้งนี้จะช่วยให้ทราบถึงแนวทางปฏิบัติเพื่อสร้างความปลอดภัยแก่เครือข่ายและข้อมูล ตลอดจนได้เรียนรู้รายละเอียดของมาตรฐาน PCI DSS ซึ่งในอนาคตจะเข้ามามีบทบาทในบ้านเราอย่างแน่นอน