SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 7 ประจำเดือน สิงหาคม 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

ปัจจุบันการซื้อขายออนไลน์เข้ามามีบทบาทในแวดวงการค้ามากขึ้น ผู้ขายและผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์จะจัดการระบบการชำระเงินให้มั่นคงปลอดภัยได้อย่างไร เพื่อให้ระบบมีประสิทธิภาพ และลูกค้าผู้ใช้บริการเกิดความมั่นใจ SRAN e-Newsletter ฉบับนี้มีคำตอบค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- โกลบอลเทค จับมือ Qualys หน้า 2
- มารู้จักมาตรฐาน PCI DSS หน้า 2–4
- Message from SRAN หน้า 5

โกลบอลเทค จับมือ Qualys

เสนอบริการ

IT Security Audit และ Policy Compliance

บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด ผู้นำด้านการพัฒนาผลิตภัณฑ์และให้บริการด้านความปลอดภัยข้อมูลสารสนเทศของไทย ร่วมมือกับบริษัท Qualys Inc. ผู้นำด้านการประเมินความเสี่ยงเครือข่ายสารสนเทศระดับโลก...

อ่านต่อหน้า 2

มารู้จักมาตรฐาน PCI DSS

มาตรฐาน PCI DSS ย่อมาจาก "Payment Card Industry Data Security Standard" เป็นมาตรฐานความปลอดภัยสารสนเทศที่แพร่หลาย ทั่วโลก...

อ่านต่อหน้า 2–4

Message from SRAN

SRAN Light – The New Generation

จากสถิติที่เพิ่มสูงขึ้นของภัยคุกคามภายใน (Insider Threat) และความต้องการของลูกค้า – SRAN จึงได้พัฒนาผลิตภัณฑ์ใหม่ ซึ่งคงคุณสมบัติด้านการเก็บ Log File ตาม พ.ร.บ.คอมพ์ผนวกเทคโนโลยีใหม่ "HBW" หรือ Human Behavioral Warning...

อ่านต่อหน้า 5

SRAN กับการตรวจจับ twitter

จากกระแสของ Twitter ที่เข้ามามีบทบาทในโลกเครือข่ายสังคมบ้านเรา ทีมงาน SRAN จึงได้พัฒนา Rule Base ในการตรวจจับ twitter ลงบน SRAN Security Center เพื่อมองหาไอพีต้นทางที่เข้าถึงระบบ Twitter ทั้งผ่านเว็บและผ่านโปรแกรมเฉพาะของ Twitter...

อ่านต่อหน้า 5

SRAN Promotion :

สำหรับลูกค้าและตัวแทนจำหน่าย ตั้งแต่วันนี้ ถึง 31 ธันวาคม 2552

บริการ SRAN Data Safehouse ฟรี เพื่อความปลอดภัยของเว็บไซต์ พร้อมเก็บบันทึกข้อมูลจราจร และสถิติการใช้งานเว็บไซต์ สมัครได้ที่ www.datasafehouse.net โดยระบุชื่อบริษัทที่ช่อง Company Name

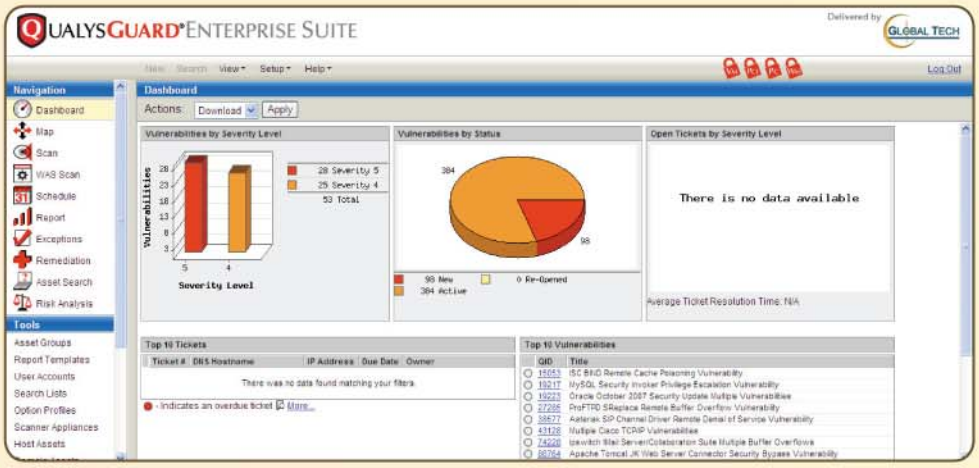
บริการให้คำปรึกษาแนะนำ ฟรี เรื่องการออกแบบและจัดทำระบบเครือข่ายสารสนเทศให้ปลอดภัย

กำหนดการฝึกอบรมการใช้งาน SRAN Security Center ฟรี สำหรับลูกค้า (ระยะเวลาอบรม 2 วัน)

ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.
20–21	17–18	15–16	19–20	17–18

โกลบอลเทค จับมือ Qualys

บริษัท โกลบอล เทคโนโลยี อินทิเกรเทด จำกัด ผู้นำด้านการพัฒนาผลิตภัณฑ์และให้บริการด้านความปลอดภัยข้อมูลสารสนเทศของไทย ร่วมมือกับบริษัท Qualys Inc. ผู้นำด้านการประเมินความเสี่ยงเครือข่ายสารสนเทศระดับโลก นำเสนอบริการด้านการรักษาความมั่นคงปลอดภัยสำหรับองค์กรที่ต้องการจัดทำ IT Security และ Policy Compliance เพื่อช่วยตรวจหาช่องโหว่และแนะนำกระบวนการแก้ไข รวมถึงการเปรียบเทียบผลการตรวจสอบกับข้อกำหนดและแนวทางปฏิบัติตามมาตรฐาน PCI DSS, Sarbanes-Oxley (SOX), GLBA, HIPAA, Basel II ช่วยเพิ่มประสิทธิภาพในการตรวจรักษาความปลอดภัยและการกำหนดนโยบายให้สอดคล้องกับแนวทางปฏิบัติตามมาตรฐานต่าง ๆ ซึ่งได้รับการยอมรับและรับรองจากหน่วยงานด้านการ Audit ระดับโลก ทั้งยังช่วยอำนวยความสะดวกและลดค่าใช้จ่ายในการดูแลความปลอดภัยระบบสารสนเทศขององค์กรอีกด้วย



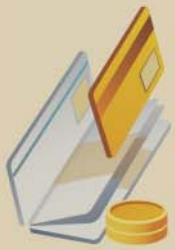
มารู้จักมาตรฐาน PCI DSS

มาตรฐาน PCI DSS ได้เริ่มใช้ในโครงการรักษาความปลอดภัยข้อมูลของบัตรเครดิต 5 ค่ายยักษ์ คือ Visa, MasterCard, American Express, Discover และ JCB ซึ่งมีจุดหมายร่วมกันเพื่อยกระดับการคุ้มครองลูกค้า โดยสร้างความมั่นใจว่าผู้ขาย (ผู้รับชำระเงินด้วยบัตรเครดิต) มีมาตรการรักษาความปลอดภัยที่เหมาะสมในการเก็บรักษา การประมวลผล และการรับส่งข้อมูลของผู้ถือบัตรเครดิต

มาตรฐาน PCI DSS ย่อมาจาก "Payment Card Industry Data Security Standard" เป็นมาตรฐานความปลอดภัยสารสนเทศที่แพร่หลายทั่วโลก รวบรวมโดยคณะกรรมการ Payment Card Industry Security Standards Council (PCI SSC) มาตรฐานนี้ถูกกำหนดขึ้นเพื่อช่วยให้องค์กรต่างๆ ที่มีการรับชำระเงินด้วยบัตรเครดิต สามารถป้องกันการฉ้อโกงบัตรเครดิต โดยการควบคุมข้อมูลและช่องโหว่ต่างๆ ให้เข้มงวดมากยิ่งขึ้น และได้นำไปใช้กับทุกองค์กรที่เก็บรักษา ประมวลผล หรือรับส่งข้อมูลของผู้ถือบัตรเครดิต ไม่ว่าจะเป็นบัตรของค่ายใดก็ตาม

การตรวจสอบการปฏิบัติตามมาตรฐานอาจทำได้โดยตรวจสอบเองด้วยบุคลากรภายในองค์กรหรือให้หน่วยงานภายนอกเป็นผู้ตรวจสอบก็ได้ ซึ่งจะใช้วิธีใดไม่เกี่ยวกับขนาดองค์กร แต่ขึ้นกับปริมาณการทำธุรกรรมผ่านบัตรเครดิตขององค์กรนั้นๆ การประเมินการปฏิบัติตามมาตรฐาน PCI DSS จะต้องทำเป็นประจำทุกปี โดยองค์กรที่มีปริมาณธุรกรรมผ่านบัตรเครดิตมาก จะต้องได้รับการตรวจประเมินจากผู้ตรวจประเมินอิสระ (Qualified Security Assessor : QSA)

ส่วนบริษัทที่มีปริมาณธุรกรรมไม่มากนัก สามารถเลือกที่จะตรวจประเมินได้ด้วยตนเองผ่านแบบสำรวจประเมินตนเอง (Self-Assessment Questionnaire : SAQ)



มารู้จักมาตรฐาน PCI DSS

ในประเทศสหรัฐอเมริกา องค์กรที่มีธุรกรรมทางการเงินผ่านบัตรเครดิตตั้งแต่หนึ่งค่ายขึ้นไป แต่ไม่ดำเนินการให้สอดคล้องกับข้อกำหนด PCI DSS จะไม่สามารถรับชำระเงินผ่านบัตรเครดิตได้ ทั้งยังต้องถูกตรวจสอบ และอาจถึงขั้นเสียเงินค่าปรับอีกด้วย

ข้อกำหนด PCI DSS

ปัจจุบันมาตรฐาน PCI DSS เป็นเวอร์ชั่น 1.2 ระบุข้อกำหนดไว้ 12 ข้อ จำแนกตามวัตถุประสงค์ได้เป็น 6 กลุ่ม คือ

วัตถุประสงค์ที่ควบคุม	ข้อกำหนด PCI DSS
สร้างเครือข่ายที่ปลอดภัยและบำรุงรักษาไว้	ติดตั้งและดูแลรักษาค่าที่ตั้งไว้ของไฟร์วอลล์เพื่อปกป้องข้อมูลผู้ถือบัตร ไม่ใช้ค่าที่ตั้งมาพร้อมกับผลิตภัณฑ์สำหรับรหัสผ่านและการรักษาความปลอดภัยอื่นๆ ของระบบ
ปกป้องข้อมูลผู้ถือบัตร	ปกป้องข้อมูลของผู้ถือบัตรที่ได้เก็บรักษาไว้ เข้ารหัสข้อมูลผู้ถือบัตรก่อนส่งผ่านเครือข่ายสาธารณะแบบเปิด
บำรุงรักษาโปรแกรมที่ใช้จัดการกับช่องโหว่	ใช้โปรแกรมแอนตี้ไวรัสและอัพเดตสม่ำเสมอ สำหรับทุกระบบที่มักได้รับผลกระทบจากมัลแวร์ พัฒนาและดูแลรักษาระบบและแอพพลิเคชั่นต่าง ๆ ให้ปลอดภัย
ใช้มาตรการที่รัดกุมในการควบคุมการเข้าถึง	จำกัดการเข้าถึงข้อมูลผู้ถือบัตรเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น กำหนดหมายเลขประจำตัวเฉพาะ (unique ID) ให้กับผู้ที่สามารถเข้าถึงคอมพิวเตอร์ได้ จำกัดการเข้าถึงทางกายภาพ สำหรับข้อมูลผู้ถือบัตร
ตรวจตราและทดสอบเครือข่ายต่างๆ อย่างสม่ำเสมอ	ติดตามและเฝ้าดูการเข้าถึงทรัพยากรทางเครือข่ายและข้อมูลผู้ถือบัตร ทดสอบระบบและขั้นตอนต่าง ๆ ในการรักษาความปลอดภัยอย่างสม่ำเสมอ
คงไว้ซึ่งนโยบายความปลอดภัยสารสนเทศ	คงไว้ซึ่งนโยบายด้านการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ

สำหรับในประเทศไทยมี พ.ร.ฎ. ว่าด้วยการควบคุมดูแลธุรกิจบริการการชำระเงินทางอิเล็กทรอนิกส์ พ.ศ. 2551 ซึ่งตราขึ้นเพื่อยกระดับความเชื่อมั่นในการทำธุรกรรมทางการเงินออนไลน์ ทำให้ระบบข้อมูลอิเล็กทรอนิกส์มีความน่าเชื่อถือและเป็นที่ยอมรับ และสร้างความความมั่นคงปลอดภัยทางระบบสารสนเทศ ดังนั้นผู้ให้บริการการชำระเงินทางอิเล็กทรอนิกส์ จึงต้องมีนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยทางระบบสารสนเทศ ซึ่งธนาคารแห่งประเทศไทยได้กำหนดหลักเกณฑ์ไว้ สรุปได้ดังนี้

1. การควบคุมการเข้าถึง และการพิสูจน์ตัวตนผู้ใช้ โดย

1.1 กำหนดหน้าที่และความรับผิดชอบของบุคลากรหรือหน่วยงานที่ดูแลด้าน IT Security ขององค์กร พร้อมการอบรมเพื่อเพิ่มเติมความรู้แก่บุคลากรอย่างสม่ำเสมอ

1.2 ควบคุมและจำกัดสิทธิการใช้ระบบสารสนเทศที่เกี่ยวกับการให้บริการ และข้อมูลตามความจำเป็นในการใช้งาน ป้องกันการลักลอบการเข้าถึงระบบโดยผู้ที่ไม่มีสิทธิ ทั้งจากภายในและภายนอกองค์กร พร้อมบันทึกการเข้าใช้ระบบสารสนเทศของผู้ใช้บริการและบุคลากรที่เกี่ยวข้อง

1.3 ระบุหรือพิสูจน์ตัวตนและตรวจสอบสิทธิของผู้ใช้ระบบ โดยใช้เทคโนโลยีที่เหมาะสม เช่น รหัสผ่าน, เลขประจำตัว (Personal Identification Number), อุปกรณ์หรือบัตรที่เก็บข้อมูลส่วนบุคคล (Token หรือ Smart Card) เป็นต้น เพื่อป้องกันการปฏิเสธการรับผิดกรณีมีข้อพิพาทเกิดขึ้น

2. การรักษาความลับของข้อมูลและความถูกต้องเชื่อถือได้ของระบบสารสนเทศ โดย

2.1 กำหนดชั้นความลับของข้อมูลตามระดับความสำคัญและสิทธิผู้ที่สามารถเข้าถึงข้อมูลดังกล่าว รวมทั้งจัดให้มีวิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลลับในลักษณะที่มั่นคงปลอดภัยตามระดับความสำคัญ

2.2 บริหารจัดการเครือข่ายที่เกี่ยวกับการให้บริการ เพื่อป้องกันภัยคุกคามทางเครือข่าย หรือข้อมูลที่ส่งผ่านทางเครือข่าย

3. การรักษาสภาพความพร้อมใช้งานของการให้บริการ โดยการประเมินและจัดการความเสี่ยงของระบบที่ให้บริการ พร้อมติดตามตรวจสอบความผิดปกติและความล่อแหลมของระบบสารสนเทศ โดยประเมินช่องโหว่ของระบบ (Vulnerability Assessment) โดยเฉพาะในส่วนของระบบเครือข่ายที่เกี่ยวกับการให้บริการ

หากระบบมีความเสี่ยงสูง ควรจัดให้มีการทดสอบเจาะระบบ (Penetration Test) ด้วยเพื่อทดสอบประสิทธิภาพของเทคโนโลยีการรักษาความมั่นคงปลอดภัย

4. การตรวจสอบความมั่นคงปลอดภัยทางระบบสารสนเทศ โดยจัดให้มีผู้ตรวจสอบและดำเนินการตรวจสอบในเรื่องที่มีความเสี่ยงหรือมีความสำคัญต่อการให้บริการอย่างน้อยปีละ 1 ครั้ง

มาตรฐาน PCI DSS กับ SRAN Data Safehouse

SRAN Data Safehouse ซึ่งเป็นบริการเก็บบันทึก Log File และเฝ้าระวังภัยคุกคามสำหรับเว็บไซต์ พร้อมตรวจหาช่องโหว่และประเมินความเสี่ยงเว็บไซต์ ได้พัฒนาคุณสมบัติขึ้นเป็นลำดับ โดยเพิ่มการประเมินการปฏิบัติตามมาตรฐานของ PCI DSS ซึ่งเน้นที่การตรวจสอบปัญหาต่าง ๆ ที่พบใน web server เป็นหลัก

PCI DSS COMPLIANT PCI DSS Compliance check

หน้ารายงานในส่วนของ PCI DSS สามารถเปิดดูได้จากเมนู Status > Security scan เมื่อเข้ามาที่หน้า Security scan แล้วให้คลิกที่ลิงค์ PCI DSS Compliance check

จากนั้นจึงเลือกเปิดดูรายงานตามวันที่ที่ต้องการ โดยคลิกที่ลิงค์ view report

Date	Results
2009-05-13 01:58:11	view report
2009-05-01 15:37:20	view report

จะปรากฏหน้าที่บอกรายละเอียดการประเมินผล พร้อมทั้งผลที่บอกว่า web server นั้น สอดคล้องกับข้อกำหนดในมาตรฐาน PCI DSS หรือไม่ ซึ่งสามารถอ่านรายละเอียดเพิ่มเติมได้จากรายงานการประเมินช่องโหว่ของระบบ

PCI DSS COMPLIANT NOT COMPLIANT

Vulnerability Assessme

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and proc eradicate these threats.

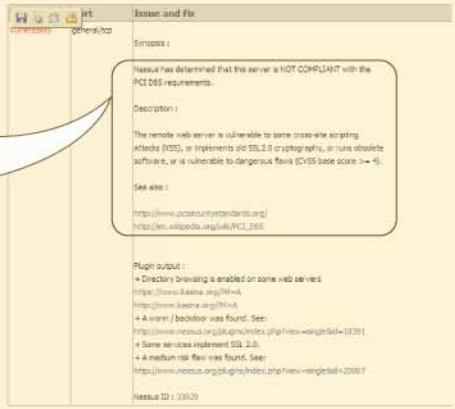
Nessus has determined that this server is NOT COMPLIANT with the PCI DSS requirements.

Description :

The remote web server is vulnerable to some cross-site scripting attacks (XSS), or implements old SSL2.0 cryptography, or runs obsolete software, or is vulnerable to dangerous flaws (CVSS base score >= 4).

See also :

http://www.pcisecuritystandards.org/
http://en.wikipedia.org/wiki/PCI_DSS



ตัวอย่างรายงานการประเมินช่องโหว่ของระบบ

จากสถิติที่เพิ่มสูงขึ้นของภัยคุกคามภายใน (Insider Threat) และความต้องการของลูกค้า – SRAN จึงได้พัฒนาผลิตภัณฑ์ใหม่ "SRAN Light" ซึ่งคงคุณสมบัติด้านการเก็บ Log File ตาม พ.ร.บ.คอมพ์ ผนวกเทคโนโลยีใหม่ "HBW" หรือ Human Behavioral Warning

ทั้งนี้ **ลูกค้า SRAN Security Center** สามารถอัพเกรดอุปกรณ์เพื่อเพิ่มเทคโนโลยี HBW นี้ได้ในราคาพิเศษ

SRAN Light - The New Generation

เพื่อเชื่อมโยงระบบ IT Security ขององค์กร เข้ากับงานบริหารทรัพยากรบุคคล พร้อมระบบจัดเก็บคลังข้อมูล (Inventory) ซึ่งมีคุณสมบัติเด่น ดังนี้

1. ช่วยให้ทราบถึงพฤติกรรมการใช้งาน IT ภายในองค์กร โดยเชื่อมโยง IP Address และ MAC Address เข้ากับข้อมูลรายชื่อพนักงาน ซึ่งสามารถเพิ่มรูปพนักงานเข้าไปในระบบได้ พร้อมเก็บประวัติการใช้งาน

2. เฝ้าระวังพฤติกรรมการใช้งาน โดยสามารถกำหนด Rule Policy ตามนโยบายบริษัทได้ เพื่อป้องกันการละเมิดสิทธิส่วนบุคคลของพนักงานในองค์กร

3. รายงานผลการใช้งานข้อมูลสารสนเทศเป็นรายแผนก, รายบุคคล และภาพรวมของบริษัทได้ พร้อมสถิติการใช้งานรายแผนก รายบุคคล ช่วยให้การพยากรณ์การลงทุนระบบไอซีทีในองค์กรมีประสิทธิภาพมากขึ้น

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

SRAN กับการตรวจจับ Twitter

http://www.sran.net/archives/214