

SRAN e-Newsletter



จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 3 ประจำเดือน เมษายน 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

SRAN ต้อนรับเดือนที่ร้อนที่สุดของปี ด้วยข้อมูลสถิติเว็บไซต์ที่มีช่องโหว่ เสี่ยงต่อการถูกโจมตี พร้อมเนื้อหาเกี่ยวกับการเก็บ Log File สำหรับเว็บไซต์ให้สอดคล้องกับพ.ร.บ.คอมพ์ เพื่อเป็นหลักฐานประกอบหากเกิดความออนไลน์ขึ้น

สำหรับลูกค้า SRAN สามารถอัปเดตข่าวสารและโปรโมชั่น ได้ที่ Message from SRAN และอ่านคำถามที่พบบ่อยได้ที่ FAQ ค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- SRAN เดือนเว็บไทยเสี่ยงถูกเจาะระบบ หน้า 2
- หมิ่นประมาทออนไลน์ หลักฐานใดเชื่อถือได้ หน้า 3
- Message from SRAN หน้า 1
- FAQ for SRAN Security Center หน้า 2-3

FAQ for SRAN Security Center



- สังเกตอย่างไรว่า Harddisk โกงได้เต็มหรือไม่?
- หากพบว่า Harddisk โกงได้เต็ม (ส่วน /backup) ควรทำอย่างไร?
- ทำอย่างไรหากต้องการดู Log ย้อนหลัง?
- สามารถดาวน์โหลด Log มาเปิดดูภายนอกได้หรือไม่?

Message from SRAN



บริการ SRAN Data Safehouse ฟรี สำหรับลูกค้าและตัวแทนจำหน่าย SRAN สมัครใช้บริการได้ที่ www.datasafehouse.net โดยระบุชื่อบริษัทที่ช่อง Company Name ตั้งแต่วันที่ถึง 31 ธ.ค. 52

อบรมการใช้งาน SRAN Security Center (ฟรี) สำหรับลูกค้า SRAN ทูกราย สอบถามรายละเอียดและสำรองที่นั่ง โทร.02-982-5445

23-24	14-15	18-19	16-17	20-21	17-18	15-16	19-20	17-18
เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.

หมายเหตุ : ระยะเวลาในการอบรม 2 วัน

SRAN เดือนเว็บไทย เสี่ยงถูกเจาะระบบ

ข้อมูลจาก SRAN Data Safehouse ซึ่งเป็นระบบเก็บ Log File สำหรับเว็บไซต์, เก็บสถิติการใช้งานเว็บไซต์แบบ Real Time และปกป้องเว็บไซต์จากภัยคุกคามออนไลน์ เผยสถิติเว็บไซต์ที่มีช่องโหว่ เสี่ยงต่อการถูกโจมตี โดยเก็บรวบรวมข้อมูลเว็บไซต์ที่มีช่องโหว่จากทั่วโลก คัดเฉพาะเว็บไซต์ในประเทศไทย พร้อมจัดทำระบบตรวจสอบอัตโนมัติเพื่อเก็บข้อมูลสถิติรายวัน พบว่ามีเว็บไซต์ในประเทศไทยที่พบช่องโหว่ชนิด XSS (Cross Site Scripting) มีโอกาสถูกฝังโค้ดจากนักโจมตีระบบ (Hacker) ถึง 41 เว็บไซต์!.. อ่านรายละเอียด หน้า 2



หมิ่นประมาทออนไลน์ หลักฐานใดเชื่อถือได้

การใส่ความผู้อื่นต่อบุคคลที่สาม หรือการหมิ่นประมาท เกิดขึ้นได้ง่ายดายบนปลายนิ้ว คำถามคือ หากเกิดคดีความขึ้น หลักฐานใดเชื่อถือได้ในชั้นศาล?

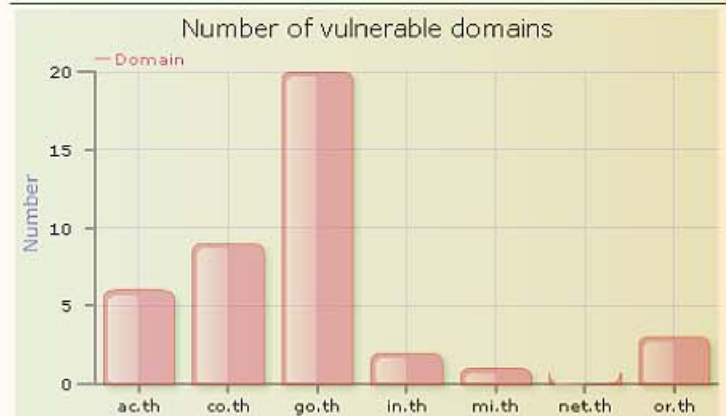
ยินดีรับทุกข้อเสนอแนะที่ info@gbtech.co.th อ่านจดหมายข่าวย้อนหลังได้ที่ www.gbtech.co.th

SRAN e-Newsletter by Global Technology Integrated Co.,Ltd

ข้อมูลจาก SRAN Data Safehouse ซึ่งเป็นระบบเก็บ Log File สำหรับเว็บไซต์, เก็บสถิติการใช้งานเว็บไซต์แบบ Real Time และปกป้องเว็บไซต์จากภัยคุกคามออนไลน์ เผยสถิติเว็บไซต์ที่มีช่องโหว่ เสี่ยงต่อการถูกโจมตี โดยเก็บรวบรวมข้อมูลเว็บไซต์ที่มีช่องโหว่จากทั่วโลก คัดเฉพาะเว็บไซต์ในประเทศไทย พร้อมจัดทำระบบตรวจสอบอัตโนมัติเพื่อเก็บข้อมูลสถิติรายวัน พบว่ามีเว็บไซต์ในประเทศไทยที่พบช่องโหว่ชนิด XSS (Cross Site Scripting) มีโอกาสถูกฝังโค้ดจากนักโจมตีระบบ (Hacker) ถึง 41 เว็บไซต์ (ข้อมูล ณ วันที่ 31 มี.ค. 52) ซึ่ง เว็บไซต์เหล่านี้มีโอกาสถูกเปลี่ยนหน้าเว็บเพจหรือแก้ไขข้อมูลเว็บไซต์โดย มิชอบ กระทั่งต่อสภาพลักษณะ องค์กร และสร้าง ความสูญเสียนี่ไม่อาจตีมูลค่าได้

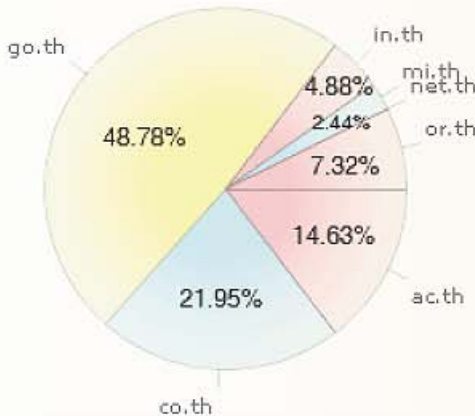


SRAN เดือนเว็บไทย เสี่ยงถูกเจาะระบบ



ผลการประเมินช่องโหว่ชนิด XSS พบว่าเว็บไซต์ที่เสี่ยงต่อการถูกโจมตีจัดหมวดหมู่ตามโดเมน เรียงลำดับได้ดังนี้ หน่วยงานราชการ (.go.th) พบเว็บไซต์ที่มีความเสี่ยงมากที่สุดจำนวน 20 โดเมน คิดเป็น 48.78% รองลงมาคือ องค์กรเอกชน (.co.th) จำนวน 9 โดเมน (21.95%), สถาบันการศึกษา (.ac.th) จำนวน 6 โดเมน (14.63%), องค์กรไม่แสวงกำไร (.or.th) จำนวน 3 โดเมน (7.32%), องค์กรอื่นๆ หรือเว็บส่วนบุคคล (.in.th) จำนวน 2 โดเมน (4.88%) และหน่วยงานด้านการทหาร (.mi.th) จำนวน 1 โดเมน (2.44%) ตามลำดับ นอกจากนี้ยังพบว่าช่องโหว่ที่ตรวจพบส่วนใหญ่ยังไม่ได้รับการแก้ไข ดูรายละเอียดเพิ่มเติมได้ที่ www.datasafehouse.net หน้า Archive

domain percentages



FAQ for SRAN Security Center

Q: หากพบว่า Harddisk โกงเต็ม (ส่วน /backup) ควรทำอย่างไร?

A: ทำการสำรองข้อมูล Log โดยการ Export Log ออกมาเก็บไว้ ภายนอก โดยเลือกที่ Management → Services → Log Export เลือก Enable ใส่ IP Address ที่จะเก็บ Log สำหรับ Backup จากนั้นตั้งชื่อ Share Directory ให้ตรงกับ Folder ของเครื่อง ที่ใช้ Backup Log โดยต้องกำหนดค่า ให้ Share Folder ของเครื่องที่ใช้ Backup Log ด้วย

Q: สังเกตอย่างไรว่า Harddisk โกงเต็มหรือไม่?

A: เข้าไปดูได้ที่หน้า Management → Services → Data Archive ดูที่ Total ว่าใช้ไปกี่ % โดยที่

- ส่วน /backup คือส่วนที่ใช้ในการเก็บ Log
- ส่วน /srn คือ partition ในส่วนของตัวระบบ

บทบาทของอินเทอร์เน็ตในปัจจุบันนั้น นอกจากจะเป็นแหล่งเผยแพร่ข้อมูล ข่าวสาร, ตลาดนัดออนไลน์, ตลาดแรงงาน, สถานีวิทยุ/โทรทัศน์ ที่เข้าถึงได้ง่าย ประหยัดทั้งเวลาและค่าใช้จ่ายแล้ว ยังวิวัฒนาการกลายเป็นสังคมเสมือน ที่ผู้คนทุกเพศ ทุกวัย สามารถพูดคุย แลกเปลี่ยนทัศนคติและข้อมูลที่มีอยู่ได้ ผ่านเครือข่ายสังคม "Social Networking" ถือเป็นจุดเปลี่ยนทางสังคม ซึ่งคนรุ่นใหม่มีแนวโน้มที่ไม่เคยสื่อสารผ่านช่องทางนี้



หมิ่นประมาทออนไลน์ หลักฐานใดเชื่อถือได้

การใส่ความผู้อื่นต่อบุคคลที่สาม หรือการหมิ่นประมาทจึงไม่จำเป็นต้องเกิดบนเวทีปราศรัย, บทสัมภาษณ์ผ่านสื่อ ฯลฯ อีกต่อไป หากเกิดขึ้นง่ายดายบนปลายนิ้ว คำถามคือ หากเกิดคดีความขึ้นหลักฐานใดเชื่อถือได้ในชั้นศาล?

หากนาย ก. โพสต์ว่าร้ายนาย ข. ลงบน Hi5 ของนาย ก. เอง มีคนเข้าอ่านมากมายจนรู้ถึงหู นาย ข. นาย ข. เข้ามาเห็น จึง save หน้าจอ และพิมพ์ข้อความเก็บไว้เป็นหลักฐาน พร้อมแจ้งความดำเนินคดีกับนาย ก. ข้อหาหมิ่นประมาท กระดาษแผ่นนั้นถือเป็นหลักฐานได้หรือไม่? เทคโนโลยีที่ก้าวล้ำสามารถสร้างและ แต่งเติมข้อความหรือรูปภาพได้ด้วยคอมพิวเตอร์ แล้วจะเชื่อได้อย่างไรว่านาย ข. มิได้สร้างหลักฐานเท็จขึ้นมาใส่ความ นาย ก. อีกมุมหนึ่ง หากนาย ก. กระทำผิดจริง และได้ลบข้อความนั้นออกไปแล้ว

ก็ย้อนสู่คำถามเดียวกัน ศาลจะประทับรับฟ้องด้วยหลักฐาน กระดาษพิมพ์ข้อความหรือ?

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้ผู้ให้บริการเว็บไซต์ต้องเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log File) เพื่อใช้เป็นหลักฐานหากเกิดคดี ความออนไลน์ขึ้น แต่หากผู้ดูแลเว็บไซต์ เป็นผู้กระทำความผิดเสียเอง เราจะ มั่นใจได้อย่างไรว่าจะไม่เกิดการลบหรือแก้ไขข้อความเพื่อให้ตนพ้นผิด

ด้วยเหตุนี้ เจ้าของเว็บไซต์ ทั้งเว็บไซต์ส่วนบุคคลและเว็บไซต์องค์กร/หน่วยงานต่างๆ โดยเฉพาะเว็บไซต์ที่ให้บริการเว็บบอร์ด เว็บบล็อก จึงควรใช้โปรแกรมเก็บบันทึกข้อมูลการใช้งานเว็บไซต์ของตน เพื่อให้ทราบว่า มีใครเข้ามาใช้บริการที่เพจไหน ทำอะไร เมื่อไร อย่างไร โดยจัดเก็บข้อมูลดังกล่าวไว้ไม่ต่ำกว่า 90 วัน สามารถสืบค้นย้อนหลัง และยืนยันได้ว่าข้อความดังกล่าวจะไม่ถูกแก้ไข สอดคล้องกับพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่ออำนวยความสะดวกแก่พนักงานเจ้าหน้าที่ ให้สามารถตรวจสอบหลักฐานย้อนหลังได้หากเกิดคดีความออนไลน์ ซึ่งคาดว่าจะมีแนวโน้มเพิ่มสูงขึ้น ตามสภาพสังคมที่เปลี่ยนแปลงไป

← FAQ for SRAN Security Center

Q: ทำอย่างไรหากต้องการดู Log ย้อนหลัง?

A: เข้าไปดูได้ที่หน้า Management → Services → Data Archive เลือกวันที่ที่ต้องการดู Log ย้อนหลัง ที่ปฏิทินทาง ด้านข้าง

Q: สามารถดาวน์โหลด Log มาเปิดดูภายนอกได้หรือไม่?

A: ได้ โดยดาวน์โหลดโปรแกรม SRAN Viewer และศึกษาคู่มือการใช้งานที่ www.gbtech.co.th/th/product/usm เพื่อความสะดวกในการวิเคราะห์ Log และอ่าน Log File ขนาดใหญ่ (500 MB ขึ้นไป)



ดูข้อมูล FAQ เพิ่มเติมได้ที่ www.gbtech.co.th/th/contacts/faq