SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 6 ประจำเดือน กรกฎาคม 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

จากที่ลูกค้าหลายท่านสนใจอยากทราบถึงวิธีการป้องกันตนให้ปลอดจากภัยคุกคาม จดหมายข่าวฉบับนี้จึงขอนำเสนอวิธีป้องกันภัยคุกคามออนไลน์ ที่ทำได้ง่ายๆ ด้วยตนเอง พร้อมแนะนำบริการใหม่ "SRAN Anti-Hacking & IT Forensic Services เพื่อปกป้องเครื่องแม่ข่ายให้ปลอดภัยจากการโจมตีโดยผู้ไม่ประสงค์ดี พร้อมบริการสืบหาผู้กระทำความผิด ดูรายละเอียดได้ใน Message from SRAN ค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

In This Issue:

- 10 วิธีรู้ทันภัยคุกคามอินเตอร์เน็ต หน้า 2-3
- Message from SRAN หน้า 4
- FAQ for SRAN Secrity Center หน้า 4

10 วิธีรู้ทันภัยคุกคามอินเตอร์เน็ต

เมื่อโลกอินเตอร์เน็ตเข้ามามีบทบาทในชีวิตมากขึ้นภัยร้ายก็มาเยือนถึงตัวได้แบบไม่เว้นวัน SRAN จึงขอนำเสนอเทคนิคป้องกันภัยคุกคามออนไลน์ ที่ใครก็ทำได้มาให้รับทราบกันดังนี้

1. ตั้งสติก่อนเปิดเครื่อง
2. กำหนด Password ที่ยากแก่การคาดเดา
3. สังเกตโปรแกรมไม่พึงประสงค์ขณะเปิดเครื่อง
4. หมั่นตรวจสอบและอัพเดต OS หรือซอฟต์แวร์ที่ใช้

Message from SRAN

แนะนำบริการใหม่ : **SRAN Anti-Hacking & IT Forensic Services**

SRAN Anti-Hacking Service ภัยคุกคามทางอินเตอร์เน็ตสำหรับ Server ที่มีความสำคัญต่อธุรกิจ → อ่านต่อหน้า 4

SRAN IT Forensic Service บริการสืบหาผู้กระทำความผิดทางอินเตอร์เน็ตและคอมพิวเตอร์สำหรับลูกค้าที่ถูกโจมตีระบบแล้ว และต้องการผลลัพธ์ที่รวดเร็วในการสืบหาผู้กระทำความผิด รับรองผลภายใน 14 วัน (ไม่คิดค่าบริการหากหาร่องรอยการกระทำผิดไม่พบ) → อ่านต่อหน้า 4

FAQ for SRAN Security Center

เวลาในเครื่อง SRAN ไม่ตรงตามเวลามาตรฐาน ต้องทำอย่างไร?

กำหนดการฝึกอบรมการใช้งาน SRAN Security Center ฟรี สำหรับลูกค้า (ระยะเวลาอบรม 2 วัน)

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

SRAN Promotion :

สำหรับลูกค้าและตัวแทนจำหน่าย ตั้งแต่วันนี้ ถึง 31 ธันวาคม 2552

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

เมื่อโลกอินเตอร์เน็ตเข้ามามีบทบาทในชีวิตมากขึ้น ภัยร้ายก็มาเยือนถึงตัวได้แบบไม่เว้นวัน SRAN จึงขอนำเสนอเทคนิคป้องกันภัยคุกคามออนไลน์ ที่ใครก็ทำได้มาให้รับทราบกันดังนี้

10 วิธีรู้ทันภัยคุกคามอินเตอร์เน็ต

1. ตั้งสติก่อนเปิดเครื่อง ก่อนเปิดเครื่องคอมพิวเตอร์ ให้รู้ตัวเสมอว่าเราอยู่ที่ไหน ที่บ้าน ที่ทำงาน หรือที่สาธารณะ และระมัดระวังการใช้งานคอมพิวเตอร์ ตั้งแต่เริ่มเปิดเครื่อง ดังนี้

- ก่อน Login เข้าใช้งานคอมพิวเตอร์ ต้องมั่นใจว่าไม่มีใครแอบดู Password ของเราได้
- เมื่อไม่ได้อยู่หน้าจอคอมพิวเตอร์ควรล็อคหน้าจอให้อยู่ในสถานะ ที่ต้องใส่ค่า Login ป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์ของเราได้อย่างสะดวก
- อย่าประมาทในการใช้งานอินเตอร์เน็ตตระหนักไว้ว่า ข้อมูลความลับ และความเป็นส่วนตัวของเราอาจถูกเปิดเผยได้เสมอในโลกออนไลน์ แม้เราจะระมัดระวังมากเพียงใดก็ตาม

2. กำหนด Password ที่ยากแก่การคาดเดา ควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และใช้อักขระพิเศษ ไม่ตรงกับความหมายในพจนานุกรม เพื่อให้เดาได้ยากมากขึ้น และการใช้งานอินเตอร์เน็ตทั่วไป เช่น การ Login ระบบ e-mail , ระบบสนทนาออนไลน์ (chat) ระบบเว็บไซต์ที่เราเป็นสมาชิกอยู่ ทางที่ดีควรใช้ password ที่ต่างกันบ้างพอให้จำได้ หรือมีเครื่องมือช่วยจำ password เข้ามาช่วย

3. สังเกตขณะเปิดเครื่องว่ามีโปรแกรมไม่พึงประสงค์รันมาพร้อมๆ กับการเปิดเครื่องหรือไม่ ถ้าดูไม่ทันให้สังเกตระยะเวลาบูตเครื่อง หากนานผิดปกติอาจเป็นไปได้ว่าเครื่องคอมพิวเตอร์ติดปัญหาจากไวรัส หรือ อื่นๆได้

4. หมั่นตรวจสอบและอัพเดต OS หรือซอฟต์แวร์ที่ใช้ ให้เป็นเวอร์ชั่นปัจจุบัน โดยเฉพาะโปรแกรมป้องกันภัยในเครื่อง และควรใช้ระบบปฏิบัติการและซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย นอกจากนี้ ควรอัพเดตอินเตอร์เน็ตบราวเซอร์ให้ทันสมัยอยู่เสมอ เนื่องจาก Application Software สมัยใหม่มักพึ่งพาอินเตอร์เน็ตบราวเซอร์ ก่อให้เกิดช่องโหว่ใหม่ๆ ให้ภัยคุกคามเจาะผ่านบราวเซอร์สร้างปัญหาให้เราได้

5. ไม่ลงซอฟต์แวร์มากเกินจำเป็น จนเกินศักยภาพการทำงานของเครื่องคอมพิวเตอร์

ซอฟต์แวร์ที่**จำเป็น**ต้องลงในเครื่องคอมพิวเตอร์ได้แก่	**ซอฟต์แวร์ที่ไม่ควรมี**บนเครื่อง คอมพิวเตอร์ที่เราใช้งานได้แก่
อินเตอร์เน็ตบราวเซอร์ เพื่อใช้เปิดเว็บไซต์ต่างๆ E-mail พื่อใช้รับส่งข้อมูลและติดต่อสื่อสาร โปรแกรมสำหรับงานด้านเอกสาร, โปรแกรมตกแต่งภาพ เสียง วิดีโอ โปรแกรมป้องกันไวรัสคอมพิวเตอร์	ซอฟต์แวร์ที่ใช้ในการ Crack โปรแกรม ซอฟต์แวร์สำเร็จรูปที่ใช้ในการโจมตีระบบ, เจาะระบบ (Hacking Tools) โปรแกรมที่เกี่ยวกับการสแกนข้อมูล ดัก รับข้อมูล (Sniffer) และอื่นๆ ที่อยู่ในรูปซอฟต์แวร์สำเร็จรูป ที่ไม่เป็นที่รู้จักแม้ค้นหาข้อมูลก็ไม่พบรายละเอียด ซึ่งหากเป็นเช่นนี้เราควรระมัดระวังหากจำเป็นต้อง ใช้ชุดซอฟต์แวร์ดังกล่าว ซอฟต์แวร์ที่ใช้หลบหลีกการป้องกัน เช่น โปรแกรมซ่อน IP address เพื่อป้องกันคนไม่ให้เห็น IP ที่แท้จริงนั้น มักใช้เส้นทางระบบเครือข่ายของอาสาสมัครต่างๆ ซึ่งหนึ่งในนี้อาจเป็นเครื่องของผู้ไม่ประสงค์ดีที่ต้องการดักข้อมูลของผู้ใช้งานบริสุทธิ์ก็ได้

10 วิธีรู้ทันภัยคุกคามอินเตอร์เน็ต

6. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย เว็บไซต์ ประเภทนี้ ได้แก่

- เว็บไซต์ลามกอนาจาร
- เว็บไซต์การพนัน
- เว็บไซต์ที่มีหัวเรื่อง "Free" แม้กระทั่ง Free Wi-Fi ที่เราคิดว่าได้เล่นอินเตอร์เน็ตฟรี แต่อาจเป็นแผนของ Hacker ให้เรามาใช้ระบบ Wi-Fi ก็เป็นได้ ให้คิดเสมอว่า "ไม่มีของฟรีในโลก" หากมีการให้ฟรีก็ต้องของต่างตอบแทน เช่น โฆษณาแฝง เป็นต้น
- เว็บไซต์ที่ให้โหลดโปรแกรม ซึ่งมีการแนบ file พร้อมทำงานในเครื่องคอมพิวเตอร์ ได้แก่ ไฟล์นามสกุล .exe .dll .vbs เป็นต้น
- เว็บไซต์ที่แจก Serial Number เพื่อใช้ crack โปรแกรม
- เว็บไซต์ที่ให้ download เครื่องมือในการเจาะระบบ (Hacking Tools)
- เว็บไซต์ที่เกี่ยวข้องกับยาเสพติด
- เว็บไซต์ที่มี Link ไม่ตรงกับชื่อ โดย Redirect ไปอีกหน้าเพจหนึ่งที่ชื่อไม่ตรงกับ domain ที่ต้องการใช้งาน
- เว็บไซต์ที่มีหน้าต่าง pop-up ขึ้นหลายเพจ
- เว็บไซต์ที่มีชื่อ domain ยาวและมีเครื่องหมายมากเกินปกติ ไม่ใช่ชื่อที่เหมาะแก่การตั้ง เช่น www.abc-xyz-xxx.com มีเครื่องหมาย "-" มากเกินไป
- เว็บที่ทำตัวเองเป็น Proxy อนุญาตให้เราใช้งานแบบไม่ระบุชื่อ (anonymous) เนื่องจากผู้ใช้ Free proxy มักประมาทและคิดถึงแต่ผลประโยชน์ จนลืมคิดไปว่าการได้ IP Address ปลอม จากการใช้ Anonymous Proxy อาจจะถูกสร้างมาเพื่อดักข้อมูลของเราเสียเองก็ได้

ทั้งหมดที่ กล่าวมานั้นเป็นข้อสังเกตเว็บไซต์เสี่ยงภัย หากหลีกเลี่ยงการเข้าเว็บที่มีลักษณะดังกล่าวไม่ได้ ก็ควรตั้งสติรอบคอบ และระมัดระวังในการใช้งานเว็บไซต์ข้างต้นเป็นพิเศษ

7. สังเกตความปลอดภัยของเว็บไซต์ที่ให้บริการธุรกรรมออนไลน์ เว็บไซต์ e-Commerce ที่ปลอดภัยควรมีลักษณะดังนี้

- มีการทำ HTTPS เนื่องจาก HTTPS จะมีการเข้ารหัสข้อมูล เพื่อป้องกันการดัก User name และ Password ในเวลาที่เราทำการ Login เข้าใช้บริการ e-commerce
- มีใบรับรองทางอิเล็กทรอนิกส์ (Certificate Authority : CA) เพื่อช่วยในการยืนยันตัวบุคคลและรักษาความปลอดภัยในการรับส่งข้อมูลผ่านระบบอินเทอร์เน็ตที่ใช้บนเครื่องให้บริการนั้น
- มีมาตรฐาน (Compliance) รองรับ เช่น ผ่านมาตรฐาน PCI/DSS สำหรับเว็บไซต์ E-commerce เป็นต้น

8. ไม่เปิดเผยข้อมูลส่วนตัวลงบนเว็บ Social Network ชื่อที่ใช้ควรเป็นชื่อเล่นหรือฉายาที่กลุ่มเพื่อนรู้จัก และไม่ควรเปิดเผยข้อมูลดังต่อไปนี้

- เลขที่บัตรประชาชน
- เบอร์โทรศัพท์ส่วนตัว
- หมายเลขบัตรเครดิต
- หมายเลขหนังสือเดินทาง
- ข้อมูลทางการแพทย์
- ประวัติการทำงาน

หากจำเป็นต้องกรอกข้อมูลดังกล่าว ให้สังเกตว่าเว็บไซต์นั้นน่าเชื่อถือหรือไม่ พิจารณาจากเนื้อหาในเว็บไซต์ที่ควรบ่งบอกความตั้งใจในการให้บริการ และควรเป็นเว็บไซต์ที่รู้จักกันแพร่หลาย เพื่อหลีกเลี่ยงปัญหาถูกดักข้อมูลส่วนตัวจากการสร้างเว็บไซต์หลอกลวง (Phishing) และป้องกันข้อมูลปรากฏในระบบค้นหา (Search Engine) ที่ตนเองไม่ประสงค์จะให้สาธารณชนได้รับรู้

9. ศึกษาถึงข้อกฎหมายเกี่ยวกับการใช้สื่ออินเตอร์เน็ต ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยมีหลักการง่ายๆ ที่จะช่วยให้สังคมออนไลน์สงบสุข คือ ***ให้คิดถึงใจเขาใจเรา*** หากเราไม่ชอบสิ่งใด ก็ไม่ควรทำสิ่งนั้นกับผู้อื่นเวลาแสดง ความคิดเห็นบนกระดาน แสดงความคิด เห็น (Web board), การรับส่ง e-mail, หรือการกระทำใดๆ กับข้อมูลบน อินเตอร์เน็ต

10. ไม่หลงเชื่อโดยง่าย อย่าเชื่อในสิ่งที่เห็น และงมงายกับข้อมูลบนอินเตอร์เน็ตควรหมั่นศึกษาหาความรู้จาก เทคโนโลยีอินเตอร์เน็ต และศึกษาข้อมูลให้รอบด้าน ก่อนปักใจเชื่อในสิ่งที่ได้รับรู้

10 วิธีข้างต้นถือเป็นคาถาสำหรับนักท่องเน็ต เพื่อเพิ่มความระมัดระวังในการใช้งานอินเตอร์เน็ตให้มากขึ้น เพราะภัยคุกคามจากการใช้อินเตอร์เน็ตมักเกิดจากพฤติกรรมการใช้งานของเราเอง การมีชุดซอฟต์แวร์ป้องกันในเครื่องมิใช่คำตอบสุดท้าย ความปลอดภัยจะเกิดขึ้นได้ล้วนแล้วแต่พึ่งพาสติและความรู้เท่าทันของเราเอง

ระลึกไว้เสมอว่า **ความมั่นคงปลอดภัยข้อมูลจะเกิดขึ้นได้ ต้องเริ่มต้นจากตัวเองเสียก่อน** หากผู้ใช้งานปลอดภัยระบบเครือข่ายภายในองค์กรนั้นก็จะปลอดภัย เครือข่ายองค์กรอื่นๆ ที่มาร่วมใช้งานระบบก็ปลอดภัย เกิดเป็นห่วงโซ่แห่งความปลอดภัยจาก ระดับเล็กสู่ระดับใหญ่ ไปถึงระดับชาติ ช่วยให้ประเทศของเราปลอดภัยจากการใช้ระบบสารสนเทศได้

จากแนวโน้มที่เพิ่มสูงขึ้นของภัยออนไลน์ด้วยวิธีการโจมตีเครื่องแม่ข่าย (Server) ที่มีความสำคัญต่อธุรกิจ เจ้าของกิจการส่วนใหญ่ โดยเฉพาะที่มีการทำธุรกรรมออนไลน์ (E-Commerce) จึงจำเป็นต้องปกป้องเครื่องแม่ข่ายของตนให้ปลอดภัยจากการโจมตีโดยผู้ไม่ประสงค์ดี ที่อาจบุกรุกเข้ามาขโมยข้อมูลชั้นความลับ, การบิดเบือนข้อมูล, การทำให้เครื่องแม่ข่ายไม่สามารถใช้งานได้ตามปกติ หรือทำให้ธุรกิจออนไลน์ต้องหยุดชะงัก สร้างความเสียหายและส่งผลกระทบต่อรายได้

SRAN จึงเปิดให้บริการรูปแบบใหม่ ซึ่งเหมาะสำหรับหน่วยงานที่ต้องการความปลอดภัยข้อมูลสารสนเทศในระดับสูง ได้แก่ ผู้ให้บริการ ISP, ผู้ให้บริการ Co-location, ผู้ให้บริการ Web Hosting, ผู้ให้บริการ Mail Server, Database Server, Game Server, P2P Server ตลอดจนบริษัทที่ติดตั้ง Web Server ที่ IDC เป็นต้น รายละเอียดดังนี้

สำหรับ**ลูกค้าที่ใช้บริการ SRAN IT Forensic Service** จะได้รับ
ส่วนลดพิเศษเมื่อรับบริการ SRAN Anti-Hacking Service
สนใจบริการติดต่อ โทร. 02-982-5445 หรือ info@gbtech.co.th

Message from SRAN

SRAN Anti-Hacking & IT Forensic Services

SRAN Anti-Hacking Service บริการป้องกันภัยคุกคามทางอินเตอร์เน็ตสำหรับ Server ที่มีความสำคัญต่อธุรกิจ โดยมีขอบเขตการให้บริการดังนี้

- ป้องกันภัยคุกคามระบบ E-Commerce โดยรับประกันว่าเครื่องแม่ข่ายที่สำคัญต่อธุรกิจจะไม่ถูกโจมตี ได้แก่ Web Server, Game Server, Mail Server, File Sharing Server, IM Server, Database Server, P2P Server เป็นต้น
- ออกแบบการสร้างระบบให้มีความมั่นคงปลอดภัย
- แจ้งเตือนหากมีภัยคุกคามรุนแรง ที่เกิดขึ้นกับ Server ที่ใช้บริการ เช่น DDoS/DoS, Web Application Hacking, Sniffer, Remote Exploit, Virus/Worm Attack, Backdoor/Trojan Horse Attack, Spoof IP Attack, Brute Force Password Attack เป็นต้น
- เก็บบันทึก Log พร้อมระบบ Data Archive เพื่อให้สอดคล้องตาม พ.ร.บ. คอมพ์ฯ
- ออกรายงานผล

  - ขนาด Bandwidth การใช้งานของ Server ที่สำคัญต่อธุรกิจ
  - ภัยคุกคามที่มีผลกระทบต่อ Server เป็นรายวัน
  - สถิติ IP รายวันที่เข้าถึง Server ที่สำคัญต่อธุรกิจ
  - รายงานผลเกี่ยวข้องกับฐานความผิดตาม พ.ร.บ. คอมพ์ฯ เป็นรายวัน

ประเมินความเสี่ยง Server เดือนละ 1 ครั้งพร้อมออกรายงาน

SRAN IT Forensic Service บริการสืบหาผู้กระทำความผิดทางอินเตอร์เน็ตและคอมพิวเตอร์ สำหรับลูกค้าที่ถูกโจมตีระบบแล้ว และต้องการผลลัพธ์ที่รวดเร็วในการสืบหาผู้กระทำความผิด รับรองผลภายใน 14 วัน (ไม่คิดค่าบริการหากหาร่องรอยการกระทำผิดไม่พบ) โดยมีขอบเขตการให้บริการดังนี้

- สืบหาผู้กระทำความผิดด้วยเครื่องมือที่ทันสมัย ด้วยกระบวนการแบบมืออาชีพ
- วิเคราะห์ผลจากผลลัพธ์การสืบสวนสอบสวน โดยทีมงานผู้เชี่ยวชาญและสามารถประสานงานกับพนักงานเจ้าหน้าที่ ตามที่ประกาศในพ.ร.บ.คอมพ์ฯ, เจ้าหน้าที่ตำรวจ, สำนักข่าวกรอง, DSI และเจ้าหน้าที่ ฝ่ายงานด้านความมั่นคง
- ออกรายงานผลสรุปการทำงาน พร้อมลำดับเหตุการณ์และความสำคัญของเหตุการณ์ เชื่อมโยงโดยใช้เครื่องมือที่ทันสมัย เพื่อใช้เป็นประโยชน์ต่อรูปคดี และการสืบสวนสอบสวนของเจ้าหน้าที่ตำรวจ และสามารถใช้ประกอบในชั้นศาลได้

FAQ for SRAN Security Center

Q: เวลาในเครื่อง SRAN ไม่ตรงตามเวลามาตรฐาน ต้องทำอย่างไร?

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

A: ให้ตรวจสอบที่หน้า Management –> System –> Time Setting

- ในช่อง NTP Server ให้ใส่ "time1.nimt.or.th time.navy.mi.th" แล้วกด Update Now
- แต่ถ้าภายในองค์กรมี Time Server แล้วในช่อง NTP Server ให้ใส่เป็น IP ของ Time Server ภายในองค์กรแทน
- ทดสอบเปลี่ยนค่าวัน เดือน ปี และเวลาในช่องบรรทัด Enter New Time แล้วกด Update Time หลังจากนั้นสังเกตจากบรรทัดบนค่าของวัน เดือน ปี และเวลาจะเปลี่ยนไปตามที่ Set ไว้ (ถ้าเวลาไม่เปลี่ยน อาจเกิดจากปัญหาที่ตัวอุปกรณ์) ต่อไปที่บรรทัด NTP Server ให้กรอกค่าตามที่กำหนดแล้วกด Update Now
- ถ้ายังไม่ได้อีกแสดงว่าเครื่อง SRAN ไม่สามารถต่อออก Internet ได้ ทำให้เวลาไม่สามารถไป Sync กับ Server ภายนอกได้ ซึ่งวิธีตรวจสอบว่า SRAN ออก Internet ได้หรือไม่ คือเข้าไปที่ Management –> License จะต้องแสดงช่องให้ใส่ License Key ถ้าใช่แสดงว่า SRAN สามารถออก Internet ได้