SRAN e-Newsletter

จดหมายข่าวออนไลน์ เพื่อความปลอดภัยทางข้อมูลสารสนเทศ ปีที่ 1 ฉบับที่ 2 ประจำเดือน มีนาคม 2552

Editor's talk

สวัสดีค่ะคุณผู้อ่านทุกท่าน

SRAN e-Newsletter ฉบับนี้มาพร้อมเนื้อหาเกี่ยวกับเว็บไซต์ที่ไม่เหมาะสม ซึ่งถือเป็นประเด็นร้อนระดับประเทศในช่วงที่ผ่านมา เว็บไซต์ถือเป็นเครื่องมือสื่อสารทันสมัยในโลกดิจิตอลทุกวันนี้ เปิดประเด็นด้วยคำถามสะกิดใจ *"มีบ้างไหม ที่ท่องโลกอินเตอร์เน็ต โดยไม่เปิดเว็บไซต์?"* สถิติจากสำนักบริการเทคโนโลยีสารสนเทศภาครัฐ (สบทร.) เผยว่าจำนวนเครื่องที่เข้าเยี่ยมชมเว็บไซต์ (ณ วันที่ 18 ก.พ. 52) มีทั้งสิ้น 4,008,728 เครื่อง เว็บไซต์จึงถือเป็นหัวใจของการท่องเน็ต ทว่า เราจะกรองเว็บไซต์ไม่เหมาะสมออกจากเว็บไซต์ทั่วไปได้อย่างไร?

ลองมาดูคำเฉลยกันค่ะ

กฤตยา รามโกมุท
บรรณาธิการ

เทคนิค การเฝ้าระวังภัยเว็บไซต์

WWW เฝ้าระวังภัย ! เว็บไซต์ที่ไม่เหมาะสม

เกณฑ์การประเมินเว็บไซต์คงไม่มีรูปแบบแน่นอนตายตัว ว่าเว็บไซต์ใดเหมาะสม/ไม่เหมาะสม ขึ้นอยู่กับคุณธรรมและสามัญสำนึกของผู้ใช้งานเป็นสำคัญ ตระหนักคิดด้วยวิจารณญาณว่าเว็บไซต์ที่ไปเยือน ณ เวลานั้นผิดศีลธรรม ประเพณีวัฒนธรรม หรือดูหมิ่นบุคคลอื่นอย่างไม่มีเหตุผลหรือไม่ เป็นเว็บไซต์ที่แฝงภัยคุกคามหรือไม่ ในขณะที่เว็บไซต์ไม่เหมาะสม และภัยคุกคามที่เกิดจากเว็บไซต์นั้นมีสถิติเพิ่มสูงขึ้นทุกปีในอัตราปีละ 2 เท่า เพื่อเป็นการกลั่นกรองเว็บไซต์, เฝ้าระวังภัยคุกคามทางเว็บไซต์ และปิดกั้นเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม ทีม SRAN จึงขอนำเสนอแนวทางและเทคนิคให้ได้รับทราบกัน ทั้งในมุมมองระดับองค์กร และระดับผู้ให้บริการอินเตอร์เน็ต

ประเภทของเว็บไซต์ แบ่งได้ดังนี้

- เว็บ Blog
- เว็บบอร์ด
- เว็บที่ใช้ในการ upload/download
- เว็บเผยแพร่วิดีโอ
- เว็บหน่วยงาน/ห้างร้าน/บริษัท
- เว็บซื้อขายสินค้าทางอินเตอร์เน็ต (E-commerce)
- เว็บ Social Network ฯลฯ

Switch Aggregation
WEB FILTERING
URL TRACKING
Web Monitoring Sensor
Web Proxy Caching
NIPS
NIDS
Blacklist domain
SEM
Application Firewall

ประเภทของภัยคุกคามที่เกิดขึ้นบนเว็บไซต์

ประเภทของภัยคุกคามที่เกิดขึ้นบนเว็บไซต์

1. ภัยคุกคามจากเว็บไซต์หลอกลวง ได้แก่ เว็บที่มีการหลอกให้ทำธุรกรรมออนไลน์ เพื่อดักข้อมูลในการกรอกค่า User ID และ Password ซึ่งมักจะตั้งชื่อ URL หรือ Domain name ใกล้เคียงกับเว็บไซต์จริง, เว็บไซต์ที่หลอกให้ผู้ใช้งาน download โปรแกรมไม่พึงประสงค์ ที่มีคุณสมบัติในการดักข้อมูล โดยหลอกให้ผู้ใช้งานตกเป็นเหยื่อของเนื้อหาชวนเชื่อจำพวกยาลดความอ้วน, งานที่ได้รับค่าตอบแทนสูงเกินปกติ, โปรแกรม crack serial no., กลโกงเกมส์ เป็นต้น

2. ภัยคุกคามจากเว็บที่มีเนื้อหาไม่เหมาะสม ได้แก่ เว็บไซต์ลามกอนาจาร, เว็บไซต์พนัน, เว็บข้อมูลขยะ เช่น เว็บบอร์ดที่มี Botnet มาตั้งศูนย์ส่งข้อมูลชวนเชื่อ เช่น โฆษณาขายสินค้า ขายยา ขายบริการต่างๆ, เว็บไซต์ที่มีเนื้อหากระทบความมั่นคง ซึ่งอาจเข้าข่ายหมิ่นสถาบันหลักของชาติ

3. ภัยคุกคามที่เกิดจากเว็บเครือข่ายสังคม ได้แก่ เว็บเกมส์ออนไลน์, เว็บ Social Network เช่น Hi5, Facebook ในส่วนนี้อาจเชื่อมกับภัยคุกคามจากการหลอกลวงในรูปแบบอื่นได้ เช่น การขายบริการทางเพศ, การสอนเสพยาเสพติด ดังที่พบเห็นเป็นข่าวเมื่อเร็วๆ นี้

ประโยชน์ของการเฝ้าระวังภัยเว็บไซต์ที่ไม่เหมาะสม

<u>ในระดับเครือข่ายทั่วไป</u> เช่น บริษัท ห้างร้าน เครือข่ายขนาดกลาง/เล็ก สามารถปิดกั้นเว็บไซต์ไม่เหมาะสมเพื่อให้พนักงานใช้ช่วงเวลาทำงานให้เกิดประสิทธิภาพสูงสุด และเก็บบันทึกข้อมูลหลักฐานที่สามารถสืบค้นได้ เพื่อเป็นประโยชน์ในการเก็บสถิติและประเมินพฤติกรรมการใช้งานอินเตอร์เน็ตในองค์กร

<u>ในระดับประเทศ หรือในระดับผู้ให้บริการอินเตอร์เน็ต</u> ประโยชน์ที่ได้รับคือหลักฐานประกอบคดี เพื่อใช้สืบหาผู้กระทำความผิด

เทคนิคการจัดการกับเว็บไซต์ที่ไม่เหมาะสม

การดำเนินการแบ่งเป็นสองส่วน คือ การสืบหาเว็บไซต์ที่ไม่เหมาะสม (URL Tracking) แล้วจึงส่งข้อมูลไปยังระบบปิดกั้น (Web Filtering) รายละเอียดดังนี้

1. เทคนิคการทำ URL Tracking สามารถแบ่งออกได้ 3 วิธีหลักๆ คือ

1.1 **วิธีรับ Log จากเว็บไซต์นั้นๆ** คล้ายกับเทคนิคเว็บสถิติ ซึ่งจะได้รับข้อมูลที่ละเอียดสามารถตรวจสอบได้ว่าใครเข้าใช้บริการที่หน้าเพจใด เมื่อใด ใช้ระบบอะไรเพื่อเรียกใช้บริการ รวมถึงมาจากเว็บไซต์ หรือเว็บค้นหาใด ด้วยคำค้นหาอะไร เป็นต้น โดยรวมวิธีการนี้เป็นวิธีที่ดี ติดตรงที่จะสามารถดู URL Tracking ได้ก็ต่อเมื่อเจ้าของเว็บไซต์นั้นๆ ต้องให้ความร่วมมือติด Script ในแต่ละหน้าเพจ บนเว็บไซต์

1.2 **วิธีติดตั้งระบบ Caching หรือระบบ Web Proxy Caching** เป็นการติดตั้งในระดับเครือข่ายคอมพิวเตอร์ (Network) ซึ่งเป็นที่นิยมในระดับองค์กร แต่ไม่เหมาะกับการติดตั้งในระดับประเทศหรือระดับผู้ให้บริการอินเตอร์เน็ต ข้อดีของวิธีนี้คือ ทำให้การเปิดเว็บซ้ำเดิมทำได้เร็วขึ้น เพราะมีข้อมูลใน Caching สามารถสืบค้นข้อมูลได้ แต่การติดตั้งระบบนี้ส่งผลกระทบกับระบบเครือข่ายหลักและเครือข่ายเดิม ทำให้เกิดความล่าช้า จึงต้องออกแบบเป็นอย่างดี ตลอดจนค่าใช้จ่ายที่ค่อนข้างสูง

1.3 **วิธีเฝ้าระวังด้วยอุปกรณ์ตรวจจับผู้บุกรุก** เป็นวิธีที่ส่งผลกระทบกับเครือข่ายเดิมน้อยที่สุด โดยนำระบบ Network Intrusion Detection มาประยุกต์ใช้ สำหรับองค์กรทั่วไปทำได้โดยติดตั้งที่ Switch ที่ทำการ Mirror port ได้ หรือใช้อุปกรณ์ TAP ส่วนระดับผู้ให้บริการอินเตอร์เน็ตนั้น ทำโดยติดตั้งตามโหนดต่างๆ แล้วอาศัย Switch Aggregation ทำการกระจายโหลดไปยังอุปกรณ์เฝ้าระวังภัย ซึ่งได้ผลใกล้เคียงกับวิธีติดตั้งระบบ Caching โดยที่งบประมาณในการลงทุนต่ำกว่ามาก

2. เทคนิคการปิดกั้นเว็บไซต์ (Web Filtering) แบ่งออกเป็น 3 วิธี คือ

2.1 **ปิดกั้น Domain ทั้งหมด** เทคนิคนี้ซับซ้อนน้อยที่สุด ทำได้สะดวก และได้รับผลกระทบค่อนข้างน้อย แต่ในมุมของผู้ใช้งานแล้วไม่ใคร่พอใจนัก เช่นเดียวกับกรณี Block ทั้ง domain ของเว็บ www.youtube.com ซึ่งได้เสียงตอบรับกลับมาในแง่ลบมากกว่าบวก

2. เทคนิคการปิดกั้นเว็บไซต์ (Web Filtering)

2.2 ปิดกั้น URL ส่วนนี้ต้องอาศัยการติดตั้งเทคโนโลยีเสริม ซึ่งอาจแบ่งเทคนิคได้ดังนี้

a) ระบบ Web Proxy Caching ที่สามารถตั้ง Rule Base ในการใส่ค่า Blacklist URL ที่ไม่เหมาะสมลงไปได้ ซึ่งส่วนใหญ่ต้องออกแบบให้เหมาะสม เช่น ต้องติดตั้งแบบ Transparent mode หรือ in-line mode และส่วนใหญ่ต้องอาศัยซอฟต์แวร์เสริมในการปิดกั้นเว็บไซต์ในระดับ URL

b) ระบบ Firewall ที่เป็นระดับ Application Firewall โดยทั่วไปติดตั้งเป็น Gateway หลัก เทคนิคนี้ก็สามารถป้องกัน URL ที่ไม่เหมาะสมได้

c) ระบบ Network Intrusion Prevention System (NIPS) ส่วนนี้สามารถปิดกั้น URL ที่ไม่เหมาะสม และลงลึกถึงระดับเนื้อหาใน URL โดยปิดกั้นเนื้อหาบนเว็บไซต์ที่ผู้ใช้งานเรียกใช้ได้ ซึ่งถือเป็นเทคนิคที่ละเอียดที่สุด แต่มีผลกระทบต่อระบบเครือข่ายและบางครั้งอาจเกิดความเข้าใจผิดในเนื้อหา อย่างไรก็ดีเทคนิคนี้ต้องอาศัย "คน" ในการวิเคราะห์และสั่งปิดกั้น URL

d) ระบบ TCP Hijack เป็นการ Hijack session ในการเรียกเปิดเว็บไซต์จากผู้ใช้บริการ ซึ่งสามารถปิดกั้น Blacklist URL ที่มีในฐานข้อมูลได้

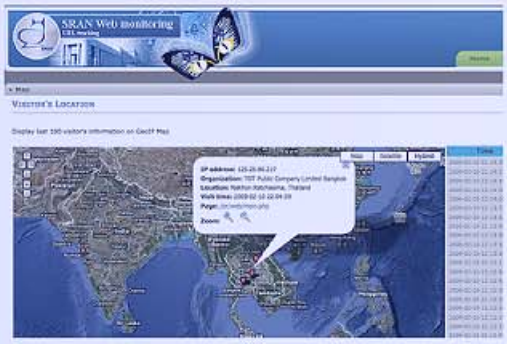
2.3 ปิดกั้นเนื้อหาบนเว็บไซต์ที่ไม่เหมาะสม แบ่งได้ 2 แบบดังนี้

a) ปิดกั้นได้เองโดยไม่ต้องพึ่งพาเทคโนโลยีอื่น มีเทคนิคเดียวคือต้องใช้ NIPS ซึ่งเทคนิคนี้หากตั้ง Blacklist ไว้จำนวนมากอาจส่งผลให้เกิดคอขวดในระบบเครือข่ายได้ แต่สำหรับหน่วยงาน/องค์กรขนาดกลางและเล็ก สามารถใช้เทคนิคนี้ได้ โดยไม่เกิดผลกระทบมากนัก

b) ปิดกั้นได้แต่ต้องอาศัยเทคโนโลยีอื่น เช่น ใช้ระบบ Web Proxy Caching ซึ่งต้องอาศัยการส่งข้อมูลไปวิเคราะห์ที่ระบบ Syslog Server ที่ทำการเปรียบเทียบเหตุการณ์เชิงวิเคราะห์ (Correlation Event) ได้ โดยทั่วไปเรียกระบบนี้ว่า SEM (Security Event Management) ซึ่งจะปิดกั้นได้ก็ต่อเมื่อจุดติดตั้ง Web Proxy Caching นั้นต้องเป็นการติดตั้งแบบ in-line หรือ Transparent เท่านั้น อีกเทคนิคหนึ่งคือใช้ NIDS (Network Intrusion Detection System) ร่วมกับเทคนิค TCP Hijack และอาศัยความสามารถบน Core Switch ในการเลือก Protocol หากตรงกับค่าในฐานข้อมูล ก็ทำการปิดกั้นเนื้อหาในเว็บไซต์นั้นได้ ซึ่งจะสำเร็จผลหรือไม่นั้นขึ้นกับการตั้งค่า NIDS ในการตรวจจับเนื้อหาที่เพิ่มลงไป

บทสรุปในเชิงเทคนิคนั้น งานนี้ไม่ง่ายและไม่สำเร็จรูป ต้องอาศัยทีมงานที่มีความเข้าใจการไหลเวียนข้อมูลบนระบบเครือข่ายเป็นอย่างดี และสามารถปรับแต่งข้อมูลในการตรวจจับได้ ทั้งนี้การปิดกั้นเว็บไซต์ โดยการลงซอฟต์แวร์ในระดับเครื่องคอมพิวเตอร์ผู้ใช้งานนั้น ต้องได้รับการยินยอมและความร่วมมือจากผู้ใช้งานเป็นหลัก ซึ่งกระทำได้ยาก ดังนั้นหากไม่ต้องการให้กระทบกับผู้ใช้งาน และผู้ให้บริการแล้ว ต้องทำบนระบบเครือข่าย (Network) เท่านั้น

ทีมพัฒนา SRAN จึงได้พัฒนาระบบ "Web Monitoring Sensor" ขึ้น เพื่อตรวจการใช้งานเว็บไซต์ในระดับเครือข่ายคอมพิวเตอร์ หากติดตั้งระบบนี้ในระดับเครือข่ายองค์กร ก็สามารถติดตั้งตามทางเข้า-ออกเครือข่าย หรือจุดที่มีการเชื่อมต่ออินเตอร์เน็ต เช่น Core Switch ขององค์กร โดยใช้อุปกรณ์เสริมมาช่วย เช่น Switch mirror port หรือ อุปกรณ์ TAP ในระดับเครือข่ายผู้ให้บริการ ก็ติดตั้งได้หลายรูปแบบ โดยติดตั้งตามโหนด, Core Switch หลัก, จุดเชื่อมต่อที่ส่งข้อมูลออกไปทาง Router หลัก เป็นต้น



คุณสมบัติเด่นของ SRAN Web Monitoring Sensor

- เปรียบเสมือนกล้องวงจรปิดที่ช่วยเฝ้าระวังการใช้งานอินเตอร์เน็ต/เว็บไซต์
- สืบค้น URL ที่มี keyword ตามที่กำหนดไว้ได้
- รายงานเหตุการณ์ที่ตรวจพบได้แบบ Real Time
- บันทึกข้อมูลที่เกิดขึ้นตาม Chain of Event (ใคร, ทำอะไร, ที่ไหน, เมื่อไร, อย่างไร)
- สามารถค้นหาไอพีต้นทางได้สะดวกรวดเร็ว ทั้งไอพีที่ทำการเปิดเว็บ หรือโพสต์เว็บ
- ระบุชื่อบริษัท/หน่วยงาน, ตำแหน่งที่ตั้ง และชื่อเมือง รวมถึง URL ปลายทางได้
- เรียกดูข้อมูลประวัติการใช้งานไอพีที่ต้องสงสัยได้
- ใช้ได้กับทั้งเครือข่ายระดับผู้ให้บริการอินเตอร์เน็ต และเครือข่ายองค์กรทั่วไป