

THNIC แนะนำทุกหน่วยงานตรวจสอบ DNS เตรียมพร้อมรับมือ DNS Flag Day วันที่ 1 ก.พ. 2562



มูลนิธิศูนย์สารสนเทศเครือข่ายไทย (THNIC Foundation) เผยวันที่ 1 ก.พ. 2562 จะเกิดการเปลี่ยนแปลงครั้งใหญ่หรือ DNS Flag Day ในกลุ่มผู้พัฒนาซอฟต์แวร์ DNS และเป็นที่ยกย่องว่าอินเทอร์เน็ตในวันนั้นอาจเกิดติดขัดจนกระทบการใช้งานได้ ทั้งนี้มูลนิธิสารสนเทศเครือข่ายไทย และภาควิชาวิศวกรรมคอมพิวเตอร์ ม.เกษตรศาสตร์ได้ร่วมกันตรวจสอบโดเมนในประเทศไทยทั้งหมดจำนวน 69,938 โดเมน พบว่ามีโดเมนที่อาจได้รับผลกระทบมากกว่า 10,000 โดเมน หรือราว 15% ของโดเมน .TH ในประเทศไทย หน่วยงานเหล่านี้ยังคงมีเวลาแก้ไขปัญหายู่อีกระยะหนึ่ง ก่อนที่จะถึงเส้นตาย 1 ก.พ. 2562 และผู้บริหารไอทีควรเตรียมการให้ความรู้เจ้าหน้าที่กลุ่ม Help Desk และ Call Center ไว้ด้วย เพราะเมื่อถึงวันดังกล่าว ผู้ใช้อาจโทรแจ้งปัญหาซึ่งอาจขึ้นเพราะ DNS ของหน่วยงานอื่นที่ไม่ได้มาตรฐานก็จะส่งผลกระทบต่อตามมาด้วย

รศ. สุรศักดิ์ สงวนพงษ์ รองศาสตราจารย์ประจำภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ และกรรมการมูลนิธิศูนย์สารสนเทศเครือข่ายไทย (THNIC Foundation) เปิดเผยว่า ระบบชื่อโดเมนหรือ DNS (Domain Name System) เป็นบริการพื้นฐานที่สำคัญมากในอินเทอร์เน็ต หากไม่มี DNS แล้ว บริการเว็บ อีเมล คลาวด์ ที่เราใช้อยู่ทุกวันนี้ก็แทบจะทำงานไม่ได้เลย

ตั้งแต่วันที่ 1 ก.พ. 2562 นี้เป็นต้นไป ผู้พัฒนาซอฟต์แวร์ DNS หลักรายใหญ่ เช่น BIND, Knot, NSD, PowerDNS ตกลงที่จะบังคับใช้มาตรการเด็ดขาด โดยจะถอนรหัสซอฟต์แวร์ที่ใช้แก้ไขปัญหาเฉพาะหน้าแบบขัดตาทัพที่ใช้อยู่เดิมออกไป หรืออีกนัยหนึ่งก็คือ การประกาศว่าซอฟต์แวร์ DNS ของแต่ละหน่วยงานในอินเทอร์เน็ตจะต้องได้มาตรฐาน EDNS (Extension Mechanism for DNS) ที่ถูกต้องครบถ้วนเท่านั้น ดังนั้น DNS ของหน่วยงานใดๆที่มี “สุขภาวะ” ไม่ได้มาตรฐาน จะเกิดความเสี่ยงที่ผู้ใช้บริการภายนอกจะเข้าใช้เซิร์ฟเวอร์ได้ล่าช้า ติดขัด หรือเข้าไม่ได้เลย ดังนั้นหน่วยงานจึงควรตรวจสอบ DNS และปรับแก้หากพบปัญหา

สรุปเหตุการณ์ที่จะเกิดในวันที่ 1 ก.พ. 2562

ซอฟต์แวร์ DNS หลักคือ BIND, Knot, Unbound, และ PowerDNS จะออกรุ่นปรับปรุง โดยยกเลิกรหัสแก้ไขปัญหา EDNS เฉพาะกิจออกไป

ผู้ให้บริการ DNS สาธารณะเช่น Google, Quad 9, Cloudflare จะเริ่มให้บริการ DNS ตามมาตรฐาน EDNS หน่วยงานซึ่งมี DNS ที่ไม่ได้มาตรฐาน EDNS ผู้ใช้ภายนอกอาจเข้าใช้บริการไม่ได้

หน่วยงานซึ่งมี DNS ที่ได้มาตรฐาน EDNS แล้ว ผู้ใช้ภายในอาจใช้บริการบางเซิร์ฟเวอร์ข้างนอกไม่ได้ เพราะ DNS ปลายทางไม่ได้มาตรฐาน EDNS

รู้จักกับ DNS และความสำคัญ

DNS ทำหน้าที่เป็นเสมือนสมุดหน้าเหลืองประจำอินเทอร์เน็ต ช่วยให้ไม่ต้องจดจำไอพีแอดเดรสเครื่องที่ต้องการติดต่อ เหมือนกับที่เราใช้สมาร์ตโฟนแล้วโทรออกด้วยชื่อโดยไม่ต้องจำเบอร์โทร แต่สำหรับอินเทอร์เน็ตแล้วการจดไอพีแอดเดรสเก็บไว้เองทำได้ยากเพราะมีเครื่องที่อาจต้องใช้บริการมากมาย และหมายเลขอาจเปลี่ยนได้ตลอด เครือข่ายในอินเทอร์เน็ตจึงต่างมีสมุดหน้าเหลืองประจำตัว แต่ละแห่งจะมี DNS ใช้แลกเปลี่ยนข้อมูลข้ามระบบกัน

DNS เป็นระบบที่พัฒนาขึ้นมาแล้วกว่า 35 ปีผู้พัฒนาได้ขยายความสามารถใหม่ๆเพิ่มขึ้นอีกหลายอย่าง ในปี พ.ศ. 2542 ได้กำหนดให้ส่วนขยายนี้เป็นมาตรฐานเรียกว่า EDNS (Extension Mechanism for DNS) ตัวอย่างเช่น การใช้คุกกี้เพื่อลดปัญหาการโจมตี การเข้ารหัสยืนยันตัวตนเซิร์ฟเวอร์ด้วย DNSSEC หรือการเพิ่มขนาดข้อมูลให้ส่งคราวเดียวได้ใหญ่ขึ้นจากเดิมจำกัดเพียง 512 ไบต์ เป็นต้น

ปัจจุบันมีผู้พัฒนาซอฟต์แวร์ DNS อยู่หลายราย แต่บางรายไม่ได้ทำให้ซอฟต์แวร์ของตนได้มาตรฐาน EDNS อย่างถูกต้องครบถ้วน ผู้พัฒนา DNS รายหลักต่างก็ต้องช่วยปรับแก้ความไม่เข้ากันแบบเฉพาะหน้าไปก่อน โดยที่เซิร์ฟเวอร์ DNS จะมีกลไกวิเคราะห์ปัญหาและพยายามแก้ไขตามสภาพการณ์ให้ลุล่วงแบบอัตโนมัติ ในมุมหนึ่งก็นับเป็นเรื่องที่ดีสำหรับผู้ใช้ แต่ก็กลายเป็นว่า DNS ฝ่ายหนึ่งต้องคอยรับภาระแก้ปัญหาให้ DNS อีกฝ่ายหนึ่งที่ไม่ยอมทำตามกฎกติกา และเกิดความล่าช้าเป็นผลกระทบตามมา ในที่สุดผู้พัฒนาซอฟต์แวร์ DNS กลุ่มหลักจึงตกลงกันว่า 1 กุมภาพันธ์ 2562 จะเป็นวัน DNS Flag Day หรือวันยกธงประกาศเจตจำนงให้ทั้งหมดเข้าสู่มาตรฐาน

บริการตรวจสอบ EDNS

เว็บไซต์ EDNS Compliance (<https://ednscomp.isc.org/ednscomp>) ใ้บริการออนไลน์ตรวจสอบว่า DNS ทำงานได้มาตรฐาน EDNS หรือไม่ โดยป้อนชื่อโดเมนของหน่วยงานที่ต้องการตรวจสอบในช่อง Zone Name ตัวอย่างเช่น ตรวจสอบโดเมน facebook.com จะพบรายงานว่า DNS ของ facebook ทำงานได้ตามข้อกำหนด (สังเกต รายงาน All Ok)

แต่เมื่อทดลองป้อนโดเมน mytcas.com จะพบรายงานปัญหาเนื่องจากเซิร์ฟเวอร์ DNS ทั้งสองตัวที่ดูแลโดเมน mytcas.com คือ ns1.domain.com และ ns2.domain.com. ยังไม่ได้มาตรฐาน EDNS บางส่วน

ผู้ให้บริการอินเทอร์เน็ตในประเทศไทยรวมทั้งหน่วยงานที่มีชื่อโดเมนทั้งที่จดทะเบียนภายใต้ .TH และชื่ออื่นๆ ล้วนอยู่ในข่ายที่ต้องตรวจสอบ DNS ของตนเองเพื่อปรับแก้หากพบปัญหา ปัญหาที่ตรวจพบมักเกิดขึ้นจากสาเหตุหลัก 2 ประการคือ 1) ใช้ซอฟต์แวร์รุ่นเก่าหรือปรับตั้งซอฟต์แวร์ไม่ถูกต้อง และ 2) ปรับตั้งไฟร์วอลล์ไม่ถูกต้อง หากพบปัญหา ผู้ดูแลระบบมีหน้าที่แก้ไขโดยปรับปรุงซอฟต์แวร์ DNS ให้เป็นรุ่นล่าสุดและปรับตั้งค่าให้ถูกต้องเป็นลำดับ

แรก หากยังพบปัญหาอยู่ให้ตรวจสอบและปรับตั้งไฟร์วอลล์เป็นลำดับถัดไป ไฟร์วอลล์ต้องไม่ปิดกั้นบริการ EDNS และต้องอนุญาตให้ยูดีพีแพ็กเก็ตสำหรับ DNS ซึ่งมีขนาดเกิน 512 ไบต์ผ่านเข้าออกได้

เอกสารอ่านเพิ่มเติม

1. DNS flag Day, <http://dnsflagday.net>
2. Extension Mechanisms for DNS (EDNS0), <https://www.ietf.org/rfc/rfc2671.txt>

เกี่ยวกับมูลนิธิศูนย์สารสนเทศเครือข่ายไทย

มูลนิธิศูนย์สารสนเทศเครือข่ายไทย (Thai Network Information Center Foundation หรือ THNIC Foundation) เป็นองค์กรไม่แสวงผลกำไรที่มุ่งเน้นการพัฒนาการใช้งานอินเทอร์เน็ตและโครงสร้างพื้นฐานอินเทอร์เน็ตในประเทศไทย ก่อตั้งขึ้นเมื่อปี 2550 โดยมีเป้าหมายหลักเพื่อส่งเสริมการใช้งานโดเมน “.TH” และ “.ไทย” สนับสนุนการศึกษา การวิจัย และการพัฒนาเพื่อส่งเสริมความรู้เกี่ยวกับเทคโนโลยีอินเทอร์เน็ต สำหรับข้อมูลเพิ่มเติม กรุณาติดต่อ: ดร. พจนันท์ รัตนไชยพันธ์

มูลนิธิศูนย์สารสนเทศเครือข่ายไทย (THNIC Foundation)

159 ถนนพิชัย แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพฯ 10300

photchanan@thnic.or.th