เรียน ผอ.สำนัก/กอง, ผอ.สปข.๑-๘, ประชาสัมพันธ์จังหวัด

เมื่อวันที่ ๑๑ ก.พ.๕๘ เว็บไซต์ สนข. (thainews.prdgo.th) ได้ถูกผู้ไม่ประสงค์ดี (Hacker) ทำการแก้ไขหน้าเพจหลัก (Web Defacement) ทำให้เกิดความเสียหายกับข้อมูลในหน้าหลัก ตามรายละเอียดข้างต้น ดังนั้น อปส. จึงสั่งการให้หน่วยงานภายใน กปส. ที่พัฒนาระบบขึ้นเอง, เช่าบริการเว็บไซต์ เพื่อการให้บริการข้อมูลข่าวสารผ่านสื่อสารสนเทศ ดำเนินการตรวจสอบระบบความมั่นคงปลอดภัยเพื่อการบริหารความเสี่ยงและป้องกันการโจมตีจากผู้ไม่หวังดีในลักษณะเดียวกัน

จึงเรียนมาเพื่อโปรดดำเนินการตามที่ อปส. สั่งการ จะขอบคุณยิ่ง

(นายนรกิจ ศรัทธา)
ผอ.ศสช.

๑๑ ก.พ. ๒๕๕๘

ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ ฝบห. โทร. ๐-๒๖๑๘-๒๓๒๓ ต่อ ๑๐๑๕

ที่ นร ๐๒๐๖.๐๑/ ๗๕ **วันที่** ๑๑ กุมภาพันธ์ ๒๕๕๘

เรื่อง รายงานการแก้ไขปัญหาเว็บไซต์ สนข. โดนโจมตีจากผู้ไม่ประสงค์ดี

เรียน อปส.

ตามที่ อปส. ได้มอบหมายให้ ศสช. เป็นผู้รับผิดชอบประสานงานร่วมกับ สนข. ในการแก้ไขปัญหากรณีเว็บไซต์ สนข. (thainews.prd.go.th) ถูกผู้ไม่ประสงค์ดี (Hacker) เข้าทำการแก้ไขข้อมูลในหน้าหลัก ตามที่ปรากฏในสื่อสังคมออนไลน์ นั้น

ในการนี้ ศสช. ขอสรุปข้อปัญหาและการแก้ไขปัญหาดังนี้

ปัญหา	การแก้ไข
- เว็บไซต์ สนข. ถูกโจมตีด้วยวิธีการของ Website Defacement ซึ่งมีลักษณะวัตถุประสงค์คือ ปรับเปลี่ยนหน้าเว็บไซต์เป้าหมายให้เปลี่ยนไปจากเดิม ซึ่งการโจมตีแบบนี้ หวังผลให้หน่วยงานสูญเสียความน่าเชื่อถือ	- ได้ประสานด้านเทคนิคกับบริษัทผู้พัฒนาและหน่วยงาน thaicert (Thailand Computer Emergncy Response team) ซึ่งอยู่ภายใต้กระทรวง ICT เพื่อเร่งดำเนินการตรวจสอบแก้ไขแล้ว โดยกปส. จะเร่งส่งข้อมูลจราจรทางคอมพิวเตอร์ (logfile) ให้ thaicert เพื่อทำการตรวจสอบ
- ลักษณะข้อมูลที่เกิดความเสียหาย	- จากการตรวจสอบเบื้องต้น ถูกโจมตีจากกลุ่ม INDONESIAN CYBER CRASHยังไม่พบข้อมูลที่ถูกลักลอบนำออกไป แต่มีลักษณะความเสียหายเกิดขึ้น คือ Hacker ได้ทำการเพิ่มผู้ใช้เข้าในระบบและแทรกข้อมูลในหน้าเว็บไซต์หลัก
- ลักษณะการให้บริการแบบ two-way ในปัจจุบันซึ่งค่อนข้างล่อแหลมต่อการโดนโจมตี	- ได้ดำเนินการปิดพอร์ตที่ไม่จำเป็น ลบการให้บริการเสริมอื่น และเพิ่มความเข้มงวดในการเข้าใช้งาน เพิ่มการคัดกรองการส่งข้อมูลเข้าจะรับเฉพาะ IP Address ภายในประเทศเท่านั้น
- เนื่องจากระบบการให้บริการจัดวางอยู่ที่ CAT INTERNET Datacenter จำเป็นต้องเปิดทางเข้าบริหารจัดการระบบแบบ Remote	- ปิดการให้บริการดังกล่าวทุกระบบ เจ้าหน้าที่ต้องเข้าไปที่ Internet Datacenter เท่านั้น

ทั้งนี้ ศสช. ได้ประสานงานไปที่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) แล้วเมื่อเวลา ๑๑.๐๐ น. พร้อมได้รับคำแนะนำและแนวทางในการตรวจสอบแก้ไขในระยะเร่งด่วน ดังนั้น เพื่อให้การดำเนินการดังกล่าว เกิดความรวดเร็ว และมีประสิทธิภาพเห็นควรสั่งการดังนี้

๑. มอบให้ สนข. จัดเก็บและรวบรวมข้อมูลการจราจรทางคอมพิวเตอร์ (logfile) ของระบบที่เกี่ยวข้องทั้งหมด และจัดส่งให้ thaicert โดยด่วนที่ report@thaicert.or.th หรือ ๐-๒๑๒๓-๑๒๑๒ เพื่อทำการวิเคราะห์และตรวจสอบ

๒. มอบให้ สนข. ประสานกับผู้พัฒนาระบบในการวิเคราะห์ตรวจสอบช่องโหว่ของระบบในปัจจุบันให้มีความเข้มงวดและรัดกุมขึ้น

๓. มอบให้หน่วยงานภายใน กปส. ที่มีและใช้ระบบการให้บริการข้อมูลข่าวสารผ่านสื่อสารสนเทศ ดำเนินการตรวจสอบระบบความมั่นคงปลอดภัยเพื่อการบริหารความเสี่ยงและป้องกันการโจมตี จากผู้ไม่หวังดีในลักษณะเดียวกัน

๔. มอบ กกร. แจ้งความตามกฎหมาย ในกรณี กปส. เป็นผู้เสียหายจากการถูกปลอมแปลงข้อมูลในเว็บไซต์ของ สนข. ซึ่งทำให้เกิดความเสียหายกับหน่วยงาน

จึงเรียนมาเพื่อโปรดพิจารณาสั่งการตามข้อ ๑-๔ ต่อไปด้วย จะขอบพระคุณยิ่ง

(นายนรกิจ ศรัทธา)
ผอ.ศสช.

1. ทราบ
2. ดำเนินการตามที่ ผอ.ศสช. เสนอ ใน 1-4
3. ให้ ศสช. ประสาน Thaicert เพื่อ [illegible]

(นายอภินันท์ จันทรังษี)
อปส.
๑๑ กพ. ๕๘

อปส. (นายอภินันท์ จันทรังษี) 894
๑๑ กพ. ๒๕๕๘