



ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ

ตร.

โทร ๐๒ ๒๐๕ ๒๖๒๘

ที่ ๐๐๓๓.๓๓/๔๗๓๖

วันที่ ๒๗ ธันวาคม ๒๕๕๙

เรื่อง มาตรการในการดำเนินการกรณีเว็บไซต์ของหน่วยถูกกระทำกรณเข้าถึงโดยมิชอบ

เรียน จตช., รอง ผบ.ตร. หรือตำแหน่งเทียบเท่า

ผู้ช่วย ผบ.ตร. หรือตำแหน่งเทียบเท่า

ผบช. หรือตำแหน่งเทียบเท่า

ผบก.ในสังกัด ตร.

ด้วย ตร.มีวิทยุ ด่วนที่สุด ที่ ๐๐๐๗.๒๒/๔๖๓๑ ลง ๒๒ ธ.ค. ๕๙ แจ้งว่าจากเหตุการณ์กรณีมีกลุ่มแฮกเกอร์ ได้ใช้วิธีการทางเทคนิคกระทำกรณเข้าถึงหรือโดยวิธีการอื่นใดโดยมิชอบ ซึ่งระบบคอมพิวเตอร์ของหลายหน่วยงาน โดยเฉพาะหน่วยงานของรัฐที่เกี่ยวข้องกับด้านความมั่นคง ความปลอดภัยในชีวิตและทรัพย์สินของประชาชน ทำให้เกิดความไม่เชื่อมั่นในความปลอดภัยในการใช้งานในระบบซึ่งในส่วนของ ตร.อาจมีหน่วยงานที่ถูกเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ อันเป็นความผิดตามกฎหมายและเพื่อให้เกิดความปลอดภัยในเครือข่ายระบบคอมพิวเตอร์ในส่วนของ ตร. สร้างความเชื่อมั่นให้แก่ผู้ใช้งานในระบบ

เพื่อให้การป้องกันปราบปราม และรับมือกับกลุ่มแฮกเกอร์ดังกล่าวข้างต้นเป็นไปอย่างมีประสิทธิภาพและทันต่อสถานการณ์ ตร.จึงกำหนดมาตรการและแนวทางการรักษาความปลอดภัยของเว็บไซต์ เพื่อระงับยับยั้งความเสียหายที่จะเกิดขึ้นดังนี้

๑. มาตรการป้องกัน

๑.๑ ให้ทุกหน่วยงานในสังกัด ตร. ที่มีระบบคอมพิวเตอร์ขนาดใหญ่ เช่น สพฐ.ตร., สตม., บช.ส. เป็นต้น ประสานกับกลุ่มงานตรวจสอบและควบคุมมาตรฐานการรักษาความปลอดภัย บก.สสท. ดำเนินการตรวจสอบเพื่อให้เป็นไปตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยอย่างเคร่งครัด

๑.๒ ให้สำรองข้อมูลเป็นระยะ อย่างน้อยเดือนละ ๑ ครั้ง

๑.๓ ให้ตรวจสอบและปรับปรุงการตั้งรหัสผ่านสำหรับเข้าถึงระบบคอมพิวเตอร์และอีเมล ให้มีความปลอดภัย โดยมีความยาวของรหัสผ่านไม่น้อยกว่า ๘ ตัว ประกอบไปด้วยตัวเลข ตัวอักษร และอักขระพิเศษ และห้ามมิให้ใช้รหัสผู้ใช้งานกับรหัสผ่านเป็นตัวเดียวกัน โดยรักษารหัสผ่านไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นล่วงรู้

๑.๔ ให้ระมัดระวังการหลอกลวงผ่านทางอีเมล (Phishing) โดยมักจะอ้างว่าส่งมาจากผู้ดูแลระบบ เนื่องจากพื้นที่ในการจัดเก็บเต็ม หรือระบบขัดข้อง เพื่อให้ทำให้เจ้าของอีเมลหลงเชื่อ และส่งมอบรหัสผู้ใช้งานและรหัสผ่าน โดยให้ศึกษาภัยคุกคามรูปแบบใหม่เพิ่มเติมได้ที่เว็บไซต์ www.HighTechCrime.org

๑.๕ ห้ามมิให้นำข้อมูลสำคัญ หรือคำสั่งใด ๆ ที่ปรากฏข้อมูลส่วนบุคคลของข้าราชการตำรวจ เช่นหมายเลขบัตรประชาชน, รูปถ่ายบัตรข้าราชการตำรวจ เป็นต้น ไปเผยแพร่ผ่านทางอินเทอร์เน็ต โดยไม่มีมาตรการรักษาความปลอดภัยของข้อมูล

/๑.๖ การจัดทำเว็บไซต์...

๑.๖ การจัดทำเว็บไซต์ ให้หลีกเลี่ยงการใช้โปรแกรมบริหารจัดการข้อมูล เช่น Joomla และ Wordpress เป็นต้น เนื่องจากเป็นจุดอ่อนหลักที่ผู้กระทำความผิดใช้ในการเจาะระบบคอมพิวเตอร์ หากไม่สามารถหลีกเลี่ยงได้ จะต้องหมั่นตรวจสอบและปรับปรุงโปรแกรมให้เป็นรุ่นใหม่ล่าสุดอยู่ตลอดเวลา โดยควรพัฒนาโปรแกรมเพื่อจัดทำเว็บไซต์เอง หากไม่สามารถพัฒนาเองได้ ให้ใช้บริการในการจัดทำเว็บไซต์ของ ตร. และสำนักงานรัฐบาลอิเล็กทรอนิกส์ (สรอ.) เป็นหลัก หรือสมัครใช้ Gmail เพื่อจัดทำเว็บโดยใช้ Google Site ตามต้นแบบที่ทางกลุ่มงานอินเทอร์เน็ต บก.สสท. ได้จัดเตรียมไว้ให้

๑.๗ ห้ามเชื่อมต่ออินเทอร์เน็ตเข้ากับระบบเครือข่ายภายในของ ตร. (VPN) เพื่อเข้าถึงระบบสารสนเทศหลักของ ตร. โดยไม่ได้รับอนุญาต เช่น POLIS, CRIMES หรือ AFIS เป็นต้น

๒. มาตรการปราบปราม

๒.๑ เมื่อตรวจพบว่าระบบคอมพิวเตอร์ หรือเว็บไซต์ที่อยู่ในความดูแลของหน่วยงานในสังกัด ตร. ถูกโจมตีหรือกระทำการใด ๆ อันเป็นความผิดตามกฎหมาย ให้รีบรายงานผู้บังคับบัญชาระดับ ตร.ทราบผ่าน ศปก.ตร. โดยมีข้อมูลสำคัญประกอบด้วยชื่อเว็บ(URL), ภาพถ่ายหน้าเว็บไซต์, วันเวลาที่เกิดเหตุ และเหตุการณ์ เป็นต้น แล้วรายงานความคืบหน้าให้ กลุ่มงานอินเทอร์เน็ต บก.สสท.ทราบเป็นระยะ

๒.๒ กรณีที่ตรวจสอบพบว่า มีผู้เจาะเข้าสู่ระบบคอมพิวเตอร์ได้แล้ว ให้รีบแจ้งผู้ดูแลระบบ ดึงสายเคเบิ้ลสำหรับเชื่อมต่ออินเทอร์เน็ตออกจากเครื่องคอมพิวเตอร์ดังกล่าวทันที โดยไม่ต้องปิดเครื่องคอมพิวเตอร์ เพื่อลดความเสียหาย และป้องกันการทำลายพยานหลักฐานทางอิเล็กทรอนิกส์

๒.๓ ให้หัวหน้าหน่วย มอบหมายผู้รับผิดชอบเพื่อแจ้งความดำเนินคดีที่ บก.ปอท. พร้อมขอรับการสนับสนุนผู้เชี่ยวชาญในการเก็บพยานหลักฐานทางอิเล็กทรอนิกส์จากหน่วยความจำและ Log Files ของทุกระบบที่เกี่ยวข้อง

๒.๔ หากตรวจสอบพบว่ามีผู้กระทำความผิดโดยใช้เครือข่ายสื่อสารคอมพิวเตอร์ในการปลุกระดมให้ประชาชนกระทำความผิดกฎหมาย หรือมีการใช้หมายเลขไอพีจากต่างประเทศในการกระทำความผิด ให้พนักงานสอบสวนขอความร่วมมือในการตรวจสอบข้อมูลจากต่างประเทศ ผ่านทาง ตท. ทุกกรณี

ทั้งนี้ กำชับให้ทุกหน่วยปฏิบัติตามมาตรการนี้โดยเคร่งครัด หากเกิดความเสียหายให้หน่วยพิจารณาข้อบกพร่องเป็นกรณี ๆ ไป

จึงแจ้งมาเพื่อทราบ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป

พล.ต.ท.



(ฌนิตศักดิ์ ธีระสวัสดิ์)

รรท.ผู้ช่วย ผบ.ตร.ปรท.ผบ.ตร.