ที่ ศย ๐๑๓/ว ๓๑๐

สำนักงานศาลยุติธรรม
ถนนรัชดาภิเษก เขตจตุจักร
กทม. ๑๐๙๐๐

๑๗ เมษายน ๒๕๕๖

เรื่อง การใช้งานเครือข่ายศาลยุติธรรมทั่วประเทศ ประจำปีงบประมาณ พ.ศ.๒๕๕๖ โดยใช้เทคโนโลยี MPLS

เรียน หัวหน้าหน่วยงานในสังกัดสำนักงานศาลยุติธรรม

อ้างถึง ๑.หนังสือสำนักงานศาลยุติธรรม ที่ ศย ๐๑๓/ว ๘ ลงวันที่ ๓ มกราคม ๒๕๕๖
๒.หนังสือสำนักเทคโนโลยีสารสนเทศ ที่ ศย ๐๑๓(ส)/ว ๘ ลงวันที่ ๑๒ มีนาคม ๒๕๕๖

สิ่งที่ส่งมาด้วย รายละเอียดการใช้งานเครือข่ายศาลยุติธรรม จำนวน ๑ ชุด

ตามหนังสือที่อ้างถึง สำนักงานศาลยุติธรรมได้แจ้งการปรับระบบคอมพิวเตอร์เพื่อรองรับการเชื่อมโยงเครือข่ายศาลยุติธรรมทั่วประเทศ ประจำปีงบประมาณ พ.ศ.๒๕๕๖ โดยใช้เทคโนโลยี MPLS และเพื่อเป็นการเตรียมความพร้อมรองรับการเชื่อมโยงระบบเครือข่าย จึงให้มอบหมายนักวิชาการคอมพิวเตอร์ หรือพนักงานราชการ ตำแหน่งพนักงานคอมพิวเตอร์ของหน่วยงานดำเนินการตรวจสอบและปรับค่าทางเครือข่ายก่อนและหลังการติดตั้งเครือข่าย MPLS ของผู้ให้บริการ ซึ่งได้แจ้งแผนการติดตั้งและใช้งานเครือข่ายไปยังหน่วยงานศาลยุติธรรมทั่วประเทศ ความละเอียดแจ้งอยู่แล้ว นั้น

ในการนี้ เพื่อให้หน่วยงานในสังกัดสำนักงานศาลยุติธรรมสามารถใช้ระบบเครือข่ายและระบบอินเทอร์เน็ตในการปฏิบัติงานร่วมกันได้อย่างมีประสิทธิภาพ สำนักงานศาลยุติธรรมจึงได้นำระบบรักษาความปลอดภัย ระบบบริหารจัดการคุณภาพการให้บริการอินเทอร์เน็ต และระบบพิสูจน์ตัวตนมาใช้ร่วมกับระบบเครือข่าย MPLS โดยมีรายละเอียดการใช้งาน ดังนี้

๑. กำหนดให้นำระบบรักษาความปลอดภัยและการบริหารจัดการคุณภาพการให้บริการอินเทอร์เน็ตที่สำนักงานศาลยุติธรรมติดตั้งและใช้งานร่วมกับระบบเครือข่าย MPLS ประกอบด้วย การควบคุมกลุ่มของเว็บไซต์ที่ไม่เหมาะสมและไม่เกี่ยวข้องกับการปฏิบัติราชการ การกำหนดให้การบริการเครือข่ายอินทราเน็ตและเครือข่ายอินเทอร์เน็ตของศาลยุติธรรมตามระดับความสำคัญ โดยงานที่เกี่ยวข้องกับพันธกิจของศาลยุติธรรมและงานที่ต้องการสื่อสารอย่างต่อเนื่องจะมีความสำคัญสูงสุด นอกจากนี้ยังนำรูปแบบการดำเนินการป้องกันรักษาความปลอดภัยที่สำนักงานศาลยุติธรรมได้จัดหาและติดตั้งอยู่ไปใช้ป้องกันรักษาความปลอดภัยในระบบเครือข่าย MPLS ได้แก่ ระบบป้องกันรักษาความปลอดภัยจากเครือข่ายภายนอกหรืออินเทอร์เน็ต (Firewall) เพื่อตรวจสอบพฤติกรรมที่มีความผิดปกติและทำการป้องกัน ระบบตรวจสอบและป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System) ระบบกลั่นกรองและป้องกันไวรัสจากเว็บไซต์ (Antivirus Gateway) และระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Center) เป็นต้น

๒.กำหนด ...

๒. กำหนดให้นำระบบพิสูจน์ตัวตน (Authentication) เพื่อใช้ในการตรวจสอบสิทธิ์การใช้งานอินเทอร์เน็ต ให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ โดยบุคลากรในสังกัดสำนักงานศาลยุติธรรม ประกอบด้วย ข้าราชการตุลาการ ข้าราชการศาลยุติธรรม ลูกจ้างประจำ พนักงานราชการ และลูกจ้างชั่วคราว สามารถลงทะเบียนได้ทางเว็บไซต์ https://it.coj.go.th/Authen ตั้งแต่บัดนี้เป็นต้นไป และนำรหัสที่ได้มาใช้ในการพิสูจน์ตัวตนการใช้งานอินเทอร์เน็ตผ่านเครือข่าย MPLS และเครือข่ายไร้สายในอาคารบริเวณถนนรัชดาภิเษกแทนระบบเดิม ตั้งแต่วันที่ ๑ มิถุนายน ๒๕๕๖ เป็นต้นไป

โดยมีรายละเอียดการกำหนดระบบรักษาความปลอดภัย การบริหารจัดการคุณภาพการให้บริการอินเทอร์เน็ตและระบบพิสูจน์ตัวตนมาใช้ร่วมกับระบบเครือข่าย MPLS ศาลยุติธรรมทั่วประเทศ รายละเอียดปรากฏตามสิ่งที่ส่งมาด้วย ทั้งนี้ หากมีปัญหาข้อขัดข้องในการใช้งานดังกล่าว สามารถสอบถามรายละเอียดเพิ่มเติมได้ที่ กลุ่มระบบเครือข่ายคอมพิวเตอร์ สำนักเทคโนโลยีสารสนเทศ หมายเลขโทรศัพท์ ๐ ๒๕๑๒ ๒๒๐๗ และ ๐ ๒๕๑๓ ๐๕๕๗

จึงเรียนมาเพื่อโปรดทราบและพิจารณาดำเนินการในส่วนที่เกี่ยวข้องต่อไป

ขอแสดงความนับถือ

(นายวิรัช ขินวินิจกุล)
เลขาธิการสำนักงานศาลยุติธรรม

สำนักเทคโนโลยีสารสนเทศ
กลุ่มระบบเครือข่ายคอมพิวเตอร์
โทร. ๐ ๒๕๑๓ ๐๕๕๗
โทรสาร ๐ ๒๕๑๒ ๘๔๔๗

สรุปรายละเอียดและเอกสาร

การใช้งานเครือข่ายศาลยุติธรรมทั่วประเทศ

ลำดับ/รายการ	การดำเนินการของศาล	เอกสารแนบ
๑.การกรองเว็บไซต์ (Web Filtering)	ให้ผู้เกี่ยวข้องกับการใช้งานระบบเครือข่ายทราบ	รายละเอียดการกรองเว็บไซต์
๒.การบริหารจัดการคุณภาพการใช้บริการเครือข่ายอินทราเน็ตและเครือข่ายอินเทอร์เน็ต (Quality of Service)	ให้ผู้เกี่ยวข้องกับการใช้งานระบบเครือข่ายทราบ	รายละเอียดการทำ QoS
๓.การป้องกันรักษาความปลอดภัยระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ โดยนำ รูปแบบการดำเนินการป้องกันรักษาความปลอดภัยที่สำนักงานศาลยุติธรรมได้จัดหาและติดตั้งอยู่ไปใช้ป้องกันรักษาความปลอดภัยในระบบเครือข่าย MPLS	ให้ผู้เกี่ยวข้องกับการใช้งานระบบเครือข่ายทราบ	รายละเอียดการป้องกันรักษาความปลอดภัย
๔. ระบบพิสูจน์ตัวตน (Authentication)	ลงทะเบียนการใช้งานระบบพิสูจน์ตัวตนทางเว็บไซต์ https://it.coj.go.th/Authen และนำรหัสที่ได้ไปใช้งานอินเทอร์เน็ตผ่านเครือข่าย MPLS และเครือข่ายไร้สายในอาคารบริเวณถนนรัชดาภิเษกแทนระบบเดิม ตั้งแต่วันที่ ๑ มิถุนายน ๒๕๕๖ เป็นต้นไป ดังนี้ - ข้าราชการตุลาการ ข้าราชการศาลยุติธรรม ลูกจ้างประจำ และพนักงานราชการ สามารถลงทะเบียนโดยยันยันข้อมูลส่วนตัวกับฐานข้อมูลที่มีอยู่แล้ว - ลูกจ้างชั่วคราว เนื่องจากอยู่ระหว่างจัดเก็บฐานข้อมูลจึงต้องกรอกข้อมูลส่วนตัวใหม่เพื่อทำการลงทะเบียน และกำหนดรหัสในการใช้งาน แต่เมื่อจัดเก็บข้อมูลลงฐานข้อมูลเรียบร้อยแล้วจะสามารถใช้งานยืนยันข้อมูลเพื่อลงทะเบียนได้โดยไม่ต้องกรอกข้อมูลใหม่	คู่มือการพิสูจน์ตัวตน Authentication

รายการกลุ่มของเว็บไซต์ที่ควรควบคุมในช่วงเวลาปฏิบัติราชการ

๑. ประเภทที่ควรมีการ Block ถาวร (ตลอด ๒๔ ชั่วโมง)

ลำดับ	กลุ่มเว็บไซต์	ชื่อกลุ่ม(MacAfee)	ผลกระทบเมื่อไม่มีการควบคุม
๑	ข้อมูลที่เด็กอายุต่ำกว่า ๑๘ ปี ไม่ควรเข้าชม	Incidental Nudity Sexual Materials	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๒	การใช้ยาเสพติด, ยาต้องห้าม	Drugs	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน
๓	การพนัน	Gambling Gambling Related	ไม่เหมาะสมต่อการใช้งานและอาจผิดกฎหมาย
๔	การใช้เครื่องมือในการ Hack	Potential Hacking / Computer Crime Browser Exploits	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๕	การเหยียดสีผิว เชื้อชาติ ศาสนา	Discrimination	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๖	ข้อมูล วิธีการหรือสอนการฉ้อโกง การ backmail	Illegal UK	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๗	เว็บไซต์ที่มีภาพเปลือย	Nudity	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ลำดับ	กลุ่มเว็บไซต์	ชื่อกลุ่ม(MacAfee)	ผลกระทบเมื่อไม่มีการควบคุม
๘	เว็บไซต์ที่เก็บข้อมูลบุคคลเช่น ชื่อ ที่อยู่ เลขที่บัตรเครดิตเพื่อกระทำการล่อลวง	Phishing	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๙	เผยแพร่ข้อมูลหรือขโมยข้อมูลผู้อื่น ไปขาย	Computer Crime	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๑๐	เว็บลามก	Pornography Provocative Attire	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๑๑	เว็บที่ส่งพวก SPAM	Spam URLs	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๑๒	เว็บไซต์ที่มีส่งข้อมูลไฟล์แบบ peer –to –peer หรือมีการส่ง Spyware	Spyware / Adware / Keyloggers P2P / File Sharing Personal Network Storage Potential Illegal Software Media Download Media Sharing	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๑๓	ข้อมูลความรุนแรงเช่น ภาพความตาย การบาดเจ็บ การต่อสู้ (ซึ่งไม่ใช่ข้อมูลข่าวหรือประวัติศาสตร์)	Violence Game/Cartoon Violence	ไม่เหมาะสมต่อการใช้งานและอาจมีผลกระทบต่อการทำงาน

ลำดับ	กลุ่มเว็บไซต์	ชื่อกลุ่ม(MacAfee)	ผลกระทบเมื่อไม่มีการควบคุม
๑๔	เว็บไซต์ที่แสดงข้อมูลและมีการขายพวกอาวุธต่างๆ	Weapons	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน
๑๕	เว็บไซต์ที่แสดงข้อมูลคำแนะนำเกี่ยวกับการทำผิดกฎหมาย เช่น การขโมยของ และ คำแนะนำเกี่ยวกับการฆ่าตัวตาย	Potential Criminal Activities	อาจมีความผิดตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
๑๖	เกมส์	Games	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน

๒. เว็บไซต์ที่ควร Block เฉพาะช่วงเวลาทำงาน (จันทร์-ศุกร์ เวลา ๘.๓๐-๑๒.๐๐ น. และ ๑๓.๐๐-๑๗.๓๐ น.)

ลำดับ	กลุ่มเว็บไซต์	ชื่อกลุ่ม(MacAfee)	
๑	การดูทีวีหรือ ฟังเพลงผ่านเว็บไซต์	Internet Radio / TV	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน
๒	โทรศัพท์ผ่านเว็บไซต์	Mobile Phone, Web Phone	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน
๓	เว็บไซต์ให้ดาวโหลดเพลง	Streaming Media	ไม่เหมาะสมต่อการใช้งานและอาจมีผลต่อการทำงาน

ทั้งนี้ หากสำนักหรือหน่วยงานใดมีความประสงค์จะเข้าใช้งานเว็บไซต์ที่อยู่ในกลุ่มเว็บไซต์ที่ถูกควบคุม สามารถกรอกแบบฟอร์มคำขอพร้อมแจ้งเหตุผลความจำเป็นในการเข้าใช้เว็บไซต์ให้สำนักเทคโนโลยีสารสนเทศพิจารณายกเว้นได้เป็นรายกรณีไป

การบริหารจัดการคุณภาพการใช้บริการเครือข่ายอินทราเน็ตและอินเทอร์เน็ต

(Quality Of Service)ของศาลยุติธรรม

ประเภทของการให้บริการ	รายละเอียด	ระดับความสำคัญ	สัดส่วนคิดเป็นเปอร์เซ็นต์ของขนาดช่องสัญญาณ
ประเภท ๑.	■ งานที่เกี่ยวข้องกับพันธกิจของศาลยุติธรรม Mission Critical ประกอบด้วย ๑.๑ งานที่ปฏิบัติบนเครือข่ายอินทราเน็ตของศาลยุติธรรม หรืองานที่ปฏิบัติบนระบบคอมพิวเตอร์แม่ข่าย ที่ศูนย์ปฏิบัติการเครือข่ายสำนักงานศาลยุติธรรม ๑.๒ งานที่ปฏิบัติบนระบบคอมพิวเตอร์แม่ข่ายที่ Internet Data Center ■ Real time Package ของศาลยุติธรรม (เกี่ยวข้องกับ Protocol H.264, SVC, AVC เป็นต้น) เช่น Video Conference, Web Conference	ระดับที่ ๑ (มีความสำคัญสูงสุด)	๐-๗๐ %
ประเภท ๒.	งานที่ให้บริการสำหรับดาวน์โหลดข้อมูล (File Transfer) * การจำกัดขนาดในการดาวน์โหลดเพื่อไม่ให้ส่งผลกระทบต่อการใช้งานในกลุ่มที่ให้ความสำคัญสูงสุด	ระดับที่ ๒	๐-๕%
ประเภท ๓.	งานให้บริการอื่นๆ ที่ไม่ได้อยู่ในงานประเภทที่ ๑ ถึง ๒ * หากไม่มีการใช้งานในกลุ่มที่มีความสำคัญสูงกว่า งานในกลุ่มนี้จะสามารถใช้งานวงจรได้ทั้งหมด	ระดับที่ ๓	๐-๒๕%

ระบบป้องกันรักษาความปลอดภัยจากเครือข่ายภายนอกหรืออินเทอร์เน็ต (Firewall)
เพื่อตรวจสอบพฤติกรรมที่มีความผิดปกติและทำการป้องกัน

ปัจจุบันได้มีการกำหนดโดยจำแนกพฤติกรรมผิดปกติที่เกิดขึ้นเป็น ๗ ส่วน ดังนี้

๑. ส่วนของผู้ใช้งาน/หน่วยงาน ศาลยุติธรรมทั่วประเทศ (Trust Zone)
๒. ส่วนของระบบเครือข่ายอินเทอร์เน็ต (Untrusted Zone)
๓. ส่วนของระบบเครือข่ายที่เชื่อมต่อระบบบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (RAS Zone)
๔. ส่วนของระบบเครือข่ายไร้สายที่อยู่ในอาคารศาลบริเวณถนนรัชดาภิเษก (Wireless-Ratchada Zone) ได้แก่ อาคารศาลอาญา อาคารศาลแพ่ง อาคารศาลอุทธรณ์ อาคารศาลแขวงพระนครเหนือ และอาคารสถาบันพัฒนาข้าราชการฝ่ายตุลาการศาลยุติธรรม
๕. ส่วนของระบบคอมพิวเตอร์ที่ให้บริการสืบค้นข้อมูลทะเบียนราษฎร (SSL VPN-AMI)
๖. ส่วนของระบบคอมพิวเตอร์ที่ให้บริการระบบงานต่างๆ (Server Farm) ผ่านทางระบบเครือข่ายภายใน (Intranet-DMZ Zone)
๗. ส่วนของระบบคอมพิวเตอร์ที่ให้บริการระบบงานต่างๆ (Server Farm) ผ่านทางระบบเครือข่ายอินเทอร์เน็ต (External-DMZ Zone)

พฤติกรรมผิดปกติ โดยพฤติกรรมที่ตรวจพบและป้องกันได้ ได้แก่

- การพยายามส่งข้อมูลปริมาณมากๆ ไปที่เครื่องคอมพิวเตอร์ปลายทาง (UDP Flood, ICMP Flood)
- ตรวจหาช่องทางให้บริการที่เครื่องปลายทางเปิดอยู่ (Port Scan, IP Sweep)
- พยายามปลอมแปลงเป็นผู้ใช้งานอย่างถูกต้องในระบบเครือข่ายคอมพิวเตอร์ (IP Spoof Attack)
- ข้อมูลที่ส่งบนระบบเครือข่ายมีโครงสร้างของข้อมูลที่อาจเป็นอันตราย (Unknown Protocol)
- มีโครงสร้างของข้อมูลใหญ่ผิดปกติ (Large ICMP packet)
- ข้อมูลที่ส่งบนระบบเครือข่ายมีโครงสร้างข้อมูลผิดปกติ (SYN and FIN bits set, FIN bit but no ACK Bit, ICMP Ping ID Zero, TCP Packet Without Flags)
- เว็บไซต์ที่อาจเป็นอันตราย (Malicious URL Code Red)
- ผลต่อการรับข้อมูลของเครื่องคอมพิวเตอร์ (Fragmented Packet)
- เครื่องคอมพิวเตอร์หลายเครื่องสร้างการเชื่อมต่อไปยังเครื่องปลายทางเดียวกัน (Dst IP Based Session Limiting)
- เครื่องคอมพิวเตอร์สร้างการเชื่อมต่อไปยังเครื่องปลายทางหลายเครื่อง (Src IP-Based Session Limiting)

ระบบตรวจสอบและป้องกันการบุกรุกทางเครือข่าย (Intrusion Prevention System)

<u>ปัจจุบันได้กำหนดระดับความรุนแรง (Severity)</u> ดังนี้

๑. Critical เป็นระดับที่มีผลกระทบต่อระบบคอมพิวเตอร์และเครือข่ายรุ่นแรงมาก ถึงขั้นระบบหยุดทำงานหรือเสียหายจนไม่สามารถใช้งานได้
   - พฤติกรรมการบุกรุกโจมตีจะมีรูปแบบการหลบหลีกจากระบบป้องกันภัยและพยายามเข้าถึงสิทธิของผู้ดูแลระบบเพื่อนำสิทธิไปใช้ในการสร้างความเสียหายกับระบบอย่างรุนแรง

๒. Major เป็นระดับความรุนแรงแต่น้อยกว่าระดับ Critical กล่าวคือระบบคอมพิวเตอร์และเครือข่ายที่ถูกบุกรุกหรือโจมตีไม่ได้เสียหายร้ายแรง แต่ไม่สามารถให้บริการหรือใช้งานได้
   - พฤติกรรมการบุกรุกโจมตีจะพยายามเข้าถึงสิทธิในระดับผู้ใช้งาน และนำสิทธิที่ได้ไปทำให้การบริการของระบบหยุดชะงักหรือใช้งานไม่ได้

๓. Minor เป็นระดับที่มีความรุนแรงปานกลาง กล่าวคือระบบที่ถูกบุกรุกหรือโจมตียังทำงานและให้บริการได้
   - พฤติกรรมการบุกรุกโจมตีจะทำการสอดแนมเพื่อรวบรวมข้อมูลที่สำคัญจากระบบ ทำให้ระบบสูญเสียความน่าเชื่อถือและข้อมูลที่เป็นความลับอาจถูกเปิดเผย

๔. Warning เป็นระดับที่มีความรุนแรงน้อย กล่าวคือระบบที่ถูกบุกรุกหรือโจมตีจะไม่ปรากฏความเสียหายใดๆ ชัดเจน
   - พฤติกรรมการบุกรุกหรือโจมตีเป็นพฤติกรรมที่ผู้บุกรุกหรือโจมตี ค้นหาและรวบรวมข้อมูลเกี่ยวกับช่องทางการเข้าระบบคอมพิวเตอร์และเครือข่ายที่ให้บริการเพื่อใช้เป็นข้อมูลในการบุกรุกและโจมตี

๕. Info เป็นระดับที่เตือนให้ระวัง กล่าวคือ พฤติกรรมการทำงานของระบบที่ผิดพลาดหรือผิดปกติ