แนวทางการจัดเก็บข้อมูลล็อกสำหรับองค์กรเพื่อให้สอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
Log implementation and auditing guideline compliance with Computer Crime Act B.E 2550 (2007)

ปรับปรุงครั้งที่ 1: 2 กันยายน 2551
เผยแพร่: 23 สิงหาคม 2551

เลอศักดิ์ ลิ้มวิวัฒน์กุล และ ดร. บรรจง หะรังษี และ ดร. โกเมน พิบูลย์โรจน์
โปรแกรมเทคโนโลยีเพื่อความมั่นคง
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

วีรยา จุลมณีวงศ์ และ สุรางคณา วายุภาพ
ฝ่ายศึกษาวิจัยประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

ที่ผ่านมาการติดตามและตรวจสอบพยานหลักฐานที่เกี่ยวข้องกับระบบคอมพิวเตอร์ในประเทศไทย หรือนำข้อมูลการบันทึกเหตุการณ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ไม่สามารถทำได้โดยตรง หรือไม่สามารถกำหนดให้ผู้ที่เกี่ยวข้องเก็บข้อมูลการเข้าถึงระบบคอมพิวเตอร์ที่จำเป็นได้ ยกตัวอย่างเช่นเมื่อพบว่ามีผู้กระทำความผิดโดยใช้ระบบคอมพิวเตอร์ผ่านร้านอินเทอร์เน็ตคาเฟ่ในการเข้าถึงระบบคอมพิวเตอร์เซิร์ฟเวอร์ของผู้อื่นโดยไม่ได้รับอนุญาต ซึ่งเมื่อมีการสอบสวนหรือต้องการพลักฐานเพิ่มเติมกลับพบว่าไม่สามารถติดตามข้อมูลการใช้งานอินเทอร์เน็ตตั้งแต่ร้านอินเทอร์เน็ตคาเฟ่ ผู้ให้บริการอินเทอร์เน็ตหรือ Internet Service Provider (ISP) เพื่อนำข้อมูลมาวิเคราะห์ได้ ซึ่งเจ้าหน้าที่พนักงานจำเป็นต้องหามาตรการอื่นที่ไม่เกี่ยวข้องกับเทคโนโลยีในการสืบสวนพยานหลักฐาน

นอกจากนี้ยังพบว่าเมื่อมีคดีความที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทั้งที่ผู้กระทำความผิดใช้ระบบคอมพิวเตอร์โดยตรงเพื่อกระทำความผิด หรือทางอ้อมยังไม่มีบทบัญญัติที่ชัดเจนว่าจะดำเนินคดีในลักษณะใด ซึ่งพนักงานเจ้าหน้าที่ที่เกี่ยวข้องจำเป็นต้องอ้างอิงด้วยกฎหมายฉบับอื่นเช่น กฎหมายลักษณะความอาญาเพื่อวิเคราะห์ประกอบพยานหลักฐาน เป็นต้น

ข้อมูลจากศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ ประเทศไทย (ThaiCERT) ภายใต้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (NECTEC) ที่ผ่านมาเมื่อมีการรับมือเหตุการณ์ละเมิดความมั่นคงปลอดภัยคอมพิวเตอร์ภายในประเทศไทย การทำหน้าที่ประสานงานระหว่างผู้ที่แจ้งเหตุการณ์ละเมิดความมั่นคงปลอดภัยและผู้ที่เกี่ยวข้อง จำเป็นต้องใช้ข้อมูลที่บันทึกในระบบคอมพิวเตอร์เพื่อวิเคราะห์หาสาเหตุ ที่มาของผู้ละเมิดความมั่นคงปลอดภัย รวมถึงข้อมูลที่จำเป็นเพิ่มเติม ซึ่งบ่อยครั้งพบว่ามีข้อมูลที่ไม่เพียงพอ โดยเฉพาะเมื่อมีการติดตามข้อมูลเพิ่มเติมจากผู้ดูแลระบบเครือข่ายภายในองค์กร หรือผู้ให้บริการอินเทอร์เน็ตภายในประเทศ

จากการประกาศใช้ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งมีจุดมุ่งหมายเพื่อบัญญัติการกระทำความผิดที่เกี่ยวกับคอมพิวเตอร์ กำหนดแนวปฏิบัติในทิศทางเดียวกันสำหรับผู้ที่เกี่ยวข้องกับระบบสารสนเทศหรือระบบคอมพิวเตอร์ และกำหนดให้ต้องมีการเก็บข้อมูลที่บันทึกเหตุการณ์ที่เกิดขึ้นบนระบบคอมพิวเตอร์ ข้อมูลดังกล่าวนี้ได้นิยามว่าเป็น "ข้อมูลจราจรคอมพิวเตอร์" และ "ข้อมูลผู้ใช้บริการ" และเพื่อกำหนดความชัดเจนเพิ่มเติม ได้ประกาศลงในราชกิจจานุเบกษาเรื่องประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 เพื่อขยายความหลักเกณฑ์ทางเทคนิคในการเก็บข้อมูลจราจรคอมพิวเตอร์ ทั้งนี้เพื่อให้ผู้ให้บริการในแต่ละประเภทได้เก็บข้อมูลดังกล่าวและสามารถนำมาใช้ต่อไปได้

ทั้งนี้คำว่า "ข้อมูลจราจรคอมพิวเตอร์" และ "ข้อมูลผู้ใช้บริการ" เป็นข้อมูลการบันทึกเหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์ ศัพท์ทางเทคนิคเรียกข้อมูลลักษณะนี้ว่า ข้อมูลล็อกหรือ Log ตามคำนิยามในเอกสารอ้างอิง [3] ซึ่งจะได้กล่าวในรายละเอียดเพิ่มเติมในเอกสารฉบับนี้ ดังนั้นคำว่า "ข้อมูลล็อก" มีความหมายเดียวกันกับคำว่า "ข้อมูลจราจรคอมพิวเตอร์" และ "ข้อมูลผู้ใช้บริการ"

หน้าที่ของผู้ให้บริการที่ต้องปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์คือ การปรับแต่งระบบคอมพิวเตอร์ให้สามารถเก็บ "ข้อมูลล็อก" ให้ได้อย่างน้อยตามที่ "ข้อมูลจราจรคอมพิวเตอร์" และ "ข้อมูลผู้ใช้บริการ" ได้กำหนดไว้ให้ดำเนินการเก็บ และที่สำคัญคือ

- มีการรักษาความมั่นคงปลอดภัยของข้อมูลล็อก เพื่อให้ข้อมูลล็อกมีความถูกต้องและเชื่อถือ
- มีการควบคุมการเข้าถึงข้อมูลล็อก กำหนดลำดับเวลาของการเก็บข้อมูลล็อกให้ถูกต้อง เพื่อให้ข้อมูลล็อกที่เก็บไว้นั้นใช้วิเคราะห์ตามความต้องการของพนักงานเจ้าหน้าที่หรือผู้ที่เกี่ยวข้องได้ รวมทั้งใช้เป็นพยานหลักฐานในชั้นศาลได้
- มีการกำหนดวิธีการรักษาระยะเวลาการเก็บข้อมูลล็อก เพื่อให้มีข้อมูลล็อกที่นำมาวิเคราะห์สืบย้อนหลังและติดตามเหตุการณ์ที่เกิดขึ้นมาแล้วได้

ซึ่งได้กำหนดรายละเอียดการปฏิบัติไว้โดยละเอียดใน ประกาศลงในราชกิจจานุเบกษาเรื่องประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 แล้ว

เอกสารฉบับนี้จัดทำขึ้นเพื่อรวบรวมและสรุปประเด็นที่สำคัญ และนำเสนอแนวทางในทางปฏิบัติเพื่อผู้ให้บริการสามารถเก็บ "ข้อมูลล็อก" ได้สอดคล้องตามที่ พ.ร.บ ฯ ต้องการ

ผู้อ่านสามารถเลือกเนื้อหาในส่วนที่ต้องการอ่านทำความเข้าใจ ได้ตามเนื้อหาของเอกสารฉบับนี้ตามลำดับนี้

โดยสรุปแล้ว ผู้ให้บริการสามารถนำแนวทางปฏิบัติการจัดเก็บข้อมูลล็อกต่อไปนี้ไปปรับใช้ภายในองค์กร ทั้งนี้ได้จัดแบ่งตามระดับการดำเนินการเป็น

- **M – Mandatory** หมายความว่าเป็นสิ่งที่จำเป็นต้องดำเนินการ เพื่อให้เป็นไปสอดคล้องตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550
- **I – ISO/IEC 27001** หมายความว่ามาตรฐาน ISO/IEC 27001 ได้กำหนดให้นำมาตรการนี้ไปดำเนินการ ซึ่งเป็นมาตรการทางด้านความมั่นคงปลอดภัยของระบบสารสนเทศที่ดี
- **B – Best Practice** หมายความว่าเป็นคำแนะนำเพิ่มเติมที่สามารถนำไปพัฒนาและดำเนินใช้ภายในองค์กรได้ หรือเป็นทางเลือกที่ดีในระยะยาวต่อองค์กร

ตามตารางนี้

ประเด็น	ข้อพิจารณา/แนวทางการดำเนินการ/ตัวอย่าง	M	I	B
เก็บรักษาข้อมูลจราจรคอมพิวเตอร์	ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ – ตั้งแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ และ – เก็บไว้ไม่น้อยกว่า 90 วัน – พนักงานเจ้าหน้าที่สามารถสั่งให้เก็บเพิ่มเติมจาก 90 วันแต่ไม่เกิน 1 ปีได้ เป็นกรณีๆ ไป	✓		
เก็บรักษาข้อมูลผู้ใช้บริการ	ต้องเก็บรักษาข้อมูลผู้ใช้บริการ – ตั้งแต่วันที่ผู้ใช้เริ่มใช้บริการ และ – เก็บไว้ไม่น้อยกว่า 90 วันตั้งแต่การใช้บริการสิ้นสุดลง	✓		
พิจารณาว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการใด	เพื่อพิจารณาว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการ – 5 (1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต – 5 (2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม 5 (1)	✓		
พิจารณาหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์	พิจารณารายละเอียดการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ว่าจะใช้กับผู้ให้บริการประเภทใดตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550			✓
จัดทำนโยบายการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ และข้อมูลผู้ใช้บริการตาม พ.ร.บ.	– นโยบายดังกล่าวควรครอบคลุมหัวข้อต่อไปนี้ ▪ นิยามที่เกี่ยวข้องเช่น ข้อมูลจราจรคอมพิวเตอร์ ข้อมูลผู้ใช้บริการ ใครเป็นผู้ใช้บริการ เป็นต้น ▪ องค์กรจัดอยู่ในประเภทของผู้ให้บริการใด ▪ กำหนดรายละเอียดวันเวลาที่ดำเนินการ ▪ บทบาทหน้าที่ความรับผิดชอบ ของแต่ละหน่วยงาน เช่นการดำเนินการ การกำกับให้ปฏิบัติตาม การตรวจความสอดคล้องกับ พ.ร.บ. ▪ แนวทางปฏิบัติที่จำเป็นต้องดำเนินการ โดยอาจทำเป็นเอกสารกำหนดคุณสมบัติทางเทคนิคการเก็บข้อมูลล็อกแยกจากนโยบายฉบับนี้อีก 1 ฉบับเพื่อระบุว่าในองค์กรมีเซิร์ฟเวอร์หรืออุปกรณ์ใดที่ต้องเก็บข้อมูลล็อก และดำเนินการเก็บข้อมูลล็อกให้สอดคล้องตามเอกสารอ้างอิง [7] ได้อย่างไร ▪ กำหนดหรือแต่งตั้งเจ้าหน้าที่ประสานงานกับพนักงานเจ้าหน้าที่ของรัฐในกรณีที่ต้องการข้อมูล ▪ กำหนดหรือจัดทำบัญชีรายชื่อผู้ที่มีสิทธิเข้าถึงข้อมูลล็อก ▪ ระบุมาตรการควบคุมที่นำมาใช้เพื่อป้องกันข้อมูลล็อกให้มั่นคงปลอดภัยและเชื่อถือได้ เช่นการป้องกันการเปลี่ยนแปลงข้อมูลล็อกโดยไม่ได้รับอนุญาต การพิสูจน์ตัวตน การ		✓	

ประเด็น	ข้อพิจารณา/แนวทางการดำเนินการ/ตัวอย่าง	M	I	B
	เข้ารหัสหรือมาตรการอื่นที่นำมาใช้เป็นต้น ▪ การทบทวนนโยบายเช่นทุก 1 ปีเป็นต้น หรือจัดให้มีการทบทวนเมื่อมีการปรับปรุงโครงสร้างพื้นฐานระบบสารสนเทศ หรือโครงสร้างธุรกิจขององค์กรเป็นต้น – นโยบายควรลงนามโดยผู้บริหารระดับสูง หรือผู้บริหารระบบสารสนเทศเป็นอย่างน้อย			
จัดทำเอกสารและดำเนินการปฏิบัติตามข้อกำหนดคุณสมบัติที่ต้องดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการตามข้อกำหนดใน พ.ร.บ.	– ดำเนินการ ▪ จัดทำเอกสารเพื่อระบุว่าองค์กรจัดเป็นผู้ให้บริการประเภทใด ▪ จัดทำเอกสารกำหนดคุณสมบัติทางเทคนิคที่องค์กรต้องดำเนินการเพื่อให้สามารถเก็บข้อมูลล็อกให้สอดคล้องตามที่ พ.ร.บ. ได้กำหนดไว้ ▪ ดำเนินการประเมินความเสี่ยงเฉพาะในแง่ของเก็บข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการเพื่อหาว่าจำเป็นจะต้องดำเนินการเสริมสร้างความมั่นคงปลอดภัยหรือลดความเสี่ยงในด้านใดบ้าง ▪ ดำเนินการประเมินผลกระทบ และขีดความสามารถในการเก็บข้อมูลให้ได้ตาม พ.ร.บ. และกำหนดมาตรการเพิ่มเติม เช่นจัดซื้อเซิร์ฟเวอร์สำหรับเก็บข้อมูลล็อกโดยเฉพาะเป็นต้น – กำหนดแผนการดำเนินงาน ผู้รับผิดชอบดำเนินการ เอกสารการดำเนินงาน และแนวทางการบำรุงรักษาระบบการเก็บข้อมูลล็อก			✓
ดำเนินการจัดเก็บข้อมูลล็อกตามประเภทของผู้ให้บริการ	<u>ตัวอย่างการดำเนินการ</u> – ประชุมหารือร่วมกันระหว่างที่ผู้ที่เกี่ยวข้อง และดำเนินการกำหนดคุณสมบัติรายละเอียดทางเทคนิคของการเก็บข้อมูลล็อกให้สอดคล้องตามประเภทของผู้ให้บริการ – จัดทำและดำเนินการตามนโยบายการเก็บข้อมูลจราจรคอมพิวเตอร์ – แต่งตั้งเจ้าหน้าที่ผู้เข้าถึงข้อมูลจราจรคอมพิวเตอร์และติดต่อประสานงานกับเจ้าหน้าที่พนักงานของรัฐ รวมถึงให้การในชั้นศาล อย่างน้อยดังนี้ ▪ เจ้าหน้าที่ที่ดูแลรักษาข้อมูลล็อก ▪ ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) ▪ ผู้บริหารองค์กร – จัดทำการเก็บข้อมูลล็อกตามรายละเอียดคุณสมบัติทางเทคนิคของการเก็บข้อมูลล็อกตามประเภทของผู้ให้บริการ – ดำเนินการตรวจสอบว่าการเก็บข้อมูลล็อกนั้นสอดคล้องตามที่ พ.ร.บ. ได้กำหนดไว้แล้วหรือไม่	✓	✓	
เก็บข้อมูลล็อกในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity)	<u>ตัวอย่างการดำเนินการ</u> – จัดเก็บข้อมูลล็อกบน Harddisk ที่ใช้เทคโนโลยี RAID – กำหนดวิธีการสำรองข้อมูลล็อกเช่น การสำรองบนดีวีดี การสำรองบนเทปอัตโนมัติ – ในกรณีที่มีการสำรองข้อมูล ให้กำหนดวิธีการป้องกันสื่อบันทึกข้อมูลสำรองข้อมูลล็อก เช่นจัดเก็บในบริเวณที่ปลอดภัย เช่นตู้เซฟเป็นต้น <u>เทคโนโลยีที่สามารถนำมาใช้ได้</u> – จัดทำล็อกเซิร์ฟเวอร์หรือ Log Server เพื่อเก็บข้อมูลแบบ Secondary Logging เพื่อให้สามารถบริหารจัดการและควบคุมการเข้าถึงข้อมูลล็อกที่ล็อกเซิร์ฟเวอร์จากศูนย์กลางและทำให้มีความมั่นคง	✓	✓	

ประเด็น	ข้อพิจารณา/แนวทางการดำเนินการ/ตัวอย่าง	M	I	B
	ปลอดภัยมากยิ่งขึ้น หาข้อมูลเพิ่มเติมได้ที่หัวข้อ Secondary Logging			
ระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อ (Media) ที่เก็บข้อมูลล็อก	ตัวอย่างการดำเนินการ – แต่งตั้งเจ้าหน้าที่ผู้เข้าถึงข้อมูลล็อก เพื่อแต่งตั้งบุคลากรหรือทีมงานผู้รับผิดชอบการดูแลการเก็บรักษาข้อมูลล็อก และติดต่อกับเจ้าหน้าที่พนักงานของรัฐในกรณีที่ต้องการข้อมูล – บุคลากรดังกล่าวไม่ควรเป็นผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย ผู้พัฒนา หรือผู้ที่เกี่ยวข้องอื่น เพื่อแยกบทบาทหน้าที่ให้ชัดเจนและเป็นการป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อมูลล็อกโดยไม่ได้รับอนุญาต – กำหนดมาตรการควบคุมการเข้าถึงข้อมูลล็อก โดยการพิสูจน์ตัวตนตามรายชื่อของผู้ที่มีสิทธิเข้าถึงข้อมูลล็อกที่กำหนดไว้ รวมถึงจัดให้มีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง	✓	✓	
มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้	ตัวอย่างการดำเนินการ – จัดทำเอกสารควบคุมชั้นความลับของข้อมูล โดยควรมีหัวข้อต่อไปนี้ ▪ ชั้นความลับของข้อมูล เช่น ลับมาก ลับ ใช้เป็นการภายใน เปิดเผยได้ ▪ ขอบเขตหรือประเภทของข้อมูลตามระดับชั้นความลับ ▪ วิธีการดำเนินการในแต่ละชั้นความลับ ตั้งแต่การสร้าง การใช้งาน การแจกจ่าย การเก็บ การส่ง การทำลาย – จัดระดับชั้นความลับของข้อมูลล็อกบนระบบ – จัดให้มีการดำเนินการตามเอกสารกำหนดชั้นความลับของข้อมูล โดยเฉพาะข้อมูลล็อก – จัดให้มีการการพิสูจน์ตัวตนก่อนเข้าถึงข้อมูลล็อก เทคโนโลยีที่สามารถนำมาใช้ได้ – นำวิธีการ Digital Hashing มาใช้เพื่อตรวจสอบความเปลี่ยนแปลงที่เกิดขึ้นบนข้อมูลล็อก เช่นการใช้ MD5 หรือ GPG เป็นต้น – จัดเก็บข้อมูลล็อกไว้ในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียวเช่น CD-ROM เป็นต้น	✓	✓	
จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับแต่งตั้งตาม พ.ร.บ. ฯ เพื่อให้การส่งมอบข้อมูลนั้นเป็นไปด้วยความรวดเร็ว	ตัวอย่างการดำเนินการ – จัดทำนโยบายการเก็บข้อมูลจราจรคอมพิวเตอร์ และระบุบทบาทและหน้าที่ของเจ้าหน้าที่ประสานงานกับพนักงานเจ้าหน้าที่ฯ ในกรณีที่ต้องการข้อมูลล็อก – จัดทำหนังสือแต่งตั้งเจ้าหน้าที่ประสานงานอย่างเป็นทางการ เจ้าหน้าที่ดังกล่าวไม่ควรเป็นผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย ผู้พัฒนาหรือบุคลากรอื่นที่เกี่ยวข้องกับระบบที่เกี่ยวข้องกับข้อมูลล็อก	✓		
ใช้ระบบของบุคคลที่สามเพื่อพิสูจน์ตัวตน ต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย	ตัวอย่างการดำเนินการ – จัดให้มีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้เช่น Username หรือ Login ที่กำหนด เพื่อระบุ Identification ของการใช้งาน และกำหนดวิธีการพิสูจน์ตัวตนหรือ Authentication ที่เหมาะสมเช่น รหัสผ่าน หรือหมายเลข PIN บัตร Smartcard หรือ ลายนิ้วมือ เป็นต้น – จัดทำระบบลงทะเบียนผู้ใช้งานเพื่อให้กระบวนการ Identification ด้วย Username หรือ Login ของระบบสามารถยืนยันตัวบุคคลการใช้งานระบบเป็นรายบุคคลได้จริง โดยอาจเลือกเก็บข้อมูลเพิ่มเติมเช่น บัตรประจำตัวประชาชน หมายเลขพาสพอร์ต บัตรประจำตัว	✓		

ประเด็น	ข้อพิจารณา/แนวทางการดำเนินการ/ตัวอย่าง	M	I	B
	พนักงาน หรือหมายเลขประจำตัวพนักงาน ส่วนข้อมูลพนักงานสามารถใช้ข้อมูลจากฝ่ายบุคคลขององค์กรได้เป็นต้น – กระบวนการ I&A ที่ดีและมีความมั่นคงปลอดภัยและสามารถยืนยันบุคคลที่ใช้เป็นรายบุคคลได้ ไม่ควรอนุญาตให้สร้างบัญชีผู้ใช้หรือ Username ที่ใช้งานร่วมกัน <u>เทคโนโลยีที่สามารถนำมาใช้ได้</u> – นำระบบพิสูจน์ตัวตนแบบศูนย์กลางมาใช้เช่น Microsoft Active Directory หรือการควบคุมการเข้าถึงเครือข่ายด้วย Proxy แบบที่ต้องมีการพิสูจน์ตัวตนเป็นต้น			
เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที	– จัดให้มีการตั้งสัญญาณเวลาด้วยโพรโตคอล Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ตามเอกสารอ้างอิง [9] ระบุว่าในเมืองไทยมีผู้ให้บริการ ▪ สถาบันมาตรวิทยาแห่งชาติ เครื่อง time1.nimt.or.th หรือ 203.185.69.60 ▪ กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83 ▪ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.185.129.186 หรือ 203.185.129.187 – ในต่างประเทศ ▪ National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18 – ควรกำหนดให้มีการตั้งค่าเวลาผ่าน NTP ไปที่เซิร์ฟเวอร์ NTP Server ที่มีค่า Stratum เป็น 1 อย่างน้อย 2 หรือ 3 เซิร์ฟเวอร์เป็นอย่างน้อย <u>เทคโนโลยีที่สามารถนำมาใช้ได้</u> – การติดตั้ง NTP Server ภายในองค์กร โดยกำหนดให้รับค่าสัญญาณนาฬิกาจากเซิร์ฟเวอร์ NTP ที่ระดับ Stratum 1 ซึ่งทำให้ NTP Server ภายในองค์กรเป็น Stratum 2 และตั้งค่าให้เครื่องเซิร์ฟเวอร์ อุปกรณ์ภายในเครือข่าย รวมถึงเครื่องลูกข่ายรับค่าฐานเวลาด้วยโพรโตคอล NTP ที่เซิร์ฟเวอร์นี้ เพื่อลดทราฟฟิกการใช้งาน NTP ภายในองค์กร และประสิทธิภาพของการตั้งค่าฐานเวลาผ่านโพรโตคอล NTP	✓	✓	

ข้อกำหนดการจัดเก็บข้อมูลล็อกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการตามความหมายใน พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 นั้นมีความหมายสอดคล้องกับคำว่าข้อมูลล็อกหรือ Log ซึ่งหมายถึงข้อมูลของการบันทึกเหตุการณ์ที่เกิดขึ้นจากระบบหรือเครือข่ายตามเอกสารอ้างอิง [4] หรือที่เรียกว่า Audit Trail ซึ่งได้อธิบายเพิ่มเติมในหัวข้อ "ข้อกำหนดการเก็บข้อมูลล็อกตามมาตรฐานความมั่นคงปลอดภัย ISO/IEC 27001" และในหัวข้อ "การบริหารจัดการการเก็บข้อมูลล็อกสำหรับองค์กร"

1. ข้อกำหนดการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการ

จากประกาศ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งระบุมาตราที่ 26 ไว้ว่า [1]

> **มาตรา ๒๖** ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็นพนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใดเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้
>
> ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา
>
> ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

โดยอิงจากความหมายของ "ผู้ให้บริการ" และ "ข้อมูลจราจรทางคอมพิวเตอร์" ในมาตรา 3 ไว้ว่า [1]

> "**ข้อมูลจราจรทางคอมพิวเตอร์**" หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
>
> "**ผู้ให้บริการ**" หมายความว่า
>
> (๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น
>
> (๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

เพื่อความกระจ่างและตีความถูกต้องตรงกัน พิจารณาการตีความจากเอกสาร "คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐" หรือเอกสารอ้างอิง [2] ได้อธิบายขยายความเพิ่มเติมตามมาตราที่ 26 ในบทที่ 6 ว่าด้วยความรับผิดของผู้ให้บริการและบุคคลทั่วไปไว้โดยละเอียดดังต่อไปนี้

> **มาตรา ๒๖** กำหนดหน้าที่และความรับผิดชอบ กล่าวคือผู้ให้บริการมีหน้าที่ต้องเก็บรักษาข้อมูล ๒ ประการ คือ
>
> **(๑) ข้อมูลจราจรทางคอมพิวเตอร์**
>
> ความหมายของข้อมูลจราจรทางคอมพิวเตอร์ปรากฏตามมาตรา ๓ โดยผู้ให้บริการจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์แต่อาจขยายออกไปได้กรณีที่พนักงานเจ้าหน้าที่สั่งให้เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินหนึ่งปีเป็นกรณีพิเศษเฉพาะรายและเฉพาะคราวก็ได้
>
> การกำหนดหลักเกณฑ์ในเรื่องการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ว่าจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใดนั้นจะเป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา
>
> **(๒) ข้อมูลผู้ใช้บริการ**
>
> หมายถึง ข้อมูลที่บันทึกถึงตัวตนของบุคคลในการเข้าใช้บริการทางเครือข่ายของผู้ให้บริการ ไม่ว่าจะเป็นชื่อ สกุล รหัสเลขประจำตัว user name หรือ pin code ใดๆ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูล

ของผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรา ๒๖ คือไม่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ หรือข้อมูลผู้ใช้บริการจะต้องระวางโทษตามวรรคสี่ คือปรับไม่เกินห้าแสนบาท

ประเด็นที่ต้องปฏิบัติตาม พ.ร.บ. สรุปได้ตามตาราง

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	เก็บรักษาข้อมูลจราจรคอมพิวเตอร์	ต้องเก็บรักษาข้อมูลจราจรคอมพิวเตอร์ – ตั้งแต่วันที่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์ และ – เก็บไว้ไม่น้อยกว่า 90 วัน – พนักงานเจ้าหน้าที่สามารถสั่งให้เก็บเพิ่มเติมจาก 90 วันแต่ไม่เกิน 1 ปีได้ เป็นกรณีๆ ไป	– ตัวอย่างข้อมูลจราจรคอมพิวเตอร์ เช่น ▪ ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลาชนิดของบริการหรืออื่น ๆ ▪ เวลา ไอพีแอดเดรสต้นทาง ไอพีแอดเดรสปลายทาง หมายเลขพอร์ตต้นทาง หมายเลขพอร์ตปลายทาง โพรโตคอลที่ใช้ ขนาดของข้อมูล ระยะเวลาที่ติดต่อสื่อสาร
2	พิจารณาหลักเกณฑ์การเก็บรักษาข้อมูลจราจรคอมพิวเตอร์	การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ว่าจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใดนั้นจะเป็นไปตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550	– พิจารณาตาม ประกาศราชกิจจานุเบกษาหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 หรือในเอกสารอ้างอิง [7]
3	เก็บรักษาข้อมูลผู้ใช้บริการ	ต้องเก็บรักษาข้อมูลผู้ใช้บริการ – ตั้งแต่วันที่ผู้ใช้เริ่มใช้บริการ และ – เก็บไว้ไม่น้อยกว่า 90 วันตั้งแต่การใช้บริการสิ้นสุดลง	– ตัวอย่างข้อมูลผู้ใช้บริการเช่น ▪ ชื่อ สกุล รหัสเลขประจำตัว user name หรือ pin code ▪ ชื่อ นามสกุล อีเมล์ ทะเบียนบ้าน หมายเลขบัตรประจำตัวประชาชน หรือเบอร์พาสปอร์ต รหัสยืนยันตัวบุคคล ชื่อบัญชีผู้ใช้ วันเวลาที่ลงทะเบียนใช้งานกับระบบ วันเวลาที่เข้าใช้งานระบบ

2. แนวทางปฏิบัติการเก็บข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการ

จากประเด็นข้อ 2 นั้นกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ประกาศในราชกิจจานุเบกษาเรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 ตามเอกสารอ้างอิง [7] ได้กำหนดหลักเกณฑ์การดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์ไว้โดยมีใจความว่า

อาศัยอำนาจตามความใน**มาตรา ๒๖** วรรค ๓ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ดังนั้น รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้กำหนดหลักเกณฑ์ไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

ข้อ ๓ ให้รัฐมนตรีว่าการกระทรวงเทคโนโลยีสารสนเทศและการสื่อสารรักษาการตามประกาศนี้

ข้อ ๔ ในประกาศนี้ "ผู้ใช้บริการ" หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

ข้อ ๕ ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ประเภทของผู้ให้บริการซึ่งมีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์แบ่งได้ ดังนี้

(๑) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่าง ๆ (Host Service Provider) ประกอบด้วยผู้ให้บริการดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

ง. ผู้ให้บริการร้านอินเทอร์เน็ต ดังปรากฏตามภาคผนวก ก. แนบท้ายประกาศนี้

(๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม (๑) (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่าง ๆ (Application Service Provider) ประกอบด้วยผู้ให้บริการดังภาคผนวก ก. แนบท้ายประกาศนี้

ข้อ ๖ ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องเก็บรักษา ปรากฏดังภาคผนวก ข. แนบท้ายประกาศนี้

ข้อ ๗ ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๑

(๒) ผู้ให้บริการตามข้อ ๕ (๑) ข. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามตามประเภท ชนิดและหน้าที่การให้บริการ

(๓) ผู้ให้บริการตามข้อ ๕ (๑) ค. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๒ ตามประเภท ชนิดและหน้าที่การให้บริการ

(๔) ผู้ให้บริการตามข้อ ๕ (๑) ง. มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๓

(๕) ผู้ให้บริการตามข้อ ๕ (๒) มีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามภาคผนวก ข. ๔

ทั้งนี้ ในการเก็บรักษาข้อมูลจราจรตามภาคผนวกต่าง ๆ ที่กล่าวไปข้างต้นนั้น ให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น

ข้อ ๘ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ผู้ให้บริการต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

(๒) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เช่น การเก็บไว้ใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เป็นต้น เว้นแต่ ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์กร กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) หรือบุคคลที่องค์กรมอบหมาย เป็นต้น รวมทั้งพนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้

(๓) จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ เพื่อให้การส่งมอบข้อมูลนั้น เป็นไปด้วยความรวดเร็ว

(๔) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้ (Identification and Authentication) เช่น ลักษณะการใช้บริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ 1222 หรือ Wi-Fi Hotspot ต้องสามารถระบุตัวตนของผู้ใช้บริการเป็นรายบุคคลได้จริง

(๕) ในกรณีที่ผู้ให้บริการประเภทหนึ่งประเภทใด ในข้อ ๑ ถึงข้อ ๔ ข้างต้น ได้ให้บริการในนามตนเอง แต่บริการดังกล่าวเป็นบริการที่ใช้ระบบของผู้ให้บริการซึ่งเป็นบุคคลที่สาม เป็นเหตุให้

ผู้ให้บริการในข้อ ๑ ถึงข้อ ๔ ไม่สามารถรู้ได้ว่า ผู้ใช้บริการที่เข้ามาในระบบนั้นเป็นใคร ผู้ให้บริการเช่นว่านั้นต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย

ข้อ ๙ เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที

ข้อ ๑๐ ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้

(๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

(๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

ผู้ให้บริการในแต่ละประเภทสามารถประยุกต์จากแนวทางปฏิบัติด้านล่างนี้ได้

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	พิจารณาว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการใด	เพื่อพิจารณาว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการ – 5 (1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต – 5 (2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม 5 (1)	– ประชุมหารือร่วมกันหรือจัดทำ Workshop ระหว่างผู้ประสานงาน ตัวแทนผู้ดูแลระบบ ตัวแทนผู้ดูแลระบบเครือข่าย ตัวแทนผู้พัฒนาระบบ ผู้ดูแลความมั่นคงปลอดภัย ผู้บริหารระบบสารสนเทศ เพื่อกำหนดว่าองค์กรถูกจัดให้เป็นผู้ให้บริการประเภทใด
2	จัดทำนโยบายการเก็บรักษาข้อมูลจราจร คอมพิวเตอร์ และข้อมูลผู้ใช้บริการ ตาม พ.ร.บ.	กำหนดเป็นนโยบายการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์และผู้ใช้บริการ ตาม พ.ร.บ. เพื่อกำหนดบทบาทหน้าที่ผู้ที่เกี่ยวข้อง วันที่บังคับใช้ การดำเนินการ บทลงโทษ ผู้ติดต่อประสานงานและประกาศให้เป็นที่ทราบโดยทั่วกัน และนำไปใช้ทั่วทั้งองค์กร	– นโยบายดังกล่าวควรครอบคลุมหัวข้อต่อไปนี้ ▪ นิยามที่เกี่ยวข้องเช่น ข้อมูลจราจรคอมพิวเตอร์ ข้อมูลผู้ใช้บริการ ใครเป็นผู้ใช้บริการเป็นต้น ▪ องค์กรจัดอยู่ในประเภทของผู้ให้บริการใด ▪ กำหนดรายละเอียดวันเวลาที่ดำเนินการ ▪ บทบาทหน้าที่ความรับผิดชอบของแต่ละหน่วยงาน เช่นการดำเนินการ การกำกับให้ปฏิบัติตาม การตรวจความสอดคล้องกับ พ.ร.บ. ▪ แนวทางปฏิบัติที่จำเป็นต้องดำเนินการ โดยอาจทำเป็นเอกสารกำหนดคุณสมบัติทางเทคนิคการเก็บข้อมูลล็อกแยกจากนโยบายฉบับนี้อีก 1 ฉบับ เพื่อระบุว่าในองค์กรมีเซิร์ฟเวอร์หรืออุปกรณ์ใดที่ต้องเก็บข้อมูลล็อก และดำเนินการเก็บข้อมูลล็อกให้สอดคล้องตามเอกสารอ้างอิง [7] ได้อย่างไร ▪ กำหนดหรือแต่งตั้งเจ้าหน้าที่ประสานงานกับพนักงาน

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
			เจ้าหน้าที่ของรัฐในกรณีที่ต้องการข้อมูล ▪ กำหนดหรือจัดทำบัญชีรายชื่อผู้ที่มีสิทธิเข้าถึงข้อมูลล็อก ▪ ระบุมาตรการควบคุมที่นำมาใช้เพื่อป้องกันข้อมูลล็อกให้มั่นคงปลอดภัยและเชื่อถือได้ เช่นการป้องกันการเปลี่ยนแปลงข้อมูลล็อกโดยไม่ได้รับอนุญาต การพิสูจน์ตัวตน การเข้ารหัสหรือมาตรการอื่นที่นำมาใช้เป็นต้น ▪ การทบทวนนโยบายเช่นทุก 1 ปี เป็นต้น หรือจัดให้มีการทบทวนเมื่อมีการปรับปรุงโครงสร้างพื้นฐานระบบสารสนเทศ หรือโครงสร้างธุรกิจขององค์กรเป็นต้น – นโยบายควรลงนามโดยผู้บริหารระดับสูง หรือผู้บริหารระบบสารสนเทศเป็นอย่างน้อย
3	จัดทำเอกสารและดำเนินการปฏิบัติตามข้อกำหนดคุณสมบัติที่ต้องดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการตามข้อกำหนดใน พ.ร.บ.	เพื่อใช้ในการวางแผนดำเนินงาน ตรวจสอบความสอดคล้องกับข้อกำหนดตาม พ.ร.บ. และสามารถกำหนดมาตรการในการป้องกันข้อมูลล็อก มาตรการป้องกันการเปลี่ยนแปลงข้อมูลล็อก รวมถึงมาตรการในการดำเนินการอื่นๆ	– ดำเนินการ ▪ จัดทำเอกสารเพื่อระบุว่าองค์กรจัดเป็นผู้ให้บริการประเภทใด ▪ จัดทำเอกสารกำหนดคุณสมบัติทางเทคนิคที่องค์กรต้องดำเนินการเพื่อให้สามารถเก็บข้อมูลล็อกให้สอดคล้องตามที่ พ.ร.บ. ได้กำหนดไว้ ▪ ดำเนินการประเมินความเสี่ยงเฉพาะในแง่ของเก็บข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการเพื่อหาว่าจำเป็นจะต้องดำเนินการเสริมสร้างความมั่นคงปลอดภัยหรือลดความเสี่ยงในด้านใดบ้าง ▪ ดำเนินการประเมินผลกระทบ และขีดความสามารถในการเก็บข้อมูลให้ได้ตาม พ.ร.บ. และกำหนดมาตรการเพิ่มเติม เช่นจัดซื้อเซิร์ฟเวอร์สำหรับเก็บข้อมูลล็อกโดยเฉพาะเป็นต้น ▪ กำหนดแผนการดำเนินงาน ผู้รับผิดชอบดำเนินการ เอกสารการดำเนินงาน และแนวทางการบำรุงรักษาระบบการเก็บข้อมูลล็อก

3. ข้อกำหนดการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลล็อกให้มั่นคงปลอดภัย

คำว่า "ความมั่นคงปลอดภัยของข้อมูลล็อก" อิงตามความหมายของความมั่นคงปลอดภัยระบบสารสนเทศโดยรวม หมายถึงว่าข้อมูลล็อกนั้นต้องยังคงรักษา

- **ความลับหรือ Confidentiality** ของข้อมูลล็อกให้เข้าถึงได้เฉพาะผู้ที่กำหนดหรือแต่งตั้งให้เป็นเจ้าหน้าที่ผู้เข้าถึงข้อมูลล็อก และไม่ควรจะเป็นผู้ดูแลระบบ ผู้ดูแลเครือข่าย ผู้พัฒนาแอพพลิเคชันภายในองค์กร

- **ความถูกต้องสมบูรณ์หรือ Integrity** ของข้อมูลล็อกหรือมีการกำหนดมาตรการป้องกันและตรวจจับการเปลี่ยนแปลงของข้อมูลล็อก

- **ความพร้อมใช้หรือ Availability** ของข้อมูลล็อก ซึ่งมีการจัดเก็บรักษาข้อมูลล็อกหรือ Data archival (ดูรายละเอียดเพิ่มเติมได้ที่หัวข้อ "การจัดเก็บข้อมูลล็อก" ในส่วน "Log Archival") ให้ครบตามระยะเวลารักษาข้อมูลล็อกซึ่งสอดคล้องกับข้อกำหนดทางกฎหมาย ข้อบังคับ หรือพ.ร.บ. หรือตามจุดประสงค์ขององค์กร เช่นข้อมูลล็อกตามความหมายของข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลผู้ใช้บริการต้องเก็บไว้ไม่น้อยกว่า 90 วันนับตั้งแต่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์เป็นต้น และที่สำคัญ ควรกำหนดมาตรการการสำรองข้อมูลล็อกเพื่อให้สามารถรักษาความพร้อมใช้ของข้อมูลล็อกเมื่อผู้ที่ได้รับอนุญาตต้องการใช้งานข้อมูลล็อกด้วยเช่นเดียวกัน

จากประกาศในราชกิจจานุเบกษาเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 ตามข้อ 8 และข้อ 9 หรือตามเอกสารอ้างอิง [7] นั้นต้องการให้ผู้ให้บริการต้องดำเนินการเก็บข้อมูลล็อกตามประเภทของผู้ให้บริการให้ครบถ้วนและต้องมีการรักษาข้อมูลจราจรคอมพิวเตอร์ หรือข้อมูลล็อกให้มีความมั่นคงปลอดภัยและสามารถนำมาใช้สืบสวนตามกระบวนการต่อไปได้

ข้อกำหนดดังกล่าวสามารถสรุปแนวทางการดำเนินการ โดยจัดกลุ่มตามระดับความสำคัญได้ 2 ระดับ[1] คือ

- จำเป็นต้องดำเนินการ หมายถึง เป็นกระบวนการและวิธีการที่จำเป็นต้องนำมาใช้ เพื่อให้สามารถปฏิบัติตาม หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 ตามข้อ 8 และข้อ 9 ได้เป็นอย่างน้อย อย่างไรก็ตามอาจเลือกใช้วิธีการอื่นในส่วนที่ระบุภายใต้ ควรดำเนินการได้

- ควรดำเนินการ หมายถึง เป็นกระบวนการและวิธีการที่แนะนำให้เลือกนำมาใช้ หรือเป็น Best Practice ที่สามารถนำมาใช้และเกิดผลดีในระยะยาว หรือเป็นตัวเลือกที่องค์กรโดยส่วนใหญ่แนะนำให้ทำ

โดยแบ่งเป็นประเด็นดังต่อไปนี้

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
1	ดำเนินการจัดเก็บข้อมูลล็อกตามประเภทของผู้ให้บริการ	ตรวจสอบว่าองค์กรจัดอยู่ในประเภทของผู้ให้บริการประเภทใด – 5 (1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต – 5 (2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม 5 (1)	ควรดำเนินการ – ประชุมหารือร่วมกันระหว่างที่ผู้ที่เกี่ยวข้อง และดำเนินการกำหนดคุณสมบัติรายละเอียดทางเทคนิคของการเก็บข้อมูลล็อกให้สอดคล้องตามประเภทของผู้ให้บริการ – จัดทำและดำเนินการตามนโยบายการเก็บข้อมูลจราจรคอมพิวเตอร์ – แต่งตั้งเจ้าหน้าที่ผู้เข้าถึงข้อมูลจราจรคอมพิวเตอร์และติดต่อประสานงานกับเจ้าหน้าที่พนักงานของรัฐ รวมถึงให้

[1] แนวทางการดำเนินการและตัวอย่างการดำเนินการในตารางดังกล่าว ซึ่งได้จัดระดับความสำคัญของการดำเนินการเป็น "จำเป็นต้องดำเนินการ" และ "ควรดำเนินการ" เป็นคำแนะนำจากคณะผู้เขียน ไม่ได้เป็นข้อบังคับตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 เมื่อวันที่ 23 สิงหาคม 2550 ตามข้อ 8 และข้อ 9 แต่อย่างใด (ตามหลักเกณฑ์ฯ นั้น สังเกตว่าใช้คำว่า "เช่น" เพื่อระบุแนวทางหรือตัวอย่างการดำเนินการที่เหมาะสมให้เช่นเดียวกัน)

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
		และดำเนินการจัดเก็บข้อมูลจราจรคอมพิวเตอร์	การในชั้นศาล อย่างน้อยดังนี้ ▪ เจ้าหน้าที่ที่ดูแลรักษาข้อมูลล็อก ▪ ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) ▪ ผู้บริหารองค์กร – จัดทำการเก็บข้อมูลล็อกตามรายละเอียดคุณสมบัติทางเทคนิคของการเก็บข้อมูลล็อก – ดำเนินการตรวจสอบเป็นการภายในว่าการเก็บข้อมูลล็อกนั้นสอดคล้องตามที่ พ.ร.บ. ได้กำหนดไว้แล้วหรือไม่
2	เก็บข้อมูลล็อกในสื่อ (Media) ที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง (Integrity)	กำหนดวิธีการในการจัดเก็บข้อมูลล็อกบนสื่อบันทึกข้อมูลหรือฮาร์ดดิสก์ (Harddisk) บนเซิร์ฟเวอร์หรืออุปกรณ์ที่รับประกันความคงอยู่ของข้อมูล	<u>ควรดำเนินการ</u> – จัดเก็บข้อมูลล็อกบน Harddisk ที่ใช้เทคโนโลยี RAID หรือ Redundancy Array of Independent Disks เช่น RAID 1 หรือ RAID 3 หรือ RAID 5 เป็นอย่างน้อยเพื่อป้องกันความเสียหายที่เกิดขึ้นบน Harddisk แบบถาวร หรือที่เรียกว่า Physical Error หรือ Disk Error – กำหนดวิธีการสำรองข้อมูลล็อกอย่างเป็นรูปธรรมเช่น การสำรองบนดีวีดี การสำรองบนเทปอัตโนมัติ หรือการทำ Disk mirror เป็นต้น – ในกรณีที่มีการสำรองข้อมูล ให้กำหนดวิธีการป้องกันสื่อบันทึกข้อมูลสำรองข้อมูลล็อกเช่น เทป ซีดีรอม หรือดีวีดี หรือ Harddisk เช่นจัดเก็บในบริเวณที่ปลอดภัย เช่นตู้เซฟเป็นต้น
3	ระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อ (Media) ที่เก็บข้อมูลล็อก	มีประเด็นพิจารณา 2 ประเด็น คือ – แต่งตั้งเจ้าหน้าที่ผู้เข้าถึงข้อมูลล็อก เพื่อแต่งตั้งบุคลากรหรือทีมงานผู้รับผิดชอบการดูแลการเก็บรักษาข้อมูลล็อก และติดต่อกับเจ้าหน้าที่พนักงานของรัฐในกรณีที่ต้องการข้อมูล – บุคลากรดังกล่าวไม่ควรเป็นผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย ผู้พัฒนา หรือผู้ที่เกี่ยวข้องอื่น เพื่อแยกบทบาทหน้าที่ให้ชัดเจนและเป็นการป้องกันการแก้ไขหรือเปลี่ยนแปลงข้อมูลล็อกโดยไม่ได้รับอนุญาต – กำหนดมาตรการควบคุมการเข้าถึงข้อมูลล็อก โดยการพิสูจน์ตัวตนตามรายชื่อของผู้ที่มีสิทธิเข้าถึงข้อมูลล็อกที่กำหนดไว้ รวมถึงจัดให้มีการบันทึกการเข้าถึงข้อมูล	<u>จำเป็นต้องดำเนินการ</u> – จัดทำมาตรการควบคุมทางเทคโนโลยี เช่น การกำหนดสิทธิบนอุปกรณ์ที่เก็บข้อมูลล็อกให้เป็นไปตามบัญชีรายชื่อที่กำหนดขึ้นนี้ รวมถึงจัดให้มีการบันทึกการเข้าถึงข้อมูลล็อก <u>ควรดำเนินการ</u> – จัดทำนโยบายการเก็บข้อมูลจราจรคอมพิวเตอร์ เพื่อระบุบทบาทและหน้าที่ของผู้ที่เกี่ยวข้อง – จัดทำบัญชีรายชื่อผู้ที่สามารถเข้าถึงข้อมูลล็อก และเพื่อใช้ตรวจสอบสิทธิการเข้าถึงข้อมูลล็อกโดยผู้ตรวจสอบระบบสารสนเทศในภายหลัง – จัดทำล็อกเซิร์ฟเวอร์หรือ Log Server เพื่อเก็บข้อมูลแบบ Secondary Logging เพื่อให้สามารถบริหารจัดการและควบคุมการเข้าถึงข้อมูลล็อกที่ล็อกเซิร์ฟเวอร์จากศูนย์กลางและทำให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น หาข้อมูลเพิ่มเติมได้ที่หัวข้อ Secondary Logging

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
		ล็อกทุกครั้ง	
4	มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้	การกำหนดชั้นความลับของข้อมูลเช่น ลับมาก ลับ เปิดเผยได้ โดยเฉพาะกับข้อมูลล็อก	<u>จำเป็นต้องดำเนินการ</u> – จัดทำเอกสารควบคุมชั้นความลับของข้อมูล โดยควรมีหัวข้อต่อไปนี้ ▪ ชั้นความลับของข้อมูล เช่น ลับมาก ลับ ใช้เป็นการภายใน เปิดเผยได้ ▪ ขอบเขตหรือประเภทของข้อมูลตามระดับชั้นความลับ ▪ วิธีการดำเนินการในแต่ละชั้นความลับ ตั้งแต่การสร้าง การใช้งาน การแจกจ่าย การเก็บ การส่ง การทำลาย – จัดระดับชั้นความลับของข้อมูลล็อกบนระบบ
		กำหนดวิธีการรักษาความลับตามชั้นความลับของข้อมูลล็อก	<u>จำเป็นต้องดำเนินการ</u> – จัดให้มีการดำเนินการตามเอกสารกำหนดชั้นความลับของข้อมูลโดยเฉพาะข้อมูลล็อก <u>ควรดำเนินการ</u> – กำหนดให้มีการตรวจสอบการดำเนินการตามชั้นความลับของข้อมูลล็อกเช่น ตรวจสอบโดยผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) เป็นต้น
		ออกแบบโครงสร้างพื้นฐานระบบสารสนเทศที่เอื้อให้มีการจัดเก็บข้อมูลล็อกอย่างมั่นคงปลอดภัย	<u>ควรดำเนินการ</u> – ปรับปรุงความมั่นคงปลอดภัยของเซิร์ฟเวอร์ – ดำเนินการจัดทำล็อกเซิร์ฟเวอร์หรือ Log Server – ปรับปรุงระบบเครือข่ายให้มีการแบ่งแยกเครือข่ายในการจัดเก็บล็อก – ปรับปรุงไฟร์วอลล์ให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น – การควบคุมการเข้าถึงข้อมูลล็อก – การป้องกันการเปลี่ยนแปลงข้อมูลล็อก – การเข้ารหัสข้อมูลล็อกที่จำเป็น
		กำหนดมาตรการควบคุมการเข้าถึงข้อมูลล็อก โดยการพิสูจน์ตัวตนตามรายชื่อของผู้ที่มีสิทธิเข้าถึงข้อมูลล็อกที่กำหนดไว้ รวมถึงจัดให้มีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง	<u>จำเป็นต้องดำเนินการ</u> – จัดให้มีการการพิสูจน์ตัวตนก่อนเข้าถึงข้อมูลล็อก <u>ควรดำเนินการ</u> – กำหนดให้มีการจัดทำล็อกเซิร์ฟเวอร์ที่เก็บเฉพาะข้อมูลล็อกซึ่งจะสามารถควบคุมการเข้าถึงข้อมูลล็อกได้อย่างมีประสิทธิภาพยิ่งขึ้น
		กำหนดมาตรการในการระบุการเปลี่ยนแปลงที่เกิดขึ้นบนข้อมูลล็อก และตรวจสอบได้ว่าเป็นการเปลี่ยนแปลงที่ถูกต้อง	<u>จำเป็นต้องดำเนินการ</u> – จัดให้มีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง เช่นผู้ใช้ที่เข้าถึง ไอพีแอดเดรสของผู้ใช้ที่เข้าถึงข้อมูลล็อก การลบหรือแก้ไขข้อมูลล็อก เป็นต้น <u>ควรดำเนินการ</u>

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
			– นำวิธีการ Digital Hashing มาใช้เพื่อตรวจสอบความเปลี่ยนแปลงที่เกิดขึ้นบนข้อมูลล็อก เช่นการใช้ MD5 หรือ GPG เป็นต้น – จัดเก็บข้อมูลล็อกไว้ในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียวเช่น CD-ROM เป็นต้น
		กำหนดมาตรการป้องกันการเข้าถึงหรือเปลี่ยนแปลงข้อมูลล็อกที่ส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต	ควรดำเนินการ – ออกแบบระบบเครือข่ายให้รองรับการส่งข้อมูลล็อกผ่านระบบเครือข่ายให้ปลอดภัย เช่นการแบ่งเครือข่ายของล็อกเซิร์ฟเวอร์โดยเฉพาะ การควบคุมผ่านไฟร์วอลล์เป็นต้น – เข้ารหัสข้อมูลล็อกที่มีการส่งผ่านระบบเครือข่าย เช่นเข้ารหัสข้อมูลก่อนแล้วค่อยส่งไปที่ล็อกเซิร์ฟเวอร์เป็นต้น
		ข้อมูลล็อกต้องเข้าถึงได้จากผู้ที่ได้รับอนุญาตหรือได้สิทธิและเมื่อต้องการเข้าถึงข้อมูลล็อกควรจะเข้าถึงได้ตามต้องการโดยทันที	จำเป็นต้องดำเนินการ – จัดทำระบบสำรองข้อมูลล็อก โดยกำหนดตามแผนการสำรองข้อมูลล็อก เช่นดำเนินการสำรองข้อมูลแบบ Full ทุก 1 เดือนเป็นต้น หรือการบีบข้อมูลล็อก (Archive Log) และเขียนในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียว ควรดำเนินการ – ควรกำหนดปริมาณข้อมูลล็อกที่สามารถสืบค้นได้ทันที เช่นกำหนดให้สืบค้นได้ย้อนหลังไป 10 วัน ถ้าต้องการสืบค้นย้อนหลังไปมากกว่านั้นต้องไปดึงข้อมูลจากข้อมูลในเทปสำรองข้อมูลเป็นต้น – ควรมีการกำหนดระบบทดแทนระบบเก็บข้อมูลล็อก เช่นมี 2 เซิร์ฟเวอร์ทำหน้าที่เก็บข้อมูลล็อกเป็นต้น หรือพิจารณาทำ RAID บนฮาร์ดดิสก์ที่ใช้เก็บข้อมูลล็อกเพื่อให้รองรับความเสียหายที่อาจจะเกิดขึ้นบนฮาร์ดดิสก์เพื่อเพิ่มระดับความพร้อมใช้ของการให้บริการข้อมูลล็อก – ควรมีการประเมินและติดตามปริมาณข้อมูลล็อกต่อวัน เพื่อให้สามารถวางแผนและกำหนดขีดความสามารถในการจัดเก็บข้อมูลล็อกบนเซิร์ฟเวอร์เก็บข้อมูลล็อกได้
5	จัดให้มีผู้มีหน้าที่ประสานงานและให้ข้อมูลกับพนักงานเจ้าหน้าที่ซึ่งได้รับแต่งตั้งตาม พ.ร.บ. ฯ เพื่อให้การส่งมอบข้อมูลนั้นเป็นไปด้วยความรวดเร็ว	เมื่อเกิดเหตุการณ์ที่จำเป็นต้องประสานงานขอข้อมูลจราจรคอมพิวเตอร์หรือข้อมูลผู้ใช้บริการ หรือข้อมูลล็อกแล้วองค์กรควรจะจัดให้มีเจ้าหน้าที่ที่เข้าถึงข้อมูลล็อกเพื่อส่งมอบให้พนักงานเจ้าหน้าที่ฯ ได้อย่างรวดเร็ว	ควรดำเนินการ – จัดทำนโยบายการเก็บข้อมูลจราจรคอมพิวเตอร์ และระบุบทบาทและหน้าที่ของเจ้าหน้าที่ประสานงานกับพนักงานเจ้าหน้าที่ฯ ในกรณีที่ต้องการข้อมูลล็อก – จัดทำหนังสือแต่งตั้งเจ้าหน้าที่ประสานงานอย่างเป็นทางการ เจ้าหน้าที่ดังกล่าวไม่ควรเป็นผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย ผู้พัฒนา หรือบุคลากรอื่นที่เกี่ยวข้องกับระบบที่เกี่ยวข้องกับข้อมูลล็อก

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
6	ข้อมูลจราจรคอมพิวเตอร์ต้องสามารถระบุรายละเอียดของผู้ใช้บริการเป็นรายบุคคลได้ (Identification an Authentication หรือ I&A)	ต้องจัดให้มีการดำเนินการเพื่อให้ระบบสามารถระบุและพิสูจน์ตัวตนผู้ใช้งานระบบเป็นรายบุคคลได้ โดยเฉพาะเมื่อมีการใช้ระบบต่อไปนี้ – Proxy Server หรือ Cache Server หรือ Proxy Cache หรือ Cache Engine – อุปกรณ์ที่ทำ Network Address Translation หรือ NAT – บริการเครือข่ายไร้สายแบบ Hotspot เช่น Wi-Fi Hotspot	ในกรณีที่มีการใช้งานระบบตามที่กำหนดไว้ข้างต้น ควรจัดให้ <u>ควรดำเนินการ</u> – จัดให้มีการพิสูจน์ตัวตนโดยใช้บัญชีผู้ใช้เช่น Username หรือ Login ที่กำหนด เพื่อระบุ Identification ของการใช้งาน และกำหนดวิธีการพิสูจน์ตัวตนหรือ Authentication ที่เหมาะสมเช่น ▪ ใช้ร่วมกับ What you know เช่น รหัสผ่าน หรือหมายเลข PIN ▪ ใช้ร่วมกับ What you have เช่น บัตร Smartcard ▪ ใช้ร่วมกับ What you are เช่น ลายนิ้วมือ ม่านตา หรือมือเป็นต้น ▪ ใช้มาตราการพิสูจน์ตัวตนหรือ Authentication มากกว่า 1 วิธีการเพื่อเพิ่มความมั่นคงปลอดภัยของกระบวนการ I&A นี้ – จัดทำระบบลงทะเบียนผู้ใช้งานเพื่อให้กระบวนการ Identification ด้วย Username หรือ Login ของระบบสามารถยืนยันตัวบุคคลการใช้งานระบบเป็นรายบุคคลได้จริง โดยอาจะเลือกเก็บข้อมูลเพิ่มเติมเช่น ▪ บัตรประจำตัวประชาชน ▪ หมายเลขพาสพอร์ต ▪ บัตรประจำตัวพนักงาน หรือหมายเลขประจำตัวพนักงาน ส่วนข้อมูลพนักงานสามารถใช้ข้อมูลจากฝ่ายบุคคลขององค์กรได้ เป็นต้น ▪ การยืนยันผ่านหมายเลขบัตรเครดิตจากทางธนาคารหรือผู้ให้บริการบัตรเครดิตเป็นต้น – กระบวนการ I&A ที่ดีและมีความมั่นคงปลอดภัยและสามารถยืนยันบุคคลที่ใช้เป็นรายบุคคลได้ ไม่ควรอนุญาตให้สร้างบัญชีผู้ใช้หรือ Username ที่ใช้งานร่วมกัน – นำระบบพิสูจน์ตัวตนแบบศูนย์กลางมาใช้เช่น Microsoft Active Directory หรือการควบคุมการเข้าถึงเครือข่ายด้วย Proxy แบบที่ต้องมีการพิสูจน์ตัวตนเป็นต้น
7	ใช้ระบบของบุคคลที่สามเพื่อพิสูจน์ตัวตน ต้องดำเนินการให้มีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผู้ใช้บริการผ่านบริการของตนเองด้วย	ในกรณีที่ Outsource กระบวนการพิสูจน์ตัวตนให้กับ 3rd Party หรือ Vendor ทางองค์กรต้องดำเนินการจัดให้มี I&A ของระบบที่เชื่อมต่อกับ Outsource ควบคู่ไปด้วย	

ที่	ประเด็น	แนวทางการดำเนินการ	ตัวอย่างการดำเนินการ
8	เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน ๑๐ มิลลิวินาที	กำหนดให้ปรับเวลาบนเครื่องเซิร์ฟเวอร์หรืออุปกรณ์ที่เกี่ยวข้องกับการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ให้เดินตามเวลามาตรฐาน ผ่านโพรโตคอล Network Time Protocol หรือ NTP ไปที่ NTP Server ที่มีค่าเป็น Stratum อยู่ในช่วง 1-15 เพื่อให้เวลาผิดพลาดไม่เกิน 10 มิลลิวินาที ควรเลือก NTP Server ที่มีค่า Stratum น้อยๆ ซึ่งหมายถึงเวลาจะตรงกับมาตรฐานสากลที่สุด การวิเคราะห์ข้อมูลล็อกหรือข้อมูลจราจรคอมพิวเตอร์ได้อย่างถูกต้อง ค่าเวลาที่ปรากฏบนข้อมูลล็อกต้องตรงกับเวลาจริง ดังนั้นการนำข้อมูลล็อกจากหลายแหล่งมาวิเคราะห์จะสามารถลำดับเหตุการณ์ที่เกิดขึ้นได้อย่างถูกต้อง	จำเป็นต้องดำเนินการ – จัดให้มีการตั้งสัญญาณเวลาด้วยโพรโตคอล Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ตามเอกสารอ้างอิง [9] ระบุว่าในเมืองไทยมีผู้ให้บริการ ดังต่อไปนี้ ▪ สถาบันมาตรวิทยาแห่งชาติ เครื่อง time1.nimt.or.th หรือ 203.185.69.60 ▪ กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83 ▪ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.185.129.186 หรือ 203.185.129.187 – ในต่างประเทศ ▪ National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18 – ควรกำหนดให้มีการตั้งค่าเวลาผ่าน NTP ไปที่เซิร์ฟเวอร์ NTP Server ที่มีค่า Stratum เป็น 1 อย่างน้อย 2 หรือ 3 เซิร์ฟเวอร์เป็นอย่างน้อย

การปรับค่าเวลาโดยการใช้ NTP สามารถหารายละเอียดเพิ่มเติมได้ตามเอกสารอ้างอิงต่อไปนี้

- ความหมายของคำว่า Stratum หารายละเอียดเพิ่มเติมได้ที่เอกสารอ้างอิง [10] หรือ "*การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*" ที่ http://www.thaicert.org/paper/basic/NTPandLAW.php
- การปรับแต่งค่าเวลาด้วย Network Time Protocol สำหรับเซิร์ฟเวอร์และอุปกรณ์เครือข่าย หารายละเอียดเพิ่มเติมได้ที่เอกสารอ้างอิง [11] หรือ "*คู่มือการใช้บริการ Time Server [ฉบับปรับปรุง]*" ที่ http://www.thaicert.org/paper/basic/manualTimeServer.php
- รายชื่อของเซิร์ฟเวอร์ NTP ระดับ Stratum 1 สามารถสืบค้นได้ที่ http://support.ntp.org/bin/view/Servers/StratumOneTimeServers

4. ประเภทผู้ให้บริการในการเก็บข้อมูลจราจรคอมพิวเตอร์

ลำดับถัดไปคือการประชุมหรือหารือร่วมกันในองค์กร เพื่อจัดว่าองค์กรเป็นผู้ให้บริการประเภทใด ตามเอกสารอ้างอิง [7] ซึ่งได้จำแนกประเภทของผู้ให้บริการไว้ดังนี้

ที่	ประเภทผู้ให้บริการ	ประเภท	ตัวอย่างผู้ให้บริการ
5 (1)	ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น	ก. ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	1) ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider) 2) ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider) 3) ผู้ให้บริการวงจรเช่า (Leased Circuit Service Provider) – ผู้ให้บริการ Leased Line – ผู้ให้บริการสายเช่า (Fiber Optic) – ผู้ให้บริการ ADSL (Asymmetric Digital Subscriber Line) – ผู้ให้บริการ Frame Relay – ผู้ให้บริการ ATM (Asynchronous Transfer Mode) – ผู้ให้บริการ MPLS (Multi Protocol Label Switching) ยกเว้นให้บริการเฉพาะ Physical Media หรือสายสัญญาณหรือ Cabling ซึ่งไม่มีสัญญาณ Internet หรือไม่มี IP Traffic เช่น – ผู้ให้บริการ Dark Fiber – ผู้ให้บริการสายใยแก้วนำแสง 4) ผู้ให้บริการดาวเทียม (Satellite Service Provider)
		ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	1) ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider – ISP) ทั้งมีสายและไร้สาย 2) ผู้ให้บริการซึ่งให้บริการเข้าถึงระบบเครือข่าย – ห้องพัก – ห้องเช่า – โรงแรม – ร้านอาหารเครื่องดื่ม 3) ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ สำหรับองค์กร เช่น – หน่วยงานราชการ หรือบริษัท – สถาบันการศึกษา – ธนาคาร
		ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	1) ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) การให้บริการเช่า Web Server 2) ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) 3) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) 4) ผู้ให้บริการศูนย์รับฝากข้อมูลทาง

ที่	ประเภทผู้ให้บริการ	ประเภท	ตัวอย่างผู้ให้บริการ
			อิเล็กทรอนิกส์ (Internet Data Center – IDC)
		ง. ผู้ให้บริการร้านอินเทอร์เน็ต	1) ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café’) 2) ผู้ให้บริการร้านเกมออนไลน์ (Game Online)
5 (2)	ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ 5(1)	ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชันต่างๆ (Content and Application Service Provider)	1) ผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อก (Blog) 2) ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider) 3) ผู้ให้บริการเว็บเซอร์วิส (Web Services) 4) ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

พิจารณาจากช่อง “ตัวอย่างผู้ให้บริการ” ว่าจัดอยู่ในประเภทใด องค์กรหรือหน่วยงานหนึ่งๆ อาจอยู่มากกว่าหนึ่งประเภทผู้ให้บริการได้ ตัวอย่างเช่นบริษัท X เปิดให้บริการเว็บบอร์ดสำหรับให้บริการบนอินเทอร์เน็ต และได้ให้บริการพนักงานภายในบริษัทสามารถเชื่อมต่ออินเทอร์เน็ตจากบริษัทผ่าน ADSL ของผู้ให้บริการรายหนึ่งในประเทศไทย จากตัวอย่างข้างต้นบริษัท X จัดอยู่ในประเภทผู้ให้บริการดังนี้

- เป็น “*ผู้ให้บริการเว็บบอร์ด*” ดังนั้นจัดเป็น *5 (2) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตามข้อ 5 (1)*
- เป็น “*ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ สำหรับบริษัท*” ดังนั้นจัดเป็น *5 (1) ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต* ประเภท *ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)* หรือเรียกโดยย่อว่า *5 (1) ข.*

จากตัวอย่างข้างต้นจะเห็นได้ว่าบริษัท X จัดเป็นผู้ให้บริการประเภท 5 (1) ข. และ 5 (2) ซึ่งต้องดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์ให้สอดคล้องตามเอกสารอ้างอิง [7] ต่อไปหรือตามรายละเอียดที่จะกล่าวถึงในลำดับถัดไป

5. การเก็บข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการประเภท 5 (1)

ผู้ให้บริการประเภท 5 (1) หมายถึงผู้ให้บริการ
- แก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือ
- ให้สามารถติดต่อถึงกันโดยประการอื่น

ทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น ทั้งนี้ตามเอกสารอ้างอิง [7] ได้จำแนกผู้ให้บริการประเภท 5 (1) เป็น 4 ประเภทโดยมีรายละเอียดตามลำดับดังนี้

5.1. ผู้ให้บริการประเภท 5 (1) ก. ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)

การเก็บข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการประเภท 5 (1) ก. หรือผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ซึ่งมีตัวอย่างผู้ให้บริการดังนี้

- ผู้ให้บริการโทรศัพท์พื้นฐาน (Fixed Line Service Provider)
- ผู้ให้บริการโทรศัพท์เคลื่อนที่ (Mobile Service Provider)
- ผู้ให้บริการวงจรเช่า (Leased Circuit Service Provider)
- ผู้ให้บริการ Leased Line
  - ผู้ให้บริการสายเช่า (Fiber Optic)
  - ผู้ให้บริการ ADSL (Asymmetric Digital Subscriber Line)
  - ผู้ให้บริการ Frame Relay
  - ผู้ให้บริการ ATM (Asynchronous Transfer Mode)
  - ผู้ให้บริการ MPLS (Multi Protocol Label Switching)

  ยกเว้นให้บริการเฉพาะ Physical Media หรือสายสัญญาณหรือ Cabling ซึ่งไม่มีสัญญาณ Internet หรือไม่มี IP Traffic เช่น
  - ผู้ให้บริการ Dark Fiber
  - ผู้ให้บริการสายใยแก้วนำแสง
- ผู้ให้บริการดาวเทียม (Satellite Service Provider)

ซึ่งต้องดำเนินการจัดเก็บดังต่อไปนี้

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ
ก.	ข้อมูลที่สามารถระบุและติดตามแหล่งกำเนิด ต้นทาง ปลายทาง และทางสายที่ผ่านของการติดต่อสื่อสารของระบบคอมพิวเตอร์	ข้อมูลระบบชุมสายโทรศัพท์พื้นฐาน โทรศัพท์วิทยุมือถือ และระบบตู้โทรศัพท์สาขา (Fixed Network Telephony and Mobile Telephony)
		หมายเลขโทรศัพท์ หรือ เลขหมายวงจร รวมทั้งบริการเสริมอื่นๆ เช่น บริการโอนสาย และหมายเลขโทรศัพท์ที่ได้โอนสาย รวมทั้งหมายเลขโทรศัพท์ซึ่งถูกเรียกจากโทรศัพท์ที่มีการโอน
		ชื่อ ที่อยู่ของผู้ใช้บริการหรือผู้ใช้งานที่ลงทะเบียน (Name and Address of Subscriber or Registered User)
		ข้อมูลเกี่ยวกับวันที่ เวลา และที่ตั้งของ Cell ID ซึ่งมีการใช้บริการ (Date and Time of the Initial Activation of the Service and the Location Label (Cell ID)
ข.	ข้อมูลที่สามารถระบุวันที่ เวลา และระยะเวลาของการติดต่อสื่อสารของระบบคอมพิวเตอร์	วันที่ รวมทั้งเวลาเริ่มต้นและสิ้นสุดของการใช้งาน (Fixed Network Telephony and Mobile Telephony, the Date and Time of the Start and End of the Communication)
ค.	ข้อมูลซึ่งสามารถระบุที่ตั้งในการใช้โทรศัพท์มือถือ หรืออุปกรณ์ติดต่อสื่อสารแบบไร้สาย (Mobile Communication	1) ที่ตั้ง Label ในการเชื่อมต่อ (Cell ID) ณ สถานที่เริ่มติดต่อสื่อสาร
		2) ข้อมูลซึ่งระบุที่ตั้งทางกายภาพของโทรศัพท์มือถือ อันเชื่อมโยงกับข้อมูลที่ตั้งของ Cell ID ขณะที่มีการติดต่อสื่อสาร
		3) จัดให้มีระบบบริการตรวจสอบบุคคลผู้ใช้บริการ

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ
	Equipment)	

5.2. ผู้ให้บริการประเภท 5 (1) ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) และ ผู้ให้บริการประเภท 5 (1) ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)

ผู้ให้บริการประเภท 5 (1) ข. เป็นผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ซึ่งประกอบด้วย

- ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider – ISP) ทั้งมีสายและไร้สาย
- ผู้ให้บริการซึ่งให้บริการเข้าถึงระบบเครือข่าย
  - ห้องพัก
  - ห้องเช่า
  - โรงแรม
  - ร้านอาหารเครื่องดื่ม
- ผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ สำหรับองค์กร เช่น
  - หน่วยงานราชการ
  - บริษัท
  - สถาบันการศึกษา
  - ธนาคาร

ผู้ให้บริการประเภท 5 (1) ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider) ประกอบด้วย

- ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) การให้บริการเช่า Web Server
- ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing)
- ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider)
- ผู้ให้บริการศูนย์รับฝากข้อมูลทางอิเล็กทรอนิกส์ (Internet Data Center – IDC)

ต้องดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์ที่เซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายที่ทำหน้าที่ต่อไปนี้

ที่	ประเภท	รายละเอียดทางเทคนิค	ตัวอย่างระบบ
ก.	ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	**Authentication Server** เป็นข้อมูลล็อกการพิสูจน์ตัวตนของเซิร์ฟเวอร์หรืออุปกรณ์พิสูจน์ตัวตนและกำหนดสิทธิบนการใช้งานบนระบบเครือข่าย	– เซิร์ฟเวอร์ RADIUS เช่น ▪ FreeRadius ▪ OpenRadius ▪ Microsoft Internet Authentication Service หรือ Microsoft IAS ▪ Steel Belt Radius ▪ Cisco Access Control Server (Cisco ACS) ▪ หรือเซิร์ฟเวอร์ RADIUS ตามรายชื่อในเอกสารอ้างอิง [12] – เซิร์ฟเวอร์ TACACS+ หรือเซิร์ฟเวอร์ DIAMETER – เซิร์ฟเวอร์ที่ใช้โพรโตคอล Lightweight Directory Access Protocol หรือ LDAP เช่น ▪ ไมโครซอฟต์ Active Directory ▪ Red Hat Directory Service ▪ SUN iPlanet ▪ OpenLDAP – เซิร์ฟเวอร์หรืออุปกรณ์ที่ใช้เป็น Network Access Control เพื่อควบคุมการเข้าถึงระบบเครือข่าย

ที่	ประเภท	รายละเอียดทางเทคนิค	ตัวอย่างระบบ
			▪ Cisco NAC ▪ FreeNAC ▪ เซิร์ฟเวอร์หรืออุปกรณ์ที่ใช้โพรโตคอล IEEE 802.1X เพื่อพิสูจน์ตัวตน ▪ หรือรายชื่อ NAC ตามเอกสารอ้างอิง [17] – เซิร์ฟเวอร์หรืออุปกรณ์ Proxy Server ซึ่งจัดให้มีการพิสูจน์ตัวตน ▪ Squid ที่เปิดให้มีการพิสูจน์ตัวตนก่อนการใช้งานระบบเครือข่าย ▪ Bluecoat ▪ หรือเซิร์ฟเวอร์ Proxy ตามรายชื่อในเอกสารอ้างอิง [18] – เซิร์ฟเวอร์หรืออุปกรณ์ที่ให้บริการเป็น Wireless Hotspot เช่นซอฟต์แวร์ Chillispot, NoCAT เป็นต้น
ข.	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)	**SMTP Server** หรือ **POP/IMAP Server** เป็นข้อมูลล็อกของอีเมล์เซิร์ฟเวอร์ที่สื่อสารข้อมูลด้วยโพรโตคอลต่อไปนี้ – Simple Mail Transfer Protocol หรือ SMTP – Post Office Protocol version 3 หรือ POP3 ซึ่งรวมถึง POP3S ด้วย – Internet Message Access Protocol version 4 หรือ IMAP4 ซึ่งรวมถึง IMAP4S	– เซิร์ฟเวอร์ไมโครซอฟต์ Exchange ทั้ง Backend และ Frontend Server ซึ่งรวมถึงการเปิดใช้ POP3 หรือ IMAP4 – เซิร์ฟเวอร์ที่ใช้ IBM Lotus Domino – เซิร์ฟเวอร์ที่ใช้ MailEnable – เซิร์ฟเวอร์ Merak Mail Server – เซิร์ฟเวอร์ Novell Groupwise – เซิร์ฟเวอร์ Sun Java System Messaging Server – เซิร์ฟเวอร์ Zimbra – เซิร์ฟเวอร์ Sendmail เซิร์ฟเวอร์ Postfix หรือ Qmail เป็นต้น – เซิร์ฟเวอร์ที่ให้บริการ POP3 หรือ IMAP4 ภายในองค์กรเช่นติดตั้งซอฟต์แวร์ Courier Mail Server หรือ Cyrus IMAP Server หรือ Dovecot หรือ Binc IMAP Server เป็นต้น หรือเซิร์ฟเวอร์ตามเอกสารอ้างอิง [13]
ค.	ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล	**FTP Server** เป็นข้อมูลล็อกจากเซิร์ฟเวอร์ที่ถ่ายโอนไฟล์ข้อมูลด้วยโพรโตคอล File Transfer Protocol หรือ FTP	– เซิร์ฟเวอร์ที่ใช้งานไมโครซอฟต์ Internet Information Services หรือ IIS เปิดใช้ให้บริการ FTP – เซิร์ฟเวอร์ WS_FTP Server – เซิร์ฟเวอร์ FileZilla Server – เซิร์ฟเวอร์ติดตั้ง ProFTPD หรือ VsFTPD หรือ WU-FTPD หรือเซิร์ฟเวอร์ตามเอกสารอ้างอิง [14]
ง.	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	**Web Server** เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Hypertext Transfer Protocol หรือ HTTP ซึ่งรวมถึง HTTPS	– เซิร์ฟเวอร์ Apache Web Server – เซิร์ฟเวอร์ไมโครซอฟต์ Internet Information Services หรือ IIS – เซิร์ฟเวอร์ IBM HTTP Server – เซิร์ฟเวอร์ WebLogic – เซิร์ฟเวอร์ JBoss – เซิร์ฟเวอร์ WebSphere Application Server หรือเซิร์ฟเวอร์ตามเอกสารอ้างอิง [15]
จ.	ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาด	**News Server** เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Network News	– เซิร์ฟเวอร์ไมโครซอฟต์ Exchange Server ที่เปิดใช้บริการ NNTP – เซิร์ฟเวอร์ Java Apache Mail

ที่	ประเภท	รายละเอียดทางเทคนิค	ตัวอย่างระบบ
	ใหญ่ (Usenet)	Transfer Protocol หรือ NNTP	Enterprise Server หรือ Apache James – เซิร์ฟเวอร์ Diablo หรือเซิร์ฟเวอร์ตามเอกสารอ้างอิง [16]
ฉ.	ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น		แบ่งเป็น 2 กรณีคือ – ในกรณีที่เป็นผู้ให้บริการ IRC Server และ IM Server ต้องเก็บข้อมูลล็อกบนเซิร์ฟเวอร์ทั้งหมด – ในกรณีที่ไม่ได้เป็นผู้ให้บริการสามารถเก็บข้อมูลล็อกได้ 2 รูปแบบคือ ▪ เก็บข้อมูลล็อกที่ **Firewall** หรือ **Router** ที่ใช้เป็นการเชื่อมระหว่างเครื่องผู้ใช้งานและอินเทอร์เน็ตโดยเฉพาะข้อมูลการเชื่อมต่อ ในกรณีที่มีการใช้งาน Network Address Translation หรือ NAT ต้องเก็บข้อมูล NAT เพื่อให้มีข้อมูลการเปลี่ยนไอพีแอดเดรสภายในเป็นไอพีแอดเดรสภายนอก หรือที่เรียกว่า NAT Log ▪ เก็บข้อมูลที่ **Authentication Server** เช่น Proxy Server เป็นต้น ซึ่งจะทราบว่าผู้ใช้ในเวลานั้นกำลังเริ่มต้นใช้บริการ IRC หรือ IM และสามารถเก็บบันทึกเป็นข้อมูลล็อกได้

และเอกสารอ้างอิง [7] ได้ระบุถึงข้อมูลล็อกที่ต้องมีการบันทึกโดยแยกประเภทชนิดของเซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายที่ทำหน้าที่ข้างต้น ไว้เป็นลำดับกล่าวคือ

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างข้อมูลล็อก

ก.	ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย
	
	Authentication Server เป็นข้อมูลล็อกการพิสูจน์ตัวตนของเซิร์ฟเวอร์หรืออุปกรณ์พิสูจน์ตัวตน
		1) ข้อมูลล็อกที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย หรือ Access Logs	ตัวอย่างของ Radius Log
			`Sun Mar 18 04:35:24 2008 localhost@server radiusd[2305]: Login OK: [8uJY5653/<CHAP-Password>] (from client APF2 port 7 cli 00-1B-77-F3-18-C3)`
			
			ตัวอย่าง Squid Log
			`192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET /images/bgON.gif HTTP/1.1" 304 - "http://virus.thaicert.org/stylesheets/_menu.css?1213106214" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4) Gecko/20060602 Firefox/1.5.0.4"`
			
			ตัวอย่าง Chillispot Log
			`Aug 13 20:34:05 192.168.1.21 chillispot[1099]: chilli.c: 3200: Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.1.122`
			
			`Aug 13 20:34:10 192.168.1.21`

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างข้อมูลล็อก
			chillispot[1102]: chilli.c: 3502: Successful UAM login from username=56F7hesa IP=192.168.1.122
		2) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)	Sun Mar 18 04:35:24 2008
		3) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)	ตัวอย่างของ Radius Accounting Log User-Name = “uXas36yT” ตัวอย่าง Squid Log 192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700]
		4) ข้อมูลหมายเลขอินเทอร์เน็ตที่ถูกกำหนดโดยระบบผู้ให้บริการ (Assigned IP Address)	ตัวอย่างของ Radius Accounting Log Framed-IP-Address = 192.168.1.5 ตัวอย่าง Chillispot Log Aug 13 20:34:05 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 3200: Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.12.122
		5) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้ามา (Calling Line Identification)	ตัวอย่างของ Radius Accounting Log Calling-Station-Id = “00-14-2A-4B-D8-71” NAS-IP-Address = 192.168.1.1
ข.	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers) **SMTP Server** หรือ **POP/IMAP Server** เป็นข้อมูลล็อกของอีเมล์เซิร์ฟเวอร์ที่สื่อสารข้อมูลด้วย SMTP หรือ POP3 หรือ IMAP4	1) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็กทรอนิกส์ (SMTP) ซึ่งได้แก่ - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender E-mail Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver E-mail Address) - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น	Aug 24 05:18:14 admin@example.com sendmail[10900]: m7OMIE38010900: from=<test@example.com>, size=690, class=0, nrcpts=1, msgid=<200805242102.m7OL24r5010202@example.com>, proto=ESMTP, daemon=MTA, relay=mail.example.com [14.36.11.2] Aug 24 05:18:14 admin@example.com sendmail[10202]: m7OL24r5010202: to=lersak@gmail.com, ctladdr=192.168.1.50 (0/0), delay=01:16:10, xdelay=00:00:00, mailer=relay, pri=30451, relay=[mail.example.com] [14.36.11.2], dsn=2.0.0, stat=Sent (m7OMIE38010900 Message accepted for delivery)
		2) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server)	ctladdr=192.168.1.50

ที่	ประเภท/รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างข้อมูลล็อก
		3) ข้อมูลวันและเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)	`Aug 24 05:18:14`
		4) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)	`relay=mail.example.com [14.36.11.2]`
		5) ชื่อผู้ใช้งาน (User ID) (ถ้ามี)	`Login: user=<suwarut>,`
		6) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ หรือ POP3 log หรือ IMAP4 Log	`2007-06-21 11:14:27 Info: imap-login: Login: user=<suwarut>, method=plain, rip=192.168.1.200, lip=192.168.1.35`

ค.	ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล
	
	FTP Server เป็นข้อมูลล็อกจากเซิร์ฟเวอร์ที่ถ่ายโอนไฟล์ข้อมูลด้วยโพรโตคอล File Transfer Protocol หรือ FTP
		1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล	`#Software: Microsoft Internet Information Services 5.0`
			`#Version: 1.0`
			`#Date: 2007-11-16 10:54:13`
			`#Fields: time c-ip cs-username s-port cs-method cs-uri-stem sc-status`
			`17:40:30 192.168.1.67 anonymous 21 [139]USER anonymous 331`
			`17:40:30 192.168.1.67 - 21 [139]PASS IEUser@ 530`
			`17:40:41 192.168.1.67 Administrator 21 [140]USER Administrator 331`
			`17:40:41 192.168.1.67 Administrator 21 [140]PASS - 230`

		2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)	`#Date: 2007-11-16 17:40:30`
		3) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address)	`17:40:30 192.168.1.67 anonymous 21 [139]USER anonymous 331`
		4) ข้อมลชื่อผู้ใช้งาน (User ID) (ถ้ามี)	`17:40:41 192.168.1.67 Administrator 21 [140]USER Administrator 331`
		5) ข้อมูลตำแหน่ง (Path) และ	`Mon Feb 26 12:51:52 2008 6`

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างข้อมูลล็อก
		ชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการ ส่งขึ้นมาบันทึก หรือดึงให้ข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)	`3.example.com 62823 \ /var/ftp/pubinfo/jpeg/EtaCarD.jpg b _ o a mozilla@ ftp 0 * c`

ง.	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ
	
	Web Server เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Hypertext Transfer Protocol หรือ HTTP ซึ่งรวมถึง HTTPS
		1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บ	`192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET /images/bgDIVIDER.gif HTTP/1.1" 304 - "http://www.google.com /stylesheets/_menu.css?1213106214" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4) Gecko/20060602 Firefox/1.5.0.4"`
			
			`192.168.99.7 - lersak [18/Aug/2008:21:06:48 +0700] "GET /images/bgON.gif HTTP/1.1" 304 - "http://virus.thaicert.org/stylesheets/_menu.css?1213106214" "Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.8.0.4) Gecko/20060602 Firefox/1.5.0.4"`

		2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ	`[18/Aug/2008:21:06:48 +0700]`
		3) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น	`192.168.99.7`
		4) ข้อมูลคำสั่งการใช้งานระบบ	`"GET /images/bgON.gif HTTP/1.1"`
		5) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI: Uniform Resource Identifier) เช่นตำแหน่งของเว็บเพ็จ	`"GET /images/bgON.gif HTTP/1.1"`

จ.	ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet) **News Server** เป็นข้อมูลล็อกบนเซิร์ฟเวอร์ที่สื่อสารด้วยโพรโตคอล Network News Transfer Protocol หรือ NNTP	1) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP หรือ Network News Transfer Protocol Log)	`187.58.96.87, user, 12/1/2007, 14:37:37, NNTPSVC1, NEWS_Server, 134.56.87.11, 2814, 11, 513, 220, 0, article, 6 arlQl#SH#GA.425@serve, microsoft.public.ins`
			
			`207.46.248.16, <feed>, 4/29/2007, 11:49:10, NNTPSVC1, NEWS_Server, 134.56.87.11, 890, 0, 61, 502, 0, newnews, Access Denied., microsoft.public.windows.server .sbs 060101 080000 GMT,`

		2) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to	`187.58.96.87, user, 12/1/2007, 14:37:37,`
			
			`207.46.248.16, <feed>, 4/29/2007, 11:49:10`

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างข้อมูลล็อก
		Server)	
		3) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID)	-
		4) ข้อมูลชื่อเครื่องให้บริการ (Host Name)	NNTPSVC1, NEWS_Server
		5) ข้อมูลหมายเลขลำดับข้อความที่ได้ถูกส่งไปแล้ว (Posted Message ID)	article, 6 arlQl#SH#GA.425@serve,
ฉ.	ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	1) ข้อมูลเกี่ยวกับวัน เวลาการติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server)	1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT login.live.com:443/ - DIRECT/login.live.com - CMF:40 DCF:20 ERR:0 DEFAULT_CASE-DefaultGroup
		2) ข้อมูลชื่อเครื่องบนเครือข่าย (Client Hostname and/or IP Address)	1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT login.live.com:443/ - DIRECT/login.live.com
		3) หมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Destination Hostname and/or IP Address)	1205326745.661 1912 192.168.42.165 TCP_MISS/200 8460 CONNECT login.live.com:443/ - DIRECT/login.live.com

และหาข้อมูลเพิ่มเติมได้ที่เอกสารอ้างอิง [19]

5.3. ผู้ให้บริการประเภท 5 (1) ง. ผู้ให้บริการร้านอินเทอร์เน็ต

ผู้ให้บริการประเภท 5 (1) ง. เป็นผู้ให้บริการร้านอินเทอร์เน็ต ประกอบด้วย

- ผู้ให้บริการร้านอินเทอร์เน็ต (Internet Café)
- ผู้ให้บริการร้านเกมออนไลน์ (Game Online)

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างการดำเนินการ
ก.	ผู้ให้บริการร้านอินเทอร์เน็ต	1) ข้อมูลที่สามารถระบุตัวบุคคล	บัญชีผู้ใช้ที่ล็อกอินเข้าใช้งานภายในร้าน ทั้งผ่านระบบปฏิบัติการหรือผ่าน Proxy Server และบัญชีผู้ใช้นั้นควรจะมีผูกพันถึง – บัตรประจำตัวประชาชนของผู้เข้ามาใช้บริการ หรือ – ทะเบียนบ้าน หรือ – รูปถ่ายจากเว็บแคมเป็นต้น บางร้านใช้ระบบสมาชิก ในการเก็บบันทึกเพียงครั้งแรกครั้งเดียว
		2) เวลาของการเข้าใช้ และเลิกใช้บริการ	– วันและเวลาที่เริ่มต้นใช้งาน – วันและเวลาที่หยุดใช้งาน – ระยะเวลาการใช้งาน – เครื่องคอมพิวเตอร์ที่ใช้งาน – หมายเลขไอพีที่ใช้งาน ข้อมูลดังกล่าวนี้สามารถบันทึกด้วยการนำระบบ Proxy Server หรือ Authentication Gateway มาใช้
		3) หมายเลขเครื่องที่ใช้ IP Address (Internet Protocol Address)	

6. การเก็บข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการประเภท 5 (2)

หมายถึงผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ 5(1) ซึ่งหมายถึงผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชันต่างๆ (Content and Application Service Provider) ประกอบด้วย

- ผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อก (Blog)
- ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking)
- ผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider)
- ผู้ให้บริการเว็บเซอร์วิส (Web Services)
- ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

จากเอกสารอ้างอิง [7] ได้กำหนดรายละเอียดไว้ดังนี้

ที่	ประเภท/ รายละเอียดทางเทคนิค	รายการข้อมูลล็อกที่ต้องจัดเก็บ	ตัวอย่างการดำเนินการ
ก.	ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	1) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือเลขประจำตัว (User ID) ของผู้ขายสินค้าหรือบริการ หรือเลขประจำตัวผู้ใช้บริการ (User ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ	– จัดทำระบบสมาชิกหรือระบบลงทะเบียนสมัครเพื่อบันทึกข้อมูลประจำตัวผู้ใช้ ก่อนการใช้งานบริการ เช่นข้อมูลชื่อนามสกุล อีเมล์ หมายเลขบัตรประจำตัวประชาชนเป็นต้น – กำหนดวิธีการยืนยันผู้ใช้งานที่ระบุตัวตนผู้ใช้ได้จริง เช่น ▪ อีเมล์ในกรณีที่สามารถผูกพันบัญชีอีเมล์กับตัวตนได้จริง เช่นผู้ใช้ภายในองค์กร ▪ หมายเลขบัตรประจำตัวประชาชนหรือหมายเลขพาสพอร์ต ซึ่งต้องกำหนดวิธีการตรวจสอบความถูกต้อง ▪ หมายเลขบัตรเครดิต ซึ่งสามารถทดสอบตัดเงินจริงและวิธีการตรวจสอบว่าตัดเงินเป็นจำนวนเท่าใด เพื่อยืนยันตัวเจ้าของบัตรเป็นต้น – ทุกครั้งที่ผู้ใช้ล็อกอินเพื่อเข้าสู่ระบบต้องบันทึกชื่อบัญชีผู้ใช้หรือ Username ที่ใช้ วันเวลาที่เข้ามาและไอพีแอดเดรสที่เข้ามาด้วย
		2) บันทึกข้อมูลการเข้าใช้บริการ	– วันและเวลาที่เริ่มต้นใช้งาน – วันและเวลาที่หยุดใช้งาน – ระยะเวลาการใช้งาน – หมายเลขไอพีที่ใช้งาน – ข้อมูลที่เข้าถึง เช่นเว็บเพจเป็นต้น หรือไฟล์ข้อมูลที่เข้าถึง
		3) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล	– วันและเวลาที่ประกาศข้อความ – ไอพีแอดเดรสที่ใช้ – ข้อความที่ประกาศ – ข้อมูลที่เกี่ยวข้องอื่นๆ

7. การเริ่มเก็บข้อมูลจราจรคอมพิวเตอร์ของผู้ให้บริการ

จากเอกสารอ้างอิง [7] ได้กำหนดให้ผู้ให้บริการแต่ละประเภทเริ่มดำเนินการเก็บข้อมูลจราจรคอมพิวเตอร์ โดยมีรายละเอียดดังนี้

> **ข้อ ๑๐** ผู้ให้บริการซึ่งมีหน้าที่เก็บข้อมูลจราจรทางคอมพิวเตอร์ตามข้อ ๗ เริ่มเก็บข้อมูลดังกล่าวตามลำดับ ดังนี้
>
> (๑) ผู้ให้บริการตามข้อ ๕ (๑) ก. เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นสามสิบวันนับจากวันประกาศในราชกิจจานุเบกษา
>
> (๒) ให้ผู้ให้บริการตามข้อ ๕ (๑) ข. เฉพาะผู้ให้บริการเครือข่ายสาธารณะหรือผู้ให้บริการอินเทอร์เน็ต (ISP) เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศในราชกิจจานุเบกษา
>
> ผู้ให้บริการอื่นนอกจากที่กล่าวมาในข้อ ๑๐ (๑) และข้อ ๑๐ (๒) ข้างต้น ให้เริ่มเก็บข้อมูลจราจรทางคอมพิวเตอร์เมื่อพ้นหนึ่งปีนับจากวันประกาศในราชกิจจานุเบกษา

และสามารถสรุป โดยแยกประเภทของผู้ให้บริการตาม 5 (1) และ 5 (2) ได้ตามตาราง

ที่	ประเภทผู้ให้บริการ	ประเภท	การเริ่มเก็บข้อมูลจราจรคอมพิวเตอร์
5 (1)	ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น ทั้งนี้โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือเพื่อประโยชน์ของบุคคลอื่น	ก. ผู้ประกอบกิจการโทรคมนาคมและกิจการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)	23 กันยายน 2550
		ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) เฉพาะ ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider – ISP) ทั้งมีสายและไร้สาย	23 กุมภาพันธ์ 2551
		ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider)	23 สิงหาคม 2551
		ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์เพื่อให้บริการโปรแกรมประยุกต์ต่างๆ (Hosting Service Provider)	
		ง. ผู้ให้บริการร้านอินเทอร์เน็ต	
5 (2)	ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลตาม ข้อ 5(1)	ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชันต่างๆ (Content and Application Service Provider)	

ข้อกำหนดการเก็บข้อมูลล็อกตามมาตรฐานความมั่นคงปลอดภัย ISO/IEC 27001

ข้อมูลล็อกในความหมายตามมาตรฐานความมั่นคงปลอดภัย ISO/IEC 27001 หมายถึงข้อมูลที่เป็นการบันทึกเหตุการณ์ที่เกิดขึ้นบนระบบ อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เครือข่าย และมีความหมายเดียวกันกับข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการตามที่ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

หรือกล่าวได้ว่าข้อมูลจราจรคอมพิวเตอร์และข้อมูลผู้ใช้บริการตามความหมายใน พ.ร.บ. นั้นเป็นข้อมูลที่ระบบหรืออุปกรณ์คอมพิวเตอร์ทำการบันทึกไว้หรือเรียกว่าข้อมูลล็อกหรือ Log ซึ่งควรจะมี วันเวลาของเหตุการณ์ ข้อมูลที่เกี่ยวข้องเช่น ถ้าเป็นทราฟฟิกเครือข่ายหรือข้อมูลการติดต่อจะมีข้อมูลไอพีแอดเดรสต้นทาง ปลายทาง โพรโตคอลที่ใช้ซึ่งสอดคล้องตามความหมายของคำว่าข้อมูลจราจรคอมพิวเตอร์ ในกรณีที่เป็นการทำงานของแอพพลิเคชัน ข้อมูลล็อกดังกล่าวควรมีการบันทึกวันเวลาการเชื่อมต่อ ฟังก์ชันของแอพพลิเคชันที่เรียกใช้ ชื่อบัญชีผู้ใช้ที่ใช้งาน ซึ่งสอดคล้องกับความหมายของข้อมูลผู้ใช้บริการ

โดยสรุปคำว่า "ข้อมูลล็อก" มีความหมายรวมความว่าเป็นได้ทั้ง "ข้อมูลจราจรคอมพิวเตอร์" หรือเป็น "ข้อมูลผู้ใช้บริการ" ก็ได้ขึ้นอยู่กับว่าจะมองในมุมใด

ข้อปฏิบัติที่ต้องกระทำให้สอดคล้องตามที่ พ.ร.บ.ฯ ได้กำหนดไว้คือ

- ในกรณีที่ข้อมูลล็อกบนระบบทั้งเซิร์ฟเวอร์ และระบบเครือข่าย หรือแอพพลิเคชัน ไม่ได้มีการจัดเก็บตามที่ พ.ร.บ.ฯ ได้กำหนดไว้ต้องดำเนินการปรับแต่งค่าบนอุปกรณ์ เซิร์ฟเวอร์ แอพพลิเคชันให้ดำเนินการเก็บข้อมูลล็อกให้ได้ตามประเภทของผู้ให้บริการ
- จัดให้มีการกำหนดมาตรการป้องกันข้อมูลล็อกให้มีความมั่นคงปลอดภัยและเชื่อถือได้
- แต่งตั้งเจ้าหน้าที่ในองค์กรหรือหน่วยงานเพื่อติดต่อประสานงานกับพนักงานเจ้าหน้าที่ที่ได้รับแต่งตั้งของรัฐ เพื่อสะดวกรวดเร็วเมื่อมีเหตุการณ์ที่ขัดต่อ พ.ร.บ. หรือเมื่อพนักงานเจ้าหน้าที่ต้องการข้อมูล

ตามหนังสือ มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550 ในเอกสารอ้างอิง [3] ได้กล่าวถึงมาตราการการเฝ้าระวังทางด้านความมั่นคงปลอดภัยในหน้า 41 ไว้โดยมีรายละเอียดดังต่อไปนี้

> **6.10 การเฝ้าระวังทางด้านความมั่นคงปลอดภัย (Monitoring)**
> **จุดประสงค์** เพื่อตรวจจับกิจกรรมการประมวลผลสารสนเทศที่ไม่ได้รับอนุญาต
>
> **6.10.1** การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)
> (หัวหน้างานสารสนเทศ) ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้
>
> **6.10.2** การตรวจสอบการใช้งานระบบ (Monitoring system use)
> (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีขั้นตอนปฏิบัติ เพื่อตรวจสอบการใช้งานทรัพย์สินสารสนเทศอย่างสม่ำเสมอ อาทิ เพื่อดูว่ามีสิ่งผิดปกติเกิดขึ้นหรือไม่
>
> **6.10.3** การป้องกันข้อมูลบันทึกเหตุการณ์ (Protection of log information)
> (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีมาตรการป้องกันข้อมูลบันทึกกิจกรรมและเหตุการณ์ต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขโดยไม่ได้รับอนุญาต
>
> **6.10.4** บันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบ (Administrator and operator logs)
> (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบหรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่นๆ
>
> **6.10.5** การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)
> (หัวหน้างานสารสนเทศ) ต้องกำหนดให้มีการบันทึกเหตุการณ์ข้อผิดพลาดต่างๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ วิเคราะห์ข้อผิดพลาดเหล่านั้น และดำเนินการแก้ไขตามสมควร
>
> **6.10.6** การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)

(ผู้ดูแลระบบ) ต้องตั้งเวลาของเครื่องคอมพิวเตอร์ทุกเครื่องในสำนักงานให้ตรงกันโดยอ้างอิงจากแหล่งเวลาที่ถูกต้องเพื่อช่วยในการตรวจสอบช่วงเวลา หากเครื่องคอมพิวเตอร์ขององค์กรถูกบุกรุกอ้างอิงตามมาตรฐาน ISO/IEC 27001 และ ISO/IEC 17799 หรือตามเอกสารอ้างอิง [8] แล้ว สามารถกำหนดแนวทางการบริหารจัดการข้อมูลล็อกภายในองค์กร ได้ดังต่อไปนี้

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานสารสนเทศ (Audit logging)	กำหนดให้มีการเก็บข้อมูลล็อกของเซิร์ฟเวอร์และอุปกรณ์ภายในระบบสารสนเทศ เพื่อให้สามารถติดตามกิจกรรมการใช้งานของผู้ใช้ การโจมตีระบบเครือข่ายเช่น Denial of Service หรือการโจมตีเพื่อให้ปฏิเสธการให้บริการ หรือเหตุการณ์ที่กระทบกับความมั่นคงปลอดภัยระบบสารสนเทศ	– ควรกำหนดให้มีการเก็บข้อมูลล็อกที่สำคัญตัวอย่างเช่น ▪ ชื่อผู้ใช้งาน ▪ วันเวลา และเหตุการณ์ที่เกิดขึ้น เช่นการล็อกอิน ▪ หมายเลขไอพีแอดเดรสที่เชื่อมต่อเข้ามา รวมถึงโพรโตคอลการเชื่อมต่อที่ใช้งาน ▪ สถานะของเหตุการณ์เช่น ถ้าเป็นล็อกอินต้องระบุว่าสำเร็จ ในกรณีที่ไม่สำเร็จควรระบุเหตุผลที่ไม่สำเร็จเช่นรหัสผ่านผิดพลาด ▪ ข้อมูลของเหตุการณ์ เช่นถ้ามีการแก้ไขเปลี่ยนแปลงไฟล์บนระบบ ควรมีการบันทึกว่าผู้ใช้งานทำการเปลี่ยนแปลงไฟล์ใดถูกเปลี่ยนแปลง ข้อมูลที่ถูกเปลี่ยนแปลง ▪ ข้อมูลอื่นที่สำคัญต่อการติดตามกิจกรรมที่เกิดขึ้นกับระบบเป็นต้น
		กำหนดให้ดำเนินการเก็บข้อมูลล็อกตามระยะเวลาที่กำหนด	– ตัวอย่างเช่นถ้าเป็นผู้ให้บริการตาม พ.ร.บ. ฯ ต้องกำหนดให้มีการเก็บข้อมูลล็อกมีระยะเวลาไม่น้อยกว่า 90 วันนับตั้งแต่ข้อมูลเข้าสู่ระบบคอมพิวเตอร์เป็นต้น
		กำหนดเหตุการณ์ในการเฝ้าระวังโดยพิจารณาจากข้อมูลล็อก ทั้งนี้เพื่อให้มีการติดตามเหตุการณ์ความผิดปกติที่เกิดขึ้นนำไปสู่การแก้ไขปัญหาเพื่อหาสาเหตุของปัญหาที่แท้จริง	– ตัวอย่างเหตุการณ์ที่ควรกำหนดให้เฝ้าระวังจากข้อมูลล็อกเช่น ▪ ความพยายามในการล็อกอินผิดพลาดจำนวน 3 ครั้ง (หรือเท่ากับที่กำหนดไว้) ▪ การล็อกอินเข้าใช้งานระบบในช่วงเวลาหลังเลิกงานเช่น 18.00 ถึง 8.00 ▪ การเพิ่มสิทธิบนระบบ ▪ การเปลี่ยนแปลงแก้ไข ข้อมูลหรือไฟล์บนระบบงานสำคัญ ▪ การเพิ่มขึ้นของทราฟฟิกในระบบเครือข่ายอย่างผิดปกติ ▪ ปริมาณการใช้งานพื้นที่ของฮาร์ดดิสก์มากเกินกว่า 70% เป็นต้น
2	การตรวจสอบการใช้งานระบบ (Monitoring system use)	กำหนดขั้นตอนปฏิบัติในการเฝ้าระวังและติดตามการตรวจสอบข้อมูลล็อก เพื่อตรวจสอบความผิดปกติในระบบสารสนเทศตามที่กำหนดไว้	– ขั้นตอนปฏิบัติในการเฝ้าระวังเช่น ▪ ขั้นตอนปฏิบัติรับมือกับเหตุการณ์แพร่ระบาดของไวรัสในองค์กร ▪ ขั้นตอนปฏิบัติเมื่อระบบถูกบุกรุกโดยไม่ได้รับอนุญาต – กำหนดความถีและบุคลากรในการติดตามเฝ้าระวังข้อมูลล็อก เช่นทุก 1

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
			วันเป็นต้น
3	การป้องกันข้อมูลล็อกบันทึกเหตุการณ์ (Protection of log information)	กำหนดมาตรการป้องกันข้อมูลล็อกที่บันทึกเหตุการณ์ที่เกิดขึ้นกับระบบสารสนเทศจากการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต	– ระบุบุคลากร ไอพีแอดเดรสของบุคลากรผู้ที่มีสิทธิเข้าถึงข้อมูลล็อกบนล็อกเซิร์ฟเวอร์ – กำหนดมาตราการควบคุมการเข้าถึงให้สอดคล้องกับรายชื่อของผู้ที่มีสิทธิเข้าถึงข้อมูลล็อก – ข้อมูลล็อกบนล็อกเซิร์ฟเวอร์ควรจะเข้าถึงได้เฉพาะเจ้าหน้าที่ที่ได้รับการติดตั้งเป็นการเฉพาะ และไม่ควรเป็นผู้ดูแลระบบ เพื่อป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต – จัดทำ Data Hashing เพื่อระบุการเปลี่ยนแปลงที่เกิดขึ้นกับล็อกไฟล์
4	การบันทึกเหตุการณ์ข้อผิดพลาด (Fault logging)	กำหนดขั้นตอนปฏิบัติเพื่อรับมือกับข้อมูลล็อกของข้อผิดพลาดการทำงานของระบบสารสนเทศ เช่น รวมไปถึงจัดให้มีการทบทวนข้อมูลล็อกเพื่อวิเคราะห์ความผิดพลาดและมุ่งเน้นวิธีการแก้ไขปัญหาในระยะยาว	– เมื่อมีการพัฒนาแอพพลิเคชันต้องมีการกำหนดให้มีการบันทึกข้อผิดพลาดหรือ Error จากการทำงานหรือเมื่อต้องรับข้อมูลจากผู้ใช้
5	การตั้งเวลาของเครื่องคอมพิวเตอร์ให้ตรงกัน (Clock synchronization)	ตั้งเวลาของเครื่องเซิร์ฟเวอร์และอุปกรณ์บนเครือข่ายให้ตรงกัน โดยอ้างอิงเวลาจากแหล่งเวลาที่ถูกต้อง เพื่อให้สามารถลำดับเวลาของเหตุการณ์ที่เกิดขึ้น และวิเคราะห์ข้อมูลล็อกได้อย่างถูกต้อง	– จัดให้มีการตั้งสัญญาณเวลาด้วยโพรโตคอล Network Time Protocol หรือ NTP ไปยังเซิร์ฟเวอร์ที่ให้บริการข้อมูลเวลาอย่างน้อยที่เป็น Stratum 1 ตามเอกสารอ้างอิ [9] ระบุว่าในเมืองไทยมีผู้ให้บริการดังต่อไปนี้ ▪ สถาบันมาตรวิทยาแห่งชาติ เครื่อง time1.nimt.or.th หรือ 203.185.69.60 ▪ กรมอุทกศาสตร์ กองทัพเรือ เครื่องเซิร์ฟเวอร์ time.navy.mi.th หรือ 118.175.67.83 ▪ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทยหรือ ThaiCERT เครื่องเซิร์ฟเวอร์ clock.thaicert.org หรือ 203.185.129.186 หรือ 203.185.129.187 – ในต่างประเทศ ▪ National Institute of Standards and Technology ประเทศสหรัฐอเมริกา เครื่องเซิร์ฟเวอร์ time.nist.gov หรือ 192.43.244.18

การบริหารจัดการการเก็บข้อมูลล็อกสำหรับองค์กร

ข้อมูลล็อกหรือ Log หมายถึงข้อมูลของการบันทึกเหตุการณ์ที่เกิดขึ้นจากระบบหรือเครือข่าย [4] หรือเรียกว่า Audit Trail ข้อมูลล็อกนำมาใช้เป็นข้อมูลเพื่อ

- วิเคราะห์ปัญหาที่เกิดขึ้นกับระบบหรือเครือข่าย เพื่อนำไปสู่การแก้ไขปัญหาทั้งระยะสั้นหรือการแก้ไขปัญหาชั่วคราว และระยะยาวหรือการแก้ไขปัญหาถาวร
- ปรับปรุงประสิทธิภาพของระบบและเครือข่ายภายในองค์กร
- วิเคราะห์ปัญหาทางด้านความมั่นคงปลอดภัย เช่นการโจมตีทางเว็บเซิร์ฟเวอร์ การเข้าถึงระบบโดยไม่ได้รับอนุญาต การส่งข้อความบิดเบือนข้อเท็จจริง หรือการส่งสแปมเมล์เป็นต้น

ดังนั้นจากที่ได้กล่าวไปแล้วคำว่า ข้อมูลล็อกหรือ Log หรือ Audit Trail หรือข้อมูลจราจรคอมพิวเตอร์ หรือข้อมูลผู้ใช้บริการที่ได้นิยามไว้ใน พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และที่ได้กำหนดจากมาตรฐาน ISO/IEC 27001 นั้นเป็นคำเดียวกัน หรือเป็นข้อมูลที่เกิดจากการบันทึกเหตุการณ์ที่เกิดขึ้นของระบบสารสนเทศภายในองค์กรหรือหน่วยงานนั้นๆ

ความสำคัญของกระบวนการบริหารจัดการข้อมูลล็อกระบบคอมพิวเตอร์เพื่อให้สามารถรองรับการขยายตัวของระบบแอพพลิเคชัน หรือความต้องการของทั้งองค์กรภาครัฐและภาคเอกชนที่นำระบบคอมพิวเตอร์หรือระบบสารสนเทศมาใช้เพิ่มมากขึ้น ต้องคำนึงถึงข้อมูลล็อกจากที่เกิดขึ้นจากระบบสารสนเทศ การส่งข้อมูลล็อก การเก็บข้อมูลล็อก การควบคุมการเข้าถึงข้อมูลล็อก การวิเคราะห์ข้อมูลล็อก และการทำลายข้อมูลล็อก

ในเอกสารฉบับนี้คำว่า "ล็อก" และ "ข้อมูลล็อก" มีความหมายเช่นเดียวกัน

1. การบริหารจัดการข้อมูลล็อก (Log management)

การบริหารจัดการเก็บข้อมูลล็อกที่ดี ควรพิจารณาทางเลือกการดำเนินการดังต่อไปนี้

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	กำหนดความสำคัญของการจัดเก็บข้อมูลล็อก	กำหนดความต้องการในการเก็บข้อมูลล็อกและจัดให้มีการเก็บข้อมูลล็อก ติดตามการเก็บข้อมูลล็อก กระบวนการนำข้อมูลล็อกมาใช้วิเคราะห์เพื่อหาสาเหตุของปัญหาทางด้านความมั่นคงปลอดภัยที่เกิดขึ้น หรือปรับปรุงประสิทธิภาพของการให้บริการ	– ความสำคัญของการจัดเก็บข้อมูลล็อกในประเทศไทยเนื่องมาจาก พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่กำหนดให้ผู้บริการต้องมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ตามมาตราที่ 26 เป็นต้น
2	จัดทำนโยบายและขั้นตอนปฏิบัติในการบริหารจัดการข้อมูลล็อก (Policies and Procedures for Log Management)	เพื่อระบุนโยบายจากฝ่ายบริหารตามความต้องการของการเก็บข้อมูลล็อก และระบุขั้นตอนปฏิบัติเพื่อให้ผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย ผู้พัฒนาระบบจัดทำและดำเนินการเก็บล็อกตามขั้นตอนปฏิบัติให้ครบถ้วน และสอดคล้องตามนโยบายที่ได้กำหนดขึ้น นอกจากนี้ควรจัดให้มีการตรวจสอบหรือ Audit การบริหารจัดการข้อมูลล็อกเพื่อตรวจสอบการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติขององค์กร	– นโยบายการจัดเก็บข้อมูลล็อกสำหรับองค์กร (ดูรายละเอียดการจัดทำนโยบายได้ที่ นโยบายการเก็บรักษาข้อมูลจราจรคอมพิวเตอร์) – นโยบายการทำลายข้อมูลล็อก – ขั้นตอนปฏิบัติสำหรับการจัดทำล็อกเซิร์ฟเวอร์ – ขั้นตอนปฏิบัติสำหรับการเก็บข้อมูลล็อกสำหรับระบบปฏิบัติการ Microsoft Windows
3	จัดทำระบบจัดเก็บข้อมูลล็อกอย่างมั่นคง	โดยออกแบบโครงสร้างพื้นฐานระบบสารสนเทศที่เอื้อให้มีการจัดเก็บข้อมูลล็อกอย่างมั่นคง	– ปรับปรุงความมั่นคงปลอดภัยของเซิร์ฟเวอร์ – ดำเนินการจัดทำล็อกเซิร์ฟเวอร์หรือ

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
	ปลอดภัย	ปลอดภัย	Log Server – ปรับปรุงระบบเครือข่ายให้มีการแบ่งแยกเครือข่ายในการจัดเก็บล็อก – ปรับปรุงไฟร์วอลล์ให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น – การควบคุมการเข้าถึงข้อมูลล็อก – การป้องกันการเปลี่ยนแปลงข้อมูลล็อก – การเข้ารหัสข้อมูลล็อกที่จำเป็น
4	กำหนดหน้าที่ความรับผิดชอบในการบริหารจัดการข้อมูลล็อก	โดยระบุผู้ที่มีหน้าที่รับผิดชอบในการดำเนินการจัดเก็บข้อมูลล็อก บุคลากรในการจัดทำนโยบายการเก็บข้อมูลล็อก บุคลากรในการปรับปรุงระบบเครือข่ายให้มั่นคงปลอดภัยและเอื้อต่อการเก็บข้อมูลล็อก การจัดอบรมสร้างความตระหนักในการจัดทำระบบเก็บข้อมูลล็อก หรือการอบรมการใช้วิเคราะห์ข้อมูลล็อก การสำรองข้อมูลล็อก การกำหนดการเข้าถึงข้อมูลล็อกเป็นต้น	– หน้าที่ความรับผิดชอบของฝ่ายบริหารต่อการเก็บข้อมูลล็อก – หน้าที่ความรับผิดชอบของผู้ดูแลระบบ ผู้ดูแลเครือข่าย และผู้พัฒนาระบบ

การออกแบบการบริหารจัดการข้อมูลล็อก มีประเด็นที่ควรคำนึงถึงหลายประการ ทั้งจากข้อมูลล็อกมีต้นกำเนิดจากแหล่งข้อมูลล็อกหลายแหล่งเช่นข้อมูลล็อกจากระบบปฏิบัติการ ข้อมูลล็อกจากแอพพลิเคชัน หรือจากการจัดการความแตกต่างของข้อมูลล็อก เช่นรูปแบบของวันเวลาจากข้อมูลล็อกบนระบบปฏิบัติการไม่เหมือนกับรูปแบบวันเวลาของข้อมูลล็อกจากแอพพลิเคชัน หรือเวลาบนข้อมูลล็อกไม่ตรงกัน ซึ่งสามารถทำให้การวิเคราะห์ข้อมูลล็อกไม่ถูกต้องได้ ยังมีประเด็นเรื่องของความถูกต้อง ความปลอดภัยในการจัดเก็บและส่งข้อมูลล็อก ซึ่งส่งผลโดยตรงต่อการนำข้อมูลล็อกไปวิเคราะห์ ที่สำคัญคือผู้วิเคราะห์ล็อกควรเป็นผู้เชี่ยวชาญที่ผ่านการอบรม ผ่านการประเมินหรือมีประสบการณ์ในการวิเคราะห์ข้อมูลล็อกโดยตรง เพื่อป้องกันความผิดพลาดจากการวิเคราะห์และแปลผลจากข้อมูลล็อกอีกปัญหาหนึ่งด้วย

1.1. การสร้างและการจัดเก็บข้อมูลล็อก

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่าง
1	จำนวนของข้อมูลล็อกจากต้นกำเนิดข้อมูลล็อก	การพิจารณาการเก็บข้อมูลล็อกควรพิจารณาจากจำนวนข้อมูลล็อกที่เกิดจากระบบนั้นว่ามีแหล่งกำเนิดข้อมูลล็อกที่แตกต่างกันเป็นจำนวนเท่าใดมาจากแหล่งกำเนิดใดบ้าง	– ตัวอย่างที่ 1 ข้อมูลล็อกจากเว็บเซิร์ฟเวอร์ ประกอบไปด้วยข้อมูลล็อกของระบบปฏิบัติการ และข้อมูลล็อกของเว็บเซิร์ฟเวอร์แอพพลิเคชัน รวมเป็นข้อมูลล็อก 2 แหล่งเป็นต้น – ตัวอย่างที่ 2 ข้อมูลล็อกของแอพพลิเคชันพัฒนาให้มีการจับเก็บข้อมูลล็อกแยกระหว่างล็อกของการพิสูจน์ตัวตน (Authentication log) และล็อกของการทำงานของแอพพลิเคชัน (Operation log)
2	รูปแบบของข้อมูลล็อก	การวิเคราะห์หาความสัมพันธ์ของเหตุการณ์จากข้อมูลล็อกจำเป็นต้องมีการปรับรูปแบบข้อมูลล็อกให้อยู่ในรูปแบบเดียวกัน ทั้งนี้เพื่อความสะดวกในการจัดเก็บข้อมูล ความถูกต้องแม่นยำในการวิเคราะห์ข้อมูล รวมถึงป้องกันความสับสนขณะวิเคราะห์ข้อมูลล็อกได้อีกทางหนึ่งด้วย	รูปแบบของข้อมูลล็อกที่มีความแตกต่าง – กรณีที่หนึ่ง เป็นการเก็บข้อมูลที่ไม่เหมือนกัน ตัวอย่างเช่นข้อมูลล็อกจากอุปกรณ์เครือข่ายจากอุปกรณ์ A บันทึกข้อมูลทั้งไอพีแอดเดรสและชื่อผู้ใช้ที่ล็อกอินเข้าสู่ระบบ แต่อุปกรณ์เครือข่ายจากอุปกรณ์ B บันทึกเฉพาะชื่อผู้ใช้ที่ล็อกอินเข้าสู่ระบบเพียงอย่างเดียวเป็นต้น – กรณีที่สอง เป็นจัดเก็บเหมือนกันแต่มี

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่าง
			รูปแบบการบันทึกไม่เหมือนกัน เช่น ระบบปฏิบัติการระบบ X บันทึกวันเวลาในข้อมูลล็อกเป็น MM-DD-YYYY ในขณะที่ระบบปฏิบัติการ Y บันทึกเวลาในข้อมูลล็อกเป็น YYDDMM – กรณีที่สาม เป็นรูปแบบที่ซับซ้อนขึ้น เช่นการเก็บข้อมูลล็อกของแอพพลิเคชัน M เก็บเป็น File Transfer Protocol (FTP) ในขณะที่แอพพลิคัน N เก็บเป็นหมายเลขของพอร์ตเช่น 21/TCP เป็นต้น
3	รูปแบบเวลาบนข้อมูลล็อก	Timestamp บนข้อมูลล็อกที่ระบุวันเวลาของเหตุการณ์ที่เกิดขึ้น โดยปกติวันเวลาบนข้อมูลล็อกหรือ Timestamp ได้มาจากวันเวลาบนระบบหรืออุปกรณ์ ดังนั้นถ้าวันเวลาบนระบบหรืออุปกรณ์เดินไม่ตรงเวลา จะทำให้วันเวลาของการประมวลผลข้อมูลล็อกคลาดเคลื่อนและอาจส่งผลโดยตรงต่อการวิเคราะห์ปัญหาที่เกิดขึ้นบนระบบ	ตามพ.ร.บ. ได้กำหนดให้อุปกรณ์ที่จำต้องมีการเก็บข้อมูลล็อกต้องดำเนินการปรับปรุงเวลาบนระบบให้ตรงกับเวลามาตรฐานสากล สามารถดำเนินการผ่าน Network Time Protocol หรือ NTP ได้
4	รูปแบบการสร้างและส่งข้อมูลล็อก	รูปแบบของการสร้างข้อมูลล็อกมีจุดประสงค์แตกต่างกันตามวิธีการเก็บข้อมูลล็อกของระบบที่เกี่ยวข้อง ตัวอย่างเช่นการสร้างข้อมูลล็อกในรูปแบบไฟล์ฐานข้อมูลมักมีจุดประสงค์เพื่อเก็บข้อมูลล็อกลงระบบบริหารจัดการฐานข้อมูลโดยตรง หรือการส่งข้อมูลล็อกตามรูปแบบมาตรฐาน Syslog ซึ่งผู้ดูแลระบบสามารถเข้าถึงและวิเคราะห์ได้ง่ายกว่า สามารถจัดเก็บในรูปแบบของไฟล์บนระบบได้เป็นต้น ดังนั้นการออกแบบระบบเก็บข้อมูลล็อกอาจต้องคำนึงถึงการสร้างข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อก เพื่อให้สามารถรองรับการเก็บข้อมูลได้หลากหลายมากยิ่งขึ้น	การสร้างและส่งข้อมูลล็อกจากแหล่งต้นกำเนิดข้อมูลล็อกอาจแตกต่างกันได้ เช่น – จัดส่งในรูปแบบของไฟล์ CSV หรือไฟล์ Comma-Separated – รูปแบบของไฟล์ฐานข้อมูลหรือ Database Management System หรือด้วยโครงสร้างภาษา SQL หรือ Structure Query Language – รูปแบบมาตรฐาน Syslog – รูปแบบของ Eventlog บนระบบปฏิบัติการไมโครซอฟต์ – ส่งในรูปแบบของโพรโตคอล Simple Network Management Protocol หรือ SNMP – ส่งในรูปแบบของ XML หรือ XHTML – ส่งในรูปแบบไฟล์ไบนารี เป็นต้น

โดยสรุป การสร้างและการจัดเก็บข้อมูลล็อกมีประเด็นที่ต้องคำนึงถึงคือ

1. การปรับเวลาของเครื่องเซิร์ฟเวอร์และอุปกรณ์ให้เป็นเวลามาตรฐาน เพื่อให้ข้อมูลล็อกบนล็อกเซิร์ฟเวอร์มีเวลาต่อเนื่องกันโดยตลอด สามารถดำเนินการได้ผ่านโพรโตคอล Network Time Protocol หรือ NTP
2. การปรับรูปแบบของการสร้างข้อมูลล็อก ให้อยู่ในรูปแบบที่สามารถส่งและจัดเก็บไว้ที่ล็อกเซิร์ฟเวอร์และสามารถวิเคราะห์ต่อได้โดยง่าย
3. การวิเคราะห์จำนวนข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อก ว่ามีจำนวนล็อกอย่างไร มีรูปแบบเป็นอย่างไร และจะดำเนินการจัดเก็บในรูปแบบใด

1.2. การป้องกันข้อมูลล็อก

ผู้ที่เกี่ยวข้องมีหน้าที่ในการดำเนินการจัดทำความมั่นคงปลอดภัยให้กับข้อมูลล็อก เพื่อให้ข้อมูลล็อกมีความน่าเชื่อถือและตรงตามความเป็นจริงสำหรับการวิเคราะห์เพื่อหาสาเหตุของปัญหาทางด้านประสิทธิภาพหรือความมั่นคงปลอดภัยได้อย่างถูกต้อง และใช้ประกอบเป็นหลักฐานในชั้นศาลได้ การส่งข้อมูลล็อกผ่านทางระบบเครือข่าย มีประเด็นสำคัญที่ต้องพิจารณาดังต่อไปนี้

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	การควบคุมการเข้าถึงข้อมูลล็อก	ต้องมีการกำหนดมาตรการควบคุมการเข้าถึงข้อมูลล็อกโดยการพิสูจน์ตัวตนตามรายชื่อของผู้ที่มีสิทธิเข้าถึงข้อมูลล็อกที่กำหนดไว้ รวมถึงจัดให้มีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง	– จัดให้มีการการพิสูจน์ตัวตนก่อนเข้าถึงข้อมูลล็อก – กำหนดให้มีการจัดทำล็อกเซิร์ฟเวอร์ที่เก็บเฉพาะข้อมูลล็อกซึ่งจะสามารถควบคุมการเข้าถึงข้อมูลล็อกได้อย่างมีประสิทธิภาพยิ่งขึ้น
2	การป้องกันการเปลี่ยนแปลงข้อมูลล็อกโดยไม่ได้รับอนุญาต	ต้องมีการกำหนดมาตรการในการระบุการเปลี่ยนแปลงที่เกิดขึ้นบนข้อมูลล็อก และตรวจสอบได้ว่าเป็นการเปลี่ยนแปลงที่ถูกต้อง	– จัดให้มีการบันทึกการเข้าถึงข้อมูลล็อกทุกครั้ง เช่นผู้ใช้ที่เข้าถึง ไอพีแอดเดรสของผู้ใช้ที่เข้าถึงข้อมูลล็อก การลบหรือแก้ไขข้อมูลล็อก เป็นต้น – นำวิธีการ Digital Hashing มาใช้เพื่อตรวจสอบความเปลี่ยนแปลงที่เกิดขึ้นบนข้อมูลล็อก เช่นการใช้ MD5 หรือ GPG เป็นต้น – จัดเก็บข้อมูลล็อกไว้ในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียวเช่น CD-ROM เป็นต้น
3	การจัดทำล็อกเซิร์ฟเวอร์ หรือ Log Server	เพื่อป้องกันการเปลี่ยนแปลงข้อมูลล็อกบนเซิร์ฟเวอร์หรืออุปกรณ์กำเนิดข้อมูลล็อก นำรูปแบบที่เรียกว่า Secondary Logging หรือการจัดทำล็อกเซิร์ฟเวอร์และปรับแต่งให้เซิร์ฟเวอร์หรืออุปกรณ์กำเนิดข้อมูลล็อกจัดส่งข้อมูลล็อกไปที่ล็อกเซิร์ฟเวอร์ด้วย	– โดยปกติข้อมูลล็อกจะจัดเก็บบนอุปกรณ์หรือเซิร์ฟเวอร์ต้นกำเนิดข้อมูลล็อก ▪ ระบบปฏิบัติการไมโครซอฟต์วินโดวส์เก็บบันทึกล็อกผ่าน Eventlog ▪ ระบบปฏิบัติการลีนุกซ์ปกติจะเก็บล็อกที่ /var/log – การส่งข้อมูลล็อกไปที่ล็อกเซิร์ฟเวอร์สามารถป้องกันความเสี่ยงที่ผู้บุกรุกสามารถเข้าถึงระบบและแก้ไขข้อมูลล็อกเพื่อลบร่องรอยการบุกรุก ซึ่งข้อมูลล็อกบนเซิร์ฟเวอร์จะถูกเปลี่ยนแปลงไป แต่ข้อมูลล็อกบนล็อกเซิร์ฟเวอร์จะไม่ได้ถูกเปลี่ยนแปลง (ยกเว้นผู้บุกรุกจะสามารถบุกรุกล็อกเซิร์ฟเวอร์ด้วย) – กำหนดมาตรการป้องกันการเข้าถึงข้อมูลล็อกบนล็อกเซิร์ฟเวอร์ ให้รัดกุมและปลอดภัยเช่นการใช้ Two-factor Authentication เป็นต้น – กำหนดมาตรการป้องกันบนระบบเครือข่ายเพื่อป้องกันการเข้าถึงล็อกเซิร์ฟเวอร์โดยไม่ได้รับอนุญาต
4	การป้องกันข้อมูลล็อกที่มีข้อมูลส่วนบุคคล	ต้องมีการกำหนดมาตรการการป้องกันและควบคุมการเข้าถึงข้อมูลล็อกกรณีที่ข้อมูลล็อกมีการบันทึกข้อมูลที่เกี่ยวข้องกับข้อมูลส่วนบุคคล	– กำหนดให้มีการเข้ารหัสข้อมูลส่วนบุคคล หรือเก็บเฉพาะบางส่วนของข้อมูลเช่นเก็บเฉพาะเลข 4 หลักสุดท้ายของบัตรประจำตัวประชาชน เป็นต้น

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
			▪ ข้อมูลส่วนบุคคลตัวอย่างเช่น ชื่อ นามสกุล ที่อยู่ หมายเลขบัตรประจำตัวประชนชน เงินเดือน ภาษี ▪ ข้อมูลส่วนบคคลที่เกี่ยวข้องการใช้งานระบบ เช่นรหัสผ่าน เนื้อหาอีเมล์ของผู้ใช้ หรือข้อมูลอื่นๆ
5	การป้องกันข้อมูลล็อกที่ส่งผ่านระบบเครือข่าย	ต้องมีการกำหนดมาตรการป้องกันการเข้าถึงหรือเปลี่ยนแปลงข้อมูลล็อกที่ส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต	– ออกแบบระบบเครือข่ายให้รองรับการส่งข้อมูลล็อกผ่านระบบเครือข่ายให้ปลอดภัย เช่นการแบ่งเครือข่ายของล็อกเซิร์ฟเวอร์โดยเฉพาะ การควบคุมผ่านไฟร์วอลล์เป็นต้น – เข้ารหัสข้อมูลล็อกที่มีการส่งผ่านระบบเครือข่าย เช่นเข้ารหัสข้อมูลก่อนแล้วค่อยส่งไปที่ล็อกเซิร์ฟเวอร์เป็นต้น
6	การรักษาความพร้อมใช้ของข้อมูลล็อก	ข้อมูลล็อกต้องเข้าถึงได้จากผู้ที่ได้รับอนุญาตหรือได้สิทธิและเมื่อต้องการเข้าถึงข้อมูลล็อกควรจะเข้าถึงได้ตามต้องการโดยทันที	– จัดทำระบบสำรองข้อมูลล็อก โดยกำหนดตามแผนการสำรองข้อมูลล็อก เช่นดำเนินการสำรองข้อมูลแบบ Full ทุก 1 เดือนเป็นต้น หรือการบีบข้อมูลล็อก (Archive Log) และเขียนในสื่อบันทึกข้อมูลชนิดเขียนได้อย่างเดียว – ควรกำหนดปริมาณข้อมูลล็อกที่สามารถสืบค้นได้ทันที เช่นกำหนดให้สืบค้นได้ย้อนหลังไป 10 วัน ถ้าต้องการสืบค้นย้อนหลังไปมากกว่านั้นต้องไปดึงข้อมูลจากข้อมูลในเทปสำรองข้อมูลเป็นต้น – ควรมีการกำหนดระบบทดแทนระบบเก็บข้อมูลล็อก เช่นมี 2 เซิร์ฟเวอร์ทำหน้าที่เก็บข้อมูลล็อกเป็นต้น หรือพิจารณาทำ RAID บนฮาร์ดดิสก์ที่ใช้เก็บข้อมูลล็อกเพื่อให้รองรับความเสียหายที่อาจจะเกิดขึ้นบนฮาร์ดดิสก์เพื่อเพิ่มระดับความพร้อมใช้ของการให้บริการข้อมูลล็อก – ควรมีการประเมินและติดตามปริมาณข้อมูลล็อกต่อวัน เพื่อให้สามารถวางแผนและกำหนดขีดความสามารถในการจัดเก็บข้อมูลล็อกบนเซิร์ฟเวอร์เก็บข้อมูลล็อกได้
7	การรักษาระยะเวลาของการเก็บข้อมูลล็อก หรือ Log Archival	การนำข้อมูลล็อกมาวิเคราะห์เพื่อหาสาเหตุของปัญหาหรือปรับปรุงประสิทธิภาพด้านความปลอดภัย ต้องการข้อมูลล็อกที่น่าเชื่อถือ และต้องใช้ข้อมูลล็อกในวันที่มีเหตุการณ์ที่ต้องการนำมาใช้วิเคราะห์ และโดยปกติมักจะต้องใช้ข้อมูลล็อกย้อนหลังร่วมด้วย การรักษาระยะเวลาการจัดเก็บข้อมูลล็อกจึงมีความเป็นจำเป็น และควรกำหนดมาตรการป้องกันให้ข้อมูลล็อกมีการจัดเก็บตามระยะเวลาที่กำหนดไว้ ตาม พ.ร.บ. ว่าด้วยการกระทำ	– กำหนดวิธีการรักษาระยะเวลาการจัดเก็บข้อมูลล็อกให้ได้ตามที่กำหนด เช่นการทำ Archive Log ของข้อมูลล็อกที่เก่ากว่า 30 วันเก็บลงบนสื่อบันทึกข้อมูลแยกต่างหาก เพื่อลดการเก็บข้อมูลล็อกบนเซิร์ฟเวอร์หลัก เป็นต้น – กำหนดมาตรการสำรองข้อมูลล็อกเพื่อให้สามารถนำข้อมูลล็อกย้อนหลังได้ตามที่ต้องการ – ควรมีการประเมินและติดตามปริมาณข้อมูลล็อกต่อวัน เพื่อให้สามารถวางแผนและกำหนดขีดความสามารถในการจัดเก็บข้อมูลล็อกบนล็อกเซิร์ฟเวอร์

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
		ความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 กำหนดให้มีการจัดเก็บข้อมูล 90 วันหรือต้องการให้รักษาระยะเวลาการเก็บข้อมูลล็อกย้อนหลังไป 90 วัน (ในกรณีพิเศษอาจสั่งให้มีการเก็บเพิ่มเติมได้ แต่ไม่เกิน 1 ปี)	

1.3. การวิเคราะห์ข้อมูลล็อก

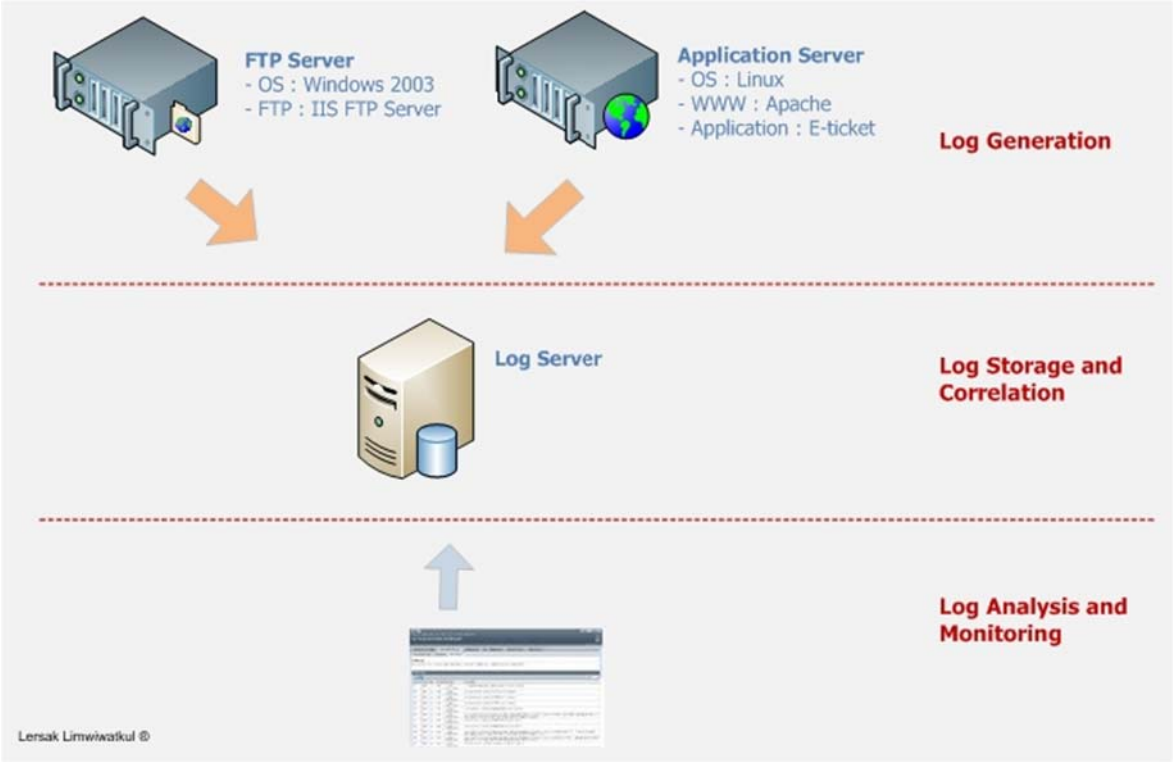
โดยปกติผู้ดูแลระบบ (System Administrator) ผู้ดูแลระบบเครือข่าย (Network Administrator) และผู้พัฒนา (Developer) มีหน้าที่ความรับผิดชอบโดยตรงในการวิเคราะห์ข้อมูลล็อก อาจมีนักวิเคราะห์ความมั่นคงปลอดภัยระบบ (Security Analyst) เพื่อวิเคราะห์ข้อมูลล็อกจากอุปกรณ์ทางด้านความปลอดภัยเช่นไฟร์วอลล์หรือระบบป้องกันการบุกรุกโดยตรง และมีประเด็นสำคัญ 2 ประเด็นคือ

ที่	ประเด็น	ข้อพิจารณา	ตัวอย่างการดำเนินการ
1	การอบรมความรู้ในการวิเคราะห์ข้อมูลล็อก	การวิเคราะห์ข้อมูลล็อกจำเป็นต้องใช้ความเชี่ยวชาญและทักษะระดับสูงของผู้ที่มีหน้าที่รับผิดชอบโดยตรง เพื่อวิเคราะห์ลำดับของเหตุการณ์ สาเหตุของเหตุการณ์ และแนวทางการแก้ไขที่ถูกต้องให้ได้ ดังนั้นการอบรมความรู้ให้กับผู้ที่มีหน้าที่รับผิดชอบโดยตรงเพื่อป้องกันปัญหาการขาดความรู้และทักษะความเชี่ยวชาญในการวิเคราะห์ข้อมูลล็อก	– จัดให้การอบรมการวิเคราะห์ข้อมูลล็อก โดยบริษัทผู้ติดตั้งล็อกเซิร์ฟเวอร์
2	เครื่องมือสำหรับการวิเคราะห์ข้อมูลล็อก	เพื่อให้สามารถวิเคราะห์ข้อมูลล็อกจำนวนมากได้อย่างรวดเร็วและถูกต้อง การใช้เครื่องมือเช่นการเรียงเวลาลำดับการเกิดเหตุการณ์ การแปลงข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อกที่แตกต่างกัน ซึ่งจะช่วยให้ผู้ที่มีหน้าที่รับผิดชอบสามารถดำเนินการวิเคราะห์ได้ต่อไป	– ตรวจสอบความสามารถในการวิเคราะห์ล็อกของซอฟต์แวร์ในการจัดเก็บข้อมูลล็อกบนเซิร์ฟเวอร์ หรือความสามารถของล็อกเซิร์ฟเวอร์ในการวิเคราะห์เหตุการณ์ตามที่ต้องการ

2. โครงสร้างระบบเก็บข้อมูลล็อกสำหรับองค์กร

โครงสร้างพื้นฐานระบบเก็บข้อมูลล็อกเกี่ยวข้องทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย และสื่อบันทึกข้อมูลที่เลือกมาใช้เพื่อให้เกิดการจัดเก็บข้อมูลล็อกได้ตามความต้องการ ทั้งการสร้างข้อมูลล็อก การส่งข้อมูลล็อก การเก็บข้อมูลล็อก การวิเคราะห์ข้อมูลล็อก และการลบข้อมูลล็อกเมื่อไม่มีความจำเป็นต้องเก็บในระบบแล้ว

โดยทั่วไปรูปแบบระบบเก็บข้อมูลล็อกสำหรับองค์กร ตามเอกสารอ้างอิง [4] ได้แบ่งส่วนประกอบหลักเป็น 3 ส่วนดังรูป



2.1. ส่วนประกอบของระบบเก็บข้อมูลล็อก

Log Generation หรือ Log Source เป็นแหล่งกำเนิดข้อมูลล็อกหรือสร้างข้อมูลล็อก เป็นเซิร์ฟเวอร์หรืออุปกรณ์บนระบบเครือข่ายที่มีข้อมูลล็อกจากระบบปฏิบัติการและแอพพลิเคชัน การจัดเก็บข้อมูลล็อกบนเครื่องเซิร์ฟเวอร์หรืออุปกรณ์ในตัวเองเรียกว่า Primary Logging ในกรณีที่มีการจัดส่งข้อมูลล็อกไปยังล็อกเซิร์ฟเวอร์หรือ Log server จะเรียกลักษณะการส่งข้อมูลล็อกนี้ว่า Secondary Logging

Log Storage and Correlation เป็นล็อกเซิร์ฟเวอร์สำหรับรับข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อกหรือ Log Generation เพื่อจัดเก็บตามรูปแบบที่กำหนดไว้ รวมทั้งการแปลงข้อมูลล็อกให้อยู่ในรูปแบบที่สามารถจัดเก็บได้ ซึ่งอาจรวมถึงการแปลงข้อมูลล็อกให้มีรูปแบบที่พร้อมจะนำไปวิเคราะห์ต่อได้ ไม่ว่าจะมีรูปแบบของข้อมูลล็อกแตกต่างกัน ในกรณีที่เซิร์ฟเวอร์ดังกล่าวรับข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อกจำนวนมากจะเรียกว่า Collectors หรือ Aggregators

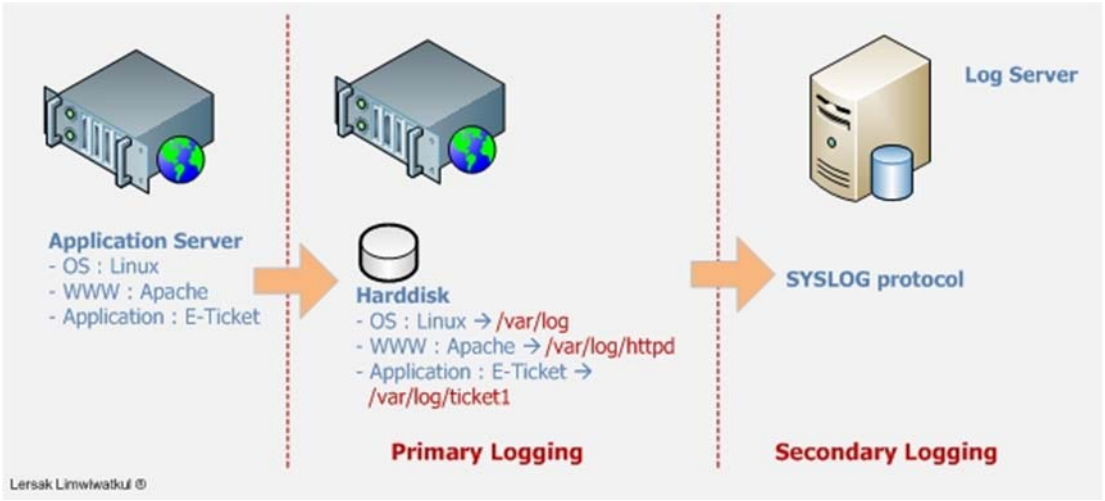
Log Analysis and Monitoring เป็นหน้าต่างสำหรับผู้ดูแลระบบหรือผู้ที่มีหน้าที่รับผิดชอบในการวิเคราะห์ข้อมูลล็อก และติดตามตรวจสอบความถูกต้องของข้อมูลล็อก ระบบจัดเก็บข้อมูลล็อกบางระบบสนับสนุนการสร้างรายงานการวิเคราะห์ข้อมูลล็อก ทั้งนี้เพื่อให้ข้อมูลเร็วและตรงกับความเป็นจริงในปัจจุบันที่สุด

2.2. การจัดเก็บข้อมูลล็อกแบบ Primary Logging และ Secondary Logging

โดยปกติแล้วเครื่องเซิร์ฟเวอร์หรืออุปกรณ์สามารถบันทึกข้อมูลล็อกได้ และ/หรือสามารถส่งข้อมูลล็อกไปยังเซิร์ฟเวอร์อื่นได้ ทั้งนี้ได้แยกรูปแบบเป็น 2 แบบคือ

- การบันทึกข้อมูลล็อกบนตัวระบบเองเรียกว่า Primary Logging หรือการบันทึกข้อมูลล็อกแบบปฐมภูมิ
- การส่งข้อมูลล็อกไปบันทึกหรือจัดเก็บที่ล็อกเซิร์ฟเวอร์เรียกว่า Secondary Logging หรือการบันทึกข้อมูลล็อกแบบทุติยภูมิ ซึ่งชื่อวิธีการส่งข้อมูลแบบนี้ใช้ตามเอกสารอ้างอิง [5]

ตามรูป



การจัดเก็บข้อมูลล็อกแบบ Primary Logging เป็นการจัดเก็บข้อมูลบนฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลบนตัวอุปกรณ์หรือระบบที่กำเนิดข้อมูลล็อกเอง จากในรูปเป็นตัวอย่างการเก็บข้อมูลล็อกแยกตามข้อมูลล็อกของระบบปฏิบัติการ เป็นระบบปฏิบัติการลีนุกซ์ ข้อมูลล็อกของเว็บเซิร์ฟเวอร์และข้อมูลล็อกของระบบแอพพลิเคชัน ในตัวอย่างเป็นระบบ E-ticket ระบบปฏิบัติการลีนุกซ์จะบันทึกข้อมูลล็อกไว้ในไดเรกทอรี /var/log เป็นต้น

การส่งข้อมูลล็อกไปที่ล็อกเซิร์ฟเวอร์นั้น สามารถส่งผ่านระบบเครือข่ายได้หลายวิธีการ ตัวอย่างเช่น

- ส่งข้อมูลตามรูปแบบของไฟล์ไบนารีหรือการเรียกใช้ Application Programming Interface หรือ API ของล็อกเซิร์ฟเวอร์เพื่อส่งข้อมูลล็อก
- ส่งข้อมูลในรูปแบบของไฟล์เช่นส่งไฟล์เป็น TEXT หรือรูปแบบไฟล์ CSV (Comma-Separated) ผ่านการส่งไฟล์ข้ามเครื่องด้วย File Transfer Protocol หรือ FTP
- ส่งข้อมูลในรูปแบบมาตรฐาน SYSLOG เป็นโพรโตคอล UDP ใช้หมายเลขพอร์ตเป็น 514 นิยมใช้กับระบบปฏิบัติตระกูลยูนิกซ์และลีนุกซ์ ซึ่งเป็นตัวอย่างที่ใช้ในรูป
- ส่งข้อมูลในรูปแบบมาตรฐาน EVENTLOG ซึ่งเป็นรูปแบบของไฟล์หรือผ่านสคริปต์การส่งข้อมูล EVENTLOG นิยมใช้บนระบบปฏิบัติการตระกูลไมโครซอฟต์วินโดวส์
- ส่งข้อมูลในรูปแบบของระบบฐานข้อมูลด้วยโครงสร้างภาษา SQL หรือ Structure Query Language เพื่อส่งข้อมูลล็อกไปเก็บที่ระบบบริหารจัดการฐานข้อมูลหรือ Database Management System บนล็อกเซิร์ฟเวอร์โดยตรง
- ใช้การส่งข้อมูลผ่านโพรโตคอล Simple Network Management Protocol หรือ SNMP
- ส่งข้อมูลในรูปแบบ XML หรือ XHTML ผ่านโพรโตคอล SOAP

ล็อกเซิร์ฟเวอร์หรือ Log Server สำหรับการบันทึกข้อมูลตามแบบ Secondary Logging ซึ่งทำหน้าที่หลักในการจัดเก็บข้อมูลล็อก สำรองข้อมูลล็อก มีระบบป้องกันการเข้าถึงหรือควบคุมการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต อาจมีความสามารถในการวิเคราะห์ข้อมูลล็อก รวมถึงบริหารจัดการข้อมูลล็อกชั้นสูงอื่นๆ เป็นต้น มีชื่อเรียกในการใช้งานหลายชื่อ เช่น

- Centralized Log Server หรือเซิร์ฟเวอร์จัดเก็บข้อมูลล็อกแบบศูนย์กลาง
- Centralized Log Management Server หรือเซิร์ฟเวอร์บริหารจัดเก็บข้อมูลล็อกแบบศูนย์กลาง
- Security Event Manager System หรือ SEM หรือระบบบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย ทำหน้าที่เก็บบันทึกข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้นภายในระบบสารสนเทศ
- Security Information Management System หรือ SIM หรือระบบบริหารจัดการข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัย ทำหน้าที่เก็บบันทึกข้อมูลเหตุการณ์ ตอบสนองผ่านการวิเคราะห์และสรุป เพื่อให้ผู้เชี่ยวชาญระบบความมั่นคงปลอดภัยนำไปวิเคราะห์ต่อได้อย่างแม่นยำ มักมีการนำไปใช้ในระบบวิเคราะห์ข้อมูลล็อกระดับสูง เพื่อติดตามปัญหา วิเคราะห์ปัญหา และหาสาเหตุของปัญหาทางด้านความมั่นคงปลอดภัยอย่างเป็นระบบ

จากเหตุผลของการรักษาความถูกต้องและเชื่อถือได้ของข้อมูลล็อก ทำให้ประเด็นการพิจารณาเลือกวิธีการติดตั้งล็อกเซิร์ฟเวอร์และบันทึกข้อมูลแบบ Secondary Logging ร่วมด้วยนั้นเป็นทางเลือกที่ดี เพราะ

- สามารถควบคุมและบริหารจัดการความมั่นคงปลอดภัยของข้อมูลล็อก ผ่านการควบคุมการเข้าถึง การป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต การสำรองข้อมูลล็อก ดำเนินการผ่านศูนย์กลางหรือล็อกเซิร์ฟเวอร์เพียงจุดเดียว
- เพิ่มระดับความมั่นคงปลอดภัยให้กับข้อมูลล็อก ในกรณีที่ผู้บุกรุกเข้าถึงระบบโดยไม่ได้รับอนุญาตนั้น ข้อมูลล็อกที่ Primary Logging มักจะถูกแก้ไขหรือถูกลบข้อมูลการเข้ามาในระบบ หรือโดยมากมักจะพิจารณาได้โดยทันทีว่าในกรณีที่ระบบถูกบุกรุกโดยไม่ได้รับอนุญาตนั้น ข้อมูลล็อกที่ Primary Logging จะมีความน่าเชื่อถือและความถูกต้องน้อยมากจนไม่สามารถนำมาพิจารณาได้ทั้งหมด
- สามารถประเมินระดับความต้องการและขีดความสามารถในการรองรับการเก็บข้อมูลล็อกได้อย่างมีประสิทธิภาพ เช่นการติดตามปริมาณของการเก็บข้อมูลล็อกบนสื่อบันทึกข้อมูลหรือฮาร์ดดิสก์เฉพาะที่ล็อกเซิร์ฟเวอร์ เพื่อประเมินแนวโน้มอัตราการเติบโตของข้อมูลล็อกเป็นต้น
- สามารถนำข้อมูลล็อกที่ศูนย์กลางไปใช้วิเคราะห์ได้อย่างรวดเร็วและมีประสิทธิภาพ รวมถึงการตั้งแจ้งเตือนเป็น Real-time หรือการวิเคราะห์ข้อมูลล็อกแบบ Off-line ก็ย่อมได้

2.3. ฟังก์ชันการทำงานล็อกเซิร์ฟเวอร์

ถ้าพิจารณาตาม พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แล้วเจตนารมณ์การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ และข้อมูลผู้ใช้ต้องการให้ข้อมูลล็อกนั้นต้องการให้

- ข้อมูลล็อกควรมีความถูกต้องและเชื่อถือได้
- มีการกำหนดมาตราการป้องกันข้อมูลล็อก
- มีการกำหนดให้รักษาระยะเวลาเก็บข้อมูลล็อกให้เหมาะสมเช่น 90 วันเป็นอย่างน้อย
- สามารถวิเคราะห์ข้อมูลหาผู้ที่เกี่ยวข้องกับระบบสารสนเทศ และรูปแบบของเหตุการณ์ที่เกิดขึ้นจากข้อมูลล็อกได้

นอกจากการเก็บข้อมูลล็อกแล้ว ตามตาม พ.ร.บ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในมาตรา 28 ได้กำหนดให้มีการแต่งตั้งพนักงานเจ้าหน้าที่ความเชี่ยวชาญในการวิเคราะห์หลักฐานข้อมูลคอมพิวเตอร์หรือ Computer Forensic ซึ่งต้องดำเนินการเก็บหลักฐานและวิเคราะห์ข้อมูลคอมพิวเตอร์ และมีวิธีการในการเก็บและจัดการกับหลักฐานทางอิเล็กทรอนิกส์เพื่อให้สามารถนำไปพิจารณาได้ในชั้นศาลอย่างถูกต้องหรือที่เรียกว่ามีความรู้ความเข้าใจและดำเนินการตามระเบียบวิธีการรักษา Chain of Custody ได้ซึ้งได้กล่าวเน้นไว้ในเอกสารอ้างอิง [6]

ถ้าพิจารณาเฉพาะความสามารถของล็อกเซิร์ฟเวอร์ที่สามารถทำได้ จะครอบคลุมฟังก์ชันการทำงานทั้งหมดดังต่อไปนี้ อ้างอิงข้อมูลจาก [4]

ความสามารถทั่วไป

- **Log parsing** ทำหน้าที่ในการดึงข้อมูลล็อกเพื่อให้สามารถเก็บบนระบบฐานข้อมูล หรือส่งต่อให้กับระบบเก็บฐานข้อมูลล็อกอื่นได้ ยังรวมถึงการแปลงข้อมูลล็อกหรือ Log Conversation ให้อยู่ในรูปแบบที่ต้องการหรือพร้อมสำหรับนำไปใช้งานต่อไป

- **Event filtering** ทำหน้าที่กรองข้อมูลล็อกเพื่อใช้สำหรับการวิเคราะห์ การรายงานหรือการประเมินแนวโน้มของเหตุการณ์ตามคุณลักษณะของเหตุการณ์หรือความผิดปกติที่เกิดขึ้น รวมถึงคัดกรองเหตุการณ์หรือข้อมูลล็อกที่ไม่เกี่ยวข้อง ฟังก์ชันของ Event filtering ควรมีการป้องกันการเปลี่ยนแปลงข้อมูลล็อกด้วย

- **Event aggregation** ทำหน้าที่ในการรวบรวมข้อมูลหรือปรับเปลี่ยนข้อมูลให้อยู่ที่เดียวกัน เพื่อให้สะดวกต่อการร้องขอหรือการสร้างรายงาน

การจัดเก็บข้อมูลล็อก

- **Log rotation** เป็นการจัดเก็บล็อกไฟล์โดยการหมุนข้อมูลล็อก หมายถึงการบันทึกไฟล์ข้อมูลล็อกไว้เป็นชื่ออื่น และสร้างไฟล์ล็อกใหม่เพื่อรองรับการบันทึกข้อมูลต่อไป ตัวอย่างเช่นการบันทึกไฟล์ล็อกเป็น /var/log/message เมื่อมีการหมุนข้อมูลล็อกจะบันทึกข้อมูลล็อกเป็น /var/log/message.1 และสร้างไฟล์ล็อกใหม่เป็นชื่อ /var/log/message เป็นต้น เพื่อป้องกันไม่ให้มีไฟล์ข้อมูลล็อกขนาดใหญ่เกินจนไม่สามารถใช้งานได้ โดยปกติการหมุนข้อมูลล็อกจะดำเนินการตามระยะเวลาที่เหมาะสมเช่น ทุกวัน หรือทุกสัปดาห์ หรือเมื่อมีขนาดของไฟล์ข้อมูลล็อกมีขนาดถึงที่กำหนดไว้ นอกจากนี้ยังนำข้อมูลล็อกเดิมเมื่อมีการหมุนข้อมูลล็อกไปบีบอัดข้อมูลเพื่อเพิ่มพื้นที่เก็บข้อมูล หรือทำ Log archive ได้ การหมุนข้อมูลล็อกที่เหมาะสมคือการบันทึกข้อมูลล็อกแยกเป็นรายวัน และแยกตามเซิร์ฟเวอร์หรืออุปกรณ์ในระบบเครือข่าย

- **Log archival** คือการสำรองข้อมูลล็อกเพื่อให้สามารถรักษาระยะเวลาในการจัดเก็บข้อมูลล็อกตามความต้องการ โดยการบันทึกข้อมูลล็อกบนสื่อบันทึกข้อมูลภายนอก หรือการบันทึกข้อมูลบน Storage area network หรือ SAN หรือการบันทึกบนเซิร์ฟเวอร์หรือข้อมูลที่ทำหน้าที่เฉพาะในการบันทึกข้อมูลล็อกเป็นต้น ยังรวมถึงการสำรองข้อมูลล้อกบนสื่อบันทึกข้อมูลอื่นเช่น เทปสำรองข้อมูล ซีดีรอมหรือดีวีดีเป็นต้น การจัดทำ Log archival แบ่งเป็นสองแบบคือ

    - Log retention เป็นการบันทึกข้อมูลล็อกของเหตุการณ์จากระบบอย่างสม่ำเสมอ
    - Log preservation เป็นกระบวนการรักษาข้อมูลล็อกเพื่อให้สามารถนำไปใช้ร่วมกับการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย หรือเหตุการณ์ผิดปกติที่เกิดขึ้นกับระบบสารสนเทศ และสามารถรักษาข้อมูลล็อกได้ตามระยะเวลาที่กำหนดไว้หรือตามความต้องการจากภายนอก เช่นความต้องการของ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น

- **Log compression** คือการบีบอัดข้อมูลล็อกเพื่อเพิ่มพื้นที่ในการจัดเก็บข้อมูลล็อก และง่ายในการสำรองข้อมูลล็อกหรือการย้ายข้อมูลล็อกไปเก็บไว้บนสื่อบันทึกข้อมูลอื่น มักดำเนินการต่อเนื่องจาก Log rotation หรือ Log archival

- **Log reduction** เป็นการตัด ลบ หรือลดข้อมูลล็อกบางส่วนที่ไม่เกี่ยวข้อง เช่นการลบตัวอักษรหรืออักขระที่ไม่จำเป็นต่อเก็บบันทึกข้อมูลล็อก มักจะดำเนินการควบคู่กับกระบวนการ Log archival เพื่อลดข้อมูลล็อกที่ไม่เกี่ยวข้องก่อนจะบันทึกข้อมูลล็อกในสื่อบันทึกข้อมูล

- **Log conversion** เป็นการแปลงรูปแบบการจัดเก็บข้อมูลล็อกเช่น แปลงข้อมูลล็อกจากรูปแบบของไฟล์ TEXT เป็นรูปแบบข้อมูลล็อกแบบ XML เป็นต้น เป็นวิธีการแปลงรูปแบบการเก็บข้อมูลล็อกจากรูปแบบหนึ่งไปเป็นอีกรูปแบบหนึ่ง ส่วนหนึ่งแล้วการทำ Log conversion มักทำกระบวนการ Event filtering และ Event aggregation จนถึง Log normalization

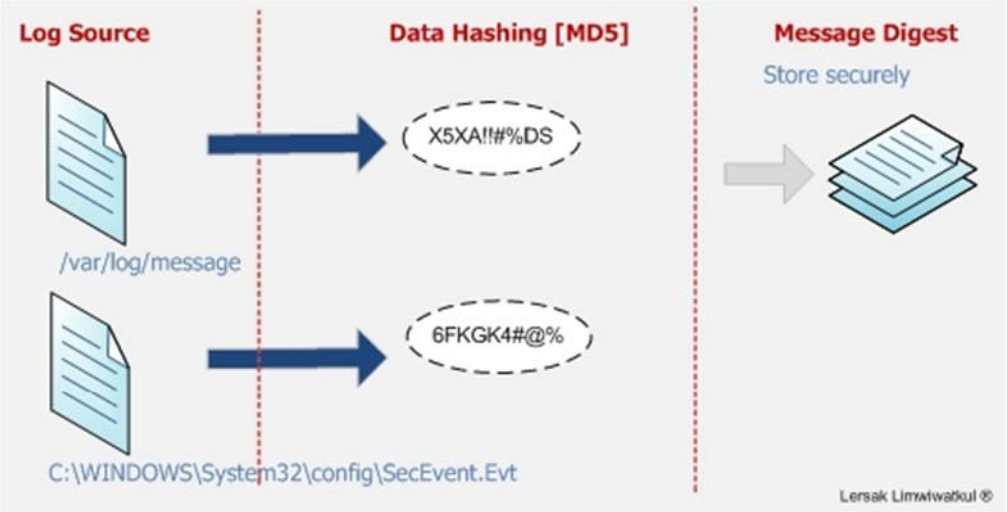
- **Log normalization** เป็นการปรับรูปแบบของข้อมูลล็อกให้อยู่ในรูปแบบเดียวกัน เช่นการปรับรูปแบบของวันที่ที่แตกต่างกัน เช่น หรือความแตกต่างของชื่อตำแหน่งของข้อมูลล็อก เช่น

    - ข้อมูลล็อกวันที่จากเว็บเซิร์ฟเวอร์เป็นรูปแบบ 12 ชั่วโมงหรือเขียนเป็น 2:34:56 P.M. IDT ในขณะที่ข้อมูลล็อกวันที่ของเว็บเซิร์ฟเวอร์อีกเซิร์ฟเวอร์จัดเก็บในรูปแบบ 24 ชั่วโมง เช่น 14:34 GMT+7 เป็นต้น
    - ในระบบหนึ่งเรียกข้อมูลล็อกวันที่ว่า Timestamp ในขณะที่อีกระบบหนึ่งเรียกว่า Event Time เป็นต้น

- บางระบบเก็บข้อมูลล็อกของ Timezone เป็น GMT+7 ในขณะที่อีกระบบหนึ่งเก็บข้อมูลล็อกเป็น Zone-21 เป็นต้น ดังนั้นกระบวนการ Log normalization ต้องทราบว่าความหมายของ Zone-21 หมายถึง GMT+7 เป็นต้น

กระบวนการ Log normalization มีความสำคัญมากยิ่งเฉพาะกับการใช้ล็อกเซิร์ฟเวอร์แบบศูนย์กลางเพื่อเก็บข้อมูลล็อก และสามารถวิเคราะห์ข้อมูลล็อก ซึ่งต้องมีความสามารถในการรับข้อมูลล็อกหลายรูปแบบและต้องทำ Log normalization ในการแปลงข้อมูลล็อกให้อยู่ในรูปแบบที่สามารถจัดเก็บ สืบค้น และวิเคราะห์ได้โดยผู้ที่มีความรู้ความเชี่ยวชาญต่อไป

– **Log file integrity checking** เป็นกระบวนการตรวจสอบความถูกต้องของล็อกไฟล์ โดยการทำ **Data Hashing** กับล็อกไฟล์ที่ไม่มีการเขียนข้อมูลแล้ว ตัวอย่างดำเนินการทำ Log rotation เป็นวันดังนั้นสามารถนำข้อมูลล็อกไฟล์ของเดือนก่อนหน้ามาเข้ากระบวนการนี้ได้ หรือการทำ Log compression กับล็อกไฟล์ที่ผ่านกระบวนการ Log archival แล้วเช่นข้อมูลล็อกของสัปดาห์ที่แล้วนำมาบีบอัดและคำนวณด้วยวิธีการนี้เป็นต้น ซึ่งจะได้เป็นข้อมูลเป็น Message Digest เช่นการคำนวณด้วยอัลกอริทึม MD5 ขนาด 128 บิต หรือใช้อัลกอริทึม SHA-1 ขนาด 128 บิตเป็นต้น ผลลัพธ์ที่ได้หรือที่เรียกว่า Message Digest จะมีความยาวขนาด 128 บิตเพื่อใช้เป็นตัวแทนของล็อกไฟล์ ข้อมูล Message Digest ควรจะต้องเก็บไว้ในสื่อบันทึกข้อมูลที่ปลอดภัยเช่น สื่อบันทึกข้อมูลแบบเขียนได้อย่างเดียวเป็นต้น ตัวอย่างในรูปเป็นการใช้งาน Data Hashing



ล็อกไฟล์ /var/log/message และ C:\WINDOWS\System32\config\SecEvent.Evt ตามรูปบนระบบปฏิบัติการยูนิกซ์และข้อมูลล็อกไฟล์ของ Security Log บนระบบปฏิบัติการวินโดวส์ตามลำดับที่จัดเก็บบนล็อกเซิร์ฟเวอร์ นำมาคำนวณผ่านกระบวนการ Data Hashing และข้อมูล Message Digest ที่ได้นำไปเก็บไว้บนสื่อบันทึกข้อมูลประเภท CD-ROM ซึ่งเขียนได้อย่างเดียวเป็นต้น

เมื่อต้องการเทียบว่าล็อกไฟล์ดังกล่าวมีการเปลี่ยนแปลงหรือไม่ ให้คำนวณเทียบด้วยวิธีการเช่นเดิม และนำผลลัพธ์ของ Message Digest ไปเทียบกับค่าของ Message Digest ที่คำนวณไว้ตอนต้น ถ้าค่าที่ได้ไม่เท่ากัน แสดงว่าเกิดการเปลี่ยนแปลงโดยที่ไม่ได้รับอนุญาตแล้ว

ข้อสำคัญคือข้อมูล Message Digest ที่ได้จากการคำนวณตอนแรกต้องมีการกำหนดมาตรการควบคุมการเก็บอย่างมั่นคงปลอดภัยและป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตด้วย

การวิเคราะห์ข้อมูลล็อก

– **Event correlation** เป็นกระบวนการสร้างความสัมพันธ์ของข้อมูลล็อกตัวอย่างเช่นการสร้างกฎความสัมพันธ์หรือ Rule-based correlation ระหว่างข้อมูลล็อก เช่นการสร้างความสัมพันธ์ของข้อมูลล็อกจาก วันเวลา จากไอพีแอดเดรส จากชนิดของเหตุการณ์จากข้อมูลล็อกเป็นต้น

กระบวนการ Event correlation สามารถนำระเบียบวิธีการประมวลผลข้อมูลระดับสูงมาใช้ร่วมได้ เช่นการใช้วิธีการทางสถิติมาหาแนวโน้มของเหตุการณ์ที่เกี่ยวข้องกัน หรือการใช้ความน่าจะเป็นมาคำนวณเพื่อวิเคราะห์หาความสัมพันธ์ของเหตุการณ์เป็นต้น จนถึงการนำเทคนิคของ Data Mining มาใช้เพิ่มเติมเพื่อจัดแบ่งกลุ่มข้อมูลและความสัมพันธ์ของข้อมูลล็อกหรือเหตุการณ์ที่เกิดขึ้นได้อย่างแม่นยำมากขึ้น

- **Log viewing** เป็นระบบการแสดงข้อมูลล็อก มีความสามารถของ Event filtering เช่นสามารถการจัดเรียงข้อมูลล็อกตามวันที่ การแยกข้อมูลล็อกตามเซิร์ฟเวอร์หรืออุปกรณ์

- **Log reporting** เป็นการแสดงผลลัพท์จากการวิเคราะห์ข้อมูลล็อก ระบุความสัมพันธ์ที่เกี่ยวข้อง หรือข้อมูลสรุปการวิเคราะห์ข้อมูลล็อกหรือเหตุการณ์ที่เกี่ยวข้อง แสดงความต่อเนื่องของเหตุการณ์ที่เกิดขึ้นและคัดกรองรวมถึงแสดงเป็นกราฟหรือแผนภูมิเพื่อให้ง่ายต่อการแสดงผลเป็นต้น

การทำลายหรือยกเลิกใช้งานข้อมูลล็อก

- **Log clearing** คือการลบข้อมูลจากล็อกไฟล์ตามวันเวลาที่กำหนดไว้ ซึ่งเป็นการลบข้อมูลที่ไม่ได้ใช้งานแล้วหรือไม่มีความสำคัญต่อการใช้งานแล้ว การลบข้อมูลล็อกต้องคำนึงถึง Log archival

3. ประเภทของของข้อมูลล็อกจากแหล่งกำเนิดข้อมูลล็อก (Log source หรือ Log generation)

แหล่งกำเนิดข้อมูลล็อกที่นำมาใช้เพื่อวิเคราะห์ปัญหาทางด้านความมั่นคงปลอดภัย ประกอบด้วย

- ข้อมูลล็อกที่เกิดจากระบบปฏิบัติการของอุปกรณ์คอมพิวเตอร์ทั้งเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่าย
- ข้อมูลล็อกที่เกิดจากแอพพลิเคชันบนระบบ
- ข้อมูลล็อกที่เกิดจากอุปกรณ์หรือซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบ

การบันทึกข้อมูลล็อกและการส่งข้อมูลล็อก สามารถบันทึกข้อมูลล็อกได้สองรูปแบบ

- การบันทึกข้อมูลล็อกอย่างต่อเนื่องหรือ Continuous คือเมื่อมีเหตุการณ์เกิดขึ้นจะบันทึกข้อมูลล็อกทันที
- การบันทึกข้อมูลล็อกตามระยะเวลาที่กำหนดไว้ หรือเมื่อถึงจำนวนของข้อมูลที่กำหนดไว้แล้วแต่กรณี เรียกว่า Batches กล่าวคือเมื่อเกิดเหตุการณ์บนระบบ ระบบจะรวบรวมบันทึกไว้ในที่พักชั่วคราวจนช่วงเวลาที่กำหนดหรือจำนวนข้อมูลที่กำหนดไว้ จะนำข้อมูลบันทึกในสื่อบันทึกข้อมูลที่กำหนดไว้หรือส่งข้อมูลล็อกไปที่ล็อกเซิร์ฟเวอร์เป็นต้น ในกรณีที่บันทึกแบบ Batches ควรคำนึงถึงความต้องการข้อมูลล็อกภายในระยะเวลาที่กำหนดว่าจะมีข้อมูลล็อกเพื่อให้นำมาใช้วิเคราะห์ได้ทันเวลาหรือไม่

3.1. ข้อมูลล็อกที่เกิดจากระบบปฏิบัติการ (Operating system log)

ระบบปฏิบัติการสำหรับเซิร์ฟเวอร์ (Servers) เครื่องผู้ใช้งาน (Workstations) รวมถึงอุปกรณ์เครือข่าย เช่น Routers หรือ Switches สามารถบันทึกข้อมูลล็อกของกิจกรรมที่เกิดขึ้นที่เกี่ยวเนื่องกับระบบ โดยสามารถแบ่งได้เป็นสองประเภทคือ

System Events หรือข้อมูลล็อกบันทึกเหตุการณ์ที่เกิดขึ้นและเกี่ยวข้องกับระบบปฏิบัติการหรือส่วนประกอบของระบบปฏิบัติการเอง ตัวอย่างเช่นการปิดระบบปฏิบัติการหรือการเปิดใช้งานระบบปฏิบัติการ (Boot and Shutting down Operating System) หรือการเริ่มต้นทำงานของซอฟต์แวร์ที่ให้บริการบนเครื่องเซิร์ฟเวอร์เป็นต้น ข้อมูลล็อกดังกล่าวนีสำคัญต่อการวิเคราะห์และแก้ไขปัญหาที่เกิดขึ้นต่อระบบโดยตรง และมักจะเกี่ยวข้องกับการวิเคราะห์ปัญหาทางด้านความมั่นคงปลอดภัยของระบบปฏิบัติการด้วย ตัวอย่างเช่น

```
Aug 16 06:01:50 localhost@server kernel: kjournald starting.  Commit
interval 5 seconds
Aug 16 06:01:50 localhost@server kjournald starting.  Commit interval 5
seconds
```

```
Aug 17 06:01:51 localhost@server Allocating PCI resources starting at
40000000 (gap: 3c000000:c2c00000)
Aug 17 06:01:51 localhost@server kernel: ehci_hcd 0000:00:10.4: USB 2.0
started, EHCI 1.00, driver 10 Dec 2004
…
Aug 25 06:00:42 localhost@server syslog-ng[2005]: Termination requested via
signal, terminating;
Aug 25 06:00:42 localhost@server syslog-ng[2005]: syslog-ng shutting down;
version='2.0.9'
Aug 25 06:01:51 localhost@server syslog-ng[2004]: syslog-ng starting up;
version='2.0.9'
…
Aug 25 04:02:04 localhost@server logrotate: ALERT exited abnormally with [1]
Aug 25 06:00:01 localhost@server shutdown[11127]: shutting down for system
reboot
Aug 25 06:01:51 localhost@server kernel: SI 27 (level, low) -> IRQ 169
```

Audit Records หรือข้อมูลล็อกทางด้านความมั่นคงปลอดภัยบนระบบปฏิบัติการเช่น ข้อมูลล็อกการพิสูจน์ตัวตน การเข้าถึงไฟล์ในระบบ การเปลี่ยนแปลงไฟล์คอนฟิกกูเรชันของระบบ การเปลี่ยนแปลงบัญชีผู้ใช้ การเปลี่ยนแปลงสิทธิของผู้ใช้บนระบบ เป็นต้น โดยทั่วไปผู้ดูแลระบบจำเป็นจะต้องดำเนินการปรับแต่งระบบปฏิบัติการเพิ่มเติมเพื่อให้สามารถเก็บบันทึกข้อมูลล็อกที่เกี่ยวข้องกับความมั่นคงปลอดภัยนี้ด้วยตัวเอง

ตัวอย่างข้อมูลล็อกที่เกี่ยวข้องกับความมั่นคงปลอดภัยของระบบ

```
Aug 1 22:25:41 localhost@server sshd[7876]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.96.6  user=teerapap
Aug 1 22:25:43 localhost@server sshd[7876]: Failed password for teerapap
from 192.168.1.6 port 1068 ssh2
Aug 1 22:25:46 localhost@server sshd[7876]: Accepted password for teerapap
from 192.168.1.6 port 1068 ssh2
Aug 1 22:25:46 localhost@server sshd[7876]: pam_unix(sshd:session): session
opened for user suwit by (uid=0)
Aug 1 22:25:55 localhost@server sshd[7909]: Connection closed by
192.168.1.96
Aug 1 22:26:52 localhost@server su: pam_unix(su-l:auth): authentication
failure; logname=suwit uid=502 euid=0 tty=pts/0 ruser=suwit rhost=
user=root
Aug 1 22:27:00 localhost@server su: pam_unix(su-l:auth): authentication
failure; logname=suwit uid=502 euid=0 tty=pts/0 ruser=suwit rhost=
user=root
Aug 1 22:27:05 localhost@server sshd[7919]: Connection closed by
192.168.1.96
Aug 1 22:27:10 localhost@server su: pam_unix(su-l:auth): authentication
failure; logname=suwit uid=502 euid=0 tty=pts/0 ruser=suwit rhost=
user=root
Aug 1 22:27:38 src@serverwifi su: pam_unix(su-l:session): session opened for
user root by suwit(uid=502)
```

การวิเคราะห์ปัญหาของการใช้งานและปัญหาทางด้านความมั่นคงปลอดภัยของระบบเกี่ยวข้องกับการนำข้อมูลล็อกทีเกี่ยวข้องกับระบบปฏิบัติการทั้ง 2 ประเภทนี้มาวิเคราะห์โดยตรง เนื่องจากว่าเป็นข้อมูลล็อกโดยตรงที่เกิดขึ้นบนเครื่องที่เซิร์ฟเวอร์ที่ให้บริการ หรือเครื่องใช้งานของผู้ใช้งานโดยตรง ตัวอย่างเช่น ข้อมูลล็อกบนอุปกรณ์ไฟร์วอลล์ระบุว่ามีการเชื่อมต่อเกิดขึ้นบนเซิร์ฟเวอร์จากภายนอก แต่ไม่ได้ระบุรายละเอียดของการเข้าถึง ซึ่งต้องใช้ข้อมูลล็อกที่เกิดขึ้นจากระบบปฏิบัติการของเซิร์ฟเวอร์ที่เกียวข้อง ซึ่งควรจะมีข้อมูลล็อกของการพิสูจน์ตัวตน การเข้าถึงไฟล์บนระบบ หรือเหตุการณ์ผิดปกติอื่นเช่นการปิดเครื่องเซิร์ฟเวอร์เป็นต้น ข้อมูลล็อกบนระบบปฏิบัติการที่นำมาวิเคราะห์เพิ่มเติมสามารถบอกรายละเอียดเพิ่มเติมได้ครอบคลุมมากยิ่งขึ้น บางครั้งจำเป็นจะต้องใช้ข้อมูลล็อกที่เกิดจากแอพพลิเคชันบนเซิร์ฟเวอร์นำมาวิเคราะห์ร่วมด้วยเป็นต้น

3.2. ข้อมูลล็อกที่เกิดจากแอพพลิเคชันบนระบบ (Application log)

แอพพลิเคชันบนระบบหรือ Application สามารถจำแนกได้เป็นสองประเภท ประเภทแรกเป็นแอพพลิเคชันให้บริการทั่วไปเช่นแอพพลิเคชันระบบอีเมล์ แอพพลิเคชันระบบเว็บเซิร์ฟเวอร์ แอพพลิเคชันระบบอินทราเน็ต แอพพลิเคชันสำหรับการโอนย้ายไฟล์ระยะไกล (FTP Application Server) ประเภทที่สองเป็นแอพพลิเคชันที่สัมพันธ์กับระบบธุรกิจโดยตรงหรือเป็นแอพพลิเคชันเฉพาะทาง เช่นแอพพลิเคชันทางด้านการเงิน (Financial Application) แอพพลิเคชันระบบงานสารบรรณเพื่อบริหารจัดการเอกสารภายในหน่วยงาน แอพพลิเคชันระบบการวางแผนทรัพยากรภายในองค์กรหรือ Enterprise Resource Planning (ERP) แอพพลิเคชันของงานจัดซื้อภายในองค์กร แอพพลิเคชันทางด้าน Logistic เป็นต้น

ข้อมูลล็อกที่เกิดจากแอพพลิเคชันบนระบบมีรูปแบบการจัดเก็บข้อมูลล็อกเป็น 2 แบบคือแบบแรกคือแอพพลิเคชันที่เก็บบันทึกข้อมูลล็อกโดยตรง หรือแบบที่สองคือแอพพลิเคชันส่งข้อมูลล็อกให้ระบบปฏิบัติการเก็บให้ ประเภทของข้อมูลล็อกที่เป็นประโยชน์ต่อการนำมาวิเคราะห์ปัญหาทางด้านความมั่นคงปลอดภัยที่น่าสนใจ มีรายละเอียดดังนี้

ข้อมูลล็อกการร้องขอและการตอบกลับของแอพพลิเคชันหรือ **Application requests and responses**: เป็นการบันทึกลำดับการเชื่อมต่อที่เกิดขึ้นจากการร้องขอของผู้ใช้งานมาที่แอพพลิเคชัน ตัวอย่างเช่นข้อมูลล็อกบนแอพพลิเคชันอี-เมล์ (E-mail application server) สามารถบันทึกลำดับการเชื่อมต่อเพื่อส่งอี-เมล์ได้โดยละเอียดตั้งแต่ผู้ส่ง ผู้รับ วันเวลาที่ทำการส่ง หัวข้อจดหมายอี-เมล์ ไฟล์แนบได้ หรือกรณีของข้อมูลล็อกของแอพพลิเคชันเว็บเซิร์ฟเวอร์ (Web server application) เก็บบันทึกข้อมูลการเชื่อมต่อจากไอพีแอดเดรสต้นทาง หน้าเว็บที่เข้าถึง ข้อมูลตอบกลับผู้ใช้ หรือแอพพลิเคชันทางด้านการเงิน ซึ่งจะมีการบันทึกข้อมูลล็อกของ Transaction ที่เกิดขึ้นกับธุรกรรมทางการเงินของผู้ใช้โดยละเอียดเป็นต้น

ตัวอย่างข้อมูลล็อกของ Sendmail และ Net-SNMP ซึ่งแสดงการร้องขอและตอบกลับของแอพพลิเคชันบนเซิร์ฟเวอร์ตระกูลยูนิกซ์

```
Nov 21 12:21:29 server sendmail[28855]: jALHLTNW028855:
to=Dr_xxx@hotmail.com, ctladdr=apache (48/48), delay=00:00:00,
xdelay=00:00:00, mailer=relay, pri=31029, relay=[127.0.0.1] [127.0.0.1],
dsn=2.0.0, stat=Sent (jALHLTs3028856 Message accepted for delivery)
…
Aug 25 22:30:31 localhost@server snmpd[2271]: Received SNMP packet(s) from
UDP: [127.0.0.1]:10503
Aug 25 22:30:33 localhost@server snmpd[2271]: Connection from UDP:
[192.168.1.1]:10503
Aug 25 22:30:33 localhost@server snmpd[2271]: Received SNMP packet(s) from
UDP: [192.168.1.1]:10503
Aug 25 22:31:41 localhost@server snmpd[2271]: Connection from UDP:
[127.0.0.1]:10503
```

ข้อมูลล็อกการเข้าใช้งานระบบหรือ **Account Information**: เป็นการบันทึกข้อมูลล็อกการพิสูจน์ตัวตนทั้งในกรณีที่สำเร็จและไม่สำเร็จที่เกิดขึ้นกับแอพพลิเคชัน การเปลี่ยนแปลงบัญชีผู้ใช้งานบนระบบแอพพลิเคชันเช่นการเปลี่ยนสิทธิหรือหน้าที่บนแอพพลิเคชัน ระบบแอพพลิเคชันบางระบบสามารถบันทึกข้อมูลล็อกเงื่อนไขพิเศษได้เช่น เมื่อพบว่ามีการพยายามจะเดาสุ่มรหัสผ่านในหน้าล็อกอินก่อนเข้าใช้งานแอพพลิเคชันระบบจะบันทึกเหตุการณ์นี้ไว้เป็นข้อมูลล็อกและยกเลิกใช้งานบัญชีผู้ใช้นี้ชั่วคราวได้เป็นต้น

ตัวอย่างข้อมูลล็อกการพิสูจน์ตัวตนผ่าน SSH บนระบบปฏิบัติการลีนุกซ์ และข้อมูลล็อกการพิสูจน์ตัวตนเข้ามาผ่าน OpenVPN

```
Aug 15 22:25:41 localhost@server sshd[7876]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=192.168.96.6  user=tawatchai
Aug 15 22:26:04 localhost@server  su: pam_unix(su-l:auth): authentication
failure; logname=seewat uid=502 euid=0 tty=pts/0 ruser=seewat rhost=
user=root
…
Aug 20 13:29:39 localhost@server openvpn[2235]: 203.48.33.231:2686 Data
Channel Decrypt: Using 160 bit message hash 'SHA1' for HMAC authentication
Aug 20 14:29:56 localhost@server openvpn[2235]: client/203.48.33.231:2686
Data Channel Encrypt: Using 160 bit message hash 'SHA1' for HMAC
authentication
```

```
Aug 20 14:29:56 localhost@server openvpn[2235]: client/203.48.33.231:2686
Data Channel
```

ข้อมูลการใช้งานแอพพลิเคชันหรือ **Usage information**: เป็นข้อมูลล็อกบันทึกการใช้งานแอพพลิเคชัน โดยมากจะนำมาใช้เป็นข้อมูลเพื่อปรับปรุงประสิทธิภาพการทำงานของแอพพลิเคชัน หรือนำมาใช้รายงานสถานะการทำงานของแอพพลิเคชัน เช่นข้อมูลล็อกบันทึกจำนวนของข้อมูลที่ระบบแอพพลิเคชันประมวลผลต่อวัน หรือความเร็วในการตอบสนองการร้องขอข้อมูล ขนาดของไฟล์ที่มีการแนบกับระบบงาน ข้อมูลล็อกเหล่านี้สามารถนำมาใช้เป็นข้อมูลเพื่อวิเคราะห์เหตุการณ์ทางด้านความมั่นคงปลอดภัยได้เช่นเดียวกัน เช่นการใช้งานแอพพลิเคชันโดยปกติจะมีการประมวลผลงานจำนวนหนึ่งต่อวัน เมื่อพบจำนวนการประมวลผลมากผิดปกติอาจเป็นการแจ้งเตือนหรือสัญญาณความผิดปกติของเหตุการณ์ได้ ตัวอย่างเช่น

```
Aug  1 00:50:01 localhost@server  snmpd[2271]: Connection from UDP:
[127.0.0.1]:10525
Aug  1 00:50:01 localhost@server snmpd[2271]: Connection from UDP:
[127.0.0.1]:10525
Aug  1 00:50:01 localhost@server snmpd[2271]: Connection from UDP:
[127.0.0.1]:10525
Aug  1 00:50:01 localhost@server snmpd[2271]: Connection from UDP:
[127.0.0.1]:10525
…
Aug  1 16:39:57 localhost@server named[2042]: unexpected RCODE (SERVFAIL)
resolving 'webindex.siamzab.com/AAAA/IN': 192.168.99.1#53
…
Aug  1 06:01:25 localhost@server kernel: TCP bind hash table entries: 65536
(order: 7, 524288 bytes)
Aug  1 06:01:25 localhost@server kernel: TCP: Hash tables configured
(established 131072 bind 65536)
Aug  2 06:01:18 localhost@server kernel: TCP bind hash table entries: 65536
(order: 7, 524288 bytes)
```

ข้อมูลล็อกการทำงานของแอพพลิเคชันหรือ **Operational actions**: เช่นการเริ่มหรือหยุดทำงานของแอพพลิเคชัน การทำงานผิดพลาดที่เกิดขึ้นบนแอพพลิเคชัน การเปลี่ยนแปลงค่าบนแอพพลิเคชัน เป็นต้น ตัวอย่างเช่น

```
Aug 11 06:05:51 192.168.1.21/192.168.1.21 syslog: chilli : chilli daemon
successfully started
Aug 11 06:05:51 192.168.1.21/192.168.1.21 syslog: ttraff : traffic counter
daemon successfully started
Aug 11 06:05:51 192.168.1.21/192.168.1.21 syslog: ttraff: data collection
started
Aug 11 06:05:53 192.168.1.21/192.168.1.21 syslog: chilli : chilli daemon
successfully started
Aug 11 06:05:53 192.168.1.21/192.168.1.21 syslog: klogd : klog daemon
successfully stopped
…
Aug 12 06:01:58 localhost@server monit[2481]: Monit started
Aug 12 06:01:48 localhost@server named[2040]: starting BIND 9.3.3rc2 -u
named -t /var/named/chroot
Aug 12 06:02:02 localhost@server monit[2481]: monit HTTP server started
Aug 12 06:02:02 localhost@server monit[2481]: Monit started
…
Aug 13 17:40:09 localhost@server monit[2481]: 'ADMIN-sshd' trying to restart
Aug 13 17:40:10 localhost@server monit[2481]: 'ADMIN-sshd' start:
/etc/init.d/sshd
Aug 13 17:43:57 localhost@server monit[2481]: 'WWW-httpd' trying to restart
```

นักออกแบบระบบ นักพัฒนาระบบสามารถใช้ข้อมูลล็อกที่เกิดจากแอพพลิเคชันบนระบบเพื่อวิเคราะห์ปัญหาการทำงานรวมถึงการปรับปรุงประสิทธิภาพการทำงานของแอพพลิเคชัน รวมถึงนำไปใช้วิเคราะห์ปัญหาทางด้านความมั่นคงปลอดภัย การวิเคราะห์ความสอดคล้องตามข้อกำหนดการออกแบบของระบบแอพพลิเคชัน รูปแบบล็อกของแอพพลิเคชันที่แตกต่างกันนั้นขึ้นอยู่กับการออกแบบระบบหรือการพัฒนาระบบ

3.3. ข้อมูลล็อกที่เกิดจากอุปกรณ์หรือซอฟต์แวร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของระบบ (Security-related device/software log)

อุปกรณ์หรือซอฟต์แวร์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของระบบเป็นได้ทั้งอยู่ในรูปแบบของอุปกรณ์เครือข่ายหรือ Network-based หรืออยู่บนระบบเซิร์ฟเวอร์ เครื่องลูกข่ายหรือเครื่องผู้ใช้ หรือ Host-based เพื่อใช้บันทึกเหตุการณ์ทางด้านความมั่นคงปลอดภัย มีจุดประสงค์เพื่อป้องกัน ตรวจจับ รวมถึงมีความสามารถในการแก้ไขหรือกู้คืนความเสียหายได้ตามความจำเป็น ตัวอย่างเช่น

Routers หรืออุปกรณ์เลือกเส้นทางระบบเครือข่าย: ควบคุมการใช้งานระบบเครือข่ายและสามารถควบคุมการเชื่อมต่อระบบเครือข่ายได้ บ่อยครั้งมีการทำ Network Address Translation (NAT) เพื่อแปลงไอพีแอดเดรสภายในให้สามารถเชื่อมต่ออินเทอร์เน็ตได้ ข้อมูลล็อกการทำ NAT เป็นข้อมูลล็อกที่สำคัญเพราะบอกถึงการเชื่อมต่อระหว่างเครื่องลูกข่ายภายในและอินเทอร์เน็ตภายนอก นอกจากนี้เป็นข้อมูลล็อกการเชื่อมต่อเครือข่ายที่เกิดขึ้นเป็นต้น

ไฟร์วอลล์ หรือ Firewall: อุปกรณ์หรือซอฟต์แวร์ใช้สำหรับควบคุมการเข้าถึงเครือข่ายด้วยกฎไฟร์วอลล์ สามารถกำหนดไอพีแอดเดรสของการเชื่อมต่อ พอร์ตสำหรับการเชื่อมต่อ สามารถกรองเนื้อความของข้อมูลจราจรคอมพิวเตอร์หรือทราฟฟิกเครือข่ายได้ มีความสามารถในการป้องกันการโจมตีทางระบบเครือข่ายเช่นการป้องกัน Denial of Service หรือการป้องกัน IP Spoofing เป็นต้น ข้อมูลล็อกบนไฟร์วอลล์ถือเป็นแหล่งข้อมูลล็อกสำคัญอีกส่วนหนึ่ง เนื่องจากบันทึกข้อมูลการเชื่อมต่อ การอนุญาตและการไม่อนุญาตให้เชื่อมต่อ รวมถึงข้อมูลล็อกการโจมตีที่เกิดขึ้นบนเครือข่ายเป็นต้น

ตัวอย่างข้อมูลล็อกไฟร์วอลล์ของ IPTables บนระบบปฏิบัติลีนุกซ์

```
Aug 25 22:20:17 192.168.1.21/192.168.1.21 kernel: DROP IN=vlan1 OUT=
MAC=01:00:5e:00:00:01:00:02:cf:b4:b7:84:08:00:46:00:00:24 SRC=192.168.1.1
DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=64587 OPT (94040000)
PROTO=2
Aug 25 22:25:02 192.168.1.21/192.168.1.21 kernel: ACCEPT IN=vlan1 OUT=
MAC=00:1d:7e:dc:1b:37:00:1d:60:8f:44:b6:08:00:45:00:00:41 SRC=192.168.1.99
DST=192.168.1.21 LEN=65 TOS=0x00 PREC=0x00 TTL=64 ID=0 DF PROTO=UDP
SPT=10499 DPT=161 LEN=45
Aug 25 22:26:31 192.168.1.21/192.168.1.21 kernel: DROP IN=vlan1 OUT=
MAC=01:00:5e:00:00:01:00:02:cf:b4:b7:84:08:00:46:00:00:24 SRC=192.168.1.1
DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=64982 OPT (94040000)
PROTO=2
Aug 25 22:28:36 192.168.1.21/192.168.1.21 kernel: DROP IN=vlan1 OUT=
MAC=01:00:5e:00:00:01:00:02:cf:b4:b7:84:08:00:46:00:00:24 SRC=192.168.1.1
DST=224.0.0.1 LEN=36 TOS=0x00 PREC=0x00 TTL=1 ID=65212 OPT (94040000)
PROTO=2
```

พร็อกซีเซิร์ฟเวอร์ (Proxy Server) หรือ เว็บพร็อกซี (Web Proxies): ทำหน้าที่เหมือนไฟร์วอลล์ในระดับแอพพลิเคชัน ควบคุมการเข้าใช้งานเว็บแอพพลิเคชันที่เข้าถึงด้วยโปรโตคอล HTTP หรือ FTP เป็นต้น และยังช่วยเพิ่มความเร็วการใช้งานอินเทอร์เน็ต สนับสนุนการควบคุมการไม่อนุญาตให้เข้าถึงเว็บไม่พึงประสงค์ได้ ข้อมูลล็อกในเว็บพร็อกซีประกอบไปด้วย วันเวลาที่ผู้ใช้เข้าถึงข้อมูลเว็บ เว็บที่เข้าถึง ขนาดของข้อมูล ไอพีแอดเดรสของผู้ใช้เป็นต้น ตัวอย่างซอฟต์แวร์เช่น Squid หรือ Microsoft ISA Server หรืออุปกรณ์โดยเฉพาะ (Appliance) เช่นผลิตภัณฑ์ของ Bluecoat เป็นต้น

ตัวอย่างข้อมูลล็อกที่ผู้ใช้งานการเข้าถึงเว็บของ Squid

```
1219678885.680    245 192.168.56.80 TCP_MISS/200 19875 GET
http://directory.narak.com/vote.php? - DIRECT/203.121.145.220 text/html
1219678885.776    748 192.168.56.78 TCP_MISS/200 337 GET
http://widget.alot.com/geocode - DIRECT/208.76.11.230 text/html
1219678885.791    839 192.168.56.73 TCP_MISS/200 424 GET
http://www.thaiebayuser.com/forum/index.php? - DIRECT/74.86.247.98 text/html
1219678885.832     25 192.168.56.78 TCP_IMS_HIT/304 325 GET
http://www.sanook.com/temp/hdmbg2.jpg - NONE/- image/jpeg
1219678885.980    144 192.168.56.80 TCP_MISS/200 426 GET
http://lvs.truehits.in.th/goggen.php? - DIRECT/164.115.2.135 image/jpeg
1219678886.547   1044 192.168.56.54 TCP_MISS/200 360 GET
http://tracker.prq.to/scrape.php? - DIRECT/77.247.176.136 text/plain
```

```
1219678886.643    610 192.168.56.80 TCP_MISS/200 82392 GET
http://images2.narak.com/banner/jobs_468x60.gif - DIRECT/203.151.233.144
image/gif
```

ซอฟต์แวร์ป้องกันมัลแวร์หรือ**โปรแกรมป้องกันไวรัส**: ซอฟต์แวร์เพื่อป้องกันมัลแวร์หรือ (Malware หรือ Malicious Software หรือโปรแกรมไม่ประสงค์ดี ซึ่งรวมถึงสปายแวร์ หนอนอินเตอร์เน็ต โทรจัน รูทคิท (Rootkit) เช่นซอฟต์แวร์ Antivirus ทำการบันทึกวันเวลาที่สามารถตรวจจับมัลแวร์บนเครื่องคอมพิวเตอร์ หรือผลลัพธ์จากการสแกนฮาร์ดดิสก์เพื่อหาไวรัสบนเครื่อง ตัวอย่างเช่น Kaspersky, ESET NOD, Symantec Antivirus, Trend Micro, McAfee เป็นต้น

อุปกรณ์หรือซอฟต์แวร์เพื่อเข้าถึงระบบจากระยะไกลผ่านทางเครือข่ายหรือ Remote Access Software: การเข้าถึงระยะไกลผ่านทางเครือข่ายเป็นการเชื่อมต่อผ่านช่องทางที่เรียกว่า Virtual Private Network หรือ VPN เพื่อเป็นการสร้างช่องทางการเชื่อมต่อที่มีการเข้ารหัสและพิสูจน์ตัวตนก่อนเชื่อมต่อเข้าสู่ระบบเครือข่ายขององค์กร และเข้าถึงระบบภายในองค์กรผ่านทาง VPN ได้ อุปกรณ์หรือซอฟต์แวร์ Remote Access จะบันทึกข้อมูลล็อกการพิสูจน์ตัวตนและการเชื่อมต่อที่เกิดขึ้น บางระบบสามารถบันทึกระยะเวลาการเข้าใช้งาน ขนาดข้อมูลที่เครื่องลูกข่ายใช้ทั้งการดาวน์โหลดและการอัพโหลด และอาจรวมถึงปริมาณการใช้งานทรัพยากรบนระบบเครือข่ายด้วย เช่น SSL VPN อย่างอุปกรณ์ Juniper SSL VPN หรือใช้ Microsoft ISA Server เพื่ออนุญาตให้เข้าถึงด้วยโพรโตคอล PPTP หรือ L2TP เป็นต้น หรือการใช้ซอฟต์แวร์ POPTOP บนระบบปฏิบัติการยูนิกซ์เป็นต้น

ระบบตรวจจับผู้บุกรุกหรือ Intrusion Detection Systems (IDS) และ**ระบบป้องกันผู้บุกรุก**หรือ Intrusion Prevention Systems (IPS): ทำการบันทึกข้อมูลล็อกจากการตรวจจับเหตุการณ์การบุกรุก การโจมตีระบบ หรือเหตุการณ์น่าสงสัยอื่น รวมถึงข้อมูลล็อกการป้องกันการบุกรุกที่เกิดขึ้น ระบบตรวจจับผู้บุกรุกเช่น Snort

ซอฟต์แวร์บริหารจัดการช่องโหว่ระบบคอมพิวเตอร์หรือ Vulnerability Management Software: เป็นซอฟต์แวร์เพื่อบริการจัดการช่องโหว่บนระบบปฏิบัติการหรือระบบเครือข่ายที่สนับสนุน ซอฟต์แวร์บริหารจัดการแพตซ์หรือ Patch Management Software ใช้สำหรับปรับปรุงช่องโหว่และเก็บบันทึกข้อมูลการปรับปรุงช่องโหว่ของระบบ และสถานะข้อมูลช่องโหว่ของแต่ละอุปกรณ์ รวมถึงซอฟต์แวร์ตรวจประเมินช่องโหว่หรือ Vulnerability Assessment Software เพื่อค้นหาช่องโหว่บนระบบคอมพิวเตอร์และหาแนวทางปรับปรุงในลำดับถัดไป ในแต่ละครั้งของการตรวจประเมินช่องโหว่ ข้อมูลล็อกที่บันทึกประกอบไปด้วย วันเวลาที่ดำเนินการตรวจสอบ เครื่องหรืออุปกรณ์ที่ดำเนินการตรวจสอบ ช่องโหว่ที่พบ คำแนะนำเป็นต้น ตัวอย่างซอฟต์แวร์เช่น Microsoft Baseline Security Analyzer (MBSA), Nessus หรือผลิตภัณฑ์จาก GFI Network Security เป็นต้น

เซิร์ฟเวอร์สำหรับการพิสูจน์ตัวตนหรือ **Authentication Servers**: เซิร์ฟเวอร์ให้บริการการพิสูจน์ตัวตนและการเข้าถึงข้อมูลผู้ใช้ด้วยโปรโตคอล Lightweight Directory Access Protocol หรือ LDAP เช่น Microsoft Active Directory หรือ Novell E-Directory เป็นต้น หรือความสามารถทางด้าน Single Sign-on เพิ่มเติม รวมถึงการพิสูจน์ตัวตนด้วยโปรโตคอล RADIUS หรือ TACAC+ เช่น FreeRadius หรือ Funk ด้วย ข้อมูลล็อกที่พบได้เช่นล็อกของการพิสูจน์ตัวตนซึ่งบันทึกข้อมูลบัญชีผู้ใช้ รหัสผ่าน สถานะการพิสูจน์ตัวตน วันเวลาเป็นต้น

ตัวอย่างข้อมูลล็อกการพิสูจน์ตัวตนของ FreeRadius หรือ Authentication Log

```
Aug 12 19:49:46 localhost@server radiusd[2305]: Login OK: [6HN3fe5/<CHAP-
Password>] (from client APF2 port 3 cli 00-17-C4-23-A3-2D)
Aug 12 20:17:26 localhost@server radiusd[2305]: Login OK: [8uJY5653/<CHAP-
Password>] (from client APF2 port 7 cli 00-1B-77-F3-18-C3)
Aug 12 20:25:07 localhost@server radiusd[2305]: Invalid user
(rlm_sqlcounter: Maximum never usage time reached): [AU33WHq/<CHAP-
Password>] (from client APF5 port 8 cli 00-18-DE-46-8A-12)
Aug 12 21:31:57 localhost@server radiusd[2305]: Login OK: [VU6agCw/<CHAP-
Password>] (from client APF5 port 10 cli 00-0E-35-58-BA-8D)
Aug 12 21:34:53 localhost@server radiusd[2305]: Multiple logins (max 1) :
[RU4XgCw/<CHAP-Password>] (from client APF2 port 0 cli 00-0E-35-58-BA-8D)
```

ตัวอย่างข้อมูลล็อกการบันทึกการใช้งานของผู้ใช้งานที่พิสูจน์ตัวตนแล้วของ FreeRadius หรือ Accounting Log

```
Sun Mar 18 04:35:24 2008
       Acct-Status-Type = Start
       User-Name = “uXas36yT”
       Calling-Station-Id = “00-14-2A-4B-D8-71”
       Called-Station-Id = “00-14-22-17-0A-11”
       NAS-Port-Type = Wireless-802.11
       NAS-Port = 103
       NAS-Port-Id = “00000103”
       NAS-IP-Address = 192.168.1.1
       NAS-Identifier = “AP221”
       Framed-IP-Address = 192.168.1.5
       Acct-Session-Id = “4921040504040422”
       Acct-Unique-Session-Id = “d6e75vbd643333a754”
       Timestamp = 5040232301
```

เกตเวย์ที่ต้องมีการพิสูจน์ตัวตนก่อนการใช้งานหรือ **Authentication Gateway** ถ้านำไปใช้งานในระบบเครือข่ายไร้สายจะเรียกว่า Captive Portal เพื่อเข้าถึงเครือข่ายไร้สายแบบ HotSpot หรือถ้าอุปกรณ์หรือเซิร์ฟเวอร์มีการตรวจสอบคุณสมบัติของเครื่องลูกข่ายก่อนเชื่อมต่อเข้าระบบเครือข่ายเช่น ตรวจสอบว่าเครื่องลูกข่ายได้รับการปรับปรุงความมั่นคงปลอดภัยตามนโยบายการเชื่อมต่อเครือข่ายแล้วหรือไม่ได้เป็นต้น และคัดแยกโดยจัดให้เครื่องลูกข่ายที่ผ่านการตรวจสอบสามารถเข้าเชื่อมต่อเครือข่ายได้ตามปกติ ในกรณีที่ไม่ผ่านจะต้องดำเนินการปรับปรุงเครื่องลูกข่ายก่อน อุปกรณ์ลักษณะนี้เรียกว่า **Network Quarantine Server** ข้อมูลล็อกโดยมากจะประกอบไปด้วย วันเวลาของเครื่องผู้ใช้ หมายเลขไอพีแอดเดรสก่อนการเชื่อมต่อและหลังการเชื่อมต่อ (อาจจะเป็นหมายเลขไอพีแอดเดรสหมายเลขเดียวกันได้) สถานะการพิสูจน์ตัวตน ชื่อผู้ใช้สำหรับพิสูจน์ตัวตนเป็นต้น

ตัวอย่างข้อมูลล็อกของระบบ Authentication Gateway ที่ใช้ ChilliSpot ให้บริการเครือข่ายไร้สาย

```
Aug 13 20:34:03 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 3230:
New DHCP request from MAC=00-1B-77-0A-F8-20
Aug 13 20:34:05 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 3200:
Client MAC=00-1B-77-0A-F8-20 assigned IP 192.168.12.122
Aug 13 20:34:10 192.168.1.21/192.168.1.21 chillispot[1102]: chilli.c: 3502:
Successful UAM login from username=56F7hesa IP=192.168.12.122
Aug 19 23:31:25 192.168.1.21/192.168.1.21 chillispot[1102]: chilli.c: 3502:
Successful UAM login from username=6A7eRkc IP=192.168.12.73
Aug 20 06:59:34 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 3502:
Successful UAM login from username=Yb4agCw IP=192.168.12.97
Aug 25 20:58:31 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 3280:
DHCP addr released by MAC=00-1B-77-0A-F8-20 IP=192.168.12.56
Aug 25 21:05:53 192.168.1.21/192.168.1.21 chillispot[1099]: chilli.c: 968:
Rereading configuration file and doing DNS lookup
```

เอกสารอ้างอิง

[1] ประกาศราชกิจจานุเบกษา, "*พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐*", วันที่ 18 มิถุนายน 2550

[2] นายพรเพชร วิชิตชลชัย ประธานศาลอุทธรณ์ภาค ๔, "*คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐*"

[3] หน่วยปฏิบัติการวิจัยเทคโนโลยีและนวัตกรรมเพื่อความมั่นคงของประเทศ และคณะอนุกรรมการด้านความมั่นคง ภายใต้ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ ในคณะอนุกรรมการธุรกรรมทางอิเล็กทรอนิกส์, "*มาตรฐานการรักษาความมั่นคงปลอดภัย ในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน 2.5) ประจำปี 2550*", ISBN: 978-974-229-584-4, พิมพ์ครั้งที่ 1, ธันวาคม 2550

[4] Karen Kent and Murugiah Souppaya, NIST, Special Publication 800-92, "*Guide to Computer Security Log Management*", September 2006

[5] Roger Meyer, "*Auditing a Corporate Log Server*" GAIC Gold Certification, GIAC Systems and Network Auditor (GSNA), SANS Institute 2006 Reading Room, 17 September 2006

[6] อ. ปริญญา หอมเอนก และทีมงาน ACIS Professional Center & ACIS i-Secure, "*คู่มือวิธีปฏิบัติสำหรับองค์กรตาม พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐*", http://www.acisonline.net

[7] ประกาศราชกิจจานุเบกษา, "*ประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐*", วันที่ 23 สิงหาคม 2550

[8] SN ISO/IEC 17799:2005, "*Information technology – Security Technique – Code of practice for information security management (ISO/IEC 17799:2005)*", Second Edition, 2005-06-15

[9] Chaiyakorn Apiwathanokul, "*Computer Time Synchronization Scheme*" , http://www.etcommission.go.th/documents/standard/time_sync_server_v1_0.pdf, 3 October 2007

[10] อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, "*การเทียบเวลาด้วย Network Time Protocol ให้สอดคล้องกับ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550*" http://www.thaicert.org/paper/basic/NTPandLAW.php, 27 กุมภาพันธ์ 2551

[11] อสมาภรณ์ ฉัตรัตติกรณ์ และ ชวลิต ทินกรสูติบุตร, "*คู่มือการใช้บริการ Time Server [ฉบับปรับปรุง]*", http://www.thaicert.org/paper/basic/manualTimeServer.php, 27 กุมภาพันธ์ 2551

[12] Wikipedia, "*List of RADIUS Servers*", http://en.wikipedia.org/wiki/List_of_RADIUS_Servers

[13] Wikipedia, "*List of mail servers*", http://en.wikipedia.org/wiki/List_of_mail_servers

[14] Wikipedia, "*List of FTP server software*", http://en.wikipedia.org/wiki/List_of_FTP_server_software

[15] Wikipedia, "*Comparison of web server software*" http://en.wikipedia.org/wiki/Comparison_of_web_servers

[16] Wikipedia, "*News server*", http://en.wikipedia.org/wiki/News_server

[17] Wikipedia, "*Network Access Control*", http://en.wikipedia.org/wiki/Network_Access_Control

[18] Wikipedia, "*Proxy Server*", http://en.wikipedia.org/wiki/Proxy_server

[19] สุรางคณา วายุภาพ, "ข้อควรรู้เกี่ยวกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550", ฝ่ายศึกษาประเด็นด้านจริยธรรม กฎหมาย และผลกระทบทางสังคมของเทคโนโลยีสารสนเทศและการสื่อสาร (Ethical, Legal and Social Impacts of ICT : ELSIT), ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ