ชุดความรู้

Firewall and Logs

โดย นายยุทธชัย เครือแก้ว

โครงการพัฒนาระบบมาตรฐานการการให้บริการ
๒๕๕๗ : ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน

Firewall and Logs

ระบบรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย

ปัจจุบันเป็นที่ยอมรับกันโดยทั่วไปว่าระบบเครือข่ายอินเทอร์เน็ต ได้เข้ามีบทบาทและมีส่วนเกี่ยวข้องกับกิจกรรมของมนุษย์ในหลายด้าน เช่น การสนทนาพูดคุย การสื่อสารข้อมูล การแลกเปลี่ยนข่าวสารความรู้ การซื้อขายแบบอิเล็กทรอนิกส์ การศึกษาทางไกล การเผยแพร่ข่าวสาร การประชาสัมพันธ์ เป็นต้น กล่าวได้ว่าอิทธิพลของเทคโนโลยีทางด้านคอมพิวเตอร์และอินเทอร์เน็ตได้เข้ามา ส่วนสำคัญต่อการดำเนินชีวิตของคนเราเป็นอย่างมาก แต่อย่างไรก็ตามสิ่งเหล่านี้ก็ส่งผลต่อความปลอดภัยของระบบเครือข่ายเช่นกัน เนื่องจากผู้บุกรุกจะอาศัยช่องทางการสื่อสารบนระบบเครือข่ายในการบุกรุกหรือ โจมตีระบบนั่นเอง

ปัญหาการรักษาความมั่นคง ปลอดภัยของระบบเครือข่ายและข้อมูลสารสนเทศจึงเป็นปัญหาที่สำคัญมากใน ปัจจุบัน เนื่องจากการถูกคุกคามจากผู้ไม่สงค์ดี หรือจากโปรแกรมบางประเภทที่มุ่งทำลายข้อมูลมีเพิ่มมากขึ้น และทำให้เกิดความเสียหายเป็นอย่างมากต่อระบบงานสารสนเทศขององค์กร ตลอดจนภาพลักษณ์ขององค์กรด้วย ดังนั้น แต่ละองค์กรควรมีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และ เครือข่าย ซึ่งเป็นกระบวนการที่เกี่ยวข้องกับการป้องกันและตรวจสอบการเข้าใช้งานโดยไม่ ได้รับอนุญาต กล่าวคือการป้องกันจะช่วยสกัดกั้นไม่ให้ผู้ที่ไม่ได้รับอนุญาต หรือที่เรียกว่า “ผู้บุกรุก” เข้าถึงระบบของหน่วยงานได้ไม่ว่าจะเป็นส่วนใดก็ตาม ส่วนการตรวจสอบจะทำให้ทราบว่ามีใครพยายามบุกรุกเข้ามาในระบบหรือไม่ การบุกรุกสำเร็จหรือไม่ และผู้บุกรุกได้ทำอะไรกับระบบบ้าง

ดัง นั้น หากแต่ละองค์กรมีเครื่องมือในการรักษาความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และเครือข่ายที่ดี จะทำให้ช่วยลดโอกาสเสี่ยงต่อการถูกโจมตีหรือคุมคามจากผู้ไม่ประสงค์ดีได้

องค์ประกอบของความมั่นคงปลอดภัย (Security Requirement)

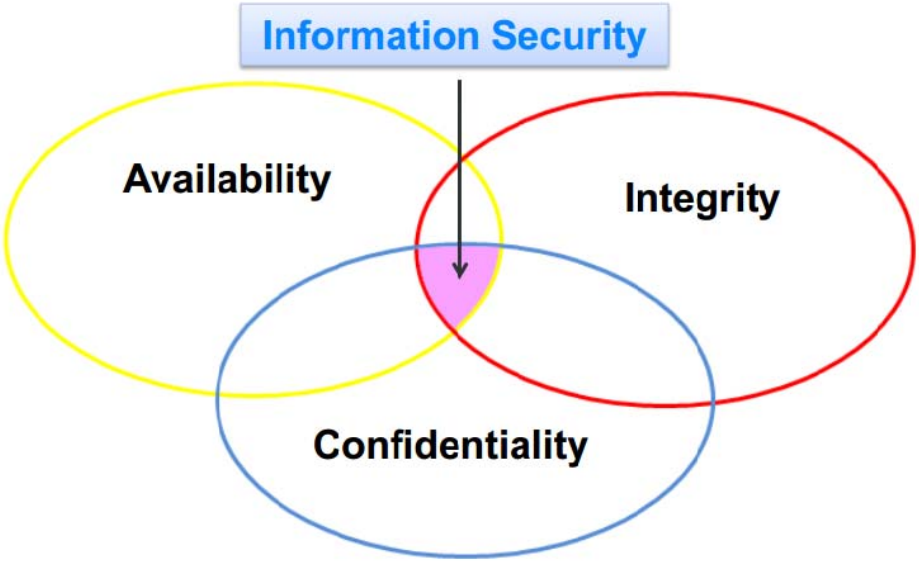
การที่จะบอกได้ว่าข้อมูลมีความมั่นคงปลอดภัยหรือไม่ ก็ด้วยการวิเคราะห์จากคุณสมบัติขององค์ประกอบของความมั่นคงปลอดภัย 3 ด้าน คือ

1. <u>ความลับ (Confidentiality)</u> การ รักษาความลับของข้อมูล หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เนื่องจากข้อมูลบางอย่างมีความสำคัญและจำเป็นต้องเก็บไว้เป็นความลับ เพราะถ้าถูกเปิดเผยอาจมีผลเสียหรือเป็นอันตรายต่อเจ้าของได้

2. <u>ความถูกต้อง (Integrity)</u> ความถูกต้องและความสมบูรณ์ของข้อมูล คือความครบถ้วน ความถูกต้องและไม่มีสิ่งแปลกปลอม ดังนั้นสารสนเทศที่มีความถูกต้องและความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน ในขณะที่ภัยคุกคามที่สำคัญที่มีผลต่อความถูกต้องและความสมบูรณ์ของสารสนเทศ คือ ไวรัส เวิร์ม แฮคเกอร์ หรือสัญญาณรบกวน เป็นต้น

3. ความพร้อมใช้งาน (Availability)

ความพร้อมใช้งานของข้อมูลและสารสนเทศ (Availability) เป็นการรับรองได้ว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศต่างๆพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน อีกทั้งเป็นการให้ผู้ที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลหรือทรัพยากรได้ตามที่ต้องการ



ภัยคุกคามและการโจมตี

ภัย คุกคาม หมายถึง สิ่งที่อาจก่อให้เกิดความเสียหายกับระบบคอมพิวเตอร์ในรูปแบบของการทำลาย เปิดเผย แก้ไขข้อมูล รวมถึงการทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้ได้ ไม่ว่าจะเป็นภัยคุกคามที่เกิดขึ้นโดยอุบัติเหตุ เช่น ไฟไหม้ น้ำท่วม หรือเกิดขึ้นจากเจตนาของบุคคลที่ประสงค์ร้ายต่อระบบ เรียกว่า “ผู้บุกรุก” (Intruder) หรือ “ผู้โจมตี”(Attacker) หรืออาจเรียกว่า “แฮคเกอร์”(Hacker) หรือ “แคร็คเกอร์”(Cracker) โดยจะทำการโจมตีระบบ (Attack) เพื่อสร้างความเสียหายให้เกิดขึ้นกับระบบ ซึ่งเป็นการกระทำที่พยายามจะข้ามผ่าน (bypass) กระบวนการควบคุมความปลอดภัยของระบบคอมพิวเตอร์

สำหรับบุคคลที่เจตนากระทำการโจมตีระบบ สามารถแบ่งเป็น 2 ประเภท คือ

1. ผู้บุกรุกจากภายนอก (Outsider Intruder) หมายถึง ผู้บุกรุกที่มาจากภายนอกเครือข่ายของหน่วยงาน เช่น การโจมตีระบบผ่านเครือข่ายอินเทอร์เน็ตรูปแบบต่างๆ

2. ผู้บุกรุกจากภายใน (Insider Intruder) หมายถึง ผู้บุกรุกที่เป็นผู้ใช้งาน ซึ่งเป็นผู้มีสิทธิ์ในการใช้ระบบหรือเครือข่ายภายในหน่วยงาน ตลอดจนผู้ใช้ที่ใช้สิทธิ์ไปในทางที่ผิด หรือการลักลอบใช้สิทธิ์ของผู้ใช้คนอื่น

ระดับของการรักษาความปลอดภัย

ในการรักษาความปลอดภัยของระบบคอมพิวเตอร์นั้น สามารถแบ่งได้หลายระดับ ดังนี้

1. Physical Security หมายถึง ความปลอดภัยของตัวระบบในการป้องกันการเข้าถึงต้องเครื่องของผู้ไม่

ประสงค์ดี เช่น ศูนย์ควบคุมระบบคอมพิวเตอร์พร้อมกุญแจ (Server and Control Room) ซึ่งผู้ที่ได้รับอนุญาตเท่านั้น จึงจะสามารถเข้าถึงตัวเครื่องคอมพิวเตอร์แม่ข่ายได้

2. Host Security หมายถึง ระดับความปลอดภัยของตัวระบบเอง ระบบปฏิบัติการ (Operation System) โปรแกรม และบริการงานสารสนเทศต่างๆ บัญชีผู้ใช้งาน เหล่านี้จะต้องมีการตั้งรหัสผ่านที่ไม่ง่ายจนเกินไป มีการบันทึกเหตุการณ์จราจรทางคอมพิวเตอร์ (Logging)

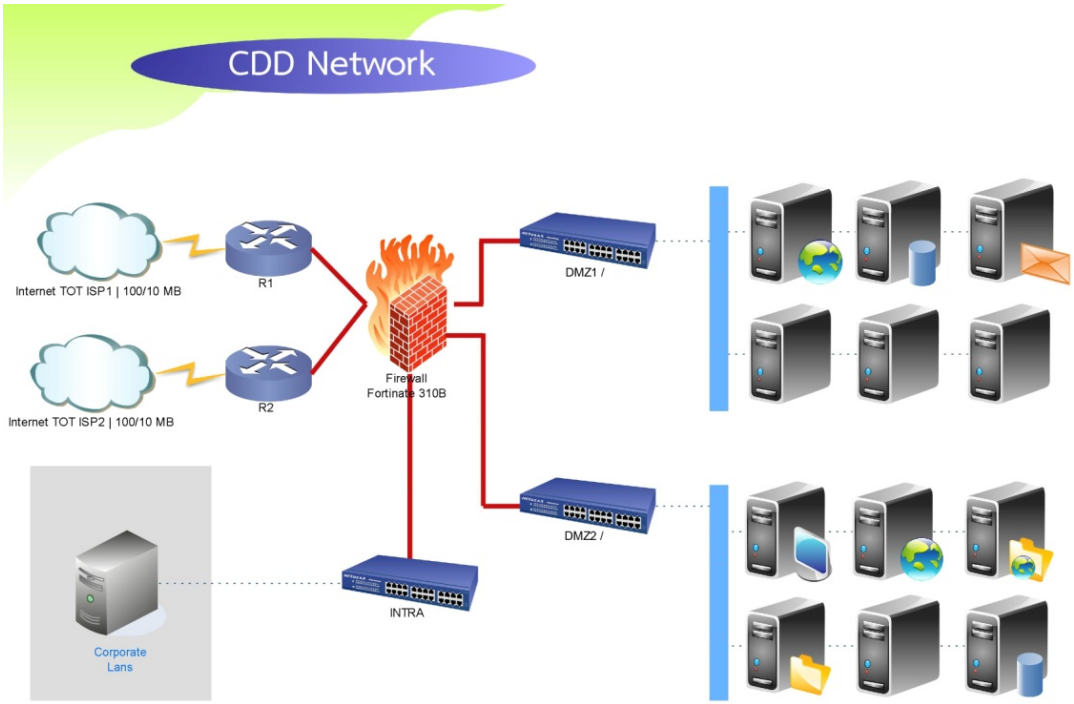
3. Network Security เป็น การป้องกันไม่ให้ผู้ประสงค์ดี บุกรุกหรือโจมตีเข้ามาในระบบเครือข่ายขององค์กรโดยรวม โดยใช้เครื่องมือต่างๆ เช่น ระบบรักษาความมั่นคงปลอดภัย ระบบตรวจสอบผู้บุกรุก

ทำไมต้องคำนึงถึงความมั่นคงปลอดภัยของระบบเครือข่าย ?

เนื่อง จากการพัฒนาทางเทคโนโลยีและการสื่อสารที่มีอยู่อย่างต่อเนื่อง รวมถึงการเพิ่มขึ้นของช่องทางในการติดต่อสื่อสารระหว่างกันภายในเครือข่าย ทำให้เกิดความรวดเร็ว มีประสิทธิภาพ และสามารถติดต่อสื่อสารกันได้สะดวกขึ้น ตลอดจนมีระบบการให้บริการเทคโนโลยีใหม่ๆ บนระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ตจำนวนมาก จำนวนผู้ใช้บริการทางเครือข่ายอินเทอร์เน็ตจึงมีจำนวนเพิ่มมากขึ้นด้วย ซึ่งผู้บุกรุกก็อาศัยสิ่งเหล่านี้มาใช้ในการบุกรุกและโจมตีระบบมากขึ้นเช่น กัน ส่งผลทำให้ภัยคุกคามและการบุกรุกต่างๆ ทางคอมพิวเตอร์ก็มีหลากหลาย และมีแนวโน้มเพิ่มสูงขึ้นมากในปัจจุบัน และส่งผลกระทบต่อความปลอดภัยของระบบเครือข่าย (Network) ด้วยเหตุนี้ จึงมีความจำเป็นอย่างยิ่งที่แต่ละองค์กรจะต้องมีเครื่องมือที่ทำหน้าที่ป้องกันความเสี่ยงอันอาจจะเกิดกับระบบเครือข่าย (Network) ขององค์กร นั่นคือ ระบบรักษาความมั่นคงปลอดภัย (Firewall) ซึ่งเป็นอีกหนึ่งเครื่องมือที่ทำหน้าที่ป้องกันการบุกรุกโจมตีระบบเครือข่าย ทั้งจากเครือข่ายภายใน (Intranet) และเครือข่ายภายนอก (Internet) จากผู้ไม่ประสงค์ดีที่ไม่ได้รับอนุญาต

รู้จักกับระบบรักษาความมั่นคงปลอดภัย (Firewall)

Firewall เป็นเครื่องมือที่ใช้สำหรับป้องกันระบบเครือข่าย (Network) จาก การสื่อสารทั่วไปที่อาจจะถูกบุกรุกหรือโจมตี จากผู้ที่ไม่ได้รับอนุญาต กล่าวคือเป็นเรื่องที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในระบบเครือ ข่ายขององค์กร (Network) ซึ่งการป้องกันโดยการใช้ระบบ Firewall นี้ จะเป็นการกำหนดกฎเกณฑ์ เพื่อควบคุมการเข้า – ออก หรือเป็นการควบคุมการรับและส่งข้อมูลภายในระบบเครือข่าย



คุณสมบัติของระบบรักษาความมั่นคงปลอดภัย (Firewall)

Protect Firewall เป็นเครื่องมือที่ใช้ในการป้องกันระบบคอมพิวเตอร์ โดยภายในระบบเครือข่ายคอมพิวเตอร์จะมีการรับและส่งข้อมูลภายในระบบเครือข่าย (Package : ข้อมูลที่มีการรับส่งภายในหรือภายนอกระบบเครือข่าย) ซึ่งจะถูกกำหนดเป็นกฎเกณฑ์ เพื่อใช้บังคับในการสื่อสารภายในระบบเครือข่าย

Rule Base คือข้อกำหนดในการควบคุมการรับและส่งข้อมูลภายในระบบเครือข่าย ซึ่งระบบรักษาความมั่นคงปลอดภัย (Firewall) จะต้องมีการกำหนดกฎเกณฑ์ สำหรับควบคุมการทำงานในระบบเครือข่าย

Access Control หมายถึงการควบคุมระดับการเข้าถึงการรับและส่งข้อมูลภายในระบบเครือข่าย

ประเภทของระบบรักษาความมั่นคงปลอดภัย (Firewall)

Firewall สามารถแบ่งออกได้เป็นหลายประเภทโดยขึ้นอยู่กับเกณฑ์ที่ใช้ตัดสิน เช่น ถ้าพิจารณาตามรูปแบบการไหลของข้อมูลผ่านระบบรักษาความมั่นคงปลอดภัย (Firewall) สามารถแบ่งออกได้เป็น 2 ประเภทคือ

- Network Based Firewall เป็นอุปกรณ์ติดตั้งในระบบเครือข่ายเพื่อคัดกรองปริมาณการใช้งาน ของระบบเครือข่าย (Traffic)

- Host Based Firewall เป็นซอฟต์แวร์ติดตั้งที่เครื่องคอมพิวเตอร์เพื่อคัดกรองปริมาณการใช้งาน ของระบบเครือข่าย (Traffic) ที่เข้าสู่เครื่องก่อนที่จะนำข้อมูลไปประมวลผล

นอกจากนี้ยังสามารถแบ่งประเภทของ Firewall ตามลักษณะการทำงานของ Firewall ออกได้เป็น 3 ประเภท ได้แก่

1. Network Level Firewall หรือ Packet Filtering Firewall

Packet Filter ทำงานโดยทำการหาเส้นทางและส่งต่ออย่างมีเงื่อนไข (Screening Router) โดยจะพิจารณาจากข้อมูลส่วนที่อยู่ในเฮดเดอร์ (header) ของแพ็กเก็ตที่ผ่านเข้ามา เทียบกับกฎ (Rules) ที่กำหนดไว้ และตัดสินว่าควรจะทิ้ง (drop) แพ็กเก็ตนั้นไปหรือว่าจะยอม (accept) ให้แพ็กเก็ตนั้นผ่านไปได้

2. Stateful Inspection Firewall

Stateful Inspection Firewall มีหลักการทำงานทุกอย่างเหมือนกับ Packet Filtering Firewall แต่มีส่วนที่เพิ่มเข้ามาคือ จะบันทึกข้อมูลเกี่ยวกับคอนเน็กชั่นที่เกิดขึ้นลงใน State Table ก่อนที่จะส่งแพ็กเก็ตนี้ต่อให้กับเลเยอร์อื่น

3. Application Layer Firewall

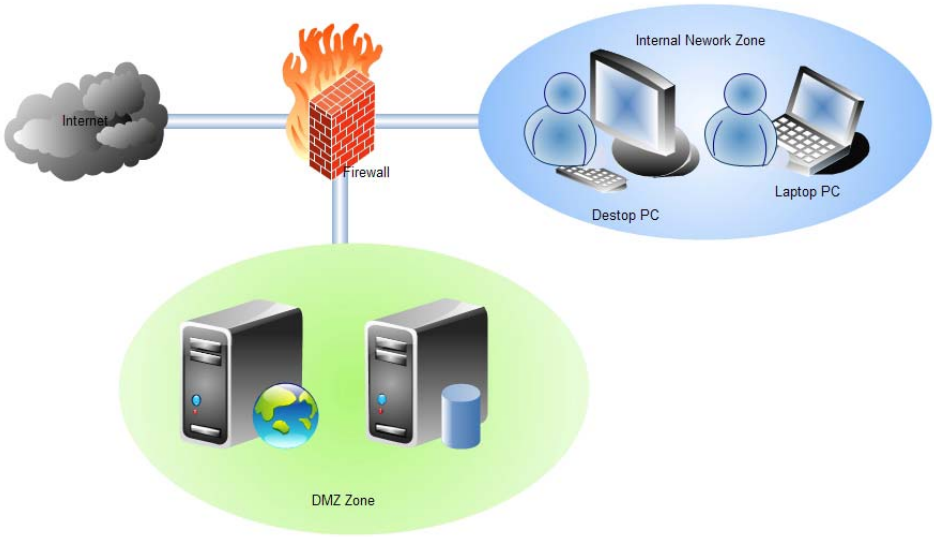
Firewall ที่ทำงานในระดับ Application Layer บางทีก็เรียกว่า Proxy Firewall ซึ่งหมายถึงโปรแกรมที่ทำงานบนระบบปฏิบัติการทั่วๆ ไป โดยการทำงานจะเริ่มจากเครื่องลูกข่าย (Client) ส่ง การร้องขอไปยังอุปกรณ์ไฟร์วอลล์ หลังจากนั้นอุปกรณ์ไฟร์วอลล์ จะดำเนินการตรวจสอบจากนโยบายการรักษาความปลอดภัยว่าข้อมูลปริมาณการใช้งาน (Traffic) นี้ สามารถผ่านไปได้หรือไม่ ซึ่งหากข้อมูลปริมาณการใช้งานดังกล่าวเป็นไปตามกฎที่กำหนดขึ้น (Rules) หรือได้รับอนุญาตจากระบบ อุปกรณ์ไฟร์วอลล์จะสร้างการเชื่อมต่อกับเซิร์ฟเวอร์แทนเครื่องคอมพิวเตอร์ลูกข่าย (Client) เอง

นโยบายการรักษาความปลอดภัยของระบบเครือข่าย (Network Security Policy)

นโยบายการรักษาความปลอดภัยของระบบเครือข่าย นับเป็นสิ่งที่สำคัญที่สุดสำหรับการใช้งานระบบ Firewall เพราะถึงแม้ว่าระบบ Firewall จะมีประสิทธิภาพเพียงใด หากมีนโยบายการรักษาความปลอดภัยที่หละหลวม ระบบ Firewall ก็ไม่มีประโยชน์มากนัก ดังนั้น จึงควรกำหนดนโยบายที่สามารถควบคุม หรือป้องกันปริมาณการใช้งานบนระบบเครือข่าย (Traffic) ที่อาจมีผลกระทบต่อการใช้งานระบบเครือข่ายให้มากที่สุด หลังจากนั้นจึงนำไปบังคับใช้กับระบบ Firewall ซึ่งกฎที่บังคับใช้นโยบายการรักษาความปลอดภัยในระบบ Firewall นั้นจะเรียกว่า ACL (Access Control List) หรือ Firewall Rule

ระบบเครือข่ายคอมพิวเตอร์โดยพื้นฐานแล้ว จะแบ่งเขตหรือที่เรียกว่า โซน (Zone) ออกเป็น 3 โซน ได้แก่ เขตแรกหรือโซนแรก คือโซนอินเทอร์เน็ต (Internet) ซึ่งเป็นเขตที่มีความไม่น่าเชื่อถือ เนื่องจากเป็นส่วนที่อยู่หน้าอุปกรณ์ไฟร์วอลล์ เขตที่สอง คือ อินทราเน็ต (Intranet) ซึ่ง ถือเป็นเขตที่มีความปลอดภัย เนื่องจากเป็นเขตที่อยู่ด้านหลังไฟร์วอลล์ กล่าวได้ว่าเป็นเขตที่ติดตั้งเครื่องคอมพิวเตอร์ของผู้ใช้งานภายในองค์กร และเขตที่สาม คือ โซน DMZ (Demilitarized Zone) เป็นเขตที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) ที่ให้บริการระบบงานต่างๆ แก่ผู้ใช้งานทั่วไป

ในอุปกรณ์ไฟร์วอลล์จะมีการกำหนดกฎและระเบียบมาบังคับใช้ ซึ่งกฎเหล่านี้อาจจะเรียกว่า “นโยบายด้านความปลอดภัย (Policy)” โดยหลักการทำงานของอุปกรณ์ไฟร์วอลล์จะประกอบไปด้วยกลไก 2 ส่วน คือส่วนแรกจะทำหน้าที่ให้การสกัดกั้นปริมาณการใช้งานที่เกิดขึ้นบนเครือข่าย (Traffic) และส่วนที่สองจะทำหน้าที่ในการปล่อยปริมาณการใช้งานที่เกิดขึ้นให้ผ่านไป



ข้อจำกัดของระบบรักษาความมั่นคงปลอดภัย (Firewall)

- Firewall ไม่สามารถป้องกันการโจมตีที่ไม่ได้กระทำผ่าน Firewall เช่น การโจมตีจากภายในเครือข่ายเอง
- ไม่สามารถป้องกันการโจมตีที่มากับ Application Protocols ต่างๆ ที่เรียกว่าการ Tunneling หรือกับโปรแกรม client ที่มีความล่อแหลมและถูกดัดแปลงให้กระทำการโจมตีได้ (โปรแกรมที่ถูกทำให้เป็น Trojan horse)
- ไม่สามารถป้องกันไวรัส (Virus) ได้อย่างมีประสิทธิภาพ เนื่องจากจำนวนไวรัสที่มีอยู่มากมาย จึงเป็นการยากมากที่ Firewall จะสามารถตรวจจับ pattern ของไวรัสทั้งหมดได้

ระบบจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log file)

เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 26 ผู้ให้บริการเครือ ข่ายคอมพิวเตอร์ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้า สิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ซึ่งผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้ระบุตัวผู้ใช้บริการได้ นอกจากนี้กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารได้ออกประกาศ เมื่อวันที่ 21 สิงหาคม 2550 ว่าด้วยเรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้บริการ พ.ศ. 2550 เพื่อให้รายละเอียดเกี่ยวกับชนิดและรูปแบบของข้อมูลคอมพิวเตอร์ที่จัดเก็บของแต่ละประเภทผู้ให้บริการ ตลอดจนมีผลบังคับใช้ต่อหน่วยงานต่างๆ ทั้งภาครัฐและภาคเอกชน ซึ่งทุกหน่วยงานจะต้องปฏิบัติตามข้อกำหนดต่างๆ เพื่อให้มีข้อมูลจราจรทางคอมพิวเตอร์ใช้เป็นหลักฐานในการลงโทษ หากพบว่ามีผู้กระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์เกิดขึ้น

กรมการ พัฒนาชุมชน ถือเป็นหน่วยงานหนึ่งที่ให้บริการแก่ผู้ใช้บริการ คือ ข้าราชการและเจ้าหน้าที่ของรัฐในการเข้าสู่เครือข่ายอินเทอร์เน็ตและให้สามารถติดต่อสื่อสารผ่านระบบเครือ ข่ายคอมพิวเตอร์และอินเทอร์เน็ต ดังนั้น กรมการพัฒนาชุมชน ตลอดจนหน่วยงานภายในสังกัด จึงมีฐานะเป็นผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ซึ่งมีหน้าที่และความรับผิดในทางกฎหมายตามพระราชบัญญัติว่าด้วยการกระทำความ ผิดเกี่ยวกับ

คอมพิวเตอร์ พ.ศ. 2550 จึงมีความจำเป็น อย่างยิ่งที่กรมฯ และหน่วยงานภายในสังกัดต้องพัฒนาระบบเครือข่ายคอมพิวเตอร์ เพื่อให้มีเครื่องมือในการระบุตัวผู้ใช้บริการ และเครื่องมือในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ให้เป็นไปตามบทบัญญัติ ของกฎหมาย อีกทั้งข้าราชการและเจ้าหน้าที่ของรัฐที่ปฏิบัติงานภายในสังกัดกรมการพัฒนา ชุมชน จะต้องตระหนักถึงความสำคัญของการใช้งานระบบเครือข่ายคอมพิวเตอร์และอินเทอร์เน็ต

แนวทางปฏิบัติการเก็บข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลผู้ใช้บริการ

ปัจจุบัน เป็นที่ทราบกันดีว่าการติดต่อสื่อสารผ่านระบบเครือข่ายคอมพิวเตอร์และอิน เทอร์เน็ตมีบทบาทสำคัญต่อการดำเนินชีวิตประจำวันของคนเราเป็นอย่างมาก อย่างไรก็ดี ปัญหาการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ก็มีแนวโน้มขยายวงกว้างและรุนแรง ตามไปด้วย ข้อมูลจราจรทางคอมพิวเตอร์จึงเป็นพยานหลักฐานที่สำคัญในการดำเนินคดี อันเป็นประโยชน์ต่อการสืบสวน สอบสวน เพื่อนำตัวผู้กระทำความผิดมาลงโทษ จึงสมควรกำหนดให้ผู้ให้บริการมีหน้าที่ในการเก็บรักษาข้อมูลจราจรทาง คอมพิวเตอร์ ด้วยเหตุนี้ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร จึงได้ออกประกาศกระทรวงฯ สำหรับหลักเกณฑ์ในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ดังกล่าว เพื่อให้เกิดความเหมาะสมในทางปฏิบัติและเพื่อให้หลายองค์กรได้มีแนวทางที่ชัดเจนในการปฏิบัติว่าข้อมูลจราจรอะไรบ้างที่ควรจัดเก็บ ข้อมูลอะไรที่ไม่ต้องจัดเก็บ ตลอดจนวิธีการจัดเก็บอย่างถูกต้องตรงตามลักษณะการใช้ระบบสารสนเทศหรือระบบ อินเตอร์เน็ตของแต่ละองค์กร เช่น การจัดเก็บในลักษณะ “Centralized Log” เป็นต้น

“หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ของผู้ให้บริการ พ.ศ. 2550” มี วัตถุประสงค์ที่แท้จริง คือเมื่อเกิดอาชญากรรมทางคอมพิวเตอร์ หลักฐานต่างๆ ทางคอมพิวเตอร์จัดว่ามีความน่าเชื่อถือค่อนข้างน้อย และมีโอกาสที่จะไม่พบร่องรอยของการก่ออาชญากรรม ทำให้หลายครั้งเมื่อตำรวจหรือพนักงานเจ้าหน้าที่ได้เข้าไปขอข้อมูลจราจรทาง คอมพิวเตอร์จากผู้ให้บริการ ยกตัวอย่างเช่น ISPพบว่า ISP ไม่ ได้เก็บข้อมูลจราจรดังกล่าว หรือ เก็บไว้ไม่นานเพียงพอเนื่องจากมีพื้นที่จัดเก็บค่อนข้างจำกัด ทำให้การพิสูจน์หลักฐานทางคอมพิวเตอร์ทำได้ยากลำบาก หรือไม่สามารถทำได้เนื่องจากข้อมูลไม่เพียงพอ ดังนั้นในพระราชบัญญัติฯ จึงจำเป็นที่จะต้องกำหนดระยะเวลาในการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ไว้ อย่างชัดเจน โดยให้ถือว่าเป็นความรับผิดชอบต่อสังคมที่องค์กรทุกองค์กรต้องปฏิบัติและให้ ความร่วมมือ เมื่อมีการขอเรียกดูข้อมูลดังกล่าวโดยพนักงานเจ้าหน้าที่หลังจากมีอาชญากรรม เกิดขึ้น

ประเภทข้อมูลที่ต้องเก็บรักษา

1. ข้อมูลจราจรคอมพิวเตอร์ที่เกิดจากการเข้าถึงระบบเครือข่าย
2. ข้อมูลจราจรคอมพิวเตอร์บนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์
3. ข้อมูลจราจรคอมพิวเตอร์จากการโอนแฟ้มข้อมูลบนเครื่องให้บริการโอนแฟ้มข้อมูล
4. ข้อมูลจราจรคอมพิวเตอร์บนเครื่องผู้ให้บริการเว็บ

5. ข้อมูลจราจรคอมพิวเตอร์ของเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (USENET)

6. ข้อมูลจราจรคอมพิวเตอร์ที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต

วิธีการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์

ต้องมีการจัดเก็บรักษาข้อมูลจราจรโดยการใช้วิธีการที่มั่นคงและปลอดภัย คือ

1. มีการเก็บบันทึกในสื่อที่สามารถรักษาความครบถ้วน

2. มีระบบเก็บรักษาความลับและชั้นความลับของข้อมูลที่เก็บรักษาไว้ เพื่อผู้จัดเก็บไม่อาจแก้ไขเปลี่ยนแปลงได้

3. กำหนดให้ผู้บริการจะต้องตั้งตัวแทนขึ้นมาประสาน และให้ข้อมูลได้อย่างรวดเร็วแก่เจ้าหน้าที่ที่ได้รับแต่งตั้งตามพระราชบัญญัติฯ

4. ให้มีการระบุตัวตนของผู้ใช้บริการ

- ระบุตัวบุคคลที่เข้าถึงสื่อนั้นๆ เป็นรายบุคคลได้จริงโดยไม่ให้มีการใช้ชื่อบริการร่วมกัน
- ระบุลักษณะของการใช้บริการได้ (proxy server, Network Address Translation, proxy cache, proxy engine)

5. ใน กรณีตาม 1-4 ที่ผู้ให้บริการใช้ระบบของผู้ให้บริการบุคคลที่สาม ทำให้ไม่ทราบว่าผู้ใช้บริการป็นใคร ต้องจัดวิธีการให้ผู้เข้ามาใช้ ต้องระบุและยืนยันตัวตน

เอกสารอ้างอิง

http://linux.thai.net/~ott/books/linuxbook1/BuildInternetServerUsingLinux-Pattara.pdf

http://file.snru.ac.th/download.aspx?NFILE=TEACHER_398_16062012151612298.pdf

http://122.154.237.2/mhsict/images/file/media/media2.pdf

http://www.stou.ac.th/Website/Subbj/fileUpload/99412-12-1.pdf

http://sci.feu.ac.th/boonrit/security/ch8%20เทคโนโลยีและเครื่องมือรักษาความมั่นคงปลอดภัย (Firewall).pdf

http://dmsc2.dmsc.moph.go.th/itc/files/Firewall.pdf

https://www.acisonline.net/article_prinya_eleader_0950.htm

http://www.servertoday.com/docs/Computer_Crimes_Act_B.E._2550_Thai.pdf

http://mail.mof.go.th/SkinFiles/mof.go.th/MOF/46_1_Traffic%20Data.pdf

http://www.msit.mut.ac.th/newweb/phpfile/Thesis/Thesis_2555/086%20ระบบการจัดเก็บข้อมูลจราจรคอมพิวเตอร์.pdf

ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน กรมการพัฒนาชุมชน กระทรวงมหาดไทย

ศูนย์ราชการเฉลิมพระเกียรติฯ อาคารรัฐประศาสนภักดี (อาคาร B) ชั้น ๕

ถนนแจ้งวัฒนะ หลักสี่ กทม ๑๐๒๑๐

โทรศัพท์ ๐-๑๔๑-๖๒๖๓ – ๓๐๕

www.itcenter.cdd.go.th