ข้อกำหนดการบริหารจัดการระบบป้องกันการบุกรุกทางเครือข่าย (Firewall)

สำนักหอสมุด มหาวิทยาลัยเกษตรศาสตร์

---

1. ต้องดำเนินการจัดแบ่งเครือข่ายภายใน (Internal Zone) เครือข่ายที่อนุญาตให้เข้าถึงได้ (DMC Zone) และเครือข่ายสาธารณะ (Public Zone) ออกจากกัน โดยมีอุปกรณ์ป้องกันการบุกรุกทางเครือข่าย (Firewall) กั้น DMZ Zone ออกจาก Internal Zone และ External Zone
2. การเข้าถึงระบบสารสนเทศจากเครือข่ายสาธารณะ จะต้องทำผ่านอุปกรณ์ป้องกันการบุกรุกทางเครือข่าย (Firewall) เพื่อป้องกันการเข้าถึงระบบสารสนเทศจากผู้ไม่ได้รับอนุญาต โดยกำหนดให้ผู้ดูแลระบบเป็นผู้ดำเนินการในการกำหนดนโยบาย (Policy) เข้าออก
3. การอนุญาตเปิด Service Port ของ Firewall ให้เข้าถึงระบบสารสนเทศได้จากเครือข่ายสาธารณะนั้น ให้พิจารณาเปิดเท่าที่จำเป็นเท่านั้น โดยพอร์ต (Port) ที่มีความเสี่ยงไม่ควรเข้าถึงได้จากเครือข่ายสาธารณะ และควรจำกัดการเข้าถึงด้วย IP Address ที่ได้รับอนุญาตเท่านั้น
4. จะต้องพิจารณาปิดพอร์ตที่ไม่จำเป็น ไม่ปลอดภัย หรือพอร์ตที่มีช่องโหว่ ทั้งหมดไม่ให้สามารถเข้าถึงได้จากเครือข่ายสาธารณะเพื่อลดความเสี่ยงต่อการถูกโจมตี
5. ไม่ควรเปิดให้มีช่องทางในการเข้าถึงฐานข้อมูลที่สำคัญจากเครือข่ายสาธารณะ หากมีความจำเป็นควรให้เข้าถึงโดยใช้ VPN (Virtual Private Network)
6. หากตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อและแก้ไขปัญหาที่เครื่องหรืออุปกรณ์นั้นๆ ทันที
7. ติดตามและตรวจสอบรายงานภัยคุกคามกับแหล่งข้อมูลที่มีความน่าเชื่อถือ เช่น CVE (Common Vulnerabilities and Exposures) และพิจารณาปรับปรุงตามคำแนะนำเพื่อป้องกันการโจมตี
8. ระบบป้องกันการบุกรุกทางเครือข่าย (Firewall) จะต้องได้รับการบำรุงรักษาเชิงป้องกันอย่างต่อเนื่องทุกปี โดยมีการอัพเดต Virus Signature และ IDS/IPS ให้เป็นปัจจุบัน
9. ต้องกำหนดให้มีการบันทึกข้อมูลจราจร (Traffic logs) อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง
10. ผู้ดูแลระบบจะต้องดำเนินการ
    - 10.1 ตรวจสอบสถานะการทำงานของระบบป้องกันการบุกรุกทางเครือข่าย (Firewall) ข้อมูลจราจร (Traffic logs) รายงานภัยคุกคาม (Threat logs) เป็นประจำทุกวันอย่างสม่ำเสมอ
    - 10.2 ทำการสำรองข้อมูลค่าการทำงาน (Configuration Log) ทุกครั้งก่อนแก้ไขหรือสร้าง Policy ใหม่
    - 10.3 ต้องตรวจสอบการใช้งานตาม Policy และทำการปิด Port หรือยกเลิก Service ที่ไม่มีการใช้งานแล้วอยู่เสมอ