เครื่องมือรักษาความปลอดภัยซอฟต์แวร์ by TaskS

ระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ที่จากการถูกโจมตีจากผู้ไม่หวังดีทั้งหลาย หรือการสื่อสารที่ไม่ได้รับอนุญาต ซึ่งส่วนใหญ่จะมาจากระบบเครือข่ายอินเทอร์เน็ต รวมถึงเครือข่าย LAN ด้วย ซึ่งในปัจจุบัน มีทั้งรูปแบบ Hardware และ Software ในที่นี้จะกล่าวถึง Software

ที่มา: https://www.safetydetectives.com/wp-content/uploads/2019/02/Firewall-uses-800x600.jpg.webp

ระบบซอฟต์แวร์ ที่ต้องรู้จัก ได้แก่

1. Firewall คือเครื่องมือที่ใช้ในการป้องกันเน็ตเวิร์กจากการสื่อสารทั่วไปที่ไม่ได้รับอนุญาต โดยที่เครื่องมือที่ว่านี้อาจจะเป็น Hardware หรือ Software หรือทั้งสองรวมกันขึ้นอยู่กับวิธีการหรือ Firewall Architecture ที่ใช้ เปรียบเสมือนการที่เราสร้างกำแพงให้กับเครื่องคอมพิวเตอร์ตรวจสอบการเชื่อมต่อต่าง ๆ ให้เป็นไปตามกฎ ซึ่ง Firewall จะเป็นตัวกรองข้อมูลว่า ข้อมูลชนิดนี้คือ ใคร (Source) จะไปที่ไหน (Destination) และข้อมูลชนิดนี้จะให้ให้หรือทำอะไร (Service/Port) ถ้าข้อมูลที่ได้รับนั้นไม่ปลอดภัย Firewall จะไม่ยอมให้ข้อมูลนั้นเข้าไปได้

คุณสมบัติทั่วไปของ Firewall นั้นจะมีอยู่ 3 อย่างด้วยกันคือ

1) Protect **เป็นการป้องกัน packet ที่จะสามารถผ่านเข้า-ออกได้นั้น จะต้องเป็น packet ที่มันเห็นว่าปลอดภัย หาก packet ใดที่เห็นว่าไม่ปลอดภัย ก็จะไม่อนุญาตให้ผ่าน โดยการตัดสินว่า packet ปลอดภัยหรือไม่นั้นขึ้นอยู่กับกฎพื้นฐานที่ Administrator ได้กำหนดไว้**

2) Access Control **เป็นการควบคุมการ Access ของ Host ต่างๆ ให้เป็นไปตามกฎพื้นฐานที่ Administrator ได้กำหนดไว้**

3) Rule Base **เป็นการควบคุมการ Access โดยอาศัยการเปรียบเทียบคุณสมบัติของ Packet ที่จะผ่านเข้า-ออก กับกฎพื้นฐานที่ Administrator ได้กำหนดไว้ หากพบว่าไม่มีกฎห้ามไว้ก็จะอนุญาตให้ผ่านไปได้ แต่ถ้ามีกฎข้อใดข้อหนึ่งห้ามมันก็จะไม่ยอมให้ผ่าน**

ความสามารถที่ Firewall ที่ป้องกันได้

1) Network Scanning – ด้วยคุณสมบัติที่ Firewall สามารถควบคุมการเข้า-ออก ของ packet ได้ มันจึงสามารถจำกัดปลายทางของ packet ที่ผ่านเข้ามาเฉพาะ Host ที่ได้รับอนุญาตให้ติดต่อได้เท่านั้น

2) Network Denial of Service – ป้องกันการก่อกวนเพื่อไม่ให้ Host สามารถให้บริการได้ เช่นการทำให้เน็ตเวิร์กท่วมไปด้วยข้อมูล (Network Flooding) ทำการส่ง packet จำนวนมากไปยัง Host เพื่อขอใช้บริการ (SYN Flooding)

3) Host Scanning – Firewall จะทำการตรวจจับการ scan เพื่อหาว่ามีการรัน Service อะไรบ้างบน host

4) Inbound Access - ควบคุมการเข้ามาของ packet เฉพาะที่ได้รับอนุญาตตาม Rule Base

5) Outbound Access - ควบคุมการออกไปของ packet เฉพาะที่ได้รับอนุญาตตาม Rule Base

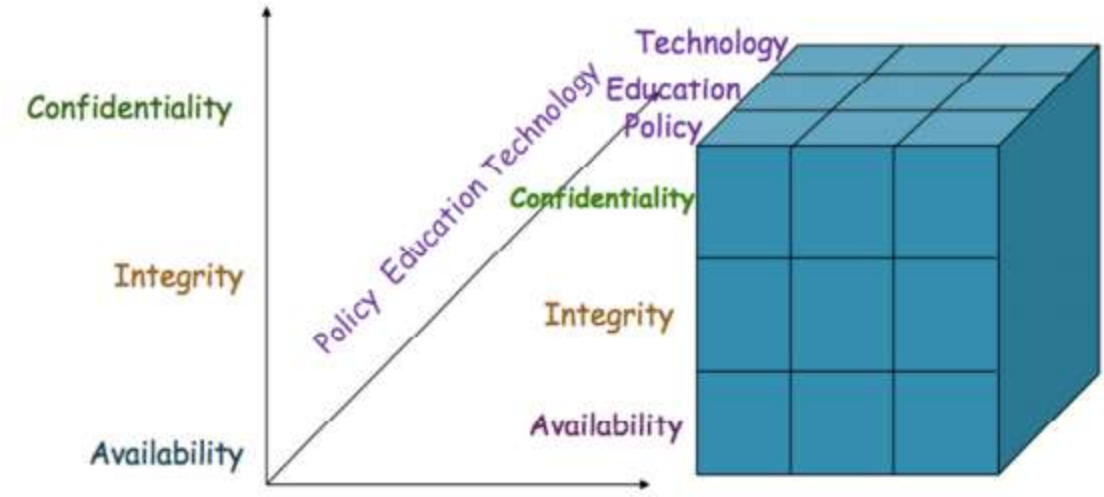
6) Trojan Horse, Backdoor, Back Orifice, Hijacking - การลักลอบเก็บหรือส่งข้อมูล

ตัวอย่างโปรแกรมซอฟต์แวร์ Firewall

- Windows Firewall
- ZoneAlarm
- Tiny Personal Firewall
- Sygate Personal Firewall (ปัจจุบันได้ถูกบริษัท Symantec นำไปพัฒนาต่อ)
- Filseclab Personal Firewall
- Comodo Firewall Pro
- Pc Tools Firewall Plus
- Agitum Outpost Firewall
- Ashampoo Firewall

- Lavasoft Personal Firewall
- Sunbelt Personal Firewall
- Webroot Desktop Firewall
- Sunbelt Kerio Personal Firewall
- Jetico Personal Firewall
- SoftPerfect Personal Firewall
- Dynamic Security Agent
- Ghostwall Firewall
- R-Firewall

2. องค์ประกอบของความมั่นคงปลอดภัยของข้อมูล NSTISSC (Nation Security Telecommunications and Information Systems Security) หรือคณะกรรมการด้านความมั่นคงด้านโทรคมนาคมและระบบสารสนเทศแห่งชาติของสหรัฐอเมริกา ได้กำหนดแนวคิดความมั่นคงปลอดภัยขึ้นมา ต่อมาได้กลายเป็นมาตรฐานการประเมินความมั่นคงของระบบสารสนเทศที่ได้รับการยอมรับ



ที่มา: https://dd4e0555-a-62cb3a1a-s-sites.googlegroups.com/site/ges0503chiwitkabthekhnoloyi/bth-thi-5-khwam-mankhng-plxdphay-khxng-rabb-sarsnthes/4-xngkh-prakxb-khxng-khwam-mankhng-plxdphay-khxng-khxmul/capture-20170403-033859.png?attachauth=ANoY7co7m-ONZTzM3Wweedfnabg49_5W5l3ejOyy5PO2KE_0nSXjRHLSt019fYtnVMkgEYklHOiLySZOL1aAidROEiTMibwCLx4rvfLkH2j7XeoaZOnOAI56qOCNLQnpBoVN2g5DbGhXfPUwlOCkwu_kUBXWuYNyvYD1x7mur0oR8rFv_GadEPRlcjbcZ1zibW2Wb0cGuWIrCgTKWVqGAG0lP7qKXe-_x1L-Dup2VoJAeq523GcMFTgY-iTAs4-CdEjUh5EqB98jOmggFjXUhKl65esA0YEEa7WdV8xQQnmQXW3jKwKfAAZy0bSnnx4gnk-OHQ7ktd99FXcfz7MoHNj4kGOFQP_IMfVVlZvLOyCc0lYSoQWC1ydN4EguQmMTFJzcqU3sVBwFF0755ZosesKW6tfteXSbJQ%3D%3D&attredirects=0

สิ่งที่สำคัญต้องกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศและต้องมีหลักดังนี้

1) ความลับ (Confidentiality) คือ การรักษาความลับเป็นการรับประกันว่าผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ ได้แก่ Login/Password

2) ความคงสภาพ (Integrity) คือ ความครบถ้วน ถูกต้อง และไม่มีสิ่งแปลก ประกอบด้วย 2 ส่วน คือ การป้องกัน (Prevention) และการตรวจสอบ (Detection)

2.1) การป้องกัน (Prevention) การเปลี่ยนแปลงแก้ไขข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต รวมถึงป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลนอกเหนือขอบเขตของผู้ได้รับอนุญาต ซึ่งอาจใช้การพิสูจน์ตัวตน (Authentication) และการควบคุมการเข้าถึง (Access Control) ในประเด็นแรก และใช้การตรวจสอบสิทธิ์ (Authorization) ในประเด็นหลัง

2.2) การตรวจสอบ (Detection) เพื่อดูว่าข้อมูลยังคงมีความน่าเชื่อถือได้อยู่หรือไม่ ซึ่งสามารถตรวจเช็ควิเคราะห์เหตุการณ์ต่างๆ ที่เกิดขึ้นจาก Log File

3) ความพร้อมใช้ (Availability) คือ ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ จัดเป็นส่วนหนึ่งของความมั่นคง ความน่าเชื่อถือ (Reliability) ของระบบ ได้แก่ การทำระบบสำรอง (Backup System)