การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

ประกิต พรหมดี prakit@pfengineering.com

(MCSE Security , MCT , CCNA)

P.F Engineering & Services Co., Ltd.

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

Information Security System

P.F Engineering & Services Co., Ltd.

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

วัตถุประสงค์ : เพื่อให้เข้าใจและตระหนักถึง
ความสำคัญของระบบการรักษาความปลอดภัย

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ระบบสารสนเทศ

Information System

Information Security Risk

ระบบสารสนเทศประกอบด้วย 5 องค์ประกอบ คือ

1. Hardware – อุปกรณ์
2. Software – โปรแกรมประยุกต์, ระบบ, OS, DB, Application
3. Data – ข้อมูลดิบ, Information, Knowledge
4. People (User) – คน (Personnel)
5. Business Process (Process, Procedure)

Information Security Risk

องค์ประกอบของความมั่นคงปลอดภัยของสารสนเทศ

1. ความลับ (Confidentiality)
   เฉพาะผู้มีสิทธิ์หรือได้รับอนุญาตเท่านั้น
2. ความถูกต้องสมบูรณ์ (Integrity)
   ต้องมีกลไกในการตรวจสอบสิทธิ์
3. ความพร้อมใช้งาน (Availability)
   ผู้ใช้งานที่มีสิทธิ์เข้าถึงระบบได้เมื่อต้องการ

Information Security Risk

สิ่งที่ต้องคำนึงถึง

ในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ คือ

1. ระบบรักษาความมั่นคงปลอดภัยต้องป้องกันสม่ำเสมอ
2. ระบบรักษาความมั่นคงปลอดภัยต้องป้องกันตามมูลค่า
3. ไม่มีระบบที่สมบูรณ์แบบ ไม่มีระบบที่ใช้ได้ตลอดไป
4. เป็นกระบวนการที่ต้องทำต่อเนื่องตลอดไป
5. การเข้ามาโจมตีระบบสารสนเทศ จะเลือกเข้ามาในทิศทางที่คุณคาดไม่ถึงเสมอ

Information Security Risk

การปรับปรุงให้ดียิ่งขึ้น ให้ทันต่อภัยคุกคาม โดยใช้ PDCA

P (Plan) คือ การวางแผน

D (Do) คือ ดำเนินการตามแผน

C (Check) คือ ตรวจสอบสอบทานการดำเนินงานตามแผน

A (Act) คือ เมื่อพบข้อผิดพลาดต้องหาแนวทางในการดำเนินการแก้ไข

Information Security Risk

หลักการของการทำให้ปลอดภัย แบ่งเป็น 3 วิธี คือ

1. **Prevention** – ป้องกัน : เป็นวิธีที่ดีที่สุด
2. **Detection** – ตรวจสอบ : รู้ทันทีที่เกิด ทำให้มีปฏิกิริยาตอบสนองได้เร็ว
3. **Recovery** – แก้ไข : ปล่อยให้เกิดแล้วตามไปแก้ไข

Information Security Risk

ความเสี่ยงระบบสารสนเทศ เกิดจาก

1.ระบบเครือข่าย

2.โปรแกรมไวรัส

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ความเสี่ยงจากระบบเครือข่าย

Network Risk

5 ขั้นตอน เพื่อให้ระบบเครือข่ายของคุณมีความปลอดภัย

1. ปกป้องทรัพย์สินที่มีค่าที่สุดของคุณเป็นสิ่งแรก
2. ปกป้องที่บริเวณรอบๆ
3. การป้องกันระบบภายในที่สำคัญ
4. สร้างเครือข่ายที่ง่ายไม่ซับซ้อน
5. ศึกษาความรู้เรื่องความปลอดภัยอย่างต่อเนื่อง

Network Risk

I. ปกป้องทรัพย์สินที่มีค่าที่สุดของคุณ เป็นสิ่งแรก

1. อะไรคือข้อมูลที่สำคัญที่สุด ?
2. อะไรคืองานแรกที่ต้องบริการ ?
3. ระบบแวดล้อมพื้นฐานเป็นอย่างไร ?
4. ระบบสำรองข้อมูลมีหรือไม่ ?
5. การกู้ข้อมูลเบื้องต้น จะทำอย่างไร ?

Network Risk

อุบัติเหตุ และความเสี่ยง

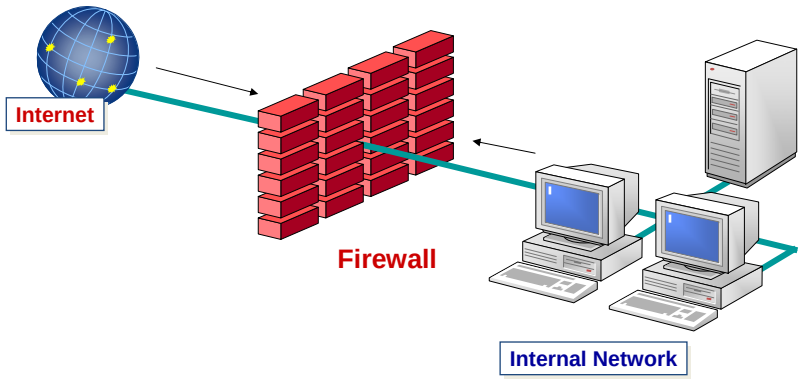
1. ดิสก์ขัดข้อง
2. กระแสไฟฟ้าขัดข้องหรือไม่สม่ำเสมอ
3. การถูกโจรกรรม
4. ไม่ทำการสำรองข้อมูลที่สำคัญ
5. ไม่มีแผ่นบูทเพื่อใช้งานในกรณีที่เครื่องคอมพิวเตอร์เกิดความเสียหายหรือถูกบุกรุก

II. ปกป้องที่บริเวณรอบๆ

Firewall คือ โปรแกรมหรือ **hardware** ที่ได้รับการออกแบบมา เพื่อควบคุมการเข้าออกของโปรแกรมต่างๆ โดยมีพื้นฐานมาจากการอ่านข้อมูลต่างๆที่ไหลผ่านเข้ามาในเครื่องทั้งขาเข้าและขาออก โดยจะนำข้อมูล(packet)ไปเปรียบเทียบกับกฎที่เราได้ตั้งเอาไว้ (rule) และจะทำการตัดสินใจว่าจะทำการปฏิเสธ (deny) หรือว่า อนุญาต (allow)

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์



P.F Engineering & Services Co., Ltd.

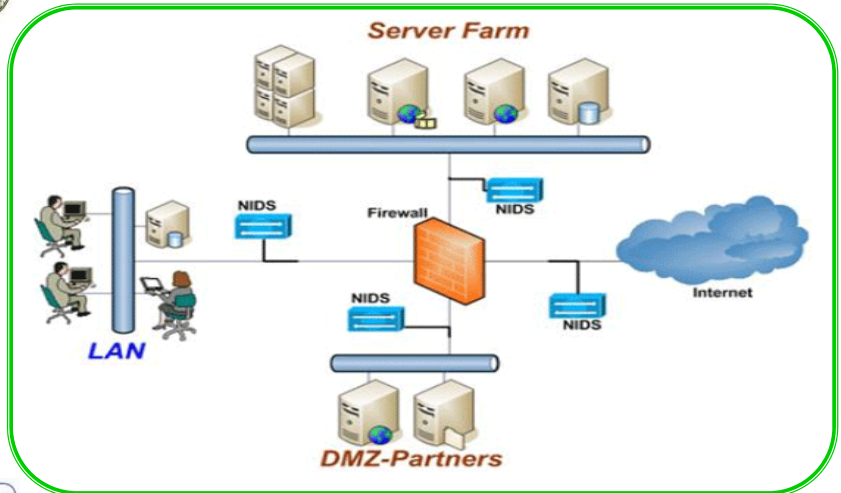
Intrusion detection system (IDS)

ระบบตรวจสอบการบุกรุก

คือ software หรือ hardware ที่ออกแบบมาเพื่อให้ตรวจสอบการเชื่อมต่อที่ไม่พึงประสงค์หรือความพยายามที่จะเข้ามาทำอันตรายต่อเครือข่าย โดยผ่านระบบต่างๆ เช่น Internet, LAN แต่มีข้อจำกัดคือไม่สามารถที่จะตรวจสอบ Packet ที่เข้ารหัสได้

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์



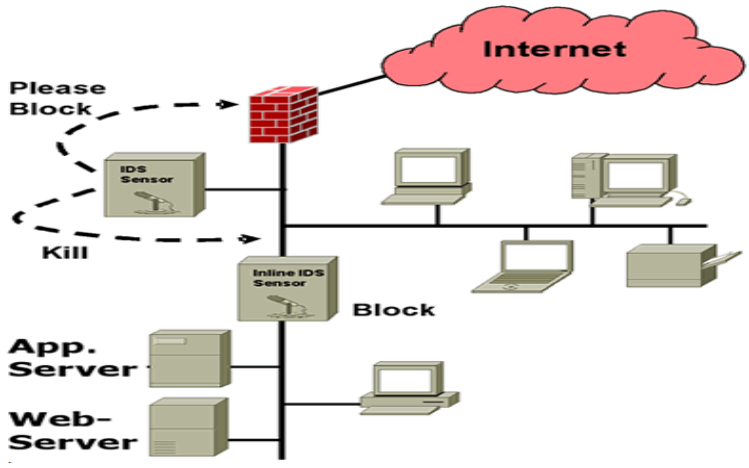
P.F Engineering & Services Co., Ltd.

IPS (Intrusion Prevention System)

ระบบตรวจสอบและตอบโต้การบุกรุก คือ Software หรือ hardware ที่ได้รับการออกแบบมาเพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆกับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ hardware ตัวอื่นๆ

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์



P.F Engineering & Services Co., Ltd.

III. การป้องกันระบบภายในที่สำคัญ

1. Service Packs and hot fixes
2. Hardening your system
   กรรมวิธีลดช่องโหว่ต่างๆ ที่มีขึ้นของระบบ เช่น
   ไม่อนุญาติให้ใช้ Telnet , การ Install Patch ต่างๆ ฯลฯ
3. Auditing ตรวจสอบความมั่นคงของระบบว่าสิ่งที่ปฏิบัติ
   ตรงตามนโยบายที่วางไว้หรือไม่
4. Password and account policies
5. Vulnerability scanners
   ตรวจหาจุดที่มีความอ่อนแอในระบบ

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

IV. สร้างเครือข่ายที่ง่ายไม่ซับซ้อน

ตามหลักการแล้ว ระบบเครือข่ายที่ไม่มีความซับซ้อนจะสามารถจัดการและทำการรักษาความปลอดภัยได้ง่ายกว่าเครือข่ายที่ยุ่งยากซับซ้อน

"ความซับซ้อนเป็นศัตรูที่ร้ายที่สุดของความปลอดภัย" ดังนั้นยิ่งถ้าเครือข่ายของคุณถูกออกแบบให้ง่ายเท่าไหร่ คุณก็จะเข้าใจ และสามารถจัดการ รวมทั้งป้องกันมันได้ดีเท่านั้น

P.F Engineering & Services Co., Ltd.

V. ศึกษาความรู้ เรื่องความปลอดภัย

อย่างต่อเนื่อง

Network Risk
กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

นิยามคำศัพท์ต่างๆเกี่ยวกับเรื่อง hacker

Hacker
คือบุคคลที่มีความรู้ความสามารถเกี่ยวกับ Computer แล้วใช้ความรู้ความสามารถนั้นในด้านที่ดี เช่น หาช่องโหว่ของ Computer แล้วแจ้งแก่ผู้ดูแลระบบ

P.F Engineering & Services Co., Ltd.

นิยามคำศัพท์ต่างๆเกี่ยวกับเรื่อง hacker

Cracker

บุคคลที่มีความรู้ความสามารถเกี่ยวกับ Computer แล้วใช้ความรู้ความสามารถที่มี ไปในทางที่ไม่ดี เช่น เจาะระบบไปแก้ไขข้อมูลผู้อื่น

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

นิยามคำศัพท์ต่างๆเกี่ยวกับเรื่อง hacker

Script-Kiddies

มีความสามารถทางด้านของ Computer เหนือกว่าคนธรรมดาทั่วๆไป แต่ต่ำกว่า Hacker และ Cracker โดยมีจำนวนมากที่สุดในบรรดาผู้ไม่ประสงค์ดีบน Internet

P.F Engineering & Services Co., Ltd.

Network Risk

DoS Attack (Denial of Service)

หมายถึง การขัดขวางหรือก่อกวนระบบเครือข่ายหรือ Server จนทำให้ไม่สามารถให้บริการได้ตามปกติ

โดยการโจมตีจะกระทำโดยการใช้ทรัพยากรของ Server หรือระบบไปจนหมด เช่น การส่ง Packet TCP/SYN เข้าไปหาเครื่องเป้าหมายจำนวนมากขึ้นเรื่อยๆ จนทำให้เครื่องเป้าหมาย เกิดการใช้ทรัพยากรไปจนกระทั่งหมดและยุติการให้บริการในที่สุด

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

Social Engineering Attack

คือ เทคนิคการ Hacking ของ Hackerซึ่งอาศัยช่องโหว่จาก "พฤติกรรมของผู้ใช้" (Human behavior) โดย Hacker จะปลอมตัวเป็นใครหรือ หน่วยงานอะไรสักอย่าง เพื่อ หลอกให้เหยื่อ เปิดเผยข้อมูลซึ่งอาจจะเป็น การสอบถาม Password หรือข้อมูล ที่ สำคัญอะไรบางอย่าง เพื่อการเดาไปสู่ Password หรือข้อมูลสำคัญได้ง่ายขึ้น ซึ่งมีหลายๆ รูปแบบ เช่น Phishing e-mail or Pharming Sites หรือแม้แต่การปลอมเป็นคนที่น่าเชื่อถือโทรศัพท์เข้ามาสอบถามข้อมูลของตัวคุณ

P.F Engineering & Services Co., Ltd.

Network Risk

Phishing

คือ การปลอมแปลง e-mail หรือ web site โดยมีวัตถุประสงค์ ต้องการข้อมูลต่างๆ เช่น User, Password และหมายเลขบัตรเครดิต โดยบริษัทที่ถูกแอบอ้าง ได้แก่ eBay.com, PayPal.com และ Online Banks ต่าง

Phishing มาจากคำว่า Fishing ซึ่งมีการใช้ Ph แทน F กันซึ่งก็เหมือนกับการตกปลาโดยต้องมีการใส่เหยื่อลงไปและรอให้คนมาติดเบ็ดเอง

Network Risk

Insider Attack

เป็นปัญหาที่รุนแรงกว่าการรู้เท่าไม่ถึงการณ์ของการใช้คอมพิวเตอร์ทั่วไป เนื่องจากพนักงานบางคนอาจมีเจตนามุ่งร้ายในการลักลอบโจรกรรมข้อมูลขององค์กร เพื่อผลประโยชน์ส่วนตัวหรืออาจจะเกิดจากความแค้นในบางเรื่อง

การเจาะระบบจากภายใน ทำให้ข้อมูลรั่วไหลออกไปโดยง่ายและอัตราการเพิ่มของ Insider Attack มีปริมาณเพิ่มขึ้นทุกปี

ระบบเครือข่ายไร้สาย (Wireless LAN)

เกิดขึ้นครั้งแรก ในปี ค.ศ. 1971 บนเกาะฮาวาย โดยโปรเจกต์ ของนักศึกษาของมหาวิทยาลัยฮาวาย ที่ชื่อว่า “ALOHNET” ขณะนั้นลักษณะการส่งข้อมูลเป็นแบบ Bi-directional ส่งไป-กลับง่ายๆ ผ่านคลื่นวิทยุ สื่อสารกันระหว่างคอมพิวเตอร์ 7 เครื่อง ซึ่งตั้งอยู่บนเกาะ 4 เกาะ โดยรอบ และมีศูนย์กลางการเชื่อมต่ออยู่ที่เกาะๆหนึ่ง ที่ชื่อว่า Oahu

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

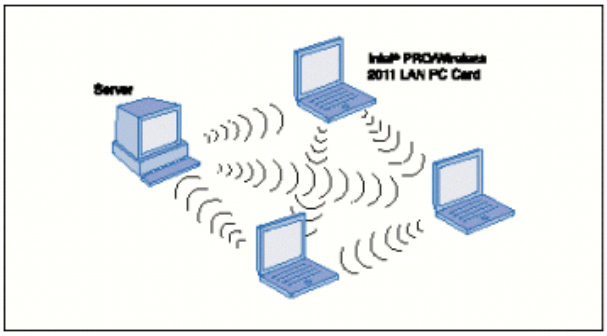
ระบบเครือข่ายไร้สาย (Wireless LAN)

IEEE (Institute of Electrical and Electronic Engineer) กำหนดมาตรฐานระบบเครือข่ายไร้สาย โดยใช้การกำหนดตัวเลข 802.11 แล้วตามด้วยตัวอักษร

1. 802.11b ทำงานที่ย่านความถี่ 2.4 GHz ส่งถ่ายข้อมูลที่ความเร็ว 11 Mbps
2. 802.11g ทำงานที่ย่านความถี่ 2.4 GHz ส่งถ่ายข้อมูลที่ความเร็ว 54 Mbps
3. 802.11n ทำงานที่ย่านความถี่ 2.4 , 5 GHz ส่งถ่ายข้อมูลที่ความเร็ว 100 Mbps
4. 802.11 Wi-Fi เป็นมาตรฐานที่ IEEE ไม่ได้ประกาศใช้งาน แต่เป็นการรวมกลุ่มกันของผู้ผลิตอุปกรณ์ เพื่อเป็นการกำหนดมาตรฐานเอง โดยใช้เครื่องหมาย Wi-Fi สำหรับอุปกรณ์ที่ใช้ งานร่วมกันได้ มาตรฐานนี้ใช้การรักษาความปลอดภัยแบบ WPA (Wi-Fi Protected Access) ทำงาน

รูปแบบระบบเครือข่ายไร้สาย

Peer-to-peer (ad hoc mode)

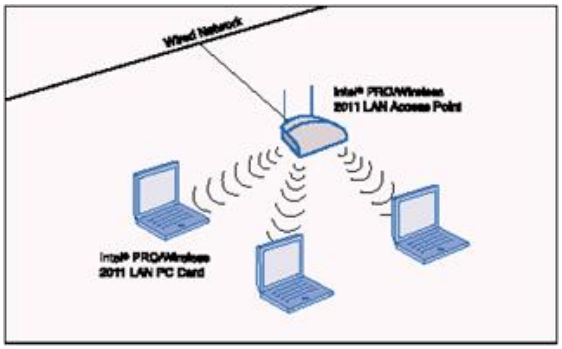


Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

รูปแบบระบบเครือข่ายไร้สาย

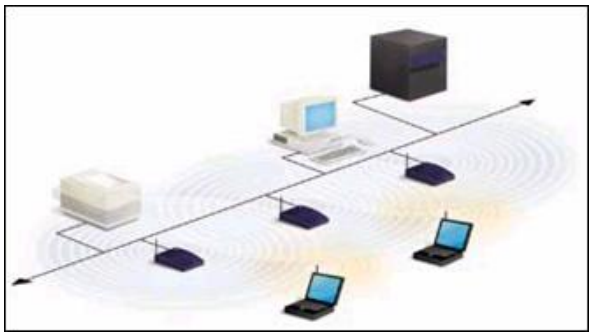
Client/server (Infrastructure mode)



P.F Engineering & Services Co., Ltd.

รูปแบบระบบเครือข่ายไร้สาย

Multiple access points and roaming

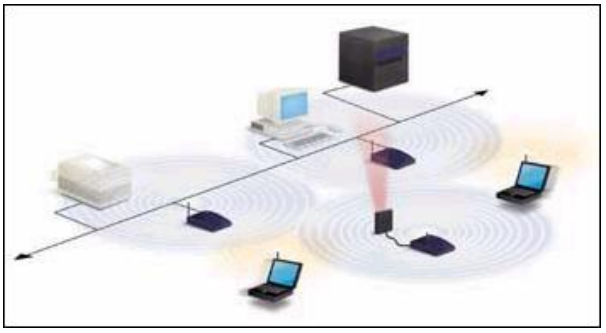


Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

รูปแบบระบบเครือข่ายไร้สาย

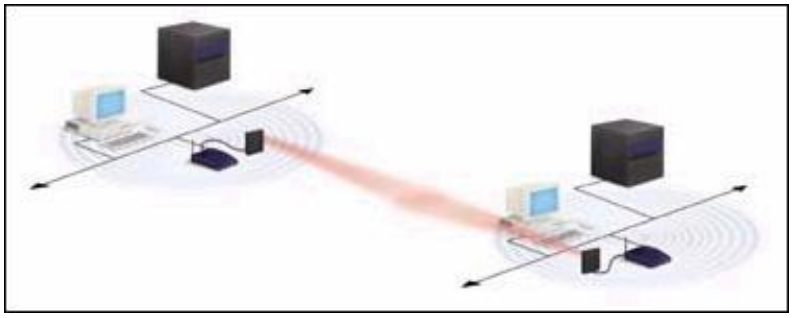
Use of an Extension Point



P.F Engineering & Services Co., Ltd.

รูปแบบระบบเครือข่ายไร้สาย

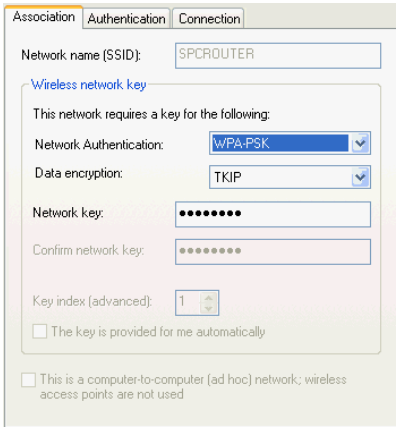
The Use of Directional Antennas

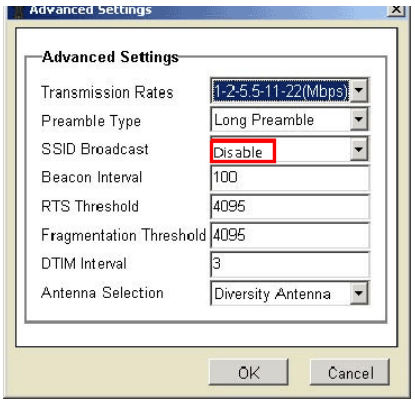


การป้องกันระบบเครือข่ายไร้สาย

1. เปลี่ยน default passwords
2. Restrict access : MAC address Control
3. Encrypt : WEP (Wired Equivalent Privacy) , WPA (Wi-Fi Protected Access)
4. เปลี่ยน default ของ SSID

การป้องกันระบบเครือข่ายไร้สาย





11 วิธีการที่ผู้ใช้งาน ควรใช้ในการป้องกันระบบ คอมพิวเตอร์ของตน

Network Risk

1. ขอคำปรึกษาจากผู้ให้บริการหรือผู้ดูแลโดยตรง
2. นำซอฟต์แวร์ป้องกันไวรัสมาใช้งาน
3. ใช้ไฟร์วอลล์
4. ไม่เปิดไฟล์ที่ไม่รู้จักซึ่งถูกแนบมากับ e-mail
5. ไม่เรียกใช้งานโปรแกรมที่ไม่ทราบที่มา
6. ติดตั้ง patch ให้กับแอพลิเคชันที่ใช้งาน
7. ปิดเครื่องคอมพิวเตอร์ทันทีที่เลิกใช้งาน
8. ยกเลิกการใช้งาน Java, JavaScript และ ActiveX ให้มากที่สุด
9. ทำการสำรองข้อมูลที่สำคัญ
10. ทำแผ่นบูทเพื่อใช้งานในกรณีที่เครื่องคอมพิวเตอร์เกิดความเสียหาย

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ความเสี่ยงจากปัญหาไวรัสคอมพิวเตอร์

ความหมายของมัลแวร์ (Malware)

มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software ซึ่งจะใช้แทนโปรแกรมประสงค์ร้ายต่างๆ เช่น ไวรัส เวิร์ม และโทรจันฮอร์ส ซึ่งเป็นโปรแกรมที่อันตรายต่อระบบคอมพิวเตอร์

เนื่องจากปัจจุบันโปรแกรมร้ายๆเหล่านี้มีหลากหลายและแตกต่างกันไป ทำให้ยากต่อการให้คำจำกัดความของโปรแกรมร้ายๆ แต่ละประเภทเพื่อให้ง่ายและเข้าใจตรงกัน

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

คำจำกัดความของโปรแกรมประสงค์ร้าย

โทรจันฮอร์ส (Trojan Horse) : คือ โปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตรายแต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์หรือทำลายระบบที่รัน โดยโปรแกรมนี้ส่วนใหญ่จะถูกแนบมากับอีเมล์

จุดมุ่งหมายของโทรจันฮอร์สก็เพื่อสร้างความรำคาญให้กับผู้ใช้ หรือขัดขวางการทำงานประจำของระบบ ยกตัวอย่างเช่น โทรจันฮอร์สอาจสร้าง แบ็คดอร์เพื่อเปิดทางให้แฮคเกอร์เข้ามาในระบบเพื่อขโมยข้อมูลหรือเปลี่ยนคอนฟิกของระบบใหม่ เป็นต้น

P.F Engineering & Services Co., Ltd.

คำจำกัดความของโปรแกรมประสงค์ร้าย

เวิร์ม (Worm) : คุณสมบัติพิเศษของเวิร์มคือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ

ความสามารถ : ใช้แบนด์วิธของเครือข่าย หรือใช้รีซอร์สอื่นๆของเครือข่าย, โจมตีแบบปฏิเสธการให้บริการหรือ DOS (Denial of Service), แพร่กระจายตัวเองโดยที่ไม่ต้องอาศัยการช่วยหรือจากผู้ใช้เลย, แพร่กระจายเมื่อผู้ใช้รันโปรแกรมบางโปรแกรม

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การทำงาน : เวิร์มส่วนใหญ่จะพยายามก๊อปปี้ตัวเองไปไว้ในระบบคอมพิวเตอร์ แล้วใช้ช่องทางสื่อสารของระบบหรือเครือข่ายในการแพร่ กระจายตัวเองไปยังเครื่องอื่น ยกตัวอย่าง เช่น เวิร์มซาสเซอร์ (Sasser worm) จะอาศัยช่องโหว่ของเซอร์วิสของวินโดวส์ แล้วใช้ช่องทางการเชื่อมต่อเข้ากับเครือข่ายของระบบในการแพร่กระจายตัวเอง แต่ถ้ามีการอัพเดตระบบปฏิบัติการหรือใช้ไฟล์วอลล์บล็อกพอร์ตที่เวิร์มนี้ใช้ การโจมตีหรือการแพร่กระจายก็จะไม่เกิดขึ้น

คำจำกัดความของโปรแกรมประสงค์ร้าย

ไวรัส (Virus) : ไวรัสเป็นโปรแกรมที่สามารถติดต่อจากไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกันหรือจากคอมพิวเตอร์เครื่องหนึ่งไปเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น มันสามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

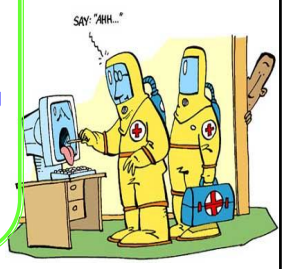
ไวรัสเองอาจทำให้ไฟล์ข้อมูลใช้งานไม่ได้ แต่ใช้พื้นที่ในการจัดเก็บ ใช้รีซอร์สของระบบ และใช้แบนด์วิธของเครือข่ายเมื่อมีการแพร่กระจายตัวเอง

พาหะนำมัลแวร์

ถ้ามัลแวร์เป็นไวรัส มันจะพยายามทำให้เป้าหมายติดไวรัส จำนวนและประเภทของออปเจ็กต์ที่เป็นเป้าหมายได้นั้นมีหลากหลาย

- ตัวอย่าง:

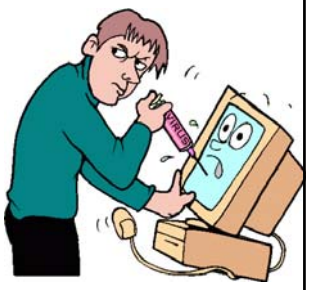
  - **Executable file :** เป็นเป้าหมายคลาสสิกหรือดั้งเดิม ไวรัสสามารถแพร่กระจายโดยการฝังตัวเองไปกับโปรแกรมอื่น นอกเหนือจากไฟล์ที่สามารถเอ็กซ์คิวต์ได้ ซึ่งจะมีนามสกุลเป็น .exe แล้วไฟล์อื่นที่สามารถรันได้ เช่น .com , .sys, .dll, .ovl, .ocx, และ .prg ก็สามารถรันได้เช่นกัน



พาหะนำมัลแวร์

- ตัวอย่าง:

  - **Script :** การโจมตีนี้อาจอาศัยภาษาสคริปต์เพื่อรันและทำให้ติดไวรัส ซึ่งภาษาสคริปต์ที่ว่านี้ เช่น Visual Basic, Javascript, AppleScript หรือ Perl เป็นต้น โดยไฟล์สคริปต์จะมีนามสกุลคือ .vbs, .js, .wsh และ .pl เป็นต้น



VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

พาหะนำมัลแวร์

- ตัวอย่าง:

  - **Macros :** มาโครเป็นภาษาสคริปต์ของแอพพลิเคชั่นบางตัว เช่น ไมโครซอฟท์ออฟฟิศ มัลแวร์ จะอาศัยการรันมาโครสคริปต์นี้ในการแพร่กระจายหรือติดต่อไปยังไฟล์อื่นหรือระบบอื่น หรือทำอันตรายให้กับระบบที่ติด เช่น ไวรัสสามารถใช้ภาษามาโครของไมโครซอฟท์เวิร์ดหรือ Lotus Ami Pro เพื่อสร้างผลกระทบให้ฉบับระบบหรือโปรแกรมในรูปแบบต่างๆ เช่น การเปลี่ยนคำบางคำหรือการเปลี่ยนสี หรือบางทีสามารถฟอร์แมตฮาร์ดดิสก์ก็ได้

P.F Engineering & Services Co., Ltd

พาหะนำมัลแวร์

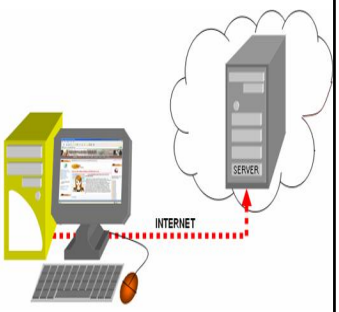
- ตัวอย่าง:

  - Boot Sector : พื้นที่บางส่วนของฮาร์ดดิสก์หรือ CD-Rom เช่น MBR (Master boot record) หรือ Dos boot record อาจเป็นเป้าหมายก็ได้ เนื่องจากส่วนนี้สามารถรันโค้ดได้ เมื่อดิสก์ติดไวรัสในส่วนนี้แล้ว การแพร่กระจายก็สามารถเกิดขึ้นได้กับดิสก์นี้ใช้สำหรับบูตระบบอื่น ถ้าไวรัสนั้นสามารถติดได้ทั้งไฟล์ทั่วไปและบูตเซ็กเตอร์ ไวรัสประเภทนี้เรียกว่า มัลติพาร์ไทต์ไวรัส (Multipartite Virus)

พาหะที่ใช้สำหรับการแพร่ระบาด

- ช่องทางต่างๆที่อาจถูกใช้สำหรับการโจมตีโดยไวรัสหรือมัลแวร์ได้

  เครือข่ายภายนอก : ส่วนของเครือข่ายที่ไม่ได้อยู่ภายใต้การควบคุมขององค์กรควรจัดว่าเป็นพื้นที่เสี่ยงที่อาจถูกโจมตี หรือเป็นแหล่งที่มาของการโจมตีได้ เนื่องจากอินเตอร์เน็ตเป็นระบบเปิดที่อาจมีใครก็ได้ที่มีจุดประสงค์มุ่งร้าย และเป็นแหล่งที่สามารถเรียนรู้วิธีการใช้โปรแกรมประสงค์ร้ายเพื่อโจมตีเป้าหมายได้หลากหลายรูปแบบ



พาหะที่ใช้สำหรับการแพร่ระบาด

คอมพิวเตอร์ของแขกที่มาเยือน : ในขณะที่ความนิยมในการใช้โน้ตบุ๊ค อุปกรณ์อิเล็กทรอนิกส์แบบพกพาอื่นๆเพิ่มขึ้นเรื่อยๆ อุปกรณ์เหล่านี้ต้องเคลื่อนย้ายเข้าออกองค์กรเป็นประจำ ถ้าอุปกรณ์เหล่านี้ไม่มีระบบป้องกันไวรัสที่ดีก็อาจเป็นแหล่งที่มาของการแพร่กระจายของไวรัสได้ ดังนั้น จึงควรให้ความสำคัญ

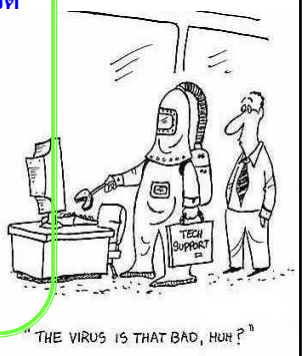
VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

พาหะที่ใช้สำหรับการแพร่ระบาด

เอ็กซีคิวต์ไฟต์ : ทุกๆโค้ดที่สามารถรันหรือเอ็กซีคิวต์ได้อาจเป็นมัลแวร์ได้นี่ไม่ใช่แค่โปรแกรมแต่รวมถึงสคริปต์ แบตไฟล์ และแอ็คทีฟออบเจ็กต์ เช่น ไมโครซอฟท์แอ็คทีฟคอนโทรล เป็นต้น

ไฟล์เอกสาร : ในขณะที่โปรแกรมเวิร์ดโพรเซสเซอร์และสเปรดชีทมีความสามารถมากขึ้นเรื่อยๆ แต่ก็กลายเป็นเป้าหมายของการโจมตี โดยเฉพาะมาโครที่รองรับโดยแอพพลิเคชั่นเหล่านี้เป็นจุดอ่อนที่ทำให้สามารถรันไวรัสหรือมัลแวร์ได้

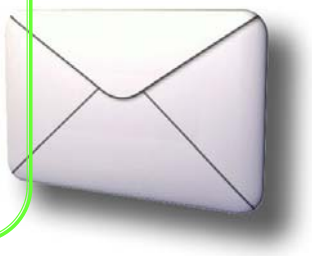


P.F Engineering & Services Co., Ltd.

พาหะที่ใช้สำหรับการแพร่ระบาด

อีเมล : นักเขียนไวรัสหรือมัลแวร์อาจใช้ประโยชน์ทั้งจากไฟล์ที่แนบมากับอีเมลและแอ็คทีฟ HTML โค้ดที่ส่งมาพร้อมกับอีเมลก็อาจเป็นแหล่งที่มาของไวรัสหรือมัลแวร์อื่นๆ

มีเดียเก็บข้อมูล : การถ่ายโอนไฟล์ผ่านทางอุปกรณ์จัดเก็บข้อมูลที่ถอดเข้าออกได้ ก็อาจเป็นช่องทางหนึ่งของการแพร่กระจายไวรัสหรือมัลแวร์ได้ มีเดียประเภทนี้ เช่น



VIRUS Risk

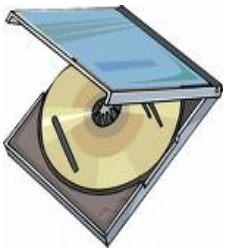
กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

พาหะที่ใช้สำหรับการแพร่ระบาด

- ตัวอย่าง: มีเดียเก็บข้อมูล

CD-ROM และ DVD-ROM : การพัฒนา cd และ dvd จนกลายเป็นสื่อที่มีราคาถูกหาซื้อได้ง่าย ก็อาจเป็นเครื่องมือสำหรับนักพัฒนาไวรัสหรือมัลแวร์ได้

Floppy และ Zip drives : มีเดียประเภทนี้มีความนิยมลดลงเรื่อยๆเนื่องจากขนาดพื้นที่ในการจัดเก็บข้อมูลมีน้อย และความเร็วต่ำ แต่ก็ยังมีความเสี่ยงและอาจเป็นแหล่งของการแพร่กระจายไวรัสได้เช่นกัน



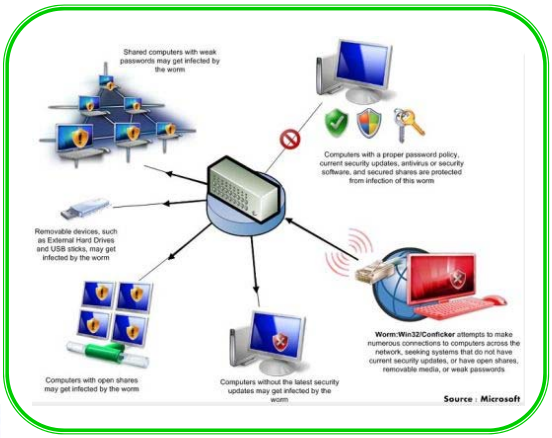
P.F Engineering & Services Co., Ltd.

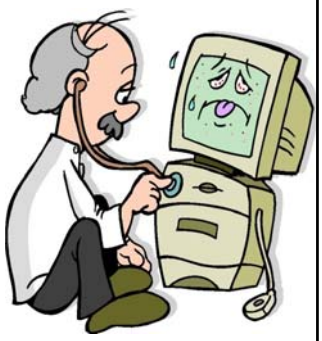
- ตัวอย่าง: มีเดียเก็บข้อมูล

USB drives : อุปกรณ์อุปกรณ์มาตรฐานที่ติดตั้งมาพร้อมกับคอมพิวเตอร์พีซีที่ใช้ทั่วไป ประเภทนี้กำลังได้รับความนิยมเพิ่มขึ้นเรื่อยๆ เนื่องจากความสะดวกในการพกพา ขนาดพื้นที่ที่ใช้สำหรับจัดเก็บข้อมูล และประสิทธิภาพ อุปกรณ์เหล่านี้ก็อาจเป็นสื่อที่ดีของไวรัสและมัลแวร์

Memory cards : กล้องดิจิตอลและอุปกรณ์มือถืออื่นๆ เช่น PDA และโทรศัพท์มือถือช่วยทำให้เมมโมรีการ์ดได้รับความนิยม

แนวทางการป้องกันไวรัส





การป้องกันไวรัสที่เครื่องไคลเอนท์

- **การลบโปรแกรมที่ไม่ได้ใช้งาน**

  ขั้นตอนแรกในการป้องกันคือ การลดช่องทางที่ไวรัสอาจจะใช้เป็นสื่อที่จะเข้ามาในเครื่อง ตัวอย่างเช่นการลบแอพพลิเคชั่นหรือเซอร์วิสที่ไม่จำเป็นออกจากเครื่อง บางระบบปฏิบัติการนั้นเมื่อติดตั้งโดยดีฟอลต์อาจมีบางเซอร์วิสที่ไม่จำเป็นต้องใช้ เช่น เว็บเซิร์ฟเวอร์ FTP เซิร์ฟเวอร์ และเมลเซิร์ฟเวอร์ เป็นต้น ซึ่งถ้าไม่จำเป็นต้องใช้ก็ไม่ควรติดตั้ง

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การป้องกันไวรัสที่เครื่องไคลเอนท์

- **เครื่องมือที่ช่วยในการบริหารจัดการเกี่ยวกับการอัพเดตแพตช์**

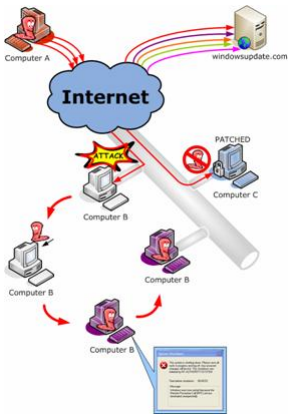
  Software Update Service (SUS) : ไมโครซอฟท์ได้ออกแบบเซอร์วิสเพื่อให้บริการในการอัพเดตซอฟต์แวร์ของไมโครซอฟท์สำหรับองค์กร เพื่อช่วยให้การอัพเดตซอฟต์แวร์ต่างๆที่ใช้ในองค์กรเป็นไปอย่างมีประสิทธิภาพ รายละเอียดเกี่ยวกับการใช้เครื่องมือสามารถดูได้จาก

  http://www.microsoft.com/windowsserversystem/sus/

การป้องกันไวรัสที่เครื่องไคลเอนท์

การติดตั้งโฮสต์เบสไฟร์วอลล์

โฮสต์เบสไฟร์วอลล์หรือเพอร์ซันนอลไฟร์วอลล์เป็นอีกเครื่องมือที่สำคัญสำหรับไคลเอนท์ โดยเฉพาะโน้ตบุ๊คที่อาจถูกนำออกไปใช้นอกเครือข่าย และไม่ได้อยู่ภายใต้ระบบป้องกันของเครือข่ายภายใน ไฟร์วอลล์จะทำหน้าที่กรองข้อมูลที่ไหลเข้าออกคอมพิวเตอร์เครื่องนั้น



VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การติดตั้งซอฟต์แวร์ป้องกันไวรัส

ปัจจุบันได้มีหลายบริษัทที่ผลิตซอฟต์แวร์ป้องกันไวรัสออกจำหน่าย ซึ่งซอฟต์แวร์เหล่านี้ถูกออกแบบมาเพื่อป้องกันคอมพิวเตอร์จากการโจมตีของไวรัส และพยายามให้มีผลกระทบต่อการใช้งานของผู้ใช้ให้น้อยที่สุด ส่วนใหญ่แล้วซอฟต์แวร์นี้จะมีประสิทธิภาพสูงในการป้องกันและกำจัดไวรัส แต่จำเป็นที่จะต้องมีการอัพเดตซิกเนเจอร์เป็นประจำเพื่อป้องกันไวรัสใหม่ๆ โดยซอฟต์แวร์ป้องกันไวรัสควรมีบริการในการอัพเดตซิกเนเจอร์ไฟล์อย่างรวดเร็วและง่ายที่สุด

P.F Engineering & Services Co., Ltd.

วิธีการหรือคำแนะนำทั่วๆ ไปในการป้องกันมัลแวร์

1. ติดตั้งโปรแกรมป้องกันไวรัสและสปายแวร์ โดยต้องทำการอัพเดตฐานข้อมูลไวรัสและสปายแวร์อย่างสม่ำเสมอ
2. ทำการสแกนไวรัสอย่างสม่ำเสมอ
3. ปิดการใช้งาน Auto play ในทุกๆ ไดรฟ์
4. ทำการสแกนสื่อเก็บข้อมูลแบบพกพาทุกครั้ง ก่อนการใช้งาน

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

วิธีการหรือคำแนะนำทั่วๆ ไปในการป้องกันมัลแวร์

5. ในกรณีที่ต้องทำการแชร์ไฟล์ข้อมูลต่างๆ ให้ทำการแชร์แบบอ่านอย่างเดียว (Read Only) เพื่อป้องกันปัญหาเกี่ยวกับไวรัส สปายแวร์ และมัลแวร์ (Virus, Spyware and Malware) ถ้าจำเป็นต้องทำการแชร์แบบ Read-Write ให้กำหนดรหัสผ่านสำหรับการแชร์แบบ Write ทุกๆ ครั้ง

P.F Engineering & Services Co., Ltd

วิธีการหรือคำแนะนำทั่วๆ ไปในการป้องกันมัลแวร์

6. เพื่อเพิ่มประสิทธิภาพการทำงานของเครื่อง และป้องกันการสูญหายของข้อมูลเนื่องจากระบบวินโดวส์เสีย ให้แยกข้อมูลต่างๆ ไปเก็บไว้บนไดร์ฟอื่น ที่ไม่ใช่ไดร์ฟที่ระบบปฏิบัติการติดตั้งอยู่

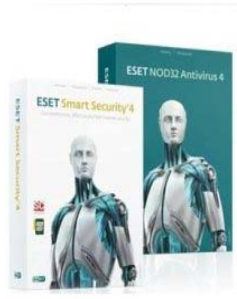
7. เพื่อป้องกันการสูญหายของข้อมูลเนื่องจากฮาร์ดดิสก์เสีย ให้ทำการสำรองข้อมูลที่สำคัญๆ ลงแผ่นซีดีหรือดีวีดี

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

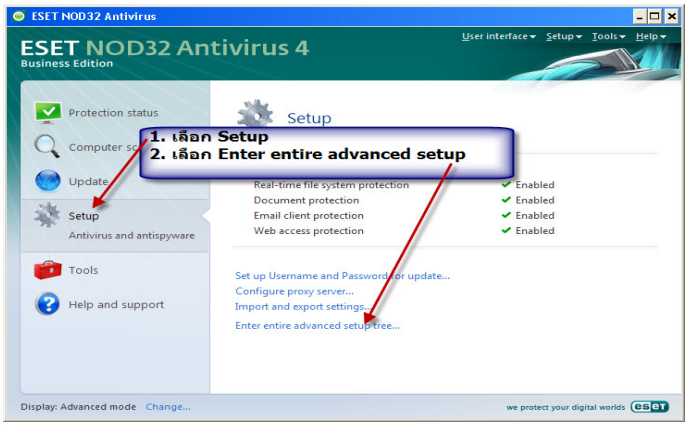
Antivirus Eset Smart Security Business Edition

- Eset Nod32Smart Security
- Protection Status
- Update Signature
- Scan Virus
- Tools
- Advanced Setup
- Firewall
- Uninstall Eset Nod32Smart Security



P.F Engineering & Services Co., Ltd

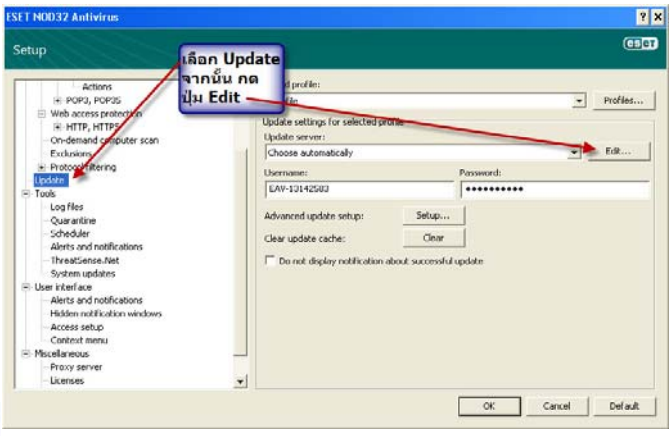
การกำหนดค่า Update Server สำหรับ Nod32



VIRUS Risk

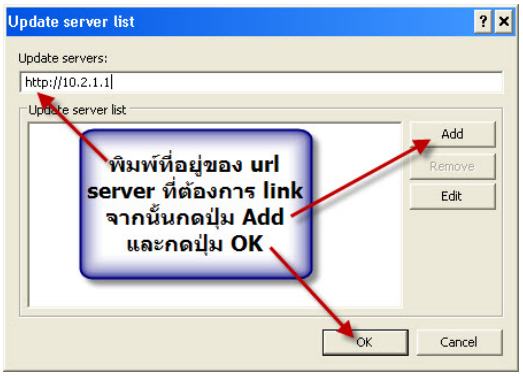
กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การกำหนดค่า Update Server สำหรับ Nod32



P.F Engineering & Services Co., Ltd

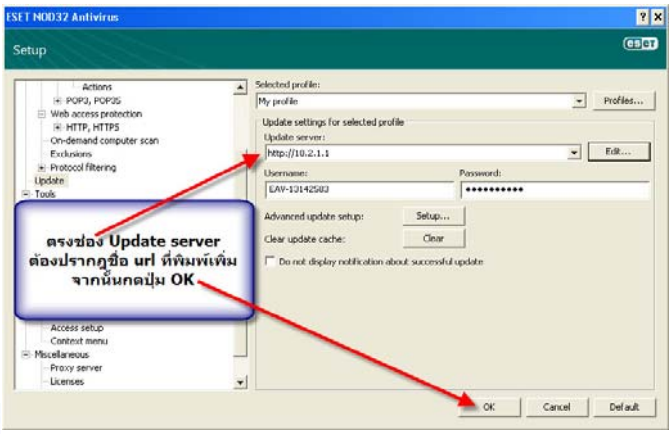
การกำหนดค่า Update Server สำหรับ Nod32



VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การกำหนดค่า Update Server สำหรับ Nod32

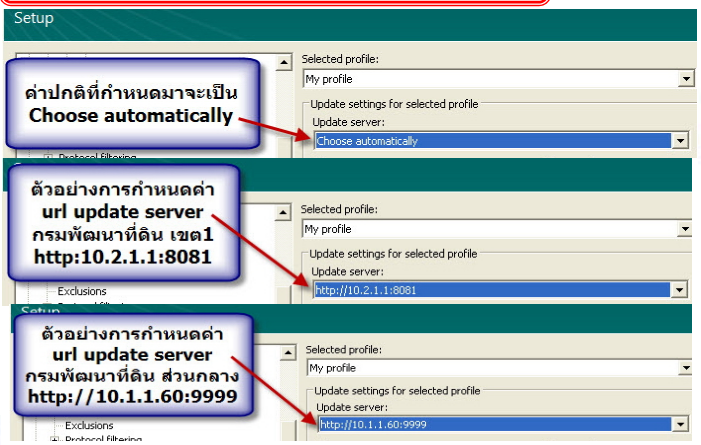


P.F Engineering & Services Co., Ltd

VIRUS Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

การกำหนดค่า Update Server สำหรับ Nod32



P.F Engineering & Services Co., Ltd

Network Risk

กรมพัฒนาที่ดิน กระทรวงเกษตรและสหกรณ์

รู้เขา รู้เรา

รบร้อยครั้ง ชนะทั้งร้อยครั้ง

P.F Engineering & Services Co., Ltd