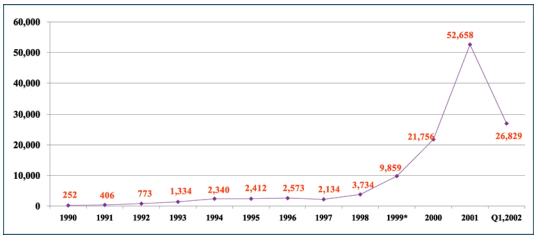
ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

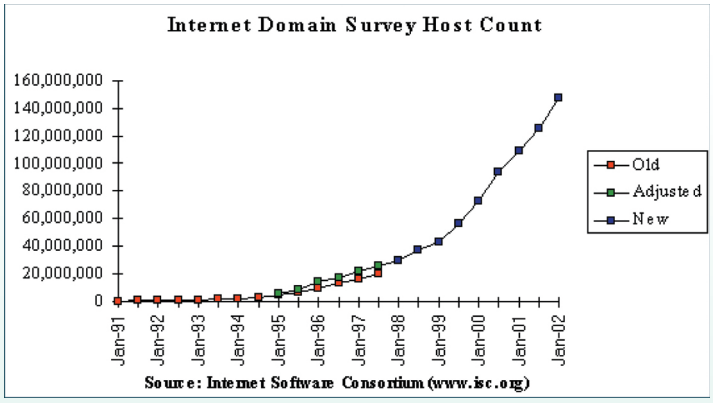
Thai Computer Emergency Response Team: Thai CERT

ปัจจุบันมีการใช้งานอินเทอร์เน็ตอย่างแพร่หลาย ในองค์กรต่างๆ ทั้งภาครัฐและภาคเอกชนรวมถึงประชาชนโดยทั่วไปก็ใช้อินเทอร์เน็ตในการติดต่อสื่อสาร เผยแพร่ข้อมูล หรือเป็นแหล่งข้อมูล ทั้งนี้เพื่อวัตถุประสงค์ทางด้านต่างๆ อาทิเช่น การศึกษา การพาณิชย์ การดำเนินงานขององค์กร ภารกิจส่วนตัว หรือแม้แต่เพื่อความบันเทิง จากการที่มีผู้ใช้อินเทอร์เน็ตทั่วโลกจำนวนมากและมีแนวโน้มที่เพิ่มขึ้นอย่างรวดเร็ว ประกอบกับข้อมูลที่อยู่บนอินเทอร์เน็ตมีมูลค่าทางเศรษฐกิจ สังคม และ/หรือความมั่นคงต่อบุคคล/องค์กร/ประเทศ ทำให้เป็นแรงจูงใจให้เกิดอาชญากรรมชนิดใหม่ขึ้นบนอินเทอร์เน็ต นั่นคืออาชญากรรมคอมพิวเตอร์โดย รูปแบบของอาชญากรรมมีได้หลากหลาย อาทิเช่น การโจรกรรมข้อมูล การลักลอบเปลี่ยนแปลง การรบกวนหรือขัดขวางการให้บริการ การทำลายระบบคอมพิวเตอร์ ทั้งนี้เนื่องจากเทคโนโลยีที่เอื้ออำนวยและไม่มีข้อจำกัดทางด้านสถานที่ตั้งซึ่งอาชญากรสามารถเลือกโจมตีต่อเป้าหมาย ณ จุดใดๆ ก็ได้บนโลก โดยอาศัยเพียงการเชื่อมต่อคอมพิวเตอร์ส่วนบุคคลเข้ากับระบบอินเทอร์เน็ต ยังผลให้การก่ออาชญากรรมคอมพิวเตอร์นี้สามารถกระทำได้โดยง่าย ซึ่งก่อให้เกิดความสูญเสียมูลค่ามหาศาลและยากต่อการจับกุม ปัจจุบันมีอาชญากรรมคอมพิวเตอร์เกิดขึ้นเป็นจำนวนมากแต่องค์กรที่เป็นผู้เสียหายมักไม่เปิดเผยเหตุการณ์ต่อสาธารณะเนื่องจากกลัวจะกระทบกระเทือนต่อภาพพจน์และการดำเนินงานขององค์กร



ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ หรือมีชื่อภาษาอังกฤษว่า Computer Security Incident Response Team (CISRT) หรือ Computer Emergency Response Team (CERT) มีหน้าที่หลักๆ ในการตอบโต้ และจัดการต่อเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยคอมพิวเตอร์บนอินเทอร์เน็ต โดยมีความมุ่งหมายเพื่อให้เกิดความปลอดภัยในการใช้งานระบบคอมพิวเตอร์และลดความเสี่ยงต่ออาชญากรรมคอมพิวเตอร์ให้กับสมาชิก หรือผู้ขอรับบริการ ซึ่งงานในหน้าที่ของ CERT ได้แก่

- การตอบสนองต่อเหตุการณ์ความปลอดภัยคอมพิวเตอร์ (Incidental Response)
- การให้คำแนะนำในการปฏิบัติเพื่อความปลอดภัย (Alert and Advisory)
  - การพัฒนาเครื่องมือและแนวทางในการปฏิบัติเพื่อเพิ่มความปลอดภัยในการใช้งานคอมพิวเตอร์
  - การตรวจสอบความปลอดภัย (Security Audit)
  - การจัดสัมมนาอบรมในเรื่องความปลอดภัยคอมพิวเตอร์ (Security Training)
  - การเผยแพร่ข่าวสารความปลอดภัยคอมพิวเตอร์ (Public Awareness)



ปัจจุบันมีหน่วยงานในหลายประเทศทั้งจากภาครัฐและภาคเอกชนได้จัดตั้งองค์กรในลักษณะ CERT อาทิเช่น CERT/CC-Pitsburg สหรัฐอเมริกา, AUSCERT ออสเตรเลีย, JPCERT/CC ญี่ปุ่น, SigCERT สิงคโปร์, NISER มาเลเซีย และอื่นๆ อีกมากกว่า 80 แห่งทั่วโลก ซึ่ง CERT ทุกแห่งก็มีความมุ่งหมายอันเดียวกัน คือการสร้างความปลอดภัยให้แก่ผู้ใช้งานคอมพิวเตอร์ที่เชื่อมต่อกับอินเทอร์เน็ต ต่างกันเพียงแต่รายละเอียดปลีกย่อยของการให้บริการต่อสมาชิก

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

Thai Computer Emergency Response Team: Thai CERT

เหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์ นั้นเกิดจากการที่*ผู้โจมตี*อาศัย*เครื่องมือ* ต่างๆ มาฉวยโอกาสถึง *ความล่อแหลม* ของระบบเพื่อจะสามารถ*กระทำต่อเป้าหมาย*ให้บังเกิด*ผลที่ไม่ได้รับอนุญาต* เพื่อให้บรรลุ*วัตถุประสงค์* ของผู้โจมตี ดังแสดงในรูปด้านล่าง

เหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์

ผู้โจมตี	เครื่องมือ	ความล่อแหลม	การกระทำ	เป้าหมาย	ผลที่ไม่ได้รับอนุญาต	จุดประสงค์
Hackers	การโจมตีทางกายภาพ	การออกแบบ	Probe	account	การเข้าถึงที่เพิ่มขึ้น	ท้าทาย, สถานะ, ตื่นเต้น
Spies	การหาข้อมูล	การใช้งาน	Scan	Process	การเปิดเผยข้อมูล	ผลประโยชน์ทางการเมือง
ผู้ก่อการร้าย	ใช้คำสั่งของผู้ใช้	การตั้งค่า	Flood	ข้อมูล	ข้อมูลเสียหาย	ผลประโยชน์ทางการเงิน
สายลับในองค์กร	โปรแกรม หรือ script		Authenticate	Component	Denial Of Service	ความเสียหาย
อาชญากรมืออาชีพ	Autonomous Agent		Bypass	คอมพิวเตอร์	การขโมย resources	
Vandals	Distributed Tool		Spoof	เครือข่าย		
Voyeurs	การดักอ่านข้อมูล		อ่าน	Internetwork		
			สำเนา			
			ขโมย			
			เปลี่ยนแปลง			
			ลบ			

ตัวอย่างเหตุการณ์ฯ เช่น ในกรณีของ Nimda worm ที่ผ่านมาจะเห็นได้ว่าจะประกอบไปด้วย

1. ผู้โจมตี – ในที่นี้คาดว่าจะเป็น Hacker, ผู้เขียนไวรัส, ผู้ประสงค์ร้าย
2. เครื่องมือ – คือโปรแกรม
3. ความล่อแหลม – เป็นความล่อแหลมที่เกิดขึ้นจากการออกแบบตัวโปรแกรมต่างๆ ที่ worm นี้ทำงานอยู่ได้ ได้แก่ โปรแกรมอ่าน e-mail ช่องโหว่ของระบบปฏิบัติการ (OS) การแชร์ไฟล์ผ่านเครือข่าย
4. การกระทำ – การกระทำของ worm นี้คือการคัดลอก (ตัวเอง), กระจายตัวผ่านเครือข่ายเพิ่ม traffic ของเครือข่ายทำให้เครือข่ายใช้งานไม่ได้
5. เป้าหมาย – เป้าหมายของ worm นี้คือข้อมูลบนเครื่องคอมพิวเตอร์และเครือข่าย
6. ผลที่ไม่ได้รับอนุญาต – ในที่นี้คือทำให้เกิดการเปิดเผยของข้อมูลและข้อเสียหาย
7. จุดประสงค์ – คาดว่าจะเพื่อความท้าทาย ความตื่นเต้น หรือผลประโยชน์อื่นแอบแฝง

จะเห็นได้ว่าในการที่จะเกิดเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์นั้น จะต้องมีการเชื่อมต่อกันอย่างสมบูรณ์ของทั้ง 7 ขั้นตอนดังกล่าวนี้ ดังนั้น หากเราสามารถป้องกันไม่ให้มีการเชื่อมต่อที่สมบูรณ์ได้เราก็จะสามารถป้องกันไม่ให้เกิดเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์ขึ้นได้

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

Thai Computer Emergency Response Team: Thai CERT

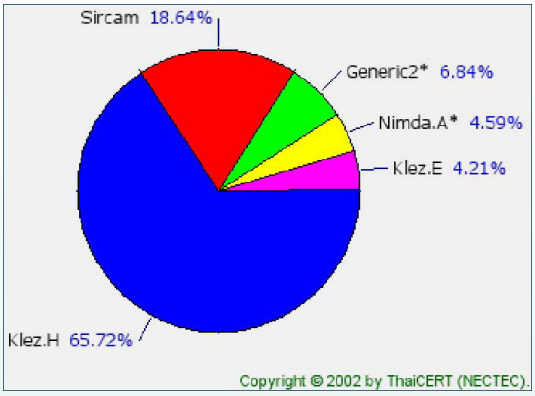
ไวรัส คือ โปรแกรมขนาดเล็กที่แฝงตัวมากับโปรแกรมหรือไฟล์อื่นๆ ซึ่งไวรัสมีความสามารถที่จะสำเนาตัวเองได้โดยอัตโนมัติ และสามารถกระจายตัวเองโดยการแทรกตัวไปติดไฟล์ต่างๆ นอกจากนี้ไวรัสยังมีความสามารถที่จะสำเนาตัวเองไปยังคอมพิวเตอร์เครื่องอื่นได้โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ หรืออาศัยสื่อทางคอมพิวเตอร์อื่น เช่น แผ่นดิสก์ ซีดี เอ็ม.ดี. ฯลฯ

การกระจายตัวของไวรัส (Virus Infection)

การกระจายตัวของไวรัสระหว่างเครื่องคอมพิวเตอร์ภายในเครือข่ายเดียวกัน หรือระหว่างเครือข่ายสามารถเกิดขึ้นได้หลายวิธี เช่น

- การแชร์ไฟล์ในระบบเครือข่าย
- อี-เมล์ซึ่งมี attachment file ที่มีไวรัสแอบแฝงอยู่
- โปรแกรมที่ติดตั้งจากแผ่น diskette หรือ cd-rom เมื่อโปรแกรมนั้นๆ มีไวรัสแอบแฝงอยู่
- การสำเนาไฟล์หรือข้อมูลจากเครื่องให้บริการ (Server)
- Internet News Group ต่างๆ
- การรับส่งไฟล์ผ่านทางอินเทอร์เน็ต เมื่อไฟล์นั้นๆ เป็นไฟล์ที่ประกอบด้วยไวรัส ไม่ว่าจะเป็น WWW หรือ ICQ
- การแทรกตัวของไวรัสที่แฝงตัวในเว็บเพจ ผ่าน ActiveX หรือ Java Script

แผนภูมิวงกลมแสดงการแพร่กระจายไวรัสคอมพิวเตอร์
ในช่วง 10 ก.พ. – 10 พ.ค. 2545



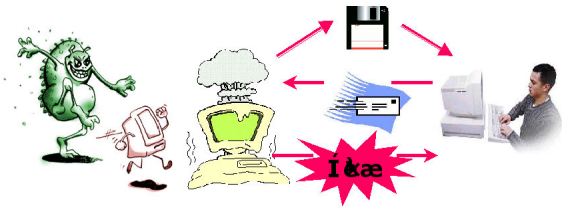
มูลค่าความเสียหายที่เกิดขึ้นจากไวรัสคอมพิวเตอร์ทั่วโลก

ปี พ.ศ.	มูลค่าโดยรวมของความเสียหายที่เกิดขึ้นจากไวรัสคอมพิวเตอร์ (หมื่นล้าน ดอลลาร์สหรัฐ)
2001 Nimda	0.63
2001 CodeRed(s)	2.62
2001 Sircam	1.05
2000 Love Bug	8.75
1999 Melissa	1.10
1999 Explorer	1.02

อ้างอิงจาก Computer Economics, Inc: 2001

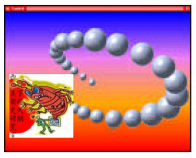
ไวรัสคืออะไร

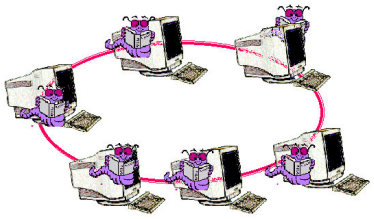
โปรแกรมคอมพิวเตอร์ที่กระจายตัวเองไปสู่ไฟล์ต่างๆ ในเครื่องคอมพิวเตอร์ โดยอาศัยพาหะเช่น อีเมล์(E-mail) ผู้ใช้ไฟล์แนบแผ่นดิสก์(Floppy disk)



หนอน (Worm)

โปรแกรมคอมพิวเตอร์ที่สามารถแพร่กระจายได้ด้วยตัวเองผ่านระบบเน็ตเวิร์ก (E-mail) หรืออาศัยคุณสมบัติในตัวเองเช่น SMTP ทำให้แพร่กระจายรวดเร็ว





โทรจัน (Trojan)

โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบให้แฝงตัวเองเข้าไปในระบบกับโปรแกรมอื่น เช่น รูปแบบ Flash เพื่อ ดัก จับ ดู และควบคุมการทำงานเครื่องคอมพิวเตอร์ของเป้าหมาย แต่จะไม่สำเนาตัวเองแพร่ไปสู่ระบบอื่น

ข่าวหลอกลวง (Hoax)

เป็นการส่งข้อความต่อๆ กันเหมือนจดหมายลูกโซ่เพื่อให้เกิดความเข้าใจผิด โดยอาศัยเทคนิคจิตวิทยา ทำให้ข่าวสารนั้นน่าเชื่อถือ เช่น
ไวรัส A virtual card for you.
โปรดอย่าดื่ม..... มือถือยี่ห้อ..... ฯลฯ

ฉันได้รับเรื่องนี้จากอีเมล์ของฉัน โปรดระวัง!! อ่านโดยทันทีและส่งผ่านให้ทุกๆ คนที่คุณรู้จัก ตอนนี้ อาจมีใครบางคนกำลังส่ง Screensaver สุดสวยงามเป็นรูปกบของเบียร์ Budweiser มาให้ถ้าคุณดาวน์โหลดมัน คุณจะสูญเสียข้อมูลทุกสิ่ง ฮาร์ดไดร์ฟของของคุณจะพังและใครบางคนจากอินเทอร์เน็ตของคุณ ห้ามดาวน์โหลดมันได้สภาพการณ์ใดๆ โดยเด็ดขาด!! มันเพิ่งออกอาละวาดเมื่อวานนี้ โปรดแจกจ่ายเอกสารนี้ออกไป นี่คือ ไวรัสตัวใหม่ มุ่งร้ายมากและผู้คน จำนวนมากมายยังไม่รู้เรื่องเกี่ยวกับมัน คำแนะนำนี้ถูกประกาศเมื่อวานตอนเช้าจากไมโครซอฟท์ โปรดแชร์ข่าวนี้กับทุกๆ คนที่อาจจะเข้าถึงอินเทอร์เน็ต อีกครั้ง! ผ่านข้อความนี้ไปยังทุกๆ คนใน Address book ของคุณเพื่อหยุดยั้งการแพร่ระบาดของมัน AOL บอกว่านี่คือไวรัสที่อันตรายและยังไม่มีวิธีแก้ในตอนนี้

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

Thai Computer Emergency Response Team: Thai CERT

สวทช NSTDA

NECTEC
Electronic • Computer • Telecommunication • Information

วิธีการป้องกันไวรัสคอมพิวเตอร์

ทาง E-mail (อีเมล์)

- อย่าเปิดไฟล์ที่แนบมา จากบุคคลที่ไม่รู้จัก หรือไม่แน่ใจ
- อย่าเปิดไฟล์ที่แนบมา จนกว่าจะรู้ที่มา
- อย่าเปิด E-mail ที่มี subject ที่เป็นข้อความจูงใจ เช่น ภาพเด็ด รหัสผ่าน เป็นต้น
- ลบ E-mail ที่ไม่แน่ใจทิ้งทันที เพื่อตัดปัญหาทั้งปวง
- อัปเดต โปรแกรมที่ใช้อ่าน อีเมล์ เช่น IE. และ Outlook Express
- สร้าง Filter Rule ในโปรแกรมรับ-ส่ง E-mail
- แยกความสำคัญของเมล์บ็อกซ์ตามลำดับ ความสำคัญของ E-mail

วิธีการป้องกันไวรัสคอมพิวเตอร์

ทางไฟล์ (File) และสื่อ (Media) เช่น Diskett, CD-ROM,DVD, Tape back up

- scan virus กับ สื่อ (Media) ก่อนใช้งานทุกครั้ง
- ไม่ใช้ สื่อ (Media) ที่ไม่ทราบแหล่งที่มา เช่น แผ่น pantip
- สร้าง virus - free start up disk สำหรับใช้เวลาจำเป็น
- ควรใช้งานเอกสารเป็น RichTextFormat (.rtf) แทน Document Format (.doc)
- ไม่ควรเปิดไฟล์ (file) ที่มีนามสกุลแปลกๆ เช่น image.txt.vbs ให้ลบทิ้งทันที

วิธีการป้องกันไวรัสคอมพิวเตอร์

ทางอินเทอร์เน็ต

- ไม่เปิดไฟล์ที่แนบมากับ E-mail หรือ ICQ, IRC หรือ การแลกเปลี่ยนไฟล์ โดยเฉพาะ .exe .pif .com .bat .vbs
- ไม่ควรเข้าเว็บไซต์ที่มากับ E-mail, ICQ โฆษณาชวนเชื่อ
- ไม่ดาวน์โหลดไฟล์ต่างๆ จากเว็บไซต์ที่ไม่มั่นใจความปลอดภัย
- ติดตามข่าวสารข้อมูลไวรัสและแจ้งเตือนไวรัสอยู่เสมอ

วิธีการป้องกันไวรัสคอมพิวเตอร์

ทางระบบ

- ติดตั้งโปรแกรม Antivirus
- ปรับปรุงฐานข้อมูลไวรัสอยู่เสมอ (Update Antivirus)
- ติดตั้ง patch ใหม่ๆ ระบบปฏิบัติการ
- ตั้งค่าของ OS ให้เห็นไฟล์ที่มีอยู่ทั้งหมด
- งดแชร์ไฟล์ต่างๆ ในองค์กร
- งดใช้ E-mail free ภายในองค์กร

วิธีการป้องกันไวรัสคอมพิวเตอร์

นโยบายขององค์กร

- สำรองข้อมูลสำคัญไว้เสมอ
- จำกัดจำนวนและผู้ใช้ ในการใช้งานเครื่อง
- เลือกใช้การสแกน E-mail ตรวจสอบไวรัส ก่อนส่งผ่านเข้ามาในระบบ
- ห้ามรับ-ส่ง เอกสารที่ลงท้ายด้วย .exe หรือ .vbs ในองค์กร
- พนักงานต้องไม่กำจัดไวรัสด้วยตนเอง ถ้าไม่มีความรู้
- ตรวจสอบการดาวน์โหลดไฟล์ และการนำโปรแกรมต่างๆ มาใช้ในองค์กร

คาถาป้องกันไวรัส

ไม่ใช้แผ่นมั่ว
ไม่ชัวร์อย่าเปิด
อย่าละเมิด Security (policy)
ติดตามข่าวสารไวรัสดีๆ
สำรองข้อมูลที่สำคัญ

AP8 งานเทคโนโลยีเพื่อความมั่นคงของประเทศ
ฝ่ายประยุกต์เทคโนโลยี
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

www.nectec.or.th/info/posters/

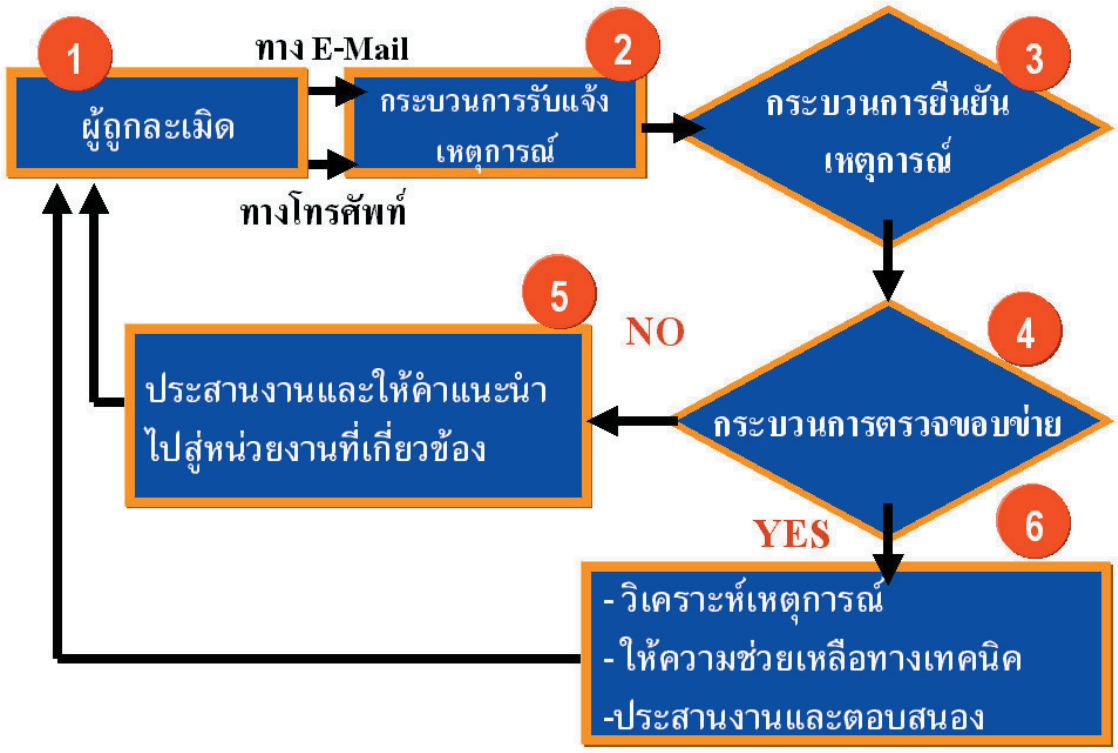
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

Thai Computer Emergency Response Team: Thai CERT

ผังขั้นตอนการดำเนินงานในการตอบสนองความปลอดภัยคอมพิวเตอร์ ของ ThaiCERT



การตรวจสอบกระบวนการแจ้งเหตุเพื่อพิสูจน์ตัวตน

- ที่อยู่.....
- ชื่อ-นามสกุล.....
  ชื่อองค์กร.....
- เบอร์โทรศัพท์..... โทรสาร.....
- อีเมล์ (E-mail) .....
- ประเภทขององค์กร (รัฐ, เอกชน, ส่วนตัว)

รายละเอียดของเหตุการณ์

- ชื่อ Host และ IP address
- หน้าที่ของ Host
- เวลา และย่านเวลา
- รายละเอียดของเหตุการณ์ (Log File วันที่ เวลา)
  - Log file
  - วันที่และเวลา
  - เวอร์ชัน ของซอฟต์แวร์
  - Patch
  - ผลที่เกิดขึ้น

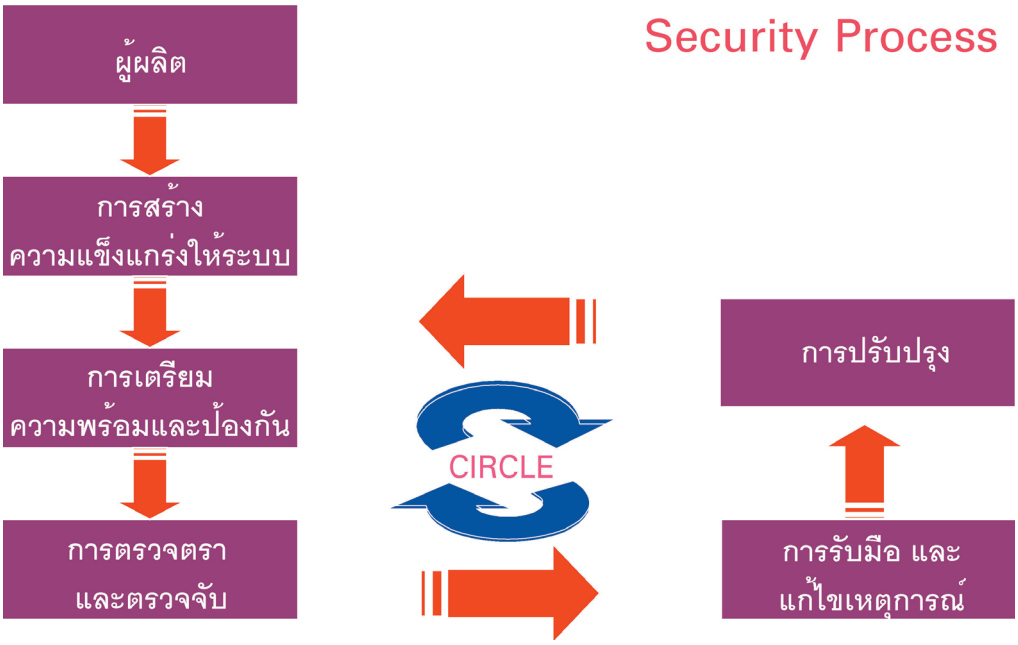
ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545

ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์

Thai Computer Emergency Response Team: Thai CERT

กระบวนการรักษาความปลอดภัย
Security Process



Vendor/developer

ช่องโหว่ (Hole),
ข้อบกพร่อง (Bug)
โปรแกรมแก้ไขข้อบกพร่อง (Patch Release)
การยกระดับโปรแกรม (Upgrade)
การติดตั้งค่าโดยปริยาย (Default Installation)

Detect/Capture

การวิเคราะห์ (Analysis)
การตรวจดู เฝ้าดูข้อมูล (Monitor Info)
ระบบการตรวจจับการบุกรุก (IDS)
กระบวนการแจ้งเตือน (Alarm process)
นโยบายการตรวจจับ (Policy)
การตรวจสอบ (Audit)
การดักจับข้อมูล (Sniffer)
ไฟร์วอลล์ (Firewall)
โปรแกรมป้องกันไวรัส (Antivirus Software)

Hardening

ข้อมูล (Data)
โฮสต์ (Host)
เครือข่าย (Network)
อินเทอร์เน็ต (Internet)
ทางกายภาพ (Physical)
เชิงตรรกะ (Logical)
นโยบายการเสริมสร้างความแข็งแกร่ง
ของระบบ (Policy)

Response/Recovery

การวิเคราะห์ (Analysis)
การวิเคราะห์จากหลักฐาน (Forensics)
การประชาสัมพันธ์ (PR)
การรับมือกับเหตุการณ์ความปลอดภัยคอมพิวเตอร์
(Incident Response)
การสำรองข้อมูล (Back up)
การดำเนินคดีตามกฎหมาย (Law enforcement)
นโยบายการรับมือกับเหตุการณ์ (Policy)
ระบบรับมือกับเหตุการณ์อัตโนมัติ
(Auto-Response System)
ทีมวิเคราะห์นโยบาย (Policy Team)

Prepare/Prevent

ไฟล์ และไดเรกทอรี (File + Directory)
กระบวนการ (Process)
เคอร์แนล (Kernel)
ประสิทธิภาพ (Performance)
เครือข่าย (Network)
การกู้ระบบ (Disaster Recovery)
ความลับของผู้ใช้ (User Confidential)
กระบวนการ (Procedure)
สมุดบันทึก (Log book)
การติดต่อ (Contacts)
ระบบทดสอบ (Test Evironment)
นโยบายการเตรียมพร้อมและป้องกัน (Policy)

Improve

โปรแกรมแก้ไขข้อบกพร่อง (Patch)
การฝึกอบรม (Training)
ฐานความรู้ (Knowledge Base)
นโยบายการปรับปรุง (Policy)

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
112 ถนนพหลโยธิน คลองหลวง จังหวัดปทุมธานี 12120
โทรศัพท์ 0-2564-6900 โทรสาร 0-2564-6901..3
http://www.nectec.or.th/ e-mail: info@nectec.or.th

BA801-V2-45
6 มิถุนายน 2545