030523114 Network Security

สาขาวิชาเทคโนโลยีอิเล็กทรอนิกส์ (ต่อเนื่อง)

ภาควิชาเทคโนโลยีวิศวกรรมอิเล็กทรอนิกส์

วิทยาลัยเทคโนโลยีอุตสาหกรรม

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

อาจารย์ ดร.เลอสรรค์ กิรสมุทรานนท์

ครั้งที่ 13 “System Restore”

System Restore

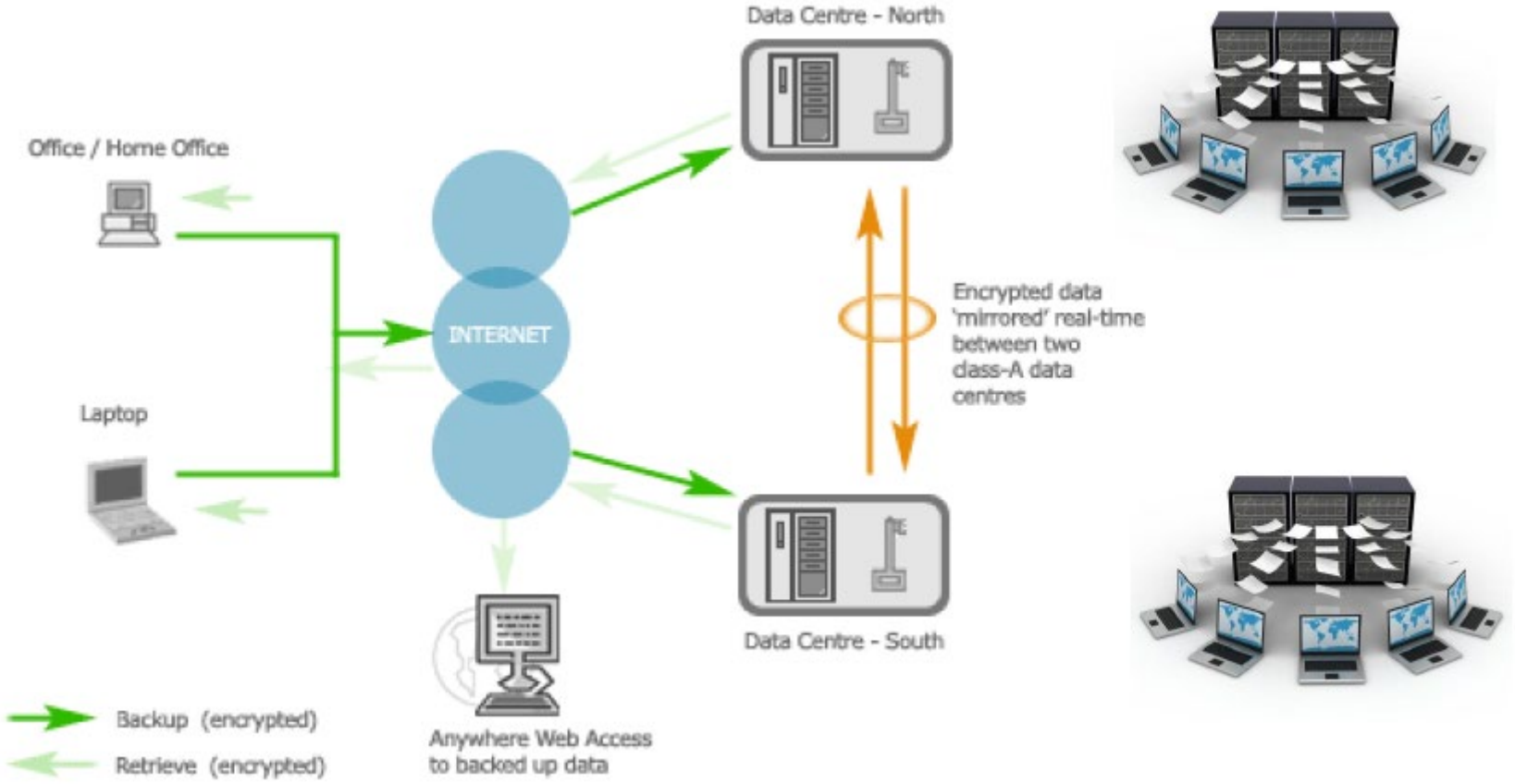
- **Outline**
  - Intro System Restore
  - การเตรียมการสำหรับการกู้คืนระบบ
  - การวิเคราะห์การถูกโจมตี
  - การกู้คืนระบบ (System Recovery)
  - ขั้นตอนหลังจากการกู้คืนระบบ
  - สรุป

Intro
System Restore

- ในปัจจุบันระบบสารสนเทศกลายเป็นหัวใจหลักของระบบธุรกิจส่วนใหญ่ทั้งภาครัฐและเอกชนล้วนนำระบบสารสนเทศมาใช้ในองค์กรอย่างกว้างขวาง
- ปัญหาที่หลายองค์กรกำลังเผชิญอยู่ คือ ปัญหาระบบสารสนเทศไม่สามารถทำงานตามปกติหรือปัญหาระบบสารสนเทศล่ม ทำให้องค์กรไม่สามารถดำเนินธุรกิจธุรกรรมต่าง ๆ ได้ตามปกติ ส่งผลให้องค์กรเกิดความเสียหายได้

System Restore

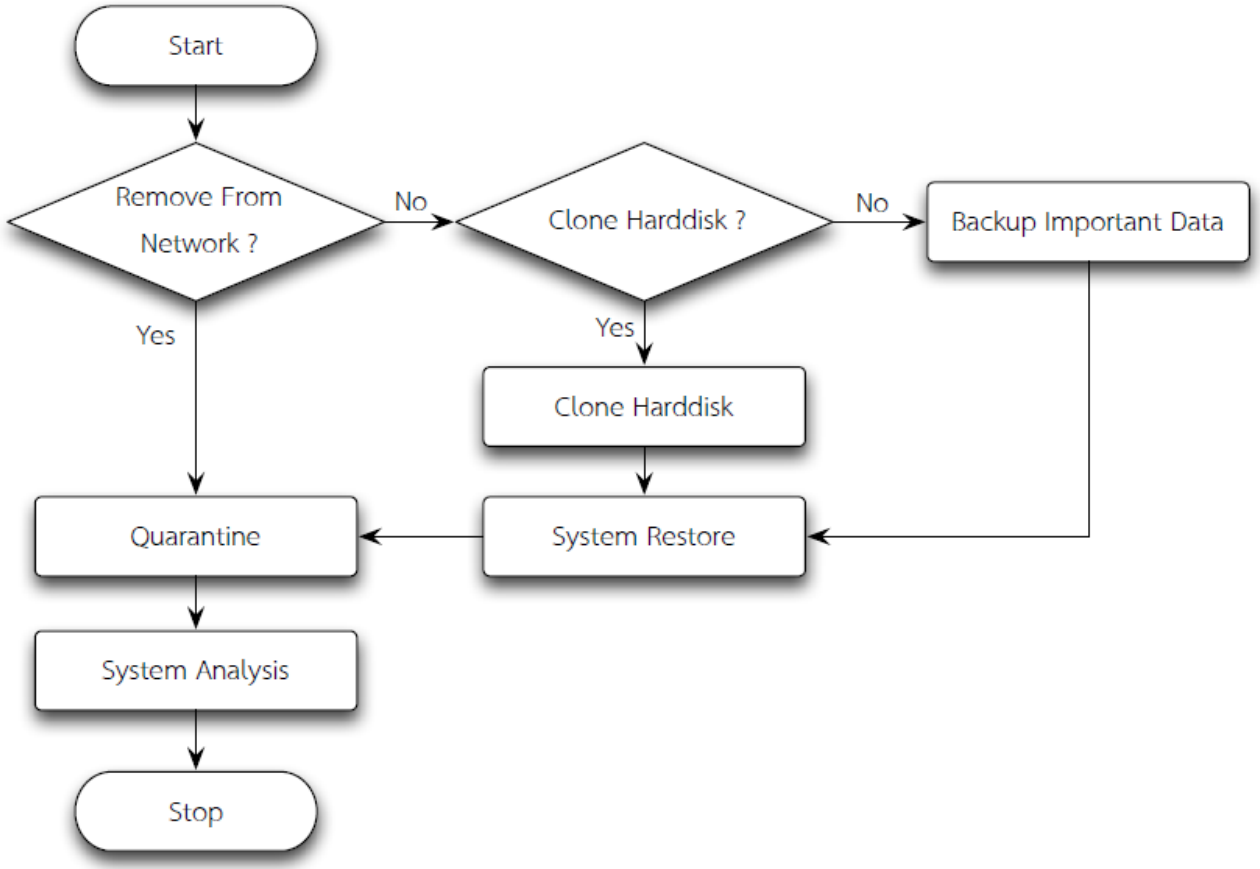
Example : System Infrastructure



System Restore
การเตรียมการสำหรับการกู้คืนระบบ

- มีผลกระทบต่อการใช้งานขององค์กรน้อยที่สุด
- ใช้เวลาในการกู้คืนระบบให้เร็วที่สุด
- เก็บข้อมูลหรือหลักฐานเพื่อไว้สาหรับดำเนินการในทางกฎหมาย
- เก็บข้อมูลเพื่อสำหรับการติดตั้งระบบป้องกันและรักษาความปลอดภัยเพิ่มเติม
- ป้องกันการโจมตีแบบเดิมกับระบบที่ถูกกู้คืนเรียบร้อยแล้ว

System Restore
การเตรียมการสาหรับการกู้คืนระบบ



รูปแสดงขั้นตอนการกู้คืนระบบก่อนการวิเคราะห์

System Restore
การวิเคราะห์การถูกโจมตี

- การตรวจเช็คโพรเซสและเซอร์วิสที่กำลังทำงานอยู่
- การตรวจเช็คสตาร์อัพโฟลเดอร์
- การตรวจเช็ค Scheduled Applications
- การวิเคราะห์ Local Registry
- การตรวจค้นหามัลแวร์และคอร์รัพต์ไฟล์
- การตรวจสอบบัญชีผู้ใช้และบัญชีกลุ่มผู้ใช้
- การตรวจสอบแชร์โฟลเดอร์
- การตรวจสอบพอร์ตที่เปิดไว้
- การตรวจสอบอีเวนต์ล็อกของระบบ ฯลฯ

System Restore
การกู้คืนระบบ (System Recovery)

การคลีนระบบ	การติดตั้งระบบใหม่
เป็นวิธีที่ง่าย ถ้ามีเครื่องมือกำจัดไวรัสที่พร้อมใช้งาน	ขั้นตอนซับซ้อนกว่า โดยเฉพาะถ้าไม่มีเครื่องมือสำหรับแบ็คอัพและกู้คืนระบบก่อนที่จะมีไวรัส
ขั้นตอนน้อยกว่า	ขั้นตอนมากกว่า เพราะต้องเก็บข้อมูล แบ็คอัพ การกำจัดไวรัส สแกน และการกู้คืนระบบ
ใช้รีซอร์สน้อยกว่าในการกำจัดไวรัส	การติดตั้งระบบใหม่ส่วนใหญ่จะใช้เวลาและรีซอร์สมากกว่าในการทำให้ระบบสมบูรณ์
ความเสี่ยงเกี่ยวกับว่าระบบนั้นยังมีมัลแวร์หรือไวรัสอยู่	ความเสี่ยงในการที่มัลแวร์ยังคงอยู่นั้นน้อย

- ควรกำจัดมัลแวร์ออกจากระบบหรือติดตั้งระบบใหม่

System Restore
การกู้คืนระบบ (System Recovery)

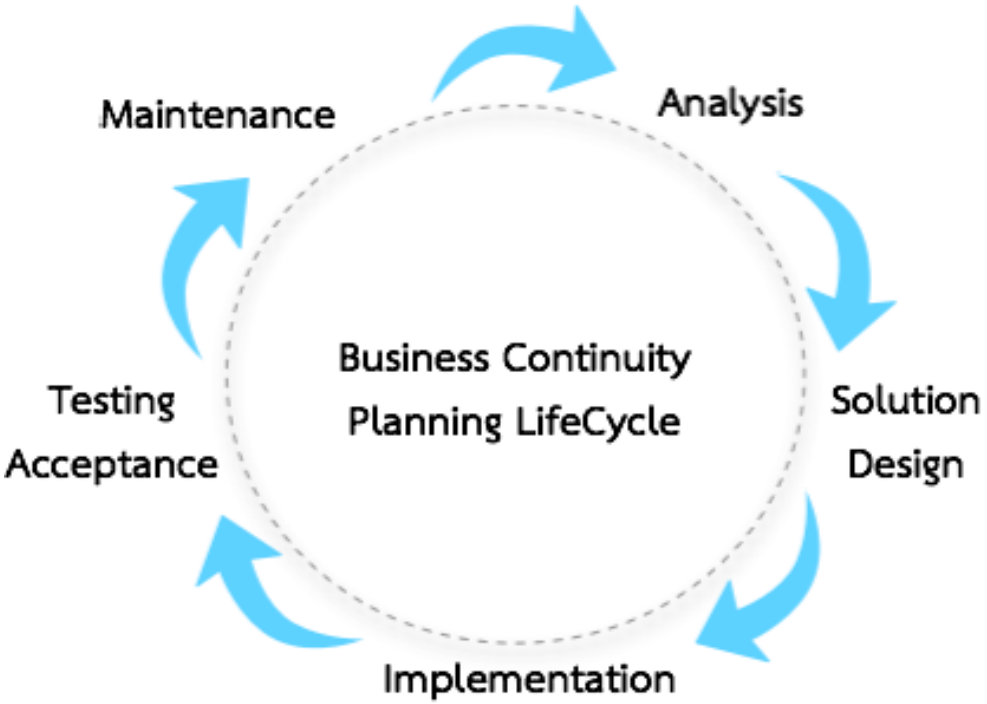
- การกำจัดมัลแวร์ออกจากระบบ ควรเลือกที่จะกำจัดมัลแวร์ออกจากระบบ เฉพาะกรณีที่เราเข้าใจพฤติกรรมของมัลแวร์ และแน่ใจว่าขบวนการกำจัดไวรัสนั้นได้ผลจริง
- การแบ็คอัพไฟล์หรือระบบ
- การกู้คืนข้อมูลจากระบบที่ติดไวรัส ข้อมูลค่าคอนฟิกของระบบปฏิบัติการ, ข้อมูลของแอพพลิเคชัน, ข้อมูลของผู้ใช้
- การติดตั้งระบบใหม่ ติดตั้งจากแบ็คอัพของระบบล่าสุดที่แน่ใจว่าไม่มีไวรัสแน่นอน

System Restore
ขั้นตอนหลังจากการกู้คืนระบบ

- การประชุมเพื่อสรุปสถานการณ์
  - การดำเนินการทางกฎหมายกับผู้ที่บุกรุก
  - รายงานความเสียหาย
  - วิเคราะห์ว่าจุดอ่อนหรือช่องโหว่
  - ข้อเสนอในการปรับเปลี่ยนนโยบายการรักษาความปลอดภัย

Business Continuity Management (BCM)

- องค์ความรู้ทางด้านการบริหารจัดการให้องค์กรสามารถดำเนินธุรกิจได้อย่างต่อเนื่องภายใต้ภาวะวิกฤติ



System Restore

Business Continuity Management (BCM)

- ขั้นตอนที่ 1 : Analysis Phase การวิเคราะห์ปัจจัยเสี่ยงและผลกระทบ
- ขั้นตอนที่ 2 : Solution Design Phase ออกแบบยุทธศาสตร์ในการกู้ข้อมูล
- ขั้นตอนที่ 3 : Implementation Phase นายุทธศาสตร์ที่ออกแบบไว้ทำเป็นแผนปฏิบัติการ
- ขั้นตอนที่ 4 : Testing and Organization Acceptance Phase การทดสอบแผน
- ขั้นตอนที่ 5 : Maintenance Phase เป็นขั้นตอนในการปรับปรุงแผน BCP ในคู่มือ BCP ให้เป็นปัจจุบัน

สรุป

- ถ้าองค์กรมีมาตรการป้องกันที่ดีและมีประสิทธิภาพมากแล้ว โอกาสที่จะถูกโจมตีและที่ต้องกู้คืนระบบนั้นก็น้อยลง อย่างไรก็ตามการไม่ได้วางแผนรับมือกับเหตุการณ์ที่เลวร้ายที่สุดก็อาจเป็นการเพิ่มความเป็นไปได้ที่องศ์กรอาจเผชิญกับความเสียหายขั้นรุนแรงก็ได้ถ้าหากการโจมตีนั้นสำเร็จ

  ทิศทางของการประยุกต์ใช้มาตรฐาน BS 25999 ในเรื่องการจัดทำ BCM และการรับรองผู้เชี่ยวชาญด้าน BCM ของสถาบัน BCI ตามกระแสความต้องการบุคลากรด้าน BCM นั้นมีแนวโน้มที่จะได้รับความนิยมมากขึ้นในอนาคตอันใกล้นี้

Reference

- [1] Pennsylvania State University. Hacking Techniques in Wired Networks (2004). Retrieved July 5, 2010, from http://whitepapers.techrepublic.com.com/abstract.aspx?kw=wired+network+hacking&docid=178151&tag=tr-left
- [2] Security Statistics (2001). Retrieved July 8, 2010, from http://www.computerworld.com/s/article/62002/Security_Statistics_
- [3] Bellovin, S. M. (1989). Security problems in the TCP/IP protocol suite, ACM SIGCOMM Computer Communication Review, vol. 19, pp. 32-48.
- [4] Bellovin, S. (1995). Using the Domain Name System for System Break-ins, Proceeding of the 5th UNIX Security Symposium, pp.199-208.
- [5] Boulanger, A. (1998). Catapults and grappling hooks: The tools and techniques of Information warfare, IBM System Journal, vol. 37, no 1, pp. 106-114.
- [6] CERT® Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks (2000). Retrieved May 20, 2004, from http://www.cert.org/advisories/CA-1998-01.html.
- [7] CERT® Advisory CA-1999-04 Melissa Macro Virus (1999). Retrieved May 20, 2004, from http://www.cert.org/advisories/CA-1999-04.html.
- [8] CERT® Advisory CA-2001-19 “Code Red” Worm Exploiting Buffer Overflow In IIS Indexing Service DLL (2002). Retrieved May 20, 2004, from http://www.cert.org/advisories/CA-2001-19.html.
- [9] CERT® Advisory CA-1999-16 Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind (2000). Retrieved May 20, 2004, from http://www.cert.org/advisories/CA-1999-16.html.
- [10] CERT® Advisory CA-2001-26 Nimda Worm (2001). Retrieved May 20, 2004, from http://www.cert.org/advisories/CA-2001-26.html.