Faisal Syafar
Teknik Elektronika dan TI
Universitas Negeri Makassar

Pengelolaan Kasus Forensik

Komputer Forensik teknologi Informasi

Pra Insiden

- Jenis insiden menurut the information security management :
  - Virus
  - Unauthorized access
  - Pencurian atau kehilangan kepercayaan pada informasi
  - Serangan denial of service pada sistem
  - Korupsi informasi

Persiapan

- Pengunaan beberapa tool untuk mencegah penyusupan dengan deteksi
- Backup sistem
- Kebijakan password
- Kebijakan keamanan sistem
- Lakukan instalasi patch security
- Pergunakan security – auditing tools
- Pelajari sistem lebih lama
- Aktifkan fasilitas logging dan accounting
- Lakukan audit dan pengujian pada sistem secara rutin

Prosedur penanganan insiden

- Bagaimana mengamankan dan menjaga barang bukti
- Dimana dan bagaimana mencari barang bukti
- Daftar yang dipersiapkan untuk laporan menyeluruh
- Daftar orang untuk keperluan pelaporan
- Daftar software yang digunakan
- Daftar ahli

Prosedur penanganan insiden

- Jika ahli forensik tidak dimiliki atau tidak berada ditempat dan terdapat insiden, yang harus dilakukan oleh seorang staff :
  - Membuat image
  - Analisis forensik dilakukan semua dari copy
  - Memelihara rincian media dalam proses

Prosedur penanganan insiden secara sederhana

- Menurut Scott Grace " Computer incident response and computer forensics overview" :
  - Amankan lingkungan
  - Shutting down komputer after finding potential evidence
  - Label barang bukti
  - Dokumentasikan barang bukti
  - Transportasikan barang bukti
  - Dokumentasikan rangkaian penyimpanan

Prosedur penanganan insiden

- Dokumen penanganan insiden dari SANS institute :
  - Semua partisipan menyarankan elemen dan perubahan
  - Proses berjalan dengan banyak perulangan
  - Beberapa masalah disajikan dengan banyak pilihan
  - Setiap partisipan harus menyetujui keseluruhan dokumen

Fase merespon insiden

- Fase 1 : Persipan (42 tindakan)
- Fase 2 : Identifikasi (6 tindakan)
- Fase 3 : Pengisian (17 tindakan)
- Fase 4 : Pembasmian (10 tindakan)
- Fase 5 : Pemulihan (6 tindakan)
- Fase 6 : Tindak lanjut (9 tindakan)

Emergency action card

1. Tetap tenang sehingga terhindari kesalahan fatal
2. Buatlah catatan yang baik dan relevan
3. Beritahu orang yang tepat dan carilah pertolongan
4. Tetapkan kebijakan yang hanya orang – orang terpercaya yang boleh tahu
5. Gunakan jalur komunikasi terpisah dari sistem yang mengalami compromise

Emergency action card

6. Isolasi masalah sehingga tidak bertambah buruk
7. Buat backup sistem
8. Temukan sumber masalah
9. Kembali ke pekerjaan semula setelah backup terjamin dan lakukan restore sistem
10. Belajar dari pengalaman

Pemrosesan Barang Bukti

- Menurut Lori Willer “ Computer forensics”, panduan :
  1. Shut down komputer, dan perlu dipertimbangkan kerusakan proses yang berjalan dibackground
  2. Dokumentasikan konfigurasi hardware dari sistem
  3. Pindahkan sistem komputer ke lokasi yang aman
  4. Buat backup bit dari hard disk dan floppy

Panduan

5. Uji otentifikasi data dari semua penyimpanan
6. Dokumentasikan tanggal dan waktu yang berhubungan dengan file komputer
7. Buat daftar key word pencarian
8. Evaluasi swap file
9. Evaluasi file slack, dari dump memori yang terjadi selama file ditutup
10. Evaluasi unallocated space – erased file

Panduan

11. Pencarian keyword pada file, file slack dan unallocated space
12. Dokumentasikan nama file (atribut tanggal dan file)
13. Identifikasikan anomali file, program dan storage
14. Evaluasi fungsionalitas program untuk mengetahui kegunaannya
15. Dokumentasikan temuan dan software yang dipergunakan
16. Buat copy dari software yang dipergunakan

Tahapan pemrosesan barang bukti

- Menurut Jim Mc Millan, lima tahapam pemrosesan barang bukti :
  - Persiapan
  - Snapshot
  - Transport
  - Pengujian
  - Analisa

Persiapan

- Sterilkan semua media dari virus
- Pastikan semua tool forensik bisa dipergunakan secara resmi
- Periksa kerja semua peralatan lab
- Pilih ahli forensik yang tepat dan mampu memberikan kesaksian dan penjelasan di persidangan

Snapshot

- Foto lingkungan
- Catat rinciannya
- Foto barang bukti
- Dokumentasikan konfigurasi hardware
- Labeli barang bukti sesuai metodologi
- Foto barang bukti lagi setelah dilabeli
- Dokumentasikan apa terjadi

Transport

- Lakukan pengemasan secara aman
- Foto dan dokumentasikan penanganan barang bukti meninggalkan tempat kejadian sampai ke lab pengujian

Pengujian

- Lakukan unpack sesuai metodologi
- Lakukan uji visual dan catat setiap konfigurasi yang tidak semestinya
- Buatlah image hard disk
- Setelah menbuat image simpan barang bukti di tempat aman dan catat
- Lakukan pembuat image kedua

Analisa

- Analisa barang bukti dilakukan secara dua level :
  - Level fisik
  - Level lojik
- Perhitungan rangkaian kepercayaan – chain of evidence

Rangkaian kepercayaan

- Shell (CLI. GUI)
- Command
- Dynamic libraries
- Device driver
- Kernel
- Controller
- Hardware

Terima Kasih

See you next week