IT Forensics

IT Forensics

- IT Forensik adalah cabang dari ilmu komputer tetapi menjurus ke bagian forensik yaitu berkaitan dengan bukti hukum yang ditemukan di komputer dan media penyimpanan digital.
- Komputer forensik juga dikenal sebagai **Digital Forensik** yang terdiri dari aplikasi dari ilmu pengetahuan kepada indetifikasi, koleksi, analisa, dan pengujian dari bukti digital.
- IT Forensik adalah penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk memelihara barang bukti tindakan kriminal.

- **IT Audit** adalah proses kontrol pengujian terhadap infrastruktur teknologi informasi yang memiliki hubungan dengan masalah audit finansial dan audit internal.
- IT Audit ini lebih dikenal dengan sebutan *EDP Auditing* **(Electronic Data Processing)**, yang digunakan untuk menguraikan dua jenis aktifitas yang berkaitan dengan komputer.
- IT Audit sendiri merupakan gabungan dari berbagai macam ilmu, antara lain **Traditional Audit**, **Manajemen Sistem Informasi**, **Sistem Informasi Akuntansi**, **Ilmu Komputer**, dan **Behavioral Science**. IT Audit bertujuan untuk meninjau dan mengevaluasi faktor-faktor ketersediaan (availability), kerahasiaan (confidentiality), dan keutuhan (integrity) dari sistem informasi organisasi.

Audit around computer

1. Dokumen sumber tersedia dalam bentuk kertas (bahasa non-mesin), artinya masih kasat mata dan dilihat secara visual.
2. Dokumen-dokumen disimpan dalam file dengan cara yang mudah ditemukan
3. Keluaran dapat diperoleh dari daftar yang terinci dan auditor mudah menelusuri setiap transaksi dari dokumen sumber kepada keluaran dan sebaliknya.

Audit Through the computer

1. Sistem aplikasi komputer memroses input yang cukup besar dan menghasilkan output yang cukup besar pula, sehingga memperuas audit untuk meneliti keabsahannya.
2. Bagian penting dari struktur pengendalian intern perusahaan terdapat di dalam komputerisasi yang digunakan.

Keunggulan

Audit around computer

1. Pelaksanaan audit lebih sederhana.
2. Auditor yang memiliki pengetahuan minimal di bidang komputer dapat dilihat dengan mudah untuk melaksanakan audit.

Audit Through the computer

1. Auditor memperoleh kemampuasn yang besar dan efketif dalam melakukan pengujian terhadap sistem komputer.
2. Auditor akan merasa lebih yakin terhadap kebenaran hasil kerjanya.
3. Auditor dapat melihat kemampuan sistem komputer tersebut untuk menghadapi perubahan lingkungan.

Elemen Kunci IT Forensics

- ✓ Identifikasi
- ✓ Penyimpanan Bukti Digital
- ✓ Analisa Bukti Digital, Pengambilan, Pemrosesan, dan Interpretasi
- ✓ Presentasi Bukti Digital

Prosedur IT Audit

- **Kontrol Lingkungan**
  1. Apakah kebijakan keamanan (security policy) memadai dan efektif ?
  2. Jika data dipegang oleh vendor, periksa laporan ttg kebijakan dan prosedural yg terikini dari external auditor
  3. Jika sistem dibeli dari vendor, periksa kestabilan financial
  4. Memeriksa persetujuan lisen (license agreement)
- **Kontrol Keamanan fisik**
  1. Periksa apakah keamanan fisik perangkat keras dan penyimpanan data memadai
  2. Periksa apakah backup administrator keamanan sudah memadai (trained,tested)
  3. Periksa apakah rencana kelanjutan bisnis memadai dan efektif
  4. Periksa apakah asuransi perangkat-keras, OS, aplikasi, dan data memadai
- **Kontrol keamanan logical**
  1. Periksa apakah password memadai dan perubahannya dilakukan regular
  2. Apakah administrator keamanan memprint akses kontrol setiap user

Contoh

- **Internal IT** Deparment Outputnya Solusi teknologi meningkat, menyeluruh & mendalam dan Fokus kepada global, menuju ke standard2 yang diakui.

- **External IT** Consultant Outputnya Rekrutmen staff, teknologi baru dan kompleksitasnya Outsourcing yang tepat dan Benchmark / Best-Practices

Lembar Kerja IT Audit

- **Stakeholders:** Internal IT Deparment, External IT Consultant, Board of Commision, Management, Internal IT Auditor, External IT Auditor
- **Kualifikasi Auditor:** Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA), Certified Information Systems Security Professional (CISSP), dll.
- **Output Internal IT:** Solusi teknologi meningkat, menyeluruh & mendalam, Fokus kepada global, menuju ke standard-standard yang diakui.

- **Output External IT:** Rekrutmen staff, teknologi baru dan kompleksitasnya, Outsourcing yang tepat, Benchmark / Best-Practices.
- **Output Internal Audit & Business:** Menjamin keseluruhan audit, Budget & Alokasi sumber daya, Reporting.

IT Audit Tools (Software)

- **ACL**

  sebuah software TABK *(TEKNIK AUDIT BERBASIS KOMPUTER)* untuk membantu auditor dalam melakukan pemeriksaan di lingkungan sistem informasi berbasis komputer atau Pemrosesan Data Elektronik.

- **Picalo**

  Powertech Compliance Assessment Picalo bekerja dengan menggunakan GUI Front end, dan memiliki banyak fitur untuk ETL sebagai proses utama dalam mengekstrak dan membuka data,

  kelebihan utamanya adalah fleksibilitas dan front end yang baik hingga Librari Python numerik

- **Nipper**

  Nipper merupakan audit automation software yang dapat dipergunakan untuk mengaudit dan mem-benchmark konfigurasi sebuah router.

- **Nessus**

  Nessus merupakan sebuah vulnerability assessment software, yaitu sebuah software yang digunakan untuk mengecek tingkat vulnerabilitas suatu sistem dalam ruang lingkup keamanan yang digunakan dalam sebuah perusahaan

- **Metasploit**

  Metasploit Framework merupakan sebuah penetration testing tool, yaitu sebuah software yang digunakan untuk mencari celah keamanan.

- **NMAP**

  software untuk mengeksplorasi jaringan, banyak administrator sistem dan jaringan yang menggunakan aplikasi ini menemukan banyak fungsi dalam inventori jaringan, mengatur jadwal peningkatan service, dan memonitor host atau waktu pelayanan.

- **Wireshark**

  Wireshark bisa mengcapture data dan secara interaktif menelusuri lalu lintas yang berjalan pada jaringan komputer, berstandartkan de facto dibanyak industri dan lembaga pendidikan.


Thank You