FORENSIK KOMPUTER SEBUAH PENANGANAN KEJAHATAN KOMPUTER

Oleh :
Singgih Sudarto, S.Kom, M.MSi

ABSTRAK

Pemakaian Jaringan komputer untuk operasional perusahaan sudah merupakan suatu kebutuhan, sama seperti penggunaan ATM pada pelayanan perbankan untuk para pelanggannya. Akan tetapi biasanya jaringan yang dikembangkan oleh perusahaan tidak didukung dengan fasilitas keamanan yang memadai, seperti yang telah disurvey oleh Ernest dan Young tentang keamanan informasi, bahwa 66% responden mengatakan security dan privacy merupakan penghambat besar penggunaan electronic commerce. Analisis Forensik Komputer merupakan usaha untuk mendapatkan bukti-bukti legal terhadap terjadinya suatu insiden, agar bukti-bukti tersebut dapat dijadikan pendukung untuk tindakan lanjut terhadap tindak kejahatan komputer.

1. PENDAHULUAN

Kemajuan teknologi informasi telah mengubah tatanan dunia begitu dratis baik secara ideologi, politik maupun sosial budaya. Begitu pula dengan kejahatan yang dilakukan oleh para 'petualang-petualang' kejahatan (para kriminal). Serangan-serangan pada komputer khususnya jaringan komputer semakin membuat perusahaan atau para pemilik perusahaan khawatir dan was-was terhadap sumber daya yang dimilikinya. Padahal penggunaan jaringan komputer baik intranet maupun internet merupakan kebutuhan yang harus ada guna mendukung efektif dan efisiennya operasional perusahaan, akan tetapi di sisi lain kejahatan komputer semakin maju yang ditandai dengan semakin canggihnya para cracker melakukan penyerangan terhadap komputer-komputer yang ada. Dan kejahatan komputer ini dapat dilakukan oleh para cracker dimanapun, bisa-bisa mereka menyerang hanya berjarak beberapa meter atau bahkan puluhan kilometer dengan hasil yang sama.

Dalam sebuah survey oleh Ernest and Young tentang Information Security diperoleh informasi bahwa 66% responden mengatakan security dan privacy merupakan penghambat lebih besar penggunaan electronic commerce.

Kejahatan apapun bentuknya merupakan hal yang harus dihadapi, demikian pula kejahatan yang berkaitan dengan serangan terhadap komputer, perlu penanganan yang sistematis agar

diperoleh pencegahan dan penanganan yang tuntas. Forensik komputer secara awam dapat dianalogikan sebagaimana penanganan yang dilakukan jika terjadi suatu insiden atau kejadian kejahatan di suatu lokasi.

Saat sebuah insiden tindak kejahatan atau kecelakaan terjadi, pihak berwajib segera mengamankan lokasi kejadian. Kemudian mereka berusaha mengumpulkan bukti-bukti yang diperlukan dari tempat kejadian perkara (TKP) yang dapat menghubungkannya dengan pelaku kejahatan, motif, korban, maupun hal-hal yang berkaitan dengan sebab peristiwa tersebut.

Mereka mencoba merangkaikan benang merah yang menghubungkan kejadian tersebut, yang biasanya dilakukan oleh detektif maupun ahli forensik.

Teknis perlakuan di atas dapat disinonimkan dengan saat terjadinya insiden pada keamanan komputer. Bila terjadi suatu penyusupan atau perusakan data, maka akan diusahakan dengan mencari dan mendeteksi "jejak-jejak" yang tertinggal dengan melakukan analisa untuk melacak kejadian tersebut. Begitu pula bila diduga muncul gejala-gejala yang menampakkan adanya usaha penyusupan, seperti halnya polisi yang mencoba melakukan pemeriksaan bila dicurigai telah terjadi suatu t indak kejahatan. Proses-proses t ersebut dalam lingkungan komputer biasa dikenal dengan istilah analisis forensik/software forensic

2. DEFINISI

Komputer forensik adalah penyelidikan dan analisis komputer untuk menentukan adanya potensi bukti legal yang tertinggal untuk dapat digunakan sebagai pendukung tindakan berikutnya. Seperti diketahui bersama bahwa bertahun-tahun yang lalu, kebanyakan bukti dikumpulkan pada kertas. Saat ini, kebanyakan bukti bertempat pada komputer sehingga membuatnya lebih rapuh, karena sifat alaminya. Bukti dalam bentuk data elektronik bisa muncul dalam bentuk dokumen, informasi keuangan, e-mail, *job schedule*, log, atau transkripsi *voice-mail*.

Berikut beberapa definisi dari komputer forensic menurut beberapa pengamat, antara lain :

- Definisi sederhana menurut James J. Dougherty : "Penggunaan sekumpulan prosedur untuk melakukan pengujian secara menyeluruh suatu sistem komputer dengan mempergunakan software dan tool untuk mengekstrak dan memelihara barang bukti tindakan kriminal"
- Menurut Judd Robin, seorang ahli komputer forensik: "Penerapan secara sederhana dari penyelidikan komputer dan teknik analisisnya untuk menentukan bukti-bukti hukum yang mungkin"

- New Technologies memperluas definisi Robin dengan: "Komputer forensik berkaitan dengan pemeliharaan, identifikasi, ekstraksi dan dokumentasi dari bukti-bukti komputer yang tersimpan dalam wujud informasi magnetik"

3. KECENDERUNGAN INSIDEN

Jaringan komputer digunakan oleh perusahaan dan juga berbagai organisasi untuk melaksanakan berbagai jenis operasional kegiatan setiap harinya. Dengan menggunakan jaringan sejumlah sumberdaya termasuk data dapat digunakan secara bersama dengan sangat efisien. Umumnya kerjasama atau penggunaan sumberdaya secara bersama dengan menggunakan jaringan tidak dirancang dan diimplementasikan dengan mem-berikan fasilitas keamanan yang memadai, sehingga masalah-masalah keamanan muncul kemudian, hal ini tentu mempunyai dampak pada biaya recovery yang sangat mahal untuk menangani dan memperbaiki kembali sumberdaya yang telah rusak atau bahkan hancur/lenyap.

Kebanyakan jaringan komputer yang digunakan pada perusahaan bekerja dengan menggunakan prinsip client – server, dimana pegawai/user menggunakan workstation untuk berhubungan dengan server untuk berbagi informasi. Server pada prinsipnya sebagai sebuah "hub" yang menyimpan semua informasi perusahaan, dan kecen-derungannya para crackers selalu menargetkan pertama kali pada server yang dimiliki oleh perusahaan. Apabila seorang crackers telah berhasil mengakses server, sisa penyerangan berikutnya semakin mudah dilakukan. Berikut lembaga-lembaga atau organisasi yang seringkali menjadi sasaran para crackers :

Financial institutions dan banks

Pada lembaga keuangan dan perbankan para cracker biasanya melakukan penyerangan melalui pengacauan data moneter/simpanan dana, telah banyak bank yang menjadi sasaran dengan cara ini. Dan biasanya kejadian yang dilakukan oleh para cracker ini oleh bank yang bersangkutan tidak dipublikasikan. Hal ini masuk akal karena bank / lembaga keuangan yang bersangkutan khawatir akan kehilangan kepercayaan dari para nasabahnya.

Internet service providers

Server ISP umumnya mudah diakses melalui internet, sehingga dalam banyak kasus para Jasa Pelayanan Internet (internet service provider) menjadi sasaran mudah para cracker. Di samping itu

para Jasa Pelayanan Internet juga memiliki akses ke Jaringan fiber optic yang lebih besar, sehingga dapat digunakan oleh para cracker mengambil sejumlah besar data melalui internet. Jasa Pelayanan Internet yang besar biasanya juga memiliki database data-data penting tentang para pelanggannya, seperti informasi tentang kerahasiaan user seperti nomor kartu kredit, alamat dan informasi-informasi penting lainnya.

Pharmaceutical companies

Para mafia obat-obat terlarang biasanya menjadikan perusahaan-perusahaan farmasi sebagai sasaran utama dari usaha mereka. Mereka memanfaatkan keahlian cracker atau sekelompok cracker untuk mendapatkan data-data mengenai farmasi atau obat-obat yang mereka butuhkan atau mengenai data-data penelitian dan pengembangan farmasi.

Government and defense agencies

Pemerintahan dan agen-agen pertahanan Amerika Serikat beberapa tahun belakangan ini benar-benar telah menjadi korban penyerangan para cracker melalui internet. Hal ini berkitan dengan anggaran dan policy terhadap keamanan informasi yang sangat rendah, sehingga keamanan informasi menjadi sesuatu yang sangat mudah diserang oleh para cracker.

Contractors to various goverment agencies

Meskipun para cracker sadar tentang keamanan yang dimiliki oleh para kontraktor / supplier pertahanan, akan tetapi mereka tetap menjadikan supplier pertahanan ini sebagai salah satu sasarannya untuk mendapatkan data-data militer yang khusus dan rahasia. Setelah data diperoleh kemudian mereka menginformasikan ke kelompok yang lain. Meskipun kasus ini sangat sedikit akan tetapi aktivitas ini sangat mengkhawatirkan

Multinational corporations

Sasaran utama berikutnya adalah perusahaan Multinasional yang biasanya mempunyai kantor cabang yang ada di berbagai lokasi di belahan dunia. Umumnya mereka memiliki jaringan komputer yang besar yang dibangun untuk para pekerjanya. Jaringan ini dibangun/dikembangkan dengan fungsi agar para pekerja perusahaan dapat menggunakan informasi perusahaan secara bersama dengan efisien. Seperti pada perusahaan farmasi, perusahaan multinasional beroperasi

dengan menggunakan jaringan elektronik, berhubungan dengan industri hardware - software dan menghabiskan jutaan dollar untuk penelitian dan pengembangan teknologi baru. Data-data ini sangat menarik bagi para kompetitor, sehingga keadaan ini akan memunculkan ide kompetitor untuk mencoba mendapatkan data tersebut melalui para cracker.

4. PENCEGAHAN INSIDEN DAN RESPON PASCA INSIDEN

a. Jenis insiden

Berdasarkan survey pada bulan Desember 2000 yang dilakukan oleh James J. Dougherty yang dilansir dalam bukunya berjudul "Computer Forensic", ancaman terbesar dari jaringan komputer berasal dari kalangan yang terdiri dari : 68% karyawan, 17% hacker, 9% kompetitor, dan 6% customer. Artinya unsur yang terlibat langsung pada operasional yang ada di dalam internal perusahaan jangan sampai diabaikan dalam melakukan proses pencegahan. Karena dari data penelitian, personal internal merupakan penyebab terbesar dari munculnya kesalahan / kejahatan komputer. Oleh karena itu para pimpinan organisasi harus mewaspadai keadaan ini, sehingga organisasi dalam melakukan perlindungan jaringannya harus baik dari dalam maupun dari luar.

Berikut jenis insiden pada komputer yang sering terjadi :

- Virus
- *Unauthorized access*
- Pencurian atau kehilangan kepercayaan pada informasi
- Serangan d*enial of service* pada sistem
- Korupsi informasi

b. Pencegahan serangan

Untuk menghadapi penyusupan dan serangan menurut John R Dysart dalam buku "Learning from what intruders leave behind" dapat dilakukan persiapan berikut :

- Melakukan pendeteksian guna mencegah terjadinya penyusupan dengan meng-gunakan alat-alat (tools) deteksi. Amati aktivitas pada port-port yang biasanya ber-kaitan dengan *trojan, backdoor, denial of service* tool, dan yang serupa. Pergunakan tool semacam *Tripwire* untuk

mengamati perubahan pada sistem, yang me-mungkinkan membuat *snapshot* sistem Pemeriksaan lainnya adalah mode *promiscous* pada network card.

- Gunakan backup sistem yang baik untuk bisa melakukan *restore* data sebelum penyusupan.
- Jika diasumsikan penyusup mempergunakan *sniffer* untuk menangkap password, maka perlu diterapkan kebijakan password yang tepat, seperti penggunaan system password *one time password. Practical Unix & Internet Security,* oleh Simson Garfinkel dan Gene Spafford, merekomendasikan "Jangan mengirimkan *clear text password* yang bisa dipergunakan kembali lewat koneksi jaringan. Pergunakan *one-time password* atau metode rahasia "
- Suatu kebijakan keamanan harus diterapkan untuk menangani insiden yang muncul, dan harus cukup mudah diimplementasikan dan dimengerti oleh setiap orang . Misalkan *capture* tampilan, jangan matikan komputer, lakukan *shutdown* normal, copot modem, labeli semua alat, dan tulis semua yang mungkin. Harus ditentukan *standard operating procedures* (SOP) di mana akan memastikan tidak ada kontaminasi dengan data lain atau data kasus sebelumnya.
- Lakukan instalasi *patch* security dari vendor sistem operasi atau aplikasi.
- Matikan semua service jaringan yang tidak dipergunakan, dan pergunakan security / auditing tool
- Luangkan lebih banyak waktu untuk mempelajari sistem anda dengan lebih baik
- Aktifkan fasilitas *logging* dan *accounting*
- Lakukan audit dan pengujian pada sistem secara rutin

Banyak organisasi tidak hanya mengabaikan penerapan keamanan untuk melindungi jaringan dan data mereka, tetapi juga tidak siap untuk menangani penyusupan dan insiden [Dorothy A. Lunn, 2001]. Organisasi harus menerapkan perencanaan respon dan pelaporan insiden, serta membuat team untuk menanganinya. Hal itu bisa juga dilakukan dengan menyewa ahli forensik dari perusahaan keamanan. Saat diduga terdapat kecurigaan *compromise* keamanan atau tindakan ilegal yang berkaitan dengan komputer, maka akan merupakan suatu hal yang penting untuk melakukan langkah-langkah dalam menjamin perlindungan terhadap data pada komputer atau media penyimpanan. Penyimpanan data diperlukan untuk menentukan *compromise* tingkat keamanan dan letak bukti-bukti yang mungkin berkaitan dengan tindakan ilegal.

c. Penanganan Dan Respon Pada Insiden

Respon awal pada penanganan insiden bisa sangat mempengaruhi analisis laboratorium. Orang-orang tidak berkepentingan tidak seharusnya dibiarkan di sekitar tempat kejadian perkara. Perlu adanya dokumentasi mengenai perlindungan barang bukti, analisis dan laporan penemuan.

Suatu kebijakan dan prosedur penanganan insiden sangat penting untuk setiap organisasi. Hal-hal yang harus diingat adalah :

- Bagaimana untuk mengamankan atau menjaga barang bukti, baik dengan membuat copy image dan mengunci yang asli, sampai kedatangan ahli forensik
- Di mana atau bagaimana untuk mencari barang bukti, baik itu di drive lokal, backup sistem, komputer atau laptop
- Daftar yang harus dipersiapkan untuk laporan menyeluruh
- Daftar orang untuk keperluan pelaporan, pada suatu situasi tertentu
- Daftar software yang disarankan digunakan secara internal oleh penyelidik
- Daftar ahli yang disarankan untuk konsultasi

Tidak semua perusahaan memiliki ahli forensik, kalau pun ada mereka tidak selalu berada di tempat. Sehingga pada saat terjadi insiden staf harus terlatih sekurang-kurangnya :

- Membuat image, sehingga yang asli tetap terjaga
- Analisis forensik dilakukan semua dari copy
- Memelihara rincian media dalam proses

Respon awal pada keamanan komputer bisa jadi lebih penting daripada analisis teknis selanjutnya dari sistem komputer, karena dampak tindakan yang dilakukan oleh tim penanganan insiden. Dalam suatu kejadian yang dicurigai sebagai insiden komputer, harus ada perlakuan secara berhati-hati untuk menjaga barang bukti dalam keadaan aslinya. Meski kelihatan sesederhana melihat file pada suatu sistem yang tidak akan menghasilkan perubahan media asli, membuka file tersebut akan mengakibatkan perubahan. Dari sudut pandang legal, hal tersebut tidak lagi menjadi bukti orisinil dan tidak bisa diterima oleh proses administratif hukum.

Tiap organisasi harus memiliki suatu tim penanganan insiden. Tim harus menulis prosedur penanganan insiden. Prosedur sederhana untuk mengamankan suatu insiden komputer :

1. Amankan lingkungan
2. *Shutting down* komputer

3. Label barang bukti
4. Dokumentasikan barang bukti
5. Transportasikan barang bukti
6. Dokumentasi rangkaian penyimpanan

Berikut adalah dokumen penanganan insiden yang populer dari SANS Insititute. Ini merupakan dokumen konsensus di mana:

- Semua partisipan menyarankan elemen dan perubahan
- Proses berjalan dengan banyak perulangan
- Beberapa masalah disajikan dengan banyak pilihan
- Setiap partisipan harus menyetujui keseluruhan dokumen

Hasilnya adalah panduan untuk persiapan dan respon pada insiden keamanan. Terdiri dari 44 halaman, menyatakan 90 tindakan dalam 31 langkah dan 6 fase. Di sini ditunjukkan bagaimana respon pada jenis insiden tertentu seperti *probing*, spionase, dan lainnya. 6 Fase tersebut adalah:

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

Salah satu bagian dari dokumen yang bisa dipergunakan perusahaan yang belum siap menghadapi insiden adalah *Emergency Action Card,* berupa sepuluh langkah berikut:

1. Tetap tenang sehingga menghindari kesalahan fatal
2. Buatlah catatan yang baik dan relevan: siapa, apa, bagaimana, kapan, di mana, mengapa
3. Beritahu orang yang tepat dan carilah pertolongan, mulai dari koordinator keamanan dan manajer
4. Tetapkan kebijakan orang-orang terpercaya yang boleh tahu
5. Gunakan jalur komunikasi terpisah dari sistem yang mengalami *compromise*
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

Beberapa aspek yang bisa dipelajari untuk meningkatkan kemampuan penyelidikan :

- Lakukan pemeriksaan ulang dengan tool yang berbeda sehingga cukup memberikan keyakinan
- Salah satu hal yang tersulit adalah berusaha tetap obyektif selama penyelidikan. Berhentilah sebentar dan periksalah kenyataan yang ada untuk meyakinkan anda cukup beralasan. Perlu diingat pekerjaan ini berkaitan dengan mengumpulkan semua bukti yang tersedia bukan hanya bukti yang mendukung penuntutan
- Yakinkan langkah-langkah anda disetujui oleh pihak manajemen dan staf hukum.
- Kaitkan barang bukti dengan hardware tertentu
- Buatlah log tertulis untuk menjamin penyelidikan mengikuti langkah-langkah yang logis dan mampu menulis laporan yang akurat nantinya
- Gunakan *capture full screen*
- Backup barang bukti
- Kumpulkan juga barang bukti pada tempat terpisah

5. KESIMPULAN

Komputer forensik menjadi topik yang hangat dalam dunia keamanan informasi. Memiliki perencanaan penanganan insiden dan melindungi barang bukti dalam suatu komputer adalah krusial. Terdapat peningkatan kepedulian pada keamanan, privacy dan masalah-masalah penyelidikan, tetapi begitu juga tindak kejahatan yang terjadi. Teknologi-teknologi yang baru seperti komunikasi wireless akan terus berkembang, yang mana akan memunculkan ancaman baru pada industri keamanan, termasuk komputer forensik dan penanganan insiden.

6. DAFTAR PUSTAKA

Dorothy A. Lunn, "Computer Forensic – An Overview", SANS Institute, 2001

Dan Farmer & Wietse Venema, "Computer Forensic Analysis : An Introduction", Doctor Dobb's Journal, 2000

Firrar Utdirartatmo, "Tinjauan analisis forensic dan kontribusinya pada keamanan komputer", ITB, 2001

James J. Dougherty, "Computer Forensics", SANS Institute, 2001

John D. Dysart, "Learning from what intruders leave behind", SANS Institute, 2000