MAKALAH

Kejahatan di Internet

Oleh:

James Situmorang

2000

KEJAHATAN DI INTERNET

Oleh: James R. Situmorang

Pendahuluan

Tak terhitung lagi berita baik yang datang bersama internet. Pebisnis makin yakin internet mendatangkan kemudahan dan keuntungan baru dalam berbisnis internet juga memungkinkan para eksekutif berkomunikasi dan bertransaksi bisnis secara mobile : di rumah, di mobil, di mana-mana. Internet membuat roda perusahaan berjalan lebih efisien dan catatan keuntungan banyak perusahaan meningkat dari tahun ke tahun.

Namun, seperti lazimnya perubahan teknologi yang mengakibatkan perubahan besar, selain membawa berita baik, hal ini juga diiringi sejumlah ekses. Misalnya, makin banyak orang mencemaskan bentuk kejahatan jenis baru yang juga menggunakan sarana internet. Hal ittu makin lama makin mengancam aktivitas dunia bisnis, lebih-lebih lagi yang kehidupan bisnisnya bergantung pada sarana internet. Ia harus terus menerus waspada setiap detik kemungkinan dirinya diserang kejahatan yang juga menggunakan sarana internet atau lebih popular dengan sebutan *cybercrime*

Macam-macam Cybercrime

Dos hanyalah salah satu jenis dari cybercrime, diluar itu masih banyak jenis cyber crime yang harus dihadapi pelaku bisnis berbasis internet. Menurut Edmon Makarim, staf pengajar Fakultas Hukum Universitas Indonesia, cybercrime pada dasarnya adalah satu pindak pidana yang berkenaan dengan cyberspace, baik yang menyerang fasilitas umum didalam cyberspace maupun kepemilkan seseorang di cyberspace. Bentuk konkretnya bisa berupa penyebaran virus, hacker yang menjebol system komputer milik orang lain

dan melakukan tindakan melawan hukum. "Jadi, intinya adalah penyerangan dicontent, computing system dan communication system milik orang lain atau umum, ujar Edmon.

Sementara itu dalam ruang lingkup transaksi elektronik atau e-commerce menurut Edmon, segala tindakan yang menghambat dan mengatas namakan orang lain dalam perdagangan itu dapat dimasukan dlam cybercrime. " misalnya : sudah ada kunci atau password, tetapi kuncinya dibobol memperoleh nama domain tanpa hak atau penyalahgunaan kartu kredit milik orang lain di internet itupun cybercrime", ungkap Edmon.

Saat ini kejahatan internet memang harus sangat diwaspadai. Harus diingat bahwa kejahatan ini berbeda dengan kejahatan lain umumnya cybercrime dap[at dilakukan tanpa mengenal batas territorial dan tidak diperlukan interaksi secara langsung antara pelaku kejahatan dan korban kejahatan, misalnya seseorang yang berada di AS cukup bermodalkan komputer dan akses internet dapat merusak jaringan system komputer milik sebuah bank di Indonesia ataupun mencuri kode aksesnya, sekaligus melakukan kejahatan lainnya. Bisa dipastikan pula dengan sifatnya yang global semua negara yang melakukan kegiatan internet hampir pasti akan terimbas perkembangan cybercrime.

Lantas aksi cybercrime apa saja di Indonesia yang menyusahkan kegiatan bisnis berbasis di Indomesia ? Menurut RM.Roy Surya, staf pengajar Universitas Gajah Mada, saat ini kasus-kasus cybercrime yang sangat banyak terjadi di Indonesiasetidaknya ada 3 jenis berdasarkan modusnya, Pertama, pencurian nomor-nomor kartu kredit yang pelakunya disebut carder. Kedua adalah hacking yaitu memakai, memodifikasi, atau merusak homepage atau situs milik orang lain yang pelakunya disebut hacker. Ketiga,

menyerang situs atau email milik orang lain dengan mengirimkan virus, bom email, spaming, ujar Roy.

Carder, Hacker dan Virus

Bagi para pelaku berbasis internet, 3 modus utama cybercrime yang sering terjadi di Indonesia yaitu penyalahgunaan kartu kredit milik orang lain di internet, hackering dan pengiriman virus memang sangat merugikan. Romzy Alkraterie, wakil ketua bidang informatika Kamar Dagang Indonesia, menjelaskan bahwa penyalahgunaan kartu kredit milik orang lain di internet merupakan kasus cybercrime terbesar yang berkaitan dengan dunia bisnis internet di Indonesia. " kasus pembobolan kartu kredit di Indonesia betul-betul perbuatan kriminal", ungkap Romzy. Artinya, menurut Romzy, perbuatan seperti itu tidak bisa disebut perbuatan iseng, kalau ketahuan harus bisa dihukum.

Penyalahgunaan kartu kredit milik orang lain di internet memang tidak rumit, bisa secara fisik maupun secara online. Secara fisik artinya, nama dan nomor kartu kredit seseorang bisa di peroleh melalui restaurant, pusat perbelanjaan atau mall, hotel atau segala tempat orang melakukan pembayaran melalui kartu kredit. Nama dan nomor kartu kredit orang lain yang sudah diperoleh inilah yang kemudian ketika melakukan pembayaran atau transaksi finansial di internet, misalnya membeli barang di sebuah situs toko online.

Kini bahkan berbagai nama dan nomor kartu kresit dapat diperoleh di warnet-warnet yang menawarkan secara terbuka dan cuma-cuma. Bursa tukar menukar nomor kartu kredit yang bisa dicuri diam-diam juga sudah terjadi. Jika sudah memperoleh nomor kartu kredit itu, pengguna kartu kredit tidak sah ini tinggal menulis aplikasi

pembelian barang, memasukkan nomor kartu kredit dan meminta dikirim ke tempat sesuai yang dikehendaki pengguna illegal itu. Besarnya nilai hasil curian dan kartu kreditpun bisa mencapai ribuan dollar Amerika Serikat.

Roy mensinyalir hal itu banyak dilakukan oleh kalangan mahasiswa yang lebih melek internet daripada lapisan masyarakat yang lain. "Memang kalangan mahasiswa banyak yang melakukan itu, mereka bisa mendapatkan handphone, laptop, jam tangan dengan tanpa membayar alias yang membayar orang yang memilki kartu kredit itu, tutur Roy.

Modus cybercrime lainnya sering kali mengganggu aktivitas pelaku bisnis yang menggunakan sarana internet di Indonesia adalah masalah hacking. Sebutan hacker sering ditujukan bagi seseorang ahli komputer tetapi menggunakan keahliannya untuk mengganggu atau merusak situs-situs milik orang lain. Menurut Roy, hacking atau tindakan orang merusak situs atau homepage milik perusahaan-perusahaan dan lembaga-lembaga pemerintah, kini sering terjadi di Indonesia.

Modus cybercrime ketiga yang juga mengganggu bisnis berbasis internet di Indonesia adalah mengirim virus ke situs-situs perusahaan. Modus yang paling sering terjadi adalah mengirim virus melalui email.

Tiadanya Cyberlaw

Bagi sebagian pelaku bisnis yang memanfaatkan sarana internet, tiadanya cyberlaw atau regulasi dunia virtual di Indonesia adalah penyebab utama makin merajalelanya tindakan cybercrime di Indonesia. Cyberlaw yang melindungi hak-hak konsumen, hak pribadi , hak kekayaan intelektual, hukum komersial, dan keamanan yang

ada di Indonesia masih sebatas konsep. Perjalanannya masih jauh sehingga mewujudkan menjadi hukum positif bisnis internasional se Indonesia. Belum ada produk peraturan perundangan khusus yang menjadi dasar hukum aturan main bisnis internet di Indonesia, padahal bisnis internet di Indonesia sendiri sudah terlanjur bergulir dan terus berkembang.

Menurut Edmon Makarim, cyberlaw kini belum dipunyai Indonesia, tetapi jika melihat ketentuan pidana umum yang ada di Indonesia, sebenarnya bisa juga diterapkan untuk kasus-kasus cybercrime. "Misalnya untuk kasus pembajakan program via internet dengan cara mendownload program tanpa memilki lisensi. Itu bisa dikenai pasal undang-undang hak cipta ", jelas Edmon. Dalam UU hak cipta itu jelas-jelas disebut bahwa sekedar menggandakan tanpa izin sudah bisa dikenai tuntutan hukum.

Strategi Mengatasi Cybercrime

Lantas langkah apa yang harus dilakukan para pelaku bisnis berbasis internet di Indonesia dalam menghadapi kian berkembang dan beragam kejahatan dunia cyber di Indonesia pada saat cyberlaw belum juga terbentuk ? Menurut A'sad Yusuf, saat e-commerce telah berjalan dan perlindungan hukum atas kejahatan online atau cybercrime belum ada, maka tindakan yang bisa dilakukan user maupun pelaku bisnis adalah meningkatkan kewaspadaan dan kehati-hatian.

"Sangat perlu bagi penyelenggara e-commerce untuk meningkatkan keamanan di jaringan komputernya, " kata A'sad. Tujuannya adalah untuk meminimalisasi kemungkinan kerugian yang lebih besar dan memberikan keamanan bagi user untuk

melakukan transaksi. Begitu juga dengan bank yang terjun di bisnis berbagai internet." "Asas prudent bank juga perlu juga dijaga dalam pelaksana transaksi online,"tegas A'sad.

Bersikap waspada dan berhati-hati tampaknya merupakan sikap yang tidak terelakkan, meski bentuknya bisa berbeda-beda. Toko ritel online Rad-Clike.com, misalnya, memilih untuk tindakan klarifikasi berlipat – lipat terhadap internet yang membeli barang di toko online-nya," karena perlindungan hukumnya belum ada terpaksa kami lakukan dua hingga empat kali klarifikasi untuk transaksi online yang kami lakukan", ungkap John S. Tumiwa.

John mengaku bahwa dengan klarifikasi yang berlipat-lipat itu, proses bisnis yang dilakukan perusahaanya menjadi lebih panjang dan lebih lama sehingga peluang memperoleh pendapatan besar makin mengecil. Namun bagi John, langkah itu merupakan langkah yang paling realistis mengingat cyberlaw mencegah terjadinya cybercrime berada di Indonesia." Sebagai pengusaha kami memang tidak bisa menunggu hujan baru membeli payung, tetapi tetap harus mengantisipasi terjadinya cybercrime', jelas John.

Sementara itu PT Stocks Solution Dot Com, perusahaan portal simulai saham.com, mengembangkan system voucher transaksi simulasi saham di situs," mekanisme voucher memberikan keamanan transakasi dan kepercayaan dari para pengguna. Selain itu mekanisme voucher mempunyai keunggulan mudah dilakukan dan sudah terbiasanya masyarakat menggunakan voucher seperti dalam hal voucher untuk mengisi pulsa telepon selular. Mekanisme voucher untuk transaksi online seperti yang dilakukan simulasi saham dot com memang tergolong cukup mudah bagi pengguna internet. Dengan membeli voucher yang diedarkan di sejumlah warnet dan pusat

perbelanjaan, pemilik voucher akan memilki nomor PIN yang harus dimasukan ketika ingin menggunakan fasilitas bermain saham yang disediakan di situs simulasi saham dot com.

Setelah melalui mekanisme voucher akan memperoleh kepercayaan dalam menuju transaksi online dengan menggunakan kartu kredit pada Maret 2001. Bagaimanapun transaksi online dengan kartu kredit bagi perusahaan penyelenggara e-commerce lebih menguntungkan mengingat pemberian komisi ke distribusi voucher lebih besar dibandingkan dengan komisi ke bank.

Adapun untuk mengantisipasi kesalahgunaan kartu kredit, Irwan mengungkapkan pihaknya telah merancang 2 sistem pengamanan. Pertama, pengamanan dari bank yaitu konfirmasi dari bank mengenai keabsahan kartu kredit yang digunakan dalam transaksi online. "Kedua, kami sendiri juga mengambil langkah pengamanan berupa persyaratan bahwa nama customer harus sama denga nama yang tertera di kartu kredit yang digunakan", jelas Irwan.

Lain halnya dengan bentuk kehati – hatian yang ditempuh PT Kopitime Dot Com Tbk. "Kami mengandalkan pemasangan perangkat ssstem sekuriti yang up to date setiap saat sehingga hacker atau virus susah menembusnya,' ujar Indrajaya. Bagi Indrajaya, suatu perusahaan provider e-commerce memang dituntut membuat seaman mungkin situsnya demi kepentingan konsumen.

"Sebenarnya gejala adanya serangan hacker bisa dimonitor dan tertangkap basah," tutur Indrajaya. Seseorang hacker, menurut Indrajaya, bisa diketahui sedang beroperasi ketika ia dikethui sedang meng-update suatu data sehingga bisa dilacak files original si hacker lengkap dengan data identitasnya. "Jadi kita sendiri yang harus bisa

mengantisipasi dan mengerti pola kejahatan mereka yang selalu berusaha mencari celah kelemahan situs kita.

Sikap berhati – hati juga ditunjukan oleh pengelola toko online lainnya, lipposhop.com. "Sejauh ini Lipposhop.com belum menerapkan sisitem pembayaran online sepenuhnya atau yang biasa disebut e-payment, hingga kini metoda pembayaran cara tunai, transfer melalui ATM, bank, debet rekening dan kartu kredit yang disertai tanda tangan tertulis.

Lebih jauh, Romzy Alakaterie menyarankan bahwa untuk mengantisipasi adanya serangan cybercrime, sebenarnya ada 3 cara yang bisa dilakukan. Pertama, mengusahakan adanya certicate autority yaitu adanya jaminan dari suatu perusahaan menjamin untuk keamanan transaksi yang dilakukan dengan sebuah perusahaan penyelenggara e-commerce. Kedua, menggunakan smart carda, yaitu semacam identitas nomor khusus untuk transakasi online yang harus online juga dengan perusahaan penylenggara jasa smart card. Ketiga, melengkapai transaksi online dengna tanda tangan digitalnya, maka kartu itu tidak bisa digunakan untuk transaksi. Tanda tangan digital ini ada pada masing – msaing pemegang kartu, bukan pada kartu kreditnya.

HACKER

Fabian Clone mungkin hanya sekedar main – main ketika menyusup ke beberapa situs terkenal di Iindonesia bukan mencari untung motifnya ketika meng-*hack* situs – situs milik Pusat Data dan Analisa Tempo (PDAT), Bank Central Asia dan Aetna Life baru – baru ini. Sebagaimana dia sampaikan kepada Detik.com, ia melakukan itu sekedar untuk mengeceksistem sekuriti situs – situs itu karena disinyalir seorang *cracker* yang mengaku dari Australia dan mengancam akan mengobrak-abrik situs Indonesia, "ujarnya.

Ia kaget ketika menemukan banyak situs yang tidak memilki system pengamanan yang baik sehingga dengan mudah ia masuki. Pada beberapa situs yang ia susupi, Clone meninggalkan jejak berupa sebuah *subdirectory* dengan nama fabianclone. Dari sanalah orang mengetahui kalau dialah pelakunya.

Kisah beraksinya *hacker* pada *e-business* di Indonesia bukan hanya sekali dua kali. Clone yang pernah melakukannya. Konon beberapa tahun yang laluu, di Institut Teknologi Bandung banyak bersemayam hacker muda yang rata – rata masih berstatus mahasiswa. Kini banyak diantara mereka yang telah "bertaubat" dan mulai membangun bisnisnya dengan baik.

Terakhir, situs milik Kopitime Dotcom pun ikut disusupi *hacker*. Pelaku sebut saja Mr.XX, menurut Indrajaya Putra Januar, presiden direktur Kopitime Dotcom Tbk. Masuk ke dalam system *front office* Kopitime dan mengubah tampilan warna situs tersebut

"Kami memang sudah mem-protec system, tetapi namanya saja *hacker* selalu mencari celah. Kami melakukan monitoring terus saat dia masuk, bahkan seperi orang

main kucing – kucinga. Dia rubah tampilan, kami ganti, dia ubah lagi, kami ganti lagi. Begitu seterusnya sehingga bisa kami lacak identifikasi orangnya dengan jelas.

Indrajaya mengatakan bahwa perusahaan sekelas Microsoft, lembaga semacam Pentagon yang selalu memprotec situs mereka dengan baik pun mampu dijebol. Jadi, tidak ada jaminan bahwa systen keamanan yang baik bisa meniadakan sama sekali kemungkinan menyusupnya hacker kedalam system sebuah perusahaan.

Kendati menurut beberapa pengamat maupun pelaku *e-business* aksi *hacker* ke banyak pihak. Apalagi untuk Kopitime, berita mengenai penyusupan *hacker* ke system mereka bisa mempengaruhi kepercayaan pasar terhadap keberadaan mereka sebagai perusahaan publik. Asal tahu saja, kasus ini mencuat beberapa hari setelah mereka melakukan *initial public offering* (IPO).

Hal itu diakui juga oleh John S. Tumiwa, *chief executive operation* Radioclick.Com. Ia mengatakan ada juga *hacker* yang baik yakni mereka yang masuk ke sebuah system, membuktikan bahwa system itu tidak aman lalu memberitahukan kelemahan itu. Menurutnya, *hacker* seperti ini adalah *hacker* yang baik. Mengapa? Pasalnya, dengan ulahnya pemilik system atau situs itu bisa meningkatkan keamanan.

Barangkali Tumiwa benar. Ambil sontoh pengalaman Bank Internasional Indosnesia setahun yang lalu. Menurut Rudy N. Hamdan, *managing director commercial, consumer and e-banking homepage* kami yang ketika itu belum dilengkapi *security system* yang baik."

Menurut dia, kasus yang menimpa BII ini terjadi pada beberapa bank lain di Jakarta. Walau tidak ada system yang dirusak, ia mengakui untuk sesaat penampilan *homepage* BII berubah. "Jadi,begitu anda masuk ke *homepage* BII, layarnya menjadi

blank, dan muncul tulisan Napster sehingga bisa jadi ada yang menyimpulkan Napsterlah *hacker*-nya.

Jika Tumiwa mengatakan bahwa ada *hacker* yang baik, bisa jadi Clone termasuk dalam kategori *hacker* yang baik. Ia tidak mengacak – ngacak database dari System yang disusupinya sehingga tidak merugikan secara ekonomi.

Hanya jika system atau situs itu diumpankan sebai sebuah halaman rumah, para hacker jelas melakukan pelanggaran. Siapa pun yang masuk halaman rumah orang tanpa izin tentunya sudah melanggar, kendati tidak mencuri atau melakukan sesuatu yang mencurigkan.

Kopitime sendiri, telah menangkap basah Mr.XX itu, tidak melakukan tindakan hukum. Mereka hanya memintanya membuat pernyataan unutk tidak melakukan tindakan itu lagi. "Jika kami menuntut secara hukum, tidak ada perangkat yang bisa mengaturnya dan juga kami tidak menderita kerrugian secara material," tegas Indrajaya.

Sementara itu, untuk mengidentifikasi pelakunya, pihak Kopitime tidak ada kesulitan lagi. "kami bahkan sudah tahu alamatnya dimana, nomor teleponnya berapa, keluarga siapa, semuanya sudha jelas." Kata Indrajaya.

Ada juga yang menduga bahwa persaingan bisnis bisa menjadi dasar aktivitas para hacker, tidak terkecuali Mr.xx ini. Indrajaya pun memberikan keuntungan akan hal itu.

"Mungkin saya tidak perlu perusahaan atau dimana orang bekerja. Namun yang jelas, orang itu bekerja di sebuah perusaan yang bisnisnya samadengan kami. Jadi bisa kalim bahwa persaingan bisinisnya sama dengan kami. Jaidi bisa klaim bahwa ada yang tidak sehat.

Walau Indrajaya enggan menyebutkan perusahaan asal Mr.xx, ada ifnormasi yang menyebutkan bahwa inbekerja pada PT.Myoh dotcom Indonesia Tbk. Pihak Myoh dotcom semiri mengaui hal itu. "Orang itu memeang bekerja di perusahaan kami, tetapi dia melakukan itu dengan ketidaktahuan," ungkap David J. Elisafan, presiden directur PT Myohdotcom Indonesia Tbk. Menurut Elisafan, pelakunya bahkan tidak mengetahui kalau system yang dia masuki milik kopitime.

Terlepas dari benar atau tidaknya penagakuan pelaku sebagaimana disebutkan Elisafan, masalah ini sudah selesai secara damai."Kami sudah selesaikan secara baik dengan kopitime dan orang itu kami beri peringatan keras,"katanya.

Jika di Indonesia pihak-pihak yang mengalami kebobolan akibat ulah hacker seperti indrajaya kerap mendiamkan persoalan ini, tidak demikian di beberapa negara lain.Di Inggris misalnya, hukum ntelah memposisikan hacker setara dengan teroris. Untuk itu, siapa pun yang mencoba merusak system elektronik dengan tujuan untuk mengancam pemerintah dan publik akan dijaring dengan UU ini.

Di Indonesia barangkali masih jauh dari kondisi ini. Cyberlaw-nya saja masih belum rampung digarap. Itupun belum ketahuan apakah isinya mengatur seketat ala Inggris.

Dalam kondisi seperti ini, Indrajaya mengajukan agar pelaku e-business memperhatikan factor keamanan dari system atau situsnya. Bahkan tidak ada garansi akan aman seratus persen, itu pasti. " Namun, dengan menjaga system sekuriti secara sungguh-sungguh serta selalu memonitor traffic dalam system itu, hacker bisa di tanggulangi," kata dia.

Virus.

Jangan sekali-kali terburu-buru membuka pessan-pesan manis melalui internet. Sepintas pessan itu menarik tetapi jangan salah, isinya bisa membuat pusing kepala. Anda masih ingat bukan, ketika virus bertanda cinta muncul beberapa waktu yang lalu dan memporakporandakan data pengguna internet yang ceroboh di seantero dunia ? judul yang disampaikan cukup menarik sehingga dengan membuat orang sukarela karena penasaran segera membuka pesan tersebut. Akibatnya fatal.

" Kita harus hati-hati menerima email yang mengandung sisipan. Kadang-kadang namanya menarik tetapi ternyata sebuah program virus," kata R.M.Suryo, pengamat TI UGM. Roy mencontohkan virus yang baru-baru ini semapat membuat gempar, Ana Kournikova, nama seorang petenis cantik asal Rusia. Virus baru yang mengecoh pengguna internet dengan pesan seolah-olah mereka menerima foto dari bintang tennis Anna Kournikova menyebar dengan cepat melalui internet. Untunglah, meski sebelumnya diyakini sebagai virus yang tergolong *high risk*, belakang diketahui daya rusak yang dimiliki tidak terlalu ampuh untuk merusak komputer yang diserangnya.

Namun bagi para pebisnis didunia maya, keberadaan virus tidak terlalu berdampak pada bisnis mereka. Sebut saja Adi Kusna presdir Biznet.com, yang mengaku belum pernah terkena imbas dari adanya virus itu. Hal itu terjadi karena perusahaannya sudah menerapkan pengamanan system anti virus. Untuk itu dia rela merogoh kantongnya untuk menyediakan penagkal virus yang tidak bisa dibilang murah. US$75.00 sampai US$100.000.

Hal yang sama juga dikemukakan oleh Darma Putra, *finance offer* Bolebet.com, meski sebagai pribadi dia pernah juga terganggu dengan adanya virus file yang

menyerang sebuah *file* miliknya. "saat itu saya menerima *file attachment* dari satu perusahaan. Pada saat itu tidak ada dampak langsung. Membuka file masih bisa, tetapi beberapa saat kemudian baru ketahuan saya terkontaminasi *virus hiworm*."ujar Putra.

Secara umum mereka masih bersuara sama bahwa sejauh ini yang mencemaskan untuk dunia bisnis internet Indonesia. Kecemasan memang ada, hanya pada tingkat yang wajar, yakni pada virus yang sejauh ini masih belum terdeteksi. Karena itulah perusahaan umum menyediakan system pengaman dari serangan virus. Meskipun demikian Putra mengatakan, sebuah perusahaan tidak akan berani terbuka untul mengakui kelemahan dari system pengamanannya, termasuk massalah virus ini akan berimplikasi pada menurunnya keprcayaan masyarakat terhadap system – system di perusahaan.

Jika berbicara tentang virus, Microsoft, sebagai salah satu perusahaan software terbesar di dunia, merasa bangga tetapi juga sedih. Bangga karena produknya *familiar* banyak dipakai masyarakat. Namun dengan familiar itu orang akan sangat paham akan produk ini. Maka produk microssoft kerap " diobrak abrik" oleh para petualang nakal. " Produk kami terutama Microsoft Office, pemakainya hampir 85% dari pengguna komputer. Jadi mau tidak mau harus siap dengan serangan dari orang – orang iseng," ujar Paul Hardiman, direktur pemasaran PT.Microsoft Indonesia.

Sebenarnya awal diciptakannya virus kesannya tidak seseram sekarang. Virus *Sherlock Holmes*, misalnya, tidak menyebabkan kerusakan serius. Virus ini hanya mengubah nama pemiliknya menjadi Sherlock dan alamat user berubah ke alamat *email* milik mahasiswa Teknik Elektro UGM. Apalagi belasan tahun lalu, saat internet belum memasyarakat, penciptaan virus hanya digunakan sebagai *ajang* nampang agar namanya

lebih dikenal. Sebut saja Deny Zuko, seorang mahasiswa ITB yang sekitar tahun 1985 berhasil membuat virus Denzuko, singkatan dari namanya sendiri.

Serangan bagi Microsoft yang lebih dahsyat terjadi beberapa bulan lalu saat berkembang virus cinta. Virus ini menyerang komputer yang menggunakan system operasi Microsoft Windows, sedangkan system operasi berbasis Linux dan Apple sama sekali tidak terserang. Diperkirakan virus cinta telah merusak sebanyak 3,1 juta komputer diseluruh dunia dengan kerugian ditaksir mencapai US$10 miliar.

Akibat adanya virus ini, perusahaan jasa security internet yang professional, menjadikannya peluang bisnis. Bahkan sampai ada yang mencurigai bahwa banyaknya virus dengan gangguan keamanan di dunia *cyber* lainnya tidak lepas dari tangan-tangan mereka. Anggapan ini dibantah oleh Romzy Alkateri, Dirut PT Karya Asta Ultramedia." Seseorang yang akan membangun rumah, dia membutuhkan tukang kunci. Apakah tukang kunci itu adalah seorang pencuri ? kan tidak," jelasnya. Pendapat senada juga dikemukakan Budi Rahardjo, pengamat TI dari ITB. Dikatakannya bahwa sebuah perusahaan sekuirtas tidak bisa dissamakan dengan *hacker*. " Keduanya sudah lain dalam hal filosofi dan pendekatannya, " ujar Budi.

Sebenarnya yang paling meersakan dampak virus adalah pengguna internet perseorangan. Dengan pendanaan mereka yang terbatas proteksinya kurang memadai Sementara itu, perusahaan rata-rata sudah menyediakan anggaran khusus untuk pengamanan. Untuk itu Roy mencoba memberikan solusi yang murah dan tetap"higienis" berinternet. Resepnya adalah jangan, pertama, menerima email, kedua, membuka attachment, ketiga, masuk situs yang "aneh-aneh", keempat, melakukan chating, kelima, mangadakan transaksi dan berbagai aktifitas lain yang belum anda kenal sebelumnya.