KEJAHATAN TERHADAP INFORMASI *(CYBERCRIME)* DALAM KONTEKS PERPUSTAKAAN DIGITAL

Oleh :

IRHAMNI ALI

TUGAS MATA KULIAH ORGANISASI INFORMASI

SEKOLAH PASCASARJANA

INSTITUT PERTANIAN BOGOR

BOGOR

2011

KEJAHATAN TERHADAP INFORMASI *(CYBERCRIME)* DALAM KONTEKS PERPUSTAKAAN DIGITAL

Irhamni Ali

ABSTRAK

Perkembangan teknologi informasi-komputer saat ini sudah mencapai pada tahap di mana ukurannya semakin kecil, kecepatannya semakin tinggi, namun harganya semakin murah dibandingkan dengan kemampuan kerjanya. Perpustakaan Online atau perpustakaan digital bisa dianggap sebagai institusi informasi dalam bentuk baru atau sebagai perluasan dari pelayanan perpustakaan yang sudah ada. Namun dibalik kemudahan yang ditawarkan perpustakaan digital terdapat suatu bahaya yang mengancam keutuhan data dan koleksi perpustakaan digital. Pencurian data, vandalism dan mutilasi data serta ancaman lain siap meyerang setiap saat , untuk itu pustakawan di era digital perlu mengenal modus kejahatan cybercrime dalam perpustakaan digital dan titik lemah sistem mereka agar kejahatan cybercrime yang mengincar perpustakaan digital dapat di minimalisasi.

Keyword

Data elektronik; vandalime data, cybercrime, perpustakaan digital

KEJAHATAN TERHADAP INFORMASI *(CYBERCRIME)* DALAM KONTEKS PERPUSTAKAAN DIGITAL

A. PENDAHULUAN

Perkembangan teknologi informasi-komputer saat ini sudah mencapai pada tahap di mana ukurannya semakin kecil, kecepatannya semakin tinggi, namun harganya semakin murah dibandingkan dengan kemampuan kerjanya. Kondisi ini mendorong masyarakat berlomba-lomba memanfaatkan komputer sebagai alat bantu pengolahan data dengan cara membangun system pengolahan data terkomputerisasi untuk penyajian informasi, baik untuk keperluan pribadi maupun organisasinya. Perpustakaan sebagai organisasi yang melakukan pengolahan data dan informasi untuk pemustakanya telah melakukan langkah revolusioner dalam melakukan pelayanan melalui sistem online yang lebih efisien dalam pelayanan, diseminasi, pemustakaan dan pelestarian data, informasi dan pengetahuan.

Perpustakaan Online atau perpustakaan digital bisa dianggap sebagai institusi informasi dalam bentuk baru atau sebagai perluasan dari pelayanan perpustakaan yang sudah ada. Namun demikian perpustakaan digital adalah kumpulan informasi yang tertata dengan baik beserta layanan-layanan yang disediakannya, informasi ini disimpan delam format digital dan dapat diakses melalui jaringan computer Pada tahun terakhir ini telah terjadi peledakan pertumbuhan ketertarikan dalam perkembangan dan pemakaian perpustakaan digital. Beberapa faktor penunjangnya adalah:

a) Telah tersedianya teknologi komputasi dan komunikasi yang memungkinkan dilakukannya
   penciptaan, pengumpulan dan manipulasi informasi.
b) Infrastruktur jaringan internasional untuk mendukung sambungan dan kemampuan
   pengoperasian bagi pemustaka.
c) Informasi online mulai berkembang.
d) Kerangka akses internet umum telah muncul.

Saat ini Salah satu tantangan dihadapi pustakawan saat ini adalah bagimana memproteksi proteksi koleksi informasi yang mereka miliki dari berbagai macam gangguan dan ancaman yang bisa terjadi perpustakaan khusunya pada perpustakaan digital. Dahulu kejahatan dalam perpustakaan yang semula bersifat konvensional seperti pencurian koleksi , vandalism, mutilasi buku , peminjaman tanpa hak, kini kejahatan dalam perpustakaan dapat dilakukan dengan menggunakan media komputer secara online dengan risiko tertangkap yang sangat kecil oleh individu maupun kelompok dengan akibat kerugian yang lebih besar bagi perpustakaan.

Tentunya, hal-hal tersebut di atas tidak dapat dipungkiri adanya bahwa teknologi informasi membawa mampu dampak negatif yang tidak kalah banyak dengan manfaat yang ada khusunya dalam dunia perpustakaan. Internet membuat juga bisa membuat data/koleksi informasi yang dimiliki perpustakaan menjadi terancam dan bisa disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab.

B. CYBERCRIME DAN PERPUSTAKAAN DIGITAL

Perkembangan teknologi jaringan komputer global atau Internet telah menciptakan dunia baru yang dinamakan *cyberspace*, sebuah dunia komunikasi berbasis komputer yang menawarkan realitas yang baru, yaitu realitas virtual. Istilah tersebut juga menghasilkan berbagai bentuk lingkungan *cyberspace* yang kemudian melahirkan istilah baru yang dikenal dengan *Cybercrime*, *Internet Fraud*, dan lain-lain.

Dalam beberapa literatur, cybercrime sering diidentikkan sebagai computer crime. The U.S. Department of Justice memberikan pengertian komputer crime sebagai:"…*any illegal act requiring knowledge of Computer technology for its perpetration, investigation, or prosecution".* Sementara itu Andi Hamzah dalam bukunya “Aspek-aspek Pidana di Bidang Komputer” (1989) mengartikan cybercrime sebagai kejahatan di bidang komputer secara umum dapat diartikan sebagai penggunaan komputer secara ilegal.

Dari beberapa pengertian di atas, *cybercrime* dirumuskan sebagai perbuatan melawan hukum yang dilakukan dengan memakai jaringan komputer sebagai

sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Perpustakaan digital sebagai ranah yang berkembang dalam dunia cyberspace yang menyimpan data baik data buku(tulisan), Gambar, suara dalam bentuk file elektronik dan mendistribusikannya dengan protocol-protokol elektronik melalui jaringan komouter. Isi dari perpustakaan digital berada dalam suatu komputer server yang bisa ditempatkan secara local maupun lokasi yang jauh namun dapat di akses dengan cepat mudah melalui jaringan computer. Karena itu perpustakaan digital menjadi mejadi salah satu objek *cybercrime* yang sangat menggiurkan bagi para pelaku kejahatan cybercrime.

Pelaku cybercrime yang menjadikan pepustakaan digital sebagai objek kejahatannya biasanya mengincar data pengguna, koleksi atau pun sistem keamanan dengan motif untuk kepentingan tertentu misalnya data pengguna untuk dijadikan objek marketing, pencurian koleksi untuk kepentingan komersil, atau hanya sekedar unjuk gigi seorang hacker sebagai pembuktian bahwa dirinya eksis.

Untuk itu pustakawan harus mampu mengidentifikasi serangan-serangan terhadap perpustakaan digital yang dikelolanya agar semua sistem, koleksi dan data yang ada pada perpustakaannya aman dari serangan yang dapat merugikan banyak pihak.

C. MODUS OPERANDI CYBERCRIME DALAM PERPUSTAKAAN DIGITAL

Modus operandi merupakan cara atau bagimana suatu kejahatan tersebut dilakukan, modus operandi cybercrime dalam perpustakaan digital sangat beragam dan terus berkembang sejalan dengan perkembangan teknologi, tetapi jika diperhatikan lebih seksama akan terlihat bahwa banyak di antara kejahatan-kejahatan tersebut memiliki sifat yang sama dengan kejahatan terhadap perpustakaan konvensional. Bentuk kejahatan terhadap buku dan perpustakaan ada 4(empat) macam, yaitu : *Thief* (pencurian), *Mutilation* (perobekan),*Vandalism* (corat-coret) serta *An-authorized borrowing* (peminjaman tak sah) namun perbedaan utamanya adalah bahwa cybercrime dalam perpustakaan digital melibatkan komputer dalam pelaksanaannya. Kejahatan

yang berkaitan perpustakaan digital perlu mendapat perhatian khusus oleh pustakawan, sebab kejahatan-kejahatan ini memiliki karakter yang berbeda dari kejahatan pada perpustakaan konvensional karena berakibat langsung terhadap kerahasiaan data, integritas data dan keberadaan data dan sistem operasional perpustakaan digital. Modus operandi yang biasanya dilakukan terhadap perpustakaan digital adalah :

a. *Data Thief* (pencurian)

   Data Thief atau pencurian data merupakan bentuk kejahatan yang kerap terjadi. Hal ini harus diantisipasi oleh para pustakawan dengan upaya meminimalisasi kemungkinan para pelaku cybercrime untuk melakukan pencurian. Dalam ranah perpustakaan digital pencurian data bisa dikategorikan sebagai *data Leakage*, yaitu menyangkut bocornya data pemustaka atau data lainnya ke luar terutama mengenai data yang harus dirahasiakan. Pembocoran data komputer itu bisa berupa berupa nama, kontak serta kebiasaan pemustaka dalam memakai koleksi perpustakaan . Hal ini bisa berbahaya jika jatuh ke tangan yang salah sehingga bisa digunakan untuk sesuatu yang tidak diinginkan seperti pelanggaran privasi pemustaka yang apabila diketahui oleh orang lain maka dapat merugikan pemustaka secara materil maupun immaterial.

   Jika data yang dicuri adalah koleksi perpustakaan yang berbentuk digital maka hal ini masuk pada *Offense Against Intellectual Property* dimana Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di Internet. Jika hal ini terjadi dapat membahayakan perpustakaan karena koleksi-koleksinya akan tercecer keluar dan di perdagangkan secara illegal dan jika hal ini terjadi bukan hanya pihak perpustakaan saja yang dirugikan namun juga pihak pengarang sebagai pemilik hak kekayaan intelektual.

b. *Joy computing*, yaitu pemakaian komputer orang lain tanpa izin, termasuk penggunaan program komputer, password komputer, kode akses, atau data sehingga seluruh atau sebagian sistem komputer dapat diakses dengan tujuan digunakan untuk melakukan akses tidak sah, intersepsi tidak sah, mengganggu data atau sistem komputer, atau melakukan perbuatan-perbuatan melawan hukum lain. Hal ini biasanya terjadi pada OPAC perpustakaan dimana OPAC digunakan sebagai sarana untuk

menyebarkan virus atau digunakan sebagai host untuk mengakses ke server tanpa izin, untuk itu pustakawan perlu memikirkan cara agar OPAC yang ada di perpustakaan tidak disalah gunakan oleh pemustaka untuk tindakan *Joy Computing*.

c. *Hacking*, yaitu mengakses secara tidak sah atau tanpa izin dengan alat suatu terminal bisa dari dalam perpustakaan dengan menggunakan OPAC atau dari luar perpustakaan dengan memanfaatkan port yang terbuka, hacking biasanya bertujuan untuk *defacing* dan *cracking*. *Defacing* merupakan aktivitas seorang hacker untuk melakukan perubahan tampilan pada web perpustakaan, biasanya pelaku *defacing* hanya bertujuan sebagai sarana untuk mengetes ilmu atau unjuk kemampuan diantara sesama hacker, sementara *cracker* bertujuan untuk menganggu jaringan komunikasi data, dan melakukan penetrasi jaringan sistem komputer untuk melakukan pencurian data, serta bertujuan membuat sistem gagal berfungsi yang mengakibatkan *Frustating data communication* atau penyia-nyiaan data komputer. Hal ini biasanya dilakukan dengan serangan DoS *(Denial Of Service)* dimana server gagal berfungsi karena terlalu banyak perintah yang masuk.

d. *Data Diddling*, yaitu suatu perbuatan yang mengubah data valid atau sah dengan cara tidak sah, mengubah input data, atau output data. Biasanya hal ini terjadi pada bagian sirkulasi dimana pihak-pihak tertentu berusaha untuk mengubah data peminjaman atau merubah data tertentu lainnya. Kejadian seperti ini perlu diantisipasi oleh pustakawan agar tidak terjadi kehilangan data atau *data loss.*

e. Electronic Mutilation dan data vandalism

Electronic Mutilation dan data vandalism muncul sebagai ekses dari menjamurnya komunitas maya dan kemudahan akses berkomunikasi melalui internet. Modus yang dilakukan adalah: masuk kesebuah database dengan sebelumnya melumpuhkan sistem keamanan database tersebut, lalu menyabotase data yang mereka perlukan dan sehingga data tersebut menjadi rusak dan tidak bisa dipergunakan kembali.

Namun Hacker bukanlah salah satu ancaman dari *Electronic Mutilation dan data vandalism* karena masih terdapat beberapa ancaman lainnya

yakni : beredarnya software illegal yang dapat menyusup dan merusak sistem komputer. Adapun jenis software tersebut adalah :

- Ulat (Worm) merupakan program yang memepunyai kemampuan menggandakan diri namun tidak mempunyai kemampuan menempelkan dirinya pada suatu program. Dia hanya memanfaatkan ruang kosong pada memori computer untuk menggandakan diri. Sehingga memori komputer akan menjadi penuh dan system computer akan terhenti.
- Bot merupakan istilah bagi suatu bagian program computer yang mempunyai kemampuan pengacauan dan perusakan pada suatu system computer berdasarkan kondisi yang telah diprogramkan didalamnya.
- Backdoor/Back office trap/ Pintu Jebakan merupakan program yang mempunyai kemampuan melumpuhkan system pengamanan suatu computer. Sehingga pembuat program dapat keluar masuk system tanpa harus melalui system pengamanan normal yang ditetapkan pada suatu sistem computer.
- *The Trojan Horse*, yaitu manipulasi data atau program dengan jalan mengubah data atau instruksi pada sebuah program, menghapus, menambah, menjadikan tidak terjangkau dengan tujuan untuk kepentingan pribadi pribadi atau orang lain.

  biasanya Program Trojan berfungsi sebagai kamuflase dari virus tidak merusak. Namun sisipan program didalamnya yang patut diwasapadai karena menyerang sistem operasi, *Directory* dan *boot record*.
- Virus (Komputer) merupakan program kecil yang dapat memperbanyak dirinya sendiri. Virus merusak secara berlahan-lahan boot record, Sistem operasi, dan directory bahkan bisa merusak fisik suatu media penyimpanan.

D. PENCEGAHAN

1. Personil

   Terbatasnya sumber daya manusia merupakan suatu masalah yang tidak dapat diabaikan, untuk itu perpustakaan perlu mengirimkan pustakawannya untuk mengikuti berbagai macam kursus mengenai keamanan data khususnya di perpustakan digital di dalam dan luar negeri agar dapat diterapkan dan diaplikasikan pada institusinya sehingga siap setiap saat dalam menangangani setiap serangan yang mungkin terjadi. Untuk itu diperlukan personil yang mampu mengenali kekuatan dan kelemahan sistem yang mereka pakai.

2. Sarana Prasarana

   Perkembangan teknologi yang cepat juga tidak dapat dihindari sehingga Pustakawan harus berusaha semaksimal mungkin untuk meng-up date dan up grade sarana dan prasarana baik perangkat keras maupun lunak yang dimiliki perpustakaan digital agar tidak ketinggalan jaman dengan hacker dan cracker khususnya pengamanan terhadap koleksi dan data dari *electronic vandalism* dengan 2 (dua) cara, yakni :

   a. Pencegahan masuknya Hacker pada jaringan internet

      Untuk mencegah hacker pustakawan perlu melakukan pengamanan database untuk menangkal Hacker dengan cara Pertama, administrator jaringan selalu meng-up to date patch. Serta menerapkan aturan fire wall yang ketat dengan memblokade port akses database pada TCP 1434 (MSQL) maupun TCP 1521-1530 (Oracle). Kedua, administrator jaringan senantiasa memeriksa tipe (integer) dan string setiap data yang masuk.Ketiga, Membuang Stored Procedure karena script –script yang kelihatannya tidak berbahaya namun bisa dimanipulasi oleh Hacker sebgai pintu masuk ke database. Keempat, Bila memungkinkan gunakan kode SQL yang sudah seringkali dipakai berulang-ulang ke Stored Procedure. Hal ini akan membatasi kode SQL yang telah diatur dalam file ASP dan mengurangi potensi manipulasi oleh Hacker

pada proses validasi input. Selanjutnya, Gunakan enkripsi session built in.

b. Pencegahan masuknya virus pada database

Terdapat bebarapa langkah yang dapat digunakan untuk pencegahan masuknya virus pada database, yaitu : Pertama, selalu up date antivirus secara teratur untuk mendapatkan program antivirus terbaru. Kedua, Jalankan antivirus secara auto protect untuk menghidnari virus yang menginfeksi. Ketiga, Berhati-hati dalam menerima email dari seseorang yang tidak dikenal. Keempat, Senantiasa menscan setiap kali sebelum menggunakan disket, flash disk ataupun CD. Selanjutnya, Senantiasa membac-up file secara teratur pada tempat yang aman.

Selain itu pustakawan juga harus mampu mengenali sistem keamanan data perpustakaan mereka. Modus operandi kejahatan cybercrime biasanya menggunakan titik lemah keamanan pada suatu sistem jaringan komputer, titik lemah tersebut berada pada :

a. **Titik Lemah HTTP**

Worl Wide Web (www) merupakan susunan protokol-protokol yang bertindak sebagai polisi lalu lintas untuk internet. HTTP menjadi protokol yang paling banyak digunakan di internet. Setiap browser dan server saling berhubungan dan bertukar informasi pada protokol ini. HTTP merupakan protokol request/respon yang memampukan komputer untuk slaing berkomunikasi secara efisien. Spesifikasi HTTP versi 1.1 merupakan perkembangan lebih lanjut dari spesifikasi asli yang ditemukan oleh Tim Bernerr Lee pada Maret 1990. Struktur umum URL HTTP 1.1 yang diluncurkan pada tahun 2001 sebagai berikut: http://host [":" port][absolute.path["?"query]]. Parameter – parameter yang melewati query (":") merupakan inti dari semua aplikasi web. Dan merupakan salah satu jalan utama kesemua ruang. Script (":") merupakan kunci proses-proses script dan sasaran serangan para hacker.

b. **URL (Uniform Resources Locator)**

URL merupakan sebuah mekanisme untuk mengenali sumber-sumber pada web, yakni: SSL dan server ftp termasuk layer aplikasi yang memuat request ke server web. Struktur umum URL adalah : protokol://server/path/to/resources ? parameter. Arsitektur protocol http menciptakan pen encode-an URL agar karakter-karakter non alfanumerik bisa dipakai pada string URL. Sehingga karakter-karakter alfanumerik dan simbol-simbol pada keyboard bisa digunakan. Namun pada web server tertentu bisa dimanipulasi dengan metode non standar dan pengkode-an karakter pada string URL. Dan 2 (dua) kelemahan web server yang paling signifikan menghasilkan kesalahan-kesalahan pada proses penguraian sandi (decode) URL.

3. Kerjasama dan koordinasi

Melakukan kerjasama dalam melakukan pengamanan data, hal ini perlu karena serangan terhadap perpustakaan digital yang sifatnya yang borderless dan tidak mengenal batas wilayah, sehingga kerjasama dan koordinasi baik dengan aparat penegak hukum atau pun dengan sesama pustakawan dan institusi terkait lainnya merupakan hal yang sangat penting untuk dilakukan.

E. PENUTUP.

Perpustakaan sebagai salah satu ranah dalam *cyberspace* sudah pasti akan selalu menjadi objek kejahatan *cybercrime,* untuk itu pustawakan di era digital sekarang ditantang untuk bisa mengerti bukan kejahatan konvensional dalam perpustakaan namun juga kejahatan yang melibatkan teknologi informasi *(cybercrime)* pada perpustakaan digital. Modus dan motif *cybercrime* kian kompleks maka itu tidak ada jaminan keamanan di *cyberspace,* dan tidak ada sistem keamanan komputer yang mampu secara terus menerus melindungi data yang ada di miliki oleh perpustakaan digital. Para *hacker* akan terus mencoba untuk menaklukkan sistem keamanan yang paling canggih, dan merupakan

kepuasan tersendiri bagi *hacker* jika dapat membobol sistem keamanan komputer orang lain. Langkah yang baik adalah dengan selalu memutakhirkan pengetahuan SDM perpustakaan digital, meng-*update* dan meng-*upgrade* sistem keamanan computer untuk melindungi data yang dimiliki dengan teknologi yang mutakhir pula serta melalukan kerjasama dengan instansi terkait dalam menangani masalah cyber crime di Indonesia.

DAFTAR PUSTAKA

Andi Hamzah, 1990.*Aspek-aspek Pidana di Bidang Komputer.* Jakarta : Sinar Grafika

Gollese, Petrus Reinhart, 2006. *Perkembangan cybercrime dan upaya penanganannya Di indonesia oleh polri.* Jakarta : Buletin Hukum Perbankan dan kebanksentralan. Volume 4 Nomor 2 Agustus 2006

Handisa, Rattahpinnusa Haresariu**.** *Ancaman Electronic Vandalism Terhadap Keamanan Data di Perpustakaan Nasional RI.* http://duniaperpustakaan.com/2010/02/24/ancaman-electronic-vandalism-terhadap-keamanan-data-di-perpustakaan-nasional-ri/ **[7 Januari 2012]**

Pendit PL. 2008. *Perpustakaan Digital Dari A sampai Z*. Jakarta: Cita KaryaKarsa Mandiri.

Sinaga, Dian, 2004. *Kejahatan Terhadap Buku dan Perpustakaan .* Jakarta : Visi Pustaka. Nomor 6 Volume 1 Juli 2004

-----. 2012. *Pengertian jenis dan modus cybercrime.* http://adrianestih.wordpress.com/2011/01/29/pengertian-jenis-dan-modus-cyber-crime-2/ [7 Januari 2012]