Modul Proteksi dan Pertukaran Informasi Kesehatan
ONLINE 11

KASUS SERANGAN KEMANAN SISTEM INFORMASI

- Situs FPI menjadi Target Serangan CRACKER Massal .FBINews, Pasca Penolakan Kedatangan Pengurus Pusat FPI(Forum Pembela Islam) ke Kalimantan Tengah oleh masyarakat setempat membangkitkan sentimen serupa di pelosok tanah air sehingga menginspirasi munculnya gerakan indonesia tanpa fpi di jantung ibukota jakarta yang kegiatannya dimulai dari situs jaring sosial seperti facebook dan twitter yang mengkristal menjadi gerakan moral turun ke jalan oleh beberapa aktifis humanis dan beberapa seniman.Gerakan Moral selain di situs jaring sosial dan aksi turun ke jalan juga dilakukan dengan serangan dunia maya(cracking)yang ditujukan kepada official website FPI http://www.fpi.or.id oleh hacker yang menggunakan id sn0wman yang memperkenalkan dirinya di sebuah blogmiliknya di http://www.hack4down.wordpress.com"dalam perkenalan singkatnya tanggal 17 februari 2012 sn0wman mengatakan bahwa dia membuat blog itu hanya sebagai pembelajaran dalam berpikir simple bahwa segala sesuautunya mesti ada keseimbangan baik dan buruk semua harus seimbang dan juga mengatakan "perang gerilya" selalu menang melawan pasukan yang bersenjata lengkap sembari mengklaim bahwa situs fpi sudah jadi targetnya dan sudah diserang yang dimulai tanggal 17 februari dengan program yang dibuatnya sendiri. keesokan harinya sn0wman juga mengajak dan mengajarkan cara menyerang situs fpi sembari membuka program yang digunakannya untuk bisa digunakan untuk umum sekaligus memberi tahu langkah2nya.Sampai berita ini diturunkan situs resmi FPI sepertinya masih down. Sumber
- 7 Februari 2000 s/d 9 Februari 2000. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E- Trade.
- 2001. Virus SirCam mengirimkan file dari harddisk korban. File rahasia bisa tersebar. Worm Code Red menyerang sistem IIS kemudian melakukan port scanning dan menyusup ke sistem IIS yang ditemukannya.
- 2004. Kejahatan “phising” (menipu orang melalui email yang seolah- olah datang dari perusahaan resmi [bank misalnya] untuk mendapatkan data- data pribadi seperti nomor PIN internet banking) mulai marak. Sumber

Beberapa Perstiwa di Indonesia

- Pencurian dan penggunaan account Internet milik orang lain . Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup menangkap “userid” dan “password” saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya “benda” yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunan dibebani biaya

penggunaan acocunt tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.

- Membajak situs web . Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksploitasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di Indonesia menunjukkan satu (1) situs web dibajak setiap harinya. Hukum apa yang dapat digunakan untuk menjerat cracker ini?
- Probing dan port scanning . Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan “port scanning” atau “probing” untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall*atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan. Apakah hal ini dapat ditolerir (dikatakan sebagai tidak bersahabat atau *unfriendly* saja) ataukah sudah dalam batas yang tidak dapat dibenarkan sehingga dapat dianggap sebagai kejahatan? Berbagai program yang digunakan untuk melakukan probing atau portscanning ini dapat diperoleh secara gratis di Internet. Salah satu program yang paling populer adalah “nmap” (untuk sistem yang berbasis UNIX, Linux) dan “Superscan” (untuk sistem yang berbasis Microsoft Windows). Selain mengidentifikasi port, nmap juga bahkan dapat mengidentifikasi jenis operating system yang digunakan.
- Virus . Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat kita lakukan. Akan tetapi, bagaimana jika ada orang Indonesia yang membuat virus (seperti kasus di Filipina)? Apakah diperbolehkan membuat virus komputer?
- Denial of Service (DoS) dan Distributed DoS (DDos) attack . DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan

bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

- Kejahatan yang berhubungan dengan nama domain . Nama domain (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingan perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.
- IDCERT (Indonesia Computer Emergency Response Team). Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “sendmail worm” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer Emergency Response Team (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia .
- Sertifikasi perangkat security . Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh Korea Information Security Agency. Sumber

Tambahan Informasi : Beberapa Cracker terkenal di Dunia

- “Seorang pria yang baik di siang hari dan nampak jahat di malam hari”, begitulah yang dapat menggambarkan pemuda yang satu ini. Poulsen adalah seorang penjahat cyber paling terkenal di Amerika yang pernah ada. Untuk menjadi seorang peretas, Poulsen belajar sendiri secara otodidak. Salah satu aksi terbaik yang pernah dilakukannya adalah mengambil alih saluran telepon yang menuju stasiun radio Los
- Angeles KIIS-FM. Poulsen ditangkap oleh FBI akibat beberapa akun yang ia retas termasuk mail, kawat dan penipuan komputer, pencucian uang dan pengganggu an pengadilan dan dihukum 51 bulan penjara dengan biaya $ 56.000 sebagai biaya kompensasi
- Albert Gonzalez, lahir pada tahun 1981. Adalah seorang hacker komputer dan criminal computer yang dituduh mendalangi pencurian kombinasi kartu kredit dan kemudian

dijual kembali lebih dari 170 juta kartu kredit dan nomor ATM dari 2005 hingga 2007, dan menjadi penipuan terbesar dalam sejarah. Gonjalez dan komplotannya menggunakan teknik injeksi SQL untuk membuat backdoor malware pada beberapa sistem perusahaan untuk meluncurkan paket sniffing yang digunakan untuk mencuri data komputer dari jaringan internet perusahaan. Gonzalez memiliki tiga dakwaan federal. Dan pada tanggal 25 Maret 2010, Gonzalez dijatuhi hukuman 20 tahun penjara federal

- Levin terkenal pada 1990-an atas upaya hacking yang terkena kerentanan situs perusahaan yang populer, salah satu yang paling terkenal dalam hal ini menjadi Citibank. Levin, pada tahun 1994, mampu mengakses rekening Citibank milik pelanggan berbagai perusahaan. Dia menggunakan layanan dial-up wire transfer dan berhasil mentransfer uang dari rekening tersebut ke rekening yang terletak di Israel, Jerman, Amerika Serikat, Finlandia, dan Belanda. Levin memiliki kaki tangan di masing-masing lokasi. Namun, 3 dari antek-anteknya diawasi ketika mereka mencoba untuk menarik uang. Mereka ditangkap dan mereka semua memberi tanda-tanda yang menunjuk keberadaan Levin. Pada tahun 1995, Levin ditangkap.
- Pada akhir semua itu, Levin bisa berhasil, tetapi secara curang mentransfer sekitar $ 10,7 dolar dari rekening Citibank ke akun yang telah dia buat. Pada tahun 1997 dia dibawa ke Amerika Serikat dan mengaku bersalah atas konspirasi untuk menipu serta mencuri $ 3,7 juta. Dia dimasukkan ke dalam penjara selama 3 tahun dan diperintahkan untuk membayar $ 240.015.
- Pada November 1988, sebuah program jahat menyebar ke sekitar 6.000 mesin komputer berbasis Unix. Komputer yang jadi korban menjadi sangat lambat dan tidak bisa digunakan. Kerugiannya ditaksir mencapai jutaan dolar. Kejadian itu kemudian dikenang sebagai The Great Worm, The Great Worm of 1988 memiliki dampak besar pada ranah cyber. Bukan hanya sebagai worm yang awal menyebar di dunia, tapi juga karena membelalakkan mata dunia – terutama masyarakat non-TI pada sebuah bentuk “ancaman jahat” baru. Di balik worm itu adalah seorang brilian bernama Robert Tappan Morris. Ketika itu Morris masih bersekolah di Cornell University, alhasil worm itu pun dinamai sesuai nama belakangnya: Morris Worm.Kengerian yang ditimbulkan akibat Morris Worm diperburuk dengan tindakan yang oleh banyak kalangan dinilai berlebihan terhadap Robert Morris. RTM, demikian ia kadang disebut, menjadi orang pertama yang dihukum dalam Undang-Undang Computer Fraud and Abuse (Penyalahgunaan dan Penipuan dengan Komputer). Dia mendapatkan hukuman 3 tahun masa percobaan dan 4.000 jam layanan masyarakat. Selain itu, Morris juga harus membayar denda dan biaya-biaya lain yang totalnya hingga mencapai US$ 10.000. Kiprah Morris di dunia akademis menunjukkan potret seorang yang cukup brilian. Sebagai lulusan terbaik di Sekolah Menengah Atas, ia telah mencicipi tiga kampus mentereng di Amerika Serikat. Morris pertama kali kuliah di Harvard, lalu melanjutkan ke Cornell dan kembali ke Harvard sebelum akhirnya, hingga saat ini, menjadi Profesor di MIT.

- Michael Calce adalah seorang anak siswa SMA dari Westland, Quebec. Sejak muda ia sudah disebut seorang hacker tepatnya pada umur 15 tahun. Ketika ia sedang melakukan aksinya ia menyamarkan namanya menjadi "MafiaBoy". Alasan mengapa dia disebut seorang hacker karena dia pernah meluncurkan serangan 9 dari 13 root server nama, namun gagal. Dan aksi terheboh nya pada tahun 2000, dia pernah mencoba menargetkan sasarannya terhadap situs-situs komersial besar seperti Yahoo, Ebay, CNN, Amazon.com, Dell, Inc, dan E-Trade, tetapi aksinya terhenti saat ia ditangkap sedang mengacak-acak situs-situs besar tersebut.
- Ketenaran Smith adalah karena menjadi pencipta virus e-mail terkenal, Melissa. Smith mengklaim bahwa virus Melissa tidak pernah dimaksudkan untuk menyebabkan kerusakan, tetapi cara sederhana propagasi (masing-masing komputer yang terinfeksi mengirim email yang terinfeksi)membuat kelebihan beban sistem komputer dan server di seluruh dunia.Virus Smith mengambil gilirannya tidak lazim karena pada awalnya tersembunyi dalam file yang berisi password untuk 80 situs porno terkenal. Nama Melissa berasal dari seorang penari yang dikenal Smith saat dalam perjalanan di Florida. Meskipun lebih dari 60.000 pc terinfeksi virus email daln melakukan pengiriman, Smith adalah satu-satunya orang yang ditahan meski dia hanya mengirim 1email.
- Adrian Lamo adalah seorang analis ancaman virus dan “grey hat” hacker. Dia pertama kali mendapat perhatian media adalah saat merusak beberapa profil jaringan komputer tinggi, termasuk The New York Times, Yahoo, dan Microsoft, yang berpuncak pada tahun 2003 penangkapannya. Pada tahun 2010, Lamo menjadi terlibat dalam skandal yang melibatkan WikiLeaks Bradley Manning, yang ditangkap setelah Lamo dilaporkan kepada otoritas federal bahwa Manning telah membocorkan ratusan ribu dokumen pemerintah AS yang sensitif. Pada bulan Februari 2002 ia masuk ke jaringan komputer internal dari The New York Times, menambahkan namanya ke database internal sumber ahli, dan menggunakan kertas account LexisNexis untuk melakukan penelitian tentang profil tinggi subyek. Tahun 2004, dia membobol New York Times untuk mendapatkan info personal dan beberapa security number dan membobol Microsoft. Dia akhirnya didenda 65.000 dollar AS. Saat ini dia jadi pembicara di beberapa acara seminar
- Hacker yang sebelumnya membuat gempar dunia dengan membuka kunci (unlock) Apple iPhone pada 2007 silam, kini pria berusia 20 tahun itu mengungkapkan dirinya berhasil meng-hack Sony PlayStation 3 (PS3).George Hotz, pria 20 tahun asal Amerika yang telah membobol celah keamanan PS3 yang disebut-sebut sangat sulit untuk ditembus. Pembongkaran PS3 ini, diakui Hotz, adalah “prakarya” terbarunya. Menurut laporan BBC, dia akan mempublikasi temuannya dengan rinci secara online, dalam waktu dekat.“PlayStation 3 seharusnya unhackable (tak bisa dihack). Tetapi, kini tidak ada lagi yang unhackable,” ujar Hotz, yang dikenal dengan nama maya ‘Geohot’. Dia sendiri menyadari perbuatannya bisa mengakibatkan orang-orang untuk memainkan software PS3 bajakan. Namun, Hotz merasa tidak ada niat khusus untuk

memasyarakatkan software bajakan. Motivasi utama Hotz adalah rasa ingin tahu, dan bagaimana membuka platform yang selama ini di rasan aman.kepada BBC.Sebelumnya, nama Hotz juga sempat populer, pada 2007, karena di usianya saat itu 17 tahun, ia berhasil meng-unlock iPhone, yang saat itu dikunci hanya bisa beroperasi dengan layanan operator AT & T. Diperkirakan akibat ulahnya ada Hacker masuk ke PlayStation Network dan mencuri informasi pribadi dari 77 juta pengguna. Namun, Hotz membantah bertanggung jawab atas serangan itu, dan menambahkan "Bisa Menjalankan keamanan homebrew dan menembus skuritas pada perangkat Anda adalah keren; hacking ke server orang lain dan mencuri database dari info pengguna.adalah tidak keren. "

- James yang nama lengkapnya joseph jonathan james lahir di Miami florida 12 Desember 1983 merupakan hacker yang sangat muda. Saat usia 16 tahun harus masuk penjara . Hacker yang dia lakukan adalah menginstal backdoor untuk membobol server Badan Pengurangan Ancaman Pertahanan. DTRA merupakan lembaga Departemen Pertahanan dibebankan dengan mengurangi ancaman terhadap AS dan sekutunya dari senjata nuklir, biologi, kimia, konvensional dan khusus.James juga masuk ke dalam komputer NASA, mencuri software bernilai sekitar $ 1,7 juta.Namun,James kemudian melanggar masa percobaan bahwa ketika ia dites positif untuk penggunaan narkoba dan yang kemudian ditahan oleh Amerika Serikat Marshall Layanan dan diterbangkan ke Alabama federal. Namun, enam bulan di penjara atas pelanggaran dia memperoleh pembebasan bersyarat. James menegaskan bahwa dia jera dan mungkin memulai sebuah perusahaan keamanan komputer.Pada tanggal 18 Mei 2008, Jonathan James ditemukan tewas dari luka tembak , diduga bunuh diri.
- Gary McKinnon, hacker yang pernah membobol 97 komputer NASA, Pentagon dan Dephankam pada 2001-2002 silam.Kelahiran Inggris berusia 41 tahun yang bekerja sebagai computer system administrator di sebuah perusahaan ini punya "achievement" yang mencengangkan: meng-hack komputer dengan tingkat security paling ketat di dunia.Alasan Gary (online nickname: Solo) hanya satu: ia ingin tahu bahwa memang ada proyek pemerintah USA terhadap UFO yang selama ini ditutup-tutupi, dan menurut pengakuan Gary, ia berhasil melihat satu image semacam aircraft yang pastinya bukan buatan bumi. Sayangnya ada suatu "kekonyolan" bahwa ia lupa meng-save image tersebut karena dalam sesaat ia lupa fungsi save pada software RemotelyAnywhere yang ia pakai untuk meng-hack.Gary muda sangat menggemari fiksi ilmiah dan UFO. Gary termotivasi dengan sang ayah tirinya yang pernah berkata kepadanya bahwa ayah tirinya pernah melihat sebuah UFO terbang di atas Bonnybridge, dekat Falkirk. Bonnybridge merupakan salah satu ibukota UFO di dunia. Disebut begitu karena penampakan UFO di sana tertinggi dari wilayah manapun di dunia. Gary juga mengaku menyusun daftar orang-orang di bumi yang bukan human beings. Kata Gary, meski mereka ETs, mereka sudah sangat menyerupai manusia. Sayangnya daftar tersebut ada di dalam komputernya yang disita oleh kepolisian Inggris.Gary terancam dihukum 7

tahun penjara atas kelakukannya dan denda US$250,000. Ia membuat US Government harus mengeluarkan dana sebesar US$700,000 untuk memperbaiki tingkat security sistemnya.Gary mesti mendekam selama tiga tahun di Inggris sebelum rencana ekstradisi ke AS. Bahkan kabarnya penjara Guantanamo sudah menantinya. Namun pada akhir Juli lalu the British House of Lord (semacam MPR (?), di atas House of Commons) bersedia untuk mendengarkan kasus ini, memberi harapan bagi Gary untuk mendapatkan semacam perlindungan. Namun jadwal hearing/pertemuan belum diketahui dengan pasti.

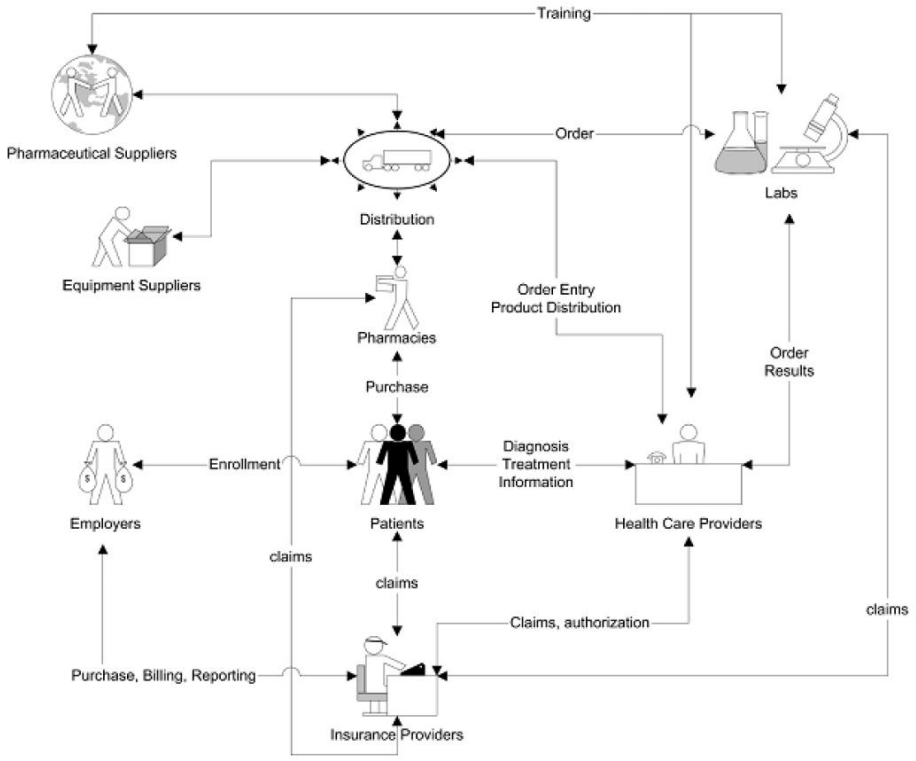
- Jakarta—Pada Mei 2017 lalu, dunia digegerkan dengan serangan *runsomware* WannaCry terhadap lebih dari 200.000 komputer di seluruh dunia. Beberapa pelaku usaha di industri siber melihat ini hanyalah permulaan dari lahirnya serangan *runsomware* yang lebih ganas pada tahun 2018. Jika sebelumnya para penyerang hanya menyasar jaringan infrastruktur berbasis *cloud services* dan perangkat cerdas, mereka tengah bersiap meningkatkan serangannya.
- Wakil kepala Technology Strategy Crowdstrike, Michael Sentonas, menyatakan di masa lalu industri keuangan dan perbankan sangat lazim menjadi incaran serangan siber. Maklum saja, selain sistem operasi dan jaringan yang lemah, industri ini dikenal sebagai gudangnya uang. Para penyerang industri perbankan atau yang dikenal sebagai “hacker economic” tidak menyasar pembobolan rekening satu dua nasabah, namun mereka mengincar data sebagai komoditas lewat *malware* (perangkat rusak) yang mereka gunakan untuk mendulang miliaran dolar AS. Kasus terbaru, pada tahun lalu penyerang melakukan pencurian uang terbesar dengan menggunakan SWIFT *enabled* transfer untuk mencuri 100 juta dolar.
- Menurut Sentonas, setidaknya ada 5 sektor yang rentan terhadap serangan siber di tahun 2018, antara lain *smart city*, transportasi, energi, farmasi, dan telekomunikasi. Pada tahun 2018, kita akan melihat industri-industri berbasis data *end user* menjadi sasaran. Jika semula industri yang disasar hanya keuangan dan perbankan, kini industri yang akan disasar bervariasi, tergantung pada motifnya. Berikut rangkumannya.
- 1. Kota Cerdas (Smart City)
- Beberapa wali kota di dunia, seperti wali kota Hongkong, Taiwan, dan Amerika serikat telah mengadopsi konsep smart city di dalam kotanya untuk meningkatkan kualitas hidup masyarakatnya. Peningkatan kualitas dilakukan melalui pengadaan smart transportation, smart utilities, smart communications, smart health, dan smart security yang biayanya tidaklah murah. Di AS misalnya, pemerintah menggelontorkan dana senilai 40 juta dolar, sementara di Taiwan pemerintah menggelontorkan 625 juta dolar.
- Namun siapa sangka, infrastruktur kota cerdas justru menjadi incaran serangan siber dengan menyisipkan *ransomware* berupa *botnet* yang menyerang Inbound Distributed Denial of Service (DDoS), seperti yang baru terjadi di San Francisco. Penyerang memasang *ransomware* ke dalam sistem dan meminta sejumlah uang tebusan.

- Pintu masuk yang kerap digunakan para penyerang siber adalah *end-point* pada server maupun email *phishing* dengan lampiran yang berisikan *malware*. Jika kontrol protokolnya lemah, para penyerang bahkan bisa menciptakan kerusakan sekunder dan tersier. Mitigasi serangan DDoS Dua Arah adalah kunci untuk menangani serangan DDoS yang bersifat *inbound* maupun *outbound* untuk kekayaan *smart cities* yang berhubungan dengan internet.
- Jaringan transportasi udara, seperti yang baru terjadi di Australia. Perangkat lunak Layanan Angkutan Udara Australia (ASA) baru-baru ini diserang sehingga gagal mengonversi operasi *shift* malam ke operasi *shift* pagi hari. Akibatnya, hanya ada satu tombol kontrol lalu lintas udara beroperasi untuk periode puncak di pagi hari. Sedangkan dalam keadaan normal, enam sampai delapan tombol beroperasi.
- Kegagalan sistem perangkat lunak di kontrol lalu lintas udara Bandara Sydney ini membuat tidak ada gambaran yang masuk ke layar radar dan tanpa hal itu, para petugas di Menara kontrol tidak dapat mengidentifikasi pesawat. Alhasil, hanya sekitar 15 pesawat bisa mendarat dan berangkat per jam dengan menggunakan metode kontrol lalu lintas udara manual, namun biasanya ada sekitar 50 pergerakan per jam dengan menggunakan perangkat lunak.
-
- Pada Juni lalu, BPPT melakukan uji coba terhadap PLTP miliknya di Garut, Jawa Barat. Dari uji coba tersebut, ditemukan ancaman terhadap serangan siber pada pembangkit listrik miliknya yang menggunakan sistem jaringan cerdas (*smart grid*). Seperti diketahui, *smart grid* memungkinkan sistem informasi dua arah antara pembangkit listrik dan penggunanya. Sistem operasi rentan terhadap serangan siber karena menggunakan sistem informasi dan komunikasi yang kurang terbaru serta rentan terhadap serangan siber.
- Pada serangan yang lebih serius, penyerang bisa saja mengambil keuntungan dalam bentuk, seperti mencuri data pelanggan yang memungkinkan pencuri untuk mengetahui apakah tempat tinggal mereka tidak dihuni, atau mengambil alih otorisasi pelanggan untuk menggunakan kartu kredit.
- Skenario yang paling buruk adalah penyerang menggunakan *worm computer* yang melintasi infrastruktur jaringan *smart grid* dan melumpuhkan ribuan kilometer jaringan listrik secara permanen atau hanya untuk sementara dalam beberapa bulan hingga satu tahun. Serangan ini bisa berbahaya jika terjadi, pada Sistem Pembangkit Listrik Jawa-Bali, misalnya.
-
- Jika motivasi penyerang sekadar mencari informasi intelijen atau propaganda besar-besaran, mereka akan menyerang departemen keamanan atau jaringan berbasis *dot gov*. Namun, jika penyerang memang ingin memeras uang, kemungkinan besar mereka akan menyerang bisnis berbasis database, seperti bisnis pengolahan obat-obatan (rumah sakit).

- Targetnya pun tidak hanya perusahaan farmasi atau rumah sakit besar, pelaku usaha mikro, kecil, dan menengah (UMKM) pun akan menjadi sasaran empuk. Di Indonesia, kabarnya sudah banyak serangan siber *ransomware* yang dirasakan di seluruh daerah, seperti meminta uang tebusan terhadap beberapa rumah sakit, dan bukan tidak mungkin target mereka selanjutnya adalah UMKM yang umumnya memiliki sistem keamanan data yang lemah.
- Director Solution & Infrastructure Business PT Multipolar Technology Tbk, Jip Ivan Sutanto menyatakan, sama seperti industri keuangan yang diatur secara ketat dan industri yang terintegrasi secara vertikal dan horizontal, industri kesehatan maupun pengolahan obat-obatan kerap menghadapi persoalan pengolahan data yang tidak hanya tumbuh secara eksponensial atau berlipat-lipat, namun juga ancaman serangan siber.
- Semakin kaya format dan jenis data yang dikumpulkan, pemprosesan dan analisis data akan menjadi semakin beragam dan luas. Untuk itu, diperlukan infrastruktur yang lebih cerdas, hemat, efisien, dan aman. “Ini merupakan hal yang menghantui setiap waktu atas kesiapan perangkat keras di pusat data. Kami sendiri menghadirkan solusi yang menggabungkan kekuatan atau kolaborasi antara teknologi, solusi *hyper-convergence*, dan solusi virtualisasi jaringan dan keamanan platform,” jelasnya.
-
- Sektor industri selanjutnya yang juga memiliki banyak data *end user* adalah telekomunikasi. Data pelanggan menjadi sasaran empuk para penyerang siber. Selain menyerang lewat *runsomware* berupa *petya* maupun *botnet*, penyerang juga akan memeras perusahaan lewat *financial trojans.* Dimulai dari serangan sederhana seperti pencurian data kredensial, mereka akan berevolusi ke sistem serangan yang lebih canggih dan beragam metode.
- Mereka akan fokus pada pertukaran koin (*coin-exchanges*) dan pengguna dompet koin (*coin-wallets*). Mereka adalah target termudah yang memberikan keuntungan tinggi bagi para penjahat siber. Korban juga akan dikelabui untuk memasang *coin-miner* di komputer dan perangkat seluler mereka, padahal sebetulnya mereka menyerahkan seluruh data di CPU mereka.
- Metode lain yang mungkin digunakan penyerang adalah penggunaan *artificial intelligence, machine learning*, serta *internet of things* sebagai medium penyerangan. Penyerang akan meretas perangkat-perangkat pintar karyawan di rumah, dan dengan akses terus-menerus, tidak peduli berapa kali korban membersihkan komputer atau melindungi komputer mereka, penyerang akan selalu memiliki akses ke pintu belakang jaringan korban dan sistem yang menghubungkannya.
- Menurut Sentonas, penggunaan *Security as a Service* (SaaS) dan *Infrastructure as a Service* (IaaS) akan semakin mengurangi peretasan di perusahan pada tahun depan. Selain itu, berbagai perangkat pintar di rumah, seperti TV pintar, AC pintar, kulkas

pintar, kompor pintar, dan jaringannya akan semakin rentan diretas, kemudian si penyerang akan mengunci data pengguna yang pada ujungnya memeras.

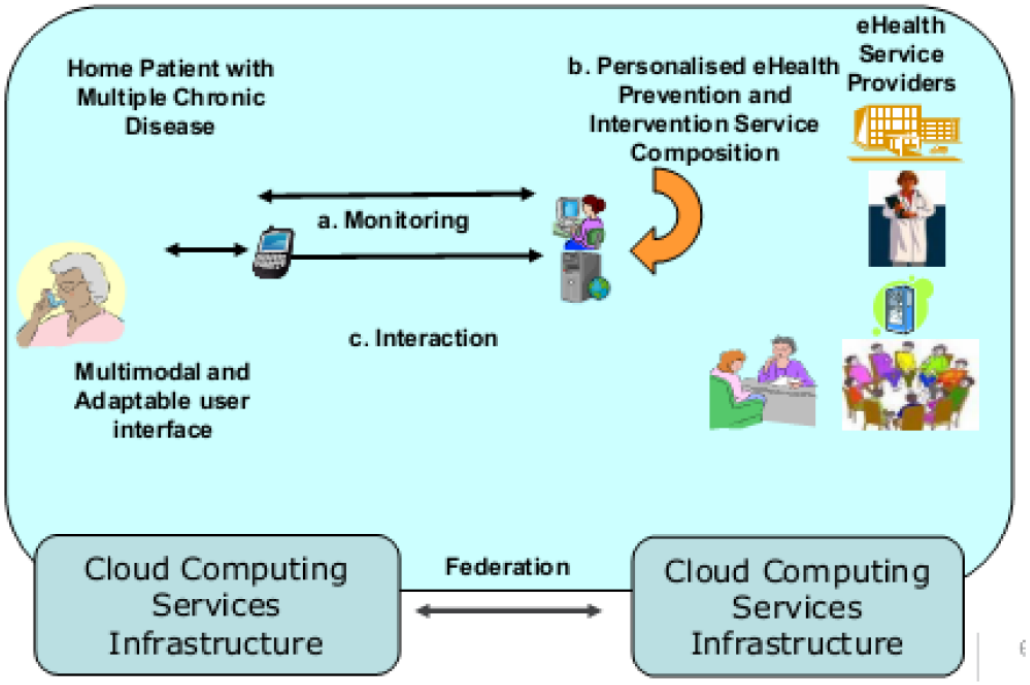
E-*health* merupakan jenis pelayanan kesehatan yang memiliki pertukaran informasi yang sangat kompleks. Kompleksitas e-*health* bisa dilihat pada layanannya, yakni: *content, commerce, connectivity,* dan *care*1. Gambar 1 menunjukkan beberapa pihak yang terlibat dan interaksinya pada jaringan pelayanan kesehatan. Dapat dilihat bahwa kompleksnya alur bisnis, data, dan informasi pada e-health.. Terdapat banyak pihak yang terhubung melalui e-health. Bisa dipastikan kompleksnya pertukaran informasi pada sistem e-health. Sehingga e-health diintegrasikan dengan cloud computing untuk menghemat sumber daya dan memudahkan dalam pertukaran informasinya.



Gambar 1. Jaringan pelayanan kesehatan[1]

Privasi pasien dan informasi kesehatan wajib dilindungi. Hal ini dikarenakan pasien tidak mungkin berbagi informasi yang sangat pribadi kecuali mereka percaya bahwa data mereka dilindungi kerahasiaannya. Kompleksitas alur pertukaran informasi dan data pada e-health menyebabkan e-health sangat rentan terhadap ancaman-ancaman keamanan sistem e-health. Gambar 4 menunjukkan skenario e-health yang terdiri atas 3 poin penting yakni monitoring, pencegahan personal e-health, komposisi intervensi

layanan dan interaksi. Isu utama yang perlu diperhatikan pada sistem e-health adalah proteksi data (privasi), kerahasiaan, properti, dan pelayanan *outsource*2*.*



Gambar 4. Skenario e-*health*[2]

Ukuran keamanan data dilihat dari integritas data, manajemen identitas, dan kontrol akses8.Untuk mendapatkan data yang konsisten dan valid maka integritas data harus diperhatikan. Enkripsi tidak hanya digunakan untuk proses pertukaran data, tetapi pada saat penyimpanan data juga harus diperhatikan. Akses kontrol digunakan untuk mengontrol siapa saja yang terlibat pada jaringan e-*health*, untuk menghindari aksesilegal terhadap sistem.

Aspek Keamanan dan Konfidensialitas Rekam Kesehatan Elektronik (RKE)

Dalam pasal 13 ayat (1) huruf b permenkes 269 tahun 2008 tentang pemanfaatan rekam medis “sebagai alat bukti hukum dalam proses penegakkan hukum, disiplin kedokteran dan kedokteran gigi dan penegakkan etika kedokteran dan etika kedokteran gigi”.
Karena rekam medis merupakan dokumen hukum,maka keamanan berkas sangatlah penting untuk menjaga keabsahan data baik Rekam Kesehatan kertas maupun Rekam Kesehatan Elektronik (RKE).
RKE juga merupakan alat bukti hukum yang sah. Hal tersebut juga ditunjang dengan Undang-Undang Informasi dan Transaksi Elektronik (ITE) pada pasal 5 dan 6 yaitu:
Pasal 5 :

1. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.
2. Informasi elektronik dan/atau dokumen elektronik dan/atau hasil cetaknya sebagaimana dimaksud pada ayat (1) merupakan perluasan dari alat bukti yang sah sesuai dengan Hukum Acara yang berlaku di Indonesia.
3. Informasi elektronik dan/atau dokumen elektronik dinyatakan sah apabila menggunakan sistem elektronik yang sesuai dengan ketentuan yang diatur dalan Undang-Undang ini

Pasal 6:
Dalam hal terdapat ketentuan lain selain yang diatur dalam pasal 5 ayat (4) yang mensyaratkan bahwa suatu informasi harus berbentuk tertulis atau asli, Informasi elektronik dan/atau dokumen elektronik dianggab sah sepanjang informasi yang tercantum di dalamnya dapat diakses, ditampilkan, dijamin keutuhannya, dan dapat dipertanggungjawabkan sehingga menerangkan suatu keadaan.

Keamanan komputer *(computer security*) melingkupi empat aspek, yaitu privacy, integrity, authentication, dan availability. Selain keempat hal di atas, masih ada dua aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu access control dan non-repudiation.

1. Privacy atau confidentiality
   Hal utama dari aspek Privacy atau confidentiality adalah bagaimana untuk menjaga informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi tersebut.

Data rekam medis yang berisi riwayat kesehatan pasien yang bersifat rahasia harus dapat dijaga kerahasiaanya, karena infomasi tersebut merupakan milik pasien. Sedangkan dokumennya merupakan milik dokter,dokter gigi, atau sarana pelayanan kesehatan . seperti yang tertuang pasa pasal 47 UU praktik kedokteran no 29 tahun 2004.

Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Privacy lebih kearah data-data yang sifatnya privat sedangkan confidentiality biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator. Contoh *confidential information* adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari confidentiality adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP).

Untuk mendapatkan kartu kredit, biasanya ditanyakan data-data pribadi. Jika saya mengetahui data-data pribadi anda, termasuk nama ibu anda, maka saya dapat melaporkan melalui telepon (dengan berpura-pura sebagai anda) bahwa kartu kredit anda hilang dan mohon penggunaannya diblokir. Institusi (bank) yang mengeluarkan kartu kredit anda akan percaya bahwa saya adalah anda dan akan menutup kartu kredit anda. Masih banyak lagi kekacauan yang dapat ditimbulkan bila data-data pribadi ini digunakan oleh orang yang tidak berhak.

Dalam bidang kesehatan (*health care*) masalah privacy merupakan topik yang sangat serius di Amerika Serikat. *Health Insurance Portability and Accountability Act* (HIPPA), dikatakan akan mulai digunakan di tahun 2002, mengatakan bahwa rumah sakit, perusahaan asuransi, dan institusi lain yang berhubungan dengan kesehatan harus menjamin keamanan dan privacy dari data-data pasien. Data-data yang dikirim harus sesuai dengan format standar dan mekanisme pengamanan yang cukup baik. Partner bisnis dari institusi yang bersangkutan juga harus menjamin hal tersebut. Suatu hal yang cukup sulit dipenuhi. Pelanggaran akan *act* ini dapat didenda US$ 250.000 atau 10 tahun di penjara.

Serangan terhadap aspek privacy misalnya adalah usaha untuk melakukan penyadapan (dengan program *sniffer*). Usaha-usaha yang dapat dilakukan untuk meningkatkan *privacy* dan *confidentiality* adalah dengan menggunakan teknologi kriptografi (dengan enkripsi dan dekripsi). Ada beberapa masalah lain yang berhubungan dengan *confidentiality*. Apabila kita menduga seorang pemakai (sebut saja X) dari sebuah ISP (Z), maka dapatkah kita meminta ISP (Z) untuk membuka data-data tentang pemakai X tersebut? Di luar negeri, ISP Z akan menolak

permintaan tersebut meskipun bukti-bukti bisa ditunjukkan bahwa pemakai X tersebut melakukan kejahatan. Biasanya ISP Z tersebut meminta kita untuk menunjukkan surat dari pihak penegak hukum (*subpoena*). Masalah privacy atau confidentiality ini sering digunakan sebagi pelindung oleh orang yang jahat/nakal.

2. Integrity

Integrity berkaitan mengenai perubahan informasi. Seperti yang tertuang dalan permenkes 269 tahun 2009, pasal 5 ayat 6 “Pembetulan sebagaimana dimaksud pada ayat (5) hanya dapat dilakukan dengan cara pencoretan tanpa menghilangkan catatan yang dibetulkan dan dibubuhi paraf dokter, dokter gigi atau tenaga kesehatan tertentu yang bersangkutan.”

Pencoretan tentu saja tidak bisa dilakukan dalam rekam kesehatan elektronik. Oleh karena itu diperlukan pengamanan atau proteksi yang lebih yaitu tidak begitu saja menghapus data yang tersimpan dalam rekam kesehatan elektronik tersebut dan segala perubahanya dapat diketahui.

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (*intercept*) di tengah jalan, diubah isinya (*altered*, *tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini.

Salah satu contoh kasus trojan horse adalah distribusi paket program *TCP Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi trojan horse tersebut, maka ketika anda merakit (*compile*) program tersebut, dia akan mengirimkan eMail kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda. Informasi ini berasal dari CERT Advisory, “*CA-99-01 Trojan-TCP-Wrappers*” yang didistribusikan 21 Januari 1999. Contoh serangan lain adalah yang disebut “*man in the middle attack*” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

3.Authentication

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli. Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan digital signature. Watermarking juga dapat digunakan untuk menjaga “*intelectual property*”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat.

Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia:

What you have (misalnya kartu ATM)
What you know (misalnya PIN atau password)
What you are (misalnya sidik jari, biometric)

Penggunaan teknologi *smart card*, saat ini kelihatannya dapat meningkatkan keamanan aspek ini. Secara umum, proteksi authentication dapat menggunakan *digital certificates*. Authentication biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada server atau mesin. Pernahkan kita bertanya bahwa mesin ATM yang sedang kita gunakan memang benar-benar milik bank yang bersangkutan? Bagaimana jika ada orang nakal yang membuat mesin seperti ATM sebuah bank dan meletakkannya di tempat umum? Dia dapat menyadap data-data (informasi yang ada di magnetic strip) dan PIN dari orang yang tertipu. Memang membuat mesin ATM palsu tidak mudah. Tapi, bisa anda bayangkan betapa mudahnya membuat web site palsu yang menyamar sebagai web site sebuah bank yang memberikan layanan Internet Banking. (Ini yang terjadi dengan kasus klikBCA.com.)

Authentication berhubungan dengan akses terhadap informasi. Dalam rekam medis tidak semua tenaga kesehatan dapat memasukkan data atau melakukan perubahan data. Setiap tenaga kesehatan mempunyai kapasitanya masing-masing. Oleh karena itu perlu adanya pembatasan akses. Setiap perubahan harus ada pertanggungjawaban.

Pada pasal 46 UU praktik kedokteran no 29 tahun 2004 menyebutkan bahwa " setiap catatan rekam medis harus dibubuhi nama, waktu, dan tanda tangan petugas yang memberikan pelayanan atau tindakan". Dan pada pasal yang sama ayat (3) menyebutkan "apabila dalam pencatan rekam medis menggunakan teknologi informasi elektronik, kewajiban membubuhi tanda tangan dapat diganti dengan menggunakan nomor identitas pribadi(PIN)"

Pada Rekam Kesehatan Elektronik juga wajib diberi tanda tangan untuk pertanggungjawaban.

Hal tersebut diatur dalam pasal 11 UU ITE yaitu :

(1) Tanda tangan elektronik memiliki kekuatan hukum akibat hukum yang sah selama memenuhi persyaratan sebagai berikut :

a. Data pembuatan tanda tangan elektronik terkait hanya kepada penanda tangan;
b. Data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kausa penanda tangan;
c. Segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. Segala perubahan terhadap informasi elektronik yang terkait tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui;
e. Terdapat cara tertentu yang dipakai untuk mengidentifikasi siapa penandatanganannya:
f. Dan terdapat cara tertentu untuk menunjukkan bahwa penanda tangan telah memberikan persetujuan terhadap informasi elektronik terkait;

4. Availability

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan "*denial of service attack*" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubitubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang*, *crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya (apalagi jika akses dilakukan melalui saluran telepon). Bayangkan apabila anda dikirimi 5000 email dan anda harus mengambil (download) email tersebut melalui telepon dari rumah.

Availability atau ketersediaan adalah aspek yang menekan pada tersediaan informasi ketika dihubungkan oleh pihak-pihak yang terkait.
Sebagai alat kominikasi rekam medis harus selalu tersedia secara cepat dan dapat menampilkan kembali data yang telah tersimpan sebelumnya. Untuk rekam kesehatan ekektronik juga harus mempunyai sifat ketersediaan.

Hal tersebut diatur dalam UU ITE pasal 16 yaitu :

(1) Sepanjang tidak ditentukan lain oleh undang undang tersendiri, setiap Penyelengaraan Sistem Elektronik wajib mengoperasikan sisten elektronik yang memenuhi persyaratan minimum sebagai berikut;
   a. Dapat menampilkan kembali Informasi elektronik dan/atau dokumen elektronik secara utuh sesuai dengan masa retensi yang diterapkan dalam peraturan perundang-undangan;

b. Dapat melindungi ketersediaan, keutuhan. Keoutentikan, kerahasiaan. Dan keteraksesan informasi elektronk dalam Penyelengaraan Sistem Elektronik tersebut;
c. Dapat beroperasi sesuai dengan prosedur atau petunjuk dalam Penyelengaraan Sistem Elektronik tersebut;
d. Dilengkapi dangan prosedur atau petunjuk yang diumumkan dengan bahasa, informasi, atau symbol yang dapat dipahami oleh pihak yang bersangkutan dengan Penyelengaraan Sistem Elektronik tersebut;
e. Memiliki mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

5. Access Control
   access control adalah aspek yang menekankan pada cara pengaturan akses terhadap informasi. access control dapat mengatur siapa-siapa saja yang berhak untuk mengakses infomasi atau siapa-siapa saja yang tidak berhak mengakses informasi.

   Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private, confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Access control seringkali dilakukan dengan menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain (seperti kartu, biometrics).

6. non-repudiation.
   Aspek ini erat kaitannya dengan suatu transaksi atau perubahan informasi. Aspek ini mencegah agar seseorang tidak dapat menyangkal telah melakukan transaksi atau perubahan terhadap suatu informasi.

   Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Sebagai contoh, seseorang yang mengirimkan email untuk memesan barang tidak dapat menyangkal bahwa dia telah mengirimkan email tersebut. Aspek ini sangat penting dalam hal *electronic commerce*. Penggunaan *digital signature*, *certifiates*, dan teknologi kriptografi secara umum dapat menjaga aspek ini. Akan tetapi hal ini masih harus didukung oleh hukum sehingga status dari *digital signature* itu jelas legal. Hal ini akan dibahas lebih rinci pada bagian tersendiri.

Hukum kesehatan mencakup segala peraturan dan aturan yang secara langsung berkaitan dengan pemeliharaan dan perawatan kesehatan yang terancam atau kesehatan yang rusak. Hukum kesehatan mencakup penerapan hukum perdata dan

hukum pidana yang berkaitan dengan hubungan hukum dalam pelayanan kesehatan. Menjaga keamanan dalam menyimpan informasi, unsur keakuratan informasi dan kemudahan akses menjadi tuntutan pihak organisasi pelayanan kesehatan, praktisi kesehatan serta pihak ke-3 yang berwenang. Sedangkan pihak yang membutuhkan informasi harus senantiasa menghormati privasi pasien. Secara keseluruhan, keamanan, privasi, kerahasiaan dan keselamatan adalah perangkat yang membentengi informasi dalam rekam medis. Dengan begitu berbagai pihak yang berwenang yang membutuhkan informasi yang lebih rinci sesuai dengan tugasnya senantiasa menjaga keempat unsur diatas. Dalam konsep pelayanan kesehatan, dikenal istilah privasi, kerahasiaan, dan keamanan.

a) Privasi adalah hak seseorang untuk mengontrol akses informasi atas rekam medis pribadinya.

b) Kerahasiaan adalah proteksi terhadap rekam medis dan informasi lain pasien dengan cara menjaga informasi pribadi pasien dan pelayanannya. Dalam pelayanan kesehatan, informasi itu hanya diperuntukkan bagi pihak tenaga kesehatan yang berwenang.

c) Keamanan adalah perlindungan terhadap privasi seseorang dan kerahasiaan rekam medis. Dengan kata lain, keamanan hanya memperbolehkan penggunan yang berhak untuk membuka rekam medis. Dalam pengertian yang lebih luas , keamanan juga termasuk proteksi informasi pelayanan kesehatan dari rusak, hilang atau pengubahan data akibat ulah pihak yang tidak berhak.

Serangan Terhadap Keamanan Sistem Informasi

Security attack, atau serangan terhadap keamanan sistem informasi, dapat dilihat dari sudut peranan komputer atau jaringan komputer yang fungsinya adalah sebagai penyedia informasi. Menurut W. Stallings [40] ada beberapa kemungkinan serangan (*attack*):

• *Interruption*: Perangkat sistem menjadi rusak atau tidak tersedia.Serangan ditujukan kepada ketersediaan (*availability*) dari sistem.
Contoh serangan adalah “denial of service attack”.

• *Interception*: Pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).

• *Modification*: Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesanpesan yang merugikan pemilik web site.

• *Fabrication*: Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesanpesan palsu seperti e-mail palsu ke dalam jaringan komputer.