PERTEMUAN 1
PENGENALAN KEAMANAN KOMPUTER

A. TUJUAN PEMBELAJARAN

Pada Pertemuan ini akan dijelaskan mengenai definisi jaringan komputer, tujuan dan manfaat jaringan komputer, kelebihan serta kekurangan pada jaringan komputer, Setelah mempelajari materi ini mahasiswa diharapkan mampu untuk:

1. Mendefinisikan keamanan komputer.
2. Memahami konsep keamanan komputer.
3. Mampu mendeskripsikan jenis-jenis ancaman keamanan komputer.

B. URAIAN MATERI

1. Mendefinisikan Keamanan Komputer

Sebuah kamus mendefinisikan keamanan sebagai "kualitas atau kondisi bebas dari bahaya" atau "tindakan yang diambil untuk mencegah pengintaian atau sabotase, kejahatan, serangan, atau kehilangan." Istilah "serangan" (*attack*) dan "ancaman" (*threat*) yang digunakan disini untuk mengidentifikasi aktivitas apapun yang bertujuan untuk mendapatkan akses ke komputer dengan maksud tujuan jahat.

Istilah "lubang keamanan" (*security hole*), "kelemahan" (*weakness*), dan "kerentanan" (*vulnerability*) mengacu pada keadaan yang dapat dieksploitasi untuk semacam serangan. Beberapa bahkan ada yang beranggapan bahwa lubang keamanan mengundang serangan. (Salomon, 2006)

Berdasarkan kutipan dari buku yang berjudul “Security in Computing, Fifth Edition” (2015), mendefinisikan keamanan komputer ialah perlindungan terhadap barang yang berharga bagi kita, yaitu *aset* komputer atau sistem komputer. (Charles P Pfleeger, 2015)

Adapun “The NIST An Introduction to Information Security” (2017) mendefinisikan keamanan komputer sebagai tindakan dan kontrol yang memastikan kerahasiaan, integritas, dan ketersediaan aset sistem informasi termasuk perangkat keras, perangkat lunak, firmware, dan informasi yang

sedang diproses, disimpan, dan dikomunikasikan. (Nieles, Dempsey, & Pillitteri, 2017)

Perangkat komputer (termasuk perangkat keras (*hardware*), komponen tambahan, dan aksesori) tentunya merupakan aset. Karena sebagian besar perangkat keras komputer tidak berguna tanpa program, perangkat lunak (software) juga merupakan aset. Perangkat lunak mencakup sistem operasi, utilitas, dan perangkat kendali, aplikasi seperti pengolah kata, pemutar media, dan bahkan program yang mungkin kita buat sendiri. Hal yang membuat komputer kita unik dan penting bagi kita adalah isinya: foto, lagu, makalah, pesan email, proyek, informasi kalender, ebooks, informasi kontak, kode yang kita buat, dan sejenisnya. Jadi, item data di komputer juga merupakan aset. Tidak seperti kebanyakan perangkat keras dan perangkat lunak, data dapat menjadi sulit jika dibuat ulang atau diganti. Demikian dapat disimpulkan apa yang perlu kita amankan diantaranya:

a. Perangkat Keras
    1) Komputer
    2) Alat (disk drive, memory, printer)
    3) Komponen Jaringan
b. Perangkat Lunak
    1) Sistem Operasi
    2) Utilitas (antivirus)
    3) Aplikasi komersil (word processing, photo editing)
    4) Aplikasi pribadi/individual
c. Data
    1) Dokumen
    2) Foto
    3) Musik, video
    4) Email
    5) Projek kelas

Klasifikasi Ancaman

Ada banyak jenis ancaman (*threat*) dan masalah keamanan komputer, tetapi secara garis besar dapat diklasifikasikan sebagai berikut:

a. Physical. Komputer pribadi dapat dicuri. Komputer pusat yang besar dapat dibobol dan peralatannya diambil. Kebakaran, lonjakan arus listrik, dan banjir

dapat merusak perangkat keras komputer dan sambungan jaringan serta menyebabkan hilangnya data.

b. Rogue Software. Kita semua pernah mendengar tentang virus komputer. Program kecil dan licik yang menyerang komputer kita dan menyebar dengan cepat dan tanpa suara. Virus hanyalah salah satu aspek dari ancaman umum yang ditimbulkan oleh rogue software.
c. Sebagian besar komputer terhubung ke jaringan, dan sebagian besar jaringan lokal terhubung ke Internet. Dengan demikian, ada ancaman keamanan komputer tingkat tinggi yang terkait dengan jaringan dan termasuk dalam kategori keamanan jaringan (*network security*). Area keamanan yang luas ini mencakup ancaman seperti pemindaian port (*port scanning*), spoofing, pembobolan kata sandi (*password cracking*), spyware, dan pencurian identitas (*identity theft*). (Salomon, 2006)

2. Konsep Keamanan Komputer

Pikirkan tentang apa yang membuat komputer berharga bagi kita. Pertama, kita menggunakannya sebagai alat untuk mengirim dan menerima email, menelusuri web, menulis makalah, dan melakukan banyak tugas lainnya, dan mengharapkannya tersedia untuk digunakan saat kita menginginkannya. Tanpa komputer, tugas-tugas tersebut akan lebih sulit, bahkan tidak mungkin.

Kedua, sangat bergantung pada integritas komputer kita. Saat mengetik dokumen dan menyimpannya, kita percaya bahwa dokumen akan dimuat ulang persis seperti kita menyimpannya. Demikian pula, kita berharap bahwa foto yang diberikan teman di flash drive akan tampak sama saat kita memuatnya di komputer pribadi seperti saat kita melihatnya di komputer teman.

Terakhir, kita mengharapkan aspek “pribadi” dari komputer pribadi tetaplah pribadi, artinya kita ingin menjaga kerahasiaannya. Misalnya kita ingin pesan email berada tepat di antara kita dan penerima yang terdaftar, kita tidak ingin pesan tersebut disiarkan pada orang lain. Contoh lainnya saat kita menulis esai atau tugas, kita berharap tidak ada yang bisa menyalinnya tanpa izin kita.

Gambar 1. Konsep C.I.A

Ketiga aspek ini (konsep C.I.A.), kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) membuat komputer berharga bagi kita. Jika seseorang mencuri komputer kita, mengacak data di disk kita, atau melihat file data pribadi kita, nilai computer kita telah berkurang atau kita telah mengalami kerugian dalam penggunaan komputer kita sendiri. Ketiga aspek tersebut merupakan tujuan utama bahasan ini yang mana bisa juga dikatakan jantung dari keamanan komputer.

a. Confidentiality

Dalam konteks keamanan komputer, kerahasiaan adalah menghindari pengungkapan informasi yang tanpa izin. Artinya, kerahasiaan melibatkan perlindungan data, memberikan akses bagi mereka yang diizinkan untuk melihatnya sementara melarang orang lain mempelajari apapun tentang isinya.

Menjaga kerahasiaan informasi sering kali menjadi inti dari keamanan informasi, dan konsep ini sebenarnya sudah ada sebelum komputer. Misalnya, dalam penggunaan kriptografi pertama yang tercatat, Julius Caesar mengkomunikasikan perintah kepada jenderalnya menggunakan sandi sederhana. Dalam sandi, Caesar mengambil setiap huruf dalam pesannya dan mengganti D dengan A, E untuk B, dan seterusnya. Sandi ini dapat dengan mudah dipecahkan, menjadikannya alat yang tidak tepat untuk mencapai kerahasiaan saat ini. Tetapi pada masanya, sandi Caesar mungkin cukup aman, karena sebagian besar musuh Caesar tidak dapat membaca bahasa Latin.

Saat ini, mencapai kerahasiaan lebih merupakan tantangan. Komputer ada di mana-mana, dan masing-masing mampu melakukan operasi yang dapat membahayakan kerahasiaan. Dengan semua ancaman terhadap kerahasiaan informasi ini, peneliti keamanan komputer dan perancang sistem telah menemukan sejumlah alat untuk melindungi informasi sensitif. Alat-alat ini menggabungkan konsep-konsep berikut:

1) *Encryption*: transformasi informasi menggunakan suatu rahasia yang disebut kunci enkripsi (*encryption key*), sehingga informasi yang diubah hanya dapat dibaca menggunakan suatu rahasia lain, yang disebut kunci dekripsi (*decryption key*) (dalam beberapa kasus mungkin sama dengan kunci enkripsi). Agar aman, skema enkripsi harus mempersulit seseorang untuk menentukan informasi asli tanpa menggunakan kunci dekripsi.
2) *Access control*: aturan dan kebijakan yang membatasi akses terhadap informasi rahasia untuk orang-orang dan atau sistem yang “perlu tahu”. “Perlu tahu” disini dapat ditentukan oleh identitas, seperti nama seseorang atau nomor seri komputer, atau peran yang dimiliki seseorang, seperti menjadi manajer atau spesialis keamanan komputer.
3) *Authentication*: penentuan identitas atau peran yang dimiliki seseorang. Penentuan ini dapat dilakukan dengan beberapa cara berbeda, tetapi biasanya didasarkan pada kombinasi dari sesuatu yang dimiliki orang tersebut (seperti kartu pintar (*smart card)* atau kunci radio yang menyimpan kunci rahasia), sesuatu yang diketahui orang tersebut (seperti kata sandi), dan sesuatu dari orang itu (seperti manusia dengan sidik jari).
4) *Authorization*: penentuan apakah seseorang atau sistem diizinkan mengakses sumber daya, berdasarkan kebijakan kontrol akses. Otorisasi tersebut harus mencegah penyerang menipu sistem agar membiarkannya memiliki akses ke sumber daya yang dilindungi.
5) *Physical security*: pembentukan penghalang fisik untuk membatasi akses ke sumber daya komputasi yang dilindungi. Penghalang tersebut antara lain kunci lemari dan pintu, penempatan komputer di ruangan tanpa jendela, penggunaan bahan peredam suara, dan bahkan pembangunan gedung atau ruangan dengan dinding yang dilengkapi jerat tembaga (disebut sangkar Faraday), sehingga sinyal elektromagnetik tidak dapat masuk atau keluar ruangan.

Goodrich & Tamassia, 2014)

b. Integrity

Aspek penting lainnya dari keamanan informasi adalah integritas, yang merupakan konsistensi, akurasi, validitas data atau informasi. Salah satu tujuan dari program keamanan informasi yang berhasil adalah untuk memastikan bahwa informasi dilindungi dari perubahan yang tidak sah (*unauthorized)* atau tidak disengaja. Program harus mencakup proses dan prosedur untuk mengelola perubahan yang disengaja, serta kemampuan untuk mendeteksi perubahan. (Panek, 2020)

Misalnya, jika mengatakan bahwa kita telah menjaga integritas suatu barang, yang kita maksud adalah item tersebut:

1) Tepat
2) Akurat
3) tidak dimodifikasi
4) dimodifikasi hanya dengan cara yang dapat diterima
5) dimodifikasi hanya oleh orang yang berwenang
6) dimodifikasi hanya dengan proses resmi
7) konsisten
8) konsisten secara internal
9) bermakna dan berguna (Charles P Pfleeger, 2015)

Beberapa proses yang dapat digunakan untuk memastikan integritas informasi secara efektif termasuk otentikasi, otorisasi, dan akuntansi. Misalnya, hak dan izin dapat digunakan untuk mengontrol siapa yang dapat mengakses informasi atau sumber daya. Selain itu, fungsi hashing (fungsi matematika) dapat dihitung sebelum dan sesudah untuk menunjukkan jika informasi telah dimodifikasi. Selain itu, sistem audit atau akuntansi dapat digunakan untuk mencatat ketika perubahan telah dilakukan. (Panek, 2020)

Selain itu, terdapat beberapa alat bantu yang dirancang khusus untuk mendukung integritas, antara lain sebagai berikut:

1) *Backups*: pengarsipan data secara berkala. Pengarsipan ini dilakukan agar file data dapat dipulihkan jika pernah diubah dengan cara yang tidak sah atau tidak disengaja.

2) *Checksums*: penghitungan fungsi yang memetakan konten file ke nilai numerik. Fungsi checksum bergantung pada seluruh konten file dan dirancang sedemikian rupa sehingga bahkan perubahan kecil pada file input sangat mungkin menghasilkan nilai output yang berbeda. Checksum seperti kabel trip yang digunakan untuk mendeteksi ketika terjadi pelanggaran integritas data.
3) *Data correcting codes*: metode untuk menyimpan data sedemikian rupa perubahan kecil dapat dengan mudah dideteksi dan dikoreksi secara otomatis. Kode ini biasanya diterapkan pada unit penyimpanan kecil (misal, ditingkat byte atau tingkat kata memori), tetapi ada juga koreksi data kode yang dapat diterapkan ke seluruh file juga. (Goodrich & Tamassia, 2014)

c. Availability

Selain kerahasiaan dan integritas, aspek penting lainnya dari keamanan informasi adalah ketersediaan, yaitu aspek di mana informasi dapat diakses dan dimodifikasi secara tepat waktu oleh mereka yang berwenang untuk melakukannya.

Informasi yang dikunci dan dijaga sepanjang waktu dapat dianggap aman. Tetapi secara praktis tidak aman dari perspektif keamanan informasi jika kita membutuhkan waktu berminggu-minggu atau berbulan-bulan untuk mendapatkannya. Kualitas beberapa informasi secara langsung terkait dengan ketersediaannya.

Misalnya, harga saham paling berguna saat masih hangat. Juga, bayangkan kerusakan yang dapat terjadi jika seseorang mencuri kartu kredit kita dan butuh waktu berminggu-minggu sebelum perusahaan kartu kredit kita dapat memberi tahu siapa pun, karena daftar nomor yang dicuri tidak tersedia bagi *merchants*. Jadi, terkait dengan kerahasiaan dan integritas, peneliti keamanan komputer dan perancang sistem telah mengembangkan sejumlah alat untuk menyediakan ketersediaan, termasuk yang berikut ini:

1) *Physical protections*: infrastruktur yang dimaksudkan untuk menjaga informasi tetap tersedia bahkan saat terjadi tantangan fisik. Perlindungan semacam itu dapat mencakup bangunan yang menampung sistem komputer penting yang akan dibangun agar tahan terhadap badai, gempa bumi, dan ledakan bom, dan dilengkapi dengan generator dan peralatan

elektronik lainnya agar dapat mengatasi pemadaman listrik dan lonjakan arus.

2) *Computational redundancies*: komputer dan perangkat penyimpanan yang berfungsi sebagai cadangan jika terjadi kegagalan. Misalnya, *redundant arrays of inexpensive disks* (RAID) menggunakan redundansi penyimpanan untuk menjaga data tetap tersedia bagi klien mereka. Selain itu, server web sering kali diatur dalam kelipatan yang disebut "farms" sehingga kegagalan satu komputer dapat ditangani tanpa menurunkan ketersediaan situs web.

Karena ketersediaan sangat penting, penyerang yang tidak peduli dengan kerahasiaan atau integritas data dapat memilih untuk menyerang ketersediaannya. Misalnya, pencuri yang mencuri banyak kartu kredit mungkin ingin menyerang ketersediaan daftar kartu kredit curian yang disimpan dan disiarkan oleh perusahaan kartu kredit besar. Dengan demikian, ketersediaan merupakan salah satu dari dukungan untuk konsep C.I.A. (Goodrich & Tamassia, 2014)

Selain konsep C.I.A. *confidentiality*, *integrity*, dan *availability*, dibahas di bagian sebelumnya, terdapat sejumlah konsep tambahan yang juga penting dalam aplikasi keamanan komputer modern. Konsep-konsep ini juga dapat dicirikan oleh akronim tiga huruf, A.A.A., yang dalam konteks ini mengacu pada *assurance*, *authenticity*, dan *anonymity*.

d. Assurance

Jaminan (*assurance*), dalam konteks keamanan komputer, mengacu pada bagaimana kepercayaan diberikan dan dikelola dalam sistem komputer. Memang, kepercayaan itu sendiri sulit untuk diukur, tetapi kita tahu itu melibatkan sejauh mana kita memiliki keyakinan bahwa orang atau sistem berperilaku seperti yang kita harapkan.

e. Authenticity

Keaslian (*authenticity*) adalah kemampuan untuk menentukan bahwa pernyataan, kebijakan, dan izin yang dikeluarkan oleh orang atau sistem adalah asli. Jika hal-hal seperti itu dapat dipalsukan, tidak ada cara untuk menegakkan kontrak tersirat yang melibatkan orang dan sistem saat membeli dan menjual barang secara online. Selain itu, seseorang atau sistem dapat

mengklaim bahwa mereka tidak membuat komitmen semacam itu, mereka dapat mengatakan bahwa komitmen tersebut dibuat oleh seseorang yang berpura-pura menjadi mereka.

f. Anonymity

Ketika orang berinteraksi dengan sistem dengan cara yang melibatkan identitas dunia nyata mereka, interaksi ini dapat memiliki sejumlah manfaat positif. Namun, ada efek samping yang tidak menguntungkan dari penggunaan identitas pribadi dalam transaksi elektronik semacam itu. Kita akhirnya menyebarkan identitas di sejumlah catatan digital, yang menghubungkan identitas kita dengan riwayat medis, riwayat pembelian, catatan hukum, komunikasi email, catatan pekerjaan, dll. Oleh karena itu, kita memiliki kebutuhan untuk anonimitas (*anonymity*), yang merupakan aspek yang catatan atau transaksi tertentu yang tidak dapat diatribusikan kepada individu mana pun.

3. Mampu mendeskripsikan jenis-jenis ancaman keamanan komputer

Ancaman (*threat*) adalah potensi pelanggaran keamanan. Pelanggaran sebenarnya tidak perlu terjadi karena ada ancaman. Fakta bahwa pelanggaran mungkin terjadi berarti bahwa tindakan-tindakan yang dapat menyebabkannya terjadi harus dijaga (atau dipersiapkan). Tindakan itu disebut serangan (*attack*). Mereka yang melakukan tindakan seperti itu, atau menyebabkannya dieksekusi, disebut penyerang.

Tiga aspek keamanan kerahasiaan, integritas, dan ketersediaan melawan ancaman terhadap keamanan sistem. Robert Shirey (Shirey, 2007) membagi ancaman menjadi empat kelas besar: pengungkapan (*disclosure*), atau akses tidak sah terhadap informasi; penipuan (*deception*), atau penerimaan data palsu; gangguan (*disruption*), atau gangguan atau pencegahan operasi yang benar; dan perampasan (*usurpation*), atau kontrol tidak sah dari beberapa bagian sistem. Empat kelas besar ini mencakup banyak ancaman umum.

Snooping/eavesdropping, penyadapan informasi yang tidak sah, adalah salah satu bentuk pengungkapan. Ini pasif, hanya menunjukkan bahwa beberapa entitas mendengarkan (atau membaca) komunikasi atau menjelajahi file atau

informasi sistem. Penyadapan pasif adalah bentuk pengintaian di mana jaringan dipantau. Layanan kerahasiaan berusaha untuk melawan ancaman ini.

Modification/alteration, perubahan informasi yang tidak sah, mencakup tiga kelas ancaman. Sasarannya mungkin penipuan, di mana beberapa entitas bergantung pada data yang dimodifikasi untuk menentukan tindakan mana yang harus diambil, atau di mana informasi yang salah diterima sebagai benar dan dirilis. Jika data yang dimodifikasi mengontrol pengoperasian sistem, ancaman gangguan dan perampasan akan muncul. Tidak seperti pengintaian, modifikasinya aktif; itu hasil dari entitas yang mengubah informasi. Penyadapan aktif adalah bentuk modifikasi di mana data yang bergerak melintasi jaringan diubah, data baru dimasukkan, atau bagian dari data dihapus; istilah "aktif" membedakannya dari *snooping* (penyadapan "pasif"). Contohnya adalah serangan man-in-the-middle, di mana penyusup membaca pesan dari pengirim dan mengirim (kemungkinan dimodifikasi) versinya ke penerima, dengan harapan penerima dan pengirim tidak akan menyadari kehadiran perantara. Layanan integritas berusaha untuk melawan ancaman ini.

Masquerading/spoofing, peniruan satu entitas oleh entitas lain, adalah bentuk penipuan dan perampasan. Ini memikat korban untuk percaya bahwa entitas yang berkomunikasi dengannya adalah entitas yang berbeda. Misalnya, jika pengguna mencoba masuk ke komputer melalui Internet tetapi menjangkau komputer lain yang mengklaim sebagai komputer yang diinginkan, pengguna tersebut telah dipalsukan. Demikian pula, jika pengguna mencoba membaca halaman web, tetapi penyerang telah mengatur agar pengguna diberi halaman yang berbeda, spoof lain telah terjadi. Ini mungkin serangan pasif (di mana pengguna hanya mengakses halaman web), tetapi biasanya merupakan serangan aktif (di mana penyerang mengeluarkan tanggapan secara dinamis untuk menyesatkan pengguna tentang halaman web). Meskipun penyamaran pada dasarnya adalah tipuan, hal ini sering digunakan untuk merebut kendali sistem oleh penyerang yang meniru manajer atau pengontrol resmi. Layanan integritas (disebut "layanan otentikasi" dalam konteks ini) berusaha untuk melawan ancaman ini. Beberapa bentuk penyamaran mungkin diperbolehkan. Delegasi terjadi ketika satu entitas mengotorisasi entitas kedua untuk menjalankan fungsi atas namanya. Perbedaan antara pendelegasian dan penyamaran itu penting. Jika Susan mendelegasikan wewenang kepada Thomas untuk bertindak atas namanya, dia memberikan izin kepadanya untuk melakukan

tindakan tertentu seolah-olah dia melakukannya sendiri. Semua pihak mengetahui adanya delegasi tersebut. Thomas tidak akan berpura-pura menjadi Susan; sebaliknya, dia akan berkata, "Saya Thomas dan saya memiliki wewenang untuk melakukan ini atas nama Susan." Jika diminta, Susan akan memverifikasi ini. Di sisi lain, dalam penyamaran, Thomas akan berpura-pura menjadi Susan. Tidak ada pihak lain (termasuk Susan) yang akan mengetahui penyamaran tersebut, dan Thomas akan berkata, "Saya Susan." Jika ada yang mengetahui bahwa dia berurusan dengan Thomas dan bertanya kepada Susan tentang hal itu, dia akan menyangkal bahwa dia mengizinkan Thomas untuk bertindak atas namanya. Meskipun penyamaran merupakan pelanggaran keamanan, delegasi tidak.

Repudiation of origin, penyangkalan palsu bahwa suatu entitas mengirim (atau menciptakan) sesuatu, adalah bentuk penipuan. Misalnya, pelanggan mengirim surat ke vendor yang setuju untuk membayar sejumlah besar uang untuk suatu produk. Vendor mengirimkan produk dan kemudian meminta pembayaran. Pelanggan menyangkal telah memesan produk dan, menurut undang-undang di negara bagian pelanggan, oleh karena itu berhak menyimpan pengiriman yang tidak diminta tanpa pembayaran. Pelanggan menolak asal muasal surat tersebut. Jika vendor tidak dapat membuktikan bahwa surat tersebut berasal dari pelanggan, serangan berhasil. Variasi dari ini adalah penolakan oleh pengguna bahwa ia membuat informasi atau entitas tertentu seperti file. Mekanisme integritas mencoba untuk mengatasi ancaman ini.

Denial of receipt, penyangkalan palsu bahwa suatu entitas menerima beberapa informasi atau pesan, adalah bentuk penipuan. Misalkan pelanggan memesan produk yang mahal, tetapi vendor meminta pembayaran sebelum pengiriman. Pelanggan membayar, dan vendor mengirimkan produk. Pelanggan kemudian bertanya kepada vendor kapan dia akan menerima produk tersebut. Jika pelanggan telah menerima produk, pertanyaan tersebut merupakan serangan penolakan penerimaan. Vendor dapat mempertahankan diri dari serangan ini hanya dengan membuktikan bahwa pelanggan memang menerima produk, meskipun menyangkal. Mekanisme integritas dan ketersediaan berusaha untuk mencegah serangan ini.

Delay, penghambatan layanan sementara, adalah bentuk perampasan, meskipun dapat memainkan peran pendukung dalam penipuan. Biasanya,

pengiriman pesan atau layanan membutuhkan waktu *t*; jika penyerang dapat memaksa pengiriman untuk memakan waktu lebih dari *t*, penyerang telah berhasil menunda pengiriman. Ini membutuhkan manipulasi struktur kontrol sistem, seperti komponen jaringan atau komponen server, dan karenanya merupakan bentuk perampasan. Jika suatu entitas menunggu pesan otorisasi yang tertunda, itu mungkin meminta server sekunder untuk otorisasi. Meskipun penyerang mungkin tidak dapat menyamar sebagai server utama, dia mungkin dapat menyamar sebagai server sekunder dan memberikan informasi yang salah. Mekanisme ketersediaan seringkali dapat menggagalkan ancaman ini.

Denial of service, penghambatan layanan jangka panjang, adalah bentuk perampasan, meskipun sering digunakan dengan mekanisme lain untuk menipu. Penyerang mencegah server menyediakan layanan. Penolakan dapat terjadi di sumber (dengan mencegah server mendapatkan sumber daya yang diperlukan untuk menjalankan fungsinya), di tujuan (dengan memblokir komunikasi dari server), atau di sepanjang jalur perantara (dengan membuang pesan dari klien atau server, atau keduanya). Denial of service menimbulkan ancaman yang sama dengan penundaan yang tak terbatas. Mekanisme ketersediaan berusaha untuk melawan ancaman ini. (Bishop, 2019)

4. Membuat Strategi Keamanan Komputer

Mengingat spesifikasi kebijakan keamanan (*security* policy) tentang tindakan "aman" dan "tidak aman", mekanisme keamanan (*security* mechanisms) dapat mencegah serangan (*prevent*), mendeteksi serangan (*detect*), atau memulihkan dari serangan (*recovery*). Strategi tersebut dapat digunakan bersama atau terpisah.

Pencegahan berarti serangan akan gagal. Misalnya, jika seseorang mencoba membobol sebuah host melalui Internet dan host tersebut tidak terhubung ke Internet, serangan tersebut telah dicegah. Biasanya, pencegahan melibatkan implementasi mekanisme yang membatasi pengguna untuk tindakan tertentu dan yang dipercaya untuk diterapkan dengan cara yang benar dan tidak dapat diubah, sehingga penyerang tidak dapat mengalahkan mekanisme tersebut dengan mengubahnya. Mekanisme pencegahan sering kali sangat rumit dan mengganggu penggunaan sistem sampai-sampai menghalangi penggunaan normal sistem. Tetapi beberapa mekanisme pencegahan sederhana, seperti kata

sandi (yang bertujuan untuk mencegah pengguna yang tidak sah mengakses sistem), telah diterima secara luas. Mekanisme pencegahan dapat mencegah kompromi bagian-bagian system, sekali di tempat, sumber daya yang dilindungi oleh mekanisme tidak perlu dipantau untuk masalah keamanan, setidaknya dalam teori.

Deteksi menunjukkan keefektifan tindakan pencegahan, dan sangat berguna jika serangan tidak dapat dicegah. Mekanisme deteksi menerima bahwa serangan akan terjadi. Tujuannya adalah untuk menentukan bahwa serangan sedang berlangsung, atau telah terjadi, dan melaporkannya. Namun, serangan tersebut dapat dipantau untuk memberikan data tentang sifat, tingkat keparahan, dan hasilnya. Mekanisme deteksi khas memantau berbagai aspek sistem, mencari tindakan atau informasi yang mengindikasikan serangan. Contoh yang baik dari mekanisme seperti itu adalah yang memberikan peringatan ketika pengguna memasukkan kata sandi yang salah tiga kali. Proses masuk dapat dilanjutkan, tetapi pesan kesalahan di log sistem melaporkan jumlah sandi salah ketik yang sangat tinggi. Mekanisme deteksi tidak mencegah gangguan pada bagian-bagian sistem, yang merupakan kelemahan serius. Sumber daya yang dilindungi oleh mekanisme deteksi terus menerus atau secara berkala dimonitor untuk masalah keamanan.

Pemulihan memiliki dua bentuk. Yang pertama adalah menghentikan serangan dan menilai serta memperbaiki kerusakan yang disebabkan oleh serangan itu. Sebagai contoh, jika penyerang menghapus file, salah satu mekanisme pemulihannya adalah memulihkan file dari media cadangan. Dalam praktiknya, pemulihan jauh lebih kompleks, karena sifat setiap serangan itu unik. Dengan demikian, jenis dan tingkat kerusakan bisa sulit untuk dikarakterisasi sepenuhnya. Selain itu, penyerang dapat kembali, jadi pemulihan melibatkan identifikasi dan perbaikan kerentanan yang digunakan oleh penyerang untuk memasuki sistem. Dalam beberapa kasus, pembalasan (dengan menyerang sistem penyerang atau mengambil langkah hukum untuk meminta pertanggungjawaban penyerang) adalah bagian dari pemulihan. Dalam semua kasus ini, fungsi sistem dihambat oleh serangan tersebut. Menurut definisi, pemulihan membutuhkan dimulainya kembali operasi yang benar.

Dalam bentuk pemulihan kedua, sistem terus berfungsi dengan benar saat serangan sedang berlangsung. Jenis pemulihan ini cukup sulit untuk diterapkan

karena kompleksitas sistem komputer. Ini mengacu pada teknik toleransi kesalahan serta teknik keamanan dan biasanya digunakan dalam sistem yang kritis terhadap keselamatan. Ini berbeda dari bentuk pemulihan pertama, karena tidak ada gunanya sistem berfungsi dengan benar. Namun, sistem dapat menonaktifkan fungsionalitas yang tidak penting. Tentu saja, jenis pemulihan ini sering diterapkan dalam bentuk yang lebih lemah di mana sistem mendeteksi kesalahan fungsi secara otomatis dan kemudian mengoreksi (atau mencoba untuk memperbaiki) kesalahan tersebut. (Bishop, 2019)

C. SOAL LATIHAN/ TUGAS

1. Jelaskan definsi keamanan komputer yang Anda ketahui!
2. Dalam konsep keamanan komputer, apakah yang perlu diamankan? Dan diamankan terhadap apa?
3. Jelaskan aspek-aspek yang menjadi konsep utama keamanan komputer!
4. Sebutkan dan jelaskan jenis-jenis ancaman yang Anda ketahui!
5. Menurut Anda, apakah yang harus di laukukan sebuah perusahaan agar informasi penting dalam perusahaan tersebut dapat terlindungi dengan baik?

D. REFERENSI

Bishop, M. (2019). *Computer Security Art and Science*. 2nd Edition. Boston: Pearson Education Inc.

Goodrich, M., & Tamassia, R. (2014). *Introduction to Computer Security*. Harlow: Pearson Education Ltd.

Panek, C. (2020). *Security Fundamental*. Canada: Sybex A Wiley Brand.

Pfleeger, P. C., Pfleeger, S. L., & Margulies, J. (2015). *Security in Computing*. 5th Edition. Westford: Pearson Education Inc.

Salomon, D. (2006). *Foundations of Computer Security*. Springer Science+Business Media

Nieles, M., Dempsey, K., & Pillitteri, P. Y. *Computer Security*. National Institute of Standards and Technology [Internet]. Juni 2017. NIST Pubs. Tersedia pada:

https://www.nist.gov/publications/introduction-computer-security-nist-handbook

Paulsen, C., & Byers, R. D. *Glossary of Key Information Security Terms* [Internet]. Juli 2019. NIST Pubs. Tersedia pada: https://www.nist.gov/publications/glossary-key-information-security-terms-2, https://csrc.nist.gov/glossary

Shirey, R. (2007). *Internet Security Glossary version 2*. (diakses 24 Oktober 2020). Tersedia pada: https://www.rfc-editor.org/info/rfc4949