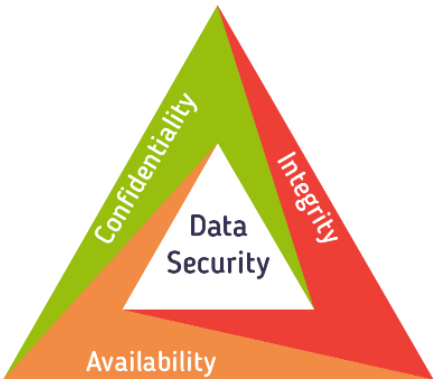
MODUL I

Konsep Dasar Keamanan Dunia Internet / Dunia Maya

1.1 Konsep Dasar Keamanan Dunia Internet Sebagai Perlindungan Berbagai Ancaman

Keamanan dunia internet adalah hal yang penting dalam perkembangan di dunia perusahaan ataupun institusi, salah satunya bidang kesehatan. Banyak orang mengabaikan ancaman di dunia internet karena berpikir tidak akan mengancam bidang kesehatan yang hanya berfokus pada pelayanan perawatan pasien. Berbagai contoh yang mengancam bidang kesehatan seperti informasi kesehatan pribadi seorang pasien dan pembayaran yang dilakukan oleh banyak pasien terhadap layanan kesehatannya melalui kartu kredit atau debit. Serangan terhadap keamanan internet di definisikan sebagai upaya untuk mendapatkan akses ilegal ke berbagai sistem komputer yang akan menyebabkan kerusakan serta membuat ketidaknyamanan bagi individu hingga gangguan ekonomi dan sosial. Penyerang akan melalukan berbagai tindakan seperti menghapus atau mencuri informasi penting bahkan bisa mengekspos informasi pribadi secara publik, juga mengunci data sehingga mereka meminta tebusan. Penyerangan tersebut dapat dilakukan oleh satu atau sekelompok orang bahkan organisasi di mana saja, sehingga diperlukan pengamanan yang meliputi proses, pelatihan dan teknologi. Tujuan dari adanya keamanan dunia internet yaitu menjaga sebuah data yang dikenal dengan istilah Confidentiality, Integrity, and Availability (CIA) :



Konsep Dasar Keamanan Dunia Internet Sebagai Perlindungan Berbagai Ancaman

- Kerahasiaan : Informasi hanya dapat dilihat oleh orang yang tepat
- Integritas : Informasi hanya dapat diubah oleh orang yang tepat
- Ketersediaan : Informasi dapat terlihat dan diakses kapan pun dibutuhkan

Adapun istilah vektor serangan sebagai titik masuk atau alur bagi penyerang agar dapat mengakses sistem di dalamnya. Cakupan lanskap ancaman dapat berupa akun email, media sosial, perangkat seluler, infrastruktur teknologi organisasi, layanan awan, dan orang – orang sekitar.

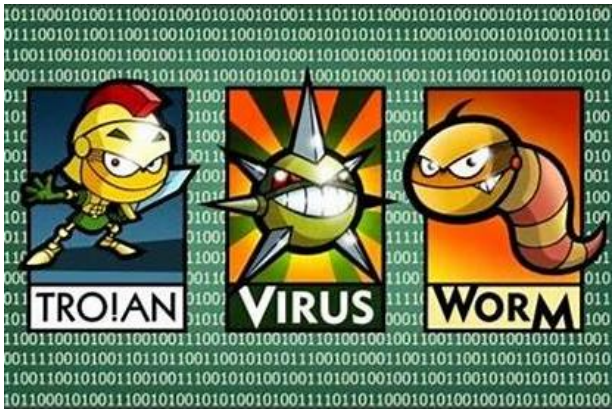
Email sudah menjadi vektor serangan paling umum karena penyerang akan mengirimkan sebuah tautan yang meyakinkan pengguna untuk membuka tautan tersebut dan nantinya akan membahayakan perangkat pengguna. Vektor serangan lainnya misalnya menggunakan jaringan nirkabel yang berada di rumah sakit, pelaku akan memanfaatkan itu dengan mencari kerentanan di perangkat pengguna yang mengakses jaringan tersebut. Contoh lainnya yaitu :

- Removable Media (Pelepasan media), para penyerang akan memuat kode berbahaya ke perangkat USB yang kemudian diberikan sebagai hadiah (gratis) kepada pengguna atau dapat dibiarkan di tempat umum untuk ditemukan.
- Browser (Peramban), penyerang akan membuat situs web berbahaya yang nantinya pengguna akan mengunduh software berbahaya di perangkatnya.
- Cloud Services (Layanan awan), penyerang dapat menyusup akun di layanan cloud dan akan mengendalikan semua layanan yang dapat di akses ke akun tersebut serta akses ke akun lain.
- Insiders (orang dalam), salah satunya karyawan yang mungkin bisa saja sebagai vektor serangan karena memiliki akses resmi sehingga digunakan secara sengaja untuk mencuri.

1.1.1 Malware

Penyerangan terhadap keamanan tidak hanya terjadi dalam kerentanan teknologi, namun dapat merekayasa sosial seperti meniru identitas pengguna untuk dapat memberi akses yang tidak sah pada suatu sistem. Misalnya, penyerang mengelabui pengguna agar dapat mengungkapkan kata sandi. Perangkat lunak yang digunakan oleh penjahat dunia internet untuk melakukan tindakan yang membahayakan disebut dengan *malware*. Malware memiliki dua komponen utama yaitu mekanisme propagasi dan payload.

1 Propagasi adalah proses dari tindakan malware dalam suatu sistem.



Malware

a. Trojan, berpura – pura menjadi perangkat lunak yang asli dan saat pengguna akan menginstal suatu program yang bentuknya seperti yang diiklankan disitulah tindakan jahat dilancarkan seperti mencuri informasi.
b. Virus, pengguna dapat mengunduh file atau menyambungkan perangkat USB yang berisi virus sehingga mempengaruhi file lainnya yang ada di dalam suatu PC pengguna tersebut.

c. Worm, menginfeksi perangkat dengan mengeksploitasi kerentanan dalam aplikasi yang sedang berjalan sehingga dapat menyebar ke perangkat lain pada jaringan yang sama.

2 Payload adalah tindakan yang dilakukan oleh malware kepada sistem yang telah terinfeksi. Beberapa jenis muatannya seperti ransomware yang mengunci sistem hingga korban membayar tebusan, spyware yang memata – matai sistem, backdoors yang mengeksploitasi kerentanan dalam sistem, serta botnet yang menghubungkan komputer atau perangkat lain ke jaringan yang terinfeksi agar bisa dikendalikan dari jarak jauh.

Sehingga dibutuhkan strategi mitigasi sebagai kumpulan langkah yang dapat diambil oleh suatu organisasi untuk mencegah atau mempertahankan diri dari serangan yang terus menerus berdatangan. Ada banyak strategi yang dapat diterapkan dalam sebuah organisasi seperti otentifikasi multifaktor, keamanan suatu peramban, mendidik para pengguna, dan intelijen ancaman yang artinya para pengguna mengumpulkan informasi mengenai kerentanan yang nantinya akan diterapkan sebagai kebijakan untuk keamanan perangkat, akses pengguna dan lainnya.

1.1.2 Kriptografi

Kriptografi berasal dari kata Yunani "Kryptos" yang artinya tersembunyi atau rahasia. Sehingga disimpulkan bahwa kriptografi adalah aplikasi komunikasi yang aman dalam bentuk apa pun antara pengirim dan penerima karena digunakan untuk mengaburkan makna pesan tertulis, tetapi juga dapat diterapkan pada gambar. Kita dapat menggunakannya untuk mengamankan dan melindungi file di penyimpanan eksternal atau internal.

Kriptografi

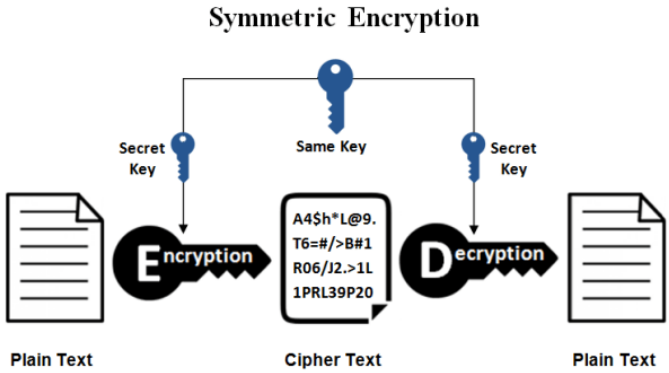
Kriptografi memiliki dua istilah dan frasanya sendiri, diantaranya yaitu :

1. *Plaintext,* meliputi pesan apa pun termasuk dokumen, musik, gambar, film, data, dan program komputer, menunggu untuk diubah secara kriptografis.
2. *Ciphertext,* suatu plaintext yang diubah menjadi pesan rahasia dan meliputi data terenkripsi/aman.

1.1.3 Enkripsi

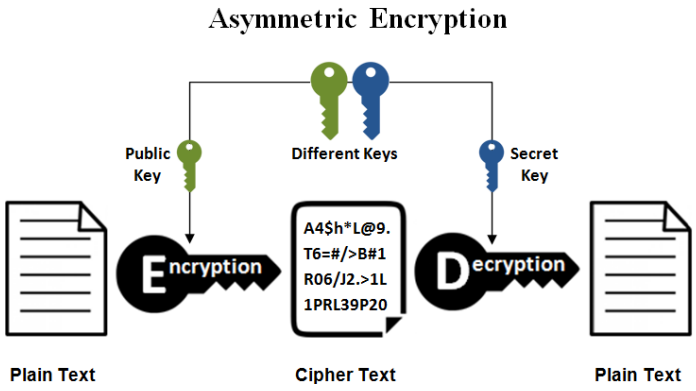
Enkripsi sekarang terjadi di dunia digital dengan menggunakan komputer dan matematika untuk menggabungkan bilangan prima acak bernilai lebih besar untuk membuat kunci yang digunakan dalam enkripsi simetris dan asimetris. Enkripsi merupakan mekanisme dimana pesan plaintext diubah menjadi ciphertext yang tidak dapat dibaca dan bertujuan untuk meningkatkan kerahasiaan data yang dibagikan dengan penerima, baik itu teman, rekan kerja, atau bisnis lain. Dekripsi adalah mekanisme penerima pesan ciphertext dapat mengubahnya kembali menjadi plaintext yang dapat dibaca. Kunci enkripsi terbagi menjadi dua bentuk yaitu :

1. Kunci simetris, berdasar pada gagasan bahwa kunci kriptografi yang sama digunakan untuk enkripsi pesan teks biasa dan deskripsi pesan teks sandi dan cepat membuat metode enkripsi. Kunci kriptografi diperlakukan sebagai rahasia bersama antara dua pihak atau lebih, harus dijaga dengan hati-hati agar tidak diketahui oleh aktor jahat. Semua pihak harus memiliki kunci kriptografi yang sama sebelum pesan aman dapat dikirim. Distribusi kunci merupakan salah satu tantangan yang terkait dengan enkripsi simetris.



Enkripsi

2. Kunci asimetris, berdasar pada distribusi yang aman dengan mengubah cara kunci kriptografi yang dibagikan. Kunci publik dapat dibagikan dengan siapa saja, sehingga individu dan organisasi tidak perlu khawatir tentang distribusinya yang aman. Kunci pribadi harus disimpan dengan aman karena hanya dapat diakses oleh orang yang membuat kunci tersebut dan tidak dibagikan. Seorang pengguna yang perlu mengenkripsi pesan akan menggunakan kunci publik, dan hanya orang yang memegang kunci pribadi yang dapat mendekripsinya.

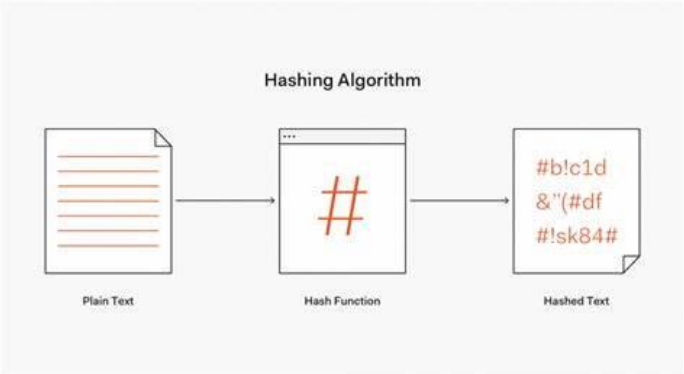


Enkripsi

Enkripsi digunakan di seluruh dunia hampir setiap aspek kehidupan kita, lebih banyak digunakan saat kita melakukan penelurusan pada suatu browser. Mungkin kita tidak menyadarinya, tetapi setiap kita membuka situs web yang alamatnya dimulai dari https:// atau yang terlihat ikon gembok maka itu termasuk pada penggunaan enkripsi. Enkripsi lainnya berupa sistem operasi yang menyediakan alat untuk mengaktifkan hard drive atau perangkat portable seperti operasi windows. Contoh dekatnya dalam kehidupan sehari – hari yaitu penggunaan komunikasi seluler menggunakan smartphone dengan enkripsi yang digunakan yaitu menara seluler terdekat agar memastikan kita memiliki kekuatan sinyal yang baik.

1.1.4 Hashing

Kriptografi juga digunakan untuk memverifikasi bahwa data seperti dokumen dan gambar, belum sepenuhnya dirusak, yang disebut hashing.



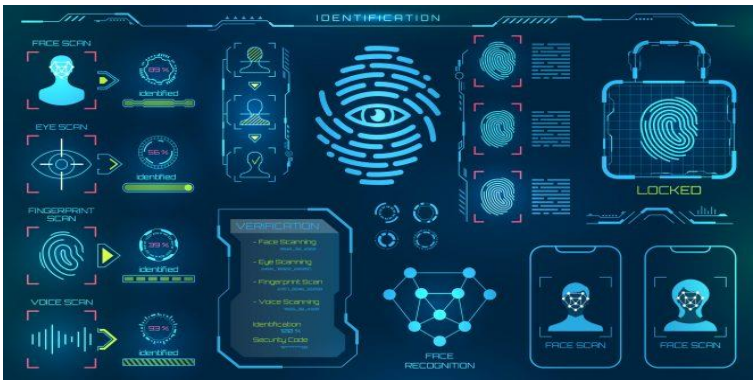
Hashing

Hashing menggunakan algoritma yang dikenal sebagai fungsi hashing untuk mengubah teks asli menjadi nilai tetap yang unik, itu disebut sebagai nilai hash. Setiap kali teks di hash menggunakan algoritma yang sama, akan menghasilkan nilai hash yang sama. Hashing berbeda dengan enkripsi karena tidak menggunakan kunci dan nilai hash tersebut tidak dapat mendekripsi kembali ke aslinya. Ada banyak jenis fungsi hash dan salah satunya yaitu *Secure Hash Algorithm (SHA)*. SHA adalah keluarga algoritma hash yang masing-masing bekerja secara berbeda dan menghasilkan nilai hash sepanjang 256 bit. Kriptografi memiliki banyak aplikasi di dunia modern saat ini.

Melalui hashing, kriptografi juga memverifikasi bahwa pesan teks biasa tidak berubah. Pada dasarnya, sertifikat digital adalah pasangan kunci yang dikeluarkan oleh otoritas sertifikat yang menjamin bahwa pasangan kunci digunakan dari sumber tepercaya, yang telah memeriksa dan memverifikasi identitas orang yang memintanya. Contohnya ketika kita ingin memiliki paspor, maka agen paspor pemerintah harus memverifikasi bahwa kita benar – benar seperti yang kita katakan sebelum mereka mengeluarkan dokumen baru. Sertifikat digital juga memiliki jangka waktu tertentu maksimal satu tahun dan setelahnya sudah kedaluwarsa. Ketika hal itu terjadi, maka kita akan menerima pemberitahuan yang menunjukkan bahwa otentifikasi server tidak dapat lagi kita akses atau konfirmasi.

1.1.5 Autentifikasi

Keamanan siber yang baik bergantung pada banyak faktor untuk memberikan keyakinan dan jaminan bahwa data aman dan digunakan seperti yang diharapkan. Ketika kita telah mengautentikasi pengguna, kita perlu memutuskan apa yang boleh mereka lakukan. Otorisasi memberi setiap pengguna tingkat akses tertentu ke data dan aset. Sebagai aturan, pengguna harus diberikan izin yang cukup untuk mengakses sumber daya yang mereka butuhkan.



Autentifikasi

Saat seseorang membeli barang dengan kartu kredit, mereka mungkin diminta untuk menunjukkan tanda pengenal tambahan. Ini membuktikan bahwa mereka adalah orang yang namanya muncul di kartu. Dalam contoh ini, pengguna dapat menunjukkan SIM yang berfungsi sebagai bentuk otentikasi dan membuktikan ID mereka. Sama halnya ketika mengakses komputer atau perangkat, kita akan menemukan jenis otentifikasi yang sama, yaitu harus memasukkan nama pengguna dan kata sandi. Metode otentikasi yang kuat sangat penting untuk menjaga keamanan dunia internet dan memastikan bahwa hanya pengguna yang dapat memperoleh akses ke data privat. Ada beberapa metode autentifikasi, di antaranya yaitu :

a. Sesuatu yang kita ketahui, termasuk :
    1. Kata sandi
    2. Nomor PIN
    3. Pertanyaan Keamanan

b. Sesuatu yang kita miliki, termasuk :
    1. Kartu identitas
    2. Komputer
    3. Handphone
c. Sesuatu yang lainnya, termasuk :
    1. Sidik jari
    2. Pengenalan wajah
    3. Bentuk lainnya dari ID biometric (karakteristik fisik yang secara unik mengidentifikasi individu tersebut)

Otentikasi faktor tunggal adalah sistem di mana hanya satu jenis otentikasi yang digunakan untuk menjadikannya metode yang paling tidak aman tetapi paling sederhana. Contoh dari sistem ini adalah ketika pengguna memberikan sesuatu yang mereka ketahui seperti kata sandi untuk di autentikasi. Kata sandi sederhana mudah diingat tetapi mudah diretas oleh penjahat. Kata sandi yang rumit mungkin tampak lebih aman, tetapi tidak mungkin untuk diingat. Otentikasi satu faktor nyaman tetapi tidak cocok untuk sistem yang sangat aman. Otentikasi multifaktor adalah sistem di mana dua atau tiga jenis otentikasi digunakan untuk mengurangi kemungkinan bahwa aktor jahat akan bisa mendapatkan akses ke informasi rahasia. Otentikasi biometrik paling sering digunakan bersama dengan metode otentikasi lainnya. Sebelum seseorang dapat memperoleh akses, mereka biasanya diminta untuk berhasil memasukkan kata sandi dan pemindaian sidik jari. Otentikasi multifaktor adalah cara penting bagi pengguna dan organisasi untuk meningkatkan keamanan sehingga harus dijadikan pendekatan default untuk otentikasi. Serangan otentikasi atau serangan identitas terjadi ketika seseorang mencoba mencuri kredensial orang lain karena tujuan dari jenis serangan ini adalah untuk menyamar sebagai pengguna yang sah.

1.1.6 Teknik Keamanan Otorisasi

Dalam istilah keamanan siber, otorisasi menentukan tingkat akses yang dimiliki orang yang diautentikasi ke datanya.

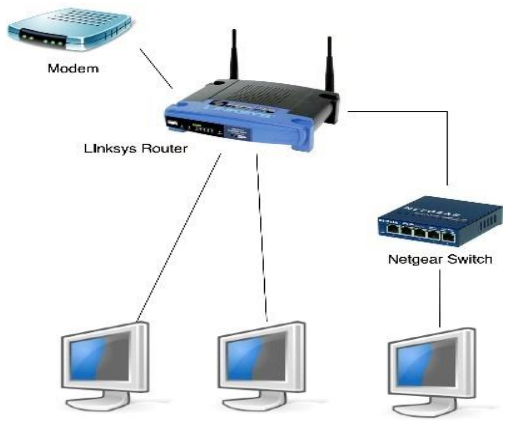
Teknik Keamanan Otorisasi

Ada berbagai teknik keamanan yang digunakan organisasi untuk mengelola otorisasi, yaitu :

1. Akses bersyarat, melibatkan akses dengan kondisi. Salah satu caranya adalah dengan pernyataan if / then. Jika sesuatu benar, Anda diberikan akses, tetapi jika itu salah, Anda ditolak.
2. Akses dengan hak istimewa paling rendah, pengguna diberikan hak minimum yang dibutuhkan.
3. Gerakan lateral, digunakan untuk menyusup ke sistem lain atau mendapatkan akses yang lebih tinggi karena penyerang akan mencoba berpindah di antara bagian yang berbeda.
4. Tanpa kepercayaan, model yang memungkinkan organisasi menyediakan akses aman ke sumber daya dengan mengajari "jangan pernah percaya, selalu verifikasi". Dengan menggunakan model keamanan *Zero Trust*, organisasi dapat lebih beradaptasi dengan tempat kerja terdistribusi modern yang menyediakan akses aman ke sumber daya.

1.1.7 Network

Jaringan digunakan untuk mengakses semua jenis informasi, mulai dari gambar yang di bagikan dengan teman, hingga informasi sensitif seperti transaksi bank dan kartu kredit. Jaringan adalah pengelompokan komponen fisik yang saling berhubungan dan bekerja bersama untuk menyediakan tulang punggung yang mulus bagi semua perangkat dalam berkomunikasi. Meskipun ada berbagai bagian yang membantu mendefinisikan jaringan, bagian yang lebih mungkin kita temui adalah router, saklar, firewall dan hub. Hal ini memungkinkan beberapa perangkat untuk berkomunikasi satu sama lain, serta router memungkinkan jaringan yang berbeda untuk berkomunikasi satu sama lain.



Network

Koneksi Kabel atau Ethernet merupakan cara umum untuk terhubung ke jaringan kantor, dengan membutuhkan kabel jaringan fisik untuk menghubungkan komputer atau laptop ke sakelar di jaringan. Koneksi Nirkabel memungkinkan perangkat kita terhubung ke jaringan menggunakan Wi-Fi. Ini biasanya digunakan di rumah atau di tempat umum. Koneksi Bluetooth adalah metode komunikasi antarperangkat dengan jarak pendek.

Perangkat kecil seperti pedometer, headphone, dan jam tangan pintar cenderung menggunakan Bluetooth. Serangan man-in-the-middle atau penyadapan dapat terjadi ketika penjahat dunia maya berkompromi atau meniru rute dalam jaringan, memungkinkan mereka untuk mencegat paket informasi. Hal ini memungkinkan penyerang untuk tidak hanya mencuri data tetapi juga membahayakan integritasnya. Serangan penolakan layanan (DDoS) terdistribusi tujuan yaitu untuk membahayakan ketersediaan jaringan atau layanan yang ditargetkan. Penyerang melakukan ini dengan membombardir jaringan atau layanan yang ditargetkan dengan jutaan permintaan simultan dari sumber yang didistribusikan di seluruh jaringan. Jaringan pribadi virtual (VPN) berfungsi sebagai koneksi khusus dan aman antara perangkat dan server di seluruh internet. VPN membuat koneksi aman melalui jaringan publik yang tidak aman. Penyedia VPN telah menjadi sangat umum tidak hanya untuk skenario kerja jarak jauh tetapi juga untuk penggunaan pribadi.

1.1.8 Langkah – Langkah Mitigasi

Mengapa perangkat merupakan bagian integral dari kehidupan kita? Karena dapat mengumpulkan, menyimpan informasi, serta membuat kita tetap terhubung ke perangkat dan layanan lain. Perangkat yang terhubung juga memungkinkan kita mengakses berbagi informasi dengan mudah. Misalnya,kita pernah menggunakan ponsel untuk berbagi foto keluarga dengan teman, mengakses dokumen kerja, atau membayar sesuatu di toko. Meskipun perangkat membantu kita menyelesaikan pekerjaan, dan menjalani kehidupan sehari-hari, perangkat juga memberikan peluang bagi penjahat dunia maya yang ingin membahayakan. Karena mereka adalah vektor ancaman, mereka menyediakan cara berbeda di mana penjahat dunia maya dapat melakukan serangan. Contohnya ponsel, laptop, atau tablet mengunduh satu aplikasi berbahaya yang mengakibatkan perangkat terkontaminasi malware yang dapat mengekstrak data yang disimpan secara lokal tanpa sepengatuhan pengguna. Sehingga membahayakan kerahasiaan dan integritas karena penyerang dapat melakukan modifikasi data.

Langkah – Langkah Mitigasi

Ada berbagai cara untuk melindungi perangkat dan data. Secara umum terdiri dari :

a. Pengerasan perangkat, proses meminimalkan kemungkinan yang kerentanan perangkatnya dapat dieksploitasi. Sehingga yang perlu kita lakukan yaitu memastikan bahwa perangkat memiliki pembaruan keamanan terbaru, mematikan semua perangkat yang tidak digunakan, mengaktifkan fitur keamanan yang didukung melalui sistem operasi perangkat, lalu kita perlu menggunakan PIN atau biometric lainnya untuk mengakses perangkat. Fitur-fitur ini mudah diaktifkan dan dapat membantu menjaga perangkat yang terhubung tetap aman untuk menjaga kerahasiaan dan integritas data yang dapat diakses.
b. Enkripsi, proses mengubah informasi pada perangkat menjadi data yang tidak dapat dipahami. Satu-satunya cara untuk membuat informasi ini berguna adalah dengan membalikkan enkripsi. Ketika informasi dienkripsi, itu menjadi tidak berguna tanpa kunci atau kata sandi yang benar. Dengan demikian, kerahasiaan data tetap terjaga.
c. Batasi akses perangkat aplikasi, memastikan bahwa aplikasi tersebut ditutup atau diamankan saat kita tidak menggunakannya dengan mengunci perangkat saat kita jauh.

1.1.9 Aplikasi

Perangkat lunak adalah kumpulan perintah dalam bentuk kode yang memerintahkan komputer atau perangkat untuk melakukan beberapa bentuk pekerjaan. Perangkat lunak berjalan di atas perangkat keras (komponen fisik) perangkat.

Aplikasi

Secara garis besar, perangkat lunak datang dalam dua jenis:

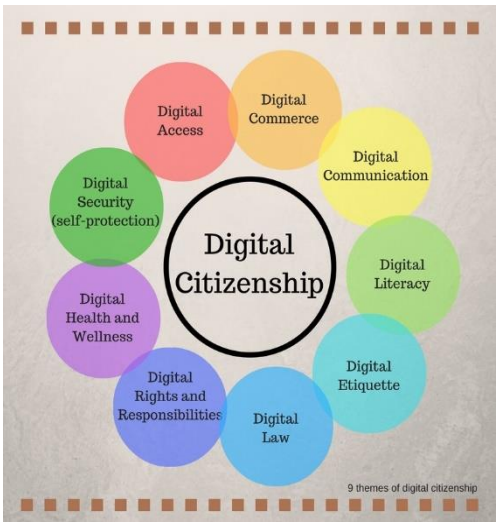
1. Sistem perangkat lunak, mengontrol atau memfasilitasi perangkat keras serta proses sistem seperti mouse, keyboard, jaringan, proses dalam sistem ini dapat berjalan dengan sendirinya dan berjalan di latar belakang. Areanya yang besar dan kompleks tetap menjadi target serangan kejahatan dunia maya.
2. Aplikasi perangkat lunak, dirancang untuk bekerja pada perangkat lunak sistem yang spesifik, dan sebagian besar tersedia untuk sistem yang paling populer. Aplikasi akan melakukan pekerjaan khusus seperti mengolah kata, mengedit video dan mengirim pesan

yang dirancang agar pengguna dapat berinteraksi secara langsung. Tidak berjalan secara independent dan membutuhkan sistem perangkat lunak yang perlu diinstal oleh pengguna.

Sebagian dari kebijakan keamanan, harus dipastikan bahwa semua aplikasi yang digunakan pada perangkat kita memiliki patch atau pembaruan terbaru. Selain itu, perlu memeriksa pengaturan konfigurasi aplikasi dan apabila memungkinkan ubahlah kata sandi pada akun dan pengaturan default. Menghapus atau melakukan pembersihan pada jendela penjelajahan di browser untuk meningkatkan keamanan yang lebih tinggi. Yang paling penting lagi yaitu apabila ingin mengunduh aplikasi maka unduhlah aplikasi dari toko atau laman yang terverifikasi dan terpercaya.

1.2 Konsep Digital Citizenship sebagai Kerangka Keamanan Sosial

Menggunakan teknologi dengan baik dan memahami bagaimana tindakan online memengaruhi diri sendiri dan orang lain. Keduanya merupakan keterampilan dasar yang diperlukan untuk memahami pentingnya mengelola dan memonitor perilaku dalam menggunakan teknologi di lingkungan pendidikan saat ini.



Konsep Digital Citizenship sebagai Kerangka Keamanan Sosial

Pendidik terkadang berasumsi bahwa semua pelajar adalah pengguna teknologi yang kompeten dengan sedikit kebutuhan akan bimbingan pendidik. Pelajar tidak sering menyadari bagaimana interaksi mereka di kelas berdampak pada orang lain melalui kata-kata dan tindakan mereka. Pendidik mendiskusikan dan memperkuat aturan, norma, dan harapan masyarakat untuk membantu menciptakan komunitas kelas yang nyaman dan saling menghormati. Sama seperti pelajar diajarkan bagaimana berinteraksi dan berkontribusi pada kenyataan kehidupan, pelajar juga harus diajarkan keterampilan yang dibutuhkan untuk melakukan hal yang sama secara online. Keterampilan mengelola digital ini berfungsi sebagai prinsip panduan agar pelajar dapat menggunakan teknologi secara tepat, aman, dan bertanggung jawab. Karena ruang akan semakin

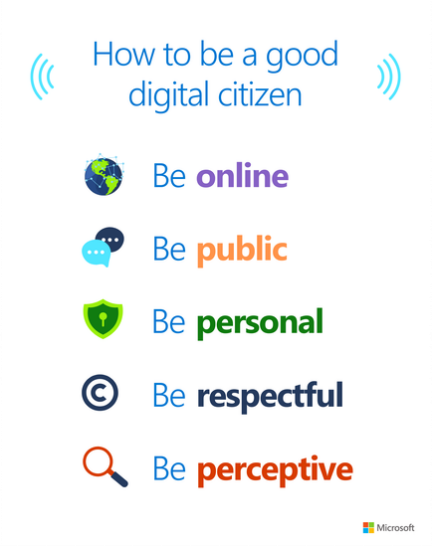
luas dan menambahkan lebih banyak teknologi untuk memberi manfaat bagi pelajar, kebutuhan untuk memodelkan dan menjelaskan penggunaan digital yang tepat akan terus meningkat.

Dr. LeeAnn Lindsey dan Dr. Kristen Mattson, yang secara kolektif dikenal sebagai "Dokter DigCit", berbagi kerangka kurikulum luar biasa yang memberikan wawasan dan implementasi praktis untuk memulai pembicaraan mengenai mengelola dan memonitor perkembangan digital. Menggunakan teknologi dalam pendidikan meruntuhkan hambatan dan memberikan kesempatan untuk berinteraksi dengan orang lain dari seluruh dunia. Seperti yang dikatakan Jennifer Fleming, Associate Professor di Departemen Jurnalisme dan Komunikasi Massa California State University, “Mengajar di era internet berarti kita harus mengajarkan keterampilan masa depan hari ini”. Dengan Internet, informasi hanya dengan menekan satu tombol. Andrew Kim, dari tim Steelcase Education Solutions mengatakan, “Teknologi mengubah dinamika pendidikan, terutama hubungan antara guru dan siswa”. Siswa yang belajar hukum akan menganalisis hukum, peraturan, dan kasus yang ada sebagai contoh, dengan keyakinan bahwa memahami sejarah akan membantu memecahkan masalah di masa depan dengan menerapkan doktrin lama ke situasi paralel baru. Pendekatan pendidikan yang “melihat ke belakang” ini pernah diterima sebagai hal yang baik, dan peran pendidik bersifat hierarkis, dengan guru memiliki semua pengetahuan untuk diberikan kepada siswa. Namun, dengan meningkatnya penggunaan laptop, tablet, dan perangkat seluler lainnya, ruang kelas telah menjadi ruang di mana pengetahuan diciptakan bukan dikonsumsi. Guru pun menggunakan teknologi untuk menciptakan pengalaman yang lebih personal dan mandiri bagi siswa. Oleh karena itu, pendidikan telah berevolusi dari sistem pengajaran transfer menjadi sistem yang lebih banyak mengeksplorasi dan membangun masa depan bersama dengan siswa lain. Mereka sadar bahwa fakta dapat dengan mudah ditemukan secara online. Yang mereka cari adalah berbagi pengalaman dan cerita untuk meningkatkan pengalaman mereka sendiri dengan belajar dari keberhasilan dan kegagalan orang lain. Profesor Matematika di Harold Washington College di Chicago, Illinois, Ignacio Estrada, mengatakan, "Jika seorang anak tidak dapat belajar dengan cara kita mengajar, mungkin kita harus mengajar dengan cara mereka belajar." dan yang dikatakan oleh George Couros, pendidik pengajaran inovatif Kanada, “Teknologi tidak akan pernah menggantikan guru-guru hebat, tetapi teknologi di tangan guru-guru hebat adalah transformasi.”

1.2.1 Pandangan Pedadogi

Dalam istilah yang paling sederhana, pedagogi adalah bagaimana pendidik mengajar termasuk interaksi yang terjadi dengan peserta didik dalam suatu lingkungan pendidikan. Interaksi yang bermakna berkembang ketika pendidik menggunakan topik dengan cara berwawasan ke depan dan berfokus pada apa yang harus dilakukan siswa. Sebagai pendidik, dapat memberdayakan peserta didik untuk menggunakan alat digital dengan cara yang positif dan menegaskan sambil

membimbing mereka untuk menghindari praktik yang mengurangi kekuatan teknologi. Ada lima pernyataan untuk menemukan pentingnya menjadi warga digital yang baik , yaitu :



Pandangan Pedadogi

- *Online*, membangun kesadaran tentang bagaimana waktu online memengaruhi kesehatan dan kebugaran. Dalam survei tahun 2017 yang dilakukan oleh American Psychological Association, 81% responden mengatakan mereka sering terhubung ke suatu perangkat. Dalam survei yang sama ini, 65% orang Amerika setuju bahwa memutuskan hubungan secara berkala dari teknologi adalah hal yang baik, tetapi hanya 28% yang menindaklanjutinya. Statistik ini memberi tahu para pendidik bahwa mengajari pelajar cara memutuskan hubungan dan tentang manfaat kesehatan dari mengelola waktu teknologi adalah penting. Menurut sebuah studi oleh University of California Irvine, dibutuhkan rata-rata 23 menit dan 15 detik untuk kembali ke focus pada tugas yang terganggu. Pola pikir utama saat berinteraksi online adalah "Apakah saya menggunakan teknologi untuk membuat sesuatu menjadi lebih baik?". Warga digital yang baik juga menyadari bagaimana tindakan mereka dilihat oleh orang lain. Online berarti kita dapat memperhatikan dengan seksama bagaimana tindakan seseorang memengaruhi orang lain dan meluangkan waktu untuk merenungkan kiriman konten sebelum mengirimnya. Ada beberapa alat untuk membantu pelajar dan pendidik memperhatikan pengalaman online, yaitu :
  a. *Alarm windows*, gunakan timer dan alarm untuk membatasi waktu layar atau istirahat dari komputer.
  b. *Tetap fokus* adalah ekstensi produktivitas *Microsoft Edge*, membantu pengguna tetap fokus dengan memblokir situs web yang mungkin menjadi gangguan selama sesi kerja.
  c. Aplikasi *Reflect* di dalam *Microsoft Teams* membantu pelajar untuk memberikan reaksi sehingga dapat mengetahui tanggapan dari para pelajar mengenai materi yang disampaikan.

d. *Survei Microsoft Forms*, untuk mengetahui bahwa para pelajar menyimak dan memahami materi yang disampaikan.
e. Fitur *Obrolan* di dalam *Microsoft Teams*, memastikan bahwa percakapan antara pengajar dan siswa dapat berlangsung.

- *Publik*, menganalisis cara merepresentasikan diri saat online dalam membangun dan memberikan jejak digital yang positif. Setiap tindakan, postingan, suka, dan komentar meninggalkan jejak di dunia digital yang tidak mudah dilupakan. Penulis Germany Kent menulis, "Apa yang anda posting secara online berbicara banyak tentang siapa anda sebenarnya. Posting dengan niat. Repost dengan hati-hati". Warga digital yang baik menjaga kesadaran bahwa semua yang mereka bagikan secara online membentuk persepsi orang lain tentang mereka. Interaksi dan postingan online menjadi kesan pertama. Penting bagi pelajar untuk tetap sadar akan gambaran dan keyakinan yang ingin mereka sampaikan dan menyelaraskannya dengan aktivitas online. Strategi untuk membantu pelajar dan pendidik memperhatikan interaksi online, yaitu :
  a. Gunakan *Bing* secara berkala untuk memahami bagaimana profil digital sedang dibentuk.
  b. Gunakan *Minecraft*, memberikan kesempatan kepada pembelajar untuk menciptakan karakter digital yang lebih mirip dengan diri mereka sendiri atau bagaimana mereka ingin direpresentasikan secara online.
  c. Gunakan *Paint 3D* di perangkat Windows, pelajar menciptakan karya seni yang mengekspresikan siapa mereka atau bagaimana perasaan mereka untuk dibagikan secara online.
  d. Gunakan *LinkedIn* untuk penggunaan profesional atau perguruan tinggi, serta menggunakan konektor untuk menjelajahi jalur karir potensial yang menarik minat.
- *Pribadi*, dapat terhubung dengan orang lain dengan aman. Alat untuk membantu menjadikan pengalaman online pribadi dan aman, yaitu:
  a. *Microsoft Stream* yang digunakan untuk mengelola konten video termasuk mengunggah, melihat, dan berbagi video serta mengatur konten ke dalam saluran dan kelompok, serta menyediakan saluran khusus untuk kebutuhan pelajar.
  b. *Flipgrid* merupakan platform pembelajaran sosial untuk memposting topik saat memulai percakapan, dan merespons dengan menggunakan video dan audio yang dibangun langsung ke dalam program.
  c. Pembelajaran berbasis game dengan *Minecraft*, mengajarkan keterampilan termasuk pemecahan masalah, kreativitas, dan pemikiran sistem. Membangun brankas digital di dalam dunia Minecraft untuk menyimpan data pribadi seperti nama pengguna dan kata sandi.

d. Pembuatan kata sandi *Microsoft Edge*, menghasilkan saran kata sandi yang kuat dan unik. Kata sandi yang dihasilkan disimpan secara otomatis di browser dan di sinkronkan di semua perangkat yang menggunakan browser Edge.

- *Patuh*, mengikuti pedoman hak cipta dan mengenali kepemilikan konten digital. Alat untuk membantu pelajar mengutip dan mengatribusikan yaitu :
  a. Pencarian *Visual Bing* untuk menemukan informasi tentang suatu gambar termasuk tautan ke tempat gambar tersebut dapat ditemukan secara online.
  b. *Bing* sebagai mesin pencari web *Microsoft*, dapat menyertakan alat filter yang memungkinkan pengguna memfilter pencarian gambar untuk pembatasan lisensi. Filter ini didasarkan pada sistem lisensi Creative Commons dan membantu pengguna menemukan gambar untuk digunakan, dibagikan, atau dimodifikasi.
  c. *Microsoft Teams* untuk penggunaan pendidikan yang dirancang untuk menandai dokumen yang diduplikat dan memeriksa bahasa yang serupa dalam tugas. Integrasi ini membantu merampingkan proses penilaian bagi pendidik.
  d. *Microsoft OneNote* digunakan untuk mengumpulkan informasi dari web ke dalam buku catatan digital. Aplikasi OneNote menyediakan kutipan otomatis, lengkap dengan tautan langsung ke situs web.
  e. Fitur *Editor* dalam *Microsoft Word* yang memungkinkan pengeditan dan revisi yang disarankan pada dokumen.
- *Tanggap*, mengevaluasi sumber dengan strategi literasi digital termasuk memahami berbagai perspektif. Alat untuk membangun keterampilan persepsi dan literasi informasi yaitu :
  a. Pencarian *Bing versi aman* untuk menyaring konten web yang tidak pantas dari hasil pencarian, termasuk teks, gambar, dan video. Mengaktifkan Pencarian Aman memungkinkan pelajar untuk fokus pada kualitas informasi yang diambil dan menghindari informasi yang tidak memenuhi harapan pencarian.
  b. *Factcheck.org*, proyek dari Annenberg Public Policy Center University of Pennsylvania, menggunakan komunitas cendekiawan untuk menangani masalah kebijakan publik. Menggunakan situs ini untuk menilai apakah informasi yang ditemukan secara online tersebut akurat.
  c. *Peramban Microsoft Edge* menggunakan ekstensi, seperti pemblokiran iklan.

Penggunaan teknologi dalam pendidikan terus berkembang dengan pesat dan begitu pula keharusan bagi peserta didik untuk memperoleh keterampilan dalam pengelolaan digital secara aman. Implementasi membutuhkan perencanaan, latihan, dan kesabaran yang cermat. Itulah sebabnya mengapa standar International Society for Technology in Education (ISTE) dibuat untuk didorong oleh pelajar dan fokus pada pemberdayaan suara pelajar.

"Be Statements" ini merupakan kolaborasi dengan rekan dan pelajar, memberikan tantangan kepada pendidik untuk memikirkan kembali bagaimana pendekatan tradisional, dan mempersiapkan pelajar untuk mempertimbangkan orang lain terlebih dahulu dan mendorong pembelajaran mereka sendiri di dunia online.

DAFTAR PUSTAKA

Describe the basic concepts of cybersecurity - Learn | Microsoft Docs

Digital citizenship prepare todays learners – Learn | Microsoft Docs/