PROTEKSI ASET INFORMASI

Yuswardi, Indrawan Ady Saputro, Angga Aditya Permana, Suwito Pomalingo, Kholidiyah Masykuroh, Fahmy Rinanda Saputri, Laila Qadriah, Sayed Achmady, Moh.Safii, Gatot Budi Santoso

ISBN 978-623-198-553-8

PROTEKSI ASET INFORMASI

Yuswardi
Indrawan Ady Saputro
Angga Aditya Permana
Suwito Pomalingo
Kholidiyah Masykuroh
Fahmy Rinanda Saputri
Laila Qadriah
Sayed Achmady
Moh. Safii
Gatot Budi Santoso

GET PREES INDONESIA

PROTEKSI ASET INFORMASI

Penulis :
Yuswardi
Indrawan Ady Saputro
Angga Aditya Permana
Suwito Pomalingo
Kholidiyah Masykuroh
Fahmy Rinanda Saputri
Laila Qadriah
Sayed Achmady
Moh. Safii
Gatot Budi Santoso

ISBN : 978-623-198-553-8

Editor : Diana Purnama Sari, S.E., M.E
Penyunting : Tri Putri Wahyuni,S.Pd
Desain Sampul dan Tata Letak : Atyka Trianisa, S.Pd

Penerbit : GET PREES INDONESIA
Anggota IKAPI No. 033/SBA/2022

Redaksi :
Jln. Palarik Air Pacah No 26 Kel. Air Pacah
Kec. Koto Tangah Kota Padang Sumatera Barat
Website : www. getpress.co.id
Email : adm.getpress@gmail.com

Cetakan pertama, 1 Agustus 2023

Hak cipta dilindungi undang-undang
Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa izin tertulis dari penerbit.

KATA PENGANTAR

Segala Puji dan syukur atas kehadirat Allah SWT dalam segala kesempatan. Sholawat beriring salam dan doa kita sampaikan kepada Nabi Muhammad SAW. Alhamdulillah atas Rahmat dan Karunia-Nya penulis telah menyelesaikan Buku Proteksi Aset Informasi ini.

Buku ini membahas *Security and privacy, Vulnerabilities, Fundamental aspects, Security mechanisms (Countermeasures), Policy, Information states, Security secvices, Foundations information security, Security models, Policies and compliance*.

Proses penulisan buku ini berhasil diselesaikan atas kerjasama tim penulis. Demi kualitas yang lebih baik dan kepuasan para pembaca, saran dan masukan yang membangun dari pembaca sangat kami harapkan.

Penulis ucapkan terima kasih kepada semua pihak yang telah mendukung dalam penyelesaian buku ini. Terutama pihak yang telah membantu terbitnya buku ini dan telah mempercayakan mendorong, dan menginisiasi terbitnya buku ini. Semoga buku ini dapat bermanfaat bagi masyarakat Indonesia.

Padang, 1 Agustus 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

BAB 1
SECURITY AND PRIVACY

Yuswardi

1.1 Pendahuluan

Security and Privacy adalah dua aspek penting dalam dunia digital yang berhubungan erat dengan perlindungan informasi dan data pribadi. Pendahuluan pada topik keamanan dan privasi bertujuan untuk memperkenalkan pentingnya kedua aspek ini serta memberikan definisi dasar untuk pemahaman yang lebih baik. Pertama-tama, penting untuk menyadari bahwa dalam era digital yang terus berkembang, informasi dan data kita berada dalam risiko yang lebih tinggi terhadap serangan dan penyalahgunaan. Oleh karena itu, keamanan dan privasi menjadi hal yang sangat relevan dan perlu diperhatikan baik oleh individu maupun organisasi Yuwinanto, H. P. (2015).

Keamanan (*security*) merujuk pada perlindungan terhadap ancaman dan serangan yang ditujukan untuk mencuri, merusak, atau mengganggu informasi dan sistem yang berhubungan dengan data kita. Ini mencakup serangan siber, malware, pelanggaran data, dan metode rekayasa sosial yang digunakan oleh pihak yang tidak berwenang untuk mendapatkan akses ilegal atau mengambil kendali atas informasi sensitif Nurhatinah, N. (2018).

Privasi (*privacy*) berfokus pada hak individu untuk menjaga kerahasiaan, kontrol, dan pengendalian atas data dan informasi pribadi mereka. Dalam dunia digital yang terhubung, banyak kegiatan online yang melibatkan pengumpulan data pribadi oleh perusahaan dan lembaga. Privasi melibatkan kekhawatiran tentang penggunaan, pengungkapan, dan penyalahgunaan data pribadi oleh pihak lain.

Pemahaman tentang keamanan dan privasi penting karena melibatkan aspek perlindungan terhadap ancaman dan risiko yang ada dalam dunia digital. Dalam dunia yang semakin terhubung, serangan siber dan pelanggaran privasi semakin umum terjadi, dan dampaknya dapat merugikan individu, organisasi, dan masyarakat secara luas. Dengan demikian, pemahaman dan kesadaran tentang keamanan dan privasi menjadi penting agar individu dan organisasi dapat mengambil tindakan yang tepat untuk melindungi informasi sensitif dan data pribadi mereka. Dalam hal ini, langkah-langkah keamanan dan privasi yang efektif serta praktik terbaik harus diterapkan untuk meminimalkan risiko dan melindungi informasi pribadi dengan sebaik-baiknya.

1.2 Privasi (Pribadi)

Privasi merupakan hak individu untuk memiliki kendali atas informasi pribadi mereka. Dalam era digital yang terus berkembang, privasi telah menjadi isu yang semakin kompleks dan penting Dhianty, R. (2022). Terdapat beberapa kekhawatiran privasi yang muncul dalam lingkungan digital:

1. Pengumpulan dan pengawasan data
   Banyak perusahaan dan organisasi mengumpulkan data pribadi dari pengguna melalui berbagai cara, seperti formulir online, aktivitas browsing, dan interaksi dengan aplikasi atau platform digital. Hal ini mengarah pada kekhawatiran tentang sejauh mana data pribadi dikumpulkan, diakses, dan digunakan oleh pihak ketiga.
2. Pelacakan dan profilisasi online
   Aktivitas online kita sering dilacak oleh berbagai entitas, termasuk perusahaan iklan dan platform media sosial. Data yang dikumpulkan digunakan untuk membuat profil pengguna yang lebih rinci, yang kemudian digunakan untuk mengarahkan iklan dan konten yang disesuaikan. Hal ini

menimbulkan kekhawatiran tentang hilangnya anonimitas dan kebebasan dalam menjelajahi dunia digital.

3. Pelanggaran privasi
   Pelanggaran keamanan dan serangan siber yang berhasil dapat mengakibatkan pengungkapan tidak sah atau pencurian data pribadi. Contohnya adalah insiden peretasan yang mengakibatkan pencurian informasi pengguna seperti nama, alamat, nomor kartu kredit, atau data sensitif lainnya. Pelanggaran privasi semacam ini dapat memiliki konsekuensi serius bagi individu yang terkena dampaknya.
4. Kebijakan privasi dan peraturan
   Perusahaan dan organisasi harus memiliki kebijakan privasi yang jelas dan transparan yang menjelaskan bagaimana data pribadi dikumpulkan, digunakan, dan diungkapkan. Selain itu, peraturan privasi seperti GDPR (*General Data Protection Regulation*) di Uni Eropa memberikan kerangka kerja yang ketat untuk melindungi privasi pengguna.
5. Persetujuan dan kontrol pengguna
   Pengguna harus diberikan kontrol yang jelas dan dapat dipahami atas pengumpulan, penggunaan, dan pengungkapan data pribadi mereka. Hal ini melibatkan memberikan persetujuan yang sadar dan jelas sebelum data pribadi dikumpulkan atau digunakan untuk tujuan tertentu.
6. Anonimisasi dan pseudonimisasi: Untuk melindungi privasi, data pribadi dapat diubah atau dienkripsi agar tidak dapat langsung diidentifikasi atau dikaitkan dengan individu tertentu. Ini dapat dilakukan melalui teknik anonimisasi dan pseudonimisasi yang mempertahankan utilitas data sambil melindungi identitas individu.
7. Teknologi pendukung privasi (*Privacy-Enhancing Technologies*, PETs):
   Pengembangan teknologi seperti jaringan privasi (*private networks*), alat enkripsi end-to-end, dan alat pengelola.

Kontrol privasi (*privacy control tools*) merupakan upaya untuk memberikan solusi teknis yang membantu individu menjaga privasi mereka dalam lingkungan digital. Selain langkah-langkah perlindungan privasi tersebut, terdapat juga praktik terbaik untuk menjaga privasi dalam kehidupan digital, antara lain: Membatasi pengumpulan dan penyimpanan data: Hindari memberikan informasi pribadi yang tidak perlu atau tidak relevan. Pertimbangkan untuk memberikan informasi secara selektif dan hanya kepada pihak yang dapat dipercaya. Mengamankan informasi pribadi: Pastikan data pribadi Anda disimpan secara aman dengan menggunakan langkah-langkah keamanan seperti penggunaan kata sandi yang kuat, enkripsi data, dan keamanan perangkat. Praktik transparansi data: Berikan informasi yang jelas dan transparan kepada pengguna tentang bagaimana data pribadi mereka dikumpulkan, digunakan, dan diungkapkan. Hal ini dapat membantu membangun kepercayaan antara organisasi dan pengguna. Evaluasi dan audit privasi secara teratur: Periksa kebijakan privasi dan praktik keamanan secara berkala untuk memastikan bahwa standar privasi terpenuhi dan perubahan kebijakan yang relevan diadopsi. Dalam kesimpulannya, privasi dalam konteks digital merupakan hak yang penting bagi individu untuk memiliki kendali atas data pribadi mereka. Dengan meningkatnya kesadaran akan pentingnya privasi dan adopsi langkah-langkah perlindungan privasi yang efektif, individu dapat menjaga keamanan data pribadi mereka dan merasa lebih nyaman dalam beroperasi di dunia digital yang semakin terhubung.

1.3 Keamanan (*security*)

Keamanan (*security*) merupakan langkah-langkah yang diambil untuk melindungi informasi, sistem, dan infrastruktur dari ancaman, serangan, atau penyalahgunaan yang dapat mengakibatkan kerugian atau kerusakan. Dalam era digital yang terus berkembang, penting bagi individu dan organisasi untuk

menerapkan langkah-langkah keamanan yang tepat guna melindungi diri mereka dari ancaman yang semakin kompleks Fitrah, E. (2015).

Beberapa jenis ancaman keamanan yang umum di lingkungan digital meliputi:

1. Serangan siber (*cyberattacks*): Ini mencakup serangan seperti peretasan (*hacking*), serangan *denial of service* (DoS), serangan *phishing*, dan serangan perusakan. Serangan siber dapat menyebabkan kebocoran data, pencurian informasi sensitif, atau kerusakan pada sistem dan infrastruktur.
2. Malware: Merupakan perangkat lunak berbahaya yang dirancang untuk menginfeksi sistem dan mencuri informasi atau merusak data. Jenis-jenis malware termasuk virus, worm, trojan, ransomware, dan spyware.
3. Pelanggaran data (data *breaches*): Terjadi ketika informasi yang sensitif atau rahasia diakses atau dicuri oleh pihak yang tidak berwenang. Pelanggaran data dapat mengakibatkan pencurian identitas, penyalahgunaan informasi pribadi, atau kerugian finansial.
4. Rekayasa sosial (*social engineering*): Merupakan metode manipulasi psikologis yang dilakukan oleh penyerang untuk memperoleh informasi sensitif atau mendapatkan akses ke sistem. Contohnya termasuk penipuan melalui telepon, phishing melalui email, atau penipuan melalui media sosial.
5. Untuk melindungi keamanan dalam lingkungan digital, ada beberapa langkah-langkah yang dapat diambil:
6. Enkripsi (*encryption*): Menggunakan teknik enkripsi untuk melindungi data sensitif agar tidak dapat dibaca oleh pihak yang tidak berwenang. Enkripsi melibatkan mengubah data menjadi format yang tidak dapat dimengerti tanpa kunci enkripsi yang sesuai.

7. Firewall: Menggunakan firewall sebagai lapisan pertahanan pertama untuk melindungi jaringan dan sistem dari serangan yang tidak diinginkan. Firewall memantau lalu lintas jaringan dan menerapkan kebijakan keamanan yang ditentukan untuk memblokir akses yang mencurigakan atau berbahaya.
8. Sistem deteksi intrusi (*intrusion detection systems*): Menggunakan sistem deteksi intrusi untuk mengidentifikasi aktivitas mencurigakan atau serangan yang sedang berlangsung. Sistem ini memantau dan menganalisis lalu lintas jaringan atau log aktivitas untuk mendeteksi tanda-tanda serangan.
9. Otentikasi dua faktor (*two-factor authentication*): Mengimplementasikan metode otentikasi yang melibatkan penggunaan lebih dari satu faktor untuk memverifikasi identitas pengguna. Selain kata sandi, ini dapat melibatkan penggunaan kode OTP (*one-time password*), sidik jari, atau token.

1.4 kekurangan *Security and Privacy*

Meskipun keamanan (*security*) dan privasi (*privacy*) memiliki peran yang penting dalam melindungi informasi dan data pribadi Kusumawardhani, D., & Masyithah, D. C. (2019). namun ada beberapa kekurangan yang perlu diperhatikan:

Kekurangan bagian Keamanan (1) Tingkat kompleksitas pada saat mengimplementasikan langkah-langkah keamanan yang efektif memerlukan pemahaman yang mendalam tentang ancaman dan teknologi yang terus berkembang. Hal ini dapat menjadi tantangan bagi individu atau organisasi yang tidak memiliki keahlian khusus di bidang keamanan. (2) di segi Biaya Menerapkan langkah-langkah keamanan yang memadai dapat melibatkan biaya yang signifikan, terutama jika melibatkan investasi dalam perangkat keras, perangkat lunak, dan sumber daya manusia yang

terlatih. Hal ini dapat menjadi hambatan bagi organisasi dengan anggaran terbatas. (3) Kekuatan serangan yang berkembang seperti para penyerang terus mengembangkan teknik dan metode serangan yang lebih canggih. Mereka memanfaatkan kerentanan baru dan menciptakan serangan yang sulit dideteksi atau dipertahankan. Oleh karena itu, keamanan harus terus ditingkatkan dan diikuti perkembangan terbaru.

Kekurangan bagian Privasi (1) Kurangnya kontrol pengguna dalam meskipun ada upaya untuk memberikan pengguna kontrol atas data pribadi mereka, sering kali pengguna tidak sepenuhnya memahami atau menyadari bagaimana data mereka dikumpulkan, digunakan, dan diungkapkan. Ini dapat mengurangi tingkat kepercayaan dan kendali yang seharusnya dimiliki oleh individu. (2) Perusahaan dan praktik yang tidak etis pada beberapa perusahaan atau entitas mungkin tidak mematuhi kebijakan privasi atau melanggar privasi pengguna dengan sengaja. Mereka dapat mengumpulkan data pribadi tanpa persetujuan yang jelas atau menjual data tersebut kepada pihak ketiga tanpa pengetahuan pengguna. (3) Ketidak sepakatan regulasi antara standar dan peraturan privasi dapat berbeda di setiap negara atau yurisdiksi. Kurangnya kesepakatan global dapat menyebabkan celah di mana data pribadi dapat dieksploitasi atau diakses secara tidak sah. (4) Keterbatasan teknologi dalam meskipun ada upaya untuk mengembangkan teknologi yang mendukung privasi (seperti alat enkripsi dan anonimisasi), terkadang keterbatasan teknis atau kendala dalam implementasi dapat menjadi hambatan untuk melindungi privasi secara efektif.

Sangat penting untuk menyadari kekurangan-kekurangan ini dan terus berupaya untuk meningkatkan keamanan dan privasi dalam dunia digital. Perkembangan teknologi dan upaya koordinasi antara individu, organisasi, dan pemerintah sangat penting untuk mengatasi tantangan yang ada dan menjaga keamanan serta privasi informasi yang sensitif.

1.5 Kelebihan Tentang Security And Privacy

Keamanan (*security*) dan privasi (*privacy)*, Meutia, E. D. (2015). memiliki beberapa kelebihan yang sangat penting dalam konteks digital:

Kelebihan Keamanan (1) Perlindungan terhadap ancaman pada Implementasi langkah-langkah keamanan yang tepat dapat melindungi informasi dan data sensitif dari ancaman seperti serangan siber, malware, dan pelanggaran data. Dengan keamanan yang kuat, risiko kerugian atau kerusakan akibat serangan dapat dikurangi atau bahkan dieliminasi. (2) Mempertahankan integritas data dalam keamanan membantu menjaga integritas data dengan mencegah perubahan, penyalahgunaan, atau modifikasi yang tidak sah. Data dapat diandalkan dan dapat dipercaya ketika langkah-langkah keamanan yang sesuai diterapkan. (3) Meningkatkan kepercayaan dalam menerapkan langkah-langkah keamanan yang kuat, individu dan organisasi dapat membangun kepercayaan dengan pengguna, pelanggan, dan mitra bisnis. Kepercayaan yang tinggi dalam keamanan dapat memberikan keunggulan kompetitif dan memperkuat hubungan dengan pihak terkait.

Kelebihan Privasi (1) Kendali atas informasi pribadi diantaranya privasi memberikan individu kendali atas informasi pribadi mereka, termasuk jenis data apa yang dikumpulkan, bagaimana data tersebut digunakan, dan dengan siapa data tersebut dibagikan. Ini memberikan rasa kepercayaan dan memberdayakan individu untuk melindungi privasi mereka. (2) Perlindungan identitas diantaranya privasi yang baik dapat melindungi identitas individu dari penyalahgunaan atau pencurian identitas. Dengan menjaga informasi pribadi tetap aman, individu dapat menghindari risiko penipuan, pencurian identitas, atau serangan siber lainnya yang dapat merugikan mereka secara finansial atau pribadi. (3) Menjaga kebebasan dan anonimitas diantaranya Privasi memungkinkan individu untuk menjelajahi dunia digital tanpa takut terpapar atau diawasi secara terus-

menerus. Ini mendukung kebebasan berekspresi, berbagi informasi, dan berpartisipasi dalam aktivitas online tanpa rasa takut atau ketakutan. (4) Kepatuhan regulasi diantaranya mematuhi peraturan privasi dan kebijakan data yang berlaku adalah kewajiban bagi organisasi. Dengan menjaga privasi dengan baik, organisasi dapat menghindari sanksi hukum, kerugian reputasi, atau tuntutan hukum yang dapat timbul akibat pelanggaran privasi Jafri, N., & Yusof, M. M. (2018).

Maka sangat penting untuk mengenali dan menghargai kelebihan-kelebihan ini untuk melindungi informasi dan data pribadi dengan lebih baik. Dalam era digital yang semakin kompleks, upaya untuk meningkatkan keamanan dan privasi harus terus berlanjut untuk melindungi individu dan organisasi dari ancaman yang terus berkembang.

1.6 Contoh-contoh tentang Security and Privacy

Berikut ini adalah beberapa contoh tentang keamanan (*security*) dan privasi (*privacy*) Revilia, D., & Irwansyah, N. (2020), dalam konteks digital:

Beberapa contoh tentang keamanan (*security*):

1. Penggunaan kata sandi yang kuat: Memilih kata sandi yang kuat dan unik untuk akun-akun online membantu melindungi informasi pribadi dari akses yang tidak sah. Contohnya, menggunakan kombinasi huruf besar dan kecil, angka, dan simbol serta menghindari kata-kata yang mudah ditebak.
2. Firewall: Menginstal firewall pada jaringan komputer atau perangkat dapat memblokir akses yang tidak diinginkan dan melindungi sistem dari serangan siber. Firewall menganalisis lalu lintas data yang masuk dan keluar untuk memastikan keamanan.
3. Sistem deteksi intrusi (*intrusion detection systems*): Menggunakan sistem deteksi intrusi membantu

mendeteksi serangan yang mencurigakan atau upaya tidak sah untuk mengakses sistem atau jaringan. Sistem ini memonitor aktivitas jaringan dan memberikan peringatan saat ada indikasi serangan.

4. Pembaruan perangkat lunak: Memastikan bahwa perangkat lunak dan sistem operasi terbaru diinstal dan diperbarui secara teratur membantu melindungi dari kerentanan yang ditemukan dalam versi sebelumnya. Pembaruan ini sering mengandung perbaikan keamanan yang penting.

Beberapa contoh tentang privasi (*privacy*):

1) Pengaturan privasi media sosial: Menggunakan pengaturan privasi pada platform media sosial untuk mengontrol siapa yang dapat melihat dan mengakses informasi pribadi. Pengguna dapat membatasi akses hanya kepada teman-teman terdekat atau kelompok tertentu.
2) *Opt-out* dari pengumpulan data: Beberapa situs web dan layanan online menyediakan opsi untuk mengopt-out dari pengumpulan data pribadi. Dengan mengaktifkan opsi ini, pengguna dapat menghindari pengumpulan data yang tidak diinginkan atau penggunaan data mereka untuk tujuan pemasaran.
3) Penggunaan VPN (*Virtual Private Network*): Menggunakan VPN dapat menyembunyikan alamat IP pengguna dan mengenkripsi data saat browsing internet. Hal ini membantu menjaga privasi dan melindungi data pengguna dari penyadapan atau penyalahgunaan.
4) Menghapus data pribadi secara teratur: Menghapus data pribadi yang tidak lagi diperlukan atau relevan dari perangkat atau akun online membantu menjaga privasi. Ini melibatkan menghapus riwayat browsing, file sementara, atau informasi pribadi yang disimpan dalam akun online.

Maka sangat penting mengetahui contoh-contoh ini dalam mencerminkan langkah-langkah konkret yang dapat diambil untuk meningkatkan keamanan dan privasi dalam kehidupan digital. Namun, penting untuk diingat bahwa setiap situasi dan kebutuhan privasi dapat bervariasi, dan langkah-langkah yang diperlukan dapat berbeda untuk setiap individu atau organisasi.

1.7 Ringkasan tentang Security and Privacy

Keamanan *(security*) dan privasi (*privacy*) adalah dua konsep yang saling terkait dan krusial dalam konteks digital. Keamanan berkaitan dengan melindungi informasi, sistem, dan infrastruktur dari ancaman dan serangan yang dapat menyebabkan kerugian atau kerusakan. Ini melibatkan langkah-langkah seperti enkripsi, firewall, sistem deteksi intrusi, dan pembaruan perangkat lunak. Sementara itu, privasi berfokus pada melindungi informasi pribadi individu dan memberikan kendali kepada individu atas pengumpulan, penggunaan, dan pengungkapan data mereka. Ini melibatkan pengaturan privasi pada platform media sosial, penggunaan VPN, penghapusan data pribadi yang tidak diperlukan, dan mengopt-out dari pengumpulan data.

Keamanan dan privasi memiliki kelebihan yang signifikan. Keamanan yang kuat melindungi informasi sensitif, mempertahankan integritas data, dan membangun kepercayaan. Sementara itu, privasi memberikan individu kendali atas informasi pribadi, melindungi identitas, menjaga kebebasan, dan mematuhi peraturan privasi. Namun, ada juga kekurangan yang perlu diperhatikan. Keamanan dapat menjadi kompleks dan mahal, dan serangan yang semakin canggih dapat menantang langkah-langkah keamanan yang ada. Sementara itu, privasi dapat terganggu oleh kurangnya kontrol pengguna, praktik tidak etis, ketidaksepakatan regulasi, dan keterbatasan teknologi. Dalam dunia digital yang terus berkembang, penting untuk meningkatkan keamanan dan

privasi. Upaya ini melibatkan pemahaman akan ancaman keamanan yang ada, implementasi langkah-langkah keamanan yang efektif, memastikan kepatuhan terhadap kebijakan privasi, dan memberikan kontrol dan kesadaran kepada individu terkait privasi mereka.

DAFTAR PUSTAKA

Yuwinanto, H. P. 2015. Privasi online dan keamanan data. Palimpsest, 31(11).

Nurhatinah, N. 2018. Pengaruh Keamanan, Privasi, Dan Reputasi Terhadap Kepercayaan Konsumen Online Shopping Di Kota Padang. Jurnal Ecogen, 1(1), 206-217.

Dhianty, R. 2022. Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. Scripta: Jurnal Kebijakan Publik dan Hukum, 2(1), 186-199.

Fitrah, E. 2015. Gagasan Human Security dan Kebijakan Keamanan Nasional Indonesia. Insignia: Journal of International Relations, 2(01), 27-41.

Kusumawardhani, D., & Masyithah, D. C. 2019. Security and Privacy of Cloud Storage as Personal Digital Archive Storage Media. RLJ., 4(2), 167.

Meutia, E. D. 2015. Internet of things–Keamanan dan Privasi. In Seminar Nasional dan Expo Teknik Elektro (Vol. 1, No. 1, pp. 85-89).

Jafri, N., & YUSOF, M. M. 2018. Managing data security risk in model software as a service (SAAS). Asia-Pacific Journal of Information Technology and Multimedia, 7(1), 99-117.

Revilia, D., & Irwansyah, N. 2020. Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. Jurnal Penelitian Komunikasi Dan Opini Publik, 24(1).

BAB 2
VULNERABILITY

Oleh Indrawan Ady Saputro

2.1 Pendahuluan

Vulnerability atau kerentanan dalam keamanan informasi merupakan sebuah situasi dimana sistem rentan terhadap serangan atau risiko tertentu karena memiliki kelemahan atau celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab. Dalam teknologi informasi, kerentanan menjadi salah satu faktor yang sangat penting untuk diperhatikan karena dapat menimbulkan berbagai macam kerugian, seperti mudahnya diserang oleh pihak yang tidak bertanggung jawab, kebocoran data, kerugian finansial, dan reputasi yang tercemar karena informasi sensitif yang dapat diakses secara publik (Aliefyan, 2020). Oleh karena itu, penting bagi organisasi atau perusahaan untuk melakukan tindakan pencegahan terhadap kerentanan sistem yang ada, agar dapat mengurangi risiko terjadinya kerentanan dan kerugian yang dapat ditimbulkan akibatnya. Beberapa hal terkait dengan kerentanan keamanan yang harus diperhatikan, seperti kerentanan keamanan dalam prosesor yang ada pada perangkat keras, kurang adanya pembatasan hak akses sistem, terjadi serangan injeksi SQL pada software, dan penggunaan kata sandi yang tidak unik sehingga mudah ditebak atau diserang oleh manusia. Hal ini perlu mendapat perhatian karena dapat menyebabkan kerugian yang signifikan pada keamanan informasi. Penyebab adanya Kerentanan atau Vulnerability disebabkan adanya kesalahan dari pengguna atau manusia, adanya masalah atau bug pada software atau perangkat lunak, sistem yang terlalu kompleks, konektivitas dengan jaringan

luar meningkat, dan adanya kontrol akses terhadap sistem yang buruk.

Seorang hacker biasanya akan melakukan serangan atau eksploitasi pada sebuah sistem atau program yang memiliki kerentanan atau kelemahan sehingga bisa masuk dan melihat file yang ada pada sistem atau program secara ilegal. Setiap program memiliki kekurangan atau kelemahan hanya saja seorang peretas belum mengetahui atau menemukan celahnya. Seorang hacker tidak semuanya dikatakan buruk atau jahat melainkan ada juga peretas yang baik yang sering disebut dengan white hat hacker. White hacker sering membantu atau memberi tahu celah keamanan kepada pengembang atau developer dari sebuah program atau sistem untuk segera memperbaiki celah keamanan yang ada. Istilah lain yang digunakan untuk menandakan si peretas itu jahat bisa disebut dengan black hat hacker dimana mereka meretas jaringan atau sistem untuk mendapatkan keuntungan sendiri. Kemudian seorang black hat hacker juga akan menjual vulnerability tersebut disebuah situs ilegal yaitu situs "*dark web*".

2.2 Jenis-Jenis Vulnerability

Seringkali, vulnerability yang sering dimanfaatkan terdapat pada perangkat lunak atau software karena memungkinkan serangan dari jarak jauh. Oleh karena itu, jenis vulnerability ini menjadi sasaran favorit bagi para hacker (Wajong, 2012) . Berikut ini adalah beberapa contoh software yang rentan terhadap peretasan karena memiliki vulnerability:

1. Firmware,
   merupakan perangkat lunak (*software*) atau sistem operasi kecil yang biasanya sudah tertanam dalam perangkat keras (*hardware*) memiliki fungsi untuk mengontrol dan mengelola operasi dasar dari perangkat. Firmware biasanya terpasang pada chip atau memori non-volatile dalam perangkat keras. Beberapa contoh perangkat yang

menggunakan firmware yaitu router, kamera, scaner, printer, mouse, telepon dan perangkat elektronik lainnya. Keterbatasan pada kapasitas mengakibatkan firmware ini tidak memiliki sistem operasi sehingga dapat menjadi sebuah celah keamanan atau vulnerabilty yang rentan terhadap serangan. Vulnerability dalam firmware dapat dieksploitasi oleh penyerang untuk mendapatkan akses tidak sah ke perangkat atau merusak fungsionalitasnya.

2. *Software* (Aplikasi)
   Merupakan perangkat lunak atau aplikasi yang sudah terinstal dalam sebuah komputer. *Software* dapat dimanfaatkan dan digunakan oleh seorang penyerang untuk melakukan serangan. Kerentanan yang ada pada software dapat muncul karena adanya kesalahan dalam desain sistem, implementasi dan perawatan perangkat lunak yang jarang diupdate. Beberapa contoh kerentanan yang ada pada software, antara lain : Injection Attacks (menyisipkan perintah berbahaya sehingga dapat merusak data pada komputer), *Cross-site scripting* (mencuri informasi yang sensitif), *Remote code execution* (mengendalikan komputer dari jarak jauh) dan lain sebagainya.
3. *Brainware* (User)
   merupakan seseorang yang menggunakan, mengelola, mengoperasikan, dan berinteraksi dengan sistem komputer. Seperti halnya hardware dan software yang memiliki kerentanan, brainware juga dapat menjadi faktor resiko dalam keamanan sistem. Kerentanan yang berkaitan dengan pengguna komputer antara lain : adanya kejahatan social engineering, kesalahan konfigurasi, kurangnya pemahaman terkait keamanan dan lain lain. Hal tersebut dapat menjadi celah keamanan sehingga peretas dapat akses dari kerentanan pengguna dan dengan mudah mengakses informasi yang ada pada sistem.

4. *Operating System* (Sistem Operasi)
   Merupakan sebuah program yang memiliki fungsi untuk menghubungkan antara software dan hardware. Sistem operasi seperti Windows, MacOS, Linux, Android dan lainnya. Setiap sistem operasi tersebut pastinya memiliki sebuah potensi celah keamanan yang dapat dimanfaatkan oleh peretas untuk melakukan serangan. Kerentanan dalam sistem operasi adalah adanya patch keamanan yang tidak diupdate oleh pengguna, adanya bug dalam sistem operasi dan lain sebagainya
5. Aplikasi Website
   Kerentanan yang ada pada aplikasi website umumnya diakibatkan karena adanya kesalahan pada pengaturan *cache* dan *cookies*, adanya *broken authentication, dan security missconfigurations.* Jika memiliki sebuah situs web, penting untuk selalu waspada terhadap kemungkinan adanya serangan eksploitasi. Serangan ini dapat dimanfaatkan tergantung pada bahasa pemrograman yang digunakan, server web, dan basis data yang digunakan.

Selain kelemahan pada software juga terdapat beberapa jenis kerentanan atau vulnerability yang ada pada sistem atau program komputer antara lain :

1. *Physical Vulnerability*, kerentanan dimana orang yang tidak memiliki akses mencoba masuk melalui server jaringan dan menguasai peralatan jaringan setelah itu melakukan pencurian data dan mencari informasi penting agar bisa masuk kedalam server dilain waktu.
2. *Natural Vulnerability*, kerentanan yang disebabkan adanya ancaman dari bencana alam seperi kebakaran, tsunami, banjir, petir yang dapat merusak data dan komputer.
3. *Hardware and Software Vulnerabilities*, kerentanan yang diakibatkan karena ada kegagalan hardware atau software sehingga dapat membuka peluang celah keamanan.

4. *Media Vulnerabilities*, kerentanan disebabkan oleh adanya kerusakan atau hilangnya pada media back-up, contohnya seperti : tape, catridge, chip memory, disk memory.
5. *Human Vulnerabilities*, kerentanan yang ditimbulkan karena adanya human errorr atau lengahnya user yang mengelola dan menggunakan sistem atau disebut seorang administrator.
6. *Exploting Vulnerabilities*, kerentanan yang disebabkan karena sebuah celah keamanan yang tidak dikontrol secara maksimal.
7. *Communication Vulnerabilities*, kerentanan yang disebabkan karena terhubung ke jaringan internet yang tersedia secara publik sehingga dapat diakses atau dipantau oleh orang lain melalui jaringan tersebut.

2.3 Vulnerability Mapping

Vulnerability mapping merupakan bagian penting dalam strategi keamanan dalam sebuah organisasi, dan membantu mengurangi risiko serangan yang berhasil dengan mengatasi sebuah kelemahan sistem sebelum dieksploitasi. Tujuan dari vulnerability mapping ialah mengidentifikasi dan melakukan prioritas kerentanan sehingga langkah yang diambil untuk mengamankan dapat sesuai dengan kerentanan sistem yang ada sehingga bisa mengurangi atau menghilangkannya (Aji, 2023). Tahapan dalam proses vulnerability mapping antara lain :

1. *Discovery*, proses ini melakukan identifikasi pada semua aset organisasi baik berupa sistem maupun komponen lainnya yang perlu dilakukan analisis kerentanan.
2. *Vulnerability Scanning*, proses ini melakukan pemindaian menggunakan tools atau alat tertentu untuk menemukan celah kerentanan berupa konfigurasi sistem yang salah, versi perangkat lunak yang sudah lama dan celah keamanan lainnya.

3. *Vulnerability Assessment*, proses ini melakukan analisis pada hasil pemindaian yang telah dilakukan sehingga dapat memetakan atau menentukan tingkat kerentanan suatu sistem.
4. *Remediation Planning,* proses ini mengembangkan rencana untuk menyelesaikan permasalahan kerentanan yang telah teridentifikasi, hal tersebut melibatkan penerapan patch, pembaharuan versi perangkat lunak, mengatur ulang konfigurasi sistem dan lainnya untuk menurunkan risiko kerentanan sistem.
5. *Remediation,* proses ini dilakukan sebuah perbaikan terhadap keamanan tingkat lanjut yang didasarkan pada rencana perbaikan.
6. *Ongoing Monitor*, proses ini melakukan monitoring pada sistem untuk menemukan kerentanan yang baru dan melakukan pemantauan terhadap kerentanan secara aktif sehingga dapat memastikan bahwa sistem dalam kondisi aman.

2.4 Vulnerability Assesment

Vulnerability Assessment atau penilaian kerentanan merupakan sebuah proses atau tahapan untuk melakukan identifikasi, evaluasi dan melakukan klasifikasi terhadap tingkat resiko pada kerentanan keamanan yang ada pada jaringan komputer, sistem, aplikasi atau lainnya yang termasuk dalam bidang IT. Kegiatan *vulnerability assessment* dapat dilakukan menggunakan tools atau platform dimana untuk menganalisis keamanan menyeluruh terhadap celah keamanan yang ada. Hal tersebut digunakan untuk dapat memonitoring atau melakukan pengawasan secara berkala ketika ada kerentanan baru sehingga dapat langsung ditindaklanjuti (Darojat, Sediyono and Sembiring, 2022). *Vulnerability Assessment* juga merupakan salah satu komponen dalam evaluasi risiko yang digambarkan oleh Michael

Greg yaitu identifikasi, analisis, penilaian, dan penanganan risiko (Priandoyo, 2006). Proses vulnerability asessment juga memiliki berbagai tingkatan, antara lain :

1. Tingkat I : Policy Assessment
   Pengukuran peraturan kebijakan, hal ini meliputi peraturan kebijakan, standar operasi.
2. Tingkat II : Evaluasi Jaringan
   Pengukuran ini melibatkan penilaian kinerja jaringan, keamanan jaringan, dan ancaman yang mungkin terjadi pada jaringan kerja. Jenis pengukuran ini membutuhkan penggunaan alat bantu seperti pemindai atau pemantau data. Evaluasi jaringan ini bertujuan untuk memperoleh informasi tentang kondisi sebenarnya yang terjadi di lapangan, sejauh mana tingkat kesadaran terhadap keamanan informasi yang telah diterapkan selama ini.
3. Tingkat III : Penetration Test
   Penetration test sebenarnya mengadopsi prinsip yang serupa dengan evaluasi jaringan, namun perbedaannya terletak pada pengujian penetrasi yang dilakukan dalam keadaan yang tidak diketahui, tanpa mengetahui konfigurasi dan kondisi sebenarnya dari sistem yang diuji. Pada pengujian penetrasi, asesor akan menganggap sistem sebagai sebuah kotak yang tertutup, menghadapi serangan penetrasi yang berasal dari luar.

2.5 Vulnerability Management

Manajemen kerentanan adalah suatu praktik yang melibatkan identifikasi, klasifikasi, pemulihan, dan pengurangan kerentanan keamanan. Ini melibatkan lebih dari sekadar pemindaian dan penambalan. Sebaliknya, manajemen kerentanan melibatkan pendekatan yang komprehensif terhadap sistem, proses, dan orang-orang dalam organisasi untuk membuat keputusan berdasarkan informasi yang diperoleh untuk mengatasi

kerentanan dengan cara terbaik. Dari sinilah, tim keamanan TI dapat melakukan tindakan remediasi melalui penerapan penambalan dan konfigurasi pengaturan keamanan yang sesuai. Empat elemen dari program vulnerability management (Pironti, 2006):

1. *Contermeasure Plans*
   Rencana tindakan pengamanan merupakan tindakan yang diambil untuk merespons adanya celah keamanan atau kerentanan pada sistem. Tujuan dari adanya contermeasure plan adalah mengurangi risiko serta melindungi asset dalam organisasi atau perusahaan dari serangan yang ditimbulkan akibat kerentanan pada sistem.
2. *Controls*
   Kontrol dalam manajemen kerentanan ialah langkah dan proses yang diterapkan untuk mengelola sebuah kerentanan pada sistem. Tindakan tersebut digunakan untuk mengidentifikasi, melakukan penilaian dan memberikan tindakn prioritas untuk mengurangi kerentanan yang ada dalam sistem.
3. *Metrics and Measures*
   Merupakan manajemen kerentanan yang didasarkan pada indikator dan metode pengukuran sehingga digunakan untuk memantau dan melakukan evaluasi efektivitas program. Tujuan dari penggunaan metrics dan measures adalah memberikan pemahaman yang lebih baik pada sebuah organisasi tentang kinerja serta ukuran keberhasilan dalam melakukan pengelolaan pada kerentanan.
4. *Intelligence*
   Intelligence dalam konteks kerentanan merujuk pada pengumpulan informasi dan pemahaman yang diperoleh tentang kerentanan yang ada dalam sistem atau aplikasi. Proses ini melibatkan pengumpulan data yang relevan dan analisis mendalam untuk memahami asal-usul,

karakteristik, dan potensi dampak dari kerentanan tersebut.

2.6 Vulnerability Scanning

Vulnerability Scanning berfungsi membantu suatu organisasi untuk melakukan identifikasi kerentanan dalam sistem sehingga dapat melakukan langkah-lanngkah yang tepat untuk mengurangi serangan terhadap kerentanan yang ada. Hal tersebut sangat berguna bagi para pemangku kepentingan untuk mengambil tindakan keamanan untuk menjaga sistem dari kerentanan dan melindungi aset informasi yang berharga Dalam rangka untuk mencapai tingkat keamanan yang optimal maka perlu dikombinasikan dengan proses lainnya seperti pengujian keamanan yang lebih detail, melakukan analisis risiko yang terjadi pada sistem dan lainnya (Zen, Gultom and Reksoprodjo, 2020). Kombinasi tersebut akan lebih efektif karena sebuah organisasi akan mengetahui secara menyeluruh tentang keadaan suatu sistem dan dapat mengambil langkah yang tepat untuk mengatasi permasalahan kerentanan yang ada. Salah satu manfaat adanya vulnerability scanning adalah mengetahui celah keamanan yang mungkin akan dieksploitasi oleh penyerang. Tools yang dapat digunakan untuk melakukan vulnerability scanning antara lain : Aircrack- NG, Wireshark, Burp Suite, NMAP, WPScan dan lain sebagainya.

2.7 Pencegahan terhadap Vulnerability

Beberapa hal yang bisa dilakukan untuk melakukan perlindungan terhadap asset sebuah organisasi atau perusahaan dari adanya kerentanan atau vulnerabilty pada sistem :

1. Update Sistem Operasi, Firmware dan Aplikasi
   menjaga sistem operasi, firmware, dan aplikasi tetap diperbarui secara teratur adalah kunci untuk mencegah adanya kelemahan atau cacat dalam keamanan. Ketiga

komponen ini perlu diperbarui secara berkala karena sering kali menjadi target serangan oleh para hacker, yang mencoba memanfaatkannya sebagai pintu masuk ke dalam sistem. Dengan demikian, penting untuk selalu melakukan pembaruan perangkat lunak guna menjaga keamanan sistem komputer. Para administator juga perlu memeriksa situs web secara rutin dan mengikuti perkembangan terkait keamanan web. Hal ini dikarenakan hacker cenderung menyerang situs web yang tidak diperbarui dengan pembaruan terbaru. Oleh karena itu, menjaga situs web tetap diperbarui dengan versi terbaru sangat penting untuk mencegah kemungkinan retasan.

2. *Vulnerability Assessments*
   tindakan ini memungkinkan perusahaan untuk mengidentifikasi dan mengatasi risiko yang mungkin timbul dari kelemahan sistem di masa depan. Vulnerability Assessment merupakan proses yang melibatkan definisi, identifikasi, klasifikasi, dan prioritisasi kelemahan dalam sistem komputer, aplikasi, dan infrastruktur jaringan. Dengan adanya tindakan penilaian kerentanan/ *vulnerability assessments* sebuah perusahaan atau organisasi dapat mengidentifikasi, mengurangi, dan mengatasi kelemahan yang ada dalam sistem mereka, serta meningkatkan keamanan keseluruhan.
3. Penetration Tests
   Umumnya lingkungan IT perusahaan atau organisasi akan melakukan tindakan penetration testing yang dilakukan oleh *ethical hacker* yang telah diberikan izin untuk melakukannya. Tujuan dari penetration testing adalah untuk menguji kekuatan dan menemukan kerentanan dalam sistem. Ethical hacker menggunakan berbagai alat peretasan yang terkenal secara online, seperti metasploit, nmap, wireshark, aircrack-ng, netcat, BeEF, dan lainnya, untuk membantu dalam proses pentesting. Tujuan dari

tindakan pentesting adalah menguji keamanan sistem komputer, jaringan atau aplikasi sehingga dapat menemukan celah keamanan yang ada dan segera melakukan perbaikan serta menutup celah keamanan tersebut.

4. *Vulnerability Management System*
   Vulnerability management system atau sistem manajemen kerentanan merupakan pendekatan yang dapa digunakan untuk menemukan, memantau dan melakukan pengelolaan dan mengurangi kerentanan dalam sistem atau jaringan. Tahapan pada vulnerability management system adalah proses identifikasi, evaluasi, pengambilan tindakan, persetujuan & evaluasi dan pemantauan serta pemeliharaan.
5. Pemasangan Antivirus
   Adanya program antivirus juga menjadi salah satu faktor untuk mengurangi adanya kerentanan yang diexploitasi oleh peretas. Perangkat lunak antivirus memiliki kemampuan untuk memindai dan mendeteksi payload berbahaya yang disampaikan oleh penyerang, namun tidak dapat secara langsung memperbaiki lubang atau kerentanan yang mungkin ada dalam sistem yang memungkinkan payload tersebut masuk. Walaupun antivirus mempunyai kemampuan dalam melakukan deteksi payload yang berbahaya namun hal tersebut tidak akan menjamin secara penuh dalam menangani semua celah atau kerentanan yang ada dalam sistem.
6. Menerapkan keamanan Wi-Fi atau Jaringan
   Salah satu langkah yang bisa dilakukan yaitu mengamankan dan menyembunyikan jaringan Wi-Fi, hal tersebut mengurangi celah kerentanan saat menggunakan jaringan Wi-Fi tersebut. Hal lain yang bisa diterapkan dalam mengamankan Wi-Fi adalah mengamankan password wifi, menggunakan enkripsi, menerapkan

kontrol akses, memperbarui perangkat firmware Wi-Fi, dan memantau aktifitas jaringan yang terhubung.

.

DAFTAR PUSTAKA

Aji, M.P. 2023. 'Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]', *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, 13(2), pp. 222–238. doi:10.22212/jp.v13i2.3299.

Aliefyan, A. 2020. 'Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web Menggunakan Standar OWASP 10 pada domain Web Perusahaan Penetration Testing Untuk Mengetahui Kerentanan Keamanan Aplikasi Web', *ResearchGate* [Preprint], (July).

Darojat, E.Z., Sediyono, E. and Sembiring, I. 2022. 'Vulnerability Assessment Website E-Government dengan NIST SP 800-115 dan OWASP Menggunakan Web Vulnerability Scanner', *Jurnal Sistem Informasi Bisnis*, 12(1), pp. 36–44. doi:10.21456/vol12iss1pp36-44.

Pironti, J.P. 2006. 'Key elements of a threat and vulnerability management program', *Information Systems Control Journal*, pp. 1–5. Available at: http://www.interop.com/newyork/2005/presentations/downloads/paid/key-elements-of-a-threat-and-vulnerability-mgmt-program-j-pironti.pdf.

Priandoyo, A. 2006. 'Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi', *Ernst & Young*, 1(2), pp. 73–83. Available at: http://majour.maranatha.edu/index.php/jurnal-sistem-informasi/article/view/pp.73 - 83/pdf.

Wajong, A.M.R. 2012. 'Di Jaringan Komputer Pada Umumnya', *Comtech*, 3(9), pp. 474–481. Available at: https://media.neliti.com/media/publications/166137-ID-kerentanan-yang-dapat-terjadi-di-jaringa.pdf.

Zen, B.P., Gultom, R.A.G. and Reksoprodjo, A.H.S. 2020. 'Analisis Security Assessment Menggunakan Metode Penetration Testing dalam Menjaga Kapabilitas Keamanan Teknologi Informasi Pertahanan Negara', *Jurnal Teknologi Penginderaan*, 2(1), pp. 105–122.

BAB 3
FUNDAMENTAL ASPECTS

Oleh Angga Aditya Permana

3.1 Pendahuluan

Proteksi aset informasi mengacu pada tindakan yang diambil untuk melindungi informasi berharga dari ancaman dan risiko yang mungkin membahayakan kerahasiaan, integritas, dan ketersediaannya. Aset informasi dapat berupa data sensitif, sistem komputer, jaringan, perangkat keras, perangkat lunak, dan sumber daya lainnya yang digunakan dalam pengolahan, penyimpanan, dan transmisi informasi. (Supradono, 2012)

Gambar 3.1. Icon Secure

Berikut adalah beberapa langkah yang dapat diambil untuk melindungi aset informasi dengan detail:

1. Identifikasi Aset Informasi: Pertama-tama, Anda perlu mengidentifikasi semua aset informasi yang ada dalam organisasi Anda. Ini melibatkan pengumpulan dan dokumentasi semua jenis informasi yang berharga, termasuk data klien, data keuangan, rencana bisnis, rahasia dagang, dll.

2. Penilaian Risiko: Selanjutnya, lakukan penilaian risiko untuk mengidentifikasi ancaman dan kerentanan yang dapat mempengaruhi aset informasi Anda. Ini melibatkan mengidentifikasi ancaman seperti serangan siber, kehilangan fisik, kebocoran data, kesalahan manusia, dan lainnya. Selain itu, identifikasi juga kerentanan yang ada dalam infrastruktur teknologi Anda, seperti kelemahan dalam sistem, kebijakan keamanan yang lemah, dll.
3. Kebijakan Keamanan Informasi: Buat kebijakan keamanan informasi yang jelas dan komprehensif. Kebijakan ini harus mencakup praktik keamanan yang harus diikuti oleh semua karyawan, termasuk penggunaan kata sandi yang kuat, kebijakan penggunaan perangkat mobile, penggunaan perangkat lunak antivirus, akses terbatas terhadap informasi penting, dan tindakan lainnya yang mendukung keamanan informasi.
4. Kendalikan Akses: Pastikan bahwa hanya orang-orang yang berwenang yang memiliki akses ke aset informasi yang sensitif. Ini dapat dicapai melalui penerapan model kebijakan pengelolaan akses yang ketat, seperti penggunaan sistem otentikasi ganda, otorisasi berbasis peran, dan pengawasan aktivitas pengguna.
5. Pelatihan dan Kesadaran: Melakukan pelatihan rutin kepada karyawan tentang praktik keamanan informasi dan kesadaran terhadap ancaman keamanan. Karyawan harus memahami pentingnya menjaga kerahasiaan informasi, menghindari serangan phishing, menggunakan kata sandi yang kuat, dan melaporkan kejadian keamanan yang mencurigakan.
6. Perlindungan Fisik: Pastikan bahwa aset informasi fisik juga terlindungi dengan baik. Ini dapat mencakup penggunaan kunci fisik atau kartu akses untuk ruangan terbatas, penguncian perangkat keras yang berisi informasi

sensitif, dan pemusnahan aman dokumen yang tidak lagi diperlukan.

7. Sistem Keamanan Teknis: Terapkan sistem keamanan teknis yang tepat, seperti firewall, sistem deteksi intrusi, enkripsi data, perangkat lunak antivirus, dan pembaruan sistem yang teratur. Pastikan bahwa semua sistem dan perangkat lunak Anda diperbarui dengan patch keamanan terbaru.
8. Pemulihan Bencana: Siapkan rencana pemulihan bencana yang efektif untuk memulihkan aset informasi jika terjadi kejadian tak terduga, seperti bencana alam, kebakaran, atau serangan siber yang merusak. Cadangkan data secara teratur, lakukan pemantauan dan pemulihan data yang efisien, serta menguji rencana pemulihan secara berkala.
9. Audit Keamanan: Lakukan audit keamanan secara teratur untuk memeriksa keefektifan kebijakan dan prosedur keamanan informasi yang telah diimplementasikan. Audit ini dapat membantu mengidentifikasi celah keamanan yang mungkin ada dan memberikan rekomendasi perbaikan.
10. Manajemen Keamanan Informasi: Terus pantau dan kelola keamanan informasi secara proaktif. Lakukan peninjauan rutin terhadap kebijakan, prosedur, dan sistem yang ada untuk memastikan keamanan informasi tetap relevan dan diperbarui sesuai dengan perubahan teknologi dan ancaman keamanan.

Penting untuk dicatat bahwa proteksi aset informasi adalah proses yang berkelanjutan dan harus diintegrasikan ke dalam budaya organisasi. Setiap organisasi harus menyesuaikan pendekatan mereka dengan kebutuhan dan sifat unik dari aset informasi yang mereka miliki.

Dalam menjaga aset informasi, terdapat beberapa aspek dasar yang perlu diperhatikan. Berikut adalah beberapa aspek

dasar dalam menjaga aset informasi: (Sulistyowati S.Kom., M.MT., 2021)

1. **Kerahasiaan (*Confidentiality*)**: Aspek ini menekankan pentingnya menjaga informasi agar hanya dapat diakses oleh pihak yang berwenang. Hal ini melibatkan penerapan kontrol akses yang ketat, seperti penggunaan kata sandi yang kuat, otorisasi berbasis peran, enkripsi data, dan tindakan lain yang mencegah akses tidak sah.
2. **Integritas (*Integrity*)**: Aspek integritas berfokus pada keutuhan informasi, yaitu memastikan bahwa informasi tetap utuh, tidak diubah atau dimanipulasi tanpa otorisasi. Langkah-langkah seperti penggunaan tanda tangan digital, kontrol versi dokumen, log pengubahan data, dan tindakan pengawasan dapat membantu menjaga integritas aset informasi.
3. **Ketersediaan (*Availability*)**: Aspek ketersediaan berkaitan dengan memastikan bahwa aset informasi dapat diakses oleh pihak yang berwenang ketika diperlukan. Untuk menjaga ketersediaan, perlu dilakukan pengelolaan kapasitas dan ketersediaan infrastruktur teknologi, cadangan data, pemulihan bencana, dan perlindungan terhadap serangan yang dapat mengganggu ketersediaan sistem.
4. **Keaslian (*Authenticity*)**: Aspek keaslian menekankan pentingnya memastikan bahwa informasi berasal dari sumber yang sah dan dapat dipercaya. Penerapan mekanisme otentikasi, seperti penggunaan kata sandi, sertifikat digital, atau sistem biometrik, dapat membantu memastikan keaslian identitas pengguna atau sumber informasi.
5. **Nonrepudiasi (*Non-repudiation*)**: Aspek nonrepudiasi menjamin bahwa pihak yang terlibat dalam sebuah transaksi atau komunikasi tidak dapat menyangkal keterlibatannya di kemudian hari. Hal ini dicapai dengan

menggunakan tanda tangan digital atau catatan audit yang dapat digunakan sebagai bukti dalam kasus perselisihan atau permasalahan hukum.

6. **Keandalan (*Reliability*)**: Aspek keandalan mencakup aspek kepercayaan dalam penggunaan dan pengolahan aset informasi. Ini melibatkan menjaga tingkat keandalan sistem, jaringan, perangkat lunak, dan perangkat keras yang digunakan untuk mengelola aset informasi. Hal ini dapat mencakup pemeliharaan rutin, pembaruan, dan pengujian yang teratur.
7. **Privasi (*Privacy*)**: Aspek privasi menyangkut perlindungan informasi pribadi atau sensitif individu. Organisasi perlu mematuhi peraturan privasi yang berlaku dan mengadopsi praktik perlindungan data yang kuat, seperti anonimisasi, pemisahan data, dan kebijakan penggunaan data yang jelas.
8. **Kepatuhan (*Compliance*)**: Aspek kepatuhan berkaitan dengan memastikan bahwa aset informasi dan praktik keamanan yang digunakan sesuai dengan peraturan dan standar yang berlaku, seperti undang-undang privasi data, standar keamanan industri, atau persyaratan kontrak dengan pihak ketiga.
9. **Kesadaran dan Pendidikan (*Awareness and Education*)**: Kesadaran dan pendidikan merupakan aspek penting dalam menjaga aset informasi. Organisasi perlu menyediakan pelatihan dan program pendidikan kepada karyawan tentang praktik keamanan informasi, kesadaran terhadap ancaman keamanan, dan tindakan yang harus diambil dalam menjaga keamanan aset informasi.

Memperhatikan dan mengimplementasikan aspek-aspek dasar ini akan membantu dalam menjaga keamanan dan melindungi aset informasi organisasi dari ancaman dan risiko yang mungkin terjadi.

3.2 Aspek Kerahasiaan

Gambar 3.2. Icon Confidentiality

Berikut ini adalah rincian lebih lanjut tentang cara menjaga kerahasiaan dalam proteksi aset informasi: (Indrajit, 2011)

1. Identifikasi Informasi Sensitif: Pertama-tama, identifikasi dan klasifikasikan informasi sensitif dalam organisasi Anda. Ini mencakup data yang jika diungkapkan dapat membahayakan organisasi, seperti data pelanggan, informasi keuangan, rencana bisnis, rahasia dagang, informasi pribadi, dan lainnya. Menetapkan tingkat kepekaan dan kerahasiaan pada setiap jenis informasi membantu dalam menentukan tingkat perlindungan yang diperlukan.
2. Kebijakan Kerahasiaan: Buat kebijakan kerahasiaan yang jelas dan komprehensif. Kebijakan ini harus mencakup definisi informasi sensitif, tanggung jawab karyawan dalam menjaga kerahasiaan, aturan penggunaan, dan langkah-langkah perlindungan yang harus diikuti. Pastikan kebijakan tersebut diterapkan secara konsisten di seluruh organisasi.
3. Pengendalian Akses yang Ketat: Terapkan kontrol akses yang ketat untuk memastikan bahwa hanya orang-orang yang berwenang yang memiliki akses ke informasi sensitif. Gunakan autentikasi yang kuat, seperti penggunaan kata

sandi yang kompleks, autentikasi berbasis faktor ganda, kartu akses, atau teknologi biometrik. Pastikan bahwa hak akses diberikan berdasarkan peran dan tanggung jawab karyawan.

4. Enkripsi Data: Gunakan teknik enkripsi untuk melindungi data saat beristirahat atau dalam penyimpanan. Enkripsi mengubah data menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang, kecuali dengan menggunakan kunci enkripsi yang sesuai. Pastikan penggunaan enkripsi yang kuat untuk melindungi kerahasiaan data.
5. Pelatihan Karyawan: Lakukan pelatihan kepada karyawan tentang pentingnya menjaga kerahasiaan informasi dan konsekuensi pelanggaran kerahasiaan. Berikan pemahaman yang jelas tentang kebijakan kerahasiaan, cara menggunakan kata sandi yang kuat, mengenali serangan phishing, dan menjaga kerahasiaan data dalam kegiatan sehari-hari.
6. Kebijakan Penggunaan Perangkat Mobile: Tetapkan kebijakan yang ketat tentang penggunaan perangkat mobile dan akses ke informasi sensitif. Gunakan teknologi dan aplikasi yang aman untuk mengenkripsi dan melindungi data pada perangkat mobile. Pastikan bahwa kebijakan ini mencakup langkah-langkah untuk mengatasi kehilangan atau pencurian perangkat mobile.
7. Peraturan dan Kepatuhan Hukum: Patuhi peraturan dan undang-undang yang berlaku yang mengatur kerahasiaan dan privasi data, seperti Regulasi Umum Perlindungan Data (GDPR) di Uni Eropa atau undang-undang privasi data di negara masing-masing. Pastikan bahwa organisasi Anda mematuhi persyaratan hukum yang berkaitan dengan kerahasiaan informasi.
8. Pengendalian Cetak dan Penghapusan: Pastikan ada kontrol atas pencetakan dan penghapusan informasi

sensitif secara fisik. Terapkan kebijakan untuk membatasi pencetakan dokumen sensitif dan pastikan bahwa dokumen yang tidak lagi diperlukan dihancurkan dengan aman menggunakan pemusnahan yang sesuai.

9. Pengawasan dan Audit: Melakukan pemantauan dan audit yang teratur untuk memastikan kepatuhan terhadap kebijakan kerahasiaan dan mendeteksi potensi pelanggaran. Pemantauan ini meliputi pemantauan aktivitas pengguna, pemeriksaan log, dan pemeriksaan keamanan rutin untuk mengidentifikasi dan menangani insiden yang melibatkan kerahasiaan informasi.
10. Pengendalian Kontrak dan Mitra Bisnis: Jika ada pertukaran informasi sensitif dengan pihak ketiga, pastikan ada perjanjian kerahasiaan yang jelas dan memadai yang mengatur penggunaan dan perlindungan informasi sensitif. Lakukan pemeriksaan keamanan dan evaluasi risiko terhadap mitra bisnis untuk memastikan bahwa mereka memenuhi standar kerahasiaan yang sesuai.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga kerahasiaan aset informasi dan mencegah akses tidak sah atau penyalahgunaan informasi sensitif.

3.3 Aspek Integritas

Gambar 3.3. Integrity Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga integritas dalam proteksi aset informasi:

1. Pengendalian Akses: Terapkan kontrol akses yang ketat untuk memastikan hanya individu yang berwenang yang memiliki izin untuk mengubah atau mengakses informasi sensitif. Gunakan autentikasi yang kuat, seperti kata sandi yang kompleks, autentikasi berbasis faktor ganda, dan otorisasi berbasis peran. Pastikan hak akses yang sesuai diberikan kepada setiap pengguna berdasarkan tanggung jawab mereka.
2. Penggunaan Tanda Tangan Digital: Gunakan tanda tangan digital atau sertifikat digital untuk memverifikasi integritas dokumen atau komunikasi. Tanda tangan digital menggunakan teknik kriptografi untuk memberikan bukti bahwa dokumen tidak diubah sejak ditandatangani dan berasal dari sumber yang sah.
3. Pengawasan dan Audit: Lakukan pemantauan dan audit secara teratur untuk mendeteksi perubahan yang tidak sah atau tidak diotorisasi pada aset informasi. Pemantauan ini mencakup pemantauan aktivitas pengguna, pemeriksaan log, dan pemeriksaan keamanan rutin untuk memastikan kepatuhan terhadap kebijakan dan prosedur serta mendeteksi adanya pelanggaran integritas.
4. Penanganan Perubahan: Tetapkan kebijakan dan prosedur yang jelas untuk pengelolaan perubahan pada aset informasi. Ini termasuk peninjauan, persetujuan, dan dokumentasi yang tepat sebelum perubahan dilakukan. Pastikan bahwa hanya perubahan yang diotorisasi yang diizinkan dan bahwa perubahan dicatat dengan baik.
5. Pengelolaan Versi: Kelola versi dokumen dan perangkat lunak untuk memastikan integritasnya. Pastikan bahwa hanya versi terbaru yang digunakan dan dibagikan, dan selalu simpan riwayat perubahan untuk referensi dan pemulihan jika diperlukan.

6. Keamanan Fisik: Lindungi aset informasi fisik untuk mencegah manipulasi atau kerusakan fisik yang dapat mempengaruhi integritas data. Gunakan tindakan keamanan fisik seperti penguncian ruangan, kartu akses, atau pengawasan fisik untuk mencegah akses tidak sah ke aset informasi.
7. Enkripsi Data: Gunakan enkripsi untuk melindungi integritas data saat beristirahat atau dalam penyimpanan. Enkripsi mengamankan data dari perubahan yang tidak diinginkan atau manipulasi dengan mengubahnya menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang tepat.
8. Pemulihan Bencana dan Cadangan Data: Tetapkan rencana pemulihan bencana yang efektif untuk melindungi integritas data jika terjadi kejadian tak terduga. Lakukan cadangan data secara teratur untuk memastikan bahwa data sensitif dapat dipulihkan jika terjadi kegagalan sistem atau kehilangan data.
9. Peninjauan Keamanan: Lakukan peninjauan keamanan secara rutin untuk memastikan bahwa sistem, perangkat lunak, dan kebijakan keamanan yang digunakan dalam pengolahan dan penyimpanan aset informasi memenuhi standar dan praktik terbaik. Identifikasi kerentanan dan kerangka kerja untuk melakukan perbaikan dan peningkatan yang diperlukan.
10. Pelatihan Karyawan: Lakukan pelatihan dan kesadaran terhadap praktik keamanan informasi kepada karyawan. Berikan pemahaman yang jelas tentang pentingnya menjaga integritas data, tanda-tanda perubahan yang mencurigakan, dan tindakan yang harus diambil dalam melaporkan insiden yang melibatkan integritas aset informasi.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga integritas aset informasi dan mencegah perubahan yang tidak sah atau tidak diinginkan pada data sensitif Anda.

3.4 Aspek Ketersediaan

Gambar 3.4. Availability Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga ketersediaan dalam proteksi aset informasi:

1. Pengelolaan Kapasitas: Pastikan infrastruktur teknologi, seperti server, jaringan, dan sistem penyimpanan, memiliki kapasitas yang cukup untuk menangani beban kerja yang ada dan pertumbuhan di masa depan. Lakukan pemantauan kapasitas secara teratur untuk mengidentifikasi dan mengatasi potensi masalah yang dapat mempengaruhi ketersediaan.
2. Redundansi dan Pemulihan Bencana: Implementasikan strategi redundansi dan rencana pemulihan bencana untuk memastikan ketersediaan aset informasi. Ini dapat meliputi replikasi data di pusat data yang terpisah secara geografis, pengaturan server cadangan, dan langkah-langkah pemulihan bencana seperti backup data reguler, pengujian pemulihan, dan pemantauan bencana alam.

3. Pemeliharaan dan Pembaruan: Lakukan pemeliharaan rutin dan pembaruan perangkat lunak dan perangkat keras untuk menjaga ketersediaan sistem. Pastikan bahwa perangkat lunak dan perangkat keras diperbarui dengan patch keamanan terbaru dan rutin melakukan pemantauan kesehatan sistem untuk mendeteksi potensi masalah yang dapat mempengaruhi ketersediaan.
4. Pengendalian Perubahan: Lakukan manajemen perubahan yang baik untuk meminimalkan dampak pada ketersediaan sistem. Implementasikan proses yang terencana dan teruji untuk perubahan pada infrastruktur teknologi, termasuk peninjauan, persetujuan, dan pengujian yang sesuai sebelum perubahan diimplementasikan.
5. Pengawasan Kinerja: Lakukan pemantauan kinerja sistem secara terus-menerus untuk mendeteksi masalah yang dapat mempengaruhi ketersediaan. Monitor ketersediaan jaringan, penggunaan sumber daya, latensi, dan beban kerja untuk mengidentifikasi potensi masalah dan mengambil tindakan yang diperlukan.
6. Perlindungan Terhadap Serangan: Terapkan langkah-langkah keamanan yang kuat untuk melindungi infrastruktur dari serangan yang dapat mengganggu ketersediaan. Ini termasuk penggunaan firewall, sistem deteksi intrusi, perlindungan terhadap serangan DDoS (Distributed Denial of Service), dan perangkat lunak antivirus yang terkini.
7. Pemantauan dan Respons Kejadian: Tetapkan sistem pemantauan dan respons kejadian yang efektif untuk mendeteksi, mengidentifikasi, dan merespons gangguan atau insiden yang dapat mempengaruhi ketersediaan. Pastikan adanya rencana tanggap darurat yang jelas dan prosedur pemulihan yang cepat.
8. Kebijakan Penanganan Data: Tetapkan kebijakan yang jelas tentang bagaimana mengelola data, penyimpanan, dan

pemulihan. Ini termasuk prosedur untuk backup data secara teratur, retensi data yang sesuai, dan metode pemulihan yang dapat dipercaya dalam situasi bencana atau kejadian tak terduga.

9. Kesadaran Karyawan: Tingkatkan kesadaran karyawan tentang pentingnya menjaga ketersediaan aset informasi. Lakukan pelatihan dan edukasi tentang tindakan yang harus diambil dalam situasi darurat atau gangguan, serta pentingnya melaporkan masalah segera.
10. Perjanjian Layanan Pihak Ketiga: Jika menggunakan layanan pihak ketiga, pastikan ada perjanjian layanan yang jelas dan memadai yang mengatur ketersediaan sistem. Pastikan penyedia layanan memiliki tingkat ketersediaan yang baik dan mematuhi persyaratan kontrak.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga ketersediaan aset informasi dan meminimalkan waktu henti yang dapat mempengaruhi operasional dan produktivitas organisasi Anda.

3.5 Aspek Keaslian

Gambar 3.5. Authentic Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga keaslian (*authenticity*) dalam proteksi aset informasi:

1. Penggunaan Tanda Tangan Digital: Gunakan tanda tangan digital atau sertifikat digital untuk memastikan keaslian dan integritas dokumen atau komunikasi. Tanda tangan digital menggunakan teknik kriptografi untuk memberikan bukti bahwa dokumen tersebut berasal dari sumber yang sah dan tidak diubah sejak ditandatangani.
2. Identifikasi dan Otorisasi Pengguna: Pastikan ada sistem identifikasi dan otorisasi pengguna yang kuat. Setiap pengguna harus memiliki akun yang unik dan harus melewati proses autentikasi yang tepat sebelum diizinkan mengakses informasi sensitif atau melakukan perubahan.
3. Keamanan Akses: Terapkan kontrol akses yang ketat untuk memastikan bahwa hanya pengguna yang berwenang yang memiliki akses ke aset informasi. Gunakan autentikasi yang kuat, seperti kata sandi yang kompleks, autentikasi berbasis faktor ganda, kartu akses, atau teknologi biometrik. Pastikan bahwa hak akses diberikan berdasarkan peran dan tanggung jawab yang tepat.
4. Penggunaan Enkripsi: Gunakan enkripsi untuk melindungi keaslian informasi saat beristirahat atau dalam penyimpanan. Enkripsi membantu mencegah perubahan atau pemalsuan data dengan mengubahnya menjadi bentuk yang tidak dapat dibaca oleh pihak yang tidak berwenang.
5. Keamanan Fisik: Lindungi aset informasi fisik dari akses yang tidak sah atau manipulasi yang dapat mempengaruhi keaslian. Gunakan tindakan keamanan fisik, seperti penguncian ruangan, kartu akses, atau pengawasan fisik, untuk mencegah akses yang tidak sah ke aset informasi.
6. Audit dan Pemantauan: Lakukan pemantauan dan audit secara teratur untuk mendeteksi perubahan atau aktivitas yang mencurigakan yang dapat mempengaruhi keaslian informasi. Pemantauan ini dapat mencakup pemantauan aktivitas pengguna, pemeriksaan log, dan pemeriksaan

keamanan rutin untuk memastikan kepatuhan terhadap kebijakan dan prosedur.

7. Kriptografi: Gunakan teknik kriptografi yang kuat untuk mengamankan informasi sensitif. Ini termasuk penggunaan algoritma kriptografi yang terbukti dan kunci enkripsi yang aman. Pastikan bahwa kunci enkripsi disimpan dengan aman dan hanya diakses oleh pihak yang berwenang.
8. Validasi Data: Lakukan validasi data untuk memastikan integritas dan keaslian informasi. Ini melibatkan pemeriksaan integritas data, verifikasi tanda tangan digital, dan pengecekan data masukan untuk memastikan bahwa data yang diterima adalah data yang sah.
9. Pemantauan Identitas: Implementasikan sistem pemantauan identitas yang efektif untuk mendeteksi tindakan yang mencurigakan atau aktivitas yang tidak biasa yang dapat mengancam keaslian informasi. Hal ini mencakup deteksi anomali, peringatan dini, dan pemeriksaan keamanan yang kontinu.
10. Pelatihan Karyawan: Tingkatkan kesadaran karyawan tentang pentingnya menjaga keaslian informasi dan konsekuensi dari pelanggaran keaslian. Lakukan pelatihan tentang praktik keamanan informasi, pengenalan serangan phishing atau teknik sosial engineering, dan pentingnya melaporkan aktivitas yang mencurigakan.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga keaslian aset informasi dan memastikan bahwa informasi yang digunakan dan dipertukarkan berasal dari sumber yang sah dan tidak diubah atau dipalsukan secara tidak sah.

3.6 Aspek Non-repudiation

Gambar 3.6. Non-repudiation Icon

Non-repudiation adalah kemampuan untuk memastikan bahwa seseorang tidak dapat menyangkal atau menolak tanggung jawab atau keaslian dari tindakan atau transaksi yang telah mereka lakukan. Berikut adalah rincian lebih lanjut tentang cara menjaga *non-repudiation* dalam proteksi aset informasi:

1. Tanda Tangan Digital: Gunakan tanda tangan digital atau sertifikat digital untuk memastikan non-repudiation dalam transaksi elektronik. Tanda tangan digital menggunakan teknik kriptografi untuk memberikan bukti bahwa transaksi tersebut dilakukan oleh pihak yang sah dan tidak dapat disangkal atau ditolak.
2. Catatan Audit: Lakukan pemantauan dan pencatatan aktivitas yang terkait dengan aset informasi. Catatan audit yang lengkap dan terperinci dapat digunakan sebagai bukti untuk memverifikasi tindakan yang dilakukan dan mengatasi argumen penyangkalan.
3. Penggunaan Sistem Keamanan yang Terpercaya: Pastikan penggunaan sistem keamanan yang terpercaya dan dapat dipercaya. Gunakan teknologi dan perangkat lunak yang dapat menghasilkan catatan audit yang akurat dan tahan terhadap perubahan atau manipulasi.

4. Enkripsi Data: Gunakan enkripsi untuk melindungi integritas data dan memastikan non-repudiation. Enkripsi data saat beristirahat atau dalam penyimpanan memastikan bahwa data tidak dapat diubah atau dimanipulasi tanpa diketahui oleh pihak yang berwenang.
5. Keamanan Fisik: Lindungi aset informasi fisik secara fisik untuk mencegah akses yang tidak sah atau manipulasi yang dapat mengancam non-repudiation. Gunakan tindakan keamanan fisik, seperti penguncian ruangan atau kartu akses, untuk membatasi akses yang tidak sah.
6. Pengendalian Akses dan Otorisasi yang Ketat: Terapkan kontrol akses yang ketat dan mekanisme otorisasi yang kuat untuk memastikan hanya individu yang berwenang yang memiliki akses dan dapat melakukan transaksi. Ini membantu dalam memperkuat non-repudiation karena transaksi dilakukan oleh pihak yang telah diidentifikasi dengan jelas.
7. Pemantauan Identitas: Implementasikan sistem pemantauan identitas yang efektif untuk mendeteksi tindakan yang mencurigakan atau aktivitas yang tidak biasa yang dapat mengancam non-repudiation. Identifikasi dan verifikasi identitas dalam setiap transaksi penting untuk memastikan tanggung jawab dan integritas.
8. Pencatatan Waktu (*Timestamping)*: Gunakan layanan pencatatan waktu yang dapat dipercaya untuk memberikan bukti tentang waktu transaksi atau tindakan yang dilakukan. Timestamping yang andal membantu menguatkan non-repudiation dan dapat digunakan sebagai bukti dalam sengketa atau perselisihan.
9. Penanganan Kontrak dan Persetujuan: Pastikan adanya kontrak dan persetujuan yang jelas dalam setiap transaksi atau tindakan. Kontrak dan persetujuan ini dapat digunakan sebagai bukti non-repudiation dalam kasus perselisihan atau penyangkalan.

10. Pelatihan Karyawan: Tingkatkan kesadaran karyawan tentang pentingnya non-repudiation dan konsekuensi pelanggaran. Lakukan pelatihan tentang pentingnya menghormati komitmen dan tanggung jawab yang terkait dengan transaksi atau tindakan yang dilakukan.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga non-repudiation dalam proteksi aset informasi dan memastikan bahwa transaksi dan tindakan yang dilakukan tidak dapat disangkal atau ditolak oleh pihak yang terlibat.

3.7 Aspek Kehandalan

Gambar 3.7. Reliability Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga kehandalan (*reliability*) dalam proteksi aset informasi:

1. Redundansi: Implementasikan redundansi pada infrastruktur teknologi untuk memastikan ketersediaan yang tinggi dan kehandalan sistem. Ini mencakup replikasi data dan pengaturan server cadangan untuk memastikan bahwa jika ada kegagalan pada satu komponen, sistem dapat tetap beroperasi dengan lancar.
2. Pemulihan Bencana: Tetapkan rencana pemulihan bencana yang efektif untuk mengatasi gangguan atau kejadian tak terduga. Rencana ini harus mencakup prosedur pemulihan

yang jelas, pengujian rutin, dan pemantauan untuk memastikan bahwa sistem dapat dengan cepat dipulihkan ke kondisi yang berfungsi setelah terjadi kegagalan atau bencana.

3. Pengelolaan Perubahan: Lakukan manajemen perubahan yang hati-hati untuk meminimalkan dampak pada kehandalan sistem. Ini melibatkan peninjauan, persetujuan, dan pengujian yang cermat sebelum melakukan perubahan pada infrastruktur teknologi. Pastikan ada prosedur yang jelas dan dipatuhi dalam mengimplementasikan perubahan.
4. Pemeliharaan Rutin: Lakukan pemeliharaan rutin pada perangkat keras dan perangkat lunak untuk menjaga kehandalan sistem. Pastikan bahwa perangkat keras dan perangkat lunak diperbarui dengan patch keamanan terbaru, melakukan pemantauan kesehatan sistem secara berkala, dan menjalankan tugas pemeliharaan yang direkomendasikan oleh vendor atau produsen.
5. Pengawasan dan Pemantauan: Lakukan pemantauan kinerja dan pemantauan sistem secara terus-menerus untuk mendeteksi masalah atau perubahan yang dapat mempengaruhi kehandalan. Gunakan alat pemantauan yang sesuai untuk memantau ketersediaan jaringan, beban kerja server, penggunaan sumber daya, dan kinerja keseluruhan sistem.
6. Pengujian dan Validasi: Lakukan pengujian reguler dan validasi untuk memastikan kehandalan sistem. Ini meliputi pengujian ketersediaan, pengujian beban, dan pengujian pemulihan bencana. Dengan menguji sistem secara rutin, Anda dapat mengidentifikasi dan mengatasi masalah potensial sebelum mereka menjadi masalah yang lebih besar.
7. Keamanan Fisik: Pastikan bahwa aset informasi fisik, seperti server dan perangkat penyimpanan, terlindungi

dengan baik untuk mencegah kerusakan atau kehilangan yang dapat mengganggu kehandalan sistem. Gunakan tindakan keamanan fisik, seperti penguncian ruangan, pengawasan fisik, dan perlindungan terhadap bencana alam, untuk menjaga keandalan infrastruktur.

8. Pelatihan Karyawan: Lakukan pelatihan dan kesadaran karyawan tentang pentingnya menjaga kehandalan sistem dan langkah-langkah yang dapat diambil dalam mengatasi masalah. Karyawan harus diberikan pemahaman tentang tugas pemeliharaan yang perlu dilakukan, prosedur pemulihan yang harus diikuti, dan cara melaporkan masalah jika terjadi kegagalan atau gangguan.
9. Keandalan Vendor dan Mitra Bisnis: Jika menggunakan layanan pihak ketiga atau berkolaborasi dengan mitra bisnis, pastikan mereka memiliki keandalan yang baik dan memenuhi standar kehandalan yang diperlukan. Tinjau kontrak atau perjanjian layanan untuk memastikan bahwa tingkat keandalan yang sesuai ditetapkan dan dipatuhi.
10. Monitoring dan Respons Kejadian: Tetapkan sistem pemantauan dan respons kejadian yang efektif untuk mendeteksi, mengidentifikasi, dan merespons masalah atau gangguan yang dapat mempengaruhi kehandalan sistem. Pastikan ada prosedur pemulihan yang jelas dan respons yang cepat untuk meminimalkan waktu henti dan dampak negatif pada operasional bisnis.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga kehandalan aset informasi dan memastikan sistem tetap berfungsi dengan baik, dapat diandalkan, dan menghindari gangguan yang dapat mempengaruhi operasional organisasi Anda.

3.8 Aspek Privasi

Gambar 3.8. Privacy Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga privasi dalam proteksi aset informasi:

1. Identifikasi Data Pribadi: Identifikasi jenis data pribadi yang Anda kumpulkan, simpan, atau kelola. Ini mencakup informasi seperti nama, alamat, nomor telepon, alamat email, informasi keuangan, atau informasi identifikasi pribadi lainnya.
2. Kebijakan Privasi: Tetapkan kebijakan privasi yang jelas dan terperinci yang menjelaskan bagaimana Anda mengumpulkan, menggunakan, menyimpan, dan melindungi data pribadi. Kebijakan ini harus menguraikan hak-hak individu terkait privasi mereka, termasuk akses, koreksi, dan penghapusan data.
3. Klasifikasi Data: Klasifikasikan data pribadi ke dalam kategori yang berbeda berdasarkan tingkat sensitivitasnya. Ini membantu Anda menentukan tingkat keamanan yang diperlukan untuk setiap jenis data dan menerapkan kontrol akses dan perlindungan yang sesuai.
4. Pengendalian Akses: Terapkan kontrol akses yang ketat untuk melindungi data pribadi. Hanya berikan akses kepada individu yang berwenang dan membutuhkan akses tersebut untuk menjalankan tugas mereka. Gunakan autentikasi yang kuat, seperti kata sandi yang kompleks,

autentikasi berbasis faktor ganda, dan penggunaan kartu akses atau token.

5. Enkripsi Data: Gunakan teknik enkripsi untuk melindungi data pribadi saat beristirahat atau dalam penyimpanan. Enkripsi mengubah data menjadi bentuk yang tidak dapat dibaca tanpa kunci enkripsi yang sesuai, menjaga kerahasiaan dan integritas data pribadi jika data tersebut diakses oleh pihak yang tidak berwenang.
6. Penghapusan Data yang Tidak Diperlukan: Hapus data pribadi yang tidak lagi diperlukan secara teratur. Pastikan bahwa metode penghapusan data yang digunakan sesuai dengan standar keamanan yang diterima, seperti penghapusan aman dengan metode pembersihan disk yang dapat menghapus data secara permanen.
7. Perlindungan Data dalam Perpindahan: Jika data pribadi dipindahkan atau ditransmisikan, pastikan adanya perlindungan yang memadai selama perpindahan tersebut. Gunakan protokol enkripsi yang kuat saat mengirim data melalui jaringan atau menggunakan jasa pihak ketiga untuk mengamankan transfer data.
8. Pengawasan dan Audit: Lakukan pemantauan dan audit secara teratur untuk mendeteksi dan mencegah akses tidak sah atau pelanggaran privasi. Pemantauan ini dapat mencakup pemantauan aktivitas pengguna, pemeriksaan log, dan pemeriksaan keamanan rutin untuk memastikan kepatuhan terhadap kebijakan privasi dan mendeteksi ancaman potensial.
9. Perlindungan Identitas: Lindungi identitas individu dengan mengurangi penggunaan identifikasi pribadi dalam sistem atau dokumentasi internal. Gunakan penggantian atau tokenisasi data pribadi saat memungkinkan.
10. Kesadaran Karyawan: Lakukan pelatihan dan kesadaran karyawan tentang pentingnya privasi data dan perlindungan privasi. Berikan pemahaman yang jelas

tentang kebijakan privasi, tindakan yang harus diambil dalam melindungi data pribadi, dan cara melaporkan pelanggaran privasi.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga privasi data pribadi dan memastikan bahwa data sensitif tidak disalahgunakan atau diakses oleh pihak yang tidak berwenang.

3.9 Aspek Kepatuhan

Gambar 3.9. Compliance Icon

Berikut ini adalah rincian lebih lanjut tentang cara menjaga kepatuhan (*compliance*) dalam proteksi aset informasi:

1. Pemahaman Regulasi dan Standar: Memahami dan mengetahui regulasi dan standar yang berlaku untuk aset informasi Anda. Ini mungkin termasuk undang-undang privasi data, peraturan keuangan, standar industri, dan persyaratan kepatuhan lainnya yang relevan dengan bisnis Anda.
2. Evaluasi Kebutuhan Kepatuhan: Lakukan evaluasi kebutuhan kepatuhan untuk aset informasi Anda berdasarkan regulasi dan standar yang berlaku. Identifikasi persyaratan spesifik yang harus dipenuhi, seperti perlindungan data pribadi, pengendalian akses, retensi data, atau laporan keuangan.

3. Penetapan Kebijakan dan Prosedur: Tetapkan kebijakan dan prosedur yang jelas untuk memenuhi persyaratan kepatuhan. Pastikan bahwa kebijakan mencakup langkah-langkah yang spesifik dan praktik terbaik untuk melindungi aset informasi dan memastikan kepatuhan.
4. Audit Kepatuhan: Lakukan audit kepatuhan secara rutin untuk memastikan bahwa kebijakan dan prosedur kepatuhan diterapkan dengan benar. Audit ini harus mencakup pemeriksaan kepatuhan terhadap regulasi dan standar yang berlaku, serta penilaian terhadap kepatuhan internal.
5. Perlindungan Data Pribadi: Pastikan kepatuhan terhadap regulasi perlindungan data pribadi yang berlaku, seperti General Data Protection Regulation (GDPR) di Uni Eropa atau Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia. Lindungi data pribadi dengan menerapkan pengaturan pengumpulan, penggunaan, penyimpanan, dan penghapusan data yang sesuai.
6. Pengendalian Akses: Terapkan kontrol akses yang ketat untuk memastikan bahwa hanya pengguna yang berwenang yang memiliki akses ke aset informasi. Gunakan autentikasi yang kuat dan otorisasi yang tepat untuk membatasi akses ke data sensitif.
7. Perlindungan Terhadap Serangan dan Ancaman: Implementasikan langkah-langkah keamanan yang tepat untuk melindungi aset informasi dari serangan dan ancaman. Ini termasuk penggunaan firewall, sistem deteksi intrusi, perlindungan terhadap serangan DDoS, dan perangkat lunak keamanan yang diperbarui.
8. Pelaporan dan Dokumentasi: Lakukan pelaporan yang akurat dan tepat waktu sesuai dengan persyaratan kepatuhan. Pastikan bahwa catatan dan dokumen kepatuhan disimpan dengan baik untuk tujuan audit dan pemeriksaan oleh otoritas yang berwenang.

9. Pemeliharaan dan Pembaruan: Lakukan pemeliharaan rutin dan pembaruan pada infrastruktur dan sistem keamanan untuk memastikan kepatuhan berkelanjutan. Pastikan bahwa perangkat lunak dan perangkat keras diperbarui dengan patch keamanan terbaru dan perlindungan yang sesuai diterapkan.
10. Pelatihan Karyawan: Lakukan pelatihan dan kesadaran kepada karyawan tentang kebijakan dan prosedur kepatuhan. Berikan pemahaman yang jelas tentang persyaratan kepatuhan yang relevan, tindakan yang harus diambil untuk memenuhi kepatuhan, dan pentingnya melaporkan pelanggaran kepatuhan.

Dengan mengikuti langkah-langkah ini, Anda dapat menjaga kepatuhan terhadap regulasi dan standar yang berlaku dalam melindungi aset informasi Anda dan memastikan kepatuhan yang berkelanjutan terhadap persyaratan kepatuhan yang relevan.

3.10 Aspek Kesadaran dan Pendidikan

Gambar 3.10. Awareness and Education Icon

Berikut ini adalah rincian lebih lanjut tentang cara meningkatkan kesadaran dan pendidikan dalam proteksi aset informasi:

1. Program Kesadaran Keamanan Informasi: Tetapkan program kesadaran keamanan informasi yang komprehensif. Ini mencakup penyusunan materi pelatihan,

penyampaian sesi pelatihan kepada karyawan, dan penyediaan sumber daya pendidikan seperti buku panduan keamanan informasi, poster, dan materi referensi lainnya.

2. Pelatihan Karyawan: Lakukan pelatihan reguler kepada karyawan tentang praktik keamanan informasi yang relevan. Fokuskan pada topik seperti kebijakan keamanan, penggunaan yang aman dari sistem dan perangkat, kesadaran terhadap serangan phishing dan sosial engineering, pengelolaan kata sandi yang kuat, dan pentingnya melaporkan insiden keamanan.
3. Kampanye Kesadaran: Jalankan kampanye kesadaran yang kreatif dan berkesinambungan untuk mempromosikan pentingnya keamanan informasi. Gunakan materi visual seperti poster, video, atau infografis untuk mengkomunikasikan pesan penting dengan cara yang menarik dan mudah dipahami.
4. Komunikasi Internal: Tingkatkan komunikasi internal tentang keamanan informasi. Gunakan saluran komunikasi seperti email, intranet, atau papan pengumuman untuk menyebarkan berita terkini tentang ancaman keamanan, perubahan kebijakan, dan praktik terbaik. Juga, dorong karyawan untuk berbagi pengalaman dan pengetahuan tentang keamanan informasi.
5. Uji Kesadaran (Phishing Test): Lakukan uji kesadaran atau simulasi serangan phishing kepada karyawan. Ini membantu menguji sejauh mana karyawan memahami ancaman dan mampu mengidentifikasi email atau pesan yang mencurigakan. Uji kesadaran ini dapat digunakan sebagai peluang untuk memberikan umpan balik dan memberikan pelatihan tambahan jika diperlukan.
6. Peran Model dari Manajemen: Manajemen harus menjadi peran model dalam mempraktikkan keamanan informasi. Mereka harus mematuhi kebijakan keamanan, menjaga kerahasiaan, dan mengikuti praktik terbaik. Hal ini akan

memperkuat kesadaran dan budaya keamanan informasi di seluruh organisasi.

7. Pembagian Informasi Keamanan: Terus-menerus berbagi informasi tentang ancaman keamanan terkini dan teknik serangan yang berkembang. Lakukan ceramah, sesi diskusi, atau webinar tentang topik keamanan informasi yang relevan agar karyawan dapat terus memperbarui pengetahuan mereka.
8. Penghargaan dan Insentif: Berikan penghargaan atau insentif kepada karyawan yang menunjukkan keterlibatan aktif dalam praktik keamanan informasi yang baik. Hal ini mendorong kesadaran dan menghargai upaya individu dalam melindungi aset informasi.
9. Pendidikan Kontinu: Pastikan bahwa pendidikan keamanan informasi adalah proses yang berkelanjutan. Selalu perbarui dan tingkatkan program pelatihan sesuai dengan ancaman dan kebutuhan baru. Tetap mengikuti perkembangan teknologi dan praktik keamanan terkini.
10. Partisipasi Eksternal: Ajak karyawan untuk mengikuti konferensi, seminar, atau pelatihan eksternal tentang keamanan informasi. Ini memberi mereka kesempatan untuk belajar dari para ahli industri dan memperluas jaringan kontak dengan profesional keamanan informasi lainnya.

Dengan mengikuti langkah-langkah ini, Anda dapat meningkatkan kesadaran dan pendidikan karyawan tentang keamanan informasi, yang merupakan langkah penting dalam melindungi aset informasi dan meminimalkan risiko keamanan.

DAFTAR PUSTAKA

Indrajit, Prof., R.E. 2011. 'Manajemen keamanan informasi', (1), pp. 1–19. Available at: https://doi.org/12.01.123.

Sulistyowati S.Kom., M.MT., I. 2021. 'Pengantar Keamanan Sistem Komputer & Jaringan Komputer', pp. 1–46.

Supradono, B. 2012. 'Pengembangan Kerangka Kerja Manajemen Keamanan Informasi (Studi Empirik : Universitas Muhammadiyah Semarang)', *Unimus*, pp. 2–11. Available at: http://download.portalgaruda.org/article.php?article=4495&val=426.

BAB 4
SECURITY MECHANISMS (COUNTERMEASURES)

Oleh Suwito Pomalingo

4.1 Pendahuluan

Di era digital saat ini, informasi telah menjadi aset yang sangat berharga bagi individu, perusahaan, dan pemerintah. Dalam konteks bisnis, informasi merupakan salah satu komponen kunci dalam menjalankan operasional, membuat keputusan strategis, dan menjaga keunggulan kompetitif. Namun, seiring dengan perkembangan teknologi informasi dan komunikasi, ancaman terhadap keamanan informasi juga semakin meningkat. Serangan siber, pencurian data, dan kebocoran informasi menjadi permasalahan yang serius dan mempengaruhi berbagai aspek kehidupan.

Untuk melindungi aset informasi dari ancaman yang ada, diperlukan strategi keamanan yang komprehensif dan efektif. Buku ini akan membahas berbagai aspek keamanan informasi dan bagaimana menerapkan mekanisme keamanan (*countermeasures*) yang tepat untuk melindungi aset informasi. Melalui pembahasan yang mendalam mengenai pengendalian akses, enkripsi, pencegahan serangan jaringan, proteksi perangkat, serta manajemen keamanan informasi dan kebijakan, buku ini bertujuan untuk memberikan pemahaman yang komprehensif mengenai keamanan informasi.

Diharapkan, dengan pengetahuan dan pemahaman yang didapat melalui buku ini, memudahkan dalam mengidentifikasi ancaman keamanan yang ada, menilai risiko yang dihadapi, dan mengimplementasikan *countermeasures* yang efektif untuk

melindungi aset informasi dan menjaga keberlanjutan operasional organisasi Anda.

4.2 Pengendalian Akses dan Otorisasi

Pengendalian Akses dan Otorisasi merupakan aspek penting dalam sistem keamanan informasi, yang bertujuan untuk mengontrol siapa yang dapat mengakses sumber daya informasi dan apa yang mereka dapat lakukan dengan sumber daya tersebut (Vimercati, Foresti and Samarati, 2008). Konsep pengendalian akses terdiri dari identifikasi, autentikasi, otorisasi, dan akuntabilitas. Identifikasi berkaitan dengan penentuan identitas pengguna, sedangkan autentikasi mengacu pada verifikasi identitas tersebut. Otorisasi mengatur hak akses yang diberikan kepada pengguna terhadap sumber daya, dan akuntabilitas melacak tindakan yang dilakukan oleh pengguna (Samarati and de Vimercati, 2001). Dalam sistem pengendalian akses, terdapat beberapa model yang telah dikembangkan, seperti model *Mandatory Access Control* (MAC), *Discretionary Access Control* (DAC), dan *Role-Based Access Control* (RBAC) (Ferraiolo *et al.*, 2001).

Implementasi pengendalian akses dan otorisasi pada sistem informasi sangat penting untuk menjaga kerahasiaan, integritas, dan ketersediaan data serta mencegah ancaman keamanan seperti serangan penolakan layanan (DoS), pencurian identitas, dan akses tidak sah (Wang and Lu, 2013). Beberapa teknologi yang digunakan dalam sistem pengendalian akses meliputi metode otentikasi berbasis kata sandi, sertifikat digital, dan teknologi biometrik (Jain, Ross and Prabhakar, 2004). Selain itu, pendekatan seperti pengendalian akses berbasis atribut (ABAC) dan pengendalian akses berbasis kebijakan (PBAC) telah diperkenalkan untuk menyediakan kontrol yang lebih fleksibel dan adaptif terhadap akses sumber daya (Hu *et al.*, 2014). Dalam konteks ini, peran manajemen kebijakan dan audit keamanan menjadi penting

untuk memastikan efektivitas dan kepatuhan dalam implementasi pengendalian akses dan otorisasi.

4.2.1 Metode Autentikasi

Metode autentikasi adalah proses yang digunakan untuk memverifikasi identitas pengguna atau sistem. Ini adalah bagian penting dari pengendalian akses dan otorisasi dalam sistem informasi.

Secara umum, ada lima metode autentikasi yang paling sering digunakan:

1. *Something you know*. Artinya adalah sesuatu yang diketahui oleh pengguna. Ini adalah jenis autentikasi yang paling umum dan melibatkan penggunaan kata sandi atau PIN. Pengguna harus menyediakan informasi ini untuk memverifikasi identitas mereka.
2. *Something you have*. Artinya adalah sesuatu yang dimiliki oleh pengguna. Metode ini membutuhkan pengguna untuk memiliki sesuatu seperti token keras, kartu akses, atau perangkat seluler yang dimiliki oleh pengguna. Token OTP (*One-Time Password*) dan aplikasi autentikasi seperti Google Authenticator adalah contoh metode ini.
3. *Something you are*. Metode ini mencakup biometrik, seperti sidik jari, pengenalan wajah, atau pengenalan suara. Teknologi ini menggunakan ciri-ciri unik pengguna untuk memverifikasi identitas mereka.
4. *Somewhere you are*. Metode ini akan memverifikasi identitas pengguna berdasarkan lokasi geografis mereka. Teknologi yang umum digunakan dalam metode autentikasi ini adalah GPS (*Global Positioning System*) dan IP (*Internet Protocol*) *address tracking*. Misalnya, sistem keamanan dapat membatasi akses ke sistem atau data tertentu kecuali pengguna berada dalam lokasi geografis tertentu, seperti dalam kampus, perusahaan, atau negara tertentu. Alternatif lainnya, sistem mungkin mengirimkan pemberitahuan atau meminta konfirmasi tambahan jika

pengguna mencoba mengakses sistem dari lokasi yang tidak biasa.

5. *Something you do*. Metode ini akan memverifikasi identitas pengguna berdasarkan pola perilaku atau aksi tertentu yang dilakukan pengguna. Ini bisa mencakup berbagai aktivitas, termasuk cara pengguna mengetik, cara mereka bergerak mouse, atau pola interaksi lainnya dengan sistem komputer. Misalnya, sistem keamanan mungkin menganalisis kecepatan dan ritme ketukan ketika pengguna mengetik kata sandi, atau menganalisis pola gerakan mouse saat pengguna berinteraksi dengan antarmuka pengguna. Sistem ini mempelajari pola perilaku ini dan menggunakannya untuk membangun profil pengguna yang dapat digunakan untuk memverifikasi identitas mereka di masa mendatang.

Setelah pengguna berhasil melewati proses autentikasi, sistem otorisasi akan menentukan hak dan batasan apa yang dimiliki pengguna tersebut. Otorisasi biasanya dikelola dengan menggunakan hak akses peran, di mana setiap peran memiliki hak akses tertentu dan pengguna diberi peran berdasarkan tugas dan tanggung jawab mereka. Mengenai hal ini akan dibahas pada bab selanjutnya.

Penerapan metode autentikasi yang tepat dan efektif dapat memberikan perlindungan yang kuat terhadap akses yang tidak sah, baik dari dalam maupun luar organisasi.

4.2.2 Pengelolaan Hak Akses Pengguna

Pengelolaan hak akses pengguna, atau yang lebih dikenal sebagai *User Access Control* (UAC), merupakan bagian vital dari keamanan informasi. Fungsinya adalah untuk membatasi akses ke sistem dan sumber daya dalam sebuah jaringan. Dengan cara ini, pengguna hanya bisa mengakses data atau fungsi yang relevan

dengan pekerjaannya, dan upaya-upaya serangan bisa diminimalisir.

Hak akses pengguna biasanya dikelola dengan sistem autentikasi dan otorisasi. Autentikasi adalah proses memverifikasi identitas pengguna, seperti yang telah diuraikan pada bab sebelumnya. Setelah autentikasi, sistem akan memverifikasi apakah pengguna memiliki hak akses ke sumber daya yang diminta (otorisasi).

Pada banyak sistem, hak akses dikelompokkan menjadi peran atau grup, seperti "karyawan", "manajer", atau "administrator". Pengguna dapat diberikan lebih dari satu peran, dan peran tersebut bisa diubah seiring waktu sesuai kebutuhan bisnis.

Pengelolaan hak akses pengguna juga melibatkan pemantauan dan audit. Pemantauan bertujuan untuk mendeteksi aktivitas mencurigakan atau penyalahgunaan hak akses, sementara audit digunakan untuk memeriksa dan memastikan bahwa sistem hak akses bekerja dengan baik dan sesuai dengan kebijakan perusahaan.

Dalam konteks keamanan informasi, salah satu kerangka kerja yang digunakan untuk pengelolaan hak akses pengguna adalah ISO/IEC 27001:2013, yang merupakan bagian dari serangkaian standar ISO 27000 yang menekankan pada manajemen keamanan informasi. Menurut standar ini, perusahaan harus menerapkan kebijakan pengendalian akses yang tepat, termasuk manajemen hak akses pengguna.

Selain itu, praktik terbaik dalam pengelolaan hak akses pengguna juga mencakup prinsip "hak akses minimal" dan "segregasi tugas". Prinsip hak akses minimal berarti bahwa setiap pengguna harus diberikan hak akses minimal yang diperlukan untuk melaksanakan tugasnya (Sandhu *et al.*, 1996). Ini bertujuan untuk mengurangi risiko kerusakan atau pencurian data jika akun pengguna dikompromikan.

Sementara itu, segregasi tugas berarti bahwa tugas kritis harus dibagi antara dua atau lebih individu, sehingga tidak ada satu individu yang memiliki kontrol penuh atas proses bisnis kritis. Misalnya, orang yang bertanggung jawab atas pembayaran di perusahaan tidak boleh juga memiliki akses ke rekonsiliasi bank. Ini mencegah penyalahgunaan hak akses dan mempromosikan transparansi dan akuntabilitas.

Pengelolaan hak akses pengguna harus dilakukan secara berkelanjutan dan diadaptasi seiring dengan perkembangan teknologi dan bisnis. Dalam konteks ini, teknologi seperti manajemen identitas dan akses (IAM) dan administrasi hak akses berbasis peran (RBAC) dapat membantu memfasilitasi dan otomatisasi proses ini (Benantar, 2006).

Namun, efektivitas pengelolaan hak akses pengguna sangat bergantung pada kebijakan, prosedur, dan teknologi yang diterapkan, serta kesadaran dan pelatihan pengguna tentang pentingnya keamanan informasi.

4.2.3 Kebijakan Pengendalian Akses yang Efektif

Kebijakan pengendalian akses merupakan komponen kunci dalam keamanan informasi. Kebijakan ini mendefinisikan siapa yang boleh mengakses sistem atau data, kapan mereka boleh mengaksesnya, dan apa yang mereka boleh lakukan terhadap data tersebut (Hu *et al.*, 2015). Kebijakan efektif dapat mencegah akses yang tidak sah dan penyalahgunaan data, serta mendukung kepatuhan terhadap peraturan dan standar keamanan.

Terdapat beberapa elemen penting dalam pembuatan kebijakan pengendalian akses yang efektif:

1. Identifikasi dan Autentikasi: Setiap pengguna harus memiliki identitas unik dan metode otentikasi yang aman, seperti kata sandi yang kuat atau autentikasi dua faktor.
2. Hak Akses: Setiap pengguna harus diberikan hak akses minimal yang diperlukan untuk melaksanakan tugasnya. Pengguna juga harus dikelompokkan ke dalam peran atau

grup berdasarkan tugas dan tanggung jawabnya (Sandhu *et al.*, 1996).

3. Manajemen dan Review: Hak akses pengguna harus ditinjau secara berkala untuk memastikan bahwa mereka tetap sesuai dengan peran dan tugas pengguna. Selain itu, ada mekanisme untuk menghapus atau mengubah hak akses ketika pengguna berhenti atau berubah posisi.
4. Pelatihan dan Kesadaran Keamanan: Pengguna harus diberi pelatihan tentang pentingnya kebijakan pengendalian akses dan bagaimana mematuhi kebijakan tersebut.
5. Pantauan dan Audit: Aktivitas akses harus dipantau dan diaudit untuk mendeteksi aktivitas mencurigakan atau penyalahgunaan hak akses.

Pada dasarnya, kebijakan pengendalian akses yang efektif harus selaras dengan tujuan bisnis dan hukum serta peraturan yang berlaku (ISO/IEC 27001:2013). Dalam mengimplementasikan kebijakan ini, dapat dipertimbangkan untuk menggunakan teknologi seperti sistem manajemen akses dan identitas (IAM), yang dapat membantu dalam otomatisasi dan penegakan kebijakan.

Implementasi kebijakan pengendalian akses yang efektif bukan hanya soal teknologi, tetapi juga melibatkan manusia dan proses. Berikut ini adalah beberapa pertimbangan tambahan:

1. Keterlibatan *Stakeholder*: Semua pihak yang berkepentingan, termasuk manajemen, IT, HR, dan pengguna, harus terlibat dalam proses pembuatan dan implementasi kebijakan pengendalian akses. Mereka memiliki wawasan berharga tentang apa yang dibutuhkan dan apa yang dapat diterima dari sudut pandang operasional dan manajemen risiko (Pfleeger, 2002).
2. *Balancing Security and Usability*: Harus ada keseimbangan antara keamanan dan kemudahan penggunaan. Jika sistem terlalu sulit untuk digunakan atau membatasi produktivitas,

pengguna mungkin mencari cara untuk menghindarinya, yang pada gilirannya dapat merusak keamanan (Sasse, Brostoff and Weirich, 2001).
3. Adaptasi dan Pembaruan: Kebijakan pengendalian akses harus dinamis dan mampu beradaptasi dengan perubahan lingkungan, termasuk perubahan teknologi, hukum, dan peraturan, serta perubahan dalam struktur dan tujuan organisasi (Anderson, 2020).
4. Pengujian dan Evaluasi: Kebijakan pengendalian akses dan sistem pendukungnya harus diuji dan dievaluasi secara rutin untuk memastikan bahwa mereka masih efektif dan sesuai dengan kebutuhan bisnis dan hukum.

Dengan mempertimbangkan semua elemen ini, organisasi dapat mengembangkan dan menerapkan kebijakan pengendalian akses yang efektif dan holistik yang membantu melindungi aset-aset informasi mereka sambil mendukung operasi dan tujuan bisnis mereka.

4.3 Enkripsi dan Kriptografi

Enkripsi dan kriptografi adalah dua konsep kunci dalam keamanan informasi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan dan integritas informasi, sedangkan enkripsi adalah teknik kriptografi yang digunakan untuk merahasiakan informasi (Stallings and Brown, 2018).

4.3.1 Konsep Dasar Kriptografi

Kriptografi adalah cabang ilmu yang mempelajari teknik-teknik matematis dalam konteks keamanan informasi seperti kerahasiaan, integritas data, autentikasi, dan non-repudiation. Istilah "kriptografi" berasal dari kata Yunani "kryptos" yang berarti "tersembunyi", dan "graphein" yang berarti "menulis".

Beberapa konsep yang perlu dipahami dalam kriptografi seperti :

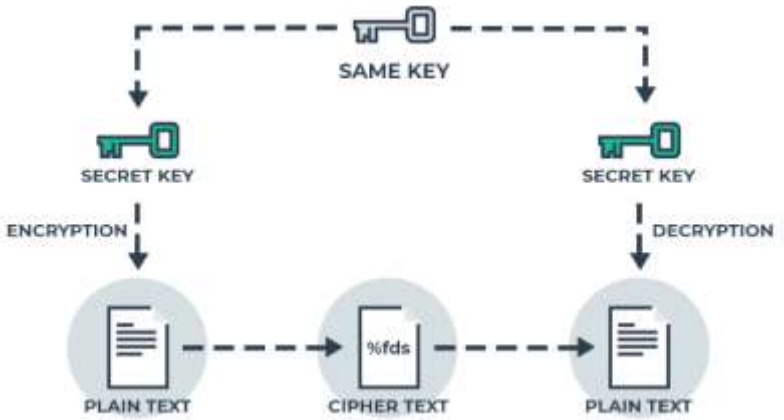
1. *Plaintext dan Ciphertext*
   Plaintext adalah informasi atau data asli yang perlu dilindungi. Sedangkan c*iphertext* adalah hasil dari proses enkripsi yang mengubah plaintext menjadi bentuk yang tidak dapat dimengerti atau dibaca tanpa pengetahuan kunci yang tepat.
2. Kunci Kriptografi
   Kunci kriptografi adalah sejumlah data yang digunakan oleh algoritma kriptografi untuk mengubah plaintext menjadi ciphertext dan sebaliknya. Dalam konteks enkripsi simetris, kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Sedangkan dalam enkripsi asimetris, digunakan dua kunci yang berbeda, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi.
3. Algoritma Kriptografi: Algoritma kriptografi adalah serangkaian instruksi matematis yang digunakan untuk proses enkripsi dan dekripsi. Algoritma kriptografi yang populer meliputi AES (*Advanced Encryption Standard*) untuk enkripsi simetris dan RSA (*Rivest-Shamir-Adleman*) untuk enkripsi asimetris (Schneier, 2015).
4. Fungsi Hash Kriptografi
   Fungsi hash kriptografi adalah proses yang mengambil input (atau 'pesan') dan mengembalikan nilai hash tetap yang unik. Fungsi ini digunakan dalam berbagai aspek keamanan informasi, termasuk autentikasi, integritas data, dan penandaan waktu digital. Contoh fungsi hash kriptografi yang populer meliputi SHA-256 dan MD5.

Konsep-konsep dasar ini membentuk pondasi dari banyak mekanisme keamanan dalam teknologi informasi, dan memahaminya adalah langkah awal yang penting dalam memahami bagaimana melindungi informasi dalam dunia digital.

4.3.2 Algoritma Enkripsi Simetris dan Asimetris

Algoritma enkripsi simetris dan asimetris merupakan dua jenis utama algoritma kriptografi yang digunakan dalam keamanan informasi.

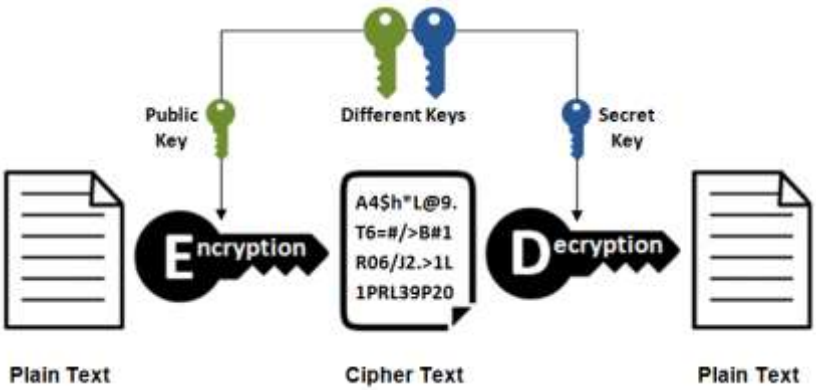
Pada algoritma enkripsi simetris, kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Ini berarti bahwa pihak yang berkomunikasi harus saling bertukar kunci secara aman sebelum mereka dapat mulai berkomunikasi. Algoritma enkripsi simetris biasanya cepat dan efisien dalam hal penggunaan komputasi, yang membuatnya ideal untuk enkripsi data dalam jumlah besar, namun kurang aman karena kuncinya harus dibagi. Contoh algoritma enkripsi simetris termasuk *Advanced Encryption Standard* (AES), *Data Encryption Standard* (DES), dan *Triple DES* (3DES).



Gambar 4.1. Enkripsi Simetris
(Sumber : www.nesabamedia.com)

Sedangkan dalam algoritma enkripsi asimetris, dua kunci yang berbeda digunakan, satu untuk enkripsi (kunci publik) dan satu untuk dekripsi (kunci privat). Kunci publik dapat dibagikan secara bebas dan digunakan oleh siapa pun untuk mengenkripsi pesan, tetapi hanya kunci privat yang dapat digunakan untuk

dekripsi. Ini memungkinkan komunikasi yang aman tanpa perlu pertukaran kunci yang aman sebelumnya. Algoritma enkripsi asimetris cenderung lebih lambat dan membutuhkan lebih banyak sumber daya komputasi daripada algoritma simetris, tetapi mereka memberikan tingkat keamanan dan fleksibilitas yang lebih tinggi. Contoh algoritma enkripsi asimetris termasuk RSA (*Rivest-Shamir-Adleman*), *Diffie-Hellman*, dan *Elliptic Curve Cryptography* (ECC).



Gambar 4.2. Enkripsi Asimetris
(Sumber : www.websiterating.com)

4.3.3 Teknik-teknik Enkripsi yang Umum Digunakan

Terdapat banyak teknik enkripsi yang digunakan secara luas dalam berbagai bidang teknologi informasi untuk melindungi kerahasiaan dan integritas data. Berikut ini adalah beberapa contoh teknik enkripsi yang paling umum digunakan:

1. *Advanced Encryption Standard* (AES). AES adalah standar enkripsi yang ditetapkan oleh *National Institute of Standards and Technology* (NIST) dari Amerika Serikat. AES adalah algoritma enkripsi blok yang menggunakan kunci dengan panjang 128, 192, atau 256 bit. Algoritma ini digunakan secara luas dalam berbagai aplikasi, mulai dari

enkripsi file dan disk hingga pengamanan komunikasi nirkabel dan internet.

2. *Data Encryption Standard* (DES) dan *Triple DES* (3DES). DES adalah algoritma enkripsi blok yang awalnya ditetapkan sebagai standar oleh pemerintah Amerika Serikat pada tahun 1977. DES menggunakan kunci 56 bit, yang kemudian dianggap tidak aman melawan serangan brute-force. 3DES, yang menggunakan tiga ronde DES dan kunci 168 bit, dikembangkan sebagai alternatif yang lebih aman.
3. *Rivest-Shamir-Adleman* (RSA). RSA adalah algoritma enkripsi asimetris yang digunakan secara luas untuk enkripsi dan tanda tangan digital. RSA menggunakan dua kunci: satu kunci publik untuk enkripsi dan satu kunci privat untuk dekripsi. Keamanan RSA berdasarkan pada kesulitan faktorisasi bilangan bulat besar.
4. *Diffie-Hellman*. Diffie-Hellman adalah metode kunci publik yang digunakan untuk pertukaran kunci secara aman melalui jaringan yang tidak aman. Metode ini sering digunakan dalam protokol keamanan seperti Secure Sockets Layer (SSL) dan Transport Layer Security (TLS) untuk membentuk kunci simetris yang kemudian digunakan untuk enkripsi data.
5. *Elliptic Curve Cryptography* (ECC): ECC adalah pendekatan terhadap kriptografi kunci publik yang berdasarkan pada struktur aljabar dari kurva eliptik. ECC menawarkan tingkat keamanan yang sama dengan RSA dengan kunci yang lebih pendek, yang berarti bahwa mereka lebih efisien dari segi komputasi.

4.4 Pencegahan Serangan Jaringan

Dalam era digital saat ini, serangan jaringan menjadi ancaman yang semakin nyata bagi organisasi dan individu di seluruh dunia. Dari serangan *ransomware* hingga *phishing*, dan

serangan *Denial of Service* (DoS), berbagai jenis serangan jaringan dapat mengekspos data sensitif, merusak sistem, dan menyebabkan gangguan operasional yang signifikan. Oleh karena itu, penting untuk memahami dan menerapkan mekanisme untuk mencegah serangan jaringan.

Pencegahan serangan jaringan melibatkan rangkaian strategi dan teknologi yang dirancang untuk melindungi integritas dan kerahasiaan informasi dalam jaringan. Tujuannya adalah untuk mendeteksi dan menghentikan serangan sebelum mereka dapat merusak sistem atau mencuri data. Teknik pencegahan serangan jaringan dapat berkisar dari *firewall* dan *Sistem Pencegahan Intrusi* (IPS), hingga pemindaian dan penyadapan jaringan, autentikasi dan otorisasi pengguna, serta penggunaan protokol keamanan seperti HTTPS.

Meski pencegahan serangan jaringan penting, perlu dipahami bahwa tidak ada sistem yang sepenuhnya aman. Oleh karena itu, pendekatan yang baik dalam keamanan jaringan adalah dengan menerapkan lapisan keamanan yang berbeda, yang sering disebut sebagai "pertahanan dalam kedalaman". Pendekatan ini melibatkan penggunaan berbagai teknik dan teknologi keamanan yang saling melengkapi, untuk memastikan bahwa jika satu lapisan keamanan gagal, lapisan lainnya akan tetap melindungi sistem dan data.

4.4.1 Firewall

Firewall adalah komponen penting dalam arsitektur keamanan jaringan. *Firewall* berfungsi sebagai barikade atau filter antara jaringan internal yang dapat dipercaya (seperti jaringan korporat atau rumah) dan jaringan eksternal yang tidak dapat dipercaya (seperti internet). Firewall sendiri dapat diklasifikasikan berdasarkan metode yang mereka gunakan untuk memfilter lalu lintas dan tempat mereka ditempatkan dalam jaringan.

Berdasarkan metode yang digunakan, firewall dibagi menjadi:

1. *Packet Firewall*. Firewall jenis ini bekerja pada lapisan jaringan dari model OSI dan mengontrol akses berdasarkan

alamat IP, port, dan protokol. Ia memeriksa setiap paket yang melewati firewall dan memutuskan apakah harus diteruskan atau diblokir berdasarkan aturan yang telah ditentukan (Chapman, 1992).

2. *Stateful Firewall. Firewall* jenis ini adalah firewall yang tidak hanya memeriksa paket data satu per satu, tetapi juga menjaga rekaman atau "state" dari koneksi jaringan yang sedang berlangsung. Informasi ini mencakup detail seperti alamat IP dan port yang terlibat dalam koneksi, nomor urutan paket, dan lainnya. Dengan informasi ini, statefull firewall bisa mengenali dan memfilter paket yang merupakan bagian dari koneksi yang sudah ada, serta memblokir paket yang mencoba memulai koneksi baru tanpa izin yang tepat. Selain itu, statefull firewall memberikan tingkat keamanan yang lebih tinggi dibandingkan *stateless firewall*, yang hanya memeriksa paket data satu per satu tanpa mempertimbangkan konteks koneksi jaringan yang lebih luas. Dengan melacak state dari koneksi jaringan, *statefull firewall* bisa lebih efektif dalam mencegah serangan yang mencoba untuk mengeksploitasi koneksi yang sah.
3. *Application Firewall*. Bekerja pada lapisan aplikasi, firewall jenis ini memeriksa isi dari setiap paket data dan dapat memblokir lalu lintas berdasarkan konten paket tersebut, seperti tipe file, komando, atau fungsi yang digunakan dalam aplikasi tertentu (Zwicky, Cooper and Chapman, 2000).

Sedangkan berdasarkan penempatannya, firewall ini dibagi menjadi:

1. *Network Firewall*. Ditempatkan pada batas antara jaringan internal dan eksternal, firewall ini melindungi seluruh jaringan dari serangan yang datang dari luar.

2. *Host Firewall*. Dijalankan pada mesin individual dan melindungi host tersebut dari serangan baik dari jaringan internal maupun eksternal. Biasanya digunakan pada server atau pada komputer pribadi sebagai lapisan pertahanan tambahan.

Pada praktiknya, banyak organisasi menggunakan kombinasi dari berbagai jenis *firewall* untuk mencapai tingkat keamanan yang optimal. Penting untuk mencatat bahwa sementara firewall adalah alat yang sangat efektif dalam melindungi jaringan, mereka bukanlah solusi keamanan yang lengkap dan harus digunakan sebagai bagian dari strategi pertahanan dalam kedalaman.

Firewall diatur menggunakan sekumpulan aturan, atau "*rules*", yang menentukan lalu lintas apa yang diperbolehkan atau diblokir. Aturan-aturan ini biasanya didasarkan pada parameter seperti alamat IP, port, dan protokol. Berikut adalah beberapa contoh aturan *firewall*:

1. Memblokir lalu lintas dari IP tertentu.
   Jika mengetahui alamat IP tertentu yang mencoba melakukan serangan atau aktivitas mencurigakan, kita dapat membuat aturan untuk memblokir semua lalu lintas dari alamat IP tersebut. Contoh aturan bisa seperti ini: "DENY FROM IP 192.168.1.100".
2. Membatasi akses ke port tertentu.
   Kita bisa membuat aturan untuk membatasi akses ke port tertentu untuk mencegah akses tidak sah. Misalnya, kita bisa membuat aturan yang mengizinkan hanya alamat IP tertentu untuk mengakses port 22 (SSH): "ALLOW TCP FROM IP 192.168.1.1 TO ANY PORT 22".
3. Memblokir protokol tertentu.
   Kita bisa membuat aturan untuk memblokir protokol tertentu jika tidak dibutuhkan atau berisiko. Misalnya, membuat aturan untuk memblokir semua lalu lintas ICMP

untuk mencegah *ping attack*: "DENY ICMP FROM ANY TO ANY".

4. Membatasi akses ke situs web tertentu.
   Dalam organisasi atau lingkungan kerja, sering kali diperlukan aturan untuk memblokir akses ke situs web tertentu. Misalnya, kita bisa membuat aturan untuk memblokir akses ke situs web media sosial selama jam kerja: "DENY TCP FROM ANY TO www.facebook.com".

Berikut adalah contoh sederhana dari sebuah tabel aturan *firewall*. Tabel ini menunjukkan aturan yang bisa diterapkan dalam sebuah firewall untuk mengendalikan lalu lintas jaringan berdasarkan protokol, alamat IP sumber, alamat IP tujuan, port sumber, dan port tujuan.

Tabel 4.1. Tabel aturan firewall

NO	Protocol	Alamat IP Sumber	Port Sumber	Alamat IP Tujuan	Port Tujuan	Aksi
1	TCP	Any	Any	192.168.1.1	22	Allow
2	TCP	Any	Any	192.168.1.2	80	Allow
3	UDP	Any	Any	192.168.1.2	53	Allow
4	TCP	192.168.1.100	Any	Any	Any	Deny
5	ICMP	Any	Any	Any	Any	Deny

Pada Tabel 4.1, aksi "*Allow*" berarti *firewall* akan membiarkan lalu lintas jaringan yang memenuhi kriteria tersebut melewati firewall. Aksi "Deny" berarti firewall akan memblokir lalu lintas jaringan yang memenuhi kriteria tersebut.

Penting untuk diingat bahwa aturan *firewall* harus ditulis dengan urutan yang benar. Firewall akan memeriksa aturan dari atas ke bawah dan menerapkan aksi dari aturan pertama yang cocok. Oleh karena itu, aturan yang lebih spesifik biasanya diletakkan di atas aturan yang lebih umum. Selain itu, aturan *firewall* juga harus dirancang dengan hati-hati, karena aturan yang

terlalu ketat bisa menghambat produktivitas dan akses ke layanan yang sah, sementara aturan yang terlalu longgar mungkin tidak memberikan perlindungan yang cukup. Oleh karena itu, penting untuk menyeimbangkan kebutuhan keamanan dengan kebutuhan operasional dan bisnis.

4.4.2 Sistem Deteksi Intrusi (IDS)

Sistem Deteksi Intrusi atau *Intrusion Detecting System* (IDS) adalah alat yang sangat penting dalam keamanan siber. IDS berfungsi untuk memantau lalu lintas jaringan dan sistem untuk mengidentifikasi aktivitas mencurigakan atau tidak biasa yang dapat menunjukkan adanya upaya intrusi atau serangan (Scarfone and Mell, 2007).

Ada dua jenis utama IDS, yaitu:

1. *Network IDS* atau IDS berbasis jaringan (NIDS)
   NIDS memantau lalu lintas jaringan dalam suatu jaringan atau sub-jaringan. NIDS memeriksa paket-paket yang berlalu lintas dalam jaringan dan mencari tanda-tanda serangan berdasarkan database dari tanda-tanda serangan yang diketahui (signature) atau melalui pendekatan berbasis anomali, di mana NIDS mencari perilaku jaringan yang tidak normal.
2. *Host IDS* atau IDS berbasis host (HIDS)
   HIDS diinstal pada sistem atau perangkat tertentu dan memantau log sistem, file, dan aktivitas pengguna pada host tersebut. HIDS bisa mendeteksi serangan yang mungkin tidak terlihat oleh NIDS, seperti serangan yang terjadi di dalam sistem host itu sendiri..

IDS dapat memberikan peringatan dini tentang upaya intrusi, memungkinkan tim keamanan siber untuk merespons dan meminimalkan kerusakan yang mungkin terjadi. Namun, mereka juga dapat menghasilkan apa yang disebut "*false positive*," di mana aktivitas yang sah disalahartikan sebagai serangan, atau "*false*

negative," di mana serangan tidak terdeteksi. IDS juga cenderung pasif, yang berarti mereka mendeteksi dan memberikan peringatan tentang intrusi tetapi biasanya tidak mengambil tindakan langsung untuk menghentikan serangan.

Berikut ini adalah cara kerja IDS:

1. Pemantauan dan Analisis: IDS berfungsi dengan memantau lalu lintas jaringan dan menganalisis informasi yang masuk dan keluar dari sistem. Hal ini dilakukan untuk mendeteksi tanda-tanda aktivitas mencurigakan atau tidak wajar.
2. Penggunaan Signature atau Pola: IDS menggunakan database yang berisi pola atau "tanda tangan" dari berbagai jenis serangan yang telah diketahui sebelumnya. Jika IDS menemukan lalu lintas jaringan atau perilaku yang sesuai dengan salah satu pola ini, sistem akan menganggap itu sebagai aktivitas mencurigakan.
3. Deteksi Anomali: Beberapa IDS juga dapat belajar tentang apa yang dianggap sebagai "normal" untuk jaringan atau sistem dan kemudian mendeteksi aktivitas yang melenceng dari norma ini, yang dikenal sebagai deteksi anomali.
4. Alarm dan Tindakan: Jika IDS mendeteksi aktivitas yang mencurigakan atau tidak wajar, sistem akan mengeluarkan peringatan atau alarm. Beberapa IDS juga dapat melakukan tindakan untuk menghentikan atau mengurangi potensi kerusakan, seperti memblokir lalu lintas jaringan dari alamat IP tertentu.
5. Laporan dan Log: IDS juga mencatat informasi tentang potensi serangan, termasuk detail tentang apa yang terdeteksi dan kapan itu terjadi. Laporan ini dapat digunakan untuk analisis lebih lanjut dan untuk membantu dalam peningkatan keamanan.

Snort adalah salah satu sistem deteksi dan pencegahan intrusi (IDS/IPS) yang paling populer. Snort bekerja dengan

menggunakan aturan atau "rules" untuk memantau lalu lintas jaringan dan mendeteksi aktivitas mencurigakan.

Aturan dalam Snort biasanya terdiri dari header dan *body* aturan. Header aturan mencakup detail seperti tindakan yang harus diambil (misalnya, "alert" atau "log"), alamat IP dan port sumber dan tujuan, dan protokol yang digunakan (misalnya, TCP, UDP, ICMP, dan sebagainya). Sementara *body* aturan biasanya berisi konten yang harus dicocokkan, serta berbagai informasi lainnya.

Berikut adalah contoh sederhana dari sebuah aturan Snort:
alert tcp any any -> 192.168.1.1 80 (content:"GET /index.html"; msg:"Attempted access to /index.html";)
Mari kita analisis aturan di atas:

1. alert: Ini adalah tindakan yang akan diambil oleh Snort jika aturan ini dicocokkan. Dalam hal ini, Snort akan mengirimkan peringatan.
2. tcp: Ini adalah protokol jaringan yang akan dipantau oleh aturan ini.
3. any any: Ini adalah alamat IP dan port sumber dari lalu lintas jaringan. "Any any" berarti aturan ini akan berlaku untuk lalu lintas dari alamat IP dan port apa pun.
4. -> 192.168.1.1 80: Ini adalah alamat IP dan port tujuan dari lalu lintas jaringan. Dalam hal ini, aturan ini akan berlaku untuk lalu lintas yang ditujukan ke alamat IP 192.168.1.1 pada port 80.
5. content:"GET /index.html": Ini adalah pola yang harus dicocokkan dalam lalu lintas jaringan. Dalam hal ini, aturan ini akan mencocokkan setiap paket yang berisi "GET /index.html".
6. msg:"Attempted access to /index.html": Ini adalah pesan yang akan ditampilkan oleh Snort jika aturan ini dicocokkan.

Aturan Snort bisa menjadi sangat kompleks dan dapat mencakup berbagai macam opsi dan pola pencocokan, tergantung

pada apa yang Anda coba deteksi. Namun, contoh di atas hanya memberikan gambaran dasar tentang bagaimana aturan Snort bekerja.

Meskipun demikian, IDS adalah komponen penting dari strategi pertahanan dalam kedalaman dan dapat memberikan lapisan perlindungan tambahan ketika digunakan bersamaan dengan mekanisme keamanan lainnya, seperti firewall dan sistem pencegahan intrusi (IPS).

4.4.3 Sistem Pencegahan Intrusi (IPS)

Jika IDS hanya berfungsi mendeteksi adanya ancaman atau serangan dalam jaringan komputer, maka IPS atau Sistem Pencegahan Intrusi bertugas untuk memblokir serangan yang ada. Sistem Pencegahan Intrusi atau *Intrusion Prevention System* (IPS) merupakan suatu teknologi keamanan yang memantau jaringan dan sistem untuk aktivitas berbahaya atau tidak wajar. Tugas utama dari IPS adalah mengidentifikasi ancaman potensial, mencatat informasi tentang ancaman tersebut, melaporkannya, dan kemudian mencoba mencegah atau memblokir serangan tersebut. Sistem semacam ini berfungsi sebagai barisan pertahanan penting dalam lingkungan jaringan dan sistem informasi.

Ada beberapa jenis utama dari IPS, masing-masing dirancang untuk melindungi aspek tertentu dari sistem atau jaringan:

1. *Network-based Intrusion Prevention System* (NIPS): NIPS memantau seluruh jaringan untuk aktivitas mencurigakan. NIPS umumnya dipasang di titik strategis dalam jaringan, seperti di depan gateway internet, untuk memantau lalu lintas yang masuk dan keluar dari jaringan tersebut.
2. *Wireless Intrusion Prevention System* (WIPS): WIPS dirancang khusus untuk memantau dan melindungi jaringan nirkabel dari ancaman seperti akses tidak sah atau serangan denial of service.

3. Host-based Intrusion Prevention System (HIPS): HIPS diinstal di perangkat individu dan melindunginya dari ancaman internal dan eksternal. HIPS bisa melindungi dari ancaman seperti virus, trojan, dan serangan lainnya yang ditujukan langsung ke host.

IDS dan IPS satu paket, sehingga cara kerjanya sangat mirip yakni bekerja dengan mendeteksi serangan berbasis signature dan deteksi berbasis perilaku (anomali). Namun, setelah serangan terdeteksi, IPS biasanya akan melakukan tindakan seperti memblokir lalu lintas yang mencurigakan atau merusak dari sumber tertentu, mencatat detil tentang insiden keamanan, seperti sumber serangan, jenis serangan, waktu serangan, dan lainnya. Informasi ini penting untuk analisis insiden dan forensik digital. Dan terakhir IPS akan mengirimkan laporan insiden kepada administrator atau sistem manajemen keamanan.

4.4.4 Manajemen Risiko Jaringan

Manajemen risiko jaringan adalah proses sistematis identifikasi, analisis, evaluasi, penanganan, pemantauan, dan peninjauan risiko yang terkait dengan infrastruktur jaringan. Proses ini dimaksudkan untuk meminimalkan dampak negatif terhadap operasional, keandalan, dan keamanan jaringan.

Tujuan dari manajemen risiko jaringan adalah untuk mencapai dan mempertahankan tingkat risiko yang dapat diterima, sambil memastikan bahwa jaringan tetap berfungsi dengan efisien dan efektif. Ini melibatkan keseimbangan antara biaya mitigasi risiko dan dampak potensial dari risiko tersebut. Manajemen risiko jaringan harus menjadi bagian integral dari praktek keamanan jaringan suatu organisasi.

Berikut adalah langkah-langkah umum dalam manajemen risiko jaringan:

1. Identifikasi Risiko: Langkah pertama dalam manajemen risiko adalah identifikasi risiko. Ini melibatkan pengenalan

dan dokumen ancaman dan kerentanan yang mungkin mempengaruhi jaringan.
2. Analisis Risiko: Setelah risiko diidentifikasi, mereka harus dianalisis untuk memahami dampak dan kemungkinan terjadinya. Analisis ini biasanya mencakup penilaian kerentanan dan dampak potensial terhadap jaringan jika risiko terjadi.
3. Evaluasi Risiko: Setelah analisis, risiko dievaluasi berdasarkan prioritas. Ini biasanya melibatkan peringkat risiko berdasarkan tingkat dampak dan kemungkinan.
4. Penanganan Risiko: Setelah risiko dievaluasi, tindakan harus diambil untuk mengelola risiko. Ini dapat berupa penerimaan risiko, penghindaran risiko, mitigasi risiko, atau transfer risiko.
5. Pemantauan dan Peninjauan: Manajemen risiko adalah proses berkelanjutan. Risiko perlu dipantau dan ditinjau secara teratur untuk memastikan bahwa tindakan mitigasi efektif dan bahwa risiko baru diidentifikasi dan dikelola tepat waktu.

Manajemen risiko jaringan tidak hanya berfokus pada aspek teknis, tetapi juga mencakup tindakan organisasional dan operasional. Untuk mendapatkan hasil terbaik dari proses manajemen risiko, organisasi perlu menciptakan budaya keamanan di mana setiap anggota organisasi memahami pentingnya keamanan jaringan dan bagaimana mereka dapat berkontribusi.

Beberapa poin penting lainnya dalam manajemen risiko jaringan termasuk:

1. Kebijakan dan Prosedur: Kebijakan dan prosedur yang jelas dan efektif adalah fondasi dari manajemen risiko jaringan yang baik. Ini harus mencakup kebijakan akses, penggunaan, dan manajemen jaringan.

2. Pelatihan dan Kesadaran: Memberikan pelatihan dan meningkatkan kesadaran tentang keamanan jaringan di seluruh organisasi adalah bagian penting dari manajemen risiko jaringan. Semua anggota organisasi harus memahami peran mereka dalam menjaga keamanan jaringan.
3. Pemantauan dan Pengecekan: Manajemen risiko jaringan membutuhkan pemantauan dan pengecekan yang konstan untuk memastikan bahwa risiko dikelola dengan efektif dan bahwa sistem dan proses tetap aman.
4. Pembaruan dan Pemeliharaan: Jaringan dan sistem yang terkait harus selalu diperbarui dan dipelihara dengan baik untuk memastikan bahwa mereka memiliki perlindungan terbaru terhadap ancaman dan risiko.
5. Pemulihan Bencana dan Rencana Kontinuitas Bisnis: Setiap organisasi harus memiliki rencana pemulihan bencana dan rencana kontinuitas bisnis yang akan memungkinkan mereka untuk pulih dengan cepat dan efisien setelah kejadian yang merugikan.

Manajemen risiko jaringan adalah proses berkelanjutan yang membutuhkan komitmen dari seluruh organisasi. Dengan pendekatan proaktif terhadap manajemen risiko, organisasi dapat secara efektif melindungi jaringan dan aset penting mereka dari berbagai ancaman keamanan.

4.5 Proteksi Perangkat dan Infrastruktur

4.5.1 Keamanan Perangkat Keras

Keamanan perangkat keras menjadi salah satu komponen penting dalam sistem keamanan teknologi informasi suatu organisasi. Perangkat keras seperti server, komputer, perangkat penyimpanan, router, dan switch merupakan bagian vital yang menunjang operasional sehari-hari. Tanpa perlindungan yang tepat, perangkat keras ini bisa menjadi target serangan yang dapat

menghancurkan data, merusak sistem, atau bahkan mengekspos informasi penting.

Perangkat keras dapat diserang dengan berbagai cara. Salah satu ancaman adalah perangkat keras fisik yang rusak, baik karena kelalaian, bencana alam, atau tindakan sengaja seperti sabotase. Selain itu, perangkat keras juga bisa diserang secara digital, misalnya melalui malware, yang bisa merusak sistem operasi, menghapus data, atau memberikan akses tidak sah kepada pihak yang tidak berhak. Serangan seperti ransomware bisa membuat data pada perangkat keras menjadi terenkripsi dan tidak dapat diakses kecuali tebusan dibayar.

Untuk melindungi perangkat keras, langkah pertama adalah menjaga keamanan fisik. Ini bisa melibatkan penggunaan kunci, sistem alarm, atau bahkan ruangan khusus yang aman untuk menyimpan perangkat keras penting. Selain itu, memastikan bahwa perangkat keras selalu diperbarui dengan patch keamanan terbaru juga sangat penting untuk melindungi dari serangan digital. Software antivirus dan firewall juga bisa membantu melindungi perangkat keras dari serangan malware dan usaha akses tidak sah.
Keamanan perangkat keras tidak hanya penting untuk melindungi data dan informasi penting, tetapi juga untuk menjaga operasional organisasi. Kegagalan dalam sistem bisa mengakibatkan kerugian waktu, uang, dan sumber daya. Oleh karena itu, investasi dalam keamanan perangkat keras adalah investasi dalam keberlangsungan dan efisiensi organisasi. Menggabungkan strategi keamanan fisik dan digital, sambil mempertahankan pembaruan dan pemantauan berkelanjutan, adalah pendekatan terbaik untuk keamanan perangkat keras.

4.5.2 Keamanan Perangkat Lunak

Perangkat lunak atau software adalah komponen inti dalam hampir semua sistem teknologi informasi. Mulai dari sistem operasi, aplikasi bisnis, hingga perangkat lunak keamanan itu sendiri, semua memiliki peran penting dalam operasional sehari-

hari. Keamanan perangkat lunak menjadi aspek krusial karena perangkat lunak yang tidak aman dapat menjadi titik masuk bagi pelaku serangan untuk merusak sistem atau mencuri data.

Ancaman terhadap perangkat lunak dapat berasal dari berbagai sumber. Virus dan malware bisa merusak perangkat lunak, mencuri data, atau memberikan akses kepada pihak yang tidak berhak. Selain itu, perangkat lunak yang memiliki celah keamanan bisa dieksploitasi oleh hacker untuk melakukan serangan. Misalnya, serangan 'zero-day' biasanya menargetkan celah keamanan yang belum dikenal oleh pembuat perangkat lunak.

Perlindungan perangkat lunak melibatkan beberapa strategi. Pertama, selalu memperbarui perangkat lunak. Pembuat perangkat lunak sering merilis pembaruan atau patch untuk memperbaiki celah keamanan. Oleh karena itu, menjaga perangkat lunak tetap diperbarui adalah salah satu cara terbaik untuk melindunginya. Kedua, menggunakan perangkat lunak keamanan seperti antivirus dan firewall. Ini dapat mendeteksi dan mencegah ancaman seperti virus dan malware.

Pada level pengguna, penting untuk mengikuti praktek keamanan perangkat lunak yang baik. Ini termasuk tidak mengunduh atau menginstal perangkat lunak dari sumber yang tidak dikenal atau tidak dapat dipercaya, tidak membuka lampiran email yang mencurigakan, dan menggunakan kata sandi yang kuat dan unik untuk setiap akun. Selain itu, penggunaan teknologi seperti otentikasi dua faktor dapat memberikan lapisan tambahan perlindungan.

Ancaman selalu berkembang dan menjadi semakin canggih, jadi perlu untuk selalu memantau perkembangan di bidang keamanan perangkat lunak dan mengambil tindakan proaktif untuk melindungi sistem dan data. Keamanan perangkat lunak bukan hanya tanggung jawab IT saja, tetapi semua pengguna perangkat lunak harus memiliki pemahaman dasar tentang cara menjaga perangkat lunak mereka tetap aman.

4.5.3 Patch Management

Manajemen patch adalah proses memperbarui sistem dan aplikasi dengan perbaikan-perbaikan keamanan atau peningkatan fungsionalitas yang dikeluarkan oleh pembuat perangkat lunak. Patch adalah bagian kode yang diterapkan ke dalam perangkat lunak yang ada untuk memperbaiki celah keamanan, memperbaiki bug, atau meningkatkan kinerja. Proses ini sangat penting untuk menjaga keamanan dan efisiensi sistem teknologi informasi.

Manajemen patch sangat penting dalam menjaga keamanan sistem dan jaringan. Banyak serangan siber memanfaatkan kerentanan dalam perangkat lunak yang belum diperbarui. Dengan menerapkan patch keamanan secara tepat waktu, organisasi dapat melindungi sistem mereka dari serangan tersebut. Selain itu, patch juga dapat memperbaiki bug dan meningkatkan kinerja sistem, yang bisa meningkatkan produktivitas dan efisiensi.

Meskipun penting, manajemen patch bisa menjadi proses yang kompleks dan memakan waktu. Hal ini memerlukan penilaian terhadap patch yang tersedia, memastikan kompatibilitas patch dengan sistem yang ada, menerapkan patch, dan kemudian memantau sistem untuk memastikan bahwa patch tidak menyebabkan masalah lain. Dalam lingkungan yang besar atau sangat kompleks, proses ini bisa menjadi sangat membebani.

Untuk melakukan manajemen patch dengan efektif, organisasi biasanya perlu mengimplementasikan kebijakan dan prosedur manajemen patch. Ini harus mencakup penjadwalan reguler untuk pengecekan dan penerapan patch, proses untuk menilai dan menguji patch sebelum penerapan, dan prosedur pemulihan jika patch menyebabkan masalah. Menggunakan perangkat lunak manajemen patch dapat membantu otomatisasi banyak dari tugas ini dan membuat proses menjadi lebih mudah dikelola.

4.5.4 Kebijakan Keamanan Fisik

Kebijakan keamanan fisik adalah seperangkat aturan dan prosedur yang dirancang untuk melindungi aset fisik organisasi, seperti gedung, perangkat keras, dan data. Ini mencakup tindakan yang dirancang untuk mencegah akses tidak sah, kerusakan, pencurian, atau kehilangan. Keamanan fisik sering dianggap sama pentingnya dengan keamanan digital, karena kedua aspek ini saling melengkapi dalam menjaga keamanan keseluruhan organisasi.

Kebijakan keamanan fisik umumnya mencakup berbagai komponen, termasuk kontrol akses fisik, seperti kunci, kartu akses, dan sistem pengawasan. Ini juga dapat mencakup kebijakan tentang bagaimana perangkat dan dokumen harus disimpan dan dibuang, serta prosedur untuk menangani kejadian seperti bencana alam atau kebakaran. Selain itu, kebijakan ini juga harus mencakup protokol untuk mengenali dan melaporkan aktivitas mencurigakan atau insiden keamanan.

Untuk efektif, kebijakan keamanan fisik harus diimplementasikan secara konsisten dan disiplin di seluruh organisasi. Setiap karyawan harus memahami dan mengikuti kebijakan, dan harus ada konsekuensi jika kebijakan dilanggar. Pelatihan dan pendidikan terus-menerus sangat penting untuk memastikan bahwa semua orang memahami peran mereka dalam menjaga keamanan fisik.

4.6 Keamanan Aplikasi dan Pengembangan Perangkat Lunak

4.6.1 Teknik Pengujian Keamanan Perangkat Lunak

Pengujian keamanan perangkat lunak adalah proses yang sistematis dan direncanakan untuk mengevaluasi efektivitas keamanan perangkat lunak dengan tujuan untuk menemukan dan memperbaiki kelemahan sebelum perangkat lunak dikeluarkan atau digunakan oleh pengguna. Pengujian ini bertujuan untuk mengekspos kerentanan yang mungkin dieksploitasi oleh

penyerang, sehingga dapat diperbaiki sebelum merugikan organisasi atau pengguna. Berikut adalah beberapa teknik pengujian keamanan perangkat lunak yang umum digunakan:

1. Pengujian Penetrasi (*Penetration Testing*)
   Pengujian penetrasi adalah metode yang melibatkan simulasi serangan oleh penyerang yang berpotensi merugikan untuk mengevaluasi keamanan sistem. Pengujian ini biasanya dilakukan oleh tim internal atau vendor eksternal yang spesialis dalam pengujian penetrasi, yang kadang-kadang disebut sebagai 'hacker etis'. Mereka mencoba menemukan dan mengeksploitasi kerentanan dalam perangkat lunak, dengan tujuan untuk memahami sejauh mana sistem bisa diserang dan bagaimana efektivitas mekanisme pertahanan yang ada.
2. Pengujian Statik (*Static Testing*)
   Pengujian statik, atau Static Application Security Testing (SAST), adalah teknik yang digunakan untuk menganalisis kode sumber perangkat lunak tanpa harus menjalankannya. Dengan menggunakan SAST, pengembang dapat menemukan kerentanan dalam kode sejak dini dalam siklus pengembangan, sehingga dapat diperbaiki sebelum kode tersebut menjadi bagian dari versi rilis. SAST dapat menemukan berbagai jenis kerentanan, seperti penggunaan variabel yang tidak tepat, kesalahan dalam pengendalian aliran program, dan lainnya.
3. Pengujian Dinamis (*Dynamic Testing*)
   Pengujian dinamis, atau Dynamic Application Security Testing (DAST), adalah proses yang melibatkan pengujian aplikasi saat aplikasi tersebut sedang berjalan. DAST mencoba menemukan kerentanan yang mungkin tidak terdeteksi oleh SAST, seperti masalah dalam konfigurasi keamanan, masalah dalam validasi input, dan kerentanan pada tingkat sistem. DAST biasanya dilakukan setelah aplikasi telah selesai dikembangkan dan siap untuk rilis.

4. Pengujian Fuzzing
   Pengujian fuzzing adalah metode yang melibatkan pengiriman data acak, tak terduga, atau tidak valid ke perangkat lunak untuk mengevaluasi bagaimana perangkat lunak tersebut bereaksi. Tujuannya adalah untuk menemukan masalah seperti kegagalan sistem, kebocoran memori, atau kondisi yang dapat dieksploitasi oleh penyerang.
5. Code Review Keamanan
   Code review keamanan adalah proses yang melibatkan penelaahan manual kode sumber perangkat lunak oleh individu atau tim untuk mencari kerentanan keamanan. Hal ini biasanya dilakukan oleh orang-orang yang memiliki pengetahuan dan pengalaman dalam keamanan perangkat lunak. Code review keamanan dapat sangat efektif dalam menemukan dan memperbaiki kerentanan, terutama kerentanan yang rumit atau halus yang mungkin tidak terdeteksi oleh alat pengujian otomatis.
6. Pengujian Kerentanan (*Vulnerability Scanning*)
   Pengujian kerentanan adalah proses otomatis untuk memindai perangkat lunak dan sistem yang terhubung dengan tujuan menemukan kerentanan yang dikenal. Alat pemindaian kerentanan biasanya memiliki database dari kerentanan yang telah diketahui dan melakukan pemindaian untuk mencari keberadaan kerentanan ini dalam perangkat lunak atau sistem. Hasil dari pemindaian ini kemudian digunakan untuk menerapkan patch atau melakukan perbaikan lainnya untuk mengatasi kerentanan yang ditemukan.
7. Pengujian Resiliensi
   Pengujian resiliensi adalah pendekatan yang berfokus pada bagaimana perangkat lunak atau sistem bereaksi ketika terjadi serangan atau kegagalan. Tujuannya adalah untuk memastikan bahwa perangkat lunak atau sistem dapat pulih

dengan cepat dan efektif dari serangan atau kegagalan dan terus beroperasi sebagaimana mestinya.

8. Pengujian Serangan Tersamar (Red Teaming)
   Red teaming adalah latihan keamanan di mana tim independen (biasanya disebut "red team") mencoba untuk menyerang organisasi dengan cara yang sama seperti penyerang nyata. Tujuan dari latihan ini adalah untuk menguji efektivitas kebijakan, prosedur, dan kontrol keamanan suatu organisasi.

Setiap teknik pengujian keamanan perangkat lunak memiliki kekuatan dan kelemahannya masing-masing. Oleh karena itu, penting untuk menggunakan pendekatan yang berlapis dan terpadu, yang mencakup berbagai teknik pengujian, untuk memastikan keamanan perangkat lunak yang efektif. Selain itu, siklus pengujian ini harus diulang secara berkala, karena perangkat lunak dan ancaman terus berubah dan berkembang seiring waktu.

4.6.2 Prinsip-prinsip Pengembangan Perangkat Lunak Aman

Pengembangan perangkat lunak yang aman adalah praktik yang berfokus pada penggabungan prinsip-prinsip, teknik, dan alat keamanan selama siklus hidup pengembangan perangkat lunak (Software Development Life Cycle - SDLC) untuk mengurangi kerentanan dan ancaman terhadap perangkat lunak.

DevSecOps adalah praktek yang mengintegrasikan tim Keamanan (*Security*) ke dalam DevOps, yang merupakan penggabungan antara tim Pengembangan (*Development)* dan Operasi (*Operations*). Pendekatan ini bertujuan untuk memasukkan keamanan dalam siklus hidup pengembangan perangkat lunak sejak dini, bukan menambahkannya di tahap akhir atau setelah perangkat lunak dikembangkan.

DevSecOps adalah filosofi yang memasukkan keamanan ke dalam proses DevOps. Dengan DevSecOps, tim pengembangan, operasi, dan keamanan bekerja sama sejak awal pengembangan.

Tujuannya adalah untuk meminimalkan kerentanan keamanan dan memastikan *delivery* perangkat lunak yang cepat dan aman. Pendekatan ini menekankan "penggeseran ke kiri" dari keamanan, yang berarti menangani masalah keamanan sejak awal pengembangan, bukan setelahnya.

Prinsip-prinsip DevSecOps meliputi kolaborasi dan komunikasi antara tim, integrasi keamanan sejak dini, penggunaan otomatisasi untuk proses keamanan, dan penekanan pada pembelajaran dan perbaikan berkelanjutan. DevSecOps juga mengadvokasi tanggung jawab bersama atas keamanan, yang berarti semua anggota tim, bukan hanya tim keamanan, bertanggung jawab atas keamanan.

Dengan DevSecOps, masalah keamanan dapat dideteksi dan diperbaiki lebih awal dalam siklus hidup pengembangan, mengurangi risiko dan biaya yang berhubungan dengan insiden keamanan. DevSecOps juga dapat meningkatkan kecepatan pengiriman perangkat lunak dengan mengintegrasikan keamanan ke dalam proses CI/CD *(Continuous Integration/Continuous Deployment)*, bukan menambahkannya sebagai langkah terpisah.

Implementasi DevSecOps melibatkan penggunaan alat dan teknologi untuk memungkinkan otomatisasi dan integrasi keamanan. Alat-alat ini dapat mencakup solusi untuk integrasi terus menerus, pengujian otomatis, pemantauan keamanan, dan manajemen konfigurasi. Implementasi DevSecOps juga memerlukan perubahan budaya untuk mendorong kolaborasi, tanggung jawab bersama, dan penekanan pada keamanan.

Tantangan dalam menerapkan DevSecOps dapat mencakup perubahan budaya, pelatihan dan pengetahuan keamanan, dan integrasi alat dan proses baru. Selain itu, mendorong kerjasama antara tim pengembangan, operasi, dan keamanan juga bisa menjadi tantangan.

Secara keseluruhan, DevSecOps mewakili evolusi dalam cara organisasi mendekati keamanan dalam pengembangan

perangkat lunak, dengan fokus pada pencegahan, deteksi, dan perbaikan cepat dari masalah keamanan.

4.6.3 Mitigasi Risiko pada Aplikasi

Mitigasi risiko merupakan langkah-langkah yang diambil untuk mengurangi dampak negatif dari ancaman atau kerentanan pada sistem atau aplikasi. Dalam konteks aplikasi, ada beberapa metode umum untuk melakukan mitigasi risiko:

1. Analisis dan Identifikasi Risiko. Langkah pertama dalam mitigasi risiko adalah mengidentifikasi ancaman atau kerentanan yang mungkin ada dalam aplikasi. Hal ini bisa melibatkan analisis kode, pengujian keamanan, dan penggunaan alat otomatis untuk menemukan kerentanan dalam kode. Mengidentifikasi risiko memungkinkan tim keamanan untuk memahami ancaman yang mereka hadapi dan merencanakan langkah-langkah untuk mengatasi risiko tersebut.
2. Penilaian Risiko. Setelah risiko diidentifikasi, mereka harus dinilai untuk menentukan tingkat keparahan dan kemungkinan risiko tersebut terjadi. Penilaian risiko ini memungkinkan tim keamanan untuk menentukan prioritas dan memutuskan langkah-langkah mitigasi mana yang harus diterapkan terlebih dahulu.
3. Strategi Mitigasi. Ada beberapa strategi mitigasi yang dapat diterapkan, tergantung pada risiko yang diidentifikasi dan dinilai. Beberapa strategi ini dapat meliputi perbaikan kerentanan dalam kode, penerapan kontrol keamanan seperti firewall atau otentikasi, atau pembuatan rencana kontinjensi untuk risiko yang tidak dapat dikelola atau dihilangkan.
4. Implementasi dan Pemantauan. Setelah strategi mitigasi dipilih, mereka harus diimplementasikan dan dipantau untuk memastikan efektivitasnya. Ini bisa melibatkan

pembaruan rutin aplikasi, audit keamanan, dan pemantauan log untuk mencari tanda-tanda aktivitas mencurigakan.
5. Review dan Perbaikan Berkelanjutan. Siklus mitigasi risiko tidak berakhir setelah langkah mitigasi diimplementasikan. Sebaliknya, proses harus diulangi secara teratur untuk mengidentifikasi risiko baru dan memastikan bahwa langkah-langkah mitigasi masih efektif.

Mitigasi risiko adalah bagian penting dari manajemen keamanan aplikasi. Dengan menerapkan proses mitigasi risiko, organisasi dapat mengurangi potensi dampak negatif dari ancaman keamanan dan melindungi aplikasi dan data mereka dari kerusakan.

4.7 Keamanan Data dan Privasi

Dalam era digital saat ini, menjaga keamanan data dan privasi adalah tantangan yang signifikan, tetapi juga menjadi suatu keharusan. Melanggar keamanan data dan privasi tidak hanya dapat merusak reputasi dan kepercayaan publik, tetapi juga dapat berujung pada sanksi hukum dan kerugian finansial. Oleh karena itu, setiap organisasi harus memprioritaskan keamanan data dan privasi dalam operasional mereka, dan berinvestasi dalam teknologi, prosedur, dan pelatihan untuk memastikannya.

Keamanan data adalah praktik yang melindungi data dari ancaman seperti akses yang tidak sah, korupsi data, atau pencurian. Ini melibatkan langkah-langkah untuk melindungi data baik dalam transit (ketika data dikirimkan antara lokasi) maupun dalam keadaan diam (ketika data disimpan dalam database atau media penyimpanan lainnya). Prinsip-prinsip utama dari keamanan data meliputi kerahasiaan, integritas, dan ketersediaan data, yang juga dikenal sebagai Triad CIA.

Berikut beberapa komponen penting dalam keamanan data:

1. Enkripsi Data. Teknik ini digunakan untuk mengubah data menjadi format yang tidak dapat dibaca tanpa kunci enkripsi yang tepat. Enkripsi sangat penting untuk melindungi data saat transit dan dalam keadaan diam.
2. Manajemen Hak Akses. Hal ini melibatkan pembatasan akses data hanya untuk pengguna yang berwenang. Hak akses yang tepat dapat dikelola melalui kontrol akses berbasis peran (RBAC) atau model kontrol akses lainnya.
3. Backup dan Pemulihan Data. Membantu dalam mengatasi insiden yang bisa merusak data seperti kegagalan sistem, serangan cyber, atau bencana alam. Rutin melakukan backup data dan memiliki rencana pemulihan yang efektif sangat penting.
4. Deteksi dan Respons Terhadap Ancaman. Sistem keamanan harus mampu mendeteksi ancaman atau serangan dan meresponsnya dengan cepat untuk meminimalkan kerusakan.

Adapun mengenai privasi data, hal ini berkaitan dengan bagaimana data pribadi dihimpun, disimpan, digunakan, dan dibagikan. Ini berfokus pada perlindungan hak individu atas data mereka dan mematuhi undang-undang dan standar privasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) di Indonesia atau *General Data Protection Regulation* (GDPR) di Uni Eropa.

Berikut beberapa aspek penting dalam privasi data:

1. Persetujuan. Organisasi harus memperoleh persetujuan dari individu sebelum mengumpulkan dan menggunakan data pribadi mereka. Persetujuan harus bebas, spesifik, dan berdasarkan informasi yang jelas.
2. Minimasi Data. Prinsip ini menekankan bahwa hanya data yang benar-benar diperlukan untuk tujuan tertentu yang harus dikumpulkan dan diproses.

3. Transparansi. Organisasi harus jujur dan terbuka tentang bagaimana mereka menggunakan data pribadi. Mereka harus memiliki kebijakan privasi yang jelas dan mudah dimengerti.
4. Hak Individu. Individu memiliki hak untuk mengakses data mereka, meminta koreksi data yang salah, dan dalam beberapa kasus, meminta penghapusan data mereka.
5. Keamanan Data Pribadi. Data pribadi harus dilindungi dari akses yang tidak sah dan kerusakan. Ini sering melibatkan teknik yang sama dengan yang digunakan dalam keamanan data secara umum.
6. Pelaporan dan Akuntabilitas. Jika terjadi pelanggaran data, organisasi harus melaporkannya kepada otoritas yang berwenang dan memberi tahu individu yang terkena dampak. Selain itu, organisasi harus menunjukkan akuntabilitas dalam hal perlindungan data dan privasi, biasanya melalui audit dan review rutin.
7. Pelatihan dan Kesadaran: Semua anggota organisasi, dari level eksekutif hingga karyawan biasa, harus memiliki pemahaman dan kesadaran yang memadai tentang pentingnya keamanan data dan privasi. Pelatihan dan edukasi berkelanjutan penting untuk menjaga praktik terbaik dan memastikan kepatuhan.

Secara keseluruhan, keamanan data dan privasi data adalah dua konsep yang saling terkait dan sama-sama penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data. Keamanan data dan privasi seringkali saling terkait dan saling mempengaruhi. Tanpa keamanan data yang kuat, data pribadi dapat menjadi rentan terhadap akses yang tidak sah dan pencurian. Sementara itu, tanpa penekanan pada privasi, data pribadi dapat disalahgunakan atau dieksploitasi, baik secara sengaja maupun tidak.

DAFTAR PUSTAKA

Anderson, R. 2020. *Security Engineering*. Wiley. Available at: https://doi.org/10.1002/9781119644682.

Benantar, M. 2006. *Access Control Systems*. Boston: Springer New York, NY. Available at: https://doi.org/10.1007/0-387-27716-1.

Chapman, D.B. 1992. 'Network (In)Security Through IP Packet Filtering', in. USENIX Summer.

Ferraiolo, D.F. *et al.* 2001. 'Proposed NIST standard for role-based access control', *ACM Transactions on Information and System Security*, 4(3), pp. 224–274. Available at: https://doi.org/10.1145/501978.501980.

Hu, V.C. *et al.* 2014. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. Gaithersburg, MD. Available at: https://doi.org/10.6028/NIST.SP.800-162.

Hu, V.C. *et al.* 2015. *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. U.S. Department of Commerce: NIST Special Publication 800-162.

Jain, A.K., Ross, A. and Prabhakar, S. 2004. 'An Introduction to Biometric Recognition', *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), pp. 4–20. Available at: https://doi.org/10.1109/TCSVT.2003.818349.

Pfleeger, S.L. 2002. *Security in Computing*. Third Edit. Prentice Hall.

Samarati, P. and de Vimercati, S.C. 2001. 'Access Control: Policies, Models, and Mechanisms', in, pp. 137–196. Available at: https://doi.org/10.1007/3-540-45608-2_3.

Sandhu, R.S. *et al.* 1996. 'Role-based access control models', *Computer*, 29(2), pp. 38–47. Available at: https://doi.org/10.1109/2.485845.

Sasse, M.A., Brostoff, S. and Weirich, D. 2001. *Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security.* Department of Computer Science, University College London.

Scarfone, K. and Mell, P. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS)*, *NIST Special Publication 800-94*.

Schneier, B. 2015. *Applied Cryptography, Second Edition*. Indianapolis, Indiana: John Wiley & Sons, Inc. Available at: https://doi.org/10.1002/9781119183471.

Stallings, W. and Brown, L. 2018. *Computer Security: Principles and Practice*. 4th edn. Pearson.

Vimercati, S.D.C. di, Foresti, S. and Samarati, P. 2008. 'Recent Advances in Access Control', in M. Gertz and S. Jajodia (eds) *Handbook of Database Security*. Boston, MA: Springer US, pp. 1–26. Available at: https://doi.org/10.1007/978-0-387-48533-1_1.

Wang, W. and Lu, Z. 2013. 'Cyber security in the Smart Grid: Survey and challenges', *Computer Networks*, 57(5), pp. 1344–1371. Available at: https://doi.org/10.1016/j.comnet.2012.12.017.

Zwicky, E.D., Cooper, S. and Chapman, D.B. 2000. *Building Internet Firewalls*. O'Reilly Media, Inc.

BAB 5
POLICY

Oleh Kholidiyah Masykuroh

5.1 Pendahuluan

Perkembangan internet memberikan kemudahan akses informasi tanpa Batasan ruang dan waktu. Pencegahan kehilangan, kerusakan, penghancuran yang tidak sah, atau akses ke informasi yang diproses oleh organisasi menjadi perhatian penting saat ini. Resiko internal dan eksternal terus dikaji untuk menemukan solusi dari keamanan informasi dan mengurangi berbagai bentuk pelanggaran. Penelitian yang dilakukan oleh Ponemon Institute (2013) menunjukkan pelanggaran disebabkan oleh 35% faktor manusia sebanyak, 29% gangguan sistem, dan 37% serangan berbahaya atau kriminal (Da Veiga & Martins, 2015).

Kebijakan keamanan informasi dan persyaratan pemrosesan informasi diarahkan oleh sejumlah persyaratan seperti, standar internasional, persyaratan peraturan dan hukum, tujuan bisnis, risiko inheren informasi, dan sebagainya (Da Veiga & Martins, 2015).

Ringkasan klasifikasi perilaku terkait keamanan yang dapat mengancam keamanan system informasi, yaitu (Guo, 2013):

1. Intensionalitas, perilaku ini mengacu pada tindakan karyawan disengaja atau tidak sengaja melakukan kesalahan manusia atau *human errors*.
2. Motif, perilaku ini mengacu pada tindakan karyawan berbahaya atau tidak. Tindakan berbahaya berupa ancaman yang disengaja diklasifikasikan sebagai tindakan berbahaya, kesalahan nai've. Dan disisi lain adalah Tindakan tidak berbahaya.

3. Keahlian, perilaku ini mengacu pada tingkat pengetahuan dan keterampilan sisntem informasi yang dibutuhkan seorang karyawan untuk perilaku berbahaya atau tidak. Misalnya, meretas komputer, meretas kata sandi, tindakan ini membutuhkan tingkat pengetahuan dan keterampilan teknis yang lebih tinggi dibandingkan menulis dan memposting kata sandi di monitor. Perilaku ini terkait dengan peran karyawan dalam organisasi tempatnya bekerja. Pengguna akhir pada umumnya berfokus pada penggunaan system informasi untuk mencapai tujuan bisnis. Sedangkan karyawan yang bekerja pada system informasi, berfokus pada pengelolaan system dan jaringan. Perbedaan peran ini dapat menimbulkan perbedaan pemahaman tentang masalah keamanan dan perilaku pantas atau tidak pantas.
4. Keterkaitan pekerjaan, perilaki ini mengacu pada Tindakan karywan terkait dengan pekerjaannya. Karena karywan menggunakan system informasi dalam pengaturan organisasi, keterkaitan pekerjaan menjadi faktor penting bagi karyawan membuat penilaian apakah perilaku tersebut sesuai atau tidak. Misalnya, menyalin data organisasi yang sensitive ke perangkat penyimpanan data seluler untuk alasan pekerjaan. Menggunakan internet untuk tujuan non bisnis merupakan permasalahan yang kerapkali dilakukan oleh karyawan.
5. Tindakan dan kelambanan, perilaku berupa tindakan atau kelambanan. Perilaku aktif membutuhkan usaha individu, dan sebaliknya, perilaku pasif tidak memerlukan upaya mental dan fisik. Faktor yang menyebabkan perilaku ini tidak sama. Misalkan merancang dan menggunakan kata sandi yang rumit dan perilaku aktif memerlukan upaya dari karyawan. Beberapa perilaku diantaranya mencoba mengingat kata sandi, gagal mengubah kata sandi dari waktu ke waktu merupakan contoh perilaku tidak aktif.

6. Aturan, perilaku ini mengacu pada perilaku melanggar aturan atau tidak. Aturan yang relevan dengan perilaku karyawan dalam keamanan system informasi adalah hukum dan kebijakan organisasi tempat bekerja. Hukum merupakan aturan yang berlaku di masyarakat, menangani kejahatan komputer seperti pencurian data. Sedangkan kebijakan organisasi hanya untuk organisasi sendiri. Kebijakan organisasi dapar berupa:
    a. Kebijakan yang diterapakan oleh sistem, misalnya kata sandi lebih daru delapan karakter.
    b. Kebijakan yang mengatur Tindakan karyawan, misalnya apa yang harus dilakukan dan tidak boleh dilakukan.
    c. Kebijakan yang mengatur manajemen keamanan umum, misalnya struktur organisasi, dan proses pengambilan keputusan.

5.2 Definisi Informasi

Informasi adalah asset penting untuk kebutuhan bisnis organisasi. Informasi dapat memiliki berbagai bentuk. Informasi dapat dicetak atau ditulis di atas kertas, disimpan di media elektronik, dikirim melalui email, ditampilkan dalam video, atau dikirim secara lisan (Grishaeva & Borzov, 2020).

Dalam Undang-Undang tentang Perlindungan Data Pribadi Nomor 27 Tahun 2022. Definisi informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun nonelektronik (Undang Undang Tentang Perlindungan Data Pribadi Nomor 27, 2022).

Setelah memahami definisi umum dari informasi, informasi dapat berupa file, gambar, suara, video. Informasi dapat dikenali dari empat atribut informasi, yaitu (Da Veiga & Martins, 2015):

1. Format, informasi memiliki berbagai format atau media. Misalnya informasi tertulis, elektronik atau digital, lisan, difoto, dicetak, diluki, digambar, foto, dan sebagainya.
2. Kategori, setiap departemen dalam organisasi memproses berbagai kategori informasi. Seperti informasi keuangan, misalnya kartu kredit, slip gaji, nomor pajak laporan bank. Informasi Kesehatan, misalnya hasil tes darah, resep. Informasi pribadi, misalnya nomor jaminan sosial, alamat, informasi ras atau etnis. Adapula yang mengikutsertakan informasi kekayaan intelektual atau strategi.
3. Siklus hidup informasi, pemrosesan informasi dapat berada dalam berbagai fase siklus hidup. Informasu yang dikumpulkan dari pelanggan melalui formulis aplikasi, pusat panggilan, atau internet berada dalam fase pengumpulan. Setelah informasi dikumpulkan, informasi tersebut disimpan dalam database, cloud, atau media lain yang disebut sebagai fase penyimpanan. Data yang dikumpulkan kemudian diproses dan digunakan untuk memberikan layanan, menjual produk, melakukan analisis, dan seterusnya, sebagai bagian fase penggunaan. Informasi juga dapat ditransfer antar unit bisnis, anak perusahaan, pihak ketiga, atau lintas batas, hal ini merupakan rangkaian fase retesni. Informsi perlu disimpan untuk memnuhi persyaratan bisnis, industry, pelanggan, hukum dan peraturan. Informasi yang tidak lagi digunakan dan telah memenuhi periode penyimpanan atau fase pengarsipan dan pada periode tertentu dapat dihancurkan. Hal ini sejalan dengan kebijakan organisasi dan persyaratan hukum.
4. Klasifikasi, informasi dapat diklasifikasikan menurut sensitivitasnya untuk menerapkan kontrol sesuai untuk

melindungi informasi. Berbagai skema klasifikasi tersedia untuk mengklasifikasikan informasi, yaitu:

a. Informasi sangat rahasia, merupakan informasi yang sangat sensitif yang berdampak material pada organisasi jika kerahasiaan, integritas, dan /atau ketersediaan atau *confidentiality, integrity, and/or availability* (CIA) terpengaruh.
b. Informasi rahaisa, merupakan informasi sensitive yang berdampak bersa pada organisasi apabila CIA terpengaruh.
c. Informasi terbatas, merupakan informasi internal terbatas pada unit bisnis atau pengguna tertentu yang dapat mengakibatkan dampak sedang pada organisasi apabila CIA terpengaruh.
d. Informasi public, merupakan informasi yang tersedia untuk karyawan dan pihak eksternal tanpa dampak jika CIA terpengaruh.

Berbagai faktor internal dan eksternal mempengaruhi format, klasifikasi, dan kategori informasi yang diproses melalui siklus hidup suatu organisasi. Misi, visi, layanan, produk, kebijakan dan prosedur internal, dan teknologi adalah faktor-faktor yang mempengaruhi atribut informasi (Da Veiga & Martins, 2015).

5.3 Regulasi Informasi

5.3.1 Regulasi Informasi di Indonesia

Undang-Undang tentang Perlindungan Data Pribadi Nomor 27 Tahun 2022, UU ini telah disahkan oleh pemerintah pada tanggal 17 Oktober 2022. UU ini dibuat karena munculnya kesadaran perlunya perlindungan data pribadi seiring dengan pertumbuhan internet dan seluler. Lima alasan utama perlu perlindungan data pribadi, yaitu (CNNindonesia.com, 2019):

1. Intimidasi online terkait gender.
2. Mencegah penyalahgunaan data pribadi oleh pihak yang tidak bertanggung jawab.
3. Menghindari potensi pencemaran nama baik.
4. Hak kendali atas data pribadi.

Definisi Data Pribadi dalam UU Nomor 27 Tahun 2022 adalah data tentang orang perseorangan yang terindentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui system elektronik dan non elektronika.

Sedangakan Perlindungan Data Pribadi dalam UU Nomor 17 Tahun 2022 adalah keseluruhan upaya untuk melindungi Data Pribadi dalam rangkaiang pemrosesan Data Pribadi guna menjamin hak konstitusional subjek Data Pribadi.

Data Pribadi yang dilindungi UU terdiri atas data pribadi yang b2ersifat spesifik dan umum. Data pribadi yang bersifat spesifik, meliputi:

1. Data dan informasi Kesehatan.
2. Data biometrik.
3. Data genetika.
4. Catatan kejahatan.
5. Data anak.
6. Data keuangan pribadi.
7. Data lain sesuai dengan ketentuan peraturan perundang-undangan.

Sedangkan Data Pribadi yang bersifat umum, meliputi:

1. Nama lengkap.
2. Jenis kelamin.
3. Kewarganegaraan.
4. Agama.
5. Status Perkawinan.

6. Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang.

5.3.2 Regulasi Informasi di Amerika

Setelah memahami undang-undang yang berlaku di Indonesia, perlu pembanding bagaimana negara lain mengatur regulasi sistem informasi. Regulasi sistem informasi yang diterapkan di Amerika akan dijelaskan pada pembahasan selanjutnya (Straub, 2008).

Keamanan informasi pada dasarnya adalah masalah ekonomi, bukan teknologi. Hal ini disebabkan jika nilai informasi lebih besar daripada biaya untuk mendapatkannya, informasi tersebut tidak aman. Kebijakan keamanan informasi adalah elemen kedua dari program keamanan informasi. Elemen utamanya adalah tata Kelola yang efektif.

Pemerintah memegang kendali dan mengatur undang-undang. Dalam perusahaan, diberikan tata kelola keamanan informasi terdiri dari mekanisme manajemen yang dirancang untuk meyakinkan tim kepemimpinan eksekutif bahwa karyawan mengethaui kebijakan keamanan informasi dan sesuai dengannya. Sementara sanksi untma untuk pelanggaran kebijakan perusahaan adalah kehilangan pekerjaan. Melalui tata Kelola yang efektif, karyawan menjalankan fungsi bisnisnya sambil mempertahankan kesesuaian dengan kebijakan.

Dalam kaitan dengan masyarakat sipil, pemerintah berperan mengatur dan menentukan undang-undang. Pemerintah membuat tata Kelola bagi kepemimpinan nasional yang dapat memastikan bahwa warga negara secara umum mengetahui kebijakan keamanan informasi, dan mematuhinya. Sanksi utama yang dijatuhkan oleh pemerintah mungkin sah, tetapi polisi jarang menangkap dan jaksa jarang mengadili warga negara karena pelanggaran keamanan informasi.

Kebijakan keamanan informasi harus memandu orang untuk memperbaiki perilaku saat menggunakan teknologi

indormasi. Banyak bentuk bimbingan efektif yang dapat diterapkan. Ada empat cara untuk mengatur perilaku, yaitu:

1. Ekonomi.
2. Tekanan sosial.
3. Arsitektur.
4. Hukum.

Tata Kelola Teknologi Informasi Melalui Ekonomi

Tata Kelola keamanan informasi sosial memiliki permasalahan yang berbeda dibandingkan dengan tata Kelola perusahaan. Kebijakan keamanan informasi perusahaan yang dibuat dengan baik memiliki pernyataan yang mirip:

Sumber daya teknologi informasi perusahaan akan digunakan hanya untuk tujuan yang disetujui manajemen. Penggunaan lainnya dapat menyebabkan Tindakan disipliner, termasuk pemutusan hubungan kerja atau tindakan hukum.

Korporasi melakukan tekanan ekonomi yang efektif pada karyawan mereka. Masyarakat madani tidak memiliki kemampuan ini. Oleh karena itu, kelompok sosial bergantung pada kekuatan pemerintah.

Tata Kelola Teknologi Informasi Melalui Tekanan Sosial

Perlindungan informasi yang menjadi bagian penting dari proses komunikasi melalui internet menjadi perhatian dewasa ini. Masyarakat Indonesia sendiri telah mengalami ancaman dari kejahatan *cyber* yang mengancam data-data penting pemerintah maupun korporasi. Kejadian ini pernah dialami diwaktu lampau. Munculnya serangan peretasan atau *hacking* ini memicu pro dan kontra di kalangan *hacker* sendiri. Kecaman atas peretasan muncul dari masyarakat sebagai bentuk penolakan. Tindakan yang dilakukan oleh komunitas ini akhirnya mampu meredam kejahatan *cyber* yang berkembang saat itu.

Selain itu, berkembangnya berbagai virus seperti Trojan, yang menyerang tempat penyimpanan atau *storage* pernah terjadi.

Munculnya berbagai virus yang beranekaragam memicu komunitas yang memiliki keahlian untuk memecahkan dan membuat kode anti-virus. Berbagai virus yang bermunculan inipun akhirnya dapat terpecahkan.

Tata Kelola Teknologi Informasi Melalui Arsitektur

Tata kelola teknologi informasi melalui arsitektur ini dapat dilakukan melalui beberapa aspek, yaitu:

1. Kebijakan kontrol akses fisik.
2. Kebijakan kontrol akses logis.
3. Kebijakan perimeter jaringan.
4. Kebijakan yang ditetapkan tentang standar eksternal. Iso 7498-2 memetakan persyaratan keamanan terhadap model referensi OSI. Standar ini mengidentifikasi lime fungsi keamanan informasi, yaitu:
    a. Identifikasi dan otentikasi, identifikasi pengguna.
    b. Kontrol akses, hak apa yang dimiliki pengguna yang teridentifikasi.
    c. Kerahasiaan data, biasanya enkripsi.
    d. Integritas data, cara memverifikasi bahwa informasi belum berubah.
    e. Non-penolakan, konsep hukum yang berarti bahwa penulis pesan tidak dapat menyangkal kepenulisan.

Tata Kelola Teknologi Informasi Melalui Hukum

Gagasan Cohen pada tahun 1984 mengenai penggunaan serangan untuk mempelajari masalah diperlukan oleh kebijakan pemerintah untuk system tepercaya.

Fakta menunjukkan bahwa kebijakan hanya mencakup kelompok individu yang memiliki akses fisik atau jaringan ke komputer. Sedangkan individu-individu yang lainnya tidak dilindungi dan dianggap sebgai pelanggar atau penjahat. Dari sudur pandang tata Kelola sipil, tidak adanya undag-undang untuk kejahatan elektronik dipandang sebagai hambata utama.

Penuntutan yang didasarkan pada tindakan seperti: penyadapan telepon illegal, pencurian, pemerasan, atau penggelapan, yang mengikut peretasan dan bukan karena peretasan itu sendiri.

5.4 Kesimpulan

Berdasarkan berbagai ulasan yang telah disampaikan sebelumnya penulis menyimpulkan bahwa negara perlu hadir dalam mengatur tata Kelola teknologi informasi. Pemerintah sebagai pemegang kekuasaan yuridiksi memegang peranan penting melalui berbagai undang-undang. Tidak dapat dipungkiri bahwa tindakan kejahatan *cyber* belum memiliki fondasi hukum yang cukup kuat saat ini di Indonesia. Tindakan yang menyertai peretasan perlu menjadi perhatian pemerintah. Hal inilah yang memunculkan kesadaran masyarakat akan pentingnya perlindungan informasi dari kejahatan *cyber*. Peran berbagai *stakeholder* yang terlibat menjadi faktor penentu apabila kebijakan dari pemerintah telah ditetapkan. Korporasi adalah lini kedua sebagai pelaksana dan juga mengatur keamanan informasi dalam setiap kegiatan operasional bisnis yang dijalankan.

DAFTAR PUSTAKA

CNNindonesia.com. 2019. *5 Alasan Mengapa Data Pribadi Perlu Dilindungi*. https://www.kominfo.go.id/content/detail/19991/5-alasan-mengapa-data-pribadi-perlu-dilindungi/0/sorotan_media

Da Veiga, A., & Martins, N. 2015. Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review*, *31*(2), 243–256. https://doi.org/10.1016/j.clsr.2015.01.005

Undang Undang tentang Perlindungan Data Pribadi Nomor 27, Pub. L. No. Nomor 27 Tahun 2022, 1 2022. https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

Grishaeva, S. A., & Borzov, V. I. 2020. Information Security Risk Management. *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, 96–98. https://doi.org/10.1109/ITQMIS51053.2020.9322901

Guo, K. H. 2013. Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security*, *32*, 242–251. https://doi.org/10.1016/j.cose.2012.10.003

Straub, D. W. (Ed.). 2008. *Information security: Policy, processes and practices*. Sharpe.

BAB 6
SECURITY DOMAIN

Oleh Fahmy Rinanda Saputri

6.1 Pendahuluan

Dalam era digital yang semakin maju, keamanan informasi menjadi hal yang sangat penting. Dalam lingkungan yang terhubung dan penuh dengan ancaman, organisasi harus memprioritaskan proteksi aset informasi mereka agar terhindar dari kerugian finansial, reputasi yang rusak, atau pelanggaran privasi yang merugikan. keamanan informasi didefinisikan sebagai upaya untuk melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang. Tujuan utama keamanan informasi adalah memastikan kerahasiaan, integritas, dan ketersediaan informasi (Indrajit, Prof., 2011).

Konsep dasar dalam keamanan informasi yang meliputi tiga aspek utama, yaitu kerahasiaan (*Confidentiality*), integritas (*Integrity*), dan ketersediaan (*Availability*) digambarkan sebagai Segitiga CIA seperti pada Gambar 6.1.

Gambar 6.1. Segitiga CIA (Hayaty, 2020)

Kerahasiaan (*Confidentiality*) berkaitan dengan menjaga informasi tetap rahasia dan hanya dapat diakses oleh pihak yang berwenang. Tujuannya adalah mencegah akses, pengungkapan, atau penggunaan informasi oleh pihak yang tidak berhak. Langkah-langkah seperti enkripsi data, pengendalian akses, dan kebijakan kerahasiaan digunakan untuk menjaga kerahasiaan informasi.

Integritas (*Integrity*) mencakup keaslian dan integritas informasi, yang berarti memastikan bahwa informasi tidak mengalami modifikasi atau manipulasi yang tidak sah. Tujuannya adalah untuk mencegah perubahan yang tidak diinginkan pada informasi dan memastikan bahwa informasi tetap akurat dan dapat diandalkan. Penerapan tanda tangan digital, verifikasi checksum, dan pengendalian akses yang tepat adalah beberapa langkah yang digunakan untuk menjaga integritas informasi.

Ketersediaan (*Availability*) berarti memastikan bahwa informasi dan sistem informasi tersedia dan dapat diakses oleh pihak yang berwenang ketika diperlukan. Tujuannya adalah untuk mencegah gangguan atau pemadaman sistem yang dapat menghambat akses dan penggunaan informasi. Upaya seperti perencanaan kontinuitas bisnis, cadangan data, dan pengelolaan kapasitas digunakan untuk menjaga ketersediaan informasi.

Setiap organisasi memiliki aset informasi berharga yang harus dilindungi, seperti data klien, informasi keuangan, strategi bisnis, atau rahasia teknis. Proteksi aset informasi ini menjadi penting karena aset informasi yang hilang, terkena serangan, atau diretas dapat mengganggu operasi bisnis secara serius. Hilangnya akses ke data kritis atau pemadaman sistem dapat menghentikan operasi bisnis, menyebabkan kerugian keuangan, dan merusak reputasi organisasi. Data pribadi pelanggan, karyawan, atau mitra bisnis juga perlu dilindungi secara ketat untuk mematuhi peraturan privasi dan menghindari pelanggaran hukum. Pelanggaran privasi dapat menyebabkan sanksi hukum, kerugian finansial, dan kerusakan reputasi yang sulit dipulihkan. Pelanggan dan mitra bisnis mengharapkan keamanan data dan informasi

mereka. Melindungi aset informasi dengan baik membantu membangun kepercayaan dan meningkatkan kepuasan pelanggan.

Security domain dapat digunakan untuk mengkonseptualisasikan kelompok-kelompok yang berbeda dari elemen-elemen teknologi informasi, seperti komputer, jaringan, atau infrastruktur lainnya yang berada di bawah protokol keamanan tertentu (Zetmagz.com, 2022). Konsep ini memungkinkan pengelompokan yang terbatas dari elemen-elemen tersebut, dengan metode otentikasi tunggal yang diterapkan untuk mengakses elemen-elemen di dalam security domain tersebut.

Kumpulan situs web, jaringan komunikasi, atau kelompok komputer dalam ruangan, dapat menjadi contoh konkret dari penggunaan security domain dalam lingkup yang lebih spesifik. Dalam pengaturan perusahaan atau organisasi, security domain juga sering kali terkait dengan layanan direktori yang mengatur otentikasi dan otorisasi akses ke sumber daya informasi dan jaringan.

Penggunaan security domain dalam pengelompokan elemen-elemen TI ini membantu meningkatkan keamanan dengan memungkinkan pengelolaan akses yang terpusat dan perlindungan yang lebih terfokus pada setiap domain tersebut. Dengan demikian, organisasi dapat menerapkan kebijakan keamanan yang konsisten dan memberikan tingkat kontrol yang lebih baik terhadap sumber daya dan data sensitif.

Keamanan informasi yang kuat dapat menjadi keunggulan kompetitif bagi organisasi. Pelanggan dan mitra bisnis cenderung bekerja dengan organisasi yang dianggap dapat diandalkan dan memiliki keamanan yang baik. Selain itu, banyak industri memiliki regulasi ketat terkait keamanan informasi, seperti perlindungan data pribadi atau persyaratan keamanan industri tertentu.

Dalam konteks proteksi atau keamanan informasi, domain digunakan sebagai konsep untuk mengelompokkan objek dan hak akses yang terkait dengan objek-objek tersebut (Syefira Salsabila., S.Gz, no date).

Setiap domain proteksi berisi pasangan objek dan hak akses yang diberikan kepada subjek atau proses yang berjalan dalam domain tersebut. Objek dalam hal ini bisa merujuk pada file, data, sumber daya jaringan, atau elemen lainnya yang perlu dilindungi. Sedangkan hak akses operasi seperti *read* (baca), *write* (tulis), *execute* (jalankan), dan lainnya menentukan tindakan yang dapat dilakukan oleh proses terhadap objek tersebut.

Dalam setiap waktu, sebuah proses berjalan dalam satu atau beberapa domain proteksi. Ini berarti bahwa proses tersebut dapat mengakses objek yang terkait dengan domain tersebut dan memiliki hak akses tertentu terhadap objek tersebut. Selain itu, dalam eksekusi, proses juga dapat berpindah dari satu domain ke domain lainnya sesuai dengan kebutuhan dan hak akses yang diperlukan.

Penerapan konsep domain dalam mekanisme proteksi membantu dalam mengatur akses dan hak operasi yang sesuai untuk mencegah akses yang tidak sah atau tidak diizinkan terhadap objek yang dilindungi. Dengan mengatur domain proteksi dengan tepat, organisasi dapat menjaga kerahasiaan, integritas, dan ketersediaan objek dan sumber daya yang sensitif, serta mengontrol operasi yang dilakukan oleh proses terhadap objek tersebut.

6.2 Keamanan Fisik

Keamanan fisik adalah salah satu aspek penting dalam melindungi aset informasi dan infrastruktur teknologi dari ancaman fisik. Dalam konteks keamanan fisik, tiga elemen utama yang perlu diperhatikan adalah pengamanan ruang server dan pusat data, kontrol akses fisik, dan pengamanan perangkat keras. Berikut adalah penjelasan lebih lanjut tentang setiap elemen:

1. Pengamanan Ruang Server dan Pusat Data: Pengamanan ruang server dan pusat data melibatkan langkah-langkah untuk melindungi fisik ruang dan lingkungan di mana server

dan perangkat keras penyimpanan data disimpan. Beberapa tindakan penting yang perlu dilakukan adalah:

a. Akses Terbatas: Memastikan bahwa hanya orang yang berwenang yang dapat mengakses ruang server dan pusat data dengan menggunakan pengendalian akses fisik seperti kartu akses, kunci, atau identifikasi biometrik.
b. Pemantauan Lingkungan: Menggunakan sistem pemantauan dan deteksi untuk mengawasi suhu, kelembaban, kebakaran, dan kondisi lingkungan lainnya yang dapat mempengaruhi keamanan perangkat keras dan integritas data.
c. Proteksi Fisik: Menggunakan sistem keamanan fisik seperti kamera pengawas (CCTV), alarm keamanan, dan penguncian perangkat keras untuk mencegah akses yang tidak sah atau mencurigakan.

2. Kontrol Akses Fisik: Kontrol akses fisik melibatkan langkah-langkah untuk mengontrol siapa yang dapat memasuki dan mengakses area yang berisi infrastruktur teknologi. Beberapa tindakan yang perlu dilakukan adalah:
   a. Pintu Keamanan: Memasang pintu keamanan yang kuat dan tahan terhadap upaya masuk paksa. Penggunaan kartu akses, identifikasi biometrik, atau sistem pengunci elektronik dapat meningkatkan keamanan akses fisik.
   b. Pengawasan Akses: Memantau dan mencatat aktivitas akses fisik untuk melacak siapa yang masuk dan keluar dari area terbatas.
   c. Keamanan Jendela dan Ventilasi: Memastikan bahwa jendela dan ventilasi dilengkapi dengan sistem keamanan yang memadai untuk mencegah akses yang tidak sah atau manipulasi.
3. Pengamanan Perangkat Keras: Pengamanan perangkat keras melibatkan langkah-langkah untuk melindungi perangkat keras dan komponen fisik lainnya yang digunakan dalam

infrastruktur teknologi. Beberapa tindakan yang perlu dilakukan adalah:

a. Rak Terkunci: Menempatkan perangkat keras dalam rak terkunci atau kabinet yang hanya dapat diakses oleh personel yang berwenang.
b. Pengawasan Fisik: Memantau dan mengawasi perangkat keras secara fisik untuk mendeteksi tanda-tanda manipulasi, kerusakan, atau pencurian.
c. Pemusnahan yang Aman: Memastikan bahwa perangkat keras yang sudah tidak digunakan atau rusak dihancurkan dengan metode yang aman untuk menghindari akses terhadap data atau informasi yang sensitif.

Dengan menerapkan pengamanan ruang server dan pusat data, kontrol akses fisik yang ketat, serta pengamanan perangkat keras yang baik, organisasi dapat meningkatkan keamanan fisik dari aset informasi mereka. Hal ini membantu mencegah akses yang tidak sah, manipulasi, atau kerusakan fisik yang dapat membahayakan keberlanjutan operasional dan kerahasiaan data.

6.3 Keamanan Jaringan

Dalam mempelajari keamanan jaringan, penting untuk memahami beberapa istilah yang terkait dengan dunia cyber. Seperti *cyberspace, cyberlaw, cyber security*, aspek-aspek keamanan informasi, manajemen risiko, dan hacker (Arifin, 2019).

Cyberspace merujuk pada lingkungan virtual yang terbentuk oleh jaringan komputer di seluruh dunia, termasuk internet. Ini adalah dunia digital yang meliputi infrastruktur jaringan, sistem, aplikasi, dan informasi yang berada dalam jaringan komputer. *Cyberlaw* (hukum *cyber*) adalah bidang hukum yang berkaitan dengan penggunaan teknologi informasi dan internet. Ini mencakup hukum yang mengatur transaksi elektronik, perlindungan data, privasi, kekayaan intelektual, dan kejahatan

komputer. *Cyber security* (keamanan cyber) adalah upaya melindungi sistem komputer, jaringan, dan data dari ancaman yang berasal dari dunia cyber. Hal ini mencakup perlindungan terhadap serangan siber, pencurian data, serangan malware, dan akses yang tidak sah ke sistem. Aspek-aspek keamanan informasi melibatkan langkah-langkah untuk melindungi informasi dari akses, penggunaan, pengungkapan, modifikasi, dan penghancuran oleh pihak yang tidak berwenang. Ini meliputi kebijakan keamanan, kontrol akses, enkripsi data, perlindungan fisik, dan tindakan pencegahan terhadap ancaman keamanan. Manajemen risiko adalah proses identifikasi, analisis, penilaian, dan pengendalian risiko yang terkait dengan keamanan informasi. Tujuannya adalah untuk mengidentifikasi potensi ancaman, mengevaluasi dampaknya, dan mengambil tindakan yang tepat untuk mengurangi risiko sesuai dengan toleransi risiko organisasi. Serta hacker adalah individu yang memiliki keahlian dalam menjelajahi, menguji, dan memanipulasi sistem komputer dan jaringan. Ada dua jenis hacker: white hat hacker (*ethical hacker*) yang melakukan kegiatan dengan izin dan tujuan baik untuk menguji keamanan sistem, dan black hat hacker yang melakukan serangan dan aktivitas ilegal untuk tujuan merugikan.

Keamanan jaringan adalah aspek penting dalam melindungi infrastruktur teknologi dan data dari serangan dan ancaman yang berpotensi merugikan. Beberapa elemen penting dalam keamanan jaringan meliputi arsitektur jaringan yang aman, firewall dan filtrasi paket, deteksi intrusi, dan pengamanan akses jaringan. Berikut adalah penjelasan lebih lanjut tentang masing-masing elemen tersebut:

1. Arsitektur Jaringan yang Aman: Arsitektur jaringan yang aman melibatkan desain dan konfigurasi jaringan dengan pertimbangan keamanan yang kuat. Beberapa langkah yang perlu diperhatikan dalam arsitektur jaringan yang aman meliputi:

a. Segmentasi Jaringan: Memisahkan jaringan internal dari jaringan eksternal dan membagi jaringan internal menjadi segmen yang terisolasi. Ini membantu dalam mengurangi penyebaran serangan dan membatasi akses ke sumber daya sensitif.
b. Zona Demilitarisasi (DMZ): Menerapkan zona DMZ yang berfungsi sebagai perantara antara jaringan internal dan eksternal. Ini memungkinkan akses terbatas ke layanan publik, seperti web server, sambil melindungi jaringan internal dari serangan langsung.

2. Firewall dan Filtrasi Paket: Firewall adalah komponen keamanan yang penting dalam jaringan yang berfungsi untuk memantau dan mengontrol lalu lintas data yang masuk dan keluar jaringan. Beberapa aspek terkait firewall dan filtrasi paket adalah:
   a. Firewall Jaringan: Mengimplementasikan firewall di antara jaringan internal dan eksternal untuk memblokir akses yang tidak sah dan mencegah serangan dari luar.
   b. Filtrasi Paket: Menggunakan teknik filtrasi paket untuk memeriksa dan memblokir paket data yang mencurigakan atau berbahaya yang melewati jaringan. Hal ini membantu dalam mencegah serangan seperti serangan DDoS atau serangan berbasis paket.
3. Deteksi Intrusi: Sistem Deteksi Intrusi (*Intrusion Detection System*, IDS) atau Sistem Deteksi Intrusi dan Pencegahan (*Intrusion Detection and Prevention System*, IDPS) digunakan untuk mendeteksi aktivitas mencurigakan atau serangan di jaringan. Beberapa aspek yang terkait dengan deteksi intrusi adalah:
   a. Deteksi Intrusi yang Berbasis Tanda Tangan: Menggunakan database tanda tangan untuk mencocokkan pola serangan yang telah diketahui.

b. Deteksi Intrusi yang Berbasis Anomali: Menganalisis pola lalu lintas jaringan dan perilaku pengguna untuk mendeteksi aktivitas yang tidak biasa atau mencurigakan.

4. Pengamanan Akses Jaringan: Pengamanan akses jaringan melibatkan langkah-langkah untuk mengendalikan siapa yang memiliki akses ke jaringan dan sumber daya jaringan. Beberapa langkah yang perlu diperhatikan dalam pengamanan akses jaringan meliputi:
   a. Autentikasi dan Otorisasi: Menerapkan mekanisme autentikasi yang kuat untuk memverifikasi identitas pengguna sebelum memberikan akses ke jaringan. Otorisasi digunakan untuk membatasi akses pengguna berdasarkan peran dan tanggung jawab mereka.
   b. Penggunaan VPN (*Virtual Private Network*): Mengimplementasikan VPN untuk mengamankan komunikasi dan mengenkripsi data yang dikirimkan melalui jaringan publik, seperti internet.

Dengan menerapkan arsitektur jaringan yang aman, menggunakan firewall dan filtrasi paket, deteksi intrusi, serta pengamanan akses jaringan yang tepat, organisasi dapat meningkatkan keamanan jaringan mereka. Hal ini membantu melindungi infrastruktur teknologi dan data sensitif dari serangan, memastikan kerahasiaan dan integritas informasi, serta menjaga ketersediaan sistem yang kritis.

6.4 Keamanan Aplikasi

Keamanan aplikasi adalah upaya untuk melindungi aplikasi perangkat lunak dari serangan dan kerentanan keamanan. Beberapa aspek penting dalam keamanan aplikasi meliputi pengujian keamanan aplikasi, pengkodean yang aman, dan penanganan kerentanan keamanan. Berikut adalah penjelasan lebih lanjut tentang masing-masing aspek:

1. Pengujian Keamanan Aplikasi: Pengujian keamanan aplikasi adalah proses untuk mengidentifikasi dan menguji kerentanan keamanan dalam aplikasi yang dikembangkan atau digunakan oleh suatu organisasi. Tujuan dari pengujian keamanan aplikasi adalah untuk mengidentifikasi kerentanan dan celah keamanan yang mungkin dapat dieksploitasi oleh penyerang. Beberapa jenis pengujian keamanan aplikasi meliputi:
    a. Pengujian Penetrasi: Mencoba mengeksploitasi kerentanan dalam aplikasi dengan cara yang sama seperti penyerang potensial.
    b. Pengujian Kerentanan: Menganalisis aplikasi untuk mencari kerentanan yang mungkin ada, seperti kerentanan umum (misalnya, injeksi SQL atau serangan XSS).
    c. Analisis Kode: Mengaudit kode aplikasi untuk mengidentifikasi kerentanan keamanan dan praktik pengkodean yang buruk.
2. Pengkodean yang Aman: Pengkodean yang aman adalah praktik untuk mengembangkan aplikasi dengan memperhatikan aspek keamanan. Beberapa langkah yang perlu diperhatikan dalam pengkodean yang aman meliputi:
    a. Validasi Input: Memverifikasi dan memvalidasi semua masukan dari pengguna untuk mencegah serangan injeksi atau serangan input lainnya.
    b. Penghindaran Kerentanan Umum: Menghindari kerentanan umum seperti injeksi SQL, serangan lintas situs, atau deserialisasi yang tidak aman.
    c. Enkripsi: Mengamankan data yang sensitif dengan menerapkan teknik enkripsi yang sesuai, baik dalam penyimpanan maupun saat data berpindah melalui jaringan.
3. Penanganan Kerentanan Keamanan: Penanganan kerentanan keamanan adalah proses mengatasi dan memperbaiki kerentanan yang ditemukan dalam aplikasi. Langkah-langkah

yang perlu dilakukan dalam penanganan kerentanan keamanan meliputi:

a. Pembaruan Rutin: Memastikan bahwa aplikasi dan komponen terkait diperbarui dengan patch keamanan terbaru untuk mengatasi kerentanan yang telah ditemukan.
b. Pemeliharaan: Melakukan pemeliharaan rutin pada aplikasi untuk memperbaiki kerentanan yang teridentifikasi, seperti memperbarui konfigurasi, menghapus atau memperbaiki kode yang tidak aman, atau memperbaiki kesalahan implementasi yang mengakibatkan kerentanan.
c. Respons Cepat terhadap Kerentanan yang Terungkap: Merespons dengan cepat terhadap kerentanan yang terungkap untuk mencegah penyerangan dan meminimalkan dampaknya.

Dengan menguji keamanan aplikasi secara menyeluruh, mengimplementasikan pengkodean yang aman, dan menangani kerentanan keamanan dengan tepat, organisasi dapat mengurangi risiko serangan pada aplikasi mereka dan melindungi data dan sistem dari kerugian yang potensial. Penting untuk menerapkan praktik pengembangan perangkat lunak yang aman dan melakukan pemantauan yang berkelanjutan terhadap kerentanan keamanan agar aplikasi tetap tahan terhadap ancaman keamanan yang terus berkembang.

6.5 Manajemen Identitas dan Akses

Manajemen identitas dan akses (*Identity and Access Management*, IAM) adalah domain keamanan yang melibatkan pengelolaan hak akses dan pengidentifikasian pengguna untuk mengontrol dan melindungi akses terhadap aset informasi.

1. Otorisasi dan Autentikasi:
    a. Autentikasi: Proses verifikasi identitas pengguna yang ingin mengakses sistem atau aset informasi. Metode autentikasi dapat meliputi penggunaan kata sandi, token, sertifikat digital, atau metode biometrik seperti pemindaian sidik jari atau pemindaian wajah.
    b. Otorisasi: Proses memberikan hak akses yang tepat kepada pengguna yang telah diotentikasi. Otorisasi memastikan bahwa pengguna hanya memiliki akses ke sumber daya atau data yang sesuai dengan peran dan tanggung jawab mereka.
2. Manajemen Hak Akses:
    a. Identifikasi dan Klasifikasi: Mengidentifikasi sumber daya atau data yang perlu dilindungi dan mengklasifikasikannya berdasarkan tingkat sensitivitas dan pentingannya.
    b. Pengaturan Hak Akses: Memberikan hak akses yang tepat kepada pengguna berdasarkan peran, tanggung jawab, dan kebutuhan bisnis. Ini melibatkan penetapan hak akses minimum yang diperlukan untuk pengguna dalam menjalankan tugas mereka.
    c. Pemantauan dan Reviu: Memantau dan melakukan peninjauan berkala terhadap hak akses pengguna untuk memastikan bahwa akses yang diberikan tetap sesuai dengan kebutuhan bisnis dan tidak ada akses yang tidak diinginkan.
3. Pengelolaan Identitas Pengguna:
    a. Pendaftaran Pengguna: Melakukan proses pendaftaran untuk membuat identitas pengguna yang unik, termasuk pengumpulan informasi pribadi dan verifikasi keaslian informasi tersebut.
    b. Pengelolaan Siklus Hidup Pengguna: Mengelola siklus hidup pengguna mulai dari pembuatan, pengaktifan,

pembaruan, hingga penghentian akun pengguna jika tidak diperlukan lagi.

c. Provisioning dan Deprovisioning: Memberikan akses ke sistem atau aplikasi yang sesuai ketika pengguna baru bergabung, dan mencabut akses ketika pengguna meninggalkan organisasi atau tidak membutuhkan lagi.

Manajemen identitas dan akses yang efektif memastikan bahwa hak akses hanya diberikan kepada pengguna yang diotentikasi, sesuai dengan peran dan tanggung jawab mereka, serta memungkinkan penggunaan yang efisien dan aman dari aset informasi. Dengan melaksanakan otorisasi dan autentikasi yang kuat, manajemen hak akses yang tepat, dan pengelolaan identitas pengguna yang baik, organisasi dapat mengurangi risiko akses yang tidak sah dan melindungi aset informasi dari penyalahgunaan atau pelanggaran.

6.6 Keamanan Operasional

Keamanan operasional adalah domain keamanan yang melibatkan kebijakan, prosedur, dan praktik operasional yang dirancang untuk melindungi aset informasi dari ancaman internal dan eksternal.

1. Kebijakan Keamanan:
    a. Penetapan kebijakan keamanan yang jelas dan komprehensif yang mengatur bagaimana aset informasi harus dikelola, diakses, dan dilindungi.
    b. Kebijakan keamanan meliputi aturan tentang penggunaan perangkat keras, perangkat lunak, jaringan, dan aplikasi yang terkait dengan aset informasi.
2. Manajemen Risiko:
    a. Identifikasi dan penilaian risiko terhadap aset informasi dan sistem yang terkait untuk mengidentifikasi ancaman potensial dan dampaknya.

b. Mengembangkan strategi mitigasi risiko yang melibatkan pengaturan prioritas, pengimplementasian kontrol keamanan, dan pengelolaan risiko secara proaktif.

3. Penanganan Insiden Keamanan:
   a. Membangun rencana respons insiden keamanan yang meliputi langkah-langkah yang harus diambil dalam menangani insiden keamanan, termasuk identifikasi, tanggapan, pengumpulan bukti, dan pemulihan.
   b. Melatih personel tentang prosedur respons insiden dan melakukan latihan simulasi insiden untuk memastikan respons yang efektif saat terjadi kejadian keamanan.
4. Pemantauan Keamanan:
   a. Melakukan pemantauan keamanan secara terus-menerus untuk mendeteksi aktivitas yang mencurigakan atau serangan yang berpotensi merugikan.
   b. Mengimplementasikan sistem pemantauan keamanan, seperti Security Information and Event Management (SIEM), yang mengumpulkan dan menganalisis log aktivitas untuk mendeteksi indikasi serangan atau pelanggaran kebijakan keamanan.

6.7 Keamanan Fisik dan Lingkungan

Keamanan fisik dan lingkungan adalah aspek penting dalam proteksi aset informasi. Ini melibatkan perlindungan fisik dari bangunan, fasilitas penyimpanan data, serta perlindungan terhadap bencana alam.

1. Keamanan Fisik Bangunan:
   a. Sistem Pengendalian Akses: Menggunakan sistem pengendalian akses seperti kunci, kartu akses, atau pengenalan biometrik untuk membatasi akses ke bangunan dan ruangan yang mengandung aset informasi penting.

b. Pengawasan CCTV: Memasang kamera pengawas yang terhubung ke sistem CCTV untuk memantau aktivitas di sekitar bangunan dan memberikan catatan visual yang dapat digunakan sebagai bukti jika terjadi pelanggaran keamanan.
c. Penjagaan Keamanan: Merekrut penjaga keamanan yang bertugas untuk menjaga keamanan bangunan dan melakukan patroli rutin.

2. Pengamanan Fasilitas Penyimpanan Data:
   a. Ruangan Pengaman: Mendesain dan mengatur ruang penyimpanan data yang memiliki lapisan keamanan tambahan, seperti pintu dan dinding yang tahan terhadap percobaan masuk paksa, serta sistem pengendalian suhu dan kelembaban yang tepat.
   b. Kunci dan Keamanan Fisik: Mengamankan ruangan penyimpanan data dengan menggunakan kunci ganda atau kunci elektronik yang hanya dapat diakses oleh pihak yang berwenang. Penggunaan lemari penyimpanan yang tahan api dan tahan air juga penting untuk melindungi data dari bencana.
3. Perlindungan Terhadap Bencana Alam:
   a. Sistem Proteksi Kebakaran: Memasang sistem deteksi kebakaran, sprinkler, dan peralatan pemadam api yang memadai untuk mencegah dan memadamkan kebakaran yang dapat merusak aset informasi.
   b. Proteksi Terhadap Air: Mengimplementasikan tindakan untuk mencegah kerusakan yang disebabkan oleh air, seperti pemasangan sistem pemadam kebocoran atau pemindahan peralatan penting ke lantai yang lebih tinggi.
   c. Perencanaan Bencana: Membuat rencana respons dan pemulihan bencana yang meliputi prosedur pengungsian, pemulihan data, dan pemulihan operasional setelah terjadinya bencana alam.

6.8 Keamanan Komunikasi

Keamanan komunikasi adalah aspek penting dalam proteksi aset informasi. Ini melibatkan perlindungan data saat transit dari satu titik ke titik lainnya. Beberapa elemen kunci dalam keamanan komunikasi meliputi:

1. Enkripsi dan Dekripsi:
    a. Enkripsi: Proses mengubah data menjadi bentuk yang tidak dapat dibaca atau dimengerti secara langsung. Ini dilakukan dengan menggunakan algoritma enkripsi dan kunci enkripsi yang khusus.
    b. Dekripsi: Proses mengembalikan data yang telah dienkripsi menjadi bentuk semula menggunakan kunci dekripsi yang sesuai. Hanya penerima yang memiliki kunci dekripsi yang dapat membaca data yang terenkripsi.
2. Protokol Keamanan:
    a. SSL/TLS (*Secure Sockets Layer*/*Transport Layer Security*): Protokol yang digunakan untuk mengamankan komunikasi antara dua entitas melalui jaringan, seperti server web dan browser.
    b. IPSec (*Internet Protocol Security*): Protokol yang mengamankan lalu lintas data pada tingkat protokol internet, menyediakan enkripsi, integritas, dan otentikasi.
    c. SSH (*Secure Shell*): Protokol yang menyediakan komunikasi yang aman dan enkripsi dalam lingkungan jaringan, khususnya untuk akses jarak jauh ke server atau perangkat.
3. Pengamanan Data Saat Transit:
    a. Tunneling: Menggunakan teknik tunneling untuk mengamankan data saat transit melalui jaringan yang tidak aman. Contohnya adalah menggunakan *Virtual Private Network* (VPN) untuk membangun koneksi terenkripsi antara dua titik.

b. Firewall: Menggunakan firewall untuk memonitor dan mengontrol lalu lintas data yang masuk dan keluar dari jaringan, serta menerapkan kebijakan keamanan yang sesuai.
c. Penyandian Pesan: Menggunakan metode penyandian pesan atau steganografi untuk menyembunyikan data sensitif di dalam pesan lainnya, sehingga hanya penerima yang dituju yang dapat mengekstrak data tersebut.

Penerapan enkripsi, penggunaan protokol keamanan yang tepat, dan pengamanan data saat transit secara efektif dapat membantu melindungi data dari pengintaian, perubahan, atau penyadapan oleh pihak yang tidak berwenang. Hal ini penting dalam mengamankan komunikasi online, seperti transaksi keuangan, pertukaran informasi sensitif, dan komunikasi bisnis yang rahasia.

6.9 Keamanan Keuangan

Dalam domain keamanan informasi, keamanan keuangan merupakan aspek penting yang melibatkan perlindungan transaksi elektronik, data keuangan, dan pencegahan kecurangan keuangan.

1. Keamanan Transaksi Elektronik:
    a. Enkripsi Data: Penggunaan enkripsi dalam mengamankan transmisi data keuangan melalui jaringan. Hal ini melibatkan penggunaan protokol keamanan seperti *Secure Sockets Layer* (SSL) atau *Transport Layer Security* (TLS) untuk melindungi informasi sensitif selama transfer.
    b. Otentikasi Pengguna: Menerapkan metode otentikasi yang kuat, seperti kata sandi yang kompleks, autentikasi multi-faktor, atau biometrik, untuk memastikan bahwa hanya pengguna yang sah yang dapat mengakses informasi keuangan.

c. Pengamanan Sistem Pembayaran: Menggunakan teknologi keamanan seperti tokenisasi atau pengamanan kartu pembayaran (*payment card security*) untuk melindungi data kartu pembayaran selama proses pembayaran elektronik.

2. Perlindungan Data Keuangan:
   a. Pengelolaan Akses: Menerapkan kontrol akses yang ketat untuk melindungi data keuangan dari akses yang tidak sah. Hal ini meliputi pengaturan hak akses, pengawasan aktivitas pengguna, dan pembatasan akses berdasarkan kebutuhan bisnis.
   b. Enkripsi Data: Mengenkripsi data keuangan yang disimpan untuk melindungi kerahasiaan dan integritasnya. Enkripsi data pada repositori penyimpanan, basis data, atau file dapat memberikan perlindungan tambahan terhadap akses yang tidak sah.
   c. Pengawasan dan Audit: Menerapkan mekanisme pemantauan dan audit yang memungkinkan pemantauan aktivitas sistem dan deteksi kejadian yang mencurigakan atau anormal terkait dengan data keuangan.
3. Pencegahan Kecurangan Keuangan:
   a. Analisis Risiko: Melakukan evaluasi risiko kecurangan keuangan untuk mengidentifikasi potensi celah atau kelemahan dalam sistem keuangan yang dapat dimanfaatkan oleh pelaku kecurangan. Hal ini dapat mencakup identifikasi dan mitigasi risiko internal dan eksternal.
   b. Kontrol Proses: Mengimplementasikan kontrol internal yang kuat untuk memastikan integritas dan validitas transaksi keuangan, termasuk pemisahan tugas, otorisasi, dan validasi data.
   c. Monitoring dan Deteksi: Melakukan pemantauan aktif terhadap transaksi keuangan untuk mendeteksi pola atau indikator kecurangan. Penggunaan analitik keuangan,

kecerdasan buatan, atau alat deteksi anomali dapat membantu mengidentifikasi perilaku yang mencurigakan atau transaksi yang tidak wajar.

d. Pelatihan dan Kesadaran: Memberikan pelatihan kepada karyawan tentang praktik keamanan keuangan, etika bisnis, dan tindakan yang harus diambil jika ada kecurigaan terhadap kecurangan keuangan.

6.10 Kepatuhan dan Hukum

Dalam domain keamanan informasi, kepatuhan terhadap peraturan dan persyaratan hukum terkait sangat penting untuk melindungi aset informasi dan menjaga privasi pengguna. Beberapa aspek yang terkait dengan kepatuhan dan hukum dalam konteks keamanan informasi meliputi:

1. Peraturan Perlindungan Data:
   a. *General Data Protection Regulation* (GDPR): Regulasi yang berlaku di Uni Eropa yang melindungi privasi dan data pribadi warga negara Uni Eropa.
   b. *California Consumer Privacy Act* (CCPA): Undang-undang California yang memberikan hak privasi tambahan kepada konsumen California dan mewajibkan perlindungan data yang lebih kuat.
   c. *Data Protection Act* (DPA): Regulasi yang mengatur perlindungan data pribadi di berbagai negara atau yurisdiksi.
2. Standar Keamanan Industri:
   a. ISO/IEC 27001: Standar internasional untuk manajemen keamanan informasi yang memberikan kerangka kerja untuk merancang, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi.
   b. Payment *Card Industry Data Security Standard* (PCI DSS): Standar keamanan yang dikembangkan oleh PCI *Security*

Standards Council untuk melindungi informasi kartu pembayaran dan transaksi.

c. NIST *Cybersecurity Framework*: Kerangka kerja yang dikembangkan oleh *National Institute of Standards and Technology* (NIST) AS untuk membantu organisasi mengelola dan mengurangi risiko keamanan siber.

3. Persyaratan Hukum Terkait:
   a. Undang-undang Perlindungan Data: Setiap negara memiliki undang-undang dan peraturan yang mengatur perlindungan data, termasuk hak individu terkait data pribadi mereka dan kewajiban organisasi dalam memproses data tersebut.
   b. Undang-undang Kekayaan Intelektual: Hukum yang melindungi hak kekayaan intelektual, termasuk hak cipta, paten, dan merek dagang yang relevan dalam konteks keamanan informasi.
   c. Peraturan Industri atau Profesi: Beberapa industri atau profesi memiliki peraturan atau kode etik sendiri yang harus diikuti untuk memastikan keamanan dan kerahasiaan informasi yang relevan.

6.11 Perencanaan dan Implementasi Keamanan

Dalam domain keamanan, perencanaan dan implementasi keamanan merupakan langkah penting dalam melindungi aset informasi. Ini melibatkan tiga aspek utama: penentuan kebutuhan keamanan, perancangan dan implementasi strategi keamanan, serta pengujian dan evaluasi keamanan.

1. Penentuan Kebutuhan Keamanan:
   a. Mengidentifikasi aset informasi yang perlu dilindungi dan menentukan tingkat sensitivitas dan nilai dari setiap aset tersebut.
   b. Menganalisis ancaman dan risiko yang mungkin dihadapi, baik dari faktor internal maupun eksternal.

c. Menentukan kebijakan dan prosedur keamanan yang sesuai dengan kebutuhan dan tujuan organisasi.
d. Melibatkan pemahaman tentang persyaratan keamanan yang ditetapkan oleh peraturan atau standar industri yang berlaku.

2. Merancang dan Mengimplementasikan Strategi Keamanan:
   a. Merancang arsitektur keamanan yang mencakup infrastruktur, teknologi, dan kontrol keamanan yang diperlukan.
   b. Memilih dan mengimplementasikan teknologi keamanan yang sesuai, seperti firewall, enkripsi, dan deteksi intrusi.
   c. Mengembangkan kebijakan, prosedur, dan panduan keamanan yang jelas untuk mengatur penggunaan, akses, dan perlindungan aset informasi.
   d. Menerapkan kontrol akses fisik dan logis yang tepat untuk mencegah akses yang tidak sah.
3. Pengujian dan Evaluasi Keamanan:
   a. Melakukan pengujian keamanan, seperti penetrasi tes (*penetration testing*) dan pengujian kerentanan (*vulnerability testing*), untuk mengidentifikasi celah keamanan yang mungkin ada dalam sistem.
   b. Melakukan audit keamanan secara berkala untuk memastikan kepatuhan terhadap kebijakan dan prosedur keamanan yang telah ditetapkan.
   c. Melakukan evaluasi keamanan secara teratur untuk mengevaluasi efektivitas kontrol keamanan yang diterapkan dan mengidentifikasi area perbaikan.
   d. Mengupdate dan meningkatkan strategi keamanan sesuai dengan perubahan teknologi, ancaman, atau persyaratan bisnis yang berlaku.

6.12 Tantangan dan Perkembangan Terkini dalam Keamanan Informasi

Tantangan dan perkembangan terkini dalam keamanan informasi mencakup berbagai aspek yang relevan dengan perkembangan teknologi dan tren terbaru. Berikut adalah beberapa poin yang mencakup tantangan dan perkembangan terkini dalam keamanan informasi:

1. Ancaman keamanan terbaru:
    a. Serangan siber yang kompleks dan canggih, seperti serangan ransomware, serangan DdoS (*Distributed Denial of Service*), dan serangan phishing yang semakin mengelabui.
    b. Ancaman dari kelompok peretas yang terorganisir dan negara-negara asing yang tertarik pada pencurian data dan informasi sensitif.
    c. Ancaman insider, yaitu ancaman yang berasal dari dalam organisasi, seperti karyawan yang tidak setia, kontraktor yang tidak tepercaya, atau kebocoran data yang disengaja.
2. Teknologi dan tren keamanan informasi terkini:
    a. Keamanan *Artificial Intelligence* (AI) dan Machine Learning (ML): Penggunaan AI dan ML dalam melawan serangan siber dan mendeteksi pola perilaku yang mencurigakan.
    b. *Internet of Things* (IoT): Keamanan yang berkaitan dengan perangkat IoT yang semakin terhubung, termasuk pengamanan perangkat, data yang dikirimkan, dan privasi pengguna.
    c. Blockchain: Penggunaan teknologi blockchain dalam memperkuat keamanan, terutama dalam konteks keamanan transaksi dan penyimpanan data yang terdesentralisasi.

d. Keamanan Big Data: Perlindungan data besar yang dikumpulkan dan dianalisis untuk menjaga kerahasiaan dan integritas data yang sensitif.
e. Keamanan cloud: Fokus pada perlindungan data yang disimpan dan diproses di lingkungan cloud, termasuk pengamanan akses, enkripsi data, dan privasi pengguna.
f. Keamanan mobile: Melindungi perangkat mobile, aplikasi, dan data yang digunakan oleh pengguna, terutama dalam hal kehilangan atau pencurian perangkat dan serangan malware mobile.

3. Keamanan dalam lingkungan cloud dan mobile:
   a. Keamanan cloud: Menangani tantangan keamanan yang terkait dengan penyimpanan, pengolahan, dan transfer data dalam lingkungan cloud, termasuk pengamanan akses, enkripsi data, pemisahan data, dan keamanan jaringan.
   b. Keamanan mobile: Perlindungan terhadap ancaman keamanan yang khusus terkait dengan perangkat mobile, seperti serangan malware, kehilangan perangkat, atau pencurian data pribadi.
   c. Pengelolaan identitas dan akses dalam lingkungan cloud dan mobile, termasuk manajemen keamanan perangkat, otentikasi ganda, dan pengelolaan hak akses.
   d. Integrasi keamanan cloud dan mobile dengan infrastruktur TI yang ada, termasuk keamanan jaringan, firewall, dan deteksi intrusi.

DAFTAR PUSTAKA

Arifin, Z. 2019. 'Keamanan dan Ancaman pada Cyberspace', pp. 1–37.

Hayaty, N. 2020. 'Buku Ajar: Sistem Keamanan', pp. 1–99.

Indrajit, Prof., R.E. 2011. 'Manajemen keamanan informasi', (1), pp. 1–19. Available at: https://doi.org/12.01.123.

Syefira Salsabila., S.Gz, M. (no date) *MODUL PROTEKSI DAN PERTUKARAN INFORMASI KESEHATAN*. Universitas Esa Unggul.

Zetmagz.com. 2022. *Apa itu Security Domain*. Available at: https://www.zetmagz.com/2022/05/apa-itu-security-domain.html.

BAB 7
INFORMATION STATES

Oleh Laila Qadriah

7.1 Pendahuluan

Kemajuan teknologi informasi yang semakin cepat sangat berpengaruh terhadap perkembangan informasi. Informasi sangatlah penting dan paling berpengaruh di era globalisasi sekarang ini. Berbagai kemudahan telah kita rasakan seperti kemudahan untuk memperoleh informasi, kemudahan dalam bertransaksi. Kemudahan ini menyebabkan pengguna biasa tertarik lebih jauh untuk menangani lebih banyak informasi baik dengan cara mentransfer, memproses, atau menyimpannya. Seperti perangkat seluler menjadi lebih mudah diakses oleh semua orang dengan biaya yang lebih murah. Teknologi jaringan yang mendasarinya memfasilitasi transfer data dengan menyediakan komunikasi yang lebih cepat dan lebih dapat diandalkan, metode pemprosesan data (seperti mengedit, mengkompres) membantu menyesuaikan format data, dan meningkatkan kapasitas penyimpanan data lebih efektif. Sejalan dengan perkembangan informasi maka masalah keamanan dan privasi dari suatu informasi juga harus diperhatikan. Keamanan informasi adalah bagaimana kita dapat mendeteksi dan mencegah adanya penipuan (*cheating*) di sebuah sistem yang berbasis informasi. Oleh karena itu diperlukan perlindungan dan perhatian terhadap informasi dan keamanan informasi serta perlu dikelola dan dikendalikan dengan baik. Terlepas dari informasi apa yang terlibat, apakah itu catatan pelanggan atau dokumentasi rahasia, ada banyak ancaman yang

membuat informasi rentan. Keamanan informasi harus diimplementasikan dan dikelola dalam organisasi untuk memastikan bahwa informasi tetap aman dan aman.

7.2 Konsep Dasar Informasi

Dalam bidang teknologi, istilah informasi bukanlah hal yang asing lagi, akan tetapi saat ini informasi dan data sering disalah artikan oleh Sebagian kalangan. Oleh karena itu perlu diketahui perbedaan antara informasi dan data serta kualitas dari informasi tersebut. Informasi merupakan data yang diolah dengan cara tertentu sehingga menjadi sesuatu yang berguna dan bermakna bagi si penerima (Laudon and Laudon, 2020). Maksudnya adalah dapat memberikan keterangan atau pengetahuan. Sehingga yang menjadi sumber informasi adalah data. Dengan kata lain, informasi adalah sebuah pengetahuan yang diperoleh dari pembelajaran, pelatihan dan pengalaman. Berdasarkan pendapat beberapa pakar, informasi didefinisikan sebagai berikut:

1. Menurut Gordon B Davis (1999), Informasi adalah data yang diolah sehingga memiliki bentuk yang berarti bagi si penerimanya. Informasi dapat digunakan dalam pengambilan keputusan, baik untuk masa sekarang atau di masa yang akan datang.
2. Menurut Burch dan Stater (1986), Informasi adalah suatu pengolahan data yang dapat menghasilkan dan memberikan pengetahuan serta pengertian.
3. Menurut George R. Tery, PhD (1958), Informasi merupakan suatu data penting yang mengandung informasi penting.
4. Menurut McFadden,dkk (1999), Informasi merupakan data yang telah diproses sehingga meningkatkan pengetahuan bagi seseorang yang menggunakan data tersebut.
5. Menurut George H. Bodnar (2000), Informasi yaitu data yang telah diolah yang dapat dijadikan dasar untuk mengambil suatu keputusan yang tepat.

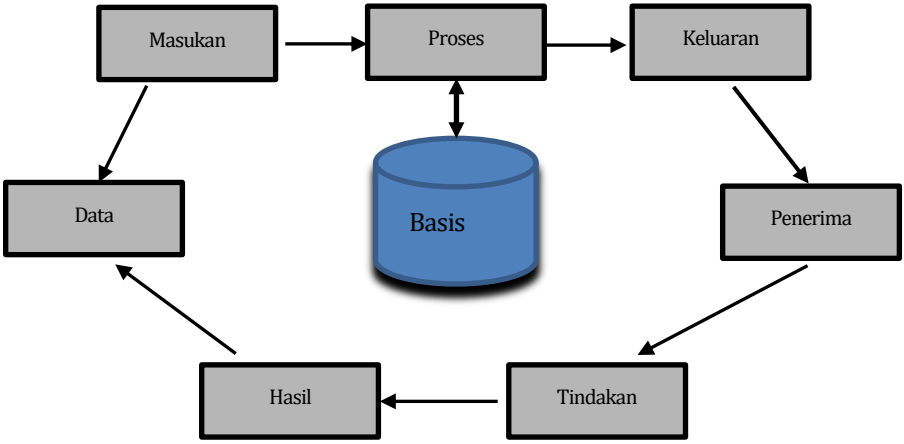
6. Menurut Anton M. Meliono (1990), Informasi merupakan data yang telah diproses dengan tujuannya adalah untuk menghasilkan sebuah keputusan.
7. Menurut Lani Sidharta (1995), Informasi merupakan data yang berguna untuk membuat keputusan.
8. Menurut Fajri (2014), informasi merupakan sebuah data yang mana telah diolah dan diubah menjadi konteks yang lebih berarti. Adanya informasi menyebabkan pengguna merasa yakin dengan keputusan yang dipilih.
9. Menurut William (2007), informasi merupakan data yang telah dimanipulasi dengan tujuan untuk pengambilan keputusan.

Dari pemaparan pakar di atas dapat diambil kesimpulan bahwa, informasi merupakan hasil dari pengolahan data dalam suatu bentuk yang lebih berarti dan bermanfaat bagi penggunanya yang menggambarkan suatu kejadian (*event*)yang nyata (*fact*) yang digunakan untuk pengambilan keputusan. Dengan kata lain sumber dari informasi adalah data. Proses perubahan data menjadi informasi dapat digambarkan sebagai berikut:

Gambar 7.1. Tranformasi data menjadi informasi
(Sumber : Edhy Sutanta, 2003)

Data yang merupakan bahan mentah dan harus diolah dengan menggunakan model pengolahan data sehingga menjadi sebuah informasi dan menghasilkan sebuah tindakan yang akan membuat sebuah data kembali. Siklus informasi (Burch dan Grudnitsi, 1989) menggambarkan pengolahan data menjadi informasi yang digambarkan dengan suatu kejadian-kejadian yang

nyata dan digunakan untuk mendapatkan suatu keputusan, sehingga menghasilkan data kembali berdasarkan tindakan hasil pengambilan keputusan. Data tersebut menjadi masukan, diproses kembali melalui sebuah model dan seterusnya membentuk suatu siklus atau disebut juga dengan siklus pengolahan data /*data processing cycle* (John Burch, 1986). Siklus informasi dapat digambarkan sebagai berikut :



Gambar 7.2. Siklus informasi
(Sumber : Jogiyanto, H.M, 2008)

Informasi yang berkualitas menurut Raymond Mc.Leod memiliki ciri-ciri sebagai berikut:

1. Akurat/tepat benar, artinya informasi yang disampaikan harus mencerminkan keadaan yang sebenarnya dan bebas dari kesalahan.
2. Andal, artinya informasi harus disajikan secara jujur dan apa adanya tanpa pengurangan, penambahan, dan perubahan.
3. Tepat waktu, informasi harus disajikan tepat waktu dan tersedia ketika informasi tersebut diperlukan serta tidak terhambat oleh apapun.

4. Relevan, informasi yang diberikan harus relevan atau memberikan manfaat yang tinggi bagi penggunanya.
5. Dapat diakses, artinya informasi harus dapat diakses secara langsung oleh penggunanya.
6. Lengkap, informasi yang diberikan harus lengkap dan dapat dipahami karena informasi yang dihasilkan akan mempengaruhi dalam pengambilan keputusan.
7. Teruji kebenarannya/*correctness*, informasi yang dihasilkan harus teruji kebenarannya atau memiliki kebenaran.
8. *Security*, informasi yang dihasilkan mempunyai nilai efektifitas dan manfaat yang lebih besar dibandingkan dengan biaya untuk mendapatkan informasi tersebut.
9. Dapat diverifikasi, artinya informasi yang diberikan dapat diuji dan dilakukan perbandingan dengan informasi yang berkaitan yang diperoleh dari pihak lain.

Menurut Edhy Susanta (2003) Nilai dari informasi (*value of information*) ditentukan berdasarkan sifatnya yaitu :

1. Kemudahan dalam mendapatkan informasi, artinya informasi dapat diperoleh dengan mudah jika sistem dengan basis datanya baik dan pengolah mampu mengolah data dengan baik untuk mendapatkan kebutuhan dari suatu informasi.
2. Luas dan lengkap, informasi akan bernilai sempurna jika mempunyai lingkup/cakupan yang luas dan lengkap. Informasi yang tidak lengkap menjadi tidak bernilai, karena tidak disajikan secara baik. Oleh karena itu, sistem harus mempunyai basis data yang cukup lengkap dan terstruktur dengan baik.
3. Ketelitian, Informasi yang tidak memiliki tingkat ketelitian yang tinggi akan menjadi informasi yang tidak bernilai, karena dapat mengakibatkan kesalahan dalam pengambilan keputusan.

4. Sesuai dengan pengguna, artinya informasi mempunyai nilai yang sempurna apabila sesuai dengan kebutuhan pengguna. Jika informasi tidak sesuai dengan kebutuhan pengguna maka informasi menjadi tidak penting atau berharga, karena tidak dapat digunakan untuk pengambilan keputusan.
5. Tepat waktu, artinya pengguna menerima informasi pada saat yang tepat. Hal ini menunjukkan bahwa informasi menjadi tidak bernilai apabila terlambat diterima oleh pengguna.
6. Kejelasan, informasi sangat dipengaruhi oleh bentuk dan format informasi. Informasi yang disajikan harus dapat dibaca dan dipahami dengan lebih mudah oleh pengguna.
7. Fleksibelitas, artinya pengguna dapat memperoleh informasi dengan mudah dan memiliki nilai fleksibel yang tinggi.
8. Dapat dibuktikan, Kebenaran dari suatu informasi sangat bergantung pada validitas dari sumber data yang akan diolah.
9. Tidak ada prasangka, artinya informasi yang disajikan tidak menimbulkan keraguan akan adanya kesalahan informasi.
10. Dapat diukur, pengukuran informasi didasari pada kebenaran data sumber yang digunakan. Dalam pengambilan keputusan membutuhkan informasi yang dapat diukur dan dapat dilacak.

Berdasarkan pendapat pakar mengenai informasi, maka secara otomatis informasi memiliki fungsi atau peran yang sangat penting terutama diera teknologi sekarang ini. Adapun fungsi dari informasi adalah :

1. Menambah pengetahuan, dengan adanya informasi akan menambah pengetahuan serta wawasan mengenai hal-hal baru sehingga dapat digunahkan sebagai bahan pertimbangan dalam proses pengambilan keputusan.

2. Sebagai Sumber berita dalam penyebaran informasi mengenai apapun.
3. Memberikan kepastian, melalui sumber informasi yang lengkap dapat mengurangi ketidakpastian atau keraguan akan hal-hal yang akan terjadi karena apa yang akan terjadi dapat diketahui sebelumnya.
4. Mengurangi resiko kegagalan, adanya informasi kemungkinan terjadi kegagalan akan dapat diantisipasi dan dikurangi dengan pengambilan keputusan yang tepat
5. Media untuk mensosialisasikan kebijakan yang ditentukan, guna memahami dengan baik dan benar sebelum diberlakukan.
6. Memberi standar, aturan-aturan dan keputusan yang tepat, artinya adanya informasi memberikan standar, aturan dan keputusan yang lebih terarah untuk mencapai sasaran dan tujuan berdasrkan informasi yang diperoleh.
7. Dasar dalam menyampaikan opini yang berbobot.

7.3 State of Information

Dalam bidang komputasi, keadaan informasi berada pada tiga posisi dalam satu waktu: informasi dalam keadaan transit (*information in transit*), informasi dalam keadaan proses (*information in process*), atau informasi dalam keadaan penyimpanan (*information in storage*). Karena informasi adalah bentuk data yang diproses, maka dua istilah ini yaitu informasi dan data akan digunakan secara saling bergantian di seluruh isi dari buku ini.

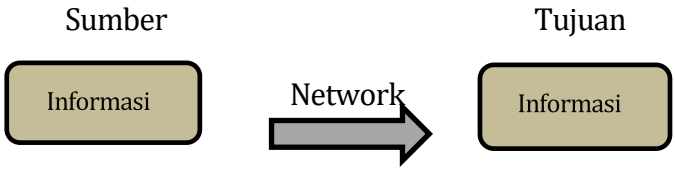
Information in transit mengacu pada status di mana jaringan dasar (*wireless*) memfasilitasi transmisi data dari satu tempat (*source*) ke tempat lain (*destination*). *Information in process* mengacu pada keadaan dimana data yang diproses mengalami perubahan dari format sumber ke format tujuan. Dan *information in storage* mengacu pada bentuk data yang sebagian yang disimpan

pada media penyimpanannya untuk referensi di masa yang akan datang. Berdasarkan deskripsi di atas menunjukkan bahwa keadaan informasi dari setiap posisi informasi berbeda satu sama lainnya, Sebagai contoh, informasi dalam transit berbeda dari informasi dalam proses dan informasi dalam penyimpanan.

Perlu juga dicatat bahwa proses suatu informasi bisa variasi dalam setiap keadaan. Seperti informasi dapat diproses terlebih dahulu dan kemudian ditransfer, atau diolah pertama dan kemudian disimpan, atau informasi yang disimpan dicari untuk pemrosesan lebih lanjut dan sebagainya. Atau dalam format yang lebih kompleks, masing-masing dari tiga keadaan informasi dapat dikombinasikan dalam urutan apapun untuk membentuk proses dari suatu informasi, seperti informasi yang diambil dari penyimpadan di dalam database dan diproses untuk menghasilkan informasi baru dan informasi baru ini kemudia ditransfer ke tujuan tertentu. Akan tetapi ketika keamanan dan privasi suatu informasi berada dalam keadaan bermasalah, masing-masing dari keadaan ini harus ditangani secara komprehensif dan eksklusif, baik dari segi keamanan jaringan, keamanan komputer, dan keamanan database (*cloud*).

7.3.1 Information in Transit

Proses pertama dari informasi adalah informasi berada dalam keadaan transit. Keadaan ini mengacu pada situasi ketika informasi yang diproses lalu ditransfer dari satu tempat (*source*) ke tempat lain (*destination*). Seperti yang ditunjukkan pada Gambar 7.3, proses informasi berada pada konteks informasi dalam keadaan transit, dimana informasi yang berada di sisi sumber ditransmisikan ke tujuan melalui jaringan yang mendasarinya. Infrastruktur jaringan yang mendasari dapat terdiri dari berbagai jenis, seperti jaringan kabel, jaringan nirkabel, dan lain-lain. Dalam hal ini, data yang akan ditransfer tidak membedakan jenis datanya, karena setiap bagian data diproses pada tingkat rendah. Ini memungkinkan transfer informasi dalam bentuk format, seperti teks sederhana, gambar tetap, film, suara, dan lain-lain.



Gambar 7.3. Information in transit

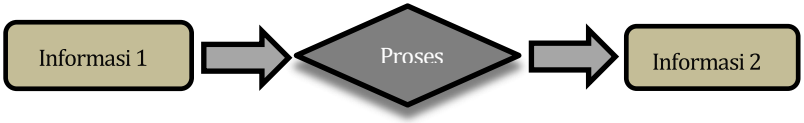
Meskipun Gambar 7.3 di atas menggambarkan bahwa informasi ditransmisikan dari sumber ke tujuan. Kondisi ini bisa berubah dimana informasi bisa ditransmisikan dari tujuan ke sumber. Dengan kata lain, sumber menjadi tujuan dan tujuan menjadi sumber. Hal ini disebabkan oleh sifat full duplex pada komunikasi.

Pada keadaan *information in transit*, jika ingin mentransfer data seharusnya format data yang akan ditransfer tidak bisa diubah. Ini menjelaskan bahwa mengapa pada Gambar 10.3, proses pengiriman informasi keduanya baik sumber dan tujuan dilakukan dengan cara yang sama. Dan untuk menjamin sifat data yang tidak berubah ini, mekanisme integritas secara intrinsik dibangun dalam sistem jaringan yang memfasilitasi informasi dalam transit. Jika sistem yang lebih kompleks dirancang dan diimplementasikan dengan menggabungkan informasi dalam transit dan informasi dalam proses, maka label dari setiap entitas informasi harus dimodifikasi. Secara khusus, entitas-entitas ini akan menandai informasi sebagai Informasi 1 dan Informasi 2 pada setiap sisi untuk menunjukkan perubahan isi informasi itu sendiri. Masalah ini akan dibahas lebih lanjut pada bagian *information in process*.
Mengirim pesan yang berisi teks, gambar, dan video dalam operasi bisnis misalnya suatu pesan dikirim dari kantor pusat ke kantor cabang adalah contoh kasus dimana informasi ditransmisikan dari sumber (kantor pusat) ke tujuan (kantor cabang).

7.3.2 Information in process

Bagian ini berfokus pada bagaimana seseorang melakukan operasi pada data untuk mengubah bentuknya. Hal ini sangat umum terjadi dimana operasi komputasi yang dilakukan untuk memproses data tidak lagi memiliki format yang asli. Sebagai contoh, seseorang dapat mengcompress data sehingga membutuhkan ruang yang lebih sedikit, dan yang lain dapat mengenkripsinya atau mengubah bentuk data menjadi kode sehingga menjadi tidak dapat dipahami oleh pihak ketiga, namun yang lain menggabungkan antara compress dan enkripsi data untuk mendapatkan manfaat dari efek gabungan keduanya.

Information in process dipresentasikan secara grafis dalam Gambar 7.4 di bawah ini, dimana serangkaian operasi diterapkan pada data input untuk menghasilkan data output. Harapan pada akhir proses dalam gambar ini adalah bahwa output (Informasi 2) akan berbeda dari input (Informasi 1). Ini adalah perbedaan dasar dari Gambar 7.3, dimana informasi di setiap sisi diharapkan sama.

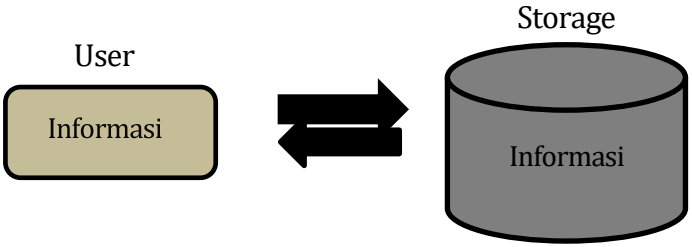


Gambar 7.4. Information in process

Dari Gambar 7.4 terlihat bahwa entitas-entitas ditandai sebagai Informasi 1 dan Informasi 2 pada setiap sisi, hal ini untuk menunjukkan perubahan atau perbedaan isi informasi 1 dan informasi 2 itu sendiri.

7.3.3 Information in storage

Information in storage merupakan keadaan dimana ketika informasi berada pada media penyimpanannya yang dipilih untuk bisa dimanfaatkan pada masa yang akan datang. Gambar 7.5 menggambarkan keadaan terakhir informasi yang disebut informasi dalam penyimpanan (*Information in storage*).



Gambar 7.5. Information in storage

Proses ini bertujuan untuk memastikan bahwa informasi tetap aman dalam media penyimpanannya dan disamping itu, tidak ada pihak lain yang tidak sah dapat mengaksesnya. Upaya ini melibatkan otentikasi pengguna yang dapat mengakses informasi, serta keutuhan dari suatu informasi yang disimpan. Persyaratan untuk menjaga data tetap utuh, yaitu dengan mencegah keutuhanya saat dilakukan penyimpanan, menjelaskan mengapa informasi ditandai sama di kedua sisi yaitu untuk pengguna dan penyimpanan seperti yang terlihat pada Gambar 7.5. Ini merupakan hal yang sama seperti yang disebutkan pada informasi dalam transit, seperti yang digambarkan dalam Gambar 7.3. Namun, karena informasi dalam proses secara intrinsik mengubah format data, label informasi pada setiap sisi proses berbeda untuk informasi diproses (lihat Gambar 7.4).

Berbagai media penyimpanan data yang tersedia contonya informasi dapat disimpan di dalam database lokal atau cloud, terutama ketika penyimpanan lokal tidak cukup untuk menampung data yang lebih besar. Setelah disimpan, informasi biasanya diakses lagi untuk tujuan pencarian, menjelaskan bentuk full duplex komunikasi antara pengguna dan penyimpanan. Adapun media penyimpanan, berbagai pilihan dimungkinkan: Informasi dapat disimpan di database lokal, atau di cloud, terutama ketika storage lokal tidak cukup untuk menampung sejumlah data besar. Setelah disimpan, informasi biasanya diakses lagi untuk

tujuan pencarian, menjelaskan bentuk duplex lengkap komunikasi antara pengguna dan penyimpanan. Sebagai contoh, seseorang dapat menyimpan foto liburan keluarga di ponselnya dan kemudian memutuskan untuk menyimpannya di DVD dengan tujuan untuk mengalokasikan lebih banyak ruang di penyimpanan ponselnya.

DAFTAR PUSTAKA

AditiaRamadhani. 2018. Keamanan Informasi. *Nusantara Journal of Information and Library Studies (N-JILS)*, 1(1), 39-51.

DeckyHenarsyah, dkk. 2022. *Manajemen Sistem Informasi.* Padang: Global Eksekutif Teknologi.

EdiVictor, H. 2012. *Jaringan Komputer*. Yogyakarta: Penerbit Andi.

EdiSusanta. 2003. *Sistem Informasi Manajemen.* Yogyakarta: Penerbit Andi.

Fauziah, Y. 2014. Tinjauan Keamanan Sistem Pada Teknologi Cloud Computing. *Jurnal Informatika Ahmad Dahlan*, 8(1), 103259. https://www.neliti.com/publications/103259/tinjauan-keamanan-sistem-pada-teknologi-cloud-computing

Gordon B. Davis. 2002. *Kerangka Dasar Sistem Informasi Manajemen.* Makassar: PT. Pustaka Binaman Pressindo.

Hariyanto, S. 2016. Sistem Informasi Manajemen. *In Sistem Informasi Manajemen*, 09 (01), 80.

https://jurnalunita.org/index.php/publiciana/article/viewFile/75/69

HM Jogiyanto. 2008. *Metodelogi Penelitian Sistem Informasi.* Yogyakarta: Andi Offeset.

IlhamPrisgunanto. 2018. Pemaknaan arti informasi di era digital. *WACANA: Jurnal Ilmiah Ilmu Komunikasi*, 17(2), 143-151.

https://journal.moestopo.ac.id/index.php/wacana/article/view/599

Irwansyah, E., & Moniaga, J. V. 2014. *Pengantar Teknologi Informasi*. Deepublish.

KasmanRukun, & Herawan, H. 2018. Sistem Informasi Berbasis Expert System. Deepublish.

Laudon, K.C., Laudon, J.P. 2020. *Management Information Systems*: *Managing the Digital Firm*, 16th ed. Pearson Education, New Jersey.

Regyna, T. F., Agustina, D., & Pramadista, F. N. 2022. *Sistem Manajemen Keamanan Informasi*. OSF Preprint.
SriAti, Nurdien, K., & Taufik, A. 2014. *Pengantar Konsep Informasi, Data, dan Pengetahuan*. Universitas Terbuka, 230.

BAB 8
FOUNDATIONS INFORMATION SECURITY

Oleh Sayed Achmady

8.1 Pendahuluan

Penggunaan teknologi informasi telah merasuk ke dalam hampir setiap aspek kehidupan kita, mulai dari bisnis hingga kehidupan pribadi. Namun, dengan kemajuan ini juga tidak tertutup kemungkinan akan risiko keamanan yang serius. Inilah sebabnya mengapa fondasi keamanan informasi sangat penting. Memahami konsep dasar dan aspek-aspek keamanan informasi adalah langkah awal yang sangat diperlukan untuk melindungi sistem dan data kita dari ancaman yang ada.

Gambar 8.1. Keamanan Informasi
(Sumber: www.wakool.id)

Apa itu Keamanan Informasi?

Keamanan Sistem Informasi Menurut (G.J. Simons, 2018) adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya celah di sebuah sistem yang berbasis informasi. Keamanan informasi mencakup praktik dan langkah-langkah yang diambil untuk melindungi informasi dari akses dan penggunaan yang tidak sah atau tidak diinginkan. Tujuan utama keamanan informasi adalah memastikan kerahasiaan, integritas, dan ketersediaan informasi.

8.2 Aspek-Aspek Fondasi Keamanan Informasi

Aspek-aspek fondasi keamanan informasi adalah elemen-elemen penting yang harus dipahami dan diterapkan untuk menjaga keamanan informasi. Berikut ini adalah beberapa aspek yang harus diperhatikan dalam fondasi keamanan informasi:

1. **Kebijakan Keamanan:** Kebijakan keamanan adalah panduan tertulis yang mengatur praktik dan prosedur keamanan informasi dalam suatu organisasi. Kebijakan ini mencakup aturan-aturan terkait penggunaan yang tepat dari sistem, perlindungan data sensitif, kebijakan akses, dan tanggung jawab pengguna.
2. **Manajemen Risiko:** Manajemen risiko melibatkan identifikasi, penilaian, dan penanganan risiko keamanan informasi. Ini mencakup mengidentifikasi ancaman potensial, mengevaluasi kerentanan sistem, dan mengambil langkah-langkah untuk mengurangi risiko melalui pemilihan kontrol keamanan yang tepat.
3. **Keamanan Fisik:** Keamanan fisik melibatkan perlindungan terhadap akses fisik yang tidak sah ke perangkat keras, infrastruktur jaringan, dan fasilitas yang mengandung informasi sensitif. Ini termasuk pengamanan ruang *server*,

penggunaan kartu akses, pengawasan CCTV, dan tindakan keamanan fisik lainnya.

4. **Keamanan Jaringan**: Keamanan jaringan melibatkan langkah-langkah untuk melindungi jaringan komputer dari serangan dan akses yang tidak sah. Ini mencakup penggunaan *firewall*, deteksi dan pencegahan intrusi, pengamanan nirkabel, dan konfigurasi jaringan yang aman.
5. **Kriptografi:** Kriptografi adalah teknik untuk melindungi informasi dengan mengenkripsi data sehingga hanya penerima yang dituju yang dapat membacanya. Ini melibatkan penggunaan algoritma enkripsi yang kuat dan pengelolaan kunci kriptografi yang aman.
6. **Keamanan Aplikasi:** Keamanan aplikasi melibatkan perlindungan terhadap kerentanan dan serangan yang terkait dengan aplikasi perangkat lunak. Ini termasuk mengimplementasikan praktik pengembangan yang aman, melakukan pengujian keamanan aplikasi, dan pemantauan terhadap ancaman yang berkaitan dengan kerentanan aplikasi.
7. **Kesadaran Pengguna:** Kesadaran pengguna adalah aspek penting dalam fondasi keamanan informasi. Mengedukasi pengguna tentang praktik keamanan yang baik, seperti penggunaan kata sandi yang kuat, menghindari serangan phishing, dan melaporkan aktivitas yang mencurigakan, sehingga dapat membantu mengurangi risiko keamanan yang disebabkan oleh kesalahan manusia.
8. **Manajemen Kejadian Keamanan:** Manajemen kejadian keamanan melibatkan respon terhadap insiden keamanan dan pemulihan setelah serangan terjadi. Ini mencakup menyusun rencana respon insiden, melacak dan menyelidiki serangan, serta memulihkan sistem dan data pasca terkena dampak.

8.3 Manajemen Keamanan Informasi

Manajemen Keamanan Informasi adalah sebuah proses yang melibatkan perencanaan, implementasi, pengawasan, dan pemeliharaan untuk melindungi informasi yang penting dan sensitif dalam sebuah organisasi. Tujuan utama dari manajemen keamanan informasi adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi agar tetap terlindungi dari ancaman dan risiko keamanan.

Beberapa aspek penting yang tercakup dalam manajemen keamanan informasi meliputi:

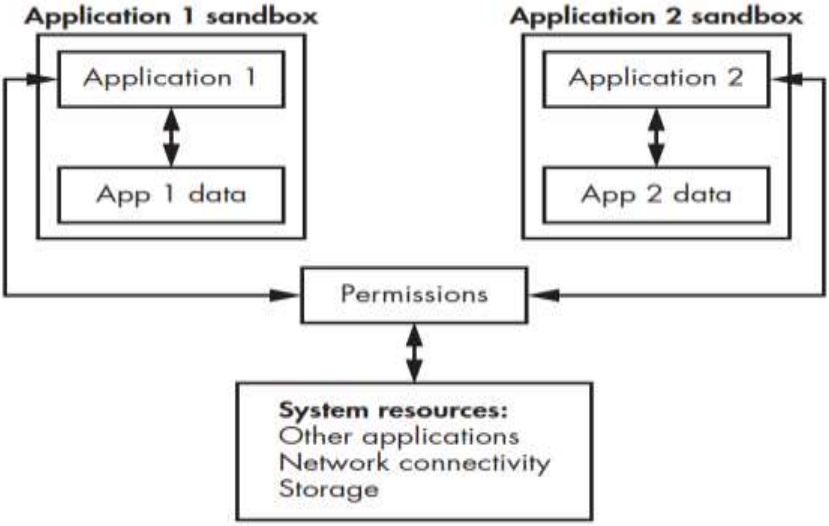
1. **Penilaian Risiko:** Identifikasi dan penilaian risiko yang mungkin terjadi terhadap informasi yang dimiliki oleh organisasi. Hal ini dapat mengidentifikasi aset informasi yang berharga, mengevaluasi potensi ancaman, dan menganalisis kerentanan yang ada.
2. **Kebijakan Keamanan Informasi:** Penetapan kebijakan dan prosedur yang jelas untuk melindungi informasi. Kebijakan ini harus mencakup kebijakan penggunaan *password*, kebijakan penggunaan perangkat seluler, kebijakan akses data, dan sebagainya.
3. **Penerapan Kontrol Keamanan:** Mengimplementasikan langkah-langkah keamanan yang relevan untuk melindungi informasi. Ini meliputi penggunaan teknologi keamanan seperti *firewall*, enkripsi data, antivirus, sistem deteksi intrusi, dan tindakan fisik seperti pengendalian akses fisik ke ruangan yang berisi informasi sensitif.
4. **Pelatihan dan Kesadaran Keamanan:** Memberikan pelatihan kepada karyawan mengenai praktik keamanan informasi yang baik, seperti cara mengelola *password* yang kuat, mengenali serangan phishing, dan menjaga kerahasiaan informasi.

5. **Manajemen Kejadian Keamanan:** Merespons dan mengelola insiden keamanan yang mungkin terjadi, seperti serangan malware, pencurian data, atau pelanggaran keamanan lainnya. Ini melibatkan identifikasi, respons cepat, investigasi, dan pemulihan dari insiden tersebut.
6. **Pemantauan dan Audit Keamanan:** Melakukan pemantauan terus-menerus terhadap sistem keamanan, serta melakukan audit keamanan secara rutin untuk memastikan kepatuhan terhadap kebijakan dan prosedur keamanan yang telah ditetapkan.
7. **Pemulihan dan Perencanaan Kontinuitas:** Mempersiapkan rencana pemulihan untuk mengatasi kehilangan data atau sistem yang parah akibat bencana alam, serangan siber, atau kejadian tidak terduga lainnya. Selain itu, merencanakan langkah-langkah untuk menjaga kelangsungan operasional bisnis dalam situasi darurat.

Manajemen Keamanan Informasi adalah pendekatan yang holistik untuk melindungi informasi dari ancaman dan risiko. Dengan menerapkan praktik-praktik keamanan yang baik, maka akan dapat menjaga kerahasiaan, integritas, dan ketersediaan informasi.

8.4 Otorisari dan Akses Kontrol

Otorisasi dan akses kontrol adalah komponen penting dari sistem keamanan yang dapat membantu melindungi informasi, sistem, dan sumber daya sensitif dari akses atau penggunaan yang tidak sah. Langkah-langkah ini memastikan bahwa hanya individu atau entitas yang berwenang yang dapat mengakses sumber daya tertentu atau melakukan tindakan tertentu dalam suatu sistem. Proses Otorisasi dan akses kontrol dapat dilihat pada gambar 12.2 berikut:



Gambar 8.2. Alur Otorisasi dan Akses Kontrol

Otorisasi merujuk pada proses yang memberikan atau menolak hak akses kepada pengguna, berdasarkan identitas dan izin yang diberikan kepada mereka. Ini melibatkan penentuan tindakan apa yang dapat dilakukan oleh pengguna, data apa yang dapat diakses, dan dalam kondisi bagaimana mereka dapat melakukannya.

Berikut ini adalah beberapa konsep terkait dengan keamanan otorisasi dan akses kontrol :

1. **Identifikasi dan Otentikasi:** Sebelum memberikan akses, pengguna harus terlebih dahulu mengidentifikasi diri mereka (memberikan nama pengguna atau ID) dan mengotentikasi identitas mereka (memverifikasi kredensial mereka, seperti kata sandi, data biometrik, atau token keamanan). Proses ini memastikan bahwa pengguna adalah orang yang mereka klaim.
2. ***Role-Based Access Control (RBAC)*:** RBAC adalah model akses kontrol yang banyak digunakan yang menetapkan

izin berdasarkan peran pengguna dalam sebuah organisasi. Pengguna dikelompokkan ke dalam peran, dan setiap peran terkait dengan seperangkat izin. Ini memudahkan administrasi dengan mengelola akses secara individu untuk setiap pengguna.

3. **Daftar Akses kontrol (ACL):** ACL adalah daftar atau matriks yang menentukan hak akses atau izin yang diberikan kepada pengguna individu atau grup untuk sumber daya tertentu. Mereka menentukan siapa yang dapat melakukan tindakan apa pada sumber daya (misalnya, membaca, menulis, menjalankan) dan membantu menentukan keputusan otorisasi.
4. **Otentikasi Dua Faktor (2FA) dan Otentikasi Multi-Faktor (MFA):** Mekanisme ini menyediakan lapisan keamanan tambahan dengan meminta pengguna untuk memberikan dua atau lebih faktor otentikasi untuk mendapatkan akses. Faktor ini dapat meliputi sesuatu yang diketahui pengguna(kata sandi), sesuatu yang dimiliki (token keamanan), atau sesuatu yang mereka miliki (data biometrik).
5. **Jejak Audit dan Pencatatan:** Pencatatan dan pemantauan aktivitas akses dapat membantu mendeteksi dan menyelidiki insiden keamanan. Dengan mencatat informasi seperti tindakan pengguna, akses sumber daya, dan peristiwa sistem, jejak audit memungkinkan tim keamanan untuk mengidentifikasi ancaman potensial atau pelanggaran kebijakan.
6. **Pencabutan Hak Akses:** Ketika hak pengguna tidak lagi diperlukan atau jika akses mereka diretas, pencabutan hak akses untuk memastikan bahwa izin mereka telah dihapus. Hal ini dapat mencegah akses tidak sah oleh mantan karyawan atau akun yang diretas.
7. **Kebijakan Kata Sandi Aman:** Menentukan kebijakan kata sandi yang kuat, seperti meminta kata sandi yang

kompleks, pergantian kata sandi secara berkala, dan penyimpanan kata sandi dalam bentuk terenkripsi, mengurangi risiko akses tidak sah seperti menebak atau memecahkan kata sandi.

8. **Enkripsi:** Mengenkripsi data sensitif untuk memastikan bahwa jika akses tidak sah terjadi, data tetap tidak terbaca dan tidak dapat digunakan. Enkripsi dapat melindungi data baik saat tidak digunakan (disimpan pada perangkat penyimpanan) maupun saat dalam perjalanan (selama komunikasi).

Menerapkan langkah-langkah otorisasi dan akses kontrol yang kuat membutuhkan kombinasi kontrol teknis, kebijakan keamanan, dan kesadaran pengguna. Evaluasi, pembaruan, dan pemantauan secara berkala sangat penting untuk mempertahankan keamanan akses kontrol dan melindungi terhadap ancaman yang terjadi.

8.5 Audit dan Akuntabilitas

Audit dan akuntabilitas adalah komponen penting dari sistem keamanan yang dapat membantu memastikan integritas, kepatuhan, dan transparansi dalam operasi suatu sistem. Langkah-langkah ini melibatkan pemantauan, analisis, dan pencatatan aktivitas dalam suatu sistem untuk mendeteksi insiden keamanan yang terjadi dan menilai kepatuhan terhadap kebijakan dan peraturan.

Berikut ini adalah beberapa konsep terkait dengan audit dan akuntabilitas keamanan:

1. **Audit *Trails*:** Audit *trails* adalah catatan atau log yang dapat mencatat informasi terperinci tentang aktivitas pengguna, peristiwa sistem, dan akses sumber daya. Sehingga memungkinkan tim keamanan untuk

merekonstruksi dan menganalisis aktivitas untuk tujuan pemantauan, pemecahan masalah, dan penyelidikan.

2. **Pencatatan dan Pemantauan:** Pencatatan yang sistematis terhadap peristiwa dan aktivitas yang relevan dengan keamanan. Pemantauan yang mengacu pada pengamatan dan analisis berkelanjutan terhadap log dan sumber data relevan lainnya secara real-time. Praktik ini dapat membantu mengidentifikasi insiden keamanan, pelanggaran kebijakan, atau aktivitas yang mencurigakan dengan cepat.
3. **Manajemen Informasi dan Peristiwa Keamanan (SIEM):** Mengumpulkan, menghubungkan, dan menganalisis data log dari berbagai sumber daya, termasuk perangkat jaringan, *server*, dan aplikasi. Menyediakan pemantauan terpusat, deteksi ancaman, dan kemampuan respon terhadap insiden untuk meningkatkan visibilitas keamanan secara keseluruhan.
4. **Audit Kepatuhan:** Audit kepatuhan yang melibatkan penilaian kepatuhan organisasi terhadap hukum, peraturan, standar industri, dan kebijakan internal yang relevan. Auditor meninjau proses, kontrol, dan catatan untuk memastikan kepatuhan dan mengidentifikasi kesenjangan atau pelanggaran yang perlu ditangani.
5. **Audit Akses:** Audit akses yang berfokus pada peninjauan dan analisis aktivitas akses pengguna dan izin untuk mendeteksi upaya akses yang tidak sah atau berlebihan. Ini dapat membantu kontrol akses diimplementasikan dengan benar dan pengguna diberikan hak akses yang sesuai.
6. **Audit Konfigurasi:** Audit konfigurasi yang melibatkan verifikasi integritas dan keamanan konfigurasi sistem, seperti sistem operasi, perangkat jaringan, dan aplikasi. Ini memastikan bahwa sistem dikonfigurasi dengan benar, dan pengaturan keamanan sesuai dengan praktik terbaik.

7. **Akuntabilitas Pengguna**: Akuntabilitas pengguna mengacu pada individu yang bertanggung jawab atas tindakan mereka dalam suatu sistem. Setiap pengguna harus memiliki pengenal yang unik, dan aktivitas mereka dapat ditelusuri melalui audit *trails*. Sehingga dapat membantu mencegah perilaku jahat, karena pengguna menyadari bahwa tindakan mereka dapat dikaitkan dengan identitas mereka.
8. **Respons dan Penyelidikan:** Data audit dan akuntabilitas memainkan peran penting dalam proses respon dan penyelidikan insiden. Ketika terjadi insiden keamanan, audit *trails* dan *log* dianalisis untuk memahami sifat insiden, menentukan cakupannya, dan mengidentifikasi penyebab akar masalah.

DAFTAR PUSTAKA

Angel R. Otero. 2018. *Information Technology Control and Audit.*

David Salomon. 2006. *Foundations of Computer Security.*

G.J. Simons. 2018. *Keamanan Sistem Informasi.*

Jule Hintzbergen, Hans Baars, André Smulders, Kees Hintzbergen. 2015. *Foundations of Information Security Based on ISO27001 and ISO27002.*

Jason Andress. 2019. *Foundations of Information Security.*

Killcrece, Georgia, Klaus-Peter Kossakowski, Robin Ruefle dan Mark Zajicek. 2003. *Organizational Models for Computer Security Incident Response Teams(CSIRTs).*

Matthew Strebe. 2006. *Network Security Foundations.*

Shimeall, Tim dan Phil Williams. 2002. *Models of Information Security Trend Analysis. Pittsburgh: CERT Analysis Center.*

Stuart Jacobs. 2015. *Engineering Information Security.*

Tim Rains. 2020. *Cybersecurity Threats, Malware Trends, and Strategies.*

BAB 9
SECURITY MODELS

Oleh Moh. Safii

9.1 Pendahuluan

Di era digital ini, informasi menjadi salah satu aset yang paling berharga bagi organisasi. Informasi yang disimpan dan dikelola dengan baik dapat memberikan keunggulan kompetitif yang signifikan. Misalnya, data pelanggan yang terkumpul dari berbagai sumber dapat memberikan wawasan yang berharga tentang preferensi dan kebutuhan pelanggan. Informasi semacam ini memungkinkan organisasi untuk mengembangkan strategi pemasaran yang lebih efektif, meningkatkan kepuasan pelanggan, dan menciptakan hubungan yang lebih kuat.

Selain itu, informasi juga dapat menjadi fondasi bagi pengambilan keputusan yang baik. Organisasi yang mampu mengumpulkan, menganalisis, dan memanfaatkan informasi dengan tepat dapat membuat keputusan yang lebih cerdas dan lebih terinformasi. Data historis, tren pasar, atau analisis kompetitor dapat memberikan pandangan yang dalam dan membantu dalam merencanakan strategi bisnis jangka panjang dan jangka pendek. Dengan demikian, informasi menjadi alat yang kuat dalam menghadapi perubahan dan ketidakpastian dalam lingkungan bisnis.

Informasi juga merupakan aset yang vital dalam menjaga kepatuhan dan keamanan. Di berbagai sektor, ada peraturan dan standar yang mengharuskan organisasi untuk melindungi informasi yang bersifat sensitif. Misalnya, dalam industri keuangan, ada regulasi ketat yang mengatur perlindungan data keuangan dan pribadi pelanggan. Melanggar peraturan tersebut dapat

berdampak serius, termasuk sanksi hukum dan reputasi yang rusak. Oleh karena itu, perlindungan informasi menjadi penting dalam menjaga kepatuhan hukum dan menjaga kepercayaan pelanggan.

Informasi juga dapat menjadi sumber daya yang berharga dalam inovasi dan pengembangan produk. Dengan memanfaatkan informasi yang ada, organisasi dapat mengidentifikasi peluang baru, mengembangkan produk yang lebih baik, dan meningkatkan efisiensi operasional. Dalam lingkungan bisnis yang kompetitif, kemampuan untuk mengumpulkan, menganalisis, dan menginterpretasikan informasi dengan cepat dapat menjadi keuntungan yang signifikan dalam menciptakan inovasi dan memimpin pasar.

Terakhir, informasi adalah aset yang rentan terhadap ancaman dan serangan. Dalam dunia yang semakin terhubung secara digital, risiko keamanan informasi semakin meningkat. Ancaman seperti peretasan, malware, pencurian identitas, atau serangan siber dapat menyebabkan kerugian finansial, kerusakan reputasi, atau pelanggaran privasi yang serius. Oleh karena itu, perlindungan aset informasi menjadi kunci untuk menjaga kontinuitas bisnis dan menjaga kepercayaan para pemangku kepentingan.

Pengantar pada security models dalam proteksi aset informasi melibatkan penggunaan kerangka atau metode yang menyediakan pendekatan sistematis dalam melindungi aset informasi organisasi dari akses, pengungkapan, perubahan, atau penghancuran yang tidak sah.

Security models membantu dalam merumuskan dan mengimplementasikan kebijakan, prosedur, dan teknologi keamanan untuk mengurangi risiko dan memastikan kerahasiaan, integritas, dan ketersediaan informasi. Model-model ini menyediakan kerangka kerja untuk mengelola dan melindungi aset informasi berharga dengan cara yang terstruktur.

Dalam konteks proteksi aset informasi, *security models* menyediakan panduan dan kontrol yang terstruktur untuk mengatasi ancaman dan risiko keamanan yang ada. Model-model ini berfokus pada aspek-aspek penting dalam keamanan informasi seperti kerahasiaan, integritas, dan ketersediaan.

Beberapa *security models* yang umum digunakan dalam proteksi aset informasi termasuk CIA Triad, Bell-LaPadula Model, Biba Model, *Clark-Wilson Model*, NIST *Cybersecurity Framework*, dan ISO/IEC 27001. Setiap model ini memiliki pendekatan unik untuk mengatasi kebutuhan keamanan informasi, seperti menjaga kerahasiaan informasi sensitif, memastikan integritas data, dan mengelola risiko keamanan dengan metode yang terstruktur.

Pemilihan security model yang tepat tergantung pada kebutuhan dan konteks keamanan organisasi. Organisasi harus mengevaluasi risiko yang mereka hadapi, kebijakan keamanan yang perlu dipatuhi, dan persyaratan kepatuhan lainnya untuk memilih model atau kombinasi model yang sesuai dengan kebutuhan mereka.

Dengan menerapkan *security models* yang tepat, organisasi dapat mengurangi risiko keamanan informasi, melindungi aset informasi dari ancaman, dan memastikan kerahasiaan, integritas, dan ketersediaan informasi yang penting bagi keberlanjutan dan sukses organisasi.

9.2 Security Models

Security models adalah kerangka atau struktur konseptual yang digunakan untuk merancang dan menerapkan langkah-langkah keamanan dalam sistem komputer dan jaringan. Model-model ini membantu dalam pemahaman dan pengelolaan risiko keamanan secara sistematis. Mereka menyediakan pendekatan terstruktur untuk memahami aspek keamanan yang berbeda dan memberikan panduan untuk merancang kebijakan dan kontrol keamanan yang efektif.

Secara umum, security models menggambarkan aturan, prinsip, dan mekanisme yang diperlukan untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan sistem. Mereka dapat berfokus pada aspek-aspek tertentu seperti kerahasiaan (seperti *Bell-LaPadula*), integritas (seperti Biba), atau konsistensi data (seperti Clark-Wilson). Model-model ini membantu dalam merancang sistem keamanan yang tepat dengan mempertimbangkan kebutuhan dan tujuan organisasi. Setiap security model memiliki karakteristik dan prinsip khususnya sendiri. Misalnya, model Bell-LaPadula menggunakan tingkatan keamanan dan menerapkan prinsip "no read up, no write down" untuk melindungi informasi yang sensitif dari akses yang tidak sah. Di sisi lain, model Clark-Wilson fokus pada integritas data dengan menggunakan kontrol transaksi dan pemisahan tugas untuk memastikan keakuratan dan keandalan data.

Model-model keamanan juga terus berkembang untuk mengakomodasi tantangan dan kebutuhan baru dalam era digital yang terus berubah. Misalnya, dengan semakin kompleksnya lingkungan IT, model-model seperti *Attribute-Based Access Control* (ABAC) telah muncul untuk memberikan kontrol akses yang lebih fleksibel berdasarkan atribut yang terkait dengan pengguna, objek, dan lingkungan.

Pentingnya mempelajari security models menurut para pakar IT dunia barat dapat diuraikan dalam beberapa aspek utama:

1. Perlindungan terhadap Ancaman Keamanan: Para pakar IT dunia barat memahami bahwa ancaman keamanan terus berkembang dan semakin kompleks. Dengan mempelajari security models, para profesional IT dapat mengidentifikasi dan mengatasi celah keamanan yang mungkin ada dalam sistem mereka. Mereka dapat menerapkan model-model keamanan yang tepat untuk melindungi data dan infrastruktur mereka dari serangan dan ancaman berbahaya.

2. Kepatuhan Regulasi dan Kebijakan: Para pakar IT dunia barat memahami pentingnya mematuhi regulasi dan kebijakan yang berkaitan dengan keamanan informasi, seperti GDPR (*General Data Protection Regulation*) di Uni Eropa atau HIPAA (*Health Insurance Portability and Accountability Act*) di Amerika Serikat. Dengan mempelajari security models, mereka dapat mengembangkan sistem keamanan yang sesuai dengan persyaratan regulasi dan memastikan bahwa data dan privasi pengguna dilindungi dengan benar.
3. Pengelolaan Risiko: Studi tentang *security models* membantu para profesional IT dalam memahami dan mengelola risiko keamanan dengan lebih baik. Mereka dapat mengidentifikasi potensi ancaman, menganalisis kerentanan sistem, dan menerapkan kontrol keamanan yang efektif untuk mengurangi risiko. Dengan demikian, mereka dapat meminimalkan dampak serangan keamanan dan melindungi aset organisasi dari kerugian yang mungkin timbul.
4. Desain Sistem yang Aman: *Security models* memberikan panduan bagi para profesional IT dalam merancang sistem yang aman secara efektif. Dengan memahami konsep dan prinsip yang mendasari model-model keamanan, mereka dapat mengintegrasikan kontrol keamanan yang tepat dalam arsitektur sistem mereka. Ini membantu dalam mencegah serangan, memperkuat keamanan secara keseluruhan, dan membangun sistem yang dapat diandalkan dan terpercaya.
5. Respons Terhadap Kejadian Keamanan: Kejadian keamanan seperti pelanggaran data atau serangan cyber dapat terjadi kapan saja. Dalam hal ini, pemahaman tentang *security models* memungkinkan para profesional IT untuk merespons dengan cepat dan efektif. Mereka dapat menerapkan langkah-langkah pemulihan, menganalisis

kerentanan yang diekspos, dan mengidentifikasi area yang perlu diperkuat untuk mencegah insiden serupa di masa depan.

9.2.1 Model Bell-LaPadula

Model Bell-LaPadula adalah salah satu model dalam konsep security models yang digunakan untuk menganalisis, merancang, dan mengimplementasikan kebijakan keamanan dalam sistem informasi. Model ini mengacu pada prinsip kerahasiaan dan mengatur akses ke data dan sumber daya berdasarkan label keamanan yang diberikan pada setiap subjek dan objek dalam sistem(Bell, 1996).

Dalam Model Bell-LaPadula, setiap subjek dan objek diberikan label keamanan yang terdiri dari dua bagian: level keamanan dan kategori keamanan. Level keamanan menggambarkan tingkat keamanan subjek atau objek, sementara kategori keamanan mengidentifikasi jenis informasi yang dapat diakses oleh subjek tersebut. Terdapat tiga aturan utama dalam model ini: aturan *No Read Up* (NRU), aturan *No Write Down* (NWD), dan aturan *Simple Security Property* (SSP)(Cutinha, 2023).

Aturan NRU menyatakan bahwa subjek dengan level keamanan yang lebih rendah tidak diizinkan untuk membaca informasi dari objek dengan level keamanan yang lebih tinggi. Hal ini memastikan bahwa informasi rahasia tidak dapat bocor atau diakses oleh subjek yang tidak berhak(R. Zhang *et al.,* 2021). Aturan NWD menyatakan bahwa subjek dengan level keamanan yang lebih tinggi tidak boleh menulis informasi ke objek dengan level keamanan yang lebih rendah. Ini mencegah penyebaran informasi sensitif ke entitas yang memiliki tingkat keamanan yang lebih rendah (Tang *et al*., 2018).

Selain itu, aturan SSP menetapkan bahwa subjek hanya diizinkan untuk mengakses objek jika level keamanan subjek sama atau lebih rendah dari level keamanan objek. Ini menghindari konflik keamanan dan memastikan bahwa subjek hanya dapat

mengakses informasi yang sesuai dengan tingkat keamanannya(Yang *et al.,* 2021). Dengan menggabungkan ketiga aturan ini, Model Bell-LaPadula menyediakan kerangka kerja yang ketat untuk mencegah pelanggaran keamanan dan menjaga kerahasiaan informasi dalam sistem informasi(Roslan *et al.,* 2018). Rujukan primer tentang kajian model ini dapat dibaca lengkap pada sumber berikut.

Lampson, B. W. (1974). Protection. ACM SIGOPS Operating Systems Review, 8(1), 18-24.

Bell, D. E., & LaPadula, L. J. (1976). Secure computer systems: Unified exposition and multics interpretation. MITRE Corp Bedford MA.

9.2.2 Model Biba

Model Biba adalah salah satu model dalam konsep keamanan komputer yang dirancang untuk menjaga kerahasiaan dan integritas data dalam sebuah sistem(G. Liu *et al.,* 2015). Model ini dinamai dari penulisnya, Ken Biba, dan diperkenalkan pada tahun 1977. Tujuan utama dari Model Biba adalah mencegah aliran informasi yang tidak sah dari objek yang memiliki tingkat keamanan yang lebih rendah ke objek yang memiliki tingkat keamanan yang lebih tinggi, sehingga mencegah serangan seperti serangan "write-down" atau serangan "trojan horse"(Arthur *et al.,* 2007).

Model Biba didasarkan pada dua prinsip utama, yaitu prinsip integritas dan prinsip kerahasiaan. Prinsip integritas menjamin bahwa objek dengan tingkat keamanan yang lebih tinggi tidak dapat dimodifikasi oleh objek dengan tingkat keamanan yang lebih rendah(Santi *et al*., 2007). Ini mencegah adanya perubahan yang tidak sah pada data yang penting. Prinsip kerahasiaan, di sisi lain, memastikan bahwa objek dengan tingkat keamanan yang lebih rendah tidak dapat membaca atau mengakses objek dengan tingkat keamanan yang lebih tinggi. Hal ini melindungi data sensitif dari akses yang tidak sah(Tian & Song, 2021).

Model Biba menggunakan tiga tingkatan keamanan: tingkat keamanan terendah, tingkat keamanan tinggi, dan tingkat keamanan paling tinggi. Objek dengan tingkat keamanan terendah disebut sebagai "subjek" dan objek dengan tingkat keamanan paling tinggi disebut sebagai "objek"(Y. Liu & Chen, 2004). Subjek dapat menulis ke objek dengan tingkat keamanan yang lebih tinggi, tetapi tidak dapat menulis ke objek dengan tingkat keamanan yang lebih rendah, mengikuti prinsip integritas. Sebaliknya, subjek dapat membaca objek dengan tingkat keamanan yang lebih rendah, tetapi tidak dapat membaca objek dengan tingkat keamanan yang lebih tinggi, mengikuti prinsip kerahasiaan(Zhou et al., 2010).

Selain itu, Model Biba juga mencakup mekanisme kebijakan "*no read up*" dan "*no write down*". Kebijakan "*no read up*" memastikan bahwa subjek dengan tingkat keamanan yang lebih tinggi tidak dapat membaca data dari objek dengan tingkat keamanan yang lebih rendah(L. Xu & Liu, 2013). Kebijakan "no write down" mencegah subjek dengan tingkat keamanan yang lebih rendah menulis data ke objek dengan tingkat keamanan yang lebih tinggi. Hal ini melindungi integritas dan kerahasiaan data.

Dalam Model Biba, juga terdapat mode akses yang disebut *"strict*" dan "*lax*". Mode "*strict*" memastikan bahwa objek dengan tingkat keamanan yang lebih rendah tidak dapat diubah oleh subjek dengan tingkat keamanan yang lebih tinggi. Mode "lax" memungkinkan subjek dengan tingkat keamanan yang lebih tinggi untuk memodifikasi objek dengan tingkat keamanan yang lebih rendah, tetapi tetap menerapkan kebijakan "*no write down*"(G. Liu *et al*., 2015).

Secara keseluruhan, Model Biba menyediakan kerangka kerja yang kuat untuk memastikan integritas dan kerahasiaan data dalam sebuah sistem(Li *et al.,* 2013). Dengan menerapkan prinsip integritas dan kerahasiaan, serta menggunakan mekanisme kebijakan "*no read up*" dan "*no write down*", Model Biba membantu mencegah serangan yang dapat mengancam keamanan data. Namun, seperti model keamanan lainnya, Model Biba juga memiliki

batasan dan harus digunakan dengan bijaksana dalam konteks yang sesuai dengan kebutuhan dan lingkungan sistem yang digunakan. Rujukan utama dari model ini bisa dibaca pada sumber berikut.

Biba, K. J. (1977). Integrity considerations for secure computer systems. Mitre Corp Bedford Ma.

9.2.3 Model Clark-Wilson

Model Clark-Wilson adalah salah satu model keamanan yang dikembangkan oleh David Clark dan David Wilson pada tahun 1987. Model ini bertujuan untuk menyediakan kerangka kerja yang kokoh untuk mengelola integritas dan konsistensi data dalam sistem yang melibatkan banyak entitas yang berbeda(Q. Xu & Liu, 2009). Model Clark-Wilson memiliki beberapa komponen utama yang membentuk landasan keamanannya, yaitu aturan akses, transformasi, dan sertifikasi.

Aturan akses dalam Model Clark-Wilson digunakan untuk membatasi akses ke data yang melibatkan entitas yang tidak berwenang. Setiap entitas harus mematuhi aturan akses yang ditetapkan dalam sistem, sehingga hanya entitas yang berwenang yang dapat mengakses data dan melakukan operasi tertentu. Hal ini memberikan lapisan keamanan yang penting untuk melindungi data sensitif dari akses yang tidak sah(J. B. He et al., 2008).

Transformasi adalah komponen lain dalam Model Clark-Wilson yang berfokus pada memastikan integritas data. Transformasi mengacu pada serangkaian langkah yang harus diikuti untuk memodifikasi data dalam sistem(Tsegaye & Flowerday, 2020). Setiap transformasi harus memenuhi sejumlah persyaratan yang ditentukan, termasuk kriteria integritas dan konsistensi. Dengan menerapkan transformasi yang tepat, Model Clark-Wilson mencegah entitas yang tidak berwenang untuk secara tidak sah memodifikasi data.

Sertifikasi adalah elemen penting dalam Model Clark-Wilson yang bertujuan untuk memastikan keabsahan entitas dan

integritas data yang dikendalikan oleh entitas tersebut. Setiap entitas yang terlibat dalam sistem harus melewati proses sertifikasi yang ketat. Sertifikasi mencakup verifikasi identitas, kualifikasi keamanan, dan penilaian terhadap kredibilitas entitas tersebut. Dengan menerapkan proses sertifikasi yang kuat, Model Clark-Wilson memastikan bahwa hanya entitas yang berwenang dan dapat dipercaya yang dapat berinteraksi dengan data(Ge et al., 2004).

Selain komponen utama di atas, Model Clark-Wilson juga menekankan pada audit dan pemantauan. Setiap aktivitas yang terkait dengan data harus tercatat dan dipantau secara ketat. Hal ini memungkinkan deteksi cepat terhadap aktivitas yang mencurigakan atau tidak sah(Avorgbedor & Liu, 2020; Buława & Kowalczyk, 2016). Audit dan pemantauan juga membantu dalam memastikan kepatuhan terhadap aturan akses dan transformasi yang ditetapkan oleh model. Referensi utama untuk model ini pada sumber berikut.

Clark, D. D., & Wilson, D. R. (1987). *A comparison of commercial and military computer security policies. Proceedings of the IEEE Symposium on Security and Privacy*, 184-194.

Lampson, B. W. (1992). *Protection in operating systems. Communications of the* ACM, 35(8), 16-28.

9.2.4 Model Brewer-Nash (CAP Theorem)

Model Brewer-Nash dikemukakan oleh Eric Brewer dan Seth Gilbert serta Nancy Lynch sebagai bagian dari studi tentang sistem terdistribusi. Konsep ini pertama kali dijelaskan pada tahun 2000 dan sejak itu telah menjadi titik fokus penting dalam bidang keamanan komputasi. Model ini menyajikan teorema CAP, yang menyatakan bahwa dalam sistem terdistribusi, hanya dua dari tiga aspek penting - Konsistensi, Ketersediaan, dan Toleransi Partisi - dapat dijamin secara bersamaan(Meadows, 1990).

Penjelasan Model Brewer-Nash:

Konsistensi: Aspek pertama dalam Model Brewer-Nash adalah konsistensi. Konsistensi mengacu pada keadaan di mana semua node atau bagian dalam sistem terdistribusi melihat dan mengakses data yang sama pada waktu yang hampir bersamaan(Unsworth et al., 2010). Dalam konteks keamanan, konsistensi memastikan bahwa data yang diakses oleh entitas terotentikasi selalu valid dan sesuai dengan keadaan terkini.

Ketersediaan: Ketersediaan merujuk pada kemampuan sistem untuk tetap beroperasi dan memberikan respons kepada pengguna, bahkan ketika terjadi kegagalan atau gangguan. Dalam konteks keamanan, ketersediaan berarti bahwa sistem harus dapat mempertahankan tingkat fungsionalitas yang memadai dan tetap memberikan akses ke data yang diperlukan oleh entitas yang berwenang, bahkan dalam situasi darurat.

Toleransi Partisi: Toleransi partisi adalah aspek ketiga yang diperkenalkan oleh Model Brewer-Nash. Ini mengacu pada kemampuan sistem untuk tetap beroperasi dan mempertahankan konsistensi dan ketersediaan meskipun adanya partisi jaringan atau kegagalan node individu dalam sistem terdistribusi. Dalam konteks keamanan, toleransi partisi memastikan bahwa entitas terotentikasi dapat terus mengakses data yang diperlukan meskipun terjadi gangguan jaringan atau kegagalan komponen sistem.

Implikasi dan Penerapan:

Model Brewer-Nash memberikan panduan berharga dalam merancang dan mengimplementasikan sistem keamanan yang terdistribusi. Dalam praktiknya, para pengembang perlu mempertimbangkan keseimbangan antara konsistensi, ketersediaan, dan toleransi partisi berdasarkan kebutuhan spesifik sistem. Misalnya, dalam sistem keuangan yang kritis, konsistensi dan ketersediaan mungkin menjadi prioritas utama, sementara toleransi partisi dapat dikompromikan hingga batas tertentu(Unsworth et al., 2009). Di sisi lain, dalam sistem

komunikasi darurat, ketersediaan dan toleransi partisi mungkin lebih penting daripada konsistensi. Rujukan utama pada konsep ini sebagai berikut.

Brewer, E. A. (2000). Towards robust distributed systems. Proceedings of the Annual ACM Symposium on Principles of Distributed Computing, 7-10.

Gilbert, S., & Lynch, N. (2002). Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. ACM SIGACT News, 33(2), 51-59.

9.2.5 Model Non-Interference

Model Non-I*nterference* adalah salah satu konsep dalam bidang keamanan komputer yang bertujuan untuk mencegah intervensi tidak sah atau perubahan yang tidak diinginkan terhadap informasi yang sensitif. Model ini didasarkan pada prinsip bahwa entitas yang memiliki tingkat akses yang lebih rendah tidak boleh dapat mempengaruhi entitas yang memiliki tingkat akses yang lebih tinggi, sehingga menjaga integritas dan kerahasiaan informasi yang sensitif(Shankar et al., 2006).

Model Non-Interference mengadopsi pendekatan yang sangat ketat dalam menjaga keamanan informasi. Prinsip utama dari model ini adalah mencegah adanya aliran informasi yang tidak sah antara subjek dengan tingkat akses yang lebih rendah (low-level) ke subjek dengan tingkat akses yang lebih tinggi (high-level). Dalam konteks ini, subjek mengacu pada entitas seperti pengguna, program, atau proses yang dapat mengakses atau memanipulasi informasi. Dengan mematuhi prinsip ini, Model Non-Interference berusaha untuk meminimalkan risiko pelanggaran keamanan yang diakibatkan oleh interaksi antara subjek dengan tingkat akses yang berbeda(Enoch et al., 2021; Jin & Shen, 2012).

Model Non-Interference memandang informasi sensitif sebagai objek yang perlu dilindungi secara ketat. Untuk mencapai hal ini, model ini membagi informasi menjadi level keamanan yang berbeda. Setiap level mewakili tingkat akses yang berbeda, di mana

level yang lebih tinggi memiliki tingkat akses yang lebih tinggi dan informasi yang lebih sensitif. Model ini memastikan bahwa entitas dengan tingkat akses yang lebih rendah tidak dapat mempengaruhi atau mendapatkan informasi dari entitas dengan tingkat akses yang lebih tinggi(Zheng *et al.,* 2005). Dengan demikian, Model Non-Interference melindungi integritas dan kerahasiaan informasi sensitif.

Model Non-I*nterference* mengandalkan mekanisme kontrol akses yang kuat untuk mencegah aliran informasi yang tidak sah antara entitas dengan tingkat akses yang berbeda. Mekanisme ini meliputi kebijakan akses yang ketat, pemisahan tugas (*separation of duty*), dan isolasi lingkungan yang aman. Kebijakan akses memastikan bahwa entitas hanya dapat mengakses informasi yang relevan dengan tingkat akses mereka, sementara pemisahan tugas membatasi entitas agar hanya dapat melakukan tugas-tugas yang sesuai dengan peran dan tanggung jawab mereka. Isolasi lingkungan memastikan bahwa entitas dengan tingkat akses yang berbeda beroperasi dalam konteks yang terpisah secara fisik atau logis.

Model Non-Interference juga memperhatikan masalah non-interference temporal, yang berkaitan dengan interaksi yang terjadi pada waktu yang berbeda antara entitas dengan tingkat akses yang berbeda. Non-interference temporal berarti bahwa aksi atau perubahan yang dilakukan oleh entitas dengan tingkat akses yang lebih rendah tidak boleh mempengaruhi hasil atau perilaku entitas dengan tingkat akses yang lebih tinggi pada waktu yang berbeda. Hal ini penting untuk menjaga konsistensi dan integritas informasi sensitif dalam jangka waktu yang lebih lama(Murphy, 2021).

Meskipun Model Non-Interference memiliki keuntungan dalam menjaga keamanan informasi, namun ada juga keterbatasan yang perlu diperhatikan. Salah satu keterbatasan utamanya adalah bahwa model ini tidak mempertimbangkan interaksi yang diizinkan secara sah antara entitas dengan tingkat akses yang

berbeda. Terkadang, entitas dengan tingkat akses yang lebih rendah memerlukan akses ke informasi yang lebih tinggi untuk menjalankan tugas mereka dengan efektif. Oleh karena itu, diperlukan pendekatan yang lebih fleksibel seperti Model Lattice-Based atau Model Take-Grant yang memperhatikan perizinan khusus yang diberikan kepada entitas dengan tingkat akses yang lebih rendah. Referensi utama terkait model ini pada dokumen berikut.

Goguen, J. A., & Meseguer, J. (1982). *Security policies and security models. IEEE Symposium on Security and Privacy*, 11-20.

Denning, D. E. (1982). *A lattice model of secure information flow. Communications of the* ACM, 19(5), 236-243.

9.2.6 Model Take-Grant

Model *Take-Grant* (TG) adalah salah satu dari berbagai model keamanan yang digunakan dalam keamanan sistem informasi. Model ini dirancang untuk menganalisis dan menggambarkan bagaimana hak akses dan izin dapat dialokasikan dan dipertukarkan antara subjek dan objek dalam suatu sistem. Model TG menggunakan representasi grafik untuk menggambarkan entitas-entitas tersebut dan hubungan antara mereka (Lockman & Minsky, 1982).

Pertama-tama, Model Take-Grant terdiri dari dua elemen utama, yaitu subjek (*subject*) dan objek (*object*). Subjek merujuk pada entitas yang meminta akses atau izin, sedangkan objek merujuk pada entitas yang memiliki sumber daya atau informasi yang ingin diakses oleh subjek(Biskup, 1984). Dalam model ini, subjek dan objek direpresentasikan sebagai simpul-simpul dalam grafik, sedangkan hak akses dan izin direpresentasikan sebagai busur-busur yang menghubungkan simpul-simpul tersebut.

Kedua, Model TG menggunakan beberapa operasi dasar untuk menggambarkan hubungan antara subjek dan objek. Operasi-operasi ini meliputi "*take*" (pengambilan hak akses), "*grant*" (pemberian hak akses), "*create*" (pembuatan subjek atau

objek baru), "*remove*" (penghapusan subjek atau objek), dan "*destroy*" (penghancuran subjek atau objek). Operasi-operasi ini memungkinkan penggunaan model untuk menganalisis bagaimana hak akses dan izin dapat berpindah dari satu entitas ke entitas lain dalam sistem(Shahriari et al., 2005).

Ketiga, Model TG memperkenalkan konsep pertukaran hak akses yang penting. Pertukaran hak akses terjadi ketika subjek memperoleh hak akses baru dari objek atau subjek lain, atau ketika subjek memberikan hak aksesnya kepada objek atau subjek lain. Model ini memungkinkan analisis terperinci tentang bagaimana hak akses dapat berpindah melalui pertukaran ini, dan apakah pertukaran tersebut mematuhi kebijakan keamanan yang ditetapkan dalam sistem.

Keempat, Model TG juga mempertimbangkan tingkat kepercayaan dalam pertukaran hak akses. Tingkat kepercayaan digunakan untuk mengukur sejauh mana sebuah entitas dapat dipercaya untuk memberikan atau menerima hak akses. Dalam model ini, tingkat kepercayaan direpresentasikan sebagai angka numerik, dan pengambilan atau pemberian hak akses hanya dapat dilakukan jika tingkat kepercayaan memenuhi syarat yang ditentukan(Bishop, 1995; Snyder, 1981).

Kelima, Model TG memiliki kegunaan dalam analisis keamanan sistem informasi. Dengan menggunakan model ini, administrator sistem dapat menganalisis dan memodelkan bagaimana hak akses dan izin dapat dialokasikan dan dipertukarkan dalam suatu sistem, serta melihat apakah kebijakan keamanan yang ditetapkan terpenuhi. Model TG juga dapat membantu dalam mengidentifikasi potensi celah keamanan, misalnya jika suatu subjek memperoleh hak akses yang tidak seharusnya atau jika pertukaran hak akses tidak sesuai dengan kebijakan yang ditetapkan.

Rujukan utama dari model keamanan ini pada dokumen berikut.

Guttman, J. D. (1978). A control structure for an authorization system. ACM SIGSAC Review, 13(1), 24-32.

Lampson, B. W., & Abadi, M. (1991). Theoretical and practical foundations of security. ACM Transactions on Information and System Security (TISSEC), 2(4), 359-389.

9.2.7 *Role-Based Access Control* (RBAC)

Role-Based Access Control (RBAC) adalah salah satu konsep yang digunakan dalam model keamanan untuk mengatur akses dan pengelolaan izin pada sistem komputer. RBAC memungkinkan administrator sistem untuk memberikan hak akses berdasarkan peran atau posisi pengguna dalam organisasi, bukan berdasarkan identitas individu. Konsep ini dapat diterapkan dalam berbagai jenis sistem, mulai dari jaringan komputer hingga aplikasi perusahaan(Cruz *et al.,* 2018).

RBAC mengidentifikasi peran yang ada dalam organisasi dan kemudian memberikan hak akses berdasarkan peran tersebut. Sebagai contoh, dalam sebuah perusahaan, terdapat peran seperti administrator sistem, manajer, dan pengguna biasa(Y. He *et al.,* 2007). Setiap peran ini memiliki tanggung jawab dan kebutuhan akses yang berbeda. RBAC memungkinkan administrator sistem untuk menetapkan hak akses yang sesuai dengan setiap peran.

Model ini terdiri dari tiga komponen utama, yaitu pengguna, peran, dan izin. Pengguna adalah individu atau entitas yang menggunakan sistem. Peran adalah kumpulan tugas dan tanggung jawab yang terkait. Izin adalah hak akses yang diberikan kepada peran atau pengguna untuk mengakses sumber daya tertentu. Dalam RBAC, administrator sistem menetapkan peran kepada pengguna dan kemudian mengaitkan izin dengan peran tersebut(Nazerian *et al.,* 2019).

RBAC membantu menyederhanakan manajemen akses dan izin dalam sistem. Dengan mengelompokkan pengguna berdasarkan peran, administrator sistem dapat dengan mudah menetapkan dan mengubah izin akses. Selain itu, RBAC juga

meningkatkan keamanan dengan mengurangi risiko akses yang tidak sah atau tidak terotorisasi(Thakare *et al.,* 2020). Dengan adanya RBAC, administrator dapat memastikan bahwa setiap pengguna hanya memiliki akses yang sesuai dengan tugas dan tanggung jawab mereka.

Salah satu konsep penting dalam RBAC adalah konsep hirarki peran. Dalam hirarki peran, peran dapat memiliki hubungan induk-anak, di mana peran anak dapat mewarisi izin dari peran induk. Misalnya, jika ada peran "manajer" dan peran "staf", peran "staf" dapat mewarisi izin dari peran "manajer". Selain itu, RBAC juga dapat melibatkan konsep tugas terkait, di mana izin diberikan berdasarkan tugas tertentu yang dilakukan oleh peran(Ghafoorian et al., 2019).

Untuk menerapkan RBAC, administrator sistem perlu melakukan analisis kebutuhan akses, mengidentifikasi peran dan izin yang tepat, dan mengatur hirarki peran jika diperlukan. Setelah itu, administrator dapat menggunakan perangkat lunak manajemen. Rujukan utama model ini pada dokumen berikut.

Sandhu, R. S., Coyne, E. J., Feinstein, H. L., & Youman, C. E. (1996). *Role-based access control models*. IEEE Computer, 29(2), 38-47.

Ferraiolo, D. F., Sandhu, R. S., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). *Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security* (TISSEC), 4(3), 224-274.

9.2.8 *Attribute-Based Access Control* (ABAC)

Attribute-Based Access Control (ABAC) adalah model keamanan yang memungkinkan pengendalian akses ke sumber daya berdasarkan atribut-atribut yang terkait dengan pengguna, objek, lingkungan, dan konteks lainnya. Model ini memberikan fleksibilitas dan skala yang lebih besar dibandingkan dengan model akses kontrol tradisional seperti *Role-Based Access Control* (RBAC) atau *Access Control Lists* (ACLs) (Aghili et al., 2022). ABAC

menggunakan atribut-atribut ini untuk mengambil keputusan akses yang lebih rinci, dengan mempertimbangkan banyak faktor yang relevan dalam sistem keamanan.

Pertama, dalam model ABAC, pengendalian akses didasarkan pada atribut pengguna. Atribut-atribut seperti peran, jabatan, departemen, dan hak istimewa khusus lainnya dapat digunakan untuk membatasi akses ke sumber daya tertentu. Misalnya, hanya pengguna dengan atribut "administrator" yang dapat mengakses fungsi pengaturan sistem yang sensitif (Alohaly et al., 2019).

Kedua, atribut objek juga diperhitungkan dalam ABAC. Setiap objek dalam sistem dapat memiliki atribut yang menggambarkan karakteristiknya, seperti tingkat kerahasiaan, jenis data, atau properti khusus lainnya. Keputusan akses dapat diterapkan berdasarkan atribut ini, misalnya hanya pengguna dengan atribut "tingkat kerahasiaan: tinggi" yang dapat mengakses dokumen rahasia(M. Liu et al., 2020; Servos & Osborn, 2017).

Ketiga, konteks lingkungan juga menjadi faktor penting dalam ABAC. Atribut-atribut seperti waktu, lokasi geografis, jaringan, dan keadaan sistem lainnya dapat mempengaruhi keputusan akses. Misalnya, jika sebuah sistem hanya diizinkan diakses pada jam kerja, maka atribut waktu akan menjadi pertimbangan penting dalam mengizinkan akses(Nweke et al., 2020).

Keempat, ABAC juga memungkinkan penggunaan atribut dinamis yang dapat berubah seiring waktu. Misalnya, atribut yang menggambarkan keanggotaan pengguna dalam sebuah grup dapat berubah ketika pengguna bergabung atau keluar dari grup tersebut. Model ABAC mampu mengakomodasi perubahan ini dan mengupdate keputusan akses sesuai dengan atribut yang diperbarui(Y. Zhang et al., 2021).

Kelima, model ABAC juga memungkinkan penggunaan aturan kebijakan yang kompleks untuk mengatur akses. Aturan-aturan ini dapat menggabungkan banyak atribut dan kondisi untuk

menghasilkan keputusan akses yang lebih canggih. Misalnya, aturan kebijakan dapat menentukan bahwa hanya pengguna dengan atribut "departemen: keuangan" yang dapat mengakses data keuangan pada hari kerja di luar jam makan siang(Alohaly et al., 2022).

Secara keseluruhan, ABAC merupakan model akses kontrol yang fleksibel dan kuat dalam mengatur keamanan sistem. Dengan mempertimbangkan atribut-atribut yang berkaitan dengan pengguna, objek, lingkungan, dan konteks lainnya, ABAC dapat memberikan tingkat keamanan yang lebih tinggi dengan keputusan akses yang lebih rinci dan sesuai dengan kondisi yang berlaku (Ameller et al., 2016; Kim et al., 2021). Model ini dapat diterapkan dalam berbagai lingkungan seperti organisasi bisnis, sistem informasi, atau infrastruktur cloud untuk meningkatkan keamanan dan kontrol akses. Rujukan utama model ini sebagai berikut.

Hu, V. C., & Ferraiolo, D. F. (2004). *Guide to attribute-based access control* (ABAC) *definition and considerations.* NIST *Special Publication,* 800-162.

Park, J., & Sandhu, R. (2004). The UCONABC *usage control model.* ACM *Transactions on Information and System Security* (TISSEC), 7(1), 128-174.

Security models memberikan panduan dan kerangka kerja yang diperlukan untuk melindungi data, infrastruktur, dan sistem informasi dari ancaman keamanan yang semakin kompleks. Dengan mempelajari security models, para profesional IT dapat mengidentifikasi risiko keamanan, menerapkan kontrol yang tepat, mematuhi regulasi yang berlaku, merancang sistem yang aman, dan merespons dengan cepat terhadap insiden keamanan. Dengan pemahaman yang kuat tentang security models, mereka dapat memastikan keamanan yang optimal, melindungi privasi pengguna, dan menjaga keandalan serta ketersediaan sistem yang mereka tangani.

DAFTAR PUSTAKA

Aghili, S. F., Sedaghat, M., Singelée, D., & Gupta, M. 2022. MLS-ABAC: Efficient Multi-Level Security Attribute-Based Access Control scheme. *Future Generation Computer Systems*, *131*. https://doi.org/10.1016/j.future.2022.01.003

Alohaly, M., Balogun, O., & Takabi, D. 2022. Integrating Cyber Deception Into Attribute-Based Access Control (ABAC) for Insider Threat Detection. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3213645

Alohaly, M., Takabi, H., & Blanco, E. 2019. Automated extraction of attributes from natural language attribute-based access control (ABAC) Policies. *Cybersecurity*, *2*(1). https://doi.org/10.1186/s42400-018-0019-2

Ameller, D., Galster, M., Avgeriou, P., & Franch, X. 2016. A survey on quality attributes in service-based systems. *Software Quality Journal*, *24*(2). https://doi.org/10.1007/s11219-015-9268-4

Arthur, K., Olivier, M., & Venter, H. 2007. Applying The Biba integrity model to evidence management. *IFIP International Federation for Information Processing*, *242*. https://doi.org/10.1007/978-0-387-73742-3_22

Avorgbedor, F., & Liu, J. 2020. Enhancing User Privacy Protection by Enforcing Clark-Wilson Security Model on Facebook. *IEEE International Conference on Electro Information Technology*, *2020-July*. https://doi.org/10.1109/EIT48999.2020.9208279

Bell, D. 1996. The Bell-LaPadula model. *Journal of Computer Security*, *4*(2).

Bishop, M. 1995. Theft of information in the take-grant protection model. *Journal of Computer Security*, *3*(4). https://doi.org/10.3233/JCS-1994/1995-3405

Biskup, J. 1984. Some variants of the take-grant protection model. *Information Processing Letters*, *19*(3). https://doi.org/10.1016/0020-0190(84)90095-4

Buława, P., & Kowalczyk, M. 2016. Application of the Clark-Wilson Model for Business Intelligence System Security Improvement. *Challenges of Modern Technology*, *7*(3). https://doi.org/10.5604/01.3001.0009.5444

Cruz, J. P., Kaji, Y., & Yanai, N. 2018. RBAC-SC: Role-based access control using smart contract. *IEEE Access*, *6*. https://doi.org/10.1109/ACCESS.2018.2812844

Cutinha, J. 2023. SOFTWARE SYSTEMS SECURITY IMPLICATION UTILIZING THE BELL-LAPADULA MODEL. *International Journal of Social Science and Economic Research*, *08*(01). https://doi.org/10.46609/ijsser.2023.v08i01.012

Enoch, S. Y., Lee, J. S., & Kim, D. S. 2021. Novel security models, metrics and security assessment for maritime vessel networks. *Computer Networks*, *189*. https://doi.org/10.1016/j.comnet.2021.107934

Ge, X., Polack, F., & Laleau, R. 2004. Secure databases: An analysis of Clark-Wilson model in a database environment. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3084*. https://doi.org/10.1007/978-3-540-25975-6_18

Ghafoorian, M., Abbasinezhad-Mood, D., & Shakeri, H. 2019. A Thorough Trust and Reputation Based RBAC Model for Secure Data Storage in the Cloud. *IEEE Transactions on Parallel and Distributed Systems*, *30*(4). https://doi.org/10.1109/TPDS.2018.2870652

He, J. B., Guo, X., & Qing, S. H. 2008. Approach to enforcing clark-wilson model based on type enforcement. *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, *36*(2).

He, Y., Li, X., & Feng, D. 2007. Implementing Chinese wall policies on RBAC. *Jisuanji Yanjiu Yu Fazhan/Computer Research and Development*, *44*(4). https://doi.org/10.1360/crad20070410

Jin, J., & Shen, M. 2012. Analysis of security models based on multilevel security policy. *Proceedings - 2012 International Conference on Management of e-Commerce and e-Government, ICMeCG 2012*. https://doi.org/10.1109/ICMeCG.2012.72

Kim, B., Shin, W., Hwang, D. Y., & Kim, K. H. 2021. Attribute-Based Access Control(ABAC) with Decentralized Identifier in the Blockchain-Based Energy Transaction Platform. *International Conference on Information Networking*, *2021-January*. https://doi.org/10.1109/ICOIN50884.2021.9333894

Li, L., Lu, K., Guo, Q., Chen, Y., & Fan, X. 2013. Formal analysis of power separation mechanism based on Biba model. *Beijing Jiaotong Daxue Xuebao/Journal of Beijing Jiaotong University*, *37*(5).

Liu, G., Zhang, J., Liu, J., & Zhang, Y. 2015. Improved Biba model based on trusted computing. *Security and Communication Networks*, *8*(16). https://doi.org/10.1002/sec.1201

Liu, M., Yang, C., Li, H., & Zhang, Y. 2020. An efficient attribute-based access control (ABAC) policy retrieval method based on attribute and value levels in multimedia networks. *Sensors (Switzerland)*, *20*(6). https://doi.org/10.3390/s20061741

Liu, Y., & Chen, X. 2004. A new information security model based on BLP model and Biba model. *International Conference on Signal Processing Proceedings, ICSP*, *3*. https://doi.org/10.1109/icosp.2004.1442325

Lockman, A., & Minsky, N. 1982. Unidirectional Transport of Rights and Take-Grant Control. *IEEE Transactions on Software Engineering*, *SE-8*(6). https://doi.org/10.1109/TSE.1982.236020

Meadows, C. 1990. Extending the Brewer-Nash model to a multilevel context. *Proceedings of the Symposium on Security and Privacy*. https://doi.org/10.1109/risp.1990.63842

Murphy, S. 2021. Security Models and Architecture In. *CISSP Certification All-in-One Exam Guide*.

Nazerian, F., Motameni, H., & Nematzadeh, H. 2019. Emergency role-based access control (E-RBAC) and analysis of model specifications with alloy. *Journal of Information Security and Applications*, *45*. https://doi.org/10.1016/j.jisa.2019.01.008

Nweke, L. O., Yeng, P., Wolthusen, S. D., & Yang, B. 2020. Understanding attribute-based access control for modelling and analysing healthcare professionals' security practices. *International Journal of Advanced Computer Science and Applications*, *2*. https://doi.org/10.14569/ijacsa.2020.0110286

Roslan, S. N., Hamid, I. R. A., & Shamala, P. 2018. E-store management using bell-lapadula access control security model. *International Journal on Informatics Visualization*, *2*(3–2). https://doi.org/10.30630/joiv.2.3-2.140

Santi, I., Scarselli, M., Mariani, M., Pezzicoli, A., Masignani, V., Taddei, A., Grandi, G., Telford, J. L., & Soriani, M. 2007. BibA: A novel immunogenic bacterial adhesin contributing to group B Streptococcus survival in human blood. *Molecular Microbiology*, *63*(3). https://doi.org/10.1111/j.1365-2958.2006.05555.x

Servos, D., & Osborn, S. L. 2017. Current research and open problems in attribute-based access control. *ACM Computing Surveys*, *49*(4). https://doi.org/10.1145/3007204

Shahriari, H. R., Sadoddin, R., Jalili, R., Zakeri, R., & Omidian, A. R. 2005. Network vulnerability analysis through vulnerability take-grant model (VTG). *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *3783 LNCS*. https://doi.org/10.1007/11602897_22

Shankar, U., Jaeger, T., & Sailer, R. 2006. Toward Automated Information-Flow Integrity Verification for Security-Critical Applications. *Ndss '06*, *2*.

Snyder, L. 1981. Theft and conspiracy in the take-grant protection model. *Journal of Computer and System Sciences*, *23*(3). https://doi.org/10.1016/0022-0000(81)90069-6

Tang, Z., Ding, X., Zhong, Y., Yang, L., & Li, K. 2018. A self-adaptive bell-lapadula model based on model training with historical access logs. *IEEE Transactions on Information Forensics and Security*, *13*(8). https://doi.org/10.1109/TIFS.2018.2807793

Thakare, A., Lee, E., Kumar, A., Nikam, V. B., & Kim, Y. G. 2020. PARBAC: Priority-Attribute-Based RBAC Model for Azure IoT Cloud. *IEEE Internet of Things Journal*, *7*(4). https://doi.org/10.1109/JIOT.2019.2963794

Tian, X., & Song, H. 2021. A zero trust method based on BLP and BIBA model. *Proceedings - 2021 14th International Symposium on Computational Intelligence and Design, ISCID 2021*. https://doi.org/10.1109/ISCID52796.2021.00031

Tsegaye, T., & Flowerday, S. 2020. A Clark-Wilson and ANSI role-based access control model. *Information and Computer Security*, *28*(3). https://doi.org/10.1108/ICS-08-2019-0100

Unsworth, N., Brewer, G. A., & Spillers, G. J. 2009. There's more to the working memory capacity-fluid intelligence relationship than just secondary memory. *Psychonomic Bulletin and Review*, *16*(5). https://doi.org/10.3758/PBR.16.5.931

Unsworth, N., Spillers, G. J., & Brewer, G. A. 2010. The Contributions of Primary and Secondary Memory to Working Memory Capacity: An Individual Differences Analysis of Immediate Free Recall. *Journal of Experimental Psychology: Learning Memory and Cognition*, *36*(1). https://doi.org/10.1037/a0017739

Xu, L., & Liu, H. 2013. Automated formal verification of practical Biba model. *Hunan Daxue Xuebao/Journal of Hunan University Natural Sciences*, *40*(9).

Xu, Q., & Liu, G. 2009. Configuring Clark-Wilson integrity model to enforce flexible protection. *CIS 2009 - 2009 International Conference on Computational Intelligence and Security*, *2*. https://doi.org/10.1109/CIS.2009.249

Yang, L., Wang, J., Tang, Z., & Xiong, N. N. 2021. Using conditional random fields to optimize a self-adaptive bell-lapadula model in control systems. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *51*(7). https://doi.org/10.1109/TSMC.2019.2937551

Zhang, R., Liu, G., Kang, H., Wang, Q., Tian, Y., & Wang, C. 2021. Improved Bell-LaPadula Model with Break the Glass Mechanism. *IEEE Transactions on Reliability*, *70*(3). https://doi.org/10.1109/TR.2020.3046768

Zhang, Y., Yutaka, M., Sasabe, M., & Kasahara, S. 2021. Attribute-Based Access Control for Smart Cities: A Smart-Contract-Driven Framework. *IEEE Internet of Things Journal*, *8*(8). https://doi.org/10.1109/JIOT.2020.3033434

Zheng, Z., Cai, Y., & Shen, C. 2005. Research on an application class communication security model on operating system security framework. *Jisuanji Yanjiu Yu Fazhan/Computer Research and Development*, *42*(2). https://doi.org/10.1360/crad20050221

Zhou, Z. Y., He, Y. P., & Liang, H. L. 2010. Hybrid mandatory integrity model composed of Biba and Clark-Wilson policy. *Ruan Jian Xue Bao/Journal of Software*, *21*(1). https://doi.org/10.3724/SP.J.1001.2010.03513

BAB 10
KEBIJAKAN DAN PERATURAN PADA ASET INFORMASI

Oleh Gatot Budi Santoso

10.1 Pentingnya Kebijakan Dan Peraturan

Seperti telah dibahas pada bab sebelumnya bahwa aset informasi merupakan suatu unit informasi yang dikelola untuk dilindungi dan dibagikan antara pengguna dan pengelola. Dalam menjaga aset informasi tersebut maka munculah sebuah bahasa yaitu proteksi aset informasi.

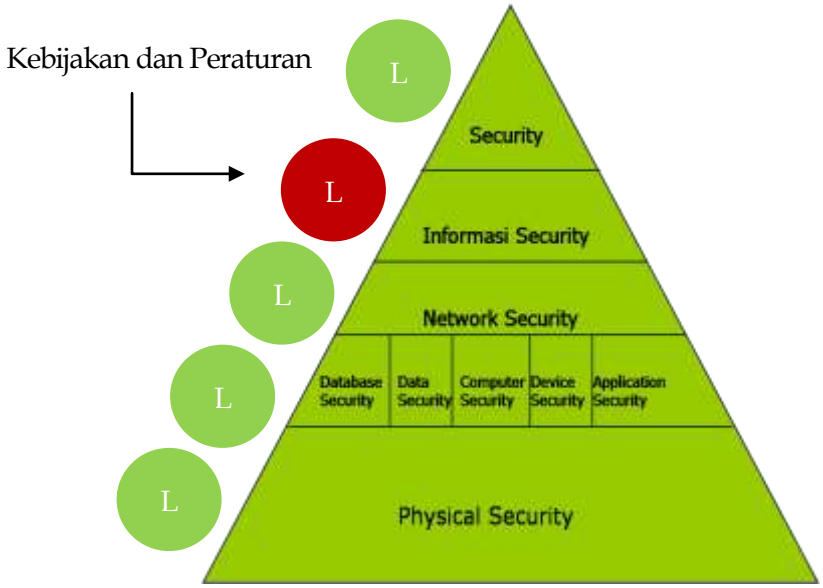
Definisi proteksi aset informasi merupakan suatu metode yang dikaji, dirancang, dan disempurnakan sistemnya untuk melindungi aset informasi tersebut dengan menggunakan teknik yang telah tersistem. Dimana terdapat batas-batas hukum yang diatur dalam kebijakan dan peraturan atau dikenal *Policies and compilence*.

Kebijakan dan peraturan dalam melakukan proteksi aset informasi memiliki ruang lingkup yang dijaga pada aset informasi tersebut seperti *database*, file-file data seperti dokumen, manual, materi dan juga prosedur.

Mengingat bahwa kegiatan manusia akhir-akhir ini disimpan dalam sebuah komputer, mulai dari data diri, data pendidikan, data kesehatan, data pekerjaan, dan bahkan data kematian serta data keuangan. Maka komputer menjadi tempat untuk menyimpan dan mendapatkan informasi.

Keamanan komputer dapat dilihat dalam bentuk piramida. Dimana terdapat level 0 sampai 4. Informasi menjadi bagian keamanan dalam komputer pada level ke 3 yaitu level yang sangat penting.

Level 0 adalah keamanan fisik yang menjadi pondasi level lain agar tetap aman karena berbentuk *hardware*. Level 1 adalah *database* seperti PC, *device*, dan aplikasi. Level 2 adalah hubungan dengan jaringan seperti LAN dan WAN. Level 3 adalah keamanan informasi didalam komputer. Sedangkan Level 4 adalah keseluruhan level.



Gambar 10.1. Piramida Keamanan Komputer

Bedasarkan pada Gambar 10.1 bahwa sebenarnya dalam menjaga informasi bisa dilakukan oleh semua kalangan yang terlibat. Kebijakan dan peraturan tersebut adalah bentuk manajemen yang didalamnya menekankan pada *user* untuk menjaga informasi seperti kata sandi dan informasi pribadi. Berikutnya adalah menekankan pada sistem agar tidak dibobol oleh *hacker* dalam mengambil informasi untuk disalahgunakan.

10.1.1 Kebijakan Proteksi Aset Informasi

Penggunaan Teknologi Informasi semakin berkembang. Seiring dengan kebutuhan sumber informasi terpercaya yang dimiliki oleh suatu individu atau kelompok.

Maka keamanan terhadap suatu informasi perlu untuk diperhatikan dan dipahami. Contohnya, pada ilmu teknik kimia seorang mahasiswa membutuhkan data informasi mengenai suatu kebutuhan dalam negeri pada bahan kimia tertentu. Maka mahasiswa tersebut akan melakukan studi literatur terhadap sumber informasi dari badan pusat statistika. Dan data tersebut berhak untuk diakses sebagai pendukung kemajuan perindustrian dan tidak bersifat rahasia atau informasi terbuka.

Berbeda dengan seorang pekerja swasta yang melakukan transaksi pembuatan kartu kredit di suatu bank dengan memberikan data individu yang bersifat rahasia, pribadi dan simbolis. Maka pihak bank tersebut harus membuat sebuah kebijakan dan peraturan terhadap kepastian perlindungan data dari nasabahnya. Artinya setiap organisasi atau kelompok harus menyadari dan menerapkan kebijakan yang tepat untuk melindungi aset informasi tersebut. Adapun kebijakan tersebut berupa:

1. **Sistem Manajeman Keamanan SNI ISO27001**

   Kebijakan aset Informasi telah diatur dalam SNI ISO 27001 yaitu sistem manajemen keamanan informasi. Dalam kebijakan tersebut sistem keamanan aset informasi merupakan suatu pendekatan sistematis dalam menjaga atau menyimpan informasi milik user (Perusahaan atau kelompok) yang bersifat sensitif agar tetap aman. Dimana dalam pelaksanaannya diatur dalam manajemen resiko.

   Manajemen resiko tersebut adalah suatu upaya yang diciptakan pada penerima akses informasi agar memiliki kedisiplinan dan penjagaan terhadap data yang dimilikinya. Dimana suatu aset informasi yang berkaitan dengan akses

biasanya diberikan kepada administrator, survei administrator dan tentunya adalah *user*.

2. Penerapan Kebijakan Proteksi Aset Informasi

Meskipun telah dijelaskan dalam SNI ISO 27001 tentang bagaimana memanajemen infomasi dalam melaksanakan kebijakannya. Suatu aset informasi juga harus didefinisikan dengan baik dalam perancangannya. Karena pada dasarnya dalam menjaga aset informasi kebijakan yang tepat oleh *user* yang dirancanganglah yang akan terlindungi.

Dokumen kebijakan harus dimiliki dan dipahami oleh suatu perusahaan atau kelompok yang ingin melindungi aset informasi. Dimana dalam dokumen kebijakan berisi kontrol manajemen, prosedur dan mekanisme, serta cara pengamanan.

Ada beberapa dalam menjalankan kebijakan proteksi aset informasi. 1) Seluruh pemangku kepentingan wajib memahami dan mengkomunikasikannya tentang kebijakan penjagaan aset informasi. 2) Mengelompokan aset informasi yang perlu, penting dan tidak perlu dilindungi. 3) Teritorial kewenangan. 4) Jaminan adanya peraturan dan sanksi. 5) SDM memiliki tanggung jawab terhadap aset informasi. 6) Penerapan yang efektif. 7) Partisipasi setiap individu dalam *team*, evaluasi dan sosialisasi dalam perlindungan aset informasi.

10.1.2 Peraturan Aset Informasi

Pemerintah telah melakukan sebuah peraturan dalam menjaga aset informasi menggunakan sistem elektronik yang bertujuan untuk melindungi aset informasi Negara, kelompok dan individu.

Adapun proteksi aset informasi tersebut diatur dalam peraturan BSSN No 4 Tahun 2021. Dalam peraturan tersebut

pemerintah memberikan pedoman manajemen yang diatur dari Bab 1 sampai dengan Bab 4 yang dilengkapi dengan pasal-pasal. Adapun latar belakang akan perlunya peraturan yang nyata terhadap proteksi aset informasi yaitu ada beberapa hal.

Hal pertama, investasi informasi cenderung mahal. Pada penelitian yang dilakukkan oleh Forrester menunjukkan bahwa total investasi mencapai USD 1,6 Triliun pada tahun 2010.

Alasan berikutnya adalah survei yang dilakukan oleh lembaga CSI menunjukkan bahwa 80% responden mengaku mengalami sebuah kerugian finansial yang diakibatkan oleh serangan data oleh oknum tertentu. Maka dalam peraturan BSSN No 4 tahun 2021, pemerintah membentuk badan *CYBER*.

1. **Peraturan Proteksi Aset Informasi Pemerintahan**

   Maka pada umumnya setiap negara dan bagian dari negara memiliki tanggung jawab terhadap keamanan aset informasi. Contoh Provinsi Aceh membuat peraturan dalam menjaga aset informasi tertuang pada nomor 34 tahun 2021 yaitu peraturan Bupati Aceh - Provinsi Aceh.

2. **Peraturan Proteksi Aset Informasi Kementrian**

   Selain berlaku peraturan proteksi aset informasi dibeberapa provinsi di Indonesia dan di lingkungan pemerintah pusat. Perlu dipahami bahwa peraturan aset informasi berlaku dalam beberapa sektor pemerintahan seperti Direktur Jenderal Pajak (DJP). Dalam surat edaran DJP Nomor SE-57/PJ/2011 tentang pengelolaan aset informasi yang didalamnya untuk melindungi data informasi yang dimiliki dan dibutuhkan oleh DJP. Adapun data tersebut seperti data keuangan, gaji, kontrak dan dokumen tata kelola.

3. **Peraturan Proteksi Aset Informasi Bidang Kesehatan/Lembaga**

   Bidang kesehatan menjadi salah satu sasaran kegiatan siber, dimana setiap tahun selalu mengalami peningkatan kebocoran data informasi dalam bidang kesehatan khususnya dari tahun 2013. Contoh kasus adalah kebocoran data EMR

pasien yang melibatkan sekitar 113 juta pasien di negara US yang diakibatkan kegiatan *hacking*, *skimming*, dan *phising*.

Dalam melindungi aset informasi maka dalam bidang kesehatan telah diatur dalam UU, PP, Permenkes, dan kepmenkes. Dalam UU nomor 11 tahun 2008 mengatur informasi dan transaksi elektronik. Peraturan Menteri Kesehatan Republik Indonesia nomor 4 tahun 2017 tentang E-Kesehatan.

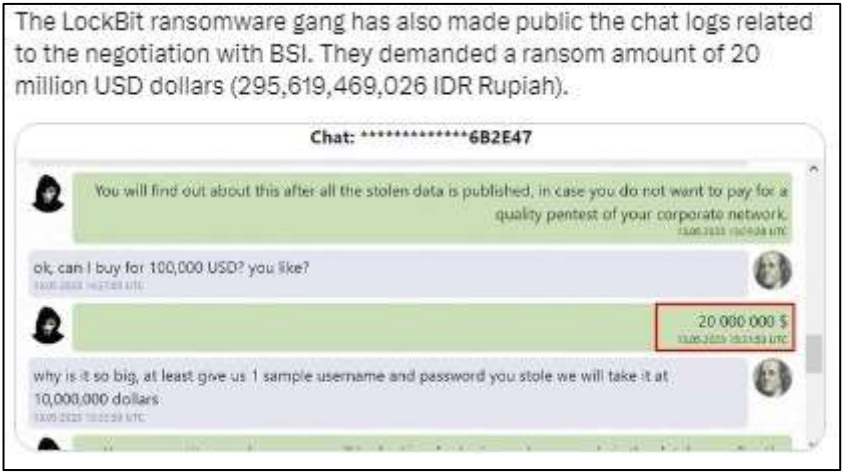
4. Peraturan Proteksi Aset Informasi Bidang Kementrian Keuangan

Dalam bidang perbankan, aset informasi merupakan bagian yang sangat penting. Dimana kebocoran data nasabah dapat menjadi hilangnya kepercayaan masyarakat.

Akhir-akhir ini, tepatnya pada bulan Mei 2023 muncul kasus serangan siber pada bank Syariah Indonesia (BSI) yang merupakan bank syariah terbesar berpelat merah seperti diperlihatkan pada Gambar 10.2. Pada gambar tersebut terlihat bahwa data - data nasabah BSI telah disebarluaskan di *dark web* atau situs gelap oleh *ransomware hacker* karena BSI menolak tuntutan yang diajukan.

Gambar 10.2. Penyebaran Data Nasabah BSI di *Dark Web*

LockBit ransomware hacker yang berhasil meretas sistem keamanan BSI dengan mencuri data pegawai serta data nasabahnya telah melakukan pengancaman dan tuntutan sejumlah 20 juta dollar Amerika kepada pihak BSI. Namun dalam proses negosiasinya mengalami kegagalan yang terlihat pada Gambar 10.3 dibawah ini.



Gambar 10.3. Percakapan Negosiasi antara *Hacker* dengan BSI

Dimana pada tahun 2022 aset BSI mencapai Rp. 305,7 Triliun yang merupakan aset terbesar ke-7 di Indonesia. Permasalahan pencurian data nasabah tersebut tentunya masih ada kelemahan dalam proteksi informasi. Otoritas Jasa Keuangan Sendiri sudah mengatur dalam nomor 11/POJK.03/2022 tentang penyelenggaraan teknologi informasi yang diatur kembali dalam edaran OJK pada nomor 21/SEOJK.03/2017 Tentang penerapan manajemen resiko dalam penggunaan teknologi informasi.

DAFTAR PUSTAKA

Conklin, White, Williams, Davis, Cothren. 2012.*Principles of computer Security: CompIT Secuirity and Beyond*, 3rd edition, Mc Graw Hill TechnologyEducation.

Hartono, Dahlan, Fadhlisyah. 2018. Sistem Operasi. Informatikan dan system informasi. Buku. Sefa Bumi Persada.

Zen Munawar, Novianti, Ivana. 2011. Keamanan Sistem Informasi Keizen Media Publishing.

Peraturan arsip nasional republik Indonesia, 2021, Sistem manajeman keamanan informasi di lingkungan arsip nasional republik Indonesia.

Modul. 2020. Proteksi dan Pertukaran Informasi Kesehatan. Universitas ESA Unggul.

BIODATA PENULIS

Yuswardi, S.T., M.T
Dosen di universitas Jabal Ghafur

Yuswardi, S.T., M.T dilahirkan di Sigli, Pidie, Aceh, pada tanggal 12 Oktober 1986 Sarjana alumni Fakultas Teknik program Studi Teknik Informatika Lulus Tahun 2010 Universitas Jabal Ghafur. Sedangkan Magister selesaikan pada tahun 2016 di program Pascasarjana Magister Teknik Elektro Bidang Kosentrasi Teknologi Informasi Universitas Syiah Kuala Banda Aceh. Saat Ini aktif Mengajar di universitas Jabal Ghafur.

BIODATA PENULIS

Indrawan Ady Saputro, M.Kom
Dosen Program Studi Informatika
STMIK Amikom Surakarta

Penulis lahir di Juwangi, Boyolali. Penulis merupakan dosen pada Program Studi Informatika di STMIK Amikom Surakarta. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Jurusan Informatika konsentrasi Forensika Digital. Salah satu motivasi dalam hidup yang masih tetap tergenggam erat dalam ingatan adalah ”Urip mung mampir ngombe”. Hidup didunia adalah perjalanan singkat menuju keabadian buatlah pengalaman dan kenangan sebaik mungkin hingga pada saatnya nanti waktu kita sudah cukup untuk melakukannya.

BIODATA PENULIS

Angga Aditya Permana
Dosen Informatika
Universitas Multimedia Nusantara

Angga Aditya Permana (lahir pada Desember 1989 di Jakarta) seorang dosen full time di bidang Computer Science pada Universitas Multimedia Nusantara sejak tahun 2021, fokus penelitian pada kriptografi, steganografi serta keamanan computer, namun pada tahun 2021 sedang mendalami topik bioinformatika dan network science. Angga juga memiliki hobi yaitu touring dan juga bermain bulutangkis, saat ini sedang menjadi mahasiswa program doctoral pada IPB University. Memulai karir pertama kali sebagai Network Enginner tahun 2011 dan memulai profesinya sebagai dosen pada 2013 di kampus swasta yang ada di Jakarta, pernah juga mengajar di kampus negri yang berada di Jakarta dan Tangerang, juga pernah di undang menjadi dosen tamu untuk mengenalkan Bioinformatika di kampus negeri di Jakarta. Terimakasih..

BIODATA PENULIS

Suwito Pomalingo, S.Kom., M.Kom.
Dosen Program Studi Informatika Fakultas Teknik dan Informatika
Universitas Multimedia Nusantara

Penulis adalah dosen tetap pada Program Studi Informatika Fakultas Teknik dan Informatika Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Informatika dan melanjutkan S2 pada Program Magister Informatika Universitas Islam Indonesia.

Saat ini sementara menyelesaikan studi Doktoral dengan topik penelitian di bidang Security Science dengan pendekatan Deep Learning. Penulis menekuni bidang keilmuan meliputi Cyber Security, Malware Analytics, Data Science, Machine Learning, dan Deep Learning, selain itu, penulis juga memiliki beberapa serifikasi internasional di bidang Cyber Security, Digital Forensics, Data Science dan Machine Learning.

BIODATA PENULIS

Kholidiyah Masykuroh, S.T., M.T.
Dosen di Institut Teknologi Telkom Purwokerto

Kholidiyah Masykuroh lahir di Kabupaten Malang, Jawa Timur pada 14 November 1986. Penulis saat ini aktif sebagai mahasiswa Program Doktor Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Angkatan 2022. Penulis telah menyelesaikan pendidikan sarjana pada tahun 2008 di Institut Teknologi Telkom Bandung mengambil jurusan Teknik Telekomunasi. Penulis telah menyelesaikan pendidikan master pada tahun 2013 di Institut Teknologi Bandung dengan mengambil jurusan Teknik Telekomunikasi. Penulis mengawali karir sebagai Dosen di Institut Teknologi Telkom Purwokerto sejak tahun 2019 hingga saat ini dan mengampu salah satu mata kuliah Praktikum Dasar Komputer. Penulis telah menerbitakan dua buku, buku pertama berjudul Sistem Komunikasi Digital Teori, Contoh Soal dan Aplikasi, dan buku kedua berjudul Tutorial Pembuatan Soal Ujian Menggunakan Examview pada tahun 2022. Kritik dan saran lebih lanjut bisa menghubungi penulis melalui email kholidiyah@ittelkom-pwt.ac.id.

BIODATA PENULIS

Fahmy Rinanda Saputri, S.T., M.Eng.
Dosen Program Studi Teknik Fisika
Fakultas Teknik dan Informatika Universitas Multimedia Nusantara

Penulis lahir pada bulan Agustus 1993 di Cilacap. Penulis adalah dosen tetap pada Program Studi Teknik Fisika Fakultas Teknik dan Informatika, Universitas Multimedia Nusantara. Menyelesaikan pendidikan S1 pada Jurusan Teknik Fisika Universitas Gadjah Mada dan melanjutkan studi pada Program Magister Teknik Fisika Universitas Gadjah Mada. Penulis menekuni bidang instrumentasi, fisika bangunan, dan energi baru terbarukan.

BIODATA PENULIS

Laila Qadriah, S.Si., M.S.
Dosen Program Studi Teknik Informatika
Fakultas Teknik Universitas Jabal Ghafur

Penulis lahir di Aceh tanggal 15 Juli 1985. Penulis adalah dosen tetap pada Program Studi Teknik Informatika Fakultas Teknik, Universitas Jabal Ghafur. Menyelesaikan pendidikan S1 pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Syiah Kuala dan melanjutkan S2 pada Master of Applied Mathematics, Dong Hwa University of Taiwan. Mengampu mata kuliah Matematika Terapan dan Riset Teknologi Informatika. Penulis menekuni bidang Menulis dan Meneliti. Kegemarannya dalam menulis dikembangkan sejak kecil. Usahanya tercurahkan dalam beberapa jurnal ilmiah baik jurnal internasional maupun nasional terakreditasi.

BIODATA PENULIS

Sayed Achmady, S.T., M.Kom
Dosen Program Studi Teknik Informatika
Fakultas Teknik Universitas Jabal Ghafur

Penulis lahir di Pidie tanggal 06 Oktober 1985. Penulis adalah dosen tetap pada Fakultas Teknik Program Studi S1 Teknik Informatika Universitas Jabal Ghafur. Penulis juga aktif dalam menerbitkan jurnal baik nasional maupun internasional. Penulis juga berpengalaman di bidang konsultan informatika dan membangun beberapa sistem informasi baik di instansi pemerintahan dan organisasi.

BIODATA PENULIS

Moh Safii
Staf Dosen Prodi Ilmu Perpustakaan Universitas Negeri Malang

Penulis lahir di Kota Malang, alumni Teknik Informatika ITS Surabaya dan S2 Ilmu Perpustakaan Universitas Indonesia. Sehari-hari berdinas di Fakultas Sastra, Prodi Ilmu Perpustakaan Universitas Negeri Malang.

Email : moh.safii@um.ac.id
Web : http://mohsafii.blog.um.ac.id/

BIODATA PENULIS

Ir. Gatot Budi Santoso, M.Kom
Dosen Program Studi Teknik Informatika
Universitas Trisakti-Jakarta

Penulis Lahir di Kebumen, 03 Oktober 1962. Penulis adalah Dosen Tetap pada program studi Teknik Informatika di Universitas Trisakti – Jakarta sejak tahun 2002. Penulis telah menyelesaikan pendidikan Sarjana Teknik Elektro di Fakultas Teknik Universitas Indonesia pada tahun 1989 dan melanjutkan pendidikan Magister pada Ilmu Komputer di Fasilkom Universitas Indonesia dengan selesai pada tahun 1998. Saat ini penulis masih aktif dalam mengajar di Universitas Trisakti, melakukan kegiatan Tri Dharma Perguruan Tinggi dan memiliki kertertarikan serta pengamat didalam perkembangan teknologi digital dan *blockchain*.