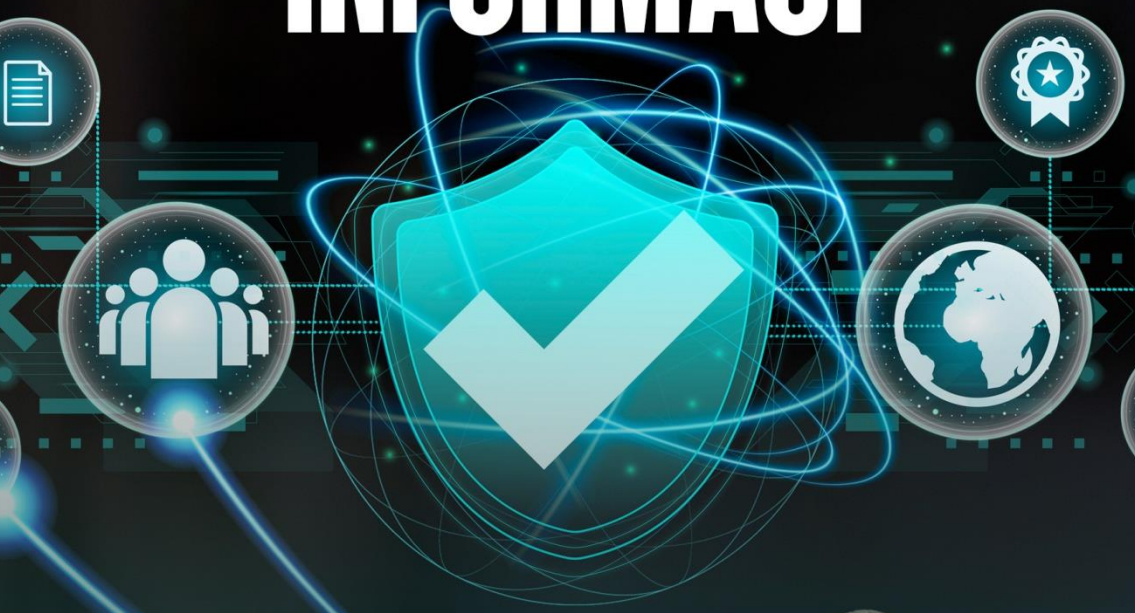
KEAMANAN SISTEM INFORMASI



Fauzan Asrin, S.Kom., M.Kom., Ismarmiaty, S.T., MMSI.,
Dr. Si. Arie Setya Putra, CA, M.T.I., Nuk Ghurroh Setyoningrum, S.Kom, M.Cs.,
Ade Yuliana, S.T., M.T., Juwari, S.Kom., M.Kom., Tati Ernawati, M.T.,
Agni Isador Harsapranata, M.M., M.Kom., Alfa Saleh, M.Kom.,
Novi Aryani Fitri, S.T., M.Tr.Kom., Putri Ariatna Alia S.ST., M.T.,
Nia Ekawati, S.Kom., M.SI., Etza Nofarita, S.T, M.Kom., Dr. Ir. Iwan Setiawan, MT.

KEAMANAN SISTEM
INFORMASI

Fauzan Asrin, S.Kom., M.Kom., Ismarmiaty, ST., MMSI.,
Dr. Si Arie Setya Putra, CA., M.T.I., Nuk Ghurroh Setyoningrum, S.Kom, M.Cs .,
Ade Yuliana, S.T., M.T., Juwari, S.Kom., M.Kom .,
Tati Ernawati, M.T. , Agni Isador Harsapranata, S.Kom.,M.M.,M.Kom.,
Alfa Saleh, M.Kom., Novi Aryani Fitri, S.T., M.Tr.Kom.,
Putri Ariatna Alia, S.ST., M.T. , Nia Ekawati, S.Kom., M. SI.,
Etza Nofarita, ST., M.Kom., Dr. Ir. Iwan Setiawan, MT.

PENAMUDA
MEDIA

Keamanan Sistem Informasi

Copyright© PT Penamudamedia, 2024

Penulis:

Fauzan Asrin, S.Kom., M.Kom., Ismarmiaty, ST., MMSI.,
Dr. Si Arie Setya Putra, CA., M.T.I., Nuk Ghurroh Setyoningrum, S.Kom, M.Cs .,
Ade Yuliana, S.T., M.T., Juwari, S.Kom., M.Kom .,
Tati Ernawati, M.T. , Agni Isador Harsapranata, S.Kom.,M.M.,M.Kom.,
Alfa Saleh, M.Kom., Novi Aryani Fitri, S.T., M.Tr.Kom.,
Putri Ariatna Alia, S.ST., M.T. , Nia Ekawati, S.Kom., M. SI.,
Etza Nofarita, ST., M.Kom., Dr. Ir. Iwan Setiawan, MT.

ISBN:
978-623-8586-06-6

Desain Sampul:
Tim PT Penamuda Media

Tata Letak:
Enbookdesign

Diterbitkan Oleh

PT Penamuda Media
Casa Sidoarium RT 03 Ngentak, Sidoarium Dodeam Sleman Yogyakarta
HP/Whatsapp : +6285700592256
Email : penamudamedia@gmail.com
Web : www.penamuda.com
Instagram : @penamudamedia

Cetakan Pertama, April 2024
xii + 251, 15x23 cm

Hak cipta dilindungi oleh undang-undang
Dilarang memperbanyak sebagian atau seluruh isi buku
tanpa izin Penerbit

Kata Pengantar

Hormat kami,

Kami dengan penuh kehormatan mempersembahkan buku ini tentang keamanan sistem informasi. Buku ini bertujuan untuk menyediakan wawasan mendalam tentang tantangan keamanan yang dihadapi dalam dunia digital yang terus berkembang.

Keamanan sistem informasi menjadi semakin penting di era di mana data menjadi aset berharga. Melalui buku ini, kami mengajak pembaca untuk menjelajahi konsep-konsep kunci dalam keamanan informasi, mulai dari enkripsi data hingga manajemen risiko keamanan, serta teknik dan strategi untuk melindungi sistem informasi dari ancaman cyber yang semakin kompleks.

Dengan pemahaman yang kuat tentang keamanan sistem informasi, pembaca diharapkan dapat mengidentifikasi potensi kerentanan, mengimplementasikan praktik terbaik dalam perlindungan data, dan merancang strategi keamanan yang efektif untuk organisasi mereka.

Kami berharap buku ini dapat menjadi sumber pengetahuan yang berharga bagi para profesional keamanan informasi, pengembang sistem, dan siapa pun yang tertarik untuk memahami lebih dalam tentang perlindungan data di era digital ini.

Terima kasih kepada semua pihak yang telah mendukung pembuatan buku ini, serta kepada pembaca yang siap untuk menjelajahi dunia yang semakin penting dan kompleks dari keamanan sistem informasi.

Daftar Isi

Bab 3

Bab 4

BAB 1

Konsep Dasar Keamanan Sistem Informasi

Fauzan Asrin, S.Kom., M.Kom

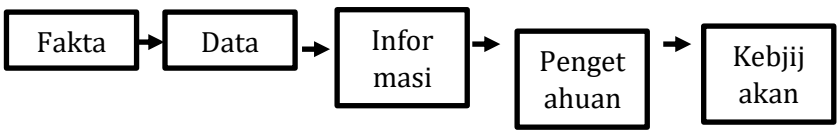
A. Apa Itu Keamanan Informasi?

Keamanan dapat dilihat dari beberapa aspek sebagai suatu yang diidentifikasikan dalam masalah teknis, manajerial, legalitas, dan politis. Aspek-aspek yang disebutkan tersebut merupakan suatu hal penting yang harus diperhatikan misalkan masalah teknis, segala

tindakan yang dilakukan untuk memastikan bahwa data dalam suatu sistem terlindungi dari ancaman, manajerial, merupakan perumusan kebijakan yang terkait perlindungan melalui organisasi terkait, legalitas, merupakan aturan yang telah disahkan untuk dipatuhi oleh siapapun untuk kepentinagan keamanan, dan politis merupakan sebuah kepentingan dalam mengamankan suatu informasi.

Secara Etimologi, Kata informasi ini berasal dari kata bahasa Perancis kuno informacion (tahun 1387) mengambil istilah dari bahasa Latin yaitu informationem yang berarti "konsep, ide atau garis besar,". Informasi ini merupakan kata benda dari informare yang berarti aktivitas Aktifitas dalam "pengetahuan yang dikomunikasikan", (Mulyadi, 2018).

Sementara informasi merupakan kumpulan dari data-data yang banyak dan saling terkait yang memiliki nilai guna bagi yang menggunakannya (Asrin, Saide and Ratna, 2021). Berikut bagan bagaimanan informasi terbentuk:



Gambar 1. Bagan terbentuknya informasi

Gambar 1 diatas merupakan bagan terbentuknya informasi yang diawalai dari kumpulan fakta, fakta merupakan kejadian sesuai dengan kenyataan, jika fakta terkumpul maka akan dapat membentuk data, data merupakan kumpulan fakta yang saling terkait antara satu dengan yang lainnya. Selanjutnya jika sudah memiliki

banyak data maka dapat dibentuk informasi yang memiliki nilai guna. Informasi yang bernilai adalah informasi yang berkualitas sehingga dapat dipertanggungjawabkan (Asrin *et al.,* 2021). Dari informasi yang terkumpul dapat memberikan oengetahuan bagi siapapun yang menggunakannya sehingga dengan adanya pengetahuan dapat membuat kebijakan yang diperlukan oleh oragnisasi ataupun sekelompok orang yang memiliki tujuan yang sama.

B. Perbedaan Kemanan Komputer dan Keamanan Sistem Informasi

Keamanan komputer / cybersecurity atau IT security adalah keamanan informasi yang diaplikasikan kepada komputer dan jaringannya. Computer security atau keamanan komputer bertujuan membantu user agar dapat mencegah penipuan atau mendeteksi adanya usaha penipuan di sebuah sistem yang berbasis informasi. Informasinya sendiri memiliki arti non fisik. Sementara keamanan sistem informasi Keamanan informasi merupakan perlindungan informasi dari berbagai ancaman agar menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, dan meningkatkan return of investment (ROI) serta peluang bisnis (Prasetyaningrum, Finda Nurmayanti and Fallya Azahra, 2022).

C. Aspek Kemanan Sistem Informasi

Aspek keamanan informasi adalah aspek-aspek keamanan informasi dalam sebuah sistem informasi:

1. privasi/kerahasiaan, menjaga kerahasiaan informasi dari semua pihak, kecuali yang memiliki kewenangan;
2. integritas, meyakinkan bahwa data tidak mengalami perubahan oleh yang tidak berhak atau oleh suatu hal lain yang tidak diketahui (misalnya buruknya transmisi data);
3. otentikasi/identifikasi, pengecekan terhadap identitas suatu entitas, bisa berupa orang, kartu kredit atau mesin;
4. tanda tangan, mengesahkan suatu informasi menjadi satu kesatuan di bawah suatu otoritas;
5. otorisasi, pemberian hak/kewenangan kepada entitas lain di dalam sistem;
6. validasi, pengecekan keabsahan suatu otorisasi;
7. kontrol akses, pembatasan akses terhadap entitas di dalam sistem;
8. sertifikasi, pengesahan/pemberian kuasa suatu informasi kepada entitas yang tepercaya;
9. pencatatan waktu, mencatat waktu pembuatan atau keberadaan suatu informasi di dalam sistem;
10. persaksian, memverifikasi pembuatan dan keberadaan suatu informasi di dalam sistem bukan oleh pembuatnya
11. tanda terima, pemberitahuan bahwa informasi telah diterima;
12. konfirmasi, pemberitahuan bahwa suatu layanan informasi telah tersedia;
13. kepemilikan, menyediakan suatu entitas dengan sah untuk menggunakan atau mengirimkan kepada pihak lain;

14. anonimitas, menyamarkan identitas dari entitas terkait dalam suatu proses transaksi;
15. penarikan, penarikan kembali suatu sertifikat atau otoritas.

D. Memahami Peran dari Subjek Pemilik Informasi

Setiap individu dalam organisasi memliki peran yang berbeda-beda terhadap informasi. Peran tersebut ialah cara bagiseluruh pengguna untuk memhami bagaimana peran dan tanggung jawab mereka terhadap informasi yang didapat. Unsur utama yang menjadi subyek dari informasi adalah peran pengguna, pemilik atau custodian terhadap pemilik informasi, yaitu (Setiawan and Yulianto, 2020).:

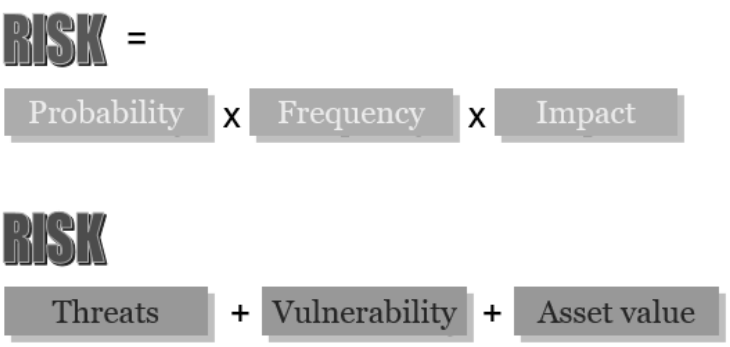
1. Pemilik, merupakan bertanggung jawab atas informasi yang haus dilindungi.
2. Custodian, merupakan pihak yang bertanggung jawab untuk melindungi informasi yang diberikan oleh pemiliknya.
3. Pengguna, merupakan pihak yang dianggap secara rutin dan massif menggunakan informasi sebagai bagian dari pekerjaanya.

E. Resiko dan Sistem Keamanan

Resiko merupakan Sesuatu yang akan terjadi yang dipengaruhi oleh faktor kemungkinan (*likelihood*), berupa ancaman terhadap beberapa kelemahan yang menghasilkan dampak (*impact*) yang merugikan perusahaan. Sistem keamanan ialah Semua tindakan yang dilakukan maupun

aset yang digunakan untuk menjamin keamanan perusahaan. Berikut klasifikasi resiko:

1. Risiko bahaya: kebakaran, banjir, pencurian, dll.
2. Risiko keuangan: harga, kredit, inflasi, dll.
3. Risiko strategis: persaingan, inovasi teknologi, perubahan peraturan, kerusakan citra merek, dll.
4. Risiko operasional: kemampuan TI, operasi bisnis, ancaman keamanan, dll.



Gambar 2. Resiko sebagai fungsi

Gambar 2 diatas merupakan bentuk penggambaran resiko sebagai suatu fungsi, sehingga akhirnya dapat dilihat dari *impact* yang didapatkan dan nilai asset yang diselamatkan. Klasifikasi ancaman dikaitkan dengan informasi dan data sebagai berikut:

1. *Loss of confidentiality of information* merupakan Informasi diperlihatkan kepada pihak yang tidak berhak untuk melihatnya
2. *Loss of integrity of information* merupakan Informasi tidak lengkap, tidak sesuai aslinya, atau telah dimodifikasi

3. *Loss of availability of information* merupakan Informasi tidak tersedia saat dibutuhkan
4. *Loss of authentication of information* merupakan Informasi tidak benar atau tidak sesuai fakta atau sumbernya tidak jelas.

BAB 2

Ancaman Terhadap Keamanan Sistem Informasi

Ismarmiaty, ST., MMSI.

Berkembangnya teknologi, berkembang pula jenis kegiatan yang dapat dilakukan dengan menggunakan teknologi. Perkembangan tersebut seringkali memiliki celah yang digunakan oleh penjahat yang cerdik dan terampil

untuk melakukan eksploitasi dalam sistem *digital*. Kejahatan yang dilakukan dapat berbentuk serangan pada sistem, pada *server* maupun pada *database* yang dimiliki oleh organisasi atau perusahaan (Soesanto, Damayanti and Samuel, 2023). Dengan berkembangnya sistem dan jumlah pengguna sistem, maka berkembang pula banyak data yang disimpan sehingga teknologi penyimpanan, keamanan, distribusi data dan lainnya juga berkembang dari berbagai sisi.

Sistem Informasi berhubungan dengan data yang diproses menjadi informasi yang berguna bagi para penggunanya. Hal ini dapat membantu kegiatan bisnis yang berjalan di perusahaan secara jarak jauh dengan melakukan transaksi melalui aplikasi sistem informasi yang terhubung dengan *internet*. *Internet* yang merupakan jaringan luas yang saling terhubung memberikan kesempatan setiap orang untuk mendapatkan data dan/ atau informasi yang dibutuhkan. Namun, selain untuk mendapatkan keuntungan dengan cara yang baik, beberapa oknum memanfaatkan keterhubungan dalam *internet* untuk melakukan kejahatan dengan objek kejahatan data/ informasi yang dimiliki oleh seseorang. Eksploitasi atau penyalahgunaan keamanan pada sistem informasi merupakan sebuah tindakan diskriminatif dimana seseorang atau suatu pihak melakukan penyerangan yang merugikan kepada sebuah sistem atau *server* (Ginting, Sahara and Nurhaliza Tambunan, 2023).

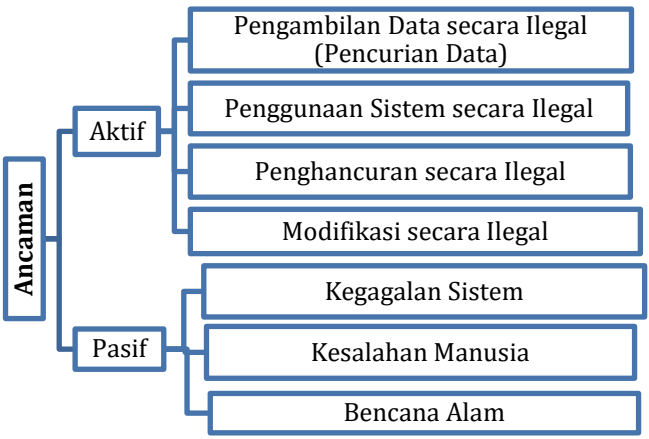
A. Definisi Ancaman

Definisi dari ancaman dalam Kamus Besar Bahasa Indonesia adalah suatu objek tindakan menyatakan maksud (niat, rencana) untuk melakukan sesuatu yang merugikan, menyulitkan, menyusahkan, atau mencelakakan pihak lain

(*Definisi Ancaman*, 2024). Mouna Jouinia dalam penelitiannya (Jouini, Rabai and Aissa, 2014) menjelaskan bahwa ancaman adalah tindakan atau kejadian yang dapat merugikan sebuh organisasi atau perusahaan dalam bentuk uang, pekerjaan, peluang, reputasi sampai dengan kegagalan atau kehancuran sebuah organisasi atau perusahaan.

Ancaman dapat berupa entitas internal yang berasal dari dalam perusahaan, entitas eksternal yang berasal dari luar perusahaan, atau dari entitas eksternal dan internal yang bekerjasama untuk melakukan kejahatan pada perusahaan. Jouini dalam penelitiannya (Jouini, Rabai and Aissa, 2014) menjelaskan bahwa sumber ancaman bisa terdiri dari manusia, lingkungan dan teknologi.

B. Jenis Ancaman



Gambar 1. Bentuk ancaman pada Sistem Informasi

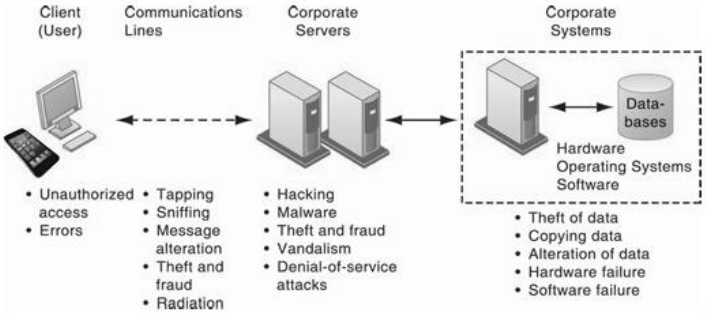
Penelitian (Febriyani, 2023) juga menjelaskan bahwa ancaman yang terjadi pada sistem informasi terbagi dalam 2

bentuk yaitu ancaman aktif dan ancaman pasif. Bentuk dari pembagian ancaman ini dapat dilihat pada Gambar 1. Gambar 1 menjelaskan bahwa ancaman terhadap sistem informasi terbagi menjadi 2 macam, yaitu ancaman aktif dan ancaman pasif. Ancaman pasif terdiri dari pengambilan data secara ilegal (pencurian data), penggunaan sistem secara ilegal, penghancuran data secara ilegal dan modifikasi ilegal data/ informasi, proses maupun hak akses oleh penjahat terhadap sistem, *server* ataupun basis data perusahaan. Selanjutnya ancaman pasif yang terdiri dari tiga bentuk yaitu kegagalan sistem, kesalahan manusia dan bencana alam. Kegagalan sistem dapat terjadi secara pasif dikarenakan kegagalan perangkat keras, perangkat lunak, aplikasi komunikasi, jaringan atau faktor perangkat pendukung yang dapat menyebabkan sistem tidak berjalan sesuai dengan tujuan yang diharapkan. Kesalahan sistem dapat berada pada semua titik sistem baik awal, tengah maupun akhir sistem. Bencana alam seperti gempa bumi, tanah longsor, tsunami, likuifaksi tanah akibat bencana gempa bumi, banjir, kebakaran, badai, hujan lebat dan petir serta bencana alam lainnya. Bencana alam sebagai faktor yang tidak dapat diprediksi secara pasti yang dapat menyebabkan kerusakan secara masif.

C. Klasifikasi Ancaman terhadap Sistem Informasi Berdasarkan Objek Sistem Informasi

Laudon & Laudon menjelaskan pada buku *Management Information Systems: Managing the Digital Firm* (Laudon and Laudon, 2014) bahwa potensi kejahatan pada sistem

informasi terkait akses tidak sah, penyalahgunaan atau penipuan dapat terjadi pada titik manapun dalam jaringan.



Gambar 2. Kejahatan yang terjadi pada Sistem Informasi

Bentuk paling umum kejahatan yang terjadi pada sistem informasi dijelaskan pula oleh Laudon & Laudon pada buku (Laudon and Laudon, 2017) yang dapat dilihat pada Gambar 2. Gambar 2 menjelaskan bahwa klien (pengguna sistem) saling terhubung dengan *server* perusahaan melalui sistem informasi yang terhubung dengan jaringan. Selain itu *Server* Perusahaan juga berhubungan dengan Sistem Perusahaan Pusat yang menangani dan mengelola basis data Perusahaan. Ancaman kejahatan yang dapat terjadi pada titik klien adalah adanya kesalahan pada sistem berupa ketidakterhubungan sistem informasi sehingga tampilan dan/ atau data/ informasi yang dibutuhkan pengguna tidak sesuai. Selain itu *error* dapat terjadi dengan adanya kejahatan pemutusan atau penyalahgunaan akses jaringan data dan informasi pada pengguna untuk menipu atau mengelabui pengguna sistem informasi.

Ancaman lainnya yang dapat terjadi pada jaringan komunikasi antara pengguna sistem dengan *server* adalah adanya kejahatan *tapping*, *sniffing*, *message alteration*, *theft and fraud* dan *radiation*. *Tapping* mengacu pada jenis kejahatan dimana data/ informasi yang direkam secara tidak sah. *Sniffer* adalah jenis program penyadapan yang memantau informasi yang dikirimkan melalui jaringan. Perubahan pesan (*message alteration*) juga dapat terjadi untuk penyalahgunaan data dan informasi atau keputusan yang berdampak pada perusahaan serta penipuan dan pencurian serta radiasi yang dilakukan pada lini komunikasi pada sistem informasi yang bertujuan merugikan perusahaan atau menguntungkan pelaku kejahatan. Pencurian data dapat juga terjadi pada data pengguna untuk mendapatkan keuntungan dengan penyalahgunaan, pemerasan untuk mendapatkan data kembali atau pengambilan keputusan secara tidak sah.

Ancaman yang dapat terjadi pada titik *server* perusahaan adalah *hacking*, *malware*, *theft* dan *fraud*, *vandalism* dan *denial-of-service attacks*. *Hacking* merupakan kegiatan akses sistem komputer secara tidak sah yang bertujuan untuk mendapatkan hak akses. *Malware* mengacu pada program perangkat lunak berbahaya yang disisipkan dalam lini komunikasi pada *server* perusahaan untuk melakukan kejahatan yang dapat berbentuk virus pada komputer, *worm* dan *trojan horse*. Pencurian dan penipuan yang dapat terjadi pada titik *server* perusahaan dapat berupa pencurian dan penyalahgunaan dengan penipuan pada data perusahaan baik data/ informasi *customer*, penjualan hingga data keuangan. Vandalism pada kejahatan sistem informasi mengacu pada serangan

destruktif dan kriminal dengan menghancurkan properti objek yang diserang. Sedangkan, *Denial of Service attack* (DoS) merupakan ancaman penyerangan yang bertujuan untuk melakukan eksploitasi pada sebuah sistem baik pada perangkat maupun *server* dalam jaringan *internet* dengan cara melumpuhkan sistem melalui banjiran permintaan layanan sehingga menghabiskan seluruh sumberdaya sistem sehingga sistem melewati batas maksimum kemampuan layanan dan tidak mampu melakukan pelayanan kepada pengguna selama serangan dilakukan (Ginting, Sahara and Nurhaliza Tambunan, 2023).

Ancaman yang dapat terjadi pada sistem perusahaan dapat terjadi pada beberapa titik antara lain: *hardware*, *operating system* dan *software*. Beberapa jenis ancaman yang dapat terjadi pada titik sistem perusahaan adalah pencurian data perusahaan, duplikasi daya perusahaan, pengubahan data perubahan dengan menyalahgunakan hak akses pada sistem perusahaan, tindakan penggagalan perangkat keras dan perangkat lunak pada perusahaan.

Perubahan manajemen hak akses terhadap fungsi, data dan informasi pada sistem perusahaan baik pada titik pengguna (*user*) ataupun *server* dan sistem perusahaan dapat mempengaruhi perusahaan secara langsung maupun tidak langsung. Manipulasi yang dilakukan dari tindakan kejahatan dapat terjadi dengan berbagai alasan tidak hanya materi namun alasan lainnya seperti politik, balas dendam maupun hanya keinginan untuk memamerkan kemampuan.

D. Dampak Ancaman terhadap Keamanan Sistem Informasi

Jouini menyampaikan bahwa dampak dari ancaman yang terjadi akibat ancaman terhadap keamanan sistem informasi terdiri dari beberapa jenis antara lain:

1. Penghancuran informasi perusahaan dengan tujuan mennganggu atau merusak operasional sistem perusahaan.
2. Korupsi informasi yang berasal dari perubahan data/ informasi perusahaan yang dilakukan secara tidak sah dengan tujuan mengganggu atau merusak data atau keputusan perusahaan.
3. Keterbukaan Informasi (*Information Leaking*) yang merupakan dampak ancaman keamanan sistem informasi dimana informasi penting dan tersembunyi oleh perusahaan diakses dan disebarkan oleh pihak tertentu dalam niat melakukan kejahatan. Tindakan ini menyebabkan pengungkapan informasi secara tidak sah antara lain paparan, intersepsi (penyadapan atau pengalihan), inferensi (penyerangan keamanan) dan intrusi (aktivitas ilegal dalam jaringan).
4. Pencurian layanan merupakan dampak dari penyalahgunaan akses terhadap layanan sistem sehingga menurunkan kinerja dan kemampuan layanan fungsional, data, perangkat lunak atau perangkat keras yang semestinya merespon pengguna.
5. Penolakan layanan merupakan dampak yang disebabkan pemblokiran sumber daya perangkat sistem informasi pada perangkat keras, perangkat lunak atau jaringan yang dilakukan secara sengaja.

6. Peningkatan hak istimewa merupakan dampak dari penyalahgunaan hak akses pengguna oleh pihak yang tidak berwenang untuk melakukan modifikasi data untuk kejahatan. Dampak dari ancaman ini adalah hak akses yang diubah sehingga menyulitkan pemulihan sistem terhadap kerusakan sistem informasi yang dilakukan sebelumnya.
7. Penggunaan ilegal adalah dampak dari ancaman sistem informasi yang meggunakan koneksi jaringan normal untuk dapat menyerang sistem lainnya, penggunaan sistem normal akan menyebabkan sulitnya pelacakan anomali kegiatan pada jaringan yang berjalan, sehingga keamanan yang dibangun harus lebih baik dalam mendeteksi dan mengetahui kesalahan/ anomali kegiatan sebagai serangan kepada keamanan sistem informasi.

Saat ini, ancaman berasal dari berbagai sumber (Jouini, Rabai and Aissa, 2014) dan menyerang ke berbagai titik tujuan sesuai dengan proses bekerja dan tujuan kegiatan pengancaman yang diinginkan pelaku. Eset Indonesia menyatakan bahwa sistem keamanan siber Indonesia mendeteksi 1.225 juta anomali kegiatan di dalam jaringan *internet* setiap hari (Ipungkarti, 2023). Anomali tersebut terdiri dari berbagai bentuk dengan sumber dan tujuan serangan yang berbeda. Laporan ID-SIRTII mencatat jumlah serangan siber yang terjadi selama bulan Januari 2022 sampai dengan bulan Agustus 2023 terjadi sebanyak 1.279.170.904 (1,28 miliyar) serangan siber. Data serangan siber per bulan dapat dilihat pada diagram Gambar 3.

Ancaman pada keamanan sistem informasi akan tetap ada dengan niat kejahatan untuk melakukan penipuan,

penyalahgunaan dan pencurian hak dan data secara tidak sah dengan tujuan mengganggu, menunda, membatalkan, merusak atau menghancurkan tujuan objek kejahatannya. Ancaman dapat berupa fisik dan non fisik dan dapat bersumber dari dan bertujuan ke titik manapun pada internal dan eksternal sistem perusahaan. Dengan adanya keamanan informasi maka akan berkembang pula teknik dan strategi ancaman serangan siber baik secara langsung maupun secara tidak langsung untuk tetap dapat melakukan tindak kejahatan. Perkembangan teknik dan serangan keamanan sistem informasi akan menuntut perbaikan keamanan dengan mengembangkan sistem keamanan.

BAB

3

Kerangka Keamanan Sistem Informasi

Dr. Si Arie Setya Putra, CA., M.T.I

A. Dasar-Dasar Keamanan Sistem Informasi

1. Konsep Dasar Keamanan

Faktor keamanan sistem informasi meliputi berbagai aspek yang penting untuk melindungi data dan infrastruktur teknologi informasi dari ancaman dan risiko yang berpotensi merugikan. Beberapa faktor utama keamanan sistem informasi meliputi:

a. Keamanan Data: Melindungi data dari akses yang tidak sah, perubahan yang tidak diizinkan, dan kerusakan atau kehilangan.
b. Keamanan Jaringan: Memastikan bahwa jaringan komputer terlindungi dari serangan seperti malware, phishing, dan serangan DDoS (Denial of Service).
c. Pengelolaan Akses: Mengontrol akses pengguna agar hanya orang yang berwenang yang dapat mengakses data dan sumber daya sistem.
d. Enkripsi: Menggunakan teknik enkripsi untuk mengamankan komunikasi dan data yang disimpan, sehingga bahkan jika data dicuri, sulit untuk dibaca.
e. Keamanan Fisik: Melindungi infrastruktur fisik sistem informasi, seperti server dan perangkat keras, dari akses yang tidak sah atau kecelakaan.
f. Pengelolaan Identitas: Memastikan bahwa identitas pengguna diverifikasi dan diotorisasi sebelum diberikan akses ke sistem atau data.
g. Pemantauan dan Deteksi Ancaman: Menggunakan alat dan teknik untuk memantau aktivitas sistem dan mendeteksi adanya ancaman atau serangan yang sedang berlangsung.
h. Kebijakan Keamanan: Menerapkan kebijakan dan prosedur keamanan yang jelas dan diterapkan secara konsisten oleh semua pengguna dan administrator sistem.
i. Pemulihan Bencana: Memiliki rencana pemulihan bencana yang efektif untuk memulihkan sistem

dan data dalam situasi kegagalan atau kerusakan yang parah.

j. Kesadaran Pengguna: Memberikan pelatihan dan edukasi kepada pengguna tentang praktik keamanan yang aman dan pentingnya melindungi informasi sensitif.

Dengan memperhatikan faktor-faktor ini dan menerapkan langkah-langkah yang sesuai, organisasi dapat meningkatkan keamanan sistem informasi mereka dan melindungi data serta operasi mereka dari ancaman yang berpotensi merugikan.

2. Aktif, Pasif, dan Kontrol Keamanan

Aktif, pasif, dan kontrol keamanan adalah konsep yang sering digunakan dalam konteks keamanan informasi dan teknologi. Berikut adalah penjelasan singkat tentang masing-masing konsep:

a. Aktif keamanan: Ini mengacu pada tindakan langsung yang diambil untuk mencegah atau merespons ancaman keamanan yang sedang terjadi. Contoh tindakan aktif keamanan meliputi penggunaan firewall untuk memblokir akses yang tidak sah, pemindaian antivirus untuk mendeteksi dan menghapus malware, serta mengimplementasikan kebijakan akses yang ketat untuk mencegah akses yang tidak sah ke sistem atau data.

b. Pasif keamanan: Ini mencakup langkah-langkah yang diambil untuk mempersiapkan dan memitigasi dampak dari ancaman keamanan, tetapi tidak langsung bertindak untuk mencegah

atau merespons secara langsung. Contoh pasif keamanan termasuk mencadangkan data secara teratur untuk memulihkan sistem jika terjadi kerusakan atau serangan, mengenkripsi data untuk melindungi privasi, dan menyimpan catatan kegiatan sistem untuk audit dan investigasi.

c. Kontrol keamanan: Ini mencakup kebijakan, prosedur, dan mekanisme yang diterapkan untuk mengelola dan mengendalikan akses ke sumber daya dan informasi yang sensitif. Kontrol keamanan bisa aktif atau pasif. Aktif dalam artian menerapkan tindakan langsung seperti yang dijelaskan di atas, sedangkan pasif dalam artian mengatur aturan, kebijakan, dan prosedur untuk mengelola akses, mengawasi aktivitas pengguna, dan membatasi risiko keamanan.

Kombinasi dari ketiga konsep ini penting untuk menciptakan lingkungan keamanan yang efektif dalam teknologi informasi dan sistem komputer. Dengan menggabungkan tindakan aktif dan pasif serta menerapkan kontrol keamanan yang tepat, organisasi dapat mengurangi risiko keamanan dan melindungi data dan sistem mereka dari ancaman yang ada dan potensial.

3. Trilema Keamanan: Keamanan, Ketersediaan, dan Integritas

Trilema keamanan, yang terdiri dari keamanan, ketersediaan, dan integritas, adalah konsep fundamental dalam keamanan informasi dan teknologi. Konsep ini menyatakan bahwa ketika Anda berupaya

untuk meningkatkan satu aspek dari trilema keamanan, biasanya akan ada dampak pada setidaknya satu atau kedua aspek lainnya. Berikut adalah penjelasan singkat tentang masing-masing aspek:

a. Keamanan: Merujuk pada upaya untuk melindungi sistem, data, dan informasi dari akses yang tidak sah, perubahan yang tidak sah, atau kerusakan. Upaya keamanan meliputi penerapan kontrol akses, enkripsi data, pemantauan kegiatan, dan penerapan kebijakan keamanan yang ketat.
b. Ketersediaan: Mengacu pada keadaan di mana sistem atau layanan tersedia dan beroperasi ketika dibutuhkan oleh pengguna. Upaya untuk memastikan ketersediaan meliputi redundansi sistem, backup data, pemulihan bencana, dan manajemen kapasitas untuk menghindari kelebihan beban.
c. Integritas: Ini berkaitan dengan keaslian, kebenaran, dan konsistensi data. Integritas data menjamin bahwa data tidak dimanipulasi atau diubah secara tidak sah, baik secara sengaja maupun tidak sengaja. Upaya untuk mempertahankan integritas meliputi penggunaan tanda tangan digital, hash, dan kontrol versi.

Trilema keamanan menunjukkan bahwa ada trade-off antara ketiga aspek tersebut. Misalnya, meningkatkan keamanan dengan menerapkan kontrol akses yang ketat mungkin dapat mengurangi ketersediaan dengan membatasi akses pengguna yang sah. Atau, upaya untuk mempertahankan ketersediaan

dengan menggunakan sistem redundansi yang kuat dapat meningkatkan biaya dan mengurangi efisiensi, yang kemudian dapat mempengaruhi keamanan karena sumber daya yang dibutuhkan untuk memelihara sistem.

Oleh karena itu, dalam merancang dan mengelola sistem informasi dan teknologi, penting untuk memperhitungkan dan menyeimbangkan kebutuhan untuk keamanan, ketersediaan, dan integritas agar dapat memenuhi tantangan trilema keamanan.

B. Tantangan Keamanan Sistem Informasi

1. Ancaman Terkini dalam Dunia Digital

Ancaman terkini dalam dunia digital terus berkembang seiring dengan perkembangan teknologi. Beberapa ancaman yang saat ini banyak diperhatikan di antaranya adalah:

a. Serangan Ransomware: Ransomware adalah jenis malware yang mengenkripsi data korban dan meminta tebusan (ransom) untuk mendapatkan kunci dekripsi. Serangan ransomware dapat menyebabkan kerugian finansial yang besar dan gangguan operasional yang signifikan bagi organisasi dan individu.

b. Serangan Phishing: Phishing adalah teknik penipuan di mana penyerang mencoba untuk memperoleh informasi sensitif seperti kata sandi, informasi kartu kredit, atau data pribadi dengan

menyamar sebagai entitas tepercaya. Serangan phishing dapat dilakukan melalui email, pesan teks, atau media sosial.

c. Serangan DDoS (Distributed Denial of Service): Serangan DDoS bertujuan untuk membuat layanan atau situs web tidak tersedia bagi pengguna dengan membanjiri server target dengan lalu lintas internet yang tidak sah. Serangan ini dapat menyebabkan gangguan serius pada layanan online dan merugikan reputasi bisnis.
d. Pelanggaran Data: Pelanggaran data terjadi ketika data sensitif, seperti informasi pribadi atau informasi keuangan, dicuri atau diakses secara tidak sah. Pelanggaran data dapat merugikan baik individu maupun organisasi, dengan potensi dampak keuangan dan reputasi yang serius.
e. Serangan Malware Lanjutan (Advanced Persistent Threats/APTs): APTs adalah serangan yang sangat terorganisir dan canggih yang dilakukan oleh penyerang yang bertujuan untuk memperoleh akses yang tidak sah ke jaringan atau sistem untuk jangka waktu yang lama. Penyerang APT sering kali memiliki sumber daya dan keterampilan yang tinggi, dan sering kali menjadi ancaman yang sulit dideteksi dan diatasi.
f. Kerentanan Perangkat IoT (Internet of Things): Perangkat IoT, seperti kamera keamanan pintar atau perangkat rumah pintar lainnya, rentan terhadap serangan karena seringkali kekurangan keamanan yang memadai. Penyerang dapat memanfaatkan kerentanan ini untuk mengambil

alih perangkat, mengumpulkan data pribadi, atau bahkan mengakses jaringan yang lebih luas.

g. Serangan terhadap Blockchain dan Cryptocurrency: Meskipun teknologi blockchain memiliki reputasi keamanan yang kuat, serangan terhadap cryptocurrency dan infrastruktur blockchain tetap menjadi ancaman. Ini termasuk serangan 51% terhadap jaringan blockchain, serangan kelemahan protokol, dan serangan phishing yang ditargetkan terhadap pemegang cryptocurrency.
h. Ancaman AI (Artificial Intelligence): Sementara AI dapat digunakan untuk meningkatkan keamanan digital melalui deteksi ancaman yang lebih cepat dan analisis risiko yang lebih baik, namun ada juga potensi untuk penggunaan yang jahat. Serangan menggunakan teknik kecerdasan buatan dapat menjadi lebih canggih dan sulit dideteksi.

Ini hanya beberapa contoh dari berbagai macam ancaman yang ada dalam dunia digital saat ini. Untuk melindungi diri dari ancaman tersebut, penting untuk mengadopsi praktik keamanan yang baik, termasuk penggunaan perangkat lunak keamanan yang terbaru, pelatihan pengguna tentang kesadaran keamanan, dan pemantauan aktif terhadap kegiatan jaringan dan sistem.

2. Faktor Internal dan Eksternal yang Mempengaruhi Keamanan

Keamanan sistem informasi dipengaruhi oleh berbagai faktor, baik internal maupun eksternal. Berikut adalah beberapa contoh faktor internal dan eksternal yang dapat mempengaruhi keamanan:

a. Faktor Internal
   1) Kebijakan dan Prosedur Keamanan: Kebijakan dan prosedur keamanan internal seperti kebijakan sandi yang kuat, kebijakan akses yang ketat, dan prosedur pengelolaan perangkat lunak dapat memengaruhi tingkat keamanan sistem.
   2) Kultur Keamanan Organisasi: Tingkat kesadaran keamanan dan kepedulian terhadap keamanan informasi di antara karyawan dan anggota organisasi dapat memainkan peran penting dalam memastikan keamanan sistem.
   3) Manajemen Risiko: Kemampuan organisasi untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi internal dapat memengaruhi seberapa baik sistem dapat dilindungi dari ancaman.
   4) Kualitas Pengembangan Perangkat Lunak: Proses pengembangan perangkat lunak yang baik, termasuk pengujian keamanan dan pemeliharaan yang berkualitas, dapat memastikan bahwa aplikasi dan sistem tidak memiliki kerentanan yang dapat dimanfaatkan oleh penyerang.

5) Kapasitas dan Sumber Daya IT: Kapasitas dan sumber daya IT internal, termasuk personel keamanan yang terlatih dan anggaran keamanan yang cukup, dapat mempengaruhi kemampuan organisasi untuk melindungi sistem dari ancaman.

b. Faktor Eksternal:
   1) Ancaman Cyber: Ancaman dari penyerang eksternal, seperti hacker, kelompok kriminal, atau negara asing, dapat mempengaruhi keamanan sistem. Ini dapat termasuk serangan malware, serangan phishing, atau serangan DDoS.
   2) Regulasi dan Kepatuhan: Persyaratan regulasi dan kepatuhan seperti GDPR (General Data Protection Regulation) di Uni Eropa atau HIPAA (Health Insurance Portability and Accountability Act) di Amerika Serikat dapat mempengaruhi praktik keamanan dan tanggung jawab organisasi dalam melindungi data.
   3) Perkembangan Teknologi: Perkembangan teknologi baru seperti Internet of Things (IoT), cloud computing, dan kecerdasan buatan (AI) dapat memperluas serangan potensial dan mempengaruhi strategi keamanan informasi.
   4) Ekonomi dan Industri: Faktor ekonomi dan industri, seperti persaingan pasar, perubahan kebutuhan pelanggan, dan tren industri, juga dapat mempengaruhi prioritas dan sumber

daya yang dialokasikan untuk keamanan informasi.

5) Lingkungan Politik dan Sosial: Faktor politik dan sosial, seperti konflik internasional atau perubahan regulasi pemerintah, juga dapat mempengaruhi ancaman keamanan informasi.

Dengan memahami faktor-faktor ini, organisasi dapat mengembangkan strategi keamanan informasi yang holistik dan efektif untuk melindungi sistem mereka dari ancaman yang ada dan potensial.

3. Perkembangan Teknologi dan Risiko Keamanan Terkait

Perkembangan teknologi membawa banyak manfaat bagi kehidupan kita, tetapi juga membawa risiko keamanan yang terkait. Berikut adalah beberapa contoh perkembangan teknologi terkini dan risiko keamanan yang terkait:

a. Internet of Things (IoT):
   1) Perkembangan: IoT menghubungkan perangkat fisik ke internet, memungkinkannya untuk berkomunikasi dan berbagi data dengan satu sama lain.
   2) Risiko Keamanan: Perangkat IoT sering kali memiliki keamanan yang lemah, rentan terhadap serangan yang dapat dimanfaatkan oleh penyerang untuk mengakses jaringan atau mencuri data.

b. Cloud Computing:
   1) Perkembangan: Layanan cloud computing memungkinkan organisasi untuk menyimpan,

mengelola, dan mengakses data dan aplikasi melalui internet.

2) Risiko Keamanan: Meskipun cloud computing menawarkan fleksibilitas dan skalabilitas, keamanan data di cloud dapat menjadi masalah jika tidak dilindungi dengan benar. Ancaman seperti pencurian data, akses yang tidak sah, dan kehilangan data dapat timbul.

c. Kecerdasan Buatan (Artificial Intelligence):
   1) Perkembangan: AI digunakan dalam berbagai aplikasi, termasuk analisis data, pengoptimalan proses bisnis, dan kecerdasan keamanan.
   2) Risiko Keamanan: Penyalahgunaan AI dapat menyebabkan serangan yang lebih canggih dan sulit dideteksi, seperti serangan phishing yang ditingkatkan oleh AI atau serangan yang memanfaatkan kelemahan dalam algoritma machine learning.

d. Blockchain:
   1) Perkembangan: Blockchain adalah teknologi yang mendasari cryptocurrency dan dapat digunakan untuk menyimpan data secara aman dan transparan.
   2) Risiko Keamanan: Meskipun blockchain dianggap aman karena sifatnya yang terdesentralisasi dan transparan, masih ada risiko keamanan terkait dengan pencurian kunci pribadi, serangan 51%, dan kerentanan dalam implementasi kontrak pintar.

e. Perangkat Lunak As A Service (SaaS):

1) Perkembangan: SaaS memungkinkan organisasi untuk mengakses perangkat lunak melalui internet tanpa harus menginstal atau mengelola aplikasi secara lokal.
2) Risiko Keamanan: Keamanan data dalam SaaS tergantung pada penyedia layanan, dan pengguna harus memastikan bahwa penyedia menyediakan langkah-langkah keamanan yang memadai, seperti enkripsi data dan akses yang terkelola dengan baik.

f. Internet Kecepatan Tinggi dan Komputasi Edge:
1) Perkembangan: Internet kecepatan tinggi dan komputasi edge memungkinkan pengolahan data yang lebih cepat dan respons yang lebih dekat dengan sumber data.
2) Risiko Keamanan: Penyimpanan dan pengolahan data yang tersebar dapat meningkatkan risiko keamanan karena perangkat dan titik akses tambahan yang perlu diamankan.
3) Dengan memahami risiko yang terkait dengan perkembangan teknologi terkini ini, organisasi dapat mengambil langkah-langkah untuk melindungi sistem dan data mereka. Ini termasuk mengadopsi praktik keamanan terbaik, seperti enkripsi data, otentikasi multi-faktor, pemantauan keamanan yang terus-menerus, dan pelatihan kesadaran keamanan untuk karyawan.

C. Klasifikasi Aset dan Identifikasi Risiko

1. Klasifikasi Aset Informasi

Klasifikasi aset informasi adalah proses mengidentifikasi dan mengelompokkan aset informasi berdasarkan nilai, sensitivitas, dan pentingannya bagi organisasi. Ini membantu organisasi dalam mengelola risiko keamanan informasi dengan fokus pada perlindungan aset yang paling berharga atau kritis. Berikut adalah beberapa kategori umum dalam klasifikasi aset informasi:

a. Data Sensitif: Ini adalah jenis data yang memiliki tingkat sensitivitas yang tinggi dan memerlukan perlindungan tambahan. Contohnya termasuk informasi pribadi (seperti NIK, alamat, atau nomor kartu kredit), informasi keuangan, rahasia dagang, atau rancangan produk.
b. Properti Intelektual: Properti intelektual mencakup informasi atau kekayaan immaterial yang diciptakan oleh organisasi, seperti paten, merek dagang, hak cipta, dan desain industri. Perlindungan properti intelektual sangat penting untuk mencegah pencurian atau penggunaan yang tidak sah.
c. Sistem dan Infrastruktur: Ini mencakup perangkat keras, perangkat lunak, dan infrastruktur teknologi informasi yang digunakan oleh organisasi. Hal ini termasuk server, jaringan, perangkat komputasi, sistem operasi, dan aplikasi bisnis.

d. Dokumen dan Catatan: Dokumen dan catatan organisasi yang berisi informasi penting atau rahasia, seperti kontrak, laporan keuangan, kebijakan internal, atau dokumen hukum, juga merupakan aset informasi yang harus diidentifikasi dan dilindungi.
e. Aset Manusia: Karyawan, mitra bisnis, dan anggota organisasi lainnya juga merupakan aset informasi. Hal ini mencakup pengetahuan, keahlian, dan hubungan yang dimiliki oleh individu yang dapat memberikan nilai tambah bagi organisasi.
f. Aset Fisik: Aset fisik yang digunakan untuk mengolah atau menyimpan informasi, seperti komputer, laptop, server, perangkat penyimpanan, atau peralatan jaringan, juga perlu diklasifikasikan dan dilindungi.

Setelah aset informasi diidentifikasi dan diklasifikasikan, organisasi dapat menetapkan tingkat perlindungan yang sesuai untuk setiap kategori aset tersebut. Ini membantu dalam alokasi sumber daya keamanan yang efisien, memastikan bahwa aset yang paling penting atau sensitif menerima tingkat perlindungan yang paling tinggi. Selain itu, hal ini memungkinkan organisasi untuk mengidentifikasi potensi ancaman dan risiko yang terkait dengan setiap kategori aset, serta mengambil tindakan yang sesuai untuk mengurangi risiko tersebut.

2. Proses Identifikasi Risiko

Proses identifikasi risiko merupakan langkah awal dalam manajemen risiko, yang bertujuan untuk mengidentifikasi, menganalisis, dan memahami potensi ancaman atau risiko yang dapat mempengaruhi tujuan atau keberhasilan suatu proyek, organisasi, atau sistem. Berikut adalah langkah-langkah umum dalam proses identifikasi risiko:

a. Penetapan Konteks: Langkah pertama dalam identifikasi risiko adalah memahami konteks dan lingkungan di mana risiko akan diidentifikasi. Ini melibatkan menetapkan tujuan, cakupan, dan batasan proses identifikasi risiko serta mengidentifikasi pemangku kepentingan yang relevan.
b. Identifikasi Sumber Risiko: Identifikasi sumber risiko melibatkan mengidentifikasi semua faktor atau entitas yang dapat menyebabkan atau berkontribusi terhadap timbulnya risiko. Ini dapat mencakup faktor internal (seperti kebijakan organisasi, proses bisnis, atau infrastruktur teknologi) dan faktor eksternal (seperti perubahan regulasi, kondisi pasar, atau ancaman lingkungan).
c. Identifikasi Ancaman atau Peristiwa: Langkah selanjutnya adalah mengidentifikasi dan menggambarkan berbagai ancaman atau peristiwa yang dapat terjadi, baik secara potensial maupun aktual. Ini dapat mencakup ancaman keamanan, risiko operasional, risiko keuangan, risiko lingkungan, dan lain-lain.

d. Analisis Konsekuensi: Setelah ancaman atau peristiwa diidentifikasi, langkah berikutnya adalah menganalisis konsekuensi atau dampak potensial dari masing-masing risiko tersebut terhadap tujuan atau keberhasilan proyek, organisasi, atau sistem. Ini melibatkan mengevaluasi konsekuensi dalam hal kerugian finansial, reputasi, kesehatan dan keselamatan, atau efisiensi operasional.
e. Analisis Probabilitas: Selain menganalisis konsekuensi, penting juga untuk mengevaluasi probabilitas atau kemungkinan terjadinya risiko. Ini melibatkan penilaian tentang seberapa sering atau seberapa mungkin risiko tersebut terjadi, berdasarkan informasi historis, pengetahuan ahli, atau analisis statistik.
f. Dokumentasi Risiko: Setelah risiko diidentifikasi dan dianalisis, langkah terakhir adalah mendokumentasikan hasilnya dalam bentuk daftar risiko atau register risiko. Dokumen ini harus mencakup deskripsi risiko, sumber atau penyebabnya, konsekuensi potensial, probabilitas terjadinya, serta rekomendasi untuk manajemen atau mitigasi risiko.
g. Proses identifikasi risiko harus dilakukan secara sistematis dan melibatkan partisipasi dari berbagai pemangku kepentingan yang relevan. Selain itu, proses ini harus diperbarui secara berkala untuk memastikan bahwa risiko yang baru muncul atau berubah dapat diidentifikasi dan dikelola dengan baik.

3. Metode Penilaian Risiko

Terdapat beberapa metode penilaian risiko yang dapat digunakan untuk mengukur dan mengevaluasi risiko dalam suatu organisasi atau proyek. Beberapa metode yang umum digunakan termasuk:

a. Metode Analisis Kuantitatif: Metode ini melibatkan pengukuran risiko dalam bentuk angka atau data kuantitatif. Beberapa teknik dalam metode ini antara lain:
   1) Analisis Probabilitas dan Dampak: Risiko dievaluasi dengan mengidentifikasi probabilitas terjadinya serta dampaknya, dan kemudian dikalikan bersama untuk menghitung risiko keseluruhan.
   2) Analisis Skenario: Metode ini melibatkan pembuatan skenario-skenario yang mungkin terjadi dan menghitung dampak finansial atau operasional dari setiap skenario.
   3) Metode Penilaian Finansial: Risiko dievaluasi berdasarkan potensi kerugian finansial yang mungkin terjadi, dengan menghitung nilai ekspektasi dari kerugian yang diharapkan.

b. Metode Analisis Kualitatif: Metode ini menggunakan penilaian subyektif dan deskriptif untuk mengidentifikasi, mengukur, dan mengevaluasi risiko. Beberapa teknik dalam metode ini antara lain:
   1) Metode Checklist: Risiko dievaluasi dengan menggunakan daftar pertanyaan atau checklist yang mencakup berbagai kategori risiko.

2) Analisis SWOT (Strengths, Weaknesses, Opportunities, Threats): Risiko dievaluasi dengan mengevaluasi kekuatan, kelemahan, peluang, dan ancaman yang terkait dengan suatu situasi atau keputusan.
3) Analisis Delphi: Metode ini melibatkan pengumpulan pendapat dari panel ahli melalui serangkaian kuesioner atau sesi diskusi untuk mencapai konsensus tentang risiko.

c. Metode Hybrid atau Kombinasi: Beberapa organisasi menggunakan pendekatan campuran yang menggabungkan elemen-elemen dari analisis kuantitatif dan kualitatif untuk mendapatkan pemahaman yang lebih lengkap tentang risiko. Pendekatan ini dapat menggabungkan pengukuran kuantitatif dampak finansial dengan penilaian kualitatif tentang probabilitas atau kompleksitas risiko.

Pemilihan metode penilaian risiko tergantung pada kebutuhan, sumber daya yang tersedia, kompleksitas risiko, dan preferensi organisasi atau proyek. Yang terpenting adalah bahwa metode yang dipilih harus relevan, komprehensif, dan dapat memberikan wawasan yang berharga untuk pengambilan keputusan terkait manajemen risiko. Selain itu, proses penilaian risiko harus dilakukan secara berkala untuk memastikan bahwa evaluasi risiko tetap relevan dan up-to-date seiring dengan perubahan lingkungan atau kondisi operasional.

D. Kebijakan dan Prosedur Keamanan

1. Pentingnya Kebijakan Keamanan

Kebijakan keamanan merupakan pondasi yang krusial dalam upaya menjaga keamanan informasi dan sistem dalam sebuah organisasi. Berikut adalah beberapa alasan mengapa kebijakan keamanan sangat penting:

a. Mengatur Tindakan Karyawan: Kebijakan keamanan memberikan pedoman tentang perilaku yang diharapkan dari karyawan dalam hal penggunaan teknologi informasi dan pengelolaan informasi sensitif. Ini termasuk praktik yang aman seperti penggunaan kata sandi yang kuat, penanganan data sensitif dengan hati-hati, dan melaporkan kejadian keamanan yang mencurigakan.
b. Melindungi Informasi Penting: Kebijakan keamanan membantu melindungi informasi penting dari akses yang tidak sah, penggunaan yang tidak sah, atau pengungkapan yang tidak diotorisasi. Dengan menetapkan aturan tentang siapa yang memiliki akses ke informasi tertentu dan bagaimana informasi tersebut harus dilindungi, organisasi dapat mengurangi risiko pencurian atau kebocoran data.
c. Kepatuhan Hukum dan Regulasi: Banyak industri diatur oleh undang-undang dan peraturan yang memerlukan organisasi untuk melindungi informasi pribadi atau sensitif. Kebijakan keamanan membantu organisasi untuk mematuhi

persyaratan peraturan tersebut dengan menetapkan standar keamanan yang diperlukan dan prosedur pengelolaan risiko.

d. Mengurangi Risiko dan Kerugian: Dengan menerapkan kebijakan keamanan yang baik, organisasi dapat mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan yang terkait dengan penggunaan teknologi informasi. Ini dapat mengurangi kemungkinan kerugian finansial, reputasi, atau operasional akibat insiden keamanan.
e. Meningkatkan Kesadaran Keamanan: Kebijakan keamanan membantu meningkatkan kesadaran keamanan di seluruh organisasi dengan menyoroti pentingnya keamanan informasi dan memberikan pedoman tentang cara melindungi diri dari ancaman keamanan. Ini termasuk pelatihan reguler tentang kesadaran keamanan dan edukasi tentang ancaman keamanan yang sedang berlangsung.
f. Membangun Kepercayaan Pelanggan dan Mitra Bisnis: Dengan memiliki kebijakan keamanan yang kuat, organisasi dapat membangun kepercayaan dengan pelanggan dan mitra bisnis dengan menunjukkan komitmen mereka untuk melindungi data dan informasi yang mereka tangani. Ini dapat meningkatkan reputasi organisasi dan membedakan mereka dari pesaing.

Secara keseluruhan, kebijakan keamanan membantu organisasi untuk melindungi informasi penting, mematuhi persyaratan hukum dan regulasi,

mengurangi risiko dan kerugian, meningkatkan kesadaran keamanan, dan membangun kepercayaan dengan pelanggan dan mitra bisnis. Oleh karena itu, kebijakan keamanan merupakan aspek krusial dalam strategi keamanan informasi suatu organisasi.

2. Proses Pembuatan Kebijakan

Proses pembuatan kebijakan keamanan melibatkan serangkaian langkah yang sistematis untuk mengembangkan dokumen yang jelas, komprehensif, dan efektif dalam mengatur praktik keamanan informasi dalam sebuah organisasi. Berikut adalah langkah-langkah umum dalam proses pembuatan kebijakan keamanan:

a. Penetapan Ruang Lingkup: Langkah pertama adalah menentukan ruang lingkup kebijakan keamanan, yaitu topik atau area yang akan dicakup oleh kebijakan tersebut. Ini bisa termasuk aspek-aspek seperti penggunaan kata sandi, akses data, penggunaan perangkat seluler, atau tindakan darurat dalam menghadapi insiden keamanan.
b. Pengumpulan Informasi: Setelah ruang lingkup ditetapkan, langkah berikutnya adalah mengumpulkan informasi yang relevan tentang praktik keamanan yang ada, peraturan hukum yang berlaku, dan standar industri atau kepatuhan yang diperlukan. Ini dapat melibatkan penelitian online, konsultasi dengan ahli keamanan, atau tinjauan dokumen kebijakan yang ada.
c. Penyusunan Draft Kebijakan: Berdasarkan informasi yang dikumpulkan, susunlah draft

kebijakan keamanan yang mencakup tujuan kebijakan, lingkup, kewajiban dan tanggung jawab, prosedur operasional, serta langkah-langkah perlindungan yang diperlukan. Pastikan kebijakan tersebut jelas, mudah dimengerti, dan sesuai dengan kebutuhan organisasi.

d. Konsultasi dan Review: Setelah draft kebijakan disusun, lakukanlah konsultasi dengan pemangku kepentingan yang relevan, termasuk manajemen senior, departemen keamanan informasi, dan departemen terkait lainnya. Mintalah masukan dan umpan balik untuk memastikan kebijakan mencakup semua aspek yang diperlukan dan diterima oleh seluruh organisasi.
e. Pengesahan dan Persetujuan: Setelah revisi yang diperlukan dilakukan, kebijakan keamanan harus disahkan atau disetujui oleh manajemen senior atau dewan direksi organisasi. Pastikan ada mekanisme untuk memastikan bahwa kebijakan tersebut memiliki dukungan resmi dari pihak yang berwenang.
f. Pengimplementasian dan Komunikasi: Setelah kebijakan disahkan, langkah berikutnya adalah mengimplementasikannya dalam operasi sehari-hari organisasi. Ini melibatkan komunikasi kebijakan kepada semua karyawan dan pemangku kepentingan yang relevan, serta memberikan pelatihan atau pembekalan yang diperlukan untuk memastikan pemahaman dan kepatuhan terhadap kebijakan tersebut.

g. Pemantauan dan Evaluasi: Proses pembuatan kebijakan keamanan tidak berakhir setelah kebijakan diimplementasikan. Penting untuk terus memantau dan mengevaluasi kepatuhan terhadap kebijakan tersebut, serta efektivitasnya dalam mencapai tujuan keamanan informasi organisasi. Lakukan evaluasi reguler dan perbarui kebijakan sesuai kebutuhan.

Dengan mengikuti langkah-langkah ini, organisasi dapat mengembangkan kebijakan keamanan informasi yang kuat dan efektif yang dapat melindungi aset dan informasi sensitif mereka dari ancaman keamanan.

3. Implementasi dan Penegakan Kebijakan

Implementasi dan penegakan kebijakan keamanan adalah langkah penting setelah kebijakan dibuat dan disahkan. Berikut adalah beberapa langkah yang dapat diambil untuk melaksanakan dan menegakkan kebijakan keamanan dengan efektif:

a. Pelatihan dan Pendidikan: Lakukan pelatihan kepada seluruh karyawan dan pemangku kepentingan yang terlibat tentang isi kebijakan keamanan. Pastikan mereka memahami pentingnya kebijakan tersebut, serta tindakan yang harus mereka ambil untuk mematuhi kebijakan.
b. Komunikasi yang Jelas: Sampaikan kebijakan keamanan secara jelas kepada seluruh anggota organisasi. Sediakan salinan kebijakan kepada semua karyawan dan pastikan bahwa mereka memiliki akses yang mudah untuk merujuk kembali kebijakan tersebut.

c. Penetapan Peran dan Tanggung Jawab: Tentukan peran dan tanggung jawab secara jelas bagi setiap anggota organisasi dalam menerapkan kebijakan keamanan. Pastikan bahwa semua orang memahami peran mereka dalam menjaga keamanan informasi.
d. Penerapan Teknologi Pendukung: Gunakan teknologi pendukung seperti perangkat lunak keamanan, enkripsi data, sistem otentikasi, dan alat pemantauan untuk mendukung penerapan kebijakan keamanan. Pastikan bahwa sistem dan infrastruktur teknologi sesuai dengan standar keamanan yang ditetapkan dalam kebijakan.
e. Pemeriksaan dan Audit Reguler: Lakukan pemeriksaan dan audit reguler untuk memastikan kepatuhan terhadap kebijakan keamanan. Tinjau kembali praktik kerja dan sistem untuk memastikan bahwa mereka sesuai dengan kebijakan yang telah ditetapkan.
f. Sanksi dan Konsekuensi: Tentukan sanksi atau konsekuensi yang akan diberikan kepada mereka yang melanggar kebijakan keamanan. Pastikan bahwa sanksi tersebut ditegakkan secara konsisten dan adil.
g. Pemantauan dan Evaluasi: Terus pantau dan evaluasi efektivitas kebijakan keamanan secara berkala. Tinjau kembali kebijakan tersebut dan lakukan perubahan atau penyesuaian jika diperlukan sesuai dengan perkembangan teknologi atau perubahan kebutuhan bisnis.

h. Budaya Keamanan: Bangun budaya keamanan di seluruh organisasi dengan mengutamakan keamanan informasi sebagai prioritas. Dorong karyawan untuk secara proaktif melaporkan kejadian keamanan yang mencurigakan dan terlibat dalam upaya menjaga keamanan informasi.

Dengan mengikuti langkah-langkah di atas, organisasi dapat memastikan bahwa kebijakan keamanan tidak hanya dibuat, tetapi juga dilaksanakan dan ditegakkan dengan efektif. Hal ini akan membantu melindungi aset dan informasi sensitif organisasi dari ancaman keamanan yang ada.

E. Teknologi Keamanan Informasi

1. Pentingnya Kriptografi dan Pengamanan Data

Kriptografi dan pengamanan data sangat penting dalam konteks keamanan informasi. Berikut adalah beberapa alasan mengapa kriptografi dan pengamanan data sangat penting:

a. Kerahasiaan Data: Kriptografi memungkinkan data untuk dienkripsi, yang berarti data tersebut diubah menjadi format yang tidak dapat dimengerti kecuali oleh penerima yang sah. Ini memastikan bahwa data tetap rahasia dan hanya dapat diakses oleh pihak yang memiliki kunci dekripsi yang tepat.
b. Integritas Data: Kriptografi juga dapat digunakan untuk memastikan integritas data, yaitu memastikan bahwa data tidak diubah atau

dimanipulasi secara tidak sah selama penyimpanan atau transmisi. Tanda tangan digital dan fungsi hash digunakan untuk memverifikasi bahwa data tetap tidak berubah.

c. Autentikasi Pengguna: Teknik kriptografi seperti sistem otentikasi dan sertifikat digital memungkinkan organisasi untuk memverifikasi identitas pengguna dan memastikan bahwa hanya pengguna yang sah yang memiliki akses ke data sensitif atau sistem yang terkait.
d. Keamanan Transmisi Data: Dalam komunikasi melalui jaringan, kriptografi digunakan untuk mengamankan transmisi data dari serangan pengintaian atau penyadapan. Protokol enkripsi seperti SSL/TLS digunakan untuk mengamankan komunikasi di internet.
e. Kepatuhan Regulasi: Banyak regulasi dan peraturan, seperti GDPR di Uni Eropa atau HIPAA di Amerika Serikat, mengharuskan organisasi untuk melindungi data pribadi atau sensitif. Kriptografi sering kali merupakan persyaratan dalam mencapai kepatuhan dengan standar tersebut.
f. Perlindungan Terhadap Serangan Malware: Kriptografi dapat membantu melindungi data dari serangan malware seperti ransomware, yang sering kali menargetkan data yang tidak dienkripsi. Dengan menerapkan enkripsi data yang kuat, organisasi dapat mencegah pencurian atau penggunaan data oleh penyerang.

g. Kepercayaan Pelanggan dan Reputasi Bisnis: Dengan menerapkan praktik kriptografi dan pengamanan data yang kuat, organisasi dapat membangun kepercayaan dengan pelanggan dan mitra bisnis dengan menunjukkan komitmen mereka terhadap perlindungan data pribadi dan sensitif.

Secara keseluruhan, kriptografi dan pengamanan data merupakan komponen kunci dalam strategi keamanan informasi suatu organisasi. Dengan menerapkan praktik kriptografi yang tepat, organisasi dapat melindungi data mereka dari ancaman keamanan yang beragam dan memastikan keamanan, integritas, dan kerahasiaan informasi mereka.

2. Keamanan Jaringan dan Proteksi Perimeter

Keamanan jaringan dan perlindungan perimeter sangat penting dalam menjaga keamanan sistem dan data dalam suatu organisasi. Berikut adalah beberapa aspek yang perlu dipertimbangkan dalam keamanan jaringan dan proteksi perimeter:

a. Firewall: Firewall adalah komponen utama dalam perlindungan perimeter yang berfungsi untuk memantau dan mengontrol lalu lintas jaringan yang masuk dan keluar dari jaringan organisasi. Firewall dapat mengizinkan atau memblokir lalu lintas berdasarkan aturan yang ditentukan, membantu melindungi jaringan dari serangan yang tidak diinginkan.
b. Intrusion Detection and Prevention Systems (IDPS): IDPS adalah sistem yang dirancang untuk

mendeteksi dan mencegah serangan yang mencoba memasuki atau merusak jaringan. Ini dapat mengidentifikasi pola lalu lintas yang mencurigakan atau perilaku aneh yang menandakan serangan potensial dan mengambil tindakan yang sesuai untuk melindungi jaringan.

c. Virtual Private Network (VPN): VPN menyediakan jalur aman untuk mengirimkan data melalui jaringan publik, seperti internet. Ini memungkinkan pengguna untuk mengakses jaringan organisasi dari lokasi eksternal dengan aman, serta mengenkripsi data yang dikirimkan melalui jaringan publik.
d. Access Control: Pengaturan kontrol akses yang ketat adalah kunci dalam menjaga keamanan jaringan. Ini termasuk penggunaan otentikasi yang kuat, pengaturan hak akses yang tepat untuk pengguna, dan pemantauan aktivitas pengguna untuk mendeteksi potensi ancaman keamanan.
e. Encryption: Enkripsi data yang sensitif saat berada dalam transit atau saat disimpan di server jaringan adalah langkah penting untuk melindungi kerahasiaan data dari serangan penyadapan atau pencurian.
f. Segmentasi Jaringan: Memisahkan jaringan internal menjadi segmen-segmen yang terisolasi dapat membantu mengurangi dampak dari serangan yang berhasil menembus lapisan perlindungan perimeter. Ini membatasi kemampuan penyerang untuk menyebar ke seluruh jaringan.

g. Pemantauan dan Respons Keamanan: Pemantauan aktif terhadap lalu lintas jaringan dan deteksi serangan secara real-time adalah kunci untuk merespons ancaman keamanan dengan cepat. Tim keamanan harus dilengkapi dengan alat pemantauan yang kuat dan memiliki prosedur tanggap darurat yang jelas untuk menangani insiden keamanan yang terjadi.

Penting untuk diingat bahwa keamanan jaringan dan proteksi perimeter hanyalah bagian dari strategi keamanan informasi yang lebih luas. Organisasi juga perlu mempertimbangkan aspek lain seperti kesadaran keamanan karyawan, pengelolaan risiko, dan pemulihan bencana untuk memastikan perlindungan yang komprehensif terhadap serangan cyber.

3. Sistem Deteksi dan Pencegahan Intrusi (IDPS)

Sistem Deteksi dan Pencegahan Intrusi (IDPS) adalah bagian penting dari strategi keamanan jaringan yang bertujuan untuk mendeteksi, mencegah, dan merespons serangan atau aktivitas yang mencurigakan dalam jaringan atau sistem komputer. Berikut adalah beberapa konsep penting terkait dengan IDPS:

a. Deteksi Intrusi: IDPS mendeteksi serangan atau aktivitas yang mencurigakan dengan memantau lalu lintas jaringan atau kejadian dalam sistem komputer. Ini melibatkan analisis terhadap pola lalu lintas, tanda-tanda serangan yang diketahui, atau perilaku yang tidak biasa.
b. Pencegahan Intrusi: Selain mendeteksi serangan, IDPS juga dapat mengambil tindakan untuk

mencegah atau memblokir serangan yang terdeteksi. Ini bisa termasuk pemblokiran lalu lintas dari sumber yang mencurigakan, memblokir alamat IP atau port tertentu, atau mengubah konfigurasi sistem untuk mengurangi kerentanan.

c. Pengumpulan Data: IDPS mengumpulkan data tentang aktivitas jaringan dan sistem, seperti log kejadian, arus jaringan, atau lalu lintas paket. Data ini digunakan untuk analisis lebih lanjut dan deteksi serangan.
d. Analisis dan Pemantauan: IDPS menganalisis data yang dikumpulkan untuk mendeteksi pola serangan atau tanda-tanda aktivitas yang mencurigakan. Ini dapat melibatkan penggunaan tanda tangan, aturan, atau model perilaku untuk mengidentifikasi serangan yang diketahui atau tidak diketahui.
e. Respon Terhadap Serangan: Setelah serangan terdeteksi, IDPS merespons dengan mengambil tindakan yang sesuai untuk menghentikan serangan, memblokir akses yang mencurigakan, atau memberikan peringatan kepada administrator atau tim keamanan.
f. Integrasi dengan Sistem Keamanan Lain: IDPS sering kali diintegrasikan dengan sistem keamanan lain seperti firewall, sistem proteksi endpoint, atau sistem manajemen keamanan informasi (SIEM) untuk memberikan perlindungan yang komprehensif.
g. Klasifikasi Serangan: IDPS dapat mengklasifikasikan serangan berdasarkan jenis,

sumber, atau dampaknya. Ini membantu administrator untuk memprioritaskan respons dan mengambil tindakan yang sesuai.

IDPS merupakan alat penting dalam pertahanan jaringan modern yang membantu organisasi untuk melindungi infrastruktur mereka dari berbagai ancaman keamanan yang ada. Dengan mengintegrasikan IDPS ke dalam strategi keamanan mereka, organisasi dapat meningkatkan kemampuan mereka untuk mendeteksi, mencegah, dan merespons serangan dengan cepat dan efektif.

F. Manajemen Keamanan Risiko

1. Siklus Manajemen Risiko

Siklus manajemen risiko adalah pendekatan sistematis untuk mengelola risiko dalam suatu organisasi atau proyek. Siklus ini terdiri dari serangkaian langkah yang bertujuan untuk mengidentifikasi, mengevaluasi, mengurangi, dan memantau risiko secara berkesinambungan. Berikut adalah langkah-langkah dalam siklus manajemen risiko:

a. Identifikasi Risiko: Langkah pertama dalam siklus manajemen risiko adalah mengidentifikasi semua risiko yang mungkin mempengaruhi tujuan organisasi atau proyek. Ini melibatkan identifikasi sumber risiko, peristiwa yang dapat terjadi, dan dampak yang mungkin timbul.

b. Analisis Risiko: Setelah risiko diidentifikasi, langkah selanjutnya adalah menganalisis risiko untuk mengevaluasi kemungkinan terjadinya dan dampaknya terhadap tujuan organisasi atau proyek. Ini melibatkan penilaian probabilitas dan dampak risiko, serta identifikasi risiko yang paling signifikan.
c. Evaluasi Risiko: Setelah risiko dianalisis, langkah berikutnya adalah mengevaluasi risiko untuk menentukan tingkat risiko yang dapat diterima oleh organisasi atau proyek. Ini melibatkan perbandingan antara tingkat risiko yang diidentifikasi dengan kriteria risiko yang telah ditetapkan sebelumnya.
d. Pengelolaan Risiko: Setelah risiko dievaluasi, langkah selanjutnya adalah mengelola risiko untuk mengurangi atau menghilangkan dampak negatifnya. Ini melibatkan pengembangan strategi pengelolaan risiko yang sesuai, seperti menghindari, mentransfer, mengurangi, atau menerima risiko.
e. Pantauan dan Pengendalian Risiko: Langkah terakhir dalam siklus manajemen risiko adalah memantau dan mengendalikan risiko secara berkesinambungan. Ini melibatkan pemantauan implementasi strategi pengelolaan risiko, memeriksa efektivitasnya, dan menyesuaikan rencana manajemen risiko sesuai kebutuhan.

Siklus manajemen risiko merupakan proses berkelanjutan yang memungkinkan organisasi untuk mengidentifikasi, mengukur, dan mengelola risiko

secara efektif dalam konteks tujuan dan strategi mereka. Dengan mengikuti siklus ini secara teratur, organisasi dapat mengurangi kemungkinan terjadinya kerugian atau kegagalan, serta meningkatkan kemungkinan mencapai tujuan mereka dengan lebih sukses.

2. Pengambilan Keputusan terkait Risiko

Pengambilan keputusan terkait risiko merupakan proses kritis dalam manajemen risiko yang melibatkan yang telah diidentifikasi, penilaian konsekuensi potensial dari risiko tersebut, dan pemilihan tindakan yang paling sesuai untuk mengelola atau meredam risiko tersebut. Berikut adalah langkah-langkah umum dalam pengambilan keputusan terkait risiko:

a. Identifikasi Risiko: Langkah pertama adalah mengidentifikasi semua risiko yang mungkin mempengaruhi tujuan organisasi atau proyek. Ini melibatkan penilaian terhadap lingkungan operasional, proses bisnis, dan sumber risiko yang mungkin timbul.
b. Analisis Risiko: Setelah risiko diidentifikasi, langkah berikutnya adalah menganalisis risiko untuk mengevaluasi kemungkinan terjadinya dan dampaknya terhadap tujuan organisasi atau proyek. Ini melibatkan penilaian probabilitas dan dampak risiko, serta identifikasi risiko yang paling signifikan.
c. Penilaian Konsekuensi: Setelah risiko dianalisis, langkah selanjutnya adalah menilai konsekuensi potensial dari terjadinya risiko tersebut. Ini

melibatkan penilaian terhadap dampak finansial, reputasi, operasional, atau hukum yang mungkin timbul akibat risiko tersebut.

d. Penentuan Tindakan Pengelolaan Risiko: Berdasarkan analisis risiko dan penilaian konsekuensi, langkah selanjutnya adalah memilih tindakan pengelolaan risiko yang paling sesuai untuk mengurangi atau mengelola risiko tersebut. Ini dapat mencakup tindakan seperti menghindari, mentransfer, mengurangi, atau menerima risiko.
e. Pemantauan dan Evaluasi: Setelah tindakan pengelolaan risiko dipilih dan diimplementasikan, langkah terakhir adalah memantau dan mengevaluasi efektivitas tindakan tersebut dalam mengurangi atau mengelola risiko. Ini melibatkan pemantauan terhadap implementasi tindakan, memeriksa efektivitasnya, dan menyesuaikan rencana manajemen risiko jika diperlukan.

Penting untuk dicatat bahwa pengambilan keputusan terkait risiko bukanlah proses yang statis, tetapi merupakan proses berkelanjutan yang memerlukan pemantauan dan evaluasi terus-menerus terhadap kondisi risiko dan efektivitas tindakan yang diambil. Dengan mengikuti langkah-langkah ini secara sistematis, organisasi dapat mengelola risiko dengan lebih efektif dan meningkatkan kemungkinan mencapai tujuan mereka dengan lebih sukses.

3. Rencana Darurat dan Tanggap Krisis

Rencana darurat dan tanggap krisis merupakan bagian penting dari strategi manajemen risiko suatu

organisasi yang bertujuan untuk menghadapi dan merespons keadaan darurat atau krisis yang mungkin terjadi. Berikut adalah komponen-komponen utama dari rencana darurat dan tanggap krisis:

a. Pengidentifikasi Ancaman: Identifikasi berbagai jenis ancaman atau kejadian darurat yang mungkin terjadi, seperti bencana alam, kecelakaan industri, serangan siber, atau insiden keamanan.
b. Penetapan Protokol Komunikasi: Menetapkan protokol komunikasi yang jelas dan efektif untuk menyampaikan informasi kepada semua pihak yang terlibat dalam tanggap darurat atau krisis, termasuk karyawan, pelanggan, media, dan pihak berwenang.
c. Penetapan Peran dan Tanggung Jawab: Menetapkan peran dan tanggung jawab yang jelas bagi anggota tim tanggap darurat atau krisis, termasuk tugas-tugas spesifik yang harus dilakukan dalam situasi darurat.
d. Pengembangan Rencana Evakuasi: Mengembangkan rencana evakuasi yang terperinci untuk mengevakuasi karyawan atau penghuni bangunan dengan cepat dan aman dalam situasi darurat seperti kebakaran atau gempa bumi.
e. Penyediaan Fasilitas dan Perlengkapan Darurat: Menyediakan fasilitas dan perlengkapan darurat yang diperlukan, seperti kit pertolongan pertama, peralatan pemadam kebakaran, generator cadangan, atau sumber air bersih.
f. Pelatihan dan Simulasi: Melakukan pelatihan dan simulasi reguler untuk memastikan bahwa semua

anggota tim tanggap darurat atau krisis memahami peran mereka dan siap bertindak dalam situasi darurat yang sebenarnya.

g. Pengujian dan Evaluasi: Mengujikan rencana darurat dan tanggap krisis secara berkala untuk mengidentifikasi kelemahan atau kekurangan dalam rencana, serta mengevaluasi kinerja tim tanggap darurat atau krisis.
h. Pemulihan dan Pembelajaran: Setelah keadaan darurat atau krisis berakhir, melakukan proses pemulihan dan evaluasi pasca-krisis untuk mengembangkan pembelajaran organisasi dan meningkatkan rencana darurat untuk masa depan.

Rencana darurat dan tanggap krisis harus disesuaikan dengan kebutuhan dan karakteristik khusus dari setiap organisasi, serta memperhitungkan faktor-faktor seperti lokasi geografis, jenis bisnis, dan risiko yang mungkin terjadi. Dengan memiliki rencana darurat yang terstruktur dan teruji dengan baik, organisasi dapat meningkatkan kemampuan mereka untuk merespons dengan cepat dan efektif dalam menghadapi situasi darurat atau krisis yang tidak terduga.

G. Keamanan Aplikasi dan Pengembangan Perangkat Lunak

1. Pengambilan Prinsip Keamanan Aplikasi

Pengambilan prinsip keamanan aplikasi merupakan langkah kunci dalam mengembangkan dan mengelola aplikasi yang aman. Prinsip-prinsip ini

membimbing pengembang dalam merancang, mengimplementasikan, dan memelihara aplikasi dengan memperhatikan aspek keamanan yang penting. Berikut adalah beberapa prinsip keamanan aplikasi yang penting:

a. Prinsip Keterbukaan (Open Design): Memastikan bahwa desain aplikasi adalah terbuka dan transparan, sehingga memungkinkan pemeriksaan independen terhadap keamanan dan kemungkinan kerentanan.
b. Prinsip Kebutuhan Prinsip Paling Sedikit (Least Privilege): Memberikan akses yang minimal yang diperlukan kepada pengguna, proses, atau sistem, untuk mengurangi risiko penyalahgunaan atau penyerangan.
c. Prinsip Pertahanan dalam Kedalaman (Defense in Depth): Menggunakan beberapa lapisan pertahanan keamanan yang saling melengkapi, seperti firewall, enkripsi, dan pemantauan keamanan, untuk mengurangi risiko serangan yang berhasil.
d. Prinsip Pengamanan Komponen (Secure Components): Memilih dan menggunakan komponen perangkat lunak atau platform yang aman, serta memastikan bahwa komponen tersebut diperbarui dan dielola dengan baik.
e. Prinsip Penggunaan Kriptografi yang Kuat (Strong Cryptography): Menggunakan algoritma kriptografi yang aman dan diterima secara umum untuk melindungi data sensitif saat berada dalam perjalanan atau saat disimpan.

f. Prinsip Pengujian Keamanan (Security Testing): Melakukan pengujian keamanan secara teratur, seperti pengujian penetrasi, pemindaian keamanan, dan analisis kerentanan, untuk mengidentifikasi dan mengatasi kerentanan yang mungkin ada dalam aplikasi.
g. Prinsip Pengelolaan Identitas dan Akses (Identity and Access Management): Mengelola identitas pengguna dengan tepat, menerapkan autentikasi yang kuat, serta mengatur hak akses secara tepat untuk memastikan hanya pengguna yang sah yang memiliki akses ke data atau fitur tertentu.
h. Prinsip Pemulihan yang Cepat (Quick Recovery): Mempersiapkan rencana pemulihan bencana dan mengimplementasikan fitur yang memungkinkan pemulihan yang cepat dalam kasus terjadinya insiden keamanan atau bencana.
i. Prinsip Pemeliharaan Keselamatan (Safety Maintenance): Memperbarui dan memelihara aplikasi secara teratur, termasuk penerapan patch keamanan yang diperlukan, pemantauan log keamanan, dan penerapan praktik keamanan terbaik.
j. Prinsip Pendidikan dan Kesadaran (Education and Awareness): Memberikan pelatihan keamanan kepada pengembang dan pengguna aplikasi, serta meningkatkan kesadaran akan praktik keamanan yang aman.

Dengan memperhatikan prinsip-prinsip ini, pengembang dapat membangun aplikasi yang lebih aman dan tahan terhadap serangan, serta melindungi

data sensitif dan infrastruktur dari ancaman keamanan yang mungkin terjadi.

2. Praktik Pengembangan Perangkat Lunak yang Aman

Praktik pengembangan perangkat lunak yang aman (Secure Software Development Practices) adalah pendekatan sistematis dalam proses pengembangan perangkat lunak yang bertujuan untuk mengintegrasikan keamanan sejak awal dalam siklus pengembangan perangkat lunak. Berikut adalah beberapa praktik penting dalam pengembangan perangkat lunak yang aman:

a. Pengujian Keamanan: Melakukan pengujian keamanan secara teratur selama seluruh siklus pengembangan perangkat lunak, termasuk pengujian penetrasi, pemindaian keamanan, dan analisis kerentanan untuk mengidentifikasi dan mengatasi masalah keamanan sejak dini.
b. Pemilihan Kerangka Kerja yang Aman: Memilih kerangka kerja atau framework pengembangan yang telah terbukti aman dan memiliki fitur keamanan yang terintegrasi, serta menerapkan praktik pengembangan yang aman secara otomatis.
c. Pemrograman yang Aman: Menggunakan praktik pemrograman yang aman, seperti validasi input, pembersihan data, penghindaran penyandian manual, dan penghindaran kerentanan umum seperti injeksi SQL atau cross-site scripting (XSS).
d. Manajemen Sumber Kode yang Aman: Memastikan bahwa sumber kode perangkat lunak disimpan, dikelola, dan disebarkan dengan aman, serta

menerapkan kontrol versi yang ketat dan pembatasan akses yang sesuai.

e. Pengelolaan Ketergantungan yang Aman: Mengelola ketergantungan perangkat lunak (third-party libraries, plugins, modules, etc.) dengan hati-hati, memperbarui secara teratur, dan memastikan bahwa ketergantungan tersebut bebas dari kerentanan keamanan yang diketahui.
f. Penerapan Enkripsi: Mengenkripsi data sensitif saat berada dalam perjalanan (misalnya, dengan SSL/TLS) dan saat disimpan (misalnya, dengan enkripsi disk atau enkripsi kolom basis data) untuk melindungi data dari akses yang tidak sah.
g. Pemantauan dan Logging: Melakukan pemantauan aktif terhadap aktivitas aplikasi dan pengumpulan log keamanan untuk mendeteksi dan merespons insiden keamanan secara cepat, serta memelihara jejak audit yang komprehensif.
h. Pemeliharaan dan Pembaruan yang Teratur: Memelihara dan memperbarui perangkat lunak secara teratur untuk mengatasi kerentanan keamanan yang baru teridentifikasi dan memperbaiki masalah keamanan yang telah ada.
i. Pendidikan dan Pelatihan: Memberikan pelatihan keamanan kepada pengembang perangkat lunak untuk meningkatkan pemahaman mereka tentang praktik pengembangan yang aman, kerentanan keamanan umum, dan teknologi keamanan terkini.
j. Penerapan Prinsip-prinsip DevSecOps: Mengintegrasikan keamanan sejak awal dalam siklus pengembangan perangkat lunak, serta

memanfaatkan praktik DevOps untuk mengotomatiskan pengujian, pengiriman, dan penerapan keamanan.

Dengan menerapkan praktik-praktik ini secara konsisten, pengembang dapat memastikan bahwa perangkat lunak yang mereka kembangkan memiliki tingkat keamanan yang tinggi dan mampu melindungi data dan infrastruktur dari ancaman keamanan yang beragam.

3. Uji Keamanan Aplikasi

Uji keamanan aplikasi adalah proses penting dalam siklus pengembangan perangkat lunak yang bertujuan untuk mengidentifikasi dan memperbaiki kerentanan keamanan yang ada dalam sebuah aplikasi sebelum diperkenalkan ke lingkungan produksi atau diakses oleh pengguna akhir. Berikut adalah beberapa praktik umum dalam melakukan uji keamanan aplikasi:

a. Pemindaian Kerentanan (Vulnerability Scanning): Melakukan pemindaian secara otomatis terhadap aplikasi untuk mengidentifikasi kerentanan yang mungkin ada, seperti celah keamanan pada kode, konfigurasi yang buruk, atau kerentanan terhadap serangan tertentu.
b. Pengujian Penetrasi (Penetration Testing): Melakukan pengujian secara aktif untuk mengevaluasi keamanan aplikasi dengan mencoba mengeksploitasi kerentanan yang ada. Ini dapat melibatkan pengujian serangan seperti SQL injection, cross-site scripting (XSS), atau serangan serupa.

c. Pemeriksaan Kode (Code Review): Melakukan pemeriksaan manual atau otomatis terhadap kode sumber aplikasi untuk mengidentifikasi potensi kerentanan keamanan, seperti penggunaan yang tidak aman dari fungsi kriptografi, manipulasi input yang tidak terverifikasi, atau celah keamanan lainnya.
d. Analisis Arsitektur dan Desain (Architecture and Design Analysis): Melakukan evaluasi terhadap arsitektur dan desain aplikasi untuk mengidentifikasi potensi risiko keamanan yang mungkin timbul dari aspek desain, seperti kelemahan konfigurasi, ketidaksesuaian terhadap standar keamanan, atau pelanggaran prinsip-prinsip keamanan.
e. Uji Integrasi dan Fungsionalitas (Integration and Functionality Testing): Melakukan pengujian untuk memastikan bahwa kontrol keamanan yang telah diimplementasikan berfungsi dengan baik dan tidak mempengaruhi fungsionalitas atau kinerja aplikasi secara keseluruhan.
f. Uji Kinerja dan Beban (Performance and Load Testing): Memastikan bahwa aplikasi tetap aman dan dapat beroperasi dengan baik di bawah tekanan atau beban tinggi, serta tidak rentan terhadap serangan seperti denial-of-service (DoS) atau serangan serupa.
g. Uji Penggunaan yang Buruk (Misuse Testing): Melakukan pengujian untuk mengevaluasi keamanan aplikasi dari serangan penggunaan yang

buruk, seperti mencoba masukan yang tidak valid, upaya manipulasi data, atau serangan serupa.

h. Pemantauan dan Analisis Log (Logging and Analysis): Memastikan bahwa aplikasi menghasilkan log aktivitas yang memadai, serta melakukan analisis log secara berkala untuk mendeteksi aktivitas mencurigakan atau ancaman keamanan yang mungkin terjadi.

i. Pemutakhiran dan Perbaikan (Patch and Remediation): Mengimplementasikan pemutakhiran perangkat lunak yang diperlukan dan perbaikan untuk mengatasi kerentanan keamanan yang teridentifikasi selama uji keamanan.

Dengan mengintegrasikan praktik-praktik tersebut ke dalam siklus pengembangan perangkat lunak, organisasi dapat meningkatkan kemampuan mereka untuk mengidentifikasi, mengurangi, dan mengelola risiko keamanan dalam aplikasi mereka, serta melindungi data sensitif dan infrastruktur dari serangan dan ancaman keamanan yang mungkin terjadi.

H. Kepatuhan dan Regulasi

1. Pengambilan Kepatuhan terhadap Standar Keamanan Industri

Pengambilan kepatuhan terhadap standar keamanan industri adalah proses penting dalam memastikan bahwa organisasi mematuhi persyaratan keamanan yang ditetapkan oleh badan standar atau regulasi yang relevan. Berikut adalah langkah-langkah

umum dalam pengambilan kepatuhan terhadap standar keamanan industri:

a. Identifikasi Standar yang Relevan: Langkah pertama adalah mengidentifikasi standar keamanan industri yang relevan bagi organisasi Anda, seperti ISO/IEC 27001, NIST SP 800-53, PCI DSS, HIPAA, atau GDPR, tergantung pada jenis bisnis dan industri tempat organisasi beroperasi.
b. Evaluasi Persyaratan Kepatuhan: Setelah standar keamanan yang relevan diidentifikasi, langkah selanjutnya adalah melakukan evaluasi menyeluruh terhadap persyaratan kepatuhan yang ditetapkan dalam standar tersebut. Ini melibatkan pemahaman mendalam terhadap setiap persyaratan dan implikasinya terhadap operasi organisasi.
c. Penetapan Tanggung Jawab: Menetapkan tanggung jawab kepada individu atau tim yang bertanggung jawab atas pengelolaan dan implementasi kepatuhan terhadap standar keamanan. Ini melibatkan pemilihan pemimpin proyek atau manajer kepatuhan, serta alokasi sumber daya yang diperlukan.
d. Penilaian Kebutuhan: Melakukan penilaian terhadap kesenjangan antara keadaan saat ini dengan persyaratan kepatuhan standar keamanan yang ditetapkan. Ini membantu dalam menentukan langkah-langkah yang diperlukan untuk mencapai kepatuhan.
e. Pengembangan Rencana Kepatuhan: Berdasarkan penilaian kebutuhan, mengembangkan rencana

tindakan yang jelas dan terstruktur untuk mencapai kepatuhan terhadap standar keamanan. Rencana ini harus mencakup langkah-langkah spesifik, batas waktu, dan tanggung jawab yang jelas.

f. Implementasi Langkah-langkah Kepatuhan: Melaksanakan langkah-langkah yang diperlukan sesuai dengan rencana kepatuhan yang telah dikembangkan. Ini dapat melibatkan penerapan kebijakan baru, pengaturan kontrol keamanan, pelatihan karyawan, atau perubahan proses operasional.
g. Pemantauan dan Pemeliharaan Kepatuhan: Melakukan pemantauan terus-menerus terhadap kepatuhan terhadap standar keamanan, serta melakukan evaluasi dan pemeliharaan secara berkala. Ini melibatkan pemantauan kinerja, audit internal, dan pembaruan kebijakan dan prosedur yang diperlukan.
h. Pengujian dan Verifikasi: Melakukan pengujian dan verifikasi secara berkala untuk memastikan bahwa kepatuhan terhadap standar keamanan tetap terjaga. Ini meliputi pengujian keamanan aplikasi, pemindaian jaringan, atau audit eksternal.
i. Pelaporan dan Sertifikasi: Melakukan pelaporan berkala terhadap kepatuhan terhadap standar keamanan kepada pihak berwenang atau pihak terkait lainnya. Jika diperlukan, mencapai sertifikasi resmi dari badan otoritas yang relevan./

Dengan mengikuti langkah-langkah ini, organisasi dapat memastikan bahwa mereka mematuhi persyaratan keamanan yang ditetapkan oleh standar

industri yang relevan, serta mengurangi risiko keamanan dan meningkatkan kepercayaan pelanggan dan mitra bisnis.

2. Peran Pemerintah dan Badan Regulasi

Peran pemerintah dan badan regulasi sangat penting dalam memastikan keamanan dan perlindungan data, infrastruktur, dan layanan yang berkaitan dengan teknologi informasi dan komunikasi. Berikut adalah beberapa peran utama pemerintah dan badan regulasi dalam konteks keamanan teknologi informasi:

a. Penetapan Standar dan Regulasi: Pemerintah dan badan regulasi bertanggung jawab untuk menetapkan standar keamanan dan regulasi yang relevan untuk industri teknologi informasi. Ini dapat mencakup standar keamanan data, persyaratan kepatuhan, dan peraturan yang berlaku untuk perlindungan informasi sensitif.
b. Pelaksanaan dan Penegakan Hukum: Pemerintah memiliki peran dalam menegakkan peraturan keamanan dan hukum terkait yang ditetapkan oleh badan regulasi. Mereka dapat menyelidiki pelanggaran keamanan, menuntut pelanggar hukum, dan memberlakukan sanksi terhadap pelanggaran yang ditemukan.
c. Pengembangan Kebijakan Publik: Pemerintah dapat mengembangkan kebijakan publik yang mempromosikan keamanan teknologi informasi, melalui inisiatif seperti keamanan siber nasional

atau strategi keamanan nasional yang melibatkan koordinasi lintas sektoral.

d. Pengawasan Infrastruktur Kritis: Pemerintah sering memiliki tanggung jawab untuk mengawasi dan melindungi infrastruktur kritis, seperti sistem komunikasi, listrik, atau transportasi, dari ancaman keamanan siber yang dapat memiliki dampak serius terhadap keamanan nasional atau kesejahteraan masyarakat.
e. Pengembangan Riset dan Inovasi: Pemerintah dapat mendukung riset dan inovasi dalam bidang keamanan teknologi informasi melalui pendanaan, insentif fiskal, atau kerja sama dengan sektor swasta dan akademis. Ini bertujuan untuk meningkatkan kemampuan negara dalam menghadapi ancaman keamanan yang terus berkembang.
f. Pendidikan dan Kesadaran: Pemerintah dapat mengambil peran dalam meningkatkan pendidikan dan kesadaran masyarakat tentang keamanan teknologi informasi, melalui kampanye publik, pelatihan, atau program pendidikan di sekolah dan perguruan tinggi.
g. Kerjasama Internasional: Pemerintah juga dapat berperan dalam kerjasama internasional untuk memerangi ancaman keamanan siber yang lintas batas. Ini dapat mencakup pertukaran informasi, kerja sama dalam penyelidikan kejahatan siber, atau pengembangan standar keamanan global.

Dengan melibatkan pemerintah dan badan regulasi secara aktif dalam upaya untuk meningkatkan

keamanan teknologi informasi, sebuah negara dapat mengembangkan ekosistem keamanan yang kuat, melindungi kepentingan nasional dan masyarakat, serta mempromosikan inovasi dan pertumbuhan ekonomi yang berkelanjutan.

3. Dampak Kepatuhan pada Strategi Keamanan

Kepatuhan pada standar keamanan memiliki dampak signifikan pada strategi keamanan suatu organisasi. Berikut adalah beberapa dampak utama dari kepatuhan pada strategi keamanan:

a. Peningkatan Keamanan Data: Kepatuhan pada standar keamanan memastikan bahwa organisasi menerapkan praktik dan kontrol keamanan yang tepat untuk melindungi data sensitif mereka. Ini termasuk langkah-langkah seperti enkripsi data, pengaturan akses yang tepat, dan pemantauan keamanan yang ketat.
b. Peningkatan Kesadaran tentang Risiko: Proses kepatuhan memaksa organisasi untuk memahami risiko keamanan yang mereka hadapi dan mengidentifikasi kerentanan potensial dalam infrastruktur mereka. Ini mendorong organisasi untuk memperkuat strategi keamanan mereka dan mengurangi risiko serangan.
c. Meningkatkan Kepercayaan Pelanggan: Organisasi yang mematuhi standar keamanan yang diakui dapat memperoleh kepercayaan pelanggan dan mitra bisnis. Hal ini karena kepatuhan menunjukkan komitmen organisasi untuk

melindungi data sensitif pelanggan dan mengelola risiko keamanan dengan serius.

d. Mengurangi Dampak Pelanggaran Keamanan: Kepatuhan pada standar keamanan membantu mengurangi risiko pelanggaran data dan serangan cyber. Dengan menerapkan kontrol keamanan yang ketat, organisasi dapat mengurangi kemungkinan serangan yang berhasil dan meminimalkan dampak dari insiden keamanan yang terjadi.
e. Meningkatkan Efisiensi Operasional: Meskipun implementasi kepatuhan mungkin membutuhkan investasi awal dalam sumber daya dan teknologi, pada akhirnya hal ini dapat meningkatkan efisiensi operasional. Standar keamanan yang jelas dan terstruktur membantu dalam mengelola risiko secara efektif dan mengurangi biaya yang terkait dengan insiden keamanan.
f. Meningkatkan Kerjasama dengan Pihak Ketiga: Banyak organisasi memerlukan pihak ketiga untuk mematuhi standar keamanan tertentu sebelum dapat melakukan bisnis bersama. Dengan memastikan kepatuhan, organisasi dapat meningkatkan kerjasama dengan mitra bisnis dan penyedia layanan yang memerlukan keamanan data yang tinggi.
g. Mengurangi Ancaman Hukuman dan Sanksi: Banyak badan regulasi menerapkan sanksi dan hukuman terhadap organisasi yang melanggar standar keamanan dan regulasi yang berlaku. Dengan mematuhi standar keamanan, organisasi

dapat menghindari sanksi hukum yang dapat merugikan reputasi dan finansial mereka.

Dengan memahami dampak dari kepatuhan pada strategi keamanan, organisasi dapat membangun lingkungan keamanan yang kokoh dan memastikan bahwa mereka memenuhi standar keamanan yang diperlukan untuk melindungi data mereka dan menjaga kepercayaan pelanggan.

I. Manajemen Insiden dan Tanggap Keamanandan Regulasi

1. Rencana Manajemen Insiden

Rencana Manajemen Insiden (Incident Management Plan) adalah dokumen strategis yang merinci prosedur yang harus diikuti oleh sebuah organisasi ketika terjadi insiden keamanan atau pelanggaran data. Berikut adalah komponen penting dari rencana manajemen insiden:

a. Definisi Insiden: Menjelaskan secara jelas apa yang dianggap sebagai insiden keamanan atau pelanggaran data dalam konteks organisasi Anda. Ini dapat mencakup jenis-jenis insiden yang mungkin terjadi, seperti serangan siber, kehilangan data, atau akses yang tidak sah.
b. Struktur Organisasi: Menetapkan struktur organisasi untuk manajemen insiden, termasuk peran dan tanggung jawab dari tim manajemen insiden, tim respons keamanan, dan personel terkait lainnya.

c. Prosedur Pelaporan Insiden: Mengatur prosedur yang harus diikuti untuk melaporkan insiden keamanan atau pelanggaran data kepada pihak yang berwenang di dalam organisasi, seperti manajer keamanan informasi atau tim manajemen insiden.
d. Penilaian Risiko dan Eskalasi: Menetapkan prosedur untuk menilai risiko insiden, menentukan tingkat keparahan, dan mengambil langkah-langkah yang tepat untuk menanggapi insiden. Ini juga mencakup kriteria untuk eskalasi insiden jika diperlukan.
e. Penanganan dan Mitigasi: Menjelaskan langkah-langkah yang harus diambil untuk menangani dan memitigasi insiden keamanan atau pelanggaran data sesegera mungkin. Ini bisa meliputi isolasi sistem yang terkena dampak, menghentikan akses yang tidak sah, atau mengambil langkah-langkah lain yang diperlukan untuk menghentikan insiden.
f. Komunikasi dan Koordinasi: Mengatur prosedur komunikasi internal dan eksternal yang harus diikuti selama manajemen insiden, termasuk penginformasian kepada pihak-pihak yang terkena dampak, manajemen senior, tim respons keamanan, dan pihak berwenang yang relevan.
g. Pemulihan dan Pemantauan: Menjelaskan langkah-langkah yang harus diambil untuk memulihkan sistem dan layanan ke kondisi normal setelah insiden terjadi. Ini termasuk verifikasi keberhasilan pemulihan, pemantauan lanjutan

terhadap sistem, dan pembelajaran dari insiden untuk meningkatkan keamanan di masa depan.

h. Pemeliharaan Catatan dan Evaluasi: Menetapkan prosedur untuk mencatat semua aktivitas yang terkait dengan manajemen insiden, termasuk langkah-langkah yang diambil, keputusan yang dibuat, dan hasil evaluasi pasca-insiden. Ini membantu dalam mempelajari dari pengalaman dan memperbaiki proses keamanan di masa mendatang.

i. Pelatihan dan Latihan: Merencanakan pelatihan reguler dan latihan simulasi untuk memastikan bahwa personel terlatih dalam menjalankan prosedur manajemen insiden dengan efektif dan efisien ketika insiden sebenarnya terjadi.

Rencana Manajemen Insiden adalah instrumen penting dalam menjaga keamanan organisasi dan merespons dengan cepat dan efektif terhadap insiden keamanan yang mungkin terjadi. Dengan memiliki rencana yang terstruktur dan teruji dengan baik, organisasi dapat meminimalkan dampak dari insiden keamanan dan memulihkan operasi mereka dengan lebih cepat.

2. Deteksi, Respons, dan Pemulihan

Mari kita bayangkan sebuah perusahaan teknologi besar yang mengelola platform online yang banyak digunakan oleh jutaan pengguna di seluruh dunia. Perusahaan ini telah mengimplementasikan rencana manajemen insiden yang komprehensif untuk

menghadapi situasi darurat dalam hal deteksi, respons, dan pemulihan.

a. Deteksi

Perusahaan ini memiliki sistem deteksi keamanan canggih yang memonitor aktivitas di seluruh jaringan dan infrastruktur mereka secara real-time. Sistem ini menggunakan analisis perilaku, pemantauan lalu lintas, dan deteksi ancaman otomatis untuk mengidentifikasi potensi insiden keamanan secepat mungkin. Ketika ada kejanggalan atau aktivitas yang mencurigakan terdeteksi, alarm secara otomatis memicu pemberitahuan kepada tim keamanan.

b. Respons

Begitu insiden keamanan terdeteksi, tim keamanan akan segera mulai merespons. Rencana manajemen insiden telah menetapkan prosedur yang jelas untuk merespons berbagai jenis insiden, mulai dari serangan DDoS hingga kebocoran data. Tim keamanan segera mengisolasi sistem yang terkena dampak dan memulai investigasi mendalam untuk menentukan sifat dan dampak insiden tersebut.

Tim manajemen insiden dipanggil, yang terdiri dari ahli keamanan, personel TI, perwakilan hukum, dan anggota manajemen senior. Mereka bertanggung jawab untuk mengkoordinasikan respons dan membuat keputusan strategis sehubungan dengan insiden tersebut. Komunikasi internal dan eksternal juga segera dilakukan untuk memberi tahu pihak-pihak yang

terpengaruh, termasuk pengguna, mitra bisnis, dan pihak berwenang.

c. Pemulihan

Setelah insiden dikendalikan dan dampaknya dievaluasi, tim keamanan beralih ke tahap pemulihan. Mereka memulihkan layanan yang terpengaruh dan memastikan bahwa sistem kembali beroperasi secara normal. Ini melibatkan penerapan pembaruan keamanan, perubahan kredensial, pemulihan data dari cadangan, dan tindakan pemulihan lainnya yang diperlukan.

Sementara itu, tim manajemen insiden terus memantau situasi, memperbarui pihak yang terkait tentang kemajuan pemulihan, dan memastikan bahwa langkah-langkah yang diperlukan diambil untuk mencegah insiden serupa terjadi di masa depan. Evaluasi pasca-insiden juga dilakukan untuk mengevaluasi efektivitas respons dan mengidentifikasi area di mana perbaikan dapat dilakukan.

Dengan rencana manajemen insiden yang baik dan tim yang terlatih, perusahaan tersebut dapat merespons dengan cepat dan efektif terhadap insiden keamanan yang mungkin terjadi, menjaga layanan mereka tetap berjalan dan melindungi data dan kepercayaan pengguna mereka.

3. Evaluasi dan Pembelajaran dari Insiden

Evaluasi dan pembelajaran dari insiden keamanan merupakan bagian penting dari proses manajemen

insiden. Berikut adalah langkah-langkah yang biasanya dilakukan dalam proses evaluasi dan pembelajaran:

a. Identifikasi Fakta: Tim manajemen insiden akan mengumpulkan data dan fakta terkait insiden, termasuk sifat insiden, metode serangan, kerugian yang dialami, dan tanggapan yang diambil.
b. Analisis Penyebab: Tim akan menganalisis penyebab insiden dan mengidentifikasi faktor-faktor yang memungkinkan terjadinya. Hal ini dapat mencakup kelemahan dalam sistem, kegagalan proses, kesalahan manusia, atau kekurangan dalam kebijakan keamanan.
c. Penilaian Dampak: Evaluasi dilakukan terhadap dampak insiden terhadap bisnis dan operasi organisasi, termasuk kerugian finansial, kerusakan reputasi, dan potensi dampak jangka panjang.
d. Evaluasi Respons: Tim akan mengevaluasi efektivitas respons terhadap insiden, termasuk kecepatan tanggapan, koordinasi tim, dan keputusan yang diambil selama proses manajemen insiden.
e. Identifikasi Peningkatan: Berdasarkan analisis insiden, tim akan mengidentifikasi area di mana perbaikan dapat dilakukan untuk mencegah insiden serupa terjadi di masa depan. Ini mungkin melibatkan perubahan proses, peningkatan keamanan teknis, atau pelatihan lebih lanjut untuk personel.
f. Perbaikan dan Implementasi: Langkah-langkah perbaikan yang diidentifikasi selama evaluasi insiden akan diimplementasikan. Ini mungkin

melibatkan pembaruan kebijakan, perubahan arsitektur keamanan, atau penerapan kontrol tambahan.

g. Pelatihan dan Kesadaran: Organisasi dapat menggunakan insiden sebagai peluang untuk meningkatkan kesadaran keamanan dan pelatihan personel. Ini dapat mencakup sesi pelatihan, pelatihan simulasi insiden, atau kampanye kesadaran keamanan.
h. Dokumentasi dan Pelaporan: Semua temuan dan langkah-langkah perbaikan yang dihasilkan dari evaluasi insiden harus didokumentasikan secara lengkap. Ini termasuk pembuatan laporan evaluasi yang mencakup ringkasan insiden, analisis penyebab, dan rekomendasi perbaikan.
i. Pemantauan dan Revisi: Organisasi harus terus memantau efektivitas langkah-langkah perbaikan yang telah diimplementasikan dan mengubah rencana manajemen insiden mereka sesuai dengan hasil evaluasi dan perubahan lingkungan keamanan.

Dengan melakukan evaluasi dan pembelajaran yang komprehensif dari insiden keamanan, organisasi dapat memperbaiki strategi keamanan mereka, meningkatkan kesiapan mereka dalam menghadapi insiden di masa depan, dan memastikan bahwa kesalahan yang sama tidak terulang lagi.

J. Tren Terkini dalam Keamanan Sistem Informasi

1. Keamanan Cloud Computing

Keamanan cloud computing menjadi semakin penting karena semakin banyak organisasi yang beralih ke infrastruktur cloud untuk menyimpan data dan menjalankan aplikasi mereka. Berikut adalah beberapa aspek penting dalam memastikan keamanan cloud computing:

a. Pengelolaan Akses: Penting untuk mengelola akses ke lingkungan cloud dengan tepat. Ini termasuk menerapkan prinsip kebutuhan prinsip paling sedikit (least privilege), menerapkan otentikasi multifaktor, dan memastikan bahwa hak akses ke data dan sumber daya cloud hanya diberikan kepada pengguna yang sah.
b. Enkripsi Data: Data harus dienkripsi saat berada dalam perjalanan (misalnya, melalui protokol HTTPS) dan saat disimpan di cloud. Ini membantu melindungi data dari akses yang tidak sah bahkan jika data tersebut dicuri.
c. Keamanan Jaringan: Penting untuk mengamankan jaringan yang menghubungkan infrastruktur cloud dengan pengguna dan perangkat lainnya. Ini bisa melibatkan penggunaan firewall, deteksi intrusi, dan enkripsi lalu lintas jaringan.
d. Pemantauan dan Audit: Perlu memiliki mekanisme pemantauan yang efektif untuk memantau aktivitas yang mencurigakan atau aneh di lingkungan cloud.

Log aktivitas harus disimpan secara teratur dan dicek untuk mendeteksi potensi insiden keamanan.

e. Kepatuhan Regulasi: Organisasi harus memastikan bahwa penggunaan cloud computing mereka mematuhi regulasi dan standar keamanan yang berlaku, seperti GDPR untuk privasi data di Uni Eropa atau HIPAA untuk kesehatan informasi di Amerika Serikat.
f. Manajemen Identitas: Manajemen identitas dan akses harus diterapkan dengan baik untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke data dan aplikasi di lingkungan cloud. Ini bisa melibatkan manajemen identitas, kontrol akses berbasis peran, dan otentikasi ganda.
g. Pemulihan Bencana: Organisasi harus memiliki rencana pemulihan bencana yang efektif untuk mengatasi potensi kerugian data atau gangguan layanan di lingkungan cloud. Ini bisa mencakup penggunaan cadangan data, replikasi data, dan rencana pemulihan yang teruji secara reguler.
h. Keamanan Aplikasi: Aplikasi yang dijalankan di lingkungan cloud juga harus diamankan. Ini termasuk melakukan pengujian keamanan aplikasi, mengimplementasikan kontrol keamanan seperti firewall aplikasi web (WAF), dan memperbarui aplikasi secara teratur untuk memperbaiki kerentanan keamanan yang diketahui.
i. Pendidikan dan Kesadaran: Pengguna cloud harus diberi pelatihan tentang praktik keamanan yang baik dan potensi risiko yang terkait dengan penggunaan cloud computing. Ini membantu

dalam mencegah insiden keamanan yang disebabkan oleh kesalahan manusia atau kelalaian.

Dengan memperhatikan aspek-aspek keamanan di atas dan menerapkan praktik keamanan yang tepat, organisasi dapat memastikan bahwa data dan aplikasi mereka tetap aman dan terlindungi di lingkungan cloud computing.

2. Internet of Things (IoT) dan Keamanan

Internet of Things (IoT) adalah jaringan perangkat fisik yang terhubung ke internet, yang dapat saling berkomunikasi dan bertukar data. Keamanan IoT menjadi semakin penting karena jumlah perangkat yang terhubung terus meningkat, dan mereka seringkali memiliki akses ke data sensitif atau mengontrol sistem yang penting. Berikut adalah beberapa aspek penting dalam memastikan keamanan IoT:

a. Otentikasi dan Otorisasi: Perangkat IoT harus memiliki mekanisme otentikasi yang kuat untuk memastikan bahwa hanya pengguna yang sah yang memiliki akses ke perangkat dan data mereka. Otorisasi juga diperlukan untuk mengontrol hak akses pengguna ke fungsi-fungsi perangkat.
b. Enkripsi Komunikasi: Data yang dikirimkan antara perangkat IoT dan infrastruktur jaringan harus dienkripsi untuk melindungi dari penyadapan atau manipulasi data oleh pihak yang tidak berwenang. Penggunaan protokol enkripsi yang kuat seperti SSL/TLS sangat penting dalam hal ini.

c. Manajemen Identitas: Manajemen identitas yang efektif diperlukan untuk memastikan bahwa hanya perangkat yang sah yang memiliki akses ke jaringan dan sistem. Ini melibatkan pemberian identitas unik kepada setiap perangkat, serta manajemen otorisasi berbasis peran.
d. Pemantauan dan Deteksi Anomali: Sistem pemantauan harus diterapkan untuk mendeteksi aktivitas yang mencurigakan atau anomali dalam perilaku perangkat IoT. Hal ini memungkinkan untuk menanggapi insiden keamanan dengan cepat sebelum menjadi serius.
e. Perangkat Lunak yang Aman: Perangkat lunak yang menjalankan perangkat IoT harus dirancang dengan keamanan yang memadai, termasuk memperbarui perangkat lunak secara teratur untuk memperbaiki kerentanan yang diketahui dan menerapkan prinsip-prinsip pengembangan perangkat lunak yang aman.
f. Keamanan Jaringan: Jaringan yang menghubungkan perangkat IoT harus diamankan dengan firewall, deteksi intrusi, dan langkah-langkah keamanan jaringan lainnya untuk mencegah akses yang tidak sah ke perangkat dan data mereka.
g. Privasi Data: Penting untuk mempertimbangkan privasi data dalam desain perangkat IoT, termasuk pengumpulan, penyimpanan, dan penggunaan data yang dikumpulkan oleh perangkat. Pengguna harus diberikan kontrol atas data pribadi mereka dan

harus diberi informasi yang jelas tentang bagaimana data mereka digunakan.

h. Pembaruan dan Pemulihan: Perangkat IoT harus dirancang untuk memungkinkan pembaruan perangkat lunak yang mudah dan cepat untuk memperbaiki kerentanan keamanan yang ditemukan. Selain itu, rencana pemulihan bencana harus disiapkan untuk mengatasi insiden keamanan yang parah atau kegagalan perangkat.
i. Pendidikan dan Kesadaran: Pengguna perangkat IoT harus diberi pelatihan tentang praktik keamanan yang baik dan potensi risiko yang terkait dengan penggunaan perangkat IoT. Hal ini membantu dalam mencegah insiden keamanan yang disebabkan oleh kesalahan manusia atau kelalaian.

Dengan memperhatikan aspek-aspek keamanan di atas dan menerapkan praktik keamanan yang tepat, organisasi dan individu dapat memastikan bahwa perangkat IoT mereka tetap aman dan terlindungi dari serangan atau penyalahgunaan.

3. Kecerdasan Buatan (AI) dan Keamanan

Kecerdasan Buatan (AI) memiliki potensi yang besar untuk meningkatkan keamanan informasi, tetapi juga dapat menjadi sumber risiko keamanan yang signifikan jika tidak dikelola dengan baik. Berikut adalah beberapa aspek kunci terkait keamanan AI:

a. Serangan Terhadap Model AI: Model AI rentan terhadap berbagai jenis serangan, termasuk serangan lapisan data (data poisoning), serangan

evasion, dan serangan model. Misalnya, serangan data poisoning dapat memanipulasi data pelatihan untuk menghasilkan prediksi yang salah atau berbahaya.

b. Privasi dan Penggunaan Data: Penggunaan AI dalam menganalisis data pribadi dapat menimbulkan masalah privasi. Penting untuk memastikan bahwa data sensitif dijaga kerahasiaannya dan bahwa pengguna memberikan izin yang tepat untuk penggunaan data mereka.
c. Bias dan Diskriminasi: Sistem AI dapat menghasilkan hasil yang bias atau diskriminatif jika data pelatihan yang digunakan tidak representatif atau memiliki bias tertentu. Penting untuk memeriksa dan mengurangi bias dalam data pelatihan dan algoritma untuk mencegah hasil yang tidak adil.
d. Keamanan Model: Model AI harus dilindungi dari serangan fisik dan serangan siber yang bertujuan mengubah atau menghancurkan model, atau mengambil alih kontrolnya. Ini bisa dilakukan melalui teknik seperti enkripsi model, tanda tangan digital, dan pengawasan penggunaan model.
e. Transparansi dan Akuntabilitas: Penting untuk menjaga transparansi dan akuntabilitas dalam penggunaan AI, terutama dalam konteks keputusan yang memengaruhi individu atau masyarakat secara luas. Penggunaan AI harus dapat dijelaskan dan dipertanggungjawabkan.
f. Keamanan Operasional: Sistem yang mengandalkan AI harus diamankan secara

menyeluruh untuk mencegah akses yang tidak sah ke data dan model AI, serta untuk melindungi integritas dan ketersediaan sistem.

g. Pendeteksian dan Respon Terhadap Ancaman: Perlu dilakukan upaya untuk mendeteksi dan merespons ancaman terhadap sistem AI dengan cepat. Ini melibatkan pemantauan aktif terhadap aktivitas yang mencurigakan, serta rencana darurat dan pemulihan bencana.
h. Pendidikan dan Kesadaran: Pengguna AI perlu diberi pelatihan tentang praktik keamanan yang baik dan potensi risiko yang terkait dengan penggunaan teknologi ini. Hal ini membantu dalam mencegah serangan yang disebabkan oleh kesalahan manusia atau kelalaian.

Dengan memperhatikan aspek-aspek keamanan di atas dan menerapkan praktik keamanan yang tepat, organisasi dapat memastikan bahwa sistem AI mereka tetap aman dan terlindungi dari serangan atau penyalahgunaan.

K. Masa Depan Keamanan Sistem Informasi

1. Tantangan dan Peluang Masa Depan

Tantangan dan peluang masa depan terkait keamanan teknologi informasi sangat berkaitan dengan perkembangan teknologi yang terus berubah dan evolusi ancaman keamanan yang semakin kompleks. Berikut adalah beberapa tantangan dan peluang yang mungkin dihadapi di masa depan:

a. Tantangan:

1) Kesenjangan Keterampilan: Permintaan akan profesional keamanan informasi yang berkualitas terus meningkat, tetapi ada kekurangan keterampilan dalam industri. Kesenjangan ini dapat menyulitkan organisasi untuk menemukan dan mempertahankan personel keamanan yang berkualitas.

2) Serangan yang Lebih Canggih: Serangan siber semakin canggih dengan adopsi teknologi baru seperti kecerdasan buatan dan teknik serangan yang terotomatisasi. Ini membuat sulit bagi organisasi untuk mendeteksi, mencegah, dan merespons serangan yang semakin kompleks.

3) Regulasi yang Berubah: Perubahan dalam regulasi privasi data dan keamanan informasi dapat menimbulkan tantangan bagi organisasi dalam mematuhi peraturan yang berkembang dan berubah. Kepatuhan yang tepat membutuhkan pemahaman mendalam tentang peraturan yang berlaku dan kemampuan untuk beradaptasi dengan cepat terhadap perubahan tersebut.

4) Perangkat IoT yang Rentan: Pertumbuhan Internet of Things (IoT) membawa tantangan baru dalam hal keamanan, karena banyak perangkat IoT rentan terhadap serangan dan dapat digunakan sebagai pintu masuk ke jaringan organisasi.

5) Privasi Data yang Diperhatikan: Kekhawatiran tentang privasi data terus meningkat, terutama dengan adopsi teknologi pengumpulan data yang besar dan analisis data. Organisasi harus menghadapi tantangan ini dengan memastikan bahwa data pelanggan dan karyawan dijaga kerahasiaannya dengan baik.

b. Peluang:
   1) Peningkatan Keamanan Berbasis AI: Penggunaan kecerdasan buatan untuk meningkatkan deteksi ancaman, analisis risiko, dan respons terhadap serangan dapat membantu organisasi untuk menjadi lebih responsif dan efektif dalam melindungi aset mereka.
   2) Kerjasama Industri: Kolaborasi antara organisasi, lembaga pemerintah, dan lembaga penegak hukum dapat meningkatkan kemampuan untuk mendeteksi, mencegah, dan merespons serangan siber. Pertukaran informasi tentang ancaman dan praktik keamanan terbaik dapat membantu memperkuat pertahanan secara keseluruhan.
   3) Pendekatan Proaktif: Organisasi dapat mengambil pendekatan proaktif terhadap keamanan dengan meningkatkan kesadaran pengguna, mengadopsi praktik keamanan yang kuat, dan melakukan pengujian keamanan secara teratur. Ini membantu mencegah insiden keamanan sebelum mereka terjadi.

4) Automasi dan Orkestrasi: Automasi dan orkestrasi proses keamanan dapat membantu mengurangi beban kerja personel keamanan, meningkatkan respons terhadap serangan, dan mempercepat deteksi dan pemulihan dari insiden keamanan.
5) Inovasi Teknologi: Inovasi dalam teknologi keamanan informasi, seperti enkripsi kuantum, keamanan post-kuantum, dan identifikasi biometrik yang maju, dapat membuka peluang baru untuk meningkatkan keamanan informasi di masa depan.

Dengan menghadapi tantangan ini dan memanfaatkan peluang yang tersedia, organisasi dapat memperkuat pertahanan mereka terhadap ancaman keamanan yang berkembang dan memastikan bahwa data dan aset mereka tetap aman di masa depan.

2. Inovasi dan Teknologi Baru

Inovasi dan teknologi baru terus membentuk lanskap keamanan informasi, baik dengan memberikan solusi baru untuk mengatasi ancaman keamanan yang ada maupun dengan memperkenalkan tantangan baru. Berikut adalah beberapa inovasi dan teknologi baru yang mempengaruhi bidang keamanan informasi:

a. Kecerdasan Buatan (AI) dan Pembelajaran Mesin (ML): AI dan ML digunakan untuk meningkatkan deteksi ancaman, mengidentifikasi pola yang mencurigakan dalam lalu lintas jaringan, dan memperbaiki respons terhadap serangan. Teknologi ini juga digunakan untuk meningkatkan

analisis risiko dan mengoptimalkan keamanan berdasarkan data.

b. Enkripsi Kuantum: Enkripsi kuantum menjanjikan keamanan yang lebih kuat dibandingkan dengan algoritma enkripsi klasik. Ini dapat menghasilkan solusi keamanan yang tangguh untuk mengamankan komunikasi dan data sensitif dari serangan kriptografi klasik dan komputasi kuantum.
c. Keamanan Blockchain: Teknologi blockchain menawarkan sistem yang terdesentralisasi dan aman yang dapat digunakan untuk menyimpan catatan transaksi dan data sensitif dengan cara yang tidak dapat diubah. Ini dapat digunakan dalam berbagai aplikasi, termasuk manajemen identitas dan layanan keuangan.
d. Teknologi Pengenal Wajah dan Biometrik: Pengenal wajah, sidik jari, dan teknologi biometrik lainnya digunakan untuk otentikasi pengguna dengan cara yang lebih aman dan nyaman. Penggunaan biometrik meningkatkan keamanan sistem dengan memastikan bahwa hanya orang yang sah yang dapat mengakses data atau sumber daya tertentu.
e. Keamanan IoT: Solusi keamanan khusus untuk Internet of Things (IoT) sedang dikembangkan untuk melindungi perangkat yang terhubung dari serangan, termasuk keamanan perangkat keras, enkripsi lalu lintas data, dan pengelolaan akses yang aman.

f. Pengujian Keamanan Otomatis: Alat dan platform pengujian keamanan otomatis terus dikembangkan untuk membantu organisasi mendeteksi dan memperbaiki kerentanan perangkat lunak dengan cepat dan efisien.
g. Teknologi Nirkabel yang Aman: Standar keamanan nirkabel seperti WPA3 untuk jaringan Wi-Fi dan 5G untuk jaringan seluler dirancang dengan keamanan yang lebih baik daripada pendahulunya, membantu melindungi data dan komunikasi dari serangan.
h. Analisis Big Data dan Data Pengelolaan: Teknologi analisis big data dan manajemen data diterapkan untuk mengidentifikasi pola ancaman yang rumit, memantau aktivitas jaringan yang mencurigakan, dan memprediksi potensi serangan berdasarkan tren data.
i. Pembaruan Terus-Menerus: Riset dan pengembangan keamanan informasi terus berlanjut, dan dengan demikian, solusi keamanan baru terus muncul untuk mengatasi ancaman yang berkembang.

Dengan memanfaatkan inovasi dan teknologi baru ini, organisasi dapat memperkuat pertahanan mereka terhadap ancaman keamanan yang terus berkembang dan menjaga data dan aset mereka tetap aman di era digital yang semakin kompleks ini.

3. Peran Profesional Keamanan Sistem Informasi

Para profesional keamanan sistem informasi memiliki peran yang krusial dalam menjaga keamanan dan integritas sistem informasi organisasi. Berikut

adalah beberapa peran kunci yang dimainkan oleh para profesional keamanan sistem informasi:

a. Analisis Risiko: Mereka bertanggung jawab untuk melakukan analisis risiko secara teratur untuk mengidentifikasi potensi ancaman, kerentanan, dan dampaknya terhadap organisasi. Ini melibatkan evaluasi keamanan sistem, aplikasi, dan infrastruktur untuk mengidentifikasi area yang rentan dan mengembangkan strategi mitigasi yang efektif.
b. Pengembangan Kebijakan Keamanan: Mereka membantu dalam pengembangan kebijakan keamanan informasi yang tepat untuk organisasi, termasuk kebijakan akses, kebijakan sandi, kebijakan keamanan jaringan, dan kebijakan penggunaan perangkat. Kebijakan ini memastikan bahwa praktik keamanan terstandarisasi dan dipatuhi oleh semua pengguna dan sistem.
c. Implementasi Kontrol Keamanan: Para profesional keamanan sistem informasi bertanggung jawab untuk menerapkan kontrol keamanan yang diperlukan, seperti firewall, enkripsi, deteksi intrusi, dan pemantauan keamanan, untuk melindungi sistem dan data organisasi dari ancaman yang ada.
d. Pendidikan dan Kesadaran: Mereka memberikan pelatihan kepada pengguna dan personel organisasi tentang praktik keamanan yang baik dan kesadaran akan ancaman keamanan. Ini membantu mengurangi risiko serangan yang disebabkan oleh kesalahan manusia atau kelalaian.

e. Deteksi dan Respons Terhadap Ancaman: Para profesional keamanan sistem informasi memantau aktivitas jaringan dan sistem secara teratur untuk mendeteksi ancaman keamanan yang potensial. Mereka juga bertanggung jawab untuk merespons terhadap insiden keamanan dengan cepat dan efektif, termasuk investigasi, pemulihan, dan pelaporan insiden.
f. Pengujian Keamanan: Mereka melakukan pengujian keamanan reguler, seperti pengujian penetrasi dan audit keamanan, untuk mengevaluasi keamanan sistem dan infrastruktur organisasi. Hal ini membantu mengidentifikasi kerentanan yang mungkin dieksploitasi oleh penyerang.
g. Kepatuhan dan Audit: Para profesional keamanan sistem informasi memastikan bahwa organisasi mematuhi standar keamanan dan peraturan yang berlaku, serta mempersiapkan organisasi untuk audit keamanan eksternal dan internal.
h. Pemulihan Bencana: Mereka mengembangkan rencana pemulihan bencana dan mengkoordinasikan upaya pemulihan setelah insiden keamanan atau bencana teknologi, seperti serangan malware, kebocoran data, atau kegagalan sistem.

Peran para profesional keamanan sistem informasi sangat penting dalam menjaga integritas, ketersediaan, dan kerahasiaan sistem informasi organisasi. Dengan memainkan peran mereka dengan baik, mereka dapat membantu organisasi menghadapi ancaman keamanan yang terus berkembang dan menjaga operasi mereka tetap aman dan terlindungi.

BAB

4

Kebijakan dan Standar Keamanan Sistem Informasi

Nuk Ghurroh Setyoningrum, S.Kom, M.Cs

Kebijakan dan standar keamanan sistem informasi merupakan pilar fundamental dalam mengelola risiko dan melindungi aset digital suatu organisasi. Dalam era di mana teknologi informasi menjadi tulang punggung operasi bisnis, kebijakan yang solid dan standar yang jelas sangatlah vital. Melalui penerapan kebijakan yang tepat dan standar yang

terukur, perusahaan dapat mengidentifikasi, mengurangi, dan mengelola ancaman keamanan dengan efektif. Selain itu, kebijakan yang komprehensif dan standar yang terkini juga memastikan bahwa organisasi mematuhi regulasi yang berlaku dan menjaga kepercayaan pemangku kepentingan. Dalam konteks ini, penting bagi perusahaan untuk memahami serta mengikuti perkembangan teknologi dan regulasi untuk memastikan kebijakan dan standar keamanan mereka tetap relevan dan efektif dalam menghadapi tantangan keamanan yang terus berkembang.

Kini, kita hidup di era digital di mana komunikasi dan pertukaran informasi terjadi melalui jaringan yang semakin meluas. Kemajuan teknologi yang menghubungkan komputer di seluruh dunia memfasilitasi pertukaran informasi, data, gambar, dan video secara efisien. Semakin pentingnya sebuah informasi, semakin esensial pula adanya standar keamanan untuk melindunginya (Pegangan Untuk Mahasiswa, Hayaty and Cs, n.d.).

Isu keamanan berkaitan erat dengan isu hukum. Istilah hukum cyber semakin populer. Bagian ini akan membahas beberapa aspek keamanan yang terkait dengan hukum.

A. Hukum dan Keamanan

Koneksi sebuah sistem informasi dengan Internet membuka peluang bagi kejahatan melalui jaringan komputer, menantang penegak hukum yang dihadapkan pada keterbatasan hukum di ranah cyber. Sebagian besar negara sedang berupaya mengembangkan kerangka hukum untuk regulasi Internet. Meskipun ada banyak aspek yang dapat diperdebatkan, buku ini hanya membahas topik yang

terkait dengan keamanan sistem, sedangkan isu-isu seperti perpajakan, perbankan, bisnis, merek dagang, serta hak kekayaan intelektual tidak disentuh. Seperti Dalam e-commerce, terdapat masalah hukum terkait privasi dan penggunaan teknologi kriptografi, seperti enkripsi. Setiap negara memiliki regulasi yang berbeda-beda; misalnya, Amerika Serikat memiliki pembatasan terhadap ekspor teknologi enkripsi. Keamanan data kesehatan juga menjadi perhatian penting, sementara hukum terkait sistem perbankan berbeda-beda di setiap negara. Kendala semacam ini membuat transaksi e-commerce menjadi rumit karena harus mempertimbangkan batasan-batasan fisik negara.

Penegakan hukum merupakan isu yang kompleks. Sebagai contoh, jika seseorang tertangkap melakukan tindakan cracking dan menyebabkan kerugian finansial, pertanyaan muncul mengenai jenis hukuman yang pantas diberikan. Sebagai ilustrasi, di Cina, dua orang pelaku cracking dihukum mati setelah tertangkap mencuri uang sebesar US$31.400 dari sebuah bank di Cina bagian Timur. Informasi lebih lanjut dapat ditemukan di tautan berikut:

http://www.news.com/News/Item/0,4,30332,00.html

http://cnn.com/WORLD/asiapcf/9812/28/BC-CHINA-HACKERS.reut/index.html

http://slashdot.org/articles/98/12/28/096231.shtml

Menurut Budi Raharjo (Rahardjo, 1998), menjelaskan hukum keamanan sistem informasi di luar negeri, Beberapa hukum yang terkait dengan masalah komputer, jaringan komputer, dan sistem informasi di luar negeri antara lain:

a. Di Amerika Serikat ada "Computer Fraud and Abuse Act" (1984) dan kemudian diperbaiki di tahun 1994.
b. Di Inggris ada "Computer Misuse Act of 1990".

B. Penggunaan Enkripsi dan Teknologi Kriptografi Secara Umum

Satu metode untuk melindungi data dan informasi adalah dengan memanfaatkan teknologi kriptografi. Sebagai contoh, data dapat disandikan menggunakan metode tertentu sehingga hanya dapat diakses oleh pihak yang ditentukan. Namun, terdapat beberapa tantangan yang terkait dengan penerapan teknologi kriptografi ini, termasuk:

1. Pembatasan ekspor teknologi kriptografi dari Amerika Serikat (AS) merupakan suatu kebijakan yang menyulitkan, meskipun AS merupakan pusat perkembangan teknologi kriptografi yang maju. Alasan di balik pembatasan ini adalah kekhawatiran pemerintah AS terhadap kemampuan mereka untuk memantau komunikasi yang dienkripsi yang terkait dengan aktivitas mafia, teroris, dan musuh negara AS. Oleh karena itu, produk-produk teknologi kriptografi dianggap sebagai barang munisi, yang penjualannya dibatasi untuk ekspor. Larangan ini mengakibatkan kesulitan dalam menciptakan interoperabilitas antara produk yang menggunakan teknologi kriptografi.

   Selain Amerika Serikat, negara lain menerima produk dengan standar keamanan yang lebih

rendah. Sebagai ilustrasi, peramban web Netscape memiliki fitur keamanan yang menggunakan sistem RSA. Saat ini, implementasi RSA dengan panjang kunci 128 bit hanya diizinkan untuk digunakan di dalam Amerika Serikat dan tidak dapat diekspor. Oleh karena itu, Netscape harus menciptakan versi internasional yang menggunakan panjang kunci 56 bit dan dapat diekspor.

Keamanan sistem yang beroperasi dengan panjang kunci 56 bit secara signifikan lebih rendah daripada yang menggunakan panjang kunci 128 bit. Sebagai contoh lain, mekanisme autentikasi (MSCHAP) dalam produk Microsoft Windows NT 4.0 menggunakan enkripsi 40 bit untuk versi internasional dan 128 bit untuk produk yang hanya tersedia di AS. Saat ini, panjang kunci 40 bit dianggap tidak memadai untuk menjaga kerahasiaan data. Akibatnya, banyak individu memilih untuk membeli produk keamanan dari negara lain daripada dari Amerika Serikat, yang pada akhirnya merugikan perusahaan-perusahaan di AS.

2. Bagi suatu negara, bergantung pada negara lain untuk masalah keamanan merupakan hal yang sangat sensitif. Kemampuan suatu negara dalam menguasai teknologi adalah hal yang sangat penting. Namun, apa yang akan terjadi jika kedua negara tersebut terlibat dalam konflik bersenjata?

3. Ketergantungan pada negara lain juga memiliki signifikansi penting dalam konteks bisnis, terutama dalam hal perdagangan elektronik. Sebagai contoh, jika e-commerce menggunakan produk yang harus dilisensi dari negara lain, hal itu dapat menyebabkan banyak devisa negara digunakan hanya untuk pembayaran lisensi teknologi tersebut.
4. Algoritma-algoritma yang sangat efektif untuk kriptografi biasanya dipatenkan, yang seringkali membuat penerapan suatu produk menjadi sulit tanpa melanggar hak paten. Selain itu, setiap negara memiliki pandangan yang berbeda terkait dengan hak paten. Sebagai contoh, meskipun algoritma RSA dipatenkan di Amerika Serikat, namun tidak diakui sebagai paten di Jepang.

Pemerintah suatu negara berupaya mengatur penggunaan teknologi enkripsi melalui peraturan, namun pendekatan ini menimbulkan keberatan dan keraguan dari banyak pihak.

C. Barang Bukti Digital

Salah satu tantangan yang muncul dari teknologi digital adalah kemampuan untuk mengubah data dengan mudah. Sebuah dokumen elektronik bisa diubah dengan cepat menggunakan perangkat pengolah kata sehingga dokumen tersebut terlihat tidak berubah. Di dunia analog, jika kita melakukan perubahan pada sebuah dokumen (seperti menghapus atau menimpanya dengan tulisan baru),

perubahan tersebut akan terlihat jelas. Karena perbedaan ini, seringkali sulit untuk mengandalkan bukti digital.

Apakah dokumen elektronik dapat dianggap sebagai bukti yang sah? Jika kita mempertimbangkan dokumen yang dibuat melalui word processor, mana yang dianggap sebagai versi asli? Apakah yang dicetak dalam bentuk kertas? Atau yang tersimpan dalam harddisk? Mungkin yang ada dalam CD? Atau yang saat ini berada dalam memori komputer?

Pertanyaan-pertanyaan di atas timbul karena kita menerapkan pemikiran konvensional. Dalam paradigma lama, hanya ada satu dokumen yang dianggap asli, sementara dalam era digital, dapat ada lebih dari satu versi dokumen yang dianggap asli. Keaslian sebuah dokumen tidak ditentukan oleh jumlahnya, tetapi oleh keaslian isinya. Dalam lingkungan digital, hal ini dapat dicapai melalui penggunaan tanda tangan digital. Tanda tangan digital adalah konsep yang memastikan bahwa isi dokumen tidak mengalami perubahan. Salah satu aspek penting yang harus dipertahankan adalah "non-repudiation" atau ketidakmampuan untuk menyangkal keaslian dokumen, yang dapat terpenuhi dengan adanya tanda tangan digital. Bahkan dengan menggunakan tanda tangan digital, sebuah dokumen yang dicetak, difotokopi, atau difaksimili tetap dianggap tidak asli.

D. Isu yang terkait dengan hak paten

Penerapan enkripsi dengan kunci publik secara signifikan meningkatkan tingkat keamanan informasi. Salah satu algoritma yang umum digunakan adalah RSA. Algoritma ini dipatenkan di Amerika Serikat dengan nomor U.S. Patent 4,405,829 yang dikeluarkan pada 20 Agustus 1983. Paten ini dimiliki oleh Public Key Partners (PKP) di Sunnyvale, California, dan akan kedaluwarsa pada tahun 2000. RSA tidak dipatenkan di luar Amerika Utara. Namun, masalah penggunaan algoritma RSA di Indonesia merupakan topik diskusi menarik, terutama mengingat penggunaan enkripsi di luar Amerika merupakan hal yang menarik untuk dibahas.

Secara keseluruhan, penting untuk mempertimbangkan secara cermat keputusan untuk mematenkan teknologi. Karena pada praktiknya, paten cenderung memberikan keuntungan kepada perusahaan besar. Proses pendaftaran paten juga membutuhkan biaya yang signifikan. Jika terjadi pelanggaran paten, pemilik paten yang tidak memiliki sumber daya finansial yang memadai akan menghadapi kesulitan dalam menghadapi perusahaan besar yang melanggar patennya. Hanya perusahaan besar yang mampu mempertahankan hak patennya dengan efektif.

Hak paten juga bisa menjadi hambatan dalam pengembangan produk. Coba bayangkan, untuk menciptakan sebuah printer, diperlukan lebih dari seribu hak paten. Bagaimana mungkin perusahaan kecil di Indonesia dapat bersaing dengan perusahaan besar dari luar negeri?

Hak paten bisa meningkatkan harga produk. Sebagai contoh, dalam kasus obat HIV/AIDS, penduduk miskin di Afrika dan India kesulitan untuk membeli obat yang harganya tinggi. Awalnya, tidak ada obat generik yang tersedia untuk penyakit ini karena masalah hak paten. Dalam kasus ini, Pemerintah Afrika Selatan mengadopsi "compulsory license" sehingga perusahaan lokal dapat memproduksi obat tersebut dengan harga yang lebih terjangkau.

E. Hak Paten Perangkat Lunak

Topik yang sedang mendapat perhatian adalah hak paten untuk perangkat lunak (software patent). Awalnya, perlindungan untuk perangkat lunak dilakukan melalui hak cipta. Namun, saat ini, Amerika Serikat menjadi pelopor dalam mendorong penggunaan hak paten untuk perangkat lunak. Yang dipatenkan dalam perangkat lunak adalah algoritmanya. Namun, masalahnya timbul ketika algoritma yang dipatenkan menjadi semakin luas. Hal ini menyebabkan hal-hal yang sebelumnya dianggap sederhana menjadi dipatenkan, yang pada gilirannya menyulitkan proses inovasi. Bayangkan, bahkan untuk membuat program sederhana, seorang pengembang perangkat lunak mungkin harus mendapatkan lisensi untuk berbagai paten. Ini menyebabkan biaya tambahan sebelum pekerjaan sebenarnya dimulai. Paten yang bisa mencegah terciptanya inovasi:

1. Algoritma Lempel-Ziv (LZW) sering digunakan untuk kompresi gambar. Sebagai contoh, algoritma ini digunakan dalam format GIF untuk menyimpan

gambar. Oleh karena itu, jika Anda membuat program yang menggunakan format GIF, Anda harus membayar royalti kepada pemilik paten algoritma LZW, yang pada saat buku ini ditulis adalah Unisys. Inilah sebabnya mengapa banyak situs web atau program gambar saat ini beralih menggunakan format PNG.

2. E-commerce satu klik. Jika Anda membuat situs web yang memfasilitasi transaksi, seperti pembeli memilih barang, menambahkannya ke keranjang belanja, dan melakukan pembayaran, Anda mungkin melanggar paten (paten AS 5,960,411, "Metode dan sistem untuk melakukan pemesanan melalui jaringan komunikasi") yang didaftarkan oleh Amazon. Penggunaan cookie untuk implementasi semacam itu merupakan hal yang sangat sederhana dan umum dilakukan.

3. Pada tahun 1980-an, perusahaan XyQuest meluncurkan produk pengolah kata yang dikenal dengan nama XyWrite, yang menjadi sangat populer pada masa itu. Namun, suatu ketika, perusahaan tersebut terpaksa menghapus fitur "automatic correction and abbreviation expansion" dari XyWrite karena dianggap melanggar paten yang dimiliki oleh perusahaan lain. Sebagai hasilnya, pengguna XyWrite tidak lagi dapat mengakses fitur tersebut. Jika Anda mempertimbangkan untuk menambahkan fitur serupa dalam program pengolah kata yang Anda buat, siap-siap untuk membayar royalti atau menghadapi tuntutan hukum.

F. Kerahasiaan Privasi

Privasi merupakan hak fundamental manusia, meskipun opini tentang kapan dan sejauh mana privasi pantas bisa berbeda-beda secara sah, mungkin dipengaruhi oleh faktor budaya, sejarah, atau personal. Namun, pada prinsipnya, hak privasi bergantung pada situasi tertentu di mana kebutuhan akan privasi, kepemilikan dan kontrol atas data, serta hak dan kewajiban hukum dari semua pihak yang terlibat berperan penting. Di samping itu, seperti yang terjadi pada kerahasiaan, integritas, dan ketersediaan, kadang-kadang privasi dapat bertentangan dengan aspek-aspek keamanan lainnya.

Privasi merujuk pada kemampuan individu atau kelompok untuk menjaga kehidupan pribadi dan urusan mereka dari publik, atau mengendalikan aliran informasi tentang diri mereka. Karena privasi memiliki dimensi yang luas, namun pada bab ini kami akan membatasi pembahasan hanya pada aspek-aspek privasi yang terkait dengan keamanan komputer. Oleh karena itu, dalam bab ini kami akan mengulas makna privasi informasi. Kami akan mengevaluasi identifikasi dan otentikasi, dua elemen penting dalam komputasi yang memiliki dampak besar pada privasi. Kami akan mempertimbangkan bagaimana privasi berkaitan dengan penggunaan Internet, terutama dalam konteks email dan akses web. Terakhir, kami akan menyelidiki beberapa teknologi komputer baru yang muncul dan mempertimbangkan relevansinya dengan privasi.

Privasi merupakan hak pribadi yang melibatkan kebebasan individu. Sebagai analogi, ketika Anda mengirim surat kepada teman, Anda cenderung menggunakan amplop tertutup meskipun isi suratnya mungkin tidak bersifat rahasia. Anda tidak memilih kartu pos sebagai alternatif pengiriman karena Anda tidak ingin orang lain membaca surat Anda.

1. Konsep Dasar Privasi

Menurut Budi Raharjo ,perbincangan tentang konsep privasi semakin relevan di era saat ini, mengingat kemajuan teknologi yang mampu merekam dan menyimpan jenis-jenis informasi pribadi baru, seperti sidik jari, wajah, dan bahkan retina seseorang. Proses perekaman dan penyimpanan ini tidak terbatas pada skala kecil, tetapi juga dalam skala besar. Bayangkan seberapa banyak pengguna ponsel, seperti iPhone, yang menggunakan pemindaian sidik jari, atau pengguna Facebook yang melakukan pengenalan atau tagging wajah (seperti yang terlihat dalam ilustrasi di atas). Penggunaan internet yang semakin meluas bersamaan dengan penggunaan ponsel telah memperluas penetrasi teknologi tersebut ke berbagai aspek kehidupan, bahkan melampaui apa yang pernah kita bayangkan sebelumnya (Raharjo, n.d.).

a. Aspek Privacy Informasi

Informasi harus terjaga keamanannya, yang berarti hanya pihak-pihak yang memiliki kepentingan yang dapat mengaksesnya sesuai dengan sifat dan tujuan informasi tersebut. Privasi informasi dapat dipahami

melalui tiga aspek utama: sensitivitas data, pihak yang terlibat, dan pengendalian dalam pengungkapan.

1) Pengungkapan yang dikendalikan

Privasi merupakan hak untuk mengendalikan siapa yang memiliki pengetahuan tentang aspek-aspek tertentu dari diri Anda, komunikasi, dan aktivitas Anda. Dengan kata lain, Anda secara sukarela memilih siapa yang memiliki akses terhadap informasi tentang Anda. Seseorang mungkin meminta nomor telepon Anda: seorang mekanik mobil, karyawan toko, petugas pajak, rekan bisnis baru, atau teman baru. Dalam setiap situasi tersebut, Anda mempertimbangkan alasan mengapa orang tersebut membutuhkan informasi tersebut dan kemudian Anda membuat keputusan apakah akan memberikannya. Yang penting, keputusan akhir berada di tangan Anda. Jadi, privasi adalah sesuatu di mana Anda memiliki pengaruh yang signifikan.

Namun, Anda tidak memiliki kontrol mutlak. Setelah Anda memberikan nomor Anda kepada seseorang atau sistem, tingkat kontrol Anda akan berkurang karena sebagian bergantung pada tindakan yang diambil oleh individu atau sistem tersebut terhadap informasi yang diberikan. Dengan memberikan nomor Anda, Anda mengalihkan atau menyerahkan wewenang dan pengendalian kepada pihak lain. Anda mungkin mengungkapkan keinginan seperti "jangan memberikan nomor saya kepada orang lain", "gunakan dengan bijaksana", atau "Saya sangat menjaga privasi saya", tetapi Anda tidak memiliki

kontrol langsung atas tindakan individu atau sistem lain. Anda harus mempercayai orang atau sistem tersebut untuk mematuhi keinginan Anda, apakah Anda menyatakannya secara tegas atau tidak. Masalah ini serupa dengan masalah propagasi keamanan komputer: siapa pun yang memiliki akses ke suatu objek dapat menyalin, mentransfer, atau menyebarkan objek tersebut atau isinya kepada orang lain tanpa batasan. Bahkan jika Anda menentukan bahwa objek tersebut harus dihapus atau dihancurkan setelah periode waktu tertentu, Anda tidak memiliki cara untuk memverifikasi apakah sistem atau individu tersebut benar-benar menghapus atau menghancurkan konten tersebut.

2) Data Sensitive

Seseorang bertanya tentang ukuran sepatu Anda. Anda dapat merespons dengan mengatakan, "Saya sangat pribadi dan sulit bagi saya untuk memahami alasan Anda ingin mengetahui rincian yang begitu intim" atau Anda dapat memberikan jawaban langsung, misalnya "10C"; beberapa orang menganggap beberapa informasi lebih rahasia daripada yang lain. Beberapa jenis informasi secara umum dianggap sebagai informasi yang sensitif, seperti status keuangan, catatan kesehatan tertentu, peristiwa traumatis di masa lalu seseorang, dan sebagainya. Oleh karena itu, jika Anda mengetahui sesuatu yang dianggap sensitif tentang seseorang, Anda cenderung untuk menjaganya kerahasiaannya kecuali jika ada alasan yang kuat untuk mengungkapkannya. Sebagai contoh, di banyak wilayah, tenaga kesehatan (yang tertarik pada

identifikasi penyakit, penanggulangan, dan pencegahan) diwajibkan untuk melaporkan kasus penyakit yang sangat menular atau mematikan, bahkan jika orang yang terkena tidak ingin informasi tersebut dipublikasikan. Namun, kebanyakan dari kita tidak terlalu mempermasalahkan ukuran sepatu kita, jadi kita biasanya tidak melindungi informasi itu jika diminta, atau jika kita mengetahui informasi tersebut tentang orang lain. Dalam banyak situasi, kita menghormati permintaan untuk menjaga kerahasiaan informasi yang sensitif seseorang.

3) Subjek yang Memerlukan

Individu, kelompok, perusahaan, organisasi, dan pemerintah semuanya memiliki data yang dianggap sensitif oleh mereka. Kami menggunakan istilah "subjek" dan "pemilik" untuk memisahkan antara individu atau entitas yang diperinci dalam data dan individu atau entitas yang menyimpan data tersebut. Sejauh ini, kami telah menjelaskan privasi dari perspektif individu, di mana subjeknya adalah individu. Namun, organisasi publik dan swasta juga tertarik pada privasi. Perusahaan mungkin memiliki data yang dianggap pribadi atau sensitif, seperti rencana produk, pelanggan kunci, margin keuntungan, dan teknologi yang baru ditemukan. Bagi perusahaan swasta, privasi biasanya terkait dengan memperoleh dan menjaga keunggulan dalam persaingan. Organisasi lain, seperti sekolah, rumah sakit, atau badan amal, mungkin perlu melindungi data pribadi tentang siswa, pasien, atau pendonor mereka. Banyak organisasi juga melindungi

informasi yang terkait dengan reputasi mereka; mereka mungkin ingin mengendalikan berita negatif atau waktu rilis informasi yang dapat mempengaruhi harga saham atau keputusan hukum. Sebagian besar pemerintah menganggap masalah militer dan diplomatik sebagai sensitif, tetapi mereka juga mengakui tanggung jawab mereka untuk memberikan informasi yang memperkaya wacana nasional. Pada saat yang sama, pemerintah memiliki tanggung jawab untuk melindungi dan menjaga kerahasiaan data yang mereka kumpulkan dari warga negara, seperti informasi pajak.

2. Masalah Privacy dalam Komputer

Anda mungkin mencatat bahwa banyak jenis data sensitif dan banyak aspek tentang privasi tidak memiliki kaitan langsung dengan komputer. Anda benar dalam hal itu: Kepekaan dan isu-isu tersebut telah ada sebelum era komputer. Komputer dan jaringan hanya mengubah cara kita mengakses, menyimpan, dan memproses informasi, serta memengaruhi seberapa cepat dan seberapa luas informasi tersebut dapat tersebar. Meskipun kantor arsip publik telah lama menjadi tempat di mana orang dapat mengakses data yang tersimpan di sana, kemajuan dalam kapasitas penyimpanan dan kecepatan komputer telah memberikan kita kemampuan untuk mengumpulkan, mencari, dan menghubungkan data dengan lebih cepat dan lebih efisien daripada sebelumnya. Dengan bantuan mesin pencari, kita dapat menemukan satu item data dari miliaran, mirip dengan

menemukan satu lembar kertas dari gudang yang penuh dengan kotak kertas. Selain itu, dengan ketersediaan jaringan dan portabilitas teknologi seperti laptop, tablet, ponsel, dan perangkat WiFi, risiko pengungkapan yang mempengaruhi privasi telah meningkat secara signifikan.

3. Pengumpulan Data

Seperti yang telah kami jelaskan sebelumnya, kemajuan dalam teknologi penyimpanan komputer telah memungkinkan penyimpanan dan pengolahan data dalam jumlah besar. Kapasitas disk pada perangkat konsumen umumnya diukur dalam ukuran gigabyte (109 atau 1 miliar byte), terabyte (1012 atau 1 triliun byte), petabyte (1015 atau 1 kuadriliun byte), dan exabyte (1018 atau 1 triliun byte). Pada tahun 2012, Ngo melaporkan pencapaian penting dalam kepadatan penyimpanan oleh Seagate: satu terabyte per inci, memungkinkan produksi hard drive dengan kapasitas hingga 60 terabyte. Plafke menyoroti upaya dari tim di Pusat Mikro-Fotonik Swinburne University yang berhasil meningkatkan kapasitas penyimpanan DVD dari 4,7 gigabyte menjadi 1 petabyte tanpa mengubah fisik cakram, melainkan dengan mengubah laser pembaca data. Solar juga melaporkan tentang kemajuan dalam media penyimpanan alternatif, seperti penggunaan bakteri sebagai perangkat penyimpanan yang aman oleh sebuah kelompok di Chinese University of Hong Kong. Dengan teknik yang diuji, mereka memperkirakan bahwa satu gram sel bakteri dapat menyimpan sekitar 900.000 gigabyte, setara dengan

kapasitas 450 hard drive berukuran 2 terabyte masing-masing. Untuk memberikan gambaran, ilmuwan memperkirakan kapasitas penyimpanan otak manusia berkisar antara satu terabyte dan satu petabyte.

4. Pemberitahuan dan Persetujuan

Dari mana semua bit ini berasal? Meskipun sebagian besar berasal dari sumber publik dan komersial seperti surat kabar, situs web, file audio digital, dan video, serta data yang ditransfer secara sengaja seperti pengajuan pajak atau laporan kepada pihak berwenang setelah kecelakaan, ada juga data yang dikumpulkan tanpa pemberitahuan. Perusahaan telekomunikasi, misalnya, mencatat detail setiap panggilan telepon termasuk tanggal, waktu, durasi, sumber, dan tujuan panggilan tersebut. Penyedia layanan internet juga melacak situs yang dikunjungi oleh pengguna, sementara beberapa situs menyimpan alamat IP setiap pengunjungnya, meskipun alamat IP tersebut umumnya tidak unik untuk setiap individu. Pengguna sering kali tidak menyadari pengumpulan data dari kategori ketiga ini, sehingga mereka tidak memberikan persetujuan secara eksplisit atas pengumpulan tersebut.

Ada berbagai cara di mana kita bisa diberi informasi tentang pengumpulan dan penggunaan data. Sebagai contoh, ketika kita mengunjungi sebuah situs web, kita mungkin diminta untuk menyetujui "syarat dan ketentuan penggunaan", yang menjelaskan apa yang akan dikumpulkan, alasan di balik pengumpulan itu, dan opsi yang tersedia jika kita memilih untuk tidak

memberikan data tersebut. Ketentuan penggunaan juga bisa memberitahu kita tentang tindakan yang dapat diambil jika terjadi kesalahan atau ketidaksesuaian dalam pengumpulan, penyimpanan, atau penggunaan data. Begitu juga, saat menggunakan aplikasi di perangkat seluler, kita mungkin diberitahu bahwa beberapa informasi, seperti lokasi atau daftar kontak, akan digunakan oleh aplikasi untuk berbagai keperluan.

Selain notifikasi, ada situasi di mana persetujuan juga diperlukan. Ini berarti Anda diminta dengan jelas untuk memberikan izin sebelum data Anda dikumpulkan dan digunakan. Sebagai contoh, aplikasi pemetaan mungkin meminta izin Anda untuk mengumpulkan lokasi secara otomatis; jika Anda menolak, Anda mungkin tidak bisa melanjutkan menggunakan aplikasi tersebut, atau harus memasukkan lokasi Anda setiap kali Anda ingin melihat peta atau mendapatkan petunjuk arah. Pemberitahuan dan persetujuan adalah prinsip yang sangat penting dalam menyediakan dan melindungi privasi. Namun, terkadang masalah terjadi dengan pemberitahuan dan persetujuan yang tidak sesuai dengan harapan. Studi kasus 5-1 menggambarkan sebuah insiden terbaru di mana toilet di sebuah pusat konvensi dianggap dapat mengumpulkan informasi untuk kepentingan publik. Meskipun akhirnya terbukti sebagai hoaks, kejadian tersebut mengingatkan kita bahwa data seringkali dikumpulkan tanpa izin dan bahkan tanpa pengetahuan kita.

G. Kajian Kebijakan Keamanan Sistem Informasi

Hasil kajian yang dilakukan oleh Rio Jumardi yang membahas mengenai penetapan kebijakan keamanan sistem informasi akan menjadi salah satu langkah untuk melindungi kerahasiaan data pribadi karyawan Perusahaan XYZ (Anon., n.d.).

Diantara beberapa kebijakan yang harus dibuat berdasarkan pada standar ISO 17799 : 27002 dan juga standar yang dikeluarkan oleh ID SIRTII meliputi EISP, ISSP dan SSP.

1. Kebijakan Tentang Perawatan Sistem Kebijakan perawatan sistem diperlukan untuk memaksimalkan perawatan terhadap sistem yang berjalan, Kebijakan perawatan sistem

   Perusahaan XYZ meliputi:

   a. Tujuan: memastikan bahwa sistem informasi yang diimplentasikan berjalan dengan baik.
   b. Standar : yang digunakan adalah standar dari ISO 17799 : 27002 dan Indeks KAMI sebagai alat evaluasi.
   c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi dan juga pihak ketiga yang menjadi vendor.
   d. Pedoman perawatan: perawatan sistem harus sesuai dengan pedoman yang berlaku.
   e. Prosedur : membuat prosedur- prosedur yang berkaitan dengan perawatan sistem yang meliputi

perawatan korektif, perawatan. adaptif, perawatan prefektif danperawatan preventif.

f. Monitoring: monitoring diperlukanuntuk memantau semua kegiatanyang berhubungan dengan perawatan sistem PerusahaanXYZ.

2. Kebijakan Penanganan Resiko Kebijakan penanganan resiko diperlukan untuk menangani resiko- resiko yang mungkin ada pada saat implemntasi sistem, Kebijakanpenanganan resiko Perusahaan XYZ meliputi:
   a. Tujuan: mengidentifikasi dan menganalisis kemungkinan resiko yang ada pada implementasi sistem informasi diperusahaan XYZ.
   b. Standar : yang digunakan adalah standar dari ISO 17799: 27002, ISO/IEC 27005, Metode Octave Allegro.
   c. Cakupan: penerapan kebijakan ini diperuntukkan kepada semua pegawai di lingkungan perusahaan XYZ yang berhubungan dengan asset informasi.
   d. Pedoman pengangan resiko: pengangan resiko terhadapsistem dan asset informasi yang berjalan harus sesuai dengan pedoman yang berlaku.
   e. Prosedur : membuat prosedur- prosedur yang berkaitan dengan manajemen resiko yang meliputi mengembangkan kriteria pengukuran resiko, mengembangkan profil asset informasi, mengidentifikasi container dari aset informasi, mengidentifikasi area masalah, mengidentifikasi scenario ancaman, mengidentifikasi resiko, menganalisis resiko, dan memilih pendekatan pemilihan pemilihan penangan risiko.

f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan penanganan resiko PerusahaanXYZ.

3. Kebijakan Sumber daya ManusiaPengaturan Hak Akses

Kebijakan sumber daya manusiadan pengaturan hak akses diperlukanuntuk mengatur batasan-batasandari pengguna sistem informasi di lingkungan Perusahaan XYZ. Kebijakan sumber daya manusia dan pengaturan hak akses perusahaan XYZ meliputi:

a. Tujuan: mengendalikan akses pengguna sistem informasi dengan mengatur hak akses pengguna. Tujuan lainnya sebagai upaya pengurangan resiko dari penyalahgunaan fungsi atau wewenang akibat kesalahan manusia.
b. Standar : yang digunakan adalah standar dari ISO 27002 dan Information Technology Infrastructur Library (ITIL) V3. 3) Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan untuk menentukan atau mengelola penentuan sumber daya manusia dengan pengaturan hak akses terhadap sistem.
c. Pedoman: penetuan pengaturan hak akses terhadap sistem harus sesuai dengan pedoman dan aturan yang berlaku dilingkungan Perusahaan XYZ. Disesuaian juga dengan kemampuan sistem informasi mengelola hak akses
d. Prosedur: membuat prosedur- prosedur yang berkaitan dengan pengaturan hak akses yang meliputi permintaan akses, pemberian akses, pemantauan identitas pengguna, penilaian kinerja

pegawai, perilaku kerja pegawai, pembatasan akses, penghapusan akses, permasalahan akses dan pencatatan akses.

e. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengelolaan sumber daya manusia dan pengaturan hak akses sistem infromasi di Perusahaan XYZ.

4. Kebijakan Keamanan dan Pengendalian Aset Informasi

Kebijakan keamanan dan pengendalian asset diperlukan untuk mengatur dan mengelola asset informasi perusahaan. Kebijakan keamanan dan pengendalian asset informasi perusahaan XYZ meliputi:

a. Tujuan: memberikan perlindungan terhadap asset perusahaan berdasarkan tingkat perlindungan yang diberikan.
b. Standar : yang digunakan adalah standar dari ISO 17799:27002.
c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan beserta seluruh pegawai terhadap keamanan asset informasi dalam penggunaan sistem informasi.
d. Pedoman: Pedoman keamanandan pengendalian asset informasi di lingkungan perusahaan XYZ harus disesuaian dengan aturan- aturan yang berlaku baik aturan dari sistem informasi maupun aturan dari perusahaan.
e. Prosedur: membuat prosedur- prosedur yang berkaitan dengan keamanan asset dan

pengendalian asset informasi meliputi klasifikasi informasi dan tanggung jawab informasi. 6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengendalian aset informasi sistem informasi di PerusahaanXYZ.

5. Kebijakan Keamanan Server

Kebijakan lain yang harus diperhatikan oleh perusahaan XYZ adalah kebijakan keamanan server. Kebijakan ini diperlukan untuk memaksimalkan keamanan terhadap server data yang secara langsung juga akan menjaga kerahasiaan data Perusahaan XYZ dan data privasi karyawan Perusahaan XYZ terhadap kejahatan komputer yang akan merugikan Perusahaan XYZ. Kebijakan Keamanan ServerPerusahaan XYZ meliputi:

a. Tujuan: memaksimalkan keamanan sistem informasi Perusahaan XYZ dari server yang digunakan.
b. Standar : yang digunakan adalah standar dari ISO 17799: 27002 dan Indeks KAMI untuk sebagai alat evaluasi.
c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi
d. Pedoman konfigurasi umum: Konfigurasi server harus sesuai dengan pedoman yang berlaku.
e. Prosedur: membuat prosedur- prosedur yang berkaitan dengan keamanan server melitputi: prosedur pembuatan server sendiri, prosedur

penyimpanan server, prosedur keamanan ruangan server, penjaga server, dan penggunaan sever.

f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan keamanan server Perusahaan XYZ.

BAB

5

Pengamanan Fisik Ruang Server dan Pusat Data

Ade Yuliana, S.T., M.T

A. Keamanan Informasi

Keamanan Informasi merupakan topik penting dalam lingkup Teknologi Informasi di Perusahaan. Organisasi menggunakan layanan komputasi dalam melakukan seluruh alur proses bisnis, sehingga keamanan ruang server sebagai lokasi penyimpanan pusat data mutlak diperlukan

untuk melindungi seluruh data penting yang tersimpan didalamnya.

Keamanan pusat data tidak hanya sekedar pertahanan terhadap berbagai faktor serangan kejahatan dunia maya namun juga harus melindungi segenap fisik aset perangkat keras agar pengoperasian pusat data tetap aman dan dapat diandalkan.

Keamanan pusat data merupakan upaya mengoperasikan keamanan siber sebagai sistem pusat informasi, dengan menempatkan sensor, perangkat keamanan dan personel. Merancang dan membangun pusat data dibutuhkan untuk mengembangkan Perusahaan, infrastruktur dan meningkatkan kapabilitas untuk melindungi Perusahaan agar lebih efektif, efisien dan aman (Nathans. D, 2015)

Langkah pertama dalam melindungi keamanan pusat data adalah dengan mengamankan ruang server agar sesuai dengan standar industri yang berlaku. Organisasi seperti *National Institute of Standards and Technology* (NIST) sebagai otoritas pengatur memberikan pedoman standar dan kerangka kerja yang mencangkup keamanan ruang server terdiri dari keamanan fisik, lingkungan dan informasi (Mughal A, 2022)

Berdasarkan penjelasan diatas dapat disimpulkan bahwa pengamanan fisik di ruang server dan pusat data merupakan aspek kritis dalam menjaga keamanan informasi dan sistem di Perusahaan agar dapat melindungi keamanan pusat data dan meminimalisir resiko terburuk yang bisa terjadi kapanpun.

B. Praktek terbaik ruang server

Menjaga keamanan fisik ruang server dan pusat data adalah proses berkelanjutan. Kerangka kerja keamanan memberikan pedoman untuk menjaga keamanan ruang server dalam konteks perubahan keadaan eksternal dan operasi TI (Fazlida. M, Said. J, 2015)

Beberapa standar dan pedoman kerangka kerja keamanan ruang serveradalah:

1. ISO 27001
2. ISO 20000-1
3. SSAE 18 SOC 1 Tipe II, SOC 2 Tipe II dan SOC 3
4. NISP SP (termasuk SP 800-14, SP 800-23, dan SP 800-53)
5. *Departement of Depense* (DoD), kerangka kerja teknis jaminan Informasi

C. Pengamanan Fisik Ruang Server dan Pusat Data

Pengamanan fisik ruang server dan pusat data merupakan upaya untuk melindungi ruang yang berisi sumber daya perangkat keras komputer, sistem penyimpanan data, dan infrastruktur layanan utilitas lainnya. Hal utama yang dilakukan adalah menyusun langkah-langkah dan strategi yang sesuai dengan sumber daya dengan tujuan untuk menjaga keamanan perangkat keras, data dan layanan yang disimpan didalamnya.

Setelah ruang server pusat data dirancang sesuai dengan standar yang berlaku, langkah selanjutnya melibatkan serangkaian pengendalian yang dapat

membantu mengurangi vektor ancaman mulai dari resiko manusia hingga ancaman bencana alam.

Berikut ini merupakan Langkah-langkah yang dapat dipertimbangkan dalam meningkatkan pengamanan fisik ruang server dan pusat data serta langkah pengendalian terkait pengamanan fisik ruang server dan pusat data

1. Akses terbatas
2. Monitoring dan Pemantauan visual
3. Sistem Alarm
4. Keamanan fisik bangunan
5. Keamanan Kelistrikan
6. Suhu dan Kelembaban
7. Proteksi terhadap kebakaran
8. Manajemen kabel yang rapih
9. Perubahan rutin dan audit keamanan
10. Pelatihan dan kesadaran keamanan

D. Akses Terbatas

Akses terbatas adalah langkah kunci dalam strategi pengamanan fisik server dan pusat data. Pengendalian dan pembatasan personel yang dapat mengakses ruangan. Mengontrol akses dengan memberlakukan langkah-langkah keamanan otentifikasi ganda seperti kartu akses dan sidik jari atau pengenalan wajah untuk memastikan hanya personel yang diijinkan yang dapat masuk. Berikut adalah beberapa praktik terkait dengan akses terbatas:

1. Kartu Akses, Kunci, atau Biometrik
2. Pengelolaan kunci
3. Sistem kontrol akses elektronik
4. Pintu tahan benda keras
5. Identifikasi ruangan
6. Pemeriksaan identitas
7. Sistem log akses
8. Sertifikasi dan audit kebijakan akses terbatas
9. Pengaturan waktu akses

Melalui implementasi praktik-praktik ini, organisasi dapat memastikan personel yang berwenang untuk memiliki akses ke ruang server dan pusat data, menjaga keamanan fisik dan mencegah akses yang tidak sah.

E. Monitoring dan Pemantauan Visual

Monitoring dan keamanan visual berperan dalam mendeteksi, mengidentifikasi, dan menanggapi potensi ancaman atau insiden keamanan. Integrasi teknologi canggih dan pemantauan yang berkelanjutan dapat meningkatkan kemampuan untuk menjaga keamanan fisik secara keseluruhan. Berikut adalah beberapa praktik terkait aspek ini:

1. Sistem Kamera Pengawas
2. Pemantauan real-time dan 24/7
3. Teknologi pencitraan
4. Penyimpanan dan pemulihan rekaman
5. Pemantauan Lingkungan
6. Integrasi dengan sistem keamanan lain
7. Peringatan audible dan visual
8. Kepatuhan dengan regulasi privasi

Monitoring dan keamanan visual yang efektif berguna untuk memantau aktivitas disekitar peralatan kritis dan memungkinkan respon cepat terhadap situasi darurat.

F. Sistem alarm

Sistem alarm adalah komponen pengamanan fisik untuk mendeteksi aktivitas mencurigakan atau insiden keamanan sehingga tindakan dapat diambil segera. Berikut adalah beberapa sensor keamanan yang dapat digunakan:

1. Sensor : gerak; pintu/jendela; getaran; asap/api; gas berbahaya; kelembaban dan suhu; air (*water leak*); radiasi elektromagnetik; keberadaan; Cahaya.
2. Sistem keamanan terintegrasi
3. Pemberitahuan langsung
4. Tindakan otomatis
5. Monitoring jarak jauh
6. Pemantauan dan log kejadian
7. Peringatan kehilangan koneksi

Dengan mengimplementasikan sistem alarm yang handal dan melakukan tindakan pencegahan yang sesuai diharapkan dapat meningkatkan dan mengurangi resiko terhadap ancaman yang merugikan.

G. Keamanan fisik bangunan

Keamanan fisik bangunan merupakan langkah yang sangat penting untuk melindungi ruang server dan pusat data dari ancaman yang mungkin datang dari luar. Berikut beberapa pertimbangan terkait hal ini:

1. Desain Bangunan yang aman
2. Dinding kokoh

3. Pintu jendela tahan benda keras
4. Sistem kontrol akses
5. Pencahayaan yang baik
6. Kunci fisik dan elektronik
7. Kunci perangkat keras
8. Kunci kabel yang penting
9. Penghalang fisik tambahan

Melalui penggunaan pintu dan jendela tahan benda keras serta langkah perlindungan tambahan dapat meningkatkan keamanan fisik ruang server dan pusat data secara signifikan.

H. Keamanan Kelistrikan

Sumber daya Listrik Cadangan dibutuhkan untuk melindungi server dan pusat data dari pemadaman Listrik yang tidak terduga. Berikut ini beberapa pertimbangan terkait dengan hal ini:

1. Sumber daya Listrik Cadangan
2. Generator darurat
3. Kapasitas daya yang cukup
4. Transfer otomatis
5. Monitoring kelistrikan
6. Perangkat Pemutus Listrik (PDU)
7. Pemisahan sirkuit
8. Konservasi energi
9. Ruang dan Pendinginan
10. Pembaharuan perangkat kelistrikan

Dengan memperhatikan keamanan kelistrikan, dapat menjaga keandalan operasional ruang server, serta

melindungi data yang disimpan dari resiko kegagalan daya Listrik.

I. Suhu dan kelembaban

Pemantauan suhu dan kelembaban adalah hal krusial dalam menjaga keamanan fisik server dan pusat data. Fluktuasi yang signifikan dalam suhu dan kelembaban dapat merusak perangkat keras dan menyebabkan kegagalan sistem. Berikut adalah beberapa pertimbangan terkait dengan hal ini:

1. Sistem pemantauan otomatis
2. Pengaturan suhu yang optimal
3. Kelembaban yang dikonrol
4. Sensor pemantauan kelembaban tanah atau air
5. Sistem pemantauan peringatan dini
6. Pemantauan Remote
7. Integrasi dengan sistem manajemen keselamatan
8. Back up pendingin
9. Pemantauan energi dan efisiensi
10. Pemantauan langsung pada perangat kritis

Dengan memantau dan menjaga suhu dan kelembaban dapat mencegah kerusakan perangkat keras akibat kondisi lingkungan yang tidak sesuai.

J. Proteksi Terhadap kebakaran

Proteksi terhadap kebakaran perlu dilakukan untuk menjaga keamanan fisik server dan pusat data. Kebakaran dapat merusak perangkat keras, data dan menyebabkan

kerugian besar. Berikut adalah beberapa pertimbangan terkait hal ini:

1. Deteksi kebakaran
2. Pemadam kebakaran otomatis
3. Pemadam kebakaran manual
4. Evaluasi dan rute darurat
5. Pengendalian asap
6. Lokasi peralata penting
7. Ujicoba sistem
8. Pencegahan kebakaran
9. Monitoring lingkungan
10. Sertifikasi kebakaran dan kepatuhan

Dengan mengimplementasikan laangkah proteksi terhadap kebakaran, minimal dapat mengurangi resiko kehilagan perangkat keras dan data akibat kebakaran, dan memastikan keamanan fisik server dan pusat data secara keseluruhan.

K. Manajemen kabel yang rapi

Manajemen kabel yang baik tidak hanya memudahkan pemeliharaan dan peningkatan, tetapi juga dapat mengurangi resiko gangguan dan meminimalkan potensi kegagalan perangkat keras. Berikut adalah beberapa pertimbangan terkait hal ini:

1. Labeling yang jelas
2. Penyusunan kabel yang tertata
3. Pemisahan kabel
4. Penggunaan kabel yang sesuai
5. Manajemen kabel vertikal dan horizontal

6. Konsolidasi dan pemisahan
7. Area akses yang jelas
8. Pengelolaan kabel di rak server
9. Dokumentasi kabel

L. Pembaharuan rutin dan Audit Keamanan

Pembaharuan rutin dan audit keamanan mutlak diperlukan dalam menjaga dan meningkatkan keamanan fisik server dan pusat data. Pembaharuan terhadap elemen krusial seperti sistem akses, kelistrikan, fisik bangunan sensor, dan sebagainya untuk memastikan keamanan tetap efektif dan dapat mendeteksi potensi resiko dan kelemahan perangkat yang digunakan. Berikut adalah beberapa pertimbangan terkait hal ini:

1. Pembaharuan kebijakan keamanan
2. Audit keamanan berkala
3. Pemeriksaan sistem keamanan
4. Uji coba sistem pemadam kebakaran
5. Audit sistem akses dan kontrol
6. Penilaian fisik perangkat dan bangunan
7. Pengujian keandalan generator dan UPS
8. Pelatihan keamanan
9. Pemantauan dan notifikasi
10. Evaluasi kegiatan pengguna
11. Revisi dan peningkatan

Dengan menjalankan pembaharuan dan audit keamanan diharapkan dapat menjaga, meningkatkan dan memastikan sistem keamanan tetap efektif dan sesuai dengan standar keamanan yang relevan.

M. Pelatihan dan kesadaran keamanan

Pelatihan personel dan meningkatkan kesadaran di lingkungan karyawan merupakan langkah penting untuk membentuk budaya keamanan yang kuat di organisasai dan mengurangi resiko keamanan fisik server dan pusat data. Berikut adalah beberapa pertimbangan terkait hal ini:

1. Program pelatihan regular
2. Pendidikan kesadaran keamanan
3. Latihan simulasi evakuasi
4. Pengembangan modul e-learning
5. Pelatihan khusus untuk personel keamanan
6. Uji penetrasi testing
7. Kampanye kesadaran keamanan
8. Pengakuan dan insentif
9. Pengujian kesadaran sosial
10. Edukasi tentang peraturan dan kepatuhan
11. Umpan balik dan evaluasi
12. Pembahasan kasus

Dengan melakukan pelatihan dan kesadaran keamanan, organisasi dapat meningkatkan kemampuan personel terhadap praktik keamanan fisik dan mengurangi resiko fisik server dan pusat data.

N. Mengamankan ruang server adalah Hal yang penting

Mengamankan ruang server dan pusat data adalah kebutahan mutlak dalam menjaga tata Kelola Perusahaan. Hal ini bukanlah upaya yang murah karena harus menjaga keseimbangan khusus antara keamanan, aksesabilitas,

biaya, pemeliharaan, peningkatan performa dan lain-lain seperti Langkah-langkah penjagaan keamanan fisik yang telah dijelaskan diatas.

Pimpinan mungkin ragu-ragu diawal untuk berinvestasi dalam keamanan fisik ruang server dan pusat data ini, namun melindungi data vital adalah kunci keberlangsungan proses bisnis Perusahaan. Mencegah lebih baik daripada kehilangan seluruh asset data yang bisa berimbas terhadap keseluruhan layanan bisnis Perusahaan.

BAB

6

Keamanan Jaringan

Juwari, S.Kom., M.Kom

A. Keamanan Jaringan

Keamanan jaringan merupakan serangkaian kebijakan dan praktik yang diterapkan untuk mencegah dan memantau akses tidak sah, modifikasi, atau penolakan jaringan komputer dan sumber daya yang dapat diakses oleh jaringan. Keamanan jaringan merupakan berkaitan tentang mengaktifkan akses ke data di jaringan, yang dikendalikan oleh administrator jaringan. Pengguna

memilih atau diberikan nama pengguna dan kata sandi atau informasi otentifikasi lainnya yang memungkinkan (Anita Sindar Sinaga 2020).

Keamanan jaringan mencakup berbagai jenis seperti keamanan fisik, keamanan akses, keamanan perangkat keras, keamanan perangkat lunak, dan keamanan data. Keamanan jaringan mencakup berbagai tindakan untuk mencegah akses tidak sah ke dalam suatu jaringan, memblokir lalu lintas jaringan yang mencurigakan dan melindungi jaringan dari serangan siber. Hal Ini termasuk penggunaan firewall, VPN, dan teknologi keamanan jaringan lainnya yang relevan (Deris Stiawan 2005; Miftahul Huda 2020).

Berikut adalah beberapa jenis keamanan jaringan yang paling umum digunakan untuk melindungi jaringan komputer dari ancaman dan serangan yang merusak, seperti serangan cyber, pencurian identitas, dan pelanggaran data:

1. Keamanan fisik: Mencakup hal-hal seperti penggunaan sensor gerak dan kamera pengawas, pengamanan ruang server, dan penempatan perangkat jaringan di lokasi yang aman dan terkendali untuk mencegah akses fisik yang tidak sah ke perangkat jaringan.
2. Keamanan akses: mencakup hal-hal seperti memasang perangkat lunak antivirus dan antispyware, melakukan pembaruan rutin perangkat lunak, dan menetapkan kebijakan penggunaan perangkat lunak yang aman untuk melindungi perangkat lunak jaringan dari serangan seperti malware, virus, atau peretasan data.

3. Keamanan jaringan: termasuk menghentikan orang yang tidak diinginkan mengakses jaringan, memblokir lalu lintas jaringan, dan melindungi data yang disimpan dalam jaringan.
4. Keamanan Website: Termasuk SSL untuk enkripsi data dan kontrol akses.
5. Keamanan Email: Melindungi dari ancaman melalui email.
6. Keamanan Nirkabel: Melindungi jaringan nirkabel dari akses yang tidak sah.
7. Keamanan Aplikasi: Melindungi aplikasi yang digunakan oleh perusahaan.
8. Keamanan Ujung (Endpoint Security): Melindungi perangkat akhir seperti komputer dan ponsel.
9. Keamanan Cloud: Sistem keamanan tambahan untuk layanan cloud.

Perkembangan Teknologi keamanan jaringan mengalami kemajuan yang sangat signifikan dan cepat. Berikut beberapa teknologi keamanan jaringan yang umum digunakan(Deris Stiawan 2005; Miftahul Huda 2020):

1. Firewall: Firewall berfungsi untuk melindungi jaringan komputer dari trafik yang membahayakan.
2. Antivirus dan antimalware: Software yang dikenal sebagai antivirus dan antimalware dimaksudkan untuk mendeteksi, menghapus, dan mencegah ancaman seperti virus dan malware dari menginfeksi komputer dan jaringan secara online.
3. Web Security: Memasang SSL (Secure Socket Layer) adalah metode umum untuk melindungi web. Ini melindungi data pengguna yang mengakses situs web.

Pada era 5.0, masalah keamanan jaringan disebabkan oleh serangan siber yang semakin canggih dan berkembang pesat. Beberapa masalah keamanan jaringan antara lain:

1. Peningkatan jumlah pengguna internet: Meskipun ada ancaman yang meningkat, jumlah pengguna internet di seluruh dunia terus meningkat.
2. Peningkatan jumlah serangan: beberapa orang percaya bahwa serangan siber tidak akan berhenti.
3. Peningkatan kompleksitas sistem: Meskipun teknologi memberikan kenyamanan, ia juga memiliki kelemahan yang signifikan. Semakin canggih teknologi, semakin sulit untuk mencegah serangan.

Untuk mengatasi masalah keamanan jaringan, sistem keamanan jaringan harus ditingkatkan, teknologi keamanan jaringan harus dikembangkan, dan kebijakan keamanan jaringan harus dibuat.

B. Perbedaan firewall, antivirus, dan antimalware

Firewall:

1. Berfungsi sebagai pertahanan pertama jaringan dan memantau dan mengontrol lalu lintas data yang masuk dan keluar.
2. Melindungi jaringan dari akses yang tidak sah dan serangan eksternal, seperti firewall Windows dan firewall pada alat router.

Antivirus:

Adalah program yang mendeteksi, menghalau, dan menghapus virus dari perangkat. Program seperti Smadav

dan Bitdefender melindungi perangkat dari serangan virus secara internal.

Antimalware:

1. Melindungi perangkat dari berbagai jenis malware, seperti virus, worm, Trojan, dan lainnya.
2. Saling melengkapi dengan antivirus untuk perlindungan lapis ganda.
3. Tidak mencoba menggantikan antivirus, melainkan saling melengkapi untuk perlindungan yang lebih baik.

Oleh karena itu, firewall menangani kontrol lalu lintas data, sedangkan antivirus dan antimalware berkonsentrasi pada deteksi dan penghapusan ancaman berbahaya dari perangkat.

C. Cara kerja Antimalware

Software antimalware melindungi perangkat dan sistem dari serangan malware, yang merupakan program atau file yang dirancang untuk mengganggu, mencuri, atau mengancam sistem komputer (Virgiawan A. Manoppo et al. 2020). Berikut adalah bagaimana itu berfungsi:

1. Pemindaian (Scanning): Anti-malware memindai semua program dan file di perangkat untuk mencari tanda-tanda malware.
2. Pemantauan Perilaku: Anti-malware mengawasi aktivitas yang mencurigakan atau tidak biasa, seperti mencoba mengakses file yang tidak biasa, mencoba mengubah pengaturan sistem, atau berkomunikasi dengan alamat IP yang mencurigakan.

3. Definisi Malware: Anti-malware menggunakan definisi malware terbaru, membuatnya mudah dipahami oleh perangkat.
4. Isolasi atau Penghapusan: Anti-malware mengisolasi atau menghapus malware.

Antimalware melindungi perangkat dan sistem dari serangan malware dengan berbagai cara, seperti virus, worm, Trojan, spyware, dan lainnya. Selain itu, antimalware membantu menjaga integritas jaringan komputer dan melindungi data.

D. Teknik antimalware untuk melindungi perangkat

1. Pemindaian (Scanning): Antimalware mencari tanda-tanda malware pada semua file dan program di perangkat. 2. Pemantauan Perilaku: Antimalware mengawasi tindakan yang mencurigakan atau tidak biasa, seperti mencoba mengakses file yang tidak biasa, mencoba mengubah pengaturan sistem, atau berkomunikasi dengan alamat IP yang mencurigakan.
2. Definisi Malware: Antimalware menggunakan definisi malware terbaru agar malware mudah dipahami oleh perangkat.
3. Isolasi atau Penghapusan: Antimalware akan mengisolasi atau menghapus malware jika terdeteksi.

Antimalware mendeteksi, menghapus, dan mencegah serangan malware seperti virus, worm, trojan, spyware, adware, dan ransomware dengan menggunakan berbagai teknik ini (Indana Zulfa et al. 2023).

E. Teknik antivirus untuk melindungi perangkat

Antivirus melindungi perangkat dengan berbagai cara, seperti:

1. Pemindaian (Scanning): Antivirus memindai semua berkas yang diubah atau disimpan, serta virus yang dibuat di bagian belakang program.
2. Pendeteksian Berbasis Perilaku (Behavior-Based Detection): Antivirus menggunakan metode baru untuk mengidentifikasi cara virus bekerja dengan melihat perilaku program di lingkungan virtual.
3. Penggunaan Tembok Api (Firewall): Beberapa antivirus memiliki fitur anti-spyware, anti-phishing, dan anti-spam untuk melindungi komputer dari serangan peretas.
4. Penggunaan Anti-Spyware dan Anti-Phishing/Spam: Beberapa antivirus juga memiliki fitur ini untuk melindungi komputer dari ancaman malware canggih seperti Zero-Day.

Antivirus menggunakan metode-metode ini untuk mencegah, mendeteksi, dan menghapus perangkat perusak serta memberikan perlindungan lapis ganda untuk melawan

F. Jenis serangan jaringan computer

Beberapa jenis serangan jaringan komputer yang sering terjadi diantaranya:

1. Phishing
2. Virus
3. Worm

4. Trojan Horse
5. Eavesdropping
6. Logic Bomb
7. Spoofing
8. Denial-of-Service (DoS)
9. Distributed Denial-of-Service (DDoS)
10. SQL Injection
11. Cross-Site Scripting (XSS)
12. Cross-Site Request Forgery (CSRF)
13. Crypto Mining
14. Social Engineering
15. Kebocoran Data
16. Hacking
17. Clickjacking
18. Botnet
19. Ransomware

G. Serangan DDoS

Serangan Distributed Denial-of-Service (DDoS) adalah serangan yang dilakukan dengan membanjiri lalu lintas jaringan internet pada server, sistem, atau jaringan dengan tujuan mengganggu layanan jaringan dan menghabiskan sumber daya aplikasi (Purba and Efendi 2020). Serangan ini dapat membuat situs web atau server tidak dapat diakses oleh pengguna karena banjir lalu lintas yang tidak biasa, membuat situs web tidak berfungsi dengan baik, atau membuatnya offline sama sekali.

Beberapa cara untuk menghindari serangan DDoS adalah:

1. Bangun redundansi ke dalam infrastruktur Anda: Bangun infrastruktur cadangan untuk menangani lonjakan lalu lintas.
2. Konfigurasi perangkat keras jaringan Anda: Konfigurasi perangkat keras jaringan Anda sehingga dapat mendeteksi dan menanggapi serangan DDoS.
3. Gunakan layanan perlindungan DDoS: Gunakan layanan perlindungan DDoS yang ditawarkan oleh penyedia hosting dan cloud.
4. Batasi akses IP: Membatasi akses IP yang dapat mengakses server atau jaringan. 5. Gunakan CDN: Menggunakan CDN untuk membagi lalu lintas web secara merata dan mengurangi beban pada server utama.

Menjaga sistem tetap aman dan siap untuk serangan DDoS sangat penting karena serangan ini dapat menyebabkan kerugian besar dalam uang dan reputasi. Beberapa jenis serangan DDoS adalah sebagai berikut:

1. Serangan Volumetrik: Ini memanfaatkan batas bandwidth pemilik website dengan membuat kemacetan. Ini membuat bandwidth kewalahan karena semua trafik yang masuk, menyebabkan server lumpuh.
2. Serangan Protokol: Ini menggunakan protokol yang tidak biasa untuk membanjiri situs web dan sumber daya server, membuat server tidak dapat mengontrol semua trafik dan menyebabkan downtime server atau sistem.
3. Serangan Layer Aplikasi: Ini menargetkan aplikasi web atau layanan dengan membanjiri server dengan banyak

permintaan yang tidak perlu, seperti permintaan HTTP atau HTTPS yang berlebihan.

H. Serangan volumetrik

Serangan volumetrik adalah jenis serangan DDoS yang menciptakan kemacetan dengan mengirimkan lalu lintas yang tampaknya sah. Amplifikasi DNS (Domain Name Server) adalah salah satu contohnya. Cara kerjanya adalah dengan memanfaatkan batas bandwidth pemilik website dengan menciptakan kemacetan (Goutama et al. 2022). Dengan demikian, bandwidth akan kewalahan dengan semua trafik yang masuk, menyebabkan server lumpuh.

Serangan volumetrik memberikan dampak pada jaringan dan system:

1. Pengurangan Kinerja: Serangan volumetrik dapat mengurangi kinerja sistem dan jaringan, membuat sistem tidak efisien.
2. Pengurangan Kesetaraan: Serangan volumetrik dapat merusak kesetaraan jaringan, membuat pengguna tidak dapat mengakses layanan yang diperlukan.
3. Pengurangan Kesetaraan Sumber Daya: Serangan volumetrik dapat mengganggu kesetaraan sumber daya, membuat sistem tidak efisien.
4. Pengurangan Kesetaraan Bandwidth: Serangan volumetrik dapat mengurangi kesetaraan bandwidth, membuat sistem tidak efisien.
5. Pengurangan Kesetaraan Koneksi: Serangan volumetrik dapat merusak kesetaraan koneksi, membuat pengguna tidak dapat mengakses layanan yang diperlukan.

6. Pengurangan Kesetaraan Aplikasi: Serangan volumetrik dapat mengurangi kesetaraan aplikasi, menyebabkan sistem tidak dapat beroperasi dengan efisiensi yang tinggi.

Serangan volumetrik pada jaringan dan sistem dapat membuat sistem tidak berfungsi dengan baik dan membuat pengguna tidak dapat mengakses layanan yang mereka butuhkan, yang dapat menyebabkan kerugian uang dan reputasi yang besar. Selain itu serangan volumetrik pada jaringan dan sistem dapat menghambat layanan dengan membanjiri server, sistem, atau jaringan dengan lalu lintas internet, sehingga menghabiskan sumber daya aplikasi dan membuat sistem tidak dapat bekerja dengan efisiensi yang tinggi.

Serangan ini juga dapat membuat situs web atau server tidak dapat diakses oleh pengguna karena banjir lalu lintas yang tidak biasa, membuat situs web tidak dapat berfungsi dengan baik, atau membuatnya offline sama sekali. Oleh karena itu, sangat penting untuk menjaga sistem tetap aman dan siap untuk serangan DDoS karena serangan ini dapat menyebabkan kerugian secara meteri.

Mendeteksi serangan volumetrik dapat menggunakan metode berikut:

1. Memonitor Lalu Lintas Jaringan: Ini melacak lalu lintas di seluruh jaringan untuk menemukan lonjakan lalu lintas yang tidak biasa.
2. Menggunakan Perangkat Lunak Pendeteksi: Anda dapat menemukan serangan DDoS dengan menggunakan perangkat lunak pendeteksi DDoS.

3. Menggunakan Sistem SIEM: Mendeteksi serangan DDoS dapat dilakukan dengan menggunakan sistem manajemen informasi keamanan dan peristiwa atau SIEM.
4. Menggunakan Layanan Proteksi DDoS: Menggunakan layanan proteksi DDoS yang diberikan oleh penyedia hosting dan cloud untuk mendeteksi dan mencegah serangan DDoS.

Untuk mengetahui kekuatan serangan volumetrik pada sistem dan jaringan, beberapa parameter penting dapat dipantau, seperti:

1. Bandwidth Utilization: Memeriksa penggunaan bandwidth untuk menemukan lonjakan lalu lintas yang tidak biasa.
2. Paket Per Second (PPS): Mencatat berapa banyak paket per detik yang diterima server atau jaringan.
3. Jumlah Koneksi: Mencatat berapa banyak koneksi yang terhubung ke server atau jaringan.
4. Latency: Mencatat lama server menanggapi permintaan.
5. Utilisasi Sumber Daya: Mengawasi penggunaan CPU, memori, dan sumber daya jaringan lainnya.

Dengan memantau parameter ini, dapat mendeteksi dan mengukur kekuatan serangan volumetrik pada sistem dan jaringan, sehingga tindakan mitigasi yang tepat dapat diambil segera. Banyak cara untuk mengukur kekuatan serangan DDoS volumetrik pada jaringan dan sistem, tetapi penting untuk diingat bahwa beberapa alat tersebut ilegal dan tidak etis. Sebagai akibatnya, disarankan untuk

menggunakan perilaku digital yang etis dan berkonsentrasi pada pertahanan digital etis.

Beberapa metode untuk mengukur kekuatan serangan DDoS volumetrik termasuk melacak penggunaan sumber daya, latensi, bandwidth, dan paket per detik (PPS). Selain itu, botnet, stressers, booters, dan serangan amplifikasi adalah beberapa alat yang digunakan untuk melakukan serangan DDoS. Namun, penting untuk diingat bahwa menggunakan alat-alat ini tidak hanya ilegal, tetapi juga tidak moral.

I. Botnet

Botnet adalah sekumpulan program yang diprogram dengan malware dan terhubung ke jaringan internet yang dikendalikan oleh individu tertentu. Botnet juga disebut sebagai zombie computer karena mereka menginfeksi sebanyak mungkin perangkat untuk menambah jaringan. Serangan DDoS, peretasan data, perambahan email, dan penyebaran malware adalah beberapa kegiatan yang melanggar hukum di internet yang dapat digunakan oleh bots. Dalam kebanyakan kasus, bots terdiri dari ribuan hingga jutaan komputer yang sangat rentan terhadap serangan peretas. Perangkat lunak command and control (C&C), yang memungkinkan pengendalian botnet, memungkinkan penyerang untuk mengatur tindakan botnet dan mengarahkan sumber daya ke target (Nam H Nguyen 2018).

Botnet biasanya bekerja dalam tiga tahap: persiapan, infeksi, dan aktivasi. Pada tahap persiapan, botmaster akan mencari dan mempelajari bug pada website, aplikasi, atau

bahkan perilaku manusia. Pada tahap infeksi, botmaster akan menginfeksi sebanyak mungkin perangkat yang terhubung, untuk memastikan bahwa ada cukup bot untuk melakukan serangan. Pada tahap aktivasi, botmaster akan mengirimkan perintah kepada semua perangkat dalam botnet untuk melakukan apa yang mereka inginkan (Catur Nugroho 2020).

Botnet dapat melakukan banyak jenis serangan, seperti:

1. Serangan DDoS (Denial of Service) yang didistribusikan: Botnet dapat digunakan untuk melakukan serangan DDoS, yang menghentikan jaringan atau sistem komputer dengan mengirimkan banyak permintaan kepada sistem.
2. Serangan Brute Force: Botnet dapat digunakan untuk melakukan serangan brute force, yang mencoba berbagai kombinasi kata sandi untuk mendapatkan akses ke akun.
3. Phishing: Serangan phishing dapat dilakukan dengan menggunakan botnet, yang menggunakan email atau pesan yang mengandung link atau file yang terinfeksi malware.
4. Pencurian data: Botnet dapat digunakan untuk mencuri data seperti kata sandi, nomor kartu kredit, dan informasi bisnis.
5. Penyebaran malware: Botnet dapat digunakan untuk menyebarkan malware ke perangkat yang terinfeksi, seperti virus, ransomware, atau trojan.

BAB

7

Konfigurasi Keamanan Sistem Operasi

Tati Ernawati, M.T.

A. Sistem Operasi

Sebelum membahas konfigurasi keamanan sistem operasi akan kita bahas tentang konsep dan tujuan dari sistem operasi. Apakah sistem operasi itu? Perangkat lunak yang memiliki fungsi untuk menghubungkan perangkat keras dan pengguna komputer disebut sistem operasi.

Sumber daya seperti CPU, memori, perangkat I/O, dan sistem penyimpanan dialokasikan dan digunakan oleh sistem operasi. Sistem operasi memainkan peran penting dalam mengelola dan mengendalikan sumber daya komputer, menjamin bahwa aplikasi berjalan dengan baik, dan melindungi dan menjaga keamanan sistem (Heryana et al. 2023). Terdapat tiga tujuan utama sistem operasi, yaitu (Watrianthos & Purnama 2018):

1. Kenyamanan, artinya membuat penggunaan komputer lebih mudah.
2. Efisiensi, yang berarti penggunaan sumber daya sistem komputer secara efektif.
3. Mampu berevolusi: hal ini memungkinkan pengembangan, pengujian, dan penggunaan sistem yang baru saat membangun sistem operasi.

B. Keamanan Sistem Operasi

Keamanan sistem operasi mencakup aturan, prosedur, dan kontrol yang mengatur siapa yang dapat mengakses sistem operasi, sumber daya (seperti *file*, program, dan *printer*), dan tindakan yang dapat dilakukan pengguna (Hall 2007). Sistem operasi memainkan peran penting dalam komunikasi data, mengontrol penggunaan memori, pemrosesan, dan penyimpanan dalam sistem berbagi waktu (*time sharing*), memastikan keamanan dengan meminta hak akses sistem untuk informasi pengguna dan autentikasi (Sinaga 2020). Jenis serangan terhadap sistem operasi (Chandra 2005):

1. *Vulnerabilitas*
    a. Memungkinkan penyerang menjalankan perintah seperti orang lain.
    b. Meskipun ada batasan pada data, memungkinkan penyerang mengakses berbagai jenis data.
    c. Memungkinkan penyerang berpura-pura sebagai orang lain
    d. Membiarkan penyerang melakukan *denial of service*
2. Exposure
    a. Memungkinkan penyerang mengambil informasi
    b. Memungkinkan penyerang menyembunyikan tindakan
    c. Menggabungkan kemampuan yang terlihat seperti yang diinginkan tetapi mudah menerima persetujuan
    d. Penyerang dapat mencoba mendapatkan akses ke sistem atau data.
    e. Dianggap memiliki hubungan dengan kebijakan keamanan tertentu.

C. Kebijakan Keamanan (*Security Policy*)

Terdapat elemen keamanan yang harus diperhatikan oleh administrator (Chandra 2005):

1. *Availability*; data penting harus selalu tersedia, sehingga sistem dapat digunakan saat pengguna memerlukannya.
2. *Utility*; untuk tujuan tertentu, sistem dan datanya harus berguna.
3. Integrity; data/sistem harus lengkap dan dapat dibaca

4. *Authenticity*; identitas pengguna dan sistem harus
5. dapat di verifikasi.
6. *Confidentially*; hanya individu yang dipilih untuk berbagi data atau orang yang memiliki data dapat mengetahuinya.
7. *Possession*; kehilangan kontrol sistem ke tangan orang yang tidak berhak akan membahayakan pengguna lainnya, pemilik sistem harus mengendalikannya.

D. Konfigurasi Keamanan Sistem Operasi

Sub bab ini membahas tentang konfigurasi keamanan untuk sistem operasi microsoft windows dan linux untuk *client*. Apa saja bagian yang perlu diamankan? Bentuk pengamanan secara terinci pada Tabel 1 (Gunawan, 2021).

Tabel 1. Bentuk Pengamanan pada Sistem Operasi

No	Bentuk Pengamanan	Langkah Pengamanan	
		Windows	Linux
1.	Akun	Aktifkan akun administrator dengan kata sandi yang kuat. Hanya untuk keperluan administrasi akun administrator digunakan.	Aktifkan akun *root* dengan kata sandi yang kuat. Hanya untuk keperluan administrasi akun root digunakan.
2.	Ancaman *Malware*	Aktivitasi/instal antivirus	Aktivitasi/instal antivirus dari pihak ketiga

No	Bentuk Pengamanan	Langkah Pengamanan	
		Windows	Linux
3.	Aplikasi	Pastikan aplikasi berasal dari vendor yang dapat diandalkan.	Pastikan aplikasi berasal dari vendor yang dapat diandalkan. Tidak menggunakan *repository* dari luar melainkan gunakan *repository* bawaan
4.	Data	Penggunaan aplikasi enkripsi baik tingkat data maupun *drive*	Penggunaan aplikasi enkripsi baik tingkat data/ direktori maupun *drive*
5.	*File System*	Pakai file sistem NTFS bukan FAT32	Pakai *file sistem* EXTA
6.	*Remote*	*Disable fitur remote*, jika *enable* gunakan enkripsi untuk komunikasi	*Disable fitur remote*, jika *enable* gunakan enkripsi untuk komunikasi dari dan keluar melalui Secure Shell (SSH)
7.	Registry	*Protect registry* dari *user* non administrator	-

No	Bentuk Pengamanan	Langkah Pengamanan	
		Windows	Linux
8.	*Windows resource protection*	*Enable* fitur *Windows resource protection*	-
9.	Akses direktori dan file	-	Gunakan hak akses dengan bijak
10.	Arus masuk dan keluar jaringan	Aktivitasi *firewall*	
11.	BIOS Access	Gunakan kata kunci jika akses BIOS	
12.	*Browser*	Gunakan versi terbaru, instal aplikasi tambahan untuk deteksi iklan/web berbahaya	
13.	Pendeteksi lokasi	Install aplikasi tambahan mendeteksi lokasi	
14.	*Services*	*Disable service* yang tidak perlu	
15.	Sistem *Backup*	*Enable backup system* dan *restore*, simpan *file backup* di tempat secara terpisah	
16.	*Spy Application*	Instal aplikasi tambahan melacak *spy*	
17.	USB Access	*Disable* port USB	
18.	Versi OS	*Update* secara berkala	

E. Konfigurasi Keamanan pada Microsoft Windows

Konfigurasi keamanan difokuskan pada Windows 10. Cara konfigurasi adalah sebagai berikut (Gunawan 2021):

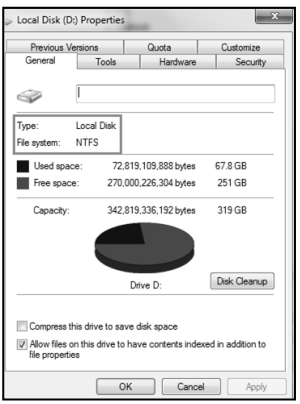
1. Akun
    a. Klik tombol 'Windows, klik 'Setiing-Account-Sign-InOption'. Pilih menu 'Password', klik 'add', masukkan password dengan minimal delapan karakter kombinasi angka dan huruf besar dan kecil.
    b. 'Show Account Detail' harus 'off' pada menu 'Privacy'
    c. Buat akun baru (non administrator), klik menu Family & Other Users'->'Someone Else to this PC'->'I don't have This Person's Sign-In Information'->'Add a User Without a Microsoft Account'-> 'User Name'->'Next'. Pilih akun baru tersebut, klik tombol 'Change Account Type', pilih' Standar User', klik 'OK'
2. Ancaman Malware
    a. Aktivasi 'Windows Defender', tahapannya adalah klik 'Windows'->'Settings'->'Update & Security' -> 'Windows
    b. Security' ->'Virus & Threat Protection'
    c. Bagian 'Virus & Threat Protection Settings' pilih menu 'Turn On'. Klik menu 'Manage Ransomware Protection Dismiss'-> 'On' pada 'Controlled Folder Access'
    d. Pilih atau tambahkan folder klik '+ Add a Protected Folder'

e. Klik ‘Allow An App Through Controlled Folder Access’ jika suatu aplikasi diperbolehkan akses ke *folder* tadi.
f. Klik ‘Add an Allow App’, pilih applikasi yang diinginkan.

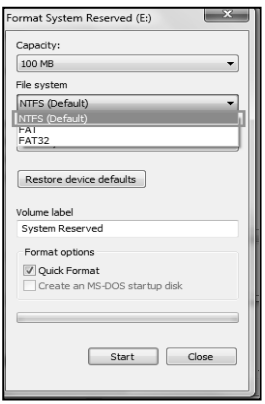
3. Aplikasi

Pastikan aplikasi tambahan yang diinstal aman, unduh aplikasi di Microsoft *store* dengan klik tombol ‘Start’ dan pilih ‘Microsoft Store’.

4. *File System*
   a. Gunakan NTFS untuk file sistem dengan cara pilih *drive*, klik kanan pilih ‘Properties’
   b. Pastikan pada ‘File System’ adalah ‘NTFS’
   c. Rubah ke ‘NTFS’ jika masih tertulis ‘FAT32’ *backu*p seluruh data ke *drive* melalui format ulang tersebut ke *drive* lain. Selanjutnya klik kanan ‘Drive’-> pilih format NTFS-> ‘Start’.



Gambar 1 Kotak Dialog Drive Properties

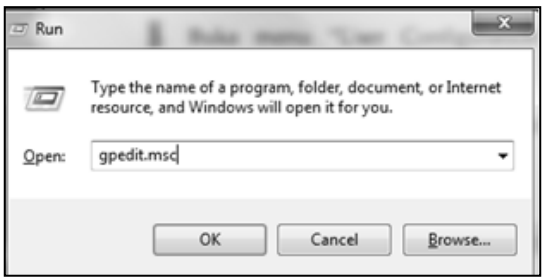


Gambar 2 Format Drive

5. Registry

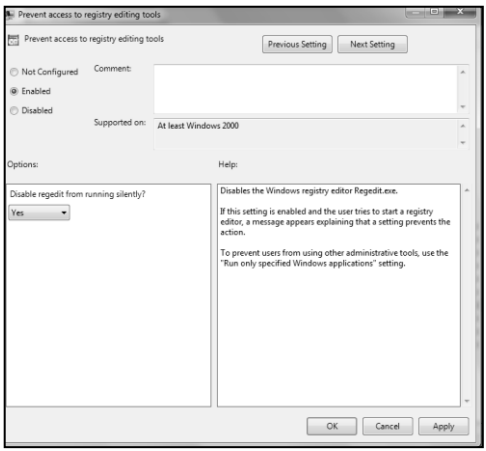
Registry adalah pusat konfigurasi Windows, untuk mencegah akses yang tidak sah lakukan hal-hal berikut:

a. Klik tombol 'Windows' + 'R' secara bersama-sama
b. Ketikan gpedit.msc, pada kotak dialog (Gambar 4).

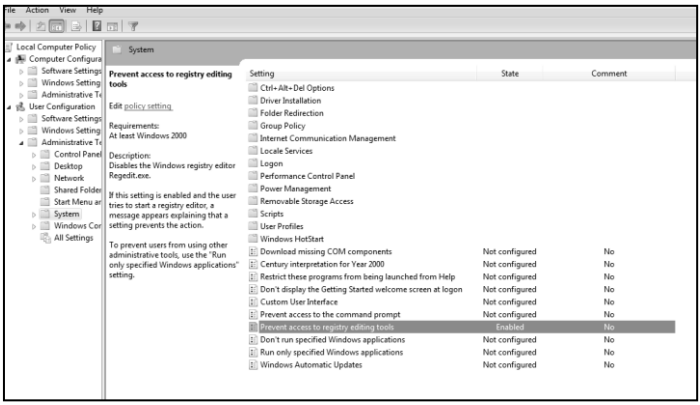


Gambar 3. Kotak Dialog Run

c. Menu 'User Configuration-> 'Administrative Template' ->'System'
d. *Double* klik pada 'Prevent Access to Registry Editing Tools' dibagian kanan-> 'Enabled'->klik 'OK'



Gambar 4. Kotak Dialog Prevent Access to Registry Editing Tools

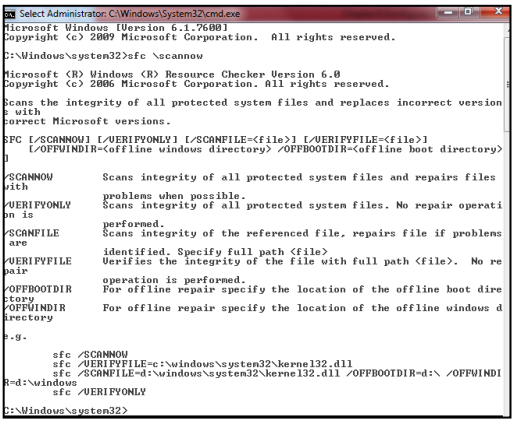


Gambar 5. Menonaktifkan Akses Registry

6. *Windows resource protection*
   a. Melindungi *file-file windows* dari modifikasi malware atau kerusakan. Langkah pengamanan klik 'Start', ketik 'cmd', klik kanan pilih 'Run as Administrator'

Gambar 6. Kotak Dialog Run as Administrator

   b. Ketik sfc \scannow, tekan enter
   c. Ketik sfc /scannow untuk proses *scan*



Gambar 7. Memeriksa File Windows

7. Akses BIOS

   Ketika menghidupkan komputer, pengguna dapat mengakses menu BIOS dengan menekan tombol "F2" atau "delete". Disarankan untuk menambahkan *password* kuat terdiri dari huruf besar, huruf kecil, karakter, dan angka, total delapan karakter.

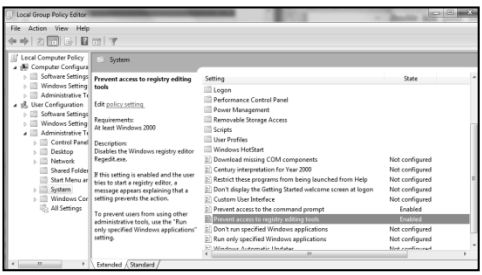
8. Sistem *Backup*
   a. Klik 'Windows'->'Settings'-> 'Update & Security'-> 'Backup', aktifkan 'On' pada 'Automatically Backup My Files'
   b. Klik 'More Options', pilih 'Backup My Files'
   c. Klik 'Add a Folder' jika akan menambahkan *folder* lain yang akan di *backup*

9. Akses USB

   Untuk mengamankan USB dari akses ilegal ke komputer, install aplikasi 'USB Blocker' pada laman https://securityxploded.com/windows-usb-blocker.php

Gambar 8. Tampilan Laman Windows USB Blocker

10. Command Promt/CMD
    a. Akses CMD, klik Windows, ketik CMD. Klik tombol 'Windows' + 'R' secara bersama-sama
    b. Ketikan gpedit.msc, pada kotak dialog
    c. Menu 'User Configuration-> 'Administrative Template' ->'System'. *Double* klik pada 'Prevent Access to Command Prompt' di bagian kanan-> 'Enabled'-> klik 'OK'



Gambar 9. Menonaktifkan akses CMD

F. Konfigurasi Keamanan pada Linux

Linux, awalnya digunakan untuk *server* web dan sistem pengembangan, telah berevolusi menjadi platform global. Keuntungan praktisnya meliputi efisiensi biaya, kemudahan penyebaran, kemampuan untuk berkembang dan fitur baru kepada pengguna (Siever et al. 2009). Ubuntu adalah linux yang banyak digunakan, dikenal karena kemudahan

penggunaannya, keandalan, dan komunitas pengembang yang aktif (Smyth 2020).

Konfigurasi Linux difokuskan pada Ubuntu Linux versi 19 berbasis desktop. Cara konfigurasi adalah sebagai berikut (Gunawan 2021):

1. Akun
    a. Gunakan perintah psswd root untuk merubah atau menggunakan *password* pada *root*
    b. Gunakan perintah sudo su untuk merubah akun *non root* menjadi *root*
    c. Gunakan perintah berikut untuk menambahkan akun lain (misal rinjani) ke dalam grup *root*
    sudo adduser rinjani
    sudo usermod –aG sudo rinjani
    d. Gunakan perintah berikut untuk masuk ke akun rinjani dengan *mode* menjadi *root*
    su – rinjani
    sudo su
2. Ancaman Malware
    a. Instal aplikasi antivirus dari vendor ketiga misal aplikasi clamAV, gunakan perintah sudo apt install clamav clamav-daemon
    b. Instal aplikasi GUI clam AVI dengan cara sudo apt install clamtk
    c. Gunakan perintah clamtk untuk membuka aplikasi
3. Aplikasi

    Gunakan perintah sudo apt-get install namaaplikasi untuk intalasi aplikasi direpository resmi

4. *Browser*
   a. Pasang ‘add on’ jenis ‘Unblock origin’ dengan cara buka *browser* (Firefox) pada laman https://addons.mozilla.org/enUS/firefox/addon/ublock-origin/?src=search.
   b. *Browser* (Edge) unduh ‘Unblock origin’ pada menu ‘Start’->’Microsoft Store’ ketikkan ‘Unblock Origin’ di menu pencarian
   c. Browser (Chrome) unduh ‘Unblock origin’ pada laman https://chrome.google.com/webstore/detail/ublock origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en.
5. Sistem *Backup*

   Secara *default* sudah terinstall, apabila belum gunakan perintah sudo apt-get instal deja-dup
6. Versi OS

   Gunakan perintah berikut untuk perbaharui sistem operasi dan aplikasi

   sudo apt-get update

   sudo apt-get upgrade

BAB 8

Pengembangan Aplikasi yang Aman

Agni Isador Harsapranata, S.Kom.,M.M.,M.Kom.

Pengembangan suatu aplikasi, atau sering juga disebut dengan pengembangan sistem informasi menggunakan tahapan yang sering disebut dengan SDLC (*Software Development Life Cycle*)(Finalita and Ahyudanari, 2021). Sebelum melangkah ke pengembangan aplikasi yang aman, dijelaskan apa yang dimaksud dengan SDLC. Didalam SDLC

terdapat tahapan tahapan dalam pengembangan sistem informasi, yaitu :

1. **Perencanaan Sistem (*Systems Planning*).**

   Dalam tahapan ini yang dianalisa merupakan kelayakan dari sistem yang akan dikembangkan. Dilakukan dalam tahapan ini meliputi pembentukan tim pengembang, menjelaskan ruang lingkup dan tujuan pengembangan sistem, menjelaskan secara detail manfaat yang dapat diperoleh dari pengembangan sistem terutama dalam menyelesaikan masalah yang ada, menjelaskan strategi yang dipergunakan dalam pengembangan sistem, menentukan teknologi yang akan dipergunakan dalam pengembangan sistem.

2. **Analisis Sistem (*Systems Analysis*)**

   Pada tahap ini, dilakukan analisa terhadap kelebihan dan kekurangan sistem yang ada, fungsi sistem, dan pengembangan dari sistem yang telah ada (peluang, masalah, solusi yang akan digunakan). Selain itu, dalam tahap ini dilakukan perencanaan alokasi sumber daya, perencanaan penjadwalan pengembangan sistem, perkiraan biaya dalam pengembangan sistem.

3. **Implementasi Sistem (*Systems Implementation*)**

   Dalam tahapan ini, dilakukan implementasi dari tahapan rancangan yang telah dilakukan sebelumnya, yaitu penerapan skema rancangan databse, penerapan desin sistem ke dalam sistem informasi, perbaikan dan pengujian dari sistem informasi yang sedang dikembangkan.

4. **Pemeliharaan Sistem (*Systems Maintenance*)**

   Dalam langkah ini, dilakukan oleh administrator dengan melakukan penjagaan sistem untuk dapat berjalan

sebagaimana mestinya, dan mampu untuk beradaptasi menurut kebutuhan pengguna sistem informasi.

Dalam pengembangan sistem SDLC terdapat beberapa model yang dijadikan landasan yaitu :

1. *Waterfall Model*(Ridwanto and Capah, 2020)

   Merupakan model aliran sistem yang linier klasik dan sederhana, model ini menyelesaikan setiap tahapan secara lengkap sebelum melangkah ke tahapan berikutnya. Untuk setiap tahapan, sebelum melangkah ke tahapan berikutnya akan dilakukan evaluasi dari tahapan yang sudah diselesaikan untuk menjamin bahwa tahapan tersebut sudah sesuai dengan yang diharapkan.

2. *Prototype Model*(Alves, Mateus-Coelho and Cruz-Cunha, 2023)

   Merupakan revolusi dari *waterfall Model*, dimana dalam pengembangan aplikasi yang ada, pengguna dilibatkan dengan mencoba *prototype* yang sudah dikembangan, dan diminta masukan sehingga aplikasi yang sedang dikembangan sesuai dengan harapan pengguna.

3. *Rapid Application Development* (RAD) *Model* (Adrianus, Edwin and Yanfi, 2023)

   Model RAD merupakan pengembangan aplikasi yang adaptif dengan kecepatan tinggi.

4. *Evolutionary Development Model*

   Model ini merupakan model yang bersifat evaluasi secara berulang, dengan menggunakan model ini dapat dihasilkan pengembangan aplikasi yang semakin lengkap dari waktu ke waktu sampau pada proses akhir pengembangan.

5. *Agile Model*(Repetto, 2023)

   Model ini merupakan pengembangan yang memerlukan adaptasi yang cepat, dan merupakan pengembangan jangka pendek,

6. *Fontain Model*

   Model ini merupakan perbaikan untuk *waterfall model*, walaupun urutan logis dalam pengembangan aplikasi tetap sama.

7. *Synchronize And Stabilize Model*

   Dalam model ini ditekankan pendekatan proses manajemen. Dilakukan pengelompokan kebutuhan kebutuhan yang paling mendasar untuk dikerjakan terlebih dahulu, kemudian dilanjutkan

8. *Rational Unified Process Model*

   Metode ini merupakan metode yang cukup sering dipergunakan dalam pengembangan aplikasi berorientasi objek.

9. *Build & Fix Method Model*

   Metode ini memberikan perawatan secara terus menerus dan pelayanan perbaikan terhadap produk yang digunakan oleh pengguna.

10. *Big Bang Model*

    Model ini merupakan pengembangan aplikasi dengan dimulai dengan menggunakan usaha dan uang sebagai masukan utama. Sehingga hasil dari aplikasi tersebut bisa dimungkinkan tidak sesuai dengan kebutuhan pelanggan.

11. *The V-Model* (Hartono, 2021)

    Merupakan pengembangan dari *Waterfall Model*, dengan penambahan pengujian disetiap tahapannya, sehingga memastikan setiap tahapan sudah selesai sesuai dengan yang diharapkan.

Pengembangan aplikasi yang aman merupakan pengembangan tahapan dari SDLC, yaitu SSDLC (*Secure Software Development Life Cycle*)(Williams, 2021). SSDLC bertujuan untuk mengembangkan aplikasi yang aman dari awal tahapan produksinya, karena keamanan aplikasi merupakan tanggungjawab semua pihak yang berkepentingan dengan pengembangan aplikasi tersebut. Dengan pengembangan aplikasi yang aman, dapat mengurangi resiko dari kerentanan aplikasi yang sudah diproduksi. Berikut merupakan perbandingan dari SDLC dan SSDLC.

Tabel 1. Perbedaan SDLC (*Software Development Life Cycle*) dan SSDLC (*Secure Software Development Life Cycle*)

SDLC (*Software Development Life Cycle*)	**SSDLC (*Secure Software Development Life Cycle*)**
a. Fokus engembangan aplikasi yang efisien, cepat, dengan biaya yang minimal	b. Fokus terhadap keamanan dalam pengembangan aplikasi dengan mengurangi pengaruh terhadap efisiensi, kecepatan dan biaya yang ditimbulkan.
c. Pengujian Aplikasi yang sudah diselesaikan dilakukan pada akhir tahapan.	d. Pengujian keamanan aplikasi dilakukan sepanjang proses pengembangan aplikasi.
e. Keamanan merupakan tahapan tersendiri dalam pengembangan aplikasi.	f. Keamanan menjadi patokan disetiap bagian aplikasi.

Secara garis besar tahapan SSDLC adalah sebagai berikut :

1. ***Security Requirement***

Dalam tahapan ini, pengembangan aplikasi diharapkan dapat memenuhi persyaratan keamanan, yaitu :

a. *Confidentiality* (Ali *et al.*, 2023), di tahap ini pengembangan aplikasi memastikan terhadap perlindungan data, apalagi untuk data data yang bersifat rahasia, dalam, perlindungan data meliputi, perlindungan terhadap pengiriman, pemrosesan, dan penyimpanan data. Beberapa mekanisme yang umum digunakan meliputi penggunaan teknologi kriptografi dan teknologi *masking*.

b. *Integrity*(Chanal and Kakkasageri, 2022)

Dalam tahap ini, memastikan aplikasi dapat berjalan dan berfungsi secara handal, dan terlindungai dari modifikasi yang tidak sah, sehingga laporan yang dihasilkan oleh aplikasi merupakan data atau informasi yang akurat.

c. *Availability*(Rimsan and Mahmood, 2020)

Dalam tahapan ini, aplikasi yang dikembangkan dipastikan tidak ada yang dapat menganggu jalanan aplikasi sehingga operasional pengguna terganggu.

d. *Authentication*(Vairagade and Brahmananda, 2020), di tahap ini memastikan validitas dan keabsahan pengguna dalam menggunakan aplikasi, bentuk autentikasi yang umum digunakan adalah autentikasi dasar (dalam bentuk *username* dan *password*), authentikasi terintegrasi (dikenal dengan teknologi *LAN Manager*), autentifikasi sertifikat elektroni(aplikasi dijamin oleh pemegang sertifikat elektronik), autentifikasi berbasis token, autentifikasi berbasis

smart card, autentifikasi biometrik, dan autentifikasi multi faktor.

e. *Authorization* (Ferretti *et al.,* 2021)

Memastikan hak yang digunakan dalam melakukan akses aplikasi sesuai dengan ketentuan keabsahan pengguna aplikasi.

f. *Accountability*(Godawatte, Branch and But, 2022)

Merupakan catatan penggunaan aplikasi oleh pengguna, sehingga dapat dilakukan pemeriksaan secara berkala dan mengetahui gangguan pelanggaran yang dilakukan oleh pengguna aplikasi.

2. Security Design

Desain ini bertujuan untuk membuat rancangan perlindungan data dan informasi.

a. *Confidentiality Design*
b. *Integrity Design*
c. *Availability Design*
d. *Authentication Design*
e. *Autorization Design*
f. *Accountability Design*

3. Security Development

Dalam tahap ini pengembang aplikasi menerapkan teknologi yang menjamin proses penulisan kode aplikasi yang aman. Menemukan dan memperbaiki kerentanan dari aplikasi yang ada berdasarkan dari standar OWASP (Applebaum, Gaber and Ahmed, 2021), merupakan proyek di kelola oleh MITRE dan SANS Institute.

4. Security testing

Memastikan aplikasi yang dikembangkan lolos dalam pengujian keamanan aplikasi dan berjalan sesuai dengan

harapan pengguna, pengujian meliputi *White Box Testing, Black Box Testing, Cryptographic Validation Testing.*

5. ***Security Deployment***

   Dalam tahap ini memastikan aplikasi dapat berfungsi sebagaimana mestinya dan aman, memastikan konfigurasi untuk melakukan *deployment* yang aman.

6. ***Security Maintenance***

   Menjamin aplikasi dapat berfungsi dengan handal.

BAB

9

Keamanan Basis Data

Alfa Saleh, M.Kom

Keamanan basis data mengacu pada serangkaian alat, kontrol, dan tindakan yang dirancang untuk membangun dan menjaga kerahasiaan, integritas, dan ketersediaan dari basis data (ibm.com). keamanan basis data mempunyai tujuan dan prinsip yang sama dengan keamanan data dan keamanan informasi, namun dalam ruang lingkup basis data. Bagaimana melindungi basis data dari penggunaan akses yang tidak sah, menjaga data yang rentan agar tetap aman.

Pada tahun 2023, setidaknya ada 4 kasus dugaan kebocoran data yang terjadi di Indonesia. Pertama, dugaan kebocoran data terjadi di BPJS Ketenagakerjaan, setidaknya ada sebanyak 19 juta data pengguna yang bocor dan diperjualbelikan. Kedua, kasus dugaan kebocoran data yang terjadi di Bank Syariah Indonesia (BSI), ada sekitar 15 juta data yang telah bocor, meliputi data pengguna dan password, tidak hanya itu dokumen-dokumen penting lainnya juga tidak luput dari kebocoran data. Ketiga, data paspor WNI yang diduga bocor, setidaknya ada sekitar 34 juta data paspor WNI yang berhasil dicuri. Keempat, data pemilih dari KPU yang juga diduga bocor hingga 204 juta data pemilih. (cnnindonesia, 2023)

Dari beberapa contoh kasus di atas, keamanan basis data sangat penting untuk dijaga, mulai dari kerahasiaan data, integritas data dan ketersediaan data harus menjadi satu kesatuan yang harus dipenuhi.

A. Kerahasian Data

Kerahasiaan data adalah sekumpulan aturan yang dibuat guna untuk membatasi data ataupun informasi yang dapat diakses. Untuk menjaga kerahasiaan data dan informasi dalam basis data, agar tidak diakses oleh pihak yang tidak berwenang, suatu sistem harus tanggap dalam mencegah terjadi hal tersebut.

Pada tingkat organisasi, Penyalahgunaan kerahasiaan data dapat menyebabkan pelanggaran yang berdampak pada operasional, finansial dan reputasi dari sebuah organisasi. Maka dari itu, penting sekali membatasi hak akses terhadap data supaya data tetap aman dari segala bentuk penyalahgunaan.

Untuk mencapai kerahasiaan dalam keamanan basis data, kita dapat menerapkan kontrol seperti hak akses dan enkripsi data. Hak akses disini adalah sebuah hak istimewa yang diberikan kepada seseorang untuk dapat berinteraksi dengan basis data di dalam sebuah sistem. Sementara enkripsi data dapat diartikan sebagai upaya menerjemahkan data dari bentuk aslinya menjadi bentuk yang telah tersandikan sehingga sulit untuk dipahami.

B. Integritas Data

Integritas data mengacu pada data yang dapat disajikan dengan konsisten, akurat, lengkap dan handal. Dengan adanya integritas data ini, sistem mampu mendeteksi ketika suatu data telah dimodifikasi dengan cara yang tidak sah. Di dalam lingkup basis data, terdapat 4 (empat) jenis integritas data yang perlu diketahui.

1. Integritas entitas

Definisi dari integritas entitas ini mirip dengan konsep relasi dalam model basis data relasional. Di mana setiap baris dalam sebuah tabel harus diidentifikasikan secara unik berdasarkan kunci utamanya (primary key). Jika kunci utamanya adalah sebuah atribut tunggal, maka semua nilai pada kolom tersebut harus unik, sama halnya jika kunci utama adalah gabungan dari beberapa atribut, maka harus dipastikan juga seluruh nilai gabungan dari kolom-kolom tersebut harus unik. Perlu dipastikan juga kunci utama itu tidak hanya harus unik, tetapi juga tidak boleh kosong tanpa nilai. Jadi, Integritas entitas ini

memastikan tidak adanya data yang sama atau duplikat di dalam basis data.

2. **Integritas Acuan (Referential Integrity)**

Integritas ini mengacu pada hubungan antar tabel yang telah memenuhi kondisi tertentu. Sebagai contoh, untuk setiap relasi basis data, nilai sebuah kunci tamu (foreign key) harus merujuk pada nilai kunci utama (primary key) yang ada.

Tabel Pegawai

IDPegawai	Nama	Alamat	Jenis Kelamin	IDDivisi
P1001	Alfa	Jln. Paku	Laki-Laki	D3
P1002	Bobby	Jln. Kenanga	Laki-Laki	D1
P1003	Citra	Jln. Bambu	Perempuan	D2
P1004	Dedi	Jln. Kebenaran	Laki-Laki	D1
P1005	Erlangga	Jln. Persatuan	Laki-Laki	D1
P1006	Fina	Jln. Perubahan	Perempuan	D2
P1007	Ghania	Jln. Pulang	Perempuan	D2
P1008	Hambali	Jln. Kendari	Laki-Laki	D1
P1009	Indah	Jln. Pertempuran	Perempuan	D2
P1010	Jeriko	Jln. Banten	Laki-Laki	D1

Tabel Divisi

IDDivisi	Nama Divisi	Manager
D1	Keuangan	P1002
D2	Penjualan	P1006
D3	Pemasaran	P1001

Misalnya, antara tabel pegawai dan tabel divisi, integritas referensialnya dapat terlihat dan terjaga sebab nilai yang ada pada tabel pegawai mengacu pada nilai yang ada pada tabel divisi. Contoh jelasnya, untuk nilai pada atribut IDDivisi di tabel pegawai harus mengacu pada nilai IDDivisi pada tabel Divisi, sehingga jika ada nilai yang berbeda di antara keduanya maka

tentu dikatakan bahwa integritas referensialnya tidak terbentuk.

3. **Integritas Jangkauan (Domain Integrity)**

Integritas jangkauan mengacu pada nilai data yang ada harus sesuai ketentuan dan dalam bentuk yang tepat. Ketika sebuah tabel dibuat, kita mendefinisikan dan membuat batasan untuk setiap atribut/field. Disinilah peran dari integritas jangkauan bekerja dalam Database Management System (DBMS) dengan memastikan nilai setiap atribut harus sesuai dengan ketentuan yang telah didefinisikan dan dibatasi. Contohnya, jika atribut IDPegawai didefinisikan sebagai sebuah atribut yang menampung nilai Integer, maka nilai yang dapat ditampung pada atribut tersebut adalah nilai numerik yang berupa bilangan bulat, sementara jika yang dimasukan adalah bukan nilai numerik maka DBMS akan memberikan notifikasi kesalahan. Begitu juga jika sebuah atribut didefinisikan dengan tipe data varchar dengan jangkauan karakter sebanyak 30 karakter, maka nilai atribut tersebut tidak boleh diisi dengan nilai teks yang lebih dari 30 karakter. Tidak hanya tipe data dan batasan jangkauan nilai yang bisa ditampung, integritas jangkauan juga memungkinkan untuk membatasi nilai Null dan Not null pada sebuah atribut di dalam tabel.

4. **Integritas Aturan Pengguna (User-Defined Integrity)**

Jenis integritas data ini mengacu pada aturan tambahan yang dapat ditentukan secara spesifik berdasarkan kebutuhan pengguna (Business Rule). Contohnya, pada sebuah perguruan tinggi, terdapat

beberapa matakuliah bersyarat, yang mana sebuah matakuliah bisa diambil ketika matakuliah sebelumnya telah selesai dijalani. Detailnya, matakuliah Bahasa Inggris II bisa diambil ketika matakuliah Bahasa Inggris I telah selesai dan lulus. Tidak akan bisa kedua matakuliah tersebut dijalani pada semester yang sama. Pada kasus ini lah, integritas aturan pengguna dapat diterapkan dalam basis data.

C. Ketersediaan Data (Data Availability)

Konsep dari ketersediaan data adalah dengan memastikan tersedianya semua data yang dapat diakses kapanpun dan dimanapun. Fokusnya adalah aksesibilitas dan kontinuitas informasi yang harus dijaga. Untuk menjamin ketersediaan data yang berkesinambungan, tentu penting sekali memahami apa yang menyebabkan data tidak dapat diakses dan tantangan apa yang akan dihadapi untuk memastikan data tetap tersedia sepanjang waktu. Jika bicara tentang data, bisnis yang mengandalkan data dalam menyampaikan produk dan layanannya akan berusaha untuk menjaga agar tetap ada dan mudah diakses. Hal ini juga berhubungan dengan ketersediaan sumber daya baik fisik maupun non-fisik. Ini juga yang menjadi tantangan untuk setiap organisasi dalam mengatasi masalah seputar ketersediaan data. Contohnya, Bagaimana infrastruktur teknologi informasi pada suatu organisasi tetap aktif meski terjadi gangguan pada jaringan. Dengan keamanan basis data, gangguan pada ketersediaan data baik berupa data hilang atau rusak dapat diatasi dengan pencadangan ataupun pemulihan data. Fitur tersebut juga tersedia pada

DBMS itu sendiri, dimana operasi pencadangan dan pemulihan dapat dilakukan dengan cepat dan mudah.

Dalam keamanan basis data, ketiga elemen ini baik integritas data, keamanan data serta ketersediaan data harus dijaga dengan baik dan tepat. Ada beberapa ancaman terhadap keamanan basis data yang mungkin bisa terjadi, seperti Ancaman Insider, Human Error, Eksplotasi kerentanan software basis data, serangan SQL Injection, serangan Buffer Overflow, serangan Denial of Service hingga Malware. Berikut beberapa tindakan yang dapat dilakukan untuk menjaga keamanan basis data.

1. **Atur Kata Sandi dan Akses Pengguna secara berkala**

   Mengatur kata sandi dan akses pengguna sangat penting apalagi jika data tersebut milik organisasi yang besar. Perlu adanya otomatisasi manajemen akses pada basis data melalui penggunaan kata sandi, sehingga yang dapat mengakses basis data tersebut hanya pengguna yang memiliki hak akses. Pembatasan penggunaan akses ini juga memungkinkan pengguna hanya mengakses data dan informasi yang diperlukan. Selain itu, hal tersebut juga membantu dalam melacak riwayat aktivitas setiap pengguna yang mengakses basis data.

2. **Uji Keamanan Basis Data yang dimiliki**

   Selain menyiapkan infrastruktur keamanan basis data yang baik, tentu perlu juga untuk mengujinya dari ancaman-ancaman yang mungkin terjadi. Melakukan audit dan uji penetrasi terhadap basis data akan membantu dalam memahami pola pikir pelaku

kejahatan dunia maya dan mengisolasi segala kerentanan yang mungkin terabaikan. Jika basis data tersebut digunakan oleh organisasi yang besar, sebaiknya libatkan penyedia layanan uji penetrasi yang terpercaya untuk menguji keamanan basis datanya, uji penetrasi tersebut akan menghasilkan laporan yang mencantumkan kerentanan pada basis data yang telah diuji. Penting untuk menyelidiki dan memulihkan basis data dari kerentanan keamanan. Setidaknya lakukan uji penetrasi keamanan basis data sekali dalam setahun.

3. **Gunakan Monitoring Basis data Real-time**

Memonitoring basis data secara terus-menerus untuk menemukan upaya pelanggaran akan meningkatkan keamanan basis data dan memungkinkan adanya tindakan cepat terhadap segala kemungkinan serangan pada basis data. Gunakan tools Pemantauan Integritas File (File Integrity Monitoring) untuk membantu mencatat segala tindakan yang dilakukan di dalam server basis data, dengan melakukan hal tersebut juga akan memberikan peringatan tentang potensi pelanggaran yang mungkin terjadi.

4. **Gunakan Firewall untuk aplikasi web dan basis data**

Firewall merupakan bagian penting dalam suatu keamanan jaringan dimana akses lalu lintas di dunia maya banyak digunakan untuk keperluaan akademis maupun pekerjaan (dwiki,2022). Menggunakan firewall sama dengan berupaya untuk melindungi server basis data dari ancama keamanan basis data itu sendiri. firewall secara default tidak akan mengizinkan akses ke trafik dan juga menghentikan basis data untuk

terhubung ke luar kecuali ada alasan khusus untuk melakukannya. Selain melindungi basis data dengan firewall, perlu juga menerapkan Web Application Firewall (WAF) untuk menghindari serangan seperti SQL Injection yang dapat mengakses basis data secara ilegal atau tidak sah. Secara garis besar WAF mampu mendeteksi serangan dan memblokirnya sebelum serangan tersebut membahayakan basis data.

BAB

10

Manajemen Kerentanan Perangkat Lunak

Novi Aryani Fitri, S.T., M.Tr.Kom

Kerentanan perangkat lunak adalah kondisi di mana terdapat kelemahan atau celah dalam suatu perangkat lunak. Celah ini dapat dieksploitasi oleh pihak yang tidak berwenang untuk melakukan tindakan yang merugikan. Kerentanan dapat muncul karena berbagai faktor, termasuk kesalahan dalam desain, implementasi, atau konfigurasi

perangkat lunak. Beberapa jenis serangan pada jaringan komputer yaitu sebagai berikut:

1. *Ping of Death*

   Serangan ini melibatkan pengiriman *ping* yang salah atau berbahaya ke komputer target. Sebuah *ping* biasanya berukuran 56 *byte* (atau 84 *bytes* ketika *header* IP dianggap). Namun, mengirimkan paket ping sebesar 65.536 *byte* dianggap ilegal menurut protokol jaringan. Meskipun demikian, sebuah paket semacam ini dapat dikirim jika paket tersebut sudah terpecah-pecah menjadi bagian yang lebih kecil.

2. Nmap *(Port Scan)*

   Nmap (*Network Mapper*) adalah sebuah aplikasi atau *tool* yang dapat berfungsi melakukan *port scanning*. Dengan menggunakan *tool* ini, dapat melihat *host* yang aktif, *port* yang terbuka, sistem operasi yang digunakan, dan fitur-fitur *scanning* lainnya.

3. *Denial of Service* (DOS)

   DOS (*Denial of Service*) bekerja dengan memanfaatkan dan menghabiskan sumber daya yang tersedia pada komputer target sehingga membuatnya tidak dapat menjalankan fungsinya secara efektif. Serangan DOS ini bertujuan untuk mencegah pengguna dari melakukan akses terhadap sistem atau jaringan yang dituju. Berbagai metode dilakukan oleh DOS untuk mencapai tujuan ini, yaitu (Putra *et al.*, 2023):

   a. Membanjiri lalu lintas jaringan atau *traffic* dengan jumlah data yang sangat besar, mengakibatkan lalu lintas yang berasal dari pengguna yang sah menjadi

tidak dapat masuk ke dalam sistem jaringan. Teknik ini sering disebut sebagai *traffic flooding*.

b. Membanjiri jaringan dengan permintaan (*request*) yang berlebihan terhadap layanan jaringan yang disediakan oleh sebuah klien, sehingga layanan tersebut tidak dapat memenuhi permintaan yang datang dari pengguna yang sah. Teknik ini dikenal sebagai *request flooding*.

4. ***Trojan Horse***

Trojan merupakan salah satu jenis *malicious software* atau *malware* yang memiliki kemampuan untuk merusak sebuah sistem. *Trojans* dapat digunakan untuk memperoleh informasi sensitif dari target, seperti *password* dan *log* sistem, serta memperoleh hak akses dari target tersebut. Yang membedakan *trojan* dengan virus atau *worm* adalah sifat *stealth*-nya dalam beroperasi, di mana *trojan* dapat menjalankan dirinya seolah-olah seperti program biasa yang tidak mencurigakan. Selain itu, *trojan* juga dapat dikendalikan dari komputer lain yang merupakan milik penyerang.

A. Ancaman Terhadap Keamanan Perangkat Lunak

Dalam melindungi perangkat lunak jaringan komputer berarti melindungi perangkat lunak yang digunakan oleh perangkat keras jaringan seperti: sistem operasi, *server protocol browser*, perangkat lunak aplikasi dan juga properti intelektual yang disimpan di dalam *database* yang disimpan di dalam jaringan (Ika Yusnita Sari *et al.*, 2020).

Ancaman terhadap keamanan perangkat lunak melibatkan penyalahgunaan kerentanan suatu perangkat lunak. Ancaman tersebut meliputi beberapa serangan seperti *malware*, exploitasi kerentanan, serangan DdoS, dan pencurian Data. *Malware* adalah perangkat lunak berbahaya yang dapat merusak, mencuri data, atau mengganggu operasi sistem. Jenis *malware* meliputi virus, *worm*, *trojan*, dan *ransomware*, apabila serangan ini terjadi pada sistem informasi maka *Malware* dapat merusak file, menginfeksi program, atau mengambil alih sistem. Ancaman lainnya adalah eksploitasi kerentanan perangkat lunak oleh penyerang, penyerang memanfaatkan kerentanan perangkat lunak untuk mendapatkan akses yang tidak sah.

Serangan *Distributed Denial of Service* (DdoS) juga dapat terjadi pada sistem informasi. Serangan ini akan membanjiri *server* dengan permintaan palsu, akibatnya situs web atau layanan menjadi lambat atau tidak dapat diakses. Serta pencurian data sensitif secara *ilegal* seperti informasi pribadi, informasi keuangan, atau rahasia bisnis.

B. Pentingnya Manajemen Kerentanan

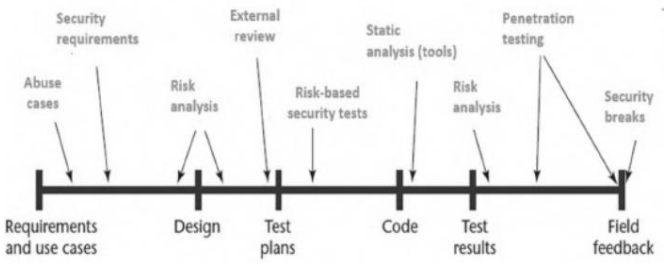
Manajemen kerentanan memainkan peran krusial dalam menjaga keamanan sistem informasi. Peran utamanya adalah mengidentifikasi, mengurangi, dan mengelola kerentanan yang mungkin ada dalam perangkat lunak atau infrastruktur IT.

Kerentanan yang tidak dikelola dengan baik dapat berdampak serius pada bisnis dan pengguna. Bisnis dapat mengalami kehilangan data, penyusupan sistem, atau

gangguan operasional yang mengakibatkan kerugian finansial dan reputasi. Pengguna juga berisiko mengalami pencurian data pribadi, identitas, atau kerugian *finansial* akibat eksploitasi kerentanan. Oleh karena itu, manajemen kerentanan harus menjadi prioritas dalam strategi keamanan.

C. Identifikasi Kerentanan Perangkat Lunak

Tim keamanan harus memantau aktivitas perangkat lunak, *log*, dan lalu lintas jaringan secara teratur untuk mendeteksi tanda-tanda aneh atau potensi kerentanan. Dengan menerapkan beberapa metode identifikasi kerentanan, organisasi dapat mengurangi risiko keamanan dan memastikan bahwa perangkat lunak mereka lebih tahan terhadap serangan. *Secure Software Development Process* (SSDP) memastikan aspek keamanan diperhatikan sejak tahap membangun perangkat lunak serta membantu pengembang meningkatkan keamanan dan mengurangi kerentanan pada perangkat lunak, sekaligus mengintegrasikan keamanan ke dalam *Software Development Life Cycle* (SDLC) (Potter and McGraw, 2004).



Gambar 1. *Software Development Life Cycle*

Perhatian pada Keamanan Selama SDLC terdiri dari memastikan keamanan diperhatikan sejak tahap perancangan hingga pengembangan, dan mengurangi kerentanan dengan mengurangi kecacatan selama desain dan pengembangan. Ketiga Keamanan "Built-In" Dimana Keamanan harus dibangun "*built-in*" ke dalam produk yang dikembangkan.

1. Metode Identifikasi

Metode indetifikasi meliput beberapa kegiatan seperti pemeriksaan kode, analisis statis, dan pengujian penetrasi. Pemeriksaan kode merupakan metode yang melibatkan analisis kode sumber perangkat lunak untuk mengidentifikasi potensi kerentanan. Tim pengembang atau peneliti memeriksa secara manual kode program dengan tujuan menemukan celah keamanan yang mungkin ada, terutama pada bagian-bagian yang berisiko tinggi seperti input pengguna yang tidak divalidasi dengan benar atau pemrosesan data sensitif. Selanjutnya, analisis statis merupakan teknik yang menggunakan alat otomatis untuk memeriksa kode tanpa menjalankannya.

Alat ini mengidentifikasi masalah potensial seperti penggunaan variabel yang tidak aman, pemanggilan fungsi berbahaya, atau ketidaksesuaian dengan pedoman keamanan. Keuntungan dari analisis statis adalah kemampuannya untuk menemukan kerentanan tanpa harus menjalankan aplikasi secara aktif.

Pengujian penetrasi merupakan metode yang melibatkan serangan simulasi terhadap perangkat lunak untuk menemukan kerentanan. Tim keamanan

menggunakan teknik yang mirip dengan serangan yang mungkin dilakukan oleh penyerang nyata, termasuk pengujian input yang tidak valid, pencarian celah keamanan, dan eksplorasi sistem secara menyeluruh.

2. *Tools* dan Teknik

Setelah dilakukan metode identifikasi, dalam hal *tools* dan teknik, terdapat beberapa pendekatan yang umum digunakan. *Static Analyzers* adalah alat yang menganalisis kode tanpa eksekusi, mengidentifikasi kerentanan dengan mencari pola yang mencurigakan. *Fuzzy Testing* adalah teknik mengirim input acak ke perangkat lunak untuk menemukan kerentanan yang mungkin terjadi saat *input* tidak terduga. *Vulnerability Scanners* adalah alat otomatis yang memeriksa perangkat lunak untuk kerentanan yang sudah diketahui, seperti yang tercatat dalam basis data CVE (*Common Vulnerabilities and Exposures*).

D. Implementasi Sistem Keamanan Terkini

Mengadopsi sistem keamanan terkini menjadi suatu keharusan, termasuk *Intrusion Detection Systems* (IDS) yang mampu mendeteksi aktivitas mencurigakan di jaringan. *Intrusion Prevention Systems* (IPS) melibatkan pencegahan serangan berdasarkan pola yang telah dikenali, sementara *Firewall* dan *Filtering Mechanisms* digunakan untuk mengontrol lalu lintas jaringan secara efektif.

1. *Intrusion Detection Systems* (IDS): *Intrusion Detection Systems* (IDS) bertugas memantau dan mendeteksi aktivitas mencurigakan atau serangan keamanan. Ini

melibatkan penggunaan sensor dan analisis *log* untuk mengidentifikasi ancaman potensial.

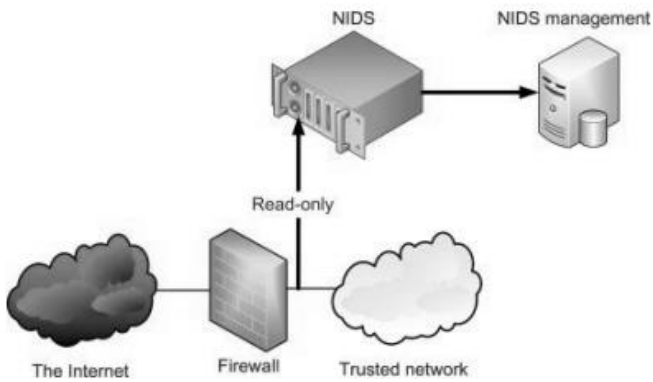
2. *Intrusion Prevention Systems* (IPS): *Intrusion Prevention Systems* (IPS) bertujuan untuk mencegah serangan keamanan secara langsung dengan mengambil tindakan otomatis untuk memblokir atau menghentikan aktivitas mencurigakan yang terdeteksi oleh IDS.
3. *Firewall* dan *Filtering Mechanisms*: Mekanisme yang bertanggungjawab dalam mengontrol lalu lintas jaringan. Firewall mengidentifikasi nama, alamat IP, aplikasi, dan karakteristik lain dari lalu lintas masuk. Ia memeriksa informasi ini terhadap aturan akses yang telah diprogram ke dalam sistem oleh administrator jaringan. Firewall terdiri dari paket penyaringan, *Network Address Translation* (NAT) dan Aplikasi *Proxy Filering.*

E. Intrusion Detection Systems (IDS)

Ketergantungan pada jaringan komputer dan Internet telah membuat keamanan menjadi kekhawatiran utama. Sistem Deteksi Intrusi memainkan peran penting dalam mengamankan sistem dengan memantau lalu lintas jaringan dan perilaku abnormal untuk mendeteksi intrusi.

Dalam lingkungan komputasi saat ini, di mana ancaman terus berkembang, sistem deteksi intrusi sangat diperlukan untuk melindungi jaringan dan sistem komputer dari serangan kompleks yang tidak bisa dideteksi oleh *firewall* biasa. Bagaimana Sistem IDS membantu tim

keamanan dalam mengidentifikasi dan menyelidiki ancaman potensial. Saat IDS melakukan pemindaian lalu lintas jaringan untuk mendeteksi kejadian, proses ini tergantung pada infrastruktur jaringan seperti pada gambar 2. Selama IDS melakukan pencarian terhadap ancaman, ancaman tersebut akan teridentifikasi dan dicatat dalam *log*.



Gambar 2. Cara Kerja NIDS. (Kumar *et al.*, 2021).

1. **Fase Deteksi:**
    a. IDS terus-menerus memantau lalu lintas jaringan dalam sebuah organisasi.
    b. Ini mendeteksi pola yang tidak biasa: percobaan *login* ulang ke *server* kritis dari alamat IP yang tidak dikenal.
    c. IDS menghasilkan peringatan, menunjukkan adanya insiden keamanan potensial.
    d. *Fase* deteksi dapat menggunakan tools seperti *Network Intrusion Detection System* (NIDS), *Host Intrusion Detection System* (HIDS), *Protocol-based*

Intrusion Detection System (PIDS), *Application Protocol-based Intrusion Detection System* (APIDS) dapat mengidentifikasi serangan seperti SQL *Injection*, *cross-site scripting* (XSS), atau serangan berbasis aplikasi web lainnya, dan *Hybrid Intrusion Detection System* Kombinasi dari berbagai jenis IDS, seperti NIDS dan HIDS. Sistem ini bekerja sama untuk memberikan tingkat keamanan yang lebih tinggi, mendeteksi ancaman baik di tingkat jaringan maupun *host*, serta pada tingkat aplikasi.

2. Generasi Peringatan

   a. Tim keamanan menerima peringatan dari IDS : Ketika IDS mendeteksi aktivitas mencurigakan, seperti percobaan *login* ulang ke *server* kritis dari alamat IP yang tidak dikenal, tim keamanan menerima peringatan. Peringatan ini menandakan adanya potensi ancaman keamanan.

   b. Investigasi Lebih Lanjut: Tim keamanan melakukan penyelidikan lebih lanjut. Tim memeriksa *log* yang terkait dengan alamat IP yang mencurigakan. *Log* ini berisi informasi tentang aktivitas jaringan yang mencurigakan, termasuk waktu kejadian dan detail lainnya.

   c. IDS memberikan detail seperti Waktu: Kapan aktivitas mencurigakan terjadi.

   d. IP Sumber: Alamat IP yang terlibat dalam percobaan *login*.

   e. *Server* Target: *Server* yang menjadi sasaran percobaan *login*.

f. Percobaan *Login* Spesifik: Informasi lebih lanjut tentang jenis percobaan *login* yang dilakukan.

3. **Penyelidikan**

   a. Analisis keamanan mengkorelasikan peringatan IDS dengan log lain (misalnya, *log firewall, log* otentikasi).

   b. Mereka menemukan bahwa alamat IP yang sama mencoba akses tidak sah ke beberapa *server*.

   c. Pola tersebut menunjukkan serangan yang terkoordinasi.

4. **Respon**

   a. Tim keamanan mengambil tindakan

   b. Pemblokiran dengan menambahkan alamat IP yang mencurigakan ke daftar hitam firewall.

   c. Notifikasi memberitahu pemilik *server* yang terpengaruh tentang insiden tersebut.

   d. Forensik mengumpulkan bukti tambahan untuk analisis lebih lanjut.

5. **Penyelesaian**

   a. Upaya akses tidak sah berhasil digagalkan.

   b. Tim keamanan memperbarui aturan firewall dan memperkuat kontrol akses.

   c. Mereka terus memantau untuk setiap aktivitas terkait.

IDS memainkan peran penting dalam deteksi dini ancaman, memungkinkan tim keamanan untuk merespons dengan cepat dan mencegah kerusakan potensial.

F. Snort

Snort adalah perangkat lunak yang dirancang untuk mendeteksi intrusi dan melakukan analisis paket secara *real-time* terhadap lalu lintas jaringan, selain itu, juga mampu menyimpan *data log* ke dalam *database*. *Snort* memiliki kemampuan untuk mengidentifikasi berbagai jenis serangan yang berasal dari luar jaringan (Ariyus, 2007:145). Program ini dapat dioperasikan dalam tiga mode yang berbeda. terdiri dari:

1. Paket *sniffer*

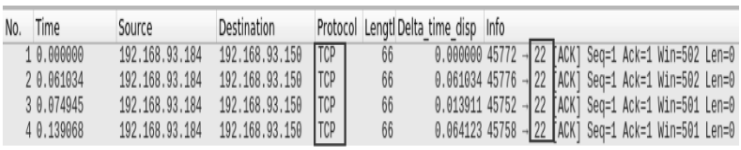
   Snort berfungsi untuk membaca paket-paket dari jaringan dan menampilkan aliran data secara kontinu pada konsol atau layar. Jika tujuannya adalah untuk melihat hanya paket-paket header dari protokol TCP/IP yang ditampilkan pada layar, perintah yang dapat digunakan yaitu:

```
./snort -v
```

2. Paket *logger*

   Untuk mencatat log dari paket-paket ke dalam disk, penting untuk menentukan direktori logging di mana data log akan disimpan. Melalui perintah yang sesuai, Snort akan dijalankan secara otomatis dalam mode pencatatan paket.

```
./snort –dev –l ./log
```



No.	Time	Source	Destination	Protocol	Length	Delta_time_disp	Info
1	0.000000	192.168.93.184	192.168.93.150	TCP	66	0.000000	45772 → 22 [ACK] Seq=1 Ack=1 Win=502 Len=0
2	0.061034	192.168.93.184	192.168.93.150	TCP	66	0.061034	45776 → 22 [ACK] Seq=1 Ack=1 Win=502 Len=0
3	0.074945	192.168.93.184	192.168.93.150	TCP	66	0.013911	45752 → 22 [ACK] Seq=1 Ack=1 Win=501 Len=0
4	0.139068	192.168.93.184	192.168.93.150	TCP	66	0.064123	45758 → 22 [ACK] Seq=1 Ack=1 Win=501 Len=0

Gambar 3. Hasil pemeriksaan *log snort pada* serangan SSH *brute force* (Damayanti and Hikmah, 2022)

3. NIDS (*Network Intrusion Detection System*)

Dalam mode ini, *Snort* berperan dalam mendeteksi serangan yang terjadi melalui jaringan komputer. Untuk mengaktifkan mode Sistem Deteksi Penyusup Jaringan (NIDS), gunakan perintah sebagai berikut:

```
./snort –dev –l ./log –h 192.168.1.0/24 –c

snort.conf
```

4. WinPcap

WinPcap merupakan sebuah *driver* yang bertugas untuk menangkap paket-paket yang mengalir dalam jaringan. Dari segi fungsinya, *WinPcap* bertugas untuk menangkap paket-paket dari kabel jaringan dan meneruskannya ke *program Snort*. Secara konseptual, *WinPcap* dapat dianggap sebagai versi *Windows* dari *libpcap*, yang sering digunakan untuk menjalankan *Snort* dalam lingkungan *Linux* atau UNIX (Rafiudin, 2010: 6). Fungsi-fungsi utama dari *driver WinPcap* untuk *Snort* meliputi:

a. Mendeteksi dan menampilkan daftar *adapter* jaringan yang sedang beroperasi beserta informasi terkait.

b. Memantau paket-paket yang melewati *adapter* yang dipilih.

c. Menyimpan paket-paket tersebut ke dalam *hard-drive*, atau lebih penting lagi, meneruskannya ke program *Snort*.

Berikut beberapa kata kunci yang ada pada penggunaan IDS dan IPS

a. *Packet sniffing*: *Snort* dapat menangkap paket jaringan dan menganalisis *header* serta *payload*-nya.

b. *Rule-based detection*: Menggunakan file aturan untuk mendeteksi lalu lintas jahat berdasarkan tanda-tanda serangan yang sudah diketahui.

c. *Protocol analysis*: Mampu menganalisis berbagai protokol seperti TCP, UDP, IP, HTTP, FTP, SMTP, dll.

d. *Preprocessor*: Memiliki *preprocessor* untuk mendekode protokol HTTP, FTP, dan lainnya, mengekstrak informasi yang berguna sebelum mesin aturan menganalisis paket.

e. *Logging* dan *alert*: Dapat mencatat paket ke *disk* dan menghasilkan peringatan untuk lalu lintas jahat.

f. Konfigurasi: Sangat dapat dikonfigurasi menggunakan file *snort.conf*. Aturan, *preprocessors*, *output*, dll, dapat dikonfigurasi.

BAB

11

Peran Manusia dalam Keamanan Sistem Informasi

Putri Ariatna Alia, S.S.T., M.T.

Keamanan sistem informasi menjadi semakin krusial seiring dengan perkembangan teknologi digital. Meskipun teknologi keamanan terus berkembang, peran manusia tetap menjadi faktor penting dalam memastikan integritas, kerahasiaan, dan ketersediaan data dalam suatu

sistem informasi. Berikut adalah beberapa aspek kunci peran manusia dalam keamanan sistem informasi:

1. **Kesadaran Keamanan:**

   Kesadaran dan pemahaman pengguna tentang risiko keamanan merupakan langkah awal yang penting. Manusia sebagai pengguna akhir harus mampu mengidentifikasi tanda-tanda serangan dan melaporkannya.

   Program pelatihan kesadaran keamanan dapat membantu meningkatkan pemahaman tentang praktik keamanan yang baik, mulai dari penggunaan kata sandi yang kuat hingga cara mengenali serangan phishing.

2. **Manajemen Akses dan Hak Pengguna:**

   Penetapan hak akses yang tepat oleh administrator sistem merupakan tanggung jawab manusia untuk memastikan bahwa setiap pengguna hanya memiliki akses yang sesuai dengan pekerjaannya.

   Melibatkan prinsip kebutuhan terhadap akses, yang memastikan bahwa pengguna hanya memiliki akses ke data dan sistem yang benar-benar diperlukan untuk menjalankan tugasnya.

3. **Keamanan Fisik:**

   Manusia bertanggung jawab atas keamanan fisik perangkat keras dan infrastruktur sistem informasi. Ini mencakup pengendalian akses fisik ke pusat data, pengamanan perangkat keras, dan tindakan pencegahan fisik lainnya.

Peran petugas keamanan, petugas pusat data, dan personel terkait dalam menjaga keamanan fisik sangat penting.

4. **Pemantauan dan Tanggapan Terhadap Ancaman:**

Proses pemantauan terus-menerus oleh manusia diperlukan untuk mendeteksi potensi ancaman dan serangan. Hal ini mencakup pemantauan log keamanan, analisis lalu lintas jaringan, dan pemeriksaan rutin.

Respon cepat terhadap serangan dan langkah-langkah perbaikan juga menjadi tanggung jawab manusia. Tim keamanan siber manusia harus siap untuk menanggapi insiden keamanan dengan cepat dan efisien.

5. **Kebijakan Keamanan dan Kepatuhan:**

Manusia berperan dalam merancang, mengimplementasikan, dan memastikan kepatuhan terhadap kebijakan keamanan. Ini mencakup pembuatan kebijakan keamanan yang sesuai dengan regulasi, serta memastikan bahwa semua pengguna memahami dan mematuhi kebijakan tersebut.

Audit keamanan oleh manusia membantu memastikan bahwa sistem dan praktik keamanan memenuhi standar dan regulasi yang berlaku.

6. **Pengembangan Kultur Keamanan:**

Membangun budaya keamanan di seluruh organisasi adalah peran manusia yang penting. Ini melibatkan pembentukan sikap dan perilaku yang mendukung praktik keamanan, sehingga keamanan menjadi tanggung jawab bersama.

Penyelenggaraan program insentif atau pengakuan bagi mereka yang berkontribusi pada keamanan juga dapat mendorong partisipasi dan kesadaran.

Dalam keseluruhan, peran manusia dalam keamanan sistem informasi tidak hanya terbatas pada teknis, tetapi juga melibatkan aspek-aspek perilaku, budaya, dan manajemen. Keberhasilan dalam memastikan keamanan sistem informasi bergantung pada kolaborasi antara teknologi dan keterlibatan manusia.

7. **Kesadaran dan Pendidikan Keamanan:**

Pemahaman Ancaman: Manusia harus memiliki pemahaman yang baik tentang berbagai ancaman keamanan, seperti serangan phishing, malware, dan serangan siber lainnya.

Pelatihan Kesadaran: Program pelatihan kesadaran keamanan dapat membantu meningkatkan pengetahuan dan kewaspadaan pengguna terhadap potensi risiko keamanan.

8. **Pengelolaan Identitas dan Otentikasi:**

Manajemen Kata Sandi: Manusia harus mengelola kata sandi secara aman dan mendorong pengguna untuk menggunakan kata sandi yang kuat.

Implementasi Otentikasi Ganda: Penerapan otentikasi ganda oleh manusia dapat meningkatkan lapisan keamanan dalam mengakses sistem.

BAB

12

Keamanan dalam Teknologi *Cloud Computing*

Nia Ekawati, S.Kom., M. SI

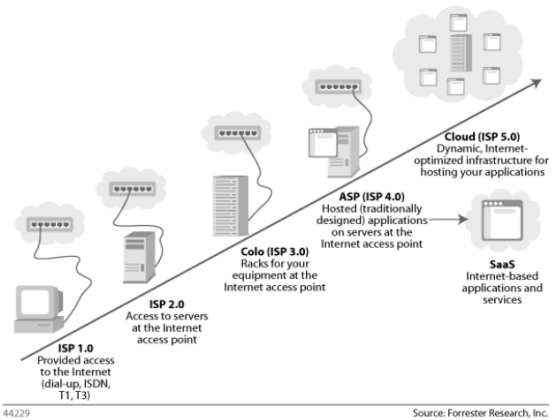
A. Teknologi Informasi

Pengertian teknologi informasi ada beberapa diungkapkan oleh para ahli. Salah satunya yang diungkapkan oleh Tata Sutarbi yakni teknologi informasi sebagai suatu teknologi yang digunakan untuk mengolah data, termasuk memproses, mendapatkan, menyusun,

menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu (Hodijah *et al.*, 2023).

Paparan diatas, merupakan pengertian dari salah satu ahli, jika dilihat dari praktiknya pada kehidupan sehari-hari kita sering melaluinya, seperti kegiatan memproses dapat dicontohkan penggunaan komputer, seorang pengguna memasukkan data pada suatu aplikasi dan selanjutnya dapat digunakan oleh pengguna lain, perpindahan data tersebut sebagai wujud proses komputerisasi berjalan dengan baik.

Sehingga teknologi informasi diimplementasikan dengan baik dalam kehidupan sehari-hari. Salah satu teknologi informasi yang sedang ramai digunakan oleh masyarakat saat ini adalah penyimpanan data secara *online* atau sebutan jargonnya adalah komputasi awan (*cloud computing*).



Gambar 1. Revolusi komputasi

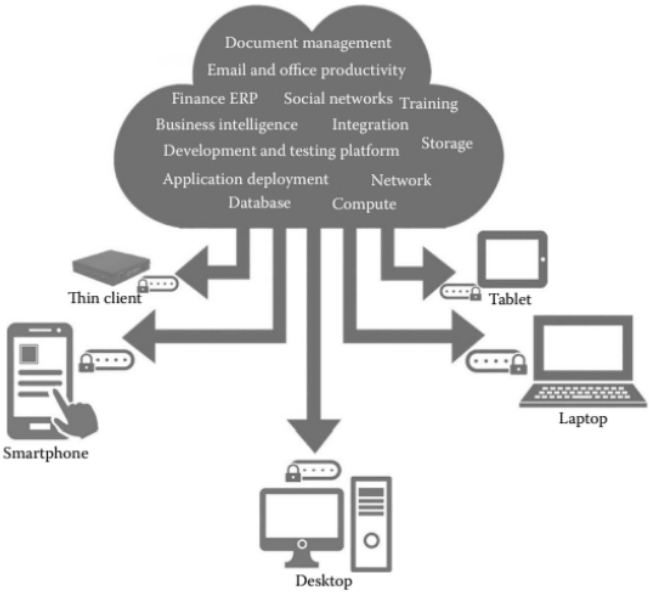
Gambar 1. bermula dari awal menawarkan konektivitas internet dasar untuk menegosiasikan perangkat lunak

sebagai proses ISP. ISP 1.0 merupakan seluruh menyiapkan internet akses ke pengguna, ISP 2.0 merupakan tahap ISP mulai leasing keluar rak dan *bandwith*. Maka dari itu, Perusahaan dapat *host server* mereka melaksanakan, *Line of Business* (LOB) aplikasi dapat diakses melampaui *web* dengan *karycloud*, mitra dagang dan pengguna. ISP 3.0 merupakan menegosiasikan aplikasi pada langganan yang berakibat *Application Service Provider* (ASP) lalu terbit *software* terbaru sebagai *Service Provider* (ASP) lalu terbit perangkat lunak terbaru sebagai *service* atau SaaS, ialah model ASP mendetail dan tindak logis untuk ISP hendak mencetuskan *cloud* (Mohidin, 2011).

B. Pengertian Cloud Computing

Fakta perancangan informasi/data lain serta terstruktunya rancangan tersebut untuk semua pengguna yang memerlukan secara cepat ketika diperlukan adalah intrepretasi ideal dan bentuk kerja dari istilah *cloud computing* (Santoso, 2023).

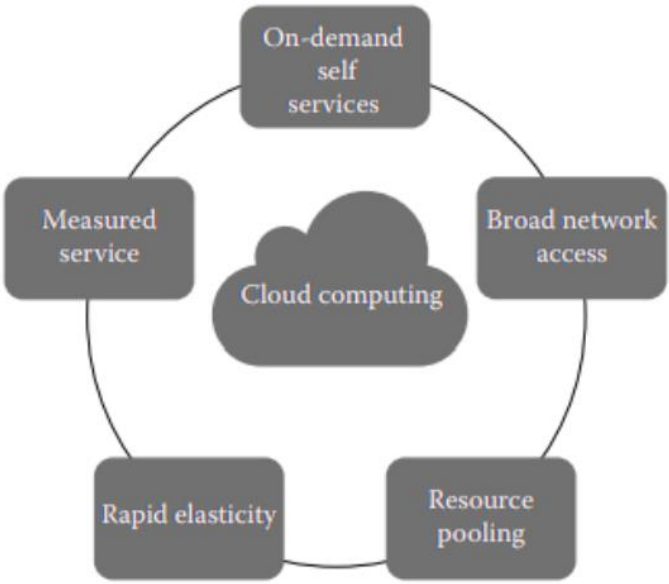
Komputasi awan atau sebutan lainnya adalah *cloud computing* yaitu bagian dari sebuah teknologi informasi dengan proses yang digunakan adalah perangkat keras serta perangkat jaringan komputer. Sebagai orang awam, tanpa disadari kita pengguna dari *cloud computing*, seperti penyimpanan data dalam suatu Perusahaan yang terpusat pada satu *platform*, penyimpanan data pada surat elektronik atau *e-mail*, dan pengiriman surat secara elektronik yang memiliki jejak digital.



Gambar 2. Komputasi awan

Tanpa kita pungkiri semua hal tersebut telah dijalani oleh sebagian pengguna diseluruh dunia. Seperti terlihat pada gambar diatas, *device* yang digunakan beragam dan mengakses dengan data yang sama atau berbeda pada satu platform penyedia dari *cloud computing* itu sendiri.

Bahasa sederhana *cloud computing* atau komputasi awan yakni mengarsip dan memfasilitasi data dan program melalui internet dari lokasi atau komputer yang jauh, tidak dari *hard drive* komputer kita (Santoso, 2023).



Gambar 3. Karakteristik komputasi awan

Komputasi awan mempunyai 5 (lima) karakteristik, diantaranya :

1. Layanan mandiri sesuai permintaan, setiap pengguna dapat melakukan akses sesuai permintaan yang diinginkan serta layanan yang disediakan sesuai kebutuhan pengguna pada suatu *platform*.
2. Akses jaringan yang luas, secara heterogen jaringan yang dimiliki sangat luas sehingga akses yang diproses mendorong pengguna tanpa batasan dari wilayah seluruh dunia.
3. Penyatuan sumber daya elastis, sumber daya yang dikelompokkan sesuai dengan kebutuhan pengguna dikumpulkan menjadi satu sehingga membentuk *multitenant*, guna memfasilitasi kebutuhan pengguna

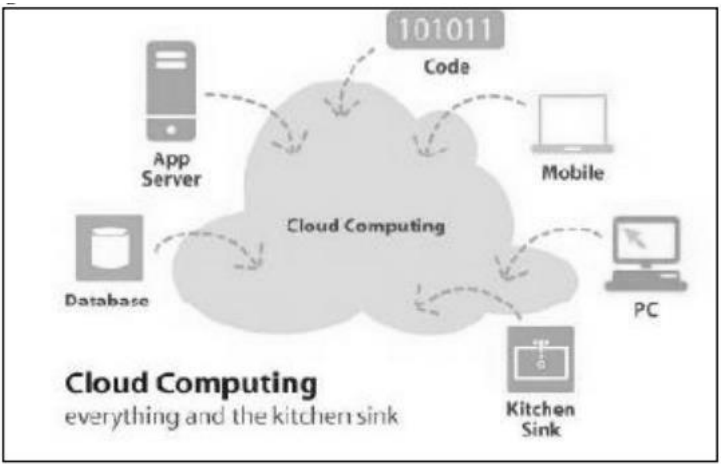
secara dinamis dan ada rasa *independent* sesuai lokasi pengguna tersebut.

4. Elastisitas yang cepat, penyedia menyediakan secara cepat dan elastis secara otomatis, supaya pengguna memiliki ketersediaan penyimpanan dengan cepat dan dapat membeli tanpa ada batasan.
5. Layanan terukur, misalnya penyimpanan, pemrosesan, *bandwidth* dan akun pengguna aktif. Hal-hal tersebut masuk dalam sistem *cloud* otomatis dan mengoptimalkan sumber daya dengan memanfaatkan kemampuan pengukuran pada beberapa tingkat abstraksi dengan jenis layanan.

C. Teknologi Cloud Computing

Teknologi *cloud computing* diartikan dalam bentuk sederhana dari sebuah Perusahaan terpusat yang mengadakan peminjaman *space storge*. Perusahaan tersebut hanya mempersiapkan infrastruktur sebagai tempat penyimpanan aplikasi dan data tentang suatu Perusahaan.

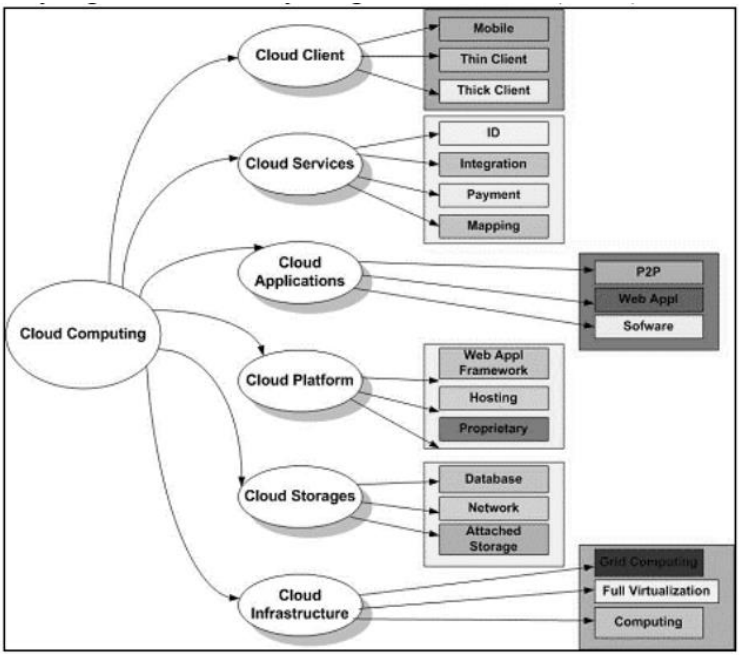
Menurut A. Rifai, (2010) memberikan penjelasan bahwa *cloud computing* adalah teknologi *on-demand*, yakni teknologi *cloud computing* bagian teknologi yang berlandaskan pada permintaan dari pengguna. Teknologi tersebut bagian dari salah satu fokus peralihan (*transition focus*), tidak hanya aplikasi perangkat lunak yang berlandaskan *cloud computing* hal ini juga meliputi *platform*, prasarana *database* maupun layanan dapat berlandaskan *cloud computing*.



Gambar 4. Paradigma dalam teknologi *cloud computing*

Cloud computing memiliki beberapa manfaat sebagai turbin dari teknologi informasi (Marks, 2010), yaitu:

1. Lebih efisien karena menggunakan anggaran yang rendah untuk sumber daya.
2. Membuat lebih *eglity*, dengan mudah dapat berorientasi pada profit dan perkembangan yang cepat.
3. Membuat operasional dan manajemen lebih mudah, dimungkinkan karena sistem pribadi atau Perusahaan yang terkoneksi dalam satu *cloud* dapat dimonitor dan diatur dengan mudah.
4. Menjadikan koloborasi yang terpercaya dan lebih ramping.
5. Membantu dalam menekan biaya operasional dan biaya modal pada saat *reliability* ditingkatkan dan kritikal sistem informasi yang dibangun.



Gambar 5. Struktur *cloud computing*

Layanan utama yang diadakan oleh *cloud computing* dipisahkan menjadi 3 (tiga) bagian (Balboni, 2009), yaitu:

1. IaaS (*Infrastructure as a Service*), keunggulan dalam mempersiapkan aksesibilitas perangkat keras kepada pengguna, diantaranya: *processing*, *storage*, *networks* dan *other fundamental computing resource*. Mencakup *operation system* dan implementasinya.
2. PaaS (*Platform as a Service*), keunggulan dala mempersiapkan layanan kepada pengguna untuk mengembangkan aplikasi yang menunjang pada infrastruktur *cloud computing*, sehingga aplikasi dapat beroperasi pada *platform* yang telah disiapkan menggunakan bahasa pemrograman.

3. SaaS (*Software as a Service*), keunggulan dalam mempersiapkan layanan difokuskan kepada pengguna untuk dapat mengoperasikan aplikasi di atas prasarana *cloud computing* yang telah disiapkan.

D. Keamanan Jaringan Informasi

Keamanan jaringan merupakan kegiatan yang dipakai dalam mengamankan jaringan komputer dari penggunaan atau serangan ilegal (Syamsu, Terisia and Masduki, 2023).

Keamanan informasi adalah bagian dari sumber yang dapat merubah Tingkat *reliability* sebuah jaringan (Putra and Toresa, 2021).

Keamanan jaringan informasi dalam *cloud computing* merupakan pembahasan sangat banyak. Keamanan jaringan informasi dalam *cloud computing*, spesifiknya berasal dari segi transmisi data (*secure transmition*). Ciri-ciri keamanan jaringan informasi dalam *cloud computing*, yaitu:

1. Struktur.
2. Metode transmisi.
3. *Transport formats*.
4. Perhitungan keamanan yang mendukung: *integrity*, *availability* dan *authentication* (bagi *private* dan *public* jaringan komunikasi).

Transmisi dalam *cloud computing* disebutkan aman apabila sudah dipastikan terdapat beberapa hal ini:

1. *Confidentiality*, menjamin: n*etwork security protocols*, *network authentication services* dan *data ecription services*.

2. Integrity, bagiannya yaitu: *firewall services*, *communications security management* dan *intrusion detection services*.
3. *Availability*, menjamin: *fault tolerance* untuk *availability* data (*backups*, *redundant disk system*), *acceptable logins and operating process performances* serta *reliable and interoperable security processes and network security mechanisms*.

BAB

13

Tantangan Keamanan dalam Penggunaan Perangkat Mobile

Etza Nofarita, ST., M.Kom.

Perkembangan teknologi di zaman sekarang ini memang maju sangat pesat dibandingkan dengan tahun-tahun sebelumnya yang merupakan sebuah transformasi dari teknologi masa dulu berubah menjadi teknologi yang canggih yang memberikan banyak kemudahan dan cepat.

Tidak dapat dipungkiri oleh semua pihak, bahwa kemajuan teknologi informasi sangat pesat dan diluar dugaan karena perkembangan teknologi informasi, implementasi internet, electronic commerce, dan lain sebagainya sudah menerobos batas-batas fisik antar negara. Perkembangan teknologi informasi sangat berbanding lurus dengan tingkat kebutuhan manusia. Dimana sebuah Teknologi informasi memiliki peranan yang sangat besar dalam penyebaran sebuah informasi yang valid dan akurat serta dapat membantu dalam pengambilan sebuah keputusan. Untuk itu diperlukan diperlukan teknologi informasi dalam pengolahan data.

Dengan perkembangan teknologi informasi berupa dalam hal ini perangkat mobile,adalah sebuah benda yang berteknologi tinggi, dan dapat bergerak tanpa menggunakan kabel seperti : Smartphone, PDA, Tablet, Laptop dimana memudahkan seorang pengguna untuk mengakses data dan informasi dimanapun dia berada. Namun dalam perjalanannya sistem ini masih membutuhkan sebuah konektivitas antara satu dengan yang lainnya yaitu hubungan antara perangkat lunak dan perangkat keras. Sehingga dalam hal ini memnculkan sesuatu hal yang baru yaitu jaringan internet. Dengan meluasnya jaringan internet dapat memudahkan seorang pengguna untuk mengakses data atau informasi tanpa perlu menyambungkan satu perangkat dengan perangkat lainnya. Perkembangan Teknologi Telekomunikasi yang sangat pesat dapat dilihat dengan pengguna internet di Indonesia yang semakin meningkat setiap tahunnya. Dengan penggunaan internet yang semakin tinggi maka diiringi dengan kejahatan internet yang semakin meningkat sehingga setiap orang harus memiliki kesadaran yang tinggi akan keamanan digital, karena

dalam dunia digital, data adalah aset yang penting yang harus dijaga keamanannya.

A. Keamanan Digital

Keamanan digital adalah perlindungan sistem digital, seperti komputer dan jaringan, dari penyadapan informasi, pencurian atau kerusakan pada perangkat keras, perangkat lunak atau data elektronik pengguna, serta dari gangguan atau penyesatan layana yang diberikan, Keamanan digital juga dapat disebut sebagai keamanan siber (cyber security) atau keamanan komputer (computer security)

Bidang keamanan digital sudah menjadi sangat penting di era yang serba digital dan memiliki kemajuan teknologi yang pesat seperti sekarang. Berbagai teknologi seperti sistem komputer, internet dan standar jaringan nirkabel seperti Bluetooth dan WI-FI serta pertumbuhan perangkat pintar, termasuk smarthphone, smart T dan berbagai perangkat yang membentuk internet of Thing (ioT) sangat bergantung pada keamanan digital.

Hampir seluruh komponen kehidupan yang ada di era sekarang, mulai dari individu, bisnis hingga pemerintahan, sangat membutuhkan keamanan digital yang canggih.

Semakin ramainya digitalisasi yang terjadi di lingkungan kita akan jelas membuat banyaknya para penjahat digital yang muncul untuk mengancam keamanannya. Oleh sebab itu, keamanan digital adalah hal yang diperhatikan supaya kita dapat melakukan pencegahan atas kejahatan digital.

Dalam era aplikasi digital, keamanan data menjadi sebuah isu krusial yang tidak boleh untuk diabaikan sehingga tantangan yang akan dihadapi dalam penggunaan perangkat mobile yaitu :

1. **Ancaman Malware dan Aplikasi Palsu**

   Aplikasi malware dan aplikasi palsu dapat menjadi sebuah resiko utama di platform aplikasi mobile. Dimana sering kali pengguna tidak menyadari bahwa data dapat diambil oleh sebuah aplikasi palsu atau dengan merusak perangkat mobile.

2. **Pelanggaran Privasi dan Pengumpulan Data yang berlebihan.**

   Aplikasi mobile sering kali dalam jumlah yang besar dalam mengumpulkan data pengguna. Sehingga untuk beberapa aplikasi kemungkinan ada menyalahgunakan data atau bahkan melakukan pelanggaran privasi yang berpotensi merugikan pengguna.

3. **Serangan Man-In-The-Middle (MITM)**

   Keterlibatan peretas dalam melakukan Serangan MITM untuk mencuri atau mengubah sebuah data saat adanya perpindahan antara perangkat dan server. Dan ini adalah merupakan suatu permasalahan yang memberikan sebuah risiko yang serius dalam transfer data di aplikasi mobile.

4. **Kurangnya Keamanan pada Proses Autentifikasi.**

   Kelemahan sistem autenfikasi atau kurangnya prosedur keamanan dapat memberikan kesempatan

bagi peretas untuk mendapatkan akses tidak sah ke akun pengguna.

B. Solusi dan Upaya Perlindungan

1. Implementasi Enkripsi Data

Untuk melindungi data selama proses transmisi dapat digunakan Enkripsi end-to-end. Ini adalah sebuah langkah untuk memastikan bahwa bahkan jika data diretas,maka peretas tidak dapat membacanya karena data terenkripsi.

2. Verifikasi Identitas yang Kuat

Penerapan metode autentifikasi yang kuat, seperti verifikasi dua fakto (2FA), memberikan kesulitan yang sangat berarti bagi peretas untuk mendapatkan akses tidak sah ke akun pengguna.

3. Pemantauan Aktivitas Aplikasi

Pemantauan aktifitas aplikasi bertujuan dapat membantu mendeteksi perilaku atau aktivitas anormal yang mencurigakan yang mengindikasikan sebuah serangan atau penyalahgunaan data.

4. Kebijakan Privasi yang jelas

Sebuah Aplikasi diharuskan menyediakan sebuah kebijakan privasi yang jelas dan transparan kepada pengguna, diharapkan untuk membangun sebuah kepercayaan dan memungkinkan pengguna membuat keputusan yang informasional tentang penggunaan data mereka.

5. **Pembaharuan Rutin dan Keamanan**

   Penerapan pembaruan perangkat lunak secara rutin dan berkala dapat membantu mengatasi kerentanan keamanan yang mungkin telah diidentifikasi dan diatasi oleh pengembang.

6. **Uji Keamanan Aplikasi (Penetration Testing)**

   Melakukan pengujian keamanan secara rutin dan berkala dapat membantu mengidentifikasi celah keamanan potensial sebelum peretas dapat memanfaatkannya.

Keamanan data dalam aplikasi mobile memerlukan perhatian serius dan upaya proaktif. Dengan menerapkan solusi keamanan yang canggih dan mendidik pengguna tentang praktik keamanan. Kita dapat menciptakan lingkungan aplikasi yang lebih aman dan terpercaya. Dalam era dimana aplikasi mobile menjadi bagian integral dari kehidupan sehari-hari. Menjaga keamanan data bukanlah pilihan melainkan suatu keharusan. Dengan terus berupaya dan berinovasi dalam bidang keamanan, kita dapat menghadapi tantangan dan menjaga data pengguna tetap aman di dunia aplikasi yang terus berkembang

BAB

14

Manajemen Risiko Kemanan Sistem Informasi

Dr. Ir. Iwan Setiawan, MT.

A. Manajemen Risiko Keamanan Informasi

1. Risiko

   Resiko adalah hasil negatif dari suatu kegiatan dengan probabilitas yang berbeda untuk setiap kegiatan. Resiko suatu kegiatan pada dasarnya tidak

dapat dihilangkan, tetapi dampaknya terhadap hasilnya dapat diperkecil. Manajemen resiko adalah proses menganalisa serta memperkirakan kemungkinan adanya risiko dalam suatu kegiatan. Meskipun demikian, resiko yang ditetapkan sebelum kegiatan tidak selalu muncul, dan terkadang muncul resiko baru di luar resiko yang telah ditetapkan. Akibatnya, risiko juga terkait dengan ketidakpastian. Jadi, ada resiko yang sudah diketahui di awal, dan resiko yang belum diketahui di awal muncul saat kegiatan sudah berjalan.

2. Manajemen Risiko

Kegiatan dalam mengidentifikasi atau menganalisis resiko yang akan muncul; mengurangi, mencegah, atau mengupayakan berbagai tindakan pencegahan untuk mengurangi dampak negatif dari resiko yang ada dan terakhir, melakukan evaluasi terhadap resiko yang muncul dan dampak mereka. Itulah yangn di sebut dengan Manajemen Risiko.

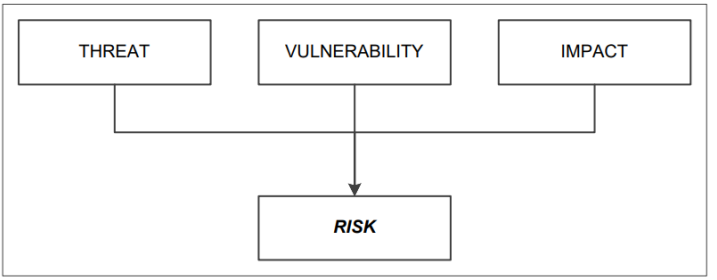
Menurut pemahaman di atas, manajemen resiko adalah kumpulan prosedur yang harus dilakukan selama siklus proyek untuk menangani potensi risiko. Oleh karena itu, kita tidak dapat melihat manajemen resiko sebagai produk yang siap digunakan dan mengabaikan prosedur yang digunakan selama proyek dan setelah proyek selesai.

3. Risiko Sistem Informasi

Komponen kejadian yang terdiri dari ancaman (ancaman), kelemahan (kelemahan), dan dampak (dampak) dikenal sebagai risiko (resiko). Kelemahan

sistem dapat dianggap sebagai kelemahan, yang dapat dimanfaatkan oleh pihak lain untuk menguasai sistem. Sedangkan dampak adalah penilaian dampak ancaman yang dilakukan terhadap aset dan tujuan organisasi dengan memanfaatkan kelemahan sistem.

.



Gambar 1. Kombinasi Komponen berkaitan dengan Risiko

Saat melakukan analisis resiko, hal-hal berikut harus dipertimbangkan:

a. Kerugian pendapatan
b. Kerugian modal
c. Kerugian reputasi di pasar
d. Kehilangan kesempatan bisnis
e. Kerugian di pasar modal
f. Kehilangan kepercayaan pelanggan, karyawan, dan pemegang saham
g. Melanggar peraturan dan peraturan
h. Kehancuran reputasi organisasi.

Menurut sumber lain, aset, risiko, dan ancaman adalah tiga elemen yang memberikan kontribusi kepada risiko. Beberapa faktor yang dapat

berkontribusi pada resiko dari ketiga elemen tersebut ditunjukkan dalam tabel 1 di bawah ini.

Table 1. Kontribusi Terdap resiko dari Komponen Asset, Vulnerabilities, dan Threats.

Komponen	Contoh Resiko
Asset	hardware software dokumentasi data komunikasi linkungan manusia
Vulnerabilities	pemakai (*users*) teroris kecelakaan (*accidents*) *crackers* penjahat kriminal nasib (*acts of God*) intel luar negeri (*foreign intelligence*)
Threats	*software bugs* *hardware bugs* radiasi (dari layar, transmisi) *tapping, crosstalk* *unauthorized users* cetakan, hardcopy atau print out keteledoran (*oversight*) *cracker* via telepon storage media

"Countermeasures" digunakan untuk mengatasi risiko tersebut, yang terdiri dari:

a. Usaha untuk mengurangi ancaman,
b. Usaha untuk melindungi,
c. Usaha untuk mengurangi dampak,
d. Mendeteksi kejadian yang tidak bersahabat, dan
e. Kembali dari kejadian.

Beberapa contoh resiko dalam proyek teknologi informasi berdasarkan tipe ketidakpastian resiko:

a. Known

Contohnya, pihak yang mengadakan proyek teknologi informasi yang akan menggunakan hasilnya kadangkala lambat dan sulit mendapatkan data dan informasi yang dibutuhkan. Ini sudah terbiasa dan merupakan resiko yang dapat diantisipasi sebelum proyek dimulai. Jadi, selama tahap kontrak proyek, pihak yang menangani proyek teknologi informasi harus memahami bahwa penyedia data dan informasi harus selalu memenuhi permintaan agar proyek berjalan lancar.

b. Known-Unknown

Contoh: Ketika proyek teknologi informasi, khususnya proyek yang menghasilkan perangkat lunak, berjalan, terkadang terjadi masalah dengan antarmuka sistem yang telah dibangun. Ketika antarmuka sistem dirancang untuk memenuhi permintaan pengguna, terkadang hasilnya tidak sesuai dengan keinginan pengguna. Ini adalah risiko yang dapat diketahui dan tidak diketahui.

c. Unknown

Contoh: Dalam proyek pembangunan teknologi informasi pembangunan perangkat lunak, kesalahan pada tahapan implementasi pemrograman adalah jenis kesalahan yang tidak diketahui yang berasal dari komponen pemrograman yang dibangun oleh pihak programmer.

B. Manajemen Resiko Sistem Informasi

Manajemen resiko sistem informasi merupakan cikal bakal pembuatan kebijakan keamanan sistem informasi pada setiap organisasi. Sebelum membuat kebijakan keamanan sistem informasi, sangat penting untuk memahami dan mengidentifikasi sumber daya yang dimiliki oleh organisasi sehingga dapat membedakan sumber daya mana yang harus dilindungi dan menetapkan skala prioritas pada setiap sumber daya tersebut. Hal ini sangat penting karena berkaitan dengan biaya. Manajemen resiko sistem informasi melibatkan penentuang:

1. Apa yang harus diproteksi dan dikontrol oleh organisasi.
2. Apa yang dibutuhkan untuk memproteksinya.
3. Bagaimana cara memproteksi dan mengontrolnya.
4. Menentukan skala prioritas.

Tujuan utama pada saat kegiatan manajeman resiko sistem informasi adalah mengidentifikasikan proteksi dan kontrol terhadap informasi. Dimana nantinya tujuan utama dari proteksi terhadap informasi adalah menciptakan lingkungan yang aman dan terjamin bagi manajemen untuk melakukan tugasnya.

Manajemen resiko proyek juga dapat mengubah resiko menjadi kesempatan yang menguntungkan. Hal tersebut dapat terjadi apabila kita memiliki langkah yang strategis dalam menanggulangi resiko yang muncul pada saat pelaksanaan proyek. Untuk dapat memudahkan pemahaman dari tujuan tersebut kita lihat dari contoh resiko yang muncul pada proyek teknologi informasi. Misalkan kita dalam pelaksanaan proyek teknologi

informasi terkendala dengan pengadaan server yang terlalu rumit dan memerlukan biaya yang sangat tinggi. Resiko tersebut diketahui setelah proyek berlangsung, sedangkan teknologi dan biaya yang tersedia tidak memungkinkan untuk menanggulangi resiko tersebut. Dalam artian kita akan mengalami kerugian dari segi keuangan apabila kita membangun server tersebut. Sebetulnya ada cara penanggulangan resiko tersebut. Kita dapat mengubah resiko yang menjadi ancaman tersebut menjadi sebuah kesempatan yang menguntungkan. Penanggulangannya yaitu dengan cara kita tidak perlu membangun server tersebut melainkan menyewa server yang disediakan oleh konsultan teknologi informasi. Dengan hal tersebut kita dapat menghemat biaya yang tersedia. Untuk biaya penyewaannya kita dapat alokasikan sebagai biaya pemeliharaan dan hasilnya kita sebagai pihak pelaksana proyek akan lebih diuntungkan.

C. Penilaian Risiko Keamanan Informasi

Menurut Whitman dan Mattord (2006) dalam menggunakan sebuah framework manajemen risiko, ada beberapa hal yang harus diperhatikan:

1. Risiko dan dampak sebaiknya dipandang secara keseluruhan dari sudut pandang perspektif bisnis.
2. Risiko berpengaruh secara signifikan jika memiliki dampak terhadap bisnis.
3. Framework yang akan digunakan haruslah menyediakan bentuk dasar untuk melakukan evaluasi segala macam risiko, mulai dari insiden keamanan

informasi yang besifat kecil hingga yang berpotensi bencana

Menurut Jones dan Ashenden (2005) terdapat formula untuk mengukur risiko yaitu:

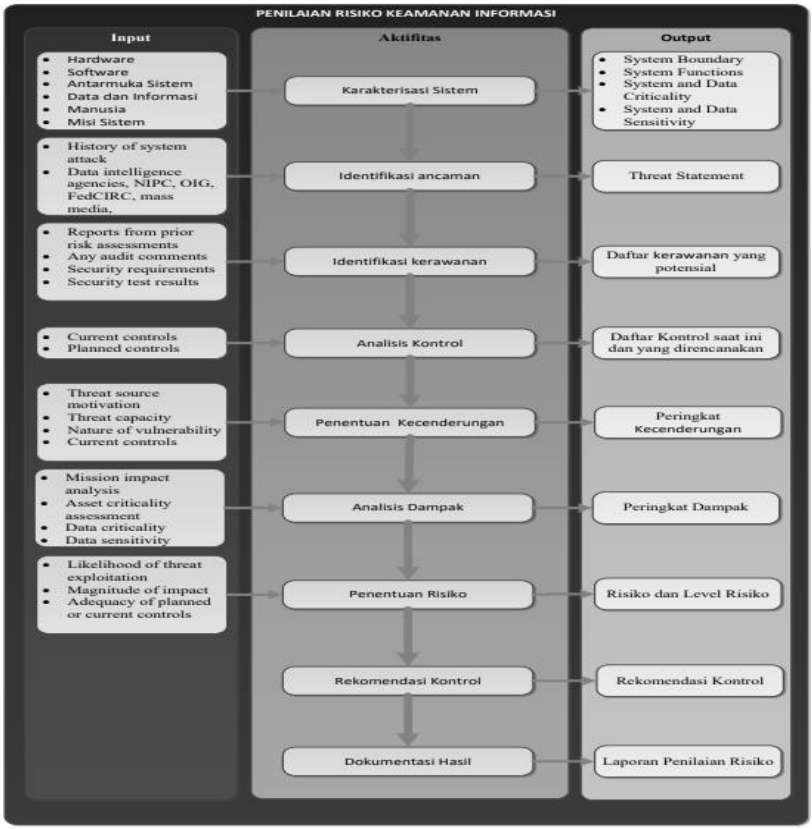
Risiko = Threat x Vulnerability x Impact

Maksud pernyataan dari formula diatas adalah threat akan melakukan eksploitasi vulnerability sehingga dapat menyebabkan impact terhadap sistem, sehingga menjadikan hal tersebut sebagai risiko terhadap organisasi. Oleh karena itu jika tidak ditemukan threat, vulnerability dan impact maka tidak terdapat risiko.

NIST 800-30 adalah dokumen standar yang dikembangkan oleh National Institute of Standards and Technology yang mana merupakan kelanjutan dari tanggung jawab hukum di bawah undangundang Computer Security Act tahun 1987 dan the Information Technology Management Reform Act tahun 1996. NIST 800-30 terdapat dua tahap penting yaitu penilaian risiko dan mitigasi risiko. Tahapan penilaian risiko berdasarkan NIST 800-30 yaitu (Syalim, Hori, dan Sakurai, 2009):

1. *System Characterization* Pada tahapan ini, batas-batas dari sistem TI harus diidentifikasi, termasuk didalamnya sumber daya dan informasi.
2. *Threat Identification* Pertimbangan atas kemungkinan untuk muncul ancaman seperti sumber, potensi kerawanan dan kontrol yang ada.
3. *Vulnerability Identification* Identifikasi terhadap kerawanan digunakan untuk pengembangan dari daftar kerawanan sistem yang dapat dimanfaatkan nantinya.

4. *Control Analysis* Analisis terhadap kontrol yang telah dilaksanakan atau direncanakan untuk implementasi oleh organisasi untuk minimalisir atau menghilangkan kemungkinankemungkinan pengembangan dari ancaman.
5. *Likelihood Determination* Proses rangking terhadap potensi dari kerawanandapat dilaksanakan dalam lingkungan dari kerawanan tersebut. Faktor yang menjadi pertimbangan adalah ancaman (sumber dan kemampuan), sifat dari kerawanan serta keberadaan dan efektifitas kontrol jika diterapkan.
6. *Impact Analysis* Tahapan ini digunakan untuk menentukan dampak negatif yang dihasilkan dari keberhasilan penerapan kerawanan.
7. *Risk Determination* Penilaian tingkat risiko pada sistem teknologi informasi dilakukan pada langkah ini.
8. *Control Recommendations* Tahapan ini menilai kontrol yang mana dapat mengurangi atau menghilangkan risiko yang telah teridentifikasi. kontrol yang direkomendasikan sebaiknya harus dapat mengurangi tingkat risiko pada sistem teknologi informasi dan data, kepada tingkat risiko yang dapat diterima.
9. *Results Documentation* Pada tahap ini, dilakukan pengembangan laporan hasil penilaian risiko (sumber ancaman, kerawanan, risiko yang dinilai dan kontrol yang direkomendasikan).



Gambar 2. Penilaian Risiko NIST SP 800-30

D. Persepsi Risiko

Risiko adalah kombinasi dari probabilitas suatu peristiwa dan penyebabnya ketika setidaknya ada kemungkinan konsekuensi negatif. Risiko yang dirasakan semata-mata adalah ketidakpastian yang dihadapi konsumen ketika ia tidak mampu memperkirakan konsekuensi keputusan pembeliannya secara umum. Risiko

yang dirasakan muncul ketika konsumen tidak yakin tentang kemajuan tindakan pembelanjaannya.

menjelaskan dalam konteks pemasaran mendefinisikan risiko yang dirasakan sebagai sifat dan jumlah risiko yang dirasakan oleh konsumen dalam merenungkan tindakan tertentu. Dimensi risiko yang dirasakan didefinisikan oleh sejumlah peneliti. Enam jenis risiko sebagaimana disajikan pada Tabel 1 berikut:

Tabel 1. Jenis Risiko

Jenis-jenis risiko yang dipersepsikan	Definisi
Risiko kinerja	adalah probabilitas bahwa produk akan mengalami kegagalan fungsi dan tidak beroperasi sebagaimana mestinya dirancang dan diiklankan
Risiko sosial	menggambarkan ketakutan bahwa suatu produk atau layanan akan menyebabkan hilangnya status dalam kelompok sosial seseorang
Risiko keuangan	mengacu pada probabilitas bahwa pembelian akan menghasilkan kerugian moneter
Risiko psikologis	kemungkinan bahwa penggunaan suatu produk akan mengakibatkan tidak konsis-tennya citra diri pelanggan.
Risiko waktu	kemungkinan bahwa pembelian mengaki-batkan hilangnya waktu ketika membuat keputusan pembelian yang buruk dengan membuang-buang waktu meneliti dan melakukan pembelian.
Risiko fisik	kemungkinan bahwa produk atau layanan yang dibeli akan menimbulkan ancaman bagi kesehatan dan keselamatan manusia.

Jumlah total risiko yang dirasakan mungkin konstan sedangkan tingkat jenis risiko yang dirasakan bervariasi dengan unsur-unsur situasi (Predmore et al., 2007) (Persamaan 1):

Total Risiko yang Dirasakan = Σ risiko = evaluasi fungsional + fisik + keuangan + sosial + psikologis + waktu.

Technology Acceptance Model (TAM) adalah model yang dibenarkan secara teoretis, berdasarkan teori reasoned action (TRA), dimaksudkan untuk menguji dan menjelaskan adopsi teknologi informasi yang mengusulkan bahwa sikap terhadap penggunaan sistem dipengaruhi oleh dua penentu kritis keyakinan pengguna: satu dianggap kegunaan dan yang lainnya dirasakan kemudahan penggunaan. TAM menyatakan bahwa penggunaan (perilaku aktual) TI ditentukan oleh niat individu untuk menggunakan teknologi dan bahwa niat seseorang ditentukan oleh sikap seseorang, serta kegunaan yang dirasakan dan kemudahan penggunaan dan berkaitan dengan niat dan akhirnya dengan perilaku (suatu peningkatan manfaat yang dirasakan mengarah pada niat yang lebih besar untuk digunakan). Persepsi kegunaan (PK), didefinisikan sebagai sejauh mana pengguna secara subyektif percaya bahwa penggunaan teknologi atau sistem baru akan bermanfaat atau akan meningkatkan kinerjanya. Persepsi kemudahan penggunaan, didefinisikan sebagai tingkat di mana seseorang percaya bahwa menggunakan teknologi atau sistem akan mudah.

E. Deskripsi Tingkat Risiko

Menggambarkan tingkat risiko yang ditunjukkan pada matriks di atas. skala risiko ini, dengan penilaian yang high, medium, low dan menjelaskan derajat atau tingkat risiko berdasarkan status stoplight pada sistem praktek keamanan penggunaan TI dapat dilihat pada tabel 2., serta fasilitas atau prosedur mungkin terkena jika kerentanan yang diberikan telah dieksekusi. Skala risiko juga menyajikan tindakan yang pihak manajemen, pemilik misi, harus mengambil risiko untuk setiap tingkat.

Table 2. Deskripsi Tingkat Risiko

Nilai Dampak	Tingkat Level	Deskripsi Risiko dan Tindakan Diperlukan
4-5	TINGGI (High)	Jika observasi atau temuan dianggap memiliki risiko tinggi, ada kebutuhan yang kuat untuk perbaikan. Meskipun sistem yang ada masih dapat digunakan, persiapan untuk memperbaikinya harus dimulai segera.
2 - 3	SEDANG (Medium)	Jika pengamatan dianggap memiliki risiko menengah, tindakan korektif harus diambil

		dan rencana harus disiapkan untuk melakukannya segera.
1	**RENDAH (Low)**	Jika pengamatan dianggap memiliki risiko rendah, perlu diputuskan apakah tindakan perbaikan masih diperlukan atau apakah harus menerima risiko.

Tabel 3. Status Stioplight

Tingkat Level	Status Stoplight	Definisi Kemungkinan /Kecendrungan
4-5	Green	Sumber ancaman yang sangat termotivasi, mampu, dan dapat mengendalikan kerentanan yang mungkin terjadi tidak efektif.
2 - 3	Yellow	Meskipun sumber ancaman ingin dan

		mampu, pengendalian saat ini dapat menghentikan kerentanan.
1	**Red**	Pengendalian yang ada tidak cukup untuk mencegah atau secara signifikan menghambat kerentanan yang mungkin terjadi, atau sumber ancaman kurang termotivasi dan mampu.

Probabilitas terkait penyebab risiko bahwa ancaman yang disebabkan oleh ancaman akan terjadi terhadap kerentanan. Penyebab risiko adalah kondisi dari elemen, komponen, atau tujuan aktivitas. Tabel 3 berisi tingkat kemungkinan.

Tabel 4.Level Probabilitas

Level	Nilai Probabilitas
1	Tidak Terjadi (<20%)
2 - 3	Jarang (20% - 80%)
4 - 5	Terjadi (> 80%)

langkah selanjutnya menentukan status stoplight pada area tersebut. Matriks status stoplight seperti yang dijelaskan pada Tabel 5.

Tabel 5. Status Stoplight

Kecenderungan	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Medium	Medium	High	High
	2	Low	Medium	Medium	Medium	High
	1	Low	Low	Medium	Medium	High
		1	2	3	4	5
DAMPAK						

F. Ancaman Keamanan Informasi

Empat sumber yang dapat mengancam sistem informasi menurut metode OCTAVE, yaitu: 1. Tindakan sengaja oleh manusia (tindakan sengaja oleh manusia) baik dari dalam maupun dari luar (dalam). 2. Tindakan tidak sengaja oleh manusia (tindakan tidak sengaja oleh manusia) baik dari dalam maupun dari luar (dalam). 3. Sistem yang bermasalah (sistem ploblem), yang terdiri dari hardware dan software yang tidak berfungsi dengan baik dan tidak berfungsi dengan baik (Albert dkk, 2005).

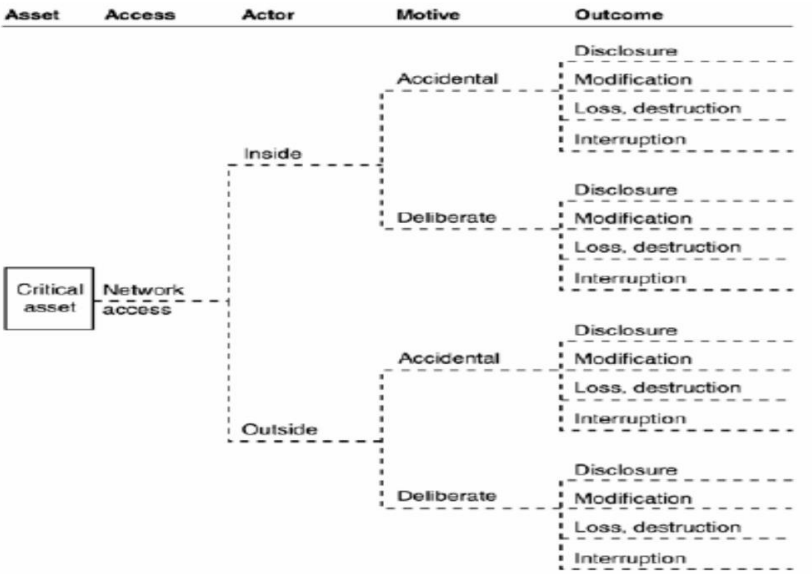
Dari ancaman memberikan hasil pengaruh (outcomes) serangan terhadap aset-aset yakni:

1. Disclosure: dapat terungkapnya informasi-informasi yang sensitive.
2. Modification: berubahnya informasi yang dilakukan oleh orang yang tidak berhak.
3. Destructive and lost: kerusakkan dan hilangnya informasi yang sensitif.
4. Interuption: gangguan akses terhadap informasi yang dibutuhkan.

Gambar 3. Hubungan sumber ancaman dan pengaruhnya terhadap asset

Untuk memudahkan pemetaan sumber ancaman dan dampaknya, kondisi digambarkan dalam diagram pohon metode OCTAVE seperti di bawah ini. Di mana properti ancaman terdiri dari aset, akses (cara mendapatkan informasi), aktor (pelaku dalam dan luar), motif (alasan mengapa orang mendapatkan informasi secara sengaja atau

tidak sengaja) dan hasil (pengungkapan, perubahan, perusakkan, dan penghilangan informasi).



Gambar 4. Diagram pohom profil Ancaman

G. Sumber Daya Sistem Informasi

Secara lebih khusus, tujuan organisasi tidak dipengaruhi oleh sumber daya sistem informasi. Solusi Informasi (SI) membantu organisasi menjalankan operasi, yang berdampak pada tujuan dan strategi perusahaan. Dengan membuat organisasi mampu mencapai keunggulan kompetitifnya dan mencapai targetnya, nilai SI mendukung nilai bisnis. Pandangan tentang nilai sistem informasi (SI) dibandingkan dengan nilai bisnis organisasi tidak lagi bersifat parsial. Sekarang dianggap sebagai sumber daya, SI

tidak lagi dipandang sebagai alat yang terpisah dari organisasi. Sebaliknya, dianggap sebagai salah satu sumber daya, dengan peran yang sama dengan sumber daya lain, seperti aset, keuangan, dan tenaga kerja manusia.

Seperti yang dijelaskan sebagai berikut:

1. Aplikasi *(application)*, merupakan suatu sarana atau tool yang digunakan untuk mengolah dan menyimpulkan atau meringkas, baik prosedur manual maupun yang terprogram.
2. Informasi (*information*), adalah data-data yang telah diolah untuk kepentingan manajemen dalam membantu mengambil keputusan dalam menjalankan roda bisnisnya. Data-data terdiri objek-objek dalam pengertian yang lebih luas (yakni internal dan eksternal), terstruktur dan tidak terstruktur, grafik suara dan sebagainya.
3. Infrastruktur (*infrastructure*), mencakup hardware, software, sistem operasi, sistem manajemen database, jaringan (networking), multimedia, dan fasilitas-fasilitas lainnya.
4. Sumber Daya Manusia/SDM (*people*), merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi. Kesadaran dan produktivitasnya dibutuhkan untuk merencanakan, mengorganisasikan, melaksanakan, memperoleh, menyampaikan, mendukung, dan memantau layanan SI perusahaan

H. Kelemahan Keamanan Sistem Informasi

Kelemahan atau kekurangan sistem dapat terjadi selama proses desain, penetapan prosedur, dan implementasi. Kelemahan ini dapat menyebabkan pelanggaran oleh individu yang mencoba memasuki sistem. Orang-orang yang tidak bertanggung jawab memanfaatkan kelemahan ini, seperti gangguan atau serangan:

1. *Confidentiality* (kerahasiaan) elemen yang menjaga kerahasiaan data atau informasi, memastikan bahwa hanya orang yang berwenang yang dapat melihat informasi, dan menjamin kerahasiaan data yang dikirim, diterima, dan disimpan.
2. *Integrity* (integritas) Keakuratan dan integritas data harus dipertahankan dengan memastikan bahwa data tidak diubah tanpa ijin pihak yang berwenang.
3. *Availability* (ketersediaan) aspek yang memastikan bahwa data dapat diakses saat dibutuhkan dan bahwa orang yang berhak dapat menggunakan informasi dan perangkat yang terkait saat diperlukan. Serangan terhadap sumber informasi, baik secara fisik maupun melalui akses jaringan, adalah salah satu dari tiga elemen keamanan yang paling rentan terhadap ancaman serangan.

I. Metode Penilaian Risiko

Metode penilaian resiko terdiri dari :

1. Kualitatif

   Melakukan pengukuran dampak relatif atas suatu kejadian dan cenderung lebih fokus pada aspek-aspek

strategis dan politis dalam menghindari atau mengurangi dampak negative atas suatu risiko

2. Kuantitatif

   Penilaian risiko dengan membandingkan rentang antara hasil nyata dengan dampak risiko yang mungkin timbul, mellaui pengujian data historis, trend, dan laporan hasil kinerja yang lebih terukur.

3. Gabungan

   Kombinasi antara dampak nyata dengan seluruh risiko yang dibandingkan dengan cakupan kegiatan, biaya dan jadwal pelaksanaan. Penilaian risiko yang komprehensif merupakan kombinasi antara metode penilaian kualitatif dan kuantitatif.

   Sedangkan dalam melakukan proses pengukuran risiko keamanan sistem informasi dibutuhkan metode yang dapat dijadikan pedoman. Berikut adalah beberapa metode yang tersedia dalam melakukan pengukuran risiko keamanan sistem informasi.

   a. Metode OCTAVE

      Metode OCTAVE, yang berasal dari teknik perencanaan dan risiko, digunakan untuk strategi dan perencanaan risiko keamanan informasi. OCTAVE berfokus pada risiko organisasi, hasil praktik, dan strategi yang saling terkait. Dengan OCTAVE, tim kecil audit operasional (atau bisnis) dan teknologi informasi bekerja sama untuk menunjukkan kebutuhan keamanan organisasi dengan menyeimbangkan tiga aspek utama: risiko operasional, praktik pengamanan, dan teknologi.

Terdapat tiga jenis metode OCTAVE yaitu:

1) Metode original OCTAVE digunakan untuk membentuk dasar pengetahuan OCTAVE.
2) Metode OCTAVE Allegro, digunakan dalam pendekatan efektif untuk keamanan informasi dan jaminan.
3) Metode OCTAVE-S digunakan pada organisasi-organisasi yang lebih kecil.

Kriteria OCTAVE, pendekatan umum untuk penghilang risiko dan pelatihan berbasis evaluasi keamanan informasi, menetapkan prinsip dasar dan karakteristik manajemen risiko yang digunakan dalam metode OCTAVE.

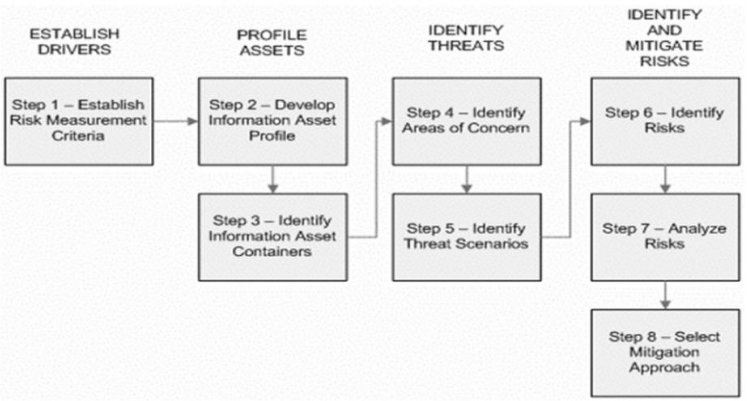
Sarana dan keuntungan metode-metode OCTAVE adalah:

1) *Self-directed* yaitu sekolompok anggota organisasi dalam unit-unit bisnis yang bekerja bersama dengan divisi IT untuk mengidentifikasi kebutuhan keamanan dari organisasi.
2) *Flexible* yaitu setiap metode dapat diterapkan pada sasaran, keamanan dan lingkungan risiko perusahaan di berbagai level.
3) *Evolved* yaitu OCTAVE menjalankan operasi berbasis risiko perusahaan pada sisi keamanan dan menempatkan teknolgi di bidang bisnis.

b. Metode OCTAVE Allegro

OCTAVE Allegro adalah metode yang disederhanakan yang berfokus pada aset informasi dan dapat dilaksanakan dengan metode workshop style dan

kolaboratif. OCTAVE Allegro terdiri dari delapan langkah yang dibagi dalam empat fase.



Gambar 5. Fase Metode OCTAVE Allegro

1. Langkah 1, Membangun Kriteria Pengukuran Risiko: Ini terdiri dari dua tindakan. Pertama, membangun penggerak organisasi digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan perusahaan, serta menentukan dampak area yang paling signifikan.
2. Langkah 2 mengembangkan profil aset informasi terdiri dari delapan aktivitas, dimulai dengan identifikasi aset informasi dan melakukan penilaian risiko terstruktur pada aset yang penting. Langkah 3 dan 4 mengumpulkan informasi tentang ukuran kualitatif yang didokumentasikan pada worksheets criteria penilaian risiko. Langkah 4 memberikan nilai prioritas impact area dengan menggunakan worksheets ranking impact area.
3. Langkah 3, Mengidentifikasi Kontainer Aset Informasi: Hanya ada satu aktivitas yang dilakukan di langkah ini. Aktivitas ini membahas tiga masalah utama terkait

keamanan dan kontainer aset informasi: cara aset informasi dilindungi, tingkat perlindungan atau pengaman aset informasi, dan kerentanan dan ancaman terhadap kontainer aset informasi.

4. Langkah 4, Mengidentifikasi Area Masalah: Aktivitas di langkah ini dimulai dengan pembuatan profil risiko untuk setiap aset informasi. Dimungkinkan untuk mencatat area yang menjadi perhatian dengan mengacu pada peta risiko aset informasi dan lembar kerja risiko aset informasi. Untuk melakukan ini, lakukan review kontainer dan catat setiap area yang menjadi perhatian dengan mengacu pada lembar kerja risiko aset informasi.
5. Langkah 5, Mengidentifikasi Skenario Ancaman: Aktivitas satu di langkah lima memungkinkan untuk mengidentifikasi skenario ancaman tambahan pada aktivitas ini. Ini dapat dilakukan dengan menggunakan skenario ancaman yang termasuk dalam survei appendix c. Semua worksheets tentang risiko aset informasi dilengkapi untuk setiap scenario ancaman yang umum.
6. Langkah 6, aktivitas satu untuk mengidentifikasi risiko menentukan apakah scenario ancaman yang telah dicatat dalam lembar kerja risiko aset dapat berdampak pada organisasi.
7. Langkah 7, Menganalisis Risiko Aktivitas harus dilakukan, yang berkaitan dengan dokumentasi yang ada pada lembar kerja risiko aset informasi. Langkah satu dimulai dengan meninjau kriteria pengukuran risiko, dan langkah kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko

dan menentukan strategi terbaik untuk menangani risiko.

8. Langkah 8, Memilih Pendekatan Pengurangan Aktivitas 1. Pada langkah delapan, pendekatan pengurangan aktivitas satu adalah menghitung nilai risiko relatif. Ini dilakukan untuk membantu dalam pengambilan keputusan tentang status mitigasi risiko. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko sesuai dengan keadaan unik organisasi.

J. Raci Chart

RACI adalah akronim untuk membantu menjelaskan peran proyek dan mencari tahu pihak yang bertanggung jawab atas tugas yang diberikan. Baik Anda belum pernah mendengar RACI atau mempertimbangkan membuat bagan RACI untuk proyek teknologi informasi selanjutnya,

RACI, yang merupakan singkatan dari tanggung jawab, bertanggung jawab, dikonsultasikan, dan diberitahu, digunakan untuk menunjukkan peran dan tanggung jawab suatu fungsi dalam organisasi terhadap suatu aktivitas tertentu dalam rangka untuk mencapai tujuan pengendalian teknologi informasi. RACI diterapkan pada setiap aktivitas dalam tujuan pengendalian teknologi informasi untuk mendukung kesuksesan proses IT pada keempat domain. Peran dan tanggung jawab adalah dua hal yang sangat berkaitan dengan proses pembuatan keputusan. Keputusan dapat dibuat oleh pihak-pihak yang memang memiliki kewenangan sebagai pembuat keputusan. Untuk membuat aktivitas lebih jelas, peran dan tanggung jawab ini

diberikan. Daftar RACI mendefinisikan apa dan kepada siapa yang harus diberikan, termasuk:

a. R = Responsible, artinya pihak yang harus memastikan aktivitas tersebut berhasil dilaksanakan.
b. A = Accountable, artinya pihak yang mempunyai kewenangan untuk menyetujui atau menerima pelaksanaan aktivitas.
c. C = Consulted, artinya pihak yang mana pendapatnya dibutuhkan dalam aktivitas (komunikasi arah).
d. I = Informed, artinya pihak yang selalu menjaga kemajuan informasi atas aktivitas yang dilakukan (komunikasi satu arah).

RACI chart dalam Framework Risk IT memiliki sepuluh peran, yang membantu auditor mengidentifikasi

Daftar Pustaka

Anon. n.d. kajian-kebijakan-keamanan-sistem-informasi.

Anita Sindar Sinaga. 2020. *Keamanan Komputer*. Solok: Penerbit Insan Cendekia Mandiri.

Adi Saputra, L. *et al.* (2023) 'Ancaman Keamanan Pada Sistem Informasi Manajemen Perusahaan', *Jurnal Pendidikan Siber Nusantara*, 1(2), pp. 58–66.

Alam, S. (2024) '[Kaleidoskop] Keamanan Siber 2023 dan Prakiraan Ancaman Siber 2024.pdf', *Radio Republik Indonesia (RRI)*. Available at: https://www.rri.co.id/.

Asrin, F. *et al.* (2021) 'Knowledge Data Discovery (Frequent Pattern Growth): The Association Rules for Evergreen Activities on Computer Monitoring', *Advances in Intelligent Systems and Computing*, 1197 AISC, pp. 807–816. doi: 10.1007/978-3-030-51156-2_93.

Asrin, F., Saide, S. and Ratna, S. (2021) 'Data to knowledge-based transformation: The association rules with rapid miner approach and predictive analysis in evergreen IT-business routines of PT chevron pacific Indonesia', *International Journal of Sociotechnology and Knowledge Development*, 13(4), pp. 141–152. doi: 10.4018/IJSKD.2021100109.

A. Rifai, Z. (2010) 'Pencurian Data di Dalam Teknologi Cloud Computing', in *Cloud Computing Strategies*. Institut Teknologi Bandung.

Adrianus, W., Edwin, M.R.S.P. and Yanfi, Y. (2023) 'Furpare: Third-party application as furniture comparison in Indonesia's e-commerce', *Procedia Computer Science*, 216, pp. 77–85. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2022.12.113.

Ali, M. *et al.* (2023) 'A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security', *Alexandria Engineering Journal*, 64, pp. 749–760. Available at: https://doi.org/https://doi.org/10.1016/j.aej.2022.10.056.

Afrina, A., Veza, O., & Harnaranda, J. (2017). Implementasi Sistem Informasi Manajemen Pengolahan Data Periklanan pada Harian Umum Singgalang Padang Menggunakan Metode Pengolahan Data Terpusat (Centralized Data Processing Method). JR: JURNAL RESPONSIVE Teknik Informatika, 1(1).

Ahmad, D (2013). "Manajemen Risiko Sistem Informasi Akademik pada Perguruan tinggi Menggunakan Metoda Octave Allegro". SNATI. Hal.37-42.

Alves, F., Mateus-Coelho, N. and Cruz-Cunha, M. (2023) 'ChevroCrypto – Blockchain Cryptographic File System Prototype', *Procedia Computer Science*, 219, pp. 1546–1554. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2023.01.446.

Applebaum, S., Gaber, T. and Ahmed, A. (2021) 'Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey', *Procedia Computer Science*, 189, pp. 359–367. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2021.05.105.

BISA. 2011. Keamanan Sistem Informasi. Yogyakarta: Andi.

Balboni, P. (2009) *Cloud computing for ehealth data protection issues*. ENISA Working Group on Cloud Computing.

Chanal, P.M. and Kakkasageri, M.S. (2022) 'Blockchain based Data Integrity Framework for Internet of Things Title: Blockchain based Data Integrity Framework for Internet of Things Blockchain based Data Integrity Framework for Internet of Things'. Available at: https://doi.org/10.21203/rs.3.rs-1641782/v1.

CNN Indonesia (2023) '4 Kasus Kebocoran Data di Semester I 2023, Mayoritas Dibantah', *CNN Indonesia*. Available at: https://www.cnnindonesia.com/.

Caralli, R. A. (2007). "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process". Software Engineering Institute. Hal.2-90.

Christopher Alberts, A. D. (2002). Managing Information Security Risks: The OCTAVE Approach.

Catur Nugroho. 2020. *Cyber Society Teknologi, Media Baru, dan Disrupsi Informasi*. Jakarta: Kencana.

Chandra, R 2005, *Sistem Kemanan Teknologi Informasi*, viewed 24 January 2024, <http://reza_chan.staff. gunadarma.ac.id/Downloads/folder/0.19>.

Deris Stiawan. 2005. *Sistem Keamanan Komputer*. Jakarta: Elex Media Komputindo.

David Nathans, *Designing and Building Security Operations Center,* Syngress, 2015, ISBN 9780128008997, https://doi.org/10.1016/B978-0-12-800899-7.00023-9.

Damayanti, T.H. and Hikmah, I.R. (2022) 'Network Forensic Serangan DoS pada Jaringan Cloud berdasarkan Generic Framework for Network Forensics (GFNF)', *Edumatic: Jurnal Pendidikan Informatika*, 6(2), pp. 334–343. Available at: https://doi.org/10.29408/edumatic.v6i2.6466.

Definisi Ancaman (2024) *Kamus Besar Bahasa Indonesia*. Available at: https://kbbi.web.id/ (Accessed: 3 February 2024).

Febriyani, N. (2023) 'Keamanan Sistem Informasi Jaringan 5G di Indonesia Masa Kini dan Masa Depan', (April).

Fazlida, M.R and Jamaliah Said, *Information Security: Risk, Governance and Implementation Setback*, Procedia Economics and Finance, Volume 28, 2015, pp. 243-248

Ferretti, L. *et al.* (2021) 'Verifiable and auditable authorizations for smart industries and industrial Internet-of-Things', *Journal of Information Security and Applications*, 59(April). Available at: https://doi.org/10.1016/j.jisa.2021.102848.

Finalita, A. and Ahyudanari, E. (2021) 'Design and Development of Data Management System to Support The Preparation Process of Accreditation form for Program Study', *IPTEK Journal of Proceedings Series*, 0(1), p. 186. Available at: https://doi.org/10.12962/j23546026.y2020i1.8486.

Goutama, S., Noertjahyana, A. and Novianus Palit, H. 2022. *Simulasi Aplikasi untuk Mendeteksi dan Mencegah Serangan DDoS pada Jaringan Berbasis Software Defined Network*. Available at: https://publication.petra.ac.id/index.php/teknik-informatika/article/view/12037/10571 [Accessed: 23 January 2024].

Godawatte, K., Branch, P. and But, J. (2022) 'Use of blockchain in health sensor networks to secure information integrity and accountability', *Procedia Computer Science*, 210, pp. 124–132. Available at: https://doi.org/https://doi.org/10.1016/j.procs.2022.10.128.

Ginting, E., Sahara, P. and Nurhaliza Tambunan, S. (2023) 'Threat of Denial of Service Attack in Information System Securitu Exploitation', *UNES Journal of Information System*, 8(1), pp. 9–19.

Gunawan, I 2021, 'Kemanan Data: Teori dan Implementasinya', CV Jejak Publisher, Sukabumi.

Hartono, B. (2021) *Cara Mudah dan Cepat Belajar Pengembangan Sistem Informasi*. 1st edn. Edited by J. Teguh Santoso. Semarang: Yayasan Prima Agus Teknik

Hall, J 2007, 'Accounting Information System 4th Edition', Salemba Empat, Jakarta.

Heryana, N, Putra, ANS, Erliyani, I, Martono, Dewi, EN, Supriyadi, A, Nurdin, AM & Dwi, R 2023, 'Prinsip Sistem Operasi', PT. Sada Kurnia Pustaka, Serang.

Hodijah, A. *et al.* (2023) *Informatika*. Bandung: Yrama Widya.

Hutahaean, J. (2014). "Konsep Sistem Informasi", Yogyakarta; Deepublish. Hal.4-5.

Isa, I. 2012. Evaluasi Pengontrolan Sistem Informasi. Yogyakarta: Graha Ilmu.

ID-SIRTII BSSN (2023) *Laporan Bulanan Publik*. Available at: www.idsirtii.or.id.

Indana Zulfa, M., Tena, S. and Dadi Rizkiono, S. 2023. *Aktivitas Sniffing Pada Malware Pencuri Uang Di Smartphone Android*. Available at: https://doi.org/10.xx/paperID.

Ika Yusnita Sari, Muttaqin, Jamaludin, J.S. *et al.* (2020) *Keamanan Data dan Informasi*. Edited by Ronal Watrianthos. Yayasan Kita Menulis.

Ipungkarti, A.A. (2023) 'Penerapan IT Security Awareness Standar Keamanan ISO 27001 Di BPJS Ketenagakerjaan Kantor Cabang Purwakarta', *Jurnal Media Infotama*, 19(1), pp. 103–110.

Jouini, M., Rabai, L.B.A. and Aissa, A. Ben (2014) 'Classification of Security Threats in Information Systems', *Procedia Computer Science*, 32, pp. 489–496.

Kamaliah, A. (2020) *Mendikbud Ingin Anak Indonesia Bisa Computational Thinking*. Available at: https://inet.detik.com/ (Accessed: 18 February 2020).

Kumar, J. *et al.* (2021) 'Analysis of Machine Learning Techniques for Detection System for Web Applications Using Data Mining', *IOP Conference Series: Materials Science and Engineering*, 1099(1), p. 012034. Available at: https://doi.org/10.1088/1757-899x/1099/1/012034.

Laudon, K.C. and Laudon, J.P. (2014) *Management Information Systems : Managing the Digital Firm (Thirteenth Edition)*. 13th edn, *Pearson*. 13th edn. Pearson.

Laudon, K.C. & Laudon, J.P. 2005. Sistem Informasi Manajemen: Mengelola Perusahaan Digital, Edisi 8. Yogyakarta: Andi.

Laudon, K.C. and Laudon, J.P. (2017) *Management Information Systems : Managing the Digital Firm*, *Pearson*. Pearson.Mulyadi, M. (2018) 'Transisi Data dan Informasi dalam Pengembangan Ilmu Pengetahuan', *Pustakaloka*, 10(1), p. 67. doi: 10.21154/pustakaloka.v10i1.1237.

Marks, J. (2010) *The Mind Behind the Fraudsters Crime: Key Behavioral and Environmental Elements*. Crowe Horwarth LLP.

Mohidin, I. (2011) *Cloud Computing Systems*. Jakarta: Redefining Civilization Meruvian.

Mughal A, Building and Securing the Modern Security Operations Center (SOC) *International Journal of Business Intelligence and Big Data Analytics (2022) 5(1) 1-15*

Miftahul Huda. 2020. *Keamanan Informasi*.

Nam H Nguyen. 2018. *Penting Cyber Security Handbook*. Vietnam.

Nugraha, U (2016). "Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka kerja NIST SP 800-300". Seminar Nasional Telekomunikasi dan Informatika. Hal.121-126.

Nugraha, U (2016). "Manajemen Risiko Sistem Informasi pada Perguruan Tinggi Menggunakan Kerangka kerja NIST SP 800-300". Seminar Nasional Telekomunikasi dan Informatika. Hal.121-126.

Putra, P.P. and Toresa, D. (2021) *Keamanan Informasi Dan Jaringan Komputer*. Pekanbaru: LPPM Universitas Lancang Kuning.

Prasetyaningrum, G., Finda Nurmayanti and Fallya Azahra (2022) 'Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat (Literature Review Sim)', *Jurnal Manajemen Pendidikan Dan Ilmu Sosial*, 3(2), pp. 520–529. doi: 10.38035/jmpis.v3i2.1115.

Potter, B. and McGraw, G. (2004) 'Software security testing', *IEEE Security and Privacy*, 2(5), pp. 81–85. Available at: https://doi.org/10.1109/MSP.2004.84.

Putra, G.K.S.A. *et al.* (2023) 'Analisis Hasil DoS SYN Flood Attack Pada Web Server', *Format : Jurnal Ilmiah Teknik Informatika*, 12(1), p. 1. Available at: https://doi.org/10.22441/format.2023.v12.i1.001.

Pegangan Untuk Mahasiswa, S., Hayaty, N. and Cs, M., n.d. *Buku Ajar: Sistem Keamanan*.

Purba, W.W. and Efendi, R. 2020. Perancangan dan analisis sistem keamanan jaringan komputer menggunakan SNORT. *AITI: Jurnal Teknologi Informasi* 17(Agustus), pp. 143–158.

Ridwanto, R. and Capah, D.A.H. (2020) 'Aplikasi Pengelolaan Dokumen dan Arsip berbasis Web untuk mengatur Sistem kearsipan dengan menggunakan Metode Waterfall', *Explore:Jurnal Sistem informasi dan telematika*, 11(2), p. 84. Available at: https://doi.org/10.36448/jsit.v11i2.1469.

Rahardjo, B., 1998. *Keamanan Sistem Informasi Berbasis Internet*. [online] Available at: <http://budi.insan.co.id/courses/el695>.

Ramadhan, A.B. (2023) 'Kapolri Ungkap Kejahatan Siber Menonjol di 2023 Ada Kripto hingga APK-Link.pdf', *detiknews*. Available at: https://news.detik.com/.

Repetto, M. (2023) 'Adaptive monitoring, detection, and response for agile digital service chains', *Computers & Security*, 132, p. 103343. Available at: https://doi.org/https://doi.org/10.1016/j.cose.2023.103343.

Rimsan, M. and Mahmood, A.K. (2020) 'Application of Blockchain to Ensure Temper-Proof Data Availability for Energy Supply Chain', *2020 International Conference on Computational Intelligence, ICCI 2020*, 47(10), pp. 322–326. Available at: https://doi.org/10.1109/ICCI51257.2020.9247768.

Raharjo, B., n.d. *P Y YAYASAN PRIMA AGUS TEKNIK YAYASAN PRIMA AGUS TEKNIK YAYASAN PRIMA AGUS TEKNIK Keamanan SISTEM INFORMASI*.Setiawan, A. and Yulianto, E. (2020) *KEAMANAN DALAM MEDIA DIGITAL*. 1st edn. Edited by R. P. Pratomo. Bandung: Informatika.

Rosini (2015), "Penilaian Risiko Kerawanan Informasi dengan Menggunakan Metode OCTAVEAllegro". Jurnal Pustakawan Indonesia. Vol.14, Hal.14-22.

Raymond McLeod, Jr. (1997). Management Information System. Prentice Hall Inc. Englewood Cliffs. New Jersey.

Sarno, R. & Iffano, I. 2010. Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001). Surabaya: ITS Press

Setyabudhi, A. L. (2017). Perancangan Sistem Informasi Pengolahan Data Absensi dan Pengambilan Surat Cuti Kerja Berbasis Web. JR: JURNAL RESPONSIVE Teknik Informatika, 1(1).

Siever, E, Figgin, S, Love, R & Robbins, A 2009, *Linux in a Nutshell, Sixth Edition*, O'ReillyMedia, Inc, Cafifornia.

Sinaga, AS 2020, 'Keamanan Komputer', ICM Publisher, Solok.

Smyth, N 2020, *Ubuntu 20.04 Essentials: A Guide to Ubuntu Desktop and Server*, Payload Media.

Santoso, J.T. (2023) 'Komputasi Awan (Cloud Computing)', in. Semarang: Universitas STEKOM.

Syamsu, M., Terisia, V. and Masduki, U. (2023) *Jaringan Komputer (Praktis & Mudah Disertai Studi Kasus)*. Purbalingga: Eureka Media Aksara.

Soesanto, E., Damayanti, V. and Samuel, I. (2023) 'Tinjauan Mengenai Sistem Informasi Dan Keamanan Informasi Pada Pt Trinusa Travelindo', *Cross-border*, 6(2), pp. 967–976.

Turban,Rainer, Potter, Introduction To Information Technology Pengantar Teknologi Informasi, Penerbit Salemba Infotek, 2006

TBNews (2023) 'Polri Kasus Kejahatan Siber di 2023 Turun hingga 1.075 Perkara dari 2022.pdf'. Available at: https://tribratanews.sulut.polri.go.id/.

Vairagade, R.S. and Brahmananda, S.H. (2020) 'Secured multi-tier mutual authentication protocol for secure IoT system', *Proceedings - 2020 IEEE 9th International Conference on Communication Systems and Network Technologies, CSNT 2020*, pp. 195–200. Available at: https://doi.org/10.1109/CSNT48778.2020.9115786.

Veza, O. (2017). Perancangan Sistem Informasi Inventory Data Barang Pada Pt. Andalas Berlian Motors (Studi Kasus: PT Andalas Berlian Motors Bukit Tinggi). Jurnal Teknik Ibnu Sina JT-IBSI, 2(2).

Virgiawan A. Manoppo, Arie S. M. Lumenta and Stanley D. S. Karouw. 2020. Analisa Malware Menggunakan Metode Dynamic Analysis Pada Jaringan Universitas Sam Ratulangi. *Jurnal Teknik Elektro dan Komputer* 9(3), pp. 181–188. Available at: https://ejournal.unsrat.ac.id/index.php/elekdankom/article/view/29567 [Accessed: 23 January 2024].

Williams, L. (2021) 'Secure Software Lifecycle Knowledge Area Version..', *Cybok.Org* [Preprint]. Available at: https://cybok.org/media/downloads/Secure_Software_Lifecycle_v1.0.2.pdf.

Watrianthos, R & Purnama, I 2018, 'Buku Ajar Sistem Operasi', Uwais Inspirasi Indonesia.

Yusuf Amrozi,Khoirun Nadya,Laylatul Rahmah,Ni'matus Shofiyah,One Thowimma, Tantangan security dan kehandalan sistem dalam aplikasi bergerak,JUKANTI,Volume 4 No 2 Nopember 2021

(2020) '245 Pernikahan Dini di Lombok Barat sejak Januari, Salah Satunya karena Hamil di Luar Nikah'. Available at: https://regional.kompas.com/ (Accessed: 25 October 2020).

https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah

https://jurnal.unpad.ac.id/farmaka/article/view/27247/pdf

https://www.imperva.com/learn/data-security/database-security/

https://jurnal.mdp.ac.id/index.php/jatisi/article/view/2103

https://www.sciencedirect.com/science/article/pii/B9780128008997000239

Tentang Penulis

Fauzan Asrin. Lahir di kota Rengat tahun 1993, pendidikan SD hingga SMA diselesaikan di kota Rengat. Menyelesaikan Sarjana Komputer tahun 2015 di UIN SUSKA RIAU, dan Magister Komputer tahun 2019 di UPI YPTK Padang, Penulis bertugas sebagai Dosen di Universitas Tanjungpura pada prodi Informatika. Disamping mengajar penulis juga aktif pada Pusat Penelitian Kepolisian Republik Indonesia dan Kemasyarakatan serta sebagai konsultan bidang IT.

Ismarmiaty, ST., MMSI. saat ini menjadi dosen di Universitas Bumigora, kota Mataram Nusa Tenggara Barat. Mengabdikan diri sejak tahun 2015 pada ilmu pengetahuan pada bidang sistem informasi dan mengajar pada bidang Sistem Informasi, Analisa dan Desain Sistem Informasi, Manajemen Proyek Sistem Informasi dan e-Commerce. Menempuh pendidikan sarjana dan magister di Universitas Gunadarma.

Arie Setya Putra Lahir di lampung pada 01 Februari 1987. Merupakan Dosen Universitas Mitra indonesia yang berfokus pada bidang Artificial Intelligence dan Security ini mengembangkan Studio Software yang di beri nama Peelteverse Studio. Studio tersebut menjadi mitra pada beberapa universitas dan institusi.

Nuk Ghurroh Setyoningrum, lahir di Semarang, Jawa Tengah 23 Agustus 1984, Adalah alumni Sarjana Komputer dari Universitas Stikubank Semarang pada tahun 2007 di program studi Sistem Informasi Fakultas Teknologi Informasi dan menyelesaikan program Magister ilmu Komputer di Universitas Gadjah Mada Yogyakarta pada tahun 2010 dengan mengambil konsentrasi Ilmu Komputer Fakultas MIPA. Sekarang Sedang menempuh studi Doktoral Informatika di Universitas AMIKOM Yogyakarta. Penulis mengabdi sebagai Dosen Tetap di Universitas Cipasung Tasikmalaya dan aktif mengajar sebagai Tutor di Universitas Terbuka sejak tahun 2019 sampai sekarang.

Ade Yuliana merupakan Dosen Dpk Di Lingkungan LLDIKTI Wilayah IV Jawa Barat diangkat tahun 2005. Ditempatkan di Politeknik TEDC Bandung Program Studi Teknik Informatika. Lahir, di Cimahi, 07 Oktober 1979. Anak kedua dari empat bersaudara ini, lulus

Pasca Sarjana dari Institut Teknologi Bandung (ITB), memperoleh sertifikasi Dosen tahun 2015 dan beberapa sertifikasi keahlian salah satunya asesor BNSP RCC 2022. Sebagai Dosen di rumpun ilmu Rekayasa Perangkat Lunak sebagian besar karya ilmiah berkaitan dengan Sistem Informasi dan beberapa karya di bidang data science. Bergabung dengan penerbit awal tahun 2024 bersama dengan team penulis lainnya dari beragam kota di Indonesia.

Juwari, S.Kom., M.Kom., lahir dari keluarga sederhana yang berada di sebuah desa kecil tengah kawasan hutan jati, Desa Bangkleyan, Kecamatan Jati, Kabupaten Blora, Jawa Tengah. Pendidikan S1 ia tempuh di Universitas Nusantara PGRI Kediri, Program Studi Sistem Informasi. Kemudian untuk Pendidikan S2 di Universitas AMIKOM Yogyakarta, Teknik Informatika. Saat ini ia aktif sebagai Dosen pada Program Studi Teknik Informatika, Fakultas Teknik, Universitas PGRI Madiun, Jawa Timur. Ia pernah mengampu mata kuliah Jaringan Komputer; Keamanan Data; Arsitektur dan Organisasi Komputer. Karya ilmiah yang pernah dihasilkan antara lain: *Analisis Noise Floor Threshold Terhadap Signal Strength Pada Wireless Local Area Network Protokol Nv2* (2022). *Analisis Redaman Kabel Fiber Optic Patchcord Single Core* (2022).

Tati Ernawati lahir di Bandung, sejak 2005 sampai sekarang bekerja sebagai dosen LLDIKTI Wilayah IV yang ditugaskan di Politeknik TEDC Bandung pada Jurusan Teknik Komputer dan Teknik Informatika yang beralokasi di kota Cimahi. Penulis merupakan alumnus SMA Negeri 1 Cicalengka lulus Tahun 1998, menempuh pendidikan S-1 Program Studi Teknik Informatika di STMIK Jabar lulus Tahun 2003 dan menempuh pendidikan S-2 di Institut Teknologi Bandung (ITB) pada Program Studi Informatika jalur pilihan Teknologi Informasi lulus Tahun 2012. Bidang penelitian penulis adalah pengelolaan dan keamanan jaringan komputer, *Internet of Things*, dan tata kelola teknologi informasi (*IT Governance*). Penulis telah menulis sejumlah buku dan makalah ilmiah di berbagai prosiding konferensi nasional/internasional dan pada jurnal nasional/internasional.

Agni Isador Harsapranata, S.Kom., M.M., M.Kom., lahir di Surakarta 20 Mei 1978, dan sekarang menetap di Bekasi. Menyelesaikan pendidikan S1 Teknik Informatika di STIMIK-AKI Semarang pada tahun 2001, menyelesaikan pendidikan S2 Magister Manajemen di Universitas Budi Luhur pada tahun 2009, menyelesaikan S2 Magister Ilmu Komputer di STMIK NUSA MANDIRI pada tahun 2013. Saat ini sebagai tenaga pengajar di Universitas BSI Jakarta dan sebagai IT Infrastruktur di group perusahaan Otomotif di Jakarta.

Alfa Saleh, M. Kom, Lulusan Sarjana (S1) program studi Teknik Informatika Universitas Potensi Utama tahun 2012, Lulusan Magister (S2) program studi Ilmu Komputer Universitas Putra Indonesia YPTK tahun 2014. Saat ini adalah dosen di Universitas Potensi Utama, mengampu mata kuliah Basis Data, Data Mining dan Sistem Bisnis Cerdas. Aktif menjadi pemakalah di seminar internasional dan menulis di jurnal nasional terakreditasi.

Novi Aryani Fitri, S.T., M.Tr.Kom – Adalah seorang dosen di Program Studi Teknik Informatika Politekniik Negeri Pontianak. Lahir di Sintang, 13 November 1991. Penulis adalah lulusan S1 Teknik Elektro Universitas Tanjungpura Pontianak pada tahun 2014 dan lulus S2 di Teknik Informatika dan Komputer Politeknik Elektronika Negeri Surabaya pada tahun 2019. Penulis memiliki minat bidang penelitian yaitu Networking and Network Security

Putri Ariatna Alia lahir pada hari selasa tanggal 5 juli 1994 di Surabaya provinsi Jawa Timur. Penulis telah menyelesaikan pendidikan S2 Teknik Elektro dengan Konsentrasi Teknik Telematika di Institut Teknologi Sepuluh Nopember dan D4 Teknik Elektro konsentrasi Teknik Telekomunikasi di Politeknik Elektronika Negeri Surabaya – Institut Teknologi Sepuluh Nopember.

Nia Ekawati lahir di Bandung pada tanggal 22 September 1984 sejak 2010 sampai sekarang masih bekerja sebagai dosen. Tahun 2010 hingga 2021 dosen Teknik Informatika Universitas Putera Batam. Tahun 2021 hingga sekarang dosen Teknik Informatika Politeknik TEDC Bandung. Adapun yang bersangkutan adalah merupakan Alumnus dari SMA Negeri 3 Cimahi lulus pada tahun 2002, Pendidikan jenjang S-1 dari Perguruan Tinggi Swasta yaitu Universitas Komputer Indonesia (UNIKOM) Bandung Jawa Barat lulus dengan gelas Sarjana Komputer pada tahun 2007, dan gelar Magister Sistem Informasi Pascasarjana dari STMIK Putera Batam lulus tahun 2014. Saat ini beliau menduduki jabatan sebagai Kepala UPPM di Politeknik TEDC Bandung.

Etza Nofarita,ST,M.Kom. Lulus S1 Teknik Industri Universitas Bung Hatta Padang pada Tahun 1998., Lulus S2 Magister Ilmu Komputer di Universitas Putra IIndonesia “UPI “ YPTK Padang pada Tahun 2013. Saat ini adalah Dosen Tetap Program studi Teknik Komputer di Akademi Manajemen Informatika dan Komputer Kosgoro (AMIK Kosgoro) dari Tahun 2014 sampai saat ini.

Iwan Setiawan, biasa dipanggal Iwan SA, lahir di Kota Sukabumi pada tanggal 20 September 1976, besar dan tumbuh di Kota Moci. Menyelesaikan Pendidikan dasar dan menengah di kota tersebut yaitu di SDN II Warudoyong Kota Sukabumi pada tahun 1989, MTs Negeri Warudoyong Kota Sukabumi pada tahun 1992 dan SMA Negeri 1 Sukaraja Kabupaten Sukabumi Pada Jurusan Fisika di tahun 1995. Kemudian melanjutkan Pendidikan Sarjana dan Pascasarjana di Kota Kembang (Bandung) pada Sekolah Tinggi Teknologi YBS Internasional Pada Program Studi Teknik Informatika bidang Sistem Kontrol Otomatis/Robotika pada tahun 1995 dan menempuh Pend. Elektronika Program Studi Fisika Institut Teknologi Bandunga (ITB) pada tahun 1996 dan Teknik Elektro Politeknik Institut teknologi bandung (ITB) pada tahun 1998. Selanjutnya menyelesaikan Program Magister Teknik Informatika di Universitas Langlangbuana Bandung (UNLA), selesai pada tahun 2009 dan mengikuti Program Doktoral di Universitas Pendidikan Indonesia (UPI) pada tahun 2011, Program Studi Administrasi Pendidikan dengan mengambil Bidang Konsentrasi Sistem Informasi Manajemen Pendidikan, yang diselesaikan pada tahun 2017.

Saat ini aktifitas kesehatiannya bekerja sebagai Tenaga Ahli Pranata Komputer di Biro Data dan Informasi Kementerian Negara Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia dan Juga Dosen di beberapa PTS yang ada di Sukabumi yaitu Dosen Teknik Informatika Nusa Putra Univesity, Dosen Pascasarjana Universitas Muhammadiyah Sukabumi, Dosen Amik Citra Buana Indonesia dan sebagai Tuton di Universitas Terbuka. Selain itu, mempunyai kegiatan

profesional di Bidang Teknologi Informasi dengan menjadi Tenaga Ahli dan di Beberapa Perusahaana IT terkemuka di Kota Bandung dan Lembaga Sertifikasi. Sedangkan aktifitas organisasi aktif sebagai pengurus dan anggota di Persatuan Insinyur Indonesai, Ikatan Ahli Informatika Indonesia (IAII), *Microsoft Certified Organization, Associate International of Engineers, ASEAN Engineer Register, IEEE Student Members*, Himpunan Fisikawan Indonesia, Masyarakat Komputasi Indonesia, Himpunan Bioinformatika Indonesia, APTIKOM Jabar, ISMAPI Jabar dan PROMAPI.

KEAMANAN SISTEM INFORMASI

Buku "Keamanan Sistem Informasi" adalah panduan menyeluruh yang membahas strategi, teknik, dan konsep-konsep penting dalam melindungi sistem informasi dari ancaman cyber. Penulis menguraikan berbagai aspek keamanan, mulai dari enkripsi data hingga manajemen risiko, yang diperlukan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi.

Dengan penekanan pada identifikasi kerentanan, deteksi serangan, dan respons cepat terhadap insiden keamanan, buku ini memberikan wawasan mendalam tentang bagaimana mengembangkan dan mengimplementasikan strategi keamanan yang efektif. Melalui studi kasus dan skenario realistis, pembaca diberikan pemahaman yang kuat tentang taktik dan teknik yang digunakan oleh penyerang serta cara melindungi sistem informasi mereka.

Selain itu, buku ini juga membahas keamanan dalam konteks teknologi baru seperti Internet of Things (IoT), komputasi awan, dan kecerdasan buatan. Penulis menyoroti pentingnya kesadaran keamanan bagi pengguna, perlindungan privasi data, dan kepatuhan regulasi dalam lingkungan yang semakin terhubung ini.

Dengan fokus pada pendekatan preventif dan proaktif, "Keamanan Sistem Informasi" menjadi acuan yang berharga bagi profesional TI, pengelola sistem informasi, dan praktisi keamanan cyber yang ingin memperkuat pertahanan mereka terhadap ancaman digital. Buku ini tidak hanya memberikan pemahaman yang mendalam tentang konsep keamanan TI, tetapi juga memberikan strategi praktis untuk melindungi informasi sensitif dan menjaga keandalan sistem informasi di era yang penuh dengan tantangan keamanan cyber.

ISBN 978-623-8586-06-6

PT Penerbit Penamuda Media
Godean, Yogyakarta
085700592256
@penamuda_media
penamuda.com