Maliki Interdisciplinary Journal (MIJ) eISSN: 3024-8140
Volume 1, Issue 6, 2023 pp. 529-540 http://urj.uin-malang.ac.id/index.php/mij/index

Rekayasa keamanan: Memperkuat keamanan sistem melalui rekayasa keamanan yang terarah

Muhammad Naufal Hibatullah
Program Studi Teknik Informatika, Universitas Islam Negeri Maulana Malik Ibrahim Malang
e-mail: 210605110116@student.uin-malang.ac.id

Kata Kunci:
rekayasa keamanan;
sistem informasi;
keamanan sistem

Keywords:
security engineering;
system information;
system security

A B S T R A K

Artikel ini membahas pentingnya rekayasa keamanan informasi dalam membangun sistem yang aman dan andal. Perencanaan keamanan adalah proses sistematis untuk mengidentifikasi, mengevaluasi, dan memitigasi risiko keamanan informasi sistem. Artikel ini menjelaskan tahapan perencanaan keamanan, termasuk analisis risiko, perencanaan keamanan, implementasi keamanan, dan evaluasi keamanan. Selain itu, artikel ini juga memberikan contoh praktis penggunaan teknologi keamanan informasi seperti enkripsi data, firewall, dan tanda tangan digital untuk meningkatkan keamanan sistem. Dengan perencanaan keamanan data yang baik, sistem dapat terlindungi dari serangan dunia maya dan data pengguna yang sensitif dapat diamankan. Oleh karena itu, penting bagi organisasi untuk meletakkan dasar yang kuat untuk keamanan sistem dengan menerapkan praktik desain keamanan yang baik.

A B S T R A C T

This article discusses the importance of information security engineering in building secure and reliable systems. Security planning is a systematic process for identifying, evaluating, and mitigating system information security risks. This article describes the stages of security planning, including risk analysis, security planning, security implementation, and security evaluation. In addition, this article also provides practical examples of the use of information security technologies such as data encryption, firewalls and digital signature to enhance system security. With good data security planning, the system can be protected from cyber attacks and sensitive user data can be secured. Therefore, it is important for organizations to lay a solid foundation for system security by implementing good security design practices.

Pendahuluan

Keamanan sistem merupakan hal yang sangat penting dalam setiap organisasi. Dalam era digitalisasi seperti sekarang ini, keamanan sistem menjadi semakin kompleks dan membutuhkan fondasi yang kuat agar terhindar dari serangan siber. Oleh karena itu, rekayasa keamanan menjadi sangat penting dalam membangun fondasi yang kuat untuk keamanan sistem.

Rekayasa keamanan adalah suatu proses untuk merancang, mengembangkan, dan membangun sistem yang memiliki tingkat keamanan yang tinggi. Proses ini melibatkan analisis risiko, pengembangan kebijakan keamanan, pengujian keamanan, serta pelatihan dan pendidikan untuk meningkatkan kesadaran akan keamanan.

Dalam artikel ini, akan dibahas mengenai pentingnya rekayasa keamanan dalam membangun fondasi yang kuat untuk keamanan sistem. Selain itu, juga akan dibahas mengenai tahapan dalam proses rekayasa keamanan, serta beberapa teknologi yang dapat digunakan untuk meningkatkan keamanan sistem.

Dengan memahami pentingnya rekayasa keamanan dan mengimplementasikannya dengan benar, organisasi dapat membangun fondasi yang kuat untuk keamanan sistem, sehingga terhindar dari serangan siber dan menjaga kepercayaan pelanggan serta reputasi organisasi.

Kajian Pustaka

Keamanan Informasi

Keamanan informasi adalah bidang penelitian yang sedang berkembang tetapi bukan penelitian yang sederhana-linear (Wilson et al., 1992). Di era internet sekarang ini, sangat mudah untuk mendapatkan dan menyebarkan informasi. Oleh karena itu, informasi menjadi sumber daya yang sangat berharga baik bagi individu maupun pemerintah. Tujuan dari keamanan data adalah untuk mencapai kerahasiaan, kemudahan penggunaan dan integritas semua sumber daya informasi perusahaan perangkat keras dan data.

Keamanan informasi merupakan aspek penting dalam usaha melindungi aset informasi dalam sebuah organisasi. Jenis keamanan informasi dapat dibagi menjadi beberapa bagian menurut Whitman & Mattord (2015) yaitu: 1) Physical security, 2) Personal security, 3) Operational security, 4) Communications security, dan 5) Network security.

Jika serangan membuat sistem tidak tersedia, maka tidak akan dapat memperbarui informasi yang berubah seiring waktu. Berarti integritas sistem dapat dikompromikan. Jika serangan berhasil dan integritas sistem terganggu, mungkin harus diturunkan untuk memperbaiki masalah. Oleh karena itu, ketersediaan sistem berkurang (Sommerville, 2011).

Keamanan adalah atribut sistem yang mencerminkan kemampuan sistem untuk melindungi dari serangan jahat internal atau eksternal. Serangan eksternal ini dimungkinkan karena sebagian besar komputer dan perangkat seluler terhubung jaringan dan dengan demikian dapat diakses oleh orang asing.

Untuk beberapa sistem, keamanan adalah atribut ketergantungan sistem yang paling penting. Sistem militer, sistem perdagangan elektronik, dan sistem yang melibatkan pemrosesan dan pertukaran informasi rahasia harus dirancang sedemikian rupa sehingga mencapai tingkat keamanan yang tinggi. Jika sistem reservasi maskapai tidak tersedia, misalnya, ini menyebabkan ketidaknyamanan dan beberapa penundaan dalam penerbitan tiket. Namun, jika sistem tidak aman, penyerang dapat menghapus semua pemesanan dan hampir tidak mungkin untuk melanjutkan operasi maskapai normal (Sommerville, 2011).

Penilaian dan Analisis Risiko

Manajemen risiko merupakan serangkaian aktivitas dalam menganalisis risiko. Risiko tersebut diidentifikasi, dinilai, dan selanjutnya disusun langkah strategis yang dapat digunakan dalam mengatasi risiko tersebut. Tujuan utama dari dilaksanakannya manajemen risiko adalah memberikan pandangan terkait kemungkinan yang bisa terjadi sehingga perusahaan dapat menyusun langkah mitigasi dan evaluasi terkait risiko. Tahapan dalam manajemen risiko menurut Stoneburner dkk. (2002) di antaranya: 1) mengidentifikasi dan mengklarifikasi risiko, 2) setiap risiko dinilai, 3) menyusun langkah penanggulangan risiko, 4) pendokumentasian dan pengimplementasian dari langkah menanggulangi risiko, 5) pendekatan portofolio risiko TI, dan 6) monitoring berkala terhadap tingkat risiko TI dan audit.

Penting untuk dicatat bahwa pendekatan dan tahapan dalam manajemen risiko dapat bervariasi tergantung pada konteks dan metodologi yang digunakan oleh organisasi atau pakar risiko tertentu. Dari perspektif organisasi, keamanan harus dipertimbangkan pada tiga tingkatan menurut Sommerville (2011) yaitu: 1) keamanan infrastruktur, yang berkaitan dengan pemeliharaan keamanan semua sistem dan jaringan yang menyediakan infrastruktur dan serangkaian layanan bersama bagi organisasi, 2) keamanan aplikasi, yang berkaitan dengan keamanan sistem aplikasi individu atau kelompok sistem terkait, dan 3) keamanan operasional, yang berkaitan dengan operasi yang aman dan penggunaan sistem organisasi.

Dengan mempertimbangkan ketiga tingkat tersebut, organisasi dapat mengadopsi pendekatan yang komprehensif untuk memastikan keamanan sistem dan melindungi aset informasi yang berharga. Penting untuk mengintegrasikan keamanan pada semua tingkat ini agar risiko keamanan dapat dikelola dengan efektif.

Persyaratan Keamanan

Persyaratan keamanan pemeliharaan sistem berkaitan dengan langkah-langkah yang diambil untuk menjaga keamanan sistem terhadap perubahan yang tidak sah atau merusak. Ini melibatkan penggunaan mekanisme seperti kontrol akses yang ketat, pengamanan fisik terhadap perangkat keras, perlindungan terhadap perubahan tidak sah pada konfigurasi sistem, dan pemantauan terus-menerus terhadap keandalan sistem.

10 jenis persyaratan keamanan yang mungkin disertakan dalam spesifikasi sistem menurut Firesmith (2003) yaitu: 1) persyaratan identifikasi menentukan apakah suatu sistem harus mengidentifikasi penggunanya sebelum berinteraksi dengan mereka, 2) persyaratan autentikasi menentukan bagaimana pengguna diidentifikasi, 3) persyaratan otorisasi menentukan hak istimewa dan izin akses dari pengguna yang diidentifikasi, 4) persyaratan kekebalan menentukan bagaimana sistem harus melindungi dirinya dari virus, worm, dan ancaman serupa, 5) persyaratan integritas menentukan bagaimana korupsi data dapat dihindari, 6) persyaratan deteksi intrusi menentukan mekanisme apa yang harus digunakan untuk mendeteksi serangan pada sistem, 7) persyaratan Non-repudiation (tidak ada penolakan) menetapkan bahwa suatu pihak dalam suatu transaksi tidak dapat menyangkal keterlibatannya dalam transaksi tersebut, 8) persyaratan privasi menentukan bagaimana privasi data harus dijaga, 9) persyaratan

audit keamanan menentukan bagaimana penggunaan sistem dapat diaudit dan diperiksa, dan 10) persyaratan keamanan pemeliharaan sistem menentukan bagaimana aplikasi dapat mencegah perubahan resmi agar tidak merusak mekanisme keamanannya secara tidak sengaja.

Dengan mempertimbangkan 10 jenis persyaratan keamanan ini, organisasi dapat merancang dan mengimplementasikan langkah-langkah keamanan yang diperlukan untuk melindungi sistem mereka dari berbagai ancaman. Penting untuk memperhatikan dan memenuhi persyaratan keamanan ini selama siklus pengembangan sistem dan juga dalam operasi sehari-hari untuk memastikan bahwa sistem tetap aman dan terlindungi dari ancaman yang mungkin timbul.

Di dalam upaya penanganan maupun pengendalian terhadap Keamanan Sistem Informasi, kiranya harus mempertimbangkan tiga aspek penting dalam keamanan informasi yang akrab dengan kependekan CIA (Confidentiality, Integrity, Availability) (Nurul dkk., 2022). Kerahasiaan (Confidentiality) merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang. Integritas (Integrity) merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi. Ketersediaan (Availability) merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapan pun dan di mana pun.

Ketiga aspek ini saling berkaitan dan saling mendukung untuk menciptakan keamanan sistem informasi yang kokoh. Keberhasilan dalam menjaga kerahasiaan, integritas, dan ketersediaan akan memberikan perlindungan yang kuat terhadap informasi dan sistem dari ancaman dan serangan yang mungkin timbul. Oleh karena itu, penting bagi organisasi untuk mengadopsi kebijakan dan langkah-langkah keamanan yang sesuai untuk mengatasi ketiga aspek ini dalam rangka melindungi informasi dan sistem mereka secara efektif.

Metodologi Penelitian

Metode penulisan artikel ilmiah ini adalah metode kualitatif dengan penelitian kepustakaan (library research). Teliti teori dan hubungan atau pengaruh antara variabel buku di e-book, Google Scholar, dan media online lainnya.

Dalam penelitian kualitatif, kajian pustaka harus digunakan secara konsisten dengan asumsi-asumsi metodologis. Artinya harus digunakan secara induktif sehingga tidak mengarahkan pertanyaan-pertanyaan yang diajukan oleh peneliti. Salah satu alasan utama untuk melakukan penelitian kualitatif yaitu bahwa penelitian tersebut bersifat eksploratif (Limakrisna dkk., 2016).

Pembahasan

Dalam era digital yang semakin maju, keamanan sistem dan data menjadi hal yang sangat penting bagi perusahaan maupun individu. Ancaman keamanan yang semakin kompleks, seperti serangan siber dan peretasan, membuat pentingnya membangun fondasi yang kuat untuk keamanan sistem dalam rekayasa keamanan menjadi lebih mendesak.

Pembangunan fondasi keamanan yang kuat harus dimulai sejak tahap perencanaan dan desain sistem. Langkah awal ini sangat penting karena fondasi keamanan yang baik harus terintegrasi dan terpadu dalam setiap aspek sistem yang dibangun. Hal ini mencakup pemikiran tentang keamanan sebagai bagian integral dari proses pengembangan, bukan sebagai tambahan setelah sistem selesai dibangun.

Keamanan harus diintegrasikan dalam seluruh tahapan pengembangan sistem, bukan hanya sebagai aspek yang ditambahkan setelah sistem selesai dibangun. Dalam konteks rekayasa keamanan, jika keamanan diabaikan atau dianggap sebagai tugas yang harus diselesaikan kemudian, maka ada kemungkinan sistem akan rentan terhadap serangan dan ancaman keamanan. Dengan memulai dari tahap perencanaan dan desain, perusahaan dapat membangun fondasi keamanan yang solid dan terintegrasi dengan baik ke dalam setiap komponen sistem.

Pentingnya Keamanan Informasi

Pentingnya keamanan data tidak dapat diabaikan dalam lingkungan bisnis yang semakin terhubung dan berbasis teknologi. Keamanan data memiliki peran sentral dalam menjaga integritas dan kerahasiaan informasi yang dimiliki oleh suatu organisasi. Menurut Febiryani dkk. (2021) bahwa keamanan data adalah faktor kunci dalam memastikan kelangsungan bisnis yang stabil, mengurangi risiko kerugian perusahaan, serta memaksimalkan peluang dan investasi yang ada.

Dalam dunia di mana pertukaran informasi secara elektronik semakin dominan, perlindungan terhadap informasi menjadi semakin vital. Perlindungan ini jauh lebih luas daripada sekadar mengamankan data dari akses yang tidak sah. Menurut Onyigwang dkk. (2016) menyatakan perlindungan informasi juga melibatkan upaya untuk melindungi integritas data dari ancaman siber yang terus berkembang.

Tidak hanya itu, keamanan informasi juga memiliki dampak yang signifikan pada citra dan reputasi perusahaan di mata pelanggan dan pemangku kepentingan lainnya. Penelitian oleh Von Solms, (1999) menunjukkan bahwa pelanggan dan mitra bisnis cenderung lebih suka untuk bekerja dengan perusahaan yang dapat memberikan jaminan akan keamanan informasi mereka.

Dalam mengelola sistem informasi, pengaturan izin dan protokol pengamanan menjadi hal penting. Menurut Bertino & Ferrari (1998), perlu dipastikan bahwa data hanya diakses oleh pihak yang memiliki hak akses, dan transmisi data dilakukan dengan aman. Hal ini melibatkan langkah-langkah seperti pengaturan izin dan implementasi protokol pengamanan yang sesuai untuk mencegah potensi ancaman seperti peretasan atau pencurian data.

Namun, penting untuk diingat bahwa investasi dalam keamanan informasi bukan hanya sebatas aspek teknologi semata. Menurut Peltier (2005) bahwa investasi dalam keamanan informasi juga melibatkan kesadaran dan pelatihan karyawan. Pengguna akhir memiliki peran kunci dalam menjaga integritas data. Pengetahuan mereka tentang praktik keamanan siber dapat membuat perbedaan yang signifikan dalam mencegah serangan.

Keamanan Sistem Informasi

Keamanan sistem mengacu pada perlindungan terhadap ancaman dan serangan yang bertujuan merusak, mencuri, atau mengganggu integritas, kerahasiaan, atau ketersediaan data dan sumber daya sistem. Keamanan sistem bertujuan untuk melindungi informasi sensitif, melawan serangan siber, dan memastikan bahwa sistem beroperasi sesuai dengan kebutuhan yang ditentukan.

Sekarang penting untuk merancang sistem untuk menahan serangan eksternal dan untuk pulih dari serangan tersebut. Tanpa tindakan pencegahan keamanan, penyerang pasti akan membahayakan sistem jaringan. Mereka mungkin menyalahgunakan perangkat keras sistem, mencuri data rahasia, atau mengganggu layanan yang ditawarkan oleh sistem.

Tiga dimensi keamanan yang harus dipertimbangkan dalam rekayasa sistem yang aman menurut Sommerville (2011) merujuk pada aspek-aspek kritis yang perlu diperhatikan dalam pengembangan sistem guna menjaga tingkat keamanan yang memadai. Dimensi pertama adalah kerahasiaan, di mana folus utamanya adalah mencegah informasi sensitif atau rahasia jatuh ke tangan yang salah. Dalam konteks ini, ancaman utama adalah potensi pengungkapan atau akses oleh individu atau program yang tidak memiliki otoritas. Sebagai contoh, peretasan yang mengakibatkan pencurian data kartu kredit dari platform e-commerce menggambarkan situasi di mana kerahasiaan terancam.

Dimensi berikutnya adalah integritas, yang menunjuk pada perlunya menjaga integritas atau kesahihan informasi dalam sistem. Hal ini berkaitan dengan mencegah adanya kerusakan atau modifikasi yang tidak sah terhadap data yang ada. Ancaman pada dimensi integritas melibatkan serangan seperti penyebaran worm yang dapat merusak atau menghapus data, mengakibatkan informasi yang tidak dapat diandalkan atau telah diubah dengan cara yang merugikan.

Ketersediaan adalah dimensi keamanan yang ketiga yang harus dipertimbangkan. Fokus dimensi ini adalah memastikan bahwa sistem dan data yang terkait dapat diakses dan digunakan sesuai kebutuhan. Ancaman terhadap ketersediaan mencakup serang penolakan layanan yang bertujuan membebani sumber daya server sehingga mengganggu akses yang normal. Dalam situasi seperti ini, layanan menjadi tidak tersedia atau hanya tersedia dengan keterbatasan, mengakibatkan gangguan operasional yang signifikan.

Penyerang fokus pada infrastruktur perangkat lunak karena komponen infrastruktur seperti browser tersedia secara luas. Penyerang dapat menyelidiki kelemahan dalam sistem ini dan berbagi informasi tentang kerentanan yang mereka temukan. Karena banyak orang menggunakan perangkat lunak yang sama, serangan tersebut memiliki aplikasi yang luas.

Ancaman terhadap Sistem Informasi

Informasi yang memiliki nilai dan merupakan aset tidak luput dari ancaman, berbagai cara digunakan untuk memperoleh informasi tersebut secara ilegal, aktivitas tersebut dikenal sebagai cybercrime. Cybercrime merupakan aktivitas kejahatan dengan

menggunakan teknologi komputer atau jaringan komputer sebagai alat, sasaran maupun tempat terjadinya kejahatan (Chazar, 2015). Ancaman terhadap sistem informasi adalah suatu aksi atau kejadian yang dapat merugikan perusahaan. Ancaman terhadap sistem informasi mengacu pada berbagai aksi atau peristiwa yang dapat membahayakan keamanan dan integritas sistem informasi suatu organisasi.

Ancaman ini dapat berasal dari berbagai sumber, termasuk serangan siber, kegagalan perangkat keras, kesalahan manusia, atau bencana alam. Aksi atau peristiwa ini dapat menyebabkan kerugian yang serius bagi perusahaan, seperti kehilangan data, gangguan operasional, penipuan, atau kerusakan reputasi. Ancaman terhadap sistem informasi dapat mencakup serangan malware, hacking, serangan phishing, serangan DDoS, serangan insider, dan lain sebagainya. Oleh karena itu, penting bagi organisasi untuk menerapkan langkah-langkah keamanan yang efektif, seperti penggunaan perangkat lunak keamanan yang mutakhir, pemantauan dan deteksi intrusi, kebijakan keamanan yang ketat, pelatihan pengguna, serta pemulihan dan pemulihan yang cepat setelah serangan atau insiden keamanan terjadi (Chazar, 2015). Ada beberapa kemungkinan serangan (attack) menurut :

1. Interuption: perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (availability) dari sistem. Contoh serangan adalah "denial of service attack"
2. Interception: pihak yang tidak berwenang berhasil mengakses aset atau informasi. Contoh dari serangan ini adalah penyadapan (wiretapping).
3. Modification: pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
4. Fabrication: pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

Pemahaman tentang jenis-jenis serangan ini penting bagi organisasi dalam merancang dan menerapkan langkah-langkah keamanan yang efektif. Dengan mengidentifikasi dan memahami kemungkinan serangan yang mungkin terjadi, organisasi dapat mengambil tindakan pencegahan yang tepat dan melindungi sistem informasi mereka dari ancaman-ancaman tersebut.

Desain sistem yang aman

Desain sistem informasi yang aman merujuk pada proses merancang dan mengimplementasikan sistem informasi dengan mempertimbangkan aspek keamanan secara menyeluruh. Hal ini dilakukan untuk melindungi data, informasi, dan infrastruktur sistem dari ancaman dan serangan yang mungkin terjadi. Pentingnya desain sistem informasi yang aman terletak pada upaya mencegah, mendeteksi, dan merespons ancaman keamanan dengan efektif. Hal-hal yang perlu dilakukan agar dapat mendesain sistem yang aman yaitu:

1. Desain penilaian risiko

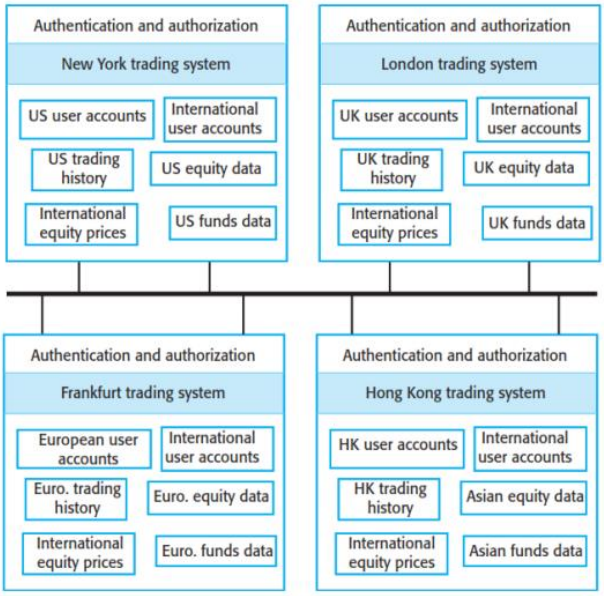
Tahap awal dalam mendesain sistem yang aman adalah melakukan penilaian risiko secara menyeluruh. Ini melibatkan mengidentifikasi potensi ancaman keamanan yang mungkin dihadap oleh sistem, mengevaluasi kemungkinan terjadinya serangan, dan mengukur dampak potensial dari serangan tersebut terhadap organisasi. Dengan penilaian risiko yang komprehensif, organisasi dapat mengidentifikasi prioritas keamanan yang perlu diperhatikan dan mengalokasikan sumber daya yang tepat untuk melindungi sistem.

Penilaian risiko keamanan selama desain pos mengidentifikasi beberapa persyaratan keamanan lanjutan dari sistem. Namun, jika sistem dibuat dan diimplementasikan, keputusan arsitektur dan teknis dibuat selama proses desain sistem mempengaruhi keamanan sistem. Keputusan ini menciptakan persyaratan desain baru dan dapat berarti bahwa persyaratan yang ada perlu diubah (Sommerville, 2011). Saat ingin menilai risiko selama perencanaan dan implementasi, dapat mempelajari lebih lanjut tentang apa yang dilindungi dan mengetahui tentang kerentanan sistem.

2. Desain arsitektur

Desain arsitektur merupakan desain makro/struktur yang mencerminkan kualitas serta fungsi dari perangkat lunak (Wirawan & Adhy, 2016). Arsitektur perangkat lunak digambarkan sebagai rancangan mengenai struktur data dan komponen program yang dibutuhkan untuk membangun sistem berbasis komputer (Pressman, 2000). Sehubungan dengan keamanan sistem, desain arsitektur memainkan peran penting dalam mencerminkan kualitas dan fungsionalitas perangkat lunak dan dalam memastikan tingkat perlindungan sistem yang memadai.

Gambar 1. Aset terdistribusi dalam sistem perdagangan ekuitas



Sumber : Sommervile, I. (2011). Software Engineering.

Gambar 1 mengilustrasikan arsitektur sistem perbankan untuk perdagangan saham dan dana di pasar New York, London, Frankfurt, dan Hong Kong. Sistem ini didistribusikan sehingga data tentang setiap pasar dipertahankan secara terpisah. Aset

yang diperlukan untuk mendukung aktivitas penting perdagangan ekuitas (akun pengguna dan harga) direplikasi dan tersedia di semua node. Jika node sistem diserang dan menjadi tidak tersedia, aktivitas penting perdagangan ekuitas dapat ditransfer ke negara lain sehingga masih dapat tersedia bagi pengguna (Sommerville, 2011).

Masalah desain sistem yang aman adalah bahwa dalam banyak kasus, gaya arsitektur yang terbaik untuk persyaratan keamanan mungkin bukan yang terbaik untuk memenuhi persyaratan kinerja. Misalnya, katakanlah suatu aplikasi memiliki persyaratan mutlak untuk menjaga kerahasiaan database besar dan persyaratan lain untuk akses yang sangat cepat ke data tersebut. Tingkat perlindungan yang tinggi menunjukkan bahwa lapisan perlindungan diperlukan, yang berarti bahwa harus ada komunikasi antara lapisan sistem. Ini memiliki overhead kinerja yang tak terelakkan sehingga akan memperlambat akses ke data (Sommerville, 2011).

Implementasi perlindungan dan jaminan kerahasiaan saat menggunakan arsitektur alternatif bisa lebih rumit dan mahal. Dalam situasi ini, harus mendiskusikan konflik tersebut menghubungkan pelanggan ke sistem pembayaran dan menyepakati bagaimana konflik akan muncul itu diselesaikan.

3. Pedoman desain

Tidak ada cara mudah untuk memastikan keamanan sistem. Berbagai jenis sistem sarana teknis yang berbeda diperlukan untuk mencapai tingkat keamanan yang dapat diterima disetujui oleh pemilik sistem. Misalnya, di bank, pengguna cenderung menerima tingkat keamanan yang lebih tinggi, dan karenanya prosedur keamanan yang lebih mengganggu daripada di universitas (Elahi & Yu, 2009).

Terdapat 10 pedoman desain keamanan menurut (Sommerville, 2011) berikut ini:

Pedoman 1: Mendasarkan keputusan keamanan pada kebijakan keamanan eksplisit

Banyak organisasi tidak memiliki kebijakan keamanan sistem yang jelas. Jika tidak ada kebijakan, Anda perlu membuatnya dari contoh dan mendiskusikannya dengan manajer. Kebijakan keamanan membantu mengarahkan evolusi sistem dengan dasar yang jelas.

Pedoman 2: Gunakan pertahanan secara mendalam

Tidak boleh hanya mengandalkan satu mekanisme keamanan. Sebaliknya, gunakan beberapa teknik berbeda untuk menjaga keamanan. Konsep ini disebut juga "pertahanan mendalam."

Pedoman 3: Gagal dengan aman

Kegagalan dalam sistem tidak dapat dihindari. Khususnya pada sistem kritis keamanan, penting untuk memastikan bahwa ketika terjadi kegagalan, sistem tetap aman. Jangan menggantikan sistem yang gagal dengan tindakan yang lebih tidak aman.

Pedoman 4: Seimbangkan keamanan dan kegunaan

Keamanan dan kemudahan penggunaan sering kali berbenturan. Sistem yang aman mungkin memerlukan langkah-langkah ekstra dari pengguna, sehingga perlu diatur dengan bijak agar tidak terlalu rumit.

Pedoman 5: Mencatat tindakan pengguna

Usahakan untuk mencatat semua tindakan pengguna. Ini termasuk siapa yang melakukan apa, aset yang digunakan, serta waktu dan tanggalnya. Log ini dapat membantu mendeteksi serangan dan jejak bagaimana penyerang masuk ke sistem.

Pedoman 6: Gunakan redundansi dan keragaman untuk mengurangi risiko

Mempertahankan beberapa versi perangkat lunak atau data dan memvariasikan teknologi yang digunakan dapat mengurangi dampak kerentanan terhadap satu titik kegagalan.

Pedoman 7: Tentukan formal input sistem

Serangan umum melibatkan memberikan input tak terduga pada sistem, yang bisa menyebabkan perilaku yang tidak diinginkan. Penting untuk mengatasi masalah ini dengan memeriksa dan memvalidasi input yang masuk.

Pedoman 8: Pisahkan aset

Tidak semua pengguna harus memiliki akses ke semua informasi dalam sistem. Informasi harus diatur dalam kompartemen, sehingga serangan hanya mempengaruhi bagian tertentu dari sistem.

Pedoman 9: Desain untuk penyebaran

Mengkonfigurasi sistem dengan benar saat digunakan adalah penting. Menerapkan perangkat lunak di lingkungan operasionalnya dengan benar dan memperhitungkan preferensi pengguna dan konfigurasi yang sesuai.

Pedoman 10: Desain untuk pemulihan

Meskipun upaya untuk menjaga keamanan, perlu merancang sistem dengan asumsi bahwa kegagalan bisa terjadi. Pertimbangkan bagaimana sistem bisa dipulihkan dari kegagalan dan dikembalikan ke kondisi operasional yang aman.

Kesimpulan

Dengan meningkatnya ancaman keamanan digital, perusahaan dan organisasi harus mengadopsi pendekatan yang terarah dalam melindungi sistem mereka. Pentingnya memperkuat keamanan sistem dengan pendekatan yang terarah.

Rekayasa keamanan adalah suatu metode yang digunakan untuk mengidentifikasi, menganalisis, dan memperkuat kerentanan dalam infrastruktur teknologi informasi. Artikel ini menjelaskan bahwa melalui rekayasa keamanan yang terarah, perusahaan dapat melindungi data sensitif, menjaga keberlanjutan operasional, serta meminimalkan risiko terhadap serangan siber. Metode ini melibatkan langkah-langkah seperti identifikasi kerentanan, analisis risiko, pengembangan rencana pemulihan bencana, dan pelatihan karyawan terkait keamanan. Dengan menerapkan rekayasa keamanan yang terarah, perusahaan dapat memperkuat pertahanan mereka terhadap ancaman yang terus berkembang di dunia digital saat ini.

Daftar Pustaka

Bertino, E., & Ferrari, E. (1998). Data security. *Proceedings. The Twenty-Second Annual International Computer Software and Applications Conference (Compsac '98) (Cat. No.98CB 36241)*, 228–237. https://doi.org/10.1109/CMPSAC.1998.716660

Chazar, C. (2015). Standar manajemen keamanan sistem informasi berbasis ISO/IEC 27001:2005. *Jurnal Informasi. Vol. VII, No. 2.* https://informasi.stmik-im.ac.id/wp-content/uploads/2016/05/04-Chalifa.pdf

Elahi, G., & Yu, E. (2009). Modeling and analysis of security trade-offs – A goal oriented approach. *Data & Knowledge Engineering*, *68*(7), 579–598. https://doi.org/10.1016/j.datak.2009.02.004

Febiryani, W., Kusumasari, T. F., & Fauzi, R. (2021). Analysis and Design of Implementation Guidelines Data Security Management Assessment Techniques Based On DAMA-DMBOKv2. *2021 IEEE 5th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 371–375. https://doi.org/10.1109/ICITISEE53823.2021.9655782

Firesmith, D. (2003). Analyzing and Specifying Reusable Security Requirements. *Journal of Object Technology - JOT*.

Limakrisna, N., Noor, Z., & Ali, H. (2016). Model of employee performance: The empirical study at civil servants in government of West Java Province. *IJER, 13 (3), 707–719.*

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi dan network (literature review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi (JEMSI). Vol 3, No. 5.*

Onyigwang, O. J., Shestak, Y., & Oksiuk, A. (2016). Information protection of data processing center against cyber attacks. *2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP)*, 397–400. https://doi.org/10.1109/DSMP.2016.7583586

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, *14*(2), 37–49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6

Pressman, R. S. (2000). *Software engineering: A practitioner's approach* (5th ed). McGraw Hill.

Sommerville, I. (2011). *Software engineering* (9th ed). Pearson.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology (NIST SP 800-30; 0 ed., p. NIST SP 800-30). *National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30*

Von Solms, R. (1999). Information security management: Why standards are important. *Information Management & Computer Security*, *7*(1), 50–58. https://doi.org/10.1108/09685229910255223

Whitman, M., & Mattord, H. (2015). *Principles of Information Security, 5th Edition*.

Wilson, J. L., Turban, E., & Zviran, M. (1992). Information systems security: A managerial perspective. *International Journal of Information Management*, *12*(2), 105–119. https://doi.org/10.1016/0268-4012(92)90017-K

Wirawan, P. W., & Adhy, S. (2016). *Desain Perangkat Lunak: Konsep dan Tantangannya*.