Pemodelan Ancaman Sistem Informasi Manajemen Logistik Menggunakan Pendekatan STRIDE dan DREAD pada Perusahaan Logistik

Affrie Ramadhan dan Hustinawaty

Universitas Gunadarma
Jl. Margonda Raya No. 100, Depok 16424, Jawa Barat
E-mail: avri.rama@yahoo.com, hustina@staff.gunadarma.ac.id*

Abstrak

Seiring dengan perkembangan Industri 4.0, ancaman siber terhadap sistem informasi manajemen logistik semakin meningkat. Sistem ini berperan krusial dalam operasional perusahaan logistik, sehingga gangguan pada sistem dapat berakibat pada kerugian finansial yang signifikan. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis ancaman keamanan menggunakan metode STRIDE dan DREAD, serta menyusun strategi mitigasi yang efektif. Hasil penelitian menunjukkan bahwa kategori ancaman dengan tingkat risiko tertinggi adalah *Spoofing, Tampering*, dan *Repudiation*, sedangkan *Information Disclosure* dan *Denial of Service* memiliki tingkat risiko sedang. Untuk mengurangi risiko tersebut, disarankan penerapan multi faktor autentikasi, *access control list*, pencatatan log otomatis, serta enkripsi data. Selain itu, pengguna diimbau untuk tidak menyimpan kredensial pada *browser* dan menghindari pembagian informasi *login*. Dengan implementasi strategi ini, diharapkan keamanan sistem informasi manajemen logistik dapat lebih ditingkatkan secara optimal.

Kata kunci : Pemodelan ancaman, STRIDE, DREAD, sistem informasi manajemen logistik.

Pendahuluan

Pengaruh teknologi informasi (TI) terhadap perkembangan bisnis modern telah menjadi topik yang semakin penting dalam beberapa dekade terakhir [16]. Perkembangan TI yang pesat telah memberikan dampak yang signifikan terhadap cara bisnis dijalankan, mulai dari proses produksi hingga pemasaran [2]. Perusahaan logistik adalah salah satu organisasi yang mengadopsi sistem informasi manajemen logistik berbasis *web* sebagai bagian dari pengelolaan administrasi terkomputerisasi. *Web services* memiliki sebuah keunikan, yaitu dapat diakses *cross platform*. Jika sistem keamanan pada layanan web services tidak dikonfigurasi dengan baik, maka dapat dengan mudah diretas, sehingga menimbulkan masalah keamanan [19].

Keamanan *website* adalah suatu cabang teknologi yang dikenal dengan nama keamanan informasi yang diterapkan pada *website* dengan sasaran perlindungan terhadap informasi atau data [13][20]. Data adalah salah satu aset berharga perusahaan logistik, sehingga sistem informasi manajemen logistik merupakan aspek krusial dalam upaya perlindungan aset tersebut. Keamanan informasi didefinisikan sebagai melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas dan kemudahan penggunaan. Timbulnya ancaman dalam sebuah sistem aplikasi disebabkan oleh kesalahan yang muncul pada saat mendesain dan mengembangkan aplikasi [7].

Dalam menghadapi ancaman, pemodelan ancaman menjadi pendekatan yang efektif untuk mengidentifikasi potensi risiko dan kerentanan. Pemodelan ancaman merupakan suatu model yang di dalamnya terdapat beberapa tahapan seperti identifikasi sistem, identifikasi aset, dan analisis ancaman dan penanggulangan dalam konteks melindungi sesuatu yang bernilai [1]. Dengan memahami ancaman dan merancang strategi perlindungan yang tepat, perusahaan dapat mengoptimalkan kinerja sistem informasi mereka sambil menjaga keamanan dan integritas data sebagai prioritas utama [18].

Pemodelan ancaman keamanan E-Health menggunakan metode STRIDE dan DREAD. Penelitian ini melibatkan identifikasi aktivitas pengguna, arsitektur SIMRS, teknologi, dan pemodelan ancaman. Metode STRIDE mengidentifikasi

DOI : http://dx.doi.org/10.32409/jikstik.24.1.3768, *)Penulis Korespondensi

kerentanan, DREAD menilai tingkat ancaman, mengungkap kerentanan *Denial of Service, Repudiation, Tampering, Spoofing*, dan *Elevation of Privilege*. Penelitian ini merinci pentingnya mengatasi potensi ancaman dalam sistem keamanan E-Health [7].

Penelitian penilaian ancaman aplikasi web menggunakan metode DREAD melibatkan identifikasi aset informasi, analisis skenario serangan, uji keamanan *website*, dan penentuan tingkat ancaman. Hasilnya berupa laporan peringkat ancaman sebagai dasar penyusunan dokumen ancaman. Dokumen ini membentuk *security report* yang berisi deskripsi ancaman, tingkat risiko, target ancaman, jenis serangan dan langkah pencegahan [17].

Indeks KAMI sebagai kerangka penelitian mengevaluasi tingkat kematangan dan kelengkapan penerapan ISO/IEC 27001:2013 serta tata kelola keamanan informasi pada organisasi. Hasil penilaian disajikan dalam diagram jaring laba-laba, memberikan gambaran kepatuhan terhadap standar tersebut. Rekomendasi perbaikan sistem dibuat berdasarkan hasil penilaian tersebut [15].

Dari tinjauan beberapa jurnal, penerapan sistem informasi manajemen di perusahaan dapat diakses tidak hanya dari pengguna internal perusahaan namun juga dari pihak eksternal. Fenomena ini mendorong perlunya analisis ancaman dan risiko pada sistem informasi manajemen logistik. Pemilihan STRIDE sebagai metode pemodelan ancaman dikarenakan lebih efektif, ringan dan mudah untuk diaplikasikan untuk mengidentifikasi kerentanan atau celah keamanan yang mungkin timbul dari sistem informasi [8]. Setelah melakukan identifikasi kerentanan, selanjutnya dilakukan penilaian Berdasarkan tingkatan ancaman dari masing-masing kerentanan menggunakan metode DREAD. Karena sistem informasi manajemen logistik terkait erat dengan proses bisnis perusahaan logistik, sistem ini harus dilindungi dari bahaya dan risiko yang dapat dihadapi perusahaan logistik. Penerapan pendekatan pemodelan ancaman diharapkan dapat dijadikan sebagai mitigasi ancaman secara tepat.

Metode Penelitian

Penelitian yang dilakukan terkait pemodelan ancaman sistem informasi manajemen logistik menggunaan metode STRIDE untuk mengidentifikasi dan mengklasifikasikan ancaman berdasarkan ancaman *Spoofing, Tampering, Repudiation, Information Disclosure* dan *Elevation of Privilege* (STRIDE). Hasil dari analisis tersebut kemudian diukur dengan bantuan kerangka kerja *Damage Potential, Reproducibility, Exploitability, Affected User* dan *Discoverability* (DREAD).

Dalam penelitian ini, yang menjadi fokus utama adalah sistem informasi logistik yang digunakan dalam kegiatan operasional perusahaan. Dalam manajemen risiko, penelitian ini selanjutnya dapat digunakan sebagai acuan untuk mengidentifikasi ancaman dan mengukur kemungkinan dampak risiko dapat lihat Gambar 1.

Gambar 1: Diagram Tahapan metode penelitian

Identifikasi Aset

Identifikasi aset informasi dalam sistem informasi manajemen logistik melibatkan proses wawancara dengan pengembang aplikasi dan pihak eksternal terkait. Wawancara ini sebagai langkah kritis yang memberikan pemahaman mendalam terhadap struktur dan keberlanjutan operasional sistem. Setelah dilakukan wawancara, proses dokumentasi diawali dengan menyusun informasi singkat tentang sistem informasi logistik. Dokumen ini berisi informasi tentang deskripsi sistem informasi manajemen logistik seperti yang disajikan dalam Tabel 1.

Tabel 1: Informasi Sistem Informasi Manajemen Logistik

Deskripsi	Merupakan sistem informasi manajemen logistik manajemen logistik berbasis *web* yang menyediakan layanan *online* bagi staff, admin logistik, dan admin kendaraan. Layanan untuk staf meliputi *control code, audit code, claim damage area*. Layanan untuk admin logistik meliputi data *domestic processing, import processing, vehicle data, destination change list, block list* dan *order list*. Adapun layanan untuk pihak admin kendaraan meliputi *truck vendor, dealer/delivery destination, overseas dealer inquiry* dan *truck master*.

Mengacu pada hal-hal lain yang dapat mengancam sistem informasi manajemen logistik selain kode pemrograman. Setiap dependensi diberi

nomor unik sebagai identifikasi dan dicatat sebagai ketergantungan eksternal (lihat Tabel 2) pada sistem informasi manajemen logistik. [4].

Tabel 2: Dependensi Eksternal

ID	Deskripsi
1	*Service web* sistem informasi manajemen logistik berjalan pada server *Linux* yang menjalankan *JEUS* sebagai *web server*
2	*Database server* yang digunakan adalah Tibero
3	Koneksi antara *web server* dan *database server* menggunakan jaringan internal perusahaan
4	Protokol komunikasi antara *web server dan database server* menggunakan TLS

Sistem Informasi Manajemen Logistik memberikan kemudahan dalam pengelolaan persediaan dan data logistik untuk perencanaan dan distribusi. Identifikasi aset informasi melibatkan pemahaman pengguna eksternal sistem. Sistem informasi manajemen logistik memberikan hak akses kepada entitas eksternal diwakili oleh tingkat kepercayaan. Proses identifikasi dan pencatatan dilakukan dengan cara memberikan nomor unik, nama dan deskripsi entitas. [4]. Hasil identifikasi tingkat kepercayaan pada Sistem Informasi Manajemen Logistik disajikan pada Tabel 3.

Tabel 3: Identifikasi Tingkat Kepercayaan pada Sistem Informasi Manajemen Logistik

ID	Pengguna	Deskripsi
TK1	*Uknown User*	Pengguna yang terkoneksi dengan *interface web* sistem informasi manajemen logistik namun tidak memiliki akses masuk
TK2	*Authorized User*	Pengguna sah yang memiliki akses masuk ke *web service* sistem informasi manajemen logistik
TK3	*Unauthorized User*	Pengguna sah yang memiliki akses namun tidak dapat masuk ke *web service* sistem informasi manajemen logistik
TK4	Staf	Pengguna yang berwenang untuk mengatur proses logistik
TK5	Admin logistik	Pengguna yang berwenang untuk mengatur logistik baik kendaraan maupun suku cadang yang memiliki kewenangan tertentu
TK6	Admin kendaraan	Pengguna yang berwenang pada bagian perakitan kendaraan
TK7	Administrator *database server*	Pengguna setingkat *administrator* yang memiliki akses penuh ke *database server* sistem informasi manajemen logistik
TK8	Administrator *web server*	Pengguna setingkat *administrator* yang memiliki akses penuh untuk mengkonfigurasi *web service* sistem informasi manajemen logistik
TK9	Proses *web server*	Proses yang dijalankan oleh *web server* sebagai kode tertentu dan memiliki akses langsung ke *database server*
TK10	*Database read user*	Pengguna yang memiliki akses hanya untuk membaca *database*
TK11	*Database read/write user*	Pengguna yang memiliki hak akses membaca dan menulis pada *database*

Tabel 4: Identifikasi Titik masuk pada Aplikasi

ID	Nama	Deskripsi	Tingkat Kepercayaan
1	*Port* HTTPS	*Web service* sistem informasi manajemen logistik hanya dapat diakses melalui protokol SSL/TLS	TK1 TK2 TK3 TK4 TK5 TK6
1.1	Halaman *login*	Pengguna wajib melakukan *login* untuk dapat mengakses layanan manajemen logistik	TK1 TK2 TK3 TK4 TK5 TK6
1.2	Fungsionalitas *login*	Fungsionalitas *login* menerima kredensial dari pengguna dan akan mencocokan kredensial tersebut dengan data yang ada di dalam *database*	TK2 TK3 TK4 TK5 TK6

Identifikasi titik masuk digunakan untuk melihat di mana penyerang dapat berinteraksi dengan aplikasi [4]. *Interface* adalah cara yang digunakan untuk melakukan interaksi antara manusia dan sistem [9]. Identifikasi juga dilakukan pada jalur komunikasi yang digunakan oleh sistem informasi manajemen logistik. Pemilihan port yang aman seperti HTTPS *(Hypertext Transfer Protocol Secure)* penting untuk mengenkripsi data yang dikirim antara pengguna dan sistem, sehingga mengurangi risiko potensial terhadap keamanan informasi yang dapat dieksploitasi oleh penyerang [3]. Berikut adalah hasil identifikasi titik masuk pada sistem informasi manajemen logistik yang disajikan pada Tabel 4.

Dalam penerapan sistem informasi manajemen logistik, setiap aset diidentifikasi yaitu *item* atau area yang mungkin menjadi celah bagi penyerang [4], termasuk pengguna *web uknown user* dan *authorized user*. Setiap proses identifikasi sistem infor-

masi manajemen logistik dikaitkan dengan tingkat kepercayaan. Hasil identifikasi aset sistem informasi manajemen logistik sistem informasi manajemen logistik selengkapnya disajikan pada Tabel 5.

Tabel 5: Identifikasi Titik masuk pada Aplikasi

ID	Nama	Deskripsi	Tingkat Kepercayaan
Aset 1	Pengguna layanan manajemen logistik	Aset yang berkaitan dengan pengguna	
Aset 1.1	Detail *Login* Pengguna	Kredensial login yang akan digunakan pegguna untuk masuk ke situs *web* sistem informasi manajemen logistik	TK2 TK4 TK5 TK6 TK7 TK9 TK10 TK11
Aset 1.2	Data logistik	*Web* sistem informasi manajemen logistik akan menyimpan informasi pengiriman berkaitan dengan pengguna	TK2 TK5 TK6 TK7 TK8 TK9 TK10 TK11
Aset 1.3	Data kendaraan	*Web* sistem informasi manajemen logistik akan menyimpan informasi kendaraan berkaitan dengan pengguna	TK4 TK5 TK6 TK7 TK8 TK9 TK10
Aset 2	Sistem	Aset yang berkaitan dengan sistem	
Aset 2.1	Ketersediaan situs *web*	*Web* sistem informasi manajemen logistik harus tersedia selama 24 jam dalam sehari dan dapat diakses oleh seluruh pengguna	TK7 TK8
Aset 2.2	Ketersediaan *database*	*Database* sistem informasi manajemen logistik harus tersedia dan dapat melayani permintaan data selama 24 jam dalam sehari	TK7 TK8
Aset 2.3	Eksekusi kode pemograman *web*	Kemampuan untuk menjalankan kode pemrograman di *web server*	TK8 TK9
Aset 2.4	Eksekusi perintah *SQL read database*	Kemampuan untuk menjalankan *SQL query select* pada *database*, bagi pengguna yang telah *login* ke sistem, sehingga dapat menerima informasi yang tersimpan pada *database*	TK5 TK6 TK7 TK10 TK11
Aset 2.5	Eksekusi perintah *SQL read/write database*	Kemampuan untuk menjalankan *SQL* bagi pengguna yang telah *login* ke sistem, sehingga memiliki akses pada *database*	TK7 TK11
Aset 2.6	Manajemen Data	Kemampuan *Administrator* untuk mengelola data pada sistem	TK5 TK6 TK7 TK11
Aset 2.7	Melihat *log*	Kemampunan *Administrator* sistem untuk melihat *log* terkait *web* dan *database*	TK7
Aset 3	Situs *Web*	Aset yang berkaitan dengan situs *web* layanan manajemen logistik	TK2
Aset 3.1	Sesi *Login*	Sesi *login* pengguna ke situs *web* layanan manajemen logistik	TK2 TK4 TK5 TK6 TK10 TK11
Aset 3.2	Layanan manajemen logistik	Pengguna yang telah *login* dapat mengakses segala layanan yang tersedia pada sistem informasi manajemen logistik	TK2 TK4 TK5 TK6 TK10 TK11
Aset 3.3	Akses ke *database server*	Memungkinkan seorang *administrator* untuk mengelola *database*, memberi akses penuh ke *database* pengguna dan semua data yang ada di dalam *database*.	TK7

Profil Aset Informasi

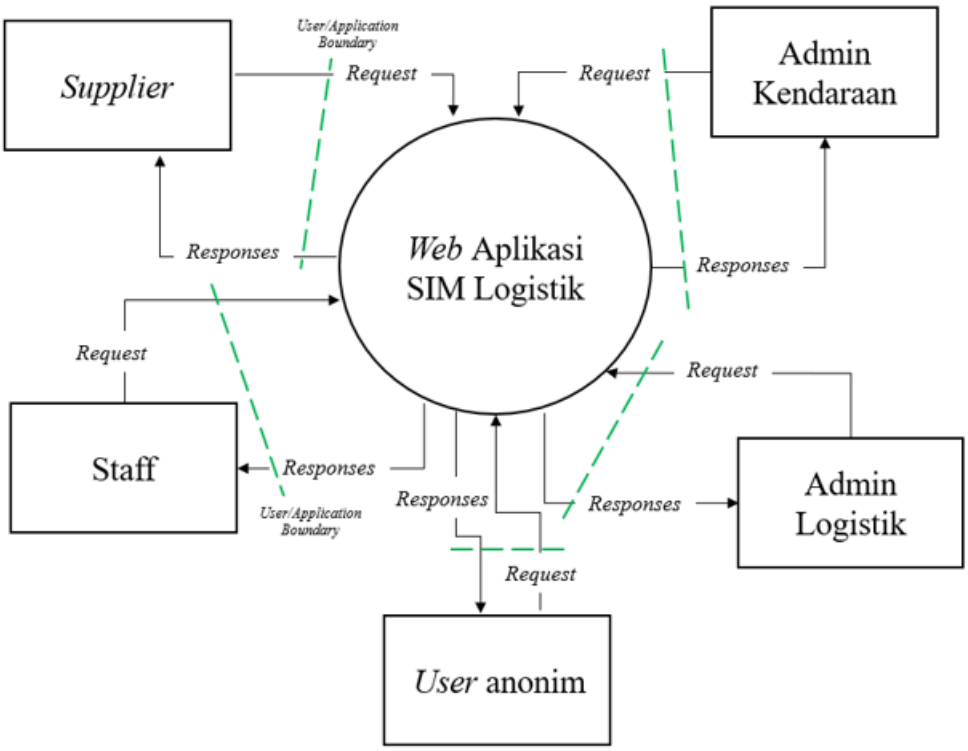
Profil aset informasi melibatkan pembuatan *Data Flow Diagram* (DFD) sebagai representasi visual alur informasi dalam sistem. DFD membantu memahami proses input, pemrosesan dan output, serta memberikan landasan untuk perancangan sistem yang efektif. Pemahaman pergerakan data dalam sistem memungkinkan pengetahuan tentang dimana data diubah atau disimpan oleh berbagai komponen [6]. Berikut adalah hasil penyusunan *Data Flow Diagram* sistem informasi manajemen logistik.

1. Context Diagram

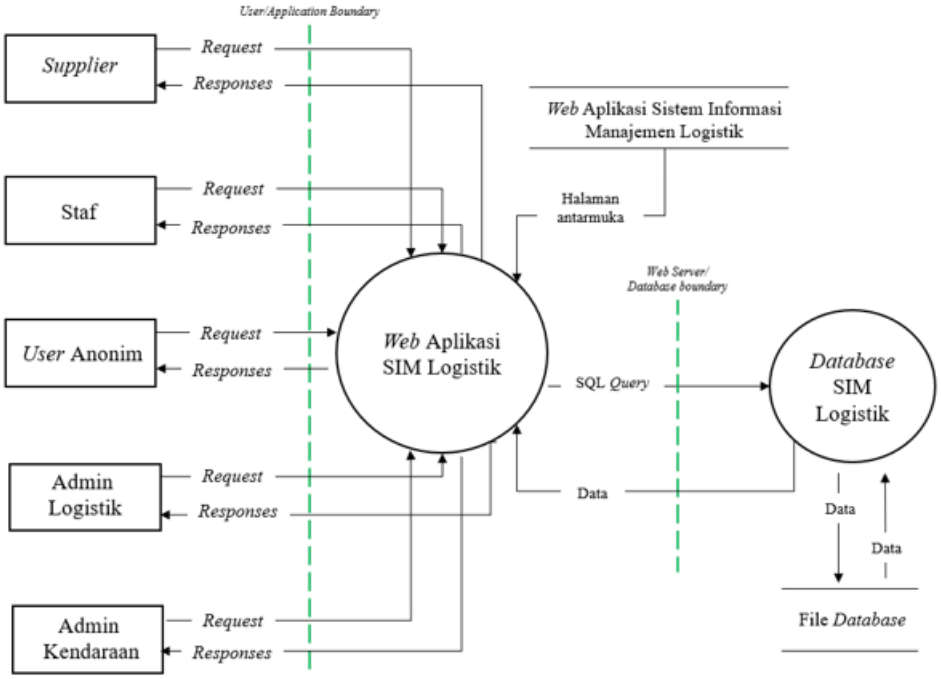
   Sistem Informasi Manajemen Logistik memulai alur data dengan input informasi dari *supplier* tentang barang dan material. Admin kendaraan juga memberikan data kendaraan. Data dari kedua sumber diproses oleh penerimaan dan penyimpanan di database logistik. Admin logistik mengelola stok dan koordinasi pengiriman dengan pemasok. Staf menggunakan sistem untuk mengatur pengiriman barang, melibatkan penjadwalan, metode pengiriman dan dokumen pengiriman. Sistem ini juga memberikan akses anonim ke informasi dan layanan. Alur DFD ini membentuk ekosistem terintegrasi, meningkatkan efisiensi dan transparansi dalam manajemen logistik seperti yang disajikan dalam Gambar 2.

2. *Data Flow Diagram* Sistem Informasi Manajemen Logistik Tingkat 1

   Pada DFD tingkat 1 untuk Sistem Informasi Manajemen Logistik, interaksi antara entitas utama dan proses utama berfokus pada akses melalui aplikasi web yang terintegrasi dengan database. Inisiasi dimulai dengan Supplier yang menggunakan interface aplikasi web untuk menyediakan informasi barang. Staf menggunakan aplikasi web untuk mengatur pengiriman, menjadwalkan operasi logistik dan membuat dokumen pengiriman. Admin logistik mengelola rantai pasokan, stok, pengiriman dan berkoordinasi dengan pemasok. Admin kendaraan memantau dan mengelola kendaraan logistik. Pengguna anonim dapat mengakses informasi umum tanpa autentikasi. Semua interaksi ini melibatkan aplikasi web yang terhubung dengan database disajikan pada Gambar 3.



Gambar 2: Context diagram sistem informasi manajemen logistik



Gambar 3: DFD sistem informasi manajemen logistik tingkat 1

Analisis Ancaman

Proses klasifikasi ancaman dilakukan dengan menerapkan metodologi STRIDE yang dikembangkan oleh Microsoft. STRIDE membantu mengidentifikasi kategori ancaman berdasarkan maksud dan tujuan serangan yang melibatkan *Spoofing, Tampering, Repudiation, Information disclosure, De-*

nial of Service, dan *Elevation of Privilege* [12]. Tujuan STRIDE adalah memastikan bahwa aplikasi memenuhi persyaratan keamanan CIA (*Confidentiality, Integrity*, dan *Availability*), serta *Authentication, Authorization* dan *Non-Repudiation*. CIA adalah standar yang digunakan banyak pihak untuk mengukur keamanan sebuah sistem [14]. Metodologi ini menyediakan serangkaian kategori ancaman dengan contoh yang membantu membuat identifikasi ancaman terstruktur dan sistematis. Dengan demikian, langkah-langkah ini bertujuan untuk menjaga keamanan aplikasi dan memastikan kepatuhan terhadap prinsip-prinsip keamanan informasi penting, seperti yang dijelaskan pada Tabel 6.

Tabel 6: Klasifikasi Ancaman STRIDE

Tipe	Jenis Ancaman
Spoofing	Ancaman akses tidak sah dan penggunaan kredensial pengguna lain, seperti nama pengguna dan kata sandi
Tamp ering	Ancaman yang mengubah data, baik dengan mengubah data yang disimpan dalam *database* atau dengan mengubah data yang dikirimkan melalui jaringan
Repudiation	Ancaman berupa tindakan ilegal dalam suatu sistem yang tidak mampu melacak tindakan yang dilakukan
Information Disclosure	Ancaman termasuk pembacaan *file* yang tidak sah atau pembacaan data selama transmisi
Denial of Service	Ancaman untuk menolak akses ke pengguna yang sah, seperti membuat *server web* tidak tersedia untuk sementara
Elevation of Privilege	Ancaman bertujuan untuk mendapatkan hak akses yang lebih tinggi, untuk mengakses informasi atau menembus sistem secara ilegal

Pengukuran Risiko dan Rencana Pengurangan Risiko

1. Pengukuran Risiko

   Metodologi DREAD digunakan untuk menilai, membandingkan dan memprioritaskan tingkat risiko yang ditimbulkan dari setiap ancaman. Istilah DREAD mengacu pada setiap kategori risiko, yaitu *Damage Potential, Reproducibility, Exploitability, Affected User* dan *Discoverability* dengan definisi sebagai berikut [4]:

   (a) *Damage potential*, yaitu seberapa besar potensi kerusakan yang terjadi jika serangan berhasil dilakukan.

   (b) *Reproducibility*, yaitu seberapa mudah untuk mereproduksi serangan.

   (c) *Exploitability*, yaitu berapa banyak waktu, tenaga, dan keahlian yang dibutuhkan untuk mengeksploitasi ancaman.

   (d) *Affected user*, yaitu seberapa banyak pengguna yang terpengaruh jika ancaman di eksploitasi.

   (e) *Discoverability*, yaitu seberapa mudah bagi penyerang untuk menemukan ancaman pada sistem.

   Risiko dengan peringkat tinggi dinilai sama dengan 3, peringkat sedang dinilai sama dengan 2 dan ancaman dengan peringkat rendah dinilai sama dengan 1, seperti yang disajikan dalam Tabel 7.

Tabel 7: Pengukuran Risiko

	Tinggi (3)	Sedang (2)	Rendah (1)
Damage Potential	Penyerang memperoleh kredensial dan otorisasi penuh, penyerang dapat menerobos keamanan sistem, memiliki akses admin, mampu mengunggah *content*	Membocorkan informasi penting perusahaan	Membocorkan informasi yang kurang penting
Reproducibility	Serangan dapat dilakukan secara berulang setiap saat	Serangan dapat diulangi dalam waktu tertentu	Serangan sulit diulangi meskipun celah keamanan sudah diketahui penyerang
Exploitability	Programmer pemula mampu membuat serangan dalam waktu yang relatif singkat	Programmer terlatih mampu membuat serangan yang dapat dipakai berulang kali	Serangan memerlukan seseorang dengan keahlian yang sangat terampil
Affected User	Seluruh pengguna	Hanya beberapa pengguna	Pengguna yang terdampak
Discoverability	Celah keamanan ditemukan pada fitur yang umum dipakai dan terlihat jelas	Celah keamanan berapa pada fitur yang jarang dipakai dan hanya pengguna tertentu yang dapat menemukannya	*Bug* tidak diketahui, pengguna tidak akan menemukan potensi celah keamanan

   Peringkat risiko diperoleh dari nilai total penjumlahan kategori ancaman DREAD dengan kategori risiko rendah dengan rentang nilai 5 - 7, kategori risiko sedang dengan rentang nilai 8 - 11 dan kategori risiko tinggi pada rentang nilai 12 - 15, seperti yang diuraikan pada Tabel 8.

Tabel 8: Peringkat Risiko

Rentang Nilai	Peringkat Risiko
5 – 7	Rendah
8 – 11	Sedang
12 – 15	Tinggi

2. Rencana Pengurangan Risiko

   Rencana keamanan merupakan hal yang strategis, yang harus dibangun dengan didahului melakukan penilaian risiko, dan mitigasi risiko [10]. Berdasarkan data pengukuran risiko pada Tabel 7, tindakan mitigasi dapat diatur berdasarkan klasifikasi ancaman. Daftar penilaian ancaman ini dapat di kelompokkan berdasarkan tingkat risiko untuk memudahkan melihat daftar ancaman yang berisiko.

Tabel 9: Klasifikasi Ancaman

ID	Deskripsi	Tingkat Kepercayaan	STRIDE
A1	Pengguna meninggalkan kredensial *login* di tempat umum, atau secara tidak sengaja menyimpan kredensial di *browser* komputer publik, atau membagikan kredensial dengan teman atau kerabat	TK2 TK4 TK5 TK6	S
A2	Pengguna secara tidak sengaja berbagi kredensial dengan orang lain, misal melalui serangan *social engineering*	TK2 TK4 TK5 TK6	S
A3	Seseorang yang mengetahui kredensial pengguna (misalnya teman atau kerabat) menyalahgunakan akun atau identitas pengguna untuk melakukan suatu tindak kejahatan	TK2 TK4	S
A4	Administrator menyalahgunakan akun atau identitas pengguna untuk melakukan kejahatan	TK5 TK6 TK7	S
A5	Penyerang memalsukan halaman *login* untuk mendapatkan kredensial pengguna	TK2 TK4 TK5 TK6	S
A6	Admin dengan sengaja atau tidak sengaja menambah, mengubah, atau menghapus data pengguna dari sistem *database* di luar peraturan	TK5 TK7	T
A7	Penyerang dengan sengaja menambah, mengubah, atau menghapus informasi yang disimpan pada sistem *database*	TK2 TK4 TK5 TK6 TK7	T
A8	Seseorang menggunakan identitas pengguna yang sah untuk melakukan tindak kejahatan	TK2 TK4 TK5 TK6 TK7	R
A9	Penyangkalan pihak pengguna yang sah bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	TK2 TK4	R
A10	Penyangkalan pihak admin bahwa tidak melakukan tindakan menambah, mengubah, atau menghapus data	TK5 TK4 TK7 TK8	R
A11	Pencatatan *log* yang minim sebagai bukti penanganan klaim penyangkalan	TK2 TK4 TK5 TK6 TK7 TK9 TK11	R
A12	Penyerang membaca informasi pribadi pengguna yang tersimpan pada sistem *database*	TK2 TK4	I
A13	Penyerang menyebarluaskan informasi tentang data pribadi pengguna	TK2 TK4	I
A14	Penyerang mengumpulkan data pengguna sebagai target tindak kejahatan	TK2 TK4	I
A15	Penyerang membanjiri *bandwidth* melalui banyak *request* dengan maksud untuk memperlambat atau bahkan menumbangkan sistem	TK9 TK11	D
A16	Penyerang mengunggah banyak *file* dengan maksud untuk memenuhi media penyimpanan *database*	TK2 TK4 TK9 TK11	D
A17	Seseorang bukan pengguna yang sah mengakses sistem menggunakan kredensial *login* pengguna yang memiliki akses lebih tinggi	TK2 TK4 TK5 TK6 TK7	E

Hasil dan Pembahasan

Berdasarkan klasifikasi ancaman STRIDE pada Tabel 6, setiap tindakan ancaman yang teridentifikasi memiliki hubungan dengan entitas eksternal yang direpresentasikan sebagai tingkat kepercayaan. Ancaman pada sistem informasi manajemen logistik akan diidentifikasi dengan mengacu pada kategori STRIDE di Tabel 6. Kemudian ancaman akan diidentifikasi keterkaitannya dengan tingkat kepercayaan pada Tabel 3. Identifikasi ancaman pertama adalah keteledoran pengguna terhadap informasi login miliknya. Ancaman ini ditandai dengan nomor identitas A1 (Ancaman 1) dan dicari keterkaitannya dengan level kepercayaan di Tabel 3. Sesuai kategori STRIDE di Tabel 6, maka diketahui bahwa tipikal ancaman A1 merupakan ancaman kategori spoofing, yaitu tindak ancaman yang ditujukan untuk mengakses dan menggunakan kredensial pengguna lain secara ilegal. Ancaman A1 kemudian diidentifikasi keterkaitannya dengan level kepercayaan dan diketahui bahwa A1 memiliki keterkaitan dengan TK2, TK4, TK5, dan TK6. Hasil identifikasi selengkapnya disajikan pada Tabel 9.

Hasil klasifikasi dapat diuraikan menjadi beberapa potensi ancaman terutama pada ancaman Spoofing dengan nilai total ancaman adalah 5 ancaman, sedangkan ancaman Tampering sebanyak 2 ancaman dan ancaman Repudiation dengan total ancaman 4. Information Disclosure sebanyak 3 ancaman, sedangkan Denial of Service terdapat 2 ancaman dan Elevation of Privilege dimana pada kategori ancaman tersebut mendapatkan total ancaman adalah 1, seperti yang disajikan pada Tabel 10.

Tabel 10: Hasil Klasifikasi Ancaman

Kategori Ancaman	Jumlah Ancaman
Spoofing	5
Tampering	2
Repudiation	4
Information Disclosure	3
Denial of Service	2
Elevation of Privilege	1

Proses pengukuran risiko menggunakan metode DREAD dengan contoh ancaman A1 (pengguna meninggalkan kredensial login di tempat umum). Ancaman ini dinilai pada 4 tingkatan kepercayaan (TK2, TK4, TK5 dan TK6). Adapun langkah penilaian ancaman A1 pada TK2 (pengguna dengan kredensial login valid) adalah sebagai berikut:

1. (D) *Damage Potential:* Potensi kerusakan rendah (nilai 1) karena hanya satu staf yang terkena dampak.
2. (R) *Reproducibility:* Mudah diproduksi (nilai 3) karena penyerang dapat memproduksi serangan secara berulang.
3. (E) *Exploitability:* Mudah di eksploitasi (nilai 3) karena keteledoran pengguna.
4. (A) *Affected User:* Jumlah pengguna terpengaruh minim (nilai 1) hanya satu akun staf.
5. (D) *Discoverability:* Mudah ditemukan (nilai 3) karena keteledoran pengguna.

Berdasarkan proses penilaian ancaman setiap kategori DREAD pada langkah ketiga, diperoleh nilai setiap kategori yaitu D = 1, R = 3, E = 3, A = 1, dan D = 3, sehingga dihasilkan total nilai ancaman A1 pada TK2 adalah 11 yang memiliki risiko sedang. Seluruh ancaman dengan tingkat kepercayaan dinilai dengan langkah-langkah yang serupa. Penilaian setiap kategori DREAD untuk setiap ancaman yang teridentifikasi disajikan pada Tabel 11.

Hasil rencana pengurangan risiko di perusahaan logistik dilaksanakan dengan cara memberikan pengetahuan kepada pengguna terkait dengan ancaman yang dapat ditimbulkan pada proses pekerjaan, antara lain untuk mengabaikan fitur penyimpanan password pada browser, mengabaikan segala bentuk permintaan kredensial yang melalui tautan yang tidak tepercaya dan tidak memberitahukan kredensial kepada siapa pun tanpa terkecuali. Pada sisi sistem juga diberikan penguatan antara lain menambahkan fitur multi faktor autentikasi terkait dengan login pengguna, penerapan timestamp yang akan tercatat otomatis pada sistem sehingga sistem dapat memberitahukan informasi terakhir yang terjadi pada sistem, melakukan access control list kepada pengguna yang memang berhak mengakses sistem dan data perusahaan juga melakukan penerapan kriptografi sehingga komunikasi antara pengguna, sistem dan database menjadi lebih aman. Rencana pengurangan risiko selengkapnya ditunjukkan pada Tabel 12.

Penutup

Pemodelan ancaman pada sistem informasi manajemen logistik dilakukan dengan menggunakan metode STRIDE guna mengidentifikasi jenis ancaman, sedangkan metode DREAD digunakan untuk mengukur tingkat ancaman dan risikonya. Adapun tujuan penelitian ini adalah memahami ancaman yang mungkin dapat timbul dan mengganggu sistem serta merancang strategi mitigasi yang efektif untuk menjaga data dan memastikan kegiatan operasional perusahaan logistik dapat berjalan dengan sebagaimana mestinya.

Tabel 11: Hasil Pengukuran Risiko

Ancaman	Tingkat Kepercayaan	D	R	E	A	D	Total	Risiko
A1	TK2	1	3	3	1	3	11	Sedang
A1	TK4	2	3	3	2	3	13	Tinggi
A1	TK5	3	3	3	3	3	15	Tinggi
A1	TK6	3	3	3	3	3	15	Tinggi
A2	TK2	1	3	2	1	2	9	Sedang
A2	TK4	2	3	2	2	2	11	Sedang
A2	TK5	3	3	2	3	2	13	Tinggi
A2	TK6	3	3	2	3	2	13	Tinggi
A3	TK2	2	3	3	1	3	12	Tinggi
A3	TK4	2	3	3	2	3	13	Tinggi
A4	TK5	2	3	3	2	3	13	Tinggi
A4	TK6	2	3	3	2	3	13	Tinggi
A4	TK7	3	3	3	3	3	15	Tinggi
A5	TK2	1	2	2	1	2	8	Sedang
A5	TK4	2	2	2	2	2	10	Sedang
A5	TK5	3	2	2	3	2	12	Tinggi
A5	TK6	3	2	2	3	2	12	Tinggi
A6	TK5	2	3	3	3	3	14	Tinggi
A6	TK7	3	3	3	3	3	15	Tinggi
A7	TK2	1	3	3	1	2	10	Sedang
A7	TK4	2	3	3	2	2	12	Tinggi
A7	TK5	2	3	3	3	2	13	Tinggi
A7	TK6	2	3	3	3	2	13	Tinggi
A7	TK7	3	3	2	3	1	12	Tinggi
A8	TK2	1	2	2	1	2	8	Sedang
A8	TK4	2	2	2	2	2	10	Sedang
A8	TK5	2	2	2	3	2	11	Sedang
A8	TK6	2	2	2	3	2	11	Sedang
A8	TK7	3	2	2	3	2	12	Tinggi
A9	TK2	1	2	2	1	2	8	Sedang
A9	TK4	2	2	2	2	2	10	Sedang
A10	TK5	2	2	2	2	2	10	Sedang
A10	TK6	2	2	2	2	2	10	Sedang
A10	TK7	3	2	2	2	2	11	Sedang
A10	TK8	3	2	2	2	2	11	Sedang
A11	TK2	1	2	2	1	2	8	Sedang
A11	TK4	2	2	2	2	2	10	Sedang
A11	TK5	2	2	2	2	2	10	Sedang
A11	TK6	2	2	2	2	2	10	Sedang
A11	TK7	3	2	2	3	2	12	Tinggi
A11	TK8	3	2	2	3	2	12	Tinggi
A11	TK9	3	2	2	3	1	11	Sedang
A11	TK11	3	2	2	3	1	11	Sedang
A12	TK2	1	2	2	1	2	8	Sedang
A12	TK4	2	2	2	2	2	10	Sedang
A13	TK2	1	2	2	1	2	8	Sedang
A13	TK4	2	2	2	2	2	10	Sedang
A14	TK2	1	2	2	1	1	7	Rendah
A14	TK4	1	2	2	1	1	7	Rendah
A15	TK9	3	1	1	3	1	9	Sedang
A15	TK11	3	1	1	3	1	9	Sedang
A16	TK2	1	2	2	3	2	10	Sedang
A16	TK4	2	2	2	3	2	11	Sedang
A16	TK9	3	1	1	3	3	11	Sedang
A16	TK11	3	1	1	3	3	11	Sedang
A17	TK2	1	2	2	1	2	8	Sedang
A17	TK4	2	2	2	2	2	10	Sedang
A17	TK5	2	1	1	3	1	8	Sedang
A17	TK6	2	1	1	3	1	8	Sedang
A17	TK7	3	1	1	3	1	9	Sedang

Tabel 12: Rencana Pengurangan Risiko

1	Ancaman	A1, A2, A3, A5
	Tingkat Kepercayaan	TK4, TK5, TK6
	Kategori	*Spoofing*
	Bidang Keamanan	*Authentication*
	Rencana Pengurangan Risiko	1. Abaikan fitur penyimpanan *username* dan *password* yang ditawarkan pada *browser* 2. Penggunaan mode *browser incognito/private* ketika menggunakan komputer publik untuk mengakses sistem 3. Menghindari pencatatan *password* di media apapun 4. Tidak memberitahukan kredensial *login* miliknya ke orang lain tanpa terkecuali 5. Abaikan segala jenis permintaan informasi kredensial *login* melalui tautan yang tidak terpercaya 6. Sosialisasi kepada pengguna tentang pentingnya keamanan dan kewaspadaan terhadap kredensial *login* miliknya. 7. Menambahkan multifaktor autentikasi pada sistem 8. Proses validasi kredensial pengguna menggunakan OTP
2	Ancaman	A6, A7
	Tingkat Kepercayaan	TK4, TK5, TK6, TK7
	Kategori	*Tampering*
	Bidang Keamanan	*Integrity*
	Rencana Pengurangan Risiko	1. Penerapan *timestamp* yang akan tercatat secara otomatis pada *log* perubahan data 2. Pencatatan *log* tentang segala perubahan data 3. Daftar kontrol akses menggunakan *Access Control List* 4. Melakukan penerapan kriptografi
3	Ancaman	A8, A11
	Tingkat Kepercayaan	TK7, TK8
	Kategori	*Repudiaction*
	Bidang Keamanan	*Confirmation*
	Rencana Pengurangan Risiko	1. Segala sesuatu tindakan pada sistem harus dicatat pada *log* untukbahan pembuktian atas terjadinya suatu tindakan pada sistem 2. Penerapan *request merge* yang akan tercatat secara otomatis pada *log* jika ada perubahan data. 3. Penerapan *digital signature* untuk memvalidasi perubahan

Hasil analisis menunjukan bahwa ancaman dengan tingkat risiko tertinggi berasal dari kategori *spoofing, tampering* dan *repudiation*. Sedangkan in*formation disclosure* dan *denial of service* memiliki risiko sedang. Selanjutnya berdasarkan pengukuran risiko dengan menggunakan metode DREAD ditemukan bahwa beberapa ancaman memiliki skor risiko tinggi. Hal ini dapat berdampak serius pada sistem dan proses operasional jika tidak segera diatasi.

Untuk mengurangi risiko tersebut, terdapat beberapa langkah mitigasi yang dapat direkomendasikan antara lain dengan cara menonaktifkan penyimpanan kredensial pada *browser*, menggunakan multi faktor autentikasi, penerapan *access control list* dan menggunakan enkripsi data agar komunikasi dan informasi pada sistem tetap dalam kondisi aman.

Dengan menerapkan strategi ini, perusahaan logistik diharapkan dapat mengurangi risiko serangan siber dan menjaga kelangsungan operasional perusahaan.

Daftar Pustaka

[1] M. Abomhara, GM, Køien, and M. Gerdes, "A STRIDE-based threat model for telehealth systems," Conference: Norsk informasjonssikkerhetskonferanse (NISK2015), 82-96, 2015.

[2] Avriyanti S, "Strategi bertahan bisnis ditengah pandemi covid-19 dengan memanfaatkan bisnis digital (studi pada ukm yang terdaftar pada dinas koperasi, usaha kecil dan menengah kabupaten Tabalong)," Jurnal PubBis. 5(1): 60–74, https://doi.org/10.35722/pubbis.v5i1.380, 2021.

[3] Anonym, "Security Considerations For Your Website (ITSM.60.005)," Canadian Centre for Cyber Security, diakses daring pada https://www.cyber.gc.ca/en/guidance/security-considerations-your-website-itsm60005, 2022.

[4] L Conklin, "CRV2 App Threat Modeling," diakses daring pada https://owasp.org/www-community/CRV2_AppThreatModeling, 2020.

[5] Tatya Fara Regyna, Dian Agustina, dan Firana Nazzilla Pramdista, "Sistem Manajemen Keamanan Informasi," OSF Preprints t7keb, Center for Open Science, doi:10.31219/osf.io/t7keb, 2022.

[6] J. Fruhlinger, "Threat Modeling Explained: A Process For Anticipating Cyber Attacks," CSO - IDG Communications Inc., diakses daring pada https://www.csoonline.com/article/3537370/threat-modeling-explained-a-process-for-anticipating-cyber-attacks.html, 2020.

[7] Muhammad Khairul Faridi, Imam Riadi, dan Yudi Prayudi, "Pemodelan ancaman sistem keamanan e-health menggunakan metode STRIDE dan DREAD," Edumatic, 5(2):157-166, doi:10.29408/edumatic.v5i2.3652, 2021.

[8] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," IEEE PES ISGT-Europe 1–6. 10.1109/ISGTEurope, 2017.8260283, 2017.

[9] FN. Khasanah, S. Rofiah, D. Setiyadi, "Metode user centered design dalam merancang tampilan antarmuka ecommerce penjualan pupuk berbasis website menggunakan aplikasi balsamiq mockups," JAST, 3(2):14-23, doi: https://doi.org/10.33366/jast.v3i2.1443, 2019.

[10] RL. Krutz and RD. Vines, "The CISSP Preparation Guide,"Indianapolis, Wiley Publishing Inc, 2003.

[11] Anonym, What Is the DREAD Cybersecurity Model, Logixconsulting, diakses daring pada https://www.logixconsulting.com/2019/12/18/what-is-the-dread-cybersecurity-model/, 2019.

[12] H. Mahmood, "Application Threat Modeling using DREAD and STRIDE," haiderm.com, diakses daring pada https://haiderm.com/application-threat-modeling-using-dread-and-stride/, 2017.

[13] R. Muttaqien, "Rancang bangun aplikasi mobile untuk peminjaman barang menggunakan layanan web (studi kasus: kantor BPN kota Langsa)," KITEKTRO, 4(4):1–9, 2019.

[14] TR. Peltier, "Information Security Risk Analysis," Second Edition, New York, Auerbach Publications, Taylor & Francis Group, 2005.

[15] DD. Prasetyowati, Indra Gamayanto, S. Wibowo, dan Suharnawi, "Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang," JOINS, 4(1):65–75, https://doi.org/10.33633/joins.v4i1.2429, 2019.

[16] NI. Putri, MI. Fudsyi, R. Komalasari, dan Z. Munawar, "Peran teknologi informasi pada perubahan organisasi dan fungsi akuntansi manajemen," JRAK, 7(2), 47–58, 2021.

[17] A. Saputra, N. elmiawati, dan Maya Armys Roma Sitorus, "Penilaian ancaman pada website transkrip aktifitas mahasiswa Politeknik Negeri Batam menggunakan metode DREAD," Jurnal Integrasi, 9(1):53, https://doi.org/10.30871/ji.v9i1.281, 2017.

[18] T. Sutabri, "Konsep Sistem Informasi," Yogyakarta, Andi, 2012.

[19] AC. Widhiyanto, "Rancang Bangun Web Server Berbasis Jaringan Cisco Catalyst Series 2960 di PT. Telekomunikasi Indonesia DIVRE V Jatim," Skripsi, Fakultas Teknologi dan Informatika, Universitas Dinamika, Surabaya, 2019.

[20] TD. Wismarini dan A. Prihandono, "Rancang bangun aplikasi android terintegrasi web service dengan volley untuk layanan publik," Dinamik, 25(1):10–19, doi: https://doi.org/10.35315/dinamik.v25i1.7515, 2020.