p-ISSN
e-ISSN
JURNAL AKUNTANSI, MANAJEMEN DAN BISNIS DIGITAL

Security Planning Identification Model in E-Business

Model Identifikasi Perencanaan Keamanan pada E-Business

Muhammad Rifki Damanik [1)]; Musdiansyah Putra [2)]
[1,2)] UIN Sumatera Utara
Email: [1)] mhdrifki77@gmail.com; [1)] musdiansyahputra2001@gmail.com

ARTICLE HISTORY
Received [30 Desember 2021]
Revised [05 Januari 2022]
Accepted (08 Januari 2022]

KEYWORDS
E-Business, Securiy Plan

ABSTRAK
E-Business sebagai salah satu entitas yang mampu menghasilkan keuntungan bagi organisasi / perusahaan maupun individu adalah aset yang berharga yang harus dijaga dan dilindungi. Dalam proses menjaga tersebut, tidaklah mudah dikarenakan banyak rintangan dan masalah yang harus dihadapi. Berbagai masalah yang mengancam keamanan e-Business perlu di lakukan identifikasi agar kedepannya sistem dapat menangkal ancaman-ancaman tersebut. Proses identifikasi sebagai lapisan pertama atau tahap awal dari tahapan-tahapan manajemen keamanan dalam e-Business, adalah sangat penting dilakukan karena tahapan selanjutnya yaitu proses evaluasi resiko, hasilnya bergantung pada temuan yang berhasil diidentifikasi dari tahap ini. Pendekatan yang dilakukan dalam merancang model identifikasi perencanaan keamanan yaitu melalui studi literatur yang berhubungan dengan proses manajemen keamanan e-Business. Hasil yang diharapkan dari perumusan adalah berupa rekomendasi proses-proses apa saja yang perlu dilakukan dalam melakukan identifikasi perencanaan keamanan pada e-Business.

ABSTRACT
E-Business as an entity that is able to generate profits for organizations / companies and individuals is a valuable asset that must be maintained and protected. In the process of maintaining this, it is not easy because there are many obstacles and problems that must be faced. Various problems that threaten the security of e-Business need to be identified so that in the future the system can ward off these threats. The identification process as the first layer or the initial stage of the stages of security management in e-Business, is very important to do because the next stage is the risk evaluation process, the results depend on the findings that have been identified from this stage. The approach taken in designing a security planning identification model is through a literature study related to the e-Business security management process. The expected results from the formulation are in the form of recommendations for what processes need to be carried out in identifying security plans in e-Business.

PENDAHULUAN

Dalam proses manajemen keamanan e-Business, dibutuhkan strategi pelaksanaan yang tepat. Tahap identifikasi rencana keamanan e-Business adalah penting artinya dikarenakan tahap tersebut merupakan tahapan awal yang menjadi dasar dari segala tahapan dalam menajemen keamanan e-Business (Vasilyevna, 2008). Dalam melakukan identifikasi perlu dipikirkan apa saja yang menjadi tujuan dari manajemen keamanan e-Business. Tujuan yang dimaksud antara lain adalah kerahasiaan (confidentiality), integritas (integrity) dan ketersediaan (availability) (Tyagi dan Srinivasan, 2011). Mengacu pada tujuan manajemen keamanan e-Business tersebut, maka dalam penelitian ini, penulis mengajukan model identifikasi dalam perencanaan manajemen keamanan e-Business dengan melakukan modifikasi pada pendekatan arsitektur perencanaan sebagai penjabaran dari model identifikasi tersebut. Pemodifikasian model ini bertujuan memberikan pendekatan yang lebih optimal melalui penambahan cakupan proses identifikasi dalam mengindentifikasi rencana keamanan dalam arsitektur keamanan e- Business.menggunakan jaringan lain untuk mendukung proses bisnisnya (Combe, 2006).

E-Business bertujuan untuk meningkatkan daya saing organisasi / perusahaan dengan menyebar luaskan informasi yang inovatif dan teknologi komunikasi di seluruh organisasi melalui link kepada mitra dan pelanggan, tidak sebatas pada penggunaan teknologi untuk melakukan otomasi proses bisnis suatu organisasi/perusahaan tetapi harus juga mencapai proses transformasi dengan menerapkan teknologi untuk mengubah proses bisnis yang telah ada (Chaffey, 2009). Dari definisi di atas dapat di tarik kesimpulan bahwa e-Business melibatkan atau mengguanakan teknologi sebagai pendukung dalam meningkatkan semua aspek yang di miliki organisasi / perusahaan sebagai salah satu usaha mengoptimalkan value chain organisasi.

LANDASAN TEORI

Definisi E-Business

Sebagai penggunaan E-Business dapat di definisikan media jaringan internet dengan harapan dapat meningkatkan proses bisnis, perdagangan elektronik, komunikasi organisasi dan

mengkolaborasikan perusahaan dengan pelanggan, pemasok dan stakeholder lainya, e-Business menggunakan internet, intranet, extranet dan menggunakan jaringan lain untuk mendukung proses bisnisnya.

E-Business bertujuan untuk meningkatkan daya saing organisasi / perusahaan dengan menyebar luaskan informasi yang inovatif dan teknologi komunikasi di seluruh organisasi melalui link kepada mitra dan pelanggan, tidak sebatas pada penggunaan teknologi untuk melakukan otomasi proses bisnis suatu organisasi/perusahaan tetapi harus juga mencapai proses transformasi dengan menerapkan teknologi untuk mengubah proses bisnis yang telah ada. Dari definisi di atas dapat di tarik kesimpulan bahwa e-Business melibatkan atau mengguanakan teknologi sebagai pendukung dalam meningkatkan semua aspek yang di miliki organisasi / perusahaan sebagai salah satu usaha mengoptimalkan value chain organisasi.

Electronic Data Interchange (EDI)

EDI (Electronic Data Intercange) merupakan standar dalam melakukan pertukaran data / dokumen dalam organisasi dalam bentuk elektronik antar aplikasi komputer, banyak prosedural yang dilakukan dalam e-Business dalam melakukan pertukaran data yang melibatkan EDI sebagai salah satu standar seperti pesanan pembelian dan faktur. Ada beberapa fitur utama dalam EDI (Minoli, 1998) diantaranya :

a. Penggunaan media transmisi elektronik.
b. Penggunaan pesan diformat berdasarkan standar yang disepakati.
c. Pengiriman dokumen elektronik dapat dilakukan dengan cepat dari pengirim ke penerima
d. Komunikasi langsung antara aplikasi dan sistem.

Infrastruktur E-Business

Infrastruktur e-Business secara langsung mempengaruhi kualitas layanan bagi para pengguna sistem baik organisasi/perusahaan dalam hal kecepatan dan responsif. Infrastruktur e-Business mengkombinasikan perangkat keras (*hardware*) dan perangkat lunak (*software*) dalam organisasi / perusahaan bertujuan memberikan pelayanan kepada para pekerja, mitra dan pelanggan mereka. Terlihat pada gambar 1 beberapa komponen arsitektur e- busines yang saling berhubungan dan perlu dikelola dengan baik, beberapa lapisan dalam komponen tersebut dapat dipahami sebagai tugas yang perlu di pahami oleh setip pengguna e-Business baik organisasi / perusahaan.

Infrastruktur Kemanan E-Business

Keamanan merupakan isu yang paling mendasar yang mempengaruhi dalam pengelolaan e-Business oleh suatu organisasi / perusahaan, transaksi yang aman menjadi tolah ukur dalam memberi nilai lebih (*high value*) kepada pelanggan dan keamanan juga menjadi dasar kepercayaan dalam bertransaksi dalam lingkungan e-Business.

Infrastruktur kemanan e-Business di rancang sebagai model desain kemanan dalam e-Business agar dapat membantu organisasi/ perusahaan untuk membangun, memelihara keamanan dalam mengoperasikan e-Business secara aman dalam menjalankan aplikasi di dalam e-busines kemanan e-Business yang terdiri dari 4-layer *physical access*, *network communication, operating systems dan application*.

Bentuk Pelanggaran Keamanan pada E- Business

Banyak cara dimana kemanan sistem dapat di langgar atau di serang mulai dari kegiatan kriminal serius, suatu organisasi / perusahaan harus mulai menentukan arah kebijakan mereka dalam menyiasati pemasalahan kemanan yang muncul dan seiring perkembangan nya yang mulai serius mengancam, perusahaan harus siap dalam membangun langkah-langka pencegahan serangan keamanan untuk dapat melindungi data internal perusahaan seperi data transaksi, konsumen dan aset komersial lainya dari beberapa serangan berikut seperti hacking, spam, fraud dan kekeliruan dalam mengidentifikasi (*misrepresentation of identity*) ini merupakan beberapa serangan yang umum dilakukan:

a. Haking
   Haking merupakan kegiatan dimana sesorang dengan sengaja dan secara ilegal melakukan akses ke suatu sistem jaringan bertujuan untuk mendapatkan informasi berharga seperti kartu kredit dan melakukan penipuan dengan cara menggunakan informasi yang telah di dapat. Ada beberapa jenis kegiatan dalam heking diantaranya pemantauan informasi, mengakses database dan *Denial Of Service*.

p-ISSN
e-ISSN
JURNAL AKUNTANSI, MANAJEMEN DAN BISNIS DIGITAL

b. Spam
Spam merupakan e-mail yang dikirim ke alamat secara acak dan disebut sebagai 'e-mail sampah', spam telah menjadi masalah yang signifikan untuk organisasi / perusahaan dan individu untuk menangani permasalahannya, motivasi pengiriman spam e-mail bermacam-macam seperti berbentuk iklan dan lainya.

c. Fraud
Fraud atau sering di sebut penipuan merupakan salah satu hambatan terbesar untuk pertumbuhan internet untuk bisnis dan perdagangan. Skala sebenarnya dari aktivitas penipuan di internet tidak pernah diketahui karena banyak korban memilih untuk tidak melaporkan kejahatan dan perusahaan memilih untuk menghindari publikasi akibat penipuan ini dengan tujuan menjaga kenyamanan dari konsumen mereka.

METODE PENELITIAN

Penelitian merupakan penelitian studi literatur dengan menelaah beberapa jurnal terkait model identifikasi perencanaan keamanan pada e-business. Hasil yang diharapkan Hasil yang diharapkan dari perumusan ini berupa rekomendasi proses-proses apa saja yang perlu dilakukan dalam melakukan identifikasi perencanaan keamanan pada e-Business.

HASIL

Proses identifikasi ini dirasa sangat penting dikarenakan proses ini adalah proses awal dan sebagai dasar untuk melakukan proses-proses selanjutnya. Dalam paper penelitian ini, rumusan Vasilyevna di modifikasi dengan penambahan 1 layer management untuk melengkapi arsitektur *three layer* yang disebutkan sebelumnya. Layer tersebut adalah *Tool Identification*. Adapun 4 (empat) layer pendekatan yang digunakan untuk menjabarkan proses perencanaan sebagai bagian dari 10 tahapan manajemen keamanan pada e-Busines yakni *aset identification*, *risk identification*, *action planning* dan *tool identification*, lebih detailnya akan dijelaskan sebagai berikut.

1. Pendekatan Aset Identification
   Dalam proses identifikasi keamanan, perlu didefinisikan aset berharga yang akan diamankan. Pada e-Business aset yang dimaksud adalah data atau informasi yang tersimpan dalam database, infrastruktur hardware (server, router, dsb) pada pusat layanan e-Business dan perangkat lunak (software) sebagai antarmuka dalam mengakses layanan e-Business
2. Pendekatan *Risk Identification*
   Untuk mempermudah mengidentifikasi resiko yang mungkin terjadi, pertama dapat kita lihat, dari aset berharga yang telah kita definisikan, maka kita dapat menentukan resiko yang mungkin terjadi. Bila aset berupa data dan informasi, resiko yang mungkin terjadi adalah data rusak, data hilang, data dimodifikasi oleh pihak yang tidak berwenang dan sejenisnya. Bila aset berupa perangkat keras, maka resiko yang akan terjadi kemungkinan besar adalah perangkat hilang dicuri, perangkat mengalami kerusakan pada komponen elektronik dan salah konfigurasi pada perangkat yang mengakibatkan perangkat beroperasi tidak sebagaimana mestinnya. Bila aset adalah perangkat lunak (software) berupa halaman web, web service, driver dan sistem operasi, maka kemungkinan resiko yang terjadi adalah apikasi dalam e-Business mudah di eksploitasi oleh pihak yang tidak kita inginkan akibat kesalahan konfigurasi, celah keamanan dan bug yang belum di patch dan sejenisnya. Dalam risk identification, tidak sebatas aset saja yang di nilai akan resiko yang berpeluang muncul. Resiko lain adalah misalnya penggunaan hak akses yang tidak sesuai, pengaksesan resource oleh tanpa ijin yang jelas dan sebagainya.
3. Pendekatan Tool Identification
   Pendekatan yang ditawarkan sebelumnya akan lebih optimal lagi bila *tool identification* disertakan kedalamnya. *Tool* atau alat, disadari sebagai bagian yang perlu di identifikasi. Alat yang dimaksud ini bukan termasuk aset yang perlu diamankan, melainkan “alat” ini yang akan digunakan untuk mengamankan aset.

KESIMPULAN DAN SARAN

Penjabaran proses perencanaan identifikasi keamanan melalui pendekatan 4 (empat) layer identifikasi yakni layer tool identification yang digabungkan bersama aset identification, risk identification, tool identification dan action planning , membuat cakupan proses identifikasi menjadi lebih luas, lengkap dan lebih detail. Proses identifikasi pun lebih terarah dan tepat sasaran.

Output dari proses identifikasi yang dilakukan dengan empat pendekatan tersebut menjadi lebih siap untuk masuk ke tahap selanjutnya yaitu dalam tahap evaluate risk sebagai bagian dari 10 tahapan strategi manajemen keamanan e-Business**.**

DAFTAR PUSTAKA

Balawe, Mateus Mas. *Tinjauan Keamanan Sistem Transaksi dan Pembayaran Pada ECommerce* Studi Kasus Toko Online www.buahonline.com. Kupang: STIKOM Artha Buana Kupang. 2013

Karmakar, N. (2003*). Digital Security, Privacy and Law in Cyberspace: A Global Overview. In Proceedings of the International Association for the Development of Information Systems (IADIS),* Lisbon, Portugal, 3 –6 June, pp. 528 –3 6.

Tumbelaka, Rolan. Dkk. *model identifikasi perencanaan keamanan pada e-business,* Seminar Nasional Aplikasi Teknologi Informasi 2012 (SNATI 2012) Yogyakarta, 15-16 Juni 201. ISSN: 1907-5022