ADMINISTRASI DAN MANAGEMEN SISTEM JARINGAN
TUGAS 1 UJIAN AKHIR SEMESTER

OLEH :

AULIA MELYNDA PUTRI

09011281722066

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

(MANAJEMEN KEAMANAN DAN PENDEKATAN MANAJEMEN RISIKO DALAM KEAMANAN CYBER DAN MANAJEMEN KEAMANAN INFORMASI)

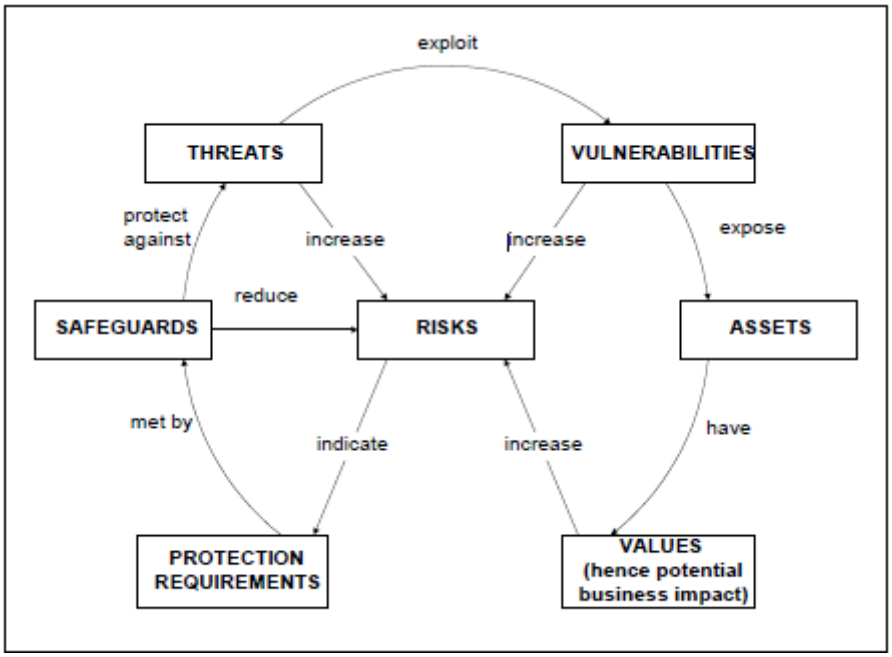
ABSTRAK

Resiko pendekatan manajemen adalah hal yang paling populer dalam manajemen keamanan kontemporer. Namun semua jenis risiko - kurang lebih terkait erat dengan keamanan, dalam manajemen risiko keamanan informasi yang terkait dengan keamanan merupakan bagian terbesar dari semua risiko. Situasi itu sering menyebabkan kesalah pahaman kedua istilah: keamanan dan manajemen risiko.

Kata kunci: Manajemen risiko, manajemen keamanan informasi, keamanan cyber.

1. MANAJEMEN KEAMANAN BERBASIS RISIKO

Istilah terkait keamanan informasi sering digunakan dalam literatur dengan cara yang ambigu. Berkaitan dengan skema yang diketahui dengan baik, menggambarkan hubungan antara elemen keamanan informasi utama, dengan semua komponen (termasuk keamanan itu sendiri) tampaknya dapat dikelola [8]. Salah satunya dapat menemukan manajemen kerentanan [4], manajemen keselamatan [6], manajemen keamanan [6], manajemen ancaman (misalnya. Dalam Microsoft Gerbang Manajemen Ancaman Forefront), manajemen risiko [7], dll.



Gambar 1 Model Hubungan Risiko.

Ambiguitas semantic terjadi antara manajemen risiko dan keamanan pengelolaan. Risiko biasanya didefinisikan sebagai efek dari ketidakpastian pada tujuan [1] dan keamanan informasi didefinisikan sebagai pelestarian seperangkat properti seperti kerahasiaan, integritas, ketersediaan informasi dan juga keasliannya, akuntabilitas dan non-penolakan [8]. Dari sudut pandang manajemen risiko, risiko yang terkait erat dengan keamanan aset (mis. risiko keamanan informasi) hanya sebuah kelompok risiko tertentu, dan manajemen risiko jenis ini (kadang-kadang keliru saat diidentifikasi dengan manajemen keamanan subjek tertentu) dapat diperlakukan sebagai bagian dari manajemen risiko keseluruhan [4]. Ini adalah situasi yang rumit, yang dapat menyebabkan kesalahan dalam memahami interaksi antara risiko dan keamanan..

Jelas bahwa semua jenis risiko kurang lebih terkait erat dengan risiko keamanan, terutama ketika keamanan dipahami dalam arti yang lebih luas, tidak hanya sebagai sebuah keadaan bebas dari bahaya maupun ancaman, tetapi juga sebagai jaminan untuk mencapai subjek (organisasi, atau grup) tujuan [5]. Selain itu di beberapa bidang risiko manajemen, pelanggaran keamanan (sering disengaja) mewakili bagian utama dari semua kemungkinan risiko sehingga manajemen risiko keamanan tertentu menjadi bagian utama dari proses manajemen risiko. Situasi ini juga berlaku untuk risiko terkait informasi. Itu minoritas risiko terkait informasi mungkin menyangkut kualitas rendah (precision, kecukupan, aktualitas, ketepatan waktu, dll.) dari konten informasi [7] dan biasanya demikian dipertimbangkan dengan aspek lain dari aktivitas organisasi (seperti analisis pasar, sistem kontrol manajemen, hubungan masyarakat, dll.), karena karakter non-material dari informasi, sebagian besar masalah yang mungkin terjadi dengan informasi berkaitan dengan pemrosesan data, yang terkait dengan keamanan informasi (secara ketat didefinisikan sebagai pelestarian kerahasiaan, integritas, ketersediaan, dan properti lainnya seperti keaslian, akuntabilitas atau penolakan informasi [8] termasuk ketersediaan dan efisiensi aset TI (sistem informasi). Kelompok risiko ini mungkin terlibat oleh pelanggaran keamanan.

Dalam konteks lain (manajemen keamanan aset selain informasi) ada banyak aspek berbeda, yang telah dimasukkan dalam keamanan keseluruhan proses manajemen, misalnya dalam pendekatan ISO 22301 salah satu langkah menciptakan BCMS (Business Continuity Management Systems), yang mendahului penilaian risiko, adalah BIA (“Business Impact Analysis - proses menganalisis kegiatan dan efek sebuah gangguan bisnis mungkin menimpa mereka ”[8], yang dapat dipahami sebagai bentuk evaluasi aset [6] dari sudut pandang kesinambungan bisnis (manajemen keberlangsungan bisnis diartikan sebagai "proses manajemen holistik itu mengidentifikasi potensi ancaman terhadap organisasi dan dampaknya terhadap operasi bisnis ancaman itu, jika direalisasikan, dapat menyebabkan, dan yang menyediakan kerangka kerja untuk membangun ketahanan organisasi dengan kemampuan respons efektif yang melindungi kepentingan pemangku kepentingan utama, reputasi, merek,

dan kegiatan penciptaan nilai mereka [8]. Juga risiko tertentu dalam kelangsungan bisnis telah dipertimbangkan dari sudut pandang tujuan dan aset organisasi, yang menawarkan jauh lebih umum pendekatan dari pada berfokus pada keamanan aset tertentu (seperti informasi). Dalam ISO / IEC 27001 pendekatan penciptaan ISMS (Information Security Management System) tidak memiliki langkah analog: proses ini berfokus pada manajemen risiko.

2. DI LUAR PENDEKATAN BERBASIS RISIKO

Masalah potensial dengan keamanan informasi termasuk spektrum masalah yang luas, termasuk kecelakaan teknis, masalah hukum (misalnya. pemrosesan data pribadi) dan disengaja dalam pelanggaran keamanan sistem informasi, sehingga keamanan informasi manajemen tidak dapat hanya mencakup manajemen risiko teknis umum komputer sistem. Masalah lain dengan pendekatan berbasis risiko terikat dengan rasa sempit "Keamanan" hanya dipahami dari sudut pandang "ex ante". Masalah keamanan mungkin dianalisis dari setidaknya tiga sudut pandang:

- sebelum masalah (penipuan, pelanggaran keamanan dll) terjadi,
- selama saat atau periode ketika risiko sedang terjadi,
- setelah materialisasi risiko.

Masing-masing orang dapat membedakan: tindakan pencegahan keamanan informasi, deteksi dan reaksi penyusup dan - dalam perspektif ex post - tindakan korektif dan investigasi.

Jelas istilah "risiko" (dipahami sebagai kombinasi dari ancaman tertentu kemungkinan dan dampaknya) tidak dapat dianalisis secara serius ketika ancaman sudah terjadi. Dalam keadaan seperti itu, kemungkinan menjadi kepastian: masalahnya adil terjadi, probabilitas kemunculannya adalah satu. Istilah "kemungkinan" dapat digunakan di analisis ex-post ketika frekuensi terjadinya masalah tertentu dapat diperlakukan sebagai sebuah ukuran kemungkinan terwujudnya masa depan. Namun standar ISO 27k mencoba untuk mencakup semua aspek sistem manajemen keamanan informasi (termasuk sebuah bukti digital [4], ada beberapa aspek keamanan dicadangkan untuk penegakan hukum dan pengadilan dari pada untuk organisasi tertentu dan tentu saja, penegakan hukum dan penerapan proses hukum harus bersifat deterministik.

Masalah lain menyangkut keamanan informasi berbasis risiko di multi-aktor lingkungan: ada strategi (seperti pembagian risiko atau transfer risiko), yang menurun risiko dari satu sudut pandang aktor, meningkatkan risiko untuk aktor lain. Dimungkinkan untuk menemukan sebuah kompromi dan membangun ISMS yang konsisten dan kompatibel dalam situasi, ketika semua aktor bermain adil dan memiliki informasi lengkap, tetapi seperti yang diketahui ada yang lain situasi dan strategi terlalu. Masalah khusus mungkin terkait dengan keamanan siber (keamanan dunia maya).

Standar internasional [7] mencakup dua definisi: cybersecurity (diadopsi dengan definisi keamanan informasi [8]: "Cybersecurity, Cyberspace security pelestarian kerahasiaan, integritas, dan ketersediaan informasi dalam Cyberspace "dengan catatan bahwa" Selain itu, properti lainnya, seperti keaslian, akuntabilitas, non-penolakan, dan keandalan juga bisa dilibatkan ” [7] dan Keamanan cyber ("Keamanan cyber - kondisi dilindungi dari fisik, sosial, spiritual, keuangan, politik, emosional, pekerjaan, psikologis, pendidikan atau jenis atau konsekuensi lain dari kegagalan, kerusakan, kesalahan, kecelakaan, kerusakan atau peristiwa lainnya di Cyberspace yang dapat dianggap tidak diinginkan ”, dengan dua catatan: CATATAN 1: Ini dapat berupa dilindungi dari acara atau dari paparan sesuatu yang menyebabkan kerugian kesehatan atau ekonomi. Itu bisa termasuk perlindungan manusia atau aset.

CATATAN 2: Keselamatan secara umum juga didefinisikan sebagai keadaan yakin bahwa efek samping tidak akan disebabkan oleh beberapa agen di bawah kondisi yang ditentukan [7]. Dunia maya didefinisikan dalam standar yang sama dengan "Lingkungan kompleks yang dihasilkan dari interaksi orang, perangkat lunak dan layanan di Internet melalui perangkat teknologi dan jaringan yang terhubung dengannya, yang tidak ada dalam bentuk fisik apa pun [7]. Lebih detail (tapi tetap saja ambigu) definisi keamanan cyber dapat ditemukan dalam tindakan hukum. Bahasa Polandia saat ini Program Pemerintah untuk Perlindungan Ruang Maya di Polandia [8] mendefinisikan Ruang cyber sebagai "area pemrosesan dan pertukaran informasi, yang diciptakan oleh Internet sistem dan jaringan komputer, bersama dengan tautan di antara mereka dan hubungan itu dengan pengguna "dan Cyberspace Republik Polandia sebagai" cyberspace dalam wilayah tersebut Negara Polandia dan di lokasi di luar wilayah di mana ada perwakilan Republik Polandia (lembaga diplomatik, kontingen militer) ". UU 30 Agustus 2011, mengamandemen Undang-undang tentang keadaan perang dan kompetensi Panglima Tertinggi angkatan bersenjata dan dasar pelaporannya otoritas konstitusional Republik Polandia dan undang-undang tertentu lainnya [8] mendefinisikannya sebagai berikut: "ruang, pemrosesan dan pertukaran informasi yang dibuat oleh TIK sistem sebagaimana dimaksud dalam pasal 4. 3 bagian 3 Undang-Undang 17 Februari 2005 tentang aktivitas komputer entitas yang menyadari tugas publik, bersama dengan tautan di antaranya mereka dan hubungan dengan pengguna "[8]

Meskipun definisi ini jauh dari kejelasan, dapat diharapkan bahwa Istilah "cyberspace" (dalam arti ISO) menunjukkan bahwa efek sinergis kontemporer Internet (terutama yang terkait dengan jejaring sosial, roleplaying online multi-pemain yang masif permainan pemerintah, komputasi awan, dll.) dan - karena "metafisik karakter cyberspace - bahwa cyber security harus melewati sistem informasi keamanan (karena sistem informasi memiliki bentuk fisik tentunya). Sulit untuk melakukannya memahami bagaimana properti keamanan informasi dapat dijamin tanpa mengambil menjadi pertimbangan keamanan sistem

pemrosesan informasi. Dalam hukum di atas definisikan dengan arti dunia maya tampaknya menjadi sesuatu yang merupakan bidang kegiatan entitas yang menyadari tugas publik dan dapat dilindungi dan diatur oleh hukum (yang, seperti: disebutkan di atas, harus deterministik) namun Program di atas [8] mengacu pada definisi dan konsep dari standar ISO 27k - tidak jelas bagaimana mungkin mungkin untuk mengevaluasi dan mengelola risiko yang terkait dengan kehilangan kemampuan Negara untuk melakukan keluar fungsi khususnya.

3. KESIMPULAN

Pendekatan manajemen risiko adalah pendekatan yang paling populer di masa kini manajemen keamanan [1], [2]). R.N.R van Os dalam esai [3] banyak menganalisis definisi tentang manajemen keamanan dan manajemen risiko dan akhirnya menyimpulkan bahwa manajemen risiko dan manajemen keamanan tidak sama (namun kedua istilah tersebut ambigu) dan mengusulkan bahwa manajemen risiko harus diperlakukan sebagai bagian manajemen keamanan. Sehubungan dengan manajemen keamanan informasi, risiko manajemen dapat diperlakukan sebagai bagian utama dari proses manajemen keamanan dan dasar pendekatan kontemporer, namun ada beberapa elemen informasi manajemen keamanan, ketika pendekatan berbasis risiko murni tampaknya tidak memadai atau tidak cukup untuk memberikan tingkat keamanan informasi yang memuaskan. Strategi lainnya (deterministik, berbasis kepatuhan, dll [6] [7]) mungkin merupakan opsi yang layak mempertimbangkan dalam situasi seperti itu.

REFERENSI

[1]. Luskova M., Buganová K .: Manajemen risiko dan perusahaan transportasi, Mekanika, Transportasi, Komunikasi, 2011, Seni. ID: 491, http: //www.mtcaj. com / library / 491_EN.pdf

[2]. Spiridonova H., Andonov A., Mihova M .: Analisis dan Penilaian Risiko di perlindungan informasi dalam sistem kontrol analitis, Mekanika, Transportasi, Komunikasi, 2013, Seni. ID: 863, http://www.mtc-aj.com/library/863.pdf

[3]. van Os. R.N.R: Manajemen risiko dan manajemen keamanan adalah sama hal?, http://members.chello.nl/~y.de.vries/Essays/Fa1r2.pdf

[4]. Staniec I., Zawiła Niedźwiecki J .: Zarządzanie ryzykiem operatsiynym, C.H. Beck, Warszawa 2008

[5]. Minisłownik Biura Bezpieczeństwa Narodowego http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbnpropozy/ 6035, MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedzinybezpieczenstwa. html

[6]. Krause M., Tipton H.F .: Buku Pegangan Manajemen Keamanan Informasi, CRC

Tekan LLC, https://www.cccure.org/Documents/HISM/244-246.html
[7]. Korzeniowski L.F .: Securitologia. Ilmu bezpieczeństwie człowieka i organizacji społecznych, EAS, Kraków 2008, http://www.sbc.org.pl/Content/13871/Korzeniowski_Securitologia.pdf
[8]. ISO / IEC 27000: 2014 Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Tinjauan umum dan kosa kata, ISO 2014