Terbit pada laman web jurnal : **http://ojsamik.amikmitragama.ac.id**

JURNAL JARINGAN SISTEM INFORMASI ROBOTIK (JSR)
Vol. 6 No. 2 TAHUN 2022 E - ISSN : 2579-373X

MANAJEMEN INSIDEN KEAMANAN SIBER PADA DUNIA PENERBANGAN

Zulkarnaim Masyhur[1], Firmansyah Ibrahim[2], Nahrun Hartono[3]
Program Studi Sistem Informasi, UIN Alauddin Makassar
Zulkarnaim.masyhur@uin-alauddin.ac.id[1], firmansyah.ibrahim@uin-alauddin.ac.id[2],
nahrunhartono@gmail.com[3]

Abstract

Cyber Security Incident Management has an important role in the aviation domain. Information sharing between air traffic control (ATC) and ground traffic management (GTM) is System Wide Information Management (SWIM), which causes the need for the concept of cyber security management in the aviation domain. Current studies are limited to studying the needs and solutions to improve these capabilities. So, there is a great need for cyber security incident management in a system-wide information management (SWIM) system in the future. This study is a review of the literature. The author conducted a search for references related to the security of privacy data. A method for evaluating, evaluating, and synthesising the results of research works and ideas produced by researchers and practises that is systematic, explicit, and explicit. risk management to be able to minimise various obstacles that may occur during the execution of the project. Risk is generally defined as the combination of the likelihood of an event and its consequences (ISO Guide 73). The point is that the business target is not being met. COBIT 5 for Risk characterises IT risk as a business risk, particularly business risk related to the utilization, operation, inclusion, impact, and acceptance of IT in a business. It has described the cybersecurity incident management scheme in the domain based on existing standards and good practices. It is hoped that this can be applied in the aviation domain in the future. This led to an increase in the broad concept of information systems management services. So that it can be a reference for improving incident management in the aviation world
Keywords: Incident Response, Risk Management , ATC

Abstrak

Cyber Security Incident Management memiliki peran penting dalam domain penerbangan. Pembagian informasi antar air traffic control (ATC) yaitu System Wide Information Management (SWIM) menyebabkan diperlukannya konsep manajemen insiden keamanan siber dalam domain penerbangan. Penelitian-penelitian yang ada saat ini terbatas hanya mempelajari kebutuhan dan solusi dalam peningkatan kemampuan tersebut. Sehingga sangat dibutuhkannya manajemen insiden keamanan siber dalam system wide information management (SWIM) di masa mendatang. Penelitian ini merupakan penelitian literature review. Penulis melakukan pencarian referensi terkait dengan keamanan privasi data. Dibutuhkan manajemen resiko untuk dapat meminimalisir berbagai kendala yang kemungkinan akan terjadi ke depannya. Risiko umumnya didefinisikan sebagai kombinasi dari kemungkinan suatu peristiwa dan konsekuensinya (ISO Guide 73). Konsekuensinya adalah target usaha tidak terpenuhi. COBIT 5 for Risk mencirikan risiko TI sebagai risiko bisnis, khususnya risiko bisnis yang terkait dengan pemanfaatan, kepemilikan, operasi, penyertaan, dampak, dan penerimaan TI di dalam suatu usaha. Telah dipaparkan terkait skema pengelolaan insiden keamanan siber di domain penerbangan berdasarkan standar dan praktik yang baik yang ada. Diharapkan hal ini dapat diterapkan dalam domain penerbangan di masa mendatang. Ini mengarah pada peningkatan konsep layanan manajemen informasi sistem yang luas. Sehingga dapat menjadi acuan dalam peningkatan manajemen insiden pada dunia penerbangan.
Kata kunci: Respon Insiden, Manajemen Risiko, ATC

1. Pendahuluan

Keamanan siber bukanlah isu terkini dalam ranah penerbangan, namun dalam keamanan penerbangan hanya berfokus pada aspek psikis misalnya perlindungan pesawat dan pencegahan orang jahat atau barang buruk dalam menaiki pesawat [1]. Pembagian informasi antar *air traffic control* (ATC) yaitu *System Wide Information Management* (SWIM) menyebabkan diperlukannya konsep manajemen insiden keamanan siber dalam domain penerbangan [2].

Meskipun SWIM membuat banyak elemen menjadi lebih mudah, SWIM juga membantu agregat dari sifat multifaset dari kerangka kerja yang mendorong tantangan keamanan baru. Satu hal yang perlu digarisbawahi adalah landasan penerbangan yang dilandasi oleh *rule of trust*, artinya berbagai kepentingan mitra bekerja sama untuk menjamin kelancaran dan kelancaran transportasi para pelancong dan produk [2].

Penelitian saat ini dalam program *Single European Sky ATM Research* (SESAR) berkisar pada memotivasi langkah-langkah keamanan untuk sumber daya ATM dengan menghadirkan pengaturan dasar kontrol keamanan yang diperbesar oleh kontrol khusus sumber daya yang tunduk pada kekritisan keuntungan yang sedang diselidiki. Bagaimanapun, transaksi langkah-langkah keamanan, penanganan ancaman dan serangan keamanan in-situ, dan strategi bersama di seluruh SoS semacam itu masih terbuka [1].

Dengan interkoneksi kerangka kerja ATM yang diperluas yang didorong oleh SWIM, pentingnya memiliki rencana yang mahir dan kuat untuk menangani insiden keamanan digital disorot. Dalam makalah ini kami akan menggunakan praktik respons insiden keamanan siber yang hebat [3], [4]dan pertemuan dari pengaturan infrastruktur penting lainnya [5] dengan mengingat tujuan akhir untuk menggambarkan proposal manajemen respons insiden untuk domain penerbangan.

2. Tinjauan Pustaka

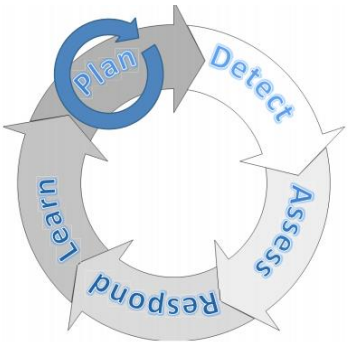
A. Peristiwa dan Insiden

Menurut Publikasi Khusus NIST 800-61 , suatu peristiwa adalah keadaan yang terlihat dalam suatu sistem atau jaringan. Ambil pengguna yang terhubung ke *server cloud*, pengguna melampirkan *file* dan mengirimkannya melalui email dan server yang menerima permintaan untuk halaman web, misalnya. *Adverse event* adalah peristiwa dengan konsekuensi yang tidak diinginkan, seperti sistem *crash*, paket banjir, penggunaan hak istimewa sistem yang tidak sah, akses tidak sah ke data sensitif, dan eksekusi *malware* yang menghancurkan data. Insiden keamanan komputer adalah pelanggaran atau ancaman pelanggaran kebijakan keamanan komputer, kebijakan penggunaan yang dapat diterima, atau praktik keamanan standar. Tentu saja, definisi ini bergantung pada keberadaan kebijakan keamanan yang, meskipun dipahami secara umum, bervariasi antar organisasi [4].

B. Tanggapan Insiden

Tanggapan insiden adalah pendekatan sistematis untuk mengidentifikasi dan menangani akibat dari kerentanan suatu sistem atau jaringan. Menangani situasi dengan cara yang membatasi bahaya dan mengurangi waktu dan biaya pemulihan adalah tujuan dari respons insiden. Selain itu, rencana respons insiden yang sangat diperlukan adalah kebijakan yang mendefinisikan, dalam istilah khusus, apa yang merupakan insiden dan menyediakan proses langkah demi langkah yang harus diikuti ketika insiden terjadi.

Tanggapan insiden organisasi dilakukan oleh tim respons insiden komputer, kelompok yang dipilih dengan cermat yang, selain staf keamanan dan TI umum, dapat mencakup perwakilan dari departemen hukum, sumber daya manusia, dan hubungan masyarakat [6].



Gambar 1 Proses Manajemen Insiden [3]

ISO/IEC 27035:2016 menyoroti bahwa ada lima fase manajemen insiden (Gambar 1). Ini adalah

a. Bersiap untuk mengelola insiden seperti menyiapkan kebijakan manajemen insiden, dan membentuk kelompok yang mampu mengelola

insiden; Mengenali dan melaporkan insiden keamanan informasi;

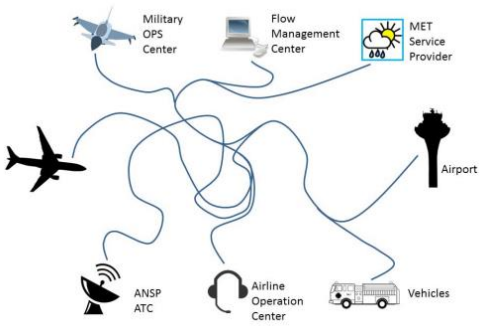
b. Menilai insiden dan menetapkan pilihan tentang bagaimana mereka akan cenderung misalnya memperbaiki keadaan dan kembali ke bisnis dengan cepat, atau mengumpulkan bukti forensik terlepas dari kemungkinan bahwa hal itu menunda penyelesaian masalah;
c. Menanggapi insiden yaitu menahannya, menjelajahinya dan menyelesaikannya;
d. Pelajari pelajarannya - lebih dari sekadar mengenali hal-hal yang mungkin telah diperbaiki, tahap ini mencakup benar-benar meluncurkan perbaikan yang menyempurnakan prosedur (ISO, 2011)

C. Tim Respons Insiden Komputer (CIRT)

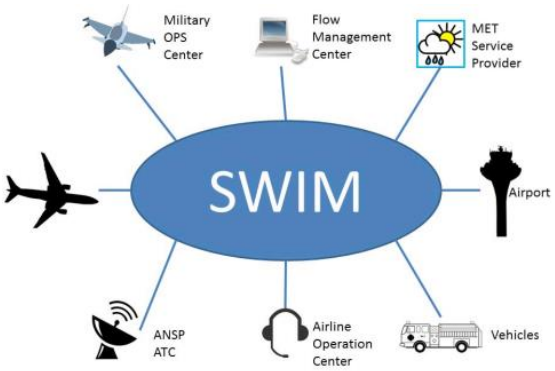
CIRT adalah motivasi pengumpulan yang dipilih dan dipersiapkan dengan baik di belakang individu yang akan menangani suatu kejadian dengan cepat dan akurat dengan tujuan agar kejadian tersebut dapat segera ditahan, dieksplorasi, dan diperoleh kembali. Hal ini umumnya berisi individu-individu dari dalam organisasi. Mereka harus menjadi individu yang dapat menghentikan apa yang mereka lakukan (atau mendelegasikan kembali kewajiban mereka) dan memiliki spesialis untuk menentukan pilihan dan mengambil tindakan. [6]

D. Sistem Manajemen Informasi Luas (SWIM)

Tujuan utama penerapan System Wide Management adalah memberdayakan keuntungan bisnis dari manajemen lalu lintas udara yang akan dihasilkan dengan menjamin pengaturan data yang dipahami secara teratur yang disampaikan kepada individu yang ideal pada waktu yang tepat [7]. (SWIM bergerak dari hubungan kusut ke titik ke titik (gambar 1) ke koneksi umum yang koheren ke banyak antarmuka komunikasi (gambar 2). [2]



Gambar 2 Komunikasi penerbangan sebelum SWIM [2]



Gambar 3 Komunikasi penerbangan setelah SWIM [2]

E. Manajemen Lalu Lintas Udara

Dengan perkembangan permintaan lalu lintas udara yang terus-menerus dan sebagai tambahan prasyarat untuk korespondensi informasi yang lebih aman dan solid, perubahan pandangan dari ATM biasa menjadi kerangka ATM mutakhir menjadi penting. Secara rinci, navigasi darat diganti dengan sistem komunikasi berbasis satelit, sistem komunikasi verbal dan radar darat diubah menjadi komunikasi digital yang lebih presisi dan andal (misalnya ADS-B) dan pesawat yang diberdayakan diganti dengan yang tradisional. Selanjutnya, saat ini, kerangka kerja ATM yang sedang berjalan dapat menyesuaikan lebih banyak aplikasi penerbangan secara signifikan, misalnya, kerangka kerja kepemimpinan dasar yang aman, deteksi dan resolusi konflik, dan operasi berbasis arah 4-D. Singkatnya, kerangka ATM saat ini secara tepat menggabungkan kemajuan pendeteksian dan pemeriksaan yang disempurnakan yang diberdayakan oleh persimpangan terkomputerisasi yang lebih solid dengan perhatian situasional yang berkelanjutan untuk pilot dan pengontrol lalu lintas udara [8].

F. Penilaian Risiko

Risiko umumnya didefinisikan sebagai kombinasi dari kemungkinan suatu peristiwa dan konsekuensinya (ISO Guide 73). Konsekuensinya adalah target usaha tidak terpenuhi. COBIT 5 for Risk mencirikan risiko TI sebagai risiko bisnis, khususnya risiko bisnis yang terkait dengan pemanfaatan, kepemilikan, operasi, penyertaan, dampak, dan penerimaan TI di dalam suatu usaha. Risiko TI terdiri dari kejadian-kejadian terkait TI yang mungkin dapat mempengaruhi bisnis. Risiko TI dapat terjadi dengan frekuensi dan pengaruh yang tidak pasti dan membuat tantangan dalam memenuhi tujuan dan sasaran vital [9].

Manajemen risiko TI sebagai prosedur yang memungkinkan manajer TI untuk menyesuaikan biaya operasional dan keuangan dalam upaya keamanan dan mencapai keuntungan dengan melindungi sistem TI bersama dengan informasi dan data yang mendukung tujuan utama organisasi [9].

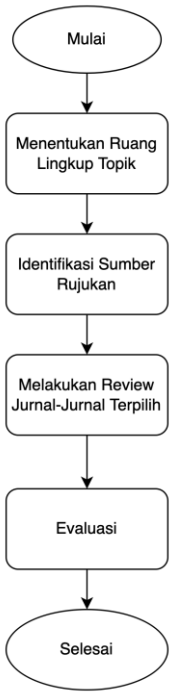
Target mendasar dari manajemen risiko adalah untuk memberdayakan asosiasi atau organisasi untuk mencapai tujuan organisasi dan tujuan utama dengan cara berikut :

a. Mengamankan sistem TI yang menyimpan, memproses, dan mengirimkan data perusahaan secara luas.
b. Memungkinkan manajemen membuat keputusan dengan mempertimbangkan penyelesaian data untuk melegitimasi pengeluaran yang merupakan bagian dari rencana pengeluaran TI.
c. Membantu manajemen dalam menyetujui dan akreditasi sistem TI dengan memanfaatkan dokumentasi yang dibuat oleh proses manajemen risiko [9].

3. Metodologi Penelitian

Penelitian ini merupakan penelitian literature review. Penulis melakukan pencarian referensi terkait dengan manajemen insiden pada dunia penerbangan. Literature review merupakan sebuah metode yang sistematis, eksplisit dan reprodusibel untuk melakukan identifikasi, evaluasi dan sintesis terhadap karya-karya hasil penelitian dan hasil pemikiran yang sudah dihasilkan oleh para peneliti dan praktisi. Beberapa tahapan yang dilakukan dalam peneltian ini yaitu:

a. Menentukan ruang lingkup topik literature yang akan direview, dalam penelitan ini ruang lingkup topiknya adalah manajemen insiden keamanan siber pada dunia penerbangan.
b. Mengidentifikasi sumber rujukan, pada penelitian ini identifikasi dilakukan dengan melihat terbitan dari literatur yang akan direview.
c. Mereview dan menulis review, tahap selanjutnya adalah mengambil subtansi dari setiap referensi yang dikumpulkan kemudian memberikan evaluasi dan menuliskannya kembali.



Gambar 4. Flowchart Tahapan Penelitian

4. Hasil dan Pembahasan

A. Manajemen Respons Insiden

I. Tahap Rencana Manajemen Insiden Keamanan

Tahap ini sesuai dengan namanya mengatur pengaturan kelompok agar siap menghadapi suatu kejadian dengan segera. Sebuah insiden dapat berjalan dari apa saja, misalnya, pemadaman listrik atau ketidakmampuan peralatan hingga insiden yang paling keterlaluan, misalnya, pelanggaran strategi hierarkis oleh perwakilan yang kecewa atau diretas oleh pemrogram yang didukung negara[10]. Meskipun alasan untuk perencanaan kejadian adalah tahap yang paling penting dibandingkan dengan sebagian besar dari yang lain, karena akan

menentukan seberapa baik kelompok Anda akan memiliki kemampuan untuk bereaksi jika terjadi keadaan darurat. [11]

Rencana manajemen insiden harus mempertimbangkan faktor organisasi dan manusia serta masalah teknis, dan harus dimaksudkan untuk beradaptasi dengan keadaan kompleks dengan administrator dan pekerja kontrak yang berbeda. Susunannya harus berkonsentrasi pada:

a. Siapa yang bertanggung jawab atas berbagai kegiatan;

b. Kapan dan bagaimana melakukan aktivitas yang berbeda.

Mekanisme teknis misalnya, Sistem Deteksi intrusi, firewall dan produk anti-virus sangat penting. Pada jaringan mesin mana pun saat ini, juga dapat mengenali (dan sering kali mencegah) sejumlah besar insiden untuk gaya terprogram. Komponen-komponen ini sendiri akan berada di luar cakupan tentang Manajemen kejadian keamanan SWIM, namun mungkin saja. Penting yang mengingatkan Juga peringatan yang mereka hasilkan membutuhkan bantuan. Diurus dengan cara yang pas, dan ditindaklanjuti oleh tim tanggap insiden. Tugas utama dalam fase Plan adalah memastikan adanya rutinitas yang memfasilitasi arus informasi, dengan mempertimbangkan aspek organisasi/manusia dan teknis.

Penilaian risiko ini harus membuat analitik penting dan hanya mereka yang ada dalam penilaian risiko keamanan keseluruhan untuk sistem informasi, untuk manfaat yang sama. Selain itu, kemungkinan untuk melakukan penilaian risiko waktu nyata sehubungan dengan berbagai bagian kerangka data dalam tahap reaksi harus lebih ditingkatkan untuk diselidiki. Jika terjadi insiden, apalagi jika kebutuhan jarak jauh untuk pemulihan di sistem ATM, penilaian risiko terus-menerus dapat memberikan bantuan pilihan yang sangat penting untuk memastikan bahwa gerakan-gerakan yang baik harus meringankan hasil dari episode yang akan dipilih [1].

II. Fase Deteksi Manajemen Insiden Keamanan

Tahap ini mengelola pengakuan dan jaminan apakah penyimpangan dari operasi normal di dalam organisasi adalah sebuah insiden, dan perluasannya menerima bahwa penyimpangan itu pasti sebuah insiden. Langkah khusus ini mengharuskan seseorang untuk mengumpulkan peristiwa dari sumber yang berbeda, misalnya, dokumen log, pesan kesalahan, dan aset lain, seperti kerangka identifikasi gangguan dan firewall, yang dapat memberikan konfirmasi untuk memutuskan apakah suatu peristiwa adalah sebuah episode. Jika peristiwa tertentu diputuskan untuk menjadi sebuah episode, dan setelah itu harus diperhitungkan secepat waktu memungkinkan mengingat tujuan akhir untuk memungkinkan CIRT cukup waktu untuk mengumpulkan konfirmasi dan bersiap-siap untuk langkah sebelumnya [10].

Pada fase episode ini, individu CIRT harus diberitahu dan komunikasi harus dikoordinasikan antara anggota bersama dengan staf pusat komando yang ditunjuk (misal manajemen dan/atau administrator sistem). Disarankan bahwa setidaknya dua penanganan insiden dapat diakses untuk menangani suatu insiden sehingga satu dapat menjadi penanganan penting yang dapat mengenali dan mengevaluasi kejadian dan yang lainnya untuk memungkinkan berkumpul untuk membuktikan. Komunikasi dan koordinasi antar individu dari CIRT (dan administrasi) adalah dasar, terutama jika tingkat episode dapat secara signifikan mempengaruhi operasi bisnis. Ini juga merupakan tahap di mana penanggap insiden harus mengarsipkan semua yang mereka lakukan, seperti yang dinyatakan sebelumnya, catatan ini harus dapat menjawab pertanyaan Siapa, Apa, Di mana, Mengapa, dan Bagaimana jika dokumentasi akan dibuat. digunakan untuk menjerat pelaku di pengadilan [12].

III. Fase Penilaian Manajemen Insiden Keamanan

Ketika insiden tersebut memberi tahu kontak orang yang bertanggung jawab untuk menangani insiden tersebut, insiden tersebut harus dievaluasi untuk memutuskan keseriusan insiden dan langkah ke depan. Dengan sungguh-sungguh, fase penilaian difokuskan untuk mengenali suatu insiden dengan jelas. Sebagaimana ditentukan di atas, fase deteksi memberikan bukti-bukti yang sekarang – di tengah fase penilaian – penilaian yang sesuai harus dilakukan. Pada tingkat dasar, fase penilaian bertujuan untuk:

a. Menentukan apakah peristiwa tersebut merupakan insiden keamanan yang sebenarnya atau peringatan palsu
b. Mengkategorikan insiden yang diidentifikasi – misalnya – sebagai minor atau mayor
c. Memicu prosedur respons masing-masing yang diberikan kategorisasi

Fase penilaian dapat digambarkan secara luas sebagai konfirmasi insiden dan proses pemilihan rencana. Dari sudut pandang itu, fase assesment merupakan pengembangan dasar yang tepat dan terfokus pada respon terhadap suatu kejadian. Mengingat penilaian, sumber daya dan prosedur yang dimulai sendiri mungkin memerlukan sumber daya. Oleh karena itu, penting untuk memberikan aturan dan contoh pilihan yang jelas untuk fase ini. Penilaian yang salah atau inisiasi rencana yang salah pada akhirnya dapat memerlukan tindakan koreksi yang Panjang [1].

IV. Fase Tanggap Manajemen Insiden Keamanan

Motivasi di balik tahap ini adalah untuk membawa sistem yang terpengaruh kembali ke lingkungan produksi dengan hati-hati, untuk memastikan bahwa itu tidak akan menyebabkan insiden lain. Sangatlah penting untuk menguji, menyaring, dan menyetujui kerangka kerja yang dikembalikan ke generasi untuk memeriksa bahwa kerangka tersebut tidak terinfeksi ulang oleh malware atau ditawar dengan cara yang berbeda. Beberapa keputusan penting yang harus diambil selama fase ini adalah:

a. Waktu dan tanggal untuk memulai kembali operasi – adalah kunci untuk membuat administrator/pemilik kerangka kerja membuat pilihan resmi berdasarkan nasihat CIRT.
b. Cara menguji dan mengonfirmasi bahwa kerangka kerja yang dinegosiasikan tidak bernoda dan sepenuhnya berguna.
c. Istilah memeriksa untuk mengawasi praktik-praktik aneh.
d. Perangkat untuk menguji, menyaring, dan menyetujui perilaku kerangka kerja. [6]

Ada banyak pilihan yang lebih berharga yang bisa direkam; meskipun demikian, data di atas harus memberikan beberapa gagasan tentang apa yang terkandung di dalamnya. Tujuan utama secara keseluruhan, seperti yang diungkapkan sebelumnya, adalah untuk mencegah episode lain terjadi karena masalah serupa yang menyebabkan masalah yang baru saja diselesaikan [4]

Sering diakui bahwa kehilangan informasi persentase mungkin lebih baik daripada kerangka kerja (yang masih) tidak stabil. Untuk pengaturan ATM itu akan selalu penting dengan pemerataan alasan kuat untuk keamanan maju dan persyaratan harus tetap dengan kerangka itu tergantung pada lebih lanjut berjalan. Dengan mengaturnya secara blak-blakan, Anda tidak dapat reboot ulang Pesawat yang berdengung. Akibatnya mungkin penting bahwa agen dari keduanya dan karakter di layar ATM (pengendali lalu lintas udara, dan sebagainya akan menyertakan pilihan yang dilakukan yang akan menyebabkan shutdown sistem, atau yang mungkin membuat kerangka kerja menjadi rapuh. [1]

V. Tahap Pembelajaran Manajemen Insiden Keamanan

Fase paling kritis setelah yang lainnya adalah Lessons Learned. Alasan untuk tahap ini adalah untuk menyelesaikan dokumentasi apa pun yang tidak dilakukan di tengah insiden, dan juga dokumentasi tambahan yang mungkin bermanfaat di insiden mendatang. Dokumen tersebut juga harus ditulis dalam bentuk laporan untuk memberikan tinjauan play-by-play dari seluruh insiden; Laporan ini harus mampu menjawab: Siapa, Apa, Dimana, Mengapa, dan Bagaimana alamat yang mungkin muncul di tengah-tengah pertemuan pembelajaran. Tujuan umumnya adalah untuk mengambil keuntungan dari kejadian yang terjadi di dalam sebuah asosiasi untuk meningkatkan kinerja kelompok dan memberikan bahan referensi jika terjadi episode yang sebanding. Dokumentasi tersebut juga dapat digunakan sebagai bahan persiapan untuk rekan kerja baru atau sebagai acuan untuk digunakan sebagai bagian dari korelasi dalam keadaan darurat di masa depan [10].

Pertemuan Lessons Learned harus dilakukan sesegera mungkin; aturan praktis yang baik adalah dalam waktu 2 minggu setelah kejadian. Rapat harus melalui laporan respon insiden dengan finalisasi dalam format ringkasan eksekutif. Itu harus dibuat singkat, agar tidak kehilangan perhatian penonton dan tetap profesional [11].

B. Penebangan, Pelaporan dan Pemantauan

I. Pencatatan

Sebagai bagian dari Keamanan SWIM secara keseluruhan, harus ada pencatatan dan pemantauan secara real time pada titik-titik kunci dalam sistem informasi. Penggunaan data logging dan monitoring di SWIM Security Incident Management :

a. Untuk mendeteksi penyimpangan dalam sistem informasi yang dapat menyebabkan insiden;
b. Untuk membantu dalam pendeteksian insiden dalam fase Deteksi;
c. Untuk mendukung forensik dalam fase Respon dan Pelajari.

II. Pelaporan

Sistem pelaporan penanganan Insiden harus dibuat. Pelaporan harus mengidentifikasi apa yang terjadi (Jaatun & Koelle, 2016), termasuk:

a. Penyebab kejadian;
b. Apa yang dihasilkan, yaitu, bagaimana Sistem Informasi terpengaruh;
c. Bagaimana penanganannya, langkah demi langkah;
d. Konsekuensi dari insiden dan apa yang dilakukan untuk mengurangi konsekuensi.[1]

III. Pemantauan

Kinerja Manajemen Insiden Keamanan SWIM harus dipantau untuk memastikan efisiensi penanganan insiden dan pembelajaran dari insiden. Untuk mendukung pemantauan, serangkaian indikator kinerja utama harus, seperti:

a. Sistem peringkat untuk sistem manajemen respons insiden;
b. Penilaian budaya keamanan informasi mengenai respon insiden;
c. Jumlah insiden yang ditanggapi;
d. Rata-rata waktu yang dihabiskan untuk menanggapi atau insiden;
e. Total konsekuensi dari insiden;
f. Jumlah insiden kerugian tinggi;
g. Waktu henti sistem ATM;
h. Total biaya yang terkait dengan respons insiden [1].

C. Persyaratan Manajemen Insiden Keamanan

Beberapa persyaratan untuk manajemen insiden keamanan sudah dicakup oleh persyaratan yang diidentifikasi untuk perlindungan diri ATM. Persyaratan tambahan diidentifikasi dalam D03:

a. Infrastruktur SWIM harus membuat pencatatan dan pemantauan secara real time pada titik-titik utama dalam sistem informasi. Penggunaan data logging dan monitoring dalam SWIM Security Incident Management akan mendeteksi ketidakberesan dalam sistem informasi yang dapat menyebabkan insiden; membantu dalam pendeteksian insiden dalam fase Deteksi dan Reaksi, mendukung forensik dalam fase Pemulihan dan Pembelajaran.
b. Infrastruktur SWIM harus membentuk sistem pelaporan penanganan Insiden. Pelaporan harus mengidentifikasi apa yang terjadi, termasuk: penyebab insiden; apa akibatnya, yaitu bagaimana Sistem Informasi terpengaruh; bagaimana hal itu ditangani, langkah demi langkah; konsekuensi dari insiden dan apa yang dilakukan untuk mengurangi konsekuensi.
c. Kinerja Manajemen Keamanan SWIM harus dipantau untuk memastikan efisiensi penanganan insiden dan pembelajaran dari insiden. Untuk mendukung pemantauan ini, serangkaian indikator kinerja utama harus diidentifikasi, seperti: sistem peringkat untuk sistem manajemen respons insiden; penilaian budaya keamanan informasi tentang respon insiden; jumlah insiden yang ditanggapi; rata-rata waktu yang dihabiskan untuk menanggapi insiden; konsekuensi total dari insiden; jumlah insiden kerugian tinggi; waktu henti sistem; dan total biaya yang terkait dengan respon insiden.
d. Pemrosesan data informasi ATM yang dipertukarkan melalui SWIM akan memungkinkannya tersedia untuk organisasi keamanan yang berwenang. [1]

5. Kesimpulan

Telah dipaparkan terkait skema pengelolaan insiden keamanan siber di domain penerbangan berdasarkan standar dan praktik yang baik yang ada dan jurnal ini juga menggambarkan manajemen respons insiden untuk domain penerbangan. Diharapkan hal ini dapat diterapkan dalam domain penerbangan di masa mendatang.

Daftar Rujukan

[1] M. G. Jaatun and R. Koelle, "Cyber security incident management in the aviation domain," *Proc. - 2016 11th Int. Conf. Availability, Reliab. Secur. ARES 2016*, pp. 510–516, 2016, doi: 10.1109/ARES.2016.41.

[2] M. G. Jaatun and T. E. Faegri, "Sink or SWIM: Information security requirements in the sky," *Proc. - 2013 Int. Conf. Availability, Reliab. Secur. ARES 2013*, pp. 794–801, 2013, doi: 10.1109/ARES.2013.106.

[3] ISO, "ISO - ISO/IEC 27035:2011 - Information technology — Security techniques — Information security incident management," *ISO/IEC 27035:2011*, 2011. [Online]. Available:

https://www.iso.org/standard/44379.html. [Accessed: 16-Aug-2022].
[4] M. B. Line, *UNDERSTANDING INFORMATION SECURITY INCIDENT MANAGEMENT PRACTICES: A case study in the electric power industry*, no. April. 2015.
[5] T. Yohannes, L. Lessa, and S. Negash, "Information security incident response management in an Ethiopian bank: A gap analysis," *25th Am. Conf. Inf. Syst. AMCIS 2019*, no. July, 2019.
[6] Heather Mahalik, "The Ultimate Guide to Getting Started in Digital Forensics & Incident Response (DFIR) | SANS Institute," *SANS White Paper*, 2022. [Online]. Available: https://www.sans.org/white-papers/ultimate-guide-getting-started-digital-forensics-incident-response/. [Accessed: 16-Aug-2022].
[7] Eurocontrol, *Guidelines ASM Support Systems Interfaces EUROCONTROL Specification for SWIM Service Description*. 2021.
[8] D. Li and R. Zhang, "A framework to mitigate airliner risk in air traffic management," *2016 IEEE Conf. Commun. Netw. Secur. CNS 2016*, pp. 324–332, 2017, doi: 10.1109/CNS.2016.7860500.
[9] A. Khrisna and Harlili, "Risk management framework with COBIT 5 and risk management framework for cloud computing integration," *Proc. - 2014 Int. Conf. Adv. Informatics Concept, Theory Appl. ICAICTA 2014*, pp. 103–108, Jan. 2015, doi: 10.1109/ICAICTA.2014.7005923.
[10] Richard Bejtlich, *The Tao of network security monitoring: beyond intrusion detection*. Boston: MA: Pearson Education, Inc, 2005.
[11] SANS, "Incident Handler's Handbook | SANS Institute," 2011. [Online]. Available: https://www.sans.org/white-papers/33901/. [Accessed: 16-Aug-2022].
[12] R. C. Newman, *Computer Forensics: Evidence Collection and Management*, 1st editio. Boca Raton,FL: Auerbach Publications, 2007.