Prosiding Seminar Nasional Sains dan Teknologi Seri III
Fakultas Sains dan Teknologi, Universitas Terbuka
Vol. 2 No. 1 (2025)
e-ISSN: 3047-6569

EVALUASI STRATEGI REAKTIF PASCA SERANGAN RANSOMWARE PADA PUSAT DATA NASIONAL SEMENTARA 2 SURABAYA

Syerlie Annisa[1*], Ajeng Ratu Langi[2]
[1]Program Studi Design Komunikasi Visual, Universitas Negeri Padang, Padang, Indonesia
[2]Program Studi Sistem Informasi, Universitas Terbuka, Tangerang Selatan, Indonesia

**Penulis korespondensi: syerlieannisa@fbs.unp.ac.id*

ABSTRAK

Penelitian ini bertujuan untuk menganalisis respons reaktif terhadap serangan ransomware yang baru baru ini menyandera data pada Pusat Data Nasional Sementara (PDNS 2) di Surabaya. Dengan menekankan pada penlianan efektifitas dari rencana strategi yang akan diimplementasikan oleh penyelenggara yaitu Kementrian Komunikasi dan Informatika, Badan Siber dan Sandi Nasional, dan TelkomSigma selaku vendor. Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus untuk memahami lebih dalam mengenai efektifitas strategi reaktif, data primer dikumpulkan melalui sumber sekunder dan dilakukan studi literatur guna menambah sumber data sekunder dan pemahaman penulis. Gap analysis digunakan sebagai instrument evaluasi, dengan membandingkan kondisi actual dengan standard ISO/IEC 27035-1: 2023 klausa 5 bagian 5 respons, prasyarat prosedur respons sebagai parameter penilaian. Hasil dari penelitian ini adalah strategi reaktif yang diambil cukup efektif namun terbatas yang disebabkan oleh basis strategi proaktif yang kurang. Namun meski terdapat batasan, badan otoritas mampu menerapkan manajemen insiden dengan baik, sehingga hal ini mengafirmasi pernyataan bahwa strategi reaktif cukup efektif meski terbatas.

Kata Kunci: Manajemen Insiden, Keamanan Informasi, Ransomware, Pusat Data Nasional Sementara (PDNS)

1. PENDAHULUAN

Masif nya penggunaan digitalisasi, menunjukkan besarnya minat masyarakat dalam teknologi digital, sehingga hal tersebut mempengaruhi aspek kehidupan secara menyeluruh baik pada sektor publik hingga swasta, dan secara langsung mempengaruhi perilaku disebabkan oleh efisiensi dan kemudahan yang diberikan. Besarnya penerapan digitalisasi sayangnya memberi peluang ancaman siber yang besar pula, menunjukkan adanya hubungan eksponensial antara keduanya. Salah satu dari ancaman siber adalah ransomware, yang memanfaatkan kerentanan sistem untuk mendapatkan akses tidak sah, dan eksploitasi data sensitif yang ada lalu melakukan enkripsi sehingga tidak dapat diakses oleh pemilik kecuali membayar tebusan yang sudah ditentukan oleh pelaku (Aggarwal, 2023; Vasoya et al., 2022).

Pada 20 Juni 2024, terjadi ketidaktersediaan layanan imigrasi bandara, hal ini membuka pada publik bahwa telah terjadi kegagalan sistem pada Pusat Data Nasional (PDNS 2) di Surabaya akibat serangan siber ransomware Brain Chiper yang dikembangkan dari LockBit 3.0. Hasibuan berpendapat bahwa kegagalan sistem yang diakibatkan enkripsi data ini juga berdampak pada Kementrian, Lembaga dan Pemerintah daerah, dengan total sebanyak 282 instansi (Tempo, n.d.). Insiden ini membuktikan bahwa adanya kerentanan yang tidak bisa dianggap remeh. Insiden siber ini memberikan dampak kerugian yang besar secara luas, tidak hanya keamanan data masyarakat yang terancam, namun juga finansial, kepercayaan serta keamanan nasioal. Dari insiden ini

menunjukkan pentingnya manajemen insiden yang optimal, terstruktur dan efektif untuk menekan dampak yang disebabkan.

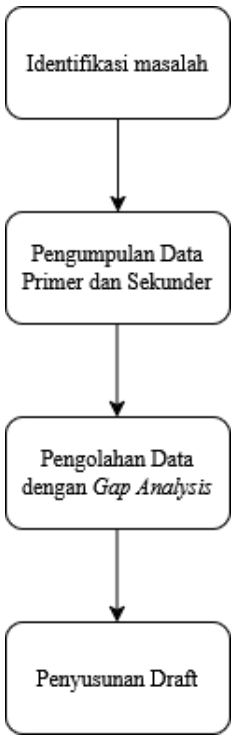
Penelitian ini dilakukan dengan tujuan untuk mengevaluasi efektivitas penerapan manajemen insiden, terutama tahap respons dan pemulihan yang diterapkan oleh badan otoritas terkait dalam menangani serangan ransomware pada kasus PDNS Surabaya dan juga guna memberikan sumbangan pikiran dari penelitian sebelumnya yang dilakukan oleh saudara Ma'ruf (Ma'ruf, 2024). Penelitian ini memiliki keterbatasan pada data, karena data primer hanya diperoleh dari sumber data sekunder. Penilitian menggunakan *gap analysis* sebagai instrument evaluasi dalam membandingkan kondisi aktual (strategi reaktif) dengan kondisi ideal (ISO/IEC 27035) untuk menilai efektifitas dan kesenjangan. Penelitian ini didasari oleh urgensi akan besarnya ancaman siber pada infrastruktur krisis. Kasus kegagalan sistem oleh serangan ransomware pada PDNS 2, dan adanya pernyataan kesulitan akan penerapan manajemen insiden, menandakan perlunya evaluasi pada strategi reaktif yang diterapkan. Penelitian ini secara praktis diharapkan dapat memberi kontribusi pemikiran untuk implementasi manajemen insiden dan rekomendasi untuk meningkatkan efektivitas strategi reaktif pada infrastruktur kritis.

2. METODE

2.1 Metode

Menurut Bogdan dan taylor (dalam Abdussamad, 2022) menjelaskan bahwa penelitian kualitatif merupakan serangkaian prosedur penelitian guna menghasilkan data deskriptif, yaitu dalam bentuk naratif atau tulisan dari objek yang diaamati. metode kualitatif merupakan metode penelitian yang memanfaatkan penggunaan data yang bersifat tidak terstruktur dan non numerical. Dalam metode ini pengumpulan data dilakukan dengan wawancara, dokumentasi, atau observasi langsung pada objek penelitian (Santosa, 2021). Penelitian ini menggunakan pendekatan studi kasus yang mana merupakan bentuk pendakatan mendalam terhadap objek terjadi dalam suatu waktu (Santosa, 2021). Metode kualitatif deskriptif dengan pendekatan studi kasus dipilih dikarenakan peneliti dapat mengeksplor secara dalam mengenai strategi reaktif dalam konteks kasus PDNS 2. Peneliti menyimpulkan bahwa metode ini relevan dengan sumber data yang dikumpulkan dengan pendekatan sekunder, dan penggunaan *gap analysis* sebagai instrument pengukuran.

Peneliti menggunakan pendekatan sekunder untuk mengumpulkan data yang meliputi sumber data dokumentasi dan berita resmi. Pendekatan ini lumrah digunakan, dan juga merupakan salah satu karakteristik dari metode kualitatif (Santosa, 2021). Pada penelitian ini sumber data yang digunakan berasal laporan resmi, berita serta siaran pers. Untuk data sekunder menggunakan literatur yang ada serta laporan tahunan BSSN. Penelitian ini memiliki alur dimulai dari identifikasi masalah hingga mengerucut ke topik. Lalu dilanjutkan dengan studi literatur mengenai topik, dan menggali data primer mengenai studi kasus. Berlanjut dilakukan pengolahan data dan penilaian menggunakan *gap analysis* untuk uji efektifitas dan kepatuhan, penggunaan instrumen ini mengacu pada penelitian sebelumnya yang telah dilakukan dengan topik pengukuran kepatuhan terhadap standar (Syahrullah et al., 2022; Yoshana et al., 2021). Berikut visualisasi alur penelitian:



Gambar 1. Alur Penelitian.

2.2 Pusat Data Nasional

Pusat data adalah sebuah fasilitas yang mampu memberikan layanan teknologi informasi dan komunikasi, dan dibangun untuk memberikan layanan yang sifatnya terintegrasi, central dan memberikan layanan jangka panjang. Umumnya memiliki infrastruktur, konektivitas, pengelolaan, manajemen dan alokasi sumber daya untuk memfasilitasi proses pemberian layanan pada tenant (Riasetiawan, 2016).

Dalam konteks nasional pusat data dianggap sebagai sebuah infrastruktur vital, yang perlu dipelihara sebagaimana infrastruktur vital lainnya, pusat data dalam konteks nasional tidak hanya memberikan layanan sistem informasi, melainkan juga akses informasi publik sampai keperluan tata kelola pemerintah akan melalui, disimpan serta dikelola oleh pusat data, dan akan menjadi infrastruktur central yang terintegrasi dengan seluruh sektor pemerintah.

Pembangunan Pusat Data Nasional merupakan implementasi dari kebijakan pemerintah yaitu pasa 27 Perpres SPBE sebagai berikut (Rahmawati, 2022):

a. Pasal 1. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data;
b. Pasal 27 ayat (4). Pusat Data Nasional sebagaimana dimaksud pada ayat (2) huruf a merupakan sekumpulan pusat data yang digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah, dan saling terhubung;
c. Pasal 27 ayat (5). Pusat Data Nasional sebagaimana dimaksud pada ayat (21) huruf a terdiri atas pusat data yang diselenggarakan oleh menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika dan/atau pusat data instansi pusat dan pemerintah daerah yang memenuhi persyaratan tertentu.Manajemen insiden.

Kominfo disamping menjalankan proses Pembangunan PDN, juga mendirikan layanan PDN Sementara yang akan memberikan layanan pada semua instansi pemerintah, sehingga nantinya pada saat migrasi data center bisa dilakukan secara bertahap. Meskipun dijelaskan terdapat cold site yang berada di lokasi berbeda, dengan tujuan untuk *backing up* sistem. Namun kenyataannya Hasibuan (DPR RI, 2024; *Kronologi Serangan Ransomware Ke PDN Dan Penanganannya Yang Tak Kunjung Usai*, n.d.) hanya terdapat 2% data backup dari keseluruhan sistem PDNS 2 yang berada di Surabaya, yang lalu ditimpali oleh Arie (dalam DPR RI, 2024) bahwasannya peraturan sebelumnya menyatakan bahwa peraturan back up bersifat optional dan tergantung kepada keinginan tenant masing masing. Tidak adanya back up yang mencukupi ini menandakan bahwa penerapan manajemen risiko jauh dari kata optimal, dan berimbas pada ketidak mampuan mengimplementasikan strategi reaktif dalam manajemen insiden dengan efektif, dan hasil optimal tidak mampu dicapai.

2.3 Manajemen Insiden

Menurut Hermadi manajemen insiden keamanan informasi adalah sebuah rangkaian proses yang dilakukan dengan tujuan untuk menyelesaikan suatu insiden yang mempengaruhi jalannya suatu layanan, dan mengembalikan ke kondisi semula (Hermadi et al., 2022).

Strategi reaktif merupakan sebuah pendekatan yang diterapkan pasca terjadinya masalah, sehingga dalam konteks keamanan informasi bisa disimpulkan merupakan pendekatan yang dilakukan secara langsung pasca terjadinya insiden guna meminimalisir dampak yang disebabkan. Berdasarkan ISO/IEC 27035 terdapat lima proses yang dilakukan dalam manajemen insiden keamanan informasi, yaitu perencanaan dan persiapan, deteksi dan pelaporan, asesmen dan pengambilan keputusan, respons, dan pembelajaran (Standar & Indonesia, 2024). Dalam ISO/IEC 27035 fase respon ini merupakan bentuk dari implementasi langsung strategi reaktif, dimana organisasi yang terdampak akan berupaya untuk mengurangi dampak, mencegah penyebaran, serta memulihkan layanan. Langkah langkah yang dilakukan tersebut selaras dengan inti dari manajemen insiden.

2.4 ISO/IEC 27035

ISO/IEC 27035 adalah standar internasional yang dikembangkan oleh *International Organization for Standarization* (ISO) untuk memberikan panduan terperinci dalam mengelola insiden keamanan (INTERNATIONAL STANDARD ISO/IEC, 2023). Standari ini mencakup siklus dari manajemen insiden yang terdiri dari lima fase utama, yaitu perencanaan dan persiapan, deteksi dan laporan, penilaian dan pengambilan keputusan, respon, dan pembelajaran pasca insiden (Wikankara et al., 2020). Standar ini bertujuan untuk membantu organisasi dalam proses perancangan pendekatan terstruktur guna mampu mengidentifikasi, menangani serta belajar dari insiden sehingga mampu meningkatkan kekuatan keamanan informasi.

ISO/IEC 27035 merupakan turunan dari ISO/IEC 27001 yang berfokus pada sistem manajemen keamanan informasi (ISMS) terutama pada bagian annex a.16 yang membahas mengenai manajemen insiden keamanan informasi, ISO/IEC 27035 ini merupakan pengembangan pembahasan dari bagian tersebut dan juga menyediakan panduan operasional secara detail dan tidak hanya fokus pada konseptual. Standar ini telah dipilih oleh Badan Standardisasi Indonesia (BSN) dan diadopsi menjadi Rancangan Standar Nasional Indonesia 3 (RSNI3) ISO/IEC 27035-1: 2023 (Standar & Indonesia, 2024)

Dilihat dari konteks manajemen insiden, strategi reaktif merupakan tindakan respons dari suatu insiden dengan tujuan untuk meminimalisir dampak yang disebabkan. Pada standar ISO/IEC 27035 terutama pada klausa 5 bagian 5 yaitu respons memberikan 16 kontrol dan 8 syarat yang perlu diterapkan untuk meraih optimalisasi manajemen insiden, terutama bagian respons. Sehingga apabila melihat konteks standar dan bagaimana standard ini dipilih sebagai standar nasional resmi, menjadikannya relevan sebagai parameter pengukuran.

Dikarenakan penelitian ini berfokus pada rencana strategi pemulihan, dan data yang dikumpulkan berupa dokumen insiden serta rancangan dan recana. Maka berdasarkan konteks standard, parameter yang akan digunakan sebagai pengukuran adalah 8 prasyarat yang harus dipenuhi sebelum diimplementasikannya strategi. Berikut metrik yang akan digunakan mengacu pada ISO/IEC 27035-1: 2023 Klausa 5 bagian 5 respons :

a. Definisi insiden yang jelas untuk dikelola dan dikontrol.
b. Daftar sumber daya yang diperlukan dan dipersyaratkan.
c. Kronologi tindakan yang akan dilakukan secara detail, dengan pengaturan waktu.
d. Jangka waktu penyelesaian target.
e. Daftar poin kontak dan saluran untuk informasi dengan kriterianya.
f. Keterampilan dan ukuran dari tim.
g. Kehadiran sumber daya.

2.5 *Gap Analysis*

Gap Analysis merupakan sebuah alat yang digunakan untuk mengidentifikasi adanya gap dan perbedaan yang ada antara kondisi ideal dengan kondisi yang ada saat ini (Kim & Ji, 2018). Dalam konteks kepatuhan terhadap standar, gap analysis dapat membandingkan apa yang harus dipenuhi berdasarkan standar atau regulasi tertentu dan apa yang dilakukan pada dunia nyata. Sehingga pada penelitian ini instrumen gap analysis digunakan dengan menggunakan checklist assessment dan dijabarkan secara naratif (Syahrullah et al., 2022; Yoshana et al., 2021).

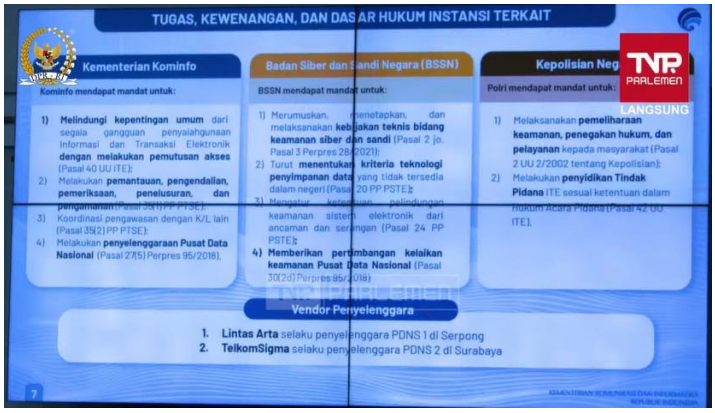
3. HASIL DAN PEMBAHASAN

3.1 Hasil

3.1.1 Langkah yang Diambil oleh Pihak Terkait

Bagian ini menjelaskan informasi yang dikumpulkan oleh penulis, membahas mengenai wewenang dan tugas pada masing masing badan otoritas terkait, serta strategi yang dilakukan sebagai bentuk tanggapan terhadap insiden dan usaha dalam meminimalisir dan memulihkan sistem dari dampak yang disebabkan oleh insiden. Langkah langkah yang dijabarkan pada penelitian ini mengacu pada ISO/IEC klausa 5 bagian 5 yaitu respons. Budie Arie selaku Menkominfo menjabarkan mengenai hal tersebut (DPR RI, 2024). Berikut penjelasan mengenai langkah yang diambil:

I. Tugas dan wewenang badan otoritas terkait (Kominfo, BSSN, Kerjasama Operasional (KSO) TelkomSigma).

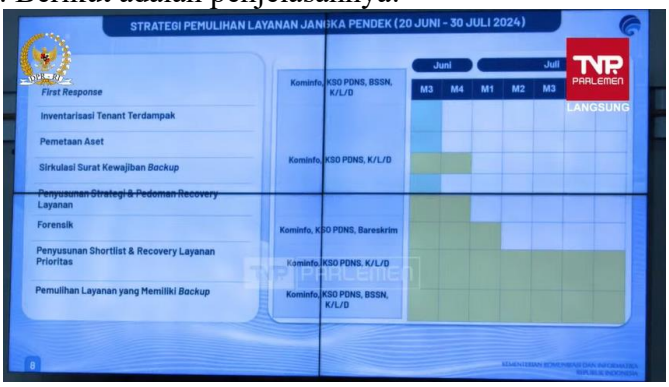


Gambar 2. Deskripsi tugas dan wewenang dengan landasan hukum (DPR RI, 2024)

Gambar 2 menjelaskan mengenai tugas, wewenang serta landasan hukum yang mendasarinya. Pada gambar diatas dijelaskan setiap posisi dan tanggung jawab yang diemban, dengan Kementrian Kominfo mendapatkan mandat sebagai pengelola dan penyelenggara PDN. BSSN mendapatkan mandat mengenai kelayakan serta keamanan sistem informasi. Kepolisian negara diberi mandat guna melaksanakan penegakan hukum dan penyidikan tindak pidana yang mengacu pada Pasal 42 UU ITE.

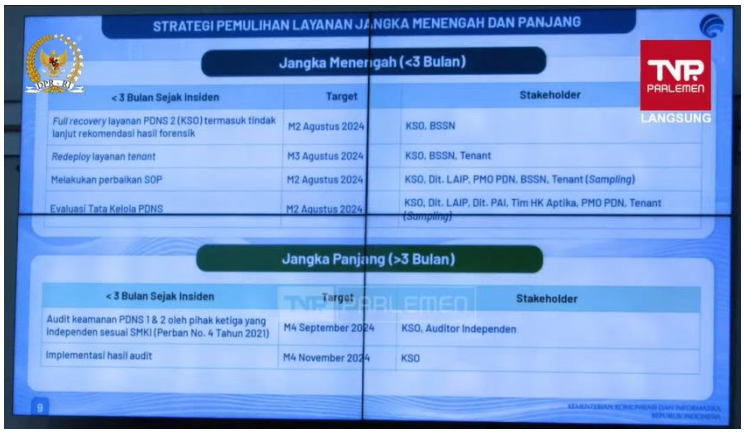
II.Strategi pemulihan layanan.

Budie Arie juga menjelaskan pada rapat mendesak menghasilkan strategi penulihan layanan yang terbagi kedalam tiga periode, yaitu jangaka pendek, jangka menengah dimana tenggat waktu pencapaian sebelum 3 bulan dari insiden terjadi, dan jangka panjang yang akan dicapai lebih dari 3 bulan setelah insiden terjadi. Berikut adalah penjelasannya:



Gambar 3. Strategi pemulihan jangka pendek (DPR RI, 2024)

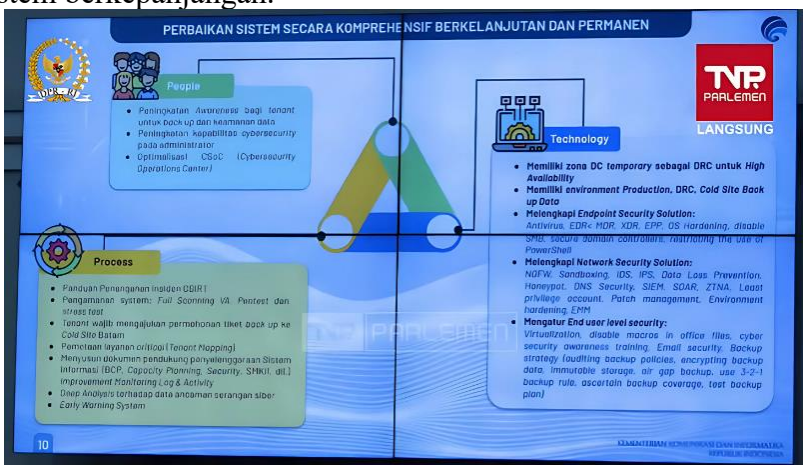
Gambar 3 menjelaskan mengenai langkah respons pertama yang diambil saat setelah insiden dilaporkan (respons pertama ini telah dijelaskan dalam bagian kronologi), dengan pemetaan waktu yang jelas dan capaian yang dapat diukur dalam jangka waktu 6 minggu.



Gambar 4. Strategi pemulihan jangka menengah dan panjang (DPR RI, 2024)

Gambar 4 menjelaskan mengenai rencana strategi pemulihan jangka menengah dan jangka panjang, Pada jangka pendek diharapkan mampu mencapai full recovery pada laynaan PDNS dan sudah mampu me-*redeploy* layanan tenant, dan dilakukan perbaikan *Standard Operation procedure* (SOP) serta evaluasi tata kelola. Pada fase jangka panjang, proses audit keamanan PDNS diharapkan selesai. Implementasi hasil audit ini ditargetkan selesai pada minggu keempat November 2024.

III.Rencana perbaikan sistem berkepanjangan.



Gambar 5. Perbaikan sistem PDNS (DPR RI, 2024)

Gambar 5 menjelaskan rencana perbaikan sistem secara komprehensif dan berkelanjutan, yang mana rencana ini dilakukan setelah proses implementasi pemulihan sisten jangka panjang berhasil dilakukan di akir November 2024. Rencana perbaikan mencakup tiga aspek utama yaitu sumber daya manusia Yang kedua adalah optimalisasi proses yang ada, dan yang terakhir meningkatkan kelengkapan teknologi dan Data Recovery Center (DRC).

3.1.2 Evaluasi Strategi Reaktif dengan Menggunakan *Gap analysis*.

Data yang telah dijabarkan sebelumnya akan diolah dengan menggunakan *gap analysis* sebagai instrument pengukuran dan menggunakan metode *checklist assessment*. Berikut adalah tabel 1, memaparkan *gap analysis* dari respons yang diambil pihak penanggung jawab PDNS 2:

Tabel 1. *Gap analysis* ISO/IEC 27035-1: 2023 dari insiden PDNS 2

Klausa	Persyaratan (Kondisi Ideal)	Kondisi Aktual	Ya	Tidak
5.5	a. Definisi insiden yang jelas untuk dikelola dan dikontrol.	Insiden didefinisikan dalam bentuk dokumen secara rinci dan lengkap.	✓	
	b. Daftar sumber daya yang diperlukan dan dipersyaratkan.	Telah didokumentasikan seluruh sumber daya yang diperlukan, baik infrastruktur, rancangan dan pihak terkait yang bertanggung jawab.	✓	
	c. Kronologi tindakan yang akan dilakukan secara detail, dengan pengaturan waktu.	Telah didokumentasikan strategi pemulihan yang runtut dan memiliki tenggat waktu masuk akal, target yang dibuat juga bisa dicapai.	✓	
	d. Jangka waktu penyelesaian target.	Jangka waktu yang dibuat selain masuk akal, namun juga telah diikuti dengan baik, dengan dibuktikan akan kemampuan cepat tanggap guna mengisolasi sistem terdampak.	✓	
	e. Daftar poin kontak dan saluran untuk informasi dengan kriterianya.	Tidak ada informasi kontak saluran informasi.		✓
	f. Keterampilan dan ukuran dari tim.	Tidak ada definisi keterampilan sumber daya manusia yang tergabung dengan tim respons.		✓
	g. Kehadiran sumber daya.	Semua sumber daya yang dibutuhkan dalam melakukan proses rspons, seperti SDM, Teknologi, dan fasilitas.	✓	

Dari tabel 1, bisa diperhatikan bahwa terdapat 6 poin yang terpenuhi dari 8 poin yang ada. Menunjukkan bahwa kepatuhan telah dilakukan oleh badan otoritas terkait, dan strategi reaktif telah sesuai dengan standard ISO/IEC 27035-1: 2023.

3.2 Pembahasan

Berikut adalah penjelasan setiap poin dengan mengacu pada standard ISO/EC 27035 (INTERNATIONAL STANDARD ISO/IEC, 2023):

a. Definisi insiden yang jelas untuk dikelola dan dikontrol.
   Pada bagian ini menjelaskan mengenai definisi insiden yang dirumuskan secara spesifik juga mencakup sifat dan tingkatan dari insiden. Hal ini akan memberikan panduan yang dapat menjadi acuan dan arahan dalam proses penanganan insiden.
   Bagian ini telah terpenuhi, dibuktikan dengan adanya pernyataan mengena tingkatan serta penyebab dari insiden. Budie Arie menjelaskan secara spesifik mengenai infrastruktur PDN serta aspek yang terdampak, penyebab, dan pernyataan bahwa mitigasi masih dalam proses (DPR RI, 2024).
b. Daftar sumber daya yang diperlukan dan dipersyaratkan.
   Bagian ini menjelaskan mengenai informasi lengkap mengenai sumber daya yang dibutuhkan guna menangani insiden. Hal ini telah terpenuhi dan dibuktikan dengan bagaimana terdapat dokumentasi baik pada infrastruktur, alat, serta tugas dan wewenang badan otoritas (DPR RI, 2024).
c. Kronologi tindakan yang akan dilakukan secara detail, dengan pengaturan waktu.
   Hal ini mengacu pada setiap daftar tindakan yang dilakukan dalam proses respons insiden disusun secara urut dan memiliki tenggat waktu. Hal ini telah dibuktikan dengan adanya strategi pemulihan yang dibuat dengan alur waktu yang terukur (DPR RI, 2024).
d. Jangka waktu penyelesaian target.
   Poin ini menjelaskan mengenai kepatuhan dalam mengikuti tenggat waktu yang telah ditetapkan. Hal ini dibuktikan dengan bagaimana beberapa langkah strategi yang telah dicapai dan hasil forensik yang keluar sesuai dengan jadwal, selain itu layanan imigrasi telah pulih berkat kepatuhan implementasi strategi pada jadwal (*Pascaserangan "Ransomware" LockBit 3.0 Ke PDN, Layanan Imigrasi Cepat Pulih Karena Data Cadangan - Kompas.Id*, n.d.)
e. Daftar poin kontak dan saluran untuk informasi dengan kriterianya.
   Poin ini membahas tentang dokumentasi poin kontak penting pada setiap instansi yang bertanggung jawab untuk mempermudah komunikasi. Poin ini tidak terpenuhi, dengan kondisi actual tidak adanya informasi secara eksplisit setiap penanggung jawab.
   Hal ini menyebabkan adanya kesenjangan berupa tidak adanya informasi mengenai kontak hingga dan standar komunikasi yang mempermudah proses komunikasi. Sehingga perlunya dokumentasi eksplisit dan penetapan standar untuk mempercepat proses komunikasi pada tahap resposn
f. Keterampilan dan ukuran dari tim.
   Poin ini membahas tentang kompetensi teknis dan non-teknis dari tim respons insiden, guna mempermudah pengukuran kemampuan dari SDM tim respons. Poin ini tidak terpenuhi, terbukti dengan kondisi actual, dimana tidak ditemukan adanya informasi mengenai hal tersebut dari setiap pihak terkait.
   Namun pada saat ditanya oleh pihak DPR mengenai hal yang sama, Hinsa Hasibuan selaku kepala BSSN menjelaskan jika memang secara SDM yang ada di bidang keamanan siber masih kurang apabila dibanding dengan kasus dan penyerangan yang ada (DPR RI, 2024).
g. Kehadiran sumber daya.
   Bagian ini membahas tentang ketersediaan sumber daya yang dibutuhkan dalam proses respons hal ini mengacu pada perangkat, fasilitas bahkan staff ahli pada saat respons dilakukan, guna memastikan sumber daya yang ada siap digunakan. Hal ini telah diterapkan dan dibuktikan dengan adanya fasilitas pendukung, dan cepatnya respons yang

diterapkan sehingga mampu mencapai target sesuai dengan jadwal yang telah ditetapkan (DPR RI, 2024).

Berdasarkan penjelasan hasil diatas, bisa disimpulkan bahwa strategi reaktif yang diterapkan oleh Badan otoritas terkait dalam meminimalisir insiden yang menimpa PDNS 2 telah memenuhi enam dari 8 parameter yang ada, hal tersebut menunjukkan bahwa strategi reaktif yang dirancang telah sesuai dan patuh terhadap standard, sehingga strategi reaktif tersebut memiliki efektivitas yang tinggi.

Namun apabila dilihat pada kronologi insiden, meski strategi reaktif telah sesuai dengan standar dan mampu memenuhi target yang telah ditentukan, namun belum mampu untuk memberikan layanan kembali pada setiap *tenant* yang terdampak (kecuali layanan imigrasi dikarenakan memiliki *backup* mandiri), dan tidak adanya tim CSIRT menjadikan sistem *data center* rentan terhadap serangan. Hal ini menunjukkan bahwa strategi proaktif secara langsung mempengaruhi efektivitas dari strategi reaktif, hal ini dibuktikan dengan keterkaitan antara standar ISO/IEC 27035-1:2023 yang merupakan perpanjangan dari standar ISO/IEC27001, terutama pada klausa 16 yang berofkus pada manajemen insiden secara umum dan klausa 6 yang membahas mengenai manajemen risiko, yang relevan dengan manajemen insiden, membahas mengenai hal hal yang perlu dilakukan organisasi guna memitigasi kemungkinanan terjadinya risiko, hal ini bisa dikelompokkan kedalam strategi proaktif (INTERNATIONAL STANDARD ISO/IEC, 2023; Standar & Indonesia, 2024).

Meskipun adanya kekurangan signifikan pada aspek strategi proaktif, dan hal tersebut memberikan pengaruh tinggi terhadap efektivitas strategi reaktif yang diambil. Namun pada bulang Agustus PDNS 2 telah sepenuhnya pulih dan layanan tenant prioritas juga telah kembali berjalan 100% menurut Nezar Patria (*Kementerian Komunikasi Dan Digital*, n.d.). Dari pernyataan tersebut menunjukkan bahwa strategi reaktif yang diambil telah efektif, meskipun memiliki beberapa kelemahan dan kesulitan implementasi dalam proses dikarenakan adanya kecurangan pada strategi proaktif.

4 SIMPULAN

Evaluasi pada delapan aspek strategi reaktif dengan mengacu pada standar prasyarat ISO/IEC 27035 yang dirancang oleh pihak terkait, telah sesuai dengan memenuhi 6 dari total 8 tolak ukur. Menunjukkan strategi reaktif cukup efektif dalam usahanya memitigasi insiden, dan juga pihak terkait telah ptauh pada standar. Namun dua parameter yang belum terpenuhi, yaitu poin kontak saluran informasi juga keterampilan dan ukuran tim respons, menunjukkan adanya kesenjangan yang berdampak pada efisiensi koordinasi dan pengukuran kesiapan kemampuan tim respons. Hal ini perlu menjadi perhatian untuk masa mendatang, terutama dalam implementasi strategi reaktif dalam upaya menghadapi insiden pada infrastruktur kritis. Pada evaluasi ini juga menunjukkan hubungan antara strategi proaktif, seperti tidak adanya tim CSIRT, kapasitan SDM pengguna sistem, serta kecurangan back up, mempengaruhi efektifitas strategi reaktif secara signifikan. Namun melihat bukti PDNS 2 pada bulan Agustus telah pulih sepenuhnya sesuai dengan perkiraan waktu yang telah ditetapkan, mendukung hasil evaluasi dari penelitian ini.

Berdasarkan penelitian diatas, ditemukan beberapa aspek yang perlu perbaikan baik dari segi proaktif dan juga reaktif. Berikut adalah perbaikan pada kedua aspek diatas:

I. Peningkatan standar yg tidak terimplementasikan

i. Dokumentasi kontak dan saluran informasi
   a) Perlunya setiap instansi mendokumentasikan daftar penanggung jawab secara rinci guna memudahkan dalam komunikasi.
   b) Membuat protocol komunikasi standar agar dapat mempercepat koordinasi dan respons.

ii. Keterampilan dan ukuran dari tim.
   a) Dokumentasikan keterampilan dan peran setiap anggota tim respons untuk memastikan ukuran dan komposisi tim yang memadai sesuai kebutuhan.
   b) Lakukan pelatihan teknis dan non-teknis secara berkala untuk meningkatkan kompetensi tim respons insiden.

II. Perbaikan strategi proaktif
   a) Dengan membentuk tim CSIRT yang mampu memantau respons insiden secara keberlanjutan secara real time dan fokus hanya pada setiap PDNS.
   b) Diberlakukan kewajiban back up oleh setiap tenant pada coldsite Batam yang merupakan bagian dari PDNS 2 Surabaya.
   c) Mengimplementasikan manajemen risiko sesuai dengan standard ISO/IEC 27001 guna memitigasi potensi risiko dan meminimalisir risiko tereskalasi menjadi insiden.

Mengacu pada siaran pers oleh wamenkominfo, badan otoritas terkait telah banyak melakukan perbaikan dan beberapa termasuk seperti saran yang penulis tampilkan, hal ini menunjukkan kemampuan tim melakukan pembelajaran dan perbaikan dari pasca insiden, menunjukkan kepatuhan terhadap ISO/IEC 27035.

UCAPAN TERIMAKASIH

Ucapan terimakasih saya sampaikan pada Ibu Syerlie Annisa selaku dosen pembimbing dalam mata kuliah karya ilmiah membantu dan membimbing saya dalam proses penyusunan. Dan terimakasih kepada Orang tua serta keluarga atas dukungan moril, doa serta motivasi yang diberikan selama proses penyusunan penelitian ini.

DAFTAR PUSTAKA

Abdussamad, Z. (2022). *Buku Metode Penelitian Kualitatif*. https://doi.org/10.31219/OSF.IO/JUWXN

Aggarwal, M. (2023). Ransomware Attack: An Evolving Targeted Threat. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*, 1–7. https://doi.org/10.1109/ICCCNT56998.2023.10308249

DPR RI. (2024, June 24). *BREAKING NEWS - KOMISI I DPR RI RAKER DENGAN MENKOMINFO DAN KA.BSSN - YouTube*. https://www.youtube.com/watch?v=tsL_jDztzC0

Hermadi, I., Wulandari, Fatimah, H. A., & Hasanah, N. (2022). MSIM4407 Manajemen Layanan Teknologi Informasi. *Universitas Terbuka*, 414. https://pustaka.ut.ac.id/lib/wp-content/uploads/pdfmk/MSIM4407-M1.pdf

INTERNATIONAL STANDARD ISO/IEC. (2023). *Information technology-Information security incident management-Part 1: Principles and process*. *2023*, 1–13. www.iso.org

Kementerian Komunikasi dan Digital. (n.d.). Retrieved December 19, 2024, from https://www.komdigi.go.id/berita/siaran-pers/detail/wamen-nezar-patria-layanan-pdns-2-sudah-pulih-total

Kim, S., & Ji, Y. (2018). Gap Analysis. *The International Encyclopedia of Strategic Communication*, 1–6. https://doi.org/10.1002/9781119010722.IESC0079

Kronologi Serangan Ransomware ke PDN dan Penanganannya yang Tak Kunjung Usai. (n.d.). Retrieved November 26, 2024, from https://tekno.kompas.com/read/2024/07/10/12350077/kronologi-serangan-ransomware-ke-pdn-dan-penanganannya-yang-tak-kunjung-usai

Ma'ruf, S. (2024). Crisis Management and Incident Response: a National Data Center Case Study. *Jurnal Intelek Dan Cendikiawan Nusantara*, *1*(3), 4619–4633. https://jicnusantara.com/index.php/jicn/article/view/674

Mardhani Riasetiawan. (2016). *Pusat Data untuk Pemerintahan @ 2016 2 Daftar Isi DAFTAR ISI 2 BAB 1. PUSAT DATA 4 1.1 DEFINISI PUSAT DATA 5 1.2 LAYANAN PUSAT DATA 6 1.3 PARADOX BIAYA DAN REVENUE 7 1.4 PENGGUNA PUSAT DATA 8 1.4.1 LAYANAN INTERNET KOMERSIAL 8 1.4.2 E---GOVERNMENT*. 1–57.

Pascaserangan "Ransomware" LockBit 3.0 ke PDN, Layanan Imigrasi Cepat Pulih karena Data Cadangan - Kompas.id. (n.d.). Retrieved December 19, 2024, from https://www.kompas.id/baca/polhuk/2024/06/28/layanan-imigrasi-cepat-pulih-karena-data-cadangan

Rahmawati, F. (2022). Pusat Data Nasional (PDN). *Kominfo*, 1–9. https://aptika.kominfo.go.id/2022/07/pusat-data-nasional-pdn/

Santosa, P. I. (2021). *MSIM4312 – Metodologi Penelitian*. 372. https://pustaka.ut.ac.id/lib/msim4312-metodologi-penelitian/

Standar, R., & Indonesia, N. (2024). *RSNI3*. *2023*.

Standards.Iteh.Ai. (2022). *Information security, cybersecurity and privacy protection-Information security management systems-Requirements iTeh STANDARD PREVIEW (standards.iteh.ai)*. *2022*, iii–5.

Syahrullah, Y., Yanti, A., Adhiana, T. P., & Imran, R. A. (2022). GAP Analysis of Higher Education Quality Assurance System Implementation Against Educational Organization Management Standards ISO 21001:2018. *Operations Excellence: Journal of Applied Industrial Engineering*, *14*(1), 67. https://doi.org/10.22441/oe.2022.v14.i1.044

Tempo. (n.d.). *Imbas Serangan Siber ke PDNS 2, Pemerintah Beberkan Skema Pemulihan Migrasi Data | tempo.co*. Retrieved November 26, 2024, from https://www.tempo.co/politik/imbas-serangan-siber-ke-pdns-2-pemerintah-beberkan-skema-pemulihan-migrasi-data-45293

Vasoya, S., Bhavsar, K., & Patel, N. (2022). *A systematic literature review on Ransomware attacks*. http://arxiv.org/abs/2212.04063

Wikankara, Hartanto, R., & Nugroho, L. E. (2020). Perancangan Sistem Manajamen Insiden Keamanan Informasi Berdasarkan SNI ISO/IEC 27035 Di Instansi Pemerintah. *Jurnal Teknologi Technoscientia*, *13*(1), 1–10.

Yoshana, A., Putra, M. F., & Ulina, N. S. (2021). Gap Analysis Implementasi Iso 14000:2015 Pada Pt. Sas International. *Jurnal Teknologi Dan Manajemen*, *19*(2), 71–78. https://doi.org/10.52330/jtm.v19i2.32