NUANSA INFORMATIKA ***p-ISSN :1858-3911 , e-ISSN : 2614-5405***
Volume 18 Nomor 2, Juli 2024 https://journal.fkom.uniku.ac.id/ilkom

Jaminan Informasi dan Keamanan yang Lebih Baik: Studi Kasus BPJS Kesehatan

Abdul Hakim Satria Nusantara*[1], Irhan Khairul Umam[2], Muharman Lubis[3]
[1,2,3]Magister Sistem Informasi, Universitas Telkom
E-mail: *[1] **ahsatrianusantara@student.telkomuniversity.ac.id** ,[2] irhankhairul@student.telkomuniversity.ac.id ,[3] muharmanlubis@telkomuniversity.ac.id

Abstrak

Pada tahun 2021, BPJS Kesehatan mengalami insiden kebocoran data yang signifikan, di mana data pribadi 279 juta penduduk Indonesia bocor dan diperjualbelikan di forum hacker. Insiden ini menimbulkan dampak serius terhadap privasi individu dan reputasi BPJS Kesehatan. Makalah ini menganalisis insiden tersebut menggunakan metode siklus hidup keamanan, yang terdiri dari tahapan identifikasi, analisa/asesmen, proteksi, dan monitoring. Temuan menunjukkan bahwa kelemahan dalam sistem keamanan IT dan kurangnya monitoring berkelanjutan berkontribusi terhadap kebocoran tersebut. Rekomendasi mencakup penguatan protokol keamanan, pelatihan staf, dan implementasi monitoring real-time untuk mencegah insiden serupa di masa depan.

Kata Kunci*—Siklus Hidup Keamanan, Jaminan Informasi, Jaminan Keamanan, Kebocoran Data*

Abstract

In 2021, BPJS Kesehatan experienced a significant data leak incident, where the personal data of 279 million Indonesians was leaked and traded on hacker forums. This incident has a serious impact on individual privacy and the reputation of BPJS Kesehatan. This paper analyzes the incident using the security lifecycle method, which consists of the stages of identification, analysis/assessment, protection, and monitoring. The findings suggest that weaknesses in IT security systems and a lack of continuous monitoring contributed to the leaks. Recommendations include strengthening security protocols, staff training, and implementing real-time monitoring to prevent similar incidents in the future.

Keywords*—Security Lifecycle, Information Assurance, Security Assurance, Data Leakage*

Diajukan: 20 June 2023 *Disetujui: 25 June 2023* *Dipublikasi: 20 Juli 2024*

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

1. PENDAHULUAN

BPJS Kesehatan merupakan badan publik yang bertanggung jawab untuk menyelenggarakan program jaminan kesehatan nasional di Indonesia. Sebagai penyelenggara asuransi kesehatan sosial terbesar, BPJS Kesehatan mengelola berbagai data sensitif, seperti data pribadi peserta, data kesehatan, dan data keuangan.

Proses bisnisnya melibatkan pengumpulan, pengelolaan, dan penyimpanan data untuk menjamin pelayanan kesehatan yang efektifdan efisien bagi para pesertanya.

Namun, BPJS Kesehatan telah mengalami beberapa insiden kebocoran data yang signifikan. Salah satu insiden terbesar terjadi pada Mei 2021, di mana data pribadi sekitar 279 juta penduduk Indonesia bocor dan diperjualbelikan di forum hacker. Insiden ini menyoroti risiko besar dalam pengelolaan data kesehatan dan pentingnya langkah-langkah keamanan yang kuat.

Kebocoran data tersebut berdampak luas, mulai dari potensi penyalahgunaan data pribadi, kerugian materiil dan imateriel bagiindividu, hingga terganggunya kepercayaan

publik terhadap BPJS Kesehatan. Upaya penanganan yang dilakukan mencakup investigasi, peningkatan protokol keamanan, dan kerja sama dengan pihak berwenang.

Jaminan informasi keamanan menjadi sangat penting di era digital saat ini, seiring dengan semakin banyaknya data yang dikumpulkan dan disimpan oleh organisasi, baik pemerintah maupun swasta. Risiko kebocoran dan penyalahgunaan data semakin meningkat, sehingga jaminan informasi keamanan sangat diperlukanuntuk melindungi data sensitif dari akses yang tidak sah, pencurian, dan serangan siber. Hal ini tidak hanya melindungi individu dari potensi kerugian, tetapi juga menjaga reputasi organisasi dan mencegah kerugian finansial yang besar akibat pelanggaran data.

Banyak negara dan industri memiliki peraturan ketat terkait perlindungan data. Dengan menerapkan praktik keamanan informasi yang kuat, organisasi dapat memastikan kepatuhan hukum dan menghindari denda yang mahal, sekaligus meningkatkan kepercayaan dari pelanggan dan mitra bisnis. Dengan demikian, jaminan informasi keamanan tidak hanya melindungi data, tetapi juga merupakan bagian integral dari tata kelola dan keberlanjutan bisnis.

Pembelajaran sistematis dari insiden keamanan menjadi penting, karena organisasi cenderung fokus pada penyebab langsung, namun sering mengabaikan penyebab tidak langsung yang lebih mendasar, seperti kurangnya pelatihan atau kesadaran keamanan staf. Dalam konteks BPJS Kesehatan, penggunaan metode terkait jaminan informasi dan keamanan sangat penting untuk mengidentifikasi mekanisme kontrol yang gagal.

Penelitian ini bertujuan untuk menganalisis pendekatan penangananinsiden kebocoran data di BPJS Kesehatan, serta memberikan temuan dan rekomendasi untuk meningkatkan keamanan data di masa mendatang. Melalui pendekatan ini, diharapkan dapat memberikan kontribusi signifikan dalam meningkatkan keamanan data di BPJS Kesehatan dan organisasi serupa lainnya.

1.1. Badan Penyelenggara Jaminan Sosial Kesehatan

BPJS Kesehatan, yang dikenal sebagai Badan Penyelenggara Jaminan Soal Kesehatan, didirikan pada tanggal 1 Januari 2014 sebagai bagian dari upaya pemerintah Indonesia untuk menawarkan cakupan kesehatan nasional kepada seluruh masyarakat. Sejarah pendirian dimulai dengan konversi PT Askes (Persero), yang sebelumnya mengelola asuransi kesehatan pegawai negeri, menjadi BPJS Kesehatan berdasarkan Undang-Undang No. 24 Tahun 2011. Tujuan utama BPJS Kesehatan adalah untuk menjamin ketersediaan layanan kesehatan yang hemat biaya dan berkualitas tinggi bagi individu dari semua latar belakang sosial ekonomi, dengan menggunakan mekanisme keadilan yang adil dan tidak memihak.

Sebagai penyelenggara inisiatif

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

jaminan kesehatan nasional terkemuka di Indonesia, BPJS Kesehatan mengoperasikan berbagai kegiatan yang meliputi penyusunan, pengawasan, dan penerapan data dan informasi. Informasi yang dikumpulkan oleh BPJS Kesehatan mencakup rincian pribadi peserta, seperti nomor identitas nasional (NIK), nama, lokasi, dan rincian kontak. Selain itu, informasi medis peserta, termasuk latar belakang medis, hasil diagnosis, dan log perawatan, juga disimpan. Data keuangan yang terkait dengan iuran peserta dan klaim perawatan kesehatan juga diatur untuk memastikan keberlanjutan program.

Sebelum kejadian signifikan pada Mei 2021, BPJS Kesehatan telah mengalami banyak kasus pelanggaran keamanan data. Pada tahun 2018, ada insiden akses tidak sah di mana data pribadi beberapa peserta dikompromikan. Kejadian ini menggarisbawahi kerentanan dalam infrastruktur keamanan dan pengelolaan data BPJS Kesehatan. Selanjutnya, pada 2019, pelanggaran lain menyebabkan penyebaran data peserta secara tidak sah di internet. Masing-masing episode ini memberikan wawasan berharga tentang pentingnya perlindungan data dan perlindungan privasi peserta, menggarisbawahi perlunya peningkatan berkelanjutan dalam aparat keamanan informasi BPJS Kesehatan.

1.2. Kasus Kebocoran Data di Indonesia

Pada tahun 2020, Tokopedia, salah satu platform e-commerce terbesar di Indonesia, mengalami peretasan besar-besaran yang mempengaruhi sekitar 91 juta akun pengguna dan 7 juta akun merchant. Insiden ini pertama kali dipublikasikan oleh peretas dengan nama Whysodank di Raid Forum pada tanggal 2 Mei 2020, meskipun peretasan tersebut terjadi pada 20 Maret 2020. Tokopedia sebelumnya melaporkan bahwa pada tahun 2019, mereka memiliki sekitar 91 juta akun aktif di platformnya. Dalam pernyataan resminya pada 2 April 2020, Tokopedia menyatakan, "Berkaitan dengan isu yang beredar, kami menemukan adanya upaya pencurian data terhadap pengguna Tokopedia. Namun, Tokopedia memastikan informasi penting pengguna, seperti password, tetap berhasil terlindungi." Sebagai respons atas kebocoran data ini, Menteri Komunikasi dan Informatika,Johnny Gerard Plate, meminta pengelola platform digital Tokopedia untuk melakukan investigasi internal. Langkah ini bertujuan untuk memastikan dugaan kebocoran data dan mengambil tindakan yang diperlukan guna menjamin keamanan data pengguna. Kasus peretasan ini menggambarkan tantangan signifikan yang dihadapi oleh platform e-commerce dalam menjaga keamanan data pengguna. Hal ini menunjukkan pentingnya penerapan praktik terbaik dalam pengelolaan data dan keamanan informasi, serta etika digital. Membangun budaya yang mendukung penggunaan teknologi secara bertanggung jawab dan efektif sangat penting untuk memastikan bahwa transformasi digital tidak hanya meningkatkan operasional, tetapi juga berkelanjutan dan memberikan dampak positif jangka panjang.

1.3. Siklus Hidup Keamanan

Dalam bidang keamanan, melakukan identifikasi awal terhadap entitas yang membutuhkan pengamanan adalah yang paling penting. Prosedur ini mencakup berbagai fase penting yang perlu dijalankan: identifikasi, analisis/penilaian, perlindungan, dan pemantauan.

Tahap awal dalam siklus hidup keamanan adalah Fase Identifikasi, di manasemua aset penting yang memerlukan perlindungan untuk memastikan keamanan diakui. Dalam menjamin suatu keamanan pada tahap ini, maka perlu didefinisikan aset yang berdampak apabila terkena serangan.

Setelah identifikasi, langkah selanjutnya melibatkan analisis atau penilaian keamanan. Ini mencakup mengukur dan menilai keseriusan dan kemungkinan ancaman, serta memastikan prioritas berdasarkan hasil penilaian. Agar terjamin keamanan yang dituju, pada proses ini penting untuk menerapkan metode pengukuran dalam penentuan skala prioritas.

Tahap Perlindungan terdiri dari pelaksanaan langkah-langkah keamanan yang penting untuk menjaga aset dan data

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

penting yang diidentifikasi. Studi kasus terbaik bisa dipelajari untuk mendapatkan kepastian kesuksesan dari salah satu strategi keamanan.

Tahap Pemantauan, meskipun sering diabaikan, adalah fase penutup dalamsiklus hidup keamanan. Proses ini sangatpenting karena memberikan umpan balik dari penegakan perlindungan dari fase identifikasi hingga perlindungan. Pemantauan yang efisien memfasilitasi identifikasi dini aktivitas mencurigakan atau pelanggaran keamanan, memungkinkan tanggapan cepat untuk mengurangi dampak.

Naskah ini bertujuan untuk menggambarkan siklus hidup keamanan, secara khusus menyoroti studi kasus kebocoran data yang dialami BPJS Kesehatan pada tahun 2021. Dan menguraikan kelayakan pelaksanaansetiap fase dalam siklus hidup keamanan untuk meningkatkan jaminan informasi dan perlindungan data, sementara juga mengurangi kemungkinan kejadian berulang dari insiden di waktu berikutnya.

2. METODE PENELITIAN

Penelitian ini menggunakan metodologi kualitatif yang memanfaatkan pendekatan studi kasus untuk memeriksa terjadinya pelanggaran data di BPJS Kesehatan pada tahun 2021. Metodologi yang digunakan mencakup berbagai fase penting yang selaras dengan siklus hidup keamanan, yaitu identifikasi, analisis/penilaian, perlindungan, dan pemantauan. Pengumpulan data dilakukan melalui tinjauan literatur secara menyeluruh, analisis insiden, dan konsultasi dengan pakar keamanan informasi.

Data yang diperoleh dari setiap tahap diperiksa secara menyeluruh untuk memahami penyebab kebocoran data, kerentanan dalam infrastruktur keamanan, dan tindakan korektif selanjutnya yang diterapkan. Kesimpulan yang diambil dari evaluasi ini digunakan untuk mengembangkan saran untuk meningkatkan keamanan informasi dan mencegah kejadian yang sebanding di kemudian hari.

3. HASIL DAN PEMBAHASAN

3.1. Kronologis Kejadian

Pada Mei 2021, BPJS Kesehatan mengalami salah satu insiden pelanggaran data paling signifikan dalam sejarah Indonesia. Terjadinya pelanggaran data di BPJS Kesehatan secara resmi diakui pada pertengahan Mei 2021. Secara khusus, pengungkapan pelanggaran ini dimulai pada 12 Mei 2021, ketika seorang individu yang diidentifikasi sebagai “Kotz” di forum RaidForums menuduh memiliki informasi pribadi dari 279 juta warga Indonesia yang terdaftar di BPJS Kesehatan (Antara News) (Kompas.com).

Pelanggaran tersebut dilakukan dengan mengeksploitasi kerentanan pada infrastruktur keamanan BPJS Kesehatan. Para peretas berhasil menyusup data menggunakan teknik yang belum diungkapkan secara eksplisit oleh pihak berwenang, mungkin melibatkankekurangan dalam sistem penyimpanan dan administrasi data BPJS (Kompas.com). Peretas menggunakan metodologi yang mengeksploitasi kerentanan tersebut untuk mengakses dan mengekstrak data dalam jumlah besar. Data yang disusupi meliputi nama, NIK, alamat, nomor telepon, alamat email, dan rincian gaji peserta BPJS Kesehatan (Antara News).

Menyusul konfirmasi pelanggaran tersebut, berbagai tindakan diprakarsai oleh BPJS Kesehatan dan pemerintah. BPJS Kesehatan segera bekerja sama dengan Kementerian Komunikasi dan Informatika (Kominfo) untuk membatasi akses ke platform penjual data. Selain itu, pemerintah melarang masuk ke RaidForums dan situs duplikatnya yang digunakan untuk menyebarluaskan data yang dicuri (Antara News). Selain itu, BPJS Kesehatan melaporkan kejadian tersebut kepada pihak berwenang terkait dan memulai penyelidikan internal untuk mengungkap asal mula pelanggaran tersebut (Kompas.com). Runtutan kronologis tindakan yang dilakukan terlihat pada

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

gambar 1.

Terkonfirmasi bahwa ditemukan adanya kebocoran data dari server BPJS Kesehatan yang rentan terhadap serangan. Hal ini menyebabkan kerugian materiil dan imateriel bagi pemegang data serta potensi tuntutan hukum. Sebagai tindakan penanggulangan, BPJS Kesehatan meningkatkan sistem keamanan dan melaksanakan pelatihan staf untuk memperkuat kemampuan mereka dalam menghadapi ancaman siber di masa mendatang (KOMPAS.com).

Gambar 1. Lini masa kejadian BPJS Kesehatan

Kerentanan mendasar yang menyebabkan insiden ini terutama berasal dari kekurangan dalam menerapkan kerangka keamanan siber BPJS Kesehatan. Aspek teknis terperinci mengenai pelanggaran ini tidak diungkapkan secara luas, tetapi dianggap melibatkan penyimpangan dalam penerapan kontrol akses yang memadai dan enkripsi data (Kompas.com).

Dampak dari pelanggaran ini sangat mendalam. Informasi pribadi 279 juta orang Indonesia, termasuk data sensitif, kini beredar di internet. Hal ini menghadirkan risiko besar terhadap privasi dan keamanan individu, termasuk potensi penyalahgunaan data untuk kegiatan ilegal seperti pencurian identitas dan pelanggaran keuangan lainnya. Selain itu, kedudukan BPJS Kesehatan sebagai penyedia layanan kesejahteraan sosial mengalami konsekuensi yang merugikan (Antara News) (Kompas.com).

3.2. Pendekatan Analisis Berdasarkan Siklus Hidup Keamanan

Kontrol keamanan dan privasi dapat digunakan secara efektif untuk melindungi organisasi, individu, dan sistem informasi dari ancaman tradisional dan lanjutan yang terus-menerus dan risiko privasi yang timbul dari pemrosesan informasi identitas pribadi (PII) bervariasi skenario operasional, lingkungan, dan teknis. Kontrol dapat digunakan untuk mendemonstrasikan kepatuhan terhadap berbagai keamanan dan privasi pemerintah, organisasi, atau institusi persyaratan. Organisasi memiliki tanggung jawab untuk memilih keamanan dan kontrol privasi, untuk menerapkan kontrol dengan benar, dan untuk menunjukkan efektivitas kontrol dalam memenuhi persyaratan keamanan dan privasi [1].

Dengan mengacu pada siklus hidup keamanan, kami menjabarkan jaminan serta langkah apa yang perlu dilakukan oleh BPJS Kesehatan dalam setiap fase. Fase siklus hidup keamanan dari identifikasi, analisis, proteksi, dan monitor tergambar pada gambar 2.

3.2.1. Mengidentifikasi

Pada tahap ini, BPJS Kesehatan harus mengidentifikasi secara menyeluruh semua aset penting dan potensi ancamanyang terkait dengan informasi pribadi dan medis di bawah pengelolaan. Hal ini mencakup identifikasi sistem teknologi informasi yang digunakan untuk penyimpanan dan pemrosesan data peserta, bersama dengan identifikasi kerentanan yang ada dalam sistem [2]. Pemilik aset harus identifikasi untuk setiap aset, untuk memberikan tanggung jawab dan akuntabilitas untuk aset tersebut. Aset tersebut tidak memiliki hak atas aset, tetapi memiliki tanggung jawab untuk pembuatan, pengembangan, pemeliharaan, penggunaan dan keamanan yang sesuai [3]. Orang yang sering mengunjungi platform RaidForums, yang mengaku memiliki informasi pribadi yang berkaitan dengan 279 juta orang Indonesia, telah mengungkap celah keamanan dalam infrastruktur BPJS Kesehatan. Akibatnya, menjadi penting untuk menentukan setiap area kelemahandan dengan cermat menyusun daftar lengkap semua aset berharga sambil memahami risiko terkait. Dengan demikian, fase identifikasi ini juga harus memastikan bahwa ada jaminan keamanan yang memadai bagi setiap aset, sehingga setiap potensi ancaman dapat diantisipasi danmitigasi secara efektif.

3.2.2. Menilai

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Setelah diidentifikasi, BPJS Kesehatan harus melakukan penilaian risiko untuk memastikan besarnya potensi dampak yang ditimbulkan oleh ancaman yang teridentifikasi [4]. Penilaian resiko adalah proses pertama dalam metodologi manajemen resiko.

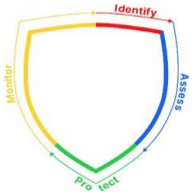
Organisasi menggunakan penilaian resiko untuk menentukan tingkat ancaman dan resiko terhadap sistem IT mereka. Hasil dari proses ini akan membantu mengidentifikasi pengendalian resiko yang sesuai untuk mengurangi atau menghilangkan resiko-resiko tersebut pada proses pengurangan resiko [5]. Proses ini melibatkan penilaian tingkat keparahan dan probabilitas ancaman.Mengenai pelanggaran data pada Mei 2021,evaluasi harus menyelidiki alasan di balik peretas dapat mengeksploitasi dan memperdagangkan informasi pribadi 279 juta orang. Analisis tersebut berperan penting dalam membantu BPJS Kesehatan memahami bidang-bidang kritis dan kedekatan tindakan yang diperlukan untuk mengurangi kerentanan keamanan yang berlaku. Selain itu, fase asesmen ini harus memastikan adanya jaminan bahwa setiap risiko yang diidentifikasi telah dinilai secara komprehensif, sehingga tindakan mitigasi yang tepat dapat diterapkan untuk melindungi integritas dan kerahasiaan data peserta secara efektif.

3.2.3. Melindungi

Fase perlindungan melibatkan penerapan langkah-langkah keamanan yang penting untuk menjaga aset dan informasi yang diidentifikasi sebagai penting. Praktik baik di berbagai kasus dapat dicermati untuk kemudian diterapkan pada BPJS Kesehatan, baik secara keseluruhan maupun secara parsial [4]. Untuk BPJS Kesehatan, ini melibatkan peningkatan sistem keamanan TI melalui pemanfaatan enkripsi data, peningkatan sistem dan perangkat lunak reguler [6], dan peningkatan pembatasan akses data sensitif [4]. Selain itu, perlindungan mencakup penyediaan pelatihan keamanan bagi karyawan untuk meningkatkan kewaspadaan mereka terhadap ancaman siber. Mengingat pelanggaran data Mei 2021, strategi perlindungan yang lebih ketat dan adopsi teknologi keamanan canggih sangat penting untuk mencegah kejadian serupa di masa depan. Dalam fase proteksi ini, BPJS Kesehatan harus memastikan adanya jaminan bahwa semua metode proteksi yang diimplementasikan, seperti enkripsi data dan pembatasan akses, benar-benar efektifdalam melindungi data sensitif. Hal ini termasuk penerapan metode proteksi yang berkelanjutan dan adaptif terhadap ancaman baru yang mungkin muncul, serta memastikan bahwa langkah-langkah ini dapat memberikan perlindungan menyeluruh dan berkelanjutan bagi seluruh data peserta.

3.2.4. Memantau

Tahap terakhir adalah fase pemantauan, di mana BPJS Kesehatan diharuskan untuk secara konsisten mengamati sistem dan mengidentifikasi aktivitas yang tidak biasa atau pelanggaran keamanan. Pemantauan yang efektif dapat mengidentifikasi dengan cepat pelanggaran keamanan dan mengurangi dampaknya. Ini mencakup pemanfaatan mekanisme pemantauan real-time untuk mengidentifikasi upaya akses yang tidak sah dan penyimpangan dalam sistem. Selain itu, BPJS Kesehatan harus melakukan evaluasi berkala terhadap protokol dan proses keamanan mereka, bersama dengan audit rutin untuk menjamin keamanan sistem yang berkelanjutan. Selain itu, BPJS Kesehatan harus melakukan evaluasi berkala terhadap protokol dan proses keamanan mereka, bersama dengan audit rutin untuk menjamin keamanan sistem yang berkelanjutan.



Gambar 2. Siklus hidup keamanan

4. KESIMPULAN

Penelitian ini meneliti kejadian kebocoran data yang ditemui BPJS

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

Kesehatan pada tahun 2021 dengan menggunakan metodologi siklus hidup keamanan, yang terdiri dari tahapan identifikasi, penilaian, perlindungan, dan pemantauan. Hasil pemeriksaan mengungkapkan bahwa kerentanan dalam kerangka keamanan TI dan tidak adanya pemantauan berkelanjutan adalah faktor utama yang berkontribusi terhadap insiden tersebut. Konsekuensi dari pelanggaran data ini patut diperhatikan, menimbulkan ancaman bagi privasi individu dan menodai reputasi BPJS Kesehatan.

Penemuan investigasi ini menggarisbawahi pentingnya pendekatan metodis dalam jaminan keamanan informasi [7]. Identifikasi dan penilaian risiko yang akurat dapat membantu dalam memahami ancaman yang ada dan menetapkan prioritas langkah-langkah keamanan. Pelaksanaan langkah-langkah perlindungan yang efisien, seperti enkripsi data dan pelatihan keamanan untuk personel, dapat mencegah akses yangtidak sah. Pemantauan berkelanjutan sangat penting untuk mengidentifikasi aktivitas yang mencurigakan dan segera mengatasi insiden keamanan dan evaluasi berkala dari keseluruhan proses sebelumnya.

Kontribusi utama dari penelitian ini adalah untuk menawarkan panduan praktis bagi entitas serupa untuk meningkatkan keamanan data mereka. Pendekatan terstruktur dan menyeluruh terhadap siklus hidup keamanan dapat membantu mengurangi kemungkinan kebocoran data dan meningkatkan kepercayaan publikdalam manajemen data yang aman. Studi ini juga menekankan perlunya penilaian berkala dan revisi protokol keamanan untuk memastikan perlindungan berkelanjutan.

5. SARAN

Penelitian ini memiliki beberapa keterbatasan yang perlu diperhatikan. Pertama, data yang digunakan sebagian besar berasal dari sumber sekunder. Penelitian lanjutan sebaiknya menggunakan data primer melalui wawancara langsung dengan pihak BPJS Kesehatan. Kedua, penelitian ini fokus pada satu insiden;analisis tambahan terhadap kasus-kasus lain akan memberikan perspektif yang lebih komprehensif. Selain itu, menggunakan metode analisis tambahan seperti analisis forensik digital dapat memperkaya hasil penelitian. Akhirnya, evaluasi jangka panjang dan pendekatan multidisiplin akan memberikan wawasan yang lebih mendalam dan holistik.

DAFTAR PUSTAKA

[1] U. S. D. of Commerce and S. Wilbur L. Ross, Jr., “Control Baselines for Information Systems and Organizations,” NIST Spec. Publ. 800-53B, no. 800–53B, 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf

[2] M. Lubis, C. Wardana, and A. Widjajarto, “The Development of Information System Security Operation Centre (SOC): Case Study of Auto Repair Company,” 6th Int. Conf. Interact. Digit. Media, ICIDM 2020,no. December 2020, 2020, doi: 10.1109/ICIDM51048.2020.9339678.

[3] R. R. Putra, “ANALISIS MANAJEMEN RISIKO TI PADA KEAMANAN DATA E - LEARNING DAN ASET IT MENGGUNAKAN NIST SP 800 – 30 Revisi 1,” JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 6, no. 1, pp. 96–105, 2019, doi: 10.35957/jatisi.v6i1.154.

[4] M. F. Safitra, M. Lubis, and M. T. Kurniawan, “Cyber Resilience: Research Opportunities,” ACM Int. Conf. Proceeding Ser., pp. 99–104, 2023, doi: 10.1145/3592307.3592323.

[5] A. Hidayat and A. A. Hendriadi, “Penanggulangan Bencana Teknologi Informasi Di Data Center Perusahaan Dengan Metoda Disaster Recovery Plan (DRP),” Syntax, vol. Vol 1, No, no. 1, pp. 7–17, 2012.

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

[6] R. Vishwakarma and A. K. Jain, "A survey of DDoS attacking techniques and defence mechanisms in the IoT network," Telecommun. Syst., vol. 73, no. 1, pp. 3–25, 2020, doi: 10.1007/s11235-019-00599-z.

[7] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Qjarterly Special Issue Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness1," Source MIS Q., vol. 34, no. 3, p. 39, 2010.