Journal Health Care Media

Volume 8 No 2 Oktober 2024
ISSN : 2089-4228
http://stikeswch-malang.e-journal.id

KEAMANAN SIBER DALAM *PICTURE ARCHIVING COMMUNICATION SYSTEM* (PACS) PADA SISTEM INFORMASI RADIOLOGI

Kus Endah Aryati[1)], Sri Sugiarti[2)], Riski Setiya Afandi[3)], Roni Prisyanto[4)]

[1,2,3,4]Program Studi D3 Radiodiagnostik dan Radioterapi
Institut Teknologi Kesehatan Malang Widya Cipta Husada
email : srisugiarti2717@gmail.com

Abstrak

Picture Archiving Communication System (PACS) merupakan sistem penting dalam sistem informasi radiologi yang menyimpan dan mengelola gambar medis digital. Keamanan siber PACS menjadi krusial karena menyimpan data sensitif pasien dan rentan terhadap serangan siber. Penelitian ini bertujuan untuk membahas tentang *cybersecurity* dalam PACS pada sistem informasi radiologi. Metode yang digunakan dalam penelitian ini adalah tinjauan pustaka dengan mengumpulkan data dari berbagai sumber seperti jurnal ilmiah, artikel, dan situs web terpercaya. Hasil tinjauan pustaka menunjukkan bahwa terdapat berbagai ancaman siber yang dapat menyerang PACS, seperti *malware*, *ransomware*, dan serangan *phishing*. Dampak dari serangan siber pada PACS dapat mengakibatkan kebocoran data pasien, gangguan layanan, dan kerusakan data. Pembahasan dalam karya tulis ini meliputi: Definisi dan arsitektur PACS Ancaman siber yang dihadapi PACS, dampak serangan siber pada PACS, upaya pencegahan dan penanggulangan serangan siber pada PACS. *Cybersecurity* dalam PACS merupakan aspek penting yang perlu diperhatikan untuk melindungi data pasien dan menjaga kelancaran layanan radiologi. Penerapan kontrol keamanan yang memadai dan edukasi pengguna yang berkelanjutan menjadi kunci utama dalam menjaga keamanan PACS.

Kata Kunci: PACS, *Cybersecurity*, Radiologi.

Abstract

Picture Archiving Communication System (PACS) is an important system in a radiology information system that stores and manages digital medical images. PACS cybersecurity is crucial because it stores sensitive patient data and is vulnerable to cyber attacks. This research aims to discuss cybersecurity in PACS in radiology information systems. The method used in this research is a literature review by collecting data from various sources such as scientific journals, articles and trusted websites. The results of the literature review show that there are various cyber threats that can attack PACS, such as malware, ransomware, and phishing attacks. The impact of cyberattacks on PACS can result in patient data leaks, service disruptions, and data corruption. The discussion in this paper includes: Definition and architecture of PACS Cyber threats faced by PACS, the impact of cyber attacks on PACS, efforts to prevent and overcome cyber attacks on PACS. Cybersecurity in PACS is an important aspect that needs to be considered to protect patient data and maintain the smooth running of radiology services. Implementing adequate security controls and ongoing user education are the main keys to maintaining PACS security.

Keywords:* PACS, *Cybersecurity, Radiology.

PENDAHULUAN

Teknologi informasi memiliki dampak positif dalam bidang pengobatan modern, termasuk penggunaan PACS dan pembacaan *softcopy*. Internet memungkinkan komunikasi yang cepat, efisien, dan ekonomis dalam informasi klinis (1).

Cybersecurity adalah aturan keamanan untuk melawan kejahatan siber seperti. *Ransomware* adalah perangkat lunak yang mengenkripsi file dan menuntut pembayaran tebusan. Layanan kesehatan adalah salah satu sektor yang paling terpengaruh oleh *ransomware*, dengan 15% dari semua *ransomware* terdeteksi secara global dalam perawatan kesehatan institusi pada tahun 2017 dan 50% dari semua insiden serangan siber di rumah sakit pada tahun 2017 terkait dengan *ransomware* (2).

Pembuat kebijakan di seluruh dunia telah mengakui bahwa institusi perawatan kesehatan membutuhkan perlindungan dari ancaman dunia maya. US *national infrastructure protection plan* menyediakan rencana khusus keamanan data pada sektor kesehatan dan masyarakat dan Uni Eropa telah membentuk Badan Uni Eropa Untuk Keamanan Jaringan Dan Informasi (ENISA), yang diantara topik lainnya menerbitkan studi yang berkaitan dengan masalah *cybersecurity* di sektor kesehatan. Di Jerman, rumah sakit besar harus menerapkan persyaratan undang-undang keamanan teknologi informasi yang ditujukan untuk penyedia infrastruktur penting pada Juli 2019 (3).

Ancaman *cybersecurity* yang dihadapi oleh rumah sakit telah mencapai kualitas baru. Serangan siber sekarang menjadi semakin ditargetkan pada sektor kesehatan, yang tampaknya dilihat sebagai target yang menarik oleh kelompok-kelompok di balik ancaman ini. Di Indonesia, jutaan data di sektor kesehatan sudah diretas, termasuk informasi pasien, rekam medis, dan gambar medis pemeriksaan. Peretasan tersebut bukan hanya untuk mencuri data tetapi juga membekukan sistem dengan mengenkripsi semua data dan menyebarkan virus (4). Studi oleh Gillum pada tahun 2019 di Amerika Serikat menunjukkan bahwa kebocoran data gambar pencitraan medis adalah masalah yang nyata, dengan ratusan sistem PACS di seluruh dunia ditemukan terkena akses dari internet (5).

Industri kesehatan semakin bergantung pada teknologi, termasuk penyimpanan dan transmisi data digital. Tren ini, dikombinasikan dengan sifat sensitif data kesehatan, menjadikan industri kesehatan sebagai target utama bagi penjahat siber. Serangan siber terhadap organisasi kesehatan dapat memiliki konsekuensi yang serius, termasuk pencurian data pasien, gangguan layanan, dan bahkan membahayakan kesehatan pasien (6).

Sistem Arsip dan Komunikasi Gambar (PACS) memainkan peran penting dalam menyimpan, mengambil, dan mendistribusikan gambar medis. Gambar medis ini sangat sensitif dan mengandung informasi pribadi pasien yang berharga. Oleh karena itu, PACS rentan terhadap berbagai ancaman keamanan siber. Serangan siber terhadap PACS dapat berdampak serius pada organisasi kesehatan, termasuk pencurian data pasien, gangguan layanan, kerusakan gambar medis, kerugian finansial (7,8).

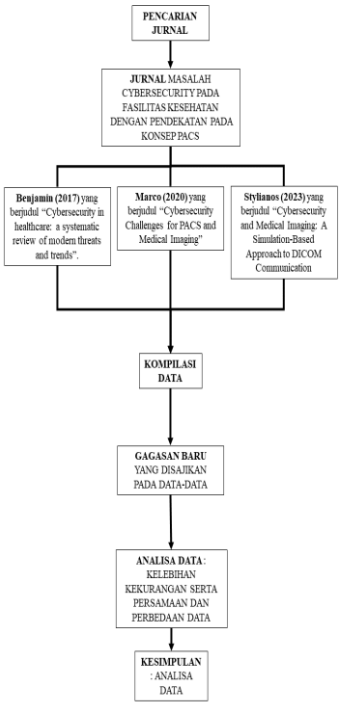
Standar *Digital Imaging and Communications in Medicine* (DICOM) telah merevolusi cara gambar medis disimpan, ditransmisikan, dan dibagikan. Namun, meskipun memiliki banyak manfaat, implementasi dan penggunaan protokol DICOM seringkali kurang dipahami, yang dapat menyebabkan kerentanan dalam ekosistem perawatan kesehatan (9,10).

METODE PENELITIAN

Penelitian ini merupakan penelitian kualitatif dengan pendekatan studi literatur. Peneliti melakukan pencarian jurnal, artikel, buku yang berhubungan dengan topik yang akan diangkat yaitu *Cybersecurity* Dalam *Picture Archiving*

Communication System (PACS) Pada Sistem Informasi Radiologi.

Metode pengambilan data menggunakan *literature review* yang dimulai dengan mencari jurnal yang berisi tentang *Cybersecurity* Dalam *Picture Archiving Communication System* (PACS) Pada Sistem Informasi Radiologi atau konsep yang mendekati *cybersecurity* dalam PACS.



Gambar 1. Kerangka Operasional

Studi literatur dimulai dengan menggunakan kata kunci di basis data yang berisi jurnal berbahasa Indonesia dan Inggris. Basis data yang digunakan adalah Google Schoolar dan DOI.org. Pencarian dibatasi untuk jurnal-jurnal yang dipublikasikan pada tahun 2013-2023 menggunakan kata kunci "*Cybersecurity*, PACS".

Langkah-langkah pengumpulan data yang penulis lakukan adalah membagi dengan beberapa kriteria kelayakan dan kriteria inklusi yang penulis gunakan untuk mereduksi sumber literatur.

HASIL DAN PEMBAHASAN

Seleksi Jurnal

Pengolahan dan analisis data dilakukan dengan cara mengkompilasi, mensintesa, mengkritisi dan menyimpulkan dari hasil penelitian sebelumnya. Peneliti mengumpulkan data dengan cara melakukan pengkajian pustaka terkait yang telah dilakukan pencarian dan pereduksian berdasarkan beberapa kriteria sehingga didapatkan data yang relevan. Setelah didapatkan data yang relevan peneliti kemudian mengumpulkan jurnal dan membuat ringkasan berdasarkan tipe artikel, nama peneliti, tahun terbit, judul, tujuan penelitian, kata kunci, metode penelitian, hasil penelitian atau temuan. Ringkasan jurnal penelitian tersebut dimasukkan kedalam tabel dan diurutkan sesuai alfabet dan tahun penelitian jurnal.

Ringkasan jurnal tersebut kemudian dilakukan analisis terhadap isi yang terdapat dalam tujuan penelitian dan hasil/temuan penellitian. Benjamin, dkk (2017) yang berjudul "*Cybersecurity in healthcare: a systematic review of modern threats and trends*"; Marco, dkk (2020) yang berjudul "*Cybersecurity Challenges for PACS and Medical Imaging*"; Stylianos, dkk (2023) yang berjudul "*Cybersecurity and Medical Imaging: A Simulation-Based Approach to DICOM Communication*". Kriteria kedua adalah kriteria kelengkapan jurnal. Artikel yang dipilih merupakan artikel yang telah terakreditasi secara internasional yang didalamnya memuat judul, nama pengarang, tahun terbit, abstrak, kata kunci, pendahuluan, metode, hasil, pembahasan, kesimpulan, saran, dan daftar pustaka.

Pemaparan Jurnal

Literature Pertama Benjamin, Dkk (2017) Yang Berjudul "*Cybersecurity In Healthcare: A Systematic Review Of Modern Threats And Trends*".

Jurnal "*Cybersecurity Challenges for PACS and Medical Imaging*" yang diterbitkan oleh *Texas State University*

dan dipublikasikan oleh IOS *Press* melalui DOI.org pada kategori *Technology And Healthcare* pada tahun 2017, volume 25 nomor 1 halaman 1-10 dengan nomor ISSN: 09287329-18787401 dengan akreditasi Q3 dalam bidang Biokimia dan Genetika yang membahas tentang kerentanan sistem PACS (*Picture Archiving and Communication System*) dan pencitraan medis terhadap serangan siber.

Isi dari penelitian ini meliputi akses tidak sah, *malware*, penyadapan data, dan kehilangan data. Solusinya mencakup kontrol akses kuat, *antivirus*/*anti-malware*, enkripsi data, dan cadangan data. Jurnal ini menggunakan metode tinjauan literatur untuk membahas tantangan keamanan siber PACS dan pencitraan medis.

Hasil dari penelitian jurnal ini adalah industri kesehatan tertinggal dalam hal keamanan dibandingkan industri lain. Serangan siber terhadap organisasi kesehatan meningkat dalam jumlah dan kompleksitas. *Ransomware* sendiri adalah jenis serangan siber yang paling umum di sektor kesehatan. Hal ini juga dikarenakan kurangnya kesadaran dan pelatihan staf yang merupakan faktor utama yang berkontribusi pada kerentanan siber. Dengan menetapkan tugas dan tanggung jawab yang jelas terkait keamanan siber, membangun prosedur yang jelas untuk *upgrade software* dan penanganan kebocoran data, menerapkan teknologi seperti VLAN, *deauthentication*, dan komputasi *cloud*, memberikan pelatihan kepada staf untuk meningkatkan kesadaran dan kemampuan mereka dalam mendeteksi dan mencegah serangan siber yang dapat mengurangi dampak tersebut.

Literature Kedua Marco, Dkk (2020) Yang Berjudul "*Cybersecurity Challenges For PACS And Medical Imaging*".

Jurnal "*Cybersecurity Challenges for PACS and Medical Imaging*" yang diterbitkan oleh *Germany* OFFIS *Institute* dan dipublikasikan oleh *Elsivier Inc* melalui DOI.org pada kategori *Health Information Technology* pada tahun 2020, volume 27 nomor 8 halaman 1126-1139 dengan nomor ISSN: 10766332 dengan akreditasi Q2 di bidang Radiologi, Nuklir dan Kedokteran yang membahas kerentanan sistem PACS (*Picture Archiving and Communication System*) dan pencitraan medis terkini terhadap serangan siber

Isi dari penelitian meliputi import data terkontaminasi *malware*, pelanggaran jaringan, *malware* dalam gambar DICOM, manipulasi gambar berbahaya, dan infiltrasi pesan HL7. Solusinya mencakup edukasi pengguna, segmentasi jaringan, pemindaian gambar DICOM, verifikasi integritas gambar, dan enkripsi pesan HL7.

Metode penelitiannya adalah studi kasus yang menunjukkan contoh eksploitasi ancaman terhadap sistem PACS dan pencitraan medis. Jurnal ini relevan untuk meningkatkan keamanan sistem PACS dan pencitraan medis.

Hasil dari penelitian jurnal ini adalah sistem PACS dan pencitraan medis rentan terhadap berbagai jenis serangan siber, seperti pencurian data, enkripsi data, gangguan layanan, dan kerusakan fisik. Serangan siber dapat mengakibatkan konsekuensi serius, seperti hilangnya data pasien, gangguan layanan kesehatan, dan kerusakan peralatan medis.

Literature Ketiga Stylianos, Dkk (2023) Yang Berjudul "*Cybersecurity And Medical Imaging: A Simulation-Based Approach To DICOM Communication*".

Jurnal "*Cybersecurity and Medical Imaging: A Simulation-Based Approach to DICOM Communication*" yang diterbitkan oleh *University Of Brigthon* dan dipublikasikan oleh *Switzerland* MDPI melalui DOI.org pada kategori *Health Sciences* pada tahun 2023, volume 13 nomor 18 halaman 2076-3417 dengan nomor ISSN : 10072 dengan akreditasi Q3 pada Pengaplikasian Sains/Ilmu Pengetahuan yang membahas tentang pentingnya keamanan siber dalam pencitraan medis

dan mengusulkan pendekatan berbasis simulasi untuk menguji dan meningkatkan keamanan komunikasi DICOM.

Isi dari penelitian ini adalah terdapat kejahatan siber dalam pencitraan medis meliputi akses tidak sah, *malware*, penyadapan data, dan manipulasi gambar. Pendekatan berbasis simulasi menggunakan simulator DICOM untuk mensimulasikan berbagai skenario komunikasi dan menguji kerentanan sistem.

Metode penelitiannya deskriptif dan presentasi hasil simulasi menunjukkan efektivitas pendekatan ini. Pendekatan ini bermanfaat karena memungkinkan pengujian yang aman, berbagai skenario, dan pengembangan solusi keamanan yang lebih cepat.

Keamanan siber dalam pencitraan medis sangat penting dan pendekatan berbasis simulasi ini dapat membantu meningkatkan keamanan komunikasi DICOM dan melindungi data pasien. Hasil dari penelitian jurnal ini adalah terkait implementasi dan penerapan protokol DICOM sering kali tidak sempurna, yang menyebabkan kerentanan dalam ekosistem kesehatan simulasi komunikasi DICOM dapat membantu menguji dan meningkatkan keamanan protokol. Simulasi dapat memberikan wawasan tentang aspek praktis komunikasi DICOM dan integrasi PACS.

Persamaan Masing –Masing Jurnal

Kesamaan Topik Utama

Ketiga jurnal memiliki kesamaan dalam topik utama, yaitu:

- ***Cybersecurity* dalam bidang kesehatan**: Jurnal-jurnal ini membahas tentang ancaman dan kerentanan keamanan siber yang dihadapi oleh sistem dan data kesehatan, termasuk pencitraan medis.
- **Pencitraan medis**: Jurnal-jurnal ini fokus pada keamanan sistem PACS (*Picture Archiving and Communication Systems*) dan DICOM (*Digital Imaging and Communications in Medicine*) yang digunakan untuk menyimpan, mengelola, dan membagikan gambar medis.

Kesamaan Temuan Utama

Meskipun memiliki fokus dan metodologi yang berbeda, ketiga jurnal ini menunjukkan beberapa temuan utama yang serupa:

- **Kerentanan sistem pencitraan medis**: Sistem PACS dan DICOM rentan terhadap berbagai serangan siber, seperti *malware*, *ransomware*, dan *phishing*.
- **Dampak serangan siber**: Serangan siber dapat menyebabkan berbagai konsekuensi serius, seperti hilangnya data pasien, gangguan layanan, dan kerusakan reputasi.
- **Pentingnya *cybersecurity***: Diperlukan langkah-langkah keamanan siber yang tepat untuk melindungi sistem pencitraan medis dan data pasien.

Ketiga jurnal ini memberikan informasi yang *valuable* tentang *cybersecurity* dalam pencitraan medis. Berikut adalah beberapa poin penting yang dapat disimpulkan dari jurnal-jurnal tersebut:

- Ancaman siber terus berkembang: Para profesional IT dan medis harus selalu mengikuti perkembangan terbaru tentang ancaman siber dan cara mengatasinya.
- Pentingnya edukasi dan pelatihan: Staf medis dan IT harus dilatih tentang kesadaran keamanan siber untuk dapat mengidentifikasi dan merespon potensi serangan.
- Implementasi teknologi keamanan: Solusi teknologi seperti autentikasi multi-faktor, enkripsi data, dan *firewall* harus diterapkan untuk melindungi sistem dan data.
- Pendekatan proaktif: Penting untuk memiliki strategi *cybersecurity* yang proaktif untuk mencegah dan

mendeteksi serangan siber sebelum terjadi.

Perbedaan Masing –Masing Jurnal

Terdapat beberapa perbedaan signifikan dalam fokus, metodologi, dan rekomendasi dari ketiga jurnal tersebut.

Perbedaan Fokus:

Jurnal pertama: "*Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*".

Jurnal ini memberikan tinjauan komprehensif tentang *cybersecurity* di seluruh bidang kesehatan. Jurnal ini membahas berbagai jenis ancaman siber yang dihadapi oleh organisasi kesehatan, termasuk serangan *malware*, *ransomware*, dan *phishing*. Jurnal ini juga membahas berbagai solusi keamanan siber yang dapat diterapkan untuk melindungi data dan sistem kesehatan.

Jurnal kedua: "*Cybersecurity Challenges for PACS and Medical Imaging*"

Jurnal ini fokus pada *cybersecurity* PACS (*Picture Archiving and Communication Systems*) dan pencitraan medis. Jurnal ini membahas berbagai kerentanan keamanan yang ada dalam sistem PACS dan DICOM (*Digital Imaging and Communications in Medicine*). Jurnal ini juga membahas lima skenario serangan siber yang umum terjadi pada sistem PACS dan solusi pencegahan/mitigasi untuk setiap skenario.

Jurnal ketiga: "*Cybersecurity and Medical Imaging: A Simulation-Based Approach to DICOM Communication*"

Jurnal ini fokus pada simulasi komunikasi DICOM dan bagaimana simulasi dapat digunakan untuk meningkatkan keamanan komunikasi DICOM. Jurnal ini menjelaskan bagaimana simulasi dapat digunakan untuk menguji dan mengevaluasi solusi keamanan siber untuk komunikasi DICOM. Jurnal ini juga memberikan contoh simulasi komunikasi DICOM yang dapat digunakan untuk meningkatkan keamanan sistem pencitraan medis.

Perbedaan Metodologi:

Jurnal pertama:

Jurnal ini menggunakan metodologi tinjauan sistematis untuk menganalisis 31 artikel ilmiah tentang *cybersecurity* di bidang kesehatan. Jurnal ini mengidentifikasi berbagai jenis ancaman siber, solusi keamanan siber, dan *best practices* untuk *cybersecurity* di bidang kesehatan.

Jurnal kedua:

Jurnal ini menggunakan metodologi studi kasus untuk membahas lima skenario serangan siber yang umum terjadi pada sistem PACS. Jurnal ini menganalisis kerentanan keamanan yang dieksploitasi dalam setiap skenario dan memberikan solusi pencegahan/mitigasi untuk setiap skenario.

Jurnal ketiga:

Jurnal ini menggunakan metodologi simulasi untuk menguji dan mengevaluasi solusi keamanan siber untuk komunikasi DICOM. Jurnal ini menjelaskan bagaimana simulasi dapat digunakan untuk mengidentifikasi kerentanan keamanan dalam komunikasi DICOM dan bagaimana simulasi dapat digunakan untuk meningkatkan keamanan sistem pencitraan medis.

Perbedaan Rekomendasi:

Jurnal pertama:

Jurnal ini merekomendasikan agar organisasi kesehatan menerapkan berbagai solusi keamanan siber untuk melindungi data dan sistem mereka, seperti autentikasi multi-faktor, enkripsi data, dan pelatihan kesadaran keamanan bagi staf. Jurnal ini juga merekomendasikan agar organisasi kesehatan mengikuti perkembangan terbaru tentang ancaman siber dan solusi keamanan siber.

Jurnal kedua:

Jurnal ini merekomendasikan agar organisasi kesehatan menerapkan

VARIABEL MITIGASI	PENGGUNA/PENGEMBANG(U/V)	CIA TRIAD	REFERENSI
Tindakan Mitigasi Secara Fisik			
Menyimpan *server* file di area aman dari akses tidak sah dan ancaman lingkungan.	U	CIA	(2)
Memasang kamera keamanan di ruang *server.*	U	CIA	
Tindakan Mitigasi Secara Teknis			
Melakukan pencadangan rutin.	U/V	A	
Menggunakan *firewall* dan segmentasi jaringan untuk mencegah intrusi jaringan.	U	CIA	
Menonaktifkan jaringan fisik dan *port* USB yang tidak digunakan.	U	CIA	
Menggunakan *white list* untuk aplikasi yang diizinkan.	U/V	CIA	
Menerapkan otentikasi pengguna dan menentukan serta menegakkan hak akses.	U/V	C	
Menginstal pembaruan dan patch secara teratur..	U/V	CIA	
Menginstal perangkat lunak *antivirus.*	U/V	CIA	
Menggunakan transmisi jaringan terenkripsi.	U/V	CI	
Menggunakan penyimpanan dokumen terenkripsi.	U/V	CI	(1,2,4)
Menyebarkan jejak audit.	U/V	CI	
Menyebarkan alat pemantauan jaringan dan deteksi intrusi.	U	CIA	
Tentukan dan terapkan kebijakan perangkat mobile.	U	CIA	
Terapkan alat penemuan inventaris aset otomatis.	U	CIA	
Pastikan konfigurasi sistem diperbarui agar tetap aman dari waktu ke waktu.	U/V	CIA	
Menyebarkan infrastruktur kunci publik yang menyediakan sertifikat klien.	U/V	CI	
Menerapkan administrasi jarak jauh untuk dilakukan melalui saluran aman.	U	C	
Tindakan Mitigasi Secara Organisasi			
Mengadakan pelatihan pengguna secara rutin dan simulasikan insiden keamanan siber.	U	CIA	
Mengadakan pengujian penetrasi secara teratur.	U	CIA	(3)
Mendefinisikan dan menerapkan prosedur manajemen insiden.	U	CIA	
Tindakan Mitigasi Secara Kesehatan			
Menggunakan gambar yang tidak de-identifikasi jika memungkinkan.	U/V	C	
Menerapkan keamanan transportasi DICOM atau enkripsi selektif *header* DICOM.	U/V	C	(1)
Menyimpan file DICOM dalam format terenkripsi.	U/V	C	
Menggunakan tanda tangan digital atau teknik *watermarking* untuk melindungi integritas gambar.	U/V	I	(3)
Membersihkan pembukaan file saat menangani file DICOM.	U/V	CIA	(2)

berbagai langkah-langkah keamanan untuk melindungi sistem PACS dan DICOM mereka, seperti segmentasi jaringan, kontrol akses, dan monitoring keamanan. Jurnal ini juga merekomendasikan agar organisasi kesehatan melakukan pelatihan kesadaran keamanan bagi staf yang bekerja dengan sistem PACS dan DICOM.

Tabel 1. Pedoman Mitigasi

Jurnal ketiga:

Jurnal ini merekomendasikan agar organisasi kesehatan menggunakan simulasi untuk menguji dan mengevaluasi solusi keamanan siber untuk komunikasi DICOM. Jurnal ini juga merekomendasikan agar organisasi kesehatan menggunakan simulasi untuk melatih staf tentang *cybersecurity* dalam pencitraan medis.

Metode CIA *Triad* Sebagai Bentuk Solusi Praktik Terbaik

CIA *Triad* adalah kerangka keamanan yang mapan dan digunakan untuk memandu pengembangan dan implementasi kebijakan dan prosedur

keamanan untuk sistem informasi.

- *Confidentiality*: Prinsip ini memastikan bahwa hanya individu atau sistem yang berwenang yang dapat mengakses dan melihat informasi sensitif. Hal ini dapat melibatkan langkah-langkah seperti kontrol akses, enkripsi, dan klasifikasi data.
- *Integrity*: Prinsip ini memastikan bahwa informasi tetap akurat dan lengkap, dan tidak dimodifikasi tanpa izin atau secara tidak sengaja. Hal ini dapat dicapai melalui validasi data, checksum, dan audit trail.
- *Availability*: Prinsip ini memastikan bahwa pengguna yang berwenang memiliki akses ke informasi dan sistem saat mereka membutuhkannya. Hal ini melibatkan memastikan waktu aktif sistem, redundansi, dan praktik pemulihan bencana.

CIA *Triad* membantu organisasi untuk:

- Mengidentifikasi kerentanan dalam sistem mereka dengan mempertimbangkan bagaimana setiap prinsip dapat disusupi.
- Mengembangkan kontrol keamanan untuk mengatasi kerentanan ini dan mengurangi risiko.
- Mengevaluasi efektivitas postur keamanan mereka dengan menilai seberapa baik kontrol mereka melindungi kerahasiaan, integritas, dan ketersediaan informasi.

Berdasarkan hasil penelitian jurnal sebelumnya, pokok masalah yang paling menonjol adalah kurang nya solusi praktif pada praktik terbaiknya. Oleh karena itu peneliti membuat tabel pedoman komprehensif secara praktis sebagai bentuk pembaharuan penelitian berdasarkan penelitian dan tinjaun pustaka sebelumnya sebagai berikut :

Tabel ini merangkum langkah-langkah keamanan siber yang berlaku untuk PACS (*Picture Archiving and Communication System*) dan pencitraan medis. Langkah-langkah ini dikategorikan berdasarkan siapa yang dapat menerapkannya dan bagaimana langkah tersebut berkontribusi pada keamanan data.

Kerangka ini terdiri dari:

Berikut adalah rincian informasi tabel:

- Pengguna vs. *Vendor*: Kolom ini menunjukkan apakah pengguna (misalnya rumah sakit) dapat menerapkan langkah tersebut secara langsung atau memerlukan dukungan *vendor*.
- Triad CIA: Kolom ini menunjukkan bagaimana langkah tersebut berkontribusi pada tiga tujuan inti keamanan informasi: Kerahasiaan (menjaga kerahasiaan data), Integritas (memastikan keakuratan data), dan Ketersediaan (memastikan aksesibilitas data). Langkah-langkah yang berkontribusi secara tidak langsung terhadap tujuan ini, seperti pelatihan pengguna.
- Referensi: Kolom ini mencantumkan sumber untuk informasi lebih lanjut tentang setiap langkah.

Terdapat poin poin penting dalam bagian ini

- Beberapa langkah memerlukan instalasi perangkat lunak tambahan atau konfigurasi sistem operasi. Dukungan *vendor* mungkin diperlukan, terutama untuk perangkat medis karena proses sertifikasi.
- *Vendor* memainkan peran penting dalam menerapkan langkah-langkah seperti otentikasi pengguna, tanda tangan digital, dan enkripsi dalam perangkat lunak perangkat.
- Infrastruktur kunci publik untuk manajemen sertifikat otomatis memerlukan kolaborasi antara organisasi pengguna (mengelola Infrastruktur kunci publik) dan *vendor* (menerapkan dukungan infrastruktur kunci publik dalam produk).

- Keamanan transportasi dapat diterapkan dengan atau tanpa dukungan *vendor*, tergantung pada metode yang digunakan (*gateway* vs. implementasi produk langsung).

Secara keseluruhan, bagian ini menekankan bahwa berbagai langkah keamanan tersedia untuk jaringan PACS, dan banyak yang dapat diterapkan dengan teknologi saat ini. Namun, kolaborasi antara pengguna dan *vendor* sangat penting untuk keamanan yang menyeluruh.

SIMPULAN DAN SARAN

Penelitian ini menyimpulkan bahwa *Cybersecurity* merupakan aspek penting dalam pengelolaan sistem pencitraan medis di rumah sakit, khususnya instalasi radiologi. Rumah sakit perlu memahami berbagai ancaman siber, menerapkan solusi dan praktik terbaik, serta mengikuti perkembangan di bidang ini untuk melindungi data medis pasien dan memastikan kelancaran operasional. Standar yang perlu diperhatikan dalam cybersecurity pada PACS meliputi De-identifikasi gambar, Enkrispi data *header* pada DICOM, Penggunaan Tanda Tangan Digital dan *Watermarking*, dan Membersihkan *File* Pada Saat Pembukaan DICOM.

Penerapan *cybersecurity* juga harus diimbangi dengan tindakan mitigasi secara institusi kesehatan dengan membuat pedoman praktis terkait tindakan mitigasi pada tabel CIA TRIAD. Panduan praktis yang peneliti buat diharapkan dapat menjadi wawasan sebagai standar penanganan *cybersecurity* dan pedoman teknis untuk instalasi radiologi.

UCAPAN TERIMA KASIH

Penelitian ini dibantu dengan wawancara, studi kasus dan tinjauan praktik di RSUD Bangil, RSUD dr,Soedarsono Pasuruan, RSUD dr.Soetomo Surabaya dan RS Khusus Bedah Hasta Husada Malang.

REFERENSI

1. Eichelberg, M., Kämmerer, M. & Kleber, K. (2020). *Cybersecurity in PACS and Medical Imaging: an Overview. Journal of Digital Imaging,* pp. 1527-1542.

2. EUROPOL (2018). *Internet Organised Crime Threat Assessment (Iocta). Europa: European Union Agency for Law Enforcement Cooperation*.

3. Agency., ENISA., 2016. *Smart hospitals: security and resilience for smart health service and infrastructure. LU: Publication Office*

4. Aviat (2022). Jutaan Data Sektor Kesehatan Jadi Incaran Hacker, Bagaimana Cara Memperkuat Keamanan Data Kesehatan RS?. [Online] https://aviat.id/jutaan-data-sektor-kesehatan-jadi-incaran-hacker-bagaimana-cara-memperkuat-keamanan-data-kesehatan-rs/ [Diakses 21 Januari 2024].

5. Jack ,Gillum (2019). *Millions of Americans' Medical Images and Data Are Available on the Internet. Anyone Can Take a Peek.. [Online]* https://www.propublica.org/article/millions-of-americans-medical-images-and-data-are-available-on-the-internet

6. Benjamin (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends. Journal of Nursing Informatics*, 21(2), 204-216.

7. Marco (2020). *Cybersecurity challenges for PACS and medical imaging. Computers in Biology and Medicine*, 125, 104011.

8. Georges El Hajal, 2019. *Designing and validating a cost effective safe*

Volume 8 No 2 Oktober 2024
ISSN : 2089-4228
http://stikeswch-malang.e-journal.id

network: application to a PACS system. Tripoli, Lebanon, IEEE.

9. Stylianos Karagiannis (2023). *Cybersecurity and Medical Imaging: A Simulation-Based Approach to DICOM Communication. Applied Sciences,* 13(18), 10072.

10. Haj, A. A., 2015. Providing Integrity, Authenticity, and Confidentiality for Header and Pixel Data of DICOM Images. *Journal of Digital Imaging,* 28(2), pp. 179-187