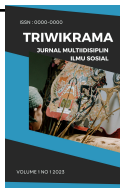
Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9, Number 4, 2025
E-ISSN: 2988-1986
Open Access:



Analisis Keamanan Siber dalam Infrastruktur Kritis: Studi Kasus Serangan Ransomware terhadap Sektor Energi Meksiko Sebagai Pembelajaran Bagi Pertahanan Indonesia

Laagimo Kasih Pakambanan
Program Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin

ARTICLE INFO

Article history:
Received Juni, 2025
Revised Juni, 2025
Accepted Juni, 2025
Available online Juni , 2025

agipakambanan@gmail.com

A B S T R A K

Penelitian ini mengkaji serangan ransomware tahun 2019 terhadap Petróleos Mexicanos (Pemex), perusahaan minyak negara Meksiko, sebagai studi kasus untuk mengidentifikasi kerentanan infrastruktur energi dan menarik pembelajaran strategis bagi Indonesia. Dengan pendekatan kualitatif dan analisis literatur, penelitian ini menelaah penyebab, dampak, dan strategi respons serangan, serta masalah utama seperti sistem teknolgi informasi yang usang dan perencanaan respons insiden yang lemah. Temuan menunjukkan bahwa serangan ransomware memiliki implikasi luas terhadap keselamatan publik, stabilitas ekonomi, dan keamanan nasional. Kasus Pemex menegaskan urgensi penguatan keamanan siber bagi Indonesia yang sektor energinya semakin digital. Rekomendasi mencakup investasi pada infrastruktur TI modern, peningkatan kesadaran karyawan, segmentasi jaringan, dan kolaborasi publik-swasta guna memperkuat ketahanan terhadap ancaman siber dan menjaga stabilitas energi nasional.

Kata kunci: Ransomware, Pemex, Keamanan siber, Infrastruktur kritis, Sektor energi, Indonesia, Serangan siber, Respons insiden

A B S T R A C T

This study examines the 2019 ransomware attack on Mexico's state-owned oil company, Petróleos Mexicanos (Pemex), as a case study to identify vulnerabilities in critical energy infrastructure and draw strategic insights for Indonesia. Using a qualitative approach and literature analysis, it explores the causes, impacts, and response strategies of the attack, highlighting key issues such as outdated IT systems and weak incident response planning. Findings reveal that ransomware poses broad threats to public safety, economic stability, and national security. The Pemex case underscores the urgent need for strengthened cybersecurity in Indonesia's increasingly digital energy sector. Recommendations include investing in modern IT infrastructure, enhancing employee awareness, implementing network segmentation, and promoting public-private collaboration to bolster resilience against cyber threats and ensure energy infrastructure stability.

Keywords: *Ransomware, Pemex, Cybersecurity, Critical infrastructure, Energy sector, Indonesia, Cyberattack, Incident response*

*Corresponding author
E-mail addresses: agipakambanan@gmail.com

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9 No 4, 2025
E-ISSN: 2988-1986
Open Access:

1. PENDAHULUAN

Meningkatnya digitalisasi infrastruktur kritis telah membawa kemajuan signifikan dalam efisiensi dan pengendalian operasional. Namun, digitalisasi infrastruktur kritis juga telah mengekspos sistem tersebut terhadap serangkaian ancaman dunia maya yang terus bertambah, khususnya serangan ransomware. Ransomware, sejenis perangkat lunak berbahaya yang dirancang untuk memblokir akses ke sistem komputer atau data hingga tebusan dibayarkan, telah muncul sebagai salah satu ancaman dunia maya yang paling luas dan merusak dalam beberapa tahun terakhir.[1] Sektor energi, sebagai landasan keamanan nasional dan stabilitas ekonomi, telah menjadi target utama serangan ransomware karena perannya yang penting dalam menopang masyarakat modern. Serangan ransomware tahun 2019 terhadap Petróleos Mexicanos (Pemex), perusahaan minyak milik negara Meksiko, menjadi pengingat yang jelas tentang kerentanan yang melekat pada infrastruktur penting dan konsekuensi yang menghancurkan dari tindakan keamanan dunia maya yang tidak memadai.[2]

Pada tanggal 10 November 2019, Pemex menjadi korban serangan ransomware yang mengganggu operasinya dan memaksa perusahaan untuk mematikan komputer di seluruh fasilitasnya. Serangan tersebut dikaitkan dengan kelompok ransomware "DoppelPaymer", yang mengenkripsi berkas milik Pemex dan meminta tebusan sekitar $5 juta dalam bentuk Bitcoin. Para penyerang mengancam akan merilis data sensitif jika tuntutan mereka tidak dipenuhi. Meskipun Pemex tidak membayar tebusan, serangan tersebut menyebabkan gangguan operasional yang signifikan, termasuk keterlambatan dalam pemrosesan penggajian, sistem penagihan, dan fungsi penting lainnya.[3] Ransomware tersebut menyusup ke jaringan Pemex dan mengganggu sistem administratif dan operasional yang penting. Meskipun Pemex mengklaim bahwa hanya 5% komputernya yang terpengaruh, laporan menunjukkan bahwa serangan tersebut berdampak luas pada kemampuan perusahaan untuk memproses pembayaran, mengelola rantai pasokan, dan menjalankan operasi rutin. Karyawan terpaksa kembali ke proses manual, yang menyebabkan inefisiensi dan kemunduran finansial.[4]

---

[1] Philip O'Kane, Sakir Sezer, dan Domhnall Carlin, "Evolution of Ransomware," IET Networks 7, no. 5 (Juni 30, 2018): 321–27, https://doi.org/10.1049/iet-net.2017.0207.

[2] Adriana Barrera, "Ransomware attack at Mexico's Pemex halts work, threatens to cripple computers," Reuters, 2019, https://www.reuters.com/article/technology/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041/.

[3] Bloomberg, "Pemex Faces Payment Problems After Cyber Attack Shut System," Bloomberg, November 12, 2019, https://www.bloomberg.com/news/articles/2019-11-11/pemex-workers-barred-from-computers-after-unexpected-shutdown.

[4] Scott N. Romaniuk dan Mary Manjikian, Routledge Companion to Global Cyber-Security Strategy, Routledge eBooks, 2020, https://doi.org/10.4324/9780429399718.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9, Number 4, 2025
E-ISSN: 2988-1986
Open Access:

Serangan terhadap Pemex bukanlah insiden tunggal, melainkan bagian dari tren serangan ransomware yang lebih luas yang menargetkan infrastruktur penting, khususnya di sektor energi. Para penyerang mengeksploitasi kerentanan dalam sistem teknologi informasi (TI) Pemex, yang menyoroti pentingnya langkah-langkah keamanan siber proaktif dalam mencegah insiden semacam itu. Kasus Pemex juga menggarisbawahi tantangan yang dihadapi oleh perusahaan milik negara dalam mengamankan infrastruktur digital mereka, khususnya dalam menghadapi ancaman siber yang semakin canggih. Penelitian ini mengkaji serangan ransomware Pemex sebagai studi kasus untuk menganalisis implikasi yang lebih luas dari ancaman ransomware pada infrastruktur kritis, dengan fokus khusus pada sektor energi. Dengan membedah metodologi, dampak, dan respons serangan, penelitian ini bertujuan untuk menarik pelajaran berharga bagi Indonesia, negara dengan sektor energi yang berkembang pesat dan semakin bergantung pada teknologi digital. Seiring dengan upaya Indonesia untuk terus memodernisasi infrastruktur energinya, pelajaran yang dipetik dari serangan Pemex dapat menjadi dasar pengembangan strategi keamanan siber yang kuat untuk melindungi aset-aset pentingnya dari ancaman serupa.

2. TINJAUAN PUSTAKA

Memetik pelajaran dari perusahaan minyak dan gas Nigeria, Ebelogu et al., dalam penelitiannya yang berjudul "*Investigation of Cybersecurity Vulnerabilities and Mitigation Strategies in Nigeria's Oil and Gas Industry*" (2025) menyatakan bahwa 70% pendapatan Nigeria berasal dari minyak dan gas dan perdagangan internasional Nigeria sebesar 90% dikontribusikan oleh industri minyak dan gas.[5] Namun, industri ini menghadapi pelanggaran keamanan; karena volume data yang diproduksi secara cepat oleh operasi hulu, tengah, dan hilir, serta sifat sensitif data ini, industri energi Nigeria menjadi target utama penjahat dunia maya. Serangan siber memiliki berbagai macam dampak kompleks terhadap industri minyak dan gas di Nigeria, termasuk potensi dampak lingkungan yang sangat besar, terutama jika serangan siber menargetkan kontrol operasional dan menyebabkan ledakan atau tumpahan minyak yang merusak ekosistem dalam jangka panjang, serta kerugian finansial yang signifikan akibat pencurian uang, pencurian kekayaan intelektual, dan gangguan bisnis. Oleh karena itu, ancaman

[5] Christopher Ubaka Ebelogu et al., "Investigation of Cybersecurity Vulnerabilities and Mitigation Strategies in Nigeria's Oil and Gas Industry," ABUAD Journal of Engineering Research and Development (AJERD) 8, no. 1 (Februari 23, 2025): 140–50, https://doi.org/10.53982/ajerd.2025.0801.15-j.

*Corresponding author
E-mail addresses: agipakambanan@gmail.com

siber terhadap infrastruktur kritis tidak boleh diremehkan dan harus diperhatikan secara khusus oleh pemerintah.

Pentingnya pemerintah untuk memperhatikan infrastruktur kritis dari ancaman ransomware juga didukung oleh Don C. Smith dalam penelitiannya yang berjudul *"Cybersecurity in the energy sector: are we really prepared?*" (2021).[6] Serangan siber terhadap infrastruktur kritis, termasuk sistem energi, menduduki peringkat risiko paling berbahaya kelima dalam Global Risk Report 2020 dari World Economic Forum International Energy Agency telah menyatakan bahwa, khususnya untuk sistem kelistrikan, "ancaman serangan siber sangat besar dan terus meningkat, dan para pelaku kejahatan siber menjadi semakin canggih dalam melakukan serangan." Amerika Serikat dengan kekuatannya masih bisa lengah dalam menjaga keamanan infrastruktur kritisnya dan mendapatkan kritik dari beberapa pengamat. Namun, ketika pemerintah Amerika Serikat mengimplementasikan *cybersecurity executive order*, hal tersebut menandakan komitmen dan kemajuan pemerintah dalam menangani ancaman siber, khususnya terhadap infrastruktur kritis. Namun, Amerika Serikat dikritik masih perlu upaya yang lebih signifikan lagi seperti pusat waktu nyata untuk melacak serangan siber dan koordinasi yang kuat antara pemerintah dan pemilik bisnis di sektor infrastruktur kritis.

Baezner dan Marie dalam penelitiannya yang berjudul *"Cyber and Information warfare in the Ukrainian conflict"* juga menyuarakan pendapatnya bahwa ancaman ransomware merupakan isu yang kritis dan masih sedikit yang menganalisis fenomena tersebut.[7] Protes publik massal dipicu oleh pembatalan Association Agreement dengan Uni Eropa oleh Presiden Ukraina pada akhir tahun 2013, yang seharusnya dapat memperkuat hubungan antara kedua organisasi tersebut. Beberapa bulan kemudian, Presiden Yanukovych yang dipermalukan melarikan diri ke Rusia, dan Rusia menginvasi Semenanjung Krimea. Lembaga dan media di Ukraina dan Rusia kemudian menjadi sasaran serangan DDoS, vandalisme situs web, dan Remote Administration Tools (RAT) yang didistribusikan melalui *email spear phishing* selama protes Euromaidan dan konflik berikutnya. Dampak ekonomi mencakup biaya hilangnya pendapatan dan kerusakan reputasi yang disebabkan oleh berbagai serangan DDoS dan perusakan situs web, serta biaya yang dikeluarkan untuk mengganti peralatan setelah serangan siber pada jaringan listrik Ukraina. Analisis menyimpulkan bahwa aktivitas siber yang dilakukan dalam konteks konflik

[6] Don C Smith, "Cybersecurity in the Energy Sector: Are We Really Prepared?" Journal of Energy & Natural Resources Law 39, no. 3 (Juli 3, 2021): 265–70, https://doi.org/10.1080/02646811.2021.1943935.
[7] Marie Baezner dan Patrice Robin, "Cyber and Information warfare in the Ukrainian conflict," *ETH Zurich*, no. 1 (Juni 1, 2017): 1–56, https://doi.org/10.3929/ethz-b-000169634.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9, Number 4, 2025
E-ISSN: 2988-1986
Open Access:

Ukraina berdampak pada Ukraina baik secara domestik maupun internasional. Selain itu, risiko terlalu bergantung pada teknologi asing, kemungkinan pasukan musuh secara fisik mengganggu infrastruktur telekomunikasi, konsekuensi serangan siber pada jaringan listrik Ukraina, dan munculnya malware baru merupakan contoh dampak teknologi.

Berdasarkan ketiga literatur terdahulu tersebut, peneliti memetik pelajaran bahwa adalah penting untuk pemerintah Indonesia mengambil langkah untuk meningkatkan dana dan penelitian di bidang keamanan siber. Perkembangan zaman yang semakin mendorong digitalisasi sistem informasi dan teknologi benar adanya memudahkan manusia, namun juga menciptakan celah bagi keamanan infrastruktur kritis Indonesia, terutama fakta bahwa Indonesia masih sangat tergantung dengan teknologi asing.[8] Hasil tinjauan pustaka juga menemukan bahwa penelitian terdahulu terkait serangan ransomware masih tergolong sedikit, terutama dalam kasus negara berkembang. Oleh karena itu, penelitian ini diharapkan dapat bermanfaat untuk berkontribusi terhadap studi keamanan infrastruktur kritis Indonesia.

3. METODE PENELITIAN

Penelitian tentang serangan ransomware terhadap Pemex ini menggunakan metodologi kualitatif. Peneliti memanfaatkan analisis data yang diperoleh dari tinjauan komprehensif literatur yang ada. Dengan memeriksa jurnal akademik, laporan industri, artikel berita, dan studi kasus, penelitian ini akan mengumpulkan dan menganalisis data sekunder untuk memahami penyebab, dampak, dan strategi respons serangan. Pendekatan kualitatif memungkinkan eksplorasi mendalam terhadap faktor kontekstual seputar insiden Pemex, seperti kerentanan perusahaan, praktik keamanan siber, dan implikasi yang lebih luas bagi infrastruktur kritis Pemex. Selain itu, untuk menganalisis insiden ini secara komprehensif dan memperoleh wawasan yang dapat ditindaklanjuti untuk sektor energi Indonesia, penelitian ini menggunakan metodologi kualitatif yang didasarkan pada tinjauan pustaka terhadap literatur terdahulu yang ada.

[8] None Tri Bagus Prabowo dan None Rezya Agnesica Sihaloho, "Analisis Ketergantungan Indonesia Pada Teknologi Asing Dalam Sektor Energi Dan Dampaknya Pada Keamanan Nasional," Jurnal Lemhannas RI 11, no. 1 (Mei 9, 2023): 72–82, https://doi.org/10.55960/jlri.v11i1.426.

*Corresponding author
E-mail addresses: agipakambanan@gmail.com

4. HASIL DAN PEMBAHASAN

Serangan ransomware Pemex mengungkap sejumlah kerentanan dalam kerangka kerja keamanan siber organisasi. Banyak sistem TI Pemex tidak ditambal atau diperbarui dengan benar, membuatnya rentan terhadap kelemahan keamanan yang diketahui. Sistem teknologi yang ketinggalan zaman serta protokol keamanan siber yang tidak memadai memudahkan penyerang untuk mengeksploitasi kerentanan Pemex. Laporan Indeks Keamanan Global & Profil Kesehatan Siber 2015 dari International Telecommunications Union (ITU) menyatakan bahwa Meksiko tidak memiliki peta jalan tata kelola nasional untuk keamanan dunia maya dan bahwa kerentanan utamanya adalah kurangnya budaya keamanan dunia maya, konfigurasi sistem yang salah, versi lama yang perlu diganti dengan teknologi baru dan kompatibel, serta masalah aplikasi.[9] Karena Meksiko tidak memiliki lembaga pemerintah atau sektor publik khusus yang tersertifikasi berdasarkan standar yang diakui secara internasional, insiden siber menjadi tantangan karena kurangnya struktur kelembagaan dan kebutuhan untuk memperkuat kapabilitas.

Kedua, segmentasi jaringan yang tidak memadai memungkinkan ransomware menyebar dengan cepat ke seluruh infrastruktur perusahaan Pemex.[10] Kurangnya kontrol akses yang tepat dan pemisahan antara sistem kritis dan non-kritis meningkatkan dampak serangan. Serangan siber yang berhasil pada sistem Internet of Things (IoT) dapat melumpuhkan operasi sistem, membahayakan nyawa, menyebabkan kerusakan ekonomi, dan bahkan menyebabkan kerugian yang tidak dapat dipulihkan. Meningkatnya konektivitas IoT dan komputasi berbasis Cloud membuat aset dan fasilitas IoT rentan terhadap berbagai ancaman siber, termasuk pelanggaran data, penolakan layanan, dan serangan canggih.[11] Pemex dapat memvisualisasikan strategi keamanan mereka dalam hal pengguna, perangkat keras, dan jaringan dengan memperkenalkan konsep lapisan (*layers*). Representasi ini komprehensif karena memperhitungkan faktor eksternal dan internal, seperti aspek fisik dan manusia, dan memungkinkan organisasi untuk lebih jauh mengelompokkan sistem menurut berbagai domain berdasarkan bagaimana struktur jaringan mereka dikonfigurasi.[12]

---

[9] International Telecommmunications Union, "Global Cybersecurity Index & Cyberwellness Profiles," ITU, April 2015, http://www.itu.int/pub/D-STR-SECU-2015.
[10] Jovita Nsoh, "'Next-Gen' Cybersecurity" (PhD Dissertation, Colorado Technical University (CTU), 2021), https://www.researchgate.net/publication/348943946_Next-Gen_Cybersecurity?enrichId=rgreq-534f8de23d420c4150fea5bd59ced5f8-XXX&enrichSource=Y292ZXJQYWdlOzM0ODk0Mzk0NjtBUzoxMTQzMTI4MTEyNTQ5NzE5NEAxNjc4MzQxNDk5OTMy&el=1_x_2&_esc=publicationCoverPdf.
[11] Ibid., 8
[12] Ibid., 12

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9, Number 4, 2025
E-ISSN: 2988-1986
Open Access:

Ketiga, terdapat kurangnya kesadaran karyawan. Serangan tersebut diduga dimulai melalui *email* phishing, yang merupakan metode umum yang digunakan oleh kelompok ransomware untuk memperoleh akses awal ke jaringan target.[13] Pemex harus berkomitmen untuk meningkatkan kewaspadaan karyawan terhadap ransomware melalui phishing, yang dapat dicapai dengan menguji respons karyawan secara berkala dan meningkatkan kewaspadaan melalui simulasi phishing; melatih karyawan untuk mengidentifikasi email phishing, seperti tautan mencurigakan, lampiran tak terduga, dan pesan mendesak; dan mempromosikan budaya kehati-hatian, di mana karyawan melaporkan email mencurigakan alih-alih menanggapinya.

Kurangnya koordinasi dan kesiapan juga menghambat respons Pemex terhadap serangan tersebut, dan rencana respons insiden perusahaan tersebut tidak memadai atau tidak dilaksanakan dengan baik, yang menyebabkan penundaan penahanan dan pemulihan. Sekitar sepertiga dari total pendapatan pemerintah Meksiko berasal dari pendapatan minyak dan gas, yang dikelola melalui PEMEX. Sektor swasta Amerika Latin terus menunjukkan kurangnya pengetahuan mengenai risiko serangan siber terhadap infrastruktur penting. Pemerintah Meksiko tidak siap untuk mengimbangi serangan siber, yang menyoroti kerentanan dan peluangnya karena meningkatnya serangan antara tahun 2013 dan 2014.

Untuk meningkatkan efisiensi dan keberlanjutan, infrastruktur energi Indonesia, yang meliputi minyak, gas, dan sumber energi terbarukan, semakin bergantung pada teknologi digital. Namun, digitalisasi ini juga membuat sektor energi Indonesia rentan terhadap ancaman siber, seperti serangan ransomware. Sebagai negara yang berkembang pesat dengan sektor energi yang sedang berkembang pesat, Indonesia menghadapi tantangan keamanan siber yang serupa dengan yang dihadapi Meksiko. Indonesia dapat memetik beberapa pelajaran penting dari serangan ransomware Pemex saat berupaya memperkuat pertahanan keamanan sibernya.

Infrastruktur TI perusahaan yang sudah ketinggalan zaman menjadi salah satu penyebab utama serangan Pemex. Maka dari itu Indonesia perlu menjadikan investasi dalam sistem TI yang canggih dan aman sebagai prioritas utama guna mengurangi kerentanan dan meningkatkan ketahanan terhadap serangan siber. Penting juga untuk menyoroti bahwa kesadaran dan pelatihan karyawan sangat penting, seperti yang ditunjukkan oleh keberhasilan serangan phishing seperti yang digunakan dalam kasus Pemex. Perusahaan energi Indonesia harus secara

[13] D. Howard Kass, "Pemex Ransomware Attack: Mexico Oil, Gas Recovery Update -," MSSP Alert, November 18, 2019, https://www.msspalert.com/news/pemex-recovery-update.

*Corresponding author
E-mail addresses: agipakambanan@gmail.com

teratur melakukan program pelatihan keamanan siber untuk memberitahu anggota staf tentang bahaya phishing dan vektor serangan umum lainnya. Serangan Pemex juga menunjukkan betapa pentingnya memiliki rencana respon insiden yang terdefinisi dengan baik dan dilaksanakan dengan baik. Untuk menjamin respons yang tepat waktu dan terkoordinasi terhadap insiden siber, sektor energi Indonesia harus membuat dan menguji rencana respon insiden secara berkala. Sektor energi Indonesia harus mengambil pendekatan proaktif terhadap keamanan siber, yang mencakup penilaian kerentanan secara berkala, penerapan sistem deteksi ancaman tingkat lanjut, dan mengikuti ancaman siber yang muncul, daripada menunggu serangan terjadi.

5. KESIMPULAN DAN SARAN

Serangan ransomware tahun 2019 terhadap Petróleos Mexicanos (Pemex) menjadi studi kasus penting untuk memahami kerentanan infrastruktur sektor energi dan konsekuensi luas dari langkah-langkah keamanan siber yang tidak memadai. Penelitian ini menyoroti bagaimana sistem TI yang ketinggalan zaman, pelatihan karyawan yang tidak memadai, dan kurangnya rencana respon insiden yang kuat dapat membuat infrastruktur penting terpapar ancaman siber yang canggih. Serangan Pemex tidak hanya mengganggu operasi dan menyebabkan kerugian finansial, tetapi juga menggarisbawahi risiko yang lebih luas yang ditimbulkan ransomware terhadap keamanan nasional, stabilitas ekonomi, dan keselamatan publik. Bagi Indonesia, negara dengan sektor energi yang berkembang pesat dan digitalisasi yang meningkat, pelajaran dari Pemex sangat relevan. Oleh karena Indonesia terus memodernisasi infrastruktur energinya, keamanan siber harus menjadi prioritas untuk mengurangi resiko serangan serupa.

Untuk memperkuat pertahanannya, Indonesia harus mengadopsi pendekatan multi-aspek terhadap keamanan siber. Pertama, berinvestasi dalam infrastruktur TI modern sangat penting untuk mengurangi kerentanan dan meningkatkan ketahanan. Sistem yang ketinggalan zaman, seperti yang terlihat dalam kasus Pemex, merupakan sasaran empuk bagi kelompok ransomware. Kedua, program pelatihan dan kesadaran karyawan harus dilaksanakan untuk memerangi phishing dan vektor serangan umum lainnya. Kesalahan manusia tetap menjadi salah satu kerentanan paling signifikan dalam keamanan siber, dan mendidik karyawan dapat menjadi garis pertahanan pertama. Ketiga, mengembangkan dan menguji rencana respons insiden secara berkala sangat penting untuk memastikan respons yang terkoordinasi dan efektif terhadap insiden siber. Serangan Pemex menunjukkan bagaimana kurangnya kesiapan dapat memperburuk dampak serangan.

Triwikrama: Jurnal Multidisiplin Ilmu Sosial
Volume 9, Number 4, 2025
E-ISSN: 2988-1986
Open Access:

DAFTAR PUSTAKA

Baezner, Marie, and Patrice Robin. "Cyber and Information warfare in the Ukrainian conflict." *ETH Zurich*, no. 1 (Juni 1, 2017): 1–56. https://doi.org/10.3929/ethz-b-000169634.

Barrera, Adriana. "Ransomware attack at Mexico's Pemex halts work, threatens to cripple computers." *Reuters*. 2019. https://www.reuters.com/article/technology/ransomware-attack-at-mexicos-pemex-halts-work-threatens-to-cripple-computers-idUSKBN1XM041/.

Bloomberg. "Pemex Faces Payment Problems After Cyber Attack Shut System." *Bloomberg*. November 12, 2019. https://www.bloomberg.com/news/articles/2019-11-11/pemex-workers-barred-from-computers-after-unexpected-shutdown.

Ebelogu, Christopher Ubaka, Rajesh Prasad, Hashim Ibrahim Bisallah, Baba Mohammed Hammawa, and Israel Musa. "Investigation of Cybersecurity Vulnerabilities and Mitigation Strategies in Nigeria's Oil and Gas Industry." *ABUAD Journal of Engineering Research and Development (AJERD)* 8, no. 1 (Februari 23, 2025): 140–50. https://doi.org/10.53982/ajerd.2025.0801.15-j.

Flowers, Lynnmarie P. "Cybersecurity: Preventing Infection in a Body of Data." *Journal of Petroleum Technology* 72, no. 08 (Agustus 1, 2020): 34–37. https://doi.org/10.2118/0820-0034-jpt.

International Telecommmunications Union. "Global Cybersecurity Index & Cyberwellness Profiles." ITU, April 2015. http://www.itu.int/pub/D-STR-SECU-2015.

Kass, D. Howard. "Pemex Ransomware Attack: Mexico Oil, Gas Recovery Update -." *MSSP Alert*, November 18, 2019. https://www.msspalert.com/news/pemex-recovery-update.

*Corresponding author
E-mail addresses: agipakambanan@gmail.com

Kobek, Luisa Parraguez. "The State of Cybersecurity in Mexico: An Overview." *Wilson Center Mexico Institute*, Januari 2017. https://latixns.mx/wp-content/uploads/2017/03/cybersecurity_in_mexico_an_overview.pdf.

Nsoh, Jovita. "'Next-Gen' Cybersecurity." PhD Dissertation, Colorado Technical University (CTU), 2021. https://www.researchgate.net/publication/348943946_Next-Gen_Cybersecurity?enrichId=rgreq-534f8de23d420c4150fea5bd59ced5f8-XXX&enrichSource=Y292ZXJQYWdlOzM0ODk0Mzk0NjtBUzoxMTQzMTI4MTEyNTQ5NzE5NEAxNjc4MzQxNDk5OTMy&el=1_x_2&_esc=publicationCoverPdf.

O'Kane, Philip, Sakir Sezer, and Domhnall Carlin. "Evolution of Ransomware." *IET Networks* 7, no. 5 (Juni 30, 2018): 321–27. https://doi.org/10.1049/iet-net.2017.0207.

Prabowo, None Tri Bagus, and None Rezya Agnesica Sihaloho. "Analisis Ketergantungan Indonesia Pada Teknologi Asing Dalam Sektor Energi Dan Dampaknya Pada Keamanan Nasional." *Jurnal Lemhannas RI* 11, no. 1 (Mei 9, 2023): 72–82. https://doi.org/10.55960/jlri.v11i1.426.

Romaniuk, Scott N., and Mary Manjikian. *Routledge Companion to Global Cyber-Security Strategy*. *Routledge eBooks*, 2020. https://doi.org/10.4324/9780429399718.

Smith, Don C. "Cybersecurity in the Energy Sector: Are We Really Prepared?" *Journal of Energy & Natural Resources Law* 39, no. 3 (Juli 3, 2021): 265–70. https://doi.org/10.1080/02646811.2021.1943935.