Betelgeuse Journal
ISSN: 3063-900X (online), 3063-7546 (print)
DOI: 10.59447

Analisis Angka *Cyber Crime Identity Theft* Guna Menumbuhkan Kesadaran *Cyber Security* pada Taruna Akademi TNI Angkatan Laut

Analysis of Cyber Crime Identity Theft Figures to Grow Cyber Security Awareness Among Cadets of the Naval Academy

Mohammad Haswin Al-Rafi[1], Unggul Firmansyah[1], Pungki Kurniawan[1], Priyono[1]
[1]Akademi Angkatan Laut, Jl. Bumimoro Morokrembangan, Surabaya, Jawa Timur, 60178, Indonesia
*Penulis korespondensi, Surel: priyondy69@gmail.com

Abstract

The advancement of technology and information, which coincides with digitalization alongside the development of Artificial Intelligence (AI), has colored human social life around the world. Currently, cadets of the Naval Academy often use gadgets/digital tools to access information or other media. With this, there are emerging threats that are very dangerous for individuals and the state. An currently prevalent case is Cyber Crime Identity Theft. Cyber crime identity theft refers to the crime of stealing someone's personal information online for the purpose of fraud or financial gain by stealing personal data such as names, identity numbers, and financial information, to carry out illegal transactions or obtain illegal benefits, which can lead to financial loss and damage the victim's reputation. Indonesia still has a very high number of cases of cyber crime identity theft, but it should be preventable by fostering. the cyber security awareness of cadets at the Naval Academy of the Indonesian National Armed Forces. The conclusion of this research is that by strengthening modern technological infrastructure, both equipment and administrative services, developing modern software and hardware with strong security systems, and tightening regulations regarding access to users' personal data in cyber services, supported by strengthening cyber security institutions, it can enhance the cyber security awareness of cadets at the Naval Academy of the Indonesian National Armed Forces.

Keywords: ***Cyber Crime Identity Theft, Cyber Security, SWOT***

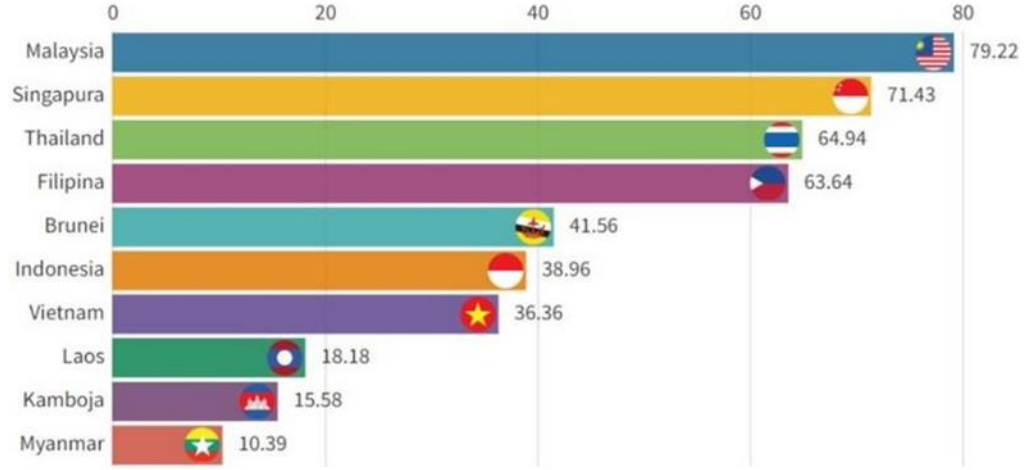
Abstrak

Kemajuan teknologi dan informasi yang terjadi bersamaan dengan digitalisasi dengan perkembangan *Artificial Intellegence* (AI) telah mewarnai kehidupan sosial manusia di seluruh dunia. Saat ini, Taruna Akademi TNI Angkatan Laut sering menggunakan *gadget*/peralatan digital untuk mengakses informasi atau media lainnya. Dengan adanya hal ini, timbul dampak ancaman yang sangat berbahaya bagi perorangan maupun negara. Kasus yang marak terjadi saat ini adalah *Cyber Crime Identity Theft*. *Cyber crime identity theft* yaitu kejahatan mencuri informasi pribadi seseorang secara daring untuk tujuan penipuan atau penguntungan finansial dengan cara mencuri data pribadi seperti nama, nomor identitas, dan informasi keuangan, untuk melakukan transaksi ilegal atau mendapatkan keuntungan secara ilegal yang dapat menyebabkan kerugian finansial dan merusak reputasi korban. Indonesia masih memiliki jumlah kasus *cyber crime identity theft* yang sangat tinggi, tetapi seharusnya dapat dicegah dengan menumbuhkan kesadaran *cyber security* sesorang. Salah satunya di lingkup Para Taruna Akademi Angkatan TNI Angkatan Laut. Penelitian ini dilakukan untuk memberikan kesadaran kepada Taruna Akademi TNI Angkatan Laut untuk menumbuhkan kesadaran *cyber security* akan bahayanya *cyber crime identity theft*. Pendekatan penelitian menggunakan metode kualitatif dengan analisis deskriptif yang dianalisis menggunakan SWOT. Hasil penelitian menyimpulkan dengan nilai strategi SWOT yang diperoleh, yaitu pada kuadran II dengan menggunakan kekuatan/*strength* dan mengatasi ancaman/*threats* dalam menumbuhkan kesadaran *cyber security* Taruna Akademi TNI Angkatan Laut. Kesimpulan dalam penelitian ini adalah dengan penguatan infrastruktur teknologi yang modern, baik peralatan maupun layanan administrasi, pengembangan *software* dan *hardware* yang modern dan memiliki sistem pengamanan yang kuat, serta pengetatan aturan-aturan terkait akses terhadap data pribadi pengguna layanan siber, yang didukung penguatan lembaga-lembaga pengamanan siber sehingga dapat meningkatkan *kesadaran cyber security* para Taruna Akademi TNI Angkatan Laut.

Kata kunci: Keamanan Siber Pencurian Identitas, Keamanan Siber, SWOT

1. Pendahuluan

Kemajuan teknologi digital, termasuk perkembangan *Artificial Intelligence* (AI), telah memberikan banyak manfaat sekaligus memunculkan ancaman serius berupa kejahatan siber, khususnya pencurian identitas (*identity theft*). Laporan *Identity Theft Resource Center* (ITRC) mencatat lebih dari 400 juta kasus pencurian data pribadi pada tahun 2022, dengan jejaring sosial menjadi sasaran utama. Sayangnya, tingkat keamanan siber Indonesia masih tergolong lemah, terbukti dari peringkat ke-83 dari 160 negara dalam NCSI *Global Security Index* (2022). Kondisi ini menunjukkan bahwa meskipun infrastruktur pertahanan siber telah dibangun melalui BSSN dan Satuan Siber TNI, celah kerentanan serta kelalaian individu masih sering dimanfaatkan peretas.



Gambar. 1.1. Indeks Keamanan Siber Negara ASEAN

Sumber: NCSI Global Security Index, 2022

2. Metode

Metode penelitian yang digunakan merupakan bentuk penelitian kualitatif dengan menggunakan metode analisis deskriptif. Penelitian kualitatif ini berdasarkan pada upaya membangun pandangan mereka yang diteliti dengan rinci, dibentuk dengan kata-kata dan gambaran holistik (Maleong, 2011). Gaya penelitian kualitatif berusaha mengkonstruksi realitas dan memahami maknanya, sehingga penelitian kualitatif sangat memperhatikan proses, peristiwa dan otentisitas. Peneliti kualitatif biasanya terlibat dalam interaksi dengan realitas yang ditelitinya. Metode analisis deskriptif merupakan salah satu cara analisis sebagai prosedur pemecahan masalah penelitian dengan menggambarkan keadaan objek penelitian berdasarkan fakta-fakta objektivitas yang tampak atau sebagaimana adanya (*das Sein*). Mengacu pada metode ini, maka pelaksanaan penelitian ini melalui studi kasus yang merupakan kombinasi dari pengamatan, pengumpulan data dan analisisnya untuk memperoleh gambaran menyeluruh terkait "Analisis Angka *Cyber Crime Identity Theft* Guna Menumbuhkan Kesadaran *Cyber Security* Pada Taruna Akademi TNI Angkatan Laut".

3. Hasil dan Pembahasan

Analisis kesadaran *cyber security* pada Taruna Akademi TNI Angkatan laut terhadap perkembangan ancaman *cyber crime identity theft*, serta strategi yang dapat digunakan untuk meningkatkan kesadaran *cyber security* pada Taruna Akademi TNI Angkatan Laut tersebut.

Dalam hal ini peneliti menggunakan Analisis SWOT sebagai pisau analisis untuk mengolah data penelitian berupa langkah-langkah sebagai berikut:

1.1 **Analisa Faktor Internal dan Faktor Eksternal.** Analisis faktor internal dan eksternal adalah pengolahan faktor-faktor strategis pada lingkungan internal dan eksternal berkaitan dengan kesadaran *cyber security* para Taruna, serta perkembangan Angka *Cyber Crime Identity Theft*. Dalam hal ini, faktor internal berupa kekuatan/*strengths (S)* dan kelemahan/*weaknesses (W)* para Taruna Akademi Angkatan Laut terkait dengan hal-hal yang berhubungan dengan kesadaran *cyber security*. Sementara itu faktor eksternal berkaitan dengan berbagai bentuk peluang/*opportunities (O)* dan ancaman/*threats (T)* terkait perkembangan angka *Cyber Crime Identity Theft* dan kesadaran *cyber security*. Pembahasan difokuskan pada mengaitkan data dan hasil analisisnya dengan permasalahan atau tujuan penelitian dan konteks teoretis yang lebih luas. Dapat juga pembahasan merupakan jawaban pertanyaan mengapa ditemukan fakta seperti pada data. Pembahasan ditulis melekat dengan data yang dibahas. Pembahasan diusahakan tidak terpisah dengan data yang dibahas.

1) Penyusunan analisis matriks SWOT. Penyusunan analisis SWOT dapat menggunakan model-model Matriks Analisis IFAS (*Internal Factor Analysis Strategy),* Matriks Analisis EFAS (*External Factor Analysis Strategy* seperti yang tergambar dalam tabel berikut:

Tabel 4.4 Analisis IFAS (*Internal Factor Analysis Strategy*)

NO	FAKTOR STRATEGI INTERNAL	BOBOT	RATING	B X R	KETERANGAN
	STRENGHT/KEKUATAN (S)				
1	Selalu melakukan Cek dan Ricek untuk merespon kepercayaan terhadap informasi digital dari saluran komunikasi umum	0.25	4	1	Faktor Kekuatan sangat besar untuk di optimalkan
2	Selalu melakukan Cek dan Ricek untuk merespon kepercayaan terhadap informasi digital dari Situs dan	0.25	4	1	
	nomor kontak resmi/terpercaya	0.20	4	0.80	
4	Kuatnya ketertarikan terhadap Pembangunan kekuatan Siber TNI dan Siber Indonesia	0.20	4	0.80	
5	Kekuatan dan kemampuan Siber Indonesia cukup kuat untuk mendukung peningkatan *Cyber Security*	0.10	4	0.40	
TOTAL		**0.50**		**4.00**	
WEAKNESS/KELEMAHAN (W)					

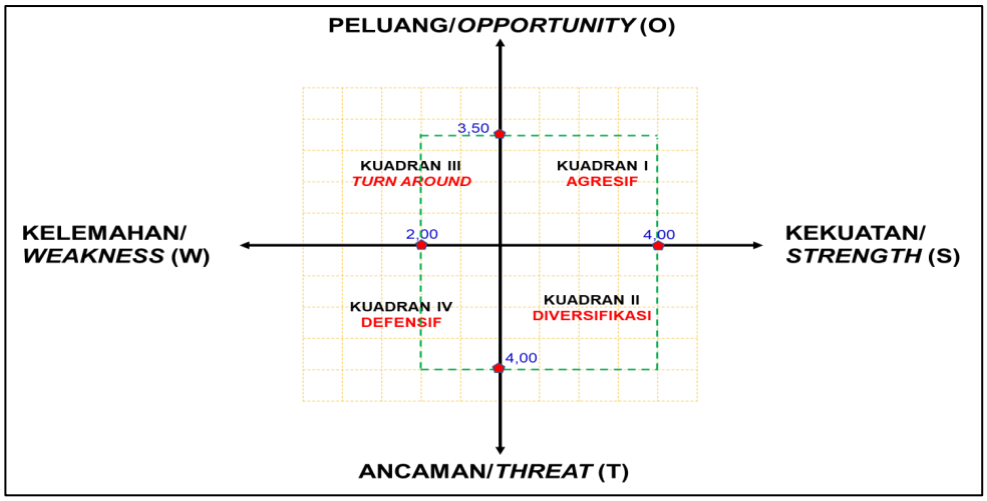
1	Selalu melakukan Cek dan Ricek untuk merespon kepercayaan terhadap informasi digital dari saluran komunikasi umum	0.20	2	0.40	Faktor Kelemahan cukup banyak untuk di perbaiki
2	Selalu melakukan Cek dan Ricek untuk merespon kepercayaan terhadap informasi digital dari Situs dan nomor kontak resmi/terpercaya	0.20	2	0.40	
3	Kuatnya kepedulian terhadap kemampuan dan kepentingan Siber	0.20	1	0.20	
4	Kuatnya ketertarikan terhadap Pembangunan kekuatan Siber TNI dan Siber Indonesia	0.20	3	0.60	
5	Kekuatan dan kemampuan Siber Indonesia cukup kuat untuk mendukung peningkatan Cyber Security	0.20	2	0.40	
TOTAL		**1.00**		**2.00**	

Sumber: Diolah Penelitian (2024).

2) Strategi umum dan penjelasan arah strategi

a) Total skor kekuatan : 4,00
b) Total skor kelemahan : 2,00
c) Total skor peluang : 3,50
d) Total skor ancaman : 4,00

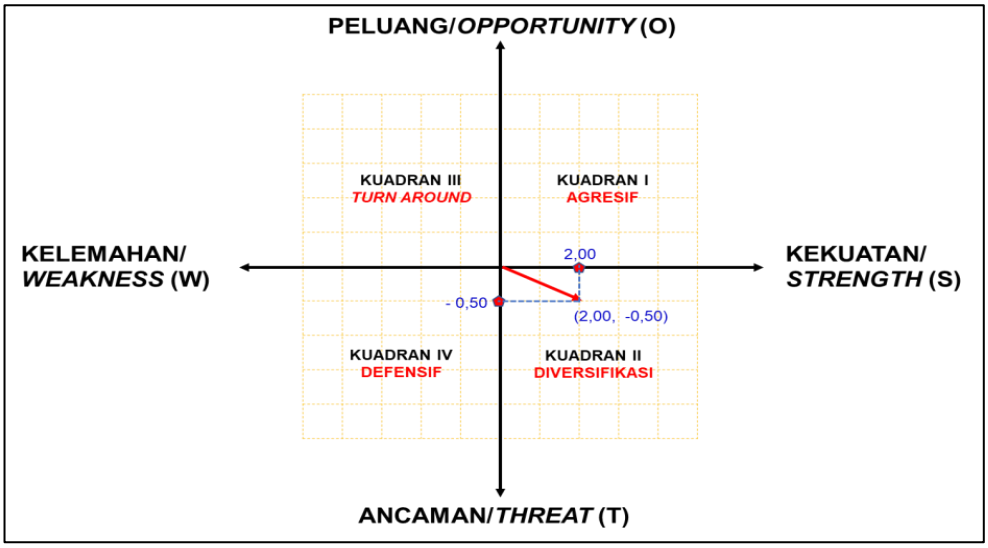
Berdasarkan total skor diatas, maka area cakupan strategi dapat digambar dalam matriks SWOT berikut:



Gambar 3.2. CMS MSI-90U Mk 2 di KRI Nanggala 402
Sumber: Gilang Perdana (2024)

Selain itu, penentuan koordinat dari gambar tersebut adalah sebagai berikut:

a) Koordinat Analisis Internal:
= (Skor total kekuatan – Skor total kelemahan)
= (4,00 – 2,00) = 2,00
b) Koordinat Analisis External:
= (Skor total peluang – Skor total ancaman)
= (3,50-4,00)
= -0,50
Titik koordinat terletak pada (2,00,-0,50)



Gambar 4.2 Titik Koordinat Strategi SWOT
Sumber : Diolah Peneliti (2024)

Dari gambar matriks dan analisa tersebut dapat disimpulkan bahwa visualisasi komponen Kekuatan/*Strength* (S), Kelemahan/*Weakness* (W), Peluang/*Opportunities* (O), dan Ancaman/*Threat* (T) menunjukkan strategi yang akan dijalankan berada pada Kuadran II. Walaupun menghadapi berbagai macam ancaman yang cukup besar, tetapi kesadaran *cyber security* para Taruna masih memiliki kekuatan sangat besar untuk dapat memaksimalkan dalam mengatasi ancaman *cyber crime identity theft*. Penetapan arah kebijakan dan strategi yang harus dijalankan adalah menggunakan kekuatan secara sinergi untuk dapat dioptimalkan dengan berbagai upaya **Diversifikasi** berupa peningkatan program pembinaan dan pengetahuan siber, serta penguatan sarana prasarana dan sistem pengamanan sibe.Bagi

3.1 PEMBAHASAN HASIL ANALISIS

Hasil penelitian pada Taruna Akademi TNI Angkatan Laut terhadap perkembangan ancaman *cyber crime* menunjukkan berbagai keadaan dan kondisi tingkat kesadaran terhadap *cyber security*. Jika memperhatikan perkembangan teknologi siber dengan berbagai ancaman di dalamnya yang sedemikian pesat harus dapat diketahui, dipahami dan diantisipasi oleh setiap anggota Taruna Akademi TNI Angkatan Laut sebagai bentuk kesadaran *cyber crime*. Dari hasil pengolahan data dan fakta serta

analisis teori SWOT menunjukkan bahwa sebagian besar Taruna pada dasarnya sudah mengetahui akan perkembangan ilmu pengetahuan dan teknologi siber karena secara umum mereka melek teknologi, serta merupakan pengguna teknologi informasi dan komunikasi data digital maupun layanan perbankan/finansial *online* yang aktif. Namun, terkait dengan pengetahuannya mengenai perkembangan pola dan teknik ancaman *cyber crime identity theft* secara umum masih cukup lemah. Di karenakan kurangnya pengetahuan yang dimiliki oleh para Taruna tidak bisa dianggap lemah begitu saja, akan tetapi masih cukup dapat diimbangi oleh upaya yang mereka lakukan dengan cek dan ricek untuk merespon kepercayaan terhadap informasi digital dari saluran komunikasi umum maupun terhadap informasi digital dari Situs dan nomor kontak resmi/terpercaya. Di samping itu, memang ada ketertarikan yang kuat dari Para Taruna Akademi TNI Angkatan Laut terhadap pengetahuan tentang siber sehingga diharapkan dapat menggugah kesadaran *cyber security* mereka.

Sementara itu, terkait banyaknya Taruna Akademi TNI Angkatan Laut yang mengalami kasus peretasan memang memperlihatkan kurang kuatnya kesadaran terkait *cyber security*, terutama menyangkut penggunaan pengamanan *gadget*/sistem yang kurang kuat. Namun, hal ini seharusnya dapat diminimalisasi oleh dukungan pihak ketiga, seperti penyedia sistem maupun satuan pengamanan siber yang ada. Seperti yang dapat kita ketahui bahwa penyedia sistem maupun satuan pengamanan siber akan selalu memberikan perlindungan maksimal bagi pengguna sistem tersebut.

4. Simpulan.

Berdasarkan hasil penelitian terkait analisis angka *cyber crime identity theft* guna menumbuhkan kesadaran *cyber security* pada Taruna Akademi TNI Angkatan Laut yang telah dijabarkan, terdapat hal penting yang perlu digaris bawahi berkaitan Kapal dengan perkembangan ancaman *cyber crime identity theft* yang sangat tinggi dan berdampak besar terhadap kerugian material maupun non-material, bahkan kerugian ini dapat bersifat fatal apabila menyangkut kehidupan sosial maupun kehidupan berbangsa dan bernegara yang lebih luas, seperti penyalahgunaan data oleh organisasi teroris atau separatis untuk menghancurkan bangsa dan negara Indonesia. Melalui metode penelitian kualitatif dengan *tool analysis* SWOT berupa kondisi internal Para Taruna Akademi TNI Angkatan Laut terkait Kesadaran *cyber security*, serta berbagai bentuk peluang dan ancaman terkait perkembangan angka *cyber crime identity theft*, maka dapat ditarik kesimpulan untuk dapat menjawab pokok-pokok persoalan yang telah ditetapkan sebagai berikut:

a. Sesuai dengan hasil analisis kesadaran *cyber security* pada Taruna Akademi TNI Angkatan Laut terhadap perkembangan ancaman *cyber crime identity theft* memperlihatkan bahwa Para Taruna Akademi TNI Angkatan Laut belum memiliki kesadaran *cyber security* yang kuat untuk dapat mengantisipasi perkembangan ancaman *cyber crime identity theft*.

b. Berdasarkan analisa formulasi strategi sesuai dengan analisis SWOT yang telah diuraikan, maka beberapa strategi yang dapat digunakan untuk meningkatkan kesadaran *cyber security* pada Taruna Akademi TNI Angkatan Laut dalam menghadapi perkembangan ancaman *cyber crime identity theft*, yaitu:

1) Strategi pertama, berupa penguatan sarana /infrastruktur pengamanan siber melalui Pembangunan infrastruktur teknologi yang modern baik alat peralatan yang digunakan maupun layanan administrasi perkantoran yang mudah

2) Strategi kedua, berupa meningkatkan program pembinaan dan penguatan kesadaran *cyber security* yang muncul secara internal pada diri seorang Taruna Akademi TNI Angkatan Laut, yaitu dengan cara lembaga-lembaga siber yang ada di Indonesia mengadakan berbagai program pembinaan secara intensif dan berkesinambungan.

3) Strategi ketiga, berupa penguatan sistem pengamanan *cyber* melalui pengembangan *software* maupun *hardware* yang modern dan memiliki sistem pengamanan yang kuat.

4) Strategi keempat, berupa peningkatan pengetahuan tentang *cyber crime identity theft* bagi para Taruna Akademi TNI Angkatan Laut dengan memperkuat muatan Kurikulum Pelajaran siber yang lebih banyak, lebih komprehensif, serta dukungan alokasi waktu pembelajaran yang lebih lama di lembaga pendidikan, seperti Akademi TNI Angkatan Laut, sehingga jelas akan lebih meningkatkan pengetahuan peserta didik, sekaligus berkontribusi besar terhadap penguatan kesadaran *cyber security* mereka.

Daftar Rujukan.

Jurnal

A Pearce II Jhon.Richard B. Robinson Jr.(2013).Manajemen Strategis : Formulasi, Implementasi, dan Pengendalian, Terj. Nia Pramita Sari. Jakarta : Salemba Empat

Anthoni. (2017). Kejahatan Dalam Dunia Maya (Cyber Crime) Dalam Simak Online. Jurnal Nurani. Volume 17 Nomor 2.

Arikunto. (2013). Prosedur Penelitian Suatu Pendekatan Praktik. Edisi Revisi. Jakarta: PT. Rineka Cipta.

Burns, Robert. B. (2000). Introduction To Research Methods. USA: Sage Publications.

Hadnagy, Christopher. (2010). Social Engineering: The Art Of Human Hacking. Indianapolis: Wiley Publications.

Hanafi. (2022). Dasar Cyber Security dan Forensic. Sleman : Deepublish. Huda, Miftahul. (2020). Keamanan Informasi. Jakarta: Nulisbuku.

Indradi, Ade Ary Syam. (2006). Carding: Modus Operandi, Penyidikan dan Penindakan. Jakarta: Pensil-324.

Maleong. (2011). Metodologi Penelitian Kualitatif. Edisi Revisi. Bandung: PT. Remaja Rosdakarya.

Mardalis. (1995). Metode Penelitian Suatu Pendekatan Proposal. Jakarta : Bumi Aksara.

Margono. (2004). Metodologi Penelitian Pendidikan. Jakarta :Rineka Cipta

Merrier. (2021). Pencurian Identitas Online Sebagai Bentuk Kejahatan Mayantara (Cyber Crime). Bandung : Universitas Pendidikan Indonesia.

Miles, M.B, Huberman, A.M, & Saldana, J. (2014). *Qualitative Data Analysis, A Methods Sourcebook, Edition 3*. USA: Sage Publications. Terjemahan Tjetjep Rohindi Rohidi, UI-Press. Nadhotul Sufi, F. Y., Putri, D. K., & Dwi Suhartini. (2023). *Analisis Ancaman Cybercrime dan Peran Sistem Biometrik: Systematic Literature Review*.Nazir, Muhammad. 2003. *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Rahmadi, Galih. (2020). *Analisis kesadar yber security pada kalangan pelaku e-commerce di Indonesia*.
Rangkuti (2001). A*nalisis SWOT Teknik Membedah Kasus Bisnis*. Jakarta: PT.Gramedia Pustaka Utama.
Rangkuti (2016). *Analisis SWOT: Teknik Membedah Kasus Bisnis*. Jakarta: PT. Gramedia Pustaka Utama.
Silalahi. (2022). *Keamanan Siber (Cyber Security)*. Semarang: Yayasan Prima Agus Teknik dengan Universitas STEKOM.
Soni, Afdhil Hafi, & Didik Sudyana. (2019). *Analisis Kesadaran Mahasiswa UMRI Terkait Penggunaan Teknologi dan Media Sosial Terhadap Bahaya cyber crime, Jurnal Fasilkom Vol. 9. N0. 3.*
Sugiyono. (2001). *Metode Penelitian Kuantitatif Kualitatif dan R&D*. Bandung: Alfabeta.
Sugiyono. (2011). *Metode Penelitian Kuantitatif, Kualitatif dan R&D*. Bandung: Afabeta..
Syahdeni, Sutan. S. (2009). *Kejahatan & Tindak Pidana Komputer.* Jakarta: Pustaka Utama.
Ulber, Silalahi. (2015). *Asas-asas Manajemen*. Bandung: Refika Aditama.
Zalavadiya, N., & Priyanka, S. (2017). *A Methodology of Malware Analysis, Tools and Technique for Windows Platform* – RAT Analisis.

Website.

Ariandi Putra, *Berada di peringkat ke-24 dengan skor 94,88 pada Global Cybersecurity Index (GCI) 2022,* dalam: https://www.bssn.go.id/indeks-keamanan-siber-indonesia-peringkat-ke-24-dari-194-negara-di-dunia/, diakses tanggal 9 Juni 2024, Jam 16.15 WIB. Edi Pramana, *Ratusan Juta Kasus Pencurian Data Pribadi Terjadi Sepanjang 2022*, dalam: https://www.jawapos.com/teknologi/01433222/ratusan-juta-kasus-pencurian-data-pribadi-terjadi-sepanjang-2022, diakses tanggal 15 Oktober 2023, Jam 22.05 WIB.
https://student-activity.binus.ac.id/himti/2023/06/13/lemahnya-keamanan-siber-di-indonesia/, diakses tanggal 15 Oktober 2023, Jam 22.20 WIB.
Lenni Septiyani, *1,64 TB Data Kementerian Pertahanan Diduga Dicuri, Ini Penjelasan Ahli,* dalam : https://katadata.co.id/yuliawati/digital/6543b30422685/1-64-tb-data-kementerian-pertahanan-diduga-dicuri-ini-penjelasan-ahli, diakses tanggal 04 November 2023, Jam 22.05 WIB.
Putra Aji Adhari, *Seorang remaja asal Jakarta Selatan, terkenal sebagai bocah white hat hacker yang pernah meretassitus* ***NASA 2019****,* dalam: https://www.codepolitan.com/blog/bocah-white-hat-hacker-pernah-hack-situs-nasa-ini-kisahnya/, di akses tanggal 9 Juni 2024, Jam 17.23 WIB.
Universitas Binus, *Lemahnya Keamanan Siber Di Indonesia 2023.*