MEUSAPAT: Jurnal Ilmu Hukum
Volume 1, Nomor 1, Juni 2022 ISSN: 0000-0000

ANALISIS YURIDIS TERHADAP TINDAK PIDANA PENIPUAN SIBER DENGAN MODUS OPERANDI BUSINESS EMAIL

Ajad Wahyudi[1], Umar Mahdi[2], M Agmar Media[3]
[1, 2, 3]
Fakultas Hukum, Universitas Jabal Ghafur
ajadwahyudi223@gmail.com[1], umarmahdi@unigha.ac.id[2], agmarmedia@unigha.ac.id[3]

Abstrak

Penipuan siber dengan modus operandi business email merupakan tindak pidana yang semakin marak terjadi di era digital saat ini. Kasus-kasus penipuan semacam ini dapat menimbulkan kerugian materil dan immateril yang besar bagi para korban, termasuk dalam hal ini perusahaan atau institusi yang menjadi sasaran. Tujuan penelitian ini Untuk mengetahui bagaimana analisis yuridis terhadap tindak pidana siber dengan modus operandi business email, apa saja hambatan yang dihadapi dalam menangani tindak pidana penipuan siber dengan modus operandi business email, apa saja upaya yang dapat dilakukan dalam pencegahan tindak pidana penipuan siber dengan modus operandi business email. Metode pengumpulan data dalam penelitian ini melalui data primer yang diperoleh melalui studi lapangan dan data sekunder yang diperoleh melalui studi kepustakaan untuk mendapatkan konsep teori atau dokrin, pendapat atau pemikiran konseptual yang berhubungan dengan. penelitian ini berupa peraturan perundang-undangan, buku, tulisan ilmiah dan karya-karya tulis lainnya yang relevan dengan penelitian ini. Penipuan Siber Dengan Modus Operandi Business Email. Putusan Nomor: 26 PID.SUS/2023/PT.BNA memberikan kepastian hukum dan panduan bagi penegak hukum dalam mengatasi kasus tindak pidana penipuan siber dengan modus operandi business email. Upaya pencegahan terhadap tindak pidana penipuan siber dengan modus operandi business email sangat penting dalam menghindari tindak pidana tersebut. Terdapat empat upaya pencegahan yang dapat dilakukan, yaitu pelatihan dan edukasi, sistem keamanan yang dapat diandalkan, verifikasi identitas pengirim email, dan peningkatan keamanan fisik. Saran, sanksi haruslah tegas dan dapat memberikan efek jera pada pelaku penipuan siber, sehingga dapat mencegah terjadinya tindakan kejahatan siber yang lebih banyak lagi di masa mendatang.

Kata Kunci: Pidana, Penipuan dan Modus Operandi.

Abstract

Cyber fraud with the modus operandi of business email is a crime that is increasingly common in today's digital era. Cases of fraud like this can cause great material and immaterial losses for the victims, including in this case the targeted company or institution. The purpose of this study is to find out how the legal analysis of cyber crimes with the modus operandi of business email, what are the obstacles faced in handling cyber fraud crimes with the modus operandi of business email, what efforts can be made in preventing cyber fraud crimes with the modus operandi of business email. The data collection method in this study is through primary data obtained through field studies and secondary data obtained through literature studies to obtain theoretical concepts or doctrines, opinions or conceptual thoughts related to. this study is in the form of laws and regulations, books, scientific papers and other written works that are relevant to this study. The results of this study are expected to contribute to the development of law, especially the law on Cyber Fraud Crimes with the Modus Operandi of Business Email. Decision Number: 26 PID.SUS/2023/PT.BNA provides legal certainty and guidance for law enforcers in dealing with cyber fraud cases with the modus operandi of business email. Efforts to prevent cyber fraud with the modus operandi of business email are very important in avoiding such crimes. There are four preventive efforts that can be made, namely training and education, a reliable security system, verification of the identity of the email sender, and increased physical security. Advice, it is hoped that the Prosecutor, in the decision, considers factors such as the severity of the crime committed by the perpetrator, the amount of money taken, and the educational and work background of the perpetrator. The amount of money taken, and the educational and work background of the perpetrator. Sanctions must be strict and can provide a deterrent effect on cyber fraud perpetrators, so that they can prevent more cyber crimes in the future.

Keywords*: Criminal, Fraud and Modus Operandi.*

Pendahuluan

Penipuan siber dengan modus operandi business email merupakan tindak pidana yang semakin marak terjadi di era digital saat ini. Kasus-kasus penipuan semacam ini dapat

menimbulkan kerugian materil dan immateril yang besar bagi para korban, termasuk dalam hal ini perusahaan atau institusi yang menjadi sasaran. Untuk itu, adanya analisis yuridis terhadap tindak pidana penipuan siber dengan modus operandi business email perlu dilakukan sebagai upaya untuk menjaga stabilitas keamanan di ranah digital.[1] Dalam analisis tersebut, aspek-aspek hukum yang terkait akan dibahas secara mendalam, termasuk mengenai jenis-jenis tindak pidana yang terkait, unsur-unsur yang harus dipenuhi dalam kasus penipuan siber, dan tindakan hukum apa yang dapat diambil oleh korban. proses pemilihan, mulai dari tahap perencanaan hingga pengumuman hasil pemilihan.[2]

Dalam studi Putusan Nomor: 26 Pid.sus/2023/PT.BNA, kasus yang ditangani adalah kasus penipuan siber dengan modus operandi business email yang melibatkan sebuah perusahaan konstruksi yang menjadi korban. Dalam kasus ini, para pelaku mengirimkan email palsu kepada perusahaan tersebut atas nama klien mereka yang sebenarnya, dengan maksud untuk mengelabui dan meminta pembayaran uang sejumlah yang signifikan. Setelah dikaji secara mendalam, hakim memutuskan bahwa para pelaku telah melanggar Pasal 32 ayat (1) Jo. Pasal 48 ayat (1) UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang mengatur tentang tindak pidana penipuan siber. Dalam konteks ini, dapat disimpulkan bahwa kasus penipuan siber dengan modus operandi business email merupakan salah satu bentuk kejahatan siber yang dapat dilakukan oleh siapa saja, termasuk baik individu maupun kelompok. Oleh karena itu, upaya-upaya preventif dan penegakan hukum yang lebih intensif dan tegas perlu dilakukan guna memberantas kejahatan siber dan melindungi masyarakat serta perusahaan dari kerugian yang mungkin dapat terjadi akibat penipuan siber.[3]

Penipuan siber dengan modus operandi business email di Indonesia masih merupakan fenomena yang cukup baru dan jarang diketahui oleh masyarakat. Padahal, praktik penipuan seperti ini juga mengancam keamanan ranah digital di Indonesia.[4] Hal ini terlihat dari beberapa kasus penipuan siber dengan modus operandi business email yang terjadi pada perusahaan besar di Indonesia. Salah satunya adalah kasus yang melibatkan salah satu perusahaan tambang di Indonesia. Para pelaku berhasil membobol sistem informasi perusahaan dan mengirimkan email yang membuat perusahaan tersebut kehilangan uang

[1]Direktorat Jenderal Aplikasi Informatika. *Panduan Penanganan Kejahatan Komputer*. Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia. 2013, hal. 21

[2]Ilyas, Muhammad. *Cybercrime*. Yogyakarta: Pustaka Pelajar. 2017, hal. 12

[3]Putri, Emiliani. *"Tinjauan Hukum tentang Penipuan dalam Perdagangan Elektronik"*. Jurnal Hukum IUS QUIA IUSTUM, 2016, hal 22

[4] Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2016 tentang Penanganan Insiden Keamanan Informasi di Sektor Telekomunikasi.

sejumlah miliaran rupiah. Kejadian seperti ini menunjukkan bahwa tindak pidana penipuan siber dengan modus operandi business email merupakan ancaman yang serius bagi keamanan perusahaan di Indonesia.

Selain itu, penanganan kasus-kasus penipuan semacam ini juga dihadapkan pada beberapa kendala, seperti kurangnya kesadaran dan pemahaman masyarakat mengenai kejahatan siber, adanya hambatan teknis untuk mengidentifikasi dan menangani kasus, serta analogi yang kurang tepat dari undang-undang yang ada dalam menangani kejahatan siber. Kondisi ini menunjukkan adanya kebutuhan untuk memperkuat penanganan dan pencegahan tindak pidana penipuan siber dengan modus operandi business email di Indonesia.[5] Oleh karena itu, penelitian analisis yuridis terhadap kasus penipuan siber dengan modus operandi business email seperti yang diadili dalam Putusan Nomor: 26 Pid.sus/2023/PT.BNA sangat penting dalam memberikan solusi hukum yang tepat dalam menangani tindak pidana semacam ini. Kejahatan siber juga berubah dan berkembang sangat cepat seiring dengan perkembangan teknologi yang semakin maju. Oleh karena itu, regulasi hukum saat ini juga perlu mempertimbangkan perkembangan teknologi agar dapat memberikan perlindungan dan penegakan hukum yang lebih efektif dalam menangani kejahatan siber.[6]

Dalam konteks Indonesia, pemerintah telah mengeluarkan beberapa regulasi hukum terkait kejahatan siber tentang Informasi dan Transaksi Elektronik. Namun, masih banyak pelanggaran kejahatan siber yang sulit ditangani karena belum ada ketentuan yang jelas dalam regulasi hukum tersebut.[7] Oleh karena itu, penelitian analisis yuridis terhadap tindak pidana penipuan siber dengan modus operandi business email seperti yang diadili dalam Putusan Nomor: 26 Pid.sus/2023/PT.BNA ini sangat penting dalam mengidentifikasi dan membahas aspek-aspek hukum yang terkait, serta memberikan rekomendasi bagi pihak-pihak terkait dalam penanganan kasus serupa di masa depan.[8]

Berdasarkan uraian latar belakang permasalahan yang telah dikemukakan, maka tepat kiranya jika penelitian mengangkat judul." Analisis Yuridis Terhadap Tindak Pidana Penipuan Siber Dengan Modus Operandi Business Email (Studi Putusan Nomor: 26 Pid.Sus/2023/Pt.Bna)".

[5] Ilyas, Muhammad. *Cybercrime*. Yogyakarta: Pustaka Pelajar. 2017, hal, 87

[6] Kamaluddin. *Serangan Siber dan Perlindungan Informasi:* Telaah dari Perspektif Undang-Undang Negara. Jakarta: Kreasi Wacana. 2019, hal 27

[7] Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2016 tentang Penanganan Insiden Keamanan Informasi di Sektor Telekomunikasi.

[8] Mardani. *Metodologi Penelitian Hukum*. PT Raja Grafindo Persada, 2017, hal. 34

Metode Penelitian

Penelitian ini menggunakan pendekatan *yuridis empiris* dan *normatif. Yuridis empiris* adalah penelitian secara lapangan, yang mengkaji ketentun hukum yang berlaku serta yang telah terjadi didalam kehidupan masyarakat dengan cara wawancara responden dan informan. Dalam penelitian ini penulis akan menggunakan tahapan penelitian bersumber dari:

a. Penelitian kepustakaan (*library research*) untuk memperoleh data sekunder dilakukan dengan cara mengkaji atau mempelajari peraturan perundang-undangan, jurnal, buku-buku teks lainnya, makalah dan dokumen lainnya yang berkaitan dengan masalah yang dibahas.
b. Penelitian lapangan (*field research*) untuk memperoleh data primer yaitu akan dilakukan penelitian lapangan dengan mewawancarai responden yang sudah ditentukan sebelumnya.

Data yang diperoleh dari hasil penelitian kepustakaan dan penelitian lapangan akan diolah dan dianalisis secara kualitatif, yaitu menyajikan data yang telah didapat dari hasil wawancara dengan responden dan informan. Selanjutnya, penyusunan hasil penelitian dilakukan dengan menggunakan metode deskriptif, yaitu berusaha memberikan gambaran secara nyata tentang fakta-fakta yang ditemukan dalam praktik di lapangan serta mengaitkan dengan data kepustakaan, berupa bahan-bahan hukum (primer, sekunder, dan tersier).

Pembahasan

Analisis Yuridis Terhadap Tindak Pidana Siber dengan Modus Operandi Business Email

1. Tindak Pidana Penipuan Siber

Tindak pidana penipuan siber bisa terjadi dalam berbagai macam bentuk. Beberapa bentuk penipuan siber yang sering terjadi diantaranya adalah hacking, phising, fake website, identity theft, dan banyak lagi. Pelaku penipuan siber bisa saja melakukan kejahatan tanpa meninggalkan tanda apapun pada korban. Oleh karena itu, sangat penting untuk selalu waspada dan berhati-hati dalam menggunakan teknologi informasi.[9]

Pasal-pasal yang mengatur mengenai tindak pidana penipuan siber antara lain Pasal 28 ayat (1), Pasal 32 ayat (1), dan Pasal 49 Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi

[9] Susilo, R. *Kupas Tuntas Kejahatan Siber dengan Penipuan Online*. Iptek Daerah. 2021.

dan Transaksi Elektronik. Sanksi yang diberikan bagi pelaku penipuan siber bisa berupa pidana penjara ataupun denda, tergantung pada tingkat keparahan tindakan pelaku.[10]

Penting untuk diingat bahwa selain dari sisi hukum, penting juga bagi kita sebagai pengguna teknologi informasi untuk selalu waspada dan hati-hati dalam menggunakan internet. Terdapat banyak cara untuk menghindari menjadi korban penipuan siber, seperti tidak meng-klik link yang mencurigakan, menjaga kerahasiaan data pribadi, tidak acuh terhadap email atau pesan yang meminta informasi pribadi, dan banyak lagi.[11] Dengan meningkatkan kesadaran akan bahaya penipuan siber, kita bisa mencegah terjadinya tindak kejahatan siber dan menciptakan dunia digital yang lebih aman dan terpercaya.

Tindak pidana penipuan siber merupakan ancaman serius bagi masyarakat modern yang memanfaatkan teknologi informasi sebagai sarana utama komunikasi dan transaksi. Pelaku penipuan siber bisa dengan mudah menjalankan aksinya dari jarak jauh tanpa diketahui korban, sehingga membuat tindakan ini semakin sulit dideteksi. Selain itu, penipuan siber juga dapat menimbulkan kerugian yang besar bagi korban, tidak hanya dalam hal finansial, tetapi juga dalam hal kehilangan data pribadi dan kerugian lain yang sulit untuk dikembalikan.[12] Oleh karena itu, pemerintah dan berbagai instansi telah melakukan upaya untuk menangani tindak kejahatan siber. Beberapa langkah yang diambil antara lain dengan menerbitkan undang-undang yang mengatur tentang kejahatan siber, meningkatkan pengawasan terhadap industri Internet dan komputer, dan mengembangkan sistem keamanan siber yang lebih canggih.

Namun, upaya untuk mengurangi tindakan kejahatan siber tidak hanya tergantung pada upaya pemerintah, tetapi juga pada partisipasi dan kesadaran masyarakat. Pengguna internet harus mampu memahami dan mengidentifikasi berbagai macam modus operandi penipuan yang terjadi di dunia maya. Mereka juga harus mampu untuk mengambil tindakan preventif dan menghindari resiko menjadi korban kejahatan siber. Beberapa tindakan preventif yang dapat diambil yaitu dengan memperbaruhi sistem keamanan perangkat komputer, menghindari memasukkan data pribadi ke dalam

[10] Mahadika, R. *Perlindungan Hukum dan Hukuman atas Kejahatan Siber (Cybercrime)*. Jurnal Hukum Respublica, 2020. hal. 195-208.

[11] Kementerian Komunikasi dan Informatika. *Pedoman Penanganan dan Penyelesaian Insiden Keamanan Siber*. Ditjen Aplikasi Informatika Kementerian Komunikasi dan Informatika. 2018. Hal. 29-45.

[12] Adan Siber dan Sandi Negara. *Penangkapan Pelaku kejahatan Siber: Pentingnya Dukungan Masyarakat*. 2019

website atau aplikasi yang mencurigakan, serta tidak mengklik link atau terbuka di email atau pesan dari pengirim yang tidak dikenal atau mencurigakan.[13]

2. Modus Operandi Business Email

Modus operandi business email menjadi salah satu moda untuk melakukan penipuan siber. Pelaku penipuan siber memanfaatkan email dengan mengatasnamakan sebuah perusahaan atau institusi terpercaya, kemudian meminta korban untuk melakukan transaksi yang diduga menguntungkan.[14] Biasanya, email penipuan ini menggunakan embel-embel dari perusahaan atau institusi terpercaya tersebut sehingga membuat korban menjadi yakin dan mempercayai email tersebut. Salah satu bentuk penipuan siber dengan modus operandi ini adalah BEC (Business Email Compromise).[15]

Dalam BEC, pelaku penipuan tidak hanya menipu korban untuk melakukan transfer uang, namun juga mengambil alih akun email karyawan dan mencuri data pribadi. BEC memiliki tiga jenis utama, yaitu bogus invoice scams, CEO fraud, dan account compromise. Bogus invoice scams adalah penipuan melalui faktur yang mengatasnamakan perusahaan terpercaya atau dijadikan sebagai partner bisnis. Dalam kasus ini, pelaku penipuan meminta korban untuk membayar faktur palsu yang bernilai sangat besar, dan kemudian memasukkan rekening pelaku penipuan. CEO fraud, seperti namanya, adalah penipuan di mana pelaku mengatasnamakan CEO atau pimpinan perusahaan dan meminta karyawan di bawahnya untuk membayar tagihan atau membuka link tertentu.[16] Dalam kasus ini, pelaku seringkali menggunakan email palsu yang terlihat seperti email resmi perusahaan. Sementara, account compromise merupakan penipuan di mana pelaku mengambil alih akun email karyawan dan kemudian menggunakan akun tersebut untuk mengirimkan email penipuan. Dalam kasus ini, pelaku bisa mengakses email karyawan dan mencuri informasi pribadi dan rahasia perusahaan.

Untuk mencegah terjadinya penipuan siber melalui modus operandi business email ini, Anda perlu selalu melakukan verifikasi email dan informasi yang Anda terima sebelum melakukan transaksi. Selalu ingat untuk tidak mengklik link atau unduhan yang mencurigakan dan menghindari email atau pesan yang meminta

[13] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[14] Jaksa Penuntut Umum, Wawancara.
[15] Romadlon, M., & Pratama, A.N.F. *Analisis Faktor-Faktor Penipuan Menggunakan Modus Operandi Business Email Compromise (BEC) pada Karyawan di Kantor Cabang Bank Syariah Mandiri Tahun 2018*. Jurnal Sistem Informasi Bisnis,2019. hal. 53-67.
[16] Jaksa Penuntut Umum, Wawancara.

informasi pribadi. Selain itu, pastikan juga selalu mengakhiri sesinya setelah selesai menggunakan layanan email dari perangkat komputer yang tidak pribadi.[17]

Dalam rangka menangani BEC, perusahaan juga perlu meningkatkan kewaspadaan dan melindungi layanan mereka dari serangan siber. Beberapa cara yang dapat dilakukan adalah meningkatkan perlindungan dengan menggunakan password yang kuat, konfigurasi akses internet yang aman, dan melakukan pelatihan kepada karyawan untuk meningkatkan kesadaran tentang keamanan siber.

3. Putusan Nomor: 26 PID.SUS/2023/PT.BNA

Putusan Nomor: 26 PID.SUS/2023/PT.BNA adalah putusan pengadilan terkait penetapan tindak pidana penipuan siber dengan modus operandi business email. Dalam putusan tersebut, terdapat beberapa hal penting yang harus dipahami sebagai contoh kasus dalam tindak pidana penipuan siber. Pengadilan dalam putusan ini menegaskan bahwa terdapat unsur-unsur yang harus dipenuhi saat menetapkan sebuah tindak pidana penipuan siber.[18] Dalam hal ini, terdapat unsur penggunaan teknologi informasi, maksud untuk merugikan atau mengambil keuntungan dari orang lain, dan adanya tindakan penipuan yang dijalankan. Ketiga unsur ini harus terpenuhi secara bersamaan agar dapat menjatuhkan vonis penjara bagi pelaku yang telah melakukan tindakan penipuan.[19]

Dalam putusan ini, pengadilan juga memberikan penjelasan tentang jenis bukti-bukti yang digunakan untuk membuktikan tindak pidana yang dilakukan oleh pelaku penipuan siber. Bukti-bukti yang kuat dan sah harus bisa digunakan untuk memperkuat dakwaan dalam kasus tindak pidana penipuan siber. Putusan ini memberikan informasi mengenai sanksi bagi pelaku yang melakukan tindak pidana penipuan siber. Pelaku yang terbukti bersalah akan dikenai hukuman penjara maupun denda, yang disesuaikan dengan tingkat keparahan pelanggaran yang dilakukan.

Putusan Nomor: 26 PID.SUS/2023/PT.BNA menegaskan pentingnya aturan hukum dalam mengatasi tindak pidana penipuan siber dengan modus operandi business email. Pengadilan dalam putusan tersebut mengacu pada undang-undang dan peraturan yang berlaku dalam menentukan sanksi bagi pelaku kejahatan siber.[20]

[17] Warnars, H.L., Lumbanraja, P., & Swings, O.S. *Business Email Compromise (BEC): Analisa Kasus dan Aspek Teknis Keamanan Informasi*. JOURNALINFO (Jurnal Informatika dan Teknologi Informasi), 2017. hal. 31-41.

[18] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.

[19] Jaksa Penuntut Umum, Wawancara.

[20] Jaksa Penuntut Umum, Wawancara.

Pengadilan dalam putusan ini juga menekankan bahwa penipuan siber melalui modus operandi business email memberikan risiko yang sangat besar bagi korban. Pengadilan menegaskan bahwa pelaku penipuan bisa saja mengambil kontrol atas akun email karyawan yang memungkinkan akses ke informasi pribadi perusahaan dan data klien. Oleh karena itu, pencegahan dan perlindungan terhadap serangan kejahatan siber harus diutamakan. Pengadilan dalam putusan tersebut juga menegaskan bahwa bukti yang digunakan dalam kasus tindak pidana penipuan siber harus memenuhi kriteria validitas. Bukti yang sah dan kuat harus dapat memperlihatkan adanya unsur penggunaan teknologi informasi, maksud untuk merugikan atau mengambil keuntungan dari orang lain, dan adanya tindakan penipuan yang dilakukan oleh pelaku.[21]

Selain itu, pengadilan juga menegaskan bahwa sanksi yang dijatuhkan bagi pelaku penipuan siber harus sesuai dengan tindakan kejahatan yang dilakukan. Pengadilan harus mempertimbangkan faktor-faktor tertentu dalam menentukan sanksi, seperti tingkat keparahan dan durasi tindakan kejahatan, jumlah uang yang diambil, dan latar belakang pendidikan dan pekerjaan pelaku.[22]

Putusan Nomor: 26 PID.SUS/2023/PT.BNA adalah tambahan penting pada aturan hukum yang mengatur tindak pidana penipuan siber dengan modus operandi business email di Indonesia. Dalam untuk menangani hal ini, peran dan partisipasi aktif dari berbagai pihak terkait, seperti pemerintah, perusahaan, dan masyarakat, penting untuk meningkatkan kesadaran dan kewaspadaan dalam menghadapi risiko kejahatan siber.[23]

4. Analisis Yuridis

Dalam putusan Nomor: 26 PID.SUS/2023/PT.BNA, terdapat beberapa analisis yuridis yang dapat dilakukan. Pertama-tama, analisis terhadap unsur-unsur tindak pidana penipuan siber yang dipenuhi dalam kasus ini. Pasal-pasal yang diatur sehubungan dengan tindak pidana penipuan siber harus dibuktikan ada pada kasus yang diproses. Kedua, terdapat analisis terhadap jenis bukti dan bagaimana bukti harus dikumpulkan dan digunakan untuk membuktikan kasus tindak pidana penipuan siber.[24] Dalam putusan tersebut, disebutkan bahwa bukti yang valid harus dapat menunjukkan tindakan penipuan ataupun adanya penggunaan teknologi informasi yang merugikan korban. Ketiga, analisis terhadap sanksi hukuman yang harus diterapkan kepada pelaku penipuan siber. Penentuan sanksi hukuman harus mempertimbangkan tingkat keparahan tindakan

[21] Jaksa Penuntut Umum, Wawancara.
[22] Korban Penipuan Siber, wawancara.
[23] Kepala Pengadilan Tinggi Banda Aceh.
[24] Jaksa Penuntut Umum, Wawancara.

kejahatan yang dilakukan oleh pelaku serta kondisi sosial, pekerjaan, dan latar belakang pendidikan pelaku. Sanksi yang tegas dan berat harus diterapkan bagi pelaku penipuan siber untuk memberikan efek jera dan menimbulkan efek prventif pada masyarakat.

Dalam putusan Nomor: 26 PID.SUS/2023/PT.BNA, analisis yuridis juga mencakup Interpretasi dan penafsiran hukum sebagai bentuk pertimbangan hakim dalam memutus suatu kasus. Hakim dalam putusan tersebut merujuk pada undang-undang yang berlaku, yaitu yang mengatur tentang tindak pidana penipuan siber.[25] Di samping itu, Hakim dalam putusan tersebut juga memberikan analisis terhadap beberapa bukti yang menjadi dasar tuntutan melakukan tindak pidana penipuan siber. Bukti-bukti tersebut termasuk bukti-bukti transaksi transfer uang, data-data korban seperti informasi akun ATM dan data bank, serta informasi perusahaan yang dijadikan sebagai korbannya.

Analisis yuridis lain yang dilakukan adalah berkaitan dengan sanksi hukuman yang harus dilakukan terhadap pelaku penipuan siber. Hakim dalam putusan tersebut mempertimbangkan faktor-faktor seperti tingkat keparahan tindakan kejahatan yang dilakukan oleh pelaku, jumlah uang yang diambil, dan latar belakang pendidikan dan pekerjaan pelaku. Sanksi haruslah tegas dan dapat memberikan efek jera pada pelaku penipuan siber, sehingga dapat mencegah terjadinya tindakan kejahatan siber yang lebih banyak lagi di masa mendatang.[26]

Dalam kesimpulan, putusan Nomor: 26 PID.SUS/2023/PT.BNA memberikan kepastian hukum dan panduan bagi penegak hukum dalam mengatasi kasus tindak pidana penipuan siber dengan modus operandi business email. Analisis yuridis yang dilakukan dalam putusan tersebut memberikan interpretasi hukum dan panduan bagi penegak hukum dalam mengambil langkah pencegahan, penyidikan, serta penuntutan untuk memastikan agar kejahatan siber demi keamanan siber berbasis hukum dapat diminimalisir dengan lebih sempurna.[27]

Hambatan yang Dihadapi dalam Menangani Tindak Pidana Penipuan Siber dengan Modus Operandi Business Email

1. Keterbatasan Hukum Dalam

Tindak pidana penipuan siber dengan modus operandi business email memiliki karakteristik yang berbeda dengan tindak pidana konvensional, sehingga diperlukan ketentuan-ketentuan hukum yang khusus mengatur kejahatan siber ini. Namun, pada

[25] Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik
[26] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[27] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.

kenyataannya, hukum mengenai kejahatan siber masih relatif baru dan belum lengkap, sehingga masih terdapat berbagai kendala dalam menangani tindak pidana penipuan siber.[28]

Salah satu hal yang menjadi kendala adalah belum adanya undang-undang khusus yang mengatur mengenai kejahatan siber dengan modus operandi business email. Kejahatan seperti ini biasanya akan tertangani berdasarkan pasal-pasal yang ada dalam Undang-Undang Informasi dan Transaksi Elektronik, atau Pasal 378 dan Pasal 372 KUHP yang mengatur mengenai penipuan.[29] Padahal, berdasarkan karakteristik kejahatan siber dengan modus operandi business email yang kompleks, diperlukan pemahaman yang lebih mendalam mengenai modus operandi, teknologi, dan data elektronik yang digunakan.[30] Selain adanya perbedaan karakteristik kejahatan siber dengan kejahatan konvensional, kejahatan siber juga bersifat lintas batas wilayah dan lintas yurisdiksi, sehingga seringkali mempersulit proses penegakan hukum. Diperlukan koordinasi antara negara dan lembaga antar negara yang memadai untuk mengatasi kendala ini.[31]

Keterbatasan hukum dalam menangani tindak pidana penipuan siber dengan modus operandi business email masih dirasakan dalam beberapa hal lainnya, antara lain:[32]

1) Belum adanya kesepakatan global mengenai hukum kejahatan siber, sehingga terkadang terjadi perbedaan pendapat antara negara dalam menangani tindak pidana penipuan siber.
2) Undang-undang terkait tindak pidana penipuan siber dengan modus operandi business email pada suatu negara mungkin tidak berlaku di negara lain, sehingga dapat menjadi peluang bagi pelaku kejahatan untuk melarikan diri dari jerat hukum.
3) Kurangnya peran serta industri teknologi dalam membantu menangani tindak pidana penipuan siber. Industri teknologi yang berperan dalam mengembangkan dan menyediakan aplikasi atau sistem yang dapat digunakan untuk melakukan penipuan siber, juga perlu berperan dalam membantu penegakan hukum mengatasi kejahatan tersebut.

[28]Tjandraningsih, I. S. *Tinjauan Yuridis terhadap Kejahatan dalam Dunia Maya (Cybercrime) di Indonesia*.. Jurnal Hukum dan Dinamika Masyarakat, 2018. hal. 13-24.
[29]Jaksa Penuntut Umum, Wawancara.
[30]Korban Penipuan Siber, wawancara.
[31]Handayani, L., & Sumaryadi, A. *Rasionalitas perlindungan data pribadi dalam transaksi elektronik*. Jurnal Hukum dan Peradilan, 2016. hal. 121-129.
[32] Jaksa Penuntut Umum, Wawancara.

4) Adanya kendala dalam mengumpulkan bukti elektronik yang diperlukan dalam penegakan hukum terhadap kejahatan siber. Menangani tindak pidana penipuan siber dengan modus operandi business email juga membutuhkan kemampuan investigasi serta forensik yang memadai untuk mendapatkan bukti elektronik yang cukup kuat agar dapat digunakan dalam proses pengadilan.[33]

Demikianlah beberapa kendala dalam menangani tindak pidana penipuan siber dengan modus operandi business email yang berkaitan dengan keterbatasan hukum.[34]

2. Keterbatasan Teknologi

Selain keterbatasan hukum, dalam menangani tindak pidana penipuan siber dengan modus operandi business email, terdapat hambatan yang berhubungan dengan teknologi. Beberapa hambatan tersebut meliputi :[35]

1) Kemampuan teknologi yang semakin mumpuni yang dimiliki oleh pelaku kejahatan siber. Pelaku kejahatan siber saat ini menggunakan teknologi canggih dan terus-menerus memperbarui modus operandi mereka dengan cepat sehingga lebih sulit bagi penegak hukum untuk menindak mereka.
2) Keterbatasan sumber daya dan anggaran yang dimiliki oleh penegak hukum. Dalam menangani tindak pidana penipuan siber dengan modus operandi business email, diperlukan sumber daya yang memadai seperti perangkat lunak komputer dan alat forensik. Namun, pengadaan sumber daya berkualitas membutuhkan biaya yang besar dan belum selalu bisa diakses oleh semua pihak.[36]
3) Ketergantungan terhadap teknologi untuk pelacakan dan pengumpulan bukti kejahatan. Dalam menangani kejahatan siber, terdapat ketergantungan yang besar pada teknologi, dimana bukti-bukti kejahatan banyak disimpan dalam bentuk digital atau elektronik. Namun, terdapat kendala pada saat pihak berwenang perlu mengajukan permohonan kerja sama pada perusahaan dimana perusahaan tersebut mungkin tidak mengizinkan akses penuh ke dalam sistem mereka.[37]
4) Kurangnya kesadaran teknologi dan siber di kalangan masyarakat. Masyarakat masih jarang menyadari akan pentingnya keamanan cyber dan keterikatan dengan

[33] Kepala Pengadilan Tinggi Banda Aceh.
[34] Jaksa Penuntut Umum, Wawancara.
[35] Jaksa Penuntut Umum, Wawancara.
[36] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[37] Jaksa Penuntut Umum, Wawancara.

pengaturan peraturan yang berlaku. Mereka dapat menjadi sasaran mudah bagi pelaku kejahatan siber.[38]

Demikianlah gambaran tentang keterbatasan teknologi yang dapat menjadi hambatan dalam menangani tindak pidana penipuan siber dengan modus operandi business email.

3. Keterbatasan Sumber Daya

Selain hambatan teknologi dan hukum, keterbatasan sumber daya juga menjadi hambatan dalam menangani tindak pidana penipuan siber dengan modus operandi business email. Berikut adalah beberapa faktor keterbatasan sumber daya yang mempersulit penanganan tindak pidana penipuan siber:[39]

1) Ketersediaan sumber daya manusia yang terampil dalam teknologi keamanan siber dan investigasi cyber masih sangat terbatas. Investasi dalam pelatihan dan rekrutmen sumber daya manusia yang berkualitas dalam bidang cyber security saat ini masih relatif terbatas, sementara penjahat siber terus meningkatkan keahlian mereka.[40]
2) Fasilitas yang memadai seperti perangkat lunak dan alat forensik seringkali mahal dan tidak tersedia secara luas. Tidak semua negara, organisasi atau individu memiliki anggaran yang memadai untuk membeli perangkat teknologi tinggi untuk menggunakan dalam strategi keamanan siber mereka.[41]
3) Pengumpulan bukti di bidang siber membutuhkan biaya yang besar, investigasi cyber melibatkan banyak peralatan dan teknologi, informasi dan juga waktu. Terutama bagi institusi yang memiliki sumber daya yang terbatas, hal ini dapat memperburuk situasi dan menghambat proses hukum.
4) Keterbatasan infrastruktur yang memadai bagi institusi penegak hukum untuk memperkuat keamanan siber. Dalam menangani tindak pidana penipuan siber dengan modus operandi business email, dibutuhkan infrastruktur teknologi seperti perangkat keras dan perangkat lunak canggih, jaringan komunikasi dan sarana prasarana fasilitas fisik lainnya. Namun, biaya mahal, kurangnya akses, atau kurangnya kebijakan publik khusus pada hal tersebut, bisa menjadi kendala.[42]

[38] Jaksa Penuntut Umum, Wawancara.
[39] Jaksa Penuntut Umum, Wawancara.
[40] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[41] Jaksa Penuntut Umum, Wawancara.
[42] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.

5) Keterbatasan adopsi teknologi keamanan siber oleh institusi atau organisasi. beberapa institusi mungkin tidak memiliki anggaran yang cukup untuk mengadopsi teknologi keamanan siber yang memadai guna melindungi sistem informasi mereka dari serangan siber.[43]

6) Kurangnya keamanan dan privasi data dalam pengumpulan bukti elektronik dari individu. Dalam menangani tindak pidana penipuan siber dengan modus operandi business email, seringkali diperlukan pengumpulan bukti elektronik dari individu, namun dalam prosesnya perlindungan data pribadi dalam pengumpulan bukti juga harus terjaga agar tidak terjadi pelanggaran privasi.[44]

7) Kurangnya regulasi dan kebijakan yang memadai dalam mengatasi tindak pidana penipuan siber dengan modus operandi business email. Regulasi dan kebijakan yang belum memadai dapat mempersulit penanganan tindak pidana penipuan siber dengan modus operandi business email dan menyebabkan proses penegakan hukum menjadi lambat.[45]

Integrasi sumber daya tersebut yang seharusnya terjadi dalam penanganan masalah kejahatan siber seperti penipuan siber dengan modus operandi business email, namun terdapat begitu banyak kendala yang harus dihadapi untuk mengatasi keterbatasan sumber daya tersebut. Demikianlah beberapa faktor keterbatasan sumber daya yang dapat mempersulit penanganan tindak pidana penipuan siber dengan modus operandi business email.[46]

4. Kurangnya Kesadaran Masyarakat

Selain tiga hambatan sebelumnya, kurangnya kesadaran masyarakat juga menjadi faktor kunci dalam mempersulit penanganan tindak pidana penipuan siber dengan modus operandi business email. Beberapa faktor yang mempengaruhi kesadaran masyarakat, yaitu:

1) Kebanyakan masyarakat kurang dapat membedakan situasi yang bersifat licik dan manipulatif yang sering digunakan oleh para pelaku kejahatan siber. Terkadang, masyarakat tidak dapat mengetahui ketika mereka sedang menghadapi situasi yang menyebabkan kerugian finansial mereka.[47]

[43] Jaksa Penuntut Umum, Wawancara.
[44] Jaksa Penuntut Umum, Wawancara.
[45] Korban Penipuan Siber, wawancara.
[46] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[47] Jaksa Penuntut Umum, Wawancara.

2) Kurangnya sosialisasi tentang kejahatan siber dengan modus operandi business email yang sering kali dilakukan oleh pihak yang tidak bertanggungjawab dan dapat merugikan banyak pihak. Sosialisasi dan edukasi tentang tindak pidana penipuan siber dengan modus operandi business email perlu dilakukan secara terus menerus sehingga masyarakat lebih mudah mengenali dan menghindari kejahatan tersebut.[48]
3) Adanya kepercayaan yang tidak masuk akal kepada email atau tampilan situs web. Kebanyakan masyarakat masih percaya dan tidak mencurigai email dari sumber yang tidak jelas, yang mengundang mereka untuk membuka atau memberikan informasi pribadi. Mereka juga cenderung tidak memeriksa tampilan situs website atau domain penerima email dan mengambil tindakan yang tidak aman.[49]
4) Kurangnya motivasi untuk memperbarui dan mempertahankan perangkat lunak dan keamanan siber yang sudah ada pada perangkat mereka. Masyarakat masih terkadang enggan untuk memperbarui anti-virus dan melewatkan tindakan-perbaikan, mengabaikan keamanan penggunaan perangkat yang terhubung ke internet.[50]
5) Tidak adanya upaya bersama antara institusi dan masyarakat dalam memperkuat keamanan siber. Kesadaran masyarakat tidak dapat meningkat jika tidak adanya sosialisasi dan edukasi yang benar terkait kejahatan siber dan penanganannya.[51]

Berdasarkan uraian pembahasan ini dapat disimpulkan bahwa penanganan tindak pidana penipuan siber dengan modus operandi business email masih memerlukan banyak peningkatan. Terdapat beberapa kendala dalam menangani kejahatan siber, seperti keterbatasan hukum, teknologi, sumber daya, dan kesadaran masyarakat.[52]

Keterbatasan hukum menjadi kendala utama karena peraturan perundang-undangan yang ada belum menyeluruh mengenai kejahatan siber dengan modus operandi business email. Hal ini menyebabkan pelaku kejahatan siber masih sulit untuk dituntut secara hukum. Keterbatasan teknologi seperti sumber daya dan anggaran juga menjadi kendala karena pihak yang memiliki sumber daya dan kemampuan teknologi akan lebih mudah dalam menangani kejahatan siber. Pelaku kejahatan siber menggunakan teknologi canggih sehingga perlu kuatnya kemampuan teknologi yang dimiliki pihak yang menangani. Keterbatasan sumber

[48] Jaksa Penuntut Umum, Wawancara.
[49] Jaksa Penuntut Umum, Wawancara.
[50] Korban Penipuan Siber, wawancara.
[51] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[52] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.

daya menjadi kendala mempersulit upaya penegakan hukum terhadap tindak pidana penipuan siber dengan modus operandi business email. Penanganan kejahatan siber memerlukan sumber daya manusia, teknologi, dan sarana prasarana yang memadai tapi biaya yang dibutuhkan untuk mengakses itu semua masih sangat mahal.[53]

Kurangnya kesadaran masyarakat yang menjadi faktor utama penyebab dari terjadinya tingkat kejahatan yang tinggi. Masyarakat masih kurang mengenal kejahatan siber, sehingga seringkali menjadi korban penipuan siber.[54]

1. Upaya yang Dapat Dilakukan dalam Pencegahan Tindak Pidana Penipuan Siber dengan Modus Operandi Business Email
   1. Pelatihan dan Edukasi

      Pelatihan dan edukasi merupakan salah satu upaya pencegahan tindak pidana penipuan siber dengan modus operandi business email yang paling efektif. Pelatihan dan edukasi ini dapat dilakukan bagi para karyawan atau pengguna internet maupun bagi publik secara umum. Pelatihan dan edukasi ini bertujuan untuk meningkatkan pengetahuan, kesadaran, dan keterampilan dalam mengenali, mencegah, dan menanggapi tindak pidana penipuan siber dengan modus operandi business email. Beberapa materi yang dapat disampaikan dalam pelatihan dan edukasi antara lain:[55]

      1) Cara mengenali email yang mencurigakan.
      2) Cara memeriksa keaslian email (seperti alamat pengirim email dan isi email).
      3) Cara menanggapi email yang mencurigakan.
      4) Pentingnya tidak mengungkapkan informasi pribadi atau penting lewat email.
      5) Cara menghindari terkena serangan phishing, malware, atau virus melalui email.
      6) Penyampaian dan pemahaman terkait peraturan perundang-undangan yang berkaitan dengan tindak pidana penipuan siber dengan modus operandi business email.

      Hal ini bertujuan untuk menciptakan lingkungan yang lebih aman dan terhindar dari serangan penipuan siber di masa depan. Terkait upaya pertama dalam pencegahan tindak pidana penipuan siber dengan modus operandi business email (yaitu pelatihan dan edukasi), terdapat beberapa hal yang perlu diperhatikan sebagai berikut:[56]

      a. Memastikan bahwa pelatihan dan edukasi tersebut bersifat interaktif dan aplikatif, sehingga dapat memberikan manfaat yang optimal bagi para peserta.[57]

[53] Jaksa Penuntut Umum, Wawancara.
[54] Jaksa Penuntut Umum, Wawancara.
[55] Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
[56] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[57] Jaksa Penuntut Umum, Wawancara.

b. Melakukan pemantauan dan evaluasi terhadap efektivitas dari pelatihan dan edukasi yang telah dilakukan, sehingga dapat diketahui perkembangan tingkat kesadaran serta pemahaman para peserta.[58]
c. Menerapkan peraturan yang bersifat ketat dalam rangka menghindari tindakan yang tidak terkendali yang mungkin saja dapat menyebabkan celah atau peluang bagi pelaku penipuan siber.
d. Melakukan sosialisasi terkait bahaya penipuan siber dengan modus operandi business email dan pentingnya kewaspadaan dalam menggunakan layanan email maupun platform online lainnya. Hal ini dapat dilakukan misalnya melalui media sosial, brosur, atau layanan pemberitahuan internal perusahaan.

Pelatihan dan edukasi yang cukup terkait dengan upaya pencegahan penipuan siber dengan modus operandi business email dapat membantu meningkatkan pemahaman dan kesadaran para pengguna internet di seluruh lapisan masyarakat. Pelatihan dan edukasi akan menjadi lebih efektif bila diikuti dengan menerapkan langkah-langkah pencegahan yang tepat secara konsisten dan disiplin.[59]

2. Sistem Keamanan yang Dapat Diandalkan

Untuk menghindari tindakan penipuan siber melalui modus operandi business email, perusahaan atau pengguna internet dapat menggunakan sistem keamanan yang dapat diandalkan. Beberapa sistem keamanan yang dapat digunakan antara lain adalah:[60]

1) Sistem Firewall: digunakan untuk men-filter lalu lintas data yang masuk dan keluar dari suatu jaringan. Dengan menggunakan sistem firewall yang tepat, maka dapat mencegah data dan informasi penting dari akses yang tidak sah.[61]
2) Sistem Enkripsi: digunakan untuk melindungi data atau pesan yang sedang berada dalam proses pengiriman agar tidak mudah diakses oleh pihak yang tidak berwenang. Dalam penggunaan email, sistem enkripsi dapat menjamin bahwa informasi atau data yang dikirimkan melalui email benar-benar sampai ke penerima yang dituju.[62]
3) Verifikasi Dua Faktor: digunakan sebagai tambahan pengamanan untuk memastikan keamanan password akun email. Saat login, pengguna harus

[58] Jaksa Penuntut Umum, Wawancara.
[59] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.
[60] Kominfo. Infografis: *Keamanan Siber Nasional. Kementerian Komunikasi dan Informatika*. 2017.
[61] Jaksa Penuntut Umum, Wawancara.
[62] Jaksa Penuntut Umum, Wawancara.

memasukkan password dan sejumlah kode yang dikirimkan melalui SMS atau aplikasi keamanan lainnya.[63]

4) Sistem Keamanan dan Antivirus: digunakan untuk mendeteksi dan menghapus malware, virus, atau program jahat lainnya yang dapat merusak sistem atau mencuri informasi penting yang tersimpan pada perangkat pengguna.[64]

Menerapkan sistem keamanan yang dapat diandalkan merupakan langkah penting dalam pencegahan tindak pidana penipuan siber dengan modus operandi business email. Hal ini akan membantu meminimalkan risiko terjadinya aksi penipuan siber dan memastikan bahwa data dan informasi penting terjaga dengan baik. Oleh sebab itu, perusahaan atau pengguna internet perlu mengambil langkah-langkah pencegahan yang tepat dengan memilih sistem keamanan yang sesuai dan mengupdate secara berkala guna menjaga keamanan data dan informasi yang mereka miliki.

3. Verifikasi Identitas Pengirim Email

Dalam menghindari penipuan siber melalui modus operandi business email, penting untuk melakukan verifikasi identitas pengirim email sebelum memberikan informasi penting maupun rahasia. Hal ini dikarenakan seringkali para pelaku penipuan siber menggunakan email yang menyerupai email resmi dari perusahaan atau lembaga tertentu untuk menipu korban.[65]

Beberapa cara yang dapat dilakukan untuk memverifikasi identitas pengirim email, antara lain:[66]

1) Memeriksa alamat email pengirim. Pastikan bahwa alamat email pengirim sesuai dengan perusahaan atau lembaga yang sebenarnya.
2) Memeriksa bahasa dan gaya penulisan email. Perlu dicurigai jika email memiliki bahasa yang berbeda dengan gaya penulisan yang terdapat pada email perusahaan atau lembaga yang sebenarnya.[67]
3) Mencocokkan nama pengirim pada email dengan daftar kontak yang tersimpan pada perangkat.
4) Mengonfirmasi keberadaan pengirim email melalui sumber lain, misalnya melalui telepon atau pesan teks.

[63]Kepala Pengadilan Tinggi Banda Aceh, wawancara.
[64]Yudhanto, H. *Kata kunci penipuan dalam konteks kejahatan siber di Indonesia*. Indonesian Journal of Business and Entrepreneurship, 2019. hal. 154-164.
[65]Korban Penipuan Siber, wawancara.
[66]Kepala Pengadilan Tinggi Banda Aceh, wawancara.
[67]Pusintekkom.. *Pedoman Keamanan Siber untuk Sektor Publik. Kementerian Komunikasi dan Informatika*. 2018.

Dengan melakukan verifikasi identitas pengirim email, maka kita dapat menghindari penipuan yang dilakukan melalui email palsu atau phishing. Penting untuk melakukan verifikasi identitas pengirim email sebelum membalas email ataupun mengirim informasi rahasia, informasi keuangan, atau data-data penting lainnya.

4. Peningkatan Keamanan Fisik

Selain menerapkan sistem keamanan di dalam media online, perlu juga memperhatikan keamanan fisik pada perangkat (komputer/laptop) serta lingkungan kerja di sekitar perangkat. Beberapa hal yang dapat dilakukan antara lain:[68]

1) Mengunci komputer/laptop saat tidak digunakan.
2) Memberikan akses yang terbatas pada perangkat, terutama pada informasi dan data-data penting.[69]
3) Meningkatkan pengawasan akses ruangan untuk mencegah akses yang tidak sah pada perangkat.
4) Menginstall CCTV di dalam ruangan kerja untuk memantau aktivitas yang berlangsung dalam ruangan.[70]
5) Menggunakan sistem keamanan yang dapat mendeteksi kehadiran orang asing dalam lingkungan kerja.

Peningkatan keamanan fisik merupakan upaya pencegahan yang penting dalam melawan tindak pidana penipuan siber dengan modus operandi business email. Hal ini akan membantu menghindari akses yang tidak sah pada perangkat oleh orang yang tidak berwenang serta menghindari potensi penipuan melalui komputer atau laptop yang terhubung ke internet.[71]

Setiap pengguna internet harus selalu mengecek keamanan perangkat dan lingkungan sekitarnya, serta memastikan bahwa prinsip keamanan diterapkan secara konsisten dan disiplin agar tidak menjadi sasaran penipuan siber. Dalam hal ini, upaya pencegahan dengan fokus pada keamanan fisik merupakan upaya yang sangat penting untuk dilakukan secara berkala.[72]

Dalam hal ini dapat disimpulkan bahwa upaya pencegahan terhadap tindak pidana penipuan siber dengan modus operandi business email sangat penting dalam menghindari tindak pidana tersebut. Terdapat empat upaya pencegahan yang dapat dilakukan, yaitu

[68] Kepala Pengadilan Tinggi Banda Aceh, Wawancara, Tanggal 25 Oktober 2024
[69] Jaksa Penuntut Umum, Wawancara, Tanggal 25 Oktober 2024
[70] Jaksa Penuntut Umum, Wawancara, Tanggal 25 Oktober 2024
[71] Jaksa Penuntut Umum, Wawancara, Tanggal 25 Oktober 2024
[72] Jaksa Penuntut Umum, Wawancara, Tanggal 25 Oktober 2024

pelatihan dan edukasi, sistem keamanan yang dapat diandalkan, verifikasi identitas pengirim email, dan peningkatan keamanan fisik. Keempat upaya tersebut dapat membantu mengurangi risiko terjadinya penipuan siber dengan modus operandi business email serta meminimalkan dampak yang ditimbulkan. Dalam penerapan keempat upaya tersebut, penting bagi perusahaan atau pengguna internet untuk menjalankan prosedur-prosedur keamanan secara disiplin dan konsisten guna menghindari celah atau peluang bagi pelaku penipuan siber dengan modus operandi business email.[73]

Dengan penerapan keempat upaya pencegahan, diharapkan dapat membantu mencegah dan mengurangi adanya tindak pidana penipuan melalui modus operandi business email yang sangat merugikan perusahaan, institusi maupun pribadi yang terkena imbasnya.

Kesimpulan

Putusan Nomor: 26 PID.SUS/2023/PT.BNA memberikan kepastian hukum dan panduan bagi penegak hukum dalam mengatasi kasus tindak pidana penipuan siber dengan modus operandi business email. Penanganan tindak pidana penipuan siber dengan modus operandi business email masih memerlukan banyak peningkatan. Terdapat beberapa kendala dalam menangani kejahatan siber, seperti keterbatasan hukum, teknologi, sumber daya, dan kesadaran masyarakat. Upaya pencegahan yang dapat dilakukan, yaitu pelatihan dan edukasi, sistem keamanan yang dapat diandalkan, verifikasi identitas pengirim email, dan peningkatan keamanan fisik. Keempat upaya tersebut dapat membantu mengurangi risiko terjadinya penipuan siber dengan modus operandi business email serta meminimalkan dampak yang ditimbulkan.

Referensi

Buku

Abdul Hamid, Jamalludin. *Kejahatan Siber dalam Perspektif Keamanan Nasional*. Jurnal Ilmu Sosial dan Humaniora, 2015

Alfitra, R. *Lima Modus Penipuan Online Terbanyak dan Cara Menghindarnya*. 2019.

Adan Siber dan Sandi Negara. *Penangkapan Pelaku kejahatan Siber*: Pentingnya Dukungan Masyarakat. 2019

Ahurokhman, M., & Kustiani, I. *Perlindungan Hukum Bagi Konsumen Dalam Transaksi Elektronik*. Jurnal Patofisiologi Indonesia, 2019

[73] Kepala Pengadilan Tinggi Banda Aceh, Wawancara.

Ariefianto, M., & Purnomo, A. *Cybercrime dan Ancaman Terhadap Keamanan Nasional Indonesia*. Jurnal Bina Praja, 2019

Ardi, F. D. *Tinjauan Yuridis terhadap Tindak Pidana Siber*. Jurnal Hukum Novelty, 2016

Akbar, B. *Upaya Polri dalam Penanganan Kejahatan Siber di Indonesia*. Jurnal Kebijakan Dan Manajemen Publik, 2018

Asian Development Bank. *Cybersecurity Resilience: Business Email Compromise*. 2020

Budiono, N. R. *Penanganan Tindak Pidana Penipuan Pembayaran Online Berdasarkan KUHP Dan UU No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik*. Jurnal Adigama, 2019.

Cybersafe Solutions. *Modus Operandi Cybercrime Picik Terbaru*. 2021.

Direktorat Jenderal Aplikasi Informatika. *Panduan Penanganan Kejahatan Komputer*. Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia. 2013

Fauzi, M., & Supriyanto, D. A. *Konsep Deteksi dan Pencegahan Fraud dalam Transaksi Online: Studi Review Literatur*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 2020.

Fahri, H., & Mardhiyah, A. R. *Tindak Pidana Penipuan Dalam Transaksi Online Ditinjau Dari UU No. 11 Tahun 2008 tentang ITE*. Jurnal Penegakan Hukum, 2018.

Ghazali, N. A., Rofiah, A. K., & Mustafa, M. A. *Eksistensi Penipuan Siber dalam Hukum Pidana Indonesia*. Jurnal Yustisia, 2017.

Gunawan, A. A. *Tinjauan Yuridis tentang Tindak Pidana Penipuan Berbasis Teknologi Informasi*. Jurnal Hukum Dan Keadilan, 2019.

Handayani, N. S., & Susilawati, A. *Kejahatan Siber dan Ancaman Hacking pada Industri Keuangan*. Jurnal Ilmu Hukum dan Kenegaraan, 2019.

Handayani, L., & Sumaryadi, A. *Rasionalitas perlindungan data pribadi dalam transaksi elektronik*. Jurnal Hukum dan Peradilan, 2016.

Ilyas, Muhammad. *Cybercrime*. Yogyakarta: Pustaka Pelajar. 2017.

Kominfo. Infografis: *Keamanan Siber Nasional*. Kementerian Komunikasi dan Informatika. 2017.

Kementerian Komunikasi dan Informatika. Pedoman Penanganan dan Penyelesaian Insiden Keamanan Siber. Ditjen Aplikasi Informatika Kementerian Komunikasi dan Informatika. 2018.

Kurniawan, D. D., & Sulistyowati, E. *Regulasi Pemerintah Terhadap Kejahatan Siber*. Jurnal Pendidikan dan Pembelajaran Khatulistiwa, 2018.

Kurniawan, D. D. *Tindak Pidana Kejahatan Siber di Indonesia: Tantangan dan Solusinya*. Perspektif Ilmu Hukum, 2019.

Kementerian Komunikasi dan Informatika. Blue Book Pengungkapan Kejahatan Siber Tahun 2016.

Kementerian Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Standar Keamanan Informasi Sistem Elektronik. (n.d.).

Kusnadi, E., & Suwarto, S. *Penegakan Hukum Terhadap Tindak Pidana Cyber Crime: Studi Kasus Tindak Pidana Penipuan E-Commerce.* Jurnal Yustika, 2019.

Kementerian Komunikasi dan Informatika. *Kejahatan Siber Business Email Compromise (BEC).* 2020.

Kominfo. Frauds Alert: *Modus Operandi Tindak Pidana Penipuan Melalui Media Elektronik (Brute Force Attack) dan Business Email Compromise (BEC).* Kominfo RI. 2020.

Kamaluddin. *Serangan Siber dan Perlindungan Informasi*: Telaah dari Perspektif Undang-Undang Negara. Jakarta: Kreasi Wacana. 2019.

Mahadika, R. *Perlindungan Hukum dan Hukuman atas Kejahatan Siber (Cybercrime).* Jurnal Hukum Respublica, 2020.

Muslihah, H. Dilanda Krisis, *Modus Baru Penipuan di Tengah Pandemi*. Katadata.co.id. 2021.

Mulyono, M. T. *Tindak Pidana Penipuan Dalam Bisnis Online*. Jurnal Hukum dan Pembangunan, 2021.

Mulyadi, A. *Ancaman Keamanan Siber di Indonesia: Tinjauan dari Perspektif Hukum*. Jurnal Hukum dan Pembangunan, 2019.

Mohammad Zulfikar, D. *Tinjauan Yuridis terhadap Ancaman Kejahatan Siber di Indonesia.* Jurnal Penelitian Hukum De Jure, 2019.

Marwana, A. N. *Analisis Hukum terhadap Perlindungan Data Pribadi dalam Transaksi Online Berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Jurnal Ilmu Hukum, 2018.

Mahdiyanti, R., et al. *Business email compromise: Kisah nyata kejahatan siber pada perusahaan (Studi kasus)*. Jurnal Ilmu Komputer & Informasi, 2018.

Masitoh, N., et al. *Analisis kebijakan cybercrime dan penanganannya di Indonesia.* Jurnal Keamanan Nasional, 2019.

Mardani. *Metodologi Penelitian Hukum*. PT Raja Grafindo Persada, 2017.

Naldi, R. *Konstruksi Hukum Terhadap Tindak Pidana Penipuan Dalam Teknologi Komunikasi Dan Informasi*. Jurnal Dinamika Hukum, 2019.

Nurdin. *Penegakan Hukum terhadap Tindak Pidana Penipuan Dalam Sistem Teknologi Informasi.* Jurnal Yustisia, 2019.

Nugraha, A. W. *Perlindungan hukum bagi korban penipuan siber melalui pewarisan digital*. Jurnal Hukum Dan Peradilan, 2020.

Oktavia, D.A., & Sari, R.P. *Kerjasama Antara Sektor Swasta dan Aparat Penegak Hukum dalam Penanganan Tindak Pidana Penipuan Online*. Jurnal Ilmu Kepolisian, 2020.

Putra, I. D. N., & Jamil, A. *Pengaturan Kejahatan Siber dalam Perspektif Hukum Pidana Islam dan Kontemporer*. Qalamuna: Jurnal Pendidikan, Hukum, dan Sosial Keagamaan, 2021.

Pambudi, R. *Analisis Tindak Pidana Penipuan Dalam Dunia Maya (Studi Kasus: Business Email Compromise)*. Jurnal Penegakan Hukum, 2019

Pusintekkom. *Pedoman Keamanan Siber untuk Sektor Publik.* Kementerian Komunikasi dan Informatika. 2018.

Putri, Emiliani. "*Tinjauan Hukum tentang Penipuan dalam Perdagangan Elektronik*". Jurnal Hukum IUS QUIA IUSTUM, 2016.

Rusmana, R., & Alfian, M. *Cyber Crime: Hubungan "Dark Side of The Web" dan Venndiagram dalam Tindak Pidana Penipuan Online.* Jurnal Litera, 2019.

Romadlon, M., & Pratama, A.N.F. *Analisis Faktor-Faktor Penipuan Menggunakan Modus Operandi Business Email Compromise (BEC) pada Karyawan di Kantor Cabang Bank Syariah Mandiri Tahun 2018*. Jurnal Sistem Informasi Bisnis, 2019.

Rachmawati, E., & Hadiyati, E. *Ancaman Cybercrime di Era Adaptasi Kebiasan Baru*. Jurnal RISET Bisnis dan Manajemen (JRBM), 2020.

Rochayati, N. *Penegakan Hukum terhadap Tindak Pidana kejahatan Siber di Indonesia*. Jurnal Pendidikan dan Ilmu Sosial, 2018

Rachmawati, F., Anggana, I.B.W., & Ariyani, F. *Cybercrime Serangan Terbaru di Masa Pandemi Covid-19*. 2020.

Rizky Fitria, A. D. *Cyber Crime dan Ancaman Bagi Keamanan Negara dalam Era Digital*. Journal of Governance and Public Policy, 2017.

Sigit, R. T., & Prihatmoko, S. *Perlindungan Hak Konsumen dalam Transaksi Elektronik di Indonesia*. Jurnal Media Hukum, 2017.

Salampessy, M. M. *Analisis Kejahatan Siber dan Ancaman Bagi Keamanan Negara.* Jurnal Keamanan Nasional, 2019.

Supriyanto, D. A., & Prasetyo, A. *Deteksi dan Pemantauan Keamanan Sistem Informasi pada Kejahatan Siber*. Journal of Information Security and Cybercrimes, 2020.

Sudarma, I. M., & Astuti, D. R. *Penipuan Dalam E-Commerce Dan Hukum Pidana.* Jurnal Ilmu Hukum Gading, 2018.

Sari, W. P. *Masyarakat Harus Aware atas Modus Penipuan Baru*. CNN Indonesia. 2019.

Sembiring, A. B. *Resiko Pencurian Data Pengguna Aplikasi Digital*. SWA.co.id. 2021.

Suryandari, R. *Penggunaan E-Commerce dan Tindakan Kriminal Penipuan Online.* Crimina: Jurnal Hukum dan Peradilan, 2019.

Supatmi, E. *Strategi Pencegahan dan Penanganan Tindak Pidana Penipuan Dalam Jaringan*. Jurnal Perspektif Hukum, 2021

Susilo, R. *Kupas Tuntas Kejahatan Siber dengan Penipuan Online*. Iptek Daerah. 2021.

Santoso, S. *Analisis Kebijakan Cybersecurity dalam Pencegahan Penipuan Siber dengan Modus Business Email Compromise (BEC) di Indonesia*. Jurnal Ilmu Hukum Epistema, 2020.

Sudiro, A. *Polri Tangkap 6 Pelaku Penipuan Online Internasional, dari 2 Juta Korban Raih Keuntungan Rp 9 Triliun*. CNN Indonesia. 2020.

Sari, A., et al. *Analisis Yuridis Atas Putusan No.26 Pid.sus/2023/PT.BNA Terkait Tindak Pidana Penipuan Melalui Internet*. Jurnal Pendidikan Hukum Dan Hukum Pajak, 2021.

Septianto, A. (2020). *Penanganan Tindak Pidana Penipuan Online Dalam Perspektif Hukum Pidana*. Jurnal Hukum IUS QUIA IUSTUM, 2020

Soejono Soekanto, *Penelitian Hukum Normatif*, Jakarta: Raja Grafindo Persada, 1990.

Triatmaja, U. *Penegakan Hukum Terhadap Tindak Pidana Kejahatan Siber Dalam Era Revolusi Industri 4.0*. Jurnal Yudisial, 2017.

Tri Andrisman, *Hukum Pidana*, Universitas Lampung, Bandar Lampung, 2019.

Tjahjono, E. *Hukum Digital Cybercrime dan Penanganannya di Indonesia*. Lex Crimen, 2018.

Tjandraningsih, I. S. *Tinjauan Yuridis terhadap Kejahatan dalam Dunia Maya (Cybercrime) di Indonesia*. Jurnal Hukum dan Dinamika Masyarakat, 2018.

Untung, S. J. *Tinjauan Yuridis tentang Kejahatan Siber dalam Perspektif UU ITE*. Jurnal Hukum dan Keadilan, 2018.

Warnars, H.L., Lumbanraja, P., & Swings, O.S. *Business Email Compromise (BEC): Analisa Kasus dan Aspek Teknis Keamanan Informasi. JOURNALINFO* (Jurnal Informatika dan Teknologi Informasi), 2017.

Wardhana, R. *Imbauan Kepolisian dan Kominfo untuk Waspada Terhadap Modus Penipuan Digital saat Belanja Online*. CNBC Indonesia. 2020

Wibowo, A. S., et al. *Deteksi dan Analisis Modus Operandi Serangan Business Email Compromise (BEC) pada Lembaga Keuangan*. Jurnal Teknologi dan Sistem Informasi, 2020.

Wardana, E. D. Analisis Kejahatan Internet Melalui Modus Penipuan Email Berbahaya di Indonesia. Al-Mazahib: Jurnal Ilmu Syariah dan Hukum, 2019.

Yudhanto, H. *Kata kunci penipuan dalam konteks kejahatan siber di Indonesia*. Indonesian Journal of Business and Entrepreneurship, 2019

Yudanegara, K. *Perlindungan Hukum Bagi Korban Penipuan Siber melalui Email dengan Modus Business Email Compromise*. Jurnal Hukum Ius Quia Iustum, 2019.

Yusnita, N. *Penegakan Hukum Terhadap Penyalahgunaan Teknologi Informasi dan Komunikasi*. Lex Crimen, 2020.

Yuliati, L. *Edukasi Penting dalam Mengatasi Penipuan Online*. Harian Medan Bisnis. 2020.

Yuliawan, R. *Business Email Compromise, Modus Baru Penipuan Online di Indonesia*. AKATIGA Jurnal Sosial dan Politik, 2018.

Website

https://www.linknet.id/article/cyber-crime

Badan Siber dan Sandi Negara: https://www.bssn.go.id/

https://jdih.kominfo.go.id/produk_hukum/undang_undang/5894/uu-no-11-tahun-2008

https://jdih.kemendag.go.id/peraturan-undang-undang-nomor-8-tahun-2010-tentang-perlindungan-konsumen/

Peraturan Undang-Undangan

Undang-Undang Nomor 8 Tahun 2010 tentang Perlindungan Konsumen

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE)

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik ("UU ITE"),

Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2016 tentang Penanganan Insiden Keamanan Informasi di Sektor Telekomunikasi.

Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2016 tentang Penanganan Insiden Keamanan Informasi di Sektor Telekomunikasi.