ANALISIS DAMPAK PANDEMI COVID-19 DITINJAU DARI SUDUT PANDANGKEAMANAN SIBER

Dewi Chirzah[1*], Yuda Arya Wardhana[2]
[1]Program Studi Sains Data, Institut Teknologi Bisnis dan Kesehatan Bhakti Putra Bangsa, Indonesia
[2]Program Studi Informatika, Universitas Perwira Purbalingga, Indonesia
yudaarya@gmail.com[1]*
dewi.chirzah@ibisa.ac.id[2]

ABSTRAK

Dunia digegerkan dengan munculnya sebuah penyakit bernama corona virus infection desease (COVID-19) pada tahun 2019. Setelah empat bulan berlalu virus ini telah berkembang ke negaralain di seluruh dunia termasuk Indonesia. Hal ini memberi dampak bagi kehidupan di setiap penjuru dunia salah satunya adalah dalam sektor keamanan siber. Peningkatan serangan siber mulai dirasakan sejak awal pandemi dan terus berlanjut hingga Juni 2022 dari data yang telah tercatat. Berbagai bentuk serangan siber yang dihasilkan adalah *Spear phishing* dan *email spam, malware, website highjack, website cloning, cyber espionage, dan cyber bullying.* Tujuan dari penelitian ini adalah melakukan analisis serta mendapatkan hasil analisis mengenai dampak yang dihasilkan dari Covid-19 dari sudut pandang keamanan siber. Penelitian ini dilakukan dengan menggunakan metode kualitatif dengan mengumpulkan berbagai macam data yang sesuai dengan topik yang dibahas. Dari data yang telah dianalisis didapatkan poin poin yang berkaitan dengan mengenai dampak pandemi covid-19 ditinjau dari sudut pandang keamanan siber yang diantaranya adalah data kejahatan siber selama pandemi covid-19, Bentuk kejahatan siber selama pandemi covid-19, Upaya pencegahan kejahatan siber, dan serangan siber dimasa yang akan dating.

Kata Kunci: Kejahatan siber. Covid-19, serangan siber

ABSTRACT

The world was shocked by the emergence of a disease called corona virus infection disease (COVID-19) in 2019. After four months, this virus has spread to other countries around the world, including Indonesia. This has an impact on life in every corner of the world, one of which is in the cybersecurity sector. The increase in cyber attacks began to be felt since the beginning of the pandemic and continued until June 2022 from recorded data. Various forms of cyber attacks that are generated are Spear phishing and spam e-mail, malware, highjack websites, website cloning, cyber espionage, and cyber bullying. The purpose of this research is to conduct an analysis and obtain the results of an analysis of the impact resulting from Covid-19 from a cybersecurity perspective. This research was conducted using qualitative methods by collecting various kinds of data according to the topics discussed. From the data that has been analyzed, there are points related to the impact of the Covid-19 pandemic from a cybersecurity point of view, which include cybercrime data during the Covid-19 pandemic, Forms of cybercrime during the Covid-19 pandemic, Cybercrime prevention efforts, and future cyber attacks.

Keywords: *Cybercrime*, Covid-19, *Cyber attack*

PENDAHULUAN

Pada tahun 2019, dunia digegerkan dengan munculnya sebuah penyakit bernama *corona virus infection desease* (COVID-19). Setelah empat bulan dari awal kemunculan di china, virus ini telah berkembang ke negara lain di seluruh dunia termasuk Indonesia. Hal ini memberi dampak bagi kehidupan di setiap penjuru dunia. Dengan kemunculan virus ini, Kemenkes memberi kebijakan kepada masyarakat untuk mengurangi aktifitas diluar rumah dan mengurangi pertemuan dengan orang lain secara langsung. Hal ini membuat kegiatan pertemuan secara tatap langsung diganti menjadi pertemuan secara tatap muka (daring). Kebijakan ini membuat semakin meningkatkan kebutuhan akan teknologi dan informasi selama pandemi COVID-19.

Semakin meningkatnya kebutuhan akan teknologi informasi pada kehidupan membuat berbagai lini kehidupan mendapatkan dampak akan hal tersebut baik itu positif maupun negatif. Tingginya kebutuhan akan teknologi informasi ini membuat munculnya jenis kejahatan melaluiinternet atau yang biasa disebut dengan *Cybercrime.*

Kejahatan mayantara (*cybercrime*) adalah salah satu bentuk atau dimensi baru dari kejahatan masa kini yang diakibatkan oleh perkembangan teknologi yang sangat pesat. Kejahatan ini bahkan sudah menjadi perhatian dunia internasional (Raodia, 2019). Kejahatan Mayantara atau cyber crime inilah salah satu yang menjadi sisi gelap dari kemajuan teknologi dengan memberikan dampak negatif yang sangat luas di segala aspek kehidupan modern saat ini. *Cybercrime* juga mengacu pada aktivitas kriminal pada komputer dan jaringan komputer. Kegiatan ini bisa dilakukan di lokasi tertentu atau bahkan dilakukan antar negara. Kejahatan ini termasuk pemalsuan kartu kredit, penipuan kepercayaan, penyebaran informasi pribadi, pornografi, dan sebagainya. (Utama Siahaan, 2018)

Keamanan Siber merupakan faktor yang sangat penting. Hal ini juga diperkuat dari (Alkhudhayr et al., 2019) yang menyatakan bahwa melindungi informasi perusahaan dan keamanan informasi sangat penting untuk dijaga. Keamanan informasi didefinisikan sebagai melindungi informasi, sistem, dan perangkat keras yangmenggunakan, menyimpan dan mengirimkan informasi, untuk memastikan integritas, kerahasiaan dan ketersediaan data. Hal inilah yang mendorong penulis untuk mengangkat kajian mengenai analisis dampak pandemi covid-19 ditinjau dari sudut pandang keamanan siber

TINJAUAN PUSTAKA

1. *Cyber Security*

   Cyber security adalah aktifitas pencegahan dan pengamanan terhadap sumber daya telematika agar tidak terjadinya kriminalitas di dunia cyber (Cyber Crime) (Rahmawati, 2019). *Cyber security* merupakan upaya upaya yang dilakukan untuk mencegah terjadinya kejahatan *cyber*. Dengan adanya *cyber security* maka resiko akan serangan *cyber* dapat menurun

2. *Cybercrime*

   Pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun

tidak langsung,menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang Chat, email, notice boards dan kelompok) dan telepon genggam (Bluetooth / SMS / MMS) (Gani, 2018).

3. *Cyberspace*

   Menurut KBBI, *cyberspace* adalah ruang informasi dan komunikasi yang terintegrasi dengan internet. *Cyberspace* memungkinkan setiap orang untuk dapat memiliki hak dalam mengekspresikan diri ataupun bersuara dengan melalui sarana aplikasi maupun website yang saling terhubung menggunakan internet. Cyberspace inilah yang menjadi ruang bagi setiap orang untuk dapat saling terhubung satu sama lain.

METODE PENELITIAN

Dalam penelitian kali ini penulis menggunakan metode penlitian kualitatif. Penelitiankualitatif adalah penelitian yang bertujuan untuk memahami fenomena yang dialami peneliti secara deskriptif holistik menurut kata-kata dan bahasa dalam konteks, terutama yang alamiah. (J, 2021). Penelitian ini dilakukan dengan mengumpulkan dan melakukan analisis berbagai datayang berkaitan dengan topik untuk diambil sebuah kesimpulan.

HASIL DAN PEMBAHASAN

Dari beberapa jurnal yang telah penulis dapatkan, penulis membuat *review* mengenai 3 jurnal yang memiliki topik mengenai dampak Covid-19 selama masa pandemi ditinjau dari sudut pandang *cyber security.*

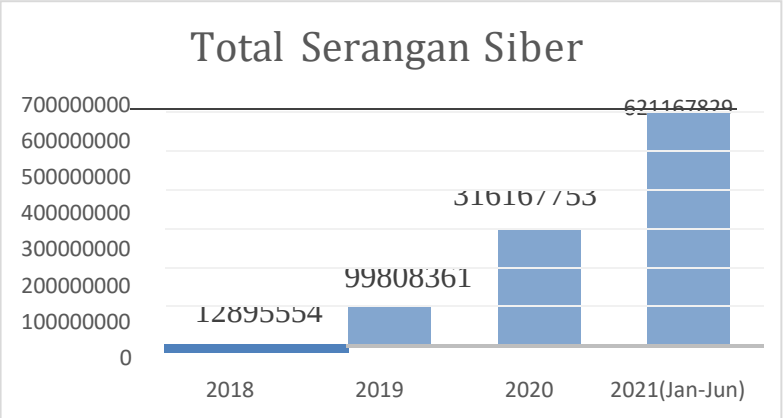
Jurnal pertama berjudul "Analisis Dampak Pandemi Covid 19 di Indonesia Ditinjau dari Sudut Pandang Keamanan Siber". Jurnal ini membahas analisis dampak Covid-19 dari perspektif keamanan siber, jurnal ini juga merinci beberapa serangan siber yang terjadi selama pandemi dan upaya pencegahannya.. Pendidikan tentang pengetahuan keamanan siber sudah menjadi kebutuhan yang utama bagi masyarakat, untuk mengamankan diri-sendiri dari serangansiber (Hadi, M. D. S., Widodo, P., & Putro, 2020)

Jurnal kedua berjudul "Kondisi Ruang Siber Selama Pandemi Covid-19 dan Upaya Mengembangkan Kebijakan Publik di Indonesia". Pada jurnal kedua ini membahas tentang kondisi dunia maya di masa pandemi Covid-19 dan upaya pengembangan kebijakan publik di Indonesia. Tujuan dari penelitian ini adalah untuk memantau secara kritis keadaan dunia maya selama pandemi Covid-19. Metode yang digunakan dalam penelitian ini adalah metode PRISMA (Preferred Reporting Items for Systematic Review and Meta-Analyses). Dari penelitian yang telah dilakukan, didapatkan target serangan, jenis serangan, dan respon beberapanegara terhadap kondisi ruang siber (Irwansyah & Nugroho, 2021)

Jurnal ketiga berjudul "analisis peningkatan jumlah kasus *cyber attack* di indonesia pada masa pandemi covid-19". Jurnal ketiga ini membahas mengenai analisa pada meningkatnya kasus penyerangan siber yang terhitung mulai dari awal bulan 2018 hingga pertengahan 2021 dan membagi menjadi dua segmen yaitu sebelum dan sesudah pandemic Covid-19 (Mulya et al.,2021).

Dari beberapa jurnal diatas, penulis mengambil poin poin yang terkait mengenai dampak pandemi covid-19 ditinjau dari sudut pandang keamanan siber. Berikut adalah poin poin dari ketiga jurnal diatas :

1. Data kejahatan siber selama Pandemi Covid-19



Gambar 1. Grafik Total Serangan Siber

Dari data yang didapatkan dari situs Honeynet report, Total penyerangan siber pertahun terus meningkat mulai dari awal pandemi pada tahun 2020. Penyerangan ini terus meningkat yang pada 2020 mendapatkan 316.167.753 serangan terus meningkat hingga angka 621.167.829 pada tahun 2021 yang terhitung mulai dari januari hingga juni.

2. Bentuk kejahatan siber selama Pandemi Covid-19

Dari penelitian yang dilakukan oleh Okereafor dan Adeliye pada tahun 2020, terdapat 6 bentuk kejahatan siber yang paling banyak dilakukan disaat pendemi diantaranya adalah *Spear phishing* dan *email spam, malware, website highjack, website cloning, cyber espionage,* dan *cyber bullying* (Okereafor & Adelaiye, 2020). Berikut adalah penjelasan lengkap mengenai bentuk kejahatan yang dilakukan selama 4sset444.

No	Jenis Serangan	Bentuk Serangan	Dampak
1	*Spear phising* dan *email spam*	Email yang tidak diminta dan menipu yang meniru merek terkenal dan tokoh terkenal, dengan maksud untuk mengekstrak informasi rahasia atau menyebarkan malware lainnya	• Kebocoran data • Perubahan data • Kehilangan data • Pelanggaran privasi

2	*Malware*	Kode perangkat lunak yang berbahaya dan mengganggu yang menyebabkan kerusakan dan hasil yang tidak diinginkan pada 4 sset 444 atau 4 sset digital korban termasuk akses tidak sah dan perubahan data 4sset 44. Misalnya. Ransomware, virus 4 sset 444 , adware, spyware, worm, trojan, dll.	• Sistem Crash • Pencurian identititas • Kehilangan reputasi • Kehilangan pendapatan • Gangguan layanan • Inefisiensi operasional • Denda • Pengungkapan public • Litigasi • Skandal dan kematian

3	*Website highjack*	Pengambilalihan situs web dengan memperoleh kendali 5 sset 555 rative penuh atas seluruh konten situs web dengan maksud memposting konten yang menyinggung dan propaganda ideologi	• Permintaan tebusan • Konten rusak • Deep fakes • Berita palsu • Skandal • Image smearing • Gangguan layanan • Gangguan pekerjaan • Kehilangan reputasi
4	*Website cloning*	Duplikasi secara 5 sset 55 situs web korban dengan tujuan menipu pengguna dengan mengalihkan permintaan web sah mereka ke situs web 5 sset 55 untuk mendapatkan informasi rahasia untuk mencari keuntungan	
5	*Cyber espionage*	Penggunaan 5 sset 5 online untuk memata-matai perilaku digital atau transaksi online seseorang atau organisasi perusahaan melalui rekayasa 5 sset 5 , spyware, shoulder surfing, cyber stalking, man-in the-middle, brute-force, keylogging, atau metode lain	• Pencurian identitas • Pelanggaran privasi • Image smearing

6	*Cyber bullying*	Penggunaan 5sset digital untuk kejahatan dengan melecehkan atau menyebarkan kebohongan dan konten yang menyinggung terhadap individu, kelompok, atau organisasi perusahaan, dengan bersembunyi di bawah anonimitas platform online, blog, dan forum.	• Skandal • Gangguan individu • Gangguan layanan • Kehilangan reputasi • Libel • Ujaran kebencian

Tabel 1. Bentuk Kejahatan Siber

3. Upaya Pencegahan kejahatan siber

Kejahatan siber merupakan hal yang tidak bisa dihindari dan terus berkembang mengikuti teknologi yang ada. Dibawah ini adalah upaya yang dapat dilakukan sebagai tindak pencegahan terhadap serangan siber.

No	Jenis Serangan	Upaya pencegahan
1	*Spear phising* dan *email spam*	• Intrusion detection • Intrusion prevention
2	*Malware*	
		• Antivirus • Kesadaran keamanan siber • Pelatihan tentang keamanan • Endpoint protection • Perimeter protection • Firewalling • Proper encryption • Steganografi • Machine learning • Anomali detection
3	*Website highjack*	• Proper encryption • Sound Password ethics • Otentikasi bimoterik • Oktentikasi multifactor • Steganografi • Honeypot
4	*Website cloning*	• Publik disclaimer • Corporate damage control • Kesadaran keamanan siber

5	*Cyber espionage*	• Counter espionage • Anti espionage • Perangkat monitoring jaringan • Otentikasi biometric • Sound Password ethics • Kesadaran keamanan siber • Antivirus • Onine ethics • Intrusion detection • Firewalling
6	*Cyber bullying*	• Publik disclaimer • Soundpassword ethics • Kesadaran keamanan siber • Online ethics

Tabel 2. Upaya Pencegahan Kejahatan Siber

4. Serangan siber dimasa yang akan datang

Serangan siber dari tahun ke tahun akan terus meningkat sesuai dengan perkembangan teknologi yang ada saat ini. Semakin canggihnya teknologi yang ada membuat kejahatan siber semakin marak dan kian berkembang. (Hadi, M. D. S., Widodo, P., & Putro, 2020) menjelaskan beberapa tren perkembangan siber yang akan menyerang dimasa yang akan datang :

1) Serangan phising yang lebih maju
2) Serangan yang berasal dari kecerdasa buatan atau AI (*Artificcial Intelegence*)
3) Resiko pada perangkat IoT (Intenet of Think) yang dapat digunakan dalam pencuriandata pribadi

KESIMPULAN

Dari analisis yang telah dilakukan, pandemi Covid-19 merupakan hal yang tidak bisa dipandang sebelah mata. Selain menyerang dari sektor Kesehatan, pandemi Covid-19 ini juga berdampak bagi sektor lain seperti *Cybersecurity*. Terbukti dari data yang didapatkan, kasus penyerangan siber terus meningkat seiring berlangsungnya pandemi mulai dari awal 2018 hingga pertengahan 2021 dengan berbagai macam bentuk serangan. Hal inilah yang membuat perlu adanya kesadaran mengenai keamanan siber dan upaya pencegahan dari serangan siber selama masa pandemi Covid-19 ini berlangsung.

DAFTAR PUSTAKA

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019). Information Security:A Review of Information Security Issues and Techniques. *2nd International Conference on Computer Applications and Information Security, ICCAIS 2019.* https://doi.org/10.1109/CAIS.2019.8769504

B. S. dan S. N. (BSSN) and I. H. P. (IHP). (2019). Laporan Tahunan Honeynet Project BSSNIHP 2019, 2019.

B. S. dan S. N. (BSSN) and I. H. P. (IHP), (2020). Laporan Tahunan Honeynet Project BSSNIHP 2020.

Gani, A. G. (2018). Cybercrime (Kejahatan Berbasis Komputer). *Jurnal Sistem Informasi*, *5*(1).Hadi,

Irwansyah, & Nugroho, R. (2021). Kondisi Ruang Siber Selama Pandemi Covid-19 dan Upaya Mengembangkan Kebijakan Publik di Indonesia. *Jurnal Analis Kebijakan*.

J, M. L. (2021). Metodologi penelitian kualitatif. *Http//Jurnal.Sttsundermann.Ac.Id./Index.Php/Sundermann/Article/View/46/30,*.

M. D. S., Widodo, P., & Putro, R. W. (2020). Analisis dampak pandemi Covid 19 di Indonesia ditinjau dari sudut pandang keamanan Siber. *Jurnal Kebangsaan*, *1*(1).

Mulya, N. B., Pradnyani, K. D. N., Wangi, A. L., Anggi, Nugraha, A., & Rimadhani, T. D. (2021). ANALISIS PENINGKATAN JUMLAH KASUS CYBER ATTACK DI INDONESIA PADA MASA PANDEMI COVID-19. *Prosiding Seminar SITASI*.

Okereafor, K., & Adelaiye, O. (2020). Randomized Cyber Attack Simulation Model: A Cybersecurity Mitigation Proposal for Post COVID-19 Digital Era. *International Journal of Recent Engineering Research and Development*, *5*(7).

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). *Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum*, *6*(2). https://doi.org/10.24252/jurisprudentie.v6i2.11399

Utama Siahaan, A. P. (2018). Pelanggaran Cybercrime Dan Kekuatan Yurisdiksi Di Indonesia. *Jurnal Teknik Dan Informatika*, *5*(1).