KESATRIA: Jurnal Penerapan Sistem Informasi (Komputer & Manajemen)
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 5, No. 2, April (2024), pp. 623-628

# Analisis Keamanan Jaringan dan Perlindungan Data Terhadap Serangan Siber di Perusahaan Luar Sekolah

*Muhammad Mikail Ziyad[1], Suprih Widodo[2]*
*[1,2]Pendidikan Sistem Teknologi Informasi, Universitas Pendidikan Indonesia*
*Kampus Daerah Purwakarta, Indonesia*
*E-mail: [1]muhammadmikailziyad@upi.edu, [2]supri@upi.edu*

***Abstract***

*Threats to vital objects and file security are growing rapidly. Cybercriminals are becoming more cunning and skilled at exploiting security vulnerabilities in digital systems. To improve cybersecurity, a thorough analysis of the threats faced in the digital environment and applicable solutions is required. The aim of this research is to analyze vital objects, identify the main challenges in protecting them from cyber attacks on personal data in Out-of-School companies. The research method uses a qualitative approach using interview and observation techniques. Potential cybercrime threats in Indonesia include hacking, cracking, cyber sabotage and spyware. The risk management process involves identifying, assessing, addressing and controlling risks. To anticipate these threats, technological experts are needed to support the development of advanced national defense systems and establish a cyber security command center.*

***Keywords:*** *cybercriminals, cyberattacks, system*

***Abstrak***

*Ancaman terhadap objek vital dan keamanan file berkembang pesat. Penjahat dunia maya menjadi lebih licik dan terampil dalam mengeksploitasi kerentanan keamanan dalam sistem digital. Untuk meningkatkan keamanan siber, diperlukan analisis menyeluruh terhadap ancaman yang dihadapi di lingkungan digital dan solusi yang dapat diterapkan. Tujuan penelitian ini adalah menganalisis objek vital, mengidentifikasi tantangan utama dalam melindunginya dari serangan dunia maya terhadap data pribadi di perusahaan Luar Sekolah Metode penelitian menggunakan pendekatan kualitatif dengan menggunakan teknik wawancara dan observasi. Potensi ancaman cybercrime di Indonesia antara lain hacking, cracking, cyber sabotage, dan spyware. Proses manajemen risiko melibatkan identifikasi, penilaian, penanganan, dan pengendalian risiko. Untuk mengantisipasi ancaman tersebut, diperlukan tenaga ahli teknologi yang mendukung pengembangan sistem pertahanan negara tingkat lanjut dan mendirikan pusat komando keamanan siber.*

***Kata Kunci:*** *keamanan siber, jaringan, system*

## 1. Pendahuluan

Perkembangan teknologi melesat dengan massif, menebas batas-batas komunikasi dan mengemasnya dalam ruang fleksibel dan efisien bernama virtual. Model komunikasi yang ada dalam ruang virtual, dibangun berdasarkan paradigma simulasi *(simulation)*, banalitas *(banality)*, dan kecepatan *(speed)*, hal itu tentu menjadi sebuah tantangan bagi konsep komunikasi sendiri, baik dalam ruang mayantara ataupun konvenional [1]. Ekses dari perubahan tersebut telak mempengaruhi kehidupan masyarakat terlebih terhadap dunia siber. Patologi kejahatan sangat massif hadir dalam ruang-ruang mayantara. Arus informasi yang terlanjur deras dalam kebebasan ruang siber justru malah menjadi sesak karena kejahatan-kejahatan siber. Berdasarkan riset dari We Are Social, penggunan internet di Indonesia mencapai 202 juta orang atau setara 73,7% penduduk Indonesia [2].

ISSN: 2720-992X

Selain itu, pada bisnis yang berkaitan dengan jaringan Indonesia berada pada urutan ke 2, dari 10 egara pemilik startup terbanyak di Asia. Potensi ancaman *cybercrime* yang telak mengancam antara lain *hacking, cracking, cyber sabotage,* dan *spyware* [3]. Dalam pesatnya perkembangan era digital, objek vital dan pengamanan file menjadi perhatian utama dalam konteks keamanan cyber. Objek vital, seperti infrastruktur kritis, data sensitif, dan sistem penting lainnya, memiliki nilai strategis yang tinggi dan rentan terhadap serangan cyber yang dapat menyebabkan kerugian yang signifikan. Pengamanan file juga menjadi krusial dalam lingkungan digital, karena file-file tersebut sering kali mengandung informasi penting dan rahasia yang harus dilindungi dari akses yang tidak sah. Ancaman terhadap objek vital dan keamanan file semakin berkembang dengan cepat. Penjahat cyber semakin cerdik dan terampil dalam mengeksploitasi celah keamanan dalam sistem digital, termasuk serangan malware, peretasan, dan serangan jaringan yang kompleks. Selain itu, dengan semakin banyaknya data yang dikirim dan disimpan secara elektronik, tantangan dalam mengamankan file juga semakin kompleks. Oleh karena itu, diperlukan analisis mendalam tentang ancaman yang dihadapi dalam lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan keamanan cyber. Studi kasus tentang serangan yang pernah terjadi dan langkah-langkah yang diambil untuk mengatasinya menjadi sangat penting dalam memahami kompleksitas dan tantangan yang dihadapi dalam pengamanan objek vital dan file. Pada penelitian, ini penulis fokus pada Analisis Keamanan Jaringan dan Perlindungan Data Terhadap Serangan Siber di Perusahaan Luar Sekolah.

Penelitian ini menggunakan metode penelitian kuantitatif, Hal yang pertama dilakukan yakni, proses pengumpulan data. Peneliti berusaha memaksimalkan data yang didapat dari ahli siber di perusahaan Luar Sekolah. Proses pengumpulan data dilakukan melalui wawancara, baik secara langsung atau melalui telepon, dan tujuannya adalah untuk mendapatkan pandangan dan pengetahuan ahli tentang jenis-jenis ancaman keamanan cyber yang sering terjadi, teknik yang digunakan oleh penyerang, serta dampak yang ditimbulkan oleh ancaman tersebut yang menganggu stabilitas keamanan siber di perusahaan Luar Sekolah. Observasi dilakukan dengan mengamati perilaku pengguna dalam hal ini Perusahaan Luar Sekolah dalam menghadapi ancaman keamanan cyber di lingkungan digital [4]. Peneliti mengamati bagaimana pengguna berinteraksi dengan perangkat dan aplikasi, tindakan yang mereka lakukan untuk menjaga keamanan data pribadi, serta respon mereka terhadap ancaman yang muncul. Selanjutnya, peneliti melakukan analisis dokumen. Data dikumpulkan dari berbagai sumber terkait seperti laporan keamanan cyber, studi kasus, dan artikel ilmiah yang berkaitan dengan ancaman keamanan cyber dan solusi yang telah diterapkan. Data dari sumber-sumber ini dianalisis[5]. Peneliti melakukan seleksi terhadap data-data yang relevann terkait penelitian. Data yang didapatkan kemudian dianalisis menggunakan teknik analisis konten. Hasil dari analisis tersebut digunakan untuk menjawab pertanyaan penelitian [6].

## 2. Metodologi Penelitian

Keamanan data adalah ilmu pengetahuan dan pembelajaran mengenai metode perlindungan data pada komputer dan sistem komunikasi. keamanandata meliputi beberapa aspek di antaranya privasi (kerahasiaan), *integrity* (konsisten), *authenticity* (keaslian), *availability* (ketersediaan), dan *access control*.

Data adalah keterangan yang benar dan nyata yang dapat dijadikan dasar kajian. Sedangkan pribadi sendiri memiliki arti manusia sebagai perseorangan (diri manusia atau diri sendiri). Sehingga dapat disimpulkan bahwa data pribadi merupakan keterangan yang benar dan nyata yang dimiliki oleh manusia sebaga perseorangan. pasal 1 ayat (1) RUU Perlindungan Data Pribadi memberikan definisi tentang data pribadi yaitu: “data pribadi adalah setiap data tentang seseorang baik yang teridentifikasi dan dapat di identifikasi secara tersendiri atau dikombinasi dengan

informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau non-elektronik".

Adapun jenis data dalam ruu perlindungan data pribadi terdapat dua pengelompokan yaitu data prinadi yang bersifat umum dan yang bersifat spesifik hal ini tertera dalam pasal 3 ayat (1-3) ruu perlindungan data pribadi.

Data bersifat umum meliputi: nama lengkap, jenis kelamin, kewarganegaraan, agama, atau data pribadi seseorang yang dikombinasikan untuk mengidentifikasi seseorang. diterangkan juga dalam *Data Protection Act* inggris tahun 1998 juga menjelaskan bahwa data pribadi adalah data yang berkaitan dengan individu hidup yang dapat diidentifikasi dari data tersebut, atau dari data atau informasi yang sedang atau akan dimiliki oleh pengontrol data.

Selain itu, data pribadi juga dapat dikaitkan dengan karakteristik orang yang diwawancarai, seperti jenis kelamin, umur, nama. Menurut kementerian, data pribadi mengacu pada data pribadi tertentu yang disimpan, dipelihara, dijaga kebenarannya dan dilindungi oleh kerahasiaan. Secara umum, data pribadi memuat fakta tentang seseorang, yaitu informasi yang sangat pribadi yang ingin disimpan oleh orang yang bersangkutan untuk dirinya sendiri dan dibatasi penyebarannya kepada pihak lain atau disalahgunakan oleh orang lain. Secara khusus, data pribadi menggambarkan informasi yang terkait erat dengan seseorang dan membedakan karakteristik setiap orang.

Jenis data yang digunakan dalam penelitian adalah kualitatif. Data kualitatif merupakan data yang disajikan dalam bentuk kata verbal bukan dalam bentuk angka [7]. Di samping itu jika dilihat dari karakteristik masalah berdasarkan kategori fungsinya, penelitian ini termasuk penelitian kepustakaan *(library Reasearch)* [8]. Atau dengan istilah disebut sebagai data deskriptif yaitu data yang digambarkan dengan kata atau kalimat yang dipisahkan berdasarkan kategorisasi untuk mendapat kesimpulan [9]. Proses pengumpulan data dalam penelitian ini yaitu kepustakaan (*Library Research)* yakni penelitian yang sumber kajiannya merupakan bahan-bahan. Buku dan non buku (seperti majalah, surat kabar, dll) dan tujuan penelitiannya yaitu ingin mendapatkan gambaran dan wawasan tentang suatu masalah yang menjadi objek kajiannya [10].

## 3. Hasil dan Pembahasan

### 3.1. Serangan Siber di Perusahaan Luar Sekolah

Berdasarkan data internal perusahaan Luar Sekolah, per tahun 2022 sejumlah serangan siber cukup menganggu dan beberapa kali hampir membuat server Luar Sekolah nyaris down. Kebanyakan serangan menyasar data pribadi pengguna (user). Serangan tersebut sesuai dengan riset yang dikeluarkan Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara (BSSN), bahwa terdapat 741 juta serangan siber sepanjang periode Januari hingga Juli pada tahun 2021. Kejahatan yang paling banyak dilakukan berbentuk percobaan pencurian data (data breach). Pada periode seragan tersebut, tercatat 36.771 akun data telah tercuri, menyasar sektor keuangan dll. Tidak berhenti disana, data yang bocor kurun waktu 2020-2021 justru mencapai 386 juta, kebocoran yang paling banyak dari BPJS Kesehatan yang mencapai hingga 279 juta, dilanjutkan Tokopedia 91 juta, Bukalapak 13 juta, Cermati 2,9 juta, dan KPU 2,3 juta.

Serangan yang menyasar kemanan siber perusahaan Luar Sekolah termasuk pada data yang disuguhkan oleh Pusat Operasi Nasional Badan Siber dan Sandi Negara (BSSN). Signifikansi kejahatan terhadap data pribadi yang terjadi di perusahaan Luar Sekolah tentu sangat merugikan. Para user yang telah terdaftar di perusahaan Luar Sekolah merasa bahwa data yang terhipun dalam ruang siber bernama Luar Sekolah tidak aman dan rentan disalahgunakan.

### 3.2. Penanganan Luar Sekolah Terhadap Serangan Data Siber dan Keamanan Data

Sebagai penyedia layanan siber yang fokus di bidang pendidikan, perusahaan Luar Sekolah tentu berkomitmen dan bertanggungjawab penuh atas keamanan dan kenyamanan privasi para penggunanya. Salah satu masalah hukum yang dapat muncul yakni berkaitan dengan perlindungan data pribadi *(the protection of privacy rights)* [3]. Dalam menangani serangan-serangan siber yang mengancam keamanan data pengguna, perusahaan Luar Sekolah berusaha secara maksimal dan optimal menjalankan langkah-langkah preventif, hal tersebut bersesuaian dengan tegulai pemerintah Indonesia yang diberlakukan kepada seluruh Penyedia Saluran Elektronik (PSE). Pertama, Luar Sekolah tentu mencari talenta *cyber security* yang mumpuni dan mampu untuk menjadi *counter* dari kejahatan-kejahatan yang mudah muncul di Internet. Kedua, Perusahaan Luar Sekolah juga berusaha mengedukasi para penggunannya agar senantiasa *aware* dan terus *upgrading* literasi mengenai keamanan informasi. Eksesnya. adalah menjaga kemanan data pribadi para penggunanya. Adapun langkah-langkah edukasin bagi para pengguna atau klien Luar Sekolah yakni, sbb:

a) Tidak memakai *password* yang mudah ditebak dan mengganti, *passworya* secara berkala,
b) Tidak diperkenankan membuka email atau link yang mencurigakan.
c) Rutin update apabila ada pembaruan.
d) Pelajari hak hukum dan regulasi terkait keamanan data dan privasi.

### 3.3. Regulasi Perlindungan Data di Indonesia

Perlindungan data secara umum pengertiannya mengacu pada praktik, perlindungan, dan aturan mengikat yang diberlakukan untuk melindungi informasi pribadi dan memastikan bahwa subjek data tetap mengendalikan informasinya. Singkatnya, pemilik data harus dapat memutuskan apabila ingin membagikan [11]. beberapa informasi atau tidak, siapa yang memiliki akses, untuk berapa lama, untuk alasan apa. Berdasarkan Pasal 799 Ayat (1) Undang-Undang Nomor 24 Tahun 2013 Tentang Perubahan Atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut UU Administrasi Kependudukan), Pasal 5810 Peraturan Pemerintah Nomor 37 Tahun 2007 Tentang Pelaksanaan Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut PP Administrasi Kependudukan), dan Pasal 26 ayat (1) Undang-Undang No. 19 tahun 2016 Tentang Perubahan Atas Undang Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Selanjutnya disebut UU ITE). Adanya regulasi tersebut secara otomatis mengharuskan adanya sebuah kepastian atas pengelolaan data dan informasi khusunya pada pengelolaan data pribadi karena tanpa dikelolanya data dengan baik dan tepat, maka akan berujung pada penyalahgunaan dan serangan kejahatan siber atau *cybercrime* [12]. Oleh karena itu, dibutuhkan analisis manajemen risiko dalam menghadapi serangan kejahatan siber *cybercrime*. resiko kejahatan siber (cybercrime) berpotensi terhadap kehilangan sistem informasi data, dan menyebabkan sulitnya seseorang dalam mengatasi masalah tersebut [13]. Hal ini disebabkan belum adanya lembaga atau penegak hukum yang bisa memproses itu. Kejahatan terhadap penyalahgunaan data pribadi seseorang sering kali ditemukan pada sebuah perusahaan, karena tidak mengetahui bagaimana data tersebut dikelola dan diamankan secara tepat [14].

Selain itu, Indonesia Data Protection System (IDPS) merupakan sebuah sistem yang mampu meminimalisasi kejahatan siber khususnya pada penyalahgunaan data dan informasi pribadi. Sistem ini bekerja untuk mengamankan data pribadi sesorang pada central data atau pusat pengumpulan data, selain itu IDPS juga memastikan pengelolaan data dan informasi sesorang dikelola dengan tepat, dengan adanya sebuah koordinasi dari sistem ini. Berikut adalah bagan mengenai kerja IDPS

sebagai sebuah sistem. Sistem IDPS ini dilekatkan kepada Kementerian Komunikasi dan Informatika (Kominfo) yang dimana IDPS mempunyai dua unsur yang sangat penting atau urgent, yaitu central data atau data authority serta data officer. Central data atau data authority fungsinya adalah untuk mengumpulkan dan mengamankan setiap data dan informasi pribadi yang masuk dari data officer, maka dari itu data officer ditempatkan pada seluruh perusahaan dan instansi pemerintahan yang melakukan pengelolaan data dan informasi pribadi agar lebih mudah untuk melakukan koordinasi terkait dengan data dan infromasi pribadi yang dimiliki seseorang. Central data atau data authority merupakan tempat ataupun pusat penyimpanan data dan hanya dikelola oleh orang yang memiliki kewenangan untuk melakukan pengelolaan data dan infromasi pribadi tersebut, central data juga harus memiliki kemanan yang sangat ketat karena merupakan tempat utama penyimpanan data.

Sedangkan data officer merupakan orang-orang yang mempunyai kewenangan dan keahlian yang ditunjuk oleh central data atau data authority untuk melakukan pengelolaan data dan informasi pribadi pada setiap perusahaan dan instansi pemerintah, yang kemudian dalam pekerjaannya ini harus melakukan koordinasi tentang pengelolaan data dan informasi pribadi yang dikelola sekali dalam 24 jam, agar central data mempunyai informasi yang up to date terhadap pengelolaan data pribadi oleh perusahaan dan instansi pemerintah. Melihat pekerjaan yang sangat sulit oleh seseorang data officer, maka dari itu harus memiliki kualifikasi tersendiri agar sumber daya manusia yang bekerja sebagai data officer adalah orang-orang yang berkompeten dan seseorang yang professional, orang-orang yang bekerja dalam bidang privasi dan perlindungan data harus memiliki keahlian yang sama baik dalam hukum dan teknologi keamanan siber untuk membantu perusahaan dan instansi pemerintah mengatur penyimpanan, pemrosesan, serta perlindungan data digital yang sesuai dengan undang-undang.

## 4. Kesimpulan

Hasil dari penelitian ini yang berjudul, “Analisis Keamanan Jaringan dan Perlindungan Data Terhadap Serangan Siber di Perusahaan Luar Sekolah. Menghasilkan beberapa catatan terhadap mekanisme perusahaan Luar Sekolah dalam menjalan keamanan data dari serangan siber. Untuk internal, penangannnya berfokus pada talenta *cyber security* yang mampu menagani apabila terjadi kebocoran data karena hal apapun. Namun, alangkah lebih baik apabila *programmer* yang membuat mekanisme digital yang melibatkan penyelenggaraan medium Luar Sekolah juga harus orang yang bisa mengantisipasi dalam proses *coding*nya. Kemudian, selain itu beberapa persoalan regulasi juga masih belum *clear*. Terlebih undang-undang yang ada masih tumpang tindih, dan peraturan turunannya cenderung tidak komprehensif. Akibatnya, implementasi penanganan dan penegakan hukum bagi para perlaku kejahatan siber tidak berjalan secara optimal. Terakhir, SDM kita juga masih minim sadar dan *awarei*. Hal tersebut tentu karena tingkat literasi media dan keamanan informasi bagi public masih sangat rendah.

## Daftar Pustaka

[1] Y. A. Piliang, “Posmodernisme Dan Ekstasi Komunikasi,” *Mediator: Jurnal Komunikasi*, Vol. 2, No. 2, 2001.

[2] S. Kemp, “Digital 2021: The Latest Insights Into The ‘State Of Digital’ - We Are Social Uk.” Accessed: Mar. 01, 2024. [Online]. Available: Https://Wearesocial.Com/Uk/Blog/2021/01/Digital-2021-The-Latest-Insights-Into-The-State-Of-Digital/

[3] N. W. Sari, "Kejahatan Cyber Dalam Perkembangan Teknologi Informasi Berbasis Komputer," *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum Dan Keadilan*, Vol. 5, No. 2, Pp. 577–593, 2018.
[4] J. W. Creswell And J. D. Creswell, *Research Design Qualitative, Quantitative, And Mixed Methods Approaches*, No. 2. Sage, 2004. [Online]. Available: Https://Eur-Lex.Europa.Eu/Legal-Content/Pt/Txt/Pdf/?Uri=Celex:32016r0679&From=Pt%0ahttp://Eur-Lex.Europa.Eu/Lexuriserv/Lexuriserv.Do?Uri=Celex:52012pc0011:Pt:Not
[5] Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif, Dan R&D ( 2nd Ed)*. 2019.
[6] P. A. Adler, *The Sage Handbook Of Qualitative Research*, 5th Ed. Sage, 1994.
[7] N. Muhadjir, *Metodologi Penelitian Kualitatif*, 3rd Ed. Rakesarasin, 1996.
[8] S. Azwar, *Metode Penelitian*. Pustaka Pelajar, 1998.
[9] S. Arikunto, *Prosedur Penelitian*. Pt. Rineka Cipta, 2016.
[10] A. H. Hanafi, *Metodologi Penelitian Bahasa: Untuk Penelitian, Tesis, Dan Disertasi*. Diadit Media Press, 2011.
[11] L. Siagian, A. Budiarto, And Simatupang, "The Role Of Cyber Security In Overcome Negative Contents To Realize National Information Resilience," *Jurnal Peperangan Asimetris*, Vol. 4, No. 3, Pp. 1–18, 2018.
[12] I. Rahmawati, "The Analysis Of Cyber Crime Threat Risk Management To Increase Cyber Defense," *Jurnal Pertahanan Dan Bela Negara*, Vol. 7, No. 2, Pp. 55–70, 2017, [Online]. Available: Https://News.Detik.Com/
[13] M. A. Lingga And B. P. Jatmiko, "Penyalahgunaan Data Pribadi Konsumen Sudah Masuk Katagori Gawat Darurat." Accessed: Mar. 01, 2024. [Online]. Available: Https://Money.Kompas.Com/Read/2019/07/27/201200426/Penyalahgunaan-Data-Pribadi-Konsumen-Sudah-Masuk-Katagori-Gawat-Darurat#Google_Vignette
[14] D. Napitupulu, "Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional," *Deviance Jurnal Kriminologi*, Vol. 1, No. 1, Pp. 100–113, 2017.