Madani: Jurnal Ilmiah Multidisiplin
Volume 1, Nomor 11, December 2023

E-ISSN: 2986-6340
DOI: https://doi.org/10.5281/zenodo.10371686

Tantangan Dalam Menjaga Keamanan Data *Official Statistics* dari Serangan *Cybercrime*

Fikri Surahman[1]
[1]Program Studi D-III Statistika, Politeknik Statistika STIS, Indonesia
e-mail: 112212611@stis.ac.id

Abstrak

Dalam era digital yang semakin maju saat ini, keamanan data telah menjadi permasalahan yang mendesak dan kompleks. Artikel ini bertujuan untuk mengkaji tantangan dalam menjaga keamanan data *Official Statistics* dari serangan *cybercrime*, serta memberikan wawasan tentang pendekatan yang dapat digunakan untuk menghadapi permasalahan ini. Serangan siber yang semakin canggih menjadi tantangan utama dalam menjaga keamanan data, dengan penyerang menggunakan metode yang rumit seperti *malware*, *ransomware*, dan serangan *phishing*. Peningkatan jumlah kejadian kebocoran data juga menjadi masalah signifikan yang dapat menyebabkan kerugian finansial dan melanggar privasi individu. Selain itu, kekurangan kebijakan dan regulasi yang memadai serta tren penggunaan teknologi seperti kecerdasan buatan dan pembelajaran mesin dalam meningkatkan keamanan data juga perlu diperhatikan. Integrasi solusi keamanan terbaru, pelatihan pegawai, dan pengembangan kebijakan yang komprehensif menjadi langkah-langkah penting dalam meningkatkan keamanan data.
Kata kunci: *keamanan data, serangan siber, malware, ransomware, phising.*

Article Info
Received date: 28 November 2023 Revised date: 3 December 2023 Accepted date: 10 December 2023

PENDAHULUAN

Seiring dengan perkembangan teknologi informasi yang kian pesat, keamanan data menjadi permasalahan yang sangat mendesak dan kompleks untuk dibahas. Ledakan data dan pertukaran informasi yang cepat membuat tantangan dalam menjaga keamanan data *official statistics* dari serangan *cybercrime* menjadi semakin rumit.

Pada tahun 2023, kasus kebocoran data sangat menjamur di berbagai instansi kementerian di Indonesia. Pada instansi Dukcapil, kebocoran data mencapai 337 juta data. Kejadian tersebut dapat menyebabkan menurunnya reputasi suatu instansi, kerugian finansial yang serius, serta melanggar privasi individu.

Dalam melakukan peretasan data, penyerang menggunakan berbagai metode serangan siber. Serangan siber yang kerap dipakai penyerang, seperti *malware*, *ransomware*, dan serangan *phishing* untuk mencuri data atau merusak sistem. Selain tantangan di atas, kurangnya kebijakan dan regulasi yang memadai oleh pemerintah menjadi tantangan lain dalam menjaga keamanan data. Oleh karena itu, tujuan dari artikel ini yaitu membahas pendekatan yang dapat diambil dalam menjaga keamanan data *official statistics* dari serangan *cybercrime* serta pengembangan kebijakan dan regulasi yang dapat dilakukan oleh pemerintah dalam menjaga keamanan data *official statistics* dari serangan *cybercrime*.

METODE

Penelitian ini menggunakan metode studi literatur (Studi Kepustakaan) suatu bentuk penelitian yang fokus pada telaah dan analisis literatur yang relevan dengan topik atau masalah penelitian tertentu. Tujuan dari kajian literatur adalah untuk memahami perkembangan pengetahuan dan temuan-temuan terkait dalam literatur yang telah ada, serta untuk mengidentifikasi celah

pengetahuan yang mungkin dapat diisi dengan penelitian lebih lanjut. Kajian literatur dapat dilakukan sebagai bagian dari tahap perencanaan penelitian atau sebagai penelitian mandiri (Sugiono, 2018).

HASIL DAN PEMBAHASAN

Menurut Murti (2005), *Cybercrime* adalah istilah yang digunakan untuk aktivitas kriminal yang melibatkan penggunaan komputer dan jaringan komputer sebagai alat untuk melakukan kejahatan. Aktivitas yang dapat dikategorikan sebagai aktivitas *cybercrime* terdiri dari:

1. Melancarkan *Denial of Service Attack / DOS Attack*

Denial of Service Attack / DOS Attack adalah serangan terhadap suatu sistem atau layanan dengan tujuan membuatnya tidak tersedia bagi pengguna yang sah. Serangan ini dilakukan dengan cara membanjiri sumber daya sistem, seperti *bandwidth*, kapasitas memori, atau daya pemrosesan, sehingga sistem tidak dapat menjalankan fungsinya dengan baik atau bahkan menjadi tidak responsif. *DOS Attack* dapat menyebabkan penurunan kinerja sistem atau, dalam kasus ekstrem, membuatnya sepenuhnya tidak dapat diakses.

2. *Hacking*

Hacker adalah sebutan bagi seseorang yang mempunyai keahlian dan pemahaman yang mendalam dalam bidang komputer dan teknologi informasi. *Hacker* yang menggunakan keterampilannya untuk tujuan etis dan konstruktif disebut sebagai *White Hat Hacker*, sedangkan hacker yang menggunakan keterampilannya untuk tujuan ilegal dan merugikan disebut sebagai *Black Hat Hacker*.

3. Menulis dan menyebarkan Virus */ Trojan Horse*

Virus komputer adalah program komputer yang dirancang untuk menyisipkan diri ke dalam program atau file lain, dan dapat menyebar dari satu komputer ke komputer lainnya. Virus komputer digunakan untuk merusak atau mengganggu kinerja sistem komputer. Saat ini seseorang tidak perlu lagi mempelajari program untuk menciptakan virus komputer karena telah tersedia program yang dirancang untuk memperoleh virus, contoh programnya yaitu *VBS Worm Generator*.

Trojan Horse adalah jenis perangkat lunak berbahaya yang menyusup ke dalam sistem atau program dengan menyamar sebagai sesuatu yang sah atau berguna, tetapi sebenarnya memiliki tujuan yang merugikan atau merusak. Nama *Trojan Horse* diambil dari mitologi Yunani, yaitu ketika pasukan Yunani menyembunyikan diri di dalam patung kuda kayu besar untuk menyerang kota Troya. Cara kerja *Trojan Horse* yaitu suatu program yang mempunyai kode-kode program yang berbahaya akan menyamar sebagai program yang sehat. Apabila program yang berisi kode-kode program berbahaya tersebut dijalankan akan mengakibatkan sistem operasi komputer sehingga si pengirim *Trojan Horse* bisa masuk ke sistem operasi komputer dan melancarkan berbagai tindakan yang diinginkan.

4. *Cyberterrorism*

Cyberterrorism adalah istilah yang merujuk pada penggunaan teknologi komputer, terutama serangan siber, untuk melakukan tindakan teroris. Serangan ini bertujuan merusak, mengancam, atau memengaruhi keamanan suatu negara atau kelompok dengan cara yang mirip dengan serangan teroris konvensional. *Cyberterrorism* melibatkan pemanfaatan teknologi informasi dan jaringan komputer untuk menyebabkan ketakutan, kerusakan, atau kekacauan.

5. *Fraud* dan Pencurian Identitas / *Phishing*

Phishing adalah jenis serangan keamanan informasi yang terjadi saat penyerang berusaha memperoleh informasi pribadi atau sensitif dengan menyamar sebagai entitas terpercaya. Umumnya, serangan *phishing* dilakukan melalui *email*, pesan teks, atau situs web palsu yang dirancang sedemikian rupa sehingga tampak sah. Penyerang *phishing* sering kali mencoba memikat korban dengan menyajikan informasi palsu atau menyamar sebagai entitas yang dikenal, seperti bank, perusahaan, atau penyedia layanan *online*. Penyerang dapat meminta korban untuk memberikan informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya.

Kebijakan dan Regulasi dalam Keamanan Data *Official Statistics*

Di Indonesia, kebijakan dan regulasi keamanan data menjadi fokus penting dalam menghadapi era digital yang berkembang pesat. Pemerintah Indonesia telah menetapkan serangkaian aturan untuk melindungi keamanan dan privasi data pengguna. Salah satu regulasi utama adalah

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE), yang memberikan dasar hukum bagi perlindungan data elektronik. Selain itu, pada tahun 2016, pemerintah juga mengeluarkan Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengatur tata cara keamanan sistem dan transaksi elektronik.

Selain regulasi tersebut, Indonesia juga menjadi salah satu negara yang mengadopsi *General Data Protection Regulation* (GDPR) versi lokal, yaitu Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Regulasi ini menetapkan standar perlindungan data pribadi dan menekankan pentingnya pengelolaan data dengan memperhatikan prinsip transparansi, keterbukaan, serta hak privasi individu.

Menurut Murti (2005), meskipun Indonesia telah mengambil langkah-langkah positif dalam mengembangkan kebijakan dan regulasi untuk menjaga keamanan data, masih ada beberapa kekurangan yang perlu diperhatikan, antara lain:

1. Implementasi regulasi seringkali belum optimal. Meskipun ada peraturan yang mengatur keamanan data, keterbatasan sumber daya manusia, teknologi, dan pemahaman yang cukup dapat menghambat pelaksanaannya secara menyeluruh.
2. Selanjutnya, kebijakan yang ada belum sepenuhnya memadai untuk mengatasi dinamika cepat dunia digital. Perkembangan teknologi informasi yang pesat memerlukan kebijakan yang dapat terus beradaptasi dan merespon perubahan dengan cepat. Oleh karena itu, perlu upaya berkelanjutan untuk melakukan revisi dan penyempurnaan regulasi guna tetap relevan dengan perkembangan teknologi terkini.
3. Ketidakjelasan dan ketidaktegasan dalam beberapa aspek regulasi juga menjadi kendala. Hal ini dapat menciptakan kebingungan di kalangan bisnis dan masyarakat terkait dengan kewajiban dan tanggung jawab mereka terhadap keamanan data. Kekurangan ini memerlukan penyelarasan dan klarifikasi lebih lanjut untuk memastikan pemahaman yang lebih baik dan kepatuhan yang efektif.
4. Di samping itu, perlu adanya mekanisme penegakan hukum yang lebih kuat untuk memastikan kepatuhan terhadap regulasi keamanan data. Tanpa sanksi yang tegas dan diberlakukan secara konsisten, regulasi tersebut mungkin tidak efektif dalam menciptakan dampak yang diinginkan.

Dalam mengatasi kekurangan ini, pemerintah dan pemangku kepentingan terkait perlu bekerja sama untuk terus meningkatkan kebijakan dan regulasi keamanan data. Pembaharuan yang berkelanjutan, peningkatan kapasitas, dan sinergi antara sektor publik dan swasta dapat membantu menciptakan lingkungan digital yang lebih aman dan terpercaya di Indonesia.

Pendekatan yang Dapat Dilakukan dalam Menjaga Keamanan Data *Official Statistics* dari Serangan *Cybercrime*

Menurut Sari dkk. (2020), pendekatan yang dapat dilakukan untuk meningkatkan keamanan data *Official statistics* dari serangan *cybercrime* antara lain :

1. Integrasi solusi keamanan data *Official statistics* terbaru. *Official statistics* harus menerapkan dan mengintegrasikan solusi keamanan terbaru yang relevan untuk melindungi data mereka. Hal ini mencakup penggunaan firewall, enkripsi data, solusi deteksi ancaman, keamanan jaringan, dan teknologi lainnya untuk melindungi data dari berbagai serangan dan ancaman.
2. Pelatihan karyawan untuk meningkatkan kesadaran keamanan data *Official statistics*. Pelatihan karyawan tentang praktik perlindungan data *Official statistics* yang baik sangatlah penting. Karyawan harus mendapat informasi lengkap tentang risiko keamanan, taktik serangan yang umum, dan tindakan yang dapat mereka ambil untuk melindungi data *Official statistics*. Hal ini mencakup kebijakan kata sandi yang ketat, kesadaran terhadap *phishing* dan serangan sosial, serta praktik keamanan data yang baik.
3. Pengembangan kebijakan dan peraturan yang komprehensif. Pemerintah dan *Official Statistics* harus bekerja sama untuk mengembangkan kebijakan dan peraturan keamanan data yang komprehensif. Undang-undang perlindungan data pribadi yang kuat dan terkini perlu dikembangkan dan ditegakkan. Peraturan ini harus mencakup persyaratan perlindungan data pribadi, mengatur perlindungan terhadap serangan siber, dan menetapkan standar keamanan yang diperlukan.

4. Melakukan audit keamanan secara teratur. *Official Statistics* harus secara teratur melakukan audit keamanan data untuk memeriksa kerentanan sistem dan infrastruktur mereka. Audit ini mencakup pengujian keamanan, mengidentifikasi kerentanan keamanan, dan menerapkan tindakan perbaikan yang diperlukan untuk memastikan keamanan data yang optimal.
5. Mengadopsi praktik pengelolaan resiko. Pendekatan manajemen risiko membantu *Official Statistics* mengidentifikasi potensi ancaman, menilai dampaknya, dan mengambil tindakan yang tepat untuk memitigasi risiko tersebut. Dengan menerapkan praktik manajemen risiko yang baik, *Official Statistics* dapat meningkatkan keamanan data secara proaktif dan holistik.
6. Membangun budaya keamanan data. Penting untuk membangun budaya keamanan data yang kuat di seluruh aspek *Official Statistics*. Hal ini termasuk mengintegrasikan keamanan data ke dalam seluruh aspek operasional dan keputusan bisnis. Budaya keamanan yang kuat mendorong individu untuk secara proaktif memprioritaskan keamanan data dan mengambil langkah-langkah yang diperlukan untuk melindungi data *Official Statistics*.

Pendekatan holistik dan kombinasi langkah-langkah ini dapat meningkatkan keamanan data *Official Statistics* secara menyeluruh. Penting untuk menyadari bahwa keamanan data *Official Statistics* adalah tanggung jawab bersama antara pemerintah, organisasi, dan individu.

SIMPULAN

Kejahatan Siber (*Cybercrime*) yang semakin canggih merupakan tantangan utama dalam menjaga keamanan data di era digital saat ini. Kegiatan *Cybercrime* mencakup serangan *Denial of Service Attack/DOS Attack, Hacking,* menyebarkan Virus*/Trojan Horse, Cyberterrorism,* dan *Fraud dan Pencurian Identitas/Phishing.* Dibutuhkan langkah-langkah yang kuat dan proaktif untuk melindungi data *Official Statistics* dari serangan *cybercrime*. Kurangnya kebijakan dan peraturan keamanan data di Indonesia merupakan masalah serius. Kurangnya perlindungan privasi, peraturan yang tidak memadai, kurangnya penegakkan hukum, dan kurangnya kesadaran dan pemahaman merupakan hambatan terhadap perlindungan data *Official Statistics* dari serangan *cybercrime*. Diperlukan komitmen yang kuat dari pemerintah untuk membentuk kebijakan dan regulasi keamanan data di Indonesia agar masalah ini dapat terselesaikan. Pendekatan untuk meningkatkan keamanan data *Official Statistics* mencakup integrasi solusi keamanan terkini, pelatihan karyawan untuk meningkatkan kesadaran keamanan, pengembangan kebijakan dan peraturan yang komprehensif, dan kolaborasi antara pemerintah dan organisasi.

Referensi

Basyari, Iqbal. 2023. “Kemendagri Investigasi Dugaan Kebocoran 337 Juta Data Dukcapil”, https://www.kompas.id/baca/polhuk/2023/07/17/337-juta-data-dukcapil-diduga-bocor. (04/12/2023).

Murti, H. (2005). Cybercrime. Jurnal Teknologi Informasi DINAMIK, 10(1). 37-39.https://media.neliti.com/media/publications/242903-none-e99410f2.pdf.

Sari, Ika Yusnita., Muttaqin., Jamaludi., Simarmata, Janner., Rahman, M. Arif., Iskandar, Akbar., Pakpahan, Andrew Fernando., Karim, Abdul., Sugianto., Giap, Yo Ceng., Hazriani., Yendrianof, Devi., Manullang, Sardjana Orba. (2020). *Keamanan Data & Informasi*. Yayasan Kita Menulis. http://repo.handayani.ac.id/id/eprint/147.

Sugiono. (2018). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta