
2025
14 – 20 April 2025
HASHCAT
SOCUD
ATTACK
Kamsib Indonesia
on Paper
Edisi 11
Tetap Aman
Bersama Kamsib
Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

Kamsib Indonesia on Paper

Edisi 11
14 – 20 April 2025

'Data is the new oil'
- Clive Humby

Keamanan Siber sebagai Alat dalam Konflik Politik Global

Penulis: **Anton Lepari**

Spionase siber (*cyber espionage*) adalah salah satu praktik yang semakin sering digunakan oleh negara-negara untuk memperoleh informasi yang bersifat sensitif, baik itu dalam konteks politik, militer, atau ekonomi. Dalam dunia yang semakin terkoneksi secara digital, serangan siber menjadi alat yang efektif untuk mendapatkan data strategis, yang tidak hanya mengancam keamanan informasi, tetapi juga bisa mengubah dinamika hubungan internasional dan kebijakan politik global.

Hal ini selaras dengan perkataan Jokowi, *"Data ini adalah jenis kekayaan baru. Saat ini data adalah new oil, bahkan lebih berharga dari minyak. Data yang valid menjadi salah satu kunci pembangunan,"* pada Jumat, 24 Januari 2020 di Istana Negara, Jakarta. Lebih mengkerucut lagi ke arah keamanan siber, Presiden Prabowo Subianto memberikan arahan dalam penguatan keamanan siber nasional melalui kebijakan CSIRT.

Penting untuk dicatat bahwa spionase siber tidak selalu melibatkan serangan langsung yang terdeteksi. Taktik yang digunakan bisa sangat halus, mulai dari pengintaian data lewat peretasan server hingga infiltrasi jaringan untuk mengakses informasi pribadi dan sensitif. Oleh karena itu, artikel ini akan mengulas praktik spionase siber dalam konteks geopolitik modern, memberikan contoh serangan terkini, serta menggali implikasi dari serangan ini terhadap hubungan antarnegara dan kebijakan keamanan.

Definisi dan Bentuk-bentuk Spionase Siber

Spionase siber mengacu pada kegiatan mata-mata yang dilakukan melalui dunia maya, di mana aktor yang terlibat berusaha memperoleh informasi yang dilindungi secara ilegal. Ini dapat mencakup data pribadi, dokumen politik, atau informasi militer yang sensitif. Dalam beberapa kasus, spionase siber bertujuan untuk merusak sistem pertahanan negara lawan atau untuk mengeksploitasi kelemahan dalam struktur pemerintahan mereka.

Ada beberapa bentuk utama dari serangan spionase siber, di antaranya:

- ***Phishing* dan *spear phishing***: Teknik ini digunakan untuk menipu individu atau organisasi agar memberikan akses ke sistem mereka, sering kali dengan cara yang sangat terfokus dan personal.

- **Akses langsung ke infrastruktur kritikal**: Aktor negara dapat mencoba untuk meretas infrastruktur penting, seperti jaringan listrik, telekomunikasi, atau sistem militer.
- ***Spyware* dan *malware***: Perangkat lunak berbahaya digunakan untuk menyusup ke dalam sistem dan mencuri data penting.

Ada banyak contoh kejadian yang diindikasikan ataupun terbukti sebagai serangan spionase siber yang bisa kita ingat kembali. Beberapa contohnya adalah serangan malware terhadap fasilitas nuklir milik sebuah negara, peretasan produk perangkat lunak dan infrastruktur jaringan, hingga dugaan penyadapan terhadap petinggi negara.

Dampak Spionase Siber terhadap Hubungan Internasional

Serangan siber yang dilakukan dengan tujuan spionase dapat memiliki dampak yang jauh lebih luas daripada hanya sekedar kerugian ekonomi atau kebocoran data. Mereka sering kali memengaruhi hubungan antarnegara dan menambah ketegangan dalam politik global.

Ada banyak dampak spionase siber yang bisa kita tinjau. Ketika sebuah negara terlibat dalam spionase siber terhadap negara lain, hal itu dapat merusak hubungan diplomatik dan memperburuk ketegangan antara negara-negara tersebut. Negara-negara yang merasa terancam sering kali merespons dengan meningkatkan kemampuan serangan dan pertahanan siber mereka. Hal ini dapat menyebabkan perlombaan senjata baru, di mana negara-negara berlomba untuk mengembangkan teknologi yang lebih canggih untuk meretas dan melindungi sistem mereka.

Beberapa negara menanggapi serangan siber dengan sanksi ekonomi atau tindakan balasan yang dapat memperburuk hubungan bilateral atau multilateral. Ini menjadi ancaman serius terhadap stabilitas politik global, karena semakin banyak negara yang terlibat dalam konflik digital.

Kebijakan dan Upaya Keamanan Global

Sebagai tanggapan terhadap ancaman ini, banyak negara telah memperkenalkan kebijakan dan strategi untuk meningkatkan keamanan siber dan melindungi data mereka. Beberapa langkah yang diambil oleh negara-negara tersebut antara lain:

- Pembentukan tim keamanan siber nasional
- Perjanjian internasional
- Peningkatan infrastruktur pertahanan siber

Implikasi Hukum dan Etika

Dalam ranah internasional, masalah hukum dan etika terkait spionase siber masih menjadi perdebatan. Beberapa pihak berpendapat bahwa serangan siber, terutama yang dilakukan oleh negara besar, harus dianggap sebagai tindakan ilegal dan pelanggaran terhadap kedaulatan negara. Namun, ada juga argumen bahwa dalam dunia yang semakin digital ini, tindakan spionase siber mungkin tidak bisa dihindari, terutama dalam konteks kompetisi geopolitik.

Spionase siber telah menjadi komponen penting dalam persaingan politik global, di mana negara-negara menggunakan teknologi untuk mendapatkan keunggulan strategis dalam konflik internasional. Serangan-serangan ini tidak hanya menargetkan data ekonomi atau militer, tetapi juga dapat merusak

hubungan diplomatik dan memperburuk ketegangan internasional. Oleh karena itu, perlunya kebijakan internasional yang jelas dan kerjasama antarnegara untuk menangani ancaman ini semakin mendesak. Di masa depan, dunia maya akan terus menjadi medan pertempuran utama, dan keberhasilan negara dalam menghadapi spionase siber akan sangat bergantung pada penguatan keamanan siber mereka.

Sumber

- Tempo. (24 Januari 2020). Jokowi: Data Adalah New Oil, Bahkan Lebih Berharga dari Minyak. https://www.tempo.co/ekonomi/jokowi-data-adalah-new-oil-bahkan-lebih-berharga-dari-minyak-660832
- Nadya Kurnia. (1 Desember 2023). *Mengapa Data Disebut Sebagai New Oil? Bernilai dan Berisiko, Ini Penjelasannya*. IDX Channel. https://www.idxchannel.com/economics/mengapa-data-disebut-sebagai-new-oil-bernilai-dan-berisiko-ini-penjelasannya
- METRO TV. (24 Oktober 2024). Prabowo Ingin Semua Instansi Punya CSIRT. https://www.youtube.com/watch?v=Vr40BAiQ3lg
- Kantor Komunikasi Kepresidenan RI (Instagram @pco.ri). (6 April 2025). *Pembentukan CSIRT di Setiap Instansi Pemerintah*. https://www.instagram.com/pco.ri/p/DIGl44VSlW2/
- Yuchong Li, Qinghui Liu, *A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments*, Energy Reports, Volume 7, 2021, Pages 8176-8186, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2021.08.126.
- Romadhoni, Muhammad & Rachman, Aulia & Cahyo, Imam. (2024). *Pengamanan Wilayah Udara: Tanggung Jawab Negara dalam Cyber Espionage di Ruang Angkasa*. Jurnal Ilmu Hukum, Humaniora dan Politik. 5. 1112-1120. 10.38035/jihhp.v5i2.3224.

CSIRT Sebagai Garda Terdepan Keamanan Siber Berdasarkan Standar RFC 2350

Penulis: **Anton Lepari**

CSIRT (*Computer Security Incident Response Team*) adalah tim yang tugasnya merespons insiden keamanan computer, seperti serangan siber, *malware*, peretasan, *data breach*, dan sebagainya. Mereka bertugas untuk mendeteksi, mengelola, menangani, dan menganalisis insiden supaya dampaknya ke organisasi bisa diminimalisir.

Pembentukan CSIRT bisa mengacu pada RFC 2350. RFC 2350 adalah dokumen standar yang diterbitkan oleh IETF pada tahun 1998, berjudul *"Expectations for Computer Security Incident Response"*. Standar ini memberikan format dan panduan tentang bagaimana sebuah CSIRT mendeskripsikan dirinya ke publik. Tujuan dari dokumen ini adalah untuk mengungkapkan harapan umum komunitas Internet terhadap Tim Tanggap Insiden Keamanan Komputer (CSIRT).

Tidak mungkin untuk menentukan serangkaian persyaratan yang sesuai untuk semua tim, tetapi mungkin dan bermanfaat untuk mencantumkan dan

menjelaskan serangkaian topik dan isu umum yang menjadi perhatian dan minat komunitas. Jika sebuah CSIRT ingin memperkenalkan dirinya secara resmi, mereka biasanya membuat dokumen "profil" yang isinya:

- Siapa mereka
- Tanggung jawab dan cakupan kerjanya
- Layanan apa yang mereka tawarkan
- Bagaimana cara menghubungi mereka
- Waktu operasional
- Informasi teknis penting lainnya

Semua informasi itu disusun mengikuti struktur yang dijelaskan di RFC 2350. Dengan mengikuti format RFC 2350, CSIRT jadi lebih terstruktur, transparan, dan mudah diakses oleh pihak-pihak yang membutuhkan bantuan saat insiden keamanan terjadi.

Sumber

- Brownlee, N., & Guttman, E. (1998). *Expectations for Computer Security Incident Response* (RFC 2350). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc2350

"Breach, breached, breaching" - Anonimus

Data Breach: Ketika Rahasia Bocor ke Dunia Maya

Penulis: **Anton Lepari**

Data breach itu adalah insiden di mana data pribadi (seperti nama, password, nomor KTP, data kartu kredit, rahasia perusahaan, dll) bocor ke pihak yang tidak berhak. Biasanya ini bisa terjadi karena serangan *hacker*, kesalahan internal (kayak salah konfigurasi server), atau bahkan karena perangkat yang hilang/dicuri. Misalnya ketika sebuah web jual-beli tempat kamu daftar dan membuat akun ternyata mengalami kebocoran yang mengakibatkan *database* dan email serta *password* kamu tersebar ke internet, itu adalah data breach.

Ada beberapa pekerjaan yang memiliki peran krusial dalam mengidentifikasi ancaman, melindungi data pribadi, dan memastikan sistem tetap aman. Berikut beberapa contoh pekerjaan yang berhubungan dengan data breach:

1. ***Cybersecurity Analyst*** bertugas mendeteksi potensi breach, monitoring sistem.
2. ***Incident Responder*** bertugas memberikan respons cepat kalau terjadi *breach*, melakukan analisis terhadap insiden, dan melakukan mitigasi.
3. ***Digital Forensic Analyst*** berugas menganalisis jejak-jejak serangan setelah *breach* terjadi.
4. ***Security Engineer*** bertugas membangun sistem yang lebih aman supaya tidak mudah *breach*.
5. ***Compliance Officer*** bertugas memastikan perusahaan mematuhi regulasi soal *data protection*, seperti GDPR dan UU PDP.
6. ***Data Protection Officer*** **(DPO)** yang merupakan jabatan wajib di perusahaan besar yang atur soal keamanan dan privasi data.

Dengan semakin banyaknya ancaman yang mengarah pada data pribadi, profesi-profesi ini menjadi sangat penting dalam melindungi informasi yang sangat berharga dan menjaga reputasi serta keamanan sebuah organisasi.

Kamsib ID *adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.*

Kamsib Indonesia on Paper *adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang.* [at]kamsib_id

Kamsib Indonesia
Jakarta, Indonesia
hubungi@kamsib.id