JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 1, No 1, Juni 2023
ISSN 9999-9999 (media online)
Hal 96-98

Perkembangan Terbaru Dalam Keamanan Siber, Ancaman Yang Diidentifikasi Dan Upaya Pencegahan

Muhammad Subhan Abdullah[1], Ines Heidiani Ikasari[1*]

[1]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pamulang
Jl. Raya Puspiptek No.46, Buaran, Kec. Serpong, Kota Tangerang Selatan Banten 15310.
subhanabdullah322@gmail.com[1], ines.heidiani@gmail.com[2]
(* : coressponding author)

Abstrak - Meningkatnya risiko serangan siber di Indonesia, terutama serangan ransomware dan malware, dan menekankan perlunya pemerintah dan penyelenggara sistem elektronik (PSE) meningkatkan keamanan sistem dan perlindungan data. Regulasi seperti Undang-Undang Pelindungan Data Pribadi (PDP) juga penting dalam menjaga keamanan dan kedaulatan ruang virtual. Kelemahan keamanan siber di Indonesia, termasuk indeks pertahanan siber yang rendah, kurangnya regulasi keamanan siber yang ditandatangani oleh Presiden, dan kesulitan memenuhi anggaran peningkatan investasi keamanan siber, berdampak negatif terhadap kepercayaan investor dan pengembangan teknologi. Ancaman dan serangan siber merupakan tantangan utama dalam era digital, terutama dengan meningkatnya aktivitas digital selama pandemi COVID-19. Faktor manusia menjadi kelemahan utama dalam keamanan siber, dan artikel ini menyoroti pentingnya meningkatkan literasi digital dan kesadaran akan keamanan siber. Layanan inovatif Security Rating yang diperkenalkan oleh ArmourZero memungkinkan penilaian tingkat keamanan informasi perusahaan dengan kolaborasi RiskRecon, menggunakan teknologi AI dan API. Artikel ini juga menekankan pentingnya memperhatikan keamanan pihak ketiga, supply chain, dan vendor yang memiliki akses ke infrastruktur perusahaan, serta meningkatnya serangan terhadap open source software (OSS) pada supply chain. Langkah proaktif dalam pemindaian dan evaluasi pihak ketiga diperlukan untuk mencegah kerugian finansial dan risiko reputasi.

Kata Kunci : Keamanan siber, serangan siber, sistem elektronik, Internet of Things (IoT), indeks pertahanan siber, teknologi, ancaman siber, kelemahan manusia, literasi digital, perlindungan, perencanaan keamanan, security rating, risiko keamanan.

Abstract *The increasing risk of cyber attacks in Indonesia, particularly ransomware and malware attacks, underscores the importance for the government and electronic system providers (PSE) to enhance system security and data protection. Regulations such as the Personal Data Protection Act (PDP) are also crucial in maintaining security and sovereignty in the virtual space. Cybersecurity weaknesses in Indonesia, including a low cybersecurity defense index, a lack of signed cybersecurity regulations by the President, and difficulties in meeting the budget for cybersecurity investment, have a negative impact on investor confidence and technological development. Cyber threats and attacks are significant challenges in the digital era, especially with the surge in digital activities during the COVID-19 pandemic. Human factors are the primary vulnerability in cybersecurity, and this article highlights the importance of improving digital literacy and awareness of cybersecurity. The innovative service called Security Rating introduced by ArmourZero enables the assessment of a company's information security level through collaboration with RiskRecon, utilizing AI and API technologies. The article also emphasizes the significance of considering the security of third parties, supply chains, and vendors with access to company infrastructure, as well as the increasing attacks on open-source software (OSS) in the supply chain. Proactive measures in scanning and evaluating third parties are necessary to prevent financial losses and reputation risks.*

Keywords: Cybersecurity, cyber attacks, electronic systems, Internet of Things (IoT), cybersecurity defense index, technology, cyber threats, human vulnerabilities, digital literacy, protection, security planning, security rating, security risks.

1. PENDAHULUAN

Penggunaan internet yang semakin luas telah menyebabkan peningkatan serangan siber. Badan Siber dan Sandi Negara (BSSN) mencatat bahwa jumlah kasus serangan siber di Indonesia telah mencapai 100 juta hingga April 2022. Kekhawatiran terhadap serangan ini mendorong pemerintah dan penyelenggara sistem elektronik (PSE) untuk meningkatkan perlindungan sistem dan penanganan terhadap serangan siber. Undang-Undang Pelindungan Data Pribadi (PDP) juga memiliki peran penting dalam menjaga kedaulatan dan keamanan data.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 1, No 1, Juni 2023
ISSN 9999-9999 (media online)
Hal 96-98

Namun, keamanan siber di Indonesia masih memiliki kelemahan yang perlu ditangani. Hal ini dapat mengurangi kepercayaan investor dan menghambat pengembangan teknologi di negara ini. Kelemahan ini meliputi indeks pertahanan siber yang rendah di Indonesia, kurangnya regulasi keamanan siber yang ditandatangani oleh Presiden, dan kesulitan dalam memenuhi anggaran peningkatan investasi keamanan siber.

Ancaman dan serangan siber menjadi perhatian utama dalam era digital, terutama selama pandemi COVID-19. Ketergantungan kita pada teknologi sehari-hari membuat keamanan siber semakin relevan dan penting. Meskipun banyak organisasi telah mengambil langkah-langkah untuk memperkuat keamanan mereka, faktor manusia tetap menjadi kelemahan utama dalam keamanan siber. Artikel ini menyoroti pentingnya meningkatkan literasi digital dan kesadaran akan keamanan siber sebagai langkah antisipasi.

Keamanan siber menjadi isu yang semakin penting dalam era digital. Untuk melindungi informasi perusahaan dan organisasi, ArmourZero telah meluncurkan layanan inovatif bernama Security Rating. Layanan ini menggunakan teknologi AI dan API untuk mengidentifikasi risiko keamanan yang berasal dari vendor dan bekerja sama dengan RiskRecon. Artikel ini juga menekankan pentingnya menjaga keamanan pihak ketiga, supply chain, dan vendor yang memiliki akses ke infrastruktur perusahaan. Selain itu, peningkatan serangan terhadap open source software pada supply chain juga menjadi perhatian utama. Dalam menghadapi tantangan ini, perusahaan perlu mengambil langkah proaktif dalam melakukan pemindaian dan evaluasi terhadap pihak ketiga dan supply chain yang terlibat.

2. METODE

Penelitian ini menggunakan pendekatan analisis deskriptif dengan mengumpulkan data dari berbagai sumber yang relevan, termasuk laporan BSSN, pandangan para ahli keamanan siber, pernyataan Gubernur Lemhannas, berita terkait, laporan industri, dan informasi dari ArmourZero dan RiskRecon. Data yang terkumpul dianalisis untuk mengidentifikasi jenis serangan siber yang dominan, tantangan dalam sistem elektronik, faktor-faktor penyebab kelemahan keamanan siber di Indonesia, security rating, dampaknya terhadap investasi dan pengembangan teknologi, serta tren dan tantangan terkait dengan kelemahan manusia dalam keamanan siber, juga pentingnya memperhatikan keamanan pihak ketiga, dan supply chain dalam rangka mencegah serangan siber

3. ANALISA DAN PEMBAHASAN

Serangan siber yang dominan di Indonesia adalah ransomware dan malware, dengan perlindungan data pribadi menjadi fokus utama dalam pencegahan. Empat potensi utama yang memicu serangan siber adalah kredensial, phising, faktor manusia, dan kerentanan server. Untuk meningkatkan keamanan, diperlukan kebijakan yang meliputi manajemen kredensial yang baik, peningkatan kesadaran terhadap phising, dan perbaikan kebijakan keamanan server. Kelemahan keamanan siber di Indonesia disebabkan oleh indeks pertahanan siber yang rendah dibandingkan dengan rata-rata global, kurangnya regulasi keamanan siber yang ditandatangani oleh Presiden, dan kesulitan dalam memenuhi anggaran peningkatan investasi keamanan siber. Hal ini berpotensi menghambat investasi di sektor teknologi dan digital, termasuk pengembangan startup. Untuk memperbaiki situasi ini, langkah-langkah seperti peningkatan indeks pertahanan siber, pengesahan regulasi keamanan siber yang kuat, dan peningkatan anggaran untuk investasi keamanan siber diperlukan.

Serangan dan ancaman siber selama pandemi COVID-19 terutama terkait dengan faktor manusia. Kurangnya literasi digital dan pengetahuan tentang keamanan siber membuat individu dan organisasi rentan terhadap serangan seperti hacking, spoofing, phishing, dan lainnya. Artikel ini juga membahas strategi antisipasi, termasuk pentingnya sinergi antara pemangku kepentingan dalam meningkatkan literasi digital dan kesadaran akan keamanan siber. Perlindungan yang efektif melibatkan penggunaan jasa konsultasi dan pendampingan dalam merancang program keamanan siber serta perencanaan ketahanan jangka pendek, menengah, dan jangka panjang.

JRIIN : Jurnal Riset Informatika dan Inovasi
Volume 1, No 1, Juni 2023
ISSN 9999-9999 (media online)
Hal 96-98

Security Rating merupakan metode proaktif yang menggunakan pemindaian dan analisis data untuk memberikan penilaian risiko yang akurat terkait keamanan siber. Melalui layanan ini, pelanggan dapat mengakses Security Operation Center (SOC) yang dilengkapi dengan tim ahli keamanan siber untuk mengatasi masalah keamanan yang mungkin timbul. Artikel ini juga menyoroti peningkatan serangan terhadap open source software pada supply chain dan pentingnya melakukan pemindaian dan evaluasi terhadap pihak ketiga serta supply chain yang terlibat guna mencegah kerugian finansial dan risiko reputasi

4. KESIMPULAN

Dalam meningkatkan keamanan sistem elektronik dan mencegah serangan siber, kerjasama antara pemerintah, PSE, dan masyarakat sangat penting. Undang-Undang Pelindungan Data Pribadi (PDP) menjadi landasan hukum yang penting dalam menjaga keamanan data pribadi dan perlindungan terhadap serangan siber. Instansi publik dan swasta perlu mengambil tindakan proaktif dalam mempersiapkan dan meningkatkan keamanan sistem elektronik mereka.

Kelemahan keamanan siber di Indonesia memiliki dampak signifikan terhadap investasi dan pengembangan teknologi. Untuk menarik investasi dan mendorong pengembangan teknologi yang lebih baik, perlu dilakukan perbaikan dalam indeks pertahanan siber, penandatanganan regulasi keamanan siber yang memadai, dan peningkatan anggaran untuk investasi keamanan siber. Tindakan ini akan meningkatkan kepercayaan investor dan membuka peluang bagi perkembangan teknologi yang lebih maju di Indonesia.

Faktor manusia menjadi kelemahan utama dalam keamanan siber. Untuk menghadapi tantangan ini, perlindungan yang efektif melibatkan pendidikan dan edukasi berkelanjutan guna meningkatkan literasi digital dan kesadaran akan keamanan siber. Sinergi antara pemangku kepentingan dalam meningkatkan literasi digital dan kesadaran akan keamanan siber sangat penting. Selain itu, strategi antisipasi yang melibatkan perencanaan ketahanan dan keamanan digital yang komprehensif juga diperlukan.

Layanan inovatif Security Rating oleh ArmourZero telah memberikan kontribusi signifikan dalam memperkuat keamanan dan perlindungan siber dalam era digital. Dengan menggunakan teknologi AI dan API, Security Rating membantu mengidentifikasi risiko keamanan yang berasal dari vendor dan memberikan akses ke Security Operation Center (SOC) dengan tim ahli keamanan siber. Peningkatan serangan terhadap open source software pada supply chain menyoroti pentingnya pemindaian dan evaluasi terhadap pihak ketiga dan supply chain yang terlibat. Perusahaan perlu mengambil langkah proaktif dalam melindungi data mereka dan mencegah kerugian finansial serta risiko reputasi yang mungkin terjadi dalam menghadapi tantangan keamanan siber.

REFERENCES

Aptika, A. (2022). Antisipasi Bersama Tingkatkan Sistem dan Cegah Serangan Siber. https://aptika.kominfo.go.id/2022/09/antisipasi-bersama-tingkatkan-sistem-dan-cegah-serangan-siber

Arini, S. C. (2023). Keamanan Siber RI Sangat Lemah Bikin Investor 'Galau', Ini 3 Faktanya! DetikFinance. https://finance.detik.com/berita-ekonomi-bisnis/d-6733529/keamanan-siber-ri-sangat-lemah-bikin-investor-galau-ini-3-faktanya

Hidayat, M. (2023). Serangan dan Ancaman Siber Makin Marak di Masa Pandemi, Manusia Ternyata Jadi Faktor Lemah. Liputan6.com. https://www.liputan6.com/tekno/read/5314302/serangan-dan-ancaman-siber-makin-marak-di-masa-pandemi-manusia-ternyata-jadi-faktor-lemah

Enam, L. (2023). Layanan Inovatif Security Rating Perkuat Keamanan Serta Perlindungan Siber. https://www.liputan6.com/regional/read/5317351/layanan-inovatif-security-rating-perkuat-keamanan-serta-perlindungan-siber