
REVIEW LITERATUR: PENTINGNYA KESADARAN KEAMANAN SIBER

(CYBER SECURITY AWARENESS) PADA ORGANISASI PENCINTA

LINGKUNGAN HIDUP

Divy Nayla Yasmin¹, Faris Baihaqi², Faiz Alfarizi³, Indra Gunawan, M.Kom⁴

¹Teknik Informatika STIKOM Tunas Bangsa

²Teknik Informatika STIKOM Tunas Bangsa

³Teknik Informatika STIKOM Tunas Bangsa

⁴STIKOM Tunas Bangsa

Email: ¹divyny@gmail.com, ²farisbaihaqi28@gmail.com, ³alfarizifaiz2025@gmail.com,

⁴indra@amiktunasbangsa.ac.id

ABSTRAK

Perkembangan teknologi digital telah memberikan kemudahan bagi organisasi, termasuk organisasi pencinta lingkungan hidup, dalam melakukan kampanye, mengelola data, serta membangun jaringan komunikasi. Namun, hal ini juga meningkatkan risiko serangan siber seperti phishing, malware, dan kebocoran data yang dapat mengancam reputasi serta keberlanjutan kegiatan organisasi. Salah satu langkah preventif yang penting adalah peningkatan kesadaran keamanan siber (*cyber security awareness*) pada setiap anggota organisasi. Penelitian ini menggunakan metode studi literatur dengan meninjau artikel ilmiah, laporan industri, dan prosiding konferensi yang terbit pada periode 2015–2024. Hasil kajian menunjukkan bahwa kesadaran keamanan siber berperan penting dalam mencegah insiden serangan, mengurangi risiko penyalahgunaan data, serta meningkatkan budaya keamanan digital di organisasi. Pada konteks organisasi pencinta lingkungan hidup, kesadaran ini juga membantu menjaga kepercayaan publik, mengamankan basis data sukarelawan, serta melindungi strategi kampanye digital yang sering kali menjadi target penyalahgunaan.

Kata kunci: Keamanan Siber, Kesadaran Keamanan, Organisasi Lingkungan, Studi Literatur

***A LITERATURE REVIEW: THE IMPORTANCE OF CYBERSECURITY AWARENESS
IN ENVIRONMENTAL ORGANIZATIONS***

ABSTRACT

The rapid growth of digital technology has facilitated organizations, including environmental organizations, in conducting campaigns, managing data, and building communication networks. However, it has also increased the risk of cyber threats such as phishing, malware, and data breaches, which may endanger their reputation and the sustainability of their activities. One of the crucial preventive measures is raising cyber security awareness among all organization members. This study employs a literature review method by analyzing scientific articles, industry reports, and conference proceedings published between 2015 and 2024. The findings indicate that cyber security awareness plays a significant role in preventing incidents, reducing data misuse risks, and strengthening the digital security culture in organizations. Specifically, for environmental organizations, this awareness is essential to maintain public trust, secure volunteer databases, and protect digital campaign strategies, which are often targeted for exploitation.

Keywords: Cyber Security, Awareness, Environmental Organizations, Literature Review

1. PENDAHULUAN

Revolusi digital pada era abad ke-21 telah mengubah cara organisasi beroperasi, berinteraksi, dan menyampaikan informasi kepada publik. Perkembangan teknologi informasi tidak hanya membawa kemudahan, tetapi juga memperluas jangkauan komunikasi melalui media sosial, website, aplikasi mobile, dan berbagai platform digital lainnya. Hal ini juga dirasakan oleh organisasi pencinta lingkungan hidup yang kini dapat menyebarkan kampanye secara cepat, menjangkau audiens global, membangun jaringan sukarelawan lintas negara, serta menggalang dukungan publik melalui kampanye digital (digital campaign).

Namun, kemajuan teknologi yang diadopsi oleh organisasi lingkungan tidak dapat dilepaskan dari berbagai risiko keamanan. Ancaman siber (cyber threats) menjadi salah satu tantangan terbesar yang dapat mengganggu keberlangsungan organisasi. Bentuk serangan yang sering muncul antara lain pencurian identitas digital (identity theft), peretasan akun media sosial yang digunakan untuk kampanye, serangan phishing melalui email resmi organisasi, hingga kebocoran data anggota dan donatur. Serangan-serangan tersebut tidak hanya berdampak pada kerugian finansial, tetapi juga dapat menurunkan kredibilitas dan reputasi organisasi di mata publik. Hilangnya kepercayaan masyarakat berpotensi melemahkan partisipasi sukarelawan dan dukungan terhadap gerakan pelestarian lingkungan.

Dalam konteks ini, kesadaran keamanan siber (cybersecurity awareness) menjadi elemen yang sangat penting bagi organisasi pencinta lingkungan. Kesadaran ini tidak hanya berkaitan dengan penggunaan perangkat lunak pengaman, melainkan juga pemahaman anggota organisasi mengenai praktik aman dalam aktivitas digital sehari-hari, seperti pengelolaan kata sandi, kewaspadaan terhadap tautan mencurigakan, serta kebiasaan dalam menjaga kerahasiaan data. Dengan adanya pemahaman dan penerapan kesadaran keamanan siber yang baik, organisasi dapat meminimalisasi risiko serangan, menjaga kepercayaan publik, dan memastikan keberlangsungan misi lingkungan hidup mereka.

Penelitian ini disusun untuk mengkaji secara mendalam pentingnya kesadaran keamanan siber dalam organisasi pencinta lingkungan hidup. Melalui pendekatan studi literatur, penelitian ini akan meninjau berbagai hasil penelitian terdahulu terkait ancaman siber, strategi mitigasi, serta praktik terbaik (best practices) yang relevan untuk

diterapkan. Dengan demikian, diharapkan hasil penelitian ini dapat memberikan kontribusi bagi organisasi lingkungan dalam merancang kebijakan keamanan siber yang efektif serta meningkatkan kapasitas anggotanya dalam menghadapi tantangan era digital..

2. TINJAUAN PUSTAKA

2.1 Keamanan Siber

Keamanan siber merupakan suatu upaya sistematis yang bertujuan untuk melindungi sistem informasi, jaringan, perangkat keras, perangkat lunak, serta data digital dari berbagai ancaman dan serangan yang berasal dari dunia maya. Menurut Stallings (2020), keamanan siber tidak hanya mencakup penggunaan teknologi perlindungan seperti firewall, enkripsi, dan antivirus, tetapi juga mencakup strategi manajemen risiko, kebijakan organisasi, serta kesadaran manusia yang mengoperasikan sistem tersebut. Ancaman keamanan siber saat ini semakin kompleks, mulai dari serangan hacker, penyebaran malware, ransomware, hingga kebocoran data yang dapat merugikan secara finansial maupun merusak reputasi organisasi. Dalam konteks organisasi modern, keamanan siber memiliki peran krusial karena berkaitan langsung dengan kepercayaan publik, keberlangsungan operasional, dan pencapaian tujuan strategis. Oleh karena itu, penerapan keamanan siber harus dilakukan secara menyeluruh, baik dari sisi teknologi maupun pengelolaan sumber daya manusia.

2.2 Kesadaran Keamanan Siber (Cyber Security Awareness)

Kesadaran keamanan siber atau cyber security awareness merupakan salah satu elemen penting dalam menjaga integritas sistem informasi. Bada & Sasse (2019) mendefinisikan kesadaran keamanan siber sebagai tingkat pengetahuan dan pemahaman individu mengenai ancaman digital serta kemampuan mereka dalam menerapkan langkah-langkah pencegahan untuk melindungi diri maupun organisasi. Kesadaran ini tidak hanya sebatas mengetahui jenis-jenis ancaman, tetapi juga mencakup kemampuan untuk mengenali tanda-tanda adanya serangan, seperti email phishing, situs web palsu, atau tautan mencurigakan. Selain itu, praktik penggunaan kata sandi yang kuat dan unik, kebiasaan melakukan pembaruan sistem, serta pemahaman tentang pentingnya enkripsi data menjadi aspek kunci dari kesadaran keamanan siber.

Dalam berbagai penelitian, kesadaran keamanan siber terbukti berperan signifikan dalam menurunkan risiko terjadinya serangan siber. Hal ini karena sebagian besar kebocoran data atau peretasan justru berawal dari kelalaian manusia, bukan kelemahan teknologi. Oleh karena itu, membangun budaya kesadaran siber di dalam organisasi melalui pelatihan, sosialisasi, dan kebijakan internal merupakan langkah strategis yang harus diutamakan. Dengan kesadaran yang tinggi, setiap individu dapat berperan sebagai “lapisan pertahanan pertama” terhadap berbagai bentuk ancaman digital..

2.3 Organisasi Pencinta Lingkungan Hidup

Organisasi pencinta lingkungan hidup merupakan entitas non-profit yang berfokus pada upaya pelestarian alam, pencegahan kerusakan lingkungan, mitigasi perubahan iklim, serta edukasi masyarakat mengenai pentingnya menjaga ekosistem. Aktivitas organisasi ini biasanya melibatkan kampanye publik, penggalangan dana, advokasi kebijakan, hingga kegiatan sosial bersama komunitas. Dalam era digital, sebagian besar aktivitas tersebut dilakukan melalui media sosial, website resmi, aplikasi komunikasi, maupun platform donasi daring. Hal ini memberikan keuntungan dalam hal jangkauan audiens yang lebih luas, efisiensi biaya, serta peningkatan keterlibatan masyarakat.

Namun demikian, ketergantungan pada platform digital juga membawa risiko baru, yaitu potensi ancaman keamanan siber. Serangan terhadap organisasi pencinta lingkungan hidup dapat berupa peretasan akun media sosial yang digunakan untuk kampanye, serangan phishing terhadap email organisasi, hingga pencurian data sukarelawan atau donatur. Jika hal tersebut terjadi, dampaknya bukan hanya berupa kerugian teknis, tetapi juga hilangnya kepercayaan masyarakat terhadap organisasi tersebut. Mengingat keberlangsungan organisasi sangat bergantung pada dukungan publik, maka keamanan data dan sistem informasi menjadi aspek vital yang tidak dapat diabaikan. Oleh karena itu, penerapan kesadaran keamanan siber di dalam organisasi pencinta lingkungan hidup menjadi semakin relevan dan mendesak, agar misi pelestarian lingkungan dapat terus berjalan tanpa hambatan dari ancaman digital.

3. METODOLOGI

Penelitian ini menggunakan metode studi literatur (*literature review*) dengan fokus pada penelusuran dan analisis terhadap publikasi yang relevan dengan topik kesadaran keamanan siber. Sumber literatur yang digunakan meliputi artikel ilmiah, prosiding konferensi, *white paper*, serta laporan industri yang

diterbitkan dalam rentang waktu 2015 hingga 2024. Pemilihan rentang waktu tersebut dimaksudkan agar literatur yang dianalisis tetap aktual dan mencerminkan perkembangan terkini dalam bidang keamanan siber.

Kriteria inklusi dalam penelusuran literatur ditetapkan untuk memastikan kesesuaian dengan fokus penelitian. Publikasi yang dipilih harus membahas setidaknya salah satu dari tiga aspek utama, yaitu: (1) konsep kesadaran keamanan siber, (2) hubungan antara kesadaran keamanan siber dengan pencegahan serangan digital, dan (3) praktik penerapan keamanan digital pada organisasi non-profit, termasuk organisasi pencinta lingkungan hidup. Literatur yang tidak memenuhi kriteria tersebut, seperti publikasi dengan konteks berbeda atau data yang sudah usang, dikeluarkan dari analisis.

Proses analisis dilakukan dengan pendekatan deskriptif-kualitatif, yaitu dengan cara mengkaji isi literatur, mengidentifikasi tema-tema utama, serta membandingkan temuan antar penelitian. Hasil sintesis dari literatur tersebut kemudian digunakan untuk merumuskan pemahaman yang lebih mendalam mengenai pentingnya kesadaran keamanan siber, sekaligus mengidentifikasi praktik terbaik (*best practices*) yang dapat diadopsi oleh organisasi pencinta lingkungan hidup dalam menjaga keamanan digital mereka.

4. HASIL DAN PEMBAHASAN

4.1 Pentingnya Kesadaran Siber

Hasil kajian literatur menunjukkan bahwa mayoritas serangan siber yang menimpa organisasi non-profit tidak semata-mata disebabkan oleh lemahnya infrastruktur teknologi, melainkan karena faktor manusia, khususnya rendahnya kesadaran keamanan digital di kalangan anggota organisasi. Banyak kasus kebocoran data atau peretasan yang terjadi akibat tindakan sederhana seperti mengklik tautan phishing, mengunduh lampiran berbahaya, atau menggunakan kata sandi yang lemah dan sama untuk berbagai akun. Hal ini memperlihatkan bahwa teknologi pertahanan yang canggih tidak akan efektif apabila tidak diimbangi dengan perilaku digital yang aman. Dengan demikian, kesadaran siber menjadi kunci utama dalam membangun pertahanan berlapis, di mana setiap individu di dalam organisasi memiliki peran penting sebagai “garis pertahanan pertama” terhadap ancaman digital.

4.2 Dampak pada Organisasi Pencinta Lingkungan Hidup

Bagi organisasi pencinta lingkungan hidup, serangan siber dapat memberikan dampak yang sangat serius dan meluas. Hilangnya data sukarelawan atau donatur, misalnya, tidak hanya menimbulkan kerugian administratif tetapi juga dapat merusak kepercayaan para pihak yang terlibat dalam mendukung kegiatan organisasi. Selain itu, peretasan akun media sosial dapat menimbulkan dampak reputasi yang signifikan, karena media sosial merupakan kanal utama dalam menyampaikan pesan lingkungan dan menggalang dukungan publik. Dalam kasus yang lebih ekstrem, serangan ransomware dapat menghentikan aktivitas kampanye digital secara total, sehingga menghambat agenda organisasi dalam melaksanakan misi pelestarian alam. Dampak ini menunjukkan bahwa keamanan digital tidak hanya menjadi masalah teknis, melainkan juga menyangkut keberlangsungan gerakan sosial dan advokasi lingkungan itu sendiri.

4.3 Strategi Peningkatan Kesadaran

Berdasarkan literatur yang dikaji, terdapat sejumlah strategi efektif yang dapat diterapkan untuk meningkatkan kesadaran keamanan siber di kalangan anggota organisasi. Salah satu strategi yang paling umum adalah penyelenggaraan pelatihan rutin mengenai ancaman digital, sehingga anggota organisasi dapat memahami jenis-jenis serangan yang mungkin terjadi serta cara mengantisipasinya. Selain itu, simulasi serangan phishing juga direkomendasikan untuk melatih kewaspadaan anggota dalam menghadapi email atau pesan mencurigakan. Organisasi juga perlu memiliki kebijakan keamanan internal yang jelas, sederhana, dan mudah dipahami agar dapat diterapkan secara konsisten oleh seluruh anggota. Tidak kalah penting, kolaborasi dengan pakar teknologi informasi sangat dianjurkan untuk melakukan monitoring sistem, memberikan masukan kebijakan, serta membantu dalam menangani potensi serangan yang lebih kompleks. Strategi-strategi ini, apabila diterapkan secara berkesinambungan, dapat membentuk budaya kesadaran siber yang kuat di dalam organisasi.

4.4 Relevansi bagi Lingkungan Hidup

Kesadaran keamanan siber memiliki relevansi yang sangat besar terhadap keberlangsungan organisasi pencinta lingkungan hidup, karena keamanan digital yang terjaga secara langsung berdampak pada efektivitas pencapaian misi lingkungan. Dengan adanya sistem keamanan yang baik dan anggota yang memiliki kesadaran tinggi, organisasi dapat

mempertahankan kepercayaan publik, yang menjadi modal sosial utama dalam menggalang dukungan dan partisipasi. Kepercayaan publik yang terjaga memungkinkan organisasi untuk terus menggalang dana, memperluas jejaring sukarelawan, serta melaksanakan kampanye lingkungan tanpa gangguan berarti dari serangan siber. Dengan kata lain, kesadaran siber bukan hanya persoalan teknis, tetapi juga merupakan fondasi penting yang mendukung keberhasilan gerakan pelestarian lingkungan di era digital.

5. KESIMPULAN

Kesadaran keamanan siber merupakan aspek penting yang perlu diperhatikan oleh organisasi pencinta lingkungan hidup. Melalui literatur yang dikaji, dapat disimpulkan bahwa kesadaran siber berperan signifikan dalam mencegah serangan, menjaga kepercayaan publik, serta melindungi data strategis organisasi. Implementasi pelatihan, simulasi, serta kebijakan keamanan digital menjadi langkah utama untuk meningkatkan budaya keamanan.

Penelitian selanjutnya dapat difokuskan pada studi empiris di organisasi pencinta lingkungan hidup di Indonesia untuk mengukur tingkat kesadaran siber dan efektivitas program pelatihan yang diterapkan.

DAFTAR PUSTAKA

- Bada, A., & Sasse, M. A. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? *International Journal of Human-Computer Studies*.
- Stallings, W. (2020). *Effective Cybersecurity: A Guide to Using Best Practices and Standards*. Pearson.
- Symantec. (2021). *Internet Security Threat Report*. Symantec Corporation.

Ponemon Institute. (2022). The Cost of Data Breaches in Non-Profit Organizations. Ponemon Research.

Renaud, K., & Goucher, W. (2020). Cybersecurity in Civil Society Organizations: Building Resilience. Journal of Information Security.