ANCAMAN PENCURIAN DATA INFORMASI DAN PENYALAHGUNAAN DATA PRIBADI DALAM KEJAHATAN SIBER

Mahbubul Wathoni[1]*, Rikaro Ramadi[1], Rabiatul Nurhasanah[1], Viesah Putra Alegra[1], Muhammad Rifki Al Fauzan[1]
[1]Universitas Muhammadiyah Jakarta, Jl. KH. Ahmad Dahlan, Ciputat, Tangerang Selatan

*mahbubul.wathoni@umj.ac.id

ABSTRAK

Di era digital ini, kejahatan siber yang merajalela di masyarakat semakin canggih dan merugikan banyak pihak. Kejahatan siber memiliki banyak bentuk, namun yang paling umum adalah phishing, malware, ransomware, dan pencurian identitas. Masing-masing jenis kejahatan ini memiliki dampak yang berbeda, namun semuanya bertujuan untuk merugikan korban. Kejahatan siber adalah ancaman serius yang dapat memengaruhi individu, organisasi, dan masyarakat secara keseluruhan. Dengan meningkatnya ketergantungan pada teknologi dan internet, memahami cara kerja kejahatan siber dan tanda-tanda menjadi korban sangatlah penting. Melindungi diri Anda dari kejahatan siber membutuhkan langkah-langkah proaktif, termasuk penggunaan kata sandi yang kuat, otentikasi dua faktor, dan kesadaran akan ancaman. Dengan menerapkan tips dan trik keamanan siber yang tepat, kita bisa mengurangi risiko dan menjaga data pribadi serta informasi sensitif tetap aman.

Kata kunci: Kejahatan Dunia Maya, Keamanan Dunia Maya, Keamanan Data, Malware, Ransomware

ABSTRACT

In this digital era, cybercrimes that are rampant in society are increasingly sophisticated and detrimental to many parties. Cybercrime takes many forms, but the most common are phishing, malware, ransomware, and identity theft. Each of these types of crime has different impacts, but all of them aim to harm the victim. Cybercrime is a serious threat that can affect individuals, organizations and society as a whole. With the increasing reliance on technology and the internet, understanding how cybercrime works and the signs of becoming a victim is essential. Protecting yourself from cybercrime requires proactive measures, including the use of strong passwords, two-factor authentication, and threat awareness. By implementing the right cybersecurity tips and tricks, we can reduce our risks and keep our personal data and sensitive information safe.

Keywords*: Cybercrime, Cybersecurity, Data Security, Malware, Ransomware.*

1. PENDAHULUAN

Menurut CISCO, keamanan siber adalah praktik melindungi sistem, jaringan, dan program dari serangan digital. Keamanan siber biasanya ditujukan untuk mengakses, mengubah, atau menghancurkan informasi sensitif, memeras uang dari pengguna, atau mengganggu pengoperasian proses bisnis.

Kesadaran keamanan siber mengacu pada pengetahuan dan pemahaman yang dimiliki individu dan organisasi tentang potensi ancaman siber dan tindakan yang dapat diambil untuk melindungi diri dari ancaman tersebut. Kesadaran keamanan siber penting karena dapat membantu individu dan organisasi untuk mengenali dan merespons potensi ancaman siber serta mencegah serangan agar tidak berhasil. Oleh karena itu, penting untuk melindungi sistem Anda dari risiko sekecil apa pun. Kesadaran keamanan siber adalah pengetahuan dan pemahaman individu dan organisasi tentang potensi ancaman siber dan tindakan yang dapat mereka lakukan untuk melindungi diri mereka sendiri dari ancaman tersebut. Kesadaran keamanan siber penting karena membantu individu dan organisasi mengidentifikasi dan merespons potensi ancaman siber dan mencegah serangan yang berhasil.

Contoh-contoh Risiko Siber:
Malware

Malware adalah singkatan dari perangkat lunak berbahaya. Malware mencakup berbagai program perangkat lunak yang memungkinkan pihak ketiga mendapatkan akses tidak sah ke informasi sensitif atau mengganggu fungsi normal infrastruktur penting.

Ransomware

Ransomware mengacu pada model bisnis dan berbagai teknologi terkait yang digunakan oleh penjahat untuk memeras uang dari berbagai organisasi.

Serangan man-in-the-middle

Dalam serangan man-in-the-middle, pihak ketiga mencoba untuk mendapatkan akses yang tidak sah melalui jaringan selama pertukaran data.

Phishing

Phishing adalah ancaman siber yang menggunakan teknik rekayasa sosial untuk mengelabui pengguna agar membocorkan informasi pribadi.

DDoS

Serangan penolakan layanan terdistribusi (DDoS) adalah upaya terkoordinasi untuk membebani server dengan mengirimkan sejumlah besar permintaan palsu.

Ancaman Orang Dalam

Ancaman orang dalam adalah risiko keamanan yang ditimbulkan oleh karyawan jahat dalam sebuah organisasi.

2. METODE PELAKSANAAN

Sosialisasi dan Penyuluhan:

- Kegiatan Seminar: Mengadakan seminar di sekolah-sekolah mengenai Ancaman Pencurian Data Informasi dan Penyalahgunaan Data Pribadi dalam Kejahatan Siber.
- Materi Pendidikan: Menyebarkan materi edukasi melalui media sosial.

3. HASIL DAN PEMBAHASAN

Dalam kegiatan seminar yang telah dilaksanakan di sekolah tersebut, penulis juga membagikan soal pre-test dan post-test yang bertujuan untuk mengetahui pemahaman guru mengenai ancaman pencurian data informasi dan penggunaan data pribadi dalam kejahatan siber. Berikut adalah hasilnya:

Gambar 1. Pertanyaan Pre-test dan Post-test

Gambar 2. Jawaban Pre-test dan Post-test

4. KESIMPULAN

Pentingnya keamanan siber tidak dapat diragukan lagi. Serangan siber dapat mengakibatkan kerusakan serius pada sistem dan infrastruktur, termasuk hilangnya data penting, gangguan layanan, dan hilangnya kepercayaan publik. Hal ini dapat berdampak negatif pada bisnis dan ekonomi secara keseluruhan.

Berikut adalah beberapa tips untuk meningkatkan keamanan siber:

- Gunakan kata sandi yang kuat dan unik
- Perbarui sistem dan perangkat lunak secara teratur
- Batasi akses pengguna
- Cadangkan data secara teratur
- Pelatihan keamanan siber
- Rencana darurat keamanan siber

UCAPAN TERIMAKASIH

Puji syukur penulis panjatkan kehadirat Ilahi Robbi Allah SWT, karena atas rahmat dan karunia-Nya, kami sebagai peneliti dapat menyelesaikan kegiatan ini. Peneliti juga mengucapkan banyak terima kasih atas segala bantuan pihak-pihak yang telah membantu kelancaran kegiatan ini.

DAFTAR PUSTAKA

Hummel, Al-Qur'an dan terjemahan. Jakarta: Kementerian Agama Republik Indonesia

Luckring, J.M. dan Hummel, D. (2008). *Bab 24 - Apa yang Dipelajari dari Eksperimen VFE-2 yang Baru*. RTO-TR-AVT-113. https://doi.org/10.2514/6.2008-383

Mat, Esaunggul.ac.id . 2023. Meningkatkan Keamanan Siber: Pentingnya Perlindungan Data di Era Digital. https://fasilkom.esaunggul.ac.id/meningkatkan-keamanan-siber-pentingnya-perlindungan-data-di-era-digital/

Permatasari, Dwiyani. 2021. Tantangan Cyber Security di Era Revolusi Industri 4.0. Sulawesi Selatan: https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca artikel/14190/Tantangan-Cyber-Security-di-Era-Reavolusi-Industri-40.html