Analisis Strategi Efektif Dalam Mendeteksi Dan Mencegah Serangan Phishing Melalui Undangan Elektronik Berformat .Apk

Davin Bramasta[1*], Rohmad Rifa Ardianto[2], Nandita Sekar Sukma Dewi[3]

[1]*Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta*
[1]220103009@mhs.udb.ac.id

[2] *Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta*
[2]220103028@mhs.udb.ac.id

[3]*Fakultas Ilmu Komputer Universitas Duta Bangsa Surakarta*
[3]220103030@mhs.udb.ac.id

Abstrak— **Keamanan informasi telah menjadi pertimbangan penting bagi individu dan organisasi. Kemajuan teknologi telah memperluas penggunaan Internet dan transformasi digital, menjadikan data sebagai aset berharga yang rentan terhadap berbagai ancaman dunia maya seperti malware, phishing, dan pencurian identitas. Tujuan Tietoturva adalah untuk melindungi kerahasiaan, integritas dan ketersediaan data terhadap penggunaan dan modifikasi yang tidak sah. Pelanggaran keamanan data dapat menyebabkan kerugian finansial, reputasi, dan operasional yang signifikan. Strategi untuk meningkatkan keamanan data mencakup penggunaan enkripsi, otentikasi dua faktor, firewall, dan praktik keamanan karyawan. Selain itu, pemerintah dan badan internasional berperan penting dalam mengeluarkan peraturan yang menjamin perlindungan data. Di masa depan, ancaman keamanan akan menjadi semakin kompleks karena teknologi baru seperti kecerdasan buatan dan Internet of Things (IoT), menjadikan inovasi dan penelitian keamanan siber yang berkelanjutan menjadi penting. Laporan singkat ini menyoroti pentingnya keamanan data di era digital dan langkah-langkah yang diperlukan untuk melindungi data dari ancaman yang terus berkembang.**
Kata kunci— keamanan, digital, penipuan, undangan.

Abstract— **Information security has become an important consideration for individuals and organizations. Technological advances have expanded Internet use and digital transformation, making data a valuable asset vulnerable to various cyber threats such as malware, phishing and identity theft. Tietoturva's goal is to protect the confidentiality, integrity and availability of data against unauthorized use and modification. Data security breaches can cause significant financial, reputational and operational losses. Strategies to improve data security include the use of encryption, two-factor authentication, firewalls, and employee security practices. In addition, governments and international bodies play an important role in issuing regulations that guarantee data protection. In the future, security threats will become increasingly complex due to new technologies such as artificial intelligence and the Internet of Things (IoT), making continuous cybersecurity innovation and research essential. This brief highlights the importance of data security in the digital era and the steps needed to protect data from evolving threats.**
Keywords— cyber, security, scam, phising.

I. PENDAHULUAN

Pesatnya perkembangan teknologi dan semakin meningkatnya penggunaan internet dalam kehidupan sehari-hari, data dan informasi kini dapat digunakan dan ditangani dengan lebih cepat dan efisien. Namun kemajuan tersebut juga membawa tantangan baru berupa ancaman keamanan informasi. Ancaman dunia maya seperti malware, phishing, dan pencurian identitas sedang meningkat dan memerlukan perlindungan yang lebih canggih dan berlapis[1][2]. Keamanan informasi harus selalu diperhatikan karena akses informasi yang tidak sah dan tidak bertanggung jawab ini dapat merugikan banyak pihak serta dapat menimbulkan kericuhan atas informasi palsu maupun modus-modus lainny yang disebarkan. Tujuan dari keamanan data adalah untuk menjaga kerahasiaan, integritas dan ketersediaan data dan untuk memastikan bahwa data hanya berada di tangan orang yang berwenang dan bahwa data dilindungi dari modifikasi atau penghapusan yang tidak sah. Seperti kejahatan digital baru ini yang perlu diperhatikan oleh seluruh pengguna internet khususnya instansi pemerintahan untuk dapat menangani kasus ini agar tidak terjadi lagi dan memakan korban lebih banyak. Modus penipuan ini sering terjadi dan menyasar kepada korban yang awam atau Gaptek (Gagap Teknologi) yaitu berupa penyebaran file atau malware dengan tulisan format tertentu supaya calon korban percaya dan malware tersebut dapat berjalan atau tereksekusi pada device calon korban.

Pentingnya keamanan data tidak dapat diabaikan karena konsekuensi dari pelanggaran data bisa sangat merugikan. Pada undang-undang Nomor 19 Tahun 2016 Tentang perubahan Atas Undang-Undang Nomor 11 Tahun 2008[3][4]

terdapat aturan terhadap perbuatan-perbuatan kejahatan yang merugikan orang lain yang terjadi didunia maya melalui transaksi elektronik yang dapat diketahui bahwa perkembangan teknologi semakin pesat. Dampak-dampak ini mencakup kerugian finansial, kerusakan reputasi, dan gangguan bisnis. Selain itu, karena peraturan yang ketat seperti Peraturan Perlindungan Data Umum (GDPR) dan Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA), organisasi harus mematuhi standar keamanan tertentu untuk melindungi informasi pribadi pengguna[5][6]. Oleh karena itu, di era digital saat ini, pemahaman dan penerapan praktik keamanan data yang efektif sangat penting untuk menjaga kepercayaan dan kelangsungan bisnis. Pendahuluan ini menyajikan latar belakang pentingnya keamanan informasi dan memperkenalkan topik terpenting yang dibahas lebih mendalam dalam artikel ini.

Maksud dan tujuan dari penelitian ini adalah untuk menganalisis pentingnya keamanan data di era digital, mengidentifikasi ancaman utama dan mengusulkan strategi perlindungan data yang efektif. Tujuan dari penelitian ini juga untuk menilai dampak peraturan terhadap praktik keamanan informasi dan memberikan rekomendasi kepada organisasi untuk meningkatkan keamanan informasi mereka. Dengan demikian, penelitian ini diharapkan dapat memberikan kontribusi yang signifikan terhadap peningkatan kesadaran dan praktik keamanan informasi di era digital.

II. METODOLOGI PENELITIAN

Metodologi penelitian ini menggunakan pendekatan kualitatif untuk mendapatkan pemahaman komprehensif tentang pentingnya keamanan informasi di era digital. Penelitian yang digunakan adalah deskriptif-analitis, dimana pendekatan deskriptif menggambarkan keadaan keamanan informasi saat ini dan berbagai ancamannya[7][8], sedangkan pendekatan analitis menganalisis data yang dikumpulkan untuk mengidentifikasi pola dan hubungan antar variabel[9]. Data dikumpulkan melalui penelitian literatur. Penelitian literatur dilakukan dengan menelusuri berbagai sumber seperti buku, jurnal ilmiah, artikel dan laporan industri mengenai keamanan informasi, ancaman siber dan peraturan terkait[10][11].

Data survei dianalisis menggunakan statistik deskriptif dan teknik analisis inferensial untuk mengidentifikasi tren dan menguji hubungan antar variabel. Data wawancara dianalisis menggunakan metode analisis tematik untuk mengidentifikasi tema dan pola penting yang membantu memahami konteks dan rincian mendalam tentang keamanan informasi. Validitas dan reliabilitas penelitian dipertahankan dengan melakukan triangulasi data dari berbagai sumber dan menguji instrumen dengan sampel kecil untuk memastikan kejelasan dan keakuratan pertanyaan. Penelitian ini juga berpegang pada prinsip etika penelitian dengan menjaga kerahasiaan informasi responden dan memperoleh persetujuan dari partisipan sebelum melakukan survei dan wawancara. Metodologi ini harus memberikan gambaran komprehensif tentang pentingnya keamanan informasi di era digital dan memberikan rekomendasi praktis kepada organisasi untuk mengelola dan melindungi informasi.

III. HASIL DAN PEMBAHASAN

Ancaman Cyber Security menjadi hal yang penting dan patut untuk di waspadai. Masih banyak masyarakat pengguna internet yang tidak peduli dengan keamanan data miliknya ataupun tidak mengetahui adanya kejatan digital pada kehidupan sehari-hari dalam media sosial. Ancaman kejahatan digital sangatlah bervariasi jenis dan modelnya serta pelaku yang cerdik dalam memilih atau mencari calon korbannya. Malware atau virus yang sering ada pada kehidupan sehari-hari kita salah satu contohnya adalah Virus Trojan[12], virus ini merupakan program yang didesain menyerupai aplikasi atau program yang resmi namun sebenarnya hanyalah program duplikat yang menyamar bagaikan aplikasi resmi berisikan script untuk melakukan tindakan ilegal seperti pencurian data dan penyalahgunaan data[13]. Virus ini terlihat sangat meyakinkan dan hampir tidak ada yang membedakan dengan aplikasi atau program

aslinya, namun software keamanan saat ini sebagian besar dapat mendeteksi adanya file yang mencurigakan pada malware tersebut meskipun menyamar bagaikan aplikasi resmi.

Kejahatan Cyber yang baru-baru saja terjadi dan cukup disorot publik yaitu malware Undangan.Apk yang disebarkan melalui WhatsApp sebagai media pencarian calon korban, dengan mengaku kepada calon korban bahwa pelaku adalah kerabatnya yang akan mengirimkan file undangan seperti pernikahan, pesta, makan bersama, atau yang lainnya. Berikut adalah ciri-ciri, dampak, alur dan cara kerja, cara menghindari, serta langkah yang harus dilakukan ketika sudah terlanjur atau tidak sengaja menginstall malware Undangan.Apk secara jelas dan terperinci.

A. Modus Dan Ciri-Ciri Ancaman

Sebuah Sotware wajib di waspadai jika di dalamnya terdapat sebagai berikut :

1) Iming-iming uang: Aplikasi atau situs web yang menawarkan uang atau hadiah gratis yang kedengarannya terlalu bagus untuk menjadi kenyataan sering kali merupakan jebakan untuk memikat korbannya.
2) Hadiah Besar: Tanpa alasan yang jelas, penawaran dengan hadiah besar biasanya digunakan untuk menarik perhatian dan memikat pengguna agar mengunduh malware.
3) Ungkapan Mendesak, Mendesak, atau Tidak Normal: Pesan yang menggunakan bahasa mendesak atau tidak biasa sering kali menunjukkan upaya untuk membuat korban bertindak tanpa berpikir.
4) Ancaman berita palsu: Penggunaan berita palsu untuk menakut-nakuti atau memanipulasi emosi pengguna agar mengambil tindakan yang diinginkan penipu.
5) Tautan eksternal: Tautan eksternal yang mengarahkan pengguna ke situs web yang tidak dikenal atau mencurigakan sering kali menjadi sumber infeksi malware.
6) File malware: File yang diunduh dan dijalankan tanpa verifikasi yang tepat mungkin berisi malware yang merusak perangkat atau mencuri data.
7) Pengirim Tidak Dikenal/Dikenal: Pesan atau email dari pengirim yang tidak dikenal sering kali merupakan tanda awal bahwa konten tersebut tidak dapat dipercaya.

Salah satu contoh dari Malware tersebut yang marak beredar di kalangan masyarakat saat ini adalah Malware Undangan.Apk, jenis Malware ini biasanya disebarkan melalu media pesan seperti WhatsApp, Telegram. Target penyebarannya adalah pengguna perangkat mobile terutama Android dikarenakan rentan nya sistem keamanan pada perangkat mobile tersebut serta memanfaatkan kurangnya informasi mengenai modus phising seperti ini di kalangan masyarakat.

B. Dampak dari Malware Undangan.Apk

Dampak yang diakibatkan dari Malware ini diantara lain adalah :

1) Overtake atau ambil alih WhatsApp: Malware dapat mengambil alih akun WhatsApp Anda.Jika berhasil, peretas dapat menggunakan akun yang ditangkap untuk menyebarkan malware tambahan ke kontak korban, sehingga infeksi dapat menyebar lebih cepat.
2) Pencurian kode OTP: Kode one-time password (OTP) sangat penting untuk transaksi dan proses login di berbagai aplikasi. Malware ini mencuri kode OTP yang masuk ke perangkat korban sehingga memungkinkan peretas mengakses akun penting seperti perbankan online, email, dan layanan lainnya tanpa sepengetahuan pemilik akun.
3) Spionase: Malware jenis ini dapat melakukan aktivitas spionase yang memungkinkan peretas memantau aktivitas layar perangkat korbannya 24 jam sehari. Ini termasuk memantau

transaksi keuangan dan menangkap kode PIN dari mobile banking dan dompet digital.Data sensitif ini dapat digunakan untuk mencuri uang atau informasi pribadi korban.

4) Penyalahgunaan informasi data: Informasi yang dicuri oleh malware, seperti informasi pribadi, kredensial login, dan informasi keuangan, dapat digunakan oleh peretas untuk tujuan jahat. Hal ini dapat mencakup penipuan identitas, penjualan informasi di pasar gelap, dan mendapatkan akses tidak sah ke akun korban.

Kerusakan Sistem: Malware tidak hanya mencuri informasi tetapi juga merusak sistem operasi perangkat Anda. Hal ini dapat menyebabkan perangkat Anda menjadi lambat, tidak responsif, atau tidak dapat digunakan sama sekali. Kerusakan ini mungkin memerlukan perbaikan atau penggantian perangkat yang mahal.

Malware seperti malware Invitation.Apk dapat menyebabkan kerugian besar bagi pengguna perangkat seluler. Penyebarannya yang cepat serta kemampuannya untuk mencuri dan merusak menjadikannya ancaman serius bagi keamanan digital pengguna. Oleh karena itu, sangat penting untuk selalu berhati-hati saat mengunduh aplikasi atau membuka pesan dari sumber yang tidak dikenal dan menggunakan langkah keamanan seperti aplikasi antivirus dan pengaturan privasi yang ketat.

C. *Cara kerja Malware Undangan.Apk*

Peretas akan menyebarkan file Undangan.Apk dan memaksa atau membujuk calon korban agar membuka atau menginstall file tersebut. Setelah file berhasil di install maka selanjutnya file tersebut akan meminta akses seperti kontak, pesan teks, kamera, mikrofon, lokasi, internet, kirim dan terima sms, serta akses network pada device korban. Izin-izin ini memungkinkan malware untuk mengumpulkan data pribadi yang dibutuhkan peretas. Kemudian file akan mengirim kode OTP kepada peretas yang akan dikirimkan ke Telegram peretas dengan atau tanpa sepengetahuan korban. Selanjutnya file tersebut akan bekerja menggunakan source code yang sudah dirancang sedemikian rupa supaya setelah file terinstall di perangkat korban, maka perangkat tersebut dapat mengirimkan kode yang dibutuhkan oleh peretas. Setelah scipt terinstall dan berhasil mengambil informasi dari device korban maka informasi tersebut akan dikirimkan melalui media Telegram dan selanjutnya penipu dapat mengakses informasi seperti kode OTP yang sifatnya sangat rahasia untuk digunakan seperti megganti pin atau password pada aplikasi mobile banking atau dompet digital, mengakses informasi rahasia pada device korban yang menimbulkan kerugian secara materil maupun immateril.

Malware ini juga dapat menyerupai sebagai aplikasi lain yang terlihat normal dan tidak berbahaya seperti pembaruan perangkat lunak, atau aplikasi-aplikasi terkenal lainnya. Penyamaran ini bertujuan untuk mengelabui calon korban supaya tidak merasa curiga dan yakin untuk mengunduh dan menginstall aplikasi ini tanpa rasa curiga.

D. *Langkah-langkah untuk menghindari Malware Undangan.Apk*

1) Gunakan atau unduh aplikasi hanya dari sumber tepercaya,Pastikan Anda hanya mengunduh aplikasi dari Google Play Store, Apple App Store, atau sumber resmi lainnya.Sumber resmi ini memiliki mekanisme penyaringan dan keamanan yang lebih ketat dibandingkan dengan situs pihak ketiga yang sering menyebarkan aplikasi berbahaya.
2) Selalu waspada terhadap nomor baru atau tidak dikenal, meskipun mereka mengaku sebagai saudara atau teman dekat, Jika anda menerima pesan dari nomor yang tidak dikenal, meskipun mereka adalah saudara atau teman dekat.
3) Jangan mendownload atau menginstal aplikasi yang dikirimkan kepada Anda oleh orang asing, Jangan mendownload atau menginstal aplikasi yang

dikirimkan kepada Anda oleh orang asing.Peretas sering kali menyamar sebagai orang yang mereka kenal untuk mendistribusikan aplikasi berbahaya.Jangan sembarangan saat membuka website atau link dari website yang tidak dikenal atau mencurigakan.

4) Jangan mengklik link atau membuka situs web yang dikirimkan kepada Anda oleh orang yang tidak Anda kenal atau dari situs web mencurigakan.Tautan ini mungkin mengarahkan Anda ke situs web yang berisi malware atau phishing.Selalu update dan gunakan antivirus versi terbaru untuk perlindungan maksimal.
5) Selalu pastikan antivirus Anda terupdate ke versi terbaru.Program antivirus yang diperbarui mencakup database ancaman terbaru dan dapat memberikan perlindungan maksimal terhadap malware baru.Menghapus atau menghapus instalan aplikasi yang terlihat mencurigakan: Jika Anda menemukan aplikasi yang tampak mencurigakan atau belum pernah Anda instal, segera hapus atau hapus instalan aplikasi tersebut.
6) Aplikasi mencurigakan ini mungkin merupakan malware yang menyusup ke perangkat Anda.

E. Langkah yang harus dilakukan jika sudah menginstall Aplikasi Undangan.Apk

Langkah pertama yang dapat di ambil saat user tidak sengaja mengunduh atau menginstall Malware adalah mematikan koneksi internet Wifi dan data seluler pada perangkat yang terinstall Malware untuk mencegah pengiriman kode data yang dicuri ke server peretas.

Langkah kedua adalah mengaktifkan mode aman
pada perangkat anda. Mode ini memungkinkan Anda untuk menjalankan perangkat hanya dengan aplikasi sistem dasar, sehingga aplikasi pihak ketiga tidak akan bisa berjalan yang dapat memudahkan untuk user menghapus aplikasi berbahaya.

Langkah ketiga melakukan scan menggunakan antivirus yang terpercaya bawaan perangkat, jalankan antivirus dan lakukan pemindain penuh untuk mencari dan mendeteksi file-file yang mencurigakan. Setelah itu user dapat mengubah kata sandi aplikasi atau mobile banking dan aktifkan autentikasi dua faktor (2FA) untuk lapisan keamanan tambahan.

Langkah terakhir kita dapat memantau aktivitas akun untuk memperhatikan transaksi yang tidak dikenal atau perubahan informasi akun. Jika semua sudah dilakukan langkah yang dapat user ambil adalah backup data demi menghindari data yang hilang.

IV. KESIMPULAN

Penelitian ini menyoroti pentingnya kewaspadaan terhadap ancaman penipuan berbasis aplikasi, khususnya yang menggunakan file undangan.apk sebagai medium serangan. Penipuan undangan.apk adalah metode di mana penyerang mengirimkan aplikasi berbahaya yang disamarkan sebagai undangan melalui pesan singkat atau email. Ketika korban mengunduh dan memasang aplikasi ini, perangkat mereka dapat terinfeksi malware, yang memungkinkan penyerang mencuri data pribadi, melakukan pemantauan aktivitas, dan bahkan mengambil alih kendali perangkat.

Studi ini menemukan bahwa serangan ini meningkat seiring dengan kemajuan teknologi dan penggunaan smartphone yang luas. Beberapa faktor utama yang mendukung keberhasilan serangan ini adalah kurangnya kesadaran pengguna tentang keamanan aplikasi, kecenderungan untuk mengunduh aplikasi dari sumber tidak terpercaya, dan rendahnya tingkat adopsi solusi keamanan pada perangkat mobile. Penelitian juga menunjukkan bahwa meskipun banyak pengguna menyadari adanya risiko malware, mereka seringkali masih terjebak oleh taktik penipuan yang semakin canggih dan meyakinkan.

Dampak dari penipuan undangan.apk sangat merugikan, baik dari segi privasi individu maupun

keamanan data perusahaan[14]. Pencurian informasi sensitif seperti data keuangan, kredensial login, dan kontak pribadi dapat mengakibatkan kerugian finansial dan pelanggaran privasi yang serius[15]. Selain itu, perusahaan yang terkena dampak dapat mengalami kerugian reputasi dan keuangan yang signifikan.

Untuk mengurangi risiko ini, edukasi pengguna tentang pentingnya hanya mengunduh aplikasi dari sumber resmi seperti Google Play Store atau Apple App Store sangatlah penting. Selain itu, pengguna harus diajarkan untuk selalu memeriksa izin aplikasi dan waspada terhadap undangan atau pesan yang tidak dikenal. Implementasi perangkat lunak keamanan mobile yang mampu mendeteksi dan mencegah malware juga merupakan langkah penting dalam melindungi perangkat dari serangan.

Secara keseluruhan, penelitian ini menegaskan bahwa peningkatan kesadaran, edukasi keamanan, dan penggunaan teknologi perlindungan yang tepat adalah kunci dalam menghadapi ancaman penipuan undangan.apk. Dengan langkah-langkah ini, risiko yang ditimbulkan oleh serangan ini dapat diminimalkan, dan keamanan informasi pribadi serta organisasi dapat lebih terjaga di era digital yang semakin kompleks.

REFERENSI

[1] E. Soesanto, A. Romadhon, B. Dwi Mardika, and M. Fahmi Setiawan, "Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File," SAMMAJIVA J. Penelit. Bisnisdan Manaj., vol. 1, no. 2, p. 186, 2023.

[2] O. W. Purbo, "Mid 2020 Cyber Security Threat, Tips dan Proposal Strategi Mitigasi Nasional," Lms.Onnocenter.or.Id, 2021, [Online]. Available: https://lms.onnocenter.or.id/pustaka/docs/INTERNET-INDONESIA/TIKTOK-ID-WP-MID-2020-REPORT.pdf

[3] A. Rajab et al., "Urgensi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Sebagai Solusi Guna Membangun Etika Bagi Pengguna Media," Dialogia Iurid. J. Huk. Bisnis dan Investasi, vol. 9, no. October, pp. 463–472, 2017.

[4] Y. J. Lalujan, "Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Ite Terhadap Kebebasan Berpendapat Di Indonesia," Lex Soc., vol. 8, no. 4, pp. 143–152, 2020, doi: 10.35796/les.v8i4.30919.

[5] K. R. Anggen Suari and I. M. Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," J. Anal. Huk., vol. 6, no. 1, pp. 132–142, 2023, doi: 10.38043/jah.v6i1.4484.

[6] R. Sabila, U. Sitompul, M. Irwan, and P. Nasution, "Pentingnya Kepatuhan Keamanan Informasi Dalam Mengurangi Risiko Data Breach," J. Ris. Ilmu Manaj. dan Kewirausahaan, vol. 2, no. 1, pp. 99–107, 2024, [Online]. Available: https://doi.org/10.61132/maeswara.v2i1.587

[7] Y. C. Mahendra and N. K. D. S. A. Pinatih, "Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia," J. Rev. Pendidik. dan Pengajaran, vol. 6, no. 4, pp. 1941–1949, 2023, [Online]. Available: http://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/20659

[8] M. Christmartha, R. A. G. Gultom, S. Aritonang, and U. Pertahanan, "Strategi Kebijakan Pengembangan Sumber Daya Manusia Siber Nasional Guna Mendukung Pertahanan Negara the Policy Strategy of National Cybersecurity Human Resources Development To Support the National Defense (a Case Study At the National Cyber and Crypto Agency 2019)," J. Manaj. Pertahanan, vol. 6, no. 2, p. 85, 2020, [Online]. Available: https://www.cnnindonesia.com/teknol

[9] Y. Rifa'i, "Analisis Metodologi Penelitian Kulitatif dalam Pengumpulan Data di Penelitian Ilmiah pada Penyusunan Mini Riset," Cendekia Inov. Dan Berbudaya, vol. 1, no. 1, pp. 31–37, 2023, doi: 10.59996/cendib.v1i1.155.

[10] L. 2023, "No Titleการบริหารจัดการการบริการที่มีคุณภาพในโรงพยาบาลสังกัดกระทรวงสาธารณสุข," วารสารวิชาการมหาวิทยาลัยอีสเทิร์นเอเชีย, vol. 4, no. 1, pp. 88–100, 2023.

[11] S. Palinggi, S. Palelleng, and L. R. Allolinggi, "Peningkatan Rasio Kejahatan Cyber Dengan Pola Interaksi Sosio Engineering Pada Periode Akhir Era Society 4.0 Di Indonesia," J. Ilm. Din. Sos., vol. 4, no. 1, p. 145, 2020, doi: 10.38043/jids.v4i1.2314.

[12] O. G. HUTAURUK, "Penerapan Manajemen Risiko Cyber Security Di Atas Mv. Ever Ocean Untuk Mewujudkan Keamanan Teknologi Informasi Di …." 2023. [Online]. Available: http://repository.stipjakarta.ac.id/bitstream/handle/123456789/3618/Overgrand Hutauruk.pdf?sequence=1

[13] Rastri Prathivi and Vensy Vydia, "Analisa Pendeteksian Worm dan Trojan Pada Jaringan Internet Universitas Semarang Menggunakan Metode Kalifikasi Pada Data Mining C45 dan Bayesian Network," J. Transform., vol. 14, no. 2, pp. 77–81, 2017.

[14] C. K. Murni, M. S. Husin, and M. R. Herdiansyah, "Perkembangan Os Android Dan Sistem Keamanan Tantangan Dan Solusi," Spirit, vol. 16, no. 1, pp. 161–169, 2024, doi: 10.53567/spirit.v16i1.337.

[15] H. Sampul, "SKRIPSI Oleh : Maharlina Darni Purwandari FAKULTAS BISNIS DAN EKONOMIKA UNIVERSITAS ISLAM INDONESIA YOGYAKARTA," 2024.