E-ISSN: 3063-9387

Peran Manajemen Sekuriti dalam Melindungi *Human Security*: Tinjauan Berdasarkan Insiden Siber di Google

Siti Nur Khofifah[1], Bianca Salikha Ramadhani[2], Haikal Azizan[3], Muhamad Rahmat Zakaria[4]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210715042@mhs.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210715034@mhs.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210715081@mhs.ubharajaya.ac.id
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210715310@mhs.ubharajaya.ac.id

Corresponding Author: 202210715042@mhs.ubharajaya.ac.id[1]

Abstract: *In this digital era, threats to individual security or human security are increasing along with the development of information and communication technology. Individual security now includes not only physical protection but also protection of personal data, privacy, and access to secure information from various cyber attacks. Large technology companies such as Google face major challenges in maintaining user data security amid increasingly complex and sophisticated cyber threats. Cyber incidents such as privacy breaches, data leaks, and malware attacks have shown how vulnerable individuals are to risks in the digital space. Therefore, the role of security management is very important in protecting human security, especially through innovative security policies, rapid response to threats, and strengthening user awareness. This study examines the role of Google's security management in protecting human security based on a number of cyber incidents that have occurred. A qualitative approach is used by analyzing Google's security policy documents, cyber incident reports, and related scientific literature. This study aims to analyze the role of security management in responding to cyber threats that impact human security and also evaluate the steps taken by Google in protecting user privacy. The results of the study show that Google has adopted various strategic steps in mitigating cyber incidents experienced by Google, including the implementation of end-to-end encryption, two-factor authentication, and the use of artificial intelligence to detect threats in real-time.*

Keyword: *Security Management, Human Security, Google, Security Policy, Personal Data, Digital Era, Cyber Security, Phishing*

Abstrak: Pada era digital ini, ancaman terhadap keamanan individu atau human security semakin meningkat seiring dengan perkembangan teknologi informasi dan komunikasi. Keamanan individu kini tidak hanya mencakup perlindungan fisik tetapi juga perlindungan data pribadi, privasi, dan akses terhadap informasi yang aman dari berbagai serangan siber.

Perusahaan teknologi besar seperti Google menghadapi tantangan besar dalam menjaga keamanan data pengguna di tengah ancaman siber yang semakin kompleks dan canggih. Insiden-insiden siber seperti pelanggaran privasi, kebocoran data, hingga serangan malware telah menunjukkan betapa rentannya individu terhadap risiko di ruang digital. Oleh karena itu, peran manajemen sekuriti menjadi sangat penting dalam melindungi human security, terutama melalui kebijakan keamanan yang inovatif, respons cepat terhadap ancaman, dan penguatan kesadaran pengguna. Penelitian ini mengkaji peran manajemen sekuriti Google dalam melindungi human security berdasarkan sejumlah insiden siber yang pernah terjadi. Pendekatan kualitatif digunakan dengan menganalisis dokumen kebijakan keamanan Google, laporan insiden siber, serta literatur ilmiah terkait. Penelitian ini bertujuan agar dapat menganalisis peran manajemen sekuriti dalam merespons ancaman siber yang berdampak pada human security dan juga mengevaluasi langkah-langkah yang diambil Google dalam melindungi privasi pengguna. Hasil penelitian menunjukkan bahwa Google telah mengadopsi berbagai langkah strategis dalam memitigasi terhadap insiden siber yang dialami oleh Google, termasuk penerapan enkripsi end-to-end, autentikasi dua faktor, dan penggunaan kecerdasan buatan untuk mendeteksi ancaman secara real-time.

Kata Kunci: Manajemen Sekuriti, Human Security, Google, Kebijakan Keamanan, Data Pribadi, Era Digital, Kemanan Siber, Phishing

PENDAHULUAN

Kemajuan teknologi di era digital telah membawa dampak besar dalam berbagai aspek kehidupan manusia. Teknologi tidak hanya memengaruhi cara individu berkomunikasi, bekerja, dan belajar, tetapi juga menciptakan transformasi dalam pola interaksi sosial, ekonomi, hingga budaya. Kehadiran internet dan perangkat pintar membuat informasi dapat diakses dalam hitungan detik, mempercepat perubahan globalisasi dan memperluas jangkauan inovasi. Sedangkan dampak negatif yang dihadirkan dari perkembangan teknologi ini adalah berupa pemanasan global, kesenjangan ekonomi, terorisme, dan juga kebocoran data diri dari suatu negara Yunanda et al. (2022). Di tengah dinamika ini, perusahaan-perusahaan teknologi raksasa, seperti Google, telah memainkan peran penting dalam memfasilitasi kehidupan modern dengan menyediakan berbagai layanan berbasis teknologi yang mendukung konektivitas global. Maulidiya, S (2022).

Google didefinisikan sebagai perusahaan teknologi multinasional yang berspesialisasi dalam jasa dan produk internet, seperti teknologi pencarian, komputasi web, perangkat lunak, dan periklanan daring. Namun, dengan meningkatnya penggunaan teknologi, muncul pula berbagai tantangan yang mengancam keamanan data dan privasi individu. Nilai dari sesuatu yang memiliki guna adalah dengan memperoleh hasil dari penggunaan sesuatu yang dapat memberikan manfaat. Sekarang ini masyarakat harus dapat menyesuaikan diri diantaranya dengan memanfaatkan kemajuan teknologi yang ada sebagai penunjang berbagai kegiatan dalam kehidupan sehari-hari Eka Putri & Agustin Wulandari. (2020). Pada level individu, konsep human security menjadi semakin relevan dalam konteks digital. Human security, yang awalnya dipahami sebagai perlindungan individu dari ancaman fisik, kini mencakup aspek digital, seperti keamanan data pribadi dan perlindungan terhadap penyalahgunaan informasi. Sintiya & Yulianto (2024).

Human security didefinisikan sebagai upaya untuk melindungi individu dari berbagai ancaman yang dapat mengganggu keamanan fisik, psikologis, martabat, dan kesejahteraan mereka. Konsep ini menekankan perlindungan hak-hak dasar individu oleh negara, termasuk dari ancaman dunia maya. Google, sebagai salah satu pemimpin industri teknologi, memiliki

tanggung jawab besar untuk melindungi data dan privasi penggunanya. Sejak awal, Google telah mengembangkan berbagai kebijakan keamanan untuk menjaga integritas sistem dan melindungi informasi pengguna dari ancaman yang mungkin muncul. Langkah-langkah ini termasuk enkripsi data, autentikasi ganda, dan program pelatihan keamanan untuk karyawan dan pengguna . Namun, meskipun telah diterapkan kebijakan ini, insiden kebocoran data dan serangan siber tetap terjadi, menunjukkan bahwa tantangan dalam melindungi human security di dunia maya sangat kompleks dan memerlukan pendekatan yang lebih komprehensif. Kasus kebocoran data, serangan siber, dan penyalahgunaan informasi menjadi isu yang semakin mendesak dan harus ditangani secara serius oleh perusahaan- perusahaan ini (Putra et al. (2023).

Manajemen Sekuriti merupakan kebutuhan yang sangat penting bagi perusahaan atau organisasi di era digitalisasi saat ini. Dengan menerapkan manajemen keamanan terintegrasi, melakukan manajemen risiko yang tepat, dan menerapkan kebijakan keamanan yang jelas, perusahaan atau organisasi dapat melindungi nformasi dan teknologinya dari serangan dunia maya dan meminimalkan risiko keamanan yang mungkin terjadi. (Muslim et al. (2024) Ancaman siber berkembang pesat, membutuhkan respons cepat dan adaptif. Tantangan utama mencakup kurangnya ahli teknologi, hadirnya penyedia telekomunikasi baru, dan minimnya regulasi global. Perlindungan keamanan siber pun menjadi sangat penting untuk mengatasi risiko yang terus meningkat. Manajemen keamanan merupakan langkah strategis untuk menghadapi ancaman cybercrime, yang mencakup berbagai bentuk kejahatan seperti akses ilegal, pemalsuan data, peretasan, hingga pelanggaran privasi. Oleh karena itu, penerapan manajemen keamanan yang komprehensif dan terintegrasi sangat penting untuk melindungi aset digital perusahaan dari potensi serangan, sekaligus memitigasi risiko kerugian yang lebih besar (Irawan et al. (2024).

Menurut (Daeng et al. (2023) Respons cepat terhadap insiden sangat penting, didukung regulasi matang dan tim ahli. Pelatihan staf serta pengawasan aturan internal menjadi langkah kunci untuk mengurangi dampak. Hal ini dapat meningkatkan keamanan siber secara keseluruhan. Sementara itu, banyak penelitian menunjukkan bahwa kesadaran akan keamanan siber di kalangan pengguna masih rendah. Oleh karena itu, Penelitian ini bertujuan untuk menganalisis peran manajemen sekuriti dalam merespons ancaman siber yang berdampak pada human security, mengevaluasi langkah-langkah yang diambil Google dalam melindungi privasi pengguna, serta mengidentifikasi strategi yang dapat memperkuat perlindungan human security di era digital.

Berdasarkan rumusan masalah diatas, maka didapat rumusan masalah sebagai berikut:

1. Bagaimana peran manajemen security dapat mendukung perlindungan *human security* pada google?
2. Sejauh mana efektivitas kebijakan keamanan google dalam menghadapi insiden siber?

METODE

Metode Kualitatif

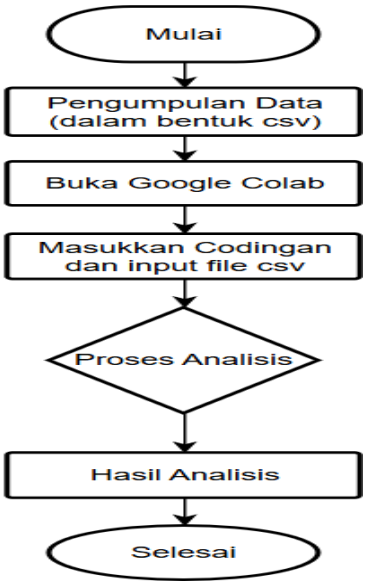
Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan fokus peneliti mencari dan membaca berbagai sumber informasi yang berhubungan dengan manajemen sekuriti dalam melindungi human sekuriti pada Google. Sumber-sumber ini diambil dari artikel dan jurnal. Tujuannya adalah untuk memahami konsep dasar dan mendapatkan referensi yang relevan dengan penelitian ini.

Metode Analisis Data

Analisis ini dilakukan menggunakan metode statis melalui analisis data, yang dimana perangkat lunak yang digunakan untuk melakukan analisis ini adalah Google Colab. Dalam

penelitian ini, data dikumpulkan dari data keamanan google dan sumber berita yang relevan dan kredible yang sesuai dengan topik penelitian mengenai tinjauan insiden siber yang terjadi pada google. Analisis yang dilakukan meliputi:

1. Analisis Klasifikasi (Pengelompokan) Data
2. Analisis Tingkat Dampak Ancaman
3. Analisis Efektivitas Tindakan
4. Analisis Pola Waktu Penyelesaian

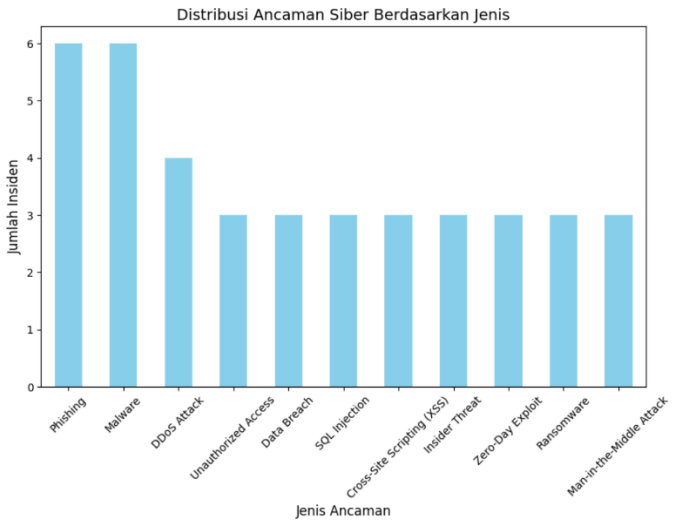


Gambar 1. Flowchart Analisis Penelitian

HASIL DAN PEMBAHASAN

Analisis Klasifikasi (Pengelompokan) data berdasarkan Jenis Ancaman dari data yang tersedia, terdapat insiden keamanan siber yang dapat diklasifikasikan ke dalam berbagai kategori ancaman. Berikut adalah hasil analisis yang dilakukan:

Gambar 2. Pengelompokan data berdasarkan jenis ancaman



Tingkat Ancaman dari hasil jumlah insiden google yang terjadi adalah sebagai berikut:

a) Phishing (15%)

Phishing menjadi salah satu ancaman siber yang paling sering terjadi di Indonesia. Berdasarkan laporan dari Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII), rendahnya tingkat kesadaran pengguna terhadap keamanan digital, khususnya dalam penggunaan email dan layanan transaksi online, menjadi penyebab utama tingginya kasus ini.

Beberapa aplikasi yang sering menjadi sasaran serangan phishing antara lain Gmail, Google Drive, dan Google Workspace. Pelaku kejahatan siber memanfaatkan teknik rekayasa sosial untuk mengelabui korban, sehingga mereka tanpa sadar memberikan informasi sensitif seperti kata sandi atau data keuangan mereka.

b) Malware (15%)

Serangan malware merupakan salah satu ancaman siber yang sering terjadi di Indonesia. Faktor utama yang meningkatkan kerentanan pengguna terhadap ancaman ini adalah kebiasaan menggunakan aplikasi ilegal, mengakses situs yang tidak aman, serta kurangnya pembaruan perangkat lunak. Beberapa platform seperti Google Chrome, Google Play Store, dan Google Cloud kerap menjadi sasaran serangan malware, termasuk ransomware, yaitu jenis malware yang mengenkripsi data pengguna dan sering kali digunakan untuk meminta tebusan.

c) DDoS Attack (10%)

Serangan Distributed Denial of Service (DDoS) di Indonesia kerap menyasar situs layanan publik, sektor perbankan, dan instansi pemerintah. Beberapa layanan populer seperti Google Search, Google Maps, dan YouTube juga dapat menjadi target serangan. Motivasi di balik serangan ini biasanya untuk mengganggu aksesibilitas layanan atau sebagai bentuk aksi protes. Kerentanan sistem sering kali disebabkan oleh infrastruktur keamanan jaringan yang belum memadai.

d) Data Breach (7,5%)

Kebocoran data merupakan ancaman serius di Indonesia, terlebih dengan diberlakukannya regulasi seperti Undang-Undang Perlindungan Data Pribadi (UU PDP). Insiden besar, seperti pelanggaran data pada kementerian, platform e-commerce, dan perusahaan fintech, sering kali melibatkan penggunaan aplikasi seperti Google Drive dan Google Analytics. Ancaman ini kini menjadi fokus utama dalam upaya meningkatkan keamanan di Indonesia.

e) Unauthorized Access (7,5%)

Akses tidak sah sering kali menjadi masalah serius yang disebabkan oleh kelemahan dalam pengelolaan kredensial, khususnya di sektor korporasi. Insiden ini biasanya melibatkan platform digital seperti YouTube, Google Photos, dan Google Drive, yang digunakan secara luas oleh perusahaan. Penyebab utamanya adalah praktik keamanan yang kurang optimal, seperti penggunaan kata sandi yang lemah, mudah ditebak, atau tidak diganti secara rutin. Selain itu, kurangnya penerapan langkah-langkah keamanan tambahan, seperti autentikasi dua faktor (two-factor authentication), turut memperbesar risiko terjadinya pelanggaran. Situasi ini menekankan pentingnya kesadaran dan upaya untuk meningkatkan manajemen keamanan siber di lingkungan kerja.

f) Zero-Day Exploit (7,5%)

Serangan zero-day semakin marak terjadi di Indonesia, khususnya dalam sektor teknologi dan layanan berbasis daring. Jenis serangan ini sering kali menargetkan aplikasi yang banyak digunakan, seperti Chrome Browser dan sistem operasi Android, yang memiliki basis pengguna besar dan kompleksitas tinggi. Para pelaku kejahatan siber memanfaatkan celah keamanan yang belum terdeteksi oleh pengembang perangkat lunak untuk melancarkan aksinya.

Kondisi ini menunjukkan pentingnya peningkatan sistem keamanan serta kecepatan respons terhadap potensi kerentanan dalam aplikasi dan platform digital.

g) Ransomware (7,5%)

Ransomware telah menjadi ancaman serius di Indonesia, terutama bagi sektor kesehatan dan pendidikan yang mengelola data sensitif dalam jumlah besar. Salah satu target utama serangan ini adalah layanan seperti Google Workspace, di mana pelaku kejahatan siber menggunakan teknik enkripsi untuk mengunci akses ke data penting. Kurangnya infrastruktur pencadangan data yang andal menjadi salah satu faktor yang memperburuk dampak serangan ransomware.

Ketika data cadangan tidak tersedia atau tidak diperbarui secara berkala, organisasi yang menjadi korban sering kali terpaksa mempertimbangkan pembayaran tebusan untuk memulihkan akses mereka.

h) Man-in-the-Middle Attack (7,5%)

Serangan ini kerap terjadi melalui jaringan Wi-Fi publik di Indonesia, yang sering kali memiliki tingkat keamanan rendah. Pelaku kejahatan siber memanfaatkan celah ini untuk menyadap komunikasi antara pengguna dan layanan yang mereka akses. Aplikasi seperti Google Meet, Google Hangouts, dan Google Voice menjadi sasaran utama, dengan tujuan utama mencuri data pribadi, termasuk informasi login akun dan detail transaksi keuangan. Risiko ini semakin meningkat karena banyak pengguna tidak menyadari bahaya menggunakan jaringan publik tanpa proteksi tambahan.

i) SQL Injection (7,5%)

Ancaman SQL injection menjadi salah satu metode serangan yang sering mengincar situs web e-commerce dan portal pemerintah di Indonesia. Serangan ini biasanya memanfaatkan kelemahan pada sistem pengamanan aplikasi untuk menyisipkan kode berbahaya ke dalam database, dengan tujuan mencuri, mengubah, atau bahkan menghapus data penting. Platform seperti Google Ads juga kerap menjadi sasaran karena tingginya nilai data yang terlibat. Kelemahan dalam penerapan pengamanan, seperti validasi input yang kurang ketat, sering kali menjadi faktor utama yang memungkinkan eksploitasi ini terjadi. Hal ini tidak hanya merugikan organisasi yang menjadi korban tetapi juga menurunkan kepercayaan pengguna terhadap layanan tersebut.

j) Cross-Site Scripting (XSS) (7,5%)

Serangan XSS terjadi pada situs web dengan validasi input yang lemah. Aplikasi seperti Google Forms dan Google Sites menjadi target serangan ini, memungkinkan penyerang menyisipkan skrip berbahaya untuk mencuri data pengguna atau mengarahkan mereka ke situs palsu.

k) Insider Threat (7,5%)

Ancaman dari dalam organisasi (insider threat) sering terjadi di Indonesia karena kurangnya pengawasan terhadap akses karyawan atau kontraktor. Insiden ini melibatkan

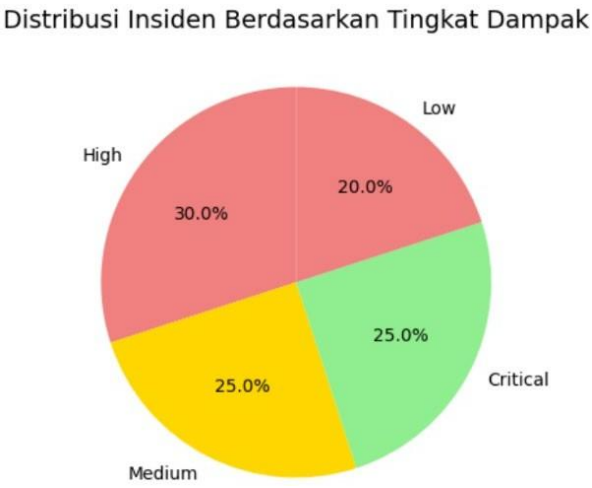
sistem internal perusahaan seperti Google Workspace dan aplikasi internal lainnya. Dampaknya bisa sangat merugikan, baik disengaja maupun tidak.

1. Pengelompokan Data: Data akan diklasifikasikan berdasarkan jenis ancaman untuk mengidentifikasi ancaman yang paling sering terjadi.

Dari hasil klasifikasi ini, terlihat bahwa ancaman berbasis manipulasi pengguna data (phishing) dan perangkat lunak berbahaya (malware) adalah jenis ancaman yang paling sering terjadi. Ancaman ini seringkali berhasil karena mengeksploitasi kelemahan pengguna, seperti kurangnya kesadaran akan keamanan siber atau kelalaian dalam mengenali ancaman. Selain itu, ancaman seperti DDoS attack dan data breach menunjukkan tantangan yang signifikan bagi platform besar seperti Google Search, Google Drive, dan Google Workspace, yang melayani jutaan pengguna secara global. Ancaman ini dapat mengganggu layanan dalam skala besar, sehingga membutuhkan mitigasi yang cepat dan efektif.

2. Analisis Tingkat Dampak Ancaman

Tingkat dampak (impact level) dari masing-masing insiden dianalisis untuk menentukan seberapa besar pengaruh ancaman terhadap sistem dan pengguna. Hasil analisis dapat diilihat pada gambar dibawah ini.



Gambar 3. Tingkatan Dampak Ancaman terhadap sistem dan pengguna

Dampak Ancaman dari jumlah insiden google yang terjadi pada data pengguna adalah sebagai berikut:

1. Critical (10 kasus, 25%)

Ancaman dengan tingkat dampak kritikal mencakup insiden serius seperti data breach, zero-day exploit, dan ransomware. Dampak dari ancaman ini dapat mencakup:

a. Kehilangan atau pencurian data pengguna dalam jumlah besar.
b. Kerugian finansial yang signifikan akibat denda atau tuntutan hukum.
c. Penurunan kepercayaan publik dan kerusakan reputasi organisasi.
d. Gangguan besar pada operasi bisnis.

2. High (15 kasus, 37,5%)

Ancaman dengan tingkat dampak tinggi melibatkan serangan seperti Distributed Denial of Service (DDoS) dan akses tidak sah pada sistem kritis. Dampak yang mungkin timbul meliputi:

a. Penurunan kinerja atau penghentian sementara layanan.
b. Biaya tambahan untuk mitigasi dan pemulihan sistem.
c. Risiko kebocoran data yang terbatas namun signifikan bagi bisnis.
d. Gangguan operasional pada skala menengah hingga besar.

3. Medium (9 kasus, 22,5%)

Ancaman dengan tingkat dampak menengah biasanya terjadi pada serangan seperti phishing atau eksploitasi celah keamanan pada aplikasi minor. Dampaknya dapat mencakup:

a. Kehilangan data dalam jumlah kecil.
b. Potensi kerugian finansial yang moderat.
c. Gangguan operasional sementara pada bagian tertentu dari sistem.
d. Kebutuhan peningkatan sistem keamanan untuk mencegah serangan lebih lanjut.

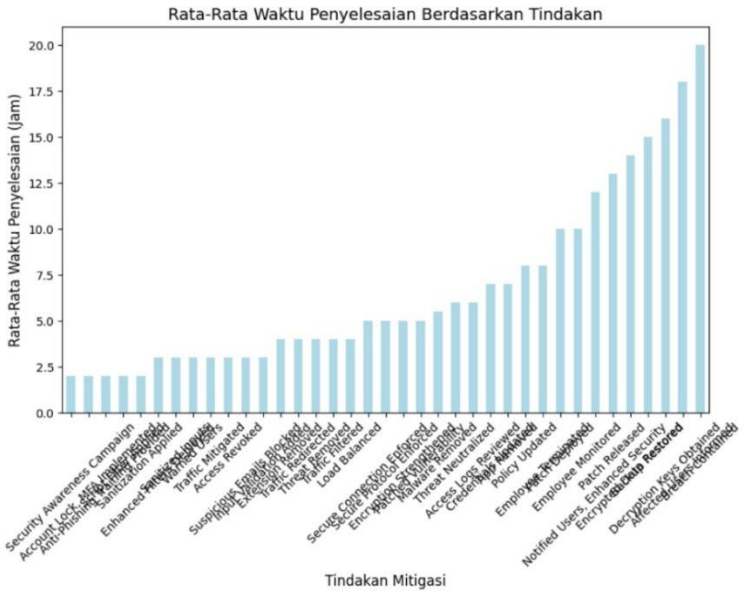
4. Low (6 kasus, 15%)

Ancaman dengan tingkat dampak rendah umumnya melibatkan serangan seperti spam atau aktivitas mencurigakan tanpa eksploitasi data. Dampaknya antara lain:

a. Gangguan kecil pada sistem atau pengguna.
b. Tidak ada kehilangan data atau kerugian finansial langsung.
c. Peningkatan beban kerja tim TI untuk menangani insiden.
d. Kesempatan untuk mengidentifikasi kelemahan sistem dan memperbaikinya.

5. Efektivitas Tindakan

Evaluasi dilakukan terhadap tindakan mitigasi yang diambil oleh perusahaan google dengan membandingkannya terhadap waktu penyelesaian (resolution time). Hasil analisis dapat diilihat pada gambar dibawah ini.



Gambar 4. Efektivitas Tindakan Mitigasi

Google telah menunjukkan tingkat efektivitas yang bervariasi dalam menangani berbagai jenis ancaman:

a. Ancaman dengan Efektivitas Tinggi (≤3 jam)

Ancaman seperti phishing dan XSS diselesaikan dengan cepat. Hal ini menunjukkan bahwa Google memiliki langkah mitigasi yang matang, seperti filter email otomatis, sanitasi inpu data, dan edukasi pengguna.

b. Ancaman dengan Efektivitas Sedang (4-10 jam)

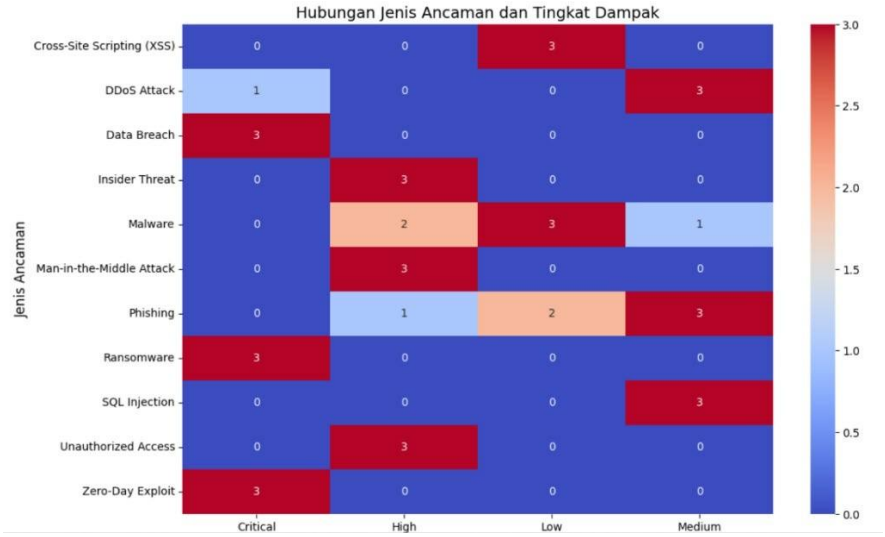
Ancaman seperti malware, unauthorized access, dan DDoS attack membutuhkan waktu lebih lama. Tantangan teknis dalam menangani ancaman ini dapat melibatkan identifikasi perangkat lunak berbahaya, memperbarui kredensial akses, atau pengelolaan lalu lintas jaringan.

c. Ancaman dengan Efektivitas Rendah (>10 jam)

Ancaman data breach, ransomware, dan zero-day exploit memerlukan waktu penyelesaian yang lebih panjang. Kompleksitas teknis, langkah mitigasi berlapis, serta pemberitahuan kepada pengguna menjadi faktor utama yang memperpanjang waktu respons.

6. Pola Penyelesaian

Mengkaji hubungan antara jenis ancaman dan waktu penyelesaian untuk mengidentifikasi efisiensi sistem manajemen sekuriti pada perusahaan google. Hasil analisis dapat diilihat pada gambar dibawah ini.



Gambar 5. Waktu Penyelesaian

Berdasarkan data, waktu penyelesaian (resolution time) untuk 40 insiden keamanan bervariasi tergantung pada jenis ancaman. Rata-rata waktu penyelesaian adalah 6,3 jam, dengan perincian sebagai berikut:

1. Phishing: 2-3 jam (rata-rata 2,5 jam).
2. Malware: 4-7 jam (rata-rata 5,6 jam).
3. DDoS attack: 3-4 jam (rata-rata 3,5 jam).
4. Unauthorized access: 3-7 jam (rata-rata 5,3 jam).
5. Data breach: 12-20 jam (rata-rata 16 jam).
6. Zero-day exploit: 10-14 jam (rata-rata 12 jam).
7. Ransomware: 14-16 jam (rata-rata 15 jam).
8. SQL injection: 3-4 jam (rata-rata 3,5 jam).
9. Cross-Site Scripting (XSS): 2-3 jam (rata-rata 2,5 jam).
10. Man-in-the-middle attack: 5 jam.

Waktu penyelesaian tercepat adalah pada kasus phishing dan XSS (2 jam), sedangkan waktu terlama ditemukan pada kasus data breach (hingga 20 jam).

KESIMPULAN

Layanan Google di Indonesia menghadapi berbagai ancaman keamanan siber, dengan phishing dan malware menjadi yang paling dominan, masing-masing mencapai 15% dari total insiden. Serangan ini sering menyasar platform populer seperti Gmail, Google Drive, dan Google Workspace, memanfaatkan kurangnya kesadaran pengguna terhadap pentingnya perlindungan digital. Selain itu, ancaman lain seperti serangan Distributed Denial of Service (DDoS), kebocoran data, ransomware, dan eksploitasi celah keamanan (7,5–10%) juga menargetkan layanan seperti Google Search, YouTube, dan Google Cloud. Dampak dari ancaman-ancaman ini sangat signifikan, mencakup gangguan operasional, kehilangan data penting, serta kerugian finansial besar.

Beberapa penyebab utama kerentanan termasuk lemahnya manajemen kredensial, kurangnya penerapan autentikasi dua faktor, dan ketidakcukupan infrastruktur keamanan. Untuk menghadapi tantangan ini, Google perlu terus meningkatkan teknologi keamanannya, memastikan adanya sistem pencadangan data yang lebih andal, mempercepat waktu respons terhadap serangan, dan memberikan edukasi menyeluruh kepada pengguna untuk meningkatkan kesadaran mereka akan pentingnya keamanan digital. Pendekatan holistik ini tidak hanya dapat mengurangi risiko, tetapi juga memperkuat kepercayaan publik terhadap layanan Google di Indonesia.

REFERENSI

Daeng, Y., Levin, J., Razzaq Prayudha, M., Putri Ramadhani, N., Imanuel, S. (2023). *Penerapan Sistem Keamanan Siber Terhadap Kejahatan Siber Di Indonesia*.

Eka Putri, R. H., & Agustin Wulandari, T. (2022). PEMANFAATAN APLIKASI ZOOM CLOUD MEETING SEBAGAI MEDIA E-LEARNING DALAM MENCAPAI PEMAHAMAN MAHASISWA DI TENGAH PANDEMI COVID-19. *Jurnal Common |*, *4*. https://doi.org/10.34010/common

Irawan, A., Hamzah, W., Fadholi, N., Erikamaretha, Z., Sinlae, F., & Informatika, P. S. (2024). *Tantangan dan Strategi Manajemen Keamanan Siber di Indonesia berbasis IoT*.

Yunanda, F., Nuari, D., Angelika Br Panjaitan, K., & Werend Renanta, F. (2022). *THE ANALYSIS OF LOCAL TERMS ON SOCIAL MEDIA OF INDONESIAN TEENAGERS* (Vol. 5, Issue 1). http://ejurnal.budiutomomalang.ac.id/index.php/journey

Muslim, A. Sephira, M. H. Abrar, S. L. S. P. Angin, and H. Hidayatullah. (2024). *Analisis Keamanan Siber (Cyber Security) Dalam Era Digital 'Tantangan Dan Strategi Pengamanan*'. https://www.researchgate.net/publication/361094518

Putra, R. G., Fauzi, A., Prasetyo, E. T., Pratama, S. R., Ramadhan, I. D., Febriyanti, F., & Nurlela, S. (2023). *Universitas Bhayangkara Jakarta Raya, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id 3. Universitas Bhayangkara Jakarta Raya, Indonesia, ery.teguh@ubharajaya.ac.id 4*. *2*(1). https://doi.org/10.38035/jim.v2i1

Sintiya, T., & Yulianto, R. (2023). *ANALISISIS KEBIJAKAN INDONESIA TERKAIT DENGAN PERLINDUNGAN DATA DIRI WARGA NEGARA INDONESIA ANALYSIS OF INDONESIAN POLICY RELATED TO PROTECTING PERSONAL DATA OF INDONESIAN CITIZENS*.