Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, 187-200
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital

Muhamad Febrian Aska [1], Deo pratama Putta [1], Caroline Julyana Magdalena Sinambela [1,*]

[1] Ilmu komputer; universitas Bhayangkara Jakarta raya; Jl raya perjuangan no.81,Bekasi utara,kotabekasi , (021) 88955882; e-mail: 202110715216@mhs.ubharajaya.ac.id 202210715049@mhs.ubharajaya.ac.id,202210715172@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715172@mhs.ubharajaya.ac.id

Diterima: 6 Jan 25; Review: 6 Jan 25; Disetujui: 9 Jan 25; Diterbitkan: 9 Jan 25

Abstract

In today's rapidly developing digital era, cyber security has become an urgent need for organizations to protect their data and information systems from increasingly complex threats. Universities are no different; in order to make their educational offerings more competitive, they must raise the caliber of their offerings. competitive. One way that institutions use information technology. The Academic Information System (AIS) is used. SIA was created to fulfill the learning process's goals, which are a component of fulfilling the college's vision and mission. fulfillment of higher education's goal and mission. Technological advances enable various cyber attacks that can result in significant losses, both in terms of finances and organizational reputation. In this context, a layered security approach and increasing awareness and competence of human resources (HR) are important strategies to achieve optimal levels of protection. This research aims to identify and analyze effective strategies that can be applied in implementing cyber security to protect organizations from various digital threats. The research method used is qualitative, which collects and analyzes interview results and related literature to understand the best approaches in cyber security. The research results show that the combination of layered security technologies such as firewalls, intrusion detection systems and data encryption, as well as security awareness training for employees, can increase an organization's resilience to cyber attacks. This approach is not only effective in resisting technical attacks but also strengthens the security culture at all levels of the organization.
***Keywords**: Digital Era, Academic Information System (AIS), Cyber Security, Layered Security Approach.*

Abstrak

Pada era digital yang berkembang pesat saat ini keamanan siber menjadi kebutuhan mendesak bagi organisasi dalam melindungi data dan sistem informasi mereka dari ancaman yang semakin kompleks. Universitas juga demikian untuk membuat penawaran pendidikan mereka lebih kompetitif, mereka harus meningkatkan kualitas penawaran mereka. Salah satu caranya adalah dengan menggunakan teknologi informasi. Salah satunya adalah dengan menggunakan Sistem Informasi Akademik (SIA). SIA diciptakan untuk memenuhi tujuan proses pembelajaran, yang merupakan komponen dari pemenuhan visi dan misi perguruan tinggi. Pemenuhan visi dan misi perguruan tinggi. Kemajuan teknologi memungkinkan berbagai serangan siber yang dapat mengakibatkan kerugian signifikan, baik dari segi finansial maupun reputasi organisasi. Dalam konteks ini, pendekatan keamanan berlapis (*layered security approach*) serta peningkatan kesadaran dan kompetensi sumber daya manusia (SDM) merupakan strategi yang penting untuk mencapai tingkat perlindungan yang optimal. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis strategi efektif yang dapat diterapkan dalam implementasi keamanan siber untuk melindungi organisasi dari berbagai ancaman digital. Metode penelitian yang digunakan adalah kualitatif, yang mengumpulkan dan menganalisis hasil wawancara dan

literatur terkait untuk memahami pendekatan-pendekatan terbaik dalam keamanan siber. Hasil penelitian menunjukkan bahwa kombinasi antara teknologi keamanan berlapis seperti firewall, sistem deteksi intrusi, dan enkripsi data, serta pelatihan kesadaran keamanan bagi karyawan, mampu meningkatkan ketahanan organisasi terhadap serangan siber. Pendekatan ini tidak hanya efektif dalam menahan serangan teknis tetapi juga memperkuat budaya keamanan di seluruh lapisan organisasi.
Kata kunci: Era Digital, Sistem Informasi Akademik (SIA), Keamanan Siber, Pendekatan Keamanan Berlapis.

1. Pendahuluan

Dalam era digital yang terus berkembang pesat saat ini teknologi informasi dan komunikasi telah menjadi tulang punggung dari berbagai aspek kehidupan manusia, mulai dari sektor bisnis, pemerintahan, hingga kehidupan pribadi. Kecanggihan teknologi telah memfasilitasi kemudahan akses terhadap informasi, transaksi elektronik, serta pengelolaan data dengan cepat dan efisien (Haris Satriyawan & Divira Salsabiil Susanto, 2023). Salah satu kegiatan yang menggunakan teknologi informasi dalam pendidikan adalah sistem informasi akademik. Tujuan dari Sistem Informasi Akademik (SIA) adalah untuk menjawab secara tepat tuntutan universitas yang menginginkan layanan pendidikan yang terkomputerisasi untuk meningkatkan daya saing, kinerja, kualitas layanan, dan kualitas sumber daya manusia yang dihasilkan. Untuk menghemat waktu dan biaya, Sistem Informasi Akademik (SIA) sangat berguna untuk mengelola data nilai mahasiswa, mata kuliah, data staf pengajar (dosen), dan administrasi fakultas/jurusan. Tugas-tugas ini saat ini dilakukan secara manual, tetapi perangkat lunak dapat membantu(Rahmawati, 2012). SIA Ubhara Jaya merupakan sistem informasi akademik online yang dikelola oleh Universitas Bhayangkara Jakarta Raya. Dalam rangka memudahkan pengguna dalam menyelesaikan tugas-tugas pengelolaan akademik kampus secara online, termasuk proses Penerimaan Mahasiswa Baru (PMB), penjadwalan kuliah, pengisian Kartu Rencana Studi (KRS), entri nilai, pengelolaan data dosen dan mahasiswa, evaluasi belajar mengajar, dan tugas-tugas lainnya.

Akan tetapi, di sisi lain, peningkatan adopsi teknologi digital juga membuka celah bagi ancaman yang lebih besar terhadap keamanan informasi. Fenomena ini menuntut adanya keamanan siber yang efektif untuk melindungi sistem informasi dari potensi gangguan, baik yang disengaja maupun tidak disengaja, yang dapat merugikan individu maupun organisasi.

Keamanan siber atau cyber security kini bukan hanya menjadi perhatian bagi kalangan profesional TI, tetapi juga pemerintah dan masyarakat luas. Berbagai kebijakan dan regulasi mulai diterapkan untuk memastikan keamanan data publik dan pribadi dari ancaman serangan digital yang semakin canggih (Khoironi, 2020). Namun, upaya ini harus didukung oleh strategi keamanan yang efektif dan komprehensif, mengingat perkembangan serangan siber yang terus beradaptasi dengan teknologi baru. Pentingnya keamanan siber tidak hanya terbatas pada perlindungan aset fisik, tetapi juga reputasi dan kepercayaan masyarakat terhadap institusi yang bersangkutan. Ancaman terhadap keamanan siber di Indonesia kian mengkhawatirkan. Beberapa tahun terakhir, serangan siber yang mencakup malware, ransomware, dan pencurian

data pribadi semakin marak terjadi. Indonesia sebagai negara dengan populasi pengguna internet yang besar sering kali menjadi target empuk bagi pelaku kejahatan siber. Serangan ini tidak hanya menyerang perusahaan besar, tetapi juga lembaga pemerintah, yang sering kali menjadi sasaran karena lemahnya sistem keamanan yang diterapkan (Mahendra & Pinatih, 2023). Lemahnya keamanan siber di berbagai sektor ini menunjukkan bahwa implementasi keamanan siber yang efektif belum sepenuhnya terpenuhi, sehingga menimbulkan kekhawatiran akan dampak jangka panjang dari kelemahan ini.c

Masalah ini semakin terlihat dengan rendahnya tingkat kesadaran akan pentingnya keamanan digital di kalangan pengguna internet di Indonesia. Banyak pihak, baik individu maupun institusi, masih abai dalam menjaga keamanan data digital mereka (Burov, 2020). Ini disebabkan oleh berbagai faktor, seperti minimnya pengetahuan, kurangnya regulasi yang ketat, dan lemahnya kontrol terhadap penggunaan perangkat yang terhubung dengan internet. Fenomena ini menuntut adanya pendekatan yang lebih efektif dan strategis dalam penerapan keamanan siber agar dapat mengimbangi laju perkembangan teknologi yang semakin cepat (Camacho, 2024).

Berdasarkan data terbaru dari Badan Siber dan Sandi Negara (BSSN), terjadi lonjakan signifikan pada jumlah serangan siber di Indonesia pada tahun 2023, di mana lebih dari 900 juta serangan terdeteksi hanya dalam kurun waktu setahun. Serangan tersebut mencakup berbagai jenis ancaman, termasuk phishing, malware, dan Distributed Denial of Service (DDoS), yang sebagian besar menargetkan sektor keuangan dan pemerintahan (Safitra et al., 2023). Data ini menunjukkan bahwa Indonesia masih menghadapi tantangan besar dalam melindungi data dan sistem informasi vital dari potensi gangguan dan kerusakan akibat serangan siber.

Salah satu kasus besar yang terjadi baru-baru ini adalah peretasan terhadap salah satu lembaga perbankan besar di Indonesia yang mengakibatkan kebocoran data pribadi nasabah secara massal. Kasus ini memicu kepanikan di kalangan masyarakat, terutama bagi pengguna yang merasa dirugikan. Insiden ini juga mengungkap betapa rawannya sistem keamanan siber yang ada saat ini dan menyoroti pentingnya langkah-langkah mitigasi yang lebih ketat dan terstruktur dalam menghadapi ancaman siber.

Untuk menciptakan strategi keamanan siber yang efektif, beberapa komponen penting harus dipertimbangkan, termasuk pemahaman mendalam tentang jenis ancaman yang berkembang dan metode pencegahan yang dapat diimplementasikan secara menyeluruh (Kumar et al., 2023). Salah satu pendekatan yang dapat diterapkan adalah model pertahanan berlapis, yang melibatkan kombinasi teknologi canggih seperti enkripsi, firewall, sistem deteksi intrusi, serta upaya pelatihan bagi pengguna. Selain itu, kolaborasi antara pemerintah, sektor swasta, dan masyarakat sangat dibutuhkan untuk menciptakan lingkungan digital yang aman dan terlindungi dari segala potensi ancaman. Pengembangan regulasi yang mendukung keamanan siber juga menjadi kunci utama. Pemerintah perlu memperkuat peraturan yang terkait dengan perlindungan data pribadi dan keamanan informasi, mengingat bahwa regulasi dapat berfungsi sebagai landasan untuk memberikan rasa aman dan melindungi privasi

pengguna. Regulasi ini perlu dirancang dengan fleksibilitas untuk beradaptasi dengan ancaman baru, sehingga setiap sektor, mulai dari perbankan, e-commerce, hingga pendidikan, dapat menerapkan standar keamanan yang memadai (Luther Kington Nwobodo et al., 2024).

Tujuan dari penulisan ini adalah untuk mengidentifikasi strategi yang efektif dalam penerapan keamanan siber di Indonesia di tengah era digital yang semakin maju. Penelitian ini diharapkan dapat memberikan wawasan dan solusi bagi berbagai pihak terkait, baik individu, organisasi, maupun pemerintah, dalam menghadapi dan mengatasi ancaman keamanan digital yang semakin kompleks dan meluas. Melalui pendekatan komprehensif, diharapkan Indonesia dapat meningkatkan kesiapan dan keandalan sistem keamanannya dalam menghadapi serangan siber yang terus berkembang.

2. Metode Penelitian

Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif dengan pendekatan deskriptif. Penelitian kualitatif ini bertujuan untuk menggambarkan dan memahami strategi yang efektif dalam implementasi keamanan siber di era digital (Sugiyono, 2019). Teknik pengumpulan data dilakukan melalui wawancara mendalam dengan para ahli di bidang keamanan siber, termasuk dosen yang memiliki pemahaman mendalam tentang keamanan digital dan regulasi terkait. Selain wawancara, observasi dan dokumentasi juga digunakan untuk memperkaya data yang diperoleh dari informan, serta untuk memahami praktik keamanan siber yang telah diterapkan di berbagai institusi.

Sumber data yang digunakan dalam penelitian ini adalah data primer dan sekunder. Data primer diperoleh langsung dari hasil wawancara dengan informan, yaitu pengelola IT yang memahami keamanan siber serta profesional di bidang teknologi informasi yang berpengalaman dalam mengelola risiko keamanan digital (Creswell & Creswell, 2018). Sementara itu, data sekunder diperoleh dari literatur. Data yang terkumpul dianalisis dengan pendekatan tematik, yang memungkinkan peneliti untuk mengidentifikasi tema-tema kunci dalam strategi keamanan siber yang efektif dan komprehensif di era digital.

3. Hasil dan Pembahasan

Dalam wawancara yang sudah dilakukan dengan pengelola IT memulai dengan menggambarkan peran sentral mereka dalam tata kelola dan kebijakan IT di lingkungan kampus. Mereka bertanggung jawab atas seluruh aspek terkait pengelolaan IT, mulai dari kebijakan penggunaan hingga dokumentasi, yang berfungsi sebagai panduan penting bagi seluruh pengguna sistem informasi akademik (SIA) di kampus. Peran ini tidak hanya terbatas pada manajemen teknis, tetapi juga mencakup pengawasan penggunaan akses untuk memastikan bahwa setiap pengguna mematuhi kebijakan yang ditetapkan. Tanggung jawab ini mencakup berbagai aspek mulai dari pengaturan akses pengguna, pemisahan peran sesuai dengan kebutuhan, hingga pengendalian akses terhadap data dan informasi yang bersifat

sensitif. Ini adalah langkah awal yang signifikan untuk menjaga keamanan, karena memberikan batasan yang jelas dan memastikan bahwa sistem tetap dalam kendali yang tepat.

Pengelola menjelaskan strategi keamanan berlapis yang diterapkan untuk melindungi sistem informasi. Keamanan berlapis ini terdiri dari beberapa tahapan, yaitu keamanan fisik, lapisan administrasi, dan lapisan teknis, yang kesemuanya memiliki fungsi spesifik untuk mencegah akses yang tidak sah dan meminimalkan risiko serangan. Pada lapisan keamanan fisik, kampus menerapkan metode autentikasi menggunakan sidik jari (fingerprint) untuk mengontrol akses ke ruangan server yang menyimpan perangkat keras penting. Dengan adanya autentikasi fisik ini, hanya individu yang memiliki izin dan telah terdaftar yang dapat masuk, sehingga meminimalkan kemungkinan intervensi fisik dari pihak yang tidak berkepentingan. Langkah ini sangat penting, terutama dalam menjaga keamanan perangkat keras yang merupakan fondasi dari seluruh infrastruktur IT.

Lapisan kedua adalah keamanan administrasi di mana pengguna dibedakan berdasarkan peran dan hak akses masing-masing. Dalam hal ini, mahasiswa, dosen, dan program studi memiliki akses yang berbeda sesuai kebutuhan fungsionalnya. Mahasiswa misalnya, hanya diberi akses untuk melihat nilai dan mengisi Kartu Rencana Studi (KRS), sementara dosen memiliki hak akses untuk memasukkan nilai. Program studi memiliki kewenangan untuk mengatur jadwal kuliah, namun dosen dan mahasiswa tidak memiliki akses ke fitur ini. Struktur peran yang teratur ini mencerminkan pendekatan keamanan berbasis hak akses (access-based security) yang memungkinkan pengguna hanya dapat mengakses informasi yang relevan bagi mereka, sehingga mengurangi risiko eksploitasi sistem dari dalam. Hal ini juga memastikan bahwa setiap informasi yang bersifat krusial tidak bisa diakses sembarangan, yang menjadi langkah preventif untuk menjaga kerahasiaan data akademik.

Lapisan keamanan yang ketiga adalah keamanan teknis di mana teknologi seperti Cloudflare dan Fortigate digunakan sebagai penghalang utama terhadap ancaman jaringan eksternal, khususnya serangan Distributed Denial of Service (DDoS). Cloudflare bertindak sebagai pelindung utama dari serangan eksternal dengan memfilter setiap trafik yang masuk dan hanya mengizinkan akses yang sah, sedangkan Fortigate memberikan keamanan tambahan pada jaringan kampus untuk mengurangi kemungkinan adanya celah yang bisa dieksploitasi oleh pihak luar. Dalam penjelasannya, pengelola IT menggunakan analogi Cloudflare dan Fortigate sebagai "satpam digital" yang berjaga di depan jaringan, memastikan bahwa trafik yang masuk sudah melewati verifikasi awal sebelum diperbolehkan mengakses sistem. Pendekatan ini sangat penting dalam konteks keamanan siber modern, mengingat DDoS menjadi salah satu ancaman yang sering kali menargetkan lembaga-lembaga pendidikan dan pemerintah yang dianggap memiliki celah keamanan yang dapat dieksploitasi.

Di samping itu kampus ini juga memiliki sistem backup otomatis yang dilakukan setiap hari pada beberapa waktu tertentu, dengan tujuan untuk melindungi data dari risiko kehilangan atau kerusakan. Data akademik yang vital di-backup secara berkala, menciptakan lapisan perlindungan tambahan apabila terjadi insiden tak terduga seperti kerusakan server atau

percobaan peretasan yang berhasil. Langkah ini menunjukkan kepedulian institusi terhadap ketahanan data jangka panjang, terutama mengingat data akademik merupakan aset penting yang mendukung kegiatan administrasi dan layanan pendidikan.

Meskipun beberapa langkah protektif telah diterapkan, pengelola IT juga menyoroti adanya kelemahan dalam sistem SIA yang masih belum menggunakan autentikasi dua faktor (2FA). Hal ini menjadikan akun-akun dalam SIA lebih rentan terhadap upaya peretasan, karena autentikasi yang terbatas pada satu lapisan saja cenderung mudah disusupi oleh pihak yang tidak berwenang. Menyadari adanya risiko ini, pengelola IT menyampaikan bahwa ke depannya institusi perlu mempertimbangkan penerapan 2FA sebagai langkah peningkatan keamanan yang lebih canggih. Autentikasi dua faktor ini akan memberikan lapisan keamanan tambahan yang dapat mengurangi risiko pencurian data pengguna secara signifikan, terutama mengingat bahwa peretasan terhadap akun-akun pengguna menjadi salah satu ancaman yang kian meningkat.

Risiko lain yang ditekankan dalam wawancara ini adalah rendahnya tingkat kesadaran pengguna terhadap keamanan digital, terutama di kalangan mahasiswa dan staf pengajar. Banyak dari mereka yang mungkin belum memahami risiko yang melekat dalam penggunaan sistem informasi tanpa praktik keamanan yang tepat. Rendahnya kesadaran ini menimbulkan potensi celah yang bisa dimanfaatkan oleh pihak-pihak yang berniat jahat untuk mengeksploitasi data pribadi atau institusi. Dalam konteks ini, pengelola IT menekankan pentingnya edukasi berkelanjutan kepada seluruh pengguna sistem untuk meningkatkan pemahaman mereka tentang ancaman siber dan cara-cara dasar melindungi akun serta data mereka. Edukasi ini mencakup pengenalan terhadap ancaman seperti phishing, malware, dan cara-cara menjaga keamanan kata sandi. Ini adalah langkah kritis yang perlu diambil agar semua pihak yang terlibat dalam penggunaan sistem dapat berpartisipasi aktif dalam menjaga keamanan lingkungan digital institusi.

Dari hasil wawancara ini dapat disimpulkan bahwa strategi keamanan siber yang diterapkan pada institusi ini telah cukup terstruktur dengan baik, mencakup berbagai aspek teknis dan administratif untuk melindungi data dan infrastruktur digital kampus. Namun, ada beberapa area yang perlu ditingkatkan, seperti implementasi autentikasi dua faktor dan peningkatan kesadaran keamanan di kalangan pengguna. Tantangan keamanan siber di lingkungan pendidikan yang bersifat dinamis membutuhkan pendekatan yang komprehensif dan adaptif, agar dapat mengimbangi perkembangan teknologi yang kian cepat. Kolaborasi antara kebijakan yang kuat, teknologi pelindung yang canggih, dan pemahaman mendalam tentang keamanan digital di kalangan pengguna akan menjadi kunci utama untuk menciptakan lingkungan digital yang aman di era siber ini.

Hasil penelitian ini menunjukkan bahwa strategi keamanan siber yang efektif di era digital memerlukan penerapan pendekatan berlapis atau *layered security*, yang mengintegrasikan berbagai elemen teknologi dan kebijakan keamanan untuk menciptakan perlindungan sistem yang lebih komprehensif. Penggunaan teknologi seperti firewall, sistem

deteksi intrusi, dan enkripsi data yang kuat terbukti sangat penting untuk mencegah akses tidak sah serta melindungi informasi sensitif dari potensi serangan. Penggabungan teknologi-teknologi ini memberikan lapisan perlindungan yang dapat menghalangi berbagai bentuk serangan siber, baik yang berasal dari luar maupun dalam organisasi. Selain itu, strategi ini menjadi lebih efektif jika didukung dengan pengelolaan risiko yang terstruktur, di mana setiap potensi ancaman diidentifikasi dan dianalisis sejak dini sehingga langkah-langkah mitigasi dapat diambil secara tepat. Oleh karena itu, pendekatan keamanan berlapis yang dipadukan dengan manajemen risiko proaktif dianggap sebagai dasar utama dalam membangun strategi keamanan siber yang kokoh dan tahan terhadap berbagai jenis ancaman.

Penelitian juga menunjukkan bahwa aspek manusia memainkan peran penting dalam efektivitas keamanan siber. Banyak kasus pelanggaran keamanan yang terjadi akibat rendahnya kesadaran dan pengetahuan karyawan mengenai ancaman siber, terutama serangan yang memanfaatkan kelemahan manusia, seperti phishing dan rekayasa sosial. Peningkatan kesadaran keamanan melalui pelatihan rutin terbukti mampu mengurangi insiden serangan yang memanfaatkan kelemahan ini. Pelatihan ini memberikan pemahaman kepada karyawan tentang pentingnya menjaga keamanan data dan mengenali tanda-tanda serangan, sehingga mereka dapat bertindak lebih waspada dalam menjalankan tugas sehari-hari. Dengan meningkatkan kesadaran dan keterampilan karyawan dalam menghadapi ancaman siber, perusahaan dapat memperkuat keamanan internalnya secara signifikan.

Pemanfaatan teknologi kecerdasan buatan (AI) dan analitik keamanan siber berbasis data besar menjadi elemen penting yang disorot dalam penelitian ini sebagai solusi efektif dalam mendeteksi ancaman secara proaktif. Sistem berbasis AI mampu mengenali pola serangan yang kompleks dan melakukan respons lebih cepat sebelum serangan tersebut berkembang menjadi ancaman yang lebih besar. Teknologi ini juga dapat digunakan untuk menganalisis lalu lintas data dalam jaringan, sehingga setiap aktivitas mencurigakan dapat segera diidentifikasi dan ditangani. Dengan begitu, AI tidak hanya mempercepat deteksi ancaman tetapi juga meningkatkan akurasi dalam mengenali pola serangan, menjadikannya alat yang sangat berharga dalam strategi keamanan siber di era digital.

Hasil penelitian ini juga menunjukkan bahwa peran regulasi dan kolaborasi antar organisasi menjadi faktor pendukung penting dalam keberhasilan implementasi keamanan siber. Negara-negara dengan regulasi keamanan siber yang ketat dan mekanisme pengawasan yang jelas memiliki tingkat keberhasilan yang lebih tinggi dalam melindungi infrastruktur penting dari ancaman siber. Selain itu, kolaborasi antar industri dan kerja sama dengan lembaga pemerintah memungkinkan berbagi informasi tentang tren ancaman terbaru, strategi pencegahan, dan respons darurat. Kolaborasi ini menciptakan jaringan perlindungan yang lebih kuat, mengingat bahwa ancaman siber dapat terjadi lintas sektor dan sering kali memerlukan respons kolektif.

3.1. Implementasi Pendekatan Keamanan Berlapis (*Layered Security Approach*)

Pendekatan keamanan berlapis, atau layered security approach, merupakan strategi penting dalam perlindungan siber yang efektif menghadapi ancaman yang semakin kompleks di era digital. Strategi ini melibatkan penerapan beberapa lapisan perlindungan yang saling mendukung, di mana setiap lapisan berfungsi secara independen namun tetap terintegrasi. Dengan cara ini, jika salah satu lapisan keamanan berhasil ditembus, lapisan lainnya tetap dapat memberikan perlindungan tambahan. Pendekatan ini menggabungkan teknologi canggih, kebijakan keamanan yang ketat, serta keterlibatan pengguna, sehingga diharapkan dapat mengurangi risiko serangan dan memperkuat ketahanan infrastruktur teknologi informasi di berbagai sektor.

Organisasi yang menerapkan pendekatan ini menyadari bahwa ancaman siber datang dari berbagai sisi dan menggunakan teknik serangan yang beragam, mulai dari brute force, rekayasa sosial, hingga malware dan ransomware. Oleh karena itu, pendekatan keamanan berlapis tidak hanya sekadar menambah perangkat keamanan, tetapi juga menyusun strategi yang komprehensif untuk menghadapi berbagai skenario ancaman. Prinsip utama dari pendekatan ini adalah menciptakan serangkaian perlindungan yang berbeda, yang dikenal sebagai "Defense in Depth" atau pertahanan mendalam, di mana setiap lapisan memiliki tujuan spesifik dalam meminimalisir risiko dan dampak serangan.

Salah satu komponen kunci dalam pendekatan ini adalah perlindungan perimeter, yang biasanya diimplementasikan melalui firewall. Firewall berfungsi sebagai garis pertahanan pertama yang mengontrol arus lalu lintas data antara jaringan internal dan eksternal, memblokir akses tidak sah, dan mengidentifikasi pola lalu lintas yang mencurigakan. Selain itu, sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) juga berperan penting dalam mendeteksi dan menghentikan serangan yang berusaha memasuki jaringan. IDS melaporkan potensi ancaman, sementara IPS bertindak lebih agresif dengan memblokir atau memutus koneksi yang dianggap berisiko tinggi. Dengan pendekatan ini, organisasi dapat menjaga kontinuitas perlindungan meskipun terdapat kekurangan pada satu aspek keamanan.Pendekatan keamanan berlapis melibatkan beberapa lapisan perlindungan, yang masing-masing memiliki fungsi spesifik dan saling mendukung. Lapisan-lapisan ini biasanya meliputi keamanan jaringan, keamanan endpoint, enkripsi data, autentikasi pengguna, manajemen akses, hingga edukasi dan pelatihan karyawan. Setiap lapisan bekerja secara sinergis untuk menciptakan sistem keamanan yang lebih kompleks dan sulit ditembus.

1. Firewall dan Sistem Deteksi/Pencegahan Intrusi

   Firewall berfungsi sebagai garis pertahanan pertama dalam keamanan jaringan dengan mengontrol lalu lintas data untuk membatasi akses yang tidak sah dan mengurangi risiko serangan eksternal. Bersama dengan sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS), firewall memberikan perlindungan tambahan dengan mendeteksi dan memblokir serangan dalam lalu lintas jaringan.
2. Keamanan Endpoint

Keamanan endpoint melindungi perangkat akhir yang terhubung ke jaringan, seperti komputer, laptop, dan ponsel, dari infeksi melalui perangkat lunak antivirus dan anti-malware. Kebijakan ketat terkait akses perangkat, seperti pembatasan akses USB dan kontrol aplikasi yang diizinkan, juga mendukung perlindungan ini.

3. Enkripsi Data

   Enkripsi adalah proses mengubah data menjadi kode yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi, sehingga melindungi data sensitif seperti informasi pelanggan atau keuangan dari kebocoran atau pencurian. Enkripsi dapat diterapkan pada data yang sedang transit di jaringan maupun data yang tersimpan di perangkat.

4. Autentikasi Multi-Faktor (MFA)

   Sistem autentikasi multi-faktor (MFA) meningkatkan keamanan akses dengan mengharuskan pengguna mengonfirmasi identitas melalui lebih dari satu faktor, seperti kombinasi kata sandi, sidik jari, atau kode OTP. Hal ini membuat akses ke sistem lebih aman, terutama dari serangan peretasan kata sandi.

5. Pelatihan dan Kesadaran Keamanan Pengguna

   Salah satu kelemahan utama dalam keamanan siber adalah faktor manusia. Pelatihan keamanan bagi karyawan untuk mengenali potensi ancaman, seperti phishing, rekayasa sosial, atau email berbahaya, dapat mengurangi risiko keamanan yang berasal dari tindakan pengguna. Dengan pemahaman yang baik tentang praktik keamanan siber, pengguna dapat mengidentifikasi ancaman dengan lebih cepat dan menghindari tindakan yang berisiko.

Meskipun pendekatan keamanan berlapis memiliki banyak manfaat, implementasinya menghadapi tantangan yang perlu diatasi oleh organisasi. Biaya penerapan teknologi dan perangkat keamanan yang beragam dapat menjadi hambatan, terutama bagi organisasi kecil dan menengah, karena setiap lapisan memerlukan investasi dalam perangkat keras, perangkat lunak, dan pelatihan. Selain itu, kompleksitas manajemen sistem meningkat, karena setiap lapisan memerlukan pemantauan yang konsisten.

Tantangan lain adalah integrasi teknologi dari vendor yang berbeda, yang dapat menciptakan celah keamanan jika tidak terintegrasi dengan baik. Oleh karena itu, penting bagi organisasi untuk memilih teknologi yang kompatibel. Pengelolaan sumber daya manusia juga menjadi tantangan, karena staf TI perlu memiliki pemahaman mendalam tentang setiap lapisan keamanan untuk memaksimalkan penggunaannya.

Implementasi pendekatan keamanan berlapis memberikan manfaat signifikan dalam melindungi organisasi dari ancaman siber yang semakin kompleks. Pendekatan ini menciptakan lingkungan yang lebih aman dengan lapisan perlindungan yang dapat mengidentifikasi, mencegah, dan merespons serangan yang mungkin lolos dari satu lapisan. Dengan berbagai lapisan perlindungan, organisasi dapat meminimalisir dampak serangan jika salah satu lapisan

berhasil ditembus. Selain itu, pendekatan ini memungkinkan organisasi menyesuaikan tingkat keamanan sesuai kebutuhan, seperti sektor keuangan atau kesehatan yang memerlukan perlindungan lebih ketat. Fleksibilitas ini memberikan kendali yang lebih baik dalam menentukan strategi keamanan. Penerapan pendekatan keamanan berlapis juga mendorong budaya keamanan di seluruh organisasi, di mana setiap karyawan berperan dalam menjaga keamanan siber.

Pendekatan keamanan berlapis atau *layered security* adalah Pendekatan keamanan berlapis adalah strategi efektif untuk melindungi sistem dan data dari serangan siber yang semakin kompleks. Dengan mengintegrasikan berbagai teknologi keamanan, manajemen risiko proaktif, dan melibatkan peran karyawan, organisasi dapat meningkatkan ketahanan terhadap berbagai ancaman. Meskipun ada tantangan dalam implementasinya, seperti biaya, integrasi teknologi, dan kebutuhan pelatihan, manfaat jangka panjangnya jauh lebih besar. Untuk meningkatkan efektivitasnya, organisasi disarankan melakukan evaluasi risiko secara berkala, memastikan kompatibilitas teknologi, dan memberikan pelatihan keamanan rutin kepada staf. Dengan pendekatan yang terencana, organisasi dapat mengurangi risiko ancaman siber dan menciptakan lingkungan digital yang lebih aman.

3.2. Peningkatan Kesadaran dan Kompetensi Sumber Daya Manusia

Dalam era digital saat ini ancaman keamanan siber tidak hanya datang dari aspek teknis, tetapi juga dari kesalahan dan ketidaktahuan manusia yang sering menjadi pintu masuk utama bagi serangan siber. Oleh karena itu, selain penerapan teknologi keamanan yang canggih, meningkatkan kesadaran dan kompetensi sumber daya manusia (SDM) telah menjadi aspek krusial dalam memperkuat pertahanan organisasi terhadap berbagai ancaman siber. Hal ini penting mengingat teknologi secanggih apapun tidak akan efektif tanpa adanya kesadaran dan keterampilan pengguna dalam mengoperasikan dan menjaga keamanan perangkat mereka. Peningkatan kompetensi SDM meliputi pemahaman terhadap ancaman siber, kemampuan mengenali indikasi serangan, hingga keterampilan dalam menerapkan langkah-langkah pencegahan.

Kelemahan utama yang sering dimanfaatkan oleh penyerang siber adalah titik lemah dari faktor manusia, yang meliputi ketidaksadaran pengguna akan risiko keamanan, kebiasaan buruk dalam pengelolaan kata sandi, serta ketidakpahaman dalam menghadapi ancaman seperti *phishing* dan *social engineering*. Ketika pengguna tidak memahami dampak dari tindakan yang tampak sederhana, seperti mengklik tautan yang mencurigakan, risiko keamanan meningkat. Selain itu, keterbatasan pengetahuan teknis juga membuat banyak individu tidak menyadari perlunya pembaruan perangkat lunak dan pembaruan keamanan. Dalam konteks inilah peningkatan kesadaran dan kompetensi SDM menjadi fokus utama dalam strategi keamanan siber. Kesadaran keamanan siber merupakan kesadaran karyawan terhadap risiko dan ancaman yang terkait dengan penggunaan teknologi dalam aktivitas sehari-hari. Kesadaran ini meliputi pemahaman tentang pentingnya menjaga informasi sensitif, mengenali teknik serangan yang sering digunakan seperti phishing dan malware, serta kemampuan untuk

bertindak dengan tepat jika menghadapi situasi yang mencurigakan. Kesadaran yang tinggi terhadap ancaman siber memungkinkan karyawan untuk lebih berhati-hati dalam setiap tindakan yang berhubungan dengan teknologi, sehingga mengurangi risiko terjadinya serangan yang melibatkan kesalahan manusia.

Peningkatan kesadaran keamanan tidak hanya relevan bagi karyawan di divisi teknologi informasi, tetapi juga bagi seluruh lapisan organisasi. Ketika seluruh karyawan memiliki pemahaman yang sama mengenai pentingnya menjaga keamanan data dan informasi, perusahaan secara keseluruhan akan memiliki pertahanan yang lebih kuat. Dalam hal ini, setiap anggota organisasi menjadi "barikade pertama" dalam menghadapi potensi serangan siber. Peningkatan kesadaran juga menciptakan budaya keamanan di mana setiap tindakan yang berhubungan dengan penggunaan teknologi dilakukan dengan penuh perhatian dan tanggung jawab.

Kompetensi atau keterampilan keamanan siber merupakan faktor penting dalam memastikan bahwa SDM memiliki kemampuan teknis yang memadai untuk menangani ancaman siber. Kompetensi ini mencakup pemahaman terhadap prosedur keamanan, penggunaan perangkat keamanan yang tepat, dan kemampuan dalam mengambil keputusan yang tepat saat menghadapi potensi ancaman. Peningkatan kompetensi keamanan siber biasanya dilakukan melalui pelatihan yang dirancang khusus untuk meningkatkan keterampilan karyawan dalam menghadapi ancaman yang terus berkembang. Kompetensi keamanan siber yang tinggi memungkinkan karyawan untuk lebih sigap dan terampil dalam menangani situasi krisis, seperti serangan phishing yang menyasar data organisasi atau malware yang mencoba mengakses sistem. Karyawan dengan kompetensi yang baik dapat menjadi aset yang berharga dalam merespons insiden keamanan, karena mereka mampu menerapkan protokol keamanan dengan tepat dan mengurangi dampak dari serangan siber. Dengan meningkatnya kompetensi ini, organisasi tidak hanya memiliki staf yang lebih sigap dalam menghadapi ancaman, tetapi juga lebih andal dalam melindungi data sensitif.

Implementasi program peningkatan kesadaran dan kompetensi keamanan siber sering kali menghadapi sejumlah tantangan, terutama dalam hal biaya, komitmen, dan resistensi dari karyawan. Tantangan utama adalah biaya yang terkait dengan penyediaan pelatihan berkualitas serta teknologi yang mendukung keamanan siber. Pelatihan yang efektif biasanya memerlukan anggaran yang cukup besar, khususnya bagi organisasi yang memiliki jumlah karyawan yang banyak. Selain itu, diperlukan waktu dan sumber daya untuk menyusun program pelatihan yang komprehensif, yang mencakup aspek teoritis dan praktik keamanan siber. Tantangan lainnya adalah komitmen dari karyawan untuk mengikuti pelatihan keamanan siber. Tidak semua karyawan menyadari pentingnya pelatihan ini atau merasa bahwa mereka tidak memiliki waktu luang untuk mempelajari topik yang teknis. Banyak karyawan yang merasa pelatihan keamanan hanya menjadi tambahan beban kerja, yang pada akhirnya menyebabkan rendahnya partisipasi dalam pelatihan. Selain itu, resistensi terhadap perubahan juga menjadi tantangan, di mana sebagian karyawan mungkin merasa tidak nyaman dengan praktik

keamanan baru atau aturan yang lebih ketat terkait penggunaan perangkat digital. Dalam hal ini, organisasi perlu menemukan cara untuk memotivasi dan meyakinkan karyawan bahwa partisipasi aktif dalam pelatihan keamanan akan memberikan manfaat besar bagi mereka dan organisasi secara keseluruhan.

Untuk mengatasi tantangan yang ada beberapa strategi dapat diimplementasikan untuk meningkatkan kesadaran dan kompetensi keamanan siber di kalangan karyawan. Pertama, pelatihan keamanan siber yang terstruktur dan interaktif dapat diberikan secara berkala, baik melalui seminar, lokakarya, atau sesi simulasi. Pelatihan ini dirancang dengan pendekatan yang mudah dipahami oleh karyawan dari berbagai latar belakang, sehingga mereka dapat memahami konsep keamanan tanpa memerlukan pengetahuan teknis yang mendalam. Simulasi serangan phishing atau praktik keamanan sederhana seperti pengelolaan kata sandi yang aman dapat meningkatkan kesadaran karyawan dengan cara yang lebih praktis.

Kampanye kesadaran keamanan juga dapat dijalankan untuk mengingatkan karyawan tentang praktik keamanan sehari-hari. Kampanye ini dapat berupa poster yang ditempatkan di lingkungan kerja, pengumuman di intranet perusahaan, atau pengingat berkala melalui email tentang pentingnya keamanan siber. Strategi ini efektif untuk menciptakan budaya keamanan siber yang terus-menerus diperkuat, sehingga karyawan selalu waspada terhadap potensi ancaman. Dengan penerapan kampanye yang konsisten, karyawan akan lebih mudah mengingat langkah-langkah yang perlu diambil untuk menjaga keamanan data dan informasi.

Pemanfaatan teknologi dalam pelatihan keamanan siber dapat membantu meningkatkan kompetensi karyawan secara efektif. Misalnya, simulasi serangan siber berbasis teknologi, seperti pelatihan menggunakan perangkat lunak *Cyber Range*, memungkinkan karyawan berlatih dalam lingkungan virtual yang menyerupai situasi nyata. Teknologi ini memberikan pengalaman praktik yang lebih mendalam, di mana karyawan bisa merasakan langsung bagaimana sistem keamanan dioperasikan serta langkah-langkah yang perlu diambil ketika menghadapi serangan. Dengan demikian, teknologi membantu karyawan mempelajari keamanan siber melalui pendekatan yang lebih interaktif dan aplikatif.

Alat berbasis kecerdasan buatan (AI) juga dapat membantu dalam mengenali pola ancaman dan memberikan pembelajaran otomatis bagi karyawan. Dengan menggunakan AI, organisasi dapat mendeteksi kesalahan keamanan yang sering dilakukan oleh karyawan dan memberikan umpan balik yang langsung dan personal. Misalnya, jika seorang karyawan sering membuka tautan yang mencurigakan, sistem AI dapat memberi peringatan dan menyarankan tindakan yang lebih aman. Pemanfaatan teknologi ini membantu karyawan mengidentifikasi kebiasaan yang dapat membahayakan keamanan serta mempelajari cara mengatasinya secara tepat.

Peningkatan kesadaran dan kompetensi SDM dalam keamanan siber tidak hanya memberikan perlindungan terhadap ancaman siber dalam jangka pendek, tetapi juga menciptakan manfaat jangka panjang bagi organisasi. Dengan memiliki karyawan yang sadar akan pentingnya keamanan dan terampil dalam menangani risiko siber, organisasi dapat

mengurangi potensi kerugian finansial yang disebabkan oleh pelanggaran keamanan. Sebuah tim SDM yang kompeten dalam keamanan siber juga mampu merespons insiden keamanan dengan lebih cepat, mengurangi risiko kebocoran data, serta meminimalisir dampak negatif terhadap reputasi perusahaan. Budaya keamanan yang terbangun melalui peningkatan kesadaran dan kompetensi SDM akan berdampak positif terhadap seluruh aspek operasional perusahaan. Ketika karyawan memiliki kebiasaan yang baik dalam menjaga keamanan digital, mereka juga akan lebih teliti dalam menjaga privasi informasi pelanggan, yang pada gilirannya meningkatkan kepercayaan pelanggan. Dalam jangka panjang, perusahaan dengan reputasi keamanan yang kuat akan memiliki keunggulan kompetitif yang lebih baik dibandingkan perusahaan yang tidak menempatkan keamanan siber sebagai prioritas.

Peningkatan kesadaran dan kompetensi sumber daya manusia dalam keamanan siber merupakan langkah esensial untuk membangun pertahanan yang kuat di era digital. Dengan memberikan pelatihan keamanan siber yang komprehensif, memanfaatkan teknologi untuk pelatihan interaktif, dan menciptakan budaya keamanan yang berkesinambungan, organisasi dapat mengurangi risiko serangan siber yang melibatkan kesalahan manusia. Selain itu, peningkatan kesadaran dan kompetensi ini juga memberikan manfaat jangka panjang dalam memperkuat kepercayaan pelanggan dan menjaga reputasi perusahaan. Untuk memaksimalkan hasil dari program ini, perusahaan disarankan untuk melakukan evaluasi berkala terhadap tingkat pemahaman karyawan dan menyesuaikan program pelatihan sesuai dengan perkembangan ancaman siber terbaru. Dengan upaya yang konsisten, peningkatan kesadaran dan kompetensi SDM akan berkontribusi secara signifikan terhadap ketahanan organisasi dalam menghadapi tantangan keamanan siber yang semakin kompleks.

4. Kesimpulan

Dalam menghadapi ancaman keamanan siber yang semakin kompleks di era digital, strategi yang efektif untuk implementasi keamanan siber harus mencakup pendekatan yang menyeluruh dan adaptif. Pendekatan berlapis (*layered security approach*) yang mengombinasikan teknologi seperti firewall, sistem deteksi intrusi, dan enkripsi data, serta kesadaran dan kompetensi SDM, terbukti meningkatkan ketahanan sistem terhadap berbagai serangan. Selain itu, peningkatan kesadaran dan kompetensi sumber daya manusia memainkan peran penting dalam memperkuat keamanan organisasi, karena karyawan yang terlatih mampu mengenali dan mencegah ancaman yang mengincar titik lemah manusia. Implementasi keamanan yang efektif tidak hanya bergantung pada teknologi, tetapi juga budaya keamanan yang diterapkan di seluruh organisasi.

Melalui strategi yang terpadu dan komprehensif, perusahaan dapat membangun sistem keamanan yang lebih kokoh dan responsif terhadap dinamika ancaman siber yang terus berkembang. Dengan perencanaan yang matang, evaluasi berkala, dan penerapan teknologi yang sesuai, organisasi akan lebih siap menghadapi risiko digital dan melindungi data yang menjadi aset penting. Ke depan, diharapkan setiap organisasi dapat terus meningkatkan

kesiapan dan keamanan sibernya sehingga mampu menjalankan operasional secara aman dan efektif, menjaga kepercayaan publik, serta menghadapi tantangan era digital dengan lebih percaya diri.

Daftar Pustaka

Burov, O. (2020). Cybersecurity and Innovative Digital Educational Environment. *Information Technologies and Learning Tools*, *80*(6), 414–430. https://doi.org/10.33407/itlt.v80i6.4159

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN:3006-4023*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

Creswell, J. W., & Creswell, J. D. (2018). Mixed Methods Procedures. In *Research Defign: Qualitative, Quantitative, and Mixed M ethods Approaches*.

Haris Satriyawan, & Divira Salsabiil Susanto. (2023). Optimasi Keamanan Smart Grid Melalui Autentikasi Dua Lapis: Meningkatkan Efisiensi dan Privasi dalam Era Digital. *Jurnal RESTIKOM : Riset Teknik Informatika Dan Komputer*, *5*(3), 319–333. https://doi.org/10.52005/restikom.v5i3.254

Khoironi, S. C. (2020). Pengaruh Analisis Kebutuhan Pelatihan Budaya Keamanan Siber Sebagai Upaya Pengembangan Kompetensi bagi Aparatur Sipil Negara di Era Digital. *Jurnal Studi Komunikasi Dan Media*, *24*(1), 37. https://doi.org/10.31445/jskm.2020.2945

Kumar, S., Gupta, U., Singh, A. K., & Singh, A. K. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era Sarvesh. *Journal of Computers, Mechanical and Management*, *2*(3), 31–42. https://doi.org/10.57159/gadl.jcmm.2.3.23064

Luther Kington Nwobodo, Chioma Susan Nwaimo, & Ayodeji Enoch Adegbola. (2024). Enhancing cybersecurity protocols in the era of big data and advanced analytics. *GSC Advanced Research and Reviews*, *19*(3), 203–214. https://doi.org/10.30574/gscarr.2024.19.3.0211

Mahendra, Y. C., & Pinatih, N. K. D. S. A. (2023). Strategi Penanganan Keamanan Siber (Cyber Security) Di Indonesia. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *6*(4), 1941–1949.

Rahmawati. (2012). Analisis penerapan sistem informasi akademik (siakad). *Jurnal Adminsitrasi Publik*, *3*, 25–31.

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. In *Sustainability (Switzerland)* (Vol. 15, Issue 18). https://doi.org/10.3390/su151813369

Sugiyono, P. D. (2019). Buku sugiyono, metode penelitian kuantitatif kualitatif. In *Revista Brasileira de Linguística Aplicada* (Vol. 5, Issue 1).