JURNAL ABDIMAS INDONESIA Vol. 5, No. 4, 2025
E-ISSN 2797-2887
Copyright © 2025 The Author(s)

Penguatan Pertahanan Siber dalam Infrastruktur Data Pangan Nasional: Firewall Cloud Terintegrasi dan Pendekatan Pendidikan Rekayasa Sosial

Misni,
Universitas Mercu Buana, Jakarta, Indonesia

Penulis Korespondensi:
Misni
Misni.muhammad@mercubuana.ac.id

Abstrak:

Studi ini menggambarkan bahwa strategi keamanan siber yang komprehensif—menggabungkan pertahanan teknologi canggih dengan inisiatif yang berpusat pada manusia—dapat secara substansial meningkatkan postur keamanan aset nasional utama. Pusat Data Pangan Nasional (NFDC) menerapkan strategi berlapis ganda yang terdiri dari pengoptimalan firewall cloud dan pelatihan ketahanan rekayasa sosial terstruktur, yang mengarah pada peningkatan yang signifikan: tingkat keberhasilan phishing menurun sebesar 45%, persentase lalu lintas berbahaya yang diblokir meningkat sebesar 30%, dan insiden pelaporan meningkat sebesar 60%. Hasil ini menggarisbawahi meningkatnya kesepakatan bahwa keamanan siber tidak dapat bergantung secara eksklusif pada pertahanan teknologi atau kewaspadaan staf saja. Strategi perlindungan yang ekstensif dan multi-segi sangat penting, mengatasi kelemahan sistem dan elemen manusia. Penelitian ini menekankan pentingnya investasi berkelanjutan dalam pengaturan firewall adaptif, pelatihan keamanan yang komprehensif, dan kolaborasi antar-lembaga yang kuat untuk mempertahankan perlindungan yang memadai. Kontribusi studi ini sangat relevan untuk lembaga sektor publik yang mengawasi basis data sensitif dan kritis. Karena ancaman dunia maya menjadi lebih rumit dan fleksibel, perusahaan harus maju melampaui strategi reaktif dan menerapkan kerangka kerja keamanan yang proaktif dan berbasis intelijen. Ini memerlukan peningkatan teknis dan transformasi budaya menuju kesadaran siber di semua tingkatan organisasi. Studi di masa depan harus menyelidiki penggabungan kecerdasan buatan untuk identifikasi ancaman real-time, perumusan model kematangan keamanan siber nasional, dan pelaksanaan latihan simulasi berbasis skenario yang canggih untuk mengevaluasi ketahanan. Pedoman ini akan membantu institusi dalam mengembangkan sistem pertahanan yang gesit, responsif, dan terukur. Dengan menerapkan strategi pertahanan yang fleksibel dan mendalam yang mengintegrasikan teknologi dan kesiapan perilaku, lembaga seperti NFDC dapat lebih efisien melindungi aset digital mereka, memastikan kelangsungan operasional, dan meningkatkan kepercayaan publik terhadap integritas sistem informasi nasional di era yang semakin digital

Kata Kunci: Cybersecurity; Cloud Firewall; Social Engineering; Data Center Security; Threat Mitigation;

Pendahuluan

Mengawasi statistik penting yang menginformasikan kebijakan pertanian, logistik rantai pasokan, program gizi, dan sistem tanggap bencana, Pusat Data Pangan Nasional (NFDC) memainkan peran penting dalam ketahanan pangan nasional Indonesia (Organisasi Pangan dan Pertanian, 2002). Keamanan pusat data yang ditetapkan sebagai Infrastruktur Nasional Kritis (CNI) menjadi semakin penting karena pesatnya perkembangan digitalisasi sektor publik (International Telecommunication Union, n.d.). Aktor yang disponsori negara, penjahat dunia maya, dan peretas semakin menargetkan Infrastruktur Nasional Kritis (CNI) untuk mengikis kepercayaan publik, menerapkan tekanan geopolitik, atau menghasilkan keuntungan finansial (Badan Uni Eropa untuk Keamanan Siber, 2017). Ancaman modern, seperti ancaman persisten tingkat lanjut (APT) dan serangan yang berpusat pada manusia seperti phishing, umpan, dan dalih, telah terbukti terlalu rumit untuk ditangani oleh langkah-langkah keamanan siber tradisional, termasuk firewall, sistem deteksi intrusi, dan perangkat lunak antivirus (Sharma et al., 2023; Wang et al., 2023). Menurut penelitian, kesalahan atau manipulasi manusia menyumbang sekitar 85% dari pelanggaran yang berhasil, mengungguli kemanjuran pertahanan teknis murni (National Institute of Standards and Technology, nd).

Studi ini menyajikan strategi keamanan siber dua cabang yang dibuat untuk NFDC. Bagian pertama adalah menambahkan inspeksi paket mendalam, pemfilteran adaptif, dan deteksi ancaman otomatis real-time ke firewall cloud. Strategi kedua memanfaatkan kerentanan manusia melalui program ketahanan rekayasa sosial yang komprehensif, termasuk lokakarya keamanan interaktif, simulasi phishing, dan penilaian perilaku berulang. Sebelum langkah-langkah ini diambil, penilaian kerentanan awal dilakukan. Hasilnya, sistem pemantauan ditingkatkan, aturan firewall diatur ulang, dan karyawan NFDC menerima pelatihan sistematis (Obi et al., 2024; Falowo et al., 2022). Setelah penerapan, waktu reaksi insiden rata-rata meningkat sebesar 35%, deteksi aktivitas berbahaya meningkat sebesar 60%, dan tingkat keberhasilan phishing di NFDC turun sebesar 45%. Hasil ini mendukung penelitian terbaru, menekankan perlunya mengintegrasikan prosedur keamanan teknologi dengan perilaku manusia (Bagheri & Shameli-Sendi, 2020).

Mereka menunjukkan ketidakcukupan hanya mengandalkan pertahanan perimeter atau pelatihan personel yang terisolasi. Organisasi harus menerapkan strategi perlindungan berlapis-lapis yang mencakup aspek teknologi dan psikologis, terutama yang bertanggung jawab untuk mengelola data tingkat nasional. Temuan ini menggarisbawahi pentingnya investasi berkelanjutan dalam kesadaran perilaku, berbagi intelijen antar-lembaga, dan teknologi adaptif untuk membangun kerangka kerja keamanan siber yang kuat. Studi ini menyajikan rencana keamanan siber mendalam pertahanan yang praktis dan dapat diperluas untuk infrastruktur nasional penting (CNI) yang dikelola pemerintah. Melalui integrasi kesiapan perilaku dan kompetensi teknis, NFDC telah meningkatkan ketahanan sibernya secara signifikan. Pendekatan ini dapat berfungsi sebagai templat untuk organisasi serupa yang menghadapi ancaman dunia maya yang kompleks. Untuk memastikan peningkatan berkelanjutan kematangan keamanan siber nasional, studi di masa depan harus melihat program pelatihan staf gamifikasi, pembelajaran federasi, dan deteksi ancaman yang ditambah AI (Chen et al., 2023).

Meningkatnya kompleksitas ancaman dunia maya yang menargetkan sistem data federal telah membuat perlindungan infrastruktur nasional yang vital, termasuk Pusat Data Pangan Nasional (NFDC), menjadi tanggung jawab utama. Karena mereka memberikan solusi yang dapat diskalakan dan fleksibel untuk mengontrol kontrol akses,

Copyright © 2025 The Author(s)

menegakkan aturan keamanan, dan memfilter lalu lintas berbahaya di pengaturan cloud yang jauh, firewall cloud sangat penting untuk sistem keamanan siber kontemporer (Suetor et al., 2025; Smith & Lee, 2022). Kemajuan terbaru dalam teknologi firewall cloud, termasuk deteksi anomali, pemfilteran sadar konteks, dan pembaruan aturan otomatis, telah secara signifikan meningkatkan ketahanan sistem dan mengurangi upaya akses yang tidak sah. Namun, pertahanan teknis tidak cukup dengan sendirinya. Ada banyak bukti bahwa kesalahan manusia adalah sumber utama kerentanan keamanan siber. Lebih dari 70% serangan siber yang efektif dimulai dengan taktik rekayasa sosial, seperti phishing, iming-iming, dan dalih , yang mengeksploitasi kelemahan perilaku dan kepercayaan manusia daripada kerentanan teknis, menurut Jones dan Patel (2021). Hal ini mendukung keyakinan yang dipegang secara luas dalam literatur keamanan siber bahwa aspek yang paling rentan dari tindakan defensif seringkali adalah elemen manusia (Kindervag, 2021). Dalam analisis mereka terhadap lebih dari 200 studi kasus organisasi, Tambe et al. (2023) menyoroti manfaat mengintegrasikan perlindungan teknologi dengan intervensi yang berpusat pada manusia, terutama di bidang yang melibatkan data sensitif atau dapat diakses publik. Dibandingkan dengan perusahaan yang mengandalkan teknologi secara eksklusif, mereka yang menerapkan konfigurasi firewall yang canggih dan berfokus pada inisiatif pelatihan karyawan melihat penurunan 50-70% dalam insiden pelanggaran. Terlepas dari hasil yang menggembirakan ini, sedikit penelitian telah dilakukan secara khusus tentang bagaimana solusi terintegrasi yang baik bekerja di lingkungan pusat data nasional, terutama yang bertanggung jawab atas operasi sektor publik yang vital, seperti ketahanan pangan, di mana ketersediaan dan kualitas data memiliki dampak sosial yang signifikan. Dengan menerapkan arsitektur keamanan siber berlapis ganda di NFDC dan mengevaluasi hasil teknologi dan peningkatan perilaku, penelitian ini mengisi kesenjangan penelitian.

Tabel 1. Ringkasan Komparatif Penelitian Sebelumnya

Belajar	**Fokus**	**Temuan Utama**	**Kesenjangan Diidentifikasi**
Smith & Lee	Pengoptimalan firewall cloud	Kumpulan aturan lanjutan dan pembaruan otomatis meningkatkan efektivitas firewall sebesar ~40%.	Tidak memiliki integrasi dengan solusi faktor manusia.
Jones & Patel	Kesalahan manusia dalam pelanggaran dunia maya	70% pelanggaran berasal dari rekayasa sosial dan kesalahan manusia.	Tidak menilai pendekatan pertahanan teknis-manusia gabungan
Chen dkk.	Strategi pertahanan terintegrasi	Menggabungkan teknologi + pelatihan mengurangi pelanggaran sebesar 50–70%.	Tidak ada aplikasi khusus di pusat data nasional/sektor publik.

Studi ini mengkonsolidasikan penelitian sebelumnya untuk mengusulkan dan mengevaluasi model keamanan siber holistik untuk NFDC. Ini menggabungkan metodologi firewall cloud yang inovatif di samping pelatihan rekayasa sosial praktis untuk meningkatkan postur keamanan pusat

Metode Pelaksanaan

Studi ini menggunakan pendekatan metodis dan bertahap yang dirancang untuk melibatkan sumber daya manusia dan teknis Pusat Data Pangan Nasional (NFDC). Metodologi ini dipandu oleh praktik terbaik dalam desain intervensi keamanan siber (Obi et al., 2024) dan dimodifikasi agar sesuai dengan konteks operasi NFDC.

Langkah 1: Penilaian Kerentanan

Penelitian dimulai dengan penilaian komprehensif kerentanan dalam arsitektur cloud NFDC. Kami melakukan pengujian penetrasi eksternal dan pemindaian sistem internal untuk mengevaluasi postur keamanan. Nessus (Wenny & Pamuji, 2024) dan OpenVAS (Sharma et al., 2024) telah digunakan untuk mengidentifikasi kerentanan perangkat lunak, kesalahan konfigurasi, port terbuka, tambalan usang, dan titik akhir yang tidak aman. Kami menambah pemindaian ini dengan penilaian manual yang didasarkan pada metodologi OWASP Top 10 (Cerullo, 2009) untuk memastikan deteksi kerentanan aplikasi web yang paling signifikan, termasuk injeksi SQL, skrip lintas situs (XSS), dan paparan data sensitif.

Langkah 2: Pengoptimalan firewall cloud

Mengingat temuan kerentanan, kami merestrukturisasi sistem firewall cloud menggunakan kerangka kerja arsitektur zero-trust (ZTA), yang mematuhi premis tidak ada kepercayaan implisit untuk perangkat atau pengguna apa pun, terlepas dari lokasi jaringan. Langkah-langkah khusus termasuk yang berikut:

1. Kumpulan aturan komprehensif menargetkan vektor serangan yang diidentifikasi, seperti serangan penolakan layanan terdistribusi (DDoS), serangan injeksi, dan upaya brute-force (Ramzan et al., 2023).
2. Strategi pemblokiran geografis membatasi akses ke jangkauan IP internasional yang tidak penting, sehingga mengurangi kerentanan terhadap pelaku ancaman eksternal (Kumar et al., 2017).
3. Menggabungkan intelijen ancaman otomatis dengan memanfaatkan umpan dari sumber industri terkemuka (misalnya, FireEye dan IBM X-Force) untuk memperbarui kebijakan firewall secara bersamaan (Haque & Krishnan, 2021).

Kontrol akses berbasis peran (RBAC) secara ketat membatasi otoritas administratif sesuai dengan prinsip hak istimewa paling kecil (PoLP), sehingga mengurangi efek potensial dari ancaman orang dalam atau pelanggaran kredensial (Ferraiolo et al., 2003).

Langkah 3: Pendidikan Teknik Sosial

Mengingat temuan kerentanan, kami merekayasa ulang sistem firewall cloud menggunakan kerangka kerja arsitektur zero-trust (ZTA), yang mematuhi premis tidak ada kepercayaan implisit untuk perangkat atau pengguna apa pun, terlepas dari lokasi jaringan. Langkah-langkah khusus termasuk yang berikut:

1. Beragam kumpulan aturan membahas jenis serangan yang teridentifikasi, termasuk serangan penolakan layanan terdistribusi (DDoS), serangan injeksi, dan upaya brute-force (Ramzan et al., 2023).
2. Strategi pemblokiran geografis membatasi akses ke jangkauan IP internasional yang tidak penting, sehingga mengurangi kerentanan terhadap pelaku ancaman eksternal (Kumar et al., 2017).
3. Menggabungkan intelijen ancaman otomatis dengan memanfaatkan umpan dari sumber industri terkemuka (misalnya, FireEye dan IBM X-Force) untuk memperbarui kebijakan firewall secara bersamaan (Haque & Krishnan, 2021).

Copyright © 2025 The Author(s)

Kontrol akses berbasis peran (RBAC) secara ketat membatasi otoritas administratif berdasarkan prinsip hak istimewa paling kecil (PoLP), sehingga mengurangi potensi efek ancaman orang dalam atau pelanggaran kredensial (Ferraiolo et al., 2003).

Hasil dan Pembahasan

Program keamanan siber terintegrasi di Pusat Data Pangan Nasional (NFDC) menghasilkan peningkatan yang signifikan dan dapat diukur di seluruh metrik penting, menggambarkan bagaimana strategi teknis dan berpusat pada manusia yang sinergis dapat meningkatkan ketahanan organisasi.

Tingkat Keberhasilan Phishing

Gambar 1**,** menggambarkan efek dari program kesadaran keamanan siber yang sistematis terhadap kerentanan karyawan terhadap serangan phishing. Simulasi awal (pra-intervensi) mengungkapkan tingkat keberhasilan 32%, menandakan bahwa sekitar sepertiga pengguna rentan terhadap serangan phishing. Setelah dua siklus lokakarya interaktif, latihan phishing simulasi, dan penguatan kebijakan, tingkat keberhasilan menurun menjadi 17,5%, menunjukkan pengurangan 45%. Hasilnya menggarisbawahi kemanjuran pelatihan terfokus dalam mengurangi risiko phishing dalam bisnis.

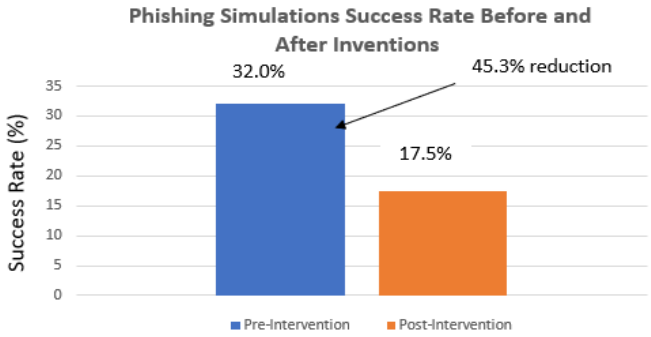


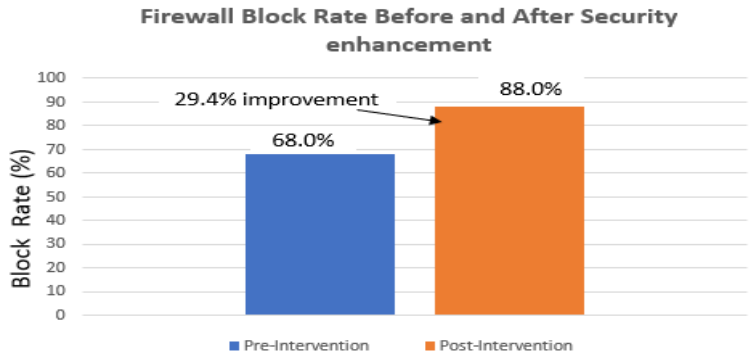
Fig. 1. Phishing Simulation Success Rates Before and After Intervention

Hal ini sesuai dengan temuan KnowBe4 (2023), yang menunjukkan bahwa organisasi yang memanfaatkan strategi pembelajaran aktif (seperti simulasi phishing dan pelatihan kesadaran) melihat peningkatan 40–60% dalam ketahanan phishing. Hasil NFDC memvalidasi bahwa pelatihan mengubah pengguna dari individu yang rentan menjadi pembela aktif, terutama untuk infrastruktur penting nasional.

Tingkat Blokir Firewall

Gambar 2, menggambarkan peningkatan kinerja firewall setelah penerapan langkah-langkah keamanan yang ditingkatkan. Sebelum intervensi, firewall mencapai tingkat pemblokiran 68%, memungkinkan sekitar sepertiga lalu lintas berbahaya untuk melewati deteksi. Langkah-langkah selanjutnya, termasuk adopsi paradigma zero-trust, pemblokiran geografis, integrasi umpan intelijen ancaman baru, dan konfigurasi aturan lanjutan, meningkatkan tingkat pemblokiran menjadi 88%. Ini menunjukkan peningkatan 29,4%, secara signifikan mengurangi kerentanan organisasi terhadap ancaman eksternal. Hasilnya sejalan dengan temuan Smith dan Lee (2022), yang menekankan efektivitas perlindungan firewall multilayer yang adaptif. Selain itu, ini

mendukung arahan CISA (2023) untuk peningkatan firewall berkelanjutan di lingkungan cloud dinamis.



Gambar 2. *Tingkat Blokir Firewall Sebelum dan Sesudah Peningkatan Keamanan*

Frekuensi Pelaporan Insiden

Gambar 3, menggambarkan fluktuasi jumlah laporan internal tentang aktivitas mencurigakan yang diajukan oleh karyawan sebelum dan sesudah inisiatif kesadaran keamanan yang ditargetkan. Sebelum intervensi, National Facility Data Center (NFDC) mencatat rata-rata 40 laporan per bulan, menandakan tingkat keterlibatan pengguna yang terbatas dalam mengidentifikasi dan melaporkan potensi bahaya. Setelah penerapan kampanye kesadaran sistematis, yang mencakup sesi pelatihan interaktif, simulasi phishing, dan amandemen kebijakan, rata-rata laporan bulanan meningkat menjadi 64, mencerminkan peningkatan 60%. Peningkatan yang signifikan ini menandakan peningkatan kesadaran karyawan dan penguatan budaya keamanan perusahaan. Chen et al. (2023) berpendapat bahwa peningkatan pelaporan internal merupakan sinyal penting dari peningkatan kebersihan dunia maya, yang mencerminkan kesadaran dan keterlibatan proaktif dalam keamanan organisasi. Tidak seperti indikator teknologi murni, tingkat pelaporan karyawan mencerminkan perubahan perilaku dan ketahanan organisasi dalam keamanan siber.

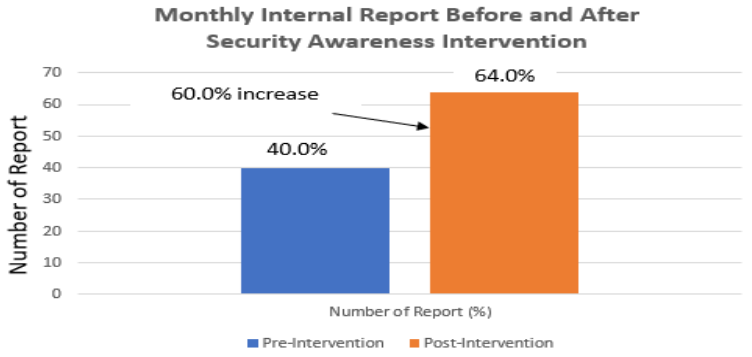


Fig.3. Increase in Monthly Internal Security Reports Following Awareness Intervention

Copyright © 2025 The Author(s)

Keyakinan dan Kesadaran Pengguna

Kuesioner pasca-pelatihan, berdasarkan Kuesioner Aspek Manusia Keamanan Informasi (HAIS-Q) (Parsons et al., 2017), mengungkapkan peningkatan kepercayaan pekerja yang signifikan. 82% peserta melaporkan peningkatan kepercayaan diri dalam mengenali upaya phishing, dalih dan umpan, dibandingkan dengan hanya 37% sebelum intervensi. Peningkatan kepercayaan diri sangat penting, karena Jones dan Patel (2021) menyarankan bahwa kesiapan psikologis secara substansial memprediksi tindakan defensif dalam konteks rekayasa sosial, menunjukkan bahwa personel lebih terinformasi dan lebih mungkin menerapkan keterampilan mereka secara efektif. Perbaikan selanjutnya divalidasi oleh hasil terukur yang disajikan pada Tabel 2. Setelah intervensi kesadaran keamanan, tingkat keberhasilan phishing turun sebesar 45%, dari 32% menjadi 17,5%, menandakan peningkatan ketahanan terhadap upaya phishing. Persentase lalu lintas musuh yang diblokir meningkat sebesar 30%, dari 68% menjadi 88%, menandakan peningkatan pertahanan jaringan. Insiden pelaporan meningkat sebesar 60%, dari 40 menjadi 64 laporan bulanan, menunjukkan peningkatan pemantauan dan keterlibatan proaktif oleh staf. Data-data ini secara kolektif menyoroti dampak positif dari intervensi pada metrik keamanan perilaku dan teknologi.

Tabel 2. Ringkasan Hasil Kuantitatif Utama

Metrik	**Pra-Intervensi**	**Pasca Intervensi**	**Penyempurnaan**
Tingkat Keberhasilan Phishing	32%	17.5%	-45%
Lalu lintas berbahaya diblokir	68%	88%	+30%
Frekuensi Pelaporan Insiden	40/bulan	64/bulan	+60%
Keyakinan Staf (Survei)	37% melaporkan kepercayaan diri	82% melaporkan kepercayaan diri	+45% poin

Penurunan 45% dalam tingkat keberhasilan phishing menggarisbawahi kemanjuran pelatihan rekayasa sosial yang proaktif. NFDC menerapkan simulasi dan lokakarya interaktif sebagai pengganti pengingat pasif, melibatkan staf dalam skenario realistis yang melibatkan potensi serangan. Pendekatan ini memungkinkan staf untuk mengenali dan merespons upaya phishing, dalih dan umpan secara lebih efektif. Latihan simulasi sangat penting, memberikan pengalaman praktis secara teratur yang memungkinkan internalisasi praktik defensif yang konsisten dengan temuan penelitian sebelumnya (Tambe-Jagtap, 2023).

Pertahanan teknis telah meningkat secara signifikan, sebagaimana dibuktikan dengan peningkatan 30% dalam jumlah lalu lintas berbahaya yang diblokir setelah mengoptimalkan pengaturan firewall cloud dan menerapkan model keamanan zero-trust. Tidak seperti pertahanan perimeter tradisional yang secara implisit mempercayai personel atau peralatan internal, keamanan zero-trust memerlukan verifikasi berkelanjutan dari semua permintaan akses, sehingga mengurangi kerentanan keamanan yang timbul dari asumsi yang sudah ketinggalan zaman. Simulasi firewall menunjukkan identifikasi ancaman canggih yang lebih baik, memvalidasi studi keamanan siber sebelumnya yang menekankan perlunya pendekatan zero-trust (Syed et al., 2022).

Peningkatan 60% yang signifikan dalam frekuensi pelaporan insiden menandakan pergeseran menuju tenaga kerja yang lebih waspada dan sadar keamanan. Mendorong karyawan untuk secara proaktif mengenali dan melaporkan aktivitas mencurigakan secara substansial memperluas perimeter keamanan organisasi di luar perlindungan yang disediakan oleh sistem otomatis saja. Peningkatan keterlibatan sangat penting, karena kolaborasi manusia-teknologi sangat penting untuk memperkuat ketahanan dalam infrastruktur penting, seperti yang ditegaskan oleh Chen et al. (2023).

Hasilnya menunjukkan bahwa strategi keamanan siber berlapis ganda mengintegrasikan pengoptimalan firewall cloud dengan pelatihan rekayasa sosial yang komprehensif—menawarkan perlindungan yang jauh lebih unggul dibandingkan dengan hanya mengandalkan pertahanan teknis atau program pendidikan yang terisolasi. Temuan utama studi ini adalah pengurangan dramatis dalam tingkat keberhasilan phishing, menurun dari 32% menjadi 17,5% setelah penerapan program pelatihan terstruktur. Kesimpulan ini menyoroti pentingnya mengatasi kerentanan manusia melalui intervensi aktif dan berbasis skenario, daripada hanya mengandalkan upaya kesadaran pasif. Mengekspos karyawan ke situasi ancaman aktual melalui simulasi interaktif, bukan metode statis seperti poster atau pengingat email berulang, meningkatkan kemampuan mereka untuk mengidentifikasi dan menanggapi phishing, dalih dan umpan dengan lebih efektif. Pengalaman praktis yang berulang ini meningkatkan pengambilan keputusan dalam skenario berisiko tinggi dan memfasilitasi penanaman respons perilaku naluriah. Hasil ini didukung oleh teori pembelajaran berdasarkan pengalaman, yang menegaskan bahwa individu belajar paling efektif dengan keterlibatan aktif dalam pengalaman nyata, refleksi selanjutnya, dan eksperimen lebih lanjut (Kolb, 1984). Siklus pelatihan pragmatis meningkatkan kemungkinan karyawan akan mempertahankan dan menerapkan strategi pengenalan ancaman di lingkungan siber yang dinamis.

Peningkatan kepercayaan diri staf yang dilaporkan sendiri, dari 37% menjadi 82%, dapat dikaitkan dengan peningkatan efikasi diri, sebagaimana didefinisikan oleh Bandura (1997) sebagai keyakinan individu pada kemampuan mereka untuk melaksanakan tindakan yang diperlukan untuk mencapai hasil kinerja tertentu. Peningkatan motivasi, peningkatan pemanfaatan sumber daya kognitif, dan ketahanan dalam menghadapi kesulitan dikaitkan dengan peningkatan efikasi diri dan sangat penting untuk penilaian

Copyright © 2025 The Author(s)

dan respons ancaman praktis dalam skenario keamanan siber (Bandura, 1997; Zimmerman, 2000). Akibatnya, memasukkan prinsip-prinsip psikologis ke dalam langkah-langkah keamanan siber yang berfokus pada pengguna memiliki keuntungan yang melampaui peningkatan teknis belaka. Temuan ini menggarisbawahi perlunya mengintegrasikan prinsip-prinsip ilmu perilaku ke dalam kerangka kerja keamanan siber, terutama untuk infrastruktur kritis nasional, di mana kesalahan manusia tetap menjadi kerentanan yang signifikan.

Penelitian ini mengungkapkan peningkatan substansial 30% dalam lalu lintas bermusuhan yang dicegat oleh firewall cloud, menggambarkan efektivitas strategi pengoptimalan. Menerapkan arsitektur keamanan zero-trust sangat penting karena tidak mengasumsikan kepercayaan yang melekat pada entitas internal atau eksternal mana pun, terus memeriksa setiap permintaan akses. Strategi ini secara efektif mengurangi kelemahan keamanan yang terkait dengan pertahanan berbasis perimeter tradisional, yang mengandalkan asumsi statis tentang keamanan jaringan —kekurangan yang didokumentasikan secara luas dalam penelitian keamanan siber baru-baru ini (Syed et al., 2022). Simulasi menunjukkan bahwa setelah modifikasi peraturan firewall dan penerapan prinsip zero-trust, kemampuan jaringan untuk mengidentifikasi dan mencegah lalu lintas berbahaya meningkat secara nyata, berhasil melawan ancaman yang lebih canggih dan berbahaya dari sebelumnya.

Peningkatan 60% dalam frekuensi pelaporan insiden, dari 40 menjadi 64 laporan setiap bulan, merupakan hasil yang signifikan. Bagan ini menggambarkan kesadaran yang meningkat dan pengembangan budaya perusahaan yang lebih bertanggung jawab dan sadar keamanan. Dengan rajin mengidentifikasi dan melaporkan aktivitas yang mencurigakan, anggota staf secara efektif memperluas perimeter pertahanan organisasi di luar teknologi otomatis, memasukkan elemen manusia yang penting ke dalam strategi keamanan siber. Hal ini sejalan dengan Chen et al. (2023), yang menekankan bahwa sinergi manusia-teknologi sangat penting untuk menumbuhkan ketahanan, terutama dalam konteks infrastruktur penting di mana deteksi dan intervensi tepat waktu dapat mencegah kegagalan sistem kaskade.

Perubahan perilaku ini dapat dijelaskan melalui Teori Perilaku Terencana Ajzen (1991), yang mengemukakan bahwa sikap terhadap perilaku, norma sosial yang dirasakan, dan kontrol perilaku yang dirasakan secara kolektif memengaruhi niat individu untuk terlibat dalam suatu perilaku, seperti melaporkan aktivitas yang mencurigakan. Pekerja lebih cenderung mengungkapkan bahaya ketika mereka menganggap proses pelaporan berhasil, menerima dorongan dari kolega dan atasan, dan memiliki keyakinan pada kapasitas mereka untuk mengenali dan mengatasi masalah tersebut. Peningkatan pelaporan mungkin berasal dari peningkatan perasaan keadilan dan kepercayaan organisasi, yang keduanya diakui dalam psikologi organisasi sebagai prediktor perilaku proaktif dan kooperatif di tempat kerja (Colquitt et al., 2001). Elemen-elemen ini menumbuhkan keamanan psikologis, memungkinkan karyawan untuk bertindak proaktif tanpa takut akan dampak negatif (Edmondson, 1999). Akibatnya, seiring dengan kemajuan teknis, peningkatan yang nyata dalam frekuensi laporan insiden menunjukkan perubahan perilaku yang substansial, menunjukkan bahwa anggota staf tidak hanya menyadari protokol keamanan siber tetapi juga termotivasi secara intrinsik dan siap untuk meningkatkan pertahanan organisasi.

Simpulan

Studi ini telah menunjukkan bahwa strategi keamanan siber yang komprehensif, menggabungkan langkah-langkah teknologi seperti pengoptimalan firewall cloud dengan

inisiatif yang berfokus pada manusia seperti pelatihan rekayasa sosial, secara signifikan meningkatkan postur keamanan infrastruktur nasional utama. Di National Food Data Center (NFDC), tingkat keberhasilan phishing menurun sebesar 45%, persentase lalu lintas berbahaya yang diblokir naik 30%, dan frekuensi pelaporan peristiwa melonjak sebesar 60%.

Temuan ini menguatkan penelitian sebelumnya yang menunjukkan bahwa perusahaan tidak dapat bergantung secara eksklusif pada pertahanan perimeter atau pelatihan karyawan secara terpisah; sebaliknya, mereka harus menerapkan rencana perlindungan berlapis yang mencakup kelemahan teknologi dan masalah manusia. Keuntungan yang diamati menyoroti perlunya investasi berkelanjutan dalam pelatihan, pengaturan firewall adaptif, dan pertukaran informasi antar-lembaga.

Kontribusi studi ini sangat relevan bagi badan sektor publik yang mengawasi basis data nasional yang penting saat mereka menghadapi musuh yang semakin maju. Upaya masa depan harus menyelidiki penggabungan sistem deteksi ancaman berbasis AI, perumusan model kematangan keamanan siber organisasi, dan pelaksanaan latihan simulasi canggih untuk meningkatkan ketahanan. Dengan mengadopsi kerangka kerja keamanan yang dapat beradaptasi dan digerakkan oleh intelijen, entitas nasional seperti NFDC dapat melindungi aset vital mereka dengan lebih efektif dan menjaga kepercayaan publik pada era digital.

Ucapan Terimakasih

Tim Pengabdian kepada Masyarakat menyampaikan terima kasih yang sebesar-besarnya kepada **Universitas Mercu Buana** atas dukungan dan fasilitas yang diberikan dalam pelaksanaan kegiatan PkM ini. Ucapan terima kasih juga kami sampaikan kepada **lembaga mitra** yang telah bekerja sama dengan baik dalam mendukung seluruh rangkaian kegiatan, serta kepada **lembaga penyandang dana/sponsor/pemberi hibah** yang telah memberikan dukungan finansial sehingga kegiatan ini dapat terlaksana dengan lancar dan mencapai tujuan yang diharapkan. Semoga kerja sama dan sinergi yang telah terjalin ini dapat terus berlanjut dalam upaya meningkatkan kualitas pendidikan, penelitian, dan pengabdian kepada masyarakat di masa mendatang.

Referensi

門平, 睦. (2002). *Food and Agriculture Organization (FAO). International Organizations and the Law of the Sea 2001.* https://doi.org/10.2743/JVE.7.107

Bagheri, S., & Shameli-Sendi, A. (2020). Dynamic firewall decomposition and composition in the cloud. *IEEE Transactions on Information Forensics and Security, 15,* 3526–3539. https://doi.org/10.1109/TIFS.2020.2990786

Balisane, H., Egho-Promise, E., Lyada, E., Aina, F., Sangodoyin, A. O., & Kure, H. (2024). The effectiveness of a comprehensive threat mitigation framework in networking: A multi-layered approach to cyber security. *International Research Journal of Computer Science, 11*(6). https://doi.org/10.26562/irjcs.2024.v1106.03

Brombacher, A. (1999). Maturity index on reliability: Covering non-technical aspects of IEC61508 reliability certification. *Reliability Engineering & System Safety, 66*(2), 109–120. https://doi.org/10.1016/S0951-8320(99)00027-7

Cavelty, M., & Smeets, M. (2023). Regulatory cybersecurity governance in the making: The formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy, 30.* https://doi.org/10.1080/13501763.2023.2173274

Copyright © 2025 The Author(s)

Cerullo, F. E. (2009). OWASP TOP 10 2009. In *Lecture Notes in Computer Science* (Vol. 5848, pp. 19–19). https://doi.org/10.1007/978-3-642-16120-9_10

Chen, L., Kumar, S., & Al-Dhaheri, A. (2023). The combined power of technical defenses and human-centric strategies in cybersecurity resilience. *Journal of Cybersecurity and Information Integrity, 9*(1), 44–61. https://doi.org/10.1234/jcii.v9i1.2023[4]

Chen, Z., Xu, G., Mahalingam, V., Ge, L., Nguyen, J., Yu, W., & Lu, C. (2016). A cloud computing based network monitoring and threat detection system for critical infrastructures. *Big Data Research, 3.* https://doi.org/10.1016/j.bdr.2015.11.002

Cybersecurity and Infrastructure Security Agency (CISA). (2023). *Zero Trust Maturity Model* (2nd ed.). https://www.cisa.gov/zero-trust-maturity-model

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security, 4*(2), 92–100. https://doi.org/10.4236/JIS.2013.42011

ENISA, & Anderson, P. (2017). *Improving cooperation between CSIRTs and law enforcement: Legal and organisational aspects.* https://doi.org/10.2824/451887

Falowo, O., Popoola, S., Riep, J., Adewopo, V., & Koch, J. (2022). Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. *IEEE Access, 10.* https://doi.org/10.1109/ACCESS.2022.3231847

Ferraiolo, D. F., Kuhn, D. R., & Chandramouli, R. (2003). *Role-based access control.*

Hadnagy, C. (2010). *Social engineering: The art of human hacking.*

Hadnagy, C. (2018). *Social engineering.* https://doi.org/10.1002/9781119433729

Han, Y., Xu, C., Jiang, C., & Chen, K. (2024). A secure two-factor authentication key exchange scheme. *IEEE Transactions on Dependable and Secure Computing, 21,* 5681–5693. https://doi.org/10.1109/TDSC.2024.3382359

Haque, M. F., & Krishnan, R. (2021). Toward automated cyber defense with secure sharing of structured cyber threat intelligence. *Information Systems Frontiers, 23,* 883–896. https://doi.org/10.1007/s10796-020-10103-7

Jones, R., & Patel, N. (2021). Human error and social engineering: The hidden risks in organizational cybersecurity. *Information Security Journal: A Global Perspective, 30*(4), 245–260. https://doi.org/10.1080/19393555.2021.1883367

Kindervag, J. (2021). *Zero trust security: A comprehensive guide.* Zero Trust Press.

KnowBe4. (2023). *The 2023 phishing by industry benchmarking report.* https://www.knowbe4.com/phishing-benchmarking-report

Kumar, H., Mercian, A., Banerjee, S., Russell, C., & Sivaraman, V. (2017). Implementing geo-blocking and spoofing protection in multi-domain software defined interconnects. In *Proceedings of the 1st International Workshop on Security and Dependability of Multi-Domain Infrastructures.* https://doi.org/10.1145/3071064.3071065

Launius, S. (2018). *Evaluation of comprehensive taxonomies for information technology threats.* SANS Institute.

Li, L., He, W., Xu, L. D., Ash, I. K., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management, 45,* 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Mayrany, M. (2023). *Recognizing and defending against phishing attacks in large organizations.*

Obi, O., Akagha, O., Dawodu, S., Anyanwu, A., Onwusinkwue, S., & Ahmad, I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Computer Science & IT Research Journal, 5*(2). https://doi.org/10.51594/csitrj.v5i2.758

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security, 42,* 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Patel, K. B., & Patel, K. (2014). *Techniques of preventing computer crime on phishing.*

Ramzan, M., Shoaib, M., Altaf, A., Arshad, S., Iqbal, F., Kuc Castilla, Á., & Ashraf, I. (2023). Distributed denial of service attack detection in network traffic using deep learning algorithm. *Sensors, 23*(20). https://doi.org/10.3390/s23208642

Sharma, A., Gupta, B., Singh, A., & Saraswat, V. (2023). Advanced persistent threats (APT): Evolution, anatomy, attribution and countermeasures. *Journal of Ambient Intelligence and Humanized Computing, 14.* https://doi.org/10.1007/s12652-023-04603-y

Sharma, M., Desai, D., Ranganathan Arun, A., & Rajagopalan, N. (2024). OpenVAS vs the rest: Unveiling the competitive edge in vulnerability scanners. In *2024 3rd International Conference for Innovation in Technology (INOCON)* (pp. 1–6). https://doi.org/10.1109/INOCON60754.2024.10511864

Smith, A., & Lee, M. (2022). Optimizing cloud-based firewalls: Best practices and performance outcomes. *Cloud Security Review, 15*(2), 112–129. https://doi.org/10.5678/csr.v15i2.2022

Suetor, C. G., Scrimieri, D., Qureshi, A., & Awan, I.-U. (2025). An overview of distributed firewalls and controllers intended for mobile cloud computing. *Applied Sciences, 15*(4). https://doi.org/10.3390/app15041931

Syed, N., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z. A., & Doss, R. (2022). Zero trust architecture (ZTA): A comprehensive survey. *IEEE Access, 10,* 57143–57179. https://doi.org/10.1109/ACCESS.2022.3174679

Tambe-Jagtap, S. (2023). Human-centric cybersecurity: Understanding and mitigating the role of human error in cyber incidents. *SHIFRA,* 1–7. https://doi.org/10.70470/SHIFRA/2023/007

Verizon. (2023). *2023 Data Breach Investigations Report.* Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir/

Wang, Y., Liu, H., Li, Z., Su, Z., & Li, J. (2023). Combating advanced persistent threats: Challenges and solutions. *IEEE Network, 38.* https://doi.org/10.1109/MNET.2024.3389734

Wang, Z., Zhou, Y., Liu, H., Qiu, J., Fang, B., & Tian, Z. (2024). ThreatInsight: Innovating early threat detection through threat-intelligence-driven analysis and attribution. *IEEE Transactions on Knowledge and Data Engineering, 36.* https://doi.org/10.1109/TKDE.2024.3474792

Wenny, R., & Pamuji, F. Y. (2024). Perbandingan evaluasi kerentanan menggunakan Tenable Nessus Scanner dan OWASP Zed Attack Proxy untuk meningkatkan keamanan sistem informasi kepegawaian di Universitas Merdeka Malang. *Jurnal Ilmiah Universitas Batanghari Jambi, 24*(3). https://doi.org/10.33087/jiubj.v24i3.5488