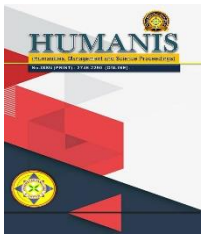
HUMANIS
(Humanities, Management and Science Proceedings)

Vol. 5 • No. 2 • Juni 2025

Pege (Hal.) : 260 – 275

ISSN (*online*) : 2746 - 4482
ISSN (*print*) : 2746 - 2250



Special Issue :
Webinar Nasional
HUMANIS 2025
Website. :
http://www.openjournal.unpam.ac.id/index.php/SNH

Program Pascasarjana Magister Manajemen
Jl. Raya Puspiptek, Buaran, Kec. Pamulang, Kota Tangerang Selatan, Banten 15310,
Email : humanismanajemen@gmail.com

MASIHKAH MANUSIA MENJADI RANTAI TERLEMAH DALAM KEAMANAN SIBER DI INDONESIA?

Galylia Aryanita Darmawan [1]; Mochammad Amin Ruwanda [2]; Rismunandar Al Amin [3] dan Nurmin Arianto [4];

[1]Universitas Pamulang, email: aryanitadarmawan@gmail.com
[2]Universitas Pamulang, email: aminruwanda1901@gmail.com
[3]Universitas Pamulang, email: rismunandaralamin@gmail.com
[3]Universitas Pamulang, email: dosen01118@unpam.ac.id

Abstract.
Cybersecurity in Indonesia continues to evolve in line with the increasing pace of digital transformation across various sectors. However, the threat of cyberattacks such as malware, phishing, and Trojans still highlights the fact that human factors often serve as the primary entry point for cybercriminals. This study aims to identify the main causes of security vulnerabilities, regardless of the advancements in protective technologies. By examining cybersecurity incident data and recent attack trends, this research seeks to answer whether humans remain the weakest link in Indonesia's cybersecurity system. Based on the analysis of past cybersecurity incidents and attack patterns, the findings indicate that despite significant technological advancements, the human factor remains the most vulnerable element, reinforcing the need for a holistic approach that integrates technology, training, and a strong cybersecurity culture.

Abstrak.
Keamanan siber di Indonesia terus berkembang seiring dengan meningkatnya transformasi digital di berbagai sektor. Namun, ancaman serangan siber, seperti malware, phishing, dan Trojan, masih menunjukkan bahwa faktor manusia sering menjadi titik masuk utama bagi pelaku kejahatan siber. Penelitian ini bertujuan untuk mengetahui penyebab utama celah keamanan, terlepas dari kemajuan teknologi proteksi yang digunakan. Dengan mengkaji data insiden siber dan tren serangan terbaru, pada penelitian ini berupaya menjawab pertanyaan apakah manusia masih menjadi rantai terlemah dalam sistem keamanan siber di Indonesia. Berdasarkan hasil penelitian dari kajian data insiden siber dan tren serangan yang terjadi pada periode waktu kebelakang, menunjukkan bahwa meskipun teknologi telah berkembang pesat, faktor manusia tetap menjadi elemen paling rentan, menegaskan pentingnya pendekatan holistik yang menggabungkan teknologi, pelatihan, dan budaya keamanan siber.
Keywords: ancaman keamanan siber; anomali trafik; keamanan siber; manusia; ruang siber;

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mendorong peningkatan signifikan dalam penetrasi internet di Indonesia. Berdasarkan hasil survei penetrasi internet di Indonesia yang dirilis Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), tingkat penetrasi internet di Indonesia mencapai 79,5% pada awal tahun 2024, meningkat dari 78,19% pada tahun sebelumnya. Peningkatan ini mencerminkan adopsi digital dan transformasi digital yang semakin luas. Transformasi digital telah menciptakan sebuah dimensi baru yang dikenal sebagai **ruang siber** (*cyberspace*), dimana interaksi sosial, transaksi ekonomi, penyimpanan data, hingga proses pemerintahan kini banyak berlangsung secara daring. Ruang siber menawarkan berbagai **kelebihan**, seperti efisiensi, kecepatan, dan keterhubungan tanpa batas. Namun, bersamaan dengan itu muncul pula **kelemahan-kelemahan** yang inheren, terutama terkait aspek kerentanan terhadap serangan dan penyalahgunaan. Perkembangan ruang siber tidak hanya membuka peluang, tetapi juga menciptakan **berbagai ancaman berskala global**. Serangan siber seperti peretasan, pencurian data, penyebaran *malware*, dan manipulasi informasi menjadi fenomena yang kian kompleks dan sulit dikendalikan. Ancaman ini tidak mengenal batas geografis dan dapat menyasar siapa pun, baik individu, korporasi, maupun institusi negara.

Salah satu contoh nyata dari dampak destruktif serangan siber adalah insiden ***WannaCry ransomware attack*** pada tahun 2017. Serangan ini menyebar secara global dalam waktu singkat, menginfeksi lebih dari 200.000 komputer di 150 negara. Rumah sakit, perusahaan, hingga institusi pemerintahan menjadi korban. *National Health Service* (NHS) yang merupakan layanan kesehatan publik di Inggris lumpuh, operasi pasien dibatalkan, dan data penting dienkripsi oleh pelaku yang meminta tebusan dalam bentuk *cryptocurrency*. Kerugian ekonomi akibat serangan ini diperkirakan mencapai **miliaran dolar AS**, menjadikannya salah satu serangan siber paling merugikan dalam sejarah.

Serangan siber di Indonesia tidak kalah destruktif, pada **20–26 Juni 2024**, Sistem Pusat Data Nasional Sementara (PDNS 2) di Surabaya dilumpuhkan oleh serangan ***ransomware* LockBit 3.0 /*Brain Cipher***. Serangan ini berdampak pada **282 instansi pemerintah**, termasuk layanan imigrasi dan paspor. Peretas menuntut tebusan sebesar USD 8 juta (sekitar Rp 131 miliar). Meskipun pemerintah menolah membayarkannya namun **kerugian ekonomi nasional** (langsung dan tidak langsung) diperkirakan mencapai sekitar **Rp 6,3 triliun**, mencakup biaya pemulihan, pengalihan layanan ke AWS, dan hilangnya efisiensi pelayanan publik.

Melihat betapa destruktifnya serangan siber, maka k**eamanan siber** (*cybersecurity*) menjadi isu strategis yang krusial. Upaya untuk menjaga keamanan ruang siber tidak hanya bergantung pada teknologi semata, melainkan membutuhkan pendekatan yang holistik. Dalam praktik terbaik keamanan informasi, dikenal konsep ***People, Process, and Technology*** (PPT) yakni bahwa keamanan yang efektif hanya dapat dicapai melalui kombinasi tiga pilar utama: **manusia (people)** sebagai aktor, **proses (process)**sebagai kerangka kerja pengendalian, dan **teknologi (technology)** sebagai alat bantu.

Dalam konteks ini, Kevin Mitnick, seorang mantan peretas yang kemudian menjadi pakar keamanan terkemuka, dalam bukunya *The Art of Deception* menyatakan bahwa "*the human factor is truly security's weakest link*". Pernyataan ini menekankan bahwa meskipun sistem telah dilengkapi teknologi tercanggih dan prosedur yang ketat, manusia tetap menjadi celah paling rentan yang sering dieksploitasi melalui teknik rekayasa sosial. Pernyataan Mitnick tersebut mengundang pertanyaan reflektif:

1. Apakah kondisi ini juga berlaku di Indonesia?
2. Apakah faktor manusia juga merupakan rantai terlemah dalam rantai keamanan siber nasional ?
3. Jika manusia menjadi rantai terlemah, Apa penyebab utama kelemahan manusia dalam sistem keamanan siber?

Pertanyaan inilah yang mendorong pentingnya penelitian lebih lanjut untuk memahami karakteristik dan tantangan keamanan siber di Indonesia secara lebih mendalam. Hasil dari penelitian ini diharapkan dapat memberikan pemahaman yang lebih mendalam kepada seluruh pemangku kepentingan dalam pentingnya mitigasi risiko dalam keamanan siber. Dengan demikian, strategi keamanan yang lebih efektif dan komprehensif dapat dikembangkan untuk menghadapi ancaman siber yang terus berkembang.

KAJIAN LITERATUR

Kemanan Siber

Menurut NIST (*National Institute of Standards and Technology*, AS), ruang siber merupakan domain global dalam lingkungan informasi yang terdiri dari jaringan infrastruktur teknologi informasi yang saling bergantung, termasuk internet, jaringan telekomunikasi, sistem komputer, serta prosesor dan pengontrol yang tertanam. Sedangkan berdasarkan Undang-undang No. 3 Tentang Pertahanan Negara, Ruang siber adalah ruang tanpa batas fisik yang terdiri atas jaringan sistem elektronik dan informasi yang saling terhubung. Sehingga dapat disimpulkan bahwa ruang siber adalah domain virtual yang terbentuk oleh jaringan sistem informasi dan komunikasi, termasuk internet, jaringan komputer, perangkat keras, perangkat lunak, dan data yang saling terhubung. Ruang siber terdiri atas 3 lapisan:

1. Jaringan fisik (Internet, telekomunikasi, media penyimpanan, dan sebagainya)
2. Logika (*software* dan *firmware*)
3. Siber-persona (SDM keamanan siber dan sandi)

Ruang siber memungkinkan terjadinya interaksi digital, pertukaran informasi, komunikasi, serta aktivitas ekonomi, sosial, dan pemerintahan secara daring (*online*). Dari definisi tersebut maka karakteristik utama ruang siber yaitu:

1. Tak berbatas secara fisik. Berbeda dengan domain tradisional seperti darat, laut, udara, dan luar angkasa yang memiliki batas secara fisik, ruang siber tidak memiliki batas fisik.
2. Bersifat global dan terdesentralisasi. Ruang siber tidak dimiliki oleh satu negara atau entitas tunggal.
3. Dibentuk oleh infrastruktur digital. Rang siber dibentuk oleh infrastruktur digital seperti *server*, *router*, perangkat pengguna, dan layanan jaringan.
4. Dinamis dan cepat berubah. Dalam ruang siber teknologi, ancaman, dan penggunaannya berkembang sangat cepat.
5. Rentan terhadap ancaman keamanan. Dengan empat ciri sebelumnya menjadikan ruang siber menjadi rentan terhadap berbagai ancaman keaman seperti serangan siber, peretasan, pencurian data, dan penyebaran disinformasi.

Keamanan siber menurut NIST, merupakan pencegahan kerusakan, perlindungan, pemulihan komputer, sistem komunikasi elektronik, layanan komunikasi elektronik, komunikasi kawat, dan komunikasi elektronik. Termasuk informasi yang terkandung di dalamnya untuk memastikan ketersediaan, integritas, autentikasi, kerahasiaan, dan anti penyangkalan. Sedangkan berdasarkan Peraturan Presiden Nomor. 28 tahun 2022 Tentang Pelindungan Infrastruktur Informasi Vital, keamanan siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik bersifat teknis

maupun sosial. Sedangkan insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.

Dalam Dalam kerangka keamanan siber, konsep People, Process, dan Technology sering muncul sebagai pondasi untuk strategi keamanan yang efektif, terutama dalam standar dan panduan seperti ISO/IEC 27001 dan NIST. Pendekatan *People, Process, and Technology* (PPT) merupakan fondasi integral yang saling melengkapi untuk membangun sistem pertahanan yang efektif.

1. ***People*** **(Manusia)**

   Manusia sering dianggap sebagai titik terlemah dalam keamanan siber. Kesalahan pengguna, kurangnya kesadaran terhadap ancaman, dan perilaku yang tidak aman seperti penggunaan kata sandi yang lemah atau mudah ditebak, berkontribusi terhadap tingginya tingkat keberhasilan serangan siber. Menurut laporan *Verizon Data Breach Investigations Report* (DBIR) 2024, sekitar 68% pelanggaran data melibatkan elemen manusia, termasuk kesalahan pengguna dan penyalahgunaan kredensial. Oleh karena itu, pelatihan kesadaran keamanan siber dan pengembangan budaya keamanan yang kuat di antara karyawan menjadi krusial.

2. ***Process*** **(Proses)**

   Proses mencakup kebijakan, prosedur, dan standar operasional yang dirancang untuk mengelola dan mengontrol aktivitas keamanan siber. Ini termasuk penilaian risiko, manajemen insiden, dan audit keamanan. Proses yang terdefinisi dengan baik memastikan bahwa organisasi dapat merespons ancaman dengan cepat dan efisien, serta meminimalkan dampak potensial dari insiden keamanan. Tanpa proses yang jelas, bahkan teknologi canggih sekalipun tidak akan efektif dalam melindungi aset informasi.

3. ***Technology*** **(Teknologi)**

   Teknologi menyediakan alat dan solusi untuk mendeteksi, mencegah, dan merespons ancaman siber. Ini mencakup firewall, sistem deteksi intrusi, enkripsi, dan solusi keamanan lainnya. Namun, teknologi harus didukung oleh proses yang tepat dan pengguna yang terlatih agar efektif. Tanpa pemahaman dan penggunaan yang benar oleh manusia, serta tanpa proses yang mendukung, teknologi tidak dapat berfungsi secara optimal.

Ketiga pilar ini tidak dapat berdiri sendiri; kelemahan pada salah satunya dapat membuka celah bagi ancaman siber.

Merujuk pada Perpres Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, disebutkan bahwa keamanan siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik yang bersifat teknis maupun sosial. Sehingga, keamanan siber dapat dikategorikan ke dalam dua jenis yaitu keamanan siber teknis dan keamanan siber sosial.

1. Keamanan Siber Sosial

   Keamanan siber sosial (*social cybersecurity*) berfokus untuk memanipulasi atau mempengaruhi individu manusia, kelompok, atau komunitas yang berdampak pada perilaku mereka terhadap isu sosial, budaya, dan politik. Keamanan siber sosial melibatkan manusia dalam menggunakan teknologi untuk mempengaruhi manusia lain. Ancaman siber sosial dapat berupa penyebaran konten pornografi, judi online, scam online, terorisme, disinformasi dan misinformasi

2. Keamanan Siber Teknis

   Keamanan siber (*cybersecurity*) yang berfokus pada infrastruktur, teknologi, dan teknik serangan yang berdampak pada kerugian materiil seperti *Data Breach*, DDos, dan *Malware*. Keamanan siber teknis melibatkan manusia dalam mengoperasikan teknologi untuk meretas teknologi lain. Ancaman keamanan siber teknis meliputi web defacement, AI *powered cyber*

threat, *phishing*, *malware*, *Advanced Persistent Threat* (APT), *Distributed Denial of Service* (DDoS), dan *stolen credential data*.

a. Ancaman Web defacement, web defacement sendiri adalah tindakan mengubah tampilan sebuah situs secara sengaja, biasanya untuk menyampaikan pesan tertentu atau merusak citra pemilik situs. Sasaran dari serangan ini sering kali adalah situs yang memiliki nilai simbolis tinggi, seperti milik instansi pemerintah, perusahaan ternama, atau lembaga strategis. Konten yang ditampilkan oleh pelaku bisa berupa tulisan, gambar, hingga pesan yang bermuatan politik atau ideologi. Para pelaku dikenal sebagai threat actor, biasanya mengeksploitasi celah keamanan dalam sistem atau memakai teknik peretasan untuk mendapatkan akses tanpa izin, lalu mengganti halaman utama situs dengan konten yang mereka kehendaki. Aksi ini bukan hanya melanggar privasi dan keutuhan situs, tapi juga dapat menimbulkan kerugian besar terhadap reputasi dan kepercayaan publik terhadap situs tersebut.
b. AI berpotensi dimanfaatkan *threat actor* untuk menciptakan *malware* adaptif, *phishing* yang dipersonalisasi, dan *deepfake* untuk manipulasi data. Teknologi ini memungkinkan eksploitasi celah keamanan lebih cepat, serangan DDoS yang menyesuaikan pola secara *real time*, serta *ransomware* yang secara otomatis memilih target paling rentan. Dengan kemampuan adaptasi dan pembelajaran mandiri, AI menjadikan serangan siber semakin canggih dan sulit dideteksi.
c. *Phishing* adalah salah satu bentuk ancaman siber yang dilakukan dengan cara membuat tampilan atau sistem yang menyerupai sistem asli untuk menipu korban. Melalui serangan ini, pelaku berusaha mencuri data kredensial, seperti *username* dan *password*, atau informasi sensitif lainnya dengan menggunakan komunikasi yang tampak sah, seperti email, situs web, atau pesan instan. Dengan menyamar sebagai entitas terpercaya, pelaku *phishing* memanfaatkan kelengahan pengguna untuk mengeklik tautan palsu atau memasukkan informasi pribadi ke dalam situs yang sebenarnya dikendalikan oleh pelaku. Serangan ini sering kali terlihat meyakinkan, sehingga penting bagi pengguna untuk selalu waspada dan memeriksa keaslian sumber komunikasi sebelum memberikan data sensitif.
d. *Malware*, atau *malicious software*, adalah istilah umum untuk perangkat lunak berbahaya yang dirancang untuk tujuan jahat, seperti merusak sistem komputer, mencuri data, atau mengganggu jalannya bisnis. Salah satu jenis *malware* yang sangat merugikan dan terus berkembang adalah *ransomware*. *Ransomware* bekerja dengan mengenkripsi data korban, membuatnya tidak dapat diakses, dan kemudian meminta tebusan sebagai imbalan untuk memberikan kunci dekripsi. Penyebaran ransomware bisa melalui berbagai cara, mulai dari email phishing yang menipu pengguna untuk mengeklik tautan atau membuka lampiran berbahaya, unduhan ilegal dari sumber yang tidak terpercaya, hingga eksploitasi kerentanan pada perangkat lunak.
e. *Advanced Persistent Threat (APT) adalah jenis serangan siber yang dilakukan oleh sekelompok pelaku, sering kali memiliki keterkaitan dengan suatu negara yang memanfaatkan teknik-teknik canggih dan beragam. Serangan ini dirancang untuk berjalan secara berkelanjutan dan tersembunyi dari sistem keamanan, dengan tujuan memperoleh akses ke jaringan target dan mempertahankannya dalam waktu lama. Fokus utama dari kelompok penyerang ini adalah mengakses, memantau, serta mengumpulkan data penting dari sistem yang disusupi, seperti dokumen rahasia perusahaan, informasi finansial, atau desain teknologi strategis, untuk kepentingan eksploitasi jangka panjang. Serangan APT umumnya menyasar sumber daya dan informasi vital milik negara atau institusi penting lainnya.*

f. Serangan *Denial of Service* (DoS) merupakan jenis serangan yang ditujukan untuk menguras sumber daya sistem jaringan, sehingga sistem tersebut tidak dapat beroperasi sebagaimana mestinya dan menghalangi akses pengguna lain ke layanan yang disediakan. Serangan ini memanfaatkan kelemahan sistem seperti keterbatasan *bandwidth*, kapasitas memori, daya *server*, atau celah lain dalam sistem. Umumnya, DoS menargetkan usaha kecil hingga menengah yang memiliki sumber daya terbatas.
g. Pencurian data kredensial adalah salah satu bentuk ancaman siber yang semakin sering terjadi. Pencurian data kredensial, milik individu maupun organisasi memiliki daya tarik tersendiri bagi *threat actor* untuk mendapatkan keuntungan materi. Tindakan ini melibatkan pengambilan informasi autentikasi secara ilegal. Informasi yang dicuri ini dapat digunakan untuk mengakses sistem korban secara tidak sah atau dijual di pasar gelap (*dark web*). Salah satu cara yang sering digunakan oleh *threat actor* adalah memanfaatkan kerentanan pada sistem atau mengirimkan *malware stealer* yang dirancang khusus untuk mencuri data tersebut.

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan tujuan untuk memahami secara mendalam peran faktor manusia dalam insiden keamanan siber di Indonesia. Pendekatan kualitatif dipilih karena sesuai untuk mengeksplorasi fenomena yang kompleks, kontekstual, dan melibatkan interpretasi terhadap data non-numerik seperti laporan insiden dan kebijakan keamanan. Data dikumpulkan melalui dokumentasi dan studi literatur terhadap berbagai sumber resmi yang relevan, baik dari dalam maupun luar negeri. Data dukung utama yang digunakan adalah laporan monitoring insiden siber dan Lanskap keamanan siber tahunan yang dirilis oleh Badan Siber dan Sandi Negara. Badan Siber dan Sandi Negara merupakan Lembaga pemerintah non-kementerian yang mempunyai tugas melaksanakan tugas dibidang keamanan siber dan sandi nasional.

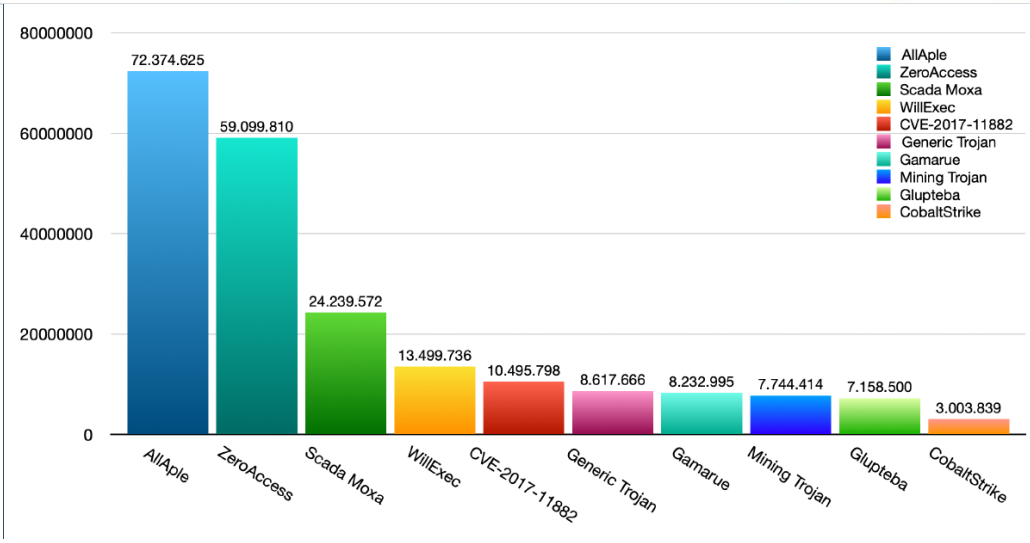
Laporan tersebut dianalisis menggunakan kombinasi dari tiga pendekatan utama yaitu : statistik deskriptif digunakan untuk menyajikan tren dan frekuensi insiden siber yang melibatkan faktor manusia, analisis komparatif digunakan untuk membandingkan data antara Indonesia dan tren global guna mengetahui kesamaan atau perbedaan karakteristik insiden serta analisis konten dilakukan terhadap laporan dan dokumen kebijakan guna mengidentifikasi narasi, penyebab utama, yang berkaitan dengan aspek manusia dalam keamanan siber. Dengan metode analisis tersebut maka dapat diidentifikasi pola, tren, serta peran faktor manusia dalam insiden yang terjadi di Indonesia.

HASIL DAN PEMBAHASAN

Analisis Data Serangan Siber di Indonesia

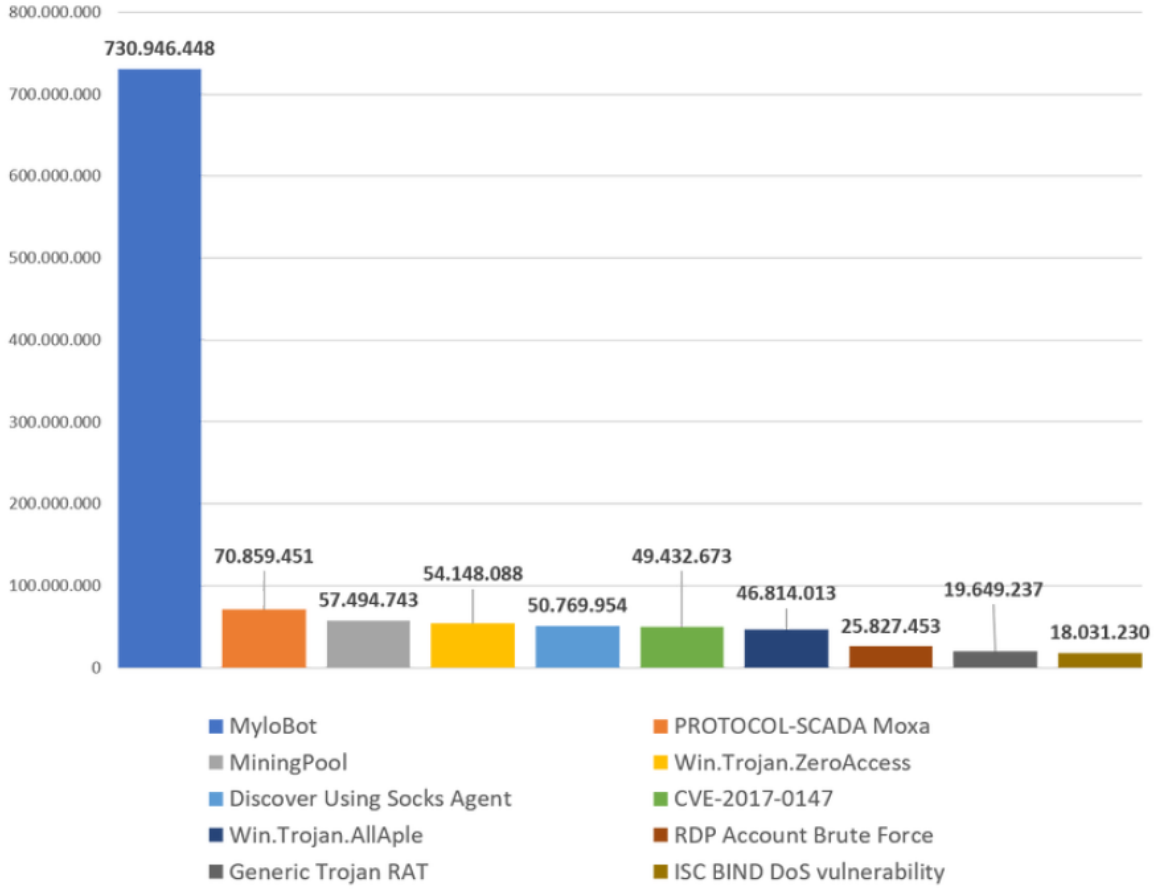
Untuk mengetahui apakah manusia masih menjadi titik lemah dalam keamanan siber Indonesia maka dilakukan telaah terhadap data hasil monitoring keamanan siber di Indonesia selama lima tahun, sebagai berikut:

1. Hasil monitoring 2020
   Berdasarkan Laporan Tahunan Hasil Monitoring Keamanan siber tahun 2020 yang diterbitkan oleh BSSN diketahui bahwa sepanjang tahun 2020 terdapat 495.337.202 anomali trafik (halaman 12). Anomali trafik dalam keamanan siber merujuk pada kondisi tidak normal atau menyimpang pada lalu lintas jaringan yang berpotensi mengindikasikan adanya tindakan yang mencurigakan atau potensi risiko serangan siber. Anomali ini bisa disebabkan oleh berbagai faktor, seperti serangan *malware*, aktivitas *botnet*, atau peningkatan lalu lintas yang tidak wajar. Berikut adalah Grafik Top 10 anomali sepanjang 2020:



Trojan menjadi anomali dengan jumlah tertinggi berdasarkan hasil monitoring Pusopskamsinas BSSN selama tahun 2020. *AllAple*, *ZeroAccess*, *WillExec*, *Glupteba*, dan *CobaltStrike* juga merupakan *malware* jenis *Trojan*. *Trojan* merupakan perangkat lunak berbahaya yang dapat merusak sebuah sistem atau jaringan. Berbeda dengan *virus* ataupun *worm*, T*rojan* bersifat tidak terlihat, dan seringkali menyerupai program, atau *file* yang wajar, seperti *file* .mp3, software gratis, antivirus palsu, atau game gratis. Tujuan *Trojan* adalah memperoleh informasi dari target, seperti: *password*, *log data*, kredensial, dan lainnya tanpa sepengetahuan korban. sepanjang 2020 tercatat 79.439 akun mengalami *data breach* berdasarkan Top 5 malware *stealer* yang menyebabkan *data breach* pada tahun 2020. Sepanjang tahun 2020, Pusat Kontak Siber menerima 1293 Aduan siber, dengan 5 aduan terbanyak adalah sebagai berikut: *Cross Site Scripting*, SQL *Injection*, *Malware*, *Phising* dan *Web Defacement*.

2. Hasil monitoring 2021
   Berdasarkan Laporan Tahunan Hasil Monitoring Keamanan siber tahun 2020 yang diterbitkan oleh BSSN diketahui bahwa sepanjang tahun 2020 terdapat 1.637.973.022 anomali trafik (halaman 16). Dengan Grafik Top 10 anomali sepanjang 2021 adalah sebagai berikut:

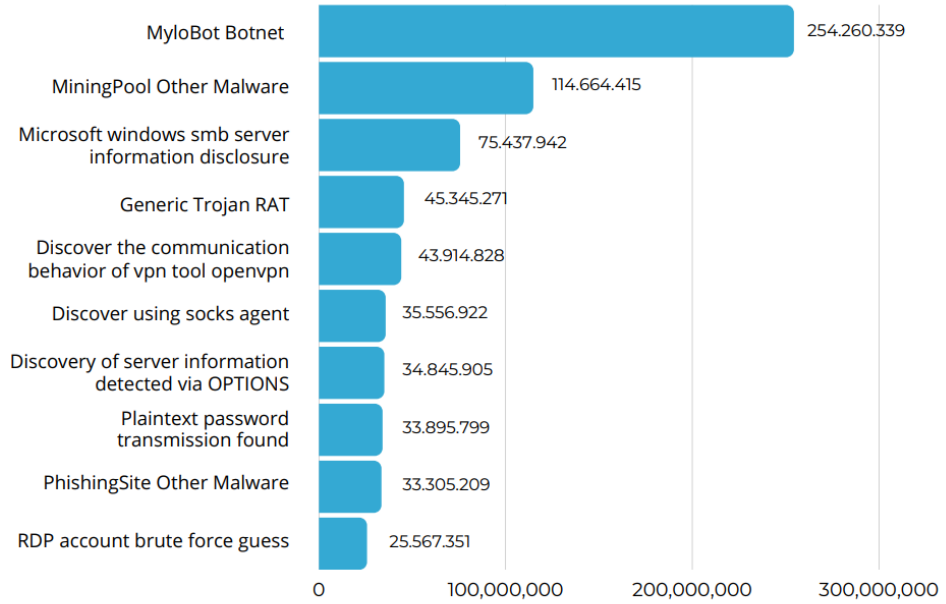


Pada tahun 2021, setidaknya sebanyak 44,62% anomali trafik didominasi oleh *MyloBot Botnet*. Tidak hanya *MyloBot Botnet*, beberapa anomali yang termasuk dalam kategori Top 10 Anomali juga memiliki keterhubungan dengan *botnet* lain dalam serangannya, seperti *ZeroAccess* dan *Discover Using Socks Agent*. *Botnet* merupakan jaringan komputer yang terinfeksi oleh malware yang berada di bawah kenadali satu pihak penyerang. *Botnet* dapat dirancang untuk pengiriman *spam*, pencurian data, *ransomware*, *click fraud*, *Denial of Service* (DoS), dan lain-lain. *MyloBot Botnet* menargetkan sistem operasi *Microsoft Windows* yang menyebar melalui *spam e-mail* dan unduhan *file* yang telah terinfeksi. Setelah terinstal, botnet mematikan *Windows Defender* dan *Windows Update* sambil memblokir port tambahan di *Firewall*. Selain itu, *botnet* juga mematikan dan menghapus *file* .exe yang berjalan dari *folder* %APPDATA%, yang dapat menyebabkan hilangnya data.

Merujuk pada temuan dari pemantauan dan evaluasi dalam Cyber Threat Intelligence (CTI), terdapat 179 laporan yang terdiri atas laporan *data breach*, *ransomware*, *profiling*, *web defacement*, *malicious activity*, *dark web enabled crime* (non fisik), *compromised account*, dan *web phishing*. Sepanjang tahun 2021, Pusat Kontak Siber menerima 332 Aduan siber, dengan 5 aduan terbanyak adalah sebagai berikut: SQL *Injection*, *Ransomware*, *Cross Site Scripting*, konten negatif, dan *Information disclosure*.

3. Hasil monitorung 2022

   Berdasarkan Lanskap Keamanan Siber Indonesia Tahun 2022 yang diterbitkan oleh BSSN diketahui bahwa sepanjang tahun 2022 terdapat 976.429.996 anomali trafik (halaman 15). Dengan Grafik Top 10 anomali sepanjang 2022 adalah sebagai berikut:

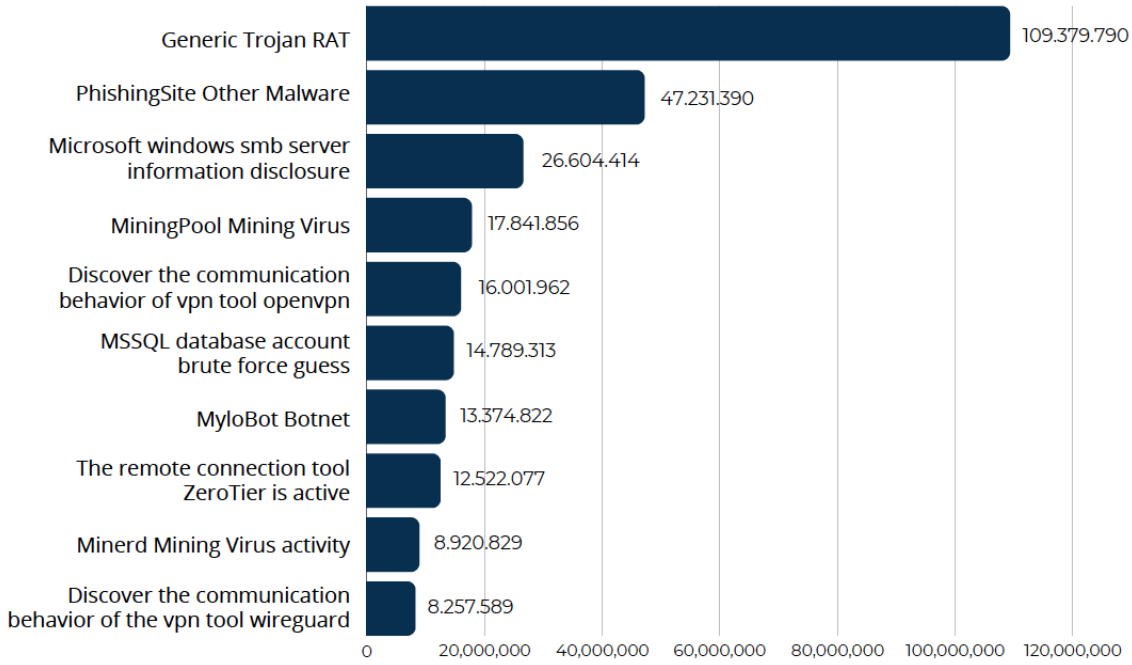


Mylobot Botnet adalah salah satu jenis *botnet* yang menargetkan dan dapat mengambil alih perangkat yang menjalankan sistem operasi *Windows*. *Botnet* ini menyebar melalui *spam e-mail* dan unduhan *file* yang telah terinfeksi. *Mylobot* sangat berbahaya karena memiliki kemampuan mengunduh dan mengeksekusi semua jenis muatan setelah berhasil menginfeksi. Fungsi utama *botnet* memungkinkan penyerang untuk mengambil kendali penuh atas sistem pengguna, salah satunya berfungsi sebagai gerbang untuk mengunduh muatan (*payload*) tambahan dari *server Command* and *Control*.

Mengacu pada hasil pengamatan dan analisis dari Cyber Threat Intelligence, BSSN turut melakukan investigasi terhadap dugaan insiden siber yang tercatat sebanyak 399 kasus dengan berbagai jenis, salah satunya adalah pelanggaran data (data breach), kerentanan, *malicious activity*, isu IPOLEKSOSBUDHANKAM, *malware*, *phising*, penanganan proaktif insiden, *profiling*, *ransomware*, *web defacement*, dan APT.

4. Hasil monitoring 2023

Berdasarkan Lanskap Keamanan Siber Indonesia Tahun 2023 yang diterbitkan oleh BSSN diketahui bahwa sepanjang tahun 2023 terdapat 403.990.813 anomali trafik (halaman 14). Dengan Grafik Top 10 anomali sepanjang 2023 adalah sebagai berikut:

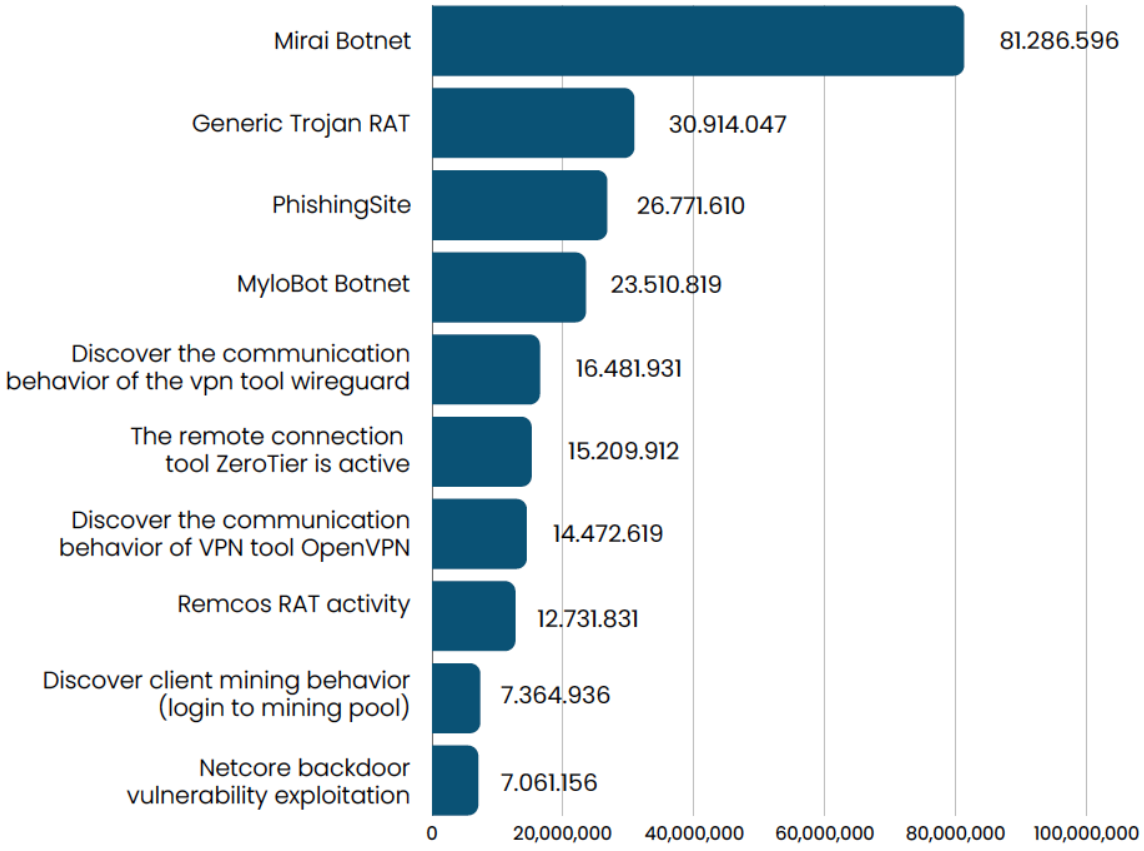


Generic Trojan RAT merupakan jenis signature yang menunjukkan adanya aktivitas komunikasi backdoor menuju domain berbahaya yang diduga sebagai server command and control (C2) milik pelaku ancaman. Aktivitas semacam ini berisiko dimanfaatkan untuk menjalankan tindakan mencurigakan seperti pencurian data, penghapusan file, pemblokiran akses, penyalinan informasi, hingga menjalankan program tertentu pada perangkat korban tanpa persetujuan pemiliknya. Malware ini secara khusus menargetkan perangkat berbasis sistem operasi Windows, dan dapat menyebar melalui berbagai cara seperti tautan pada email, pesan singkat, unduhan dari media penyimpanan (drive), atau melalui malware lain yang sudah terlebih dahulu menginfeksi perangkat.

Berdasarkan hasil pengamatan dan analisis dari Cyber Threat Intelligence, BSSN turut melakukan investigasi terhadap 347 dugaan insiden siber, dengan jenis insiden yang paling banyak ditemukan adalah kebocoran data (data breach). Sementara itu, melalui penelusuran di darknet, terdeteksi sebanyak 1.674.185 data yang terekspos, yang berdampak pada 429 pihak (stakeholder) di Indonesia. Dalam kasus perusakan tampilan situs (web defacement), terdapat 189 insiden yang telah diinformasikan oleh BSSN, dengan kategori terbanyak berupa defacement yang terjadi pada halaman tersembunyi. Sepanjang tahun 2023, Pusat Kontak Siber menerima sebanyak 1.417 laporan insiden siber, dengan lima kategori aduan terbanyak mencakup kejahatan siber (cybercrime), serangan ransomware, akses ilegal (illegal access), phishing, dan web defacement.

5. Hasil monitoring 2024

Berdasarkan Lanskap Keamanan Siber Indonesia Tahun 2024 yang diterbitkan oleh BSSN diketahui bahwa sepanjang tahun 2024 terdapat 330.527.636 anomali trafik (halaman 16). Dengan Grafik Top 10 anomali sepanjang 2024 adalah sebagai berikut:



Mirai Botnet adalah salah satu jenis botnet yang menargetkan perangkat *Internet of Things* (IoT). *Botnet* ini dibuat untuk melakukan serangan *Distributed Denial of Service* (DDoS) pada situs *web* atau layanan *online*, sehingga mengakibatkan adanya gangguan atau *downtime*. *Mirai Botnet* bekerja dengan melakukan identifikasi perangkat IoT yang memiliki *password default* atau yang mudah ditebak. Setelah itu, *Mirai* akan memanfaatkan kelemahan tersebut untuk menginfeksi perangkat dan menambahkannya ke dalam *botnet*. Perangkat-perangkat yang terinfeksi kemudian dapat dikendalikan oleh *threat actor* dan digunakan untuk meluncurkan serangan DDoS.

Mengacu pada hasil pengawasan dan analisis yang dilakukan oleh Cyber Threat Intelligence (CTI), BSSN turut menelusuri sebanyak 241 dugaan insiden kebocoran data. Sementara dari investigasi yang dilakukan di darknet, teridentifikasi sekitar 56.128.160 data yang terekspos, yang memengaruhi 461 stakeholder di wilayah Indonesia. Untuk insiden web defacement, tercatat terdapat 5.780 kasus berhasil diidentifikasi yang menargetkan beberapa domain dan sebanyak 4.071 *web defacement* terkait judi *online* yang menargetkan situs pemerintah. Berdasarkan laporan yang diterima dari *stakeholder* pada layanan aduan siber, diperoleh sebanyak 1.814 aduan pada tahun 2024, dengan 5 aduan terbanyak adalah sebagai berikut *Cybercrime, Vulnerability Indicator*, *Web Defacement*, *Ransomware*, dan *Illegal Access*.

Data laporan tahunan tersebut, berikut adalah data perbandingannya:

Table 1. Rekapitulasi Laporan Monitoring Kemanan Siber

Tahun	Jumlah Anomali	Top 10 Anomali	CTI
2020	495.337.202	1. AllAple 2. ZeroAccess 3. SCADA moxa 4. WillEcex 5. CVE-2017-11882 6. Generic Trojan 7. Gamarue 8. Mining Trojan 9. Glupteba 10. CobaltStrike	1293 Aduan: 1. Cross Site Scripting 2. SQL Injection 3. Malware 4. Phising 5. Web Defacement
2021	1.637.973.002	1. MyloBot Botnet 2. MiningPool 3. Discover Using Sock Agent 4. Win Trojan.AllAple 5. Generic Trojan RAT 6. PROTOCOL-SCADA moxa 7. Win Trojan ZeroAccess 8. CVE-2017-0147 9. RDP Account Brute Force 10. ISC BIND DoS vulnerability	179 laporan: data breach, ransomware, profiling, web defacement, malicious activity, dark web enabled crime (non fisik), compromised account, dan web phishing
2022	976.429.996	1. MyloBot Botnet 2. MiningPool Other Malware 3. Microsoft windows smb server information disclosure 4. Generic Trojan RAT 5. Discover the communication behavior of vpn tool openvpn 6. Discover using socks agent 7. Discovery of server information detected via OPTIONS 8. Plaintext password transmission found 9. PhishingSite Other Malware 10. RDP account brute force guess	1. 236 Aduan siber 2. 399 Dugaan Insiden Siber 3. 427 Instansi terdampak *darknet exposure*
2023	403.990.813	1. Generic Trojan RAT 2. PhishingSite Other Malware 3. Microsoft windows smb server information disclosure	1. 347 dugaan insiden siber 2. 1.674.185 temuan data exposure

		4. MiningPool Mining Virus 5. Discover the communication behavior of vpn tool openvpn 6. MSSQL database account brute force guess 7. MyloBot Botnet 8. The remote connection tool ZeroTier is active 9. Minerd Mining Virus activity 10. Discover the communication behavior of the vpn tool wireguard	3. 189 kasus web defacement
2024	330.527.636	1. Mirai Botnet 2. Generic Trojan RAT 3. PhishingSite 4. MyloBot Botnet 5. Discover the communication behavior of the vpn tool wireguard 6. The remote connection tool ZeroTier is active 7. Discover the communication behavior of vpn tool openvpn 8. Remcos RAT activity 9. Discover client mining behavior(login to mining pool) 10. Netcore backdoor vulnerability exploitation	1. 241 dugaan insiden kebocoran data. 2. 56.128.160 temuan data exposure 3. 4.071 web defacement

Sumber: Laporan Tahunan Monitoring Keamanan Siber BSSN

Dari data laporan monitoring tersebut diketahui bahwa jumlah anomali terbanyak terjadi pada tahun 2021, lonjakan ini erat kaitannya dengan dampak pandemi COVID-19. Selama periode ini terjadi percepatan transformasi digital secara mendadak untuk mendukung sistem kerja jarak jauh (*work from home*), pembelajaran daring, dan layanan digital lainnya. Kondisi ini menciptakan permukaan serangan (*attack surface*) yang jauh lebih luas karena banyak sistem yang belum memiliki pengamanan yang matang. Sedangkan tren anomali yang sering terjadi setiap tahunnya adalah *Malware* Trojan, *Phishing*, dan akses tidak sah.

1. Trojan adalah salah satu malware yang bersembunyi dibalik tautan, *file* atau *software* lainnya yang apabila kita mengklik tautan atau *file* dan *software* tersebut, maka penyerang bisa mengakses dan mencuri data penting yang ada. Penyerang mengirimkan pancingan atau umpan (yang menarik perhatian target) kepada target melalui email, pesan instan, atau situs *web* yang terinfeksi dengan *Trojan*. Target akan menerima umpan dan mengklik *file* atau mengunduh *software* yang mereka terima. Setelah diaktifkan, *Trojan* akan berusaha memperoleh akses ke sistem target dan mengambil alih kendali. Keberhasilan serangan Trojan ini sangat berkaitan dengan perilaku kita sebagai pengguna, apabila kita waspada dan memiliki kesadaran atas

keamanan siber maka kita tidak akan mudah mengakses tautan atau *file* yang tidak kita yakini keamanannya.

2. *Phising* adalah bentuk lain dari kata *phishing* yang berasal dari bahasa Inggris '*fishing'* yaitu memancing. *Phising* adalah serangan yang dilakukan untuk menipu atau memancing korban agar mau mengklik *link* atau tautan serta menginput informasi kredensial seperti *username* dan *password*. Keberhasilan serangan ini sangat tergantung pada kewaspadaan pengguna karena pelaku *phising* memanfaatkan kelengahan pengguna untuk mengklik tautan palsu atau memasukkan informasi pribadi ke dalam situs yang sebenarnya dikendalikan oleh pelaku.
3. Akses tidak sah (*unauthorized access*) merupakan tindakan yang dilakukan untuk mendapatkan akses ke sistem, jaringan, data, atau sumber daya lainnya tanpa izin atau persetujuan yang sah. Hal ini bisa terjadi karena berbagai cara, seperti menggunakan kredensial *login* yang dicuri, mengeksploitasi kerentanan perangkat lunak atau melewati langkah-langkah keamanan yang ada. Kredensial *login* adalah serangkaian informasi unik yang digunakan untuk memverifikasi identitas pengguna dan memberikan akses ke sistem atau aplikasi tertentu (misalnya nama pengguna dan kata sandi). Akses tidak sah berkaitan erat dengan kemampuan pengguna untuk melindungi kerahasiaannya dan menggunakan kata sandi yang kuat dan tidak mudah ditebak. Sedangkan kerentanan perangkat dan kemampuan penyerang dalam melewati pengamanan dapat berkaitan dengan penggunaan teknologi, prosedur yang diterapkan atau kemampuan manusia dalam menggunakan teknologi dan menerapkan prosedur keamanan.

Ketiga anomali tersebut berkaitan erat dengan faktor manusia. Teknologi yang canggih dan tata kelola keamanan yang baik akan tetap menghasilkan celah berbahaya apabila manusia yang berada di balik teknologi dan yang melaksanakan prosedur tersebut tidak memiliki kewaspadaan, kesadaran, pengetahuan dan keterampilan terkait keamanan siber. Kesalahan yang dianggap sepele dari satu individu dapat menimbulkan dampak finansial, reputasi, dan operasional yang sangat besar baik dalam lingkup sektoral maupun nasional. Kiranya tidak berlebihan apabila dikatakan manusia memang masih menjadi titik terlemah dalam keamanan siber di indonesia.

Aspek manusia dalam keamanan siber di Indonesia.

Data-data yang dipaparkan tersebut menunjukkan bahwa keamanan teknologi dan tata kelola yang baik tanpa diimbangi dengan perilaku aman dari manusia akan tetap menghasilkan celah berbahaya. Kesalahan kecil dari satu individu dapat menimbulkan dampak finansial, reputasi, dan operasional yang sangat besar. Ada beberapa alasan mendasar mengapa manusia tetap menjadi titik paling rentan dalam pertahanan keamanan:

1. Faktor Psikologis: Kelalaian, Kepercayaan Berlebihan, Kelelahan Digital

   Manusia secara alami rentan terhadap kesalahan, terutama ketika dihadapkan pada tekanan kerja tinggi, multitasking, atau kelelahan mental. Dalam kondisi seperti ini, mereka lebih mudah mengabaikan peringatan keamanan atau tertipu taktik rekayasa sosial. Berikut adalah beberapa sifat psikologis manusia yang berpengaruh terhadap risiko keamanan:

   a. Kecenderungan Percaya (Trust Bias)

      Manusia cenderung mempercayai pesan yang terlihat resmi, sehingga mudah tertipu oleh email phishing atau situs palsu. Penelitian Ferreira, A., Coventry, L., & Lenzini, G. (2015) menyebutkan bahwa trust bisa dimanfaatkan dalam phishing dengan menciptakan kesan kredibilitas dan urgensi. Sebagai contoh, email yang menyerupai institusi resmi seringkali lebih sukses dalam social engineering.

      Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Human aspects of information security, privacy, and trust* (pp. 36–47). Springer.

b. *Cognitive Overload* & *Decision Fatigue*

Terlalu banyak informasi atau aturan keamanan (misalnya *password* yang rumit, autentikasi ganda) menyebabkan kelelahan kognitif, sehingga pengguna mencari jalan pintas (*shortcut*).

Sumber: Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). *Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)*. Computers & Security.

c. Optimisme Tidak Realistis (Unrealistic Optimism)

Pengguna seringkali mengira bahwa mereka "tidak akan menjadi korban" serangan siber, sehingga mengabaikan pelatihan atau protokol keamanan. Penelitian Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2016) menunjukkan bahwa banyak individu yang merasa tidak akan menjadi target phishing, sehingga cenderung mengabaikan pelatihan keamanan siber yang merupakan sebuah bentuk nyata dari optimisme tidak realistis.

Caputo, D. D., Pfleeger, S. L., Freeman, J. D., & Johnson, M. E. (2016). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1), 28–38.

2. Kurangnya Edukasi Keamanan

Menurut *Fortinet's 2024 Security Awareness and Training Global Research Report*, sebanyak 67% organisasi menyatakan karyawan mereka kekurangan kesadaran keamanan dasar, meningkat dari 56% tahun sebelumnya. Banyak organisasi yang masih belum menjadikan pelatihan keamanan siber sebagai prioritas. Akibatnya, karyawan tidak memahami ancaman terbaru, teknik serangan, atau prosedur dasar pencegahan.

3. Adopsi Teknologi Tanpa Pemahaman Risiko

Semakin banyak teknologi baru yang diadopsi tanpa edukasi keamanan memadai. *Cloud services*, aplikasi kolaborasi, dan perangkat IoT memperbesar permukaan serangan jika pengguna tidak memahami cara aman menggunakannya. *The Wall Street Journal* melaporkan bahwa 78% data breach di 2023 melibatkan data yang tersimpan di cloud, menandakan kesalahan konfigurasi dan rendahnya pemahaman terhadap risiko cloud.

4. *Social Engineering*: Manusia Sebagai Sasaran Empuk

Serangan berbasis sosial, seperti *phishing*, *vishing*, atau *baiting*, memanfaatkan kepercayaan, rasa ingin tahu, atau ketergesaan manusia. Bahkan individu dengan jabatan tinggi pun tidak kebal terhadap manipulasi psikologis semacam ini. *Financial Times* melaporkan bahwa sekitar 50% serangan social engineering berupa kompromi email bisnis, dan kasusnya meningkat dua kali lipat dari 2022 ke 2023.

KESIMPULAN DAN SARAN

Berdasarkan pembahasan yang telah diuraikan, dapat disimpulkan bahwa kondisi yang digambarkan oleh Mitnick pada tahun 2002 "*the human factor is truly security's weakest link*" juga nyata terjadi di Indonesia sampai saat ini. Dalam rantai keamanan siber nasional, faktor manusia terbukti menjadi mata rantai paling rentan, bahkan ketika teknologi, sistem telah dibangun dengan canggih serta tata kelola dirancang sedemikian kuat. Sejumlah insiden seperti serangan *ransomware* terhadap PDNS 2, *Malware Trojan*, *Phishing*, dan akses tidak sah menjadi tren anomali yang sering terjadi setiap tahunnya menunjukkan bahwa kelemahan ini bersifat sistemik. Penyebab utama kelemahan manusia dalam sistem keamanan siber yaitu:

1. Faktor Psikologis: Kelalaian, Kepercayaan Berlebihan, Kelelahan Digital
2. Kurangnya Edukasi Keamanan
3. Adopsi Teknologi Tanpa Pemahaman Risiko
4. *Social Engineering*: Manusia Sebagai Sasaran Empuk

Dengan demikian, penguatan aspek manusia melalui literasi digital, pelatihan praktis, serta integrasi budaya keamanan dalam kehidupan digital sehari-hari merupakan prasyarat utama untuk membangun sistem keamanan siber nasional yang tangguh dan berkelanjutan

DAFTAR PUSTAKA

(APJII), Asosiasi Penyelenggara Jasa Internet Indonesia, 'APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang', *Asosiasi Penyelenggara Jasa Internet Indonesia (APJII)*, 2024 <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang%0A>

Aryani, Dwi Septa, and Kusminaini Armin, 'Pengaruh Tax Avoidance Terhadap Cost of Debt Pada Perusahaan Yang Terdaftar Di Indeks Pefindo 25', *Jurnal Riset Akuntansi Tridinanti (Jurnal Ratri)*, 4.1 (2022), 27–33 <http://www.univ-tridinanti.ac.id/ejournal/index.php/ratri>

Caputo, Deanna, Shari Pfleeger, Jesse Freeman, and M.Eric Johnson, 'Going Spear Phishing: Exploring Embedded Training and Awareness', *Security & Privacy, IEEE*, 12 (2014), 28–38 <https://doi.org/10.1109/MSP.2013.106>

Colback, Lucy, 'Technology and Cyber Crime: How to Keep out the Bad Guys', *Financial Times Cyber Security*, 2024 <https://www.ft.com/content/8a79ab25-c902-4110-bcb8-be2fd422f6bf>

Febrianti, Fitri Dwi, Sugiyanto Sugiyanto, and Juwita Ramandani Fitria, 'GREEN INTELLECTUAL CAPITAL CONSERVATISM EARNING MANAGEMENT, TO FUTURE STOCK RETURN AS MODERATING STOCK RETURN (Study of Mining Companies in Indonesia Listed on IDX for the Period of 2014-2019)', *The Accounting Journal of Binaniaga*, 5.2 (2020), 141 <https://doi.org/10.33062/ajb.v5i2.407>

Ferreira, Ana, Lynne Coventry, and Gabriele Lenzini, 'Principles of Persuasion in Social Engineering and Their Use in Phishing', *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9190.May 2017 (2015), 36–47 <https://doi.org/10.1007/978-3-319-20376-8_4>

Gurd, Bruce, 'Remaining Consistent with Method? An Analysis of Grounded Theory Research in Accounting', ed. by Sven Modell and Chris Humphrey, *Qualitative Research in Accounting & Management*, 5.2 (2008), 122–38 <https://doi.org/10.1108/11766090810888926>

Parsons, Kathryn, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram, 'Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers and Security*, 42.September (2014), 165–76 <https://doi.org/10.1016/j.cose.2013.12.003>

Stuart Madnick, 'What's Behind the Increase in Data Breaches?', *The Wall Street Journal*, 2024 <https://www.wsj.com/tech/cybersecurity/why-are-cybersecurity-data-breaches-still-rising-2f08866c>

Sugiyanto, 'Pengaruh Tax Avoidance Terhadap Nilai Perusahaan Dengan Pemoderasi Kepemilikan Institusional (Studi Kasus Pada Perusahaan Manufaktur Yang Terdaftar Di Bursa Efek Indonesia 2011-2015)', *Jurnal Ekonomi Akuntansi Universitas Pamulang*, 2015, 82–96

Sugiyanto, and Etty Murwaningsari, 'Earning Management, Risk Profile and Efficient Operation in the Prediction Model of Banking : Eviden from Indonesia', *International Journal of Scientific Research in Science and Technology*, 4.5 (2018), 135–50 <https://www.academia.edu/download/57069054/2727.pdf>

Sugiyanto, S, R Kartolo, and M Yusuf, 'Implikasinya Umkm Pada Ekonomi Kreatif Dan Inovasi Di Kabupaten Garut Jawa Barat', *Abdi Laksana: Jurnal …*, 2 (2021), 67–74 <http://www.openjournal.unpam.ac.id/index.php/JAL/article/view/8775>

Sugiyanto, Sugiyanto, and Fitri Dwi Febrianti, 'The Effect of Green Intellectual Capital, Conservatism, Earning Management, to Future Stock Return and Its Implications on Stock Return', *The Indonesian Accounting Review*, 11.1 (2021), 93–103 <https://doi.org/10.14414/tiar.v11i1.2286>