
2025
21 – 27 April 2025
Kamsib Indonesia on Paper
Edisi 12
Tetap Aman Bersama Kamsib
Kamsib Indonesia on Paper adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital.

Kamsib Indonesia on Paper

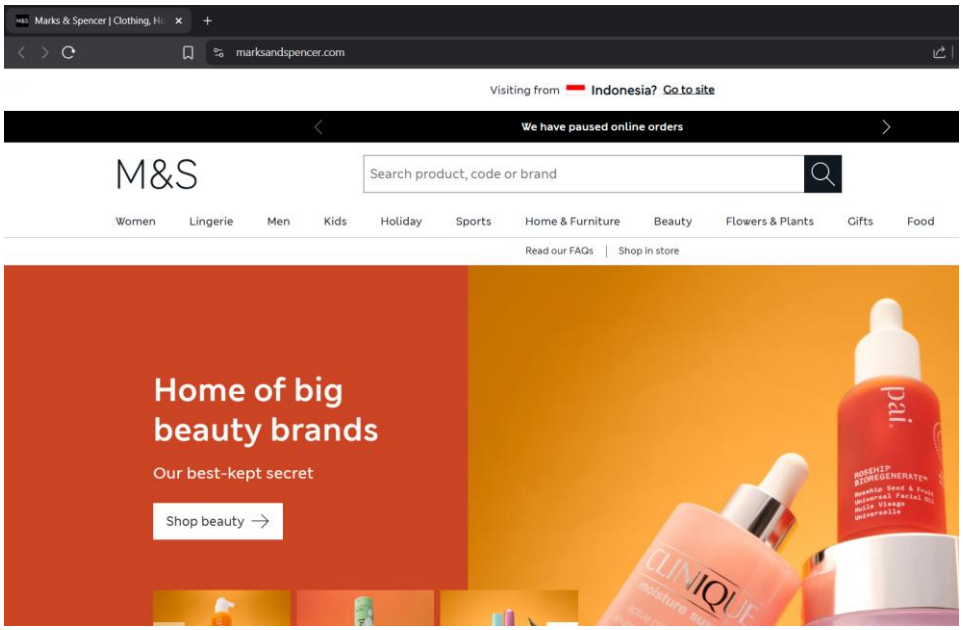
Edisi 12
21 – 27 April 2025

M&S bekerja sama dengan lembaga keamanan siber Inggris, seperti National Cyber Security Centre (NCSC) dan National Crime Agency (NCA).

Serangan Siber terhadap Marks & Spencer (M&S)

Penulis: **Anton Lepari**

Marks & Spencer (M&S) baru-baru ini mengalami gangguan besar akibat serangan siber yang menyebabkan masalah signifikan bagi pelanggan. Sebagai informasi, M&S adalah sebuah perusahaan ritel asal Inggris yang terkenal dengan produk-produk pakaian, makanan, dan peralatan rumah tangga. Serangan ini memengaruhi layanan pembayaran nirsentuh dan pemesanan daring di Inggris dan Irlandia. Sebagai respons, M&S menghentikan sementara semua pesanan online melalui situs web dan aplikasi mereka, serta menonaktifkan akses VPN untuk staf yang bekerja dari rumah guna mencegah penyebaran serangan lebih lanjut.



Gambar 1: Tampilan Situs marksandspencer.com. [Kamsib Indonesia]

Serangan tersebut memengaruhi berbagai layanan perusahaan, termasuk pemrosesan pembayaran dan sistem *Click and Collect* di toko-toko mereka. Gangguan layanan dan pembatalan pesanan terjadi sebagai akibat dari serangan ini, banyak pelanggan yang pesanan daringnya dibatalkan atau tertunda. Selain itu, pelanggan yang memilih layanan *Click and Collect* mengalami keterlambatan dalam pengambilan barang yang sudah mereka pesan sebelumnya.

Untuk mengatasi serangan ini, M&S bekerja sama dengan lembaga keamanan siber Inggris, seperti National Cyber Security Centre (NCSC) dan National Crime Agency (NCA), untuk mengidentifikasi dan mengatasi masalah yang terjadi. Mereka juga melibatkan ahli eksternal untuk membantu memulihkan sistem mereka. M&S juga memastikan bahwa tidak ada data pelanggan yang dicuri, meskipun mereka memperingatkan potensi ancaman penipuan yang bisa terjadi akibat serangan ini.

Serangan siber ini berdampak pada kepercayaan pelanggan, yang semakin merasa cemas tentang keamanan data pribadi mereka. Meskipun M&S telah mengambil langkah-langkah untuk memperbaiki situasi, dampak jangka panjang terhadap reputasi perusahaan dan keuangan masih belum dapat dipastikan.

Sumber

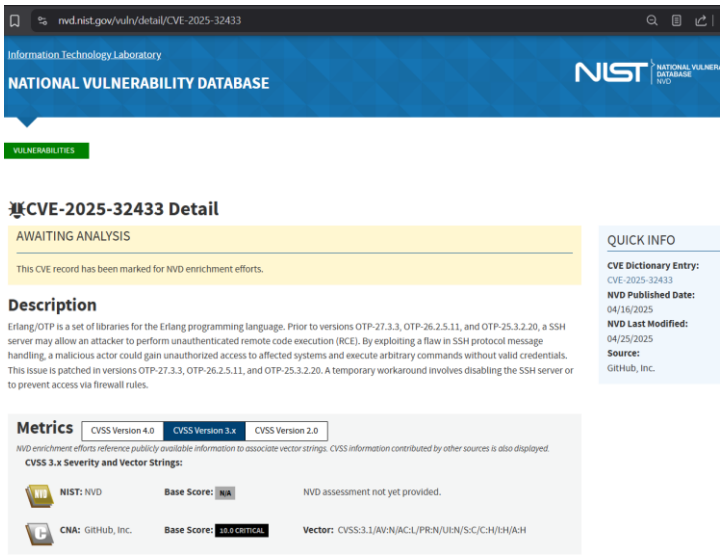
- Sarah Butler. (25 April 2025). *Marks & Spencer pauses online orders as firm struggles with cyber-attack fallout*. The Guardian.
- Tom Gerken & Graham Fraser. (26 April 2025). *M&S stops online orders and issues refunds after cyber attack*. BBC.
- Megan Howe. (26 April 2025). *M&S suspends online orders as cyber attack causes further chaos for shoppers*. The Standard.

Satu CVE Terlupa,
Seribu Masalah Menunggu

Eksploitasi Kerentanan Erlang/OTP SSH CVE-(2025-32433)

Penulis: **Anton Lepari**

Kerentanan kritis CVE-2025-32433 pada Erlang/OTP SSH dieksploitasi secara aktif, memungkinkan penyerang menjalankan kode dari jarak jauh pada perangkat yang terpengaruh. Erlang/OTP adalah sekumpulan pustaka (*library*) untuk bahasa pemrograman Erlang. Sebelum versi OTP-27.3.3, OTP-26.2.5.11, dan OTP-25.3.2.20, server SSH dapat memungkinkan penyerang untuk melakukan eksekusi kode jarak jauh (*remote code execution*/RCE) yang tidak diautentikasi.



Gambar 2: CVE-2025-32433 Detail di Situs NVD NIST. [Kamsib Indonesia]

Dengan memanfaatkan kelemahan dalam penanganan pesan protokol SSH, pelaku kejahatan dapat memperoleh akses tidak sah ke sistem yang terpengaruh dan menjalankan perintah sembarangan tanpa kredensial yang valid. Masalah ini telah ditambal dalam versi OTP-27.3.3, OTP-26.2.5.11, dan OTP-25.3.2.20. Solusi sementara melibatkan penonaktifan server SSH atau mencegah akses melalui aturan *firewall*.

Bahasa Pemrograman Erlang

Erlang adalah bahasa pemrograman fungsional, konkuren, dan fault-tolerant yang awalnya dikembangkan oleh Ericsson pada tahun 1980-an untuk membangun sistem telekomunikasi yang high-availability (waktu downtime sangat rendah). Istilah Erlang digunakan secara bergantian dengan Erlang/OTP, atau *Open Telecom Platform* (OTP), yang terdiri dari sistem runtime Erlang, beberapa komponen siap pakai (OTP) yang sebagian besar ditulis dalam Erlang, dan serangkaian prinsip desain untuk program Erlang.

Erlang sangat populer untuk:

- Sistem telekomunikasi
- *Chat server* (seperti WhatsApp awalnya)
- *Messaging system* (seperti RabbitMQ, dibangun di atas Erlang)
- Sistem *real-time* dengan kebutuhan *uptime* tinggi

Contoh sederhana program Erlang:

```
-module(chat_server).
-export([start/0, loop/1]).

start() ->
    {ok, ListenSocket} = gen_tcp:listen(1234, [binary, {packet, 0},
{active, false}]),
    accept(ListenSocket).

accept(ListenSocket) ->
    {ok, Socket} = gen_tcp:accept(ListenSocket),
    spawn(fun() -> loop(Socket) end),
    accept(ListenSocket).

loop(Socket) ->
    case gen_tcp:recv(Socket, 0) of
        {ok, Data} ->
            io:format("Received: ~p~n", [Data]),
            gen_tcp:send(Socket, <<"Message received!">>),
            loop(Socket);
        {error, closed} ->
            io:format("Connection closed~n")
    end.
```

Penjelasan:

- `start/0` membuka port 1234.
- `accept/1` menerima koneksi baru dan langsung *spawn process* baru untuk menangani setiap koneksi.
- `loop/1` membaca data dari koneksi, mencetaknya, lalu mengirim balasan.

Dalam dunia nyata, aplikasi seperti WhatsApp (sebelum diakuisisi Facebook) menggunakan Erlang karena bisa menangani jutaan koneksi sekaligus. Karena setiap koneksi dibuat di *process* berbeda, server ini bisa menangani ribuan koneksi bersamaan tanpa "pusing" dengan *thread pool* atau *blocking* seperti di bahasa lain (contoh C, Java).

Karena dalam dunia digital, bukan lagi soal "apakah akan diserang", tetapi "kapan".

Tren Serangan Siber di 2025: Apa yang Harus Diwaspadai?

Penulis: **Anton Lepari**

Tahun 2025 diprediksi akan menjadi salah satu tahun paling menantang dalam sejarah keamanan dunia maya. Dengan adopsi teknologi baru seperti kecerdasan buatan, *Internet of Things* (IoT), hingga komputasi kuantum yang mulai masuk radar, pola serangan juga ikut bertransformasi. Lalu, apa saja tren serangan siber yang harus kita waspadai di 2025? Mari kita kupas satu per satu.

1. Serangan Berbasis AI Makin Canggih

Kecerdasan buatan bukan hanya alat bagi perusahaan untuk meningkatkan efisiensi. Kini, AI juga dimanfaatkan oleh aktor jahat untuk menciptakan serangan yang lebih pintar dan sulit dideteksi. Contohnya, *deepfake phishing*, di mana email, suara, bahkan video palsu dibuat sangat realistis untuk menipu korban. Lebih buruk lagi, muncul *malware* berbasis AI yang bisa mengubah bentuk (*polymorphic malware*) secara otomatis agar lolos dari deteksi antivirus.

2. IoT dan Perangkat Pintar Jadi Sasaran Baru

Perangkat pintar seperti kamera keamanan, *smart TV*, bahkan kulkas pintar, menjadi target empuk. Banyak produsen masih mengutamakan kecepatan rilis produk daripada membangun keamanan yang kuat. Akibatnya, *hacker* dapat memanfaatkan celah pada IoT untuk masuk ke jaringan rumah atau kantor.

3. Serangan Supply Chain Semakin Rumit

Jika dulu *hacker* fokus menyerang target utama, kini mereka sering memulai dengan vendor atau pihak ketiga yang lebih rentan. *Supply chain attack* tidak hanya terjadi di *software* (seperti serangan SolarWinds), tetapi juga mulai merambah *hardware*, termasuk *chip* dan *firmware*.

4. Ransomware "As a Service" (RaaS) Semakin Terorganisasi

Ransomware kini bukan hanya alat, tetapi industri. Model *"Ransomware as a Service"* memungkinkan siapa pun —bahkan tanpa keahlian teknis tinggi— untuk meluncurkan serangan *ransomware* dengan menyewa layanan dari grup kriminal. Bahkan, beberapa kelompok menawarkan "layanan pelanggan" untuk membantu korban membayar tebusan dengan lebih mudah.

5. Infrastruktur Kritis Jadi Target Prioritas

Instalasi penting seperti listrik, air bersih, jaringan transportasi, dan sistem kesehatan makin sering menjadi sasaran. Serangan ke infrastruktur bukan lagi soal uang semata, melainkan soal pengaruh politik dan ekonomi.

6. Evolusi Social Engineering

Teknik manipulasi sosial makin halus dan personal. Dengan data bocoran dari berbagai kebocoran sebelumnya, pelaku bisa membuat serangan *phishing* yang sangat meyakinkan, bahkan menggunakan *voice cloning* untuk meniru suara atasan atau rekan kerja.

7. Kerentanan Cloud dan API Meningkat

Adopsi *cloud* besar-besaran membuka peluang baru bagi penyerang. Kesalahan konfigurasi *cloud storage* tetap menjadi penyebab utama kebocoran data. Selain itu, API (*Application Programming Interface*) menjadi titik lemah baru yang sering diabaikan oleh banyak organisasi.

8. Quantum Computing

Meskipun teknologi ini masih dalam tahap awal, ancaman dari komputasi kuantum sudah mulai diperhitungkan. Penyerang bisa melakukan "*Harvest Now, Decrypt Later*", yakni mencuri data terenkripsi hari ini, untuk didekripsi nanti ketika komputer kuantum sudah cukup kuat.

Tahun 2025 membawa tantangan baru dalam lanskap keamanan siber. Dengan serangan yang semakin canggih dan variatif, organisasi dan individu perlu meningkatkan kewaspadaan. Membangun budaya keamanan, menerapkan prinsip *zero trust*, dan terus memperbarui pertahanan digital adalah kunci untuk bertahan.

Karena dalam dunia digital, bukan lagi soal "apakah akan diserang", tetapi "kapan".

Kamsib Indonesia
Jakarta, Indonesia
hubungi@kamsib.id

Kamsib ID *adalah sebuah platform edukasi yang berfokus pada keamanan informasi dan siber dalam bahasa Indonesia. Kehadiran Kamsib dipicu oleh lonjakan pesat penggunaan internet yang tidak diimbangi dengan kesadaran akan pentingnya keamanan di dunia maya. Fenomena ini juga menjadi salah satu pemicu dari banyaknya kasus penipuan, kebocoran data, dan insiden dalam sistem elektronik, baik yang dimiliki oleh pemerintah maupun swasta.*

Kamsib Indonesia on Paper *adalah majalah yang membahas berbagai aspek keamanan siber, mulai dari ancaman terbaru, teknik perlindungan, hingga tren teknologi yang memengaruhi lanskap keamanan digital. Diterbitkan secara berkala, majalah ini menyajikan artikel mendalam, studi kasus, serta wawancara dengan para ahli untuk memberikan wawasan bagi profesional keamanan siber, peneliti, dan penggemar dunia siber. Dengan pendekatan yang informatif dan analitis, Kamsib Indonesia on Paper bertujuan menjadi referensi utama bagi siapa saja yang ingin memahami dan menghadapi tantangan di dunia siber yang terus berkembang.* [at]kamsib_id