Raksasa Medis Stryker Lumpuh Total Akibat Serangan Siber

Category: INTERNASIONAL
written by Redaksi | March 12, 2026



Penyedia peralatan medis global asal Amerika Serikat, Stryker, tengah menghadapi kelumpuhan operasional berskala internasional setelah menjadi target serangan siber masif. Kelompok peretas bernama Handala, yang dikenal memiliki kedekatan dengan kepentingan Iran, mengklaim bertanggung jawab atas gangguan yang menyebabkan sistem perusahaan di puluhan negara terhenti seketika.

Dalam pernyataan resminya, pihak peretas mengklaim telah menghapus data dari lebih dari 200.000 sistem, server, dan perangkat seluler, serta mengekstraksi sekitar 50 terabyte data sensitif milik perusahaan.

Operasi Terhenti di 79 Negara

Dampak serangan ini dirasakan paling parah di Irlandia, pusat manufaktur utama Stryker yang mempekerjakan sekitar 4.000

staf. Laporan lapangan menyebutkan seluruh lini produksi terhenti total. “Tidak ada yang bisa bekerja. Perusahaan benar-benar lumpuh dan staf tidak tahu apa yang sedang terjadi,” ungkap seorang sumber internal perusahaan.

Stryker, melalui pernyataan di laman LinkedIn, mengonfirmasi adanya “gangguan jaringan global” yang memengaruhi lingkungan perangkat lunak Microsoft mereka. Meski demikian, perusahaan yang memiliki sekitar 53.000 karyawan ini mengeklaim bahwa insiden tersebut telah berhasil dilokalisasi.

“Kami belum menemukan indikasi adanya ransomware atau malware konvensional. Tim kami bekerja cepat untuk memahami dampak penuh dari serangan ini,” tulis pernyataan resmi Stryker.

Modus Operandi: Malware Penghapus Data

Meskipun Stryker menyangkal adanya malware, para ahli keamanan siber mencurigai penggunaan data-wiping malware—perangkat lunak jahat yang dirancang khusus untuk menghapus seluruh isi cakram keras secara permanen. Laporan dari platform Reddit yang diduga berasal dari karyawan Stryker menunjukkan bahwa serangan ini menyasar sistem Microsoft Intune, platform yang digunakan perusahaan untuk mengelola perangkat seluler dan komputer secara jarak jauh.

Peneliti keamanan Kevin Beaumont mencatat bahwa kelompok Handala sering menggunakan teknik phishing canggih, terkadang menyamar sebagai vendor keamanan ternama seperti CrowdStrike, untuk menyusup ke jaringan. Peretas biasanya “bersembunyi” di dalam sistem selama berbulan-bulan sebelum meluncurkan serangan penghapusan data secara serentak.

Motif Politik dan Perang Siber

Kelompok Handala secara terang-terangan menyatakan bahwa serangan ini merupakan aksi balas dendam atas serangan rudal militer Amerika Serikat terhadap sebuah sekolah di Iran baru-

baru ini. “Ini hanyalah awal dari babak baru dalam peperangan siber,” tulis kelompok tersebut dalam situs gelapnya.

Selain Stryker, Handala juga mengeklaim telah membobol penyedia pembayaran elektronik Verifone pada hari yang sama. Namun, pihak Verifone telah memberikan bantahan resmi kepada publik dan memastikan tidak ada gangguan layanan pada sistem mereka.

Sejauh ini, fokus utama Stryker adalah memastikan bahwa serangan tidak berdampak pada fungsi peralatan medis yang telah terpasang di rumah sakit, melainkan hanya terbatas pada sistem administratif dan manajemen perangkat karyawan.