Nama : Roji Fayyumi

NIM : 2121500044

Keamanan Siber (cybersecurity) adalah praktik yang dirancang untuk melindungi sistem komputer, jaringan, perangkat, dan data dari ancaman dan serangan siber. Ini mencakup langkah-langkah seperti mengidentifikasi dan mengatasi kerentanan, mengenkripsi data, memantau aktivitas jaringan, dan mengimplementasikan perangkat lunak keamanan guna melindungi informasi sensitif dari akses yang tidak sah, perusakan, atau pencurian. Tujuannya adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi serta melindungi sistem komputer dari serangan seperti malware, peretasan, dan serangan siber lainnya.

Semakin canggih teknologi saat ini semakin banyak kasus-kasus cybercrime yang terjadi di dunia ini,salah satunya “Colonial Pipeline serangan Ransomewere pada Mei 2021”. Serangan ini menginfeksi beberapa sistem digital pipeline, mematikannya selama beberapa hari. Penutupan ini berdampak pada konsumen dan maskapai penerbangan di sepanjang Pantai Timur. Peretasan tersebut dianggap sebagai ancaman keamanan nasional, karena jalur pipa tersebut mengalirkan minyak dari kilang ke pasar industri. Hal ini menyebabkan Presiden Joe Biden mengumumkan keadaan darurat.

Jalur Pipa Kolonial adalah salah satu jalur pipa minyak terbesar dan terpenting di AS. Jalur ini dimulai pada tahun 1962 untuk membantu memindahkan minyak dari Teluk Meksiko ke negara bagian Pantai Timur. Jalur Pipa Kolonial terdiri dari lebih dari 5.500 mil jalur pipa. Ini dimulai di Texas dan terus berlanjut hingga New Jersey, memasok hampir setengah bahan bakar untuk Pantai Timur. Saluran Pipa Kolonial menyalurkan minyak olahan untuk bensin, bahan bakar jet, dan minyak pemanas rumah. Kantor pusat Colonial Pipeline berada di Alpharetta, GA.

Peretasan Colonial Pipeline adalah serangan siber terbesar yang diungkapkan secara publik terhadap infrastruktur penting di AS Serangan tersebut melibatkan beberapa tahap terhadap sistem TI Colonial Pipeline. Sistem teknologi operasional pipa yang sebenarnya memindahkan minyak tidak secara langsung dikompromikan selama serangan tersebut.

Serangan dimulai ketika kelompok peretas yang diidentifikasi sebagai DarkSide mengakses jaringan Colonial Pipeline. Para penyerang mencuri 100 gigabyte data dalam waktu dua jam. Setelah pencurian data, para penyerang menginfeksi jaringan TI Colonial Pipeline dengan ransomware yang memengaruhi banyak sistem komputer, termasuk penagihan dan akuntansi.

[Colonial Pipeline menutup saluran pipa](https://www.techtarget.com/searchsecurity/news/252500544/Colonial-Pipeline-runs-dry-following-ransomware-attack) untuk mencegah penyebaran ransomware. Perusahaan investigasi keamanan Mandiant kemudian dibawa untuk menyelidiki serangan tersebut. FBI, Badan Keamanan Siber dan Infrastruktur, Departemen Energi AS, dan Departemen Keamanan Dalam Negeri juga diberitahu tentang insiden tersebut. Colonial Pipeline membayar peretas DarkSide untuk mendapatkan kunci dekripsi, sehingga staf TI perusahaan mendapatkan kembali kendali atas sistemnya. Colonial Pipeline memulai kembali operasi pipa pada 12 Mei.

Penyebab serangan Colonial Pipeline?

Penyerang masuk ke jaringan Colonial Pipeline melalui [kata sandi yang terbuka untuk akun VPN](https://www.techtarget.com/searchsecurity/news/252502216/Mandiant-Compromised-Colonial-Pipeline-password-was-reused) , kata Charles Carmakal, wakil presiden senior dan CTO di perusahaan keamanan siber Mandiant, dalam sidang di hadapan Komite Keamanan Dalam Negeri DPR pada 8 Juni. Banyak organisasi menggunakan [VPN](https://www.techtarget.com/searchnetworking/definition/virtual-private-network) untuk menyediakan akses jarak jauh yang aman dan terenkripsi ke dalam jaringan perusahaan. Menurut kesaksian Carmakal, seorang karyawan Colonial Pipeline – yang tidak disebutkan namanya secara publik selama persidangan – kemungkinan besar menggunakan kata sandi yang sama untuk VPN di lokasi lain. Kata sandi tersebut entah bagaimana telah disusupi sebagai bagian dari pelanggaran data lainnya. [Penggunaan kembali kata sandi telah menjadi masalah umum](https://www.techtarget.com/searchsecurity/news/252457795/Ponemon-study-Poor-password-practices-remain-rampant) , karena banyak pengguna sering menggunakan kata sandi yang sama lebih dari sekali.

**Garis waktu serangan Colonial Pipeline**

Serangan dan pemulihan Jalur Pipa Kolonial terjadi dengan sangat cepat dalam waktu singkat.

**6 Mei 2021**

* Intrusi awal dan pencurian data.

**7 Mei 2021**

* Serangan Ransomware dimulai.
* Colonial Pipeline menyadari pelanggaran tersebut.
* Perusahaan keamanan Mandiant dipanggil untuk menyelidiki dan menanggapi serangan tersebut.
* Penegakan hukum dan otoritas pemerintah federal memberi tahu tentang serangan itu.
* Pipeline dibuat offline untuk mengurangi risiko paparan terhadap jaringan operasional.
* Colonial Pipeline membayar uang tebusan sebesar 75 bitcoin ($4,4 juta) kepada

**9 Mei 2021**

* Deklarasi darurat oleh Presiden Joe Biden.

**12 Mei 2021**

* Pipeline dimulai ulang saat operasi normal dilanjutkan.

**7 Juni 2021**

* Departemen Kehakiman memulihkan 63,7 bitcoin -- sekitar $2,3 juta -- dari para penyerang.

**8 Juni 2021**

* Sidang Kongres tentang serangan itu.

Ini sekilas tentang kasus cybercrime terbesar di tahun 2021, jika kalian tertarik untuk membaca kasus ini, kalian bisa membacanya di https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know