Analisis Kejahatan

Dzikri Muhammad Akbar

5520123120

Manajemen Keamanan Informasi IF D 2023

1. Insiden (kejahatan) berbasis digital yang terjadi Pada PDN (Pusat Data Nasional) dan PDNS (Pusat Data Nasional Sementara)
    a. Nama Kejahatan.
    Ransomware attack. Serangan ransomware “Brain Cipher” terhadap Pusat Data Nasional (PDN / PDNS) (Indonesia)

    Ransomware adalah jenis malware dimana sang pelaku menggunakan kode enkripsi pada data korban, sehingga korban tidak dapat mengakses data, umumnya pelaku akan meminta tebusan kepada korban.
    Menurut IBM, ransomware merupakan salah satu bentuk malware yang paling umum. Serangan ransomware dapat menyebabkan kerugian besar bagi organisasi karena data korban dienkripsi dan aksesnya diblokir hingga uang tebusan dibayarkan (IBM, n.d.).

    b. Langkah Langkah Penyusup.

Tahap	Peristiwa	Keterangan / sumber
1. Kelemahan persiapan / procurement	Dalam proyek pengadaan Pusat Data Nasional, disinyalir persyaratan keamanan dari BSSN (standar kelayakan keamanan siber) tidak dimasukkan sebagai syarat dalam tender. terhadap regulasi keamanan, sehingga sistem rentan.	“Jejak Horor Serangan Ransomware di Indonesia … dari PDNS sampai BSI”
2. Kurangnya kepatuhan regulasi / pengamanan	Penyusup menggunakan ransomware (Brain Cipher) dan memanfaatkan sistem yang tidak sepenuhnya terlindungi atau memiliki kontrol keamanan yang lemahnya (seperti backup, proteksi endpoint, patch keamanan).	Dalam laporan, disebut bahwa banyak tenant (instansi) tidak memiliki backup sebagai alasan pemulihan lambat
3. Eksploitasi kerentanan & infiltrasi	Pelaku menggunakan ransomware Brain Cipher (varian LockBit 3.0) untuk menyerang PDNS 2	“Brain Cipher varian baru dari Lockbit 3.0 menjadi biang kerok hingga data-data … terkunci” (detikinet)
4. Enkripsi / penguncian data & gangguan sistem	Banyak instansi (kementerian, lembaga, pemda) terdampak; layanan publik seperti imigrasi terganggu	Laporan menyebut bahwa layanan imigrasi menjadi yang paling parah terdampak
5. Permintaan tebusan	Pelaku meminta tebusan sekitar USD 8 juta (± Rp 131,2 miliar)	Reuters menyebut bahwa pelaku “asked for $8 million in ransom” (Reuters)

    c. Langkah Perusahaan Menemukan Insiden.

- Server PDN (Pusat Data Nasional) dan sistem pemerintahan tidak bisa diakses serta layanan terganggu secara luas.
- Ketika Windows Defender atau sistem proteksi keamanan tidak aktif atau terlambat memperbaharui patch, muncul kelemahan yang bisa dieksploitasi. (Meski belum semua detail dipublikasikan)
- Ada laporan dari publik/pihak internal tentang kegagalan layanan publik (imigrasi, keimigrasian dll) yang menimbulkan alarm.
- Pemerintah : BSSN dan Kominfo segera memeriksa insiden setelah mendengar gangguan layanan dan laporan publik.

d. Langkah Antisipasi Perusahaan.
   - Pemerintah melakukan backup data secara berlapis. Dan menjadikan backup sebagai kewajiban untuk seluruh kementrian
   - Pemerintah menyiapkan Cadangan server pada Lokasi lain
   - Melakukan audit keamanan pada PDNS 1 dan 2 oleh pihak independen, untuk mengidentifikasi kelemahan dan implementasi perbaikan
   - Pemerintah mengevaluasi secara menyeluruh prosedur keamanan siber, SOP, manajemen kredensial (password, akses), patch management, proteksi endpoint.

2. Insiden (kejahatan) berbasis digital yang terjadi Pada SolarWinds / Sunburst pada tahun 2020.
   a. Nama Kejahatan.
      SolarWinds supply-chain attack “Sunburst” backdoor / cyber espionage (2020)
      Backdor adalah tindak kejahatan digital berbentuk program malware atau modfikasi kode yang berbahaya digunakan untuk masuk ke sistem tanpa hak, dan mengambil data sensitif melalui jarak jauh atau perintah tertentu yang otomatis aktif pada kondisi yang diinginkan pelaku.

   b. Langkah Langkah Penyusup.

Tahap	Peristiwa
1. Reconnaissance / pemilihan target	Pelaku memetakan vendor perangkat lunak (SolarWinds) dan daftar pelanggan pentingnya (pemerintah, perusahaan besar).
2. Kompromisasi pipeline build / server vendor	Penyerang mendapatkan akses ke server pengembang / pipeline CI/CD SolarWinds (build system).
3. Penyisipan backdoor ke proses build	Memodifikasi proses build sehingga backdoor (Sunburst) ter-embed ke dalam binary Orion saat pembuatan rilis.
4. Penandatanganan & rilis update berbahaya	Paket update yang sudah berisi backdoor ditandatangani dan dirilis sebagai update resmi SolarWinds Orion.
5. Aktivasi backdoor & komunikasi ke C2	Setelah terinstal, backdoor melakukan beacon/komunikasi outbound ke server Command & Control (C2) untuk menerima instruksi.
6. Pengintaian internal, lateral movement & eksfiltrasi	Pelaku melakukan credential harvesting, bergerak lateral di jaringan korban, mengakses aset bernilai (email, dokumen, konfigurasi) dan mengekstrak data.

c. Langkah Perusahaan Menemukan Insiden.

a. Deteksi dari vendor/penyedia keamanan internal — laporan anomali pada tooling keamanan.
b. Alert lalu lintas keluar (outbound) abnormal — koneksi ke domain/URL tak dikenal atau pola DNS mencurigakan.
c. Peringatan EDR/AV — proses yang melakukan tindakan berbahaya (credential access, memory dump, modul asing).
d. Perubahan artefak sistem — muncul scheduled task/service baru, binary dengan hash tidak dikenal, atau file yang di-timestamp ganjil.
e. Log SIEM menunjukkan pola aneh — login admin dari host tidak biasa, eskalasi hak akses, atau akses ke repositori sensitif.
f. Laporan pengguna atau staf operasi — fungsi aplikasi terganggu, performa server turun, atau muncul pesan error tak biasa.
g. Cross-correlation intelijen ancaman — IOC yang cocok dengan laporan/alert eksternal (mis. advisori vendor keamanan).
h. Forensik awal memberi bukti — imaging/analisis memory menunjukkan implant/backdoor aktif.

d. Langkah Antisipasi Perusahaan.

a. Audit pipeline & vendor: lakukan audit keamanan pada vendor/software supply-chain (CI/CD, signing keys, SBOM).
b. Terapkan Zero Trust & least privilege: batasi akses, segmentasi jaringan, dan mikro-segmen untuk sistem kritikal.
c. Gunakan MFA & PAM: semua akses administratif wajib MFA; kelola kredensial privileged dengan PAM.
d. Deploy SIEM + EDR/XDR: monitoring terpusat, deteksi perilaku, dan hunting rutin terhadap IOC.
e. Egress filtering & network monitoring: batasi koneksi outbound, whitelist domain yang diperlukan, inspeksi trafik.
f. Proteksi kunci signing: simpan kunci tanda tangan di HSM dan audit penggunaan kunci.
g. Minta SBOM & verifikasi update: tahu komponen perangkat lunak yang terpasang dan verifikasi integritas update sebelum deploy.
h. Patch management & hardening: jalankan patch rutin, harden konfigurasi server, dan minimalkan layanan tidak perlu.
i. Latihan IR & tabletop: siapkan rencana respons insiden supply-chain dan latih berkala.
j. Threat intelligence sharing: gabung ke feed/koalisi intelijen untuk update IOC dan konteks serangan.
k. Revoke & rotate credentials setelah kompromi: cepat ubah/ cabut kredensial/sertifikat yang berisiko.
l. Isolasi dan forensik saat terdeteksi: isolate host terpengaruh, ambil image forensik, lalu lakukan remediasi terstruktur.