TUGAS

PRAKTIKUM KEAMANAN KOMPUTER

DISUSUN OLEH:

NAJWA ALAWIYAH SIREGAR

22346040

Dosen pengampu: Melri Deswina, S.Pd., M.Pd.T

PRODI INFORMATIKA

DEPARTEMEN ELEKTRONIKA

FAKULTAS TEKNIK

UNIVERSITAS NEGERI PADANG

2024/2025

Studi Kasus: Serangan SolarWinds pada 2020

Latar Belakang:

SolarWinds adalah sebuah perusahaan penyedia perangkat lunak manajemen IT yang terkenal dengan produk manajemen jaringan dan sistemnya. Pada akhir 2020, ditemukan bahwa sistem SolarWinds telah disusupi oleh serangan siber yang sangat canggih, yang dikenal sebagai serangan SolarWinds atau Sunburst. Serangan ini mempengaruhi ribuan organisasi di seluruh dunia, termasuk lembaga pemerintah, perusahaan besar, dan penyedia layanan penting.

Masalah:

Serangan ini melibatkan penyusupan ke dalam sistem SolarWinds dan menyuntikkan kode berbahaya ke dalam pembaruan perangkat lunak yang diterbitkan perusahaan tersebut. Ketika pelanggan menginstal pembaruan, kode berbahaya tersebut dieksekusi, memberikan akses tak terbatas kepada penyerang ke sistem yang terpengaruh.

Kendala yang Dihadapi:

1. **Ketersembunyian Serangan:** Kode berbahaya yang disuntikkan ke dalam pembaruan perangkat lunak sangat canggih dan dirancang untuk menghindari deteksi. Ini memungkinkan penyerang untuk melakukan pemantauan dan pengumpulan data secara diam-diam selama berbulan-bulan sebelum terdeteksi.
2. **Skala Serangan:** Karena serangan ini menargetkan perangkat lunak yang digunakan secara luas, dampaknya sangat besar. Banyak organisasi, termasuk lembaga pemerintah dan perusahaan besar, terpengaruh, menjadikan penanganan dan mitigasi serangan sangat kompleks dan memakan waktu.
3. **Keterbatasan dalam Sistem Deteksi:** Sistem deteksi intrusi dan pemantauan yang ada tidak cukup untuk mendeteksi aktivitas yang sangat canggih dan disamarkan oleh penyerang. Banyak sistem yang tidak memiliki kapabilitas untuk mendeteksi perilaku yang tidak biasa dalam konteks pembaruan perangkat lunak.

Solusi yang Diterapkan:

1. **Penanganan dan Respons Insiden:**
    - **Investigasi Mendalam:** Penyelidik dan tim keamanan siber melakukan analisis forensik mendalam untuk memahami bagaimana serangan ini terjadi, bagaimana kode berbahaya menyebar, dan dampaknya pada sistem yang terpengaruh.
    - **Pembersihan dan Pemulihan:** Organisasi yang terpengaruh segera mengidentifikasi dan menghapus kode berbahaya dari sistem mereka, memperbarui perangkat lunak yang terinfeksi, dan memperkuat keamanan sistem mereka.
2. **Peningkatan Sistem Keamanan:**
    - **Peningkatan Sistem Deteksi:** Organisasi yang terpengaruh memperbarui dan meningkatkan sistem deteksi mereka untuk menangani teknik serangan yang lebih canggih. Ini termasuk peningkatan perangkat lunak deteksi intrusi dan pemantauan yang lebih ketat.

    - **Pemeriksaan Kode dan Pembaruan Keamanan:** Implementasi kebijakan untuk memeriksa dan memvalidasi kode perangkat lunak yang diterima, serta memperketat kontrol terhadap pembaruan perangkat lunak.
3. **Kolaborasi dan Pembagian Informasi:**
    - **Kerjasama Internasional:** Berbagai lembaga pemerintah dan perusahaan bekerja sama secara internasional untuk berbagi informasi tentang teknik serangan, indikator kompromi (IoCs), dan strategi mitigasi.
    - **Peningkatan Kerja Sama Industri:** Organisasi di sektor teknologi dan keamanan siber membentuk aliansi untuk berbagi informasi tentang ancaman dan mengembangkan solusi bersama untuk meningkatkan keamanan.
4. **Peningkatan Protokol dan Kebijakan:**
    - **Audit dan Evaluasi Keamanan:** Peninjauan dan audit keamanan secara menyeluruh dilakukan untuk mengevaluasi dan meningkatkan kebijakan serta prosedur keamanan yang ada.
    - **Penegakan Kebijakan Keamanan yang Lebih Ketat:** Organisasi memperkenalkan kebijakan keamanan yang lebih ketat, termasuk pengelolaan akses yang lebih baik dan pemantauan yang lebih intensif terhadap pembaruan perangkat lunak dan sistem.

Hasil dan Kesimpulan:

Serangan SolarWinds menunjukkan betapa pentingnya keamanan perangkat lunak dan kompleksitas tantangan yang dihadapi oleh organisasi di era digital. Meskipun serangan ini menimbulkan dampak signifikan, respons yang cepat dan terkoordinasi, peningkatan sistem deteksi, serta kolaborasi antara sektor publik dan swasta membantu mengurangi dampak dan mencegah serangan serupa di masa depan. Studi kasus ini menekankan pentingnya keamanan yang proaktif, kesiapsiagaan, dan kerjasama global dalam melawan ancaman siber yang semakin canggih.