ABSTRAK

Analisis Sistematis Insiden Kerentanan Adobe ColdFusion dengan Mitigasi Risiko dan Metodologi MITRE ATTACK.

Oleh:

Mulkan Azhiman

6705210049

Penelitian terkait insiden Adobe ColdFusion exploit lead to system compromise yang terjadi pada perusahaan pelanggan. Insiden ini menyebabkan kerugian finansial dan reputasi bagi perusahaan. Penelitian ini akan menganalisis akar permasalahan, dampak insiden, dan langkah-langkah mitigasi dan pencegahan yang dapat dilakukan.

Penelitian ini bertujuan untuk menganalisis insiden tersebut secara sistematis dengan menggunakan kerangka kerja MITRE ATT&CK dan merumuskan strategi mitigasi risiko untuk mencegah insiden serupa.

Penelitian ini menggunakan metode studi kasus dengan analisis log dan dokumentasi terkait insiden. Kerangka kerja MITRE ATT&CK digunakan untuk mengidentifikasi taktik, teknik, dan prosedur (TTP) yang digunakan dalam insiden. Hasil penelitian menunjukkan bahwa insiden tersebut dieksploitasi dengan menggunakan taktik dan teknik MITRE ATT&CK.

Hasil penelitian menunjukkan secara umum bahwa insiden tersebut disebabkan oleh beberapa faktor, antara lain:

1. Kerentanan pada perangkat lunak Adobe ColdFusion yang digunakan oleh perusahaan.
2. Kurangnya kontrol keamanan dan monitoring pada sistem yang menggunakan Adobe ColdFusion.
3. Kesalahan konfigurasi dan manajemen patch yang tidak memadai.

Penelitian ini merekomendasikan beberapa Langkah mitigasi dan pencegahan untuk mencegah insiden serupa, antara lain:

1. Memperbarui perangkat lunak Adobe ColdFusion ke versi terbaru yang aman.
2. Menerapkan kontrol keamanan dan monitoring yang memadai pada sistem yang menggunakan Adobe ColdFusion.
3. Meningkatkan kesadaran dan pelatihan karyawan tentang keamanan siber.
4. Membuat dan menerapkan kebijakan manajemen patch yang efektif.

Penelitian ini diharapkan dapat memberikan pemahaman tentang insiden Adobe ColdFusion exploit lead to system compromise dan membantu perusahaan dalam meningkatkan keamanan siber.

Kata kunci: *Adobe ColdFusion, exploit, system compromise*, mitigasi, pencegahan, keamanan siber.