Laporan Penilaian Kerentanan

1 January 20XX

Deskripsi Sistem

Server Perusahaan ini memiliki beberapa perangkat keras yang terdiri dari prosesor CPU yang kuat, serta memory berkapasitas kan 128GB. Untuk menjalankan sistemnya, server ini menggunakan sistem operasi Linux dengan versi terbaru dan mempunyai pengaturan berbasiskan data berupa MySQL. Perancangan server ini diatur dengan koneksi jaringan yang stabil dengan digunakannya IPV4 sehingga dapat berinteraksi dengan server-server lain di jaringan. Untuk menerapkan keamanan data, server ini menggunakan koneksi terenkripsi SSL/TLS.

Cakupan

Kontrol aman saat ini memiliki hubungan dengan scope penilaian kerentanan di kasus ini. Penilaian akan memuat kejadian dalam periode 3 bulan, yakni dari bulan Juni 20XX sampai Agustus 20XX. Dalam proses penilaian kerentanan ini, saya menggunakan NIST SP 800-30 Rev. 1 sebagai panduan analisis risiko informasi sistem.

Tujuan

Server basis data merupakan sebuah sistem komputer yang berfungsi secara terpusat untuk menyimpan dan mengelola data dalam skala besar. Sistem ini dimanfaatkan untuk menyimpan berbagai informasi seperti data pelanggan, aktivitas kampanye, serta hasil analisis yang dapat digunakan dalam evaluasi kinerja dan pengembangan strategi pemasaran yang lebih personal. Oleh karena itu, aspek keamanan pada sistem ini menjadi sangat krusial mengingat perannya yang vital dalam mendukung operasional kegiatan pemasaran.

Penilaian Risiko

Sumber Ancaman	Jenis Ancaman	Kemungkinan	Tingkat Kerusakan	Risiko
Karyawan	*Mengganggu bagian operasi yang penting*	*4*	*5*	*5*

Kompetitor	*Memanipulasi data, seperti mengubah atau menghapus data penting sehingga operasi bisnis menjadi terganggu terganggu*	*6*	*9*	*8*
Peratas	*Mencuri data dan mengeksploitasi sistem atau server*	*3*	*4*	*9*

Pendekatan

Penilaian terhadap kasus ini dilakukan melalui pendekatan sistematis yang dimulai dengan identifikasi aset utama perusahaan, yaitu server basis data yang memiliki akses publik dan menyimpan informasi pelanggan yang bernilai tinggi. Tahap selanjutnya melibatkan analisis terhadap potensi ancaman, seperti kompetitor dan peretas, yang berpeluang mengeksploitasi kelemahan sistem untuk mencuri atau merusak data. Berdasarkan hasil analisis, dilakukan penilaian risiko dengan mempertimbangkan tingkat kemungkinan dan dampak yang menunjukkan bahwa situasi tersebut tergolong sangat kritis. Sebagai respons terhadap temuan tersebut, dirancang strategi mitigasi berupa penutupan akses publik, penerapan autentikasi yang kuat, serta penggunaan enkripsi data guna mencegah kebocoran di masa mendatang. Pendekatan ini ditutup dengan rekomendasi untuk melakukan pemantauan secara berkelanjutan agar keamanan sistem tetap terjaga secara konsisten.

Strategi Remediasi

Implementasi mekanisme autentikasi, otorisasi, dan audit untuk memastikan hanya pengguna yang berwenang yang dapat mengakses server basis data. Hal ini mencakup penggunaan kata sandi yang kuat, kontrol akses berbasis peran, dan autentikasi multifaktor untuk membatasi hak istimewa pengguna. Enkripsi data bergerak menggunakan TLS, bukan SSL. Daftar IP yang diizinkan untuk kantor perusahaan guna mencegah pengguna acak dari internet terhubung ke basis data.