Risk Profile

Risk profile adalah gambaran menyeluruh tentang resiko keamanan informasi yang akan dihadai / terjadi pada suatu sistem atau organisasi.

Identifikasi resiko

Mengidentifikasi potensi resiko pada suatu ancaman keamanan.

Analisis resiko

Menganalisis seberapa besar tingkat probabilitas dan dampak dari resiko ancaman keamanan.

Penilaian resiko

Melakukan penilaian dengan cara mengukur resiko secara keseluruhan berdasarkan hasil analisis resiko.

Prioritisasikan resiko

Menetukan urgensi dan prioritas dalam mengatasi setiap resiko.

Incident Response

Respon insiden adalah serangkaian prosedur dan Tindakan yang dilakukan untuk mengatasi dan mengelola dampak dari insiden keamanan informasi pada suatu sistem atau organisasi.

Tujuan

Memastikan insiden terjadi atau tidak

Mengumpulkan informasi secara akurat

Mengambil dan menangani bukti kejadian

5 proses mendefinisikan pendekatan keamanan

Preparation

Preparation adalah melakukan persiapan pada tahap awal agar organisasi dapat menanggapi insiden secara efektif.

Aktivitas

Mengembangkan rencana respon insiden yang mencakup tugas dan tanggung jawab personel tim, prosedur, dan alur kerja.

Membuat dan menguji rencana pemulihan keamanan sistem dan backup data.

Melakukan pelatihan kepada personel yang akan terlibat dalam respon insiden

Detection and analysis

Melakukan deteksi dan analisis kepada insiden secepat mungkin

Aktifitas

Menggunakan alat keamanan dan teknologi untuk mendeteksi aktifitas aktivitas mencurigakan

Mengumpulkan dan menganalisis informasi supaya dapat memahami sumber, metode, dan dampak dari insiden.

Containment eradication and recovery

Menghentikan penyebaran insiden, menghilangkan ancaman, mengembalikan sistem ke kondisi normal.

Aktivitas

Mengisolasi area area yang terkena insiden

Menghilangkan ancaman dan menbersihkan sistem dari sisa jejak insiden

Mengembalikan sistem ke kondisi normal

Melakukan pemulihan keamanan sistem dan data yang sudah di backup

Post incident activity

Melakukan evaluasi respon insiden dan mengambil Tindakan untuk mencegah terjadinya serangan serupa di masa depan.

Aktifitas

Mengevaluasi efiktivitas Langkah-langkah yang diambil selama respon insiden

Membuat laporan uji yang mencakup temuan, Tindakan yang diambil, dan rekomendasi.

Mengembangkan rencana respon insiden, prosedur, dan alur kerja berdasarkan pembelajaran dari insiden

Melakukan pelatihan tambahan kepada personil berdasarkan pengalaman pasca insiden.

Cybersecurity framework

Adalah sebuah pedoman atau model yang digunakan oleh perusahaan untuk merencanakan, mengimplementasikan, dan meningkatkan suatu sistem keamanan siber mereka

Menggunakan NIST. NIST dirancang untuk melindungi Arsitektur amerika dari serangan siber. NIST digunakan oleh perusahaan atau organisasi di sana untuk mengembangkan, merespon, dan memulihkan dari serangan siber.

Fungsi NIST

Identify

Memahami dan mengidentifikasi asset, resiko, dan kebijakan keamanan yang diperlukan

Protect

Mengimplementasikan Tindakan perlindungan untuk mencegah atau mengurangi dampat dari serangan keamanan

Detect

Mengembangkan dan menerapkan mekanisme deteksi untuk mendeteksi serangan keamanan secepat mungkin

Respond

Menetapkan prosedur tanggapan yang cepat dan efektif untuk mengatasi serangan keamanan yang sedang terjadi

Recovery

Mengembalikan sistem ke kondisi normal dengan melakukan pemulihan sistem keamanan dan restore data setelah terjadinya insiden penyerangan.

Iso 27701

Adalah standar internasional yang digunakan untuk sistem manajemen keamanan informasi. Standar ini menyediakan panduan dalam merencanakan, mengimplementasi, dan meningkatkan sistem manajemen keamanan informasi pada suatu organisai.

Iso 27002

Adalah suatu panduan atau kode praktik keamanan informasi. Standar ini menyediakan rekomendasi tentang Langkah-langkah yang dapat diambil untuk mengimplementasikan control keamanan infromasi pada suatu organisasi

Indeks keamanan informasi (KAMI)

Indek KAMI adalah sebuat alat bantu untuk melakukan asesmen dan evaluasi tingkat kematangan sistem dalam penerapan keamanan informasi berdasarkan kriteria dari iso 27001

Penilaian indeks KAMI

Tata Kelola

Pengelolaan resiko

Pengelolaan asset

Teknologi keamanan dan informais

Kerangka kerja

Sumplemen

Cyber maturity level

Adalah tingkat kesiapan dan kualitas sistem