Risk Profile

Risk profile adalah sebuah gambaran menyeluruh tentang resiko keamanan informasi yang mungkin dihadapi oleh suatu organisasi atau sistem. Hal ini mencakup identifikasi, analisis, dan penilaian risiko-risiko tersebut.

Elemen utama:

- Identifikasi Risiko
  Proses mengidentifikasi potensi ancaman atau kejadian yang dapat mengakibatkan kerugian atau dampak negatif.
- Analisis Risiko
  Menilai tingkat dampak dan probabilitas terjadinya setiap risiko yang diidentifikasi.
- Penilaian Risiko
  Mengukur risiko secara keseluruhan berdasarkan hasil analisis.
- Prioritisasi Risiko
  Menentukan urgensi dan pentingnya mengatasi setiap risiko.

Incident Response

Incident response adalah serangkaian prosedur dan tindakan yang dilakukan untuk mengatasi dan mengelola dampak dari insiden keamanan informasi atau pelanggaran keamanan.

Tujuan dilakukan:

- Memastikan insiden terjadi atau tidak
- Mengumpulkan informasi yang akurat
- Mengambil dan menangani bukti kejadian
- Pertahankan aktivitas dalam kerangka hukum yaitu privasi
- Meminimalkan gangguan terhadap operasional bisnis dan jaringan
- Membuat laporan dan rekomendasi yang akurat

Incident response lifecycle:

1. Preparation (Persiapan):
   Tujuannya untuk mempersiapkan organisasi untuk menanggapi insiden dengan efektif.
   Aktivitas:
   - Mengembangkan rencana respons insiden yang mencakup tugas dan tanggung jawab anggota tim, prosedur, dan alur kerja.

- Melakukan pelatihan reguler untuk personel yang terlibat dalam respons insiden.
- Membuat dan menguji rencana pemulihan keamanan dan cadangan data.
- Menilai dan meningkatkan kemampuan deteksi dan sistem keamanan.

2. Detection and Analysis (Deteksi dan Analisis):
   Tujuannya untuk mendeteksi dan menganalisis insiden secepat mungkin.
   Aktivitas:
   - Menggunakan alat keamanan dan teknologi untuk mendeteksi aktivitas mencurigakan.
   - Mengumpulkan dan menganalisis informasi untuk memahami sumber, metode, dan dampak insiden.
3. Containment Eradication and Recovery (Pembatasan, Eliminasi, dan Pemulihan):
   Tujuannya untuk menghentikan penyebaran insiden, menghilangkan ancaman, dan mengembalikan sistem ke keadaan normal.
   Aktivitas:
   - Mengambil langkah-langkah untuk mengisolasi area yang terkena insiden.
   - Menghilangkan ancaman dan membersihkan sistem dari jejak insiden.
   - Mengembalikan sistem atau layanan ke kondisi normal.
   - Melakukan pemulihan data dari cadangan yang valid dan teruji.
4. Post Incident Activity (Aktivitas Pasca Insiden):
   Tujuannya untuk mengevaluasi respons insiden dan mengambil tindakan untuk mencegah insiden serupa di masa mendatang.
   Aktivitas:
   - Mengevaluasi efektivitas langkah-langkah yang diambil selama respons insiden.
   - Membuat laporan insiden yang mencakup temuan, tindakan yang diambil, dan rekomendasi.
   - Meningkatkan rencana respons insiden dan prosedur berdasarkan pembelajaran dari insiden.
   - Melakukan pelatihan dan latihan tambahan berdasarkan pengalaman pasca-insiden.

Cybersecurity Framework

Cybersecurity framework adalah suatu panduan atau model yang digunakan untuk membantu organisasi dalam merancang, mengimplementasikan, dan meningkatkan program keamanan siber mereka.

Proses mendefinisikan pendekatan keamanan:

1. Identify (Identifikasi): Memahami dan mengidentifikasi aset, risiko, dan kebijakan keamanan yang diperlukan.
2. Protect (Perlindungan): Mengimplementasikan tindakan perlindungan untuk mencegah atau mengurangi dampak dari serangan keamanan.
3. Detect (Deteksi): Mengembangkan dan menerapkan mekanisme deteksi untuk mendeteksi serangan keamanan secepat mungkin.
4. Respond (Tanggapan): Menetapkan prosedur tanggapan yang cepat dan efektif untuk mengatasi serangan siber yang terdeteksi.

5. Recover (Pemulihan): Menyusun rencana pemulihan untuk memulihkan operasi normal setelah terjadinya insiden keamanan.

Contoh cybersecurity framework: NIST, ISO 27001 & 27002, CIS, COBIT, GDPR, HIPAA

NIST - National Institute of Standards and Technology

NIST dirancang untuk melindungi infrastruktur penting Amerika dari serangan siber. NIST digunakan sebagai alat bagi perusahaan sektor swasta untuk mendeteksi, merespons, dan memulihkan dari ancaman cyber.

Fungsi NIST: identify, protect, detect, respon, recover

ISO 27001 dan 27002

ISO 27001 adalah standar internasional untuk Sistem Manajemen Keamanan Informasi (ISMS). Standar ini memberikan panduan untuk mendirikan, mengimplementasikan serta memperbaiki sistem manajemen keamanan informasi dalam suatu organisasi.

ISO 27002 adalah panduan atau kode praktik keamanan informasi. Standar ini menyediakan rekomendasi dan langkah-langkah spesifik yang dapat diambil untuk mengimplementasikan kontrol keamanan informasi dalam suatu organisasi.

Indeks Keamanan Informasi (KAMI)

Indeks KAMI digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kematangan dalam penerapan keamanan informasi berdasarkan kriteria ISO 27001.

Penilaian Indeks Kami:

- Tata Kelola
- Pengelolaan resiko
- Pengelolaan asset
- Kerangka kerja
- Teknologi keamanan dan informasi
- Suplemen

Cyber Maturity

Cyber Maturity adalah tingkat kesiapan dan kualitas sistem keamanan siber suatu organisasi. Ini mencerminkan sejauh mana organisasi telah mengembangkan dan mengimplementasikan kebijakan, prosedur, dan teknologi keamanan yang efektif.

Semakin tinggi tingkat kematangan keamanan siber, semakin baik organisasi dapat melindungi aset informasi dan mengatasi ancaman keamanan siber.

Cyber Maturity Model adalah sebuah framework sistematis yang membantu evaluasi dan peningkatan postur keamanan siber suatu organisasi.

Ini tidak hanya mengidentifikasi status protokol keamanan yang ada tetapi juga memberikan peta jalan untuk perbaikan, menggabungkan aspek-aspek seperti layanan manajemen data dan pemantauan kontrol berkelanjutan.

Contoh Cyber Maturity Model: ISACA, CMMC, ISO/IEC 21827, OWASP, RIMS

Cyber Maturity Level

1. Tingkat 1 Initial
   - Organisasi pada tahap awal pengembangan keamanan siber.
   - Mungkin tidak memiliki kebijakan keamanan formal.
   - Reaksi terhadap insiden keamanan bersifat acak dan tidak terorganisir.
2. Tingkat 2 Developed
   - Organisasi mulai menerapkan kebijakan keamanan yang lebih terstruktur.
   - Respon terhadap insiden menjadi lebih konsisten.
   - Ada kesadaran akan kebutuhan keamanan, tetapi implementasinya belum sepenuhnya mapan.
3. Tingkat 3 Defined
   - Organisasi memiliki kebijakan keamanan yang terdefinisi dengan baik.
   - Proses keamanan sudah terdokumentasi dan diintegrasikan ke dalam operasional sehari-hari.
   - Tim keamanan dilibatkan secara aktif dalam pengembangan dan penerapan kebijakan.
4. Tingkat 4 Managed
   - Organisasi menerapkan pemantauan dan manajemen risiko secara terus-menerus.
   - Keamanan diintegrasikan ke dalam siklus hidup pengembangan dan operasional.
   - Ada upaya untuk meningkatkan keamanan melalui evaluasi dan perbaikan berkelanjutan.
5. Tingkat 5 Optimized
   - Organisasi berada pada tingkat paling tinggi dari kematangan keamanan siber.
   - Proses keamanan dioptimalkan untuk efisiensi maksimal.
   - Pemantauan ancaman dan respons terhadap insiden sangat canggih dan dapat menyesuaikan diri dengan perubahan ancaman.