Nama : Habiburrohman

Nim : 2108096076

1. IoT menerapkan konsep security by design untuk mengimplementasikan keamanan pada sebuah jaringan atau sistem yang digunakan. Jelaskan apa yang dimaksud dengan security by design !

2. Implementasi keamanan pada IoT harus dapat melindungi beberapa faktor. Jelaskan apa saja yang harus dilindungi pada sebuah sistem IoT !

3. Jelaskan dengan Analisa anda, seperti apa model security by design IoT yang diterapkan di Gedung FST UIN Walisongo! Bagaimana dampak/aplikasi dari security by design yang dirasakan bagi mahasiswa

jawaban

1. Security by design adalah pendekatan dalam pengembangan sistem atau produk yang menempatkan keamanan sebagai prioritas utama sepanjang seluruh siklus pengembangan. Konsep ini bertujuan untuk mengintegrasikan keamanan secara alami ke dalam desain dan arsitektur sebuah sistem, bukan hanya sebagai tambahan setelah produk jadi. Dengan menerapkan security by design, aspek keamanan dipertimbangkan dari tahap perencanaan awal hingga implementasi dan pemeliharaan, sehingga meminimalkan risiko keamanan yang mungkin terjadi.

Beberapa prinsip utama dari security by design termasuk:

* 1. Pemikiran Proaktif: Memikirkan keamanan sejak awal proses pengembangan, bukan sebagai reaksi terhadap ancaman yang sudah ada.
  2. Integrasi Otomatis: Mengintegrasikan kontrol keamanan secara otomatis ke dalam sistem, sehingga menjadi bagian integral dari fungsionalitas sistem.
  3. Prinsip Keterbukaan: Membuat desain dan implementasi keamanan dapat diverifikasi dan diperiksa secara independen.
  4. Pemisahan Kewenangan: Memisahkan akses dan hak pengguna sesuai dengan prinsip kebutuhan yang paling sedikit (least privilege) untuk mengurangi risiko penyalahgunaan.
  5. Kesinambungan dan Pembaruan: Memperbarui sistem secara teratur untuk mengatasi kerentanan baru dan memastikan keamanan sistem tetap relevan terhadap ancaman yang berkembang.
  6. Keselarasan dengan Regulasi: Mengikuti dan mematuhi peraturan dan standar keamanan yang relevan dalam industri atau yurisdiksi yang bersangkutan.

Dengan menerapkan prinsip-prinsip ini secara aktif dalam pengembangan sistem IoT, perusahaan atau pengembang dapat memastikan bahwa produk mereka tidak hanya berfungsi dengan baik, tetapi juga dapat diandalkan dan aman dari berbagai ancaman keamanan yang mungkin terjadi.

1. Implementasi keamanan pada sistem IoT harus dirancang untuk melindungi beberapa faktor kunci agar sistem dapat beroperasi dengan aman dan terhindar dari potensi ancaman. Berikut adalah beberapa faktor yang harus dilindungi dalam sebuah sistem IoT:
   1. Data Pengguna: Informasi pribadi dan sensitif dari pengguna harus dilindungi dari akses yang tidak sah atau pencurian data. Ini termasuk data identitas, informasi finansial, lokasi, dan lainnya yang dikumpulkan dan diproses oleh perangkat IoT.
   2. Integritas Data: Data yang dikirim dan diterima oleh perangkat IoT harus diamankan agar tidak dimanipulasi atau diubah secara tidak sah oleh pihak yang tidak berwenang. Hal ini penting terutama untuk menjaga keandalan dan keakuratan informasi yang diterima oleh sistem.
   3. Ketersediaan Layanan: Sistem IoT harus dilindungi dari serangan yang bertujuan untuk mengganggu atau meniadakan layanan yang disediakan oleh perangkat tersebut. Serangan seperti Denial-of-Service (DoS) dapat menyebabkan gangguan dalam operasi sistem dan mengganggu kinerja perangkat.
   4. Kerahasiaan Komunikasi: Komunikasi antara perangkat IoT dan infrastruktur jaringan harus diamankan untuk mencegah pengintipan atau pemantauan yang tidak sah. Teknik enkripsi dan otentikasi harus diterapkan untuk memastikan hanya pihak yang sah yang memiliki akses ke data komunikasi.
   5. Keamanan Fisik: Perangkat keras dan infrastruktur fisik dari sistem IoT juga perlu dilindungi dari akses fisik yang tidak sah. Ini termasuk perlindungan terhadap pencurian, manipulasi, atau kerusakan perangkat oleh pihak yang tidak berwenang.
   6. Keamanan Perangkat Lunak: Perangkat lunak yang digunakan dalam sistem IoT harus diamankan dari serangan seperti malware, exploit, atau serangan berbasis kode. Ini termasuk penerapan praktik pengkodean yang aman, pembaruan perangkat lunak teratur, dan penggunaan alat pengujian keamanan.
   7. Manajemen Akses: Kontrol akses yang ketat harus diterapkan untuk memastikan bahwa hanya pengguna yang diotorisasi yang memiliki hak akses ke fungsi dan data sistem IoT. Ini melibatkan penggunaan autentikasi yang kuat dan manajemen kredensial yang aman.
   8. Pemantauan dan Deteksi Intrusi: Sistem IoT harus dilengkapi dengan mekanisme pemantauan dan deteksi intrusi yang memungkinkan untuk mendeteksi aktivitas yang mencurigakan atau serangan yang sedang berlangsung, sehingga tindakan pencegahan atau respons dapat diambil dengan cepat.
2. Sebagai contoh, yang kembangkan model Security by Design untuk IoT di Gedung FST UIN Walisongo dan dampaknya bagi mahasiswa:
   1. Segmentasi Jaringan: Jaringan IoT di gedung FST UIN Walisongo dibagi menjadi beberapa segmen terpisah. Misalnya, satu segmen untuk sistem keamanan, satu untuk pencahayaan, satu untuk sistem HVAC (Heating, Ventilation, dan Air Conditioning), dan seterusnya. Setiap segmen memiliki izin akses yang sesuai dan firewall yang terkonfigurasi dengan baik untuk mengontrol aliran data.
   2. Otentikasi Kuat: Setiap perangkat IoT memerlukan otentikasi yang kuat sebelum diizinkan untuk terhubung ke jaringan. Ini bisa melibatkan penggunaan sertifikat digital atau metode otentikasi dua faktor untuk memastikan hanya perangkat yang sah yang dapat terhubung.
   3. Enkripsi Data: Seluruh komunikasi antara perangkat IoT dan servernya dienkripsi menggunakan protokol yang aman seperti SSL/TLS. Hal ini memastikan bahwa data yang dikirim dan diterima tidak dapat disadap atau dimanipulasi oleh pihak yang tidak berwenang.
   4. Pembaruan Perangkat Lunak Teratur: Setiap perangkat IoT dilengkapi dengan mekanisme pembaruan perangkat lunak otomatis yang teratur. Ini memastikan bahwa perangkat selalu diperbarui dengan patch keamanan terbaru untuk mengatasi kerentanan baru yang mungkin ditemukan.
   5. Monitoring dan Deteksi Intrusi: Sistem monitoring aktif dipasang untuk memantau aktivitas jaringan dan mendeteksi potensi serangan atau perilaku mencurigakan. Ini bisa meliputi deteksi pola lalu lintas yang tidak biasa atau upaya masuk yang mencurigakan.
   6. Pendidikan dan Kesadaran Pengguna: Mahasiswa dan staf diajarkan tentang pentingnya keamanan informasi dan praktik terbaik dalam menggunakan perangkat IoT. Mereka diberikan pelatihan tentang cara menggunakan perangkat dengan aman, menghindari tindakan yang dapat membahayakan keamanan jaringan, dan mengidentifikasi tanda-tanda potensi ancaman keamanan.

Dampak/Aplikasi bagi Mahasiswa:

1. Keamanan yang Ditingkatkan: Dengan menerapkan model Security by Design, mahasiswa dapat merasa lebih aman dalam menggunakan perangkat IoT di gedung FST UIN Walisongo. Mereka memiliki keyakinan bahwa data pribadi dan informasi sensitif mereka dilindungi dengan baik dari akses yang tidak sah atau penyalahgunaan.
2. Kontinuitas Pembelajaran yang Tidak Terganggu: Dengan adanya pembaruan perangkat lunak teratur dan sistem monitoring yang efektif, risiko gangguan pada jaringan IoT dapat diminimalkan. Ini memastikan bahwa layanan penting seperti akses internet dan sistem pembelajaran online tetap berjalan lancar, tanpa terganggu oleh serangan atau masalah keamanan.
3. Kesadaran Keamanan yang Ditingkatkan: Melalui pelatihan dan edukasi tentang keamanan informasi, mahasiswa menjadi lebih sadar akan pentingnya praktik keamanan dalam penggunaan teknologi. Mereka dapat mengaplikasikan pengetahuan ini tidak hanya di lingkungan kampus, tetapi juga dalam kehidupan pribadi dan profesional mereka di masa depan.