**TUGAS SECURITY LIFE CYCLE**

**MATA KULIAH KEAMANAAN SISTEM DAN JARINGAN KOMPUTER**

****

**Oleh:**

|  |  |
| --- | --- |
| **MOCHAMMAD ZIDAN FEBRIAN** | **: 2131740004** |
| **SAHRUL** | **: 2131740034** |

**PROGRAM STUDI D3 – TEKNOLOGI INFORMASI**

**POLITEKNIK NEGERI MALANG**

**PSDKU KAB. LUMAJANG**

**2024**

1. Asses

Merupakan proses identifikasi dan penilaina risiko, termasuk identifikasi asset, ancaman potensial dan kerentanan. Tujuannya adalah untuk memahami lingkungan keamanan dan menentukan tingkat risiko yang dapat diterima oleh organisasi.

1. Awreness and Training

* Awareness and training dalam security life cycle merupakan komponen penting yang bertujuan untuk memperluas pemahaman dan kemampuan pengguna mengenai keamanan perangkat lunak. Dengan demikian, pengguna dapat memahami dan mengimplementasikan prinsip-prinsip keamanan dalam proses pengembangan perangkat lunak.
* Awreness and training dalam security life cycle memiliki manfaat sebagai berikut:

1. Memperluas pemahaman pengguna mengenai keamanaan perangkat lunak
2. Memperluas kemampuan pengguna dalam mengimplementasikan prinsip-prinsip keamanaan
3. Memperkuat komitmen pengguna terhadap keamanaan perangkat lunak
4. Memperbaiki kemampuan pengguna dalam mengidentifikasi dan mengatasi kerentanan keamanaan

* Contoh penerapan awreness and training dalam security life cycle yaitu pelatihan mengenai pengunaan alat keamanaan, seperti sistem kontrol kesehatan informasi (IAM), sistem pengendalian resiko keamanaan (SCRM), dan sistem pengendalian kesalahan keamanan (SCA)

1. Design

Design merupakan proses perencanaan dan desain kontrol keamanan yang sesuai untuk mengurangi risiko yang telah didentifikasi.

1. Policy and procedures

* Policy and procedures dalam security life cycle merupakan panduan dan aturan yang ditetapkan untuk memastikan implementasi keamanan yang konsisten dan efektif dalam pengembangan perangkat lunak
* Tujuan dari penerapan policy and procedures dalam security life cycle adalah untuk memastikan implementasi keamanan yang konsisten dan efektif dalam pengembangan perangkat lunak
* Manfaat policy and procedures dalam security life cycle adalah untuk meningkatkan kualitas perangkat lunak, mengurangi risiko keamanan, memprioritaskan aktivitas keamanan, mengarahkan strategi perlindungan pada aset dan sistem yang paling kritis, serta mempromosikan perlindungan privasi bagi individu

1. Implement

Implement merupakan strategi kontrol keamanan yang telah dirancang dan disetujui pada tahap sebelumnya

1. Device management implementation

* Device Management Implementation dalam security life cycle melibatkan proses yang mencakup semua tahap dari pembelian, penggunaan, pemeliharaan, dan penyelesaian perangkat elektronik (DE) dalam organisasi
* Tujuan dari implementasi ini adalah untuk memastikan bahwa perangkat elektronik di dalam organisasi secara efektif dan efisien, serta mempertahankan keamanan, memenuhi peraturan dan peraturan, serta meminimalkan biaya
* Manfaat device Management Implementation dalam security life cycle yaitu membantu mencegah potensi celah keamanan dengan menginstal dan memelihara keamanan siber yang konsisten. Hal ini dapat mencakup penerapan pembaruan keamanan dan patch, serta penerapan kata sandi yang kuat dan tindakan keamanan lainnya

1. Monitoring (vendor)

* Monitoring vendor dalam security life cycle adalah proses pemantauan dan evaluasi terhadap vendor yang digunakan oleh organisasi untuk memastikan bahwa vendor tersebut memenuhi standar keamanan yang ditetapkan oleh organisasi. Tujuan dari monitoring vendor adalah untuk memastikan bahwa vendor yang digunakan oleh organisasi memenuhi persyaratan keamanan yang ditetapkan, serta meminimalkan risiko keamanan yang mungkin terjadi akibat kerentanan vendor
* Manfaat monitoring (vendor) yaitu membantu memastikan bahwa vendor yang digunakan oleh organisasi memenuhi standar keamanan yang ditetapkan oleh organisasi. Hal ini dapat membantu mencegah potensi celah keamanan yang dapat dimanfaatkan oleh penyerang

1. Maintain

Maintain merupakan pemeliharaan dan pemantauan terhadap sistem keamanaan informasi yang telah diimplementasikan

1. Incident

incident adalah istilah yang digunakan dalam keamanan IT untuk merujuk pada suatu peristiwa yang tidak terduga atau tidak diinginkan yang terjadi dalam sistem atau jaringan.. Incident bisa berupa serangan cyber, kesalahan konfigurasi, kegagalan perangkat keras, atau masalah lain yang mempengaruhi keamanan

1. Incident response investigation

Incident Response Investigation adalah proses yang dilakukan oleh tim keamanan IT setelah terjadi insiden keamanan, seperti serangan cyber, pencurian data, atau pelanggaran lainnya. Tujuan dari investigasi ini adalah untuk memahami apa yang terjadi, bagaimana insiden tersebut terjadi, dan bagaimana cara mencegah insiden serupa di masa depan.

1. Cybercrime and Forensics

Cybercrime and Forensics adalah dua konsep yang terkait erat dalam keamanan informasi dan teknologi. Cybercrime merujuk pada kejahatan yang terjadi dalam lingkungan digital, sedangkan Forensics merujuk pada proses pengumpulan, analisis, dan interpretasi bukti digital untuk keperluan hukum atau investigasi keamanan. Contoh dari Cybercrime and Forensics dalam security life cycle dapat berupa investigasi terhadap serangan ransomware yang menyandera data perusahaan. Tim forensik cyber akan mengumpulkan bukti dari sistem yang terinfeksi untuk mengidentifikasi sumber dan metode serangan, serta membantu dalam proses pemulihan data yang terpengaruh.

1. Electronic Discovery Expert Witness

Electronic Discovery Expert Witness adalah seorang ahli yang memberikan kesaksian dalam persidangan atau proses hukum terkait dengan penemuan elektronik kasus hukum. Ahli saksi ini memiliki pengetahuan dan keterampilan khusus dalam bidang teknologi informasi, hukum, dan forensik digital. Contoh seorang ahli forensik digital yang dipekerjakan oleh pengacara dalam sebuah kasus hukum yang melibatkan pencurian data dari perusahaan. Ahli ini bertanggung jawab untuk mengidentifikasi jejak digital dari peretas, menganalisis bagaimana data dicuri, dan memberikan bukti elektronik yang kuat dalam persidangan. Kesaksian ahli ini membantu pengadilan memahami teknisnya pencurian data elektronik dan dampaknya pada perusahaan.

1. Reactive service

Reactive Service adalah jenis layanan yang merespons terhadap permintaan atau kejadian yang terjadi setelah mereka terjadi, tidak secara proaktif mencegahnya. Ini berbeda dengan layanan proaktif yang berusaha untuk mencegah masalah sebelum mereka terjadi. Contohnya adalah layanan pemulihan data yang dapat mengembalikan data yang hilang setelah terjadi kegagalan perangkat keras atau perangkat lunak. Layanan ini merespons kejadian yang tidak diinginkan daripada secara aktif mencegahnya

1. Litigation Support Servives

Litigation Support Services (LSS) merupakan kumpulan layanan dan sumber daya yang komprehensif yang disediakan kepada para profesional hukum untuk membantu dalam manajemen dan presentasi bukti elektronik selama berbagai tahap proses litigasi. Layanan ini mencakup pengumpulan, peninjauan, analisis, dan produksi data elektronik, serta penyediaan saksi ahli dan manajemen basis data litigasi yang kompleks. Dengan mengintegrasikan LSS ke dalam siklus keamanan, organisasi dapat mengelola risiko keamanan dan privasi yang terkait dengan bukti elektronik, sehingga menjaga kepentingan hukum mereka dan memastikan kepatuhan dengan hukum dan regulasi yang relevan.