**PROPOSAL**

**MEMITIGASI ANCAMAN APLIKASI SISTEM INFORMASI KERUGIAN NEGARA / DAERAH DI PT. XYZ**



**CASE STUDY**

*Fadhli Azis*

*1701498805*

**Program Pascasarjana Ilmu Komputer**

**PROGRAM STUDI TEKNIK INFORMATIKA JENJANG S2**

**UNIVERSITAS BINA NUSANTARA**

**JAKARTA**

**2015**

**PROPOSAL**

**MEMITIGASI ANCAMAN APLIKASI SISTEM INFORMASI KERUGIAN NEGARA / DAERAH DI PT. XYZ**



**CASE STUDY**

*Fadhli Azis*

*1701498805*

Pembimbing :

**Benfano Soewito, M.Sc., Ph.D**

14 – 12 – 2015

# DAFTAR ISI

Halaman

Halaman Judul i

Persetujuan Pembimbing ii

[DAFTAR ISI iii](#_Toc441740934)

[DAFTAR GAMBAR v](#_Toc441740935)

[DAFTAR TABEL vi](#_Toc441740936)

[BAB I. PENDAHULUAN 1](#_Toc441740937)

[1.1. Latar Belakang 1](#_Toc441740938)

[1.2. Perumusan Masalah 4](#_Toc441740939)

[1.3. Tujuan Penelitian 4](#_Toc441740940)

[1.4. Manfaat Penelitian 4](#_Toc441740941)

[1.5. Ruang Lingkup 5](#_Toc441740942)

[BAB II. LANDASAN TEORI 6](#_Toc441740943)

[2.1. *Security Development Lifecycle* 6](#_Toc441740944)

[2.1.1. Optimasi *Security Deployment Lifecycle* 6](#_Toc441740945)

[2.2. *Threat Modeling* 12](#_Toc441740946)

[2.2.1. Konsep Dasar *Threat Model* 13](#_Toc441740947)

[2.2.2. Perbandingan Metodologi *Threat Modeling* 14](#_Toc441740948)

[2.2.3. Proses *Threat Modeling* 16](#_Toc441740949)

[2.3. Manfaat *Threat Modeling* 31](#_Toc441740950)

[BAB III. METODOLOGI 33](#_Toc441740951)

[3.1. Profil Perusahaan 33](#_Toc441740952)

[3.2. Kerangka Berpikir 44](#_Toc441740953)

[3.2. Langkah-Langkah Penelitian 46](#_Toc441740954)

[3.3. Metode Pengumpulan Data 48](#_Toc441740955)

[3.4. Metode Analisis Hasil Penelitian 49](#_Toc441740956)

[3.5. Jadwal Penelitian 50](#_Toc441740957)

[DAFTAR PUSTAKA 42](#_Toc441740958)

[LAMPIRAN 45](#_Toc441740959)

# DAFTAR GAMBAR

[Gambar 1.1 Persentase proses bisnis yang telah memanfaatkan teknologi informasi dan komunikasi PT. XYZ 2](#_Toc442015747)

[Gambar 2.1 Microsoft *Security Deployment Lifecycle – Simplified* 7](#_Toc442015748)

# DAFTAR TABEL

[Tabel II‑1 Perbandingan Metodologi *Threat Modeling* 16](#_Toc441584556)

[Tabel II‑2 Hubungan *Business and Security Objective* 17](#_Toc441584557)

[Tabel II‑3 Hubungan antara ancaman *STRIDE*, *Typical Victims*, dan *Property* *Security Objective* 22](#_Toc441584558)

[Tabel II‑4 *STRIDE* diterapkan ke *Data Flow Diagram* 23](#_Toc441584559)

[Tabel II‑5 Tabel prioritas ancaman 29](#_Toc441584560)

[Tabel II‑6 Mitigasi Ancaman *STRIDE* 31](#_Toc441584561)

[Tabel III‑1 Jadwal penelitian 41](#_Toc441584562)

# PENDAHULUAN

## Latar Belakang

Meningkatnya penggunaan teknologi informasi di suatu perusahaan sebagai faktor kesuksesan bisnis perusahaan bukan menjadi hal baru lagi pada saat ini. Pengadopsian dan penggunaan teknologi informasi dapat membawa manfaat bagi perusahaan dalam hal efisiensi, efektifitas, pertumbuhan dan keunggulan kompetitif dimana dalam hal ini membuat penggunaan teknologi informasi telah menjadi sebuah suatu yang diutamakan oleh perusahaan saat ini dan terus-menerus ditingkatkan dari hari ke hari dengan melalui inovasi-inovasi yang membuat penggunaan teknologi informasi menjadi semakin efektif dan efisien bagi perusahaan dalam melaksanakan proses bisnisnya (Consoli, 2012).

Di dalam penggunaan teknologi informasi perlu diperhatikan mengenai tingkat keamanan teknologi informasinya dalam menjaga data dan informasi yang diolah oleh aplikasi dan tersimpan di database agar tidak bocor. Keamanan telah menjadi fitur yang paling penting di aplikasi dimana dengan meningkatnya kompleksitas aplikasi, pelanggaran keamanan aplikasi dapat menyebabkan kerugian besar bagi organisasi. Meskipun aplikasi yang aman dirancang dengan *unbreakable core security services, such as authentication, access control, cryptosystem, or digital signature*, namun layanan keamanan tersebut akan rusak sewaktu - waktu (Shin, Dorbala, & Jang, 2013).

PT. XYZ adalah sebuah lembaga negara Indonesia yang berfungsi untuk melakukan pemeriksaaan keuangan dari lembaga-lembaga negara dan badan usaha milik negara dari Republik Indonesia. PT. XYZ telah mengimplementasikan teknologi informasi untuk mendukung proses bisnisnya. Dimana teknologi informasi tersebut berbentuk sebuah aplikasi yang terhubung dengan sebuah server terpusat yang menyimpan data-data dari hasil proses bisnis yang dilakukan oleh karyawan dari setiap daerah. Hal ini dapat membantu manajemen dari PT. XYZ untuk mendapatkan laporan yang *up-to-date* dan cepat sehingga dapat membantu untuk membuat keputusan.

Berdasarkan laporan akuntabilitas PT. XYZ pada tahun 2013 yang bisa dilihat pada Gambar 1.1 , bahwa persentase proses bisnis yang telah memanfaatkan teknologi informasi dan komunikasi adalah sebagai berikut:



Gambar 1.1 Persentase proses bisnis yang telah memanfaatkan teknologi informasi dan komunikasi PT. XYZ

Dengan realisasi pemanfaatan teknologi informasi sebagai proses pendukung proses bisnis pada PT. XYZ sebesar 94.12% tentunya sebagian besar proses bisnis pada PT. XYZ sudah sangat tergantung dengan teknologi informasi yang ada. Pemanfaatan teknologi informasi pada PT. XYZ tidak terlepas dari permasalahan yang muncul dimana permasalahan yang pernah dialami oleh PT. XYZ seperti potensi *user error* karena terdapat peraturan adanya mutasi karyawan setiap 4 tahun sekali ke divisi yang berbeda (diluar TI) yang menyebabkan pengetahuan karyawan akan penggunaan aplikasi sangat minim, *record* dari hasil proses audit tidak akurat ataupun salah, dan kesalahan dalam penyampaian hasil laporan. Selain itu, permasalahan terbatasnya sumber daya manusia dari bagian Biro TI sehingga proses sosialisasi terkait penggunaan aplikasi menjadi kurang maksimal. Ditambah lagi kurangnya pengetahuan mengenai *security awareness* yang menyebabkan informasi-informasi yang tersimpan pada database berpeluang untuk diakses oleh orang lain dan diubah-ubah karena adanya kegiatan *sharing password* dan *folder sharing*.

Saat ini di PT. XYZ sedang fokus-fokusnya melakukan *improvement* pada teknologi informasinya dalam rangka mengatasi permasalahan yang pernah terjadi. Salah satu permasalahan di PT. XYZ kurangnya keamanan dan pengembangan perangkat lunak yang kurang aman sehingga potensi ancaman terhadap keamanan teknologi informasi yang dapat timbul juga semakin tinggi dan bermuara menjadi resiko hingga menjadi suatu masalah. Ancaman keamanan adalah suatu usaha dan kegiatan, baik dari dalam maupun dari luar yang dinilai membahayakan aset-aset TI. Aset-aset TI yang digunakan perusahaan perlu dilindungi keamanannya dari pihak luar dan pihak dalam untuk menimalisasi ancaman atau permasalahan yang mungkin terjadi, oleh karena itu, dalam melakukan pengelolaan keamanan teknologi informasi atau pengelolaan resiko yang sistematik dan komprehensif harus memuat 3 unsur penting dari keamanan informasi, yaitu: *confidentiality* (kerahasian), *integrity* (konsistensi), *availability* (ketersediaan) yang mana ketiga unsur tersebut menjadi tolak ukur perusahaan untuk melakukan perlindungan keamanan aset-aset TI yang ada (Supardono, 2009).

Dari pengelolaan ancaman teknologi informasi tersebut membantu perusahaan mengurangi dampak dari ancaman sehingga tidak menggangu aktifitas perusahaan. Oleh karena itu, perlu adanya sebuah tindakan pengelolaan ancaman yang baik agar dapat menimalisasi dampak resiko dari ancaman-ancaman yang berpotensi terjadi pada PT. XYZ dengan menggunakan pendekatan Microsoft *Security Development Lifecycle - Threat Model* yang bertujuan untuk dapat mengidentifikasi dan mengklasifikasikan ancaman berdasarkan komponen perangkat lunak, arus data dan kepercayaan yang berbeda batas serta memberikan mitigasi ancaman pada teknologi informasi PT. XYZ.

## Perumusan Masalah

Sesuai dengan latar belakang yang telah dijelaskan, maka pokok masalah yang akan dikaji dalam penelitian ini adalah sebagai berikut:

* Bagaimana mengidentifikasi ancaman TI yang berpotensi terjadi pada proses *Security Development Lifecycle* di PT XYZ?
* Bagaimana memitigasi ancaman TI yang berpotensi menimbulkan resiko pada aplikasi di PT XYZ?

## Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

* Merancang sistem manajemen ancaman TI di PT XYZ.
* Untuk menghasilkan suatu mitigasi ancaman berdasarkan hasil analisis proses Microsoft *SDL - Threat Model*.

## Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini antara lain:

* Dapat memberikan hasil perancangan manajemen ancaman TI pada PT XYZ.
* Mampu memberikan rekomendasi mitigasi ancaman bagi PT XYZ untuk mengoptimalisasi keamanan aplikasi secara dini dari ancaman TI dalam proses siklus pengembangan aplikasi.

## Ruang Lingkup

Ruang lingkup penelitian ini adalah sebagai berikut:

* Berfokus pada kegiatan *Threat Mod*eling pada tahap desain dalam perangkat lunak.
* Analisis dan merancang manajemen ancaman TI menggunakan Microsoft *SDL - Threat Model* pada aplikasi sistem informasi kerugian negara / daerah di PT XYZ.
* Analisis mitigasi ancaman TI yang berpotensi terjadi berdasarkan hasil proses Microsoft *SDL - Threat Model* pada aplikasi sistem informasi kerugian negara / daerah.

# LANDASAN TEORI

## *Security Development Lifecycle*

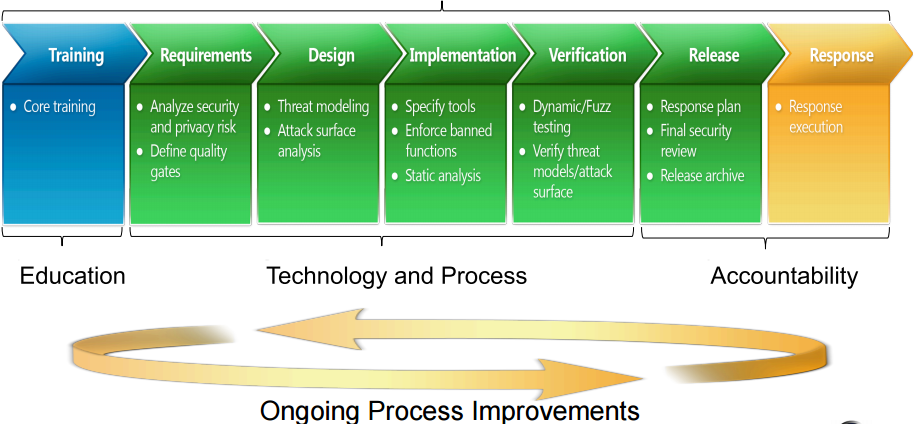
*Security Developmet Lifecycle* (SDL) adalah sebuah proses yang diadopsi oleh Microsoft dalam pengembangan perangkat lunak yang dibutuhkan untuk menahan dari serangan yang berbahaya. Proses tersebut meliputi penambahan serangkaian keamanan yang difokuskan pada kegiatan dan kiriman ke masing-masing tahapan dari proses pengembangan perangkat lunak. Sebelum perangkat lunak yang dikembangkan dengan mengikuti SDL dapat dirilis, harus menjalani peninjauan keamanan akhir oleh tim independen dari tim pengembangannya. Bila dibandingkan dengan perangkat lunak yang belum tunduk SDL, perangkat lunak yang telah mengalami SDL tingkat penemuan kerentanan keamanan berkurang sangat signifikan (Lipner & Howard, 2005).

Tujuan pengembangan dengan pendekatan SDL adalah untuk mengurangi biaya pemeliharaan dan meningkatkan kehandalan keamanan perangkat lunak terkait mengenai *bug* dan lainnya (Satapathy, 2014).

### 2.1.1. Optimasi *Security Deployment Lifecycle*

Menurut (Satapathy, 2014), Microsoft SDLC didasarkan pada konsep tiga inti: *education*, *continuous process improvement*, dan *accountability*. *Security Deployment Lifecycle* diwakili dalam urutan yang sama seperti fase tradisional *Software Development Life Cycle* (SDLC). Namun, serangkaian kegiatan tambahan dilakukan untuk menambahkan beberapa tingkat keamanan selama satu siklus proses pengembangan.

Optimasi SDL Model membagi menjadi lima fase kasar yaitu *Training, policy, and organizational capabilities; Requirements and design; Implementation; Verification; Release and response.*



Gambar 2.1 Microsoft *Security Deployment Lifecycle – Simplified*

Pada Gambar 2.1, terdapat beberapa kegiatan dalam melakukan pengembangan perangkat secara aman. Berikut penjelasan singkat terhadap 5 fase dalam mengoptimasi SDL (Satapathy, 2014):

1. *Training, Policy, and Organizational capabilities*

Semua sumber daya dari tim pengembangan harus mendapatkan informasi yang cukup dan terlatih sesuai dengan persyaratan khusus keamanan dari perangkat lunak, dasar-dasar keamanan, tren yang sedang berjalan mengenai keamanan. Pelatihan ini bisa dilanjutkan dengan cara dijadwalkan pada tahun setiap tahun dimana orang-orang teknik (*design persons, developers, testers, etc*) wajib untuk hadir.

Area Pelatihan meliputi:

* *Secure design*: Hal ini berkaitan dengan topik seperti pengurangan luas area serangan, pemahaman dasar pertahanan keamanan, hak akses secukupnya dan lainnya.
* *Threat modeling*: Hal ini mencakup topik seperti gambaran pemodelan ancaman, merancang pemodelan ancaman, hambatan pelaksanaan pemodelan ancaman.
* *Secure coding*: Hal ini mencakup pemahaman *buffer overflow* (di C, C++), kesalahan aritmatik, XSS (*Cross Site Scripting*), *SQL Injection*, kriptografi yang lemah.
* *Secure testing*: Hal ini mencakup pemahaman tentang perbedaan pengujian fungsional dan pengujian keamanan, penilaian risiko, metode pengujian keamanan dan lainnya.
* *Privacy*: Hal ini berkaitan dengan topik seperti privasi tipe data sensitif, praktek terbaik merancang privasi, praktek terbaik membangun kerahasian, praktek terbaik menguji kerahasian dan lainnya.
* *Miscellaneous*: Hal ini berkaitan dengan topik seperti kecakapan mendesain keamanan desain arsitektur, studi rinci dari kelemahan keamanan dan kerentanan, panduan mitigasi ancaman dan lainnya.

1. *Requirements and Design*
2. *Security requirement*

Untuk pengembangan sistem perangkat lunak yang aman, keamanan dan privasi perlu dipertimbangkan berdampingan. Jadi waktu yang paling penting untuk memasukkan kepercayaan kepada aplikasi adalah tahap desain. Persyaratan fungsional awal oleh pelanggan memungkinkan organisasi mengidentifikasi penting tonggak, batasan yang akan dituju, perizinan sepanjang bersama dengan privasi dan aspek keamanan sistem.

* *Quality gates/bug bars*

Penggunaan gerbang kualitas dan bug bar untuk pembentukan minimum tingkat keamanan yang dapat diterima dan memperpanjang privasi.

* *Security and Privacy risk assessment*

SRA dan PRA adalah proses yang mengidentifikasi wajah fungsional aplikasi yang direview secara mendalam.

1. *Design requirement*

Tim pengembang harus memahami perbedaan antara fitur aman dan fitur keamanan. Fitur aman adalah fitur yang fungsinya adalah baik direkayasa sesuai dengan keamanan, termasuk validasi atau implementasi kriptograsi data. Sedangkan, fitur keamanan dapat didefenisikan sebagai suatu program dengan impelementasi keamanan seperti *Firewall, SSL, IPS (Internet Prevent Security), IDS (Internet Detection Security)*. Sebuah spesifikasi desain yang baik menggambarkan pelaksanaan yang aman, lengkap, dan akurat dari semua fitur dan fungsi.

* *Attack Surface Reduction*

Ini adalah memberikan ruang lingkup penyerang yang minimum dalam menyerang ke sistem dengan mengurangi area serangan dan kerentanan. Ini termasuk seperti pembatasan hak akses pengguna, implementasi pertahanan secara berlapis (n-tier) dan lain-lain untuk menyembunyikan tempat yang dapat dieksploitasi oleh penyerang.

* *Threat Modeling*

Suatu kegiatan yang memungkinkan pengembang untuk menganalisis, mendokumentasikan, dan memberikan mitigasi terhadap potensi ancaman di tingkat desain.

1. *Implementation*

Memiliki 3 kegiatan pada tahap implementasi SDL yaitu:

* *Use of approved and updated tools*

Tim pengembang harus menggunakan *tools* versi terbaru dan disetujui sesuai standar organisasi agar meminimalisir kelemahan keamanan dan kerentanan.

* *don’t use Unsafe Functions*

Fungsi yang ada, fungsi yang umum digunakan adalah selalu di bawah pemindaian dimata penyerang untuk beberapa kerentanan. Jadi fungsi umum harus dianalisis dengan baik dalam lingkungan ancaman saat ini oleh penasehat keamanan sebelum digunakan. Semua fungsi yang dilarang atau hitam yang terdaftar harus dihindari dari penggunaan oleh tim pengembang.

* *Static analysis*

*Source code* harus dibuat secara static, terurut dan rapi untuk membantu dalam proses tinjauan keamanan untuk menimalisir kerentanan.

1. *Verification*

* *Dynamic program analysis*

Ini adalah verifikasi sistem pada waktu berjalan. Hal ini diperlukan untuk mengkonfirmasi apakah program itu bekerja sesuai dengan tuntutan dokumen desain. Tugas ini meliputi verifikasi isu pengguna hak istimewa, korupsi memori, dan masalah keamanan penting lainnya.

* *Threat Model and Attack Surface Review*

Ulasan ini melacak setiap desain atau implementasi perubahan pada sistem selain spesifikasi desain dan setiap vektor serangan baru yang diperkenalkan karena perubahan. Serangan ini telah diantisipasi setelah verifikasi rinci.

1. *Release and Response*

* *Incident Response Plan*

Dalam keadaan terburuk, terjadinya potensi program mengalami kegagalan atau mengancam pada masa depan sehingga tim pengembang harus menyiapkan bantuan dan merespon agar program tersebut dapat bertahan dan melakukan perbaikan kedepannya.

* *Final Security Review*

Sebelum di rilis, ini adalah penilaian secara rinci dari semua tahapan kegiatan keamanan yang dilakukan di dalam sistem aplikasi oleh penasihat keamanan dengan bantuan personel tim pengembang teknis dan keamanan. FSR umumnya mencakup penilaian terhadap model ancaman, *tool output*, *input, and output validation*, permintaan khusus, masalah kinerja sistem. Sebuah FSR dianggap lulus jika masalah tetap dapat dikelola dengan baik, ataupun dapat ditanggulangi sebelum liris.

Selain 5 tahapan kegiatan keamanan diatas, masih ada beberapa kegiatan keamanan tambahan yang dapat ditambahkan seperti:

1. *Manual code review*

Dilakukan oleh seorang yang berpengalaman dan terampil yang terfokus di sekitar aset penting yang paling rentan terhadap kerentanan.

1. *Penetration testing*

Analisis keamanan yang dilakukan oleh seorang yang berpengalaman yang bertujuan untuk menemukan potensi kerentanan yang ada pada sistem karena kegagalan dalam *coding* yang aman dan lainnya.

1. *Vulnerability analysis of similar applicatin*

Melakukan kegiatan dengan mencari informasi perangkat lunak yang persis sama di Internet untuk dapat menggali bagaimana upaya terhadap menghadapi kerentanan atau serangan yang muncul.

## *Threat Modeling*

Didalam *Security Deployment Lifecycle* adalah salah satu kegiatan keamanan pada tahap desain yaitu *threat modeling*. *Threat modeling* melibatkan kompleksitas sistem dan mengidentifikasi semua ancaman yang mungkin untuk sistem, terlepas dari apakah atau tidak sistem itu dapat dieksploitasi. Selama pembuatan persyaratan keamanan, ancaman yang akan dianalisis berdasarkan *critical dan likelihood*, dan keputusan yang dibuat untuk mengurangi atau menerima risiko terkait yang ditimbulkan oleh ancaman (Myagmar, Lee, & Yurcik, 2005).

### Konsep Dasar *Threat Model*

Sebelum memulai memasuki *Threat Model*, penting diketahui dan dimengerti beberapa konsep dasarnya (Michael McGrath, 2013):

* Aset adalah sesuatu yang bernilai yang dibutuhkan musuh. Misal: data di dalam database
* Ancaman adalah suatu peristiwa yang mungkin atau mungkin tidak berbahaya yang dapat merusak atau menyusup ke aset dengan melakukan serangan.
* Kerentanan adalah sebuah cacat pada beberapa bagian sistem keamanan yang dapat membuat ancaman mungkin terjadi.
* Risiko adalah kemungkinan menjad target serangan, serangan itu menjadi sukses dan berdampak jika berhasil.
* Penanggulangan (*countermeasure)* adalah suatu tindakan atau alat yang membahas ancaman dan meringankan risiko.

Konsep berikutnya adalah untuk mengeksplorasi alternatif pendekatan pemodelan ancaman. Setidaknya ada tiga umum pendekatan untuk pemodelan ancaman (Jangam, 2009):

* *Attacker-centric*: pemodelan ancaman ini dimulai dengan penyerang, dan mengevaluasi tujuan mereka, dan bagaimana mereka bisa mencapainya. Motivasi penyerang sering dianggap dan diberikan penting daripada faktor lainnya. Pendekatan ini biasanya dimulai dari salah satu atau titik masuk aset.
* *Sofware-centric*: pemodelan ancaman juga disebut sebagai “sistem sentris” atau desain sentris” atau “arsitektur sentris”. Ini dimulai dari desain sistem, mencari jenis serangan terhadap setiap elemen model. Pendekatan ini digunakan dalam pemodelan ancaman dalam Microsoft *Security Deployment Lifecycle.*
* *Asset-centric*: pemodelan ancaman ini melibatkan semua aset yang dipercayakan didalam sistem.

### Perbandingan Metodologi *Threat Modeling*

Berdasarkan (MyAppSecurity Inc, 2012), beberapa perbandingan metodologi untuk *threat modeling* yaitu:

1. Microsoft SDL – *STRIDE*

Praktek pemodelan ancaman Microsoft berfokus untuk membantu memastikan perangkat lunak aman dimulai selama tahap desain. Agar sebuah aplikasi memenuhi sifat keamanan kerahasian, integritas, dan ketersedian. Microsoft menggunakan metodologi ”*STRIDE*”. STRIDE singkatan dari *spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privileges.* Microsoft memiliki 6 tahapan proses dalam merancang pemodelan ancaman

1. P.A.S.T.A (Process for Attack Simulation and Threat Analysis)

Ini adalah pemodelan ancaman baru yang diperkenalkan oleh Macro Morana and Tony “UV.”. P.A.S.T.A memiliki 7 tahapan proses dalam merancang pemodelan ancaman

1. TRIKE

Trike adalah metodologi yang digunakan untuk membangun model ancaman untuk membantu memenuhi proses audit keamanan dari perspektif manajemen risiko. Trike memiliki kesamaan dengan proses pemodelan ancaman dengan Microsoft, hal itu berbeda karena menggunakan pendekatan berbasis risiko dengan pelaksanaan yang berbeda, ancaman, dan model risiko. Metodologi Trike tampaknya berada dalam tahap percobaan dan dengan kurangnya dokumentasi yang signifikan dan dukungan, tampaknya sulit untuk diterapkan.

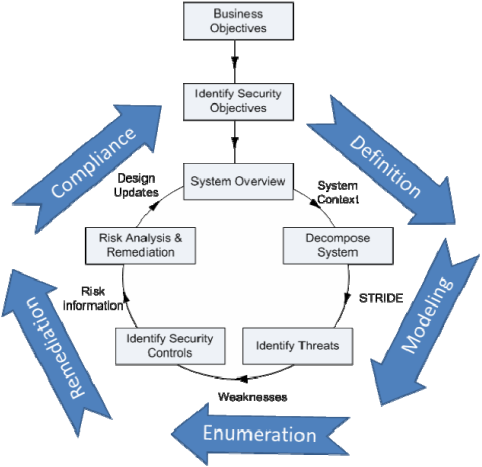
Di ringkas secara umum dan dapat dilihat pada Tabel 2.1 dibawah, perbandingan metodologi antara Microsoft, TRIKE, dan P.A.S.T.A.

|  |  |  |  |
| --- | --- | --- | --- |
| Tahapan *Threat Modeling* | **Microsoft SDL-STRIDE** (Microsoft Corporation, 2003) | **TRIKE** (Saitta, Larcom, & Eddington, 2005) | **P.A.S.T.A (Process for Attack Simulation & Threat Analysis)** (UcadaVelez, 2012) |
| *Identify assets* | *Requirements Model* | *Define The Business & Security Objectives* |
| *Create an architecture overview* | *Implementation Model* | *Define The Technical Scope* |
| *Decompose the application* | *Threat Model* | *Decompose the Application* |
| *Identify the threats* | *Risk Model* | *Threat Analysis* |
| *Document the threats* |  | *Weakness and Vulnerabilities Analysis* |
| *Rate the threats* |  | *Attacks/Exploits Enumeration & Modeling* |
|  |  | *Risk And Impact Analysis* |

Perbandingan Metodologi *Threat Modeling*

### Proses *Threat Modeling*

Menurut (Satapathy, 2014), dalam melakukan kegiatan *threat modeling* memiliki langkah-langkah yang dimulai dari tujuan bisnis (*Business Objective*), identifikasi tujuan keamanan (*Security Objective*), gambaran sistem, menguraikan sistem, mengidentifikasi ancaman, mengidentifikasi kontrol keamanan, analisis resiko dan perbaikan sistem. Berikut gambaran alur siklus dari proses *threat modeling*.



Langkah-langkah kegiatan *Threat Modeling*

1. ***Business Objectives***

Tahap ini mendefinisikan tujuan bisnis organisasi, jadwal selesai fase yang berbeda dari SDLC, analisis dan pengumpulan persyaratan untuk perangkat lunak.

1. ***Identify Security Objectives***

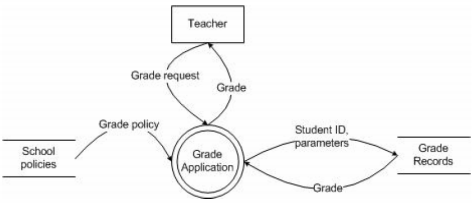
Dari tahap tujuan bisnis, tujuan keamanan dapat diidentifikasi. Pada tabel 2.2 diterangkan hubungan antara tujuan bisnis dan tujuan keamanan (Satapathy, 2014).

|  |  |  |  |
| --- | --- | --- | --- |
| *Business Objective* | *Security Objective* | *Property* | *Definition* |
| BO | SO1 | *Confidentiality* | Mencegah pengungkapan tidak sah. |
| SO2 | *Integrity* | Mencegah perubahan tidak sah. |
| SO3 | *Availability* | Selalu menampilkan sesuai kebutuhan. |
| SO4 | *Authentication* | Membangun identitas pengguna sebelum akses ke dalam sistem. |
| SO5 | *Authorization* | Memiliki rule yang berbeda-beda setiap pengguna. |
| SO6 | *Accountability* | Mempertahankan jejak audit untuk fungsi yang kritikal. |

Hubungan *Business and Security Objective*

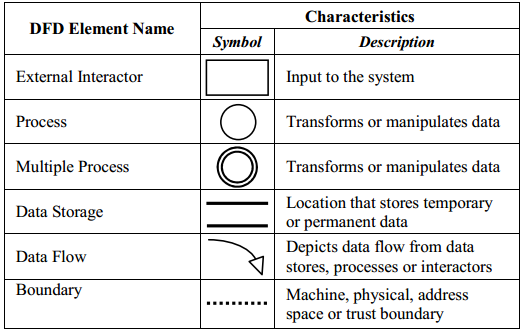
1. ***System Overview***

Pada tahap ini, fungsi sistem lengkap dari pandangan secara luas diambil dan di wakili secara garis besar. Persentasi dapat menggunakan salah satu diagram aliran data atau *Data Flow Diagram* (DFD) atau diagram aliran kontrol *Unified Modeling Language* (UML). Microsoft menggunakan DFD untuk pendekatan threat modeling. Tahap ini membutuhkan tingkat 0 DFD (dikenal juga sebagai Diagram Konteks) untuk digambarkan.



Contoh Diagram Konteks – *Threat Model*

Ini diperlukan untuk memisahkan sistem dari lingkungan eksternal dan mencari tahu entitas eksternal dan *database* eksternal untuk saling berinteraksi. Pada fase ini, aset potential diidentifikaisi. Setiap aset adalah obyek yang mana sebagai subjek *exploit* oleh penyerang.

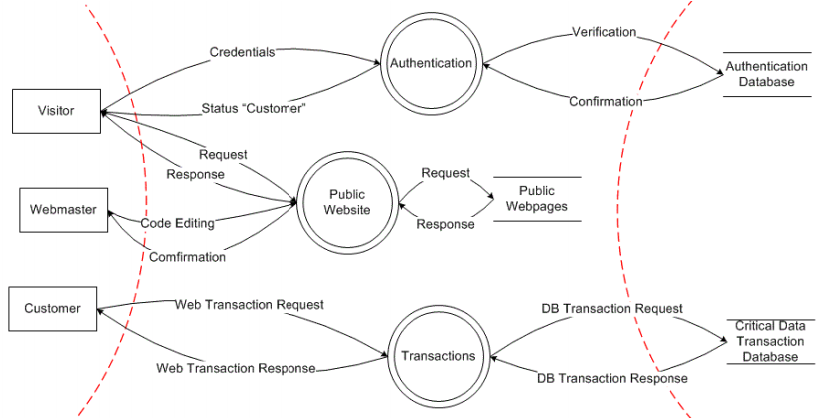


*Data Flow Diagram, Symbol, and Description* (Möckel & Abdallah, 2010)

Menggunakan Microsoft *Threat Modeling Tool* (TMT), pengguna dapat menggambarkan, mengidentifikasi proses dan arus data yang terdiri dari suatu layanan atau aplikasi.

1. ***Decompose System***

Gambaran sistem yang telah dibuat pada tahap sebelumnya, kini diuraikan menjadi komponen kecil untuk menghindari kompleksitas dalam pemodelan ancaman. Gambaran sistem yang telah diuraikan saling berhubungan satu sama lain melalui aliran data yang masuk atau keluar dari sistem. Pengenalan batas kepercayaan muncul pada tahap ini pada *user interface* pada batas sistem. Ini adalah awal mula permukaan serangan oleh penyerang dan karenanya tujuan dari tim pengembang adalah mencoba untuk meminimalkan permukaan serangan sebanyak mungkin. Ada keuntungan lain dari tahap penguraian sistem ini dan pengenalan simultan dari batas kepercayaan, yaitu data yang mengalir melalui (masuk dan keluar) batas kepercayaan akan diperiksa sedangkan arus data yang tidak melewati batas-batas tidak perlu khawatir.



*DFD of the decomposed example system* (Möckel & Abdallah, 2010)

1. ***Identify Threats***

Pada fase ini akan dikaitkan setiap elemen dari perangkat lunak dengan semua kemungkinan ancaman. Setiap elemen dari tahap *decompose system* diambil dan di periksa setiap kemungkinan ancaman. Dalam mengurangi penggunaan waktu dalam memeriksa setiap kemungkinan ancaman yang ada, Microsoft mengusulkan metodologi yang disebut Microsoft *STRIDE*. Kata *STRIDE* diambil dari inisial enam kelas ancaman yang berbeda *Spoofing, Tampering Repudiation, Information Disclosure, Denial of Service*

dan *Elevation of Privilege* (Satapathy, 2014)*.*

Ancaman *STRIDE* adalah kebalikan dari beberapa properti yang anda inginkan dijaga didalam sistem anda yaitu: *Confidentiality, Integrity, Availability, Authentication, Authorization,* dan *Accountability*. Pada tabel II-3 diringkas hubungan antara *Threat Property*, *Violated Threat, Definition, Typical Victims, Examples* (Shostack, 2014).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Threat*** | ***Property Violated*** | ***Threat Definition*** | ***Typical Victims*** | ***Examples*** |
| *Spoofing* | *Authentication* | Berpura-pura menjadi sesuatu atau orang lain selain dirinya sendiri | *Processes, external entities, people* | Barack Obama adalah seorang polisi |
| *Tampering* | *Integrity* | Memodifikasi sesuatu pada *disk*, *network*, *memory* | *Data stores, data flows, processes* | Memodifikasi, menambahkan, atau menghapus paket melalui jaringan |
| *Repudiation* | *Non-Repudiation* | Mengklaim bahwa anda tidak melakukan sesuatu, atau tidak bertanggung jawab. *Repudiation*  dapat jujur atau palsu, dan pertanyaan kunci untuk tim desain, bukti apa kamu punya? | *Process* | Aku tidak menggunakan aplikasi ini. |
| *Information Disclosure* | *Confidentiality* | Memberikan informasi kepada seseorang yang tidak berwenang melihatnya | *Processes, data stores, data flows* | Memungkinkan dapat mengakses dengan bebas ke file-file yang sensitif atau penting. |
| *Denial of Service* | *Availability* | Menyerap sumberdaya yang berpengaruh terhadap pemberian layanan | *Processes, data stores, data flows* | Sebuah program yang dapat tertipu sehingga harus menggunakan seluruh memori. |
| *Elevation of Privilege* | *Authorization* | Memungkinkan seseorang untuk melakukan sesuatu padahal mereka tidak berwenang melakukan hal tersebut | *Process* | Pengguna biasa dapat membuat pengguna baru padahal hanya admin yang dapat menjalankan perintah tersebut. |

Hubungan antara ancaman *STRIDE*, *Typical Victims*, dan *Property* *Security Objective*

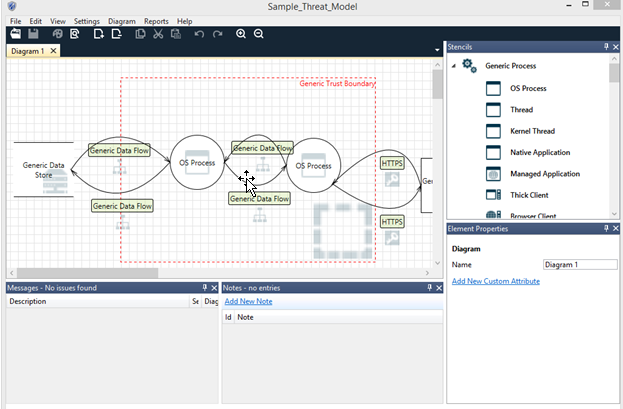
Model penggunaan *STRIDE* sebagian besar diterapkan pada diagram aliran data (DFD) dimana setiap ancaman dihubungkan dengan setiap elemen pada DFD. Metode ini sebenarnya meremas ruang lingkup tim desain untuk menguji semua serangan yang mungkin terhadap entitas tertentu, dan membuat desain lebih efisien dan akurat. Dapat dilihat pada tabel 2.4 hubungan antara STRIDE per elemen DFD.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Element type | Threat Types | | | | | |
| S | T | R | I | D | E |
| External Interactor | 🗴 |  | 🗴 |  |  |  |
| Process | 🗴 | 🗴 | 🗴 | 🗴 | 🗴 | 🗴 |
| Data Storage |  | 🗴 | 🗴 | 🗴 | 🗴 |  |
| Data Flow |  | 🗴 |  | 🗴 | 🗴 |  |

*STRIDE* diterapkan ke *Data Flow Diagram*

Dalam membuat DFD *threat model* dapat menggunakan alat bantu yaitu Microsoft *Threat Modeling Tool 2016* yang diterbitkan oleh Microsoft yang dirancang untuk membantu pengguna dalam membangun proses *threat model*. Dimana fungsinya sebagai berikut (Microsoft, 2016):

* Lingkungan gambar dapat mudah dibuat.
* Otomatis mencetak ancaman dengan pendekatan STRIDE per pendekatan interaksi.
* Dapat menentukan sendiri *template* untuk pemodelan ancaman.



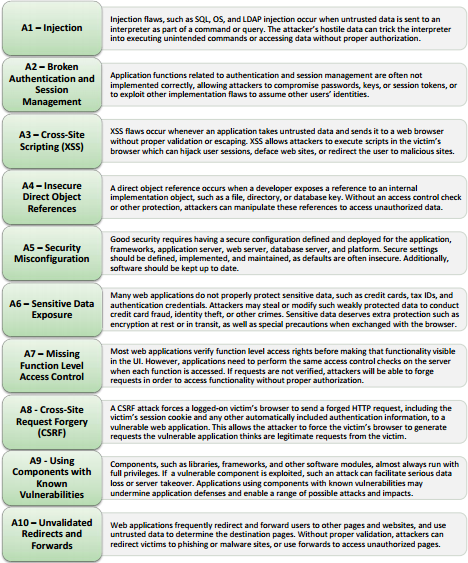
*DFD* – Microsoft *Threat Modeling Tools* 2016 (Microsoft, 2016)

Menggunakan Microsoft *Threat Modeling Tool* (TMT), pengguna dapat menggambarkan, mengidentifikasi proses dan arus data yang terdiri dari suatu layanan atau aplikasi.

1. ***Identify Security Controls***

Pada tahap ini berbagai komponen harus dievaluasi terhadap setiap ancaman. Hal ini diperiksa apakah aliran data melalui batas kepercayaan atau tidak. Jika iya, maka itu harus diambil tindakan pencegahan karena dapat dieksplotasi terhadap ancaman. Jika tidak, mitigasi ancaman pada entitas tingkat batas, hal itu akan otomatis dikurangi. Disini dilakukan kegiatan *baintsroming* untuk mengidentifikasi tipe kerentanan pada aset tertentu, pada titik tertentu, kondisi tertentu agar menghilangkan kerentanan. *Bainstroming* yang ada akan dievaluasi terhadap setiap ancaman atau dilakukan identifikasi kerentanan dapat dibantu dengan parameter berdasarkan *OWASP Top Ten*. *The Open Web Application Security Project (OWASP)* adalah organisasi yang tidak berbasis mencari keuntungan, dimana berfokus pada peningkatan keamanan perangkat lunak. (The OWASP Foundation , 2001)

*OWASP Top Ten* adalah dokumen kesadaran yang kuat untuk keamanan aplikasi web. *OWASP Top Ten* merupakan konsensus yang luas tentang apa kelemahan keamanan aplikasi web yang paling penting. Anggota proyek meliputi berbagai ahli keamanan dari seluruh dunia yang telah berbagi keahlian mereka untuk menghasilkan daftar ini.



*OWASP Top 10 Application Security Risk – 2013*

Dari *OWASP top ten application security risk, OWASP* juga memberikan informasi bagaimana melakukan pencegahan atau mitigasi terhadap serangan atau ancaman yang berpotensi terjadi.

1. ***Risk Analysis & Remediation***

***Risk analyss***

Setelah ancaman dan kerentanan telah diidentifikasi, tim pengembang pada tahap ini akan menganalisis, memprioritaskan dan membuat keputusan tentang rencana mitigasi. Untuk memprioritaskan risiko, dibutuhkan skor untuk setiap ancaman atau skor risiko ditugaskan untuk kombinasi kerentanan untuk mengetahui tingkat keparahan dan dukungan untuk pengambilan keputusan. Persamaan dasar untuk pengambilan keputusan (Satapathy, 2014).

***Risk = Probability of Occurance \* Business Impact***

Microsoft telah mengembangkan pendekatan untuk *risk* *rating* yaitu *DREAD*. *DREAD* kepanjangan dari *damage potential, reproducibility, exploitability, affected users, discoverability* (Jangam, 2009).

* *Damage potential* mendefinisikan jumlah potensi kerusakan jika serangan mungkin berhasil dijalankan.
* *Reproducibility* mendefinisikan kemudahan dimana serangan itu dapat dilaksanakan dan diulang.
* *Exploitability* mendefinisikan tingkat keterampilan dan sumber daya yang dibutuhkan untuk berhasil mengeksekusi serangan.
* *Affected users* mendefinisikan jumlah entitas pengguna yang sah terpengaruh jika serangan itu berhasil di eksekusi.
* *Discoverability* mendefinisikan seberapa cepat dan mudah terjadinya serangan dapat diidentifikasi.

Anda dapat menggunakan skala *High*, *Medium*, atau *Low* sederhana untuk memprioritaskan ancaman. Ancaman dinilai sebagai tinggi, itu menimbulkan risiko yang signifikan untuk aplikasi Anda dan perlu ditangani sesegera mungkin. Ancaman menengah perlu ditangani, tetapi dengan kurang mendesak. Anda dapat memutuskan untuk mengabaikan ancaman rendah tergantung pada berapa banyak usaha dan biaya yang diperlukan untuk mengatasi ancaman tersebut. Penilaian tidak harus menggunakan skala besar karena ini membuat sulit untuk menilai ancaman konsisten berdampingan satu sama lain. Anda dapat menggunakan skema sederhana seperti *High* (1), *Medium* (2), dan *Low* (3). Ketika Anda jelas mendefinisikan apa yang masing-masing mewakili nilai untuk sistem rating, hal ini membantu menghindari kebingungan. Tabel penilaian dapat digunakan oleh anggota tim untuk memprioritaskan ancaman (Microsoft Corporation, 2003).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *Rating* | *High (3)* | *Medium (2)* | *Low (3)* |
| D | *Damage potential* | Penyerang dapat menumbangkan sistem keamanan; mendapatkan otorisasi kepercayaan penuh; Jalankan sebagai administrator; meng-upload konten. | Membocorkan informasi sensitif. | Membocorkan informasi tidak sensitif. |
| R | *Reproducibility* | Serangan dapat direproduksi setiap waktu dan tidak memerlukan jeda waktu. | Serangan dapat direproduksi, tetapi hanya dengan jeda waktu dan situasi tertentu. | Serangan itu sangat sulit untuk mereproduksi, bahkan dengan pengetahuan tentang lubang keamanan. |
| E | *Exploitability* | Seorang programmer pemula bisa membuat serangan dalam waktu singkat. | Seorang programmer terampil bisa membuat serangan itu, kemudian ulangi langkah-langkah. | Serangan itu membutuhkan orang yang sangat terampil dan pengetahuan yang mendalam setiap kali untuk mengeksploitasi. |
| A | *Affected users* | Semua pengguna, konfigurasi default, pelanggan utama. | Beberapa pengguna, konfigurasi non-default persentase yang sangat kecil dari pengguna. | mempengaruhi pengguna anonim |
| D | *Discoverability* | Informasi yang dipublikasikan menjelaskan serangan itu. Kerentanan ditemukan dalam fitur yang paling umum digunakan dan sangat terlihat. | Kerentanan ini di bagian yang jarang digunakan produk, dan hanya beberapa pengguna harus menemukan itu. Ini akan mengambil beberapa pemikiran untuk melihat penggunaan sembarangan. | Bug tersebut tidak jelas, dan tidak mungkin bahwa pengguna akan bekerja untuk berpotensi menimbulkan kerusakan. |

Tabel penentuan tingkat prioritas ancaman

Risiko Penilaian dinilai sebagai tinggi / Medium / Low menurut skor:

* 5-8 = Risiko *Low*
* 9-12 = Risiko *Medium*
* 13-15 = Risiko *High*

Setelah risiko telah dihitung, tim desain dan pengembang melakukan remediasi dari ancaman dari yang prioritas yang lebih tinggi sampai dengan yang prioritas yang lebih rendah.

***Remediation***

Dalam melakukan pencegahan terhadap ancaman perlu diketahui strategi dan teknologinya. Berikut tabel mitigasi ancaman terhadap *STRIDE* (Michael McGrath, 2013):

|  |  |  |
| --- | --- | --- |
| ***Threat*** | ***Threat Type*** | ***DFD Elements*** |
| *Spoofing* | *Authentication* | *Authenticate principals (people or*  *components):*   * *Basic authentication* * *Digest authentication* * *Cookie authentication* * *Windows authentication (NTLM)* * *Kerberos authentication* * *PKI systems such as SSL/TLS and certificates* * *IPSec* * *Digitally signed packets*   *Authenticate code or data:*   * *Digital signatures* * *Message authentication codes* * *Hashes* |
| *Tampering* | *Integrity* | * *Access Control Lists (ACLs)* * *Digital signatures* * *Message authentication codes* |
| *Repudiation* | *Non-Repudiation* | * *Strong authentication* * *Secure auditing and logging* * *Digital signatures* * *Secure time-stamps* * *Trusted third parties* |
| *Information disclosure* | *Confidentiality* | * *Access Control Lists (ACLs)* * *Encryption* |
| *Denial of service* | *Availability* | * *Access Control Lists (ACLs)* * *Filtering* * *Quota* * *Authorization* |
| *Elevation of privilege* | *Authorization* | * *Access Control Lists (ACLs)* * *Group or role membership* * *Privilege ownership* * *Permissions* * *Privilege ownership* * *Permissions* |

Mitigasi Ancaman *STRIDE*

## Manfaat *Threat Modeling*

Penelitian tentang *threat modeling* telah menjadi populer baru-baru ini. Sebuah model ancaman pada dasarnya adalah representasi tersruktur semua informasi yang mempengaruhi aplikasi. Pada dasarnya, ini adalah pandangan dari aplikasi dan lingkungan melalui kacamata keamanan. Alasan pemodelan ancaman digunakan adalah menemukan secara dini bug keamanan, memahami kebutuhan keamanan aplikasi, dan memberikan produk atau aplikasi yang lebih baik dari sebelumnya dan menemukan permasalah-permasalahan yang sebelumnya tidak diketahui. (Shostack, 2014).

Beberapa penilitian yang telah dilakukan untuk melihat pengaruh dana manfaat *threat modeling* adalah sebagai berikut:

|  |  |  |  |
| --- | --- | --- | --- |
| Nama peneliti dan tahun | Judul | Metoda | Hasil |
| (Möckel & Abdallah, 2010) | *Threat Modeling Approaches And Tools For Securing*  *Architectural Designs Of An E-Banking Application* | * *Studi Literatur* * Menggunakan analisis desain arsitektur sistem aplikasi e-banking menggunakan DFD dan pemodelan ancaman *SDL- STRIDE* * Tidak melakukan perhitungan resiko | Ancaman yang timbul tidak dimitigasi dan menerima resiko yang dapat muncul mengingat untuk login ke aplikasi sudah dilengkapi dengan dual otentinkasi yaitu *username* & *password* dan token |
| (Myagmar, Lee, & Yurcik, 2005) | *Threat Modeling as a Basis for Security Requirements* | * *Study literatur* * Melakukan pemodelan ancaman dengan hanya tahapan pada *characterizing the system*, *identifying assets and access points*, and *identifying threats using STRIDE* pada *Software-Defined Radio, a network traffic monitoring tool (VisFlowConnect), and a cluster security monitoring tool (NVisionCC)* * Melakukan perhitungan risiko * Melakukan mitigasi | Melakukan evaluasi kembali terhadap *security requierement* pada *Software-Defined Radio, a network traffic monitoring tool (VisFlowConnect), and a cluster security monitoring tool (NVisionCC)* seperti menambahkan firewall untuk menghindari *denial of service* dan membatasi akses dari user yang tidak bertanggung jawab |
| (Hussain, Erwin, & Dunne, 2011) | *Threat modeling using Formal Methods: A New Approaach to Develop Secure Web Applications.* |  |  |
|  |  |  |  |
|  |  |  |  |

Hasil penelitian sebelumnya mengenai *Threat Modeling*

Dari penelitian yang disebutkan diatas, *threat modeling* dapat dilakukan diseluruh jenis perusahaan profit atau non-profit dan kepada jenis sistem apa saja. Yang membedakan penelitian ini dari penelitian sebelumnya adalah metode remediasi yang mengacu kepada *best practice* *OWASP* yang disesuaikan dengan kondisi perusahaan.

# METODOLOGI

## Profil Perusahaan

PT. XYZ adalah satu lembaga yang bebas dan mandiri dalam memeriksa pengelolaan dan tanggung jawab keuangan negara. PT XYZ bertugas untuk memeriksa pengelolaan dan tanggung jawab keuangan negara sebagaimana dimaksud dalam Undang-Undang Nomor 15 Tahun 2006 tentang PT. XYZ. Adapun visi dan misi dari PT. XYZ adalah sebagai berikut:

Visi : menjadi lembaga pemeriksa keuangan negara yang kredibel dengan menjunjung tinggi nilai-nilai dasar untuk berperan aktif dalam mendorong terwujudnya tata kelola keuangan negara yang akuntabel dan transparan.

Dari visi tersebut terbentuklah sebuah misi, yang mana misi dari PT. XYZ adalah :

* Memeriksa pengelolaan dan tanggung jawab keuangan negara,
* Memberikan pendapat untuk meningkatkan mutu pengelolaan dan tanggung jawab keuangan negara,
* Berperan aktif dalam menemukan dan mencegah segala bentuk penyalahgunaan dan penyelewengan keuangan negara.

Dengan visi dan misi yang telah disebutkan diatas, PT. XYZ menyusun sebuah strategi bisnis strategi bisnis yang mana strategi bisnis ini disusun untuk mencapai visi dan misi dari PT. XYZ agar dapat mencapai sesuai yang telah ditetapkan, dimana strategi bisnis dari PT. XYZ antara lain:

1. Mendorong terwujudnya pengelolaan keuangan negara yang tertib, taat pada peraturan perundang-undangan, ekonomis, efisien, efektif, transparan, dan bertanggung jawab dengan memperhatikan rasa keadilan dan kepatutan.
2. Mewujudkan pemeriksaan yang bermutu untuk menghasilkan laporan hasil pemeriksaan yang bermanfaat dan sesuai dengan kebutuhan pemangku kepentingan
3. Mewujudkan birokrasi yang modern di PT. XYZ.

Yang mana strategi bisnis dari PT. XYZ didukung oleh sekelompok nilai- nilai dasar yang harus dipatuhi oleh seluruh karyawan dari PT. XYZ yaitu:

1. Independensi

PT. XYZ menjunjung tinggi independensi, baik secara kelembagaan, organisasi, maupun individu. Dalam semua hal yang berkaitan dengan

pekerjaan pemeriksaan, kami bebas dalam sikap mental dan penampilan dari gangguan pribadi, ekstern, dan/atau organisasi yang dapat mempengaruhi independensi.

1. Integritas

PT. XYZ membangun nilai integritas dengan bersikap jujur, obyektif, dan tegas dalam menerapkan prinsip, nilai, dan keputusan.

1. Profesionalisme

PT. XYZ membangun nilai profesionalisme dengan menerapkan prinsip kehati-hatian, ketelitian, dan kecermatan, serta berpedoman kepada standar yang berlaku.

Dari strategi bisnis dan nilai – nilai dasar yang telah dibuat tersebut, PT. XYZ merumuskan sebuah sasaran strategi terkait dengan sistem informasi dan teknologi informasi yang ada pada PT. XYZ, yang mana strategi dari sistem informasi dan teknologi informasi pada PT. XYZ adalah sebagai berikut:

1. Terpenuhinya Kebutuhan Pemilik Kepentingan akan TIK (Teknologi Informasi dan Komunikasi).
2. Meningkatkan Pemanfaatan TIK.
3. Meningkatkan Mutu Pelayanan TI.
4. Meningkatkan Efektifitas Perencanaan dan Monitoring Pemanfaatan TIK.
5. Meningkatkan Mutu Pengelolaan Sumber Daya Manusia (SDM) TI.
6. Meningkatkan Efektifitas dan Efisiensi Pengembangan Sistem Aplikasi Komputer.
7. Meningkatkan Efektifitas dan Efisiensi Pembangunan dan Pengelolaan Infrastruktur TIK.
8. Meningkatkan Pemanfaatan Anggaran di Lingkungan Biro TI

Berikut struktur organisasi dan penjelasan singkat tugas dari PT. XYZ yang ditunjukan pada gambar 3.1



Struktur Organisasi PT. XYZ

PT. XYZ dipimpin oleh ketua, wakil ketua, dan 7 anggota dan staff ahli dimana memiliki divisi khusus untuk menjalankan visi dan misi PT. XYZ. Berikut penjelasan singkat tugas dari struktur organisasi PT. XYZ

* **Sekertariat Jendral**

Tugas : menyelenggarakan dan mengkoordinasikan dukungan administrasi serta sumberdaya untuk kelancaran tugas dan fungsi PT. XYZ serta pelaksana PT. XYZ.

Satuan kerja yang dibawahi : Biro Sekretariat Pimpinan, Biro Humas dan Kerja Sama Internasional, Biro Sumber Daya Manusia, Biro Keuangan, Biro Teknologi Informasi, Biro Umum, dan Pusat Pendidikan dan Pelatihan.

* **Inspektorat Utama**

Tugas : melakukan pengawasan terhadap pelaksanaan tugas dan fungsi seluruh unsur pelaksana PT. XYZ.

Satuan kerja yang dibawahi : Inspektorat Pemerolehan Keyakinan Mutu Pemeriksaan, Inspektorat Pemeriksaan Internal dan mutu Kelembagaan, dan Inspektorat Penegakan Integritas.

* **Direktorat Utama Pembinaan dan Pengembangan Hukum Pemeriksaan Keuangan Negara**

Tugas : memberikan konsultasi hukum, bantuan hukum dan pelayanan informasi hukum kepada anggota PT. XYZ dan/atau pelaksana PT. XYZ, Legislasi, penelitian dan pengembangan hukum serta tugas kepaniteraan dalam penyelesaian kerugian Negara/daerah.

Satuan kerja yang dibawahi : Direktorat LPBH dan Direktorat KHKKN/D.

* **Direktorat Utama Perencanaan, Evaluasi, Pengembangan, Pendidikan, dan Pelatihan Pemeriksaan Keuangan Negara**

Tugas : merumuskan perencanaan strategis dan manajemen kinerja, evaluasi dan pelaporan pemeriksaan, serta penelitian dan pengembangan.

Satuan kerja yang dibawahi : Direktorat PSMK, Direktorat Litbang, dan Direktorat EPP.

* **Auditorat Utama Keuangan Negara (AKN) I**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara pada bidang politik, hukum, pertahanan, dan keamanan.

Satuan kerja yang dibawahi : Auditorat I.A, I.B, I.C

* **Auditorat Utama Keuangan Negara (AKN) II**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara pada bidang perekonomian dan perencanaan pembangunan nasional.

Satuan kerja yang dibawahi : Auditorat II.A, II.B, II.C

* **Auditorat Utama Keuangan Negara (AKN) III**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara pada bidang lembaga negara, kesejahteraan rakyat, kesekretariatan negara, aparatur negara, dan riset dan teknologi.

Satuan kerja yang dibawahi : Auditorat III.A, III.B, III.C

* **Auditorat Utama Keuangan Negara (AKN) IV**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara pada bidang lingkungan hidup, pengelolaan sumber daya alam, dan infrastruktur.

Satuan kerja yang dibawahi : Auditorat IV.A, IV.B, IV.C

* **Auditorat Utama Keuangan Negara (AKN) V**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara pada Kementerian Dalam Negeri, Kementerian Agama, Badan Pengembangan Wilayah Surabaya-Madura, Badan Nasional Pengelola Perbatasan, Badan Pengusahaan Kawasan Perdagangan dan Pelabuhan Bebas Batam, Badan Pengusahaan Kawasan Perdagangan dan Pelabuhan Bebas Sabang, serta keuangan daerah dan kekayaan daerah yang dipisahkan pada pemerintah daerah di wilayah Sumatera dan Jawa.

Satuan kerja yang dibawahi : Auditorat V.A, V.B, dan 16 Kantor Perwakilan.

* **Auditorat Utama Keuangan Negara (AKN) VI**

Tugas : pemeriksaan pengelolaan dan tanggung jawab keuangan negara/daerah pada Kementerian Kesehatan, Badan Pengawasan Obat dan Makanan, Kementerian Pembangunan Daerah Tertinggal, dan Kementerian Pendidikan dan Kebudayaan, serta keuangan daerah dan kekayaan daerah yang dipisahkan pada Pemerintah Daerah di wilayah Bali, Nusa Tenggara, Kalimantan, Sulawesi, Maluku, dan Papua.

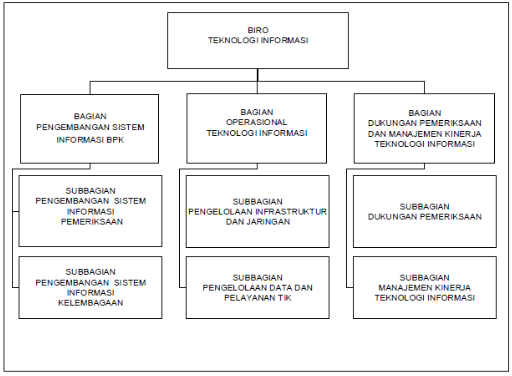
Satuan kerja yang dibawahi : Auditorat VI.A, VI.B, dan 18 Kantor Perwakilan.

* **Auditorat Utama Keuangan Negara (AKN) VII**

Tugas : memeriksa pengelolaan dan tanggung jawab keuangan negara pada bidang Kekayaan Negara yang Dipisahkan (Badan Usaha Milik Negara).

Satuan kerja yang dibawahi : Auditorat VI.A, VI.B, dan 18 Kantor Perwakil Auditorat VII.A, VII.B, VII.C, VII.D.

Biro Teknologi Informasi di PT.XYZ berada di bawah satuan kerja Sekertariat Jendral. Struktur organisasi Biro TI di PT. XYZ dapat dilihat pada gambar 3.2 berikut:



Struktur Organisasi dari Biro IT di PT. XYZ

Biro TI di PT. XYZ memiliki 3 bagian dan 6 sub bagian yang mana memiliki tugas sebagai berikut:

* **Biro TI**

Tugas : melaksanakan perencanaan, pengembangan, pelaksanaan, dan *monitoring* sistem dan teknologi informasi di lingkungan PT. XYZ.

Fungsi :

1. Perumusan dan pengevaluasian rencana aksi Biro TI dengan mengidentifikasi IKU berdasarkan RIR PT. XYZ,
2. Perumusan rencana kegiatan Biro TI berdasarkan rencana aksi serta tugas dan fungsi Biro TI,
3. Perumusan rencana dan kebijakan di bidang sistem dan teknologi informasi,
4. Pelaksanaan kebijakan sistem dan teknologi informasi di bidang perancangan, pengembangan, operasional serta dukungan sistem dan teknologi informasi,
5. Penyusunan Laporan Akuntabilitas Kinerja Biro TI, dan
6. Pelaporan hasil kegiatan secara berkala kepada Sekretaris Jenderal.

Satuan kerja yang dibawahi : Bagian Pengembangan Sistem Informasi PT. XYZ, Bagian Operasional Teknologi Informasi, dan Bagian Dukungan Pemeriksaan dan Manajemen Kinerja Teknologi Informasi.

* **Bagian Pengembangan Sistem Informasi PT. XYZ**

Tugas : melakukan pengembangan sistem informasi pemeriksaan dan kelembagaan di lingkungan PT. XYZ.

Fungsi :

1. Penyiapan bahan rencana dan kebijakan di bidang pengembangan aplikasi pemeriksaan dan kelembagaan,
2. Pelaksanaan rencana dan kebijakan di bidang pengembangan aplikasi pemeriksaan dan kelembagaan, dan
3. Penyiapan bahan penyusunan Laporan Akuntabilitas Kinerja Biro TI.

Satuan kerja yang dibawahi :

1. Subbagian Pengembangan Sistem Informasi Pemeriksaan mempunyai tugas melaksanakan desain dan pengembangan aplikasi, sosialiasi, distribusi, dan pemeliharaan aplikasi di bidang pemeriksaan.
2. Subbagian Pengembangan Sistem Informasi Kelembagaan mempunyai tugas melaksanakan desain dan pengembangan aplikasi, sosialiasi, distribusi, dan pemeliharaan aplikasi di bidang kelembagaan.

* **Bagian Operasional Teknologi Informasi**

Tugas : mengelola infrastruktur dan jaringan, pengelolaan data dan pelayanan teknologi informasi dan komunikasi (TIK) di lingkungan PT. XYZ.

Fungsi :

1. Penyiapan bahan rencana dan kebijakan di bidang pengelolaan aset teknologi informasi, pengelolaan data dan pelayanan TIK serta dukungan dan bantuan pengguna,
2. Pelaksanaan rencana dan kebijakan teknologi informasi di bidang pengelolaan aset teknologi informasi, pengelolaan data, dan pelayanan TIK,
3. Penyiapan bahan penyusunan Laporan Akuntabilitas Kinerja Biro TI.

Satuan kerja yang dibawahi :

1. Subbagian Pengelolaan Infrastruktur dan Jaringan mempunyai tugas mengelola infrastruktur teknologi informasi dan melaksanakan pemeliharaan aset teknologi informasi.
2. Subbagian Pengelolaan Data dan Pelayanan Teknologi Informasi dan Komunikasi mempunyai tugas mengelola data elektronik termasuk retensi, backup, recovery, pemusnahan, dan pengamanan data serta memberikan dukungan teknis dan bantuan untuk pengguna terkait TIK.

* **Bagian Dukungan Pemeriksaan dan Manajemen Kinerja Teknologi Informasi**

Tugas : melakukan penyiapan bahan kebijakan teknologi informasi, analisis, evaluasi, dan dukungan pemeriksaan berbasis teknologi informasi di lingkungan PT. XYZ.

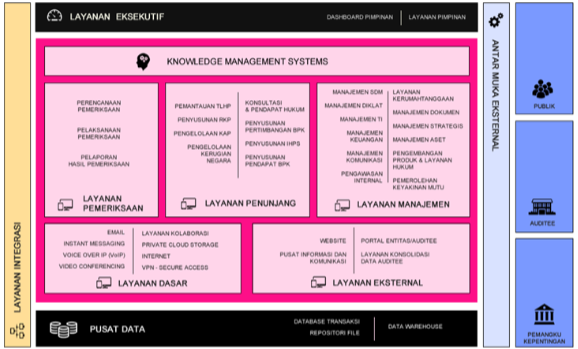
Fungsi :

1. Penyiapan bahan rencana dan kebijakan teknologi informasi di bidang dukungan pemeriksaan dan review teknologi informasi serta pemantauan kinerja sistem,
2. Pelaksanaan rencana dan kebijakan teknologi informasi di bidang dukungan pemeriksaan dan reviu teknologi informasi serta pemantauan kinerja sistem, dan
3. Penyiapan bahan penyusunan Laporan Akuntabilitas Kinerja Biro TI.

Satuan kerja yang dibawahi :

1. Subbagian Dukungan Pemeriksaan mempunyai tugas melaksanakan dukungan pemeriksaan dan reviu teknologi informasi, serta menyusun dan menyempurnakan perangkat lunak terkait audit dan reviu teknologi informasi.
2. Subbagian Manajemen Kinerja Teknologi Informasi mempunyai tugas melaksanakan penyiapan bahan perumusan Renstra dan rencana tahunan teknologi informasi, kajian teknologi informasi, pemantauan kinerja sistem, serta evaluasi dan pengembangan service level agreement.

Adapun berikut portfolio dari sistem aplikasi yang sudah ada di PT. XYZ:



Portofolio sistem aplikasi PT. XYZ

## Kerangka Berpikir

Penggunaan teknologi informasi sebagai pendukung proses bisnis merupakan sebuah inovasi yang baik yang dapat membantu PT. XYZ mempercepat aktivitasnya dan membantu dalam membuat keputusan – keputusan dari hasil proses bisnis yang dilakukan. Dimana penggunaan teknologi informasi tersebut tidak terlepas dari permasalah yang dapat menghambat keberlangsungan bisnis dimana permasalahan perusahaan tersebut harus dikelola sedemikian rupa agar tidak berdampak buruk bagi perusahaan dan menjaga keberlangsungan bisnis. Hal tersebut menjadi dasar pemilihan topik penelitian terkait dengan manajemen ancaman teknologi informasi.

Penelitian ini sendiri akan merancang sebuah pengelolaan ancaman dan memitigasi ancaman yang mana secara garis besar penelitian ini menggunakan lima tahap yaitu pengumpulan permasalahan, pengumpulan data, melakukan identifikasi ancaman dan resiko, merancang mitigasi ancaman dan memberikan rekomendasi kepada perusahaan. Dimana pada kerangka pikir dari penelitian ini secara rinci menggambarkan tahapan-tahapan penelitian tersebut dengan mengacu pada *best practices* yang dipadukan dengan teori – teori pendukung yang tertuang pada landasan teori yang ada.

Gambar 3.2 menunjukkan kerangka pikir dari penelitian ini. Secara lebih rinci, tahapan penilitian pengelolaan ancaman akan dibahas pada sub bab selanjutnya.



Kerangka berpikir

## Langkah-Langkah Penelitian

Langkah-langkah penelitian ini adalah mendefinisikan permasalahan, menentukan tujuan, manfaat dan ruang lingkup penelitian, *study literature*, pengumpulan data, analisis hasil penelitian dan mengambil kesimpulan dan saran. Pada tahap awal penelitian dimulai dengan menentukan latar belakang, manfaat dan tujuan penelitian serta mendefinisikan ruang lingkup.

Tahap kedua dari penelitian ini adalah *study literature* dilakukan untuk memperdalam pemahaman mengenai *threat model*, *risk assessment* dan melakukan pengumpulan data dengan observasi dan wawancara. T

Tahap ketiga, dilakukan rancangan pengelolaan ancaman dengan menggunakan *SDL - Threat Model* dengan melakukan langkah-langkah identifikasi tujuan bisnis dan dilanjuti *security* *objective*, mendefinisikan sistem secara garis besar baik dari fungsi, desain aplikasi dan lainnya, menguraikan sistem menjadi lebih rinci dengan membuat *DFD* dengan bantuan Microsoft *Threat Modeling Tool* 2016, melakukan identifikasi ancaman dengan pendekatan model *STRIDE*, mendefinisikan *security control* terhadap hasil analisis dan melakukan perhitungan prioritas resiko menggunakan pendekatan model DREAD terhadap ancaman yang berpotensi timbul dan memberikan mitigasi terhadap ancaman dengan pendekatan *best practice* yang sesuai dengan kriteria. Untuk tahap terakhir adalah menarik kesimpulan dan memberikan saran. Dalam gambar 3.3 berikut, terlihat dengan jelas tahapan dari penelitian ini.



Tahapan penelitian

## Metode Pengumpulan Data

Metode pengumpulan data menggunakan riset lapangan ditujuan untuk mendapatkan data faktual lapangan yang digunakan sebagai data penunjang objek penelitian. Riset lapangan dilakukan dengan melakukan hal-hal sebagai berikut:

1. Wawancara

Wawancara dengan pihak internal perusahaan dimana wawancara dilakukan secara *in-depth interview* kepada pihak – pihak yang berkaitan dengan penggunaan teknologi informasi pada PT. XYZ untuk mengetahui kondisi empiris perusahaan pada saat ini dengan menanyakan informasi secara detail dari keadaan aplikasi dengan mencari tahu aset-aset aplikasi, desain aplikasi, fungsi aplikasi dan *security control* yang saat ini sudah ada.

1. Observasi

Observasi dilakukan dengan melakukan identifikasi kondisi perusahaan dan permasalahan yang dialami perusahaan dengan mengumpulkan data-data yang dibutuhkan sebagai penunjang penelitan. Selain itu dilakukan observasi dengan *login* langsung kedalam aplikasi untuk mengetahui fitur-fitur dan cara kerja aplikasi.

1. Studi Dokumentasi (*Literatur Review*)

Studi dokumentasi dengan melakukan identifikasi dan analisis dokumentasi yang dimiliki oleh PT. XYZ yang berkaitan dengan penelitian ini yang mana bertujuan untuk mendukung proses penelitian agar dapat berjalan dengan baik.

## Metode Analisis Hasil Penelitian

Metode analisis hasil penelitian tersebut dibantu oleh riset pustaka ditujukan untuk mendapatkan teori-teori yang dapat memperkuat penelitian.

1. Metode untuk melakukan pemodelan ancaman yang akan dibahas di penelitian ini adalah dengan penggunaan kombinasi framework dari *P.A.S.T.A* dan *Microsoft SDL – STRIDE* sesuai pada gambar 3.3 bagian sub pemodelan ancaman,
2. Dalam melakukan pemodelan ancaman, dilakukan analisis tujuan bisnis dan tujuan keamanan dari aplikasi tersebut dan melakukan rangkuman secara garis besar sistem yang akan diteliti berdasarkan hasil wawancara
3. Tahap selanjutnya melakukan penguraian desain sistem dengan membuat DFD dengan menggunakan *Microsoft Threat Modeling Tools* dan mengidentifikasi setiap ancaman *STRIDE* setiap per element DFD.
4. Setelah mengidentifikasi ancaman yang terdapat pada sistem, dilakukan *brainstroming* untuk menemukan kerentanan dari hasil analisis pemodelan ancaman dengan dibantu dengan pendekatan parameter OWASP Top 10 tahun 2013 seperti yang telah di jelaskan pada gambar 2.7.
5. Terakhir melakukan perhitungan level prioritas atau *scoring* ancaman tersebut apakah termasuk kategori *high, medium, low* menggunakan pendekatan *DREAD* dan memberikan mitigasi ancaman berdasarkan *best practice OWASP*.

## Jadwal Penelitian

Jadwal penelitian untuk setiap tahapan adalah sebagai berikut ini.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Kegiatan** | **Bulan** | | | | | | |
| **11** | **12** | **1** | **2** | **3** | **4** | **5** |
| 1. | Identifikasi Permasalahan PT. XYZ |  |  |  |  |  |  |  |
| 2. | Studi Literatur |  |  |  |  |  |  |  |
| 3. | Pengumpulan Data |  |  |  |  |  |  |  |
| 4. | Analisa Data |  |  |  |  |  |  |  |
| 5. | Penulisan Tesis |  |  |  |  |  |  |  |

Jadwal penelitian

# DAFTAR PUSTAKA

Consoli, D. (2012). Literature Analysis on Determinant Factors and The Impact of ICT in SMEs. *Procedia - Social and Behavioral Sciences, 62*(Figure 1), 93-97.

Hussain, S., Erwin, H., & Dunne, P. (2011). Threat Modeling using Formal Methods: A New Approach to Develop Secure Web Applications. *IEEE*.

Jangam, E. (2009, July). *Threat Modeling and Its Usage in Mitigating Security Threats in an Application.* Retrieved January 18, 2016, from http://isea.nitk.ac.in/publications/ThreatModeling.pdf

Lipner, S., & Howard, M. (2005). *The Trustworthy Computing Security Development Lifecycle*. Retrieved from https://msdn.microsoft.com/en-us/library/ms995349.aspx

Michael McGrath, R. L. (2013). *Threat Modelling for Legacy Enterprise Applications.* Retrieved January 18, 2016, from CUAL Repository: http://cual.openrepository.com/cual/handle/10759/325583

Microsoft. (2016). *Microsoft Threat Modeling Tool 2016.* Retrieved January 19, 2016, from https://www.microsoft.com/en-us/download/details.aspx?id=49168

Microsoft Corporation. (2003). *Chapter 3 Threat Modeling*. Retrieved January 19, 2016, from https://msdn.microsoft.com/en-us/library/ff648644.aspx

Möckel, C., & Abdallah, A. E. (2010). Threat Modeling Approaches and Tools for Securing Architectural Designs of an E-Banking Application. *Sixth International Conference on Information Assurance and Security*, (pp. 1491-154).

Myagmar, S., Lee, A. J., & Yurcik, W. (2005). Threat Modeling as a Basis for Security Requirements. *In Proceedings of the Symposium on Requirements Engineering for Information Security.* Paris.

MyAppSecurity Inc. (2012). *Comparison of Threat Modeling Methodologies*. Retrieved January 19, 2016, from MyAppSecurity - SecureYourApplication: http://myappsecurity.com/comparison-threat-modeling-methodologies/

Saitta, P., Larcom, B., & Eddington, M. (2005). Trike v.1 Methodology Document [Draft].

Satapathy, S. R. (2014). *Threat Modeling in Web Applications* . Retrieved from ethesis.nitrkl.ac.in/5793/1/E-9.pdf

Shin, M., Dorbala, S., & Jang, D. (2013). Threat Modeling for Security Failure-Tolerant Requirements. *IEEE*, 594-599.

Shostack, A. (2014). Threat Modeling: Designing for Security. In A. Shostack, *Threat Modeling: Designing for Security* (pp. 62-63). Indianapolis, Indiana: John Wiley & Sons, Inc.

Supardono, B. (2009). Manajemen Resiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation). *Media Electonika*, 2.

The OWASP Foundation . (2001, December 1). *OWASP*. Retrieved January 21, 2016, from OWASP: https://www.owasp.org/index.php/Main\_Page

UcadaVelez, T. (2012). *Real World Threat Modeling Using the PASTA Methodology.* Retrieved January 19, 2016, from OWASP AppSec: https://www.owasp.org/index.php/File:AppSecEU2012\_PASTA.pdf

# LAMPIRAN

