PERANCANGAN PERLINDUNGAN PERANGKAT LUNAK SEBAGAI ASET INFORMASI TERHADAP MALICIOUS CODE DI FAKULTAS TEKNIK UNIVERITAS PASUNDAN

Basofi Adi Wicaksono[1-], Iwan Kurniawan, ST., MT.[2], Rita Rijayanti, ST., MT.[3]

[1,2,3] Informatika, Teknik, Universitas Pasundan
[1,2,3] Unpas, 40154

[1]basofi.aw@mail.unpas.ac.id, [2]iwank@unpas.ac.id, [3]rita.rijayanti@unpas.ac.id

Abstrak

Pada zaman sekarang dengan berkembang pesatnya teknologi, maka tingkat penggunaan teknologi pun seakan-akan telah membius masyarakat untuk bergantung pada teknologi. Disisi lain, perkembangan ancaman-ancaman pun semakin banyak dan berkembang memanfaatkan celah-celah yang ada. Ancaman tersebut bisa berasal dari organisasi, individu, atau celah pada software yang dapat mengakibatkan hilang, rusak, bahkan pencurian aset oleh pihak yang akan menyalahgunakan aset yang dimiliki untuk kepentingan pribadi.

Perlindungan perangkat lunak merupakan merupakan tahapan atau cara melindungi suatu perangkat lunak dari risiko (kerentanan dan ancaman) yang ada. Risiko sendiri dapat mengakibatkan terganggunya proses bekerjanya perangkat lunak tersebut. Sehingga proses bisnis dapat terganggu dan bahkan dapat merugikan pihak Fakultas Teknik Universitas Pasundan.

Hasil dari perancangan perlindungan perangkat lunak ini di rancang untuk membantu pihak Fakultas Teknik Universitas Pasundan dalam mencegah, mengelola, dan memonitoring aset perangkat lunak dari risiko yang ada. Sehingga dapat meminimalisir terjadinya gangguan pada proses bekerjanya perangkat lunak tersebut. Oleh karena itu jika perlindungan perangkat lunak ini di terapkan proses bisnis dapat terjaga dan bahkan menguntungkan pihak Fakultas Teknik Universitas Pasundan karena risiko tersebut sudah terkontrol.

Kata Kunci : Risiko, Ancaman, Kerentanan, Perlindungan, Aset, Perangkat Lunak.

1. PENDAHULUAN

1.1 Latar Belakang Tugas Akhir

Informasi merupakan salah satu aset bagi sebuah perusahaan atau organisasi, dimana aset juga memiliki nilai tertentu bagi perusahaan atau organisasi, sehingga aset harus dilindungi untuk menjamin kelangsungan perushaan atau organisasi dan meminimalisir kerusakan aset.

Keamanan aset merupakan suatu hal yang wajib diperhatikan oleh setiap organisasi, karena ancaman terhadap keamanan aset bisa berasal dari organisasi, individu, atau celah pada software yang dapat mengakibatkan hilang, rusak, bahkan pencurian aset oleh pihak yang akan menyalahgunakan aset yang dimiliki oleh organisasi tersebut. Masalah yang sering terjadi yaitu penyusupan script/crack oleh hacker. Permasalahan lainnya yang sering muncul yaitu adanya script yang tidak dikenali oleh antivirus/firewall.

Fakultas Teknik Universitas Pasundan merupakan sebuah organisasi yang bergerak dibidang pendidikan, yang menggunakan teknologi informasi sebagai alat bantu dalam bidang akademik, untuk menunjang visi dan misi Fakultas Teknik Universitas Pasundan. Teknologi yang membantu proses bisnis tersebut dapat dikategorikan sebagai aset. Aset sendiri terdiri dari perangkat keras (hardware), perangkat lunak (software), data, infrastructure, karyawan, dan outsourced service.

Fakultas Teknik Universitas Pasundan pernah mengalami masalah penyusupan oleh pihak tidak bertanggung jawab yang mengakibatkan kerugian. Masalah tersebut dapat datang dari pihak internal atau external, atau pun dari bencana alam. Maka dari itu aset-aset yang ada perlu dilindungi dari segala risiko-risiko yang dapat memberikan efek pada keberlangsungan kinerja dari organisasi, seperti menghambat atau menghentikan kelangsungan bisnis Fakultas Teknik Universitas Pasundan.

Oleh karena itu perlu dilakukan identifikasi terkait risiko-risiko yang ada pada setiap aset dan penangan yang terkait dengan tindakan perlindungan bagi aset dan seluruh hal yang berkaitan dengan Teknologi informasi. Tidak hanya berpikir tentang risiko dalam konteks kerahasiaan, integritas dan ketersediaan teknologi dan informasi, tetapi bagaimana aset tersebut dapat terlindungi dari potensi bahaya keamanan dan menilai risiko-risiko yang kemungkinan akan muncul.

1.2 Identifikasi Masalah

Berdasarkan latar belakang yang telah dipaparkan, terdapat poin – poin dari permasalahan yang akan dibahas yaitu :

1. Bagaimana cara mengidentifikasi risiko pada aset perangkat lunak di fakultas teknik UNPAS.
2. Bagaimana cara mengelola keamanan informasi aset di fakultas teknik UNPAS.

1.3 Tujuan Tugas Akhir

Tujuan ataupun solusi dari permasalahan yang ada, adalah yaitu :

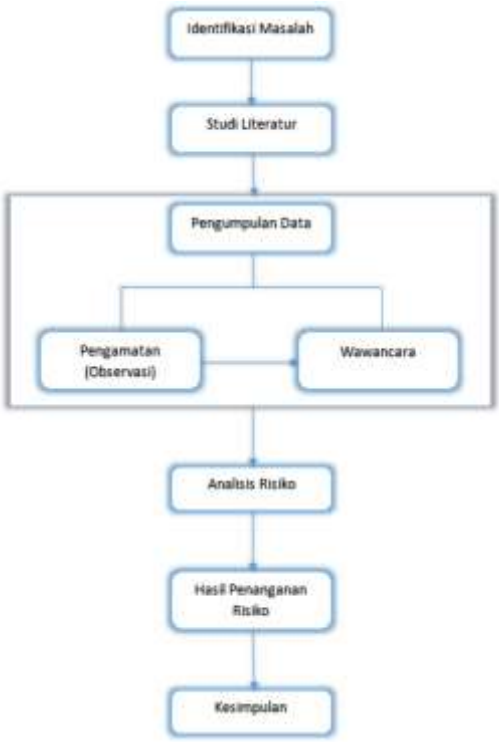
1. Dapat mengidentifikasi risiko pada aset perangkat lunak di fakultas teknik UNPAS.
2. Membuat rekomendasi penanganan keamanan aset perangkat lunak yang ada di fakultas teknik UNPAS.

1.4 Lingkup Tugas Akhir

Lingkup tugas akhir penulis meliputi :

1. Lingkup penelitian Tugas Akhir di Fakultas Teknik UNPAS bagian akademik.
2. Dititik beratkan kepada perangkat lunak yang digunakan untuk membantu proses bisnis akademik.
3. Menggunakan pendekatan standar SNI ISO/IEC 27001:2009 Klausul A.10.4.1 Pengendalian terhadap malicious code. Klausul tersebut digunkan untuk acuan dalam menetapkan pengendalian terhadap malicious code pada perangkat lunak.

1.5 Metodologi Tugas Akhir



Gambar 1.1 Metodologi Tugas Akhir

2. LANDASAN TEORI

2.1 Definisi Perlindungan Perangkat Lunak

Perlindungan menurut KBBI yaitu tempat berlindung; hal (perbuatan dan sebagainya) melindungi.

Definisi perangkat lunak menurut Melwin Daulay Syafrizal dalam bukunya yang berjudul Mengenal Hardware-Software dan Pengelolaan Instalasi Komputer yaitu "perangkat lunak berfungsi sebagai pengatur aktivitas kerja komputer dan semua instruksi yang mengarah pada system computer". [SYA07]

Menurut Suryatmo dan Rusmadi (2006:65), Perangkat lunak (software) merupakan suatu komponen di dalam suatu sistem data berupa program atau instruksi untuk mengontrol suatu sistem. Jadi dapat disimpulkan bahwa perangkat lunak yaitu kumpulan dari instruksi-instruksi pada suatu suatu sistem/program, yang berfungsi untuk memerintah, mengatur dan mengontrol program/intruksi pada suatu sistem. [SUR 06]

Aset perangkat lunak yaitu perangkat lunak yang berharga dari perusahaan/organisasi. Sehingga jika terjadi masalah pada perangkat lunak dapat menghambat jalannya proses bisnis. Aset perangkat lunak meliputi aplikasi bisnis, sistem operasi, aplikasi keamanan TI, aplikasi pengembangan, dan aplikasi pemantauan sistem.

Perlindungan perangkat lunak adalah tahapan atau cara melindungi suatu perangkat lunak dari ancaman-ancaman yang ada.

2.2 Definisi Aset Informasi

Aset menurut KBBI yaitu sesuatu yang mempunyai nilai tukar; modal; kekayaan: -- perusahaan; gerakan rakyat yang memerdekakan bangsa merupakan – nasional. Aset menurut ISO 27001:2009 adalah apapun yang memiliki nilai. [ISO09] Jadi aset bisa diartikan sesuatu yang berharga dan bernilai dari perusahaan/organisasi.

Definisi Informasi adalah data yang berguna untuk diolah sehingga dapat dijadikan dasar untuk mengambil keputusan yang tepat." (Bodnar dan Hopwood, 2001). Informasi merupakan salah satu aset yang sangat penting bagi orang yang membutuhkan informasi tersebut. Dengan berkembangnya teknologi informasi yang sangat pesat, kemungkinan terjadinya gangguan keamaan pada asset pun semakin meningkat.

2.3 Definisi Risiko

Definisi risiko menurut KBBI yaitu akibat yang kurang menyenangkan (merugikan, membahayakan) dari suatu perbuatan atau tindakan. Definisi risiko menurut ISO 31000:2009 adalah dampak dari ketidakpastian terhadap pencapaian objektif.

Jadi dapat disimpulkan bahwa risiko adalah akibat atau dampak dari suatu tindakan terhadap pencapaian objektif (mengenai keadaan yang sebenarnya tanpa dipengaruhi pendapat atau pandangan pribadi).

2.4 SNI ISO/IEC 27001:2009

Standar SNI ISO/IEC 27001:2009 "Teknologi informasi – Teknik keamanan – Sistem manajemen keaman informasi – Persyaratan" disusun secara adopsi identik terhadap standar ISO27001:2005, Information technology – Security techniques – Information security management

systems – Requirements, dengan metode terjemahan oleh panitia Teknis PK 03-02 Sistem Manajemen Mutu yang dibentuk oleh BSN. Standar ini disepakati dalam rapat konsensus yang diselenggarakan pada tanggal 12 agustus 2009 di Bogor, dengan dihadiri oleh anggota Panitia Teknis Sistem Manajemen Mutu sebagai wakil dari pemangku kepentingan (stakeholder) dan narasumber. Standar SNI ISO/IEC 27001:2009 sendiri dibuat sebagai model untuk penetepan, penerapan, pengoperasian, pemantauan, pengkajian, pemeliharan, dan Sistem Manajemen Keamanan Informasi (SMKI) dalam konteks organisasi. Ini juga mencakup persyaratan untuk penilaian risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi. Standar ini dan sistem pendukungnya diperkirakan akan berubah dari waktu ke waktu. Penerapan SMKI di sesuaikan dengan kebutuhan organisasi, misalnya situasi sederhana mensyaratkan penyelesaian yang sederhana. [ISO09]

Pendekatan proses untuk manajemen keamanan informasi yang dituangkan dalam standar ini mendorong penggunanya untuk menenkankan tentang tentang pentingnya:

a. Pemahaman persyaratan keamanan informasi dari suatu organisasi dan kebutuhan untuk membuat kebijakan dan sasaran untuk keamanan informasi.
b. Penerapan dan pengoperasian kendali untuk mengatur risiko-risiko keamanan informasi dari suatu organisasi dalam konteks risiko bisnis dari organisasi secara keseluruhan.
c. Pemantauan dan pengkajian kinerja keefektifan SMKI.
d. Perbaikan berkesinambungan berdasarkan pengukuran sasaran.

Standar ini mengadopsi model Plan-Do-Check-Act(PDCA), yang diterapkan untuk membentuk seluruh proses SMKI, serta melalui tindakan dan proses yag diperlukan akan menghasilkan keluaran keamanan informasi yang memenuhi persyaratan dan harapan tersebut.

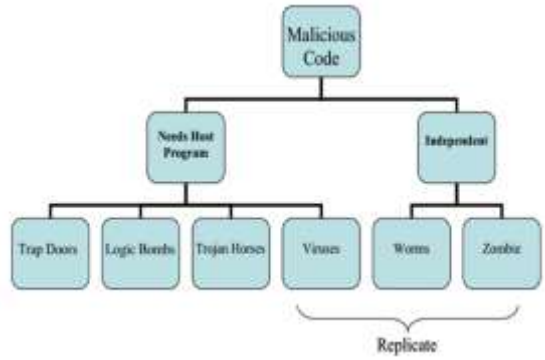
Adopsi dari model PDCA juga mencerminkan prinsip-prinsip dalam panduan OECD (2002), yang mengatur kemanan sistem informasi dan jaringan. Standar ini memberikan model yang kokoh untuk menerapkan prinsip-prinsip yang ada dalam panduan tersebut yang mengatur asesmen risiko, desain kemanan dan penerapan, manajemen keamanan dan rasesmen. [ISO09]

2.5 Risk Assessment

Risk Assessment adalah metode yang sistematis untuk menentukan apakah suatu kegiatan/aset mempunyai resiko yang dapat diterima atau tidak. Risk Assessment sangat penting karena membantu menciptakan kesadaran tentang bahaya dan resiko yang didapatkan dari aset yang dimiliki. Hal ini bertujuan untuk mengurangi kemungkinan bahaya dengan menambahkan langkah-langkah pengendalian yang diperlukan dan tindakan pencegahan. Penilaian juga memprioritaskan bahaya dan membantu menentukan apakah tindakan pengendalian yang ada memadai Risk assessment dilakukan dengan metode "Reproducible", pengukuran yang digunakan harus dapat digunakan lagi. [DIR13]

2.6 Malicious Code

Setiap kode yang memodifikasi atau merusak data, mencuri data, memungkinkan eksploitasi akses tidak sah atau merusak sistem, dan melakukan sesuatu yang pengguna tidak berniat untuk melakukan, disebut Malicious code. Malicious code atau kode berbahaya mengacu pada kategori yang luas dari ancaman perangkat lunak untuk jaringan dan sistem. Mungkin jenis yang paling canggih dari ancaman terhadap sistem komputer disajikan oleh kode berbahaya yang mengeksploitasi kerentanan dalam sistem komputer. [HEI04]



Gambar 2.1 Malicious Code [HEI04]

Sistem kalasifikasi dalam pengelompokan disarkan kepada ke unikan dari tiap-tiap karakter malicious code. Dari sifat malicious code yang berbeda tersebut dapat dibedakan ke dalam 2 tipe katagori, yaitu kategori Independets dan membutuhkan program host. Untuk kategori independents adalah kategori dimana malicious code dapat berdiri sendiri pada sebuah program yang ada pengaturan waktunya. Untuk malicious code yang membutuhkan program host, sebuah malicious code tidak dapat berdiri sendiri dalam menginfeksi sebuah computer. Program malicious code ini membutuhkan file aplikasi program lain di dalam jaringan komputer atau sistem utilitas yang ada pada program. [MUS08]

Dari perbedaan tersebut malicious code ternyata memiliki banyak jenis, jenis-jenis tersebut akan dibahas beberapa saja, diantaranya:

1. Trap Door

   Trap door adalah program yang cara masuknya secara rahasia, karena cara masuknya secara rahasia sehinggga program ini memberikan akses untuk masuk ke sistem orang lain tampa melalui prosedur tingakatan keamanan. Di dalam banyak kasus, serangan terhadap trap doors dapat memberikan akses ke program

aplikasi yang bertujuan mencuri data informasi atau memantau system komputernya. Trap door juga digunakan oleh programmer untuk mencari program debug dan test program. [MUS08]

2. Logic Bomb
   Logic bomb atau juga sering disebut dengan time bomb merupakan program yang pada saat waktu tertentu akan aktiv yang berdampak kepada tergangunya kinerja sistem computer. Pada saat logic bomb dieksekusi maka seseorang dapat masuk ke dalam sistem computer dengan mudah karena keamanan kinerja sistemnya telah dirusak. Lagic bomb dapat di sisipkan ke dalam program aplikasi sehingga program logic bomb ini sulit dilacak, selain itu logic bomb juga mampu menjalankan rutinitas pada alamat memori tertentu. [MUS08]
3. Trojan Horse
   Trojan horse merupakan program yang terselubung dan baik dalam meyelinap di dalam e-mail seseorang. Trojan horse bisanya program yang berbentuk sesuatu yang sangat menarik, sehingga seseorang menginginkan program tersebut untuk memilikinya. Apabila Trojan horse telah masuk ke dalam sistem seseorang maka program tersebut akan memberikan akses secara keseluruhan terhadap sistem yang duah terinfeksi tersebut. Trojan horse ini dibuat memang unuk mendapatkan akses untuk ke file sistem orang lain. Dengan demikian penyerang mampu melakukan pencurian file dan password, merusak file, atau memonitor apa yang dilakukan korbannya, mendownload file, menonaktifkan perangkat keras tertentu, merubah nama file, melakukan force shut down atau reboot, menonaktifkan antivirus dan jaringan keamanan computer, menggunakan computer korban sebagai zombie. [MUS08]
4. Virus
   Pengertian virus pertama kali diutarakan oleh pakar computer bernama Fred Cohen yang bahwasanya sebuah program yang dapat menginfeksi dan menyebar ke program-program lainnya dengan cara memodifikasi program tersebut. Dengan terinfeksinya suatu program maka virus dapat menyebar sepanjang seluruh jaringan sistem computer yang terkena inefeksi. Tiap-tiap program yang terkena infeksi program tersebut akan bertindak sebagai virus juga. [MUS08]
5. Worm
   Worm merupakan adalah program yang dapat mereplikasi dirinya sendiri dan mengirim kopian-kopian di jaringan internet. Ketika worm menjangkiti computer maka, worm akan mengaktifkan untuk merepliksai dan propagasi kembali. Worm terdapat tiga buah tipe yaitu true worm, protocol worm, dan hybrip worm. Perbedaan antara worm dan viru terletak kepada bagaimana merka membutuhkan intervensi user untuk melakukan penggandaan diri. Virus memiliki kelemahan yaitu proses penyebarannya yang lambat daripada worm. [MUS08]
6. Zombie
   Zombie adalah istilah sebuah program yang mengusai jaringan internet computer lain dimaan computer korban tersebut dapat melakukan perintah serangan kepada user-user lain di dunia maya. Zombie ini sulit di deteksi karean computer korban hanyalah tumbal dari dari kejahatan yang dibuat oleh pelaku yang sebenrnya. Inplementasi zombie ini sering digunakan sebagai serangan terhadap DDos (Distributed Denial of service) dimana banyak permintaan dari banyak computer yang ditujukan kepada satu buah komputer saja. [MUS08]

Tabel 2.1 Penelitian Terdahulu

No	Judul	Penulis	Tahun
1	Usulan Manajemen Risiko Berdasarkan Standar SNI ISO/IEC 27001:2009 Menggunakan Indeks KAMI (Keamanan Informasi) Studi Kasus : Badan Nasional Penempatan Dan Perlindungan Tenaga Kerja Indonesia (BNP2TKI)	Indah Kusuma Dewi, Fitroh, Suci Ratnawati.	2015
2	Analisis Kamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001:2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ)	Rosmiati, Imam Riadi	2016
3	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 PADA PT. BPR JATIM	Fine Ermana, Haryanto Tanuwijaya, Ignatius Adrian Mastan	

No	Judul	Penulis	Tahun
4	Rancangan Kebijakan Sistem Manajemen Keamanan Informasi Untuk PT.Asuransi SATU	Kurniawan Kemas Ahmad	2014
5	Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005	Melwin Syafrizal	

3. ANALISIS

3.1 Analisis Perancangan Perlindungan Keamanan Perangkat Lunak Menggunakan SNI ISO/IEC 27001:2009

Analisis dilakukan bertujuan untuk mengetahui kecocokan solusi dengan permasalahan yang ada pada penelitian ini. Sehingga permasalahan yang telah dipaparkan dapat diselesaikan dengan solusi yang sesuai. Analisis disini berisikan masalah utama penelitian, penyebab dan solusi. Analisis tersebut dapat dilihat pada Tabel 3.1 Analisis Peran.

Masalah	Solusi
- Adanya ancaman dan kerentanan pada aset perangkat lunak. - Tidak adanya prosedur secara tertulis terkait dengan keamanan infromasi khususunya perangkat lunak.	- Dapat menemukan ancaman dan kelemahan yang sering terjadi pada aset perangkat lunak. - Dapat menghitung nilai risiko dasar pada aset, sehingga dapat terlihat ancaman mana yang mendapatkan predikat tertinggi. - Membuat usulan perlindungan pada aset perangkat lunak dari ancaman dan kerentanan. Usulan ini dapat menjadi acuan pihak manajemen dalam membuat kebijakan/prosedur dalam penanganan ancaman dan kelemahan pada aset perangkat lunak.

3.2 Keadaan tempat penelitian mengenai Kebijakan SMKI saat ini

Aktivitas yang dilakukan dalam proses survei dengan cara observasi dan wawancara mengenai keadaan pengamanan/kebijakan-kebijakan informasi aset perangkat lunak terhadap risiko yang ada pada FT UNPAS. Jika dikaji dari sudut pandang SMKI, adapun hal-hal positif terkait dengan kontrol keamanan yang telah diterapkan sesuai dengan SNI ISO/IEC 27001, diantaranya seperti yang tersaji di pada tabel 3.2 kebijakan positif.

Tabel 3.2 Kebijakan Positif

No	Positif	Annex A
1	Sudah memiliki kebijakan mengenai log aplikasi	A.10.10. Pemantauan
2	Sudah memiliki prosedur/aturan dalam pemakaian aplikasi	A.13.2.1. Tanggung jawab dan prosedur
3	Sudah memiliki kebijakan mengenai pengendalian hak akses	A.11.1.1. kebijakan pengendalian akses
4	Sudah memiliki kebijakan mengenai penggunaan password	A.11.3.1. Penggunaan password
5	Sudah memiliki kebijakan terhadap kode sumber program	A.12.4.3. Pengendalian akses terhadap kode sumber program

Namun disisi lain, terdapat pula sisi negatif dari penerapan kontrol yang ada saat ini belumlah sesuai dengan standar Annex A ISO 27001:2005, kekurangan-kekurangan tersebut terdapat pada tabel 3.4 kebijakan negatif.

Tabel 3.4 Kebijakan Negatif

No	Positif	Annex A
1	Belum ada laporan tertulis mengenai usulan/keluhan dari pengguna	A.13.1. Pelaporan kejadian dan kelemahan keamanan informasi
2	Belum ada kebijakan mengenai keamanan informasi, khususnya keamanan pada aplikasi (secara tertulis)	A.5.1. Kebijakan Keamanan Informasi
3	Jarang adanya kontrol rutin	A.10.4.1 Pengendalian terhadap malicious code
4	Jarang adanya pengumpulan dan analisis data (serangan)	A.10.4.1 Pengendalian terhadap malicious code

3.3 Identifikasi Risiko

Setelah penulis mendapatkan hasil dari observasi dan wawancara, maka penulis dapat melakukan identifikasi risiko. Identifikasi risiko ini terdiri dari analisis aset, analisis ancaman dan kelemahan, dampak risiko tersebut terhadap perangkat lunak, dan risk assessment.

3.3.1 Analisis Aset

Setelah penulis melakukan observasi dan wawancara, aset aplikasi yang digunakan oleh FT Unpas yaitu :

1. Sistem Informasi Terintegrasi Universitas Pasundan (SITU).
   - Tujuan dari penggunaan SITU yaitu membantu proses bisnis akademik mulai dari PMB, KBM dan Wisuda (calon mahasiswa, mahasiswa, dosen, manajemen).
   - Peran dari penggunaan SITU yaitu sebagai alat bantu bagian akademik.
   - Pengguna aplikasi ini yaitu mahasiswa, dosen dan manajemen.

- Untuk kesesuaiannya, SITU sudah sangat sesuai dengan yang diharapkan, meskipun untuk kedepannya diharapkan untuk adanya pembaharuan/upgrade.

2. Jalak.
   - Tujuan dari penggunaan jalak yaitu untuk membantu proses bisnis akademik seperti KBM khusunya nilai dan insentif nilai (manajemen).
   - Peran dari penggunaan jalak yaitu sebagai alat bantu bagian akademik.
   - Pengguna aplikasi ini yaitu manajemen.
   - Untuk kesesuaiannya, SITU sudah sangat sesuai dengan yang diharapkan
3. Ms. Office 2010 dan 2013.
   - Tujuan dari penggunaan Ms. Office yaitu sebagai administrasi perkantoran.
   - Peran dari penggunaan Ms. Office yaitu sebagai alat bantu bagian akademik.
   - Pengguna aplikasi ini yaitu dosen dan manajemen.
   - Untuk kesesuaiannya, SITU sudah sangat sesuai dengan yang diharapkan

3.3.2 Analisis Ancaman Dan Kerentanan

Setelah penulis melakukan observasi dan wawancara, ancaman dan kelemahan yang sering terjadi pada aplikasi aset perangkat lunak yaitu :

a. Ancaman (Malcode)
   1. Cracking.
   2. SQL Injection.
   3. Cross site script (XSS).
   4. Bug program.
   5. Virus.

b. Kerentanan
   1. Ketidaktahuan pengguna terhadap keamanan informasi.
   2. Social Engineering.
   3. Password lemah.
   4. Kode program tidak optimal (bug).
   5. Jalur komunikasi tidak aman.
   6. Port pada server tidak tertutup.
   7. Firewall tidak aktif.

3.3.3 Dampak Risiko Terhadap Perangkat Lunak

Dibawah ini merupakan tabel 3.2 dari dampak risiko terhadap aset perangkat lunak.

Tabel 3.2 Dampak Risiko

No	Ancaman	Probabilitas terjadinya ancaman	Dampak
1	*Cracking*	Langka	Dapat menyebabkan dampak yang cukup serius, seperti memberhentikan kinerja aplikasi.
2	SQL *Injection*	Langka	Dapat menyebabkan dampak yang cukup serius seperti : 1. Memberhentikan kinerja aplikasi. 2. Perusakan data pada database.
3	*Cross site script (XSS)*	Sering	Dapat menyebabkan dampak gangguan kecil seperti merubah tampilan website.
4	*Bug program*	Terjadi	Dapat menyebabkan dampak serius: 1. fungsi-fungsi pada aplikasi tidak berjalan. 2. Memberhentikan kinerja aplikasi.
5	Virus	Jarang	Dapat menyebabkan dampak cukup serius: 1. fungsi-fungsi pada aplikasi tidak berjalan. 2. Memberhentikan kinerja aplikasi.

3.3.4 Risk Assessment (Penilaian Risiko)

Setelah penulis melakukan anilisis risiko, pada bagian ini penulis akan melakukan penilaian pada risiko yang telah didapat.

Tabel 3.3 Penilaian Risiko

Ancaman	Dampak	Kemungkinan	NRD	Tingkat
Cracking	*Major*	*Rare*	4+1 = 5	Menengah
SQL Injection	*Major*	*Rare*	4+1 = 5	Menengah
Cross site script (XSS)	*Insignificant*	*Almost*	1+5 = 6	Tinggi
Bug program	*Moderate*	*Likely*	3+4 = 7	Tinggi
Virus	*Major*	*Unlikely*	4+2 = 6	Tinggi

Dari hasil penilaian risiko diatas dapat terlihat bahwa ancaman yang terjadi berada pada tingkatan menengah dan tinggi, terutama pada ancaman tingkat tinggi diperlukan penanganan dengan prioritas diatas ancaman pada tingkat menengah.

4. PENANGANAN RISIKO

4.1 Pengendalian Risiko

Dari ancaman dan kerentanan yang ada akan dilakukan pengendalian menggunakan SNI ISO/IEC 27001:2009 dan ISO 27002:2009.

4.1.1 Pengendalian Ancaman Malicious Code.

Mengacu pada Annex A.10.4.1 Pengendalian terhadap malicious code, Pengendaliannya: Untuk mengendalikan ancaman dari malicious code harus melakukan pengendalian yang bersifat pendeteksian, pencegahan, pemulihan, dan menerapkan prosedur baik dalam pemakaian, perawatan, dan pemulihan perangkat lunak agar terhindar dari malicious code agar dapat membantu pihak management dalam melaksanakan tugasnya.

Petunjuk pelaksanaan: Perlindungan terhadap malicious code (kode berbahaya) harus didasarkan pada deteksi kode berbahaya dan

perbaikan perangkat lunak, kesadaran keamanan, dan akses sistem dan manajemen perubahan pengendalian yang tepat. Untuk guide-nya harus mempertimbangkan: [ISO05]

a. Menetapkan kebijakan formal yang melarang penggunaan perangkat lunak yang tidak sah agar sistem tidak terjangkit oleh malicious code.
b. Menetapkan kebijakan formal untuk melindungi terhadap risiko yang terkait dengan memperoleh file dan software baik dari pihak internal (pegawai) atau melalui jaringan eksternal, atau media lainnya, untuk menunjukkan tindakan perlindungan yang harus diambil untuk mencegah datangnya risiko.
c. Melakukan monitoring atau tinjauan rutin terhadap aset perangkat lunak dan konten data dari sistem pendukung proses bisnis. Dan siapa saja yang mengakses aset perangkat lunak dan setiap file yang masuk harus dilakukan filtering agar aman dari ancaman malicious code.
d. Melakukan Instalasi, deteksi, pembaruan (update) rutin kode program dan perbaikan perangkat lunak untuk memindai program, komputer dan media sebagai kontrol pencegahan terhadap acaman malicious code, atau secara rutin melakukan pemeriksaan yang harus mencakup:
    1. Memeriksa setiap file pada media elektronik atau optik, dan file yang diterima melalui jaringan, untuk kode berbahaya sebelum digunakan. Memeriksa kode program agar tidak terjadi bug dan kode pogram yang tidak optimal untuk segera dilakukan maintenance agar tidak tereksploitasi oleh ancaman.
    2. Memeriksa file hasil download dari malicious code sebelum digunakan. Pengecekan ini harus dilakukan di tempat yang berbeda dari sistem utama.
    3. Memeriksa halaman web agar tidak terjangkit oleh malicious code.
e. Mendefinisikan setiap prosedur dan tanggung jawab manajemen untuk menangani perlindungan dari malicious code pada sistem, melakukan pelatihan dalam penggunaan, pelaporan dan pemulihan dari serangan malicious code.
f. Mempersiapkan rencana khusus untuk kelangsungan bisnis yang tepat untuk pulih dari serangan malicious code, termasuk semua data yang diperlukan, software back-up, dan pengaturan pemulihan lainnya.
g. Menerapkan prosedur secara teratur untuk mengumpulkan informasi, seperti berlangganan mailing list atau memeriksa situs web yang relevan / resmi, untuk memberikan informasi tentang update-an dari malicious code terbaru, agar pihak manajemen bisa mengantisipasi munculnya serangan malicious code.
h. Menerapkan prosedur untuk memverifikasi informasi yang berkaitan dengan malicious code, dan memastikan bahwa buletin peringatan yang akurat dan informatif. Manajemen harus memastikan bahwa sumber harus berkualitas, misalnya jurnal terkemuka, situs internet yang handal atau suppliers yang memproduksi software kemanan, untuk terlindungi dari malicious code, yang digunakan untuk membedakan antara hoax (palsu / kabar bohong) dan kode berbahaya yang real (nyata).

Informasi lainnya:

Penggunaan dua atau lebih produk perangkat lunak untuk melindungi dari malicious code pada pengolahan informasi dari vendor yang berbeda dapat meningkatkan efektivitas perlindungan dari kode berbahaya.

Software untuk melindungi dari malicious code dapat diinstal untuk memberikan update otomatis pada file dan melakukan pemindaian untuk memastikan perlindungan yang up to date. Selain itu, software ini dapat diinstal pada setiap desktop untuk melakukan pemeriksaan otomatis.

Perawatan harus diambil untuk melindungi dari pengenalan kode berbahaya selama pemeliharaan dan prosedur darurat, yang dapat melewati kontrol dari perlindungan kode berbahaya.

4.1.2 Pengendalian Kerentanan

Dari ancaman yang ada, disebabkan dari kerentanan-kerentanan yang ada. Maka dari itu harus adanya pengendalian terhadap kerentanan tersebut mengacu pada SNI ISO/IEC 27001:2009. Annex yang digunakan yaitu:

1. Annex A.8.1.3 syarat dan aturan kepegawaian.
2. Annex A.11.3.1 Penggunaan password.
3. Annex A.12.4.3 Pengendalian akses terhadap kode sumber program.
4. Annex A.12.5.1 Prosedur pengendalian perubahan.
5. Annex A.10.6.1 Pengendalian jaringan.

4.2 Pelaporan Insiden Keamanan

Untuk memastikan kejadian dan kelemahan informasi terkait dengan sistem informasi dikomunikasikan sedemikian rupa, sehingga memungkinkan tindakan koreksi dilakukan tepat waktu (Annex A.13.1).

Mengacu pada A.13.1.1 Pelaporan kejadian keamanan informasi, pengendaliannya: Jika terjadi ancaman malicious code pada aset perangkat lunak, maka kejadian tersebut harus langsung dilaporkan melalui saluran yang tepat dan cepat kepada pihak manajemen. Kemudian dari setiap pelaporan dari ancaman dan pengendaliannya harus dibuat laporan, sehingga dapat terdokumentasikan dengan baik.

Mengacu pada A.13.1.2 Pelaporan kelemehan keamanan, pengendaliannya: Semua pegawai dan pengguna aset perangkat lunak dari sistem informasi dan layanan harus diisyaratkan untuk mencatat dan melaporkan setiap kelemahan pada keamanan yang diamati dan dicurigai dalam sistem atau layanan tersebut. Kemudian dari setiap pelaporan kelemahana tersebut dan

pengendaliannya harus dibuat laporan, sehingga dapat terdokumentasikan dengan baik.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan dari penelitian tugas akhir penulis yang dilakukan terkait dengan risiko pada perangkat lunak di Fakultas Teknik Universitas Pasundan adalah sebagai berikut:

1. Dari hasil yang didapat dengan adanya kelemahan dan ancaman akan terjadi risiko-risiko sebagai berikut:
   a. Risiko akses oleh pihak yang tidak berwenang.
   b. Risiko adanya perubahan pada aplikasi, baik itu pada tampilan atau pada fugsinya.
   c. Risiko berhentinya kinerja aplikasi.
   d. Risiko kerugian akibat terhentinya operasi kinerja aplikasi secara total atau sementara, sehingga mengganggu kelancaran operasional pihak FT UNPAS.
2. Dengan adanya perencanaan penanganan keamanan informasi ini, memungkinkan terjaganya integritas (integrity) dan ketersediaan (availability) aset perangkat lunak, sehingga dapat mencapai tingkat kerahasiaan (confidentiality) informasi aset perangkat lunak. Dan juga dapat membantu pihak manajemen sebagai referensi dalam melakukan pembuatan kebijakan atau prosedur keamanan informasi khususnya perangkat lunak.

5.2 Saran

Saran dari penelitian tugas akhir penulis yang dilakukan terkait dengan risiko pada perangkat lunak di Fakultas Teknik Universitas Pasundan adalah sebagai berikut:

1. Harapan penulis untuk kedepannya yaitu agar perencangan penanganan ini dapat dijadikan acuan oleh pihak Fakultas Teknik Uiversitas Pasundan untuk membuat kebijakan terhadap keamanan informasi khususnya terhadap ancaman malicious code pada aset perangkat lunak khususnya aplikasi.
2. Diharapkan para pengguna agar lebih aware (peduli) untuk kedepannya terhadap ancaman dan kelemahan pada aset perangkat lunak.
3. Di adakannya pelatihan mengenai keamanan informasi untuk para pengguna aset perangkat lunak.
4. Harapan penulis selanjutnya agar dari rancangan penaganan keamanan pada perangkat lunak ini dapat dikembangkan kedepannya oleh teman-teman atau oleh pihak FT UNPAS.

DAFTAR PUSTAKA

[AHM14] Ahmad, Kurniawan Kemas, "Rancangan Kebijakan Sistem Manajemen Keamanan Informasi Untuk PT. Asuransi SATU", Universitas Pasundan, Bandung, 2014.

[ALB05] Al-Bahra bin Ladjamudin, Analisis dan Desain Sistem Informasi, Graha Ilmu, Yogyakarta, 2005.

[DAN08] Dani Junian, "Pengembangan Kebijakan Keamanan Informasi Pada Perusahaan Jasa Layanan Kurir", Universitas Indonesia, Jakarta, 2008.

[DIR13] Direktorat, "Risk Assessment (Penilaian Resiko)", Universitas Airlangga, Surabaya, 2013.

[HEI04] Heidari Mohammad, *Malicious Codes in Depth*, 2004.

[JUM] Jumiati, Wahyudi Tri., "Model Kesadaran Keamanan Informasi di Lingkungan Instansi Pemerintah Indonesia Berdasarkan ISO-SNI/IEC 27001 : 2009 Sistem Manajemen Keamanan Informasi".

[MUS08] Muslim Ahmad, "Malicious Code", Universitas Sriwijaya, Palembang, 2008.

[ISO05] ISO/IEC 27002:2005, "*Information Technology – Security Techniques – Code of Practice for Information Security Management*", ISO, IEC, Switzerland, 2005.

[ISO09] ISO/IEC 27001:2009, SNI, "Teknologi Informasi - Teknik Keamananan – Sistem Manajemen Keamanan Informasi – Persyaratan", BSN, Bogor, 2009.

[ISO16] ISO, "The Story of ISO", Tersedia : 29 Agustus 2016, pukul 15:22 WIB, http://www.iso.org/iso/home/about/the_iso_story.htm, 2016.

[SUD16] Sudirman Irvan, "Perkembangan *Software* Komputer", 2003, Tersedia : 11 November 2016, pukul 08.33 WIB, https://www.scribd.com/document/7607818/perkembangan-software-komputer, 2016.

[SKO04] Skoudis Ed, "*Malware: Fighting Malicious Code"*, *Pearson Seducation, inc, New Jersey*, 2004.

[DAU07] Daulay, Melwin DAUfrizal, "Mengenal *Hardware-Software* dan Pengelolaan Instalasi Komputer", Andi, 2007.