Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute Of Standards And Technology) Sp 800-30. (Studi Kasus : Disinfolahtaau Mabes Tni Au)

[1]Anggi Elanda, [2]Djajasukma Tjahjadi
Program Studi Teknik Informatika
STMIK Rosma, Jl. Kertabumi No.62, Karawang Kulon, Karawang Bar., Kabupaten Karawang, Jawa Barat 41311 Indonesia
email : [1]anggi@rosma.ac.id, [2]djaja@likmi.ac.id

ABSTRACT
IDS (Intrusion Detection System) adalah sistem komputer (bisa merupakan kombinasi software dan hardware) yang berusaha melakukan deteksi penyusupan. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS. Software Agent (selanjutnya disebut agent saja) adalah entitas perangkat lunak yang didedikasikan untuk tujuan tertentu. NIST (National Institute of Standard and Technology) Special Publication (SP) 800-30 adalah panduan manajemen risiko untuk sistem teknologi informasi yang terstandarisasi oleh Pemerintah Pusat Amerika Serikat. Metodologi ini dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisis keamanan yang cukup sesuai dengan keinginan pemilik sistem dan ahli teknis untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman sampai dengan sumber identifikasi untuk evaluasi berkelanjutan dan penilaian. Dalam penelitian ini penulis memilih untuk analisis manajemen resiko dari aplikasi Cybersensor sebagai IDS yaitu dengan menganalisis resiko apa saja yang terjadi di masa yang akan datang, dalam hasil analisis ini akan membuat sebuah laporan untuk dilaporkan kepada pihak manajemen untuk sebagai acuan kejadian-kejadian yang telah terjadi ataupun belum terjadi sehingga lebih waspada saat sebuah serangan terjadi. Cybersensor sendiri dibuat dengan bahasa pemrograman PHP dan Python serta penggabungan dengan aplikasi Snort .

***Kata Kunci** : Intrusion Detection System, Snort, Manajemen Risiko, NIST SP 800-30*

1. Introduction

Perkembangan dunia internet pada saat ini telah mencapai suatu tahap yang begitu cepat, sehingga tidak mengherankan apabila di setiap sudut kota banyak ditemukan termpat-tempat internet yang menyajikan berbagai jasa pelayanan internet. Sejarah perjalanan internet dari mulai ditemukan hingga menjadi suatu kebutuhan manusia sampai saat ini sangatlah panjang. Internet adalah jaringan informasi yang pada awalnya (sekitar akhir 1960-an, tepatnya mulai tahun 1969) dikembangkan oleh Departeman Pertahanan dan Keamanan Amerika Serikat (DoD = Departement of Defense) USA sebagai proyek strategis yang bertujuan untuk berjaga-jaga (penanggulangan) bila terjadi gangguan pada jaringan komunikasi umum, khususnya pengaruhnya pada sistem komunikasi militer mereka. Pada saat itu perang dingin antara Amerika Serikat dengan Uni Soviet sedang mencapai puncaknya, sehingga mereka membuat antisipasi atas segala kemungkinan akibat perang yang mungkin akan terjadi. Awalnya internet hanya digunakan secara terbatas di dan antar-laboratorium penelitian teknologi di beberapa institusi pendidikan dan lembaga penelitian saja, yang terlibat langsung dalam proyek DARPA (Defence Advanced Research Projects Agency). Tetapi 45 tahunan kemudian (sekarang ini), internet telah meluas

ke seluruh dunia, dari pemerintah, perusahaan besar dan kecil, LSM hingga perorangan telah banyak yang memanfaatkannya, karena kepraktisannya sebagai sarana komunikasi dan untuk pencarian informasi Data tentang internet tahun 1998 menyebutkan bahwa e-mail telah dapat dikirim ke 150 negara lebih di dunia ini, transfer file (ftp) dapat menjangkau ke 100-an negara, dan pengguna di seluruh dunia pun diperkirakan telah sampai 60 juta-an orang, atau 5% dari jumlah total seluru penduduk dunia. Kemudian, berdasarkan data tahun 1999, pengguna internet di seluruh dunia hingga Mei 1999 sudah mencapai 163 juta orang.

Pada mulanya, internet sempat diperkirakan akan mengalami kehancuran oleh beberapa pengamat komputer di era 1980-an karena kemampuannya yang pada saat itu hanya bertukar informasi satu arah saja. Namun semakin ke depan, ternyata perkiraan tersebut meleset, dan bahkan sekarang menjadi suatu kebutuhan akan informasi yang tiada henti-hentinya dipergunakan.

Namun keindahan internet tidak seindah namanya yang dijanjikan dapat memberikan berbagai informasi yang ada di belahan dunia manapun, karena berbagai kejahatan yang ada di kehidupan nyata ternyata lebih banyak ditemukan didunia internet. Kejahatan di internet ini populer dengan nama cybercrime. Adanya cybercrime akan menjadi dampak buruk bagi kemajuan dan perkembangan negara kita serta di dunia pada umumumnya. Saat ini, internet telah menjadi bagian dari kehidupan kita sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk privat. Tetapi di balik itu masih banyak lubang kelemahan sistem di internet yang bisa dimanfaatkan oleh para cracker untuk tujuan tidak baik, seperti bom mail, pengacak-acakan home page, pencurian data, pasword ataupun nomor kartu kredit, dan lain-lain.

Saat ini perkembangan teknologi yang termasuk cepat adalah system Cloud Computing. Sudah banyak yang memakai teknologi tersebut mulai dari email, penyimpanan data, data pekerjaan maupun untuk digunakan meeting di kantor. Jaringan komputer terus mengalami perkembangan, baik dari skalabilitas, jumlah node dan teknologi yang digunakan. Hal ini memerlukan pengelolaan jaringan yang baik agar ketersediaan jaringan selalu tinggi. Tugas pengelolaan jaringan yang dilakukan administrator jaringan memiliki banyak permasalahan, diantaranya yang berkaitan dengan keamanan jaringan komputer. Penyusupan (intrusion) adalah seseorang yang berusaha merusak atau menyalahgunakan sistem, atau setiap usaha yang melakukan compromise integritas, kepercayaan atau ketersediaan suatu sumberdaya komputer . Definisi ini tidak bergantung pada sukses atau gagalnya aksi tersebut, sehingga berkaitan dengan suatu serangan pada sistem komputer. Intrusion detection (ID) singkatnya adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal cracker) atau seorang user yang sah tetapi menyalahgunakan (abuse) privelege sumberdaya sistem (misal insider threath). Intrusion Detection System (IDS) atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi software dan hardware) yang berusaha melakukan deteksi penyusupan . IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai mencurigakan atau tindakan ilegal. IDS tidak melakukan pencegahan terjadinya penyusupan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada bagaimana baik melakukan konfigurasi IDS. Software Agent (selanjutnya disebut agent saja) adalah entitas perangkat lunak yang didedikasikan untuk tujuan tertentu . Agen bisa memiliki ide sendiri mengenai bagaimana menyelesaikan suatu pekerjaan tertentu. Sejumlah riset tentang agentelah membuat bermacam aplikasi, misal untuk distributed meeting scheduler, network mapping auction, dan searching database. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu pesan, data, atau informasi. Dalam hal ini sangat terkait dengan betapa pentingnya pesan, data, atau informasi tersebut di kirim dan di terima oleh pihak atau orang yang berkepentingan, apakah pesan, data, atau informasi masih authenticity. Pesan, data, atau informasi akan tidak berguna lagi apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak atau berkepentingan. (Firrar.U., Riyanto B , 2003).

NIST (National Institute of Standard and Technology) Special Publication (SP) 800-30 adalah panduan manajemen risiko untuk sistem teknologi informasi yang terstandarisasi oleh Pemerintah Pusat Amerika Serikat. Metodologi ini dirancang untuk menjadi suatu perhitungan kualitatif dan didasarkan pada analisis keamanan yang cukup sesuai dengan keinginan pemilik sistem dan ahli teknis untuk benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko dalam sistem TI. Proses ini sangat komprehensif, meliputi segala sesuatu dari ancaman sampai dengan sumber identifikasi untuk evaluasi berkelanjutan dan penilaian. (Elky, Steve 2007).

Sumber identifikasi ancaman dapat berasal dari salah satu atau beberapa disaster diantaranya natural disaster, environment/technology disaster, dan human disaster. Disaster yang sering terjadi pada sistem berbasis web adalah human disaster. Human disaster dapat berupa kesalahan input data dan peretasan. Kesalahan input data biasanya dilakukan oleh pegawai baru yang belum menguasai operasional sistem. Sedangkan peretasan biasanya dilakukan oleh hacker/cracker dengan memanfaatkan celah – celah keamanan website yang masih terbuka. Masalah yang timbul pada sistem dapat dikategorikan sebagai risiko. Risiko yang terjadi pada sistem akan menghambat proses bisnis. Dengan demikian, manajemen risiko dibutuhkan agar risiko-risiko yang mungkin timbul bisa tertata dan terkelola dengan baik.

Berdasarkan uraian diatas, maka peneliti berencana membuat "Analisis Manajemen Resiko Sistem Keamanan IDS (Intrusion Detection System) Dengan Framework Nist (National Institute Of Standards And Technology) SP 800-30. (Studi Kasus : DISINFOLAHTAAU MABES TNI AU)". Penelitian ini diharapkan mempermudah kepada auditor untuk keamanan internet dalam melakukan audit pada IDS (Intrusion Detection System) sehingga akan banyak pengembangan kedepannya.

2. Research Method

Metodologi yang digunakan dalam penelitian ini adalah:

1. Studi literatur yaitu dengan mempelajari dari buku-buku terkait sistem maupun bahan hasil browsing dari internet.
2. Observasi yaitu dengan melakukan pengamatan terhadap kegiatan di lingkungan Mabes TNI AU pada bagian Disinfolahtaau.
3. Interview yaitu melakukan wawancara dengan pihak-pihak terkait seperti pimpinan bagian dan beberapa staff yang bekerja pada bagian Disinfolahtaau.
4. Tinjauan atas berbagai dokumen yang didapatkan dari bagian Disinfolahtaau

3. Result and Analysis

Proses penilaian risiko (*risk assessment*) dilakukan dengan beberapa tahapan, sesuai dengan Proses penilaian risiko (*risk assessment*) dilakukan dengan beberapa tahapan, sesuai dengan kerangka kerja NIST SP 800-30. Tahapan-tahapan tersebut sebagai berikut :

3.1. Karakteristik Sistem

Karakteristik sistem yang meliputi sistem *cybersensor*, diantaranya perangkat keras, perangkat lunak, data dan informasi, dan sumber daya manusia yang mendukung sistem informasi. Sumber daya perangkat keras meliputi PC yang digunakan untuk client dengan perangkat lunak program aplikasi, Windows 10 Profesional 64 bit sebagai sistem operasinya. Sedangkan perangkat lunak pada server menggunakan OS Linux dan Bahasa Pemrograman PHP. Data dan informasi meliputi data infrastruktur, data device, data server serta data penyerang.

a) Spesifikasi Perangkat Keras

Ada banyak *hardware* yang digunakan dalam menjalankan sistem ini diantaranya :

Tabel 1. Perangkat Keras

No	Nama Hardware	Jumlah	Spesifikasi
1	Server *Cybersensor*	1 Unit	Dell poweredge R730 (Intel Xeon, 16GB (1 x 16GB) DDR4 2133Mhz RDIMM, 300GB SAS 2.5" 15K Hotplug, 4 x GbE NIC, Rack Case)
2	Server Jaringan	1 Unit	Dell poweredge R730 (Intel Xeon, 16GB (1 x 16GB) DDR4 2133Mhz RDIMM, 300GB SAS 2.5" 15K Hotplug, 4 x GbE NIC, Rack Case)
3	Server *Incognito*	1 Unit	Dell poweredge R730 (Intel® Xeon®, 2 x 32 GB RDIM,HARD DRIVE 3 X 4TB)
4	Mikrotik	1 Unit	RB1100Ahx2
5	PC Client Cyber	30 Unit	HP ENVY 750-101D /Intel Core i7-6700 3,4G 8M 65 W CP Intel Skylake Z170 / 1PCI-E x 16, PCI-E x 1,4 x HDD 3,5' . 4 GB DDR4b1TB HDD Super Multi DVDRW NVDIA GEFORCE GTX 745 4GB DDR3, HP 7-in1 Multimedia Card Reader, HP Wireless Kit, Windows 10 64 bit. 500W Power Supply 1 Year Limited Warrantty HP Pavilion 23 cw IPS Monitor
6	PC Client	50 Unit	DELL Xps 8300, Core i7, RAM 8GB, HDD 500GB, VGA 4GB
7	Monitor 14 Inch	80 Unit	HP 23 Display
8	Switch 48 Port	3 Unit	Merk HP
9	CCTV	15 Unit	Merk HKVision
8	UPS	1 Unit	Galaxy VX 500kVA Scalable to 1000kVA 480V, Start up 5x8
9	Kabel LAN	20 Roll	Kabel UTP Belden CAT-6
10	TV Display 40 inch	12 Unit	Merk LG
12	TV Display 60 inch	1 Unit	Merk Samsung

b) Spesifikasi Perangkat Lunak

Untuk perangkat lunak yang digunakan dibagi kedalam dua bagian yaitu untuk server *cybersensor*, server jaringan dan *client*, dengan spesifikasi sebagai berikut :

1) *Software* untuk *Server Cybersensor* :
   - OS Debian Jessie
   - KVM
   - *Database Postgresql*
   - *Python*
   - PHP
2) *Software* untuk Server Jaringan :
   - OS FreeBSD 11
   - KVM
   - Nagios
   - Alienvault
3) *Server Incognito* :

- OS FreeBSD 11
- KVM
- *Securezone*

4) PC *Client* :
   - OS Windows 10 Professional 64bit
   - OS Kali Linux
   - *Browser Chromium/Google Chrome*

3.2. Identifikasi Ancaman

Sistem *Cybersensor* telah digunakan sejak tahun 2014, dan baru dilakukan upgrade pada tahun 2015. Dibawah ini merupakan *history threat* yang pernah terjadi :

Tabel 2. Identifikasi Ancaman

No	Uraian Kejadian	*Threat Source*	*Motivation*	*Threat Action*
1	Salah Pengoperasian Sistem yang menyebabkan sistem down	Human Disaster	Ketidaksengajaan	Pengoperasian Yang Salah
2	Serangan Virus dalam jaringan	Human Disaster	Ketidaksengajaan	Menggunakan USB Flashdrive untuk copy data
3	Listrik yang tiba-tiba mati menyebabkan memory server crash	Technology Disaster	Tegangan Listrik Yang Tidak Stabil	Tegangan listrik yang tiba-tiba down menyebabkan server mati dan ketika dinyalakan kembali memory menjadi crash
4	Kehilangan data dalam database yang sifatnya sensitif	Human Disaster	Ketidaksengajaan	User salah mengoperasikan sistem operasi yang dipakai oleh sistem cybersensor dalam database sehingga ada data-data yang hilang

3.3. Identifikasi Kerentanan

Terdapat banyak celah kelemahan yang ada pada Sistem *Cybersensor*, diantaranya :

Tabel 3. Celah Kelemahan

No	Letak Vulnerability	Penjelasan
1	Dapat menggunakan USB pada setiap PC client maupun server	Tidak ada kebijakan dilarang menggunakan USB untuk copy data sehingga memudahkan peluang adanya virus dan distribusi file tanpa ijin
2	Kondisi curah hujan yang tinggi, dan keadaan kota Jakarta yang memungkinkan terjadinya banjir	Ruang server terletak di lantai 1, sehingga jika ada banjir memungkinkan server terendam
3	Tim eksternal seperti tim vendor dan rekanan yang lainnya dengan bebasnya masuk ke ruang server, serta dapat mengakses data, dll.	Tidak adanya larangan untuk pihak eksternal mengakses ruang server, dan tidak ada tim internal Disinfolahtaau yang menguasai betul program

		Sistem Cybersensorr sehingga masih tergantung pada tim vendor dan rekanan.
4	Software yang digunakan masih versi lama	Belum adanya upgrade untuk bahasa pemrograman yang digunakan maupun versi database yang digunakan sehingga terdapat banyak kekurangan
5	Tidak adanya larangan untuk menginstall aplikasi atau program apapun pada pc server maupun client	Setiap orang dapat menginstalkan program atau aplikasi apapun pada pc client atau server walaupun dapat membahayakan sistem

3.4. Analisa Kontrol

Dari berbagai threat maupun vulnerability yang telah dikemukakan diatas, sudah ada beberapa control yang diterapkan walaupun implementasi dan penerapannya belum maksimal. *Control-control* tersebut antara lain :

Tabel 4. Analisa Kontrol

No	Control	Implementasi
1	Setiap ruangan server maupun ruangan pemantau dipasang doorlock yang menggunakan finger print, face recognition maupun access code	Hampir semua orang mengetahui
2	Ada larangan tidak boleh merokok dan makan diruangan tetapi tidak dalam bentuk tertulis dan tidak ada sanksi yang diberikan	Beberapa personel mengabaikan larangan tersebut
3	Pemasangan lantai panggung di ruang server dari bahan yang didatangkan dari Jerman untuk anti api	Ruang server lebih aman dari kebakaran karena lantai yang anti api tetapi hanya pada alas servernya saja, disisi yang lainnya menggunakan lantai panggung biasa
4	Pada setiap pc client maupun server diinstallkan anti virus	Anti virus jarang diupdate sehingga tidak dapat mendeteksi virus jenis baru

3.5. Kemungkinan Yang Menentukan

Dibawah ini dilakukan analisis mengenai seberapa sering resiko yang telah disebutkan diatas akan terjadi :

Tabel 5. Kemungkinan Yang Menentukan

No	Resiko	*Threat*	*Vulnerability*	*Likelihood*	Keterangan
1	Virus	Pc client atau pc server terkena serangan virus	Anti virus sudah diinstall tapi tidak pernah digunakan	High	Kemungkinan terjadinya sangat tinggi karena sering ada personil yang menggunakan usb pada pc client
2	Malware	Pc server terkena serangan malware	Belum ada penghalang malware	Low	Kemungkinan terjadinya low karena jarang dilakukan upgrade yang terhubung ke internet
3	Gangguan Tegangan Listrik	Listrik tiba-tiba mati ketika sistem sedang berjalan	UPS kadang-kadang tidak berfungsi	High	Kemungkinan terjadinya high karena dalam tiga bulan terakhir ini sering terjadi tegangan listrik turun

3.6. Analisa Dampak

Dibawah ini dilakukan analisis mengenai dampak yang terjadi terhadap resiko yang telah disebutkan diatas :

Tabel 6. Analisa Dampak

No	Resiko	Impact	Keterangan
1	Virus	Medium	Jika server terkena malware dampaknya medium karena sistem tidak dapat berjalan dan masih dapat dilakukan perbaikan dengan install ulang
2	Malware	Medium	Jika server terkena malware dampaknya medium karena sistem tidak dapat berjalan, reputasi Disinfolahtaau akan hancur, dan biaya yang dibutuhkan untuk melakukan perbaikan sangat tinggi karena mendatangkan tim vendor maupun rekanan untuk memperbaiki server
3	Gangguan Tegangan Listrik	High	Dampaknya sangat tinggi karena menyebabkan latihan terhambat dan kemungkinan memory server error ketika dinyalakan kembali
4	Kehilangan Data	High	Dampaknya sangat tinggi karena data yang ada didalamnya termasuk data yang sensitif
5	Salah Pengoperasian	High	Dampaknya sangat tinggi karena membutuhkan tim vendor dan rekanan yang memperbaiki program
6	Hacker	High	Dampaknya sangat tinggi karena membutuhkan tim vendor dan rekanan yang memperbaiki program
7	Pencurian Hardware	Low	Dampak terjadinya rendah karena tinggal mengganti saja
8	Distribusi File Tanpa Ijin	High	Dampaknya sangat tinggi karena data yang ada didalamnya termasuk data yang sensitif dan dapat disalahgunakan
9	Software versi lama	Low	Dampak terjadinya rendah karena sistem masih bisa berjalan pada versi lama hanya performance nya saja yang kurang
10	Unauthorized Installation of equipment programs	Medium	Dampaknya medium masih dapat dilakukan perbaikan dengan install ulang

No	Resiko	Threat	Vulnerability	Likelihood	Keterangan
11	Kehilangan Data	Database kekuatan personel maupun alutsista hilang	Tidak ada access control terhadap database	High	Kemungkinan terjadinya high karena sering adanya tim eksternal yang mengakses database dan data yang ada didalamnya termasuk data yang sensitive
12	Salah Pengoperasian	Operator salah menginputkan data menyebabkan sistem crash	Tidak ada access control dalam mengakses sistem	High	Kemungkinan terjadinya high karena sering terjadi kesalahan input data menggunakan illegal character
13	Hacker	Serangan hacker pada sistem	Belum ada Security control	Low	Kemungkinan terjadinya Low karena kurangnya motivasi orang untuk melakukan hacking
14	Pencurian Hardware	Hardware pendukung	Semua orang mengetahui	Medium	Kemungkinan terjadinya medium karena dalam

		hilang	password ruangan dan semua sama untuk setiap ruangan		satu tahun ini terjadi beberapa kehilangan hardware
15	Distribusi File Tanpa Ijin	File kekuatan personil dan alutsista tersebar kepada pihak yang tidak bertanggung jawab	Tim eksternal dengan bebasnya masuk ke ruang server, mengakses data, dll	High	Kemungkinan terjadinya high karena sering adanya tim eksternal yang mengakses database dan data yang ada didalamnya termasuk data yang sensitif
16	Software versi lama	Ada kelemahan dan error pada software	Bahasa pemrograman dan database menggunakan versi yang lama	Low	Kemungkinan terjadinya Medium karena jarang ada kesalahan yang diakibatkan oleh versi software
No	**Resiko**	**Threat**	**Vulnerability**	**Likelihood**	**Keterangan**
17	Unauthorized installation of equipment programs	Software lain yang terinstal mengandung virus dan mengganggu jalannya system	Pc client dan server enable untuk install software apapun	Medium	Kemungkinan terjadinya Medium karena terjadi ada personil yang menginstalkan Program program lain

3.7. Penentuan Risiko

Dibawah ini dilakukan analisis mengenai seberapa besar level resiko yang telah disebutkan diatas :

Tabel 7. Penentuan Risiko

No	Risiko	Likelihood	Impact	Risk
1	Virus	High	Medium	Medium
2	Malware	Low	Medum	Low
3	Gangguan Tegangan Listrik	High	High	High
4	Kehilangan Data	High	High	High
5	Salah Pengoperasian	High	High	High
6	Hacker	Low	High	Low
7	Distribusi File Tanpa Ijin	High	High	High
8	Pencurian Hardware	Medum	Low	Low
9	Software Versi Lama	Low	Low	Low
10	Unauthorized installation of equipment programs	Medium	Medium	Medium

3.8. Rekomendasi Kontrol

Dibawah ini dilakukan analisis mengenai seberapa sering resiko yang telah disebutkan diatas akan terjadi :

Tabel 8. Rekomendasi Kontrol

No	Resiko	*Risk Level*	*Control Recommendations*
1	Virus	Medium	a. Menginstalkan anti virus yang otomatis mendeteksi dan melakukan scanning virus b. Menjadikan usb port disable sehingga tidak bisa menggunakan usb c. Membuat pc tidak bisa diinstall software atau program-program lain
2	Malware	Low	Menyediakan penghalang malware pada server
3	Gangguan Tegangan Listrik	High	Mengoptimalkan fungsi ups sehingga bisa mengontrol tegangan listrik yang masuk
4	Kehilangan Data	High	Mengeluarkan kebijakan larangan mengakses database untuk pihak eksternal
5	Salah Pengoperasian	High	a. Menambahkan validasi pada program agar tidak salah input b. Mengadakan pelatihan khusus bagi para gamer untuk pengoperasian sistem
6	Hacker	Low	Menambahkan security control pada sistem
7	Pencurian Hardware	Low	a. Menambah access control pada tiap ruang pemantau b. Membuat password yang lebih secure
8	Distribusi File Tanpa Ijin	High	Mengeluarkan kebijakan larangan mengakses database untuk pihak eksternal
9	Software versi lama	Low	Melakukan upgrade software secara berkala
10	Unauthorized installation of equipment programs	Medium	a. Menjadikan usb port disable sehingga tidak bisa menggunakan usb b. Membuat pc tidak bisa diinstall software atau program-program lain

3.9. Dokumen Hasil

Dokumen untuk hasil *risk assessment* dan *risk mitigation* disajikan dalam bentuk laporan ini .

3.9.1. Analisis Kuantitatif

Selain dilakukan analisis kualitatif terhadap resiko dengan hasil yang ditampilkan diatas, penulis juga melakukan analisis kuantitatif dengan memperhitungkan *tangible* dan *intangible* value terhadap semua resiko. Hasil analisis adalah sebagai berikut :

Tabel 9. Analisis Kuantitatif

No	Resiko	Dampak Yang Terjadi	Total Kerugian
1	Virus	Install Ulang seluruh workstation	Asumsi biaya install ulang Rp. 100.000,- x 80 pc = Rp. 8.000.000 Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki sistem Rp. 10.000.000 x 2 orang = Rp. 20.000.000 Total Kerugian Rp. 28.000.000 per kejadian

2	Gangguan Tegangan Listrik	Memori Server Rusak	Pembelian Memory Server Rp. 8.000.000,- Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki sistem Rp. 10.000.000 x 2 orang = Rp. 20.000.000,- Total Kerugian Rp. 28.000.000,-
3	Kehilangan Data	Input ulang data	Biaya mendapatkan data personel dan alutsista dengan kunjungan Rp. 100.000.000,- Biaya Input Data Rp. 20.000.000,- Total Kerugian Rp. 120.000.000,-
4	Salah Pengoperasian	Sistem Crash dan harus diperbaiki	Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki server Rp. 20.000.000
5	Hacker	Sistem crash dan harus diperbaiki	Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki server Rp. 20.000.000
6	Pencurian Hardware	Pembelian hardware baru	Asumsi biaya pembelian hardware baru Rp. 5.000.000,-
7	Distribusi File Tanpa Ijin	Penyalahgunaan data alutsista TNI	Tidak ada biaya yang dikeluarkan hanya saja reputasi dan integritas data tidak terjaga
8	Software versi lama	Performance Sistem Berkurang	Asumsi biaya perbaikan dan install ulang program Rp. 10.000.000,-
9	Unauthorized installation of equipment programs	Install Ulang PC	Asumsi biaya install ulang Rp. 100.000,-

3.9.2. Mitigasi Risiko

Tahapan ini merupakan tindakan peringanan terhadap risiko yang sudah terdokumentasi. Hasil dari penilaian risiko ini berupa profil risiko dengan berbagai rekomendasi yang sekiranya dapat menjadi solusi dalam proses meringankan risiko yang sesuai dengan kebutuhan sistem informasi. Kegiatan mitigasi risiko ini meliputi prioritas aksi ini dilakukan dengan mengacu kehasil akhir penilaian risiko.

3.9.3. Prioritas Aksi

Dari daftar resiko yang telah dianalisis maka dilakukan analisis untuk memprioritaskan resiko dari yang level nya paling tinggi dan dampak yang palingbesar ke level yang paling rendah. Hasilnya adalah sebagai berikut :

Tabel 10. Prioritas Aksi

No	**Resiko**	***Risk Level***	**Total Kerugian**
1	Kehilangan Data	High	Biaya mendapatkan data personel dan alutsista dengan kunjungan Rp. 100.000.000,- Biaya Input Data Rp. 20.000.000,- Total Kerugian Rp. 120.000.000,-

2	Virus	Medium	Asumsi biaya install ulang Rp. 100.000,- x 80 pc = Rp. 8.000.000,- Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki sistem Rp. 10.000.000 x 2 orang = Rp. 20.000.000,- Total Kerugian Rp. 28.000.000 per Kejadian
3	Gangguan Tegangan Listrik	High	Pembelian Memory Server Rp. 8.000.000,- Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki sistem Rp. 10.000.000 x 2 orang = Rp. 20.000.000,- Total Kerugian Rp. 28.000.000,-
4	Malware	Low	Asumsi biaya install ulang server Rp. 5.000.000 Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki server Rp. 20.000.000 Total Kerugian Rp. 25.000.000,-
5	Salah Pengoperasian	High	Biaya Mendatangkan Tim Vendor 1 Hari untuk memperbaiki server Rp.20.000.000
6	Hacker	Low	Biaya Mendatangkan Vendor 1 Hari untuk memperbaiki server Rp. 20.000.000
7	Software versi lama	Low	Asumsi biaya perbaikan dan install ulang program Rp. 10.000.000,-
8	Pencurian Hardware	Low	Asumsi biaya pembelian hardware baru Rp. 5.000.000,-
9	Unauthorized installation of equipment programs	Medium	Asumsi biaya install ulang Rp. 100.000,-
10	Distribusi File Tanpa Ijin	High	Tidak ada biaya yang dikeluarkan hanya saja reputasi dan integritas data tidak terjaga
Total		**Rp. 256.100.000,-**	

Jika dilihat dari hasil memprioritaskannya tidak sesuai dengan urutan risk level yang ada. Hal ini dikarenakan penulis lebih memilih memprioritaskan resiko dari besarnya kerugian dampak jika resiko tersebut terjadi. Seorang pemimpin akan lebih *aware* jika melihat nominal kerugian jika dibandingkan dengan level resikonya.

3.9.4. Evaluasi Risiko (*Risk Evaluation)*

Dari hasil analisis control recommendation terhadap seluruh resiko yang ada dinyatakan bahwa semua control recommendation merupakan control yang paling efektif untuk diterapkan di Disinfolahtaau karena dari control tersebut tidak ada yang memberatkan baik dari segi biaya maupun dari segi kebijakan. Berikut adalah control yang telah sesuai :

Tabel 11. Evaluasi Risiko

No	Resiko	Risk Level	Control Recommendations
1	Virus	Medium	a. Menginstalkan anti virus yang otomatis mendeteksi dan melakukan scanning virus b. Menjadikan usb port disable sehingga tidak bisa menggunakan usb c. Membuat pc tidak bisa diinstall software atau program-program lain
2	Malware	Low	Menyediakan penghalang malware pada server
3	Gangguan Tegangan Listrik	High	Mengoptimalkan fungsi ups sehingga bisa mengontrol tegangan listrik yang masuk
4	Kehilangan Data	High	Mengeluarkan kebijakan larangan mengakses database untuk pihak eksternal
5	Salah Pengoperasian	High	a. Menambahkan validasi pada program agar tidak salah input b. Mengadakan pelatihan khusus bagi para tim untuk pengoperasian sistem
6	Hacker	Low	Menambahkan security control pada sistem
7	Pencurian Hardware	Low	a. Menambah access control pada tiap ruang pemantau b. Membuat password yang lebih secure
8	Distribusi File Tanpa Ijin	High	Mengeluarkan kebijakan larangan mengakses database untuk pihak eksternal
9	Software versi lama	Low	Melakukan upgrade software secara berkala
10	Unauthorized installation of equipment programs	Medium	a. Menjadikan usb port disable sehingga tidak bisa menggunakan usb b. Membuat pc tidak bisa diinstall software atau program-program lain

4. Conclusion

Berdasarkan hasil dan pembahasan maka dapat diperoleh bahwa dari identifikasi karakteristik dan ancaman serta kerentanan didapat beberapa sumber ancaman yang dapat menimbulkan risiko pada sistem cybersensor, diantaranya Human Disaster dan Technology Disaster, untuk Human Disaster antara lain : Virus, Malware, Kehilangan Data, Salah Pengoperasian, Hacker, Distribusi File Tanpa Ijin, Pencurian Hardware, Software Versi Lama, Instalasi Tanpa Ijin, dan untuk Technology Disaster adalah Gangguan Tegangan Listrik. Penentuan skala dengan menggunakan skala risk level dalam menganalisa lebih lanjut dari hasil analisa ancaman yang akan terjadi dan yang sudah terjadi. Analisis pengendalian dan dampak risiko yang terjadi pada system cybersensor dengan melihat skala risk level yang terjadi lalu akan memunculkan beberapa rekomendasi agar kedepannya tidak terjadi kembali hal serupa. Mitigasi risiko dengan menentukan total biaya yang didapat dalam setiap kerusakan yang ditimbulkan oleh beberapa ancaman yang terjadi. Untuk menghindari ancaman yang berdampak negatif terhadap sistem cybersensor ini maka diperlukan suatu dokumentasi mengenai hasil penilaian risiko, peringanan risiko, dan evaluasi risiko.

Penelitian manajemen risiko berikutnya diharapkan lebih spesifik terhadap manajemen risiko dibidang keamanan sistem yang berkaitan dengan sistem informasi berbasis online atau berkenaan dengan sistem cloud computing.

References

[1] A. Syalim, Y. Hori och K. Sakurai, (2009) *"Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide," I International Conference on Availability, Reliability and Security*, Fukuoka.

[2] Chen, Feiquan. (2015). *An Investigation And Evaluation Risk Assessment Methods In Information System*. Journal information system. Vol. 9

[3] Douramanis, Michail. (2014). *Risk Assessment for Cyber Threats to Networked Critical Infrastructure*. Journal information System. Vol. 1 No. 1

[4] Elky, Steve. (2007). An introduction to Information system Risk Management. © SANS Institute

[5] Firrar U., Riyanto B, (2003), Design dan Implementasi Mobile Agent Untuk Jaringan, Thesis ITB

[6] Istiningrum. (2011). Implementasi Penilaian Risiko dalam Menunjang Pencapaian Tujuan Instansi Pendidikan. UNY.

[7] International Standard Organization. (2011). ISO 27005 Information Technology, Security TechniquesInformation Security Risk Management. Switzerland: ISO/IEC.

[8] Iskandar, Iwan. (2011). *Mananajemen Risiko Teknologi Informasi Perusahaan Menggunakan Framework RiskIT*. Jurnal Teknik Informatika. Vol. 9 No. 1

[9] J.Kim, Hak. (2012). *Online Social Media Networking and Assessing Its Security Risks*. Journal Information System Vol.6 No.3

[10] National Institute of Standard and Technology. (2002). *Risk Management Guide for information Technology System*. USA: U.S. Department of Commerce

[11] Rajbandhari, Lisa. (2013). *Risk analysis Using Conflicting Incentives as an Alternatif Notion of Risk. Journal Information System*. Vol. 5 No.3

[12] Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology System Recommendations of National Institute of Standards and Technology*. NIST Laboratory.

[13] Sumantri, Iwan. (2013). *Kebijakan Keamanan Informasi* [online]. http://folder.idsirtii.or.id/pdf/ Kebijakan_Keamanan_Informasi.pdf [November 2014]

[14] Syafitri, Wenni. (2016).*Penilaian Risiko Keamanan Informasi Menggunakan Metode NIST 800-30 (Studi Kasus: Sistem Informasi Akademik Universitas XYZ)*, Pekanbaru.

[15] Trivina, Hanim dan Anisah. (2014). *Pengelolaan Risiko Aset Teknologi Informasi Pada Perusahaan Properti PT XYZ, Tangerang Berdasarkan Kerangka Kerja Cobit 4.1*. Jurnal Sistem Informasi. Vol. 9 No. 3

[16] Williams, Michael G. (2015). *A Risk Assessment on Rasberry Pi using NIST Standards*. Journal Computer Science. Vol. 15 No. 6