ANALISIS KEAMANAN SIKAPEG IVET BERBASIS ISO 27001:2013

Reni Veliyanti[1)], Marwata[2)], Irwan Sembiring[3)]
[1,2,3]Teknologi Informasi Universitas Kristen Satya Wacana
reniveliyanti@gmail.com[1)], marwata@staff.uksw.edu[2)],irwan@staff.uksw.edu[3)]

Diterima: Desember 2018. Disetujui: Desember 2018. Dipublikasikan: Desember 2018

ABSTRAK

Keamanan data sangat penting, sebab dapat memastikan kontinuitas pengelolaan, mengurangi risiko, dan menjadi peluang suatu lembaga untuk berkembang. Semakin banyak informasi yang dikelola dan di-*share* semakin besar pula risiko terjadinya kerusakan, kehilangan atau terekspos nya data ke pihak eksternal yang tidak bertanggung jawab. Tujuan penelitian untuk mendeskripsikan bentuk-bentuk ancaman keamanan dan langkah penanganan ancaman keamanan SIKAPEG. Penelitian termasuk penelitian *mixed method* yang difokuskan pada aktivitas sistem keamanan informasi terkait dengan kehadiran pegawai di IVET. Simpulan penelitian bahwa sistem keamanan SIKAPEG di IVET belum memenuhi standar ISO 27001:2013, beberapa indikator telah dilaksanakan namun ada yang kurang baik. Terjadinya ancaman termasuk pada kriteria mungkin terjadi, hal ini dilihat dari indikatornya kemungkinan terjadi ancaman rentangan antara 10-50% dalam waktu 1(satu) tahun. Sedangkan jika dikaitkan dengan skala *Likelihood* termasuk kriteria ringan, yaitu gangguan terhadap aplikasi/jaringan. Kelemahannya terletak pada tidak adanya tanggung jawab prosedur manajemen keamanan informasi, tidak ada bukti pelaporan hambatan keamanan informasi yang terdokumen, sehingga tidak bisa digunakan sebagai evaluasi mendatang, dan kurangnya kesadaran pegawai dalam melakukan presensi sidik jari, kurangnya empati dan kesadaran secara bersama menjaga dan merawat serta memelihara *hardware* pendukung. Pemeliharaan dan perawatan oleh teknisi sudah baik, namun belum dilaksanakan secara menyeluruh sehingga ada beberapa *hardware* yang mudah rusak karena titik lemah pada aplikasi, *hardware*, SDM merupakan potensi sumber ancaman keamanan yang berkembang menjadi gangguan pada SIKAPEG. Solusi sebagai rekomendasi, sebaiknya dilakukan kontrol secara periodik dan berkala, perawatan dan pemeliharaan secara menyeluruh, terdokumentasi saat dilakukan kontrol serta penetapan kebijakan secara tegas**.**

Kata kunci:keamanan sistem informasi, ISO 27001:2013.

ABSTRACT

Data security is very important, because it can ensure continuity of management, reduce risk, and become an opportunity for an institution to develop. The more information that is managed and shared, the greater the risk of data damage, loss or exposure to irresponsible external parties. The research objective is to describe the forms of security threats and steps to deal with SIKAPEG security threats. Research includes mixed method research which is focused on information security system activities related to the presence of employees at IVET. The conclusion of the study is that the SIKAPEG security system at IVET has not met the ISO 27001: 2013 standard, some indicators have been implemented but some have not been good. The occurrence of threats included in the criteria may occur which is the threat possibility indicator ranges from 10-50% within 1 (one) year. If it is associated with the Likelihood scale, it is included in the criteria of minor interference, which is the interference in the application / network. The weaknesses lie in the absence of information security management procedure responsibilities and no evidence of documented information security barriers, so that it cannot be used as an upcoming evaluation, and the lack of awareness of employees in fingerprint attendance, lack of empathy and awareness to maintain and care for the supporting hardware. Maintenance by technicians are good, but have not been carried out thoroughly so that there is some hardware that is easily damaged because of the weak points in applications, hardware, and human resources are potential sources of security threats that develop into disruptions in SIKAPEG. As solutions, a periodic control, a thorough maintenance, a documented control, and a policy determination are required.

Keywords: information system security, ISO 27001:2013.

PENDAHULUAN

Semakin banyak informasi yang dimanfaatkan oleh publik, maka semakin memiliki peluang untuk menerima risiko. Baik kerusakan, hilangnya data, dan terbacanya data oleh pihak luar yang tidak bertanggung jawab. Oleh karenanya standar layanan dan keamanan menjadi salah satu solusi, namun pada kenyataannya dalam penerapan standar baku masih sulit dilakukan pada sebuah organisasi. Hal itu dimungkinkan terjadi karena ruang lingkup atau fokus sebuah standar dirasa kurang luas cakupannya untuk memenuhi seluruh kebutuhan manajemen TI (Castro, 2016). Lebih lanjut dikemukakan bahwa semakin maju dan canggihnya teknologi terkini terkait dengan penggunaan TI, semakin meningkat potensi kejahatan manusai dengan kemampuan mengoperasikan TI yang canggih, orang jahat akan terus berimprovisasi dengan kemajuan yang ada. Ancaman bagi keamanan TI terjadinya efek yang muncul dari tiga kejadian, meliputi aspek: *confidentiality, integrity,* dan *availability* (CIA). Maka dari itu perlu dilakukan audit sistem informasi sebagai evaluasi sesuai fakta dan proses pengumpulan untuk menentukan sistem komputer yang digunakan dapat melindungi aset sutau organisasi atau tidak, kemampuan dalam melindungi integritas data, membantu pencapaian tujuan organisasi yang efektif, dan penggunaan sumber daya secara efisien (Santos, Marwata dan Sembiring, 2014).

Sistem pengelolaan keamanan informasi merupakan suatu rencana strategis perlu dilakukan untuk meminimalisir kelemahan dan mengurangi potensi risiko yang sedang berjalan, dengan proses mengurangi risiko serta melakukan penilaian dan juga kontrol. Pengelolaan keamanan informasi merupakan suatu yang penting untuk dipahami, diupayakan dan dicoba guna diterapkan agar informasi bisa dikelola dengan baik, agar lembaga fokus dalam pencapaian visi dan misi lembaga yang sudah ditetapkan, selain dilakukan pengembangan usaha untuk memberikan layanan prima kepada pelanggan termasuk yang dilakukan oleh IKIP Veteran Jawa Tengah Semarang (IVET).

IVET sebagai salah satu Perguruan Tinggi (PT) swasta yang dalam implementasi tata kelola TI belum dapat berjalan secara maksimal, sebab belum diketahuinya secara mendalam tingkat keamanan pada TI yang dapat dipakai untuk mendukung kemajuan dan perkembangan lembaga, di samping belum dimilikinya sistem yang mengkaitkan antara bagian struktur satu dengan bagian struktur lain. Peningkatan kedisiplinan kinerja pegawai (dosen dan tenaga administrasi) pada kehadiran, pimpinan IVET menempuh kebijakan dengan menggunakan mesin absensi sidik jari dan mesin absensi wajah yang telah terhubung secara online dengan sistem yang disebut Sistem Informasi Kehadiran Pegawai (SIKAPEG). Pimpinan dapat melihat langsung laporan kehadiran setiap hari dari SIKAPEG, bahkan setiap waktu. Namun seiring perjalanan waktu, sistem tersebut mengalami berbagai masalah dan kendala baik dari internal maupun eksternal. Kendala itu misalnya mesin tidak bisa membaca atau melakukan *scan* sidik jari atau wajah karena mengalami kerusakan (*error*) dan kerusakan pada sarana *hardware* pendukung seperti kerusakan komputer, sehingga kejadian itu berdampak pada perhitungan kehadiran yang berakibat pula pada insentif kehadiran yang diterima.

Penelitian tentang keamanan sistem informasi sudah dilakukan diantaranya adalah Kohar, *etal.* (2014), yang melakukan penelitian dengan tujuan untuk mengetahui ancamana terhadap keamanan sistem informasi kesehatan, khususnya Sistem Manajemen Rumah Sakit. Hasil penelitian diperoleh simpulan bahwa ancaman yang paling tinggi terhadap keamanan sistem informasi kesehatan adalah ancaman dari peretas.

Anggrini Kongo (2016) hasil

penelitiannya menyarankan perlu adanya prosedur penanganan risiko pada TI yang digunakan, dimulai dari adanya persyaratan/kontrak yang jelas dengan pihak luar untuk antisipasi jika masih terjadi risiko. Hasil penelitian juga ditemukan bahwa terkait dengan *software;* risiko dikenakan dengan regulasi DMCA karena beberapa *software* yang digunakan ternyata belum berlisensi. Pada *software;* beberapa sistem informasi sulit diakses karena web *hosting* masih dipegang oleh pihak luar. Terkait dengan infrastruktur, sebenarnya memiliki peluang besar, karena FTI memiliki infrastruktur yang memenuhi spesifikasi. Risiko kerusakan karena bencana alam dan listrik mati. Pada *hardware security*, risiko disebabkan mematikan server secara sengaja karena lokasi server yang diketahui banyak orang. Adapun dilihat dari SDM, kurangnya kemampuan SDM dalam laboran FTI-UKSW, sehingga berakibat terhambatnya pada akses data.

Darmawan (2017) dari hasil penelitiannya memberikan rekomendasi bahwa perlu peningkatan sistem keamanan FTI-UKSW karena belum maksimalnya sistem keamanan tersebut. Dikemukakan juga bahwa sistem keamanan di FTI-UKSW perlu menggunakan acuan berstandar ISO 27001:2013.

Berdasarkan penelitian relevan sebagai pendahulu terkait kajian keamanan sistem informasi dan kelemahan SDM pengoperasiannya yang belum didasarkan pada standar ISO 27001:2013, maka kelemahan tersebut dijadikan sebagai dasar peneliti untuk melakukan penelitian lanjutan, sehingga ditemukan teori baru tentang sistem keamanan informasi berstandar ISO 27001:2013.

Mengacu pada latar belakang di atas, rumusan masalah penelitian: apakah bentuk-bentuk ancaman keamanan dan langkah penanganan ancaman keamanan SIKAPEG?. Mengacu rumusan masalah, tujuan penelitian ini adalah menganalisis dan mendeskripsikan bentuk-bentuk ancaman keamanan dan langkah penanganan ancaman keamanan SIKAPEG.

TINJAUAN PUSTAKA

Tinjauan pustaka ini membicarakan tentang keamanan sistem informasi dan ISO 27001: 2013 sebagai berikut.

Keamanan Sistem Informasi

Keamanan yang efektif perlu diperhatikan semua pihak. Pentingnya pemahaman sistem informasi adalah, sebab informasi yang valid sangat diperlukan dalam sebuah organisasi publik (Laudon & Laudon, 2015). Dikemukakan lebih lanjut bahwa ancaman dalam sistem informasi dapat dikategorikan menjadi 7 (tujuh) macam, yaitu: (1) *hardware failure:* disebabkan oleh padamnya voltase listrik naik-turun, korsleting, atau *disk crashes*, (2) *software failure:* disebabkan kesalahan sistem operasi, kesalahan program *update*, tidak cukup, dan memadainya ujicoba program, (3) kegagalan SDM: dikarenakan sangat minimnya *training* bagi personel, personel yang sangat pasif atau kurang empati (*sense of belonging*), (4) alam, dikarenakan oleh cuaca, gas, banjir, gempa, proyektil atau letusan gunung, (5) keuangan: disebabkan oleh tuntutan hukum pihak ketiga, pailit, mogok kerja, atau hura-hura, (6) eksternal: sabotase, spionase, hura-hura, dan (7) internal: dalam bentuk kecurangan, pencurian, perbuatan jahat (memasukkan virus, atau membangun *malicious software*).

ISO 27001:2013

Menurut Buku Panduan Peneraan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (indeks KAMI) Ver 1.0 September 2017, SNI ISO 27001:2013 telah mengadopsi format terkini dari standar sistem manajemen dengan merujuk pada standar yang dikembangkan ISO sebelumnya

(Aprian, Rizal, & Sobri, 2015). Lampiran A dijelaskan bagian standar yang menetapkan "sasaran kontrol" dan "kontrol" langsung diadopsi dari ISO 27001:2013. Lampiran itu menguraikan 114 kontrol dari 14 area kontrol dapat digunakan untuk pelindung informasi di berbagai organisasi. Dari 14 area kontrol ISO 27001:2013 yang digunakan pada penelitian ini 10 (sepuluh) area kontrol. Keempat area kontrol tidak diterapkan di lapangan, karena tuntutan indikator dari keempatnya belum tersedia di objek penelitian. Ke-10 area kontrol yang dimaksud: (1) A.5 *Security Policies,* (2) A.6 *Organisation of Information Security,* (3) A.7 *Human Resource Security,* (4) A.8 *Asset Management,* (5) A.9 *Acces Control,* (6) A.11 *Physicaland Environmental Security*, (7) A.12 *Operations Security,* (8) A.13 *Communications Security*, (9) A.14 *System Acquisitio, Delelopmentand Maintenance*, dan (10) A.16 *Information Security Incident Management.*

METODEPENELITIAN

Jenis penelitian yang digunakan termasuk penelitian campuran (*mixed method*), yaitu penggunaan data kuantitatif dan kualitatif (Tashakkori & Teddlie, 2010). Penelitian difokuskan pada aktivitas sistem keamanan informasi terkait dengan kehadiran pegawai baik tenaga edukatif maupun adminitrasi di IVET. Sumber data diperoleh dari: (1) informan melalui wawancara, (2) dokumen, dan (3) aktivitas. Data dihimpun dari: (1) data yang dimiliki Kepala Kepegawaian, (2) data Kepala Unit TIK, (3) apresiasi tenaga edukatif dan tenaga administrasi pada kehadiran, (4) faktor pendukung dan penghambat penggunaan mesin kehadiran, serta (5) solusi yang ditawarkan terkait hambatan dalam penggunaan SIKAPEG dari hasil wawancara Kepala Unit TIK sebagai informan kunci dan Kepala Kepegawaian sebagai informan tambahan.

Analisis data digunakan metode deskriptif persentase dan model interaktif meliputi: (1) reduksi data, (2) sajian data, dan (3) penarikan simpulan/verifikasi yang disajikan dalam bentuk laporan hasil penelitian, sedangkan keabsahan data digunakan triangulasi dan *memberchek*. Ke-10 area kontrol untuk melakukan analisis ancaman terhadap SIKAPEG di IVET digunakan kriteria Sistem Manajemen Keamanan Informasi (SMKI) seperti pada tabel berikut.

Tabel 1. Kriteria Kemungkinan Terjadi Ancaman

	Kemungkinan
1. Hampir pasti (*Almostertain*)	>90% akan terjadi dalam periode waktu satu (1) tahun
2. Sering (likely)	Antara 50-90% akan terjadi dalam periode waktu satu (1) tahun
3. Mungkin (*possible*)	Antara 10-50% akan terjadi dalam periode waktu satu (1) tahun
4. Jarang (*rare*)	<10% akan terjadi dalam periode waktu satu (1) tahun

Adapun kriteria dampak (*impact*) dari jenis kejadian atau ancaman dapat digunakan skala *Likelihood* sebagai berikut.

Tabel 2. Jenis Kejadian dan Skala *Likelihood* (Kemungkinan)

Kate-gori	Sangat Kecil	Ringan	Mene-ngah	Berat
Gangguan terhadap aplikasi *e-government*	Aplikasi tidak dapat diakses <1 jam di luar jam kerja	Aplikasi tidak berfungsi > 1–4 jam selama jam kerja	Aplikasi tidak berfungsi >4–24jam selama jam kerja	Aplikasi tidak berfungsi lebih dari 24 jam selama jam keja
Gangguan terhadap aplikasi/ jarin	Jaringan tidak dapat diakses <1 jam di luar jam kerja	Sistem tidak berfungsi > 1–4 jam selama jam	Sistem tidak berfungsi >4–24jam selam	Sistem tidak berfungsi lebih dari 24 jam selama jam keja

gan		kerja	a jam kerja	
Keluhan user	Keluhan kecil dan tidak Signifikan	Keluhan dialami dan disampaikan oleh sejumlah pengguna	Keluhan dimuat di media lokal	Keluhan dimuat di mediai lokal & nasional

Wawancara Informan digunakan *Internal Control Questionnaires* (ICQs). ICQs didesain menggunakan skala Guttman sehingga diperoleh jawaban tegas "Ya" dan "Tidak" (Sugiyono, 2012). Jawaban "Ya" mengidentifikasikan bahwa penerapan 10 area kontrol pada ISO 27001:2013 telah dilaksanakan, jawaban "Tidak" mengindikasikan penerapan ke-10 area kontrol pada ISO 27001:2013 tidak dilakukan dengan baik. Sistem penilaian pada kuesioner digunakan rumus deksriptif persentase (DP) sebagai berikut.

$$\sum = \frac{N}{n} \times 100\%$$

Keterangan:

N = Skor diperoleh

n = Skor seharusnya

Berdasarkan rumus tersebut dapat ditafsirkan dengan kriteria penilaian sebagai berikut.

Tabel 3. Rentangan Kriteria Penafsiran

Interval (%)	Kriteria
75,01 – 100,00	Sangat baik
50,01 – 75,00	Baik
25,01 – 50,00	Cukup baik
1,00 –25,00	Kurang baik

HASIL DAN PEMBAHASAN

Bab ini diketengahkan mengenai hasil penelitian yang telah dilakukan dilanjutkan pembahasan sebagai bentuk diskusi dari hasil temuan penelitian.

Hasil Penelitian

SIKAPEG merupakan sistem informasi yang dirancang untuk memberikan solusi dalam menangani berbagai hal terkait dengan kepegawaian mulai dari penyimpanan dan pemusatan data pegawai secara komputerisasi hingga menangani berbagai macam laporan kepegawaian di IVET. Berdasarkan hasil wawancara dengan Kepala Kepagawaian dan Kepala Unit TIK diperoleh gambaran sebagai berikut.

Tabel 4. *Security Policies*/Kebijakan Keamanan

A.5. *Security Policies*
A.5.1. *Information Security Policy/Kebijakan Keamanan Informasi*
Objektif:
Mengarahkan manajemen dan dukungan keamanan informasi disesuaikan kebutuhan bisnis dan hukum yang relevan.
Kontrol:
1.Informasi mengenai dokumen kebijakan keamanan
2. Review tentang kebijakan keamaan informasi

Tabel di atas, kebijakan keamanan berguna untuk memberikan arahan manajemen dan dukungan pada keamanan informasi sesuai kebutuhan lembaga dan aturan di IVET. Kebijakan sudah berjalan cukup baik, karena telah tercatat pada aturan kepegawaian IVET 2017 sebagai dokumen kebijakan oleh Pimpinan IVET meski belum sesuai tuntutan ISO 27001:2013.

Tabel 5. *Organisation of Information Security*/ Organisasi Keamanan Informasi

A.6. *Organisation of Information Security*
A.6.1. *Internal Organization*/Organisasi Internal
Objektif:
Mengelola keamanan informasi dalam organisasi
Kontrol:
1. Komitmen manajemen terhadap keamanan informasi
2. Informasi koordinasi keamanan
3. Alokasi informasi dan taggung jawab keamanan
4. Proses otorisasi untuk fasiitas pengolahan informasi
5. Perjanjian kerahasiaan
6. Kontak dengan otoritas
7. Kontak dengan kelompok minat khusus
8. Ulasan independent informasi keamanan

Organisasi keamanan informasi berfungsi mengelola keamanan informasi telah ada dan berjalan baik. Kontrol ini dilakukan oleh Unit TIK yang bertugas mengelola keamanan SIKAPEG. Selama ini keamanan informasi hanya menjadi tanggungjawab Unit TIK, ini yang menjadikan kelemahan. Penerapan aturan keamanan khusus SIKAPEG hanya disampaikan secara lisan dan belum terdokumentasikan/tertulis.

Tabel 6. Kebijakan Eksternal

A.6.*Organization of Information Security*
A.6.2. *External Parties*/Pihak External
Objektif:
Menjaga keamanan informasi dan pengolahan informasi fasilitas organisasi yang diakses, diolah, dikomunikasikan kepada, atau dikelola oleh pihak ketiga.
Kontrol:
1. Identifikasi risiko berhubungan dengan pihak eksternal
2. Mengatasi keamanan ketika berhadapan dengan pelanggan
3. Mengatasi keamanan dalam perjanjian pihak ketiga

Kontrol ini sudah dilakukan sangat baik, telah terdokumentasi/tertulis bahwa adanya pihak ketiga yang ikut dalam menjaga keamanan informasi. Bukti tertulis itu dilakukan melalui perjanjian (MoU) diawal dengan pihak pemberi sewa server/vendor.

Tabel 7. *Human Resouurce Security* (Keamanan SDM)

A.7. *Human Resources Security*/Keamanan Sumber Daya Manusia
A.7.1. *Priorto Employment*/Sebelum Bekerja
Objektif:
Memastikan bahwa karyawan, kontraktor dan pengguna pihak ketiga memahami tanggung jawabnya, dan perannya pantas untuk dipertimbangkan sebagai langkah untuk mengurangi risiko pencurian, penipuan atau penyalahgunaan fasilitas.
Kontrol:
1. Peran dan tanggung jawab
2. Screening
3. Syarat dan ketentuan dari e*mployment*

Terkait kepastian bahwa pegawai dan pengguna ketiga memahami tanggung jawab dan perannya serta mengurangi risiko pencurian, penipuan dan penyalahgunaan, kontrol ini telah dilakukan cukup baik. Setelah adanya sistem *reward* pegawai cukup antusias melakukan sidik jari meski masih ada pegawai yang hadir tidak tepat waktu. Sudah ada dokumen tentang peran dan tanggung jawab dari setiap unit/personal, tetapi job deskripsi serta rincian penggunaan dan manfaat dari fasilitas informasi pada setiap unit belum dirinci secara detail, sehinggga bila ada hambatan atau kerusakan data masih menjadi tanggung jawab lembaga, yaitu Kepala Unit TIK. Hal ini menjadikan setiap unit tidak memiliki tanggung jawab terhadap pencurian data dan hambatan dalam penggunaan informasi dari unit tersebut.

Tabel 8. *Asset Management*/Menejemen Aset

A.8. *Asset Management*/Menejemen Aset
A.8.1. *Responsibility for Assets*
Objective:
Mencapai dan mempertahankan perlindungan aset organisasi
Kontrol:
1. Identifikasi aset secara jelas dan inventarisasi semua aset penting dibuat dan dipelihara
2. Aset yang terkait dengan fasilitas informasi, harus 'dimiliki' oleh bagian yang ditunjuk organisasi
3. Penggunaan informasi dan aset yang terikat dengan fasilitas informasi, harus diidentifikasi, didokumentasikan, dan diimplementasikan

Kontrol ini telah dilakukan cukup baik, inventarisasi aset *hardware* oleh Kepala Kepegawaian berkoordinasi dengan Kepala Rumah Tangga yang mencatat dan mendokumentasikan sehingga terbentuk daftar inventarisasi sebagai laporan. Inventarisasi aset *software* oleh Unit TIK, tetapi tidak dilakukan *realtime/update*. Penyajian daftar inventaris juga belum disajikan pada setiap ruang.

Tabel 9. *Acces Control*/Kontrol Akses

A.9. *Acces Control*/Kontrol Akses

Objektif:
Mengontrol akses ke informasi
Kontrols:
1. Kebijakan pengendalian akses

Kontrol ini sudah dilaksanakan baik. Kebijakan pengendalian hak akses telah dilakukan Kepala Unit TIK sebagai penanggung jawab organisasi yang mengelola keamanan SIKAPEG. Ka.Unit TIK dan Ka. Unit Kepegawaian diberikan kebijakan pengendalian hak akses dengan *username* dan *password* khusus sebagai admin untuk men-*download* data kehadiran pegawai yang digunakan sebagai bahan laporan kehadiran bulanan. Penggantian *username* dan *password* khusus dikembalikan ke masing-masing *user*, pegawai hanya bisa menggunakan maksimal 3 (tiga) sidik jari sebagai ID kehadiran. Mesin akan menolak sidik jari yang sama dengan ID berbeda, tetapi kebijakan kewenangan hak akses masih terkait dengan tugas dan kebutuhan lapangan serta belum terdokumentasi secara tertulis.

Tabel 10. *Pysical and Environmental Security*/ Keamanan Fisik dan Lingkungan

A.11. *Physical and Environmental Security*/ Keamanan Fisik dan Lingkungan
Objektif:
Mencegah akses tanpa ijin, kerusakan dan gangguan tempat dan informasi organisasi.
Kontrol:
1. Parameter keamanan fisik
2. Kontrol entri fisik
3. Mengamankan kantor, kamar dan fasilitas
4. Melindungi terhadap ancaman eksternal dan lingkungan
5. Bekerja di daerah aman
6. Akses publik, pengiriman dan pemuatan

Mencegah akses yang tidak sah terhadap kerusakan dan gangguan informasi organisasi telah dilakukan IVET dari keamanan secara fisik, kontrol fisik, dan pengamanan fasilitas yang dimiliki. Kontrol ini sudah dilakukan baik, mesin presensi sidik jari terletak di berbagai tempat yang mudah dijangkau. Ada 2 (dua) mesin kehadiran sidik jariyaitu di luar gedung A dan di dalam gedung E, serta mesin presensi wajah yang berada di dalam gedung A. Meski mesin sidik jari yang terletak di depan gedung A mudah dijangkau, hanya peletakan mesin berada di luar gedung kurang aman dari ancaman pihak eksternal (kejahatan) karena memberikan peluang untuk sabotase alat dan bila terjadi hujan badai terancam basah dan rusak. Peletakkan mesin kehadiran wajah berada di tempat yang sering dilewati pegawai, sehingga pegawai harus berhati-hati bila tanpa sengaja wajah terekam mesin, karena pegawai akan terdata meninggalkan kantor meskipun masih jam kerja. Tempat penyimpanan data/CPU aman, karena berada dalam ruang dengan pemegang kunci terpusat di BAU. Sisi lain tidak tersedia (baca: belum) alat pemadam kebakaran/APAR, ini sangat berbahaya jika terjadi kebakaran. CCTV yang dimiliki IVET tidak berfungsi baik, CCTV banyak rusak dan penempatannya kurang strategis menjadikan tidak berfungsi sebagaimana mestinya. Tidak adanya CCTV yang mengarah pada mesin kehadiran sidik jari di sekitar gedung A (Rektoriat), gedung E, di sekitar TV monitor untuk penayangan laporan kehadiran secara *online* yang terpasang di lobby/*costumer service* dan ruang tempat penyimpanan data/CPU, sehingga bila ada tindak kriminal akan mengalami kesulitan untuk dilacak karena tidak adanya bukti rekaman peristiwa. Mesin kehadiran sidik jari, CPU, monitor pernah *error*/rusak pada waktu 3 (tiga) tahun terakhir, tetapi dapat diatasi dengan *hardware* cadangan. Pemeliharan *software* dan *hardware* serta aset pendukung lain dilakukan baik secara periodik, berkala maupun insidental. Insidental dilakukan ketika ada laporan dari setiap Kepala Unit Jurusan/Fakultas, secara periodik dilakukan pada setiap bulan, dan berkala dilakukan selama satu semester/enam bulan. Tindakan

sudah dilakukan dengan baik, sebab setiap tindakan ada laporan dari penanggung jawab kepada pimpinan yang juga dibuktikan laporan setiap tindakan di kartu kontrol yang terpasang di ruang lengkap dengan barang yang dilakukan tindakan. Data kehadiran di-*backup* setiap bulan dan *auto backup* setiap hari. Hanya terdapat satu genset yang cukup digunakan di 1 (satu) gedung A/Rektorat). *Software* yang digunakan asli beralamat di http://kehadiran.ivet.ac.id. Sistem berjalan sesuai standar dan masih dapat digunakan dalam waktu panjang. Namun permasalahan dan kelemahan yang pernah muncul tidak terdokumentasi, sehingga tidak dapat digunakan sebagai bahan evaluasi ke depan.

Tabel 11. *Operations Security*/Keamanan Operasional

A.12. *Operations Security*/Keamanan Operasional
A.12.1.*Operational Procedures&Responsibilities*
Objektif:
Memastikan informasi kegiatan operasi dan organisasi aman
Kontrol:
1. Prosedur operasi yang didokumentasi
2. Merancang manajemen
3. Kapasitas manajemen
4. Pengembangan, pengujian. dan operasional lingkungan

Kontrol ini sudah dilaksanakan cukup baik. Sudah ada prosedur operasi dalam penggunaan kehadiran sidik jari, tetapi belum ada prosedur operasi penggunaan SIKAPEG. Prosedur penyimpanan aset sudah ada dan dilakukan cukup baik, karena semua kegiatan yang akan dilakukan ke depan direncanakan terlebih dahulu secara tertulis diawali dengan rapat kebutuhan. Perancangan manajemen sudah ada dalam renstra (rencana dan strategi), tetapi pengembangannya belum dilakukan

Tabel 12. *Communications Security*/Keamanan Komunikasi

A.13. *Communications Security*/Keamanan Komunikasi
A.13.1.*Network Security Management*/Manajemen Keamanan Jaringan
Objektif:
Memastikan perlindungan informasi dan fasilitas informasi pendukungnya.
Kontrol:
1. Kontrol jaringan
2. Pengamanan layanan jaringan
3. Segregasi dalam jaringan

Perlindungan informasi dan fasilitas informasi pendukung sudah dilakukan baik melalui kontrol jaringan dan pengamanan jaringan yang ketat. Kontrol ini sudah dilakukan baik, yaitu sebulan sekali tanpa ada kepastian waktu pelaksanaan. Manajemen keamanan jaringan menggunakan pergantian *password* yang dilakukan Kepala Unit TIK. Hal ini dilakukan antisipasi bila *password* dilacak oleh pihak lain berakibat pada pencurian dan perusakan data. Sudah ada pemisah/segregesi dalam jaringan. Dalam 1 (satu) tahun terakhir ± 2 (dua) kali terjadi kerusakan jaringan. Wifi pernah tersambar petir ± 4 (empat) kali pada saat musim hujan. Perbaikan jaringan terdokumentasi dalam foto dan email.

Tabel 13. *System Acquistion, Development and Maintenance*/Akuisisi Sistem, Pengembangan dan Pemeliharaan

A.14. *System Acquisition, Development and Maintenance*
A.14.1. *Security Requirements of Information System* /Aturan Sistem Keamanan Informasi
Objektif:
Memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi, sebagai syarat dalam penyediaan layanan melalui jaringan publik.
Kontrol:
1. Analisis dan spesifikasi kebutuhan keamanan informasi
2. Mengamankan layanan jaringan publik
3. Melindungi transaksi layanan aplikasi

Kontrol keamanan informasi sebagai bagian integral dari sistem informasi sudah dilakukan baik. Analisis kebutuhan

keamanan informasi belum ada, tetapi spesifikasi kebutuhan keamanan informasi sudah ada. Tahun 2017 sistem pernah terkena virus sehingga menghambat kinerja sistem. Seiring perjalanan waktu dilakukan perbaikan, saat ini sudah ada bentuk pengaman dalam layanan jaringan publik dengan dilakukan pergantian *password* sesuai kebutuhan dan *mantainance* dengan cara mengontrol pada fasilitas jaringan. Upaya pencegahan dari serangan *hacker* dengan pemanfaatan *firewall*, *setting file permission* sudah sesuai kebutuhan dan prinsip keamanan, yaitu dilakukan *backup data base* dan data aplikasi rutin harian/mingguan/bulanan. Cara melindungi transaksi layanan dilakukan *scanning* atau pembersihan sistem pada setiap kegiatan dan awal pengoperasioan program. Kegiatan ini tidak terdokumentasi, karena telah dilakukan secara rutin, sehingga keseluruhan telah dilakukan baik, tetapi belum ada aturan *mantainance* aset *software* dan *hardare*.

Tabel 14. *Information Security Incident Management/*Manajemen Insiden Keamanan Informasi

A.16. *Information Securty Incident Management*
A.16.1. *Management of Information Security Incidentand Improvement* Manajemen Keamanan Informasi dan Perbaikan
Objektif:
Memastikan pendekatan yang efektif terhadap manajemen keamaan informasi, keamanan dan kelemahan komunikasi
Kontrol:
1. Tanggung jawab dan prosedur
2. Melaporkan kejadian keamanan informasi
3. Melaporkan kejadian keamanan informasi
4. Mengarahkan dan memutuskan prosedur keamanan informasi
5. Penilaian dan keputusan tentang kejadian keamanan informasi
6. Belajar dari kejadian yang mengancam keamanan informasi
7. Kumpulan bukti

Kontrol ini dilakukan kurang baik, karena tidak ada tanggung jawab dan prosedur manajemen keamanan informasi. Sampai saat ini belum ada pelaporan kejadian keamaan informasi dan bentuk pelaporan kelemahan. Pimpinan tidak pernah (baca: belum) memberikan arahan dan memutuskan prosedur keamanan informasi. Bila terjadi *error*/permasalahan pada SIKAPEG, misalnya: mesin kehadiran rusak, tidak bisa mendeteksi, SIKAPEG tidak bisa diakses, sistem hang, jaringan tidak stabil, admin melaporkan ke Kepala Unit TIK. Oleh teknisi dilakukan penanganan perbaikan, namun bila kerusakan membutuhkan perbaikan hingga mengganti alat, Ka.Unit TIK melakukan klasifikasi parameter kerusakan kemudian dilaporkan ke pimpinan dan diajukan dana untuk perbaikan/pergantian. Bentuk penilaian dan keputusan tentang kejadian bersifat keamanan informasi belum ada. Sudah ada bentuk pembelajaran dari kejadian yang mengancam keamanan informasi dengan cara perbaikan sesuai kebutuhan. Tidak ada bukti pelaporan kelemahan keamanan informasi terdokumen, maka tidak dapat digunakan sebagai bentuk evaluasi mendatang.

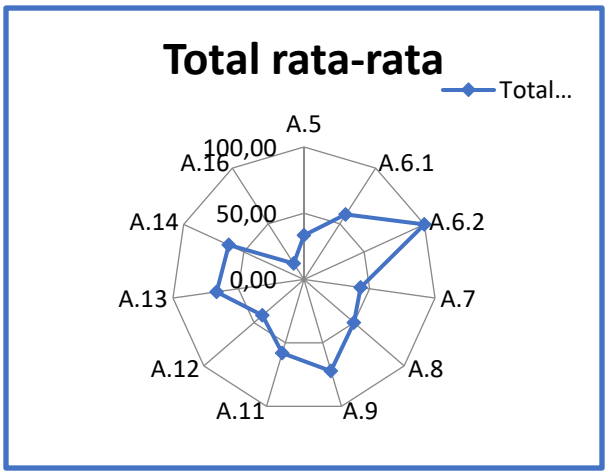
Berdasarkan analisis data hasil penelitian dari 10 area kontrol dapat direkap pada tabel berikut.

Tabel 15. Rekap Keseluruhan Tindakan Area Kontrol

Kontrol	Rata-Rata	Keterangan
A.5. *Security Policies*	33.33	Cukup Baik
A.6. *Organisation of Information Security*		
A.6.1. *Internal Organization*	58,33	Baik
A.6.2. *External Parties*	100.00	Sangat Baik
A.7. *Human Resources Security*	43.14	Cukup Baik
A.8. *Asset Management*	50.00	Cukup Baik
A.9. *Access Control*	72.22	Baik
A.11. *Physical and Environmental Security*	58.06	Baik
A.12. *Operations Security*	41.67	Baik
A.13. *Communications Security*	66.67	Baik
A.14. *System*	62.50	Baik

Acquisition, Development And Maintenance		
A.16. *Information Security Incident Management*	14.29	Kurang Baik

Berdasarkan rekap tabel di atas dapat diperjelas dengan bentuk gambar grafik *line* berikut.



Gambar 1. Grafik *line* Rekap Keseluruhan Tindakan Area Kontrol

Rekapan tabel dan grafik di atas memberikan gambaran bahwa ancaman sistem informasi dalam SIKAPEG IVET meliputi: (1) pencurian data (data *theft*), yaitu adanya akses *database* dari orang yang tidak berwenang berakibat hilangnya hasil informasi, (2) penggunanan sistem secara ilegal, yaitu orang yang tidak berhak mengakses informasi untuk data seperti terjadinya kasus penipuan pihak eksternal dengan mengirimkan pesan singkat ke salah satu dosen IVET yang meminta pengiriman/ transfer uang untuk *workshop* ke pimpinan namun ternyata informasi tidak benar dan ternyata sebagai tindak penipuan, (3) penghancuran data secara ilegal, yaitu perusakan data/informasi dan membuat berhentinya sistem operasi komputer, (4) pemodifikasian ilegal, yaitu perubahan data dan perangkat lunak secara tidak disadari, karena terdapat perubahan data dan perangkat lunak yang disebabkan oleh program aplikasi yang merusak (*malicious software*) seperti virus, (5) sabotase mesin kehadiran sidik jari dan sistem, (6) kegagalan sistem, seperti pemadaman atau tegangan listrik (*voltase*) tidak stabil dapat membuat peralatan menjadi rusak dan terbakar, (7) human *error*, yaitu kesalahan pengoperasian sistem, (8) bencana alam, seperti: kebakaran, dan hujan badai.

Diskusi

Berdasarkan hasil wawancara dengan kepala unit TIK mengacu ke-10 area kontrol dan di-*crosschek*-kan dengan kepala kepegawaian dapat diketahui bahwa kebijakan keamanan SIKAPEG di IVET termasuk kriteria baik, hasil konsultasi dengan SMKI sebagai tolak ukur diperoleh kriteria mungkin. Kemungkinan ini bisa dijelaskan bahwa sistem memiliki peluang mengalami kerusakan antara 10-50% akan terjadi pada periode waktu satu (1) tahun, jika dikaitkan dengan skala *Likelihood* termasuk kriteria ringan. Kriteria ini karena gangguan terhadap aplikasi/jaringan sistem tidak berfungsi > 1–4 jam selama jam kerja dan keluhan user disampaikan oleh sejumlah pengguna. Hal ini terjadi sebab IVET belum memiliki server besar memuat seluruh rangkaian sistem komputerisasi dan masih menyewa kepada vendor. Penyewaan ini didukung hasil wawancara dengan Kepala Unit TIK bahwa: "Sebenarnya SIKAPEG lebih aman diakses secara lokal karena tidak dibuka oleh publik, sehingga data daftar hadir tidak dibaca pihak lain, tetapi karena selama ini IVET tidak memiliki UPS data *center* dengan kapasitas data memadai, maka di-*online*-kan dengan menyewa server pada vendor (Wawancara Degha, 2017).

Organisasi keamanan informasi dengan berbagai indikator yang mengupasnya diperoleh kriteria baik, hail ini karena dalam pemanfaatan jaringan telah dilakukan kerjasama pihak Kepala Unit TIK dengan Kepala Kepegawaian dan juga dengan Kepala Rumah Tangga. Terkait

dengan SDM juga telah ditempatkan person-person sesuai bidangnya. Misalnya kepala bagian/unit ditempatkan berdasarkan basis ijazah yang dimiliki/S1, bahkan untuk Kepala Unit TIK lulusan S2 bidang keahlian TIK.

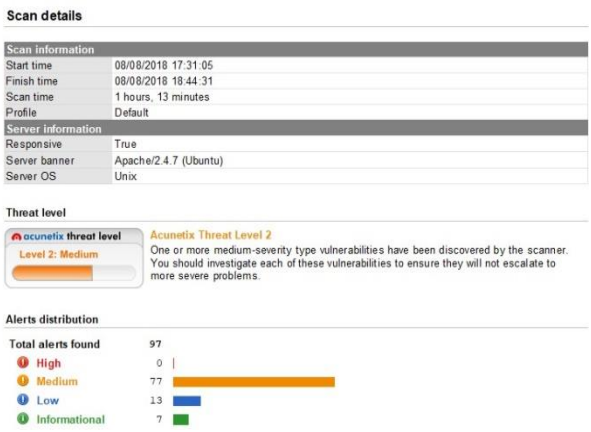
Terkait dengan aset manajemen telah dilakukan inventarisasi cukup baik, dan dilakukan secara menyeluruh juga pelaporan kepada atasan. Bukti lain dapat diketahui, Kepala Rumah Tangga membuat daftar inventarisasi pada setiap ruang, meskipun beberapa ruang belum tarpasang. Terkait dengan kontrol akses, telah dilakukan dengan baik. Hal itu dilakukan perubahan *password* sesuai kebutuhan (periodik dan berkala), karena merupakan hak setiap *user*, *maintanance* meski waktu pelaksanaan tidak tetap. Pengalaman masa lalu menjadikan perubahan *password* dilakukan secara rutin. Hal itu didukung hasil wawancara dengan Dhega (2017): "Satu pegawai bisa memilik 4 (empat) sidik jari dari pegawai lain namun dengan ID satu pegawai, sehingga pegawai dengan mudah melakukan celah kecurangan, yaitu jika salah satu pegawai tidak masuk bisa diabsenkan oleh pegawai lain yang sidik jarinya telah terekam di mesin sebagai ID yang sama. Solusi dilakukan dengan reset data atau perekaman ulang data sidik jari maksimal 3 sidik jari setiap pegawai, selanjutnya adanya migrasi *database* dari server kantor ke server pusat (vendor). Tindakan penggantian *password* pada periode tertentu, perawatan dan pemeliharaan secara periodik dan berkala tidak hanya dilakukan pada pengamanan pada SIKAPEG saja, tetapi juga sekaligus sebagai antisipasi pencurian dan perusakan data terkait keamanan fisik, keamanan pengoperasian, keamanan jaringan, pengembangan ke depan, dan keamanan informasi serta perbaikan.

Kesuluruhan diskusi ditemukan bahwa ancaman keamanan SIKAPEG IVET termasuk kriteria medium. Hal ini didukung dari proses audit *software* menggunakan *Tools Acunetix*, yaitu web audit *software* yang berfungsi untuk men-*scan* kelemahan web. Hasil analisis termasuk level rentan berdasar *Common Vulnerability Scoring System (CVSS)* seperti tersaji pada tabel berikut.

Tabel 16. *Qualitative Severety Rating Scale*

Level/Rating	CVSS Score
None	0.0
Low	0.1 – 3.0
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

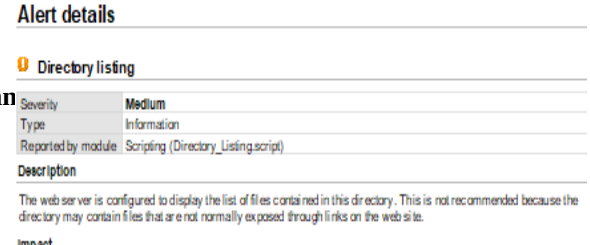
Uraian di atas dapat dikonfirmasikan dengan pengukuran atau *scanning* pada SIKAPEG pada alamat *http://kehadiran.ivet.ac.id*. Pengukuran diperoleh hasil bahwa *Acunetix* mendeteksi 97 jenis *total alerts found* (total tanda ditemukan) terdiri dari 77 jenis yang bertipe *medium*, 13 *low* dan 7 *Informational* kategori *Threat Level 2 (medium)*, seperti tersaji pada gambar berikut



Gambar 2. Hasil *Scanning* SIKAPEG

Berikut disajikan repot hasil *scanning* SIKAPEG menggunakan *Tools Acunetix*: kategori medium dengan 77 jumlah jenis kerentanan, mulai dari skor 4,0 – 6,9.

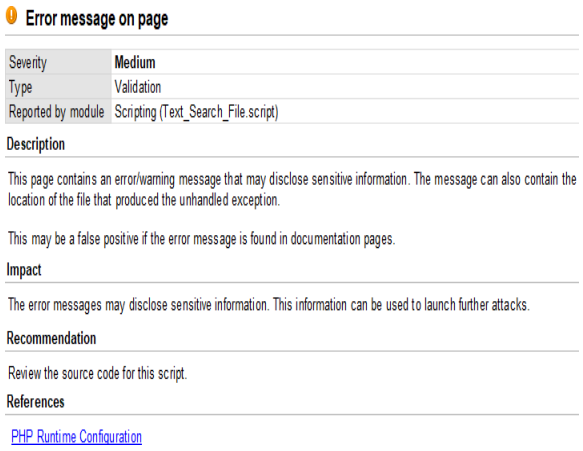
Directorylisting/Daftar Direktori



Gambar 3. *Alert Details Directory Listing*

Gambar di atas menjelaskan bahwa *web server* dikonfigurasi untuk menampilkan daftar file yang ada di *directory*. Ini tidak disarankan, karena *directory* mungkin berisi file yang tidak biasanya diekpos melalui *link* di website ini. Dampaknya pengguna dapat melihat semua file di *directory* yang mungkin terdapat informasi sensitif. Rekomendasi, untuk pastikan *directory* tidak memiliki informasi sensitif atau membatasi daftar *directory* dari konfigurasi web server.

Error Message on Page


Error message on page

Severity	Medium
Type	Validation
Reported by module	Scripting (Text_Search_File.script)

Description

This page contains an error/warning message that may disclose sensitive information. The message can also contain the location of the file that produced the unhandled exception.

This may be a false positive if the error message is found in documentation pages.

Impact

The error messages may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Review the source code for this script.

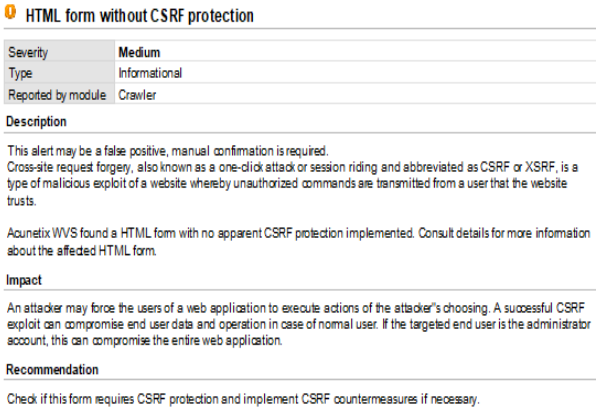
References

PHP Runtime Configuration

Gambar 4. *Error Message on Page*

Gambar diatas menjelaskan halaman ini berisikan pesan peringatan yang dapat membuka info sensitif, selain pesan juga menyajikan lokasi file tersebut. Dampaknya, *error massage* dapat membuka informasi sensitif, informasi dapat digunakan untuk menyerang. Rekomendasinya adalah *sourcode* perlu di *review*.

HTML form Without CRFS Protection


HTML form without CSRF protection

Severity	Medium
Type	Informational
Reported by module	Crawler

Description

This alert may be a false positive, manual confirmation is required.
Cross-site request forgery, also known as a one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website whereby unauthorized commands are transmitted from a user that the website trusts.

Acunetix WVS found a HTML form with no apparent CSRF protection implemented. Consult details for more information about the affected HTML form.

Impact

An attacker may force the users of a web application to execute actions of the attacker"s choosing. A successful CSRF exploit can compromise end user data and operation in case of normal user. If the targeted end user is the administrator account, this can compromise the entire web application.

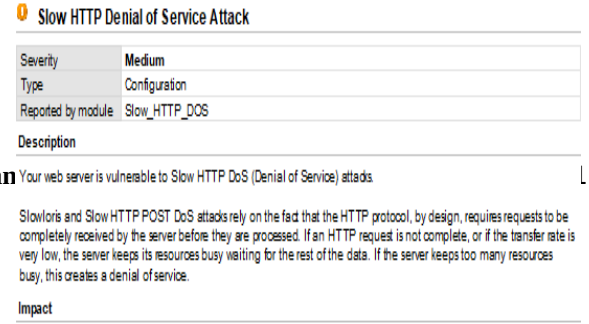
Recommendation

Check if this form requires CSRF protection and implement CSRF countermeasures if necessary.

Gambar 5. *HTML form Without CRFS Protection*

Gambar di atas menjelaskan terdapat peringatan buruk, dibutuhkan konfirmasi manual. *Cross-site* dapat menimbulkan *request* palsu atau disebut *one-click attack*/serangan satu klik atau *session ridding* (cara untuk menyimpan informasi) dan CSRF or XSRF tipe serangan dari eksploit (kumpulan *coding* program untuk menyerang web) terhadap *website*, yaitu program yang ditransmisikan kepada *user* yang dipercayai oleh pengguna tersebut. Acunetix WVS menemukan HTML tidak memiliki perlindungan pada CSRF. Dampaknya, penyerang kemungkinan akan memaksa pengguna halaman web untuk memilih sesuatu yang diinginkan penyerang. Serangan CSRF *exploit* dikatakan berhasil bila dapat menguasai seluruh akun pengguna tanpa disadari. Jika targetnya administrator, maka seluruh halaman web menjadi dibawah kekuasaannya. Rekomendasi, chek apakah ada fitur memerlukan perlindungan CSRF dan implementasikan tindakan CSRF jika diperlukan.

Slow HTTP Deniel of Service Attack


Slow HTTP Denial of Service Attack

Severity	Medium
Type	Configuration
Reported by module	Slow_HTTP_DOS

Description

Your web server is vulnerable to Slow HTTP DoS (Denial of Service) attacks.

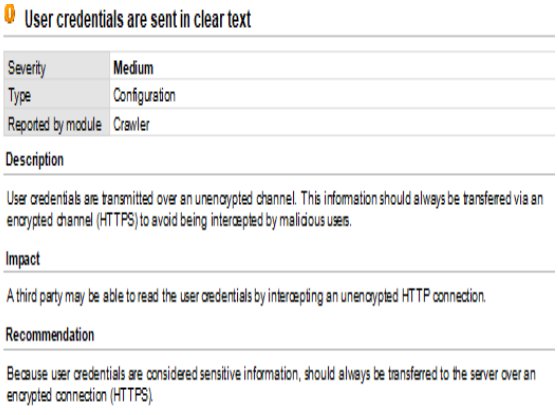
Slowloris and Slow HTTP POST DoS attacks rely on the fact that the HTTP protocol, by design, requires requests to be completely received by the server before they are processed. If an HTTP request is not complete, or if the transfer rate is very low, the server keeps its resources busy waiting for the rest of the data. If the server keeps too many resources busy, this creates a denial of service.

Impact

Gambar 6. *Slow HTTP Deniel of Service Attack*

Gambar di atas menjelaskan bahwa web server terlalu rentan ada serangan *Slow HTTP DoS*. Serangan *Slow HTTP DoS* tergantung fakta protokol HTTP. Secara desain membutuhkan permintaan agar diterima server sebelum diproses. Dampaknya, satu mesin dapat merusak mesin web server lain dengan bandwith minimal dan efek samping pada servis serta port yang tidak berkaitan. Rekomendasi, konsultasikan web referensi tentang informasi perlindungan web server melawan server tersebut.

User Credentials are Sent in Clear Text


User credentials are sent in clear text

Severity	Medium
Type	Configuration
Reported by module	Crawler

Description

User credentials are transmitted over an unencrypted channel. This information should always be transfered via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.

Impact

A third party may be able to read the user credentials by intercepting an unencrypted HTTP connection.

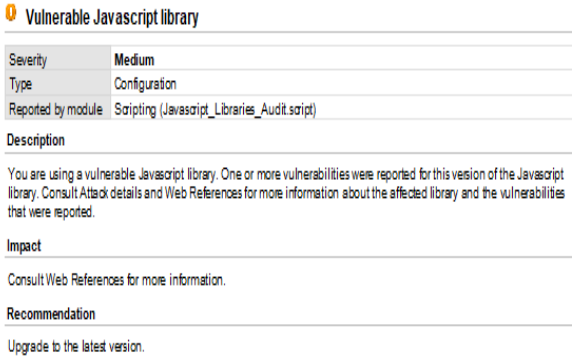
Recommendation

Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).

Gambar 7. *User Credentials are Sent in Clear Text*

Gambar di atas menjelaskan bahwa *user credentials* (surat mandat pengguna) dikirim melalui saluran yang tidak terenkripsi. Semua informasi harus selalu ditransfer melalui saluran terenkripsi (HTTPS) untuk menghindari agar tidak disadap pengguna yang jahat. Dampaknya, pihak ketiga mungkin dapat membaca *user credentials* dengan memotong koneksi HTTP yang tidak terenkripsi. Rekomendasi, karena *user credentials* dianggap sebagai informasi sensitif, informasi harus selalu ditransfer ke server melalui koneksi yang terenkripsi (HTTPS).

Vulnerable Javascript Library


Vulnerable Javascript library

Severity	Medium
Type	Configuration
Reported by module	Scripting (Javascript_Libraries_Audit.script)

Description

You are using a vulnerable Javascript library. One or more vulnerabilities were reported for this version of the Javascript library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult Web References for more information.

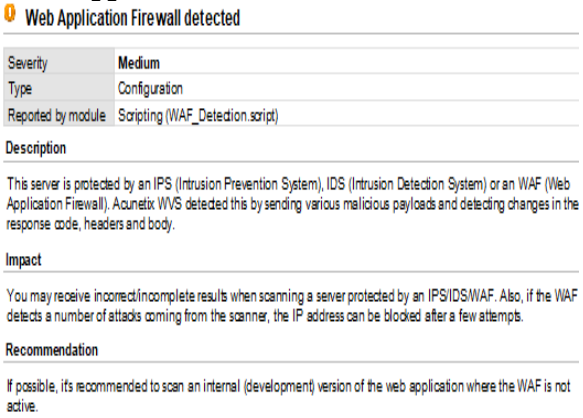
Recommendation

Upgrade to the latest version.

Gambar 8. *Vulnerable Javascript Library*

Gambar di atas menjelaskan bahwa *user* menggunakan *Java Script Library* yang rentan. Konsultasikan detail serangan dan referensi web untuk informasi lebih lanjut tentang perpustakaan yang terkena dampak dan kerentanan yang dilaporkan. Dampaknya terjadi, konsultasikan referensi web untuk informasi lebih lanjut. Rekomendasi, tingkatkan ke versi terbaru.

Web Application


Web Application Firewall detected

Severity	Medium
Type	Configuration
Reported by module	Scripting (WAF_Detection.script)

Description

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix WVS detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Gambar 9. *Web Application*

Gambar di atas menjelaskan bahwa server dilindungi oleh IPS (*Intrusion*

Prevention System/Intruksi Sistem Pencegahan) atau WAF (*Web Application Firewall)*. Acunetix WAF ini mampu mendeteksi dengan mengirimkan berbagai macam *payloads* (efek yang ditimbulkan serangan virus jahat yang dapat mendeteksi perubahan dalam kode respon, *heade*r dan *body*). Dampaknya, akan mendapatkan hasil yang tidak lengkap jika men-*scan* server yang dilindungi IPS, IDS/WAF. Jika WAF mendeteksi beberapa serangan dari *scanner*, IP *address* dapat di blok. Rekomendasi, jika memungkinkan men-*scan* versi internal dari aplikasi web, yaitu WAF tidak aktif. Berikut tabel rekap laporan celah keamanan yang ditemukan menggunakan *Tolls Acunetix*.

Tabel 17. Celah Keamanan dan Level Kerentanan

No.	Celah Keamanan	*Severity* (Level)
1	*Directory listing*	*Medium*
2	*Error message on page*	*Medium*
3	*HTML form without CRFS protection*	*Medium*
4	*Slow HTTP Denialof Service Attack*	*Medium*
5	*User credentials are sent in clear text*	*Medium*
6	*Vulnerable Java script library*	*Medium*
7	*Web Application*	*Medium*
8	*Click jacking: X-Frame-Options headre missing*	*Low*
9	*Cookie without Http Only flag set*	*Low*
10	*Options method is enabled*	*Low*
11	*Possible relative path over write*	*Low*
12	*Possible sensitive directories*	*Low*
13	*Possible sensitive files*	*Low*
14	*Possible virtual host found*	*Low*
15	*Slow response time*	*Low*
16	*Broken links*	*Informational*
17	*Email address found*	*Informational*
18	*Error page web server version diclosure*	*Informational*
19	*Password type input with auto-complete enabled*	*Informational*
20	*Possible user name or password diclosure*	*Informational*

Seluruh urain diatas menunjukkan hasil penelitian ini memberikan rekomendasi tentang mengurangi celah tindakan kriminal dari orang-orang yang tidak bertanggung jawab dan juga memberikan solusi terkait dengan perusakan data/informasi sebagai akibat kesalahan manusia atau *humen error* selain sebab-sebab dari gejala alam.

PENUTUP

Bab ini dibagi kedalam 2 (dua) sub bab, yaitu sub bab simpulan yang diperoleh dari pelaksanaan penelitian dan saran yang diharapkan dapat digunakan sebagai bahan rekomendasi.

Simpulan

Berdasar hasil analisis data, sistem keamanan Sistem Informasi Kehadiran Pegawai IVET belum memenuhi standar ISO 27001:2013, beberapa sudah dilaksanakan namun belum seluruhnya dilakukan dengan baik. Terjadinya ancaman termasuk kriteria mungkin terjadi, ini jika dilihat dari indikator kemungkinan terjadinya ancaman pada rentang antara 10-50% dalam waktu 1 (satu) tahun dan jika dikaitkan dengan skala *Likelihood* termasuk kriteria ringan, terutama gangguan terhadap aplikasi/jaringan. Kelemahan terletak tidak adanya tanggung jawab dan prosedur manajemen keamanan informasi. Bentuk ancaman dan kelemahaman itu: (1) pimpinan tidak pernah (baca: belum) memberikan arahan dan memutuskan prosedur keamanan informasi, (2) bukti pelaporan kelemahan keamanan informasi tidak terdokumentasi sehingga tidak bisa digunakan sebagai evaluasi ke depan, (3) kurangnya kesadaran pegawai dalam melakukan presensi sidik jari, secara bersama menjaga dan memelihara *hardware* pendukung. Solusinya adalah,

dilakukan kontrol baik secara periodik maupun berkala, selain adanya perawatan dan pemeliharaan menyeluruh serta terdokumentasikan setiap kegiatan pada kontrol sistem.

Saran

Saran diperuntukkan bagi 3 (tiga) pihak, yaitu bagi pimpinan, bagi pegawai, dan peneliti mendatang.

Bagi pimpinan; sebaiknya pimpinan tegas dalam menetapkan aturan kepegawaian, baik penetapan *reward* maupun *punishment*, standar kerja, pembenahan sarana dan prasarana dengan SOP-nya, perawatan dan pemeliharaan barang dengan inventarisasi serta terdokumentasikan sesuai tuntutan ISO 27001: 2013, dan sebaiknya SIKAPEG hanya di-*online*-kan pada jaringan lokal IVET sehingga tidak memberikan peluang pihak yang tidak bertanggung jawab untuk menyabotase data.

Bagi pegawai; standar penggunaan sarana dan prasarana kerja serta keamanan telah ditetapkan pimpinan, namun masih ada beberapa pegawai yang belum memiliki komitmen melaksanakan tugas sesuai tanggung jawabnya. Disarankan kepada para pegawai IVET untuk melaksanakan hasil pembinaan dari pimpinan baik secara periodik maupun berkala, sehingga dalam memberikan layanan kepada publik sesuai standar ISO 27001:2013.

Bagi peneliti mendatang; penelitian masih terbatas dilakukan di IVET Semarang, disarankan untuk peneliti mendatang memodifikasi area kontrol dengan variabel atau faktor lain agar diperoleh hasil penelitian lebih bervariatif dan lebih serta ditemukannya teori atau konsep-konsep baru.

DAFTAR PUSTAKA

Aprian. R. Rizal S & Sobri. M. 2015. Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar ISO 27001:2013, *Jurnal Informatika* Universitas Bina Darma Palembang, digilib.binadarma.ac.id

Castro. Placida Rodal. 2016. *Implementasi Plan for an ISMS according to ISO/IEC 27001:2013*, Universitat Obertade Catalunya: Information Security Management System.

Darmawan. Yohanes. 2017. *Analisis Tata Kelola Keamanan Laboraturium Fakultas Teknologi Informasi Universitas Kristen Satya Wacana Menggunakan Standart ISO 27001:2013*. Salatiga

ISACA. 2016. *Comparisonof PCI DSS and ISO/IEC 27001 Standards*, ISACA Journal Volume 1, 2016.

Kohar. Abdul & Putro. Hanson Prihantoro. 2014. *Ancaman Keamanan pada Sistem Informasi Manajemen Rumah Sakit*, Seminar Nasional Informatika Medis (SNIMed) V 2014, Magister Teknik Informatika Fakultas Teknologi Industri Universitas Islam Indonesia.

Kementerian Komunikasi dan Informatika RI. 2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI)*, Jakarta: Kementerian Komunikasi dan Informatika Republik Indonesia

Kongo. Anggrini. 2016. *Manajemen Risiko Teknologi Informasi pada Perguruan Tinggi Menggunakan Standar ISO/IEC 27001: 2013 (Studi Kasus: FTI UKSW Salatiga)*. Salatiga.

Laudon & Laudon. 2015. *Manajemen Information System: Managing the Digital Firm*, New Jersey: Prentice-Hall

Santos. AA Ternorio, Marwata, dan Sembiring. Irwan, 2014, "EMIS Information Systems Audit onthe Timor-Leste Education Ministry with a COBIT4.1 Framework, *International Journal of Computer Applications (0975-8887), Volume 89-No. 5, March 2014.*

Sugiyono. 2012. *Metode Penelitian Kuantitatif, Kualitatif, dan R&D,* Bandung: Alfabeta.

Tashakkori, Abbas dan Teddie, Charles. 2010. *Mixed Methodology Mengkombinasikan Pendekatan Kualitiatif dan Kuantitatif.* Yogyakarta: Pustaka Pelajar.

Wikipedia. 2018. *CVSS / Common Vulnerability Scoring System* (https://en.wikipedia.org/wiki/CVSS) diakses pada tanggal 18 Agustus 2018.