YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 6 Nomor 3 Edisi Agustus 2021 (164-174)

35

IMPLEMENTASI WAZUH 4.0 UNTUK PERLINDUNGAN KEAMANAN INTEGRITAS FILE

Dewi Laksmiati
Universitas Bina Sarana Informatika
(Naskah diterima: 1 Juni 2021, disetujui: 30 Juli 2021)

Abstract

Compliance is a standard that must be met by a company, this standard is related to the industry in which the company's business operates. This compliance standard in addition to assisting in risk management, it will also affect the credibility of the company. File Integrity Monitoring (FIM) is one of the compliance standards that must be met in several industry standards. One of them is compliance standards in the financial industry, commonly known as PCI DSS (Payment Card Industry Digital Security Standards). File Integrity Monitoring (FIM) is an activity to monitor the integrity of a file to maintain the integrity of a file from unauthorized changes, which is an indication of a malicious threat. In this article, the implementation of File Integrity Monitoring (FIM) will be carried out using the Wazuh application. One of the well-known open source applications in endpoint security protection.
Keywords: *Compliance, PCI DSS, File integrity, Wazuh*

Abstrak

Compliance (kepatuhan) merupakan standar yang wajib dipenuhi sebuah perusahaan, standar ini terkait dengan industry dimana bisnis perusahaan bergerak. Standar kepatuhan ini selain membantu dalam pengelolaan resiko ia juga akan berpengaruh kepada kredibilitas perusahaan. *File Integrity Monitoring* (FIM) merupakan salah satu standar kepatuhan yang harus dipenuhi dalam beberapa standar industri. Salah satunya adalah standar kepatuhan dalam dunia industri keuangan yang biasa dikenal dengan PCI DSS (*Payment Card Industry Digital Security Standards*). *File Integrity Monitoring* (FIM) merupakan aktifitas memonitor integritas sebuah file untuk menjaga keutuhan suatu file dari perubahan yang tidak terotorisasi, yang merupakan indikasi adanya ancaman. Pada penulisan ini implementasi *File Integrity Monitoring* (FIM) akan dilakukan menggunakan aplikasi Wazuh. Salah satu aplikasi open source yang cukup dikenal dalam perlindungan keamanan di *endpoint*.
Kata Kunci: *Kepatuhan, PCI DSS, Integritas File, Wazuh*

YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 6 Nomor 3 Edisi Agustus 2021 (164-174)

I. PENDAHULUAN

Ancaman dalam dunia teknologi merupakan hal yang lazim dihadap. Pengamanan perlu dilakukan pada semua lini, tidak hanya pengamanan pada sisi perimeter atau sisi pembatas dengan dunia luar dengan menggunakan *firewall*, namun juga pada sisi *endpoint* (perangkat pengguna).

Terkait dengan pengamanan tersebut, pada beberapa industri diciptakan standar kepatuhan (compliance) untuk menyeragamka standar keamanan yang harus dipenuhi oleh perusahaan. Misalnya *compliance* khusus industri keuangan, *compliance* khusus industri kesehatan, hingga *compliance* yang dibuat oleh pemerintah untuk menjaga keamanan data pengguna yang berlaku multi sektor.

Compliance atau kepatuhan IT merupakan bagian dari standar IT dimana ahli keamanan dan kepatuhan IT (*IT Security and compliance*) menangani masalah terbesar yang dihadapi perusahaan saat ini, beserta langkah-langkah apa yang dapat dilakukan oleh perusahaan untuk meminimalkan potensi risiko terkait dengan kepatuhan dan ancaman keamanan.

Dalam penulisan ini akan dibahas salah satu standar kepatuhan (*compliance*) yang wajib dipenuhi yaitu *File Integrity Monitor (FIM)* yaitu salah satu fitur yang dibutuhkan untuk menjaga keutuhan file dari perubahan yang tidak terotorisasi. Yang dimaksud dengan file di sini bukan hanya file konvensional namun juga registry yang menjadi tulang punggung konfigurasi Windows. Fitur ini ak-an diterapkan menggunakan aplikasi *open source* Wazuh.

II. KAJIAN TEORI

2.1 IT Compliance

Compliance atau kepatuhan, adalah bertindak sesuai dengan standar yang diterima (oleh peraturan, lingkungan, komunitas dll). Contohnya, mengemudi sesuai dengan batas kecepatan yang diperbolehkan adalah sebuah tindakan kepatuhan, sama halnya dengan peraturan yang hanya memperbolehkan satu buah tas tangan saja yang dibawa masuk ke pesawat. Kepatuhan juga dapat berarti mengikuti seperangkat aturan atau rambu-rambu agar suatu organisasi dapat beroperasi secara legal. Pelaksanaan prosedur untuk memenuhi kepatuhan (*compliance*) tersebut bisa memerlukan beberapa standar.

IT Compliance adalah pelaksanaan dan pengelolaan teknologi informasi yang sesuai dengan standar yang diterapkan dalam lingk-

ungan atau institusi tertentu.(Nazir, 2013). *IT Compliance* mencakup (Anonim, 2018):

1. Tujuan strategis organisasi.
2. Pelatihan dan kesadaran Peng-guna komputer.
3. Kebijakan di tingkat atas.
4. Prosedur dan standar.
5. Pengaturan konfigurasi.
6. Kontrol terhadap teknologi.
7. Pemantauan yang berkelanjut-an.
8. Penilaian risiko bisnis.
9. Auditor Internal dan Eksternal.

Di bawah ini beberapa contoh standar kepatuhan di berbagai belahan dunia terkait dengan penerapan *File Integrity Moni-toring (FIM)* yang akan dibahas dalam penulisan ini :

1. PCI DSS

Dewan Standar Keamanan Digital Industri Kartu Pembayaran atau *Payment Card Industry Digital Security Standards* (PCI DSS) telah bekerja sejak 2004 untuk mengatur aktivitas keamanan kepada "perusahaan manapun yang terkait dengan kartu pembayaran.". Jika sebuah organisasi "bekerja dengan atau terkait dengan kartu pembayaran", organisasi tersebut diharuskan untuk mematuhi level yang ditentukan (ada 4 level) dari persyaratan PCI. Ini biasanya mencakup pedagang, lembaga keuangan, vendor tempat penjualan, dan pengembang.

Secara khusus, dua bagian PCI membahas kebutuhan perangkat lunak pemantauan integritas file:

10.5.5: Gunakan perangkat lunak pemantauan integritas file atau deteksi perubahan untuk memastikan data log tidak dapat diubah tanpa membuat peringatan.

11.5: Menyebarkan pemantauan deteksi perubahan (seperti pemantauan integritas file) untuk melakukan perbandingan file penting setidaknya sekali sepekan, dan memperingatkan personel tentang modifikasi tidak sah dari file sistem kritis, file konfigurasi, atau file konten.

2. NERC-CIP

Sebagai pedoman kesiapan infrastruktur penting dari *North American Electric Reliability Corporation*, NERC-CIP didirikan untuk memastikan keandalan dalam pengiriman e-nergi. Pedoman ini bertindak sebagai kerangka kerja yang membantu dalam perlindungan aset infrastruktur penting. Ketika teknologi baru muncul, penyedia utilitas semakin mengadopsi teknologi untuk mengontrol jaringan dan aspek penting dari pengiriman energi. Mencegah akses tidak sah dan perubahan

negatif sering kali berada di urutan teratas daftar.

Pemantauan integritas file dibahas dalam NERC-CIP 007, yang berupaya mengelola keamanan sistem dengan menentukan persyaratan teknis, operasional, dan prosedural tertentu "terhadap penerobosan yang dapat menyebabkan kesalahan operasi atau ketidakstabilan.". Dokumentasi *port*-/layanan sistem dan deteksi, peringatan, dan laporan tentang perubahan status diperlukan. Manajemen perubahan konfigurasi mengenai prosedur dan dokumentasi ditekankan dengan persyaratan NERC-CIP 010-2

3. FISMA

Sejak tahun 2002, Undang-Undang Manajemen Keamanan Informasi Federal atau *Federal Information Security Management Act* (FISMA) di Amerika Serikat telah mewajibkan lembaga federal untuk menerapkan program di seluruh badan untuk keamanan informasi, dan ini termasuk kontraktor pemerintah. Program keamanan harus ditinjau setiap tahun dan dilaporkan ke Kantor Federal Manajemen dan Anggaran pemerintah Amerika Serikat, *Office of Management and Budget* (OMB).

NIST 800-171 membahas perlunya memastikan integritas dan ketersediaan Data Pemerintah Federal AS melalui program keamanan TI yang komprehensif.

NIST 800-53 Revisi 4 memberikan wawasan mendalam bagi lembaga tentang tanggung jawab, manajemen risiko, dan cara memilih garis dasar kontrol keamanan. Namun, pemilihan akhir dari kontrol khusus berada di tangan lembaga, berdasarkan kriteria yang digariskan dalam NIST 800-53 Rev 4.

Solusi pemantauan integritas file yang tepat dapat membantu lembaga dalam mencapai kepatuhan dengan Integritas Sistem FISM-A, Manajemen Konfigurasi, kategori Audit, dan membantu pemetaan **antara NIST 800-171** dan **800-53.**

4. SOX

Sarbanes-Oxley Act, juga dikenal sebagai SOX, adalah undang-undang federal yang menetapkan persyaratan akuntabilitas untuk dewan perusahaan publik AS, manajemen, dan kantor akuntan publik.

Dengan total 11 bagian di SOX, banyak *organisasi* fokus pada Bagian 404, yang disingkat sebagai ICFR. Bagian ini mensyaratkan pelaporan tentang kecukupan pengendalian internal atas pelaporan keuangan.

Persyaratan Bagian 404 termasuk, tetapi tidak terbatas pada:

- Melakukan penilaian risiko penipuan

- Mengevaluasi kontrol tingkat entitas,
- Mencegah manajemen mengabaikan kontrol.

Mirip dengan FISMA, SOX tidak secara eksplisit menyatakan jenis kontrol atau metode yang harus digunakan organisasi/bisnis untuk kepatuhan. Karena ini, kerangka kerja COBIT didirikan untuk kepatuhan. Stan-dar COBIT yang dibantu dengan peng-gunaan pemantauan integritas file meliputi:

- akuisisi dan implementasi
- pengiriman dan dukungan
- pemantauan

5. HIPAA

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan tahun 1996 atau *Health Insurance Portability and Accountability Act* of 1996 (HIPAA) membahas perlindungan untuk memastikan "kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi." Aturan Keamanan HIPAA menyebutkan lima jenis pengamanan teknis, yang meliputi otentikasi, dokumentasi, perlindungan intrusi, dan perlindungan integritas data.

Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA) berfokus pada perlindungan dengan maksud untuk memastikan "kerahasiaan, integritas, dan ketersediaan informasi kesehatan yang dilindungi (PHI)".

Aturan Keamanan HIPAA menyebutkan 5 jenis pengamanan teknis yang meliputi:

- intrusi
- perlindungan
- autentikasi
- pengamanan teknis
- perlindungan integritas data

Wawasan mendalam tentang bagaimana mencapai kepatuhan dengan standar pengamanan teknis HIPAA dapat ditemukan di Publikasi Khusus NIST 800-66. Alat pemantauan integritas file memungkinkan bisnis-/organisasi untuk tidak hanya mencapai tetapi juga menjaga kepatuhan terhadap praktik terbaik HIPAA, termasuk evaluasi berkelanjutan atas kontrol akses dan keamanan data.

6. GLBA

Gramm-Leach-Bliley Act (GLBA) tahun 2003 mewajibkan pengungkapan praktik berbagi informasi dan pengamanan data sen-sitif dari lembaga yang menawarkan produk atau layanan keuangan. Di bawah GLBA, "*Safeguards Rule*" secara khusus mewajibkan institusi untuk:

- Melindungi dari ancaman atau bahaya yang diantisipasi terhadap keamanan atau integritas informasi tersebut
- Memastikan keamanan dan keraha-siaan informasi pelanggan
- Melindungi dari akses tidak sah ke atau penggunaan informasi tersebut yang dapat mengakibatkan kerugian besar atau ketidaknyamanan bagi pelanggan mana pun.

Per teks Aturan Perlindungan GLBA, elemen program keamanan harus mencakup:

- **314.4-3:** Mendeteksi, mencegah dan menanggapi serangan, intrusi, atau kegagalan sistem lainnya.
- **314.4 (c):** Merancang dan menerapkan pengamanan informasi untuk mengendalikan risiko yang Anda identifikasi atau yang dipantau.
- Pemantauan integritas file sesuai den-gan kepatuhan terhadap aturan perlin-dungan GLBA dengan menyediakan alat untuk memantau konfigurasi dan keamanan *host,* penilaian keamanan, dan menyediakan jejak audit yang kuat.

7. GDPR

Peraturan Perlindungan Data Umum, General Data Protection Regulation (GDPR) berlaku untuk semua perusahaan yang memproses data persona subjek data yang tinggal di Uni Eropa. GDPR melindungi hak dan kebebasan subjek data yang mencakup penentuan proses/langkah yang harus diambil oleh pemegang data untuk melindungi data. Pemantauan integritas file dapat digunakan untuk membantu kepatuhan terhadap persyaratan GDPR (Ogden, 2018):

- **Pasal 25 :** Perlindungan Data Berda-sarkan Desain dan Default
- **Pasal 32:** Keamanan untuk pemro-sesan
- **Pasal 39:** Tugas Petugas Perlindungan Data (DPO)
- **Pasal 57:** Tugas
- **Pasal 59:** Laporan Kegiatan

2.2 File Integrity Monitoring (FIM)

Pemantauan integritas file atau *File Integrity Monitoring (FIM)* mengacu pada proses dan teknologi keamanan TI yang menguji dan memeriksa file sistem operasi (OS), database, dan perangkat lunak aplikasi untuk menentukan apakah file tersebut telah dirusak atau rusak. FIM, yang merupakan jenis audit perubahan, memverifikasi dan memvalidasi file-file ini dengan memban-dingkan versi terbarunya dengan "dasar" yang dikenal dan terpercaya.

Manfaat penerapan pemantauan integritas file utama diantaranya:

a. Mendeteksi Aktivitas Terlarang

Jika penyerang dunia maya mengganggu lingkungan TI Anda, Anda perlu mengetahui apakah mereka telah mencoba mengubah file apa pun yang penting bagi sistem operasi atau aplikasi Anda. Bahkan jika file log dan sistem deteksi lainnya dihindari atau diubah, FIM masih dapat mendeteksi perubahan pada bagian penting ekosistem TI Anda. Dengan FIM, Anda dapat memantau dan melindungi keamanan file, aplikasi, sistem operasi, dan data Anda.

b. Menentukan Perubahan yang Tidak Diinginkan

Seringkali, perubahan file dilakukan secara tidak sengaja oleh admin atau karya-wan lain. Terkadang konsekuensi dari peru-bahan ini mungkin kecil dan diabaikan. Di lain waktu, mereka dapat membuat pintu belakang keamanan, atau mengakibatkan disfungsi dengan operasi atau kelangsungan bisnis. Pemantauan integritas file menyederhanakan forensik dengan membantu Anda membidik perubahan yang salah, sehingga Anda dapat mengembalikannya atau melakukan perbaikan lainnya.

c. Memverifikasi Status Pembaruan dan Kesehatan Sistem Pemantauan

Anda dapat memeriksa apakah file telah ditambal ke versi terbaru dengan memindai versi yang diinstal di beberapa lokasi dan mesin dengan checksum pasca-tambalan.

d. Memenuhi Mandat Kepatuhan

Kemampuan untuk mengaudit perubahan, dan untuk memantau serta melaporkan jenis aktivitas tertentu diperlukan untuk mematuhi mandat peraturan seperti GLBA, SOX, HIPAA, dan PCI DSS. (Anonim, 2020).

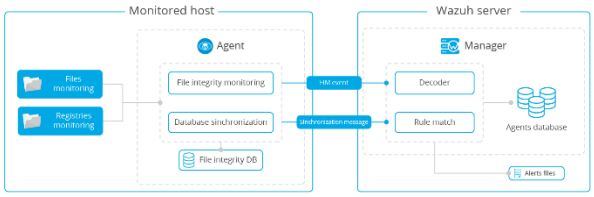
2.3 Wazuh

Wazuh merupakan perangkat berbasis *Open Source* yang berfungsi sebaga sistem deteksi intrusi berbasis *host* (*endpoint*). Wazuh melakukan analisis log, pemeriksaan integritas, pemantauan registri Windows, deteksi rootkit, peringatan berbasis waktu, dan respons aktif. (Anonim, 2020).

2.4 File Integrity Monitoring Pada Wazuh

Modul FIM terletak di agen Wazuh, tempat menjalankan pemindaian sistem secara berkala dan menyimpan checksum dan atribut file yang dipantau dan kunci registri Windows dalam database FIM lokal. Modul mencari modifikasi dengan membandingkan checksum file baru dengan *checksum* lama. Semua

perubahan yang terdeteksi dilaporkan ke manajer Wazuh.



Mekanisme sinkronisasi FIM yang baru memastikan inventaris file di manajer Wazuh selalu diperbarui sehubungan dengan agen Wazuh, memungkinkan melayani kueri API terkait FIM terkait agen Wazuh. Sinkronisasi FIM didasarkan pada perhitungan berkala integritas antara database agen Wazuh dan manajer Wazuh, memperbarui di manajer Wazuh hanya file-file yang kedaluwarsa, mengoptimalkan transfer data FIM. Setiap kali modifikasi terdeteksi dalam file yang dipantau dan/atau kunci registri, peringatan dibuat. (Anonim, 2020).

III.METODE PENELITIAN

3.1 Metode Observasi

Melakukan pengumpulan data-data dengan cara mengamati serta mencatat secara sistematis tentang perangkat dan aplikasi yang digunakan dalam konfigurasi dalam praktek langsung.

3.2 Metode Studi Pustaka

Yaitu menggunakan literatur baik dalam bentuk media online, artikel atau buku bacaan yang berkaitan dengan penyusunan artikel ini.

3.3 Metode Pengembangan Jaringan

1. Analisa Kebutuhan

Analisa akan dilakukan melalui beberapa tahapan, yaitu

a. Observasi langsung
b. Memahami semua kondisi kebutuh-an di lapangan terkait kebutuhan stega-nogtafi
c. Analisa hasil observasi.

2. Desain

Perancangan dilakukan melalui beberapa tahapan, yaitu:

a. Pemilihan aplikasi File Integrity Monitoring untuk pengujian.
b. Penentuan OS yang akan digunakan untuk pengujian

3. Testing

Melakukan pengujian perubahan file dan meneliti apakah setiap perubahan yang dilakukan terpantau dengan baik

4. Implementasi

Untuk menjalankan Wazuh diperlukan langkah berikut.

a. Instalasi dan konfigurasi Wazuh Server

Instalasi Wazuh Server berbasis Linux dilakukan pada mesin virtual (VM) pada sistem lokal. Wazuh OVA digunakan sebagai media instalasi di-karenakan siap pakai dan

konfigurasi yang dilakukan tidak banyak. *Server* diin-stall dengan spesifikasi:

Processor : 4 core

RAM : 8 GB

Hard Disk : 100 GB

b. Instalasi Agent

Setelah Wazuh Server terinstall langkah selanjutnya adalah melakukan instalasi Wazuh Agent di dalam 1 VM lain yang berbasis Windows. Dalam VM yang terinstall agent inilah kita akan melakukan pengujian fitur pem-antauan integritas file atau *File Integrity Monitor* (FIM)

IV. HASIL DAN PEMBAHASAN

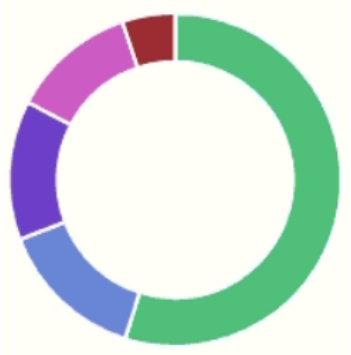
Pada bab ini akan dijelaskan mengenai hasil pengujian.

4.1. *Monitoring*

Pengujian dilakukan dengan cara menginstalasi agent ke VM yang terinstall windows. Dan kemudian VM diguakan untuk operasional sehari-hari seperti biasa. Hasil selama pengujian dijabarkan pada sub bab berikut

4.2. Hasil Pengujian

Dari hasil monitoring menggunakan agent selama 1 bulan didapatkan hasil sebagai berikut untuk monitoring pada resgistry windows.



Color	Rule	Total	%
	Registry Value Entry Added to the System	203	54.86
	Registry Key Integrity Checksum Changed	53	14.32
	Registry Key Entry Added to the System	50	13.51
	Registry Value Integrity Checksum Changed	45	12.16
	Registry Value Entry Deleted.	19	5.14

Hasil di atas di dapatkan dari aktifitas berupa

- Instalasi *software*
- *Uninstall Softawre*
- Modifikasi *Software*
- Perubahan konfigurasi windows

Hasil pengujian di atas dapat dilihat lebih detail pada halaman Events, dimana ditampilkan sebagai berikut (beserta contoh):

Waktu

Jun 15, 2021 @ 22:51:16.741

Hostname

(TEST-HOSTNAME)

Path

(HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce)

Event

Deleted

Rule description

Registry Value Entry Deleted.

V. KESIMPULAN

Dari pengujian monitoring integritas menggunakan agent diperoleh kesimpulan sebagai berikut:

1. Setiap perubahan dalam *registry* ter-catat dalam event log Wazuh
2. Event Log menampilkan data yang le-ngkap beserta timestamp
3. Data dari Event Log dapat digunakan untuk keperluan forensik digital
4. Pemenuhan standar FIM pada *com-pliance* dapat di lakukan menggunakan aplikasi Wazuh

DAFTAR PUSTAKA

Nazir Aswil, 2013, "Apa bedanya IT Compliance dengan IT Governance? ", Blog Daya Cipta Mandiri. http://blog.dayaciptamandiri.com/2013/07/apa-bedanya-it-compliance-dengan-it.html (diakses pada 11 Mei 2021 08:24 WIB)

Anonim, 2018 "IT Consulting for IT Complience",.proxsisgroup.com.https://proxsisgroup.com/it-consulting-for-it-complience/.(diakses pada 6 Mei 2021 14:11 WIB)

Ogden, Jacqueline von, 2018, "7 Regulations Requiring File Integrity Monitoring for Compliance",Cimcor.com.https://www.cimcor.com/blog/7-regulations-requiring-file-integrity-monitoring-for-compliance. (diakses pada 1 Mei 2021 21:11 WIB)

Anonim, 2020, "File Integrity Monitoring", BeyondTrust Glossary, https://www.beyondtrust.com/resources/glossary/file-integrity-monitoring (diakses pada 13 Mei 2021 14:22 WIB)

Anonim, 2020,"Tutorial Instalasi Wazuh 4.0 (Endpoint Security) pada CentOS 7", GOV-CSIRT Indonesia, https://govcsirt.bssn.go.id/tutorial-instalasi-wazuh-4-0-endpoint-security-pada-centos-7/ (diakses pada 12 Mei 2021 19:04 WIB)

Anonim, 2021, "How it works", Wazuh Documentation https://documentation.wazuh.com/current/user-manual/capabilities/file-integrity/how-it-works.html (diakses pada 22 Mei 2021 14:03 WIB)

Anonim, 2020," File integrity monitoring", Wazuh Documentation, https://documentation.wazuh.com/current/pci-dss/file-integrity-monitoring.html (diakses pada 13 Mei 2021 09:22 WIB)

Anonim, 2021, "File integrity monitoring", Wikipedia, https://en.wikipedia.org/wiki/File_integrity_monitoring (diakses pada 13 Mei 2021 09:32 WIB)

Bisson, David, 2019," What Is FIM (File Integrity Monitoring)?", TripWire.com

https://www.tripwire.com/state-of-security/security-data-rotection/security-controls/file-integrity-monitoring/
(diakses pada 3 Mei 2021 22:12 WIB)

Anonim, 2020, "File Integrity Monitoring.", Qualys.com.https://www.qualys.com/apps/file-integrity-monitoring/
(diakses pada 13 Mei 2021 10:12 WIB)