Penanganan Insiden pada Media Penyimpanan Terenkripsi

Sevierda Raniprima 23214328

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Indonesia

sevierda@students.itb.ac.id

Abstrak— Media penyimpanan dengan enkripsi mampu menyediakan kerahasiaan data bagi penggunanya. Penanganan insiden yang efektif dibutuhkan agar organisasi dapat mengurangi atau bahkan menghilangkan dampak insiden dalam waktu yang singkat. Meskipun pada dasarnya proses penanganan insiden sama, diperlukan penanganan khusus untuk menangani insiden yang melibatkan penyimpanan terenkripsi. Tulisan ini membahas proses penanganan insiden agar dapat menanggapi insiden yang melibatkan media penyimpanan terenkripsi secara efektif.

Kata kunci— penanganan insiden, media penyimpanan, enkripsi.

1 Pendahuluan

Enkripsi merupakan proses mengubah data dari bentuk yang dapat dibaca, disebut *plaintext*, menjadi bentuk yang tidak dapat dibaca, disebut *ciphertext*, menggunakan algoritma kriptografi dan kunci. Tanpa adanya kunci, data tidak akan dapat dibaca. Oleh karena itu, enkripsi merupakan cara terkuat untuk mencegah akses ke data oleh pengguna tidak terotentikasi.

Dengan meningkatnya penggunaan teknologi enkripsi, saat ini terdapat berbagai metode yang digunakan untuk mengenkripsi data at rest atau data pada media penyimpanan seperti *harddisk*. Sistem penyimpanan data berisi berbagi informasi, termasuk kumpulan data yang telah dihapus. Informasi ini berharga bagi attacker yang menginginkan organisasi mengalami kerugian.

Apabila terjadi insiden, penanggapan dan penanganan insiden menjadi lebih sulit dengan adanya penggunaan teknologi penyimpanan terenkripsi. Sebelum mengumpulkan data terkait insiden, tim penanganan insiden harus terotentikasi agar bisa mengakses sistem. Penanganan insiden yang efektif dibutuhkan agar organisasi dapat mengurangi atau bahkan menghilangkan dampak insiden dalam waktu yang singkat. Meskipun pada dasarnya proses penanganan insiden sama, diperlukan penanganan khusus untuk menangani insiden yang melibatkan penyimpanan terenkripsi.

Tulisan ini menjelaskan media penyimpanan data pada Bagian 2. Bagian 3 membahas enkripsi. Bagian 4 membahas berbagai teknologi enkripsi pada media penyimpanan. Bagian 5 membahas prosedur penanganan insiden. Bagian 6 membahas incident response yang melibatkan media penyimpanan terenkripsi. Terakhir, Bagian 7 menyimpulkan tulisan ini.

2 Penyimpanan Data

Penyimpan data pada komputer biasa disebut dengan istilah *harddisk*. Sebuah *hard drive* terdiri dari satu atau lebih piringan (*disk*) yang berputar bersamaan. Setiap piringan dilengkapi dengan dua buah *read/write head*, berada di atas dan bawahnya, yang berfungsi untuk mengakses dan menyimpan data. *Harddisk* terdiri dari banyak *track* dan *sector*. *Track* merupakan lingkaran konsentris di sekitar *disk*. *Track* terbagi menjadi *sector* yang merupakan bagian penyimpanan terkecil dari sebuah *harddisk*. [1]

2.1 Format dan Partisi *Harddisk*

Sebelum media dapat digunakan untuk menyimpan data, media harus diformat dan dipartisi menjadi *logical volumes*. Partisi merupakan pembagian media secara logis menjadi porsi yang berfungsi sebagai unit terpisah. *Logical volume* merupakan partisi atau kumpulan partisi yang berlaku sebagai kesatuan yang diformat dengan *file system*. [7]

Ada dua tipe format pada *harddisk*, yaitu format level rendah yang dilakukan oleh pabrikan dan format level tinggi oleh *file system*. Piringan pada *hard drive* kosong hingga pabrikan melakukan format level rendah yang membuat *track* dan *sector* pada setiap piringan [1]. Selama pemformatan, *file system* kosong ditulis pada piringan yang kemudian memungkinkan penyimpanan data.

2.2 *File System*

Sector pada *hard drive* dikelompokkan membentuk *cluster*. Ini merupakan unit penyimpanan terkecil yang digunakan untuk menyimpan file. *File system* mengurangi *overhead* berkaitan dengan operasi *read/write* pada *disk* akibat lebih sedikitnya area penyimpanan yang tersedia [5]. Saat *file system* menulis data pada *disk*, menulis pada *cluster* lebih efisien dibandingkan pada *sector*.

File system menentukan bagaimana data diakses, disimpan, diatur, dan dinamai. Data dapat disimpan dalam *logical unit* atau file yang dapat dinamai (file name). File dapat dikelompokkan menjadi suatu direktori atau folder [7]. *File system* juga memetakan ruang fisik *hard drive* pada *logical address* [5]. Dua file system pada Windows yang biasa digunakan yaitu *File Allocation Table* (FAT) dan *NT File Systems* (NTFS).

2.2.1 FAT

File Allocation Table (FAT), *file system* milik Microsoft, merupakan *file system* yang paling sering digunakan dan tersedia dalam dua bentuk, FAT16 dan FAT32. *File allocation table* adalah suatu *database* yang berisi nama file dan direktori, waktu file MAC (dimodifikasi, diakses, dan dibuat), nomor cluster, serta atribut lainnya, seperti *hidden* dan *read-only* [5]. Informasi ini berguna bagi tim penanganan insiden dalam memahami urutan kejadian pada sistem, termasuk kapan file dibuat, diakses, atau bahkan dihapus.

2.2.2 NTFS

NT *File System* milik Microsoft meningkatkan desain FAT dengan menambahkan informasi komprehensif mengenai semua file pada *disk* serta meningkatkan cara file dan direktori disimpan.

Bagaimana data disimpan pada *harddisk* perlu diketahui oleh tim penanganan insiden. Hal ini memudahkan saat terjadi insiden dan data disembunyikan dalam *harddisk*.

2.3 Penyimpanan Data Residu

Data yang telah dihapus dari *harddisk* serta temporary file disebut sebagai data residu. Data ini tetap terletak di media penyimpanan, sehingga data dapat didapatkan kembali untuk dianalisis. Beberapa bentuk data residu meliputi [7]:

- *Unused File Allocation Units*— unit alokasi file dalam partisi yang tidak digunakan file system.
- *Slack space*— area antara akhir file dan akhir unit alokasi file, misalnya jika data disimpan dalam blok berukuran 2 KB, file 5 KB akan menggunkaan 3 blok yang mengakibatkan 1 KB area slack space.
- *Free space*— area media penyimpanan yang tidak dialokasikan pada partisi.

3 Enkripsi

Pengamanan data agar data terjaga kerahasiannya dapat dilakukan dengan enkripsi. Data asli (*plaintext*) diubah menjadi data terenkripsi (*ciphertext*) menggunakan suatu algoritma kriptografi dan kunci rahasia, sehingga hanya pihak yang memiliki kunci yang dapat membaca data asli. Data terenkripsi tetap terlindungi selama kunci disimpan dengan baik. Oleh karena itu, melindungi kunci sangat penting untuk memastikan data terjaga kerahasiannya.

3.1 Kriptografi Kunci Simetris

Kriptografi kunci simetris menggunakan kunci yang sama untuk mengenkripsi dan mendekripsi data. Kunci harus digunakan, ditransmisikan, dan disimpan dengan baik karena data terenkripsi hanya bisa didekripsi menggunakan kunci tersebut.

Enkripsi data dilakukan dalam ukuran blok yang tetap (*block cipher*) atau perbit (*stream cipher*). *Data at rest* lebih baik dienkripsi menggunakan *block cipher*, seperti algoritma *Data Encryption Standard* (DES) dan *Advanced Encryption Standard* (AES). Sedangkan data *real time*, seperti transmisi suara, video, atau lainnya dienkripsi dengan *stream cipher*. Salah satu algoritma *stream cipher* yaitu RC4. RC4 digunakan dalam *Secure Sockets Layer* untuk mengamankan *data in transit* antara *client* dan web *server*.

3.2 Kriptografi Kunci Asimetris

Kriptografi kunci asimetris menggunakan kunci yang berbeda untuk enkripsi dan dekripsi data. Kunci publik digunakan untuk enkripsi, sedangkan kunci privat digunakan untuk dekripsi. Kriptografi kunci simetris dapat mengatasi kesulitan dalam transmisi kunci simetris.

3.3 Manajemen Kunci

Dalam komunikasi, proses manajemen kunci meliputi pembuatan, penggunaan, dan penghancuran kunci. Jika kunci hilang atau terjadi masalah berkaitan dengan kunci, solusinya yaitu membuat kunci baru dan melanjutkan operasi. Karena kunci lama digunakan untuk komunikasi dahulu yang sekarang sudah selesai, hal ini bukan masalah signifikan. Namun,

dengan penyimpanan, jika kunci hilang, akses ke data dalam media penyimpanan juga hilang. Membuat kunci baru utuk data yang terenkripsi tidak bisa membantu [2].

Kunci harus disimpan dalam suatu tempat yang aman secara fisik, tidak disimpan dalam file. Data kunci dapat pula dienkripsi dengan kunci master yang diturunkan dari suatu passphrase yang tidak disimpan dalam sistem. Kunci master merupakan kunci untuk mengenkripsi kunci, sehingga dapat disimpan dalam suatu file. Kunci master tidak perlu disimpan dalam tempat yang aman secara fisik [8].

4 Enkripsi Media Penyimpanan

Ada banyak media yang digunakan untuk menyimpan informasi digital, seperti peralatan dengan USB, *memory card*, dan *hard drive*. Penyimpan data memungkinkan adanya transportasi data antara *device* dan sistem komputer. Untuk mencegah hilangnya informasi, media penyimpanan dapat dienkripsi. Sesuai dengan NIST SP 800-111, ada beberapa pertimbangan dalam mengimplementasikan solusi media penyimpanan terenkripsi, yaitu:

a. Organisasi harus menggunakan manajemen terpusat untuk semua penyebaran enkripsi media penyimpanan.
b. Organisasi harus memastikan semua kunci kriptografi yang digunakan dalam solusi enkripsi media penyimpanan aman.
c. Organisasi harus memilih otentikasi user yang sesuai untuk solusi media penyimpanan terenkripsi.

Teknologi enkripsi media penyimpanan, seperti enkripsi file/floder, *full disk encryption* (FDE)/ *whole disk encryption* (WDE), enkripsi *virtual disk*, dan enkripsi *volume*, dapat dijadikan pilihan untuk mengenkripsi *data at rest*.

4.1 Enkripsi File/Folder

File ataupun direktori file (folder) dapat dienkripsi menggunakan enkripsi file/folder. File terenkripsi dalam media penyimpanan, tetapi daftar direktori dan file metadata tersedia. Saat pengguna mencoba membuka file terenkripsi, pengguna harus terotentikasi sebelum file didekripsi. Metode ini membutuhkan pengguna mengetahui file atau folder mana yang perlu dienkripsi. Data residu tidak dienkripsi.

4.2 Enkripsi *Full Disk / Whole Disk*

Metode enkripsi *full disk / whole disk* mengenkripsi seluruh media penyimpanan termasuk file page atau swap, temporary file, dan semua data yang tersimpan. *Software* FDE bekerja dengan mengarahkan *master boot record* (MBR) komputer, yang merupakan *reserved sector* pada *bootable media* yang menentukan *software* mana yang akan dieksekusi saat komputer *boot* dari media [7]. Setelah otentikasi, *software* FDE/WDE mendekripsi boot sector sistem operasi dan sistem operasi mulai berjalan. Setelah sistem operasi *boot*, pengguna mengotentikasi sistem operasi dan mengoperasikan komputer seperti biasanya.

Semua data residu dienkripsi pada *disk*. Metode ini menyediakan perlindungan terbesar bagi kerahasiaan data karena semua sektor dienkripsi dengan pengecualian area otentikasi pra-boot. Area ini tidak dienkripsi sebab diperkukan untuk menjalankan *software* otentikasi.

4.3 Enkipsi *Virtual Disk*

Pada enkripsi virtual *disk*, file terenkripsi yang disebut kontainer dibuat dan digunakan untuk menyimpan file dan direktori. Akses ke virtual *disk* hanya diotorisasi saat pengguna berhasil diotentikasi. *Software* enkripsi virtual *disk* mengenkripsi dan mendekripsi sektor jika diperlukan saat menulis dan membaca data kontainer. Biasanya kontainer dipasang sebagai virtual *disk* [7].

Salah satu keuntungan enkripsi *virtual disk* yaitu kontainer bersifat *portable* dan mudah di-*back up*. Kontainer yang berupa file dapat disalin dan di-*burn* dalam media lain tanpa mempengaruhi kemampuan enkripsi dan dekripsi data dalam kontainer.

4.4 Enkripsi *Volume*

Dalam enkripsi *volume*, seluruh *logical volume* dienkripsi dan hanya bisa diakses saat otentikasi pengguna berhasil. Proses ini serupa dengan FDE/WDE, namu hanya volume yang dienkripsi, tidak seluruh media penyimpanan. Data residu dapat tetap diakses di dalam atau di luar volume terenkripsi.

5 Penanganan Insiden

Insiden merupakan kejadian buruk yang mempengaruhi sistem informasi, misalnya denial of service. Selain itu, insiden mencakup sistem crash, gangguan, penggunaan yang tidak sah dari hak istimewa sistem, dan penghancuran data. Mengetahui bagaimana cara menanggapi insiden secara sistematis dan efisien membantu mengurangi dampak negatif dari gangguan sistem, downtime, dan kehilangan data [6].

Seperti yang didefinisikan pada NIST SP 800-61, *Computer Security Incident Handling Guide*, proses penanganan insiden memiliki empat tahapan utama: *preparation*, *detection*, *analysis*, *containment/eradication/recovery* dan *post-incident activity* [6]. Dalam tulisan ini, tahapan yang digunakan sedikit berbeda. Tahapan yang dijelaskan adalah persiapan, deteksi, penahanan, pemulihan sistem, dan pelaporan.

5.1 Persiapan

Sebelum terjadi insiden, alat bantu, prosedur, kebijakan perusahaan, dan manusia harus disiapkan untuk menanggapi insiden. Alat bantu yang diperlukan termasuk alat bantu forensik. Proses eskalasi, prosedur penanganan, dan dokumentasi dibuat dan *Incident Response Team* diberi pelatihan. Tim ini membutuhkan persiapan berupa kebijakan dan prosedur untuk mengantisipasi suatu insiden, yang didefinisikan secara jelas dan merinci untuk seluruh tim dan individu yang berada dalam organisasi itu sendiri.

5.1.1 Membangun Kemampuan Terkait dengan Media Penyimpanan Terenkripsi

Kemampuan yang diperlukan oleh tim penanganan insiden yang melibatkan media penyimpanan terenkripsi antara lain adalah pengetahuan mendasar mengenai media penyimpanan dan jenis enkripsi. Selain itu, organisasi harus memiliki beberapa orang yang berpengalaman dalam forensik digital serta familiar dengan alat bantu dan teknik yang perlu digunakan.

5.1.2 Membangun Fasilitas untuk Komunikasi dan Koordinasi

Salah satu masalah yang paling umum saat menangani insiden adalah komunikasi dan koordinasi yang buruk. Siapapun yang terlibat dalam penanganan insiden, termasuk seluruh anggota dalam organisasi, secara tidak sengaja dapat memperburuk situasi karena ketidakpemahaman mengenai masalah yang sedang dihadapi. Untuk meningkatkan komunikasi dan koordinasi, suatu organisasi harus menunjuk terlebih dahulu beberapa individu atau tim kecil yang bertanggung jawab untuk mengoordinasikan insiden yang sedang dihadapi organisasi. Tujuan utama koordinasi ini adalah untuk meningkatkan kesadaran situasional dengan mengumpulkan semua informasi yang terkait, membuat keputusan yang mementingkan tujuan organisasi, dan mengomunikasikan informasi yang relevan dan menjelaskan keputusan kepada semua pihak yang terkait dalam organisasi pada waktu yang tepat.

5.1.3 Sumber Daya dan Perangkat dalam Penanganan Insiden

Suatu organisasi harus memastikan bahwa mereka memiliki perangkat yang diperlukan, baik perangkat keras maupun perangkat lunak, serta sumber daya untuk membantu penanganan insiden yang melibatkan media penyimpanan terenkripsi.

5.2 Deteksi

Mendeteksi apakah suatu kejadian merupakan insiden atau bukan adalah tindakan penting. Segala sesuatu yang berhubungan dengan insiden harus didokumentasikan dengan baik sebab itu mungkin digunakan dalam proses penanganan insiden selanjutnya. *Log* memiliki peran penting dalam tahap deteksi. *Log* aplikasi, *firewall*, sistem, dan deteksi intrusi dapat berisi bukti berharga, termasuk sumber aktivitas insiden.

5.3 Penahanan

Saat suatu insiden diketahui, tahap selanjutnya adalah menghentikan insiden menyebar atau menimbulkan kerugian tambahan. Dalam menangani insiden, organisasi perlu menentukan metode penahanan sebagai langkah awal penanggapan insiden yang dilakukan. Organisasi harus memiliki strategi dan prosedur untuk membuat keputusan penahanan terkait risiko dari suatu insiden yang dapat diterima oleh organisasi. Strategi penahanan harus mendukung penanggapan insiden dalam memilih kombinasi yang tepat dari metode penahanan berdasarkan karakteristik dari suatu insiden tertentu. Metode penahanan dapat dibagi menjadi empat kategori dasar:

- Partisipasi pengguna— hal ini dapat membantu pengguna mengenai petunjuk tentang cara untuk mengidentifikasi insiden dan langkah-langkah apa yang harus diambil jika sistem terkena dampak insiden.
- Sistem deteksi otomatis— teknologi otomatis, seperti perangkat antivirus, e-mail *filtering*, dan perangkat lunak pencegahan intrusi, sering digunakan untuk penahanan insiden.
- Menonaktifkan layanan— organisasi harus siap untuk menutup atau memblok jaringan yang digunakan dan harus memahami konsekuensi dari tindakan yang diambil. Organisasi juga harus siap untuk menanggapi masalah yang disebabkan oleh organisasi lain yang menonaktifkan layanan mereka sendiri dalam menanggapi insiden.
- Menonaktifkan koneksi— organisasi harus siap untuk menempatkan pembatasan tambahan pada koneksi jaringan yang mengandung insiden dan siap menerima dampak dari pembatasan yang mungkin berpengaruh pada fungsi organisasi.

5.4 Pemulihan Sistem

Operasi organisasi kembali ke normal dalam tahap ini. Fungsi dan data sistem yang terkena insiden dikembalikan. *Monitoring* perlu diimplementasikan untuk memastikan sistem berjalan dengan baik dan masalah sudah diselesaikan.

5.5 Pelaporan

Belajar dari insiden yang terjadi saat ini membantu memastikan bahwa insiden tidak akan terjadi lagi di masa depan dan meningkatkan keamanan secara keseluruhan. Catatan yang diambil selama insiden harus ditinjau ulang dan dibandingkan dengan *Incident Response Plan*. Laporan dibuat untuk setiap insiden dan dikumpulkan pada manajemen dengan melampirkan perubahan yang diajukan, anggaran, dan dampak rekomendasi. Individu lainnya mendapatkan salinan informasi ini agar dapat meningkatkan proses penanganan insiden.

6 Incident Response Melibatkan Media Penyimpanan Terenkripsi

Hal yang harus dilakukan oleh Incident Response Team untuk menangani insiden keamanan komputer yaitu menentukan tingkat insiden, mengumpulkan sebanyak mungkin informasi mengenai insiden, mendokumentasikan semua temuan, dan membagikan informasi yang terkumpul untuk menentukan akar penyebab insiden. Tim penanganan insiden perlu dilatih dan memiliki pengetahuan dalam menjalankan tugas. Informasi atau bukti dapat hancur dengan mudah jika kesalahan dibuat. Bukti harus dijaga dengan baik untuk meminimalisasi kerusakan akibat investigasi atau disebut *chain of custody*. *Toolkit incident response* diperlukan untuk mengumpulkan data.

6.1 *Jump Bag*

Jump bag merupakan kumpulan alat bantu dan sumber daya yang berguna saat menanggapi insiden. Beberapa benda penting yang harus ada di *jump bag*, yaitu:

- Media penyimpanan kosong, termasuk CD/DVD.
- *Incident response toolkit*.
- *Laptop*.
- Berbagai kabel dan *adapter*.
- Pulpen dan buku catatan untuk mencatat semua proses.
- Formulir *incident response*, *cheatsheet*, dan *incident response plan*.
- *Incident response team* dan informasi kontak.

6.2 Mengakses Media Penyimpanan Terenkripsi

Metode enkripsi *whole disk* membutuhkan otentikasi yang berhasil sebelum memungkinkan akses ke sistem. Contoh metode otentikasi yaitu *password/passphrasse*, *smart card*, *token*, dan *biometric*. Jika otentikasi pada sistem berhasil, prosedur *incident response* dapat dilakukan untuk mengumpulkan data, baik data volatile maupun data nonvolatile. Tetapi, jika otentikasi tidak berhasil, akses ke sistem terenkripsi akan menjadi susah. Ada beberapa pilihan bagi tim *incident response* agar dapat mengakses media terenkripsi.

- *Bootable recovery media* (CD/DVD/USB). Beberapa metode tidak membutuhkan otentikasi untuk menggunakan *recovery tool* yang mungkin memiliki kunci dekripsi.

- *Enterprise Key Management System / Centralized Encryption Solution*. Sistem mungkin telah menyimpan kunci dekripsi yang dapat diambil oleh tim penangan insiden.
- File lain seperti *hibernation file* dapat berisi *password*. *Software* enkripsi menyimpan kunci enkripsi dalam *memory* dan *memory* disimpan pada *disk* dengan *hibernation*. *Hibernation file* dapat digunakan langsung atau dikonversi menjadi *memory dump* [4].

6.3 Mengumpulkan Data *Volatile*

Data yang disimpan dalam *system memory* yang hilang saat mesin dimatikan disebut sebagai data *volatile*. Data ini meliputi data pada RAM, *system register*, atau data *cache* [5]. Tim penangan insiden harus memutuskan apakah data volatile dibutuhkan untuk insiden yang terjadi. Hal ini penting jika sistem menggunakan enkripsi untuk mengamankan data dan RAM komputer mungkin memiliki password atau password hash yang dapat digunakan kemudian.

Untuk mengumpulkan data *volatile*, dilakukan langkah-langkah berikut.

1. Menyusun *command shell* menggunakan *command shell* terpercaya dari *incident response toolkit*.
2. Menyusun cara mentransmisikan dan menyimpan informasi yang terkumpul.
    a. Data dapat dikumpulkan dan ditransmisikan dalam jaringan.
    b. Media penyimpanan lokal tambahan, seperti USB drive, dapat digunakan untuk menyimpan data.
    c. Tidak menyimpan data yang terkumpul pada sistem yang diinvestigasi karena dapat mengubah bukti.
3. Hash data untuk memastikan integritas.

Mengumpulkan data *volatile* penting untuk mengetahui kondisi sistem dan penyebab insiden serta menentukan timeline insiden dan langkah apa yang diperlukan selanjutnya. Data *volatile* hanya dapat dikumpulkan sebelum sistem dimatikan.

6.4 Mengumpulkan Data *Nonvolatile*

Data *nonvolatile* atau data tetap disimpan dalam media penyimpanan. Data ini tetap tersedia walaupun sistem dimatikan. Media penyimpanan dibuat duplikasinya. Bukti duplikat diperoleh dari pembuatan salinan dari bukti digital atau disebut juga proses *imaging*. Memberikan *write-blocker* terhadap media yang hendak dianalisis juga perlu dilakukan sehingga tidak memungkinkan terjadinya penulisan atau modifikasi data terhadap media tersebut. Pada data dapat dilakukan *hashing* untuk memastikan *image* file yang dibuat berhasil.

6.5 Analisis Insiden Menggunakan *Disk Image*

Ketika data sudah terkumpul, data perlu dianalisis. Analisis dilakukan terhadap *disk image*. *Software* virtualisasi dapat digunakan untuk meninjau *disk image*. *Disk image* bisa diatur menjadi *read-only*, sehingga *image* tetap sama dengan media penyimpanan asli.

7 Kesimpulan

Penggunaan teknologi enkripsi pada media penyimpanan dibutuhkan untuk mengamankan data agar data tidak dapat diakses oleh pihak yang tidak berhak. Namun, jika terjadi insiden yang melibatkan media penyimpanan, tim penanganan insiden harus mengidentifikasi media

penyimpanan pada sistem dengan tepat. Tim penanganan insiden harus memiliki pengetahuan mengenai proses menangani dan menanggapi insiden, mengerti teknologi penyimpanan data termasuk penyimpanan data terenkripsi, dan terbiasa dengan cara-cara mengakses sistem yang menggunakan media penyimpanan terenkripsi. Dengan menangani insiden secara tepat, kerugian pada organisasi dapat diminimalisasi.

Referensi

[1] Carrier, B. 2005. *File System Forensic Analysis*. Crawfordsville: Addison-Wesley.

[2] Hughes, J. 2004. *IEEE Standard for Encrypted Storage*.

[3] Lim, S., Park, J., Lee, C., & Lee, S. 2010. Forensic Artifacts Left by Virtual *Disk* Encryption Tools. *2010 3rd International Conference on Human-Centric Computing*.

[4] Mrdovic, S., Huseinovic, A. 2011. Forensic Analysis of Encrypted Volumes Using Hibernation File. *2011 19th Telecommunications Forum*.

[5] Nolan, R., O'Sullivan, C, Branson, J, & Waits, C. 2005. *First Responders Guide to Computer Forensics*.

[6] Scarfone, K., Grance, T, & Masone, K. 2008. *Computer Security Incident Handling Guide*. (NIST Special Publication 800-61, Revision 1).

[7] Scarfone, K., Souppaya, M., & Sexton, M. 2007. *Guide to Storage Encryption Technologies for End User Devices*. (NIST Special Publication 800-111).

[8] Shanks, W. 2009. *A Guide to Encrypted Storage Incident Handling*. SANS Institute.

[9] Thurner, S., Grun, M., Schmitt, S., & Baier, H. 2015. Improving the Detection of Encrypted Data on Storage Devices. *2015 Ninth International Conference on IT Security Incident Management & IT Forensics*, pp. 26-39.