**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 14**

**Case study - Risk Assessment, Risk Calculation, and Scenario of attack**

1. **Detecting incidents**

Diantara tantangan terkini dalam proses Incident Response, para perancang harus berhadapan dengan keputusan bagaimana sebuah organisasi memilah setiap kejadian. Beberapa kejadian adalah hasil dari setiap aktivitas system yang rutin berjalan, sedangkan lain nya merupakan indikator yang kritikal dari situasi yang membutuhkan respon mendadak.

Incident Classification merupakan proses dari mengevaluasi keadaan sekitar kejadian, menentukan kejadian mana yang merupakan kemungkinan Incident atau Incident pasti, dan juga mentukan apakah peristiwa tersebut merupakan Incident.

Incident Response Team mendesain proses yang digunakan untuk mengambil keputusan saat terjadi Incident. Setiap hari proses dari mengklasifikasi setiap Incident adalah tanggung jawab Incident Response Team.

Kandidat Incident dapat dideteksi ataupun diketahui melalui laporan-laporan dari berbagai sumber, seperti end users, system pendeteksi gangguan, software manajemen virus, dan system administrator. Laporan yang dibuat dengan baik, Incident Response Team dapat dengan efektif menjalankan prosedur dari perencanaan Incident Response.

Beberapa kejadian yang berbeda berlangsung di sekitar organisasi sebagai tanda akan kemunculan kandidat Incident. Dan sayangnya, kejadian yang sama akan terjadi ketika sebuah network menjadi kelebihan, sebuah komputer atau server mengalami error, atau beberapa operasi normal dari aset infromasi menyamai kemunculan indentifkasi indikasi Incident.

Untuk membantu membuat pendeteksian aktual Incident lebih dapat diandalkan dengan membagi menjadi beberapa ketegori, dengan begini dapat mempercepat organisasi dalam melakukan decision-making saat proses klasifikasi Incident dan memastikan rencana Incident Response yang sesuai dapan dilaksanakan secepatnya.

Berikut tiga kategori idikator Incident:

1. Possible (Mungkin)

Terdapat empat tipe yang dapat termasuk dalam kandidat Possible untuk aktual Incident:

* Kemunculan dari Unfamiliar Files di direktori system computer
* Kemunculan atau pengeksekusian Unknown programs atau process system computer
* Penggunaan kapasitas memory atau harddisk pada sistem komputer yang tidak biasa atau berlebihan
* Aplikasi atau sistem pada computer mengalami Error yang tidak biasa

1. Probable (Sangat Mungkin)

Terdapat empat tipe yang dapat termasuk dalam kandidat Probable untuk aktual Incident:

* Aktivitas pada jaringan atau pada history system computer di waktu yang tidak lazim
* Kemunculan akun baru yang tidak jelas
* Mendapat laporan bahwa terserang virus ataupun perusakan pada system computer
* Notifikasi dari IDS (Intrusion Detection System)

1. Definite (Pasti)

Terdapat delapan tipe yang dapat termasuk dalam kandidat Definite untuk aktual Incident:

* Penyalahgunaan akun aktif
* Terjadi perubahaan pada logs dalam system
* Kemunculan tools yang digunakan oleh hacker
* Notifikasi oleh partner atau user lain yang terhubung dengan system computer yang digunakan
* Notifikasi oleh hacker itu sendiri
* Kehilangan data
* Kehilangan akses untuk system ataupun data
* Adanya pelanggaran pada security

Setiap organisasi harus membuat process sendiri yang dapat digunakan untuk mengumpulkan dan mengevaluasi kandidat Incident. Banyak organisasi berusaha keras dengan hubungan antara kandidat Incident yang salah dan yang benar. Di dalam system desain yang baik, setiap aktivitas yang sah sebagai kandidat Incident dinyatakan salah harus dapat disaring dengan prosedur pengumpulan data ataupun program.

Dengan kualitas dan kuantitas pelatihan, dapat meningkatkan kemampuan pengumpulan data oleh staf yang terlibat sehingga dapat menghilangkan kandidat Incident yang salah pada saat pengumpulan data.

Terkadang Sistem pengumpulan kandidat Incident yang bagus dapat mengahasilkan data yang salah. Tetapi, keakuratan menentukan kandidat Incident harus tetap dikelola untuk meningkatkan proses pengumpulan di yang akan datang

Sebagaimana telah dicatat sebelumnya, salah satu tantangan pertama yang dihadapi desainer rencana IR adalah menciptakan proses untuk mengumpulkan dan mengevaluasi calon insiden untuk menentukan apakah mereka adalah insiden yang sebenarnya (atau keadaan cenderung menjadi insiden) atau nonevents, juga disebut palsu calon insiden positif. Hal ini sangat penting karena sebagian besar organisasi dapat menemukan diri mereka dibanjiri banyak calon insiden, dan sebagian besar akan positif palsu.

Setiap organisasi harus menciptakan proses sendiri yang dapat digunakan untuk mengumpulkan dan mengevaluasi calon insiden. Beberapa orang mungkin memilih untuk memiliki sebuah pusat insiden di mana semua calon insiden yang mengirim dari saat awal pengakuan. Orang lain mungkin memilih untuk memiliki lokasi ulasan terpisah secara geografis, mungkin didasarkan pada zona waktu, di mana penentuan awal dapat memilih untuk mengisolasi evaluasi calon insiden berdasarkan unit bisnis, lini produk, atau beberapa kriteria lain.

1. **Intrusion detection systems**

Sebuah sistem pendeteksi intrusi (IDS) adalah sebuah jaringan alarm pencuri dimana didesain untuk ditempatkan pada jaringan untuk menentukan apakah jaringan yang sedang digunakan tidak melanggar peraturan dari organisasi tersebut. Untuk memahami teknologi dengan IDS, anda harus memahami sifat dari sebuah percobaan intrusi terlebih dahulu.

Sebuah intrusi adalah sebuah jenis serangan atas asset informasi dimana pelaku mencoba untuk memperoleh akses ke dalam sistem atau jaringan ataupun mengganggu operasional sistem. Walaupun tanpa bermaksud untuk mencuri atau merusak sistem, tindakan ini tetap ada diluar penggunaan sistem yang sewajarnya. Walaupun serangan dilakukan secara otomatis, seperti virus dan distributed denial of services (DDOS), serangan seperti ini hampir selalu dilakukan oleh individu yang memiliki tujuan untuk merusak sebuah organisasi.

Sekuritas informasi IDS pertama kali dikomersialkan pada akhir tahun 1990-an. Sebuah IDS bekerja seperti alarm pencuri dimana mendeteksi pelanggaran dari penggunaan sebuah jaringan sesuai dengan konfigurasinya. Ini adalah analogi sebuah alarm pencuri pada jendela atau pintu terbuka yang mengaktifasi alarm. Alarm dari IDS dapat bersuara dan/atau visual ataupun dalam keadaan tanpa suara, dengan menggunakan pesan e-mail, notifikasi pager, log aktivitas, ataupun pesan ke sistem lainnya. Dengan hampir semua IDS, admisnistrator sistem dapat memilih konfigurasi dari beberapa notifikasi dan disesuaikan dengan tingkatan alarm setiap peringatan. Banyak IDS memperbolehkan administrator untuk konfigurasi sistem untuk menotifikasi mereka langsung tanpa masalah melalui e-mail ataupun pager. Sistem juga dapat dikonfigurasi lagi seperti untuk menotifikasi layanan sekuritas umum pada saat kejadian. Konfigurasi dengan IDS untuk menyediakan level kostumisasi dari deteksi dan respon dapat menjadi cukup kompleks.

Untuk memahami sifat operasional IDS, anda harus mengenal beberapa terminology yang unik dari IDS terlebih dahulu. Berikut adalah kumpulan dari kondisi dan defisini mengenai IDS yang diperoleh melalui literature pemasaran dari sebuah perusahaan ternama dalam bidang sekuritas informasi,TruSecure,tetapi konidis ini adalah representative antar industri:

* *Alert* atau *alarm*: sebuah indikasi dimana sebuah sistem sedang diserang atau dalam masa serangan. IDS membuat peringatan untuk menotifikasi administrator bahwa sebuah serangan sedang terjadi dan mungkin berhasil. Peringatan dapat berupa suara, pesan e-mail, notifikasi pager, pop-up windwos, atau log masuk yang ditulis tanpa mengambil tindakan apapun.
* *False attack stimulus*: sebuah tindakan yang mengaktivasi alarm dan menyebabkan kesalahan dimana tidak ada serangan yang terjadi. Skenario testing yang mengevaluasi konfigurasi dari IDS dapat menggunakan metode ini untuk menentukan apakah IDS dapat membedakan antara serangan asli dan *stimulus*.
* *False negative*: Kegagalan dari sistem IDS untuk beraksi terhadap sebuh serangan. Kegagalan yang paling fatal adalah kegagalan dalam mendeteksi serangan dimana yang menjadi tujuan utama dari IDS.
* *False positive*: sebuah peringatan yang mengindikasi bahwa sebuah serangan telah berhasil terjadi dimana sebenarnya tidak ada serangan. *False positive* terkadang dapat terjadi ketika IDS salah dalam mengidentifikasi kegiatan operasional sistem menjadi sebuah serangan. Peringatan ini dapat membuat pengguna menjadi tidak sensitif atau pedul terhadap alarm, yang mengakibatkan pengguna bereaksi lambat saat serangan benar-benar terjadi.
* *Noise*: Aktivitas alarm yang akurat dan penting tetapi tidak signifikan sebagai serangan yang berpotensi berhasil. Serangan yang gagal adalah sumber dari *noise* pada IDS dan beberapa dari *noise* ini bukan merupakan serangan, tetapi pekerja menggunakan jaringan local untuk eksperimen dengan *scanning* dan alat enumerasi tanpa maksud untuk merusak. *Noise* tidak berbahaya dan tidak memiliki potensi untuk mengakibatkan kerusakan.
* *Site policy*: Peraturan dan panduan konfigurasi pemerintahan implementasi dan operasi pada IDS dalam organisasi.
* *Site policy awareness*: sebuah kelebihan IDs adalah memodifikasi *site policy* secara dinamis pada reaksi atau respon pada kegiatan lingkungan. Sebuah *smart IDS* dapat bereaksi sesuai dengan panduan yang dipelajari oleh administrator serta lingkungan local. Administrator IDS memperoleh laporan sesuai dengan *profile* dibandingkan dinotifikasi untuk perubahan kecil seperti *file* telah dirubah atau *user login* gagal. Contoh lain dari penggunaan sebuah *smart IDS* adalah ketika IDS tahu bahwa tidak perlu untuk menotifikasi administrator ketika sebuah serangan menggunakan dokumen yang telah diketahui dan dibuat untuk melawan sistem dimana IDS tahu cara untuk mengatasi serangan tersebut. Ketika IDS dapat menerima beberapa respon *profile* berdasarkan perubahan scenario serangan dan lingkungan, itu membuat IDS lebih berguna.
* *True Attack Stimulus*: sebuah kejadian yang mengaktifikasi alarm dan menyebabkan IDS bereaksi seakan-akan sebuah serangan sedang terjadi. Serangan ini mungkin adalah serangan ketika seseorang sedang mencoba masuk kedalam sistem atau mungkin sebuah *drill*, beberapa tes dari segmen jaringan oleh anggota sekuritas menggunakan alat *hacker*.
* *Confidence Value*: sebuah nilai yang berasosiasi dengan kelebihan dari IDS untuk medeteksi dan mengenali sebuah serangan dengan benar. *Confidence Value* sebuah organisasi pada IDS ditentukan berdasarkan pengalaman dan pengukuran performa sebelumnya. *Confidence Value*, jenis dari *fuzzy logic,* menyediakan sebuah bagian dari informasi untuk membantu administrator dalam menentukan apakah peringatan serangan tersebut menyatakan serangan yang sering terjadi atau IDS bereaksi terhadap *false attack stimuli* dan membuat sebuah *false positive*. Sebagai contoh, apabila sebuah sistem dianggap mampu untuk melaporkan sebuh serangan *denial of service* dengan kepastian 90% mengirim sebuah peringatan, dengan ada kemungkinan bahwa sebuah serangan sedang terjadi.
* *Alarm Filtering*: Ada proses pengelompokan peringatan serangan dimana sebuah IDS mendeteksi untuk membedakan atau menyusun *false positive* dari serangan lebih effisien. Setelah IDS di *install* dan konfigurasi, administrator dapat menentukan *alarm filterin* dengan menjalankan sistem pertama kali untuk mendeteksi apa tipe *false positives* yang dihasilkan dan kemudian disesuaikan dengan pengelompokan jenis *alarm*. Sebagai contoh, administrator membuat IDS untuk membuat *alarm* tertentu yang diproduksi oleh *false attack stimuli* atau operasi normal dari jaringan. Penyaringan a*larm* sama seperti penyaring *packet* agar dapat memfilter barang dengan *IP Address* asal atau tujuan, tetapi memperoleh kemampuan tambahan yang dapat menyaring berdasarkan *operation system*,*confidence values,*jenis alarm, atau keparahan *alarm.*
* *Alarm Clustering:* konsolidasi dari *alarm* yang memiliki kesmaan menjadi sebuah alarm dengan tingkat lebih tinggi. Dengan ini memotong jumlah *alarm* yang dihasilkan,mengurangi administrasi. Ini mengindikasi bahwa ada hubungan antara setiap element dari *alarm.*
* *Alarm Compaction: alarm clustering* berdasarkan frekuensi, kemiripan dalam jenis serangan, kemiripan dalam target serangan, atau kemiripan yang lain. Dengan *alarm clusterin* sebelumnya, ini mengurangi jumlah *alarm* yang dihasilkan, mengurangi administrasi. *Alarm clustering* juga dapat indikasi bahwa sebuah hubungan ada diantara elemen alarm ketika memiliki atribut yang sama.

1. **Incident decision making**

Kejadian yang akan terjadi harus dievaluasi untuk menentukan kejadian yang benar-benar terjadi dan tidak. Menurut US-CERT, pendekatan umum untuk membatasi dan mendeteksi kejadian yang akan terjadi terdiri dari :

1. Mengumpulkan kejadian yang akan terjadi menggunakan prosedur dokumen dengan baik
2. Menyelidiki kejadian yang akan terjadi menggunakan sistem dan metode yang ada
3. Jika kandidat ditentukan selain aktifitas yang resmi, segera memulai prosedur tanggap instruksi

Kumpulan aktifitas dan analisis data yang diperlukan untuk membantu dalam mendeteksi dan merinci insiden. Bahkan jika insiden tidak terdeteksi secara real time, data yang dikumpulkan oleh sistem perekaman otomatis dapat membantu tim dalam memahami operasi yang berjalan normal dan operasi rutin untuk proses sistem, mentransmisikan, dan penyimpanan informasi untuk organisasi.

**SIMPULAN**

Hal utama dalam IT Risk Management adalah:

1. Incident Classification merupakan proses dari mengevaluasi keadaan sekitar kejadian, menentukan kejadian mana yang merupakan kemungkinan Incident atau Incident pasti, dan juga mentukan apakah peristiwa tersebut merupakan Incident.
2. Sebuah sistem pendeteksi intrusi (IDS) adalah sebuah sistem alarm dimana didesain untuk ditempatkan pada jaringan untuk menentukan apakah jaringan yang sedang digunakan tidak melanggar peraturan dari organisasi tersebut.
3. Menurut US-CERT, pendekatan umum untuk membatasi dan mendeteksi kejadian yang akan terjadi terdiri dari :
4. Mengumpulkan kejadian yang akan terjadi menggunakan prosedur dokumen dengan baik
5. Menyelidiki kejadian yang akan terjadi menggunakan sistem dan metode yang ada
6. Jika kandidat ditentukan selain aktifitas yang resmi, segera memulai prosedur tanggap instruksi

**DAFTAR PUSTAKA**

1. Whitman, M.E., Mattoro, H.J. (2013). ***Principles of Incident Response and Disaster Recovery***.