**LECTURE NOTES**

**IT Risk Management and Disaster Recovery**

**KDS – Name SME**

**Session 11**

**Case study - Business Impact Analysis**

**Pengumpulan data dan dokumen**

Untuk membuat dokumen incident response plan, diperlukan data data kumpulan aktifitas dan analisis data yang diperlukan untuk membantu dalam mendeteksi dan merinci insiden. Termasuk 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 dalam system secara keseluruhan, termasuk proses mentransmisikan, dan penyimpanan informasi untuk organisasi. Beberapa informasi yang dibutuhkan bagi tim IRP untuk mengumpulkan insiden ditunjukkan pada Tabel 1.

Table 1 Kategori data dan tipe dan jenis data yang harus dikumpulkan

|  |  |
| --- | --- |
| Data Category | Types of Data Collect |
| Network performance | * Total traffic load in and out over time (paket byte and connection counts) and by event (such as new product or service please) * Traffic load (precentage of packets bytes, connection) – in and out over time sorted by protocol, source address, destination address and other packet header data * Error counts on all network interface |
| Other network data | * Service initiation requests * Name of the user / host requesting the service * Network traffic (packet headers) * Succesful connection * Connection duration * Connection flow (sequence of packet from initiation to termination) * States associated with network interface (up down) * Network sockets currently open * Whether or not network interface card * Network probes and scans * Result of administrator probes |
| System performance | * Total resource use over time (CPU, memory and disk) * Status and errors reported by systems and hardware devices * Changes in system status, including shutdowns and restarts * File system status (where mounted, free space by partition, open files, biggest files) over time and at specific times * File system warnings (low free space, too many open files, file exceeding allocated size) * Disk counters (input/output, queue length) over time and at specific times * Hardware availibility (modems, NIC, memory) |
| Other system data | * Action requiring special privilages * Successful and failed logins * Modem activities * Presence of new services and devices * Configuration of resources and devices |
| Process performance | * Amount of resources used (CPU, memori, disk, time) by specific process over time, top resources-consuming process * System and user processes and service executing at any given time |
| Other process | * Process start-up time arguments filenames * Process exit status, time, duration resources consumed * The means by which each process is normally initiated * Devices used by specific process * Files currently open by specific process |
| Files and directories | * List of files, directories,attributes * Cryptographic checksums for all files and directories * Accesses (open, create, modify, execute, delete), time, date * Changes to sizes, contents, protections, types, locations * Changes to access control list on system tools * Additions and deletions of files and directories * Result of virus scanners |
| Applications | * Application and service specific information such as network traffic (packet content), mail logs, FTP log, instrution detection system logs, DBMS logs * Service specific information could be :  1. For FTP request : Files transferred and connections statistics 2. For Web request : Pages accesses, credentials of the requestor, connection statistics, user request over time, which pages are most requested, and who is requesting them 3. For mail requests : Sender, receiver, size and tracing information; for a mail server, number of messages over time, number of queued messages 4. For DNS requests : Questions, answer and zone transfers 5. For a file system server : File transfer over time 6. For a database server : Transactions over time |
| Log file | * Result of scanning, filtering and reducing log file contents * Checks for log file consistency (increasing file size over time, use of consecutive, increasing time stamps with no gaps) |
| Vulnerabilities | * Result of vulnerabilitis scanners * Vulnerability patch logging |

**Mekanisme Pengumpulan Data**

Log file adalah sebuah file yang berisikan kumpulan atau catatan data transaksi. Terdapat berbagai jenis log diantaranya adalah error log, cache log, user log, update log, dan incident log. Log dapat menjadi rujukan ketika suatu incident terjadi, bai pada network, device, database, ataupun aplikasi. Berikut adalah beberapa hal yang perlu diperhatikan dalam manajemen log :

1. Log akan mencatat seluruh transaksi atau incident yang terjadi sehingga akan menghasilkan data dalam jumlah yang sangat besar yang mengakibatkan besarnya ukuran file yang dapat mencapai besaran Gigabytes atau bahkan Terabytes
2. Buatlah rotasi berjangka setiap satuan waktu yang disepakati seperti setiap satu minggu atau satu bulan sekali, di mana log transaksi atau incident yang sudah melewati satuan waktu tersebut di backup ke dalam file atau directory yang berbeda sehingga system akan selalu mencatat transaksi atau incident yang dimulai dari awal pada setiap satuan waktu tersebut
3. Log file yang telah diarsipkan setelah satuan waktu tertentu sebaiknya di musnahkan karena berhubungan dengan kemanan jika dapat diakses oleh pihak-pihak yang tidak memiliki wewenang. Seorang administratorpun juga memiliki wewenang terbatas untuk mengakses arsip tersebut
4. Jika memang arsip log file diperlukan, maka sebaiknya di enkrip.
5. Musnahkan arsip log file yang telah usang dan yang sudah tidak diperlukan lagi

Setelah semua dokumen selesai dibuat maka dokumen dokumen disusun berdasarkan 3 kriteria seperti terlihat pada gambar 1, yaitu:

* Before Attack
* After Attack
* During attack

Dokumen before attack atau before incident biasanya berisi dokumen tentang test untuk vulnerability, testing dan training.

Untuk kegiatan testing dapat mengikuti strategi dibawah ini:

* Desk check

Cocokan komoponen yang ada di dokumen dengan kenyataannya dan buat daftar komponen mana yang benar dan salah.

* Structured walk-through

Review langkah-langkah yang ada dalam dokumen dan cocokan dengan aktualnya dan diskusikan apakah langkah langkah tindakan yang ada didokumen sudah sesuai dengan kenyataannya.

* Simulation

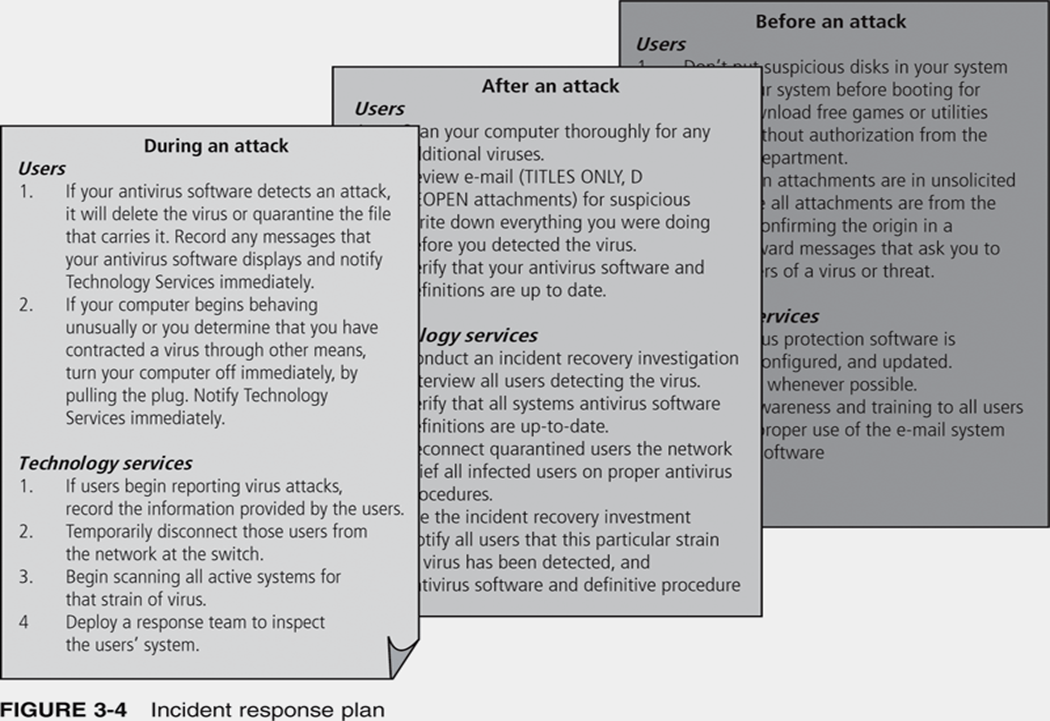
Simulasikan rencana yang ada dalam dokumen secara terpisah pisah atau pada masing masing departemen satu persatu dan perhatikan kinerja masing-masing bagian, dalam simulasi ini secara keseluruhan proses masih bisa berjalan.

* Parallel testing

Individu bertindak seolah-olah sebuah kejadian telah terjadi, namun tanpa mengganggu operasi normal

* Full interruption

Individu mengikuti setiap prosedur, termasuk gangguan layanan, pemulihan data dari backup. Simulasi ini mungkin harus menghentikan system secara keseluruhan, dan sangat beresiko.



Gambar 1. Susunan dokumen incident response plan

Selain itu kegiatan training juga masuk dalam dokumen before incident. Yang perlu diperhatikan adalah training untuk manager seharusnya berbeda dengan training untuk orang orang teknik.

Dokumen after incident berisi apa yang harus dikerjakan setelah incident, seperti bagaimana mendokumentasikan incident, rencana review dan tindak lanjut catatan pada saat incident yang tujuan nya adalah untuk memperbaiki kualitas dari dokumen during incident.

**SIMPULAN**

1. Training dan simulasi adalah merupakan hal yang sangat penting supaya dokumen incident response plan benar benar dapat sesuai dengan kondisi sebenarnya dan benar benar dapat berguna saat incident terjadi.
2. Meletakkan dokumen incident response plan juga harus diperhatikan dimana dokumen during incident harus berada paling depan, kemudian dokumen after incident dan diikuti dokumen before incident.

**DAFTAR PUSTAKA**

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