Domain 7: Operasi keamanan

TUJUAN UJIAN DALAM BAB INI

- Keamanan Administratif
- Sensitif Informasi / Media Keamanan
- Asset Management
- Kontinuitas Operasi
- Manajemen Insiden Response

KEAMANAN ADMINISTRASI

Keamanan administratif menyediakan sarana untuk mengontrol akses operasional masyarakat untuk data.

Menurut Keamanan Informasi Executive Order 12356-Nasional, Benda memiliki label dan subjek memiliki izin./Label

Informasi sensitif
Informasi sensitif membutuhkan perlindungan, dan informasi yang secara fisik berada pada beberapa bentuk media

Pelabelan / menandai

Mungkin langkah yang paling penting dalam keamanan media proses mencari informasi sensitif dan pelabelan atau penandaan sebagai sensitif. Bagaimana data diberi label harus sesuai dengan skema klasifikasi data organisasi.

Penyimpanan

Ketika menyimpan informasi sensitif, adalah lebih baik untuk mengenkripsi data. Enkripsi data pada saat istirahat sangat mengurangi kemungkinan data yang diungkapkan dalam mode terwujud unauthor- karena masalah keamanan Media. Penyimpanan fisik dari media yang mengandung informasi sensitif tidak boleh dilakukan secara sembarangan, apakah data dienkripsi atau tidak.
Penyimpanan
Media dan informasi memiliki masa manfaat yang terbatas. Retensi informasi sensitif seharusnya tidak bertahan melampaui masa manfaat atau persyaratan hukum (mana yang lebih besar), karena sia-sia memperlihatkan data ancaman pengungkapan saat data tidak lagi dibutuhkan oleh organisasi.

Data remanence
Data remanen adalah data yang berlangsung di luar kemampuan noninvasif untuk menghapusnya.

Degaussing

Dengan memperkenalkan medan magnet eksternal melalui penggunaan degausser, data pada media penyimpanan magnetik dapat dibuat tidak terpulihkan. Sebuah degausser menghancurkan berintegritas dari magnetisasi dari media penyimpanan itu sendiri, membuat data dipulihkan.

Kerusakan fisik

Kerusakan fisik, bila dilakukan dengan benar, dianggap cara yang paling aman media sanitasi. Salah satu alasan untuk tingkat yang lebih tinggi dari jaminan adalah karena kemungkinan besar kesalahan yang mengakibatkan data yang remanence dengan menyeka atau degaussing.

Shredding

Bentuk sederhana media sanitasi yang merobek-robek, jenis kerusakan fisik. Meskipun istilah ini kadang-kadang digunakan dalam kaitannya dengan Timpa data, di sini shredding mengacu pada proses pembuatan data yang dicetak pada hard copy, atau benda-benda kecil seperti floppy disk atau optical, dipulihkan. Informasi sensitif seperti dicetak informasi yang perlu diparut sebelum dibuang untuk menggagalkan serangan dumpster diving. Dumpster diving adalah serangan fisik di mana seseorang pulih sampah dengan harapan akan menemukan informasi sensitif yang belum aman terhapus atau hancur

MANAJEMEN ASET

Pendekatan holistik untuk keamanan informasi operasional mengharuskan organisasi untuk fokus pada sistem serta orang, data, dan media. Sistem keamanan komponen penting lain untuk keamanan operasi, dan ada kontrol khusus yang dapat sangat membantu sistem keamanan di seluruh siklus hidup sistem.

manajemen konfigurasi

Praktek manajemen konfigurasi dasar yang terkait dengan sistem keamanan akan melibatkan tugas-tugas seperti menonaktifkan layanan yang tidak perlu; menghapus program-program asing; memungkinkan kemampuan keamanan seperti firewall, antivirus, dan intrusi deteksi tion atau pencegahan sistem; dan keamanan dan pemeriksaan log configurating.

baselining

Keamanan baselining adalah proses menangkap titik dalam pemahaman saat konfigurasi sistem keamanan saat ini. Membangun sarana mudah untuk menangkap konfigurasi sistem keamanan saat ini dapat sangat membantu dalam menanggapi insiden keamanan potensial

manajemen kerentanan

Kerentanan pemindaian adalah cara untuk menemukan konfigurasi miskin dan patch hilang dalam lingkungan.

Kerentanan zero-day dan zero-day eksploitasi

Sebuah kerentanan zero-day adalah kerentanan yang dikenal sebelum adanya patch. Kerentanan zero-day, juga biasa ditulis 0-hari, menjadi semakin bertambah ingly penting sebagai penyerang menjadi lebih terampil dalam penemuan, dan pengungkapan kerentanan zero-day sedang menghasilkan uang.

FAKTA CEPAT

Karena variabilitas dari proses manajemen perubahan, bernama fase tertentu belum ditawarkan di bagian ini. Namun, aliran umum dari proses manajemen perubahan meliputi:
• Mengidentifikasi perubahan
• Mengusulkan perubahan
• Menilai risiko yang terkait dengan perubahan
• Pengujian perubahan
• Penjadwalan perubahan
• Memberitahukan pihak yang terkena dampak dari perubahan
• Menerapkan perubahan
• Hasil Pelaporan pelaksanaan perubahan

KONTINUITAS OPERASIONAL

Kelangsungan operasional adalah prinsipnya berhubungan dengan porsi ketersediaan kerahasiaan, integritas, dan ketersediaan triad.

Perjanjian Layanan Tingkat

Sebuah Perjanjian Layanan-Level (SLA) menetapkan semua harapan mengenai perilaku departemen atau organisasi yang bertanggung jawab untuk menyediakan layanan dan kualitas layanan yang disediakan.

Toleransi kesalahan

Agar sistem dan solusi dalam sebuah organisasi untuk dapat terus menyediakan ketersediaan operasional, mereka harus dilaksanakan dengan toleransi kesalahan dalam pikiran. Ketersediaan tidak hanya semata-mata terfokus pada persyaratan sistem uptime tetapi juga mensyaratkan bahwa data yang dapat diakses secara tepat waktu.

Backup

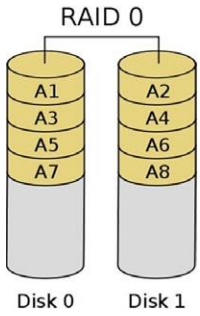
Agar data dapat dipulihkan dalam kasus kesalahan, beberapa bentuk cadangan atau redundansi harus disediakan. Meskipun media tape magnetik adalah cukup ogy technol- tua, masih repositori paling umum data cadangan. Tiga tipe dasar dari backup: backup penuh, incremental backup, dan backup diferensial.

Incremental dan diferensial

Incremental backup hanya file arsip yang telah berubah sejak terakhir cadangan apapun dilakukan. Backup diferensial akan arsip file yang telah SDTV ged sejak full backup terakhir.

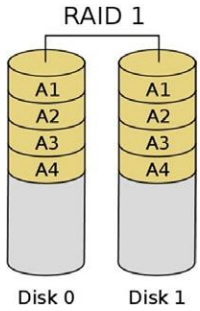
RAID 1: Cermin set

RAID 1 menciptakan / menulis duplikat yang tepat dari semua data ke disk tambahan. Menulis kinerja menurun, meskipun kinerja membaca dapat melihat peningkatan. Gambar 7.2 menunjukkan RAID 1




GAMBAR 7.1

RAID 0: bergaris diatur.




GAMBAR 7.2

RAID 1: set cermin.

RAID 2: kode Hamming

RAID 2 adalah teknologi warisan yang membutuhkan baik 14 atau 39 hard disk dan controller hardware yang dirancang khusus, yang membuat RAID 2 biaya mahal. RAID 2 garis di tingkat bit.

RAID 3: Belang set dengan paritas khusus (tingkat byte)

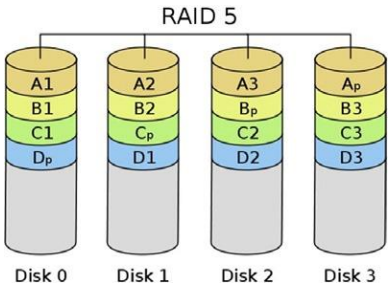
Striping diinginkan karena keuntungan kinerja yang terkait dengan penyebaran data di beberapa disk. Namun, striping saja tidak diinginkan karena kurangnya redundansi. Dengan RAID 3, data, pada tingkat byte, bergaris-garis di beberapa disk, tetapi disk tambahan memanfaatkan untuk penyimpanan informasi paritas, yang digunakan untuk pemulihan dalam hal kegagalan.

RAID 4: Belang set dengan paritas khusus (tingkat blok)

RAID 4 menyediakan fungsi yang sama dengan RAID 3 tetapi garis-garis data pada blok, bukan byte, tingkat. Seperti RAID 3, RAID 4 mempekerjakan dedicated paritas berkendara daripada memiliki data paritas didistribusikan di antara semua disk, seperti dalam RAID 5.

RAID 5: Belang set dengan paritas didistribusikan

Salah satu konfigurasi RAID yang paling populer adalah bahwa RAID 5, bergaris diatur dengan dis paritas tributed. Seperti penggerebekan 3 dan 4, RAID 5 menulis informasi paritas yang digunakan untuk tujuan pemulihan. RAID 5 menulis di tingkat blok, seperti RAID 4. Namun, tidak seperti penggerebekan 3 dan 4, yang memerlukan disk khusus untuk informasi paritas, RAID 5 dis upeti informasi paritas di beberapa disk. Salah satu alasan untuk RAID 5 ini




GAMBAR 7.3
RAID 5: bergaris diatur dengan paritas didistribusikan.

popularitas adalah bahwa biaya disk untuk redundansi adalah lebih rendah dari satu set cermin. RAID 5 memungkinkan untuk pemulihan data dalam hal bahwa setiap satu disk gagal. Gambar 7.3 menunjukkan RAID 5.

RAID 6: Belang set dengan paritas ganda didistribusikan
Sementara RAID 5 mengakomodasi kehilangan salah satu drive dalam array, RAID 6 dapat memungkinkan untuk kegagalan dua drive dan masih fungsi. Redundansi ini dicapai dengan menulis informasi paritas yang sama untuk dua disk yang berbeda.

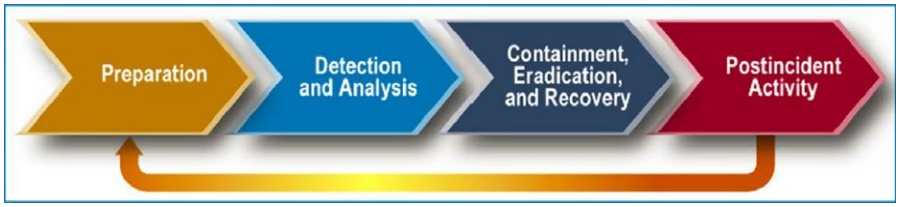
RAID 1 þ 0 atau RAID 10
RAID 1 þ 0 atau RAID 10 adalah contoh dari apa yang dikenal sebagai RAID bersarang atau RAID multi, yang berarti bahwa satu tingkat RAID standar dikemas dalam lagi. Dengan RAID 10, yang juga biasa ditulis sebagai RAID 1 þ 0 secara eksplisit menunjukkan bersarang, konfigurasi adalah bahwa satu set bergaris dari cermin.

| Tabel Tingkat 7.1 RAID | |
|---|---|
| RAID | Tingkat Keterangan |
| RAID 0 | Blok-tingkat bergaris set |
| RAID 1 | Mirrored set |
| RAID 3 | Byte-tingkat striping dengan paritas khusus |
| RAID 4 | Blok-tingkat striping dengan paritas khusus |
| RAID 5 | Blok-tingkat striping dengan paritas didistribusikan |
| RAID 6 | Blok-tingkat striping dengan paritas ganda didistribusikan |

Redundansi sistem
Meskipun redundansi dan ketahanan data, disediakan oleh RAID dan backup solusi, yang penting, pertimbangan lebih lanjut harus diberikan kepada sistem itu sendiri yang menyediakan akses ke data yang berlebihan ini.
Banyak sistem dapat memberikan redundansi hardware internal komponen yang sangat rentan terhadap kegagalan. Contoh yang paling umum dari redundansi ini built-in adalah sistem atau perangkat yang telah membazir daya onboard dalam hal kegagalan listrik. Kadang-kadang, sistem hanya memiliki versi modular lapangan-tergantikan komponen umum gagal. Meskipun secara fisik mengganti power

supply dapat meningkatkan downtime, memiliki persediaan modul cadang untuk layanan server seluruh datacenter akan menjadi lebih murah daripada memiliki semua server dikonfigurasi dengan power supply redundant diinstal.
system berlebihan membuat seluruh system yang tersedia menjadikan kegagalan system utama.

INSIDEN RESPON MANAJEMEN
Sebuah insiden keamanan adalah kejadian berbahaya pada sistem atau jaringan. Semua organisasi akan mengalami insiden keamanan. Manajemen respon insiden adalah metodologi ketat dan diuji untuk mengidentifikasi dan merespon insiden ini.
Metodologi
Gambar 7.4 adalah dari NIST Special Publication 800-61: Keamanan Komputer Insiden Panduan Penanganan (lihat http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf), yang menguraikan siklus hidup respon insiden dalam empat langkah:
Cluster ketersediaan tinggi
Sebuah cluster ketersediaan tinggi (juga disebut cluster failover) menggunakan beberapa sistem yang sudah diinstal, dikonfigurasi, dan ditancapkan, sehingga jika kegagalan menyebabkan salah satu sistem gagal maka yang lain dapat mulus dimanfaatkan untuk mempertahankan memanfaatkan- yang kemampuan layanan atau aplikasi yang disediakan.




GAMBAR 7.4
NIST Respon Insiden Hidup cycle.2

1. Persiapan
2. Deteksi dan analisis
3. kendali, pemberantasan, dan pemulihan
Kegiatan 4. Postincident
Banyak metodologi penanganan insiden mengobati penahanan, pemberantasan, dan pemulihan tiga langkah yang berbeda, seperti yang kita akan di buku ini. Nama lain untuk setiap langkah yang terkadang digunakan; di sini adalah siklus hidup enam langkah kita akan mengikuti, dengan nama-nama alternatif yang terdaftar:

1. Persiapan
2. Deteksi dan analisis (alias identifikasi)
3. Containment
4. Pemberantasan
5. Pemulihan
6. Pelajaran (aktivitas alias postincident, postmortem, atau pelaporan)
Penting untuk diingat bahwa langkah terakhir feed kembali ke langkah pertama, seperti yang ditunjukkan sebelumnya pada Gambar 7.4. Sebuah organisasi dapat menentukan staf yang

insuffi- sien dilatih untuk menangani insiden selama pelajaran fase belajar. Pelajaran yang kemudian diterapkan untuk persiapan melanjutkan, di mana staf akan dilatih dengan benar.

Persiapan

Tahap persiapan termasuk langkah-langkah yang diambil sebelum insiden terjadi. Ini termasuk pelatihan, menulis kebijakan dan prosedur penanganan insiden, dan menyediakan alat-alat seperti laptop dengan mengendus software, kabel crossover, media OS asli, removable drive, dll Persiapan harus mencakup segala sesuatu yang mungkin diperlukan untuk menangani insiden atau yang akan membuat insiden respon lebih cepat dan lebih efektif.

Pemberantasan

Tahap pemberantasan melibatkan dua langkah: menghapus perangkat lunak berbahaya dari sistem terganggu dan memahami penyebab insiden tersebut sehingga sistem dapat dipercaya dibersihkan dan aman dikembalikan ke status operasional kemudian dalam tahap pemulihan. Agar suatu organisasi untuk andal pulih dari insiden, penyebabnya harus ditentukan sehingga sistem tersebut dapat dikembalikan ke keadaan yang dikenal baik tanpa risiko kompromi Bertahan atau reoccurring.

Pemulihan

Tahap pemulihan melibatkan hati-hati mengembalikan sistem atau sistem untuk opera- Status nasional. Biasanya, unit bisnis yang bertanggung jawab untuk sistem akan menentukan kapan sistem akan kembali online. Mempertimbangkan kemungkinan bahwa infeksi mungkin telah bertahan melalui tahap pemberantasan. Untuk alasan ini, pemantauan ketat dari sistem itu setelah dikembalikan ke produksi yang diperlukan.

Jenis serangan

Bagian ini akan memberikan informasi dasar tentang jenis-jenis serangan yang lebih umum dialami dan menanggapi dalam organisasi.

Pembajakan dan MITM

Pembajakan kompromi sesi jaringan yang ada, kadang-kadang merebut kendali itu. Protokol yang lebih tua seperti Telnet mungkin rentan terhadap pembajakan.

Malware

Malware, atau kode berbahaya / software, merupakan salah satu jenis yang paling terkenal dari ancaman terhadap sistem informasi. Ada banyak jenis malware, beberapa rinci pada Tabel 7.2, yang telah berevolusi selama bertahun-tahun untuk terus menyebabkan stres untuk operasi.

| Tabel 7.2 Jenis Malware | |
|---|---|
| jahat<br>kode | |
| Virus | Virus adalah malware yang tidak propagate diri: memerlukan carrier, seperti manusia bergerak secara manual perangkat USB terinfeksi dari satu sistem ke sistem lain |
| Virus makro | Sebuah virus makro adalah malware yang menginfeksi dokumen Microsoft Office dengan cara menanamkan macro berbahaya dalam diri mereka |
| Worm | Worm adalah malware yang diri menjalar. |

| | |
|---|---|
| | Beberapa nama yang paling terkenal dari malware jatuh di bawah kategori worm: Code Red, Nimda, SQL Slammer, Blaster, MyDoom, dan Witty |
| Trojan Horse | Sebuah Trojan Horse adalah malware yang memiliki dua fungsi: satu terbuka (seperti permainan) dan satu rahasia (seperti menyediakan penyerang dengan akses backdoor persisten) |
| Rootkit | Rootkit adalah malware yang melanggar integritas sistem dan difokuskan pada bersembunyi dari administrator sistem. Kemampuan khas include file, folder, proses, dan koneksi jaringan persembunyian |

| Tabel 7.3 Denial of Service Contoh | | |
|---|---|---|
| Nama DoS | Tipe | Deskripsi |
| Tanah | paket cacat | Serangan darat menggunakan paket SYN palsu yang mencakup alamat IP korban baik sebagai sumber dan tujuan |
| Smurf | sumber daya kelelahan | Serangan Smurf melibatkan ICMP banjir. Penyerang mengirim pesan ICMP Echo Request dengan palsu alamat sumber korban ke alamat broadcast yang diarahkan dari jaringan dikenal sebagai penguat Smurf. Sebuah penguat Smurf adalah jaringan publik menghadap yang mengirimkan sejumlah besar tanggapan dari lalu lintas yang dikirim ke alamat broadcast diarahkan |
| SYN Banjir | sumber daya kelelahan | Sebuah SYN Banjir mengirimkan banyak paket TCP dengan flag SYN diatur ke korban dan mengabaikan paket SYN / ACK korban. Korban antrian koneksi setengah terbuka akhirnya dapat mengisi dan tidak dapat memproses koneksi baru |
| titik air mata | paket cacat | Serangan teardrop mengirimkan paket dengan tumpang tindih fragmen offset, yang mungkin crash sistem yang mencoba |

| | | |
|---|---|---|
| | | untuk berkumpul kembali fragmen |
| Ping dari kematian | paket PinMalformed | Ping of Death mengirimkan terfragmentasi Permintaan ICMP Echo bahwa, sekali dipasang kembali, lebih besar dari ukuran maksimum paket IP |
| Fraggle | Fragg Resource kelelahan | The Fraggle serangan adalah variasi dari serangan Smurf. sementara Smurf menggunakan ICMP, fraggle menggunakan UDP |
| DNS refleksi | | Sebuah serangan DNS refleksi mengirimkan nomor tinggi permintaan DNS palsu dari korban untuk diakses publik rekursif server nama DNS |

IKHTISAR TUJUAN UJIAN

Dalam bab ini,telah membahas keamanan operasi. Operasi keamanan menyangkut keamanan sistem dan data ketika sedang aktif digunakan dalam produksi lingkungan pemerintah. Pada akhirnya, keamanan operasi adalah tentang orang-orang, data, media, dan perangkat keras; yang semuanya adalah elemen yang perlu dipertimbangkan dari perspektif keamanan. Infrastruktur keamanan teknis terbaik di dunia akan diberikan diperdebatkan jika individual dengan akses istimewa memutuskan untuk berbalik melawan organisasi dan tidak ada kontrol preventif atau detektif di tempat dalam organisasi.