AUDITING SISTEM KEAMANAN JARINGAN

M. Rudyanto Arief
Dosen STMIK AMIKOM Yogyakarta

Abstract

The process of auditing ensures that regulations, policies, and procedures are carried out in a manner that is consistent with your organization's standards. From an audit, you can determine whether computer usage and escalation processes are in place, if security is adequate, and if privilege-granting processes are appropriate.

Keywords: *Regulations, policies, audit, privilege audit, usage audit, escalation audit.*

Pendahuluan

Tujuan keamanan komputer (security goals) adalah terjaminnya "confidentiality", "integrity", dan "availability" sebuah sistem komputer. Untuk menjamin supaya tujuan keamanan tersebut dapat tercapai maka diperlukan beberapa proses yang dilakukan secara bersama-sama. Salah satu proses tersebut adalah dengan melakukan audit terhadap sistem komputer dan jaringan komputer didalamnya.

Auditing adalah sebuah untuk melacak semua kejadian-kejadian, kesalahan-kesalahan, dan percobaan akses dan otentikasi dalam sebuah komputer server. Auditing membantu seorang administrator jaringan dan analis keamanan komputer untuk mengidentifikasi kelemahan-kelemahan jaringan komputer dalam sebuah organisasi dan sangat membantu dalam mengembangkan kebijakan dalam keamanan jaringan komputer.

Melalui proses audit, integritas data dapat dijamin, juga dapat memelihara kerahasiaan data dan ketersediaanya tetap terjamin.

Secara garis besar, audit terhadap sebuah sistem keamanan jaringan komputer dibagi kedalam 3 kategori yaitu: audit terhadap hak akses (privilege audit), audit terhadap penggunaan sumber daya (usage audit), audit terhadap eskalasi (escalation audit).

Privilege Audit

Audit jenis ini tujuannya adalah untuk melakukan verifikasi apakah "group", "roles" dan "account" sudah diterapkan dengan tepat dalam sebuah organisasi dan keamanan yang di terapkan didalamnya juga sudah tepat. Audit ini juga melakukan verifikasi apakah kebijakan-kebijakan yang di terapkan dalam sebuah organisasi sudah diikuti dengan benar atau belum, sudah akurat atau belum, dan apakah akses ke sistem sudah di terapkan dengan benar.

Gambar 1 Privilege Audit Salah Satu Metode Audit

Privilege audit dilakukan dengan cara melakukan review secara lengkap terhadap semua "group" dan "account" dalam sebuah sistem jaringan untuk sebuah organisasi. Misalnya,ketika seorang karyawan di mutasi dalam sebuah organisasi, maka nama karyawan tersebut seharusnya di hapus dari grupnya yang lama. Kesalahan dalam melakukan hal tersebut dapat menyebabkan seorang user bisa mendapatkan akses lebih tinggi dari yang seharusnya didapatkan oleh user tersebut.

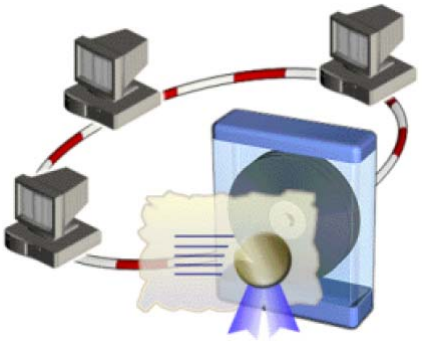
Gambar 2 Pengaturan Groups dan Account yang Tepat, Salah Satu Metode Privilege Audit

Usage Audit

Audit jenis ini melakukan verifikasi apakah perangkat lunak dan sistem yang digunakan dalam sebuah organisasi dipakai secara konsisten dan tepat sesuai dengan kebijakan yang berlaku dalam organisasi tersebut. Audit ini akan melakukan review secara lengkap dari sisi fisik sebuah sistem, mem-verifikasi konfigurasi perangkat lunak, dan aktifitas-aktifitas sistem yang lain.

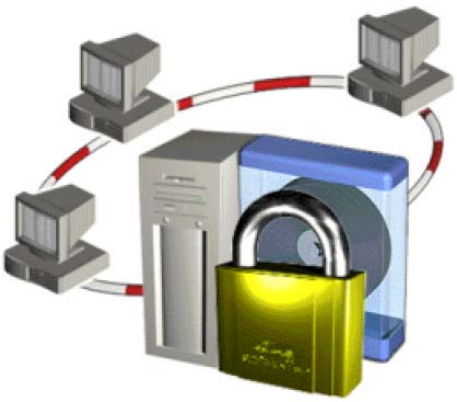
Gambar 3 Usage audit meruapakan salah satu metode audit sistem

Perhatian yang utama dari audit jenis ini adalah bagaimana peng-instalan dan lisensi perangkat lunak dengan benar. Organisasi harus menguji sistem secara berkala untuk melakukan verifikasi bahwa hanya perangkat lunak yang di lisensi oleh organisasi tersebut yang boleh di instal di setiap komputer yang ada dalam organisasi tersebut.



Gambar 4 Penggunaan Software yang ber-lisensi salah satu parameter usage audit

Selain masalah perangkat lunak dan keamanan fisik sistem yang di audit, hal yang juga menjadi pertimbangan adalah masalah lubang keamanan yang mungkin saja di timbulkan oleh perangkat lunak yang di instal di dalam sistem organisasi tersebut. Sehingga harus dapat dipastikan bahwa perangkat lunak-perangkat lunak yang di instal tersebut sudah di update sesuai dengan kebutuhannya.



Gambar 5 Mekanisme update software termasuk dalam parameter usage audit

Audit ini juga melakukan pengujian terhadap penggunaan jaringan komputer dalam sebuah organisasi. Pengecekan dilakukan untuk mengetahui apakah sumber daya jaringan komputer digunakan sesuai dengan peruntukannya atau tidak. Setiap penggunaan jaringan yang tidak sesuai penggunaannya akan diberi tanda oleh proses audit ini dan dapat di hentikan sebelum hal ini menjadi masalah di kemudian hari.

Gambar 6 Pemakaian sumber daya dalam jaringan merupakan parameter dalam usage audit

Escalation Audit

Eskalasi audit mem-fokuskan seputar bagaimana pihak manajemen/ *decision-makers* mengendalikan sistem jaringan jika menemukan masalah darurat terhadap sistem tersebut.

Gambar 7 Escalation Audit melihat bagaimana pihak pengambil keputusan ketika sistem jaringan komputer menghadapi situasi kritis

Jenis audit ini akan melakukan pengujian bagaimana sebuah organisasi mampu menghadapi masalah-masalah yang mungkin muncul ketika keadaan darurat terjadi. Misalnya, pengujian dan proses verifikasi sistem terhadap "disaster recovery plans" dan "business continuity plans". Jenis-jenis perencanaan ini dapat menjadi "outdated" secara cepat dan sebuah proses audit dapat digunakan untuk menjamin bahwa segala sesuatunya dapat di selesaikan dan rencana-rencana tersebut dapat sukses di terapkan jika masalah terjadi pada sistem jaringan komputer organisasi tersebut.

Gambar 8 Disaster Recovery Plans dan Business Continuity Plans adalah contoh parameter yang di audit dalam escalation audit

Kesimpulan

Audit sistem merupakan salah satu tahapan dalam rangka menjamin agar "security goal" tetap terpelihara dengan baik. Setelah semua kebijakan yang berhubungan dengan keamanan jaringan komputer di buat oleh sebuah organisasi, maka tahapan selanjutnya adalah melakukan pengujian apakah semua kebijakan dan aturan main yang telah dibuat tersebut sudah di terapkan dengan tepat atau belum. Ada 3 jenis audit yang biasanya dilakukan terhadap sistem keamanan jaringan dalam sebuah organisasi, yaitu: "privilege audit" yang mengaudit bagaimana pengaturan hak akses diterapkan di perusahaan tersebut sudah sesuai atau belum serta bagaimana pelaksanaannya di lapangan. "usage audit" mengaudit bagaiaman penggunaan sumber daya didalam organisasi. Apakah sudah sesuai dengan kebijakan organisasi tersebut atau belum. "escalation audit" mengaudit bagaimana sistem keamanan dalam sebuah organisasi menghadapi situasi yang kritis. Misalnya seberapa cepat proses recoveri sistem tersebut jika terjadi serangan oleh "hacker", bagaimana prosedur operasi standar yang di terapkan oleh organisasi jika terjadi masalah pada infrastruktur sistem jaringan, bagaimana menghadapi jika terjadi bencana alam. Sehingga dari semua proses audit tersebut dapat

diketahui kelemahan-kelemahan apa saja yang terdapat dalam sistem jaringan komputer organisasi tersebut. Untuk selanjutnya dapat di cari solusi yang tepat untuk menghadapi masalah-masalah tersebut.

Daftar Pustaka

CompTIA Security+, Part 1 – security concepts., www.comptia.net

Network Security Essentials., Stalling W., Prentice Hall., 2004

http://www.more.net –Network Auditing-, 2007.