PENIPUAN DAN PENGAMANAN KOMPUTER

DIANA RAHMAWATI

Pendahuluan

Fraud is any and all means a person uses to gain an unfair advantage over another person. Fraudulent acts in include lies (kebohongan), suppressions of the truth (penyembunyian kebenaran), tricks (muslihat) and cunning (kelicikan), and they often involve a violation of a trust or confidence (pelanggaran kepercayaan).

The economic losses to fraud each year are staggering; the justice departement estimated that fraud costs the united states $200 billion a year.

lanjutan

Penipuan dapat dilakukan oleh orang dalam (internal) organisasi maupun oleh orang luar (eksternal) organisasi.

Pengendalian yang ada didalam organisasi biasanya untuk melindungi aset perusahaan yang dapat mempersulit pihak luar untuk mencuri sesuatu dari perusahaan.

Penipuan internal dapat dibagi dua:

1. Penipuan aset atau penipuan pegawai
2. Penipuan laporan keuangan.

lanjutan

Penggelapan aset atau penipuan pegawai :

penipuan yang dilakukan oleh seseorang atau kelompok orang untuk keuntungan keuangan pribadi.

Penipuan pelaporan keuangan :

tindakan yang disengaja baik melalui tindakan atau penghilangan yang menghasilkan laporan keuangan yang menyesatkan secara material

lanjutan

Terdapat 4 tindakan yang direkomendaskan untuk mengurangi kemungkinan terjadinya penipuan pelaporan keuangan yaitu :

1. Bentuklah lingkungan organisasi yang memberikan kontribusi terhadap integritas proses pelaporan keuangan.
2. Identifikasi dan pahami faktor-faktor yang mendorong kearah penipuan pelaporan keuangan.
3. Nilai resiko dari penipuan pelaporan keuangan didalam perusahaan.
4. Desain dan implementasikan pengendalian internal untuk menyediakan keyakinan yang memadai sehingga penipuan pelaporan keuangan dapat dicegah.

Sebab-Sebab Terjadinya Penipuan

Terdapat tiga sebab yaitu:

1. Tekanan

   motivasi seseorang untuk melakukan

   penipuan.

2. Peluang

   kondisi atau situasi yang memungkinkan seseorang untuk melakukan dan menutupi suatu tindakan yang tidak jujur.Peluang sering kali berasal dari kurangnya pengendalian internal

3. Rasionalisasi

   alasan yang sering dikemukakan/diungkapkan untuk melakukan penipuan

Tiga Karakteristik yang Dihubungkan Dengan Kebanyakan penipuan

1. Pencurian sesuatu yang berharga seperti kas, persediaan, peralatan dan data
2. Konversi aset yang dicuri kedalam uang tunai
3. Penyembunyian kejahatan untuk menghindari pedeteksian. Cara yang umum dilakukan adalah:

a. Membebankan item yang dicuri ke suatu akun biaya

b. Dengan *lapping* (gali lubang tutup lubang): pelaku mencuri uang yang diterima dari pelanggan A dan menutupi piutang pelanggan A dengan uang yang diterima dari pelanggan B , begitu seterusnya.

c. Dengan *kiting* (didalam skema perputaran) : pelaku menutupi pencuriannyadengan cara menciptakan uang melalu transfer uang antar bank.

Penipuan Komputer

Adalah tindakan ilegal apapun yang membutuhkan pengetahuan teknolog komputer untuk melakukan tindakan awal penipuan, penyelidikan atau pelaksanaannya.

Penipuan komputer mencakup hal-hal:

1. pencurian, penggunaaan akses, modifikasi, penyalinan dan perusakan sofware atau data secara tidak sah.
2. Pencurian uang dengan mengubah catatan komputer atau pencurian waktu komputer.
3. Pencurian atau perusakan hardware komputer
4. Penggunaan atau konspirasi untuk menggunakan sumber daya komputer dalam melakukan tindak pidana
5. Keinginan untuk secara legal mendapatkan informasi atau properti melalui penggunaan komputer.

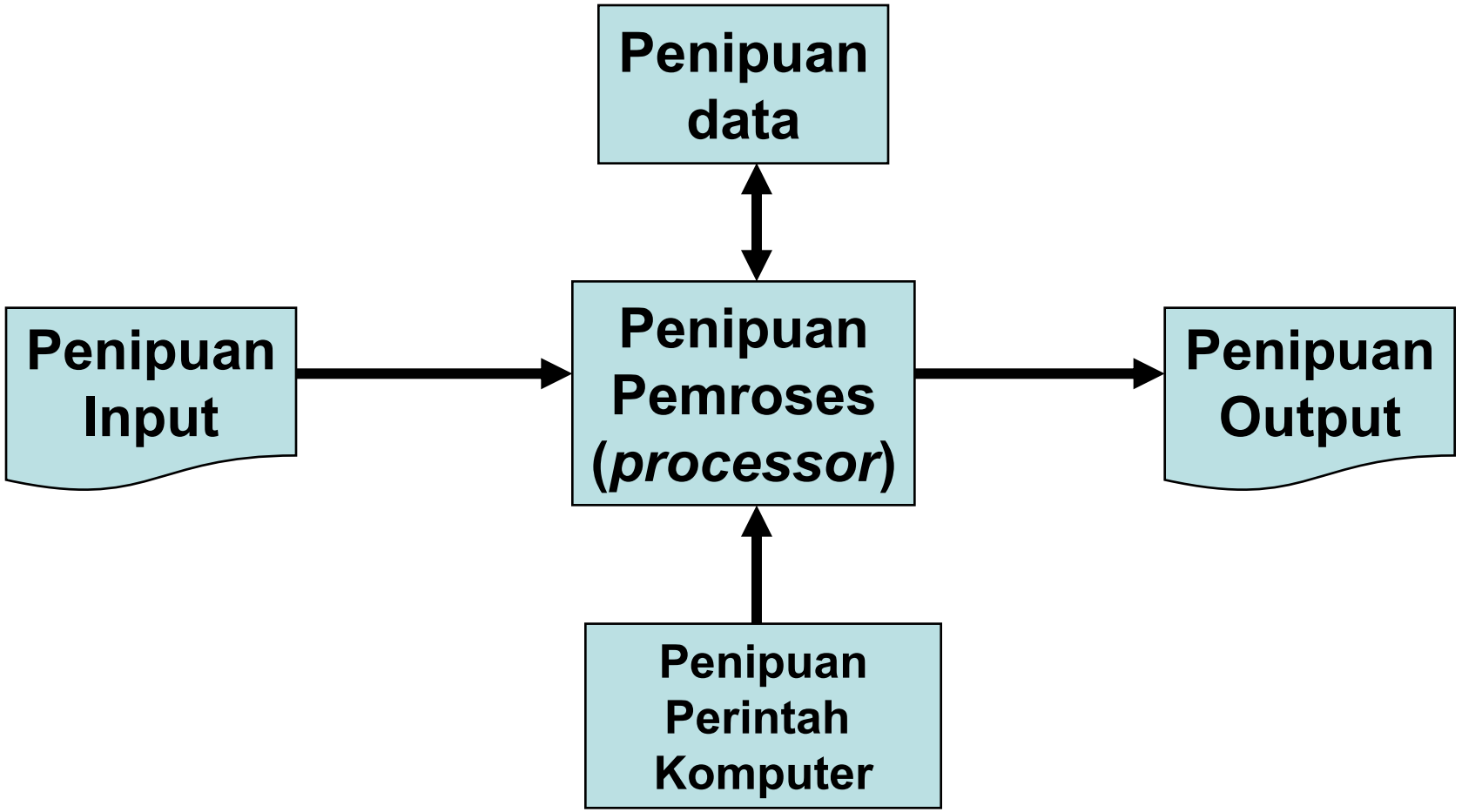
Peningkatan Penipuan Komputer

Terdapat beberapa alasan mengapa terjadi peningkatan penipua komputer yaitu:

1. Terdapatnya perdebatan mengenai hal-hal yang termasuk dalam penipuan komputer.
2. Banyaknya penipuan komputer yang tidak terdeteksi
3. 80-90 persen penipuan yang terungkap tidak dilaporkan karena adanya ketakutan adanya preseden buruk bagi perush yang berdampak pada hilangnya kepercayaan pelanggan.
4. Sebagian jaringan memiliki tingkat keamanan yang rendah
5. Banyak informasi mendetail/terperinci yang terdapat di internet mengenai bagaimana memulai kejahatan dan melakukan penyalahgunaan komputer

Klasifikasi Penipuan Komputer

Untuk menggolongkan penipuan komputer dapat dilakukan dengan menggunakan model pemrosesan data.



Penipuan dan Tehnik Penyalahgunaan Komputer

- Menjebol (*cracking*)
- Mengacak data (*data diddling*)
- Kebocoran data (*data leakage*)
- Serangan penolakan pelayanan (*denial-of-service attack*)
- Menguping (*evesdropping*)
- Pemalsuan e-mail (*e-mail forgery*)
- Ancaman e-mail (*email threats*)
- Melanggar masuk (*hacking*)
- Spamming
- Serangan cepat (*superzapping*)
- Pintu jebakan (*trap door*)
- Kuda troya (*trojan horse*)
- Virus
- Perang kontak (*war dialling*)
- Cacing (*worm*)
- Informasi yang salah di internet
- Terorisme internet
- Bom waktu logika (*logic time bomb*)
- Menyamar atau meniru (*masquerading or impersonation*)
- Penjebolan *password* (*password cracking*)
- Menyusup (*piggybacking*)
- Pembulatan kebawah (*round-down)*
- Tehnik Salami (*salami technique*)
- Pencarian (*scavenging*)
- Rekayasa sosial (*social engineering*)
- Pembajakan *software (software piracy*)

Virus Komputer

Adalah segmen dari kode pelaksana yang meletakkan dirinya pada software.

Kebanyakan virus memiliki dua tahapan yaitu:

1. Tahap replikasi: virus memperbanyak dirinya dan menyebar ke sistem atau file lainnya.
2. Tahap penyerangan : virus melaksanakan misinya misalnya merusak atau mengambil alih program, mengambil alih komputer, menghancurkan file dalam hard disk, memberi nama baru file/direktori, mengubah isi file dll

Mencegah dan Mendeteksi Penipuan Komputer

1. Membuat penipuan lebih jarang terjadi
2. Meningkatkan kesulitan untuk melakukan penipuan
3. Memperbaiki metode deteksi
4. Mengurangi kerugian akibat penipuan
5. Menuntut dan memenjarakan pelaku penipuan.

Membuat Penipuan Lebih Jarang Terjadi

- Menggunakan praktik mempekerjakan dan memecat pegawai yan semestinya.
- Mengatur para pegawai yang merasa tidak puas
- Melatih para pegawai mengenai standar keamanan dan pencegahan terhadap penipuan.
- Mengelola dan menelusuri lisensi software
- Meminta menandatangani perjanjian kerahasiaan kerja

Meningkatkan Kesulitan Untuk Melakukan Penipuan

- Mengembangkan sistem pengendalian internal yang kuat
- Memisahkan tugas
- Meminta pegawai mengambil cuti dan melakukan rotasi pekerjaan
- Membatasi akses keperlengkapan komputer dan file data
- Mengenkripsi data dan program
- Mengamankan saluran telepon
- Mengamankan sistem dari virus
- Mengendalikan data yang sensitif
- Mengendalikan komputer laptop
- Mengawasi informasi hacker

Memperbaiki Metode Deteksi

- Sering melakukan audit
- Mempekerjakan pegawai khusus untuk keamanan komputer
- Membuat saluran khusus untuk pengaduan penipuan
- Mempekerjakan konsultan komputer
- Mengawasi kegiatan sistem
- Mempekerjakan akuntan forensik
- Menggunakan software pendeteksi penipuan

Mengurangi Kerugian Akibat Penipuan

- Tetap menggunakan jaminan asuransi yang memadai
- Menyimpan salinan cadanngan program dan file data didalam lokasi luar kantor yang aman
- Mengembangkan rencana kontijensi dalam hal penipuan
- Menggunakan software untuk mengawasi kegiatan sistem dan untuk memulihkan diri dari akibat penipuan