



FAKULTAS ILMU KOMPUTER – UPN “VETERAN” JAWA TIMUR

SOAL EVALUASI TENGAH SEMESTER TA 2024/2025

MATA KULIAH : AUDIT IT
SMT / PROGRAM STUDI: 7 / INFORMATIKA
HARI / TANGGAL : SENIN / 21 OKTOBER 2024
WAKTU : 120 MENIT
SIFAT : TERTUTUP
DOSEN : AFINA LINA NURLAILI, S.KOM., M.KOM.
KELAS / PARALEL : F

PETUNJUK

- **Lembar Jawaban** : Tuliskan Nama, NPM, Paralel Kelas, di sebelah kiri atas lembar jawaban.
- **Lembar Soal** : Dikumpulkan kembali. Tuliskan Nama dan NPM di pojok kiri atas.

SOAL :

1. JERRY SCHNEIDER (25 poin)

Salah satu kasus penyalahgunaan komputer yang paling terkenal melibatkan seorang pemuda bernama Jerry Schneider. Schneider memiliki bakat dalam bidang elektronik. Saat lulus dari sekolah menengah, ia sudah mendirikan perusahaannya sendiri untuk memasarkan penemuannya. Perusahaannya juga menjual peralatan telepon Western Electric yang telah diperbarui. Pada tahun 1970, ia merancang sebuah skema di mana Pasific Telephone di Los Angeles akan memberinya peralatan berkualitas secara gratis!

Pasific Telephone menggunakan sistem pemesanan peralatan yang terkomputerisasi. Lokasi peralatan melakukan pemesanan menggunakan dialer kartu telepon dengan nada tekan (touch-tone). Pesanan tersebut kemudian dipindahkan ke kartu dengan cara dipunch (keypunched). Komputer kemudian memperbarui file induk inventaris dan mencetak pesanan. Pesanan tersebut diberikan kepada kantor transportasi yang mengirimkan pasokan tersebut.

Schneider berniat untuk mendapatkan akses ke sistem pemesanan tersebut. Ia berusaha agar Pasific Telephone mengirimkan peralatan kepadanya seolah-olah ia adalah salah satu lokasi resmi. Ia menggunakan berbagai teknik untuk mempelajari cara kerja sistem dan membobol keamanannya: Ia menyisir tempat sampah dan menemukan dokumen yang dibuang yang memberinya informasi tentang sistem pemesanan. Ia berpura-pura menjadi seorang penulis majalah dan langsung mengumpulkan informasi dari Pasific Telephone. Untuk mendukung kegiatannya, ia membeli van pengiriman Pasific Telephone di sebuah lelang, “memperoleh” kunci utama untuk lokasi pengiriman pasokan di wilayah Los Angeles, dan membeli dialer kartu telepon dengan nada tekan beserta serangkaian kartu yang mirip dengan yang digunakan oleh lokasi peralatan untuk mengirimkan pesanan.

Schneider memanfaatkan sistem penganggaran yang digunakan untuk situs pemesanan. Biasanya, situs-situs ini memiliki anggaran yang dialokasikan lebih besar dari yang mereka



butuhkan. Selama anggaran ini tidak terlampaui, tidak ada investigasi terhadap pemesanan peralatan yang dilakukan. Schneider berhasil mendapatkan akses ke sistem komputer online yang berisi informasi tentang anggaran. Dia kemudian menentukan ukuran pesanan yang bisa diterima tanpa mencurigakan. Selama tujuh bulan, Pasific Telephone mengirimkan peralatan kepadanya yang kemudian dia jual kembali kepada pelanggannya dan juga kepada Pasific Telephone. Dia memantau tingkat pemesanan ulang untuk berbagai inventaris Pasific Telephone, menghabiskan inventaris tersebut dengan pesannya, dan kemudian menjual kembali peralatan tersebut ke Pasific Telephone.

Keputusan buruk Schneider terjadi ketika dia mengungkapkan aktivitasnya kepada seorang karyawan. Dia tidak mampu mengimbangi kecepatan kegiatannya. Akibatnya, dia meminta bantuan seorang karyawan. Ketika karyawan tersebut meminta kenaikan gaji, Schneider memecatnya. Karyawan itu kemudian kembali ke Pasific Telephone dan melaporkan penipuan tersebut.

Ada berbagai laporan mengenai berapa banyak yang diambil Schneider dari Pasific Telephone. Parker (1976) memperkirakan kemungkinan peralatan senilai beberapa juta dolar telah diambil. Untuk penipuan tersebut, Schneider menerima hukuman penjara dua bulan diikuti dengan tiga tahun masa percobaan. Menariknya, setelah menyelesaikan hukuman penjara, dia mendirikan perusahaan konsultan yang mengkhususkan diri dalam keamanan komputer.

Soal : Buat laporan singkat yang menguraikan beberapa prosedur pengendalian internal dasar yang, jika diterapkan, seharusnya bisa mencegah atau mendeteksi aktivitas Schneider. Pastikan untuk menjelaskan mengapa penerapan prosedur pengendalian internal yang Anda rekomendasikan akan berhasil. (Weber, Ron. 1999. **Information Systems Control and Audit**. Prentice-Hall.Inc.)

2. UNION DIME SAVINGS BANK (25 poin)

Bank tampaknya sangat rentan terhadap penyalahgunaan komputer. Roswell Steffen menggunakan komputer untuk menggelapkan dana sebesar \$1,5 juta di Union Dime Savings Bank di New York City. Dalam wawancara dengan Miller (1974) setelah penipuan tersebut terungkap, ia mengklaim, "Siapa pun yang memiliki akal sehat bisa berhasil menggelapkan dana dari bank. Dan banyak yang melakukannya."

Steffen adalah seorang penjudi kompulsif. Awalnya, ia "meminjam" \$5.000 dari kotak kas di bank untuk mendukung kebiasaan judinya, dengan niat mengembalikan uang tersebut dari kemenangannya. Sayangnya, ia kehilangan \$5.000 tersebut. Ia kemudian menghabiskan tiga setengah tahun berikutnya mencoba mengganti uang tersebut, lagi-lagi dengan "meminjam" dari bank untuk berjudi di arena pacuan kuda.

Sebagai kepala teller di Union Dime, Steffen memiliki terminal pengawas dalam sistem komputer online bank yang ia gunakan untuk berbagai tujuan administratif. Ia mengambil



uang dari kotak kas dan menggunakan terminal tersebut untuk memanipulasi saldo rekening nasabah sehingga ketidaksesuaian tidak terlihat dalam laporan harian bank.

Ia menggunakan beberapa teknik untuk mendapatkan uang. Pertama, ia memfokuskan pada rekening dengan saldo di atas \$100.000 yang memiliki sedikit aktivitas dan menerima bunga setiap kuartal. Ia menggunakan terminal pengawas untuk mengurangi saldo di rekening-rekening tersebut. Kadang-kadang, nasabah yang marah mengeluhkan saldo yang tidak sesuai. Steffen kemudian berpura-pura melakukan panggilan telepon ke departemen pemrosesan data, memberi tahu nasabah bahwa itu hanya kesalahan sederhana, dan memperbaiki situasinya dengan memindahkan dana dari rekening lain.

Sumber dana lain yang digunakan Steffen termasuk rekening sertifikat dua tahun dan rekening baru. Untuk rekening sertifikat dua tahun, ia menyiapkan dokumen yang diperlukan tetapi tidak mencatat setoran tersebut dalam file bank. Awalnya, ia memiliki waktu dua tahun untuk memperbaiki situasi ini. Namun, masalah menjadi lebih rumit ketika bank mulai membayar bunga kuartalan pada rekening-rekening tersebut.

Untuk rekening baru, ia menggunakan dua buku tabungan baru dari persediaan buku bernomor seri di bank. Ketika membuka rekening, ia memasukkan transaksi menggunakan nomor rekening dari buku tabungan pertama tetapi mencatat entri di buku tabungan kedua. Ia kemudian menghancurkan buku tabungan pertama.

Penipuan yang dilakukan Steffen menjadi sangat rumit, dan ia melakukan banyak kesalahan. Namun, sistem pengendalian internal dan teknik audit bank yang lemah membuatnya bisa menjelaskan ketidaksesuaian tersebut dan melanjutkan aksinya. Ia tertangkap ketika polisi menggerebek bandar judi Steffen dan memperhatikan bahwa seorang teller bank dengan gaji rendah membuat taruhan yang sangat besar.

Soal: Buat laporan singkat yang menguraikan beberapa prosedur pengendalian internal dasar yang, jika diterapkan, seharusnya bisa mencegah atau mendeteksi aktivitas Steffen. Pastikan untuk menjelaskan mengapa penerapan prosedur pengendalian ini akan berhasil. (Weber, Ron. 1999. **Information Systems Control and Audit**. Prentice-Hall, Inc.)

3. PDNS 2 (25 poin)

Jakarta, CNN Indonesia -- Pemerintah akhirnya buka suara dan mengakui bahwa gangguan pada Pusat Data Nasional Sementara (PDNS) 2 akibat serangan siber ransomware atau modus pemerasan dari kelompok Lockbit 3.0. PDNS 2 mengalami gangguan sejak 20 Juni. Imbasnya beberapa layanan publik, termasuk imigrasi, lumpuh dan baru pada Senin (24/6) mulai pulih sebagian. "Yang mengalami insiden ini adalah pusat data sementara yang ada di Surabaya," kata Kepala Badan Siber dan Sandi Negara (BSSN) Hinsa Siburian, dalam konferensi pers di Kantor Kementerian Komunikasi dan Informatika, Jakarta, Senin (24/6).

Modus ransomware

Hinsa, dalam konferensi pers kemarin, mengatakan PDN mengalami gangguan sejak 20 Juni 2024 karena serangan siber yang memanfaatkan ransomware brain cipher.



"Insiden pusat data sementara ini adalah serangan siber dalam bentuk ransomware dengan nama brain chiper ransomware. Ransomware ini adalah pengembangan terbaru dari ransomware Lockbit 3.0," ujar dia.

Ransomware adalah serangan malware yang memiliki motif finansial. Biasanya, pelaku serangan meminta uang tebusan dengan ancaman mempublikasikan data pribadi korban atau memblokir akses ke layanan secara permanen.

Dalam beberapa kasus, infeksi ransomware bermula dari penyerang mendapat akses ke perangkat. Seluruh sistem operasi atau file pun dienkripsi. Uang tebusan kemudian diminta dari korban.

Soal: Buat laporan singkat yang menguraikan beberapa prosedur pengendalian internal dasar yang, jika diterapkan, seharusnya bisa mencegah atau mendeteksi serangan siber ransomware. Pastikan untuk menjelaskan mengapa penerapan prosedur pengendalian ini akan berhasil.

4. Perusahaan ABC (25 poin)

Pada tahun 2018, Perusahaan ABC menghadapi krisis internal yang cukup besar akibat kurangnya kebijakan kontrol akses dalam sistem Enterprise Resource Planning (ERP) mereka. Sebagai perusahaan besar yang mengelola berbagai divisi, mereka mengandalkan sistem ERP untuk mengintegrasikan seluruh operasional, mulai dari keuangan, produksi, hingga sumber daya manusia. Namun, dalam perjalanannya, terjadi ketidakseimbangan dalam distribusi hak akses di sistem tersebut.

Salah satu insiden paling mencolok terjadi ketika seorang staf administrasi yang bekerja di bagian pemasaran secara tidak sengaja mengakses data keuangan sensitif yang seharusnya hanya dapat diakses oleh tim akuntansi. Karyawan ini tidak memiliki niat buruk, namun dengan tidak adanya batasan akses yang tepat, ia menemukan informasi tentang saldo rekening perusahaan, rincian biaya proyek, hingga bonus karyawan yang seharusnya bersifat rahasia. Ia pun membicarakan temuan ini kepada beberapa rekan kerjanya. Tanpa disadari, gosip internal mulai menyebar.

Informasi sensitif ini kemudian bocor lebih luas dan sampai ke departemen lain, memicu kecemburuan di antara karyawan. Banyak dari mereka mulai mempertanyakan keadilan bonus dan tunjangan yang mereka terima. Hal ini menyebabkan ketegangan internal, merusak moral kerja, dan bahkan memicu pengunduran diri beberapa karyawan yang merasa tidak puas.

Masalahnya tidak berhenti di sana. Tanpa kontrol akses yang ketat, salah satu supervisor produksi juga memiliki kemampuan untuk mengakses data pelanggan, yang seharusnya hanya terbuka untuk tim penjualan dan pemasaran. Data pelanggan yang berisi informasi strategis seperti kontrak, harga, dan rencana pengembangan proyek, tanpa sengaja diunduh oleh supervisor tersebut. Ketika ia memutuskan untuk pindah ke perusahaan lain, ada kekhawatiran bahwa informasi ini bisa digunakan oleh kompetitor.



FAKULTAS ILMU KOMPUTER – UPN “VETERAN” JAWA TIMUR

SOAL EVALUASI TENGAH SEMESTER TA 2024/2025

Soal: Buat laporan singkat yang menguraikan beberapa prosedur pengendalian internal dasar yang, jika diterapkan, seharusnya bisa mencegah atau mendeteksi Ketidaksesuaian dalam Kebijakan Keamanan. Pastikan untuk menjelaskan mengapa penerapan prosedur pengendalian ini akan berhasil.