



Chapter 8

Mengamankan sistem informasi

KASUS VIDEO

Kasus 1: Stuxnet dan Cyber Warfare

Kasus 2: Cyber Spionase: Ancaman China

Kasus 3: Kunci Akses UBS: Saluran Informasi Terpercaya Zona IBM

Video Instruksional 1: Sony PlayStation Hacked; Data Dicuri dari 77 juta pengguna

Video Instruksional 2: Zappos Bekerja Untuk Memperbaiki Pelanggaran Keamanan Online

Video Instruksional 3: Temui Hacker: Pernyataan Anonim tentang Hacking SONY



Tujuan Pembelajaran

- **Jelaskan mengapa sistem informasi rentan terhadap kerusakan, kesalahan, dan penyalahgunaan.**
- **Jelaskan nilai bisnis keamanan dan kontrol.**
- **Jelaskan komponen kerangka organisasi untuk keamanan dan kontrol.**
- **Jelaskan alat dan teknologi yang digunakan untuk melindungi sumber informasi.**



Management Information Systems

Chapter 8: Securing Information Systems

Anda berada di LinkedIn? Awas!

- **Masalah: Pelanggaran data secara besar-besaran; menggunakan praktik keamanan lama**
- **Solusi: Inisiatif untuk menggunakan praktik industri minimal yang up-to-date, misalnya, mengasinkan kata sandi**
- **Mengilustrasikan kebutuhan akan praktik keamanan agar sesuai dengan standar dan ancaman saat ini**
- **Menunjukkan kurangnya regulasi untuk keamanan komputer korporat dan keamanan data jaringan sosial; Perlindungan data yang buruk oleh banyak perusahaan**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- **Keamanan:**
- **Kebijakan, prosedur, dan tindakan teknis yang digunakan untuk mencegah akses tidak sah, perubahan, pencurian, atau kerusakan fisik pada sistem informasi**
- **Kontrol:**
- **Metode, kebijakan, dan prosedur organisasi yang menjamin keamanan aset organisasi; akurasi dan reliabilitas dari catatan akuntansi; dan ketaatan operasional terhadap standar manajemen**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Mengapa sistem rentan Aksesibilitas jaringan?

Masalah perangkat keras (kerusakan, kesalahan konfigurasi, kerusakan dari penggunaan atau kejahatan yang tidak semestinya)

Masalah perangkat lunak (kesalahan pemrograman, kesalahan pemasangan, perubahan yang tidak sah)

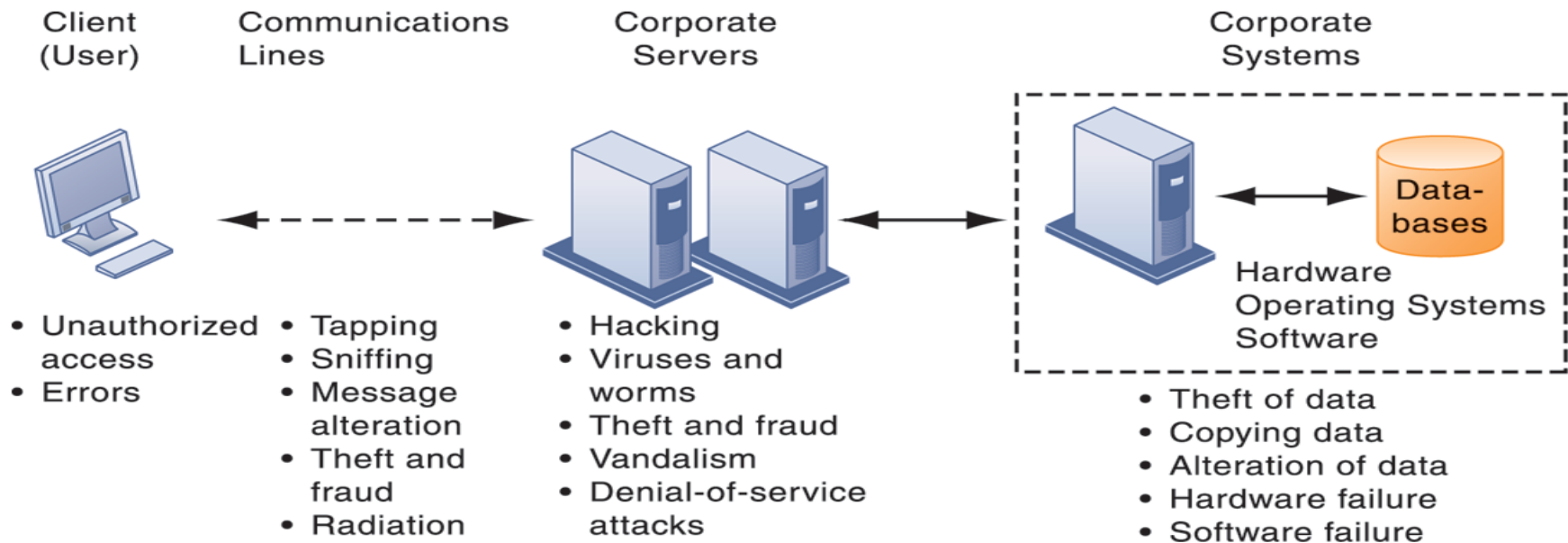
Bencana Penggunaan jaringan / komputer di luar kendali perusahaan

Kerugian dan pencurian perangkat portable

Management Information Systems

Chapter 8: Securing Information Systems

TANTANGAN KEAMANAN KONTEMPORER DAN VULNERABILITIES



GAMBAR 8-1

Arsitektur aplikasi berbasis Web biasanya mencakup klien Web, server, dan sistem informasi perusahaan yang terhubung ke database. Masing-masing komponen ini menghadirkan tantangan keamanan dan kerentanan. Banjir, kebakaran, kegagalan listrik, dan masalah listrik lainnya dapat menyebabkan gangguan pada titik manapun dalam jaringan. Arsitektur aplikasi berbasis Web biasanya mencakup klien Web, server, dan sistem informasi perusahaan yang terhubung ke database. Masing-masing komponen ini menghadirkan tantangan keamanan dan kerentanan. Banjir, kebakaran, gangguan listrik, dan masalah kelistrikan lainnya dapat menyebabkan gangguan pada jaringan manapun



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Kerentanan internet

- Jaringan terbuka untuk siapapun
- Ukuran Internet berarti penyalahgunaan bisa berdampak luas
- Penggunaan alamat internet tetap dengan modem kabel / DSL membuat target tetap untuk hacker
- VOIP yang tidak dienkripsi

-E-mail, P2P, IM

- Penangkapan
- Lampiran dengan perangkat lunak berbahaya
- Mengirimkan rahasia dagang



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- tantangan keamanan nirkabel
 - * Band frekuensi radio mudah dipindai
 - * SSID (pengenal pengaturan layanan)
 - Mengidentifikasi jalur akses
 - Broadcast beberapa kali
 - Dapat diidentifikasi dengan program sniffer
 - War mengemudi
 - * Eavesdroppers drive oleh bangunan dan mencoba untuk mendeteksi SSID dan mendapatkan akses ke jaringan dan sumber daya
- Setelah titik akses dilanggar, penyusup dapat menggunakan OS untuk mengakses drive dan file jaringan



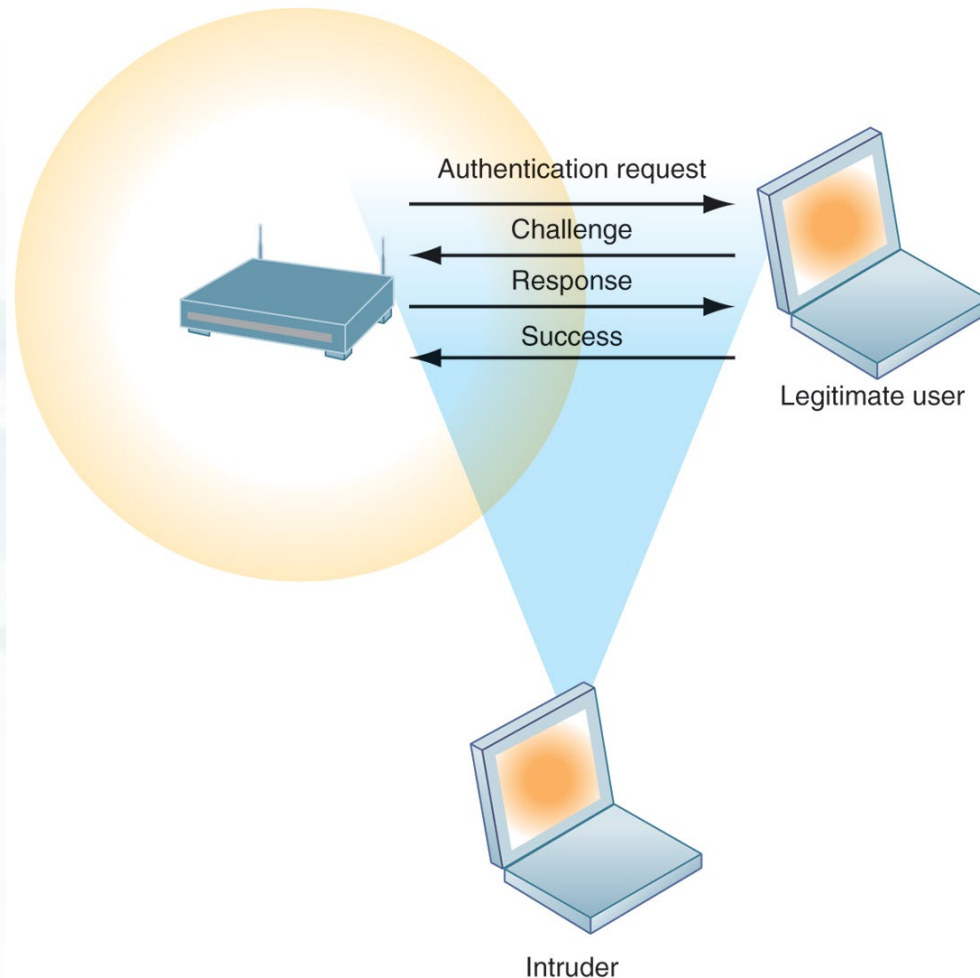
Management Information Systems

Chapter 8: Securing Information Systems

TANTANGAN KEAMANAN WI-FI

Banyak jaringan Wi-Fi dapat ditembus dengan mudah oleh penyusup menggunakan program sniffer untuk mendapatkan alamat untuk mengakses sumber daya jaringan tanpa otorisasi.

Gambar 8-2





Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Malware (perangkat lunak berbahaya)

*** Virus**

-Rogue program perangkat lunak yang menempel pada program perangkat lunak lain atau file data agar bisa dijalankan

***Cacing**

-Independent program yang menyalin diri dari satu komputer ke komputer lain melalui jaringan.

*** cacing dan virus menyebar**

-Downloads (download drive-by)

-E-mail, lampiran IM

-Downloads di situs Web dan jaringan sosial



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Malware (lanjutan)

- * Smartphone semudah komputer**

- study menemukan 13.000 jenis malware smartphone**

- * Trojan horse**

- Software yang tampak jinak tapi melakukan sesuatu selain yang diharapkan**

- * Serangan injeksi SQL**

- hackers mengirimkan data ke formulir Web yang memanfaatkan perangkat lunak yang tidak dilindungi situs tersebut dan mengirimkan query SQL nakal ke database**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Malware (lanjutan)

*** Spyware**

-Program kecil menginstal sendiri diam-diam di komputer untuk memantau aktivitas pengguna Web surfing dan menayangkan iklan

-Key penembang kayu

*** Catat setiap keystroke di komputer untuk mencuri nomor seri, kata sandi, jalankan serangan Internet**

-Tipe yang lain:

*** Setel ulang browser beranda**

*** Redirect permintaan pencarian**

*** Lambat kinerja komputer dengan mengambil memori**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Hacker dan kejahatan komputer

*** Hacker vs biskuit**

***Kegiatan meliputi:**

-Sistem intrusi

-Sistem kerusakan

-Cybervandalism

*** Disengaja gangguan, penghancuran, penghancuran situs Web atau sistem informasi perusahaan**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Spoofing

- * Salah mengartikan diri dengan menggunakan alamat e-mail palsu atau menyamar sebagai orang lain**
- * Mengalihkan link Web ke alamat yang berbeda dari yang dimaksud, dengan situs menyamar sebagai tujuan yang diinginkan**

-Sapu tangan

- * Menguping program yang memonitor informasi perjalanan melalui jaringan**
- * Memungkinkan hacker mencuri informasi kepemilikan seperti e-mail, file perusahaan, dan sebagainya**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Denial-of-service attack (DoS)

- * Banjir server dengan ribuan permintaan palsu untuk menabrak jaringan**

-Distributed denial-of-service attack (DDoS)

- * Gunakan banyak komputer untuk meluncurkan DoS**

- * Botnet**

- Jaringan PC "zombie" yang disusupi oleh bot malware**

- Deliver 90% spam dunia, 80% malware dunia**

- Grum botnet: komputer dikontrol 560K sampai 840K**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

-Komputer kejahatan

Ditetapkan sebagai "pelanggaran hukum pidana yang melibatkan pengetahuan tentang teknologi komputer untuk tindakan, investigasi, atau penuntutan mereka"

Komputer bisa jadi sasaran kejahatan, misalnya:

- Menjaga kerahasiaan data terkomputerisasi yang terproteksi**
- Menghasilkan sistem komputer tanpa otoritas**

Komputer bisa jadi alat kejahatan, misalnya:

- Theft rahasia dagang**

Menggunakan e-mail untuk ancaman atau pelecehan...



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- **Pencurian identitas**
 - Theft Informasi Pribadi (ID jaminan sosial, SIM, atau nomor kartu kredit) untuk meniru identitas orang lain
- **Phishing**
 - Menyiapkan situs Web palsu atau mengirim pesan e-mail yang terlihat seperti bisnis yang sah untuk meminta pengguna data pribadi rahasia.
- **Si kembar jahat**
 - Jaringan nirkabel yang berpura-pura menawarkan koneksi Wi-Fi yang dapat dipercaya ke Internet



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- **Pharming**
 - Meneruskan pengguna ke halaman Web palsu, bahkan ketika masing-masing jenis memperbaiki alamat halaman Web ke browsernya
- **Klik penipuan**
 - Jika program individual atau komputer menipu mengklik iklan online tanpa bermaksud untuk belajar lebih banyak tentang pengiklan atau melakukan pembelian
- **Cyberterrorisme dan Cyberwarfare**



Management Information Systems

Chapter 8: Securing Information Systems

Interactive Session: Organizations

Stuxnet and the Changing Face of Cyberwarfare

Read the Interactive Session and discuss the following questions

- **Apakah cyberwarfare merupakan masalah serius? Mengapa atau mengapa tidak?**
- **Menilai faktor manajemen, organisasi, dan teknologi yang telah menciptakan masalah ini.**
- **Apa yang membuat Stuxnet berbeda dengan serangan cyberwarfare lainnya? Seberapa serius ancaman teknologi ini?**
- **Solusi apa yang telah diajukan untuk masalah ini? Apakah Anda pikir mereka akan efektif? Mengapa atau mengapa tidak?**



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- **Ancaman internal: Karyawan**
 - Ancaman keamanan sering terjadi di dalam sebuah organisasi
- Di dalam pengetahuan**
 - Sloppy prosedur keamanan
- Kurangnya pengetahuan pengguna**
 - Sosial rekayasa:
 - Menipu karyawan untuk mengungkapkan kata sandinya dengan berpura-pura menjadi anggota sah perusahaan yang membutuhkan informasi



Management Information Systems

Chapter 8: Securing Information Systems

System Vulnerability and Abuse

- **Kerentanan perangkat lunak**
- **Perangkat lunak komersial mengandung kekurangan yang menciptakan kerentanan keamanan**
 - * **Hidden bugs (kode program cacat)**

Nol cacat tidak bisa diraih karena pengujian yang lengkap tidak memungkinkan dengan program besar

 - * **Cacat bisa membuka jaringan ke penyusup**
- **Patches**
 - * **Potongan kecil perangkat lunak untuk memperbaiki kekurangan**
 - * **Eksplorasi yang sering dibuat lebih cepat dari tambalan bisa dilepas dan diimplementasikan**



Management Information Systems

Chapter 8: Securing Information Systems

Business Value of Security and Control

- **Sistem komputer yang gagal dapat menyebabkan hilangnya fungsi bisnis secara signifikan atau total.**
- **Perusahaan sekarang lebih rentan dari sebelumnya.**
 - Komentar pribadi dan data keuangan
 - Trade rahasia, produk baru, strategi
- **Pelanggaran keamanan mungkin akan segera memotong nilai pasar sebuah perusahaan.**
- **Keamanan dan kontrol yang tidak memadai juga menimbulkan masalah pertanggungjawaban.**



Management Information Systems

Chapter 8: Securing Information Systems

Business Value of Security and Control

- **Persyaratan hukum dan peraturan untuk pengelolaan catatan elektronik dan perlindungan privasi**
 - HIPAA: Aturan dan prosedur keamanan dan privasi medis**
 - Gramm-Leach-Bliley Act: Membutuhkan lembaga keuangan untuk menjamin keamanan dan kerahasiaan data pelanggan**
 - Sarbanes-Oxley Act: Memaksakan tanggung jawab pada perusahaan dan manajemen mereka untuk menjaga keakuratan dan integritas informasi keuangan yang digunakan secara internal dan dikeluarkan secara eksternal.**



Management Information Systems

Chapter 8: Securing Information Systems

Business Value of Security and Control

- **Bukti elektronik**
 - *Kemungkinan terjadinya kerah putih sering terjadi dalam bentuk digital Data komputer, e-mail, pesan instan, transaksi e-commerce
 - *Pengendalian data dapat menghemat waktu dan uang saat merespons permintaan penemuan hukum
- **Komputer forensik:**
 - * Koleksi ilmiah, pemeriksaan, otentikasi, pelestarian, dan analisis data dari media penyimpanan komputer untuk digunakan sebagai bukti di pengadilan
 - *Termasuk pemulihan data sekitar dan data tersembunyi



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Kontrol sistem informasi**
 - Manual dan kontrol otomatis
 - Kontrol umum dan aplikasi
- **Kontrol umum**
 - Govern desain, keamanan, dan penggunaan program komputer dan keamanan file data secara umum di seluruh infrastruktur teknologi informasi organisasi
 - Terapkan ke semua aplikasi terkomputerisasi
 - Kombinasi perangkat keras, perangkat lunak, dan prosedur manual untuk menciptakan lingkungan pengendalian keseluruhan



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Jenis kontrol umum**
 - Software kontrol
 - Kontrol perangkat keras
 - Komputer operasi kontrol
 - Data kontrol keamanan
 - kontrol implementasi
 - kontrol administratif





Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Kontrol aplikasi**
 - Kontrol khusus unik untuk setiap aplikasi terkomputerisasi, seperti pemrosesan gaji atau pesanan
 - Termasuk prosedur otomatis dan manual
 - Memastikan bahwa hanya data resmi yang benar-benar dan diproses secara akurat oleh aplikasi itu
 - Include:
 - * Kontrol input
 - * Pengolahan kontrol
 - * Kontrol output



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Penilaian risiko: Menentukan tingkat risiko terhadap perusahaan jika aktivitas atau proses tertentu tidak terkontrol dengan baik**

-Tipe ancaman

-Kemungkinan terjadinya selama tahun

-Potensi kerugian, nilai ancaman

Kehilangan tahunan yang terekspresi

EXPOSURE	PROBABILITY	LOSS RANGE (AVG)	EXPECTED ANNUAL LOSS
Power failure	30%	\$5K–\$200K (\$102,500)	\$30,750
Embezzlement	5%	\$1K–\$50K (\$25,500)	\$1,275
User error	98%	\$200–\$40K (\$20,100)	\$19,698



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Kebijakan keamanan**
 - Menghitung risiko informasi, mengidentifikasi tujuan keamanan yang dapat diterima, dan mengidentifikasi mekanisme untuk mencapai tujuan ini
 - Drives kebijakan lainnya
 - * **Acceptable use policy (AUP)**
Mendefinisikan penggunaan sumber informasi perusahaan dan peralatan komputasi yang dapat diterima
 - * **Kebijakan otorisasi**
Tentukan tingkat akses pengguna yang berbeda terhadap aset informasi



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Pengelolaan identitas**
 - Proses dan alat bisnis untuk mengidentifikasi pengguna sistem dan akses kontrol yang valid
 - * Mengidentifikasi dan mengotorisasi kategori pengguna yang berbeda
 - * Menentukan bagian pengguna sistem mana yang dapat diakses
 - Otentikasi pengguna dan melindungi identitas
 - Identity management systems
 - * Menangkap aturan akses untuk berbagai



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Perencanaan pemulihan bencana: Menyusun rencana untuk pemulihan layanan yang terganggu**
- **Perencanaan kesinambungan bisnis: Fokus pada pemulihan operasi bisnis setelah bencana**
 - Baik jenis rencana yang dibutuhkan untuk mengidentifikasi sistem perusahaan yang paling kritis
 - Bisnis analisis dampak untuk menentukan dampak dari outage
 - Manajemen harus menentukan sistem mana yang dipulihkan terlebih dahulu



Management Information Systems

Chapter 8: Securing Information Systems

SECURITY PROFILES FOR A PERSONNEL SYSTEM

Dua contoh ini mewakili dua profil keamanan atau pola keamanan data yang mungkin ditemukan dalam sistem personalia. Bergantung pada profil keamanan, pengguna memiliki batasan akses pada berbagai sistem, lokasi, atau data dalam suatu organisasi.

Gambar 8-3

SECURITY PROFILE 1	
User: Personnel Dept. Clerk	
Location: Division 1	
Employee Identification Codes with This Profile:	00753, 27834, 37665, 44116
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read and Update
• Medical history data	None
• Salary	None
• Pensionable earnings	None

SECURITY PROFILE 2	
User: Divisional Personnel Manager	
Location: Division 1	
Employee Identification Codes with This Profile:	27321
Data Field Restrictions	Type of Access
All employee data for Division 1 only	Read Only



Management Information Systems

Chapter 8: Securing Information Systems

Establishing a Framework for Security and Control

- **Audit SIM**

- Kecuali lingkungan keamanan keseluruhan perusahaan serta kontrol yang mengatur sistem informasi individu

- Tepatnya teknologi, prosedur, dokumentasi, pelatihan, dan personil.

- Mungkin bahkan mensimulasikan bencana untuk menguji respon teknologi, staf IS, karyawan lainnya

- Melamat dan memberi peringkat semua kelemahan kontrol dan memperkirakan kemungkinan kemunculannya

- Mengakui dampak finansial dan organisasi dari setiap ancaman



Management Information Systems

Chapter 8: Securing Information Systems

SAMPLE AUDITOR'S LIST OF CONTROL WEAKNESSES

Bagan ini adalah contoh halaman dari daftar kelemahan kontrol yang mungkin ditemukan auditor dalam sistem pinjaman di bank komersial lokal. Formulir ini membantu auditor mencatat dan mengevaluasi kelemahan pengendalian dan menunjukkan hasil mendiskusikan kelemahan tersebut dengan manajemen, serta tindakan perbaikan yang dilakukan oleh manajemen.

Gambar 8-4

Function: Loans Location: Peoria, IL		Prepared by: J. Ericson Date: June 16, 2011		Received by: T. Benson Review date: June 28, 2011	
Nature of Weakness and Impact	Chance for Error/Abuse		Notification to Management		
	Yes/ No	Justification	Report date	Management response	
User accounts with missing passwords	Yes	Leaves system open to unauthorized outsiders or attackers	5/10/11	Eliminate accounts without passwords	
Network configured to allow some sharing of system files	Yes	Exposes critical system files to hostile parties connected to the network	5/10/11	Ensure only required directories are shared and that they are protected with strong passwords	
Software patches can update production programs without final approval from Standards and Controls group	No	All production programs require management approval; Standards and Controls group assigns such cases to a temporary production status			



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Perangkat lunak manajemen identitas**
 - Automates mencatat semua pengguna dan hak istimewa
 - Menguji pengguna, melindungi identitas, mengendalikan akses
- **Otentikasi**
 - Password sistem
 - Tokens
 - Kartu pintar
 - Biometrik otentikasi



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

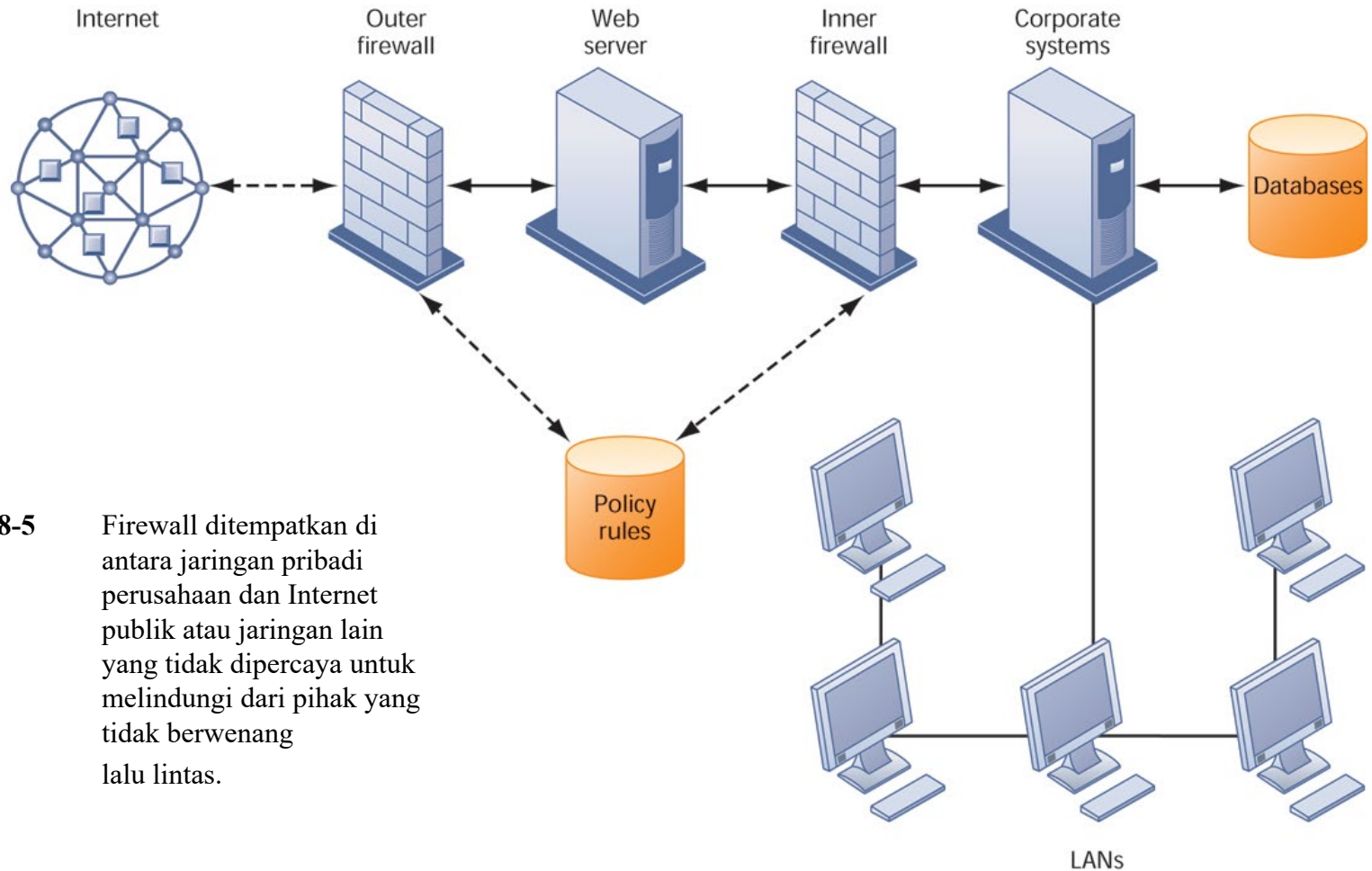
- **Firewall:**
 - Kombinasi perangkat keras dan perangkat lunak yang mencegah pengguna yang tidak sah mengakses jaringan pribadi
 - Teknologi meliputi:
 - * Penyaringan paket statis
 - * Pemeriksaan stateful
 - * Network address translation (NAT)
 - * Aplikasi proxy filtering



Management Information Systems

Chapter 8: Securing Information Systems

A CORPORATE FIREWALL



Gambar 8-5

Firewall ditempatkan di antara jaringan pribadi perusahaan dan Internet publik atau jaringan lain yang tidak dipercaya untuk melindungi dari pihak yang tidak berwenang lalu lintas.



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Sistem deteksi intrusi:**
 - Monitor hot spot di jaringan perusahaan untuk mendeteksi dan mencegah penyusup
 - Segera peristiwa seperti yang terjadi untuk menemukan serangan yang sedang berlangsung
- **Perangkat lunak antivirus dan antispyware:**
 - Periksa komputer karena adanya malware dan sering bisa menghilangkannya juga
 - Memerlukan pembaharuan terus-menerus
- **Sistem manajemen ancaman terpadu (UTM)**



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Mengamankan jaringan nirkabel**
 - Keamanan WEP dapat memberikan keamanan dengan:
 - * Menetapkan nama unik ke SSID jaringan dan tidak menyiarkan SSID
 - * Menggunakannya dengan teknologi VPN
 - Wi-Fi Alliance menyelesaikan spesifikasi WAP2, menggantikan WEP dengan standar yang lebih kuat
 - * Terus ganti kunci
 - * Sistem otentikasi terenkripsi dengan server pusat



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Enkripsi:**
 - Transformasi teks atau data ke dalam teks sandi yang tidak dapat dibaca oleh penerima yang tidak diinginkan
 - Dua metode untuk enkripsi pada jaringan
 - * Secure Sockets Layer (SSL) dan penerus Transport Layer Security (TLS)
 - * Secure Hypertext Transfer Protocol (S-HTTP)



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Dua metode enkripsi**

- Symmetric kunci enkripsi**

- Pengirim dan penerima menggunakan satu kunci bersama
 - Sublik kunci enkripsi

- Menggunakan dua kunci matematis: kunci publik dan kunci privat**

- Pengirim mengenkripsi pesan dengan kunci publik penerima
 - Dekripsi penerima dengan kunci privat



Management Information Systems

Chapter 8: Securing Information Systems

PUBLIC KEY ENCRYPTION



Gambar 8-6

Sistem enkripsi kunci publik dapat dilihat sebagai serangkaian kunci publik dan pribadi yang mengunci data saat dikirim dan membuka kunci data saat diterima. Pengirim menempatkan kunci publik penerima dalam sebuah direktori dan menggunakannya untuk mengenkripsi pesan. Pesan dikirim dalam bentuk terenkripsi melalui Internet atau jaringan pribadi. Saat pesan terenkripsi masuk, penerima menggunakan kunci pribadinya untuk mendekripsi data dan membaca pesannya.



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Sertifikat digital:**
 - Data file digunakan untuk menetapkan identitas pengguna dan aset elektronik untuk perlindungan transaksi online
 - Gunakan pihak ketiga yang terpercaya, otoritas sertifikasi (CA), untuk memvalidasi identitas pengguna
 - CA memverifikasi identitas pengguna, menyimpan informasi di server CA, yang menghasilkan sertifikat digital terenkripsi yang berisi informasi ID pemilik dan salinan kunci publik pemilik
- **Infrastruktur kunci publik (PKI)**
 - Gunakan kriptografi kunci publik yang bekerja dengan otoritas sertifikat
 - Sangat digunakan dalam e-commerce



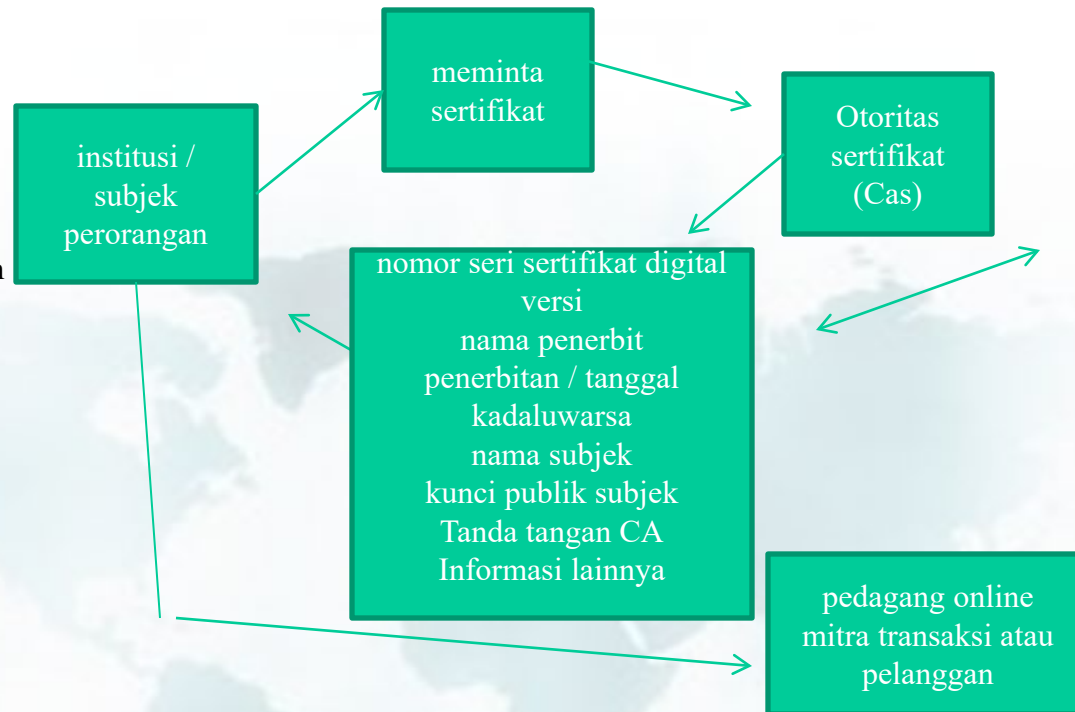
Management Information Systems

Chapter 8: Securing Information Systems

DIGITAL CERTIFICATES

Sertifikat digital membantu membangun identitas orang atau aset elektronik. Mereka melindungi transaksi online dengan menyediakan komunikasi online yang aman dan terenkripsi.

Gambar 8-7





Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Memastikan ketersediaan sistem**
- **Proses transaksi online membutuhkan ketersediaan 100%, tidak ada downtime**
- **Sistem komputer yang toleran terhadap kesalahan**
 - Untuk ketersediaan berkelanjutan, misalnya, pasar saham
 - Mengandung komponen perangkat keras, perangkat lunak, dan listrik yang berlebihan yang menciptakan lingkungan yang menyediakan layanan terus menerus tanpa gangguan
- **Komputasi dengan ketersediaan tinggi**
 - Bantu pulih dengan cepat dari tabrakan
 - Minimizes, tidak menghilangkan, downtime



Technologies and Tools for Protecting Information Resources

- **Security in the cloud**
 - **Responsibility for security resides with company owning the data**
 - **Firms must ensure providers provides adequate protection:**
 - Where data are stored
 - Meeting corporate requirements, legal privacy laws
 - Segregation of data from other clients
 - Audits and security certifications
 - **Service level agreements (SLAs)**



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Komputasi berorientasi pemulihan**
 - Desain sistem yang cepat pulih dengan kemampuan untuk membantu operator menentukan dan memperbaiki kesalahan pada sistem multi komponen
- **Mengontrol lalu lintas jaringan**
 - Menggunakan inspeksi paket (DPI)
- **Pemblokiran video dan musik**
- **Keamanan outsourcing**
 - Penyedia layanan keamanan yang dikelola (MSSPs)



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Mengamankan platform seluler**
 - Kebijakan keamanan harus mencakup dan mencakup persyaratan khusus untuk perangkat seluler
 - * Pedoman penggunaan platform dan aplikasi
 - Alat alat manajemen perangkat
 - *Otorisasi
 - * Catatan persediaan
 - * Kontrol update
 - * Kunci / hapus perangkat yang hilang
 - * Enkripsi
 - Software untuk memisahkan data perusahaan pada perangkat



Interactive Session: Technology

Seberapa Amankah Smartphone Anda?

Read the Interactive Session and discuss the following questions

- **Dikatakan bahwa smartphone adalah komputer mikro di tangan Anda. Diskusikan implikasi keamanan dari pernyataan ini.**
- **Masalah manajemen, organisasi, dan teknologi apa yang harus ditangani oleh keamanan smartphone?**
- **Masalah apa yang menyebabkan kelemahan keamanan smartphone menyebabkan bisnis?**
- **Langkah apa yang bisa dilakukan individu dan bisnis agar smartphone mereka lebih aman?**



Management Information Systems

Chapter 8: Securing Information Systems

Technologies and Tools for Protecting Information Resources

- **Memastikan kualitas perangkat lunak**

- Software metrics: Penilaian sistem secara obyektif dalam bentuk pengukuran kuantitatif

- * Jumlah transaksi

- * Waktu respon online

- * Cek gaji dicetak per jam

- * Dikenal bug per seratus baris kode

- Akhir dan pengujian reguler

- Walkthrough: Review dokumen spesifikasi atau disain oleh kelompok kecil yang orang-orang berkualitas

- Debugging: Proses dimana error adalah elimi



Management Information Systems

Chapter 8: Securing Information Systems



This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from it should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.

