BINUS UNIVERSITY ONLINE LEARNING

People
Innovation
Excellence

LECTURE NOTES

CPEN8003
Network Governance

Developing Network Security Strategies

LEARNINGOUTCOMES

1. Menampilkan pengetahuan rinci tentang teknologi keamanan yang muncul
2. Menampilkan kemampuan detil dari desain keamanan jaringan

OUTLINE MATERI:

1. Network Security Design Step
2 Security Mechanisms
3. Modularizing Security Design
4. Summary

ISIMATERI

1. Langkah-langkah Desain Keamanan Jaringan

a) Mengidentifikasi asset jaringan

b) Menganalisis risiko keamanan

c) Menganalisis kebutuhan keamanan dan konsekuensinya

d) Mengembangkan rencana keamanan

e) Menetapkan kebijakan keamanan

f) Mengembangkan prosedur untuk menerapkan kebijakan keamanan

g) Mengembangkan strategi pelaksanaan teknis

h) Mendapatkan dukungan dari pengguna, manajer, dan staf teknis

i) Melatih pengguna, manajer, dan staf teknis

j) Menerapkan strategi teknis dan prosedur keamanan

k) Uji keamanan dan update jika ada masalah yang ditemukan

l) Menjaga dan "merawat" keamanan

Menjaga keamanan dapat dilakukan dengan penjadwalan audit independen berkala, membaca log audit, menanggapi insiden, membaca literature yang terkini dan peringatan dari agency keamanan dan vendor keamanan, menginstal patch dan perbaikan keamanan, terus menguji dan melatih, dan memperbarui rencana keamanan dan kebijakan.

Network Asset terdiri dari:

1. Hardware
2. Software
3. Applications
4. Data
5. Intellectual property

6. Tradesecrets
7. Company‟s reputation

Resiko keamanan yang bias timbul adalah:

- Perangkat jaringan yang di-hack
- Data dapat dicegat, dianalisis, diubah, atau dihapus
- Password pengguna dapat dikompromikan atau diubah
- Konfigurasi perangkat yang dapat diubah
- Serangan *Reconnaissance*
- Serangan Denial-of-service

Dengan melihat resiko keamanan yang ada, maka akan ada konsekuensi atau *trade off* antara tujuan keamanan dengan tujuan bisnis, sehingga perlu dilihat kaitannya dengan:

- Affordability-kemampuan
- Usability-penggunaan
- Performance-kinerja
- Availability-ketersediaan
- Manageability–pengelolaan

Sebagai contoh dari *trade off* adalah bahwa rancangan keamanan dapat mengurangi redundansi jaringan. Jika semua lalu lintas data harus melalui perangkat enkripsi, misalnya, perangkat ini akan menjadi satu titik kegagalan (*single point of failure*). Hal ini akan mempersulit jika tujuannya adalah ketersediaan (*Availability*)

Perancangan keamanan (*Security Plan*) perlu dibuat dalam bentuk yang lebih formal (dokumen) dan high-level dokumen yang mengusulkan apa saja yang harus dilakukan organisasi untuk memenuhi persyaratan keamanan. Di dalamnya termasuk menentukan waktu, orang, dan sumber daya lainnya yang akan dibutuhkan untuk mengembangkan kebijakan keamanan dan mencapai kebijakan implementasi.

Kebijakan keamanan (Security Policy) menurut RFC 2196 “The Security Handbook” adalah "Pernyataan formal tentang aturan kepada siapa akan diberi akses ke teknologi dan aset informasi dari sebuah organisasi yang harus dipatuhi."

2. Mekanisme Keamanan (Security Mechanism)

Termasuk di dalamnya adalah:

- Physical security
- Authentication
- Authorization
- Accounting (Auditing)
- Data encryption
- Packetfilters
- Firewalls
- Intrusion Detection Systems (IDSs)

3. Rancangan Keamanan secara modular

Konsep rancangan keamanan secara modular memiliki konsep:

- Pertahanan keamanan secara mendalam

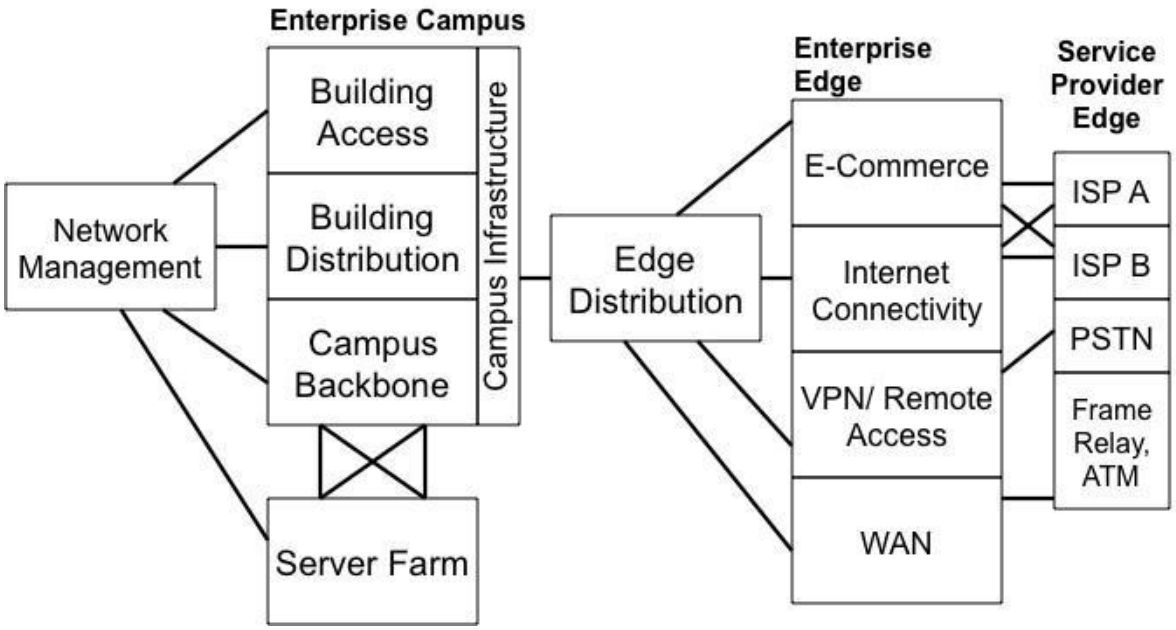
  Jaringan keamanan harus berlapis-lapis dengan berbagai teknik yang digunakan untuk melindungi jaringan

- Pendekatan Belt-dan-suspender

- Mengamankan semua komponen dari desain modular ini yaitu:
  - Koneksi internet
  - Publik server dan servere-commerce
  - Jaringan Remote akses dan VPN
  - Layanan jaringan dan manajemen jaringan
  - Server Farm atau Ruang Server
  - Layanan Pengguna melalui internet
  - Jaringan nirkabel

Contoh yang digunakan untuk sebuah enterprise adalah Cisco Enterprise Composite Network

Model:



Salah satu *blueprint* (cetak biru) dari keamanan data dibuat oleh Cisco Systems yang dinamakan Cisco SAFE (Security Architecture For the Enterprise). Blueprint Cisco SAFE ditujukan untuk keamanan di setiap modul dari arsitektur jaringan modular.

Apa saja yang harus diamankan pada modular design:

1. Mengamankan koneksi internet dengan cara:
    a. Physical security–kabel, hardware, ruang jaringan/server
    b. Firewalls and packet filters–hardware, policy, rule
    c. Auditlogs, authentication, authorization-credentials
    d. Well-defined exit and entry points–akses control
    e. Routing protocols that support authentication–OSPF

2. Mengamankan server-server untuk umum (public)
    a. Tempat server di DMZ yang dilindungi firewall
    b. Jalankan layanan firewall pada server itu sendiri
    c. Aktifkan perlindungan DoS
    d. Batasi jumlah koneksi perjangka waktu
    e. Gunakan system operasi yang handal dengan patch keamanan terbaru
    f. Menjaga modularitas
    g. Front-end server Web tidak menjalankan layanan lainnya

    Para ahli keamanan menyarankan bahwa layanan FTP jangan dijalankan pada server yang sama di server Web. Pengguna FTP memiliki lebih banyak kesempatan untuk membaca file dan juga mungkin mengubah file tersebut. Seorang hacker bias menggunakan FTP untuk merusak halaman web perusahaan, sehingga merusak citra perusahaan dan mungkin akan merusak aplikasi berbasis web seperti layanan e-commerce dan lainnya. Selain itu, setiap database server e-commerce yang menyimpan informasi pelanggan sensitive seperti keuangan harus terpisah dari server web front-end yang dilihat pengguna.

3. Mengamankan Layanan Remote-Access dan VPN, dengan menggunakan beberapa teknologi dan pengamanan seperti
    a. Keamanan Fisik–server, firewall, ruangan server (DMZ)
    b. Firewall–pengaturan policy, rule, adaptive secure network
    c. Otentikasi, otorisasi, dan audit–AAA
    d. Enkripsi–keamanan pengiriman data
    e. One-time password–token password, eq. keyBCA
    f. Keamanan protocol–protocol L3 yang aman
    g. CHAP–Challenge Handshake Authentication Protocol

h RADIUS-Radius adalah server untuk otentikasi remote user dan pencatatannya. Penggunaan utamanya adalah untuk Internet Service Provider, meskipun mungkin juga digunakan pada setiap jaringan yang membutuhkan otentikasi terpusat dan / atau layanan pencatatan user untuk work stationnya.

i. IPSec–Internet Protocol Security (IPsec) adalah protocol untuk mengamankan komunikasi data menggunakan Internet Protocol (IP) dengan otentikasi dan mengenkripsi setiap paket IP dari suatu sesi komunikasi. IP sec juga mencakup protocol untuk membangun otentikasi bersama antara agen pada awal sesi dan negosiasi kunci kriptografi yang akan digunakan selama sesi.

4. Mengamankan Layanan Jaringan

Beberapa best practice yang dapat dilakukan untuk mengamankan layanan jaringan adalah:

- Perlakukan setiap perangkat jaringan (router, switch, dan sebagainya) sebagai host yang bernilai dan perketat keamanannya terhadap gangguan yang mungkin terjadi
- Perlu ID login dan password untuk mengakses perangkat
    - Memerlukan otorisasi tambahan untuk perintah konfigurasi berisiko
- Gunakan SSH dari pada Telnet
- Mengubah MOTD (message of the day)–pesan awal diperangkat jaringan berupa peringatan

5. Mengamankan Fasilitas Server

Server merupakan jantung dari semua layanan jaringan dan aplikasi, untuk itu perlu dilakukan pengamanan pada fasilitas server ini dengan cara:

- Menggunakan server IDS pada jaringan untuk memonitor jaringan dan setiap server

- Mengkonfigurasi rule yang dapat mem-filter dan membatasi konektivitas dari server dalam kasus server dikompromikan
- Memperbaiki bug keamanan yang dikenal dalam system operasi server
- Gunakan otentikasi dan otorisasi untuk akses server dan manajemen
- Batasi password **root** untuk beberapa orang
- Matikan account "guests"

6. Mengamankan layanan untuk user

   Layanan internet untuk user sangat rentan terhadap aktifitas hacker, untuk perlu diperhatikan bagaimana menyediakan layanan seperti itu dengan:

   - Tentukan aplikasi yang diperbolehkan untuk dijalankan pada PC jaringan dalam kebijakan keamanan
   - Perlu personal firewall dan perangkat lunak antivirus pada PC jaringan
   - Menerapkan prosedur tertulis yang menentukan bagaimana perangkat lunak yang diinstal dan disimpan saat ini
   - Mendorong pengguna untuk *logout* ketika meninggalkan meja kerja mereka
   - Pertimbangkan untuk menggunakan 802.1X yaitu port berbasis keamanan pada switch

7. Mengamankan jaringan nirkabel (wireless network)

   Jaringan nirkabel saat ini sudah menjadi kebutuhan karena flexibilitasnya, namun tidak banyak fasilitas nirkabel yang memperhatikan masalah keamanan.

Beberapa hal yang perlu diperhatikan adalah:

- Tempatkan jaringan LAN nirkabel (WLAN) dalam subnet sendiri atau VLAN khusus
- Mengharuskan semua perangkat nirkabel (dan kabel) seperti laptop untuk menjalankan firewall pribadi dan perangkat lunak antivirus
- Nonaktifkan *beacon* yang menyebarkan SSID, dan gunakan otentikasi alamat MAC kalau perlu

Beberapa pilihan Security pada WiFi

- Wired Equivalent Privacy (WEP)
- IEEE802.11i
- Wi-Fi Protected Access (WPA)
- IEEE802.1XExtensible Authentication Protocol (EAP)
- Lightweight EAP or LEAP (Cisco)
- Protected EAP (PEAP)
- Virtual Private Networks (VPNs)

Beberapa hal mengenai Wired Equivalent Protocol (WEP):

- DitetapkanolehIEEE 802.11
- Pengguna harus memiliki kunci atau password WEP yang sesuai dan juga yang dikonfigurasi pada titik akses (Access Point)
- Menggunakan enkripsi kunci 64 atau 128-bit (atau pass phrase)
- WEP mengenkripsi data menggunakan metode RC4 *streamcipher*
- Tidak banyak diminati karena *crackable*

Beberapa alternative pada WEP saat ini:

- Vendor menambahkan fitur untuk WEP
- Menggunakan Temporal Key Integrity Protocol (TKIP)
- Setiap frame memiliki kunci WEP yang baru dan unik
- Menggunakan Advanced Encryption Standard(AES)
- Menggunakan standard IEEE 802.11i
- Menggunakan Wi-Fi Protected Access (WPA) dari Wi-Fi Alliance

Dengan protocol 802.1X dan EAP, perangkat memiliki salah satu dari tiga peran:

- Pemohon berada pada klien LAN nirkabel
- Authenticator berada pada titik akses
- Sebuah server otentikasi beradap ada server RADIUS
- Sebuah user yang menggunakan EAP pada klien memperoleh data otentikasi dari pengguna, yang bias menjadi user ID dan password
- Credentials yang disahkan oleh authenticator ke server dan kunci sesi dikembangkan

- Secara periodik klien harus *reauthenticate* untuk menjaga konektivitas jaringan
- Reauthentication menghasilkan, kunci WEP yang baru dan dinamis.

Cisco menggunakan Light Weight EAP (LW-EAP) dengan fitur:

- Standar EAP ditambah otentikasi bersama
- Parapengguna dan titik akses harus melakukan otentikasi
- Digunakan pada Cisco dan produk vendor lain
- EAP-Transport Layer Security (EAP-TLS) dikembangkan oleh Microsoft
- Membutuhkan sertifikat untuk klien dan server.
- Protected EAP (PEAP) didukung oleh Cisco, Microsoft, dan RSA Security
- Menggunakan sertifikat untuk klien untuk mengotentikasi server RADIUS
- Server menggunakan username dan password untuk autentikasi klien
- EAP-MD5 tidak memiliki fitur manajemen kunci atau generasi kunci dinamis
- Menggunakan teks tantangan seperti otentikasi WEP dasar
- Otentikasi ditangani oleh server RADIUS

VPN Software pada lingkungan Wireless

-
- EAP-Transport Layer Security (EAP-TLS) dikembangkan oleh Microsoft
- Membutuhkan sertifikat untuk klien dan server.
- Protected EAP (PEAP) didukung oleh Cisco, Microsoft, dan RSA Security
- Menggunakan sertifikat untuk klien untuk mengotentikasi server RADIUS
- Server menggunakan username dan password untuk autentikasi klien
- EAP-MD5 tidak memiliki fitur manajemen kunci atau generasi kunci dinamis
- Menggunakan teks tantangan (challenge) seperti otentikasi WEP dasar
- Otentikasi ditangani oleh server RADIUS

SIMPULAN

Keamanan bukan hanya secara fisik, tapi juga secara logic. Perancangan yang baik akan memudahkan dalam managedan maintain jaringan. Sebagai Enterprise, perancangan model komposit dari Cisco bisa menjadi acuan untuk membuat jaringan pada kantor. Keamanan jaringan adalah masalah end-to-end security, karena harus dibuat menyeluruh dari computer pengguna sampai ke Server dan Jaringan Internet luar.

DAFTAR PUSTAKA

1. Oppenheimer, Priscilla. (2013). ***Top Down Network Design***. 3rd Edition. Cisco Press. Indianapolis. ISBN: 978-1-58705-152-4.

2. Hummel, S. L. (2015). ***Cisco Design Fundamentals: Multilayered Network Architecture and Design for Network Engineers*.**

3. Bruno, A., & Jordan, S. (2016). ***CCDA 200-310 Official Cert Guide***. Cisco Press.