MATERI PEMBELAJARAN TEKNOLOGI INFORMASI

Sejarah Perkembangan Keamanan Jaringan

Evolusi perlindungan infrastruktur digital dari eksperimen ARPANET 1970-an hingga era Zero Trust dan Kecerdasan Buatan.

Modul Modul Keamanan Siber & Systems Network

AWAL MULA KOMPUTASI TERHUBUNG

Era 1970-an: Creeper & Eksperimen Pertama

Program Creeper (1971)

Eksperimen Mandiri: Diciptakan Bob Thomas pada jaringan ARPANET untuk menguji pergerakan program antar mainframe.

Reaper: Antivirus Pertama (1972)

Protokol Pembersihan: Program tandingan buatan Ray Tomlinson khusus untuk menghapus Creeper dari sistem.

Karakteristik Utama Era

Ancaman Akademis: Belum ada motif kejahatan finansial; fokus pada riset fleksibilitas jaringan.



STANDARDISASI & ANCAMAN NYATA

Era 1980–an: Adopsi TCP/IP & Worm Morris

Worm Morris (1988)

Serangan malware jaringan skala besar pertama yang menginfeksi sekitar 6.000 komputer terhubung ARPANET (10% dari seluruh internet saat itu).

Dampak: Lahirnya CERT/CC (Response Team)

Lahirnya Proteksi Terstruktur

Pengembangan teknologi Packet Filtering awal oleh Digital Equipment Corp (DEC) serta regulasi hukum Computer Fraud and Abuse Act.

Fokus: Penyaringan lalu lintas data mendasar

KOMERSIALISASI WEB & ENKRIPSI

Era 1990-an: Lahirnya Firewall & Enkripsi SSL

1. Stateful Inspection Firewall

Check Point merilis Firewall-1 (1994) untuk memantau status koneksi aktif secara kontekstual.

2. Enkripsi Transaksi SSL/TLS

Netscape mengembangkan SSL (1995) untuk mengamankan data e-commerce dan transaksi web.

3. Komersialisasi Antivirus & IDS

Pertumbuhan pesat perangkat lunak antivirus komersial dan Sistem Deteksi Intrusi (IDS).



EVOLUSI CYBERWARFARE & MOBILE

Era 2000-an: Perang Siber & Proteksi Nirkabel

Keamanan Nirkabel (WPA)

Pengembangan WPA & WPA2 menggantikan protokol WEP yang terbukti mudah diretas.

Ancaman Stuxnet (2010)

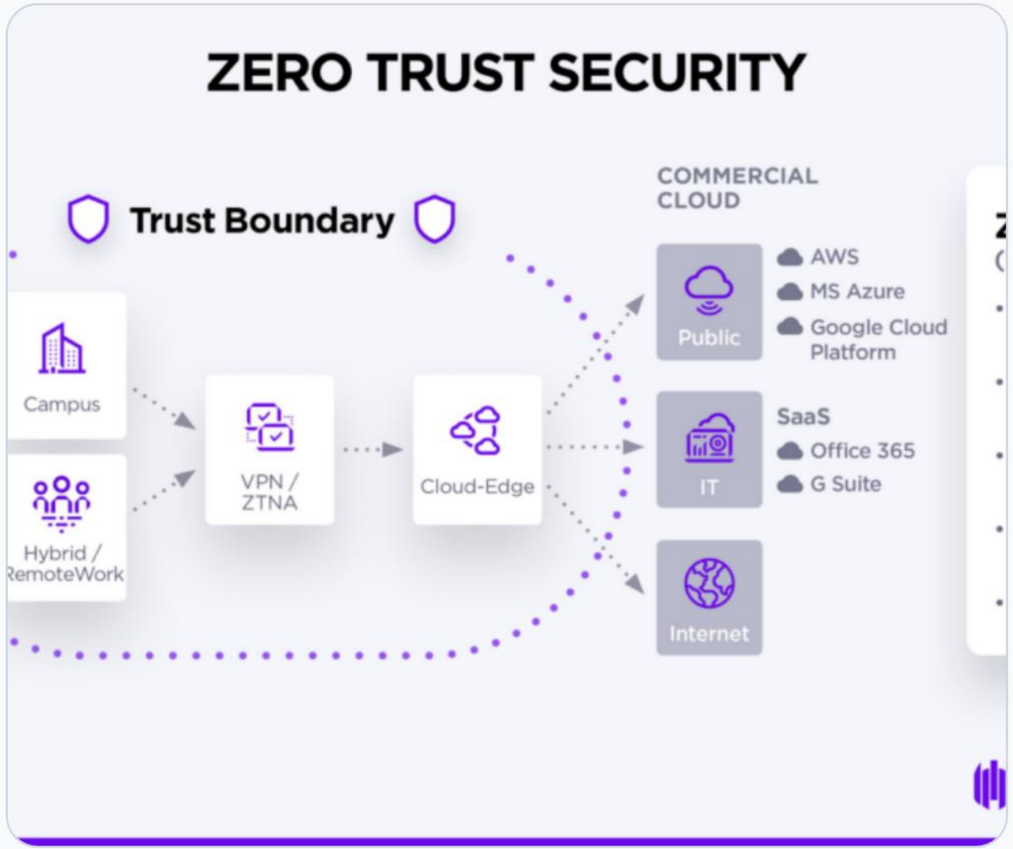
Malware pertama yang merusak infrastruktur fisik industri secara nyata.

Next-Gen Firewall (NGFW)

Pemeriksaan mendalam hingga lapisan aplikasi (Deep Packet Inspection).

TRANSFORMASI DIGITAL & CLOUD

Era 2010–an: Komputasi Cloud & Paradigm Zero Trust



Wabah Ransomware Massal

Serangan WannaCry & NotPetya (2017) memicu kerugian miliaran dolar secara global.

Adopsi Arsitektur Zero Trust

Diperkenalkan Forrester/NIST: Prinsip utama "Never Trust, Always Verify" tanpa perimeter aman.

Keamanan Berbasis Cloud (CASB)

Pengawasan akses data perusahaan pada aplikasi SaaS dan infrastruktur multi-cloud.

INOVASI MASA KINI & MENDATANG

Era Modern 2020+: AI & Kriptografi Kuantum

Deteksi Ancaman AI/ML

Analisis perilaku lalu lintas jaringan waktu-nyata untuk pencegahan anomali otomatis.

Kriptografi Post-Kuantum

Pengembangan standar enkripsi baru tahan serangan komputer kuantum masa depan.

Arsitektur SASE & SSE

Penyatuan fungsi jaringan SD-WAN dan keamanan terintegrasi penuh di cloud.

Autentikasi Tanpa Kata Kunci

Penerapan standar FIDO2 dan biometrik terdesentralisasi pengganti kata sandi.

RANGKUMAN LINTAS DEKADE

Garis Waktu Evolusi Proteksi Jaringan

1970-AN

Reaper

Antivirus pertama penangkal program Creeper.

1980-AN

Packet Filter

Penyaringan lalu lintas IP dasar awal.

1990-AN

Firewall & SSL

Stateful firewall dan enkripsi web HTTP.

2000-AN

NGFW & WPA2

Inspeksi mendalam & enkripsi Wi-Fi kuat.

2020+

Zero Trust & AI

Otomasi ancaman pintar & verifikasi total.

PERGESERAN PARADIGMA KEAMANAN

Perbandingan: Perimeter vs Zero Trust

Model Perimeter Klasik

Kepercayaan Implisit: Menganggap aman siapapun di dalam jaringan internal.

Fokus Benteng Luar: Mengandalkan Firewall & VPN batas luar.

Rentan Lateral Movement: Sekali terbobol, peretas bebas menjelajah.

Arsitektur Zero Trust Modern

Verifikasi Selalu: Autentikasi berulang setiap kali meminta akses data.

Hak Akses Minimal: Hanya memberikan hak akses seperlunya (Least Privilege).

Mikrosegmentasi: Membatasi area jaringan agar penyebaran ancaman terisolasi.

REALITAS KEAMANAN SIBER GLOBAL

Dampak Ekonomi & Urgensi Proteksi

$10.5T

Estimasi Kerugian Kejahatan Siber Global per Tahun pada 2025

277 Hari
Rata-rata Identifikasi Kebocoran Data

95%
Insiden Dipicu Faktor Kesalahan Manusia

+300%
Peningkatan Serangan Supply Chain

FONDASI SISTEM AMAN

Pilar Utama Keamanan Jaringan Modern

Kerahasiaan

Confidentiality: Memastikan data sensitif hanya dapat diakses oleh pihak berwenang.

Integritas

Integrity: Menjamin data tidak diubah atau dimanipulasi selama proses transmisi.

Ketersediaan

Availability: Memastikan sistem dan layanan jaringan selalu siap digunakan saat dibutuhkan.

Autentikasi

Authentication: Memverifikasi identitas pengguna dan perangkat sebelum memberikan akses.

RANGKUMAN & DISKUSI

Keamanan Adalah Proses Berkelanjutan, Bukan Tujuan Akhir

Ancaman siber akan terus berevolusi seiring perkembangan teknologi. Kunci keberhasilan terletak pada adaptasi arsitektur dan kesadaran pengguna.



Terima Kasih — Sesi Tanya Jawab & Diskusi

Image Sources



https://i.ytimg.com/vi/wljgZhAjQS4/sddefault.jpg

Source: www.youtube.com



https://images.pond5.com/cybersecurity-concept-showing-digital-shield-footage-328700717_iconl.jpeg

Source: www.pond5.com



https://images.contentstack.io/v3/assets/blt53c99b43892c2378/blt1aa641555e52467c/68c98dd2bcb8301e4c01773e/zero-trust-security-1024x536.png

Source: www.sentinelone.com