RANGKUMAN MATERI
CYBERSECURITY LANDSCAPE
KEAMANAN SISTEM DAN JARINGAN KOMPUTER

DISUSUN OLEH:

FANNY BAGUS RAMADHAN 1931733111

KELAS 3D

Dosen Pengampu : Toga Aldila Cinderatama, S.ST.,M.Sc.

D3 MANAJEMEN INFORMATIKA

PSDKU POLITEKNIK NEGERI MALANG KEDIRI

KOTA KEDIRI

2020

1. Kesimpulan Materi

Jaringan sangat rawan terhadap penyerangan dan pencurian data informasi. Untuk itu perlu adanya sebuah keamanan untuk jaringan yang dapat mengatasi serangan dan pencurian data informasi.

2. Rangkuman Cyber Security Landscape

A. Pegertian Dari CyberSecurity
Cyber security adalah perlindungan sistem yang terhubung ke internet, termasuk perangkat keras, perangkat lunak, dan data dari serangan cyber.

B. Konsep Dasar Cyber Security

Keamanan cyber secara keseluruhan adalah istilah yang sangat luas tetapi didasarkan pada tiga konsep dasar yang dikenal sebagai “The CIA Triad” yang terdiri atas Confidentiality (kerahasiaan), Integrity (integritas), dan Availability (ketersediaan).

1. Integrity
   Integrity memastikan bahwa data konsisten, akurat, dan dapat dipercaya selama periode tertentu. Ini berarti bahwa data dalam transit tidak boleh diubah, dihapus atau diakses secara ilegal.
2. Confidentiality
   Confidentiality atau kerahasiaan merupakan aturan yang membatasi akses informasi dengan cara mengambil langkah-langkah untuk membatasi informasi sensitif agar tidak diakses oleh peretas dunia maya.
3. Availability

Ketersediaan dalam hal ini mencakup keperluan seperti perangkat keras, perangkat lunak, jaringan, dan peralatan keamanan yang harus dipelihara dan ditingkatkan performanya.

C. Tujuan Keamanan Jaringan Menurut Garfinkel dan Spafford

1. Availability (Ketersediaan)
   Memberitahu bahwa ketersediaan informasi data yang tersedia bagi mereka yang mempunyai hak ketika dibutuhkan
2. Reliability (Kehandalan)
   Mengisyaratkan bahwa kehandalan sangat penting untuk sebuah informasi yang sangat dibutuhkan
3. Confidentiality (Kerahasiaan)
   Membutuhkan bahwa ketersediaan data informasi dapat diakses oleh siapapun yang memiliki otoritas
4. Authentication (Otentikasi)
   Membutuhkan bahwa pengirim informasi dapat diidentifikasi dengan benar dan tidak ada jaminan bahwa identitas palsu yang diperoleh
5. Integrity (Integritas)
   Membutuhkan bahwaa informasi hanya dapat diubah oleh pihak yang memiliki otoritas.

D. Contoh Keamanan Jaringan

1. Firewalls
   Firewalls mencegah pengguna yang tidak sah mengakses jaringan pribadi. Firewall adalah kombinasi perangkat keras dan lunak yang mengontrol aliran lalu lintas jaringan yang masuk dan keluar. Biasanya ditempatkan di antara internal pribadi organisasi jaringan dan jaringan eksternal yang tidak dipercaya, seperti Internet, meskipun firewall juga dapat digunakan untuk melindungi satu bagian dari jaringan perusahaan dari sisa jaringan.
2. Intrusion Detection System
   vendor keamanan komersial sekarang menyediakan alat dan layanan deteksi intrusi untuk melindungi terhadap lalu lintas dan upaya jaringan yang mencurigakan untuk mengakses file dan basis data. Bernama Intrusion Detection System fitur alat pemantauan penuh waktu ditempatkan di titik-titik yang paling rentan atau hot spot jaringan perusahaan untuk mendeteksi dan mencegah penyusup secara terus menerus. Sistem menghasilkan alarm jika ditemukan peristiwa yang mencurigakan atau anomali. Perangkat lunak pemindaian mencari pola yang mengindikasikan metode serangan komputer yang dikenal seperti kata sandi buruk, memeriksa untuk melihat apakah file penting telah dihapus atau dimodifikasi, dan mengirimkan peringatan vandalisme atau kesalahan administrasi sistem. Alat deteksi intrusi juga dapat disesuaikan untuk mematikan bagian jaringan yang sangat sensitif jika menerima lalu lintas yang tidak sah.

3. Software Antivirus dan Anti Spyware
   Paket teknologi defensif untuk individu dan bisnis harus mencakup perlindungan antimalware untuk setiap komputer. Perangkat lunak antivirus mencegah, mendeteksi, dan menghapus malware, termasuk virus komputer, worm komputer, Trojan horse, spyware, dan adware. Namun, sebagian besar perangkat lunak antivirus hanya efektif terhadap malware diketahui kapan perangkat lunak itu ditulis. Agar tetap efektif, perangkat lunak antivirus harus terus diperbarui. Meski begitu itu tidak selalu efektif karena beberapa malware bisa menghindari deteksi antivirus. Organisasi perlu menggunakan deteksi malware tambahan alat untuk perlindungan yang lebih baik

E. Contoh Ancaman Jaringan
   1. Sniffer Peralatan yang dapat memonitor proses yang sedang berlangsung
   2. Spoofing Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP.
   3. Remote Attack Segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jaruh di luar sistem jaringan atau media transmisi
   4. Hole Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi Beberapa Bentuk Ancaman Jaringan
   5. Phreaking Perilaku menjadikan sistem pengamanan telepon melemah
   6. Hacker
      – Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya.
      – Hacker tidak merusak sistem
   7. Craker
      – Orang yang secara diam-diam mempelajari sistem dengan maksud jahat
      – Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak)

SUMBER

Youtube : https://www.youtube.com/watch?v=E3IC32iErwU

Website : http://mas-daof.blogspot.com/2015/11/pentingnya-kemanan-jaringan-komputer.html

https://id.wikipedia.org/wiki/Keamanan_komputer

https://www.jagoanhosting.com/blog/pengetahuan-lengkap-tentang-ilmu-cyber-security/