TUGAS KEAMANAN TEKNOLOGI INFORMASI

Untuk Memenuhi Tugas Keamanan Teknologi Informasi

Dosen:

Gregorius Hendita A K, S.Si.,M.Cs

Disusun oleh:

Nadiyah Qasamah

4522210046

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS PANCASILA

JAKARTA

2024

Resume :

Perkembangan yang semakin hari semakin maju, sehingga memberikan dampak yang besar dalam semua kegiatan.Akan tetapi seiring dengan bertambahnya pengguna internet yang terus meningkat, serta kurangnya kesadaran akan keamanan perlindungan data. Dimana semakin meningkat juga kejahatahan yang terjadi dalam penyalahgunaan data yang bersifat pribadi oleh pihak yang tidak bertanggung jawab. Keamanan hal terpenting dalam sistem informasi sebagai pencegahan agar tidak disalah gunakan. Internet sebagai jalur informasi yang merupakan jaringan bersifat global sehingga dapat diakses secara publik.

Disisi lain serangan yang sering terjadi diera digital yaitu serangan *cyber* dapat berupa mencuri data, memanipulasi informasi, perusakan sistem, dan serangan *malware.* Hal yang dapat dilakukan yaitu melakukan menyusun strategi pemeliharan guna mengurangi resiko serangan yang terjadi. Adapun beberapa jenis *cyber crime* yang sering kali terjadi yaitu :

1. *Cybersex*

   Cybersex merupakan aktivitas pornografi yang terjadi di internet dan diakses secara bebas termasuk anak-anak yang belum mencapai usia dewasa.
2. *Hacker*

   Hacker adalah kegiatan yang dilakukan individu secara illegal dengan mengakses jaringan menggunakan alat dan program, tujuannya merusak ataupun merusak data sehingga kerusakan pada sistem jaringan. *Hacker* tidak memasuki jaringan secara fisik, tetapi melalui alat digital.
3. Penipuan OTP

   OTP atau *On Time Password* merupakan kejahatan yang sering ditemui melalui pesan yang berisi kode rahasia elektronik. Kejahatan jenis ini biasanya menyamar perwakilan dari aplikasi tertentu.
4. *Phising*

   Phising metode penipuan dengan mencuri akun korban yang dituju. Pelaku biasanya mengirim pesan melalui e-*mail* atau pesan melalui sosial media. Upaya ini dilakukan untuk mendapatkan terkait informasi pribadi.

Upaya untuk melindungi infrastruktur teknologi informasi dari serangan, diperlukan startegi pencegahan yang dilakukan secara menyeluruh. Adapun beberapa Langkah yag dapat dilakukan mengurangi dampak dari serangan :

1. Penggunaan *Firewall*

Dengan mengimplementasikan *firewall* yang kuat guna mengendalikan lalu lintas yang terjadi pada jaringan, sehingga mencegah adanya akses yang tidak sah serta melindungi sistem dari serangan eksternal.

2. Antivirus dan Anti-*Malware*

   Memperbarui secara rutin perangkat lunak antivirus dan anti *malware* untuk tujuan mendeteksi dan menghapus dari ancaman yang bisa timbul.

3. Enkripsi Data

   Menggunakan teknologi enkripsi untuk melindungi data, secara dikirim muapun saat disimpan, apabila dat dicuri, tidak dapat dibaca oleh pelaku.

4. Pemantauan Sistem

   Melakukan pemantauan secara aktif terhadap aktivitas sistem dan jaringan untuk mengidentifikasi pola atau perilaku mencurigakan.

Pelatihan pada sumber daya manusia juga merupakan faktor yang utama, dengan melakukan simulasi serangan, dann penting dilakukan untuk meningkatkan keterampilan serta kesadaran. Terlebih lagi pada era digital, perkembangan ancaman *cyber* juga menjadi kompleks dan pesat.

Sumber :

1. Samudra, Y., Hidayat, A., & Wahyu, M. F. (2023). Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital. *AMMA: Jurnal Pengabdian Masyarakat*, *1*(12), 1594-1601.
2. Susanto, E., Antira, L., Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. Journal of Business And Entrepreneurship, 11(1), 23-33.
3. Hoshmand, M. O., & Ratnawati, S. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. Jurnal Sains dan Teknologi, 5(2), 679-686.