**PRAKTIKUM KEAMANAN JARINGAN**

**“APNIC 2”**



**Oleh :**

**Andre Septian Prayogo**

**D4 LJ Teknik Informatika B**

**3122640033**

**POLITEKNIK ELEKTRONIKA NEGERI SURABAYA**

**TAHUN AJARAN**

**2023**

**APNIC MODULE 2: CYBER SECURITY IN THE ORGANIZATION**

Sebuah ancaman yang menyerang kerentanan pada suatu organisasi dapat mengganggu aktifitas dan operasi bisnis, berikut merupakan ancaman-ancaman yang mungkin saja bisa terjadi:

**Ancaman keamanan pada Organisasi**

1. **Denial of Service Attack**

DDOS attack atau Distributed Denial of Service merupakan serangan cyber dengan cara mengirimkan fake traffic atau lalu lintas palsu ke suatu sistem atau server secara terus menerus. Dampaknya, server tersebut tidak dapat mengatur seluruh traffic sehingga menyebabkan down. Umumnya serangan ini menyasar jaringan, layanan online, hingga website, dengan tujuan agar server tersebut tidak dapat mengakomodasi traffic atau lalu lintas sehingga website mengalami down dan tidak dapat beroperasi.

1. **Malware**

Malware atau Malicious software adalah perangkat lunak yang dibuat dengan tujuan memasuki dan merusak sistem komputer, jaringan, atau server tanpa diketahui oleh pemiliknya. Tujuannya tentu untuk merusak atau mencuri data dari perangkat yang dimasuki. Malware biasanya disusupkan ke dalam jaringan internet. Jika secara manual memasukkan ke dalam komputer korban tentu saja sangat sulit. Jadi kebanyakan peretas melakukan aksinya menggunakan bantuin jaringan internet. Contohnya: virus, worms, rootkits, backdoors, trojans.

1. **Identity theft**

dentity theft atau pencurian identitas adalah kejahatan yang dilakukan dengan menyalahgunakan identitas orang lain untuk memperoleh keuntungan. Kejahatan dengan mengatasnamakan orang lain ini terjadi ketika pelaku menggunakan informasi pribadi seseorang, seperti nama, identitas kependudukan, nomor kartu kredit, dan lainnya tanpa ada persetujuan. Modus Pencurian Identitas seperti phising dengan menyebarkan link palsu yang meminta korban untuk mengisikan informasi pribadinya dan data breach yaitu dengan membobol data dengan crack melalui database dengan tujuan mencari data sensitive.

1. **Web Defacement**

Sebuah serangan terhadap website dengan tujuan untuk mengganti konten sebuah website yang bertujuan untuk mengirimkan pesan tertentu, atau sebatas menunjukkan kemampuan mereka. Biasanya, pesan yang diberikan oleh pelaku deface ada dalam berbagai lingkup seperti politik, agama, ataupun kata-kata yang tidak pantas dengan tujuan mempermalukan website atau organisasi yang diserang.

Cara untuk mengurangi Resiko serangan Siber

1. Teknikal kontorl untuk mendeteksi dan mencegah seperti memasang firewall,spam filters, intrusion sistem detection, dan antivirus software.
2. Edukasi dan pelatihan karyawan khususnya saat mengatasi phising dengan cara membuat aplikasi website aman
3. Memastikan penyedia jaringan memiliki kemampuan untuk mendukung organisasi saat organisasi diserang

Meningkatkan perisapan untuk keamanan siber

1. Pendekatan manajemen risiko yang komprehensif harus melibatkan seluruh orang di organisasi untuk meningkatkan kualitas pengambilan keputusan dalam mengelola risiko.
2. Top management suatu organisasi bertanggung jawab untuk memastikan keamanan organisasi.
3. Mengetahui tingkat dan kemungkinan risiko dapat membantu organisasi menjadi lebih proaktif dan siap.
4. Upaya-upaya ini mengharuskan organisasi untuk menginvestasikan sumber daya (seperti waktu dan orang) untuk mengembangkan program keamanan siber yang komprehensif.