System Vulnerabilities, Threat, And Countermeasure (Kelemahan Sistem, Ancaman, dan Penanggulangan)

KELOMPOK 11

Sonia Eka Pratiwi :1310651025

Ryansyah A :1310651102

Wildan Wahyu Saputro :1310651135

System Vulnerabilities

ATAU KELEMAHAN DALAM SISTEM, KERENTANAN DAN PENYALAHGUNAAN SISTEM KETIKA SEJUMLAH DATA PENTING DALAM BENTUK DIGITAL, MAKA DATA TERSEBUT RENTAN TERHADAP BERBAGAI JENIS ANCAMAN, DARI PADA DATA YANG TERSIMPAN SECARA MANUAL.

ANCAMAN-ANCAMAN TERSEBUT BISA SAJA BERASAL DARI FAKTOR TEKNIS, ORGANISASI, DAN LINGKUNGAN YANG DIPERPARAH OLEH AKIBAT KEPUTUSAN MANAJEMEN YANG BURUK.

Threat

- **Unauthorized Access to Computer System and Service** : Pada kejahatan ini dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya. Biasanya pelaku kejahatan (hacker) melakukannya dengan maksud sabotase ataupun pencurian informasi penting dan rahasia.
- **Illegal Contents** : Kejahatan ini merupakan kejahatan dengan memasukkan data atau informasi ke Internet tentang sesuatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum. Sebagai contohnya, pemuatan suatu berita bohong atau fitnah yang akan menghancurkan martabat atau harga diri pihak lain, hal-hal yang berhubungan dengan pornografi atau pemuatan suatu informasi yang merupakan rahasia negara, agitasi dan propaganda untuk melawan pemerintahan yang sah dan sebagainya

Threat

- **Cyber Sabotage and Extortion** : Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan Internet. Biasanya kejahatan ini dilakukan dengan menyusupkan suatu logic bomb, virus komputer ataupun suatu program tertentu, sehingga data, program komputer atau sistem jaringan komputer tidak dapat digunakan, tidak berjalan sebagaimana mestinya, atau berjalan sebagaimana yang dikehendaki oleh pelaku.
- **Cybercrime** : Perkembangan Internet dan umumnya dunia cyber tidak selamanya menghasilkan hal-hal yang postif. Salah satu hal negatif yang merupakan efek sampingannya antara lain adalah kejahatan di dunia cyber atau disebut juga dengan nama cybercrime. Hilangnya batas ruang dan waktu di Internet mengubah banyak hal. Sebagai contoh adalah seseorang cracker di Rusia dapat masuk ke sebuah server di Pentagon tanpa ijin.

Penanggulangannya

- aktivitas pokok dari cybercrime adalah penyerangan terhadap content, computer system dan communication system milik orang lain atau umum di dalam cyberspace. Fenomena cybercrime memang harus diwaspadai karena kejahatan ini agak berbeda dengan kejahatan lain. Cybercrime dapat dilakukan tanpa mengenal batas teritorial dan tidak memerlukan interaksi langsung antara pelaku dengan korban kejahatan. Berikut ini cara penanggulangannya :

Penanggulangan

- 1. Mengamankan sistem
- 2. Penanggulangan Global melakukan modernisasi hukum pidana nasional beserta hukum acaranya. meningkatkan sistem pengamanan jaringan komputer nasional sesuai standar internasional. meningkatkan pemahaman serta keahlian aparatur penegak hukum mengenai upaya pencegahan, investigasi dan penuntutan perkara-perkara yang berhubungan dengan cybercrime. meningkatkan kesadaran warga negara mengenai masalah cybercrime serta pentingnya mencegah kejahatan tersebut terjadi. meningkatkan kerjasama antarnegara, baik bilateral, regional maupun multilateral, dalam upaya penanganan cybercrime.
- 3. Perlunya Cyberlaw
- 4. Perlunya Dukungan Lembaga Khusus