Case Study Review: Kasus “Nth Room” — Manipulasi Psikologis dalam Kejahatan Siber

Pendahuluan

Dalam era digital, kejahatan siber tidak hanya dilakukan melalui serangan teknis, tetapi juga melalui manipulasi psikologis yang dikenal sebagai *social engineering*. Salah satu kasus paling mencolok yang menggambarkan betapa berbahayanya teknik ini adalah kasus “Nth Room” di Korea Selatan. Kasus ini bukan sekadar pelanggaran privasi, melainkan bentuk eksploitasi sistematis terhadap korban melalui tipu daya, ancaman, dan kendali psikologis di ruang digital.

Kronologi Singkat

Kasus Nth Room muncul sekitar tahun 2018–2020 di platform pesan terenkripsi *Telegram*. Sejumlah pelaku, dipimpin oleh seorang pengguna dengan nama samaran “Baksa” (Dokter), membuat grup obrolan rahasia bernama *Nth Room* yang berisi konten eksploitasi seksual. Pelaku merekrut korban dengan cara menipu mereka agar mengirim foto pribadi, lalu menggunakannya untuk melakukan pemerasan (*sextortion*). Para korban dipaksa mengikuti perintah pelaku di bawah ancaman penyebaran data pribadi. Grup ini menjadi ladang kejahatan digital berskala besar: lebih dari 70.000 anggota dilaporkan berpartisipasi dalam melihat dan menyebarkan konten ilegal tersebut. Kasus ini akhirnya terbongkar setelah investigasi panjang oleh kepolisian dan media Korea Selatan.

Teknik Social Engineering yang Digunakan

Kasus Nth Room menunjukkan penerapan beberapa teknik *social engineering* yang sangat efektif:

1. **Pretexting (Penyamaran dan Dalih Palsu)**

Pelaku sering menyamar sebagai perekrut kerja, fotografer, atau figur publik untuk membangun kepercayaan awal pada korban. Dengan menciptakan identitas palsu yang meyakinkan, mereka memperoleh informasi pribadi secara sukarela dari korban.

2. **Phishing dan Manipulasi Emosional**

Korban sering diarahkan ke tautan palsu atau diminta mengirim data pribadi melalui pesan. Setelah mendapatkan materi sensitif, pelaku menggunakan *fear appeal* — ancaman akan menyebarkan konten pribadi — untuk mengendalikan korban.

3. **Authority dan Trust Exploitation**

Pelaku menciptakan ilusi otoritas dengan bahasa formal dan sistem hierarki di dalam grup, membuat korban dan anggota lainnya patuh pada instruksi tanpa banyak bertanya.

Pelajaran yang Dapat Dipetik

Kasus ini memberi sejumlah pelajaran penting tentang keamanan siber:

- Keamanan digital bukan hanya soal teknologi, tapi juga psikologi.
- Waspadai setiap permintaan data pribadi dari sumber yang tidak jelas.
- Edukasi publik tentang privasi digital serta budaya melapor menjadi kunci pencegahan kasusserupa.

Kesimpulan

Kasus Nth Room menjadi simbol gelap dari bagaimana *social engineering* dapat menghancurkan kehidupan seseorang tanpa menyentuh sistem komputer apa pun. Dengan memahami teknik manipulasi psikologis yang digunakan pelaku, masyarakat dapat lebih waspada terhadap ancaman di dunia maya. Edukasi, empati, dan kesadaran digital adalah benteng utama untuk mencegah tragedi serupa terjadi di masa depan.

Disusun oleh:
Rifky Febrian Iskandar
Kelas 12 SIJA
SMK TI Bazma