Nama : Shabrina Amalia Putri
Kelas : Keamanan Informasi A
No Absen : 30

Social Engineering

Social Engineering atau Rekayasa sosial adalah manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia. Rekayasa sosial ini pada umumnya dilakukan melalui media telepon atau Internet. Teknik ini merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi mengenai targetnya, yaitu dengan meminta informasi langsung kepada target yang mempunyai informasi. Rekayasa sosial fokus kepada rantai terlemah sistem jaringan komputer, yaitu manusia. Karena semua sistem komputer melibatkan interaksi manusia. maka, celah keamanan ini bersifat universal, tidak tergantung kepada sistem operasi, platform, protokol, perangkat lunak, ataupun juga perangkat keras. Oleh sebab itu setiap sistem mempunyai kelemahan yang sama yaitu pada faktor manusia. Jenis social engineering yaitu :

1. Phising

Phishing menjadi jenis serangan paling umum dalam social engineering. Hacker akan menggunakan email yang berisi pesan palsu dan link berbahaya untuk memancing korban agar memberikan informasi penting. Agar korban percaya, hacker akan menulis pesan semirip mungkin dengan perusahaan resmi. Pesan juga akan ditulis dengan bahasa yang mampu menimbulkan rasa urgensi sehingga korban akan membuka link berbahaya dan memberikan data sensitif seperti user id, password, atau data penting lainnya. Jika Anda menemukan email yang mencurigakan sebaiknya hindari untuk membuka attachment atau link di dalamnya karena hacker juga bisa mengirim malware melalui email tersebut. Pada video tersebut terdapat beberapa contoh taktik hacker untuk menyerang pengguna yaitu, contoh pertama hacker mengirimkan suatu email dimana isi email tersebut adalah akun si pengguna ter hacked yang mengharuskan si pengguna harus mengirimkan sejumlah uang kepada si hacker, kedua yaitu si hacker meminta si pengguna untuk me reset password akun nya di link yang disiapkan si hacker agar si hacker dapat mendapatkan informasi password pengguna, ketiga adalah si hacker mengirimkan permintaan pembayaran melalui email pengguna yang mengaku sebagai bank of Ireland dan meminta si pengguna untuk melakukan pembayaran 84.00 euro/ bulan di akunnya, dan yang keempat yaitu hacker meminta donasi amal yang berpura pura sebagai asisten yayasan swasta.

2. Pretexting

Dalam metode pretexting, hacker akan membuat skenario palsu untuk mencuri data pribadi korban. Serangan ini bisa dilakukan melalui telpon atau email. Hacker akan berpura-pura menjadi petugas bank, petugas lembaga negara, rekan kerja, atau bahkan staff IT perusahaan yang sedang membutuhkan info dari korban untuk tugas urgent. Keberhasilan pretexting ini tergantung dari kemampuan hacker dalam membangun kepercayaan dengan korban. Pada video tersebut, terdapat contoh hacker melakukan serangan ke help desk melalui telepon dan berpura pura lupa password akunnya lalu si hacker meyakinkan help desk agar memberikan password yang si hacker inginkan.

Tahapan cycle social engineering

1. Information gathering
   Kemungkinan berhasil untuk sebagian besar serangan tergantung pada fase ini sehingga wajar untuk menginvestasikan sebagian besar waktu dan perhatian di sini. Teknik pengumpulan informasi diuraikan dalam metode ini. Beberapa informasi yang dikumpulkan digunakan untuk menentukan vektor serangan, kemungkinan kata sandi, mengidentifikasi kemungkinan respons dari berbagai individu, menyempurnakan tujuan, menjadi terbiasa dan nyaman dengan target, dan merumuskan alasan kuat.

2. Developing relationship
   Fase ini dapat membangun hubungan kerja dengan target. Ini adalah titik kritis karena kualitas hubungan yang dibangun oleh penyerang menentukan tingkat kerjasama dan sejauh mana target akan pergi untuk membantu penyerang mencapai tujuan. Bisa jadi menghubungkan pada tingkat pribadi melalui telepon atau sebagai pribadi seperti menunjukkan foto keluarga dan berbagi cerita dengan. Ini juga bisa seluas membangun hubungan online dengan target melalui profil palsu di situs kencan atau jejaring sosial. Menciptakan hubungan baik dibahas secara lebih mendalam dalam metode ini.

3. Exploitation
   Eksploitasi terjadi ketika penyerang menggunakan informasi yang telah mereka kumpulkan dan hubungan yang telah mereka bangun untuk secara aktif mendapatkan akses atau menyusup ke target. Sebagian besar kelompok yang ditargetkan adalah Staf Junior, Administrator, Staf Dukungan. Mereka dapat dengan mudah dimanipulasi melalui simulasi permintaan yang menyamar sebagai "posisi yang lebih tinggi" di perusahaan. Kadang-kadang penyerang dengan sengaja menempatkan orang-orang target di bawah batasan waktu yang ditentukan, seperti penyelesaian kontrak atau pembayaran faktur, untuk menempatkan mereka di bawah tekanan yang memaksa keputusan di bawah tekanan. Di bawah tekanan ini, individu dapat membuat kesalahan dan penyerang dapat memaksa perubahan detail akun pada pembayaran atau membuat individu untuk mengungkapkan informasi sensitif seperti kata sandi dan nama pengguna.

4. Execution

   Fase ini adalah ketika tujuan akhir serangan tercapai, atau karena berbagai alasan, serangan berakhir sedemikian rupa agar tidak menimbulkan kecurigaan mengenai apa yang telah terjadi. Secara umum, itu bukan praktik yang baik untuk mengakhiri serangan dengan target mempertanyakan apa yang baru saja terjadi. Alih-alih, lebih baik membiarkan target merasa seolah-olah mereka melakukan sesuatu yang baik untuk orang lain yang memungkinkan interaksi di masa depan berlanjut. Ini juga di mana setiap tujuan yang longgar diatasi seperti menghapus jejak digital dan memastikan tidak ada item atau informasi yang tertinggal untuk target untuk menentukan apakah serangan telah terjadi atau identitas penyerang. Strategi keluar yang terencana dengan baik dan lancar adalah tujuan dan tindakan terakhir penyerang dalam serangan itu.