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. **Macam-macam social engineering yaitu** :

1. Baiting scams

Skema dimana perangkap sangat bergantung pada keingintahuan target atau keserakahan apapun dari mengirim suku flashdisk yang terinfeksi atau bahkan email lampiran pada target dapat digunakan kuncinya adalah pengirim harus melihat. Sah untuk target atau game dari membuka file dengan kekesalan mereka. Konsekuensinya mungkin tidak diketahui oleh target tetapi komputer mereka atau bahkan jaringan komputer perusahaan dan data dapt beresiko. Serangan hanya dengan memasukan disk, mengunjungi situs web yang membuka lampiran atau mencolokan perangkat penyimpanan dapat menyebabkan maleware ke komputer kita. Jaringan komputer yang di tautkan setelah menginstall akun email kita dan pesan mungkin dicegat, memungkinkan untuk lebih banyak maleware dikirim dari akun kita dan file perusahaan kita dapat rusak.

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.

3. 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.

4. Tailgating

Dalam penipuan tailgating seseorang dapat memperoleh akses ke area terbatas menggunakan lencana keamanan curian atau hanya dengan mengikuti orang yang memiliki akses.

5. Diversion scams

Diversion scams dapat terjadi ditempat kerja atau dirumah. Serangan dirumah lebih mungkin untuk memasukan kita ke layanan dan permintaan pencurian pembayaran, dari tempat kerja bisa beruoa pencurian perangkat lunak.

6. Quid pro quo scams

Penipuan ini melibatkan target memberikan beberapa informasi atau akses ke komputer dengan imbalan sesuatu misalnya kita saat menggunakan internet tiba-tiba terdapat virus detected padahal hanya agar korban menelpon si penipu dan membayar si penipu untuk menghapus virus dari komputernya. Pelaku akan meminta account dan password sebagai ganti dari hadiah yang diberikan.

Ada juga contoh social engineering lainnya yaitu :

1. Spear Phishing

Sama seperti metode phishing, namun yang ini specific untuk suatu orang atau organisasi tertentu saja, tujuannya untuk mendapatkan data data finansial atau rahasia perusahaan.

2. Vishing

Vishing adalah telepon yang setara dengan phising. Hal ini digambarkan sebagai tindakan menggunakan telepon dalam upaya untuk menipu pengguna agar menyerahkan informasi pribadi yang akan digunakan untuk pencurian identitas. Scammer biasanya berpura-pura menjadi bisnis yang sah, dan membodohi korban untuk berpikir bahwa dia akan mendapatkan keuntungan.

3. Scareware

Scareware melibatkan menipu korban agar berpikir bahwa komputernya terinfeksi malware atau secara tidak sengaja mengunduh konten ilegal. Penyerang kemudian menawarkan korban solusi yang akan memperbaiki masalah palsu; pada kenyataannya, korban hanya tertipu untuk mengunduh dan menginstal malware penyerang.

4. Water-holing

Serangan watering hole adalah ketika penyerang mencoba untuk berkompromi dengan sekelompok orang tertentu dengan menginfeksi situs web yang mereka kunjungi dan percayai untuk mendapatkan akses jaringan.

5. Honey trap

Sebuah serangan di mana seseorang berpura-pura menjadi orang yang menarik (baik secara fisik atau jabatan) untuk berinteraksi dengan orang secara online, memalsukan hubungan online dan mengumpulkan informasi sensitif melalui hubungan itu.

6. Software Malware Palsu

Sejenis malware yang menipu target untuk membayar penghapusan malware palsu. Sebenarnya software anti malware yang di tawarkan adalah malware yang asli.

7. PiggyBackRide

Singkatnya teknik ini menggunakan seseorang yang memiliki akses /wewenang agar kita mendapat hak akses seperti halnya orang tersebut.
Contohnya: kita berjalan dibelakang orang yang memiliki akses ke sebuah gedung,begitu orang tersebut membuka pintu dengan security key yang dimilikinya kita ngikut masuk dibelakang nya. contoh lain seperti ketika hujan lebat kita sengaja membawa banyak barang /membawa kotak di kiri dan kanan kemudian dengan sopan kita meminta tolong seseorang yang ada di sekitar yang memiliki akses untuk membukakan pintu dengan alasan security key yang kita miliki susah diambil karena ada di kantong /tas /lupa di taruh di dalam kotak .dll

8. TechieTalk

Kebanyakan hacker sangat mahir dalam hal teknis, ketika hacker akan meakukan social engineering maka si hacker dapat berbicara lancar seperti ahli soal komputer untuk mendapatkan kepercayaan dai si korban.
contohnya ketika hacker berpura-pura dari bagian helpdesk dan memberitahukan kepada korban nya bahwa sistem nya telah diretas dan si korban harus mengganti password baru ,maka si hacker akan memandu korban nya untuk mengganti password dan menanyakan password apa yang akan digunakan untuk memastikan password yang dipilih korban aman. nah loo.. secara gak langsung si hacker dapet password baru dari si korban.

9. WhallingAttack

Whalling attack menargetkan korban dengan profile tinggai atau orang-orang penting dalam bidang yang digelutinya. sebagai contoh : hacker bisa mendapat informasi penting seperti kartu kredit dan data pribadi lain nya dengan cara menggali informasi yang dipajang korban secara online. semisal,di dalam facebook page nya tertulis bahwa korban alumni universitas A dengan hobby golf, maka si hacker bisa membuat scam email yang seolah-olah resmi dikirim dari universitas A yang isinya ajakan untuk mengikuti turnamen golf antar alumni danmeminta untuk mengisi formulir yang telah disediakan sebagai syarat mengikuti turnamen tersebut. nah formulir yang disediakan adalah data pribadi yang harus diisi , dengan mengumpulkan data pribadi sepotong demi sepotong,si hacker bisa mendapat 100% data pribadi dari korban.

10. Neuro-linguisticProgramming(NLP)

Social engineer yang baik harus memiliki pemahaman yang kuat untuk memanipulasi pikiran manusia.
Neuro-linguistik pemrograman (NLP) adalah salah satu alat psikologis yang digunakan oleh para social engineer untuk memanipulasi korban dan jika dilakukan dengan benar hasilnya luar biasa.NLP berkaitan dengan bagaimana seseorang mendapat kepercayaan dengan cara berkomunikasi (verbal atau non verbal).

Sebagai contoh ketika seorang social engineer malancarkan aksinya dia akan berhati-hati dalam memilih kata-tata,mengatur intonasi nafas,nada suara dan gestur tubuhnya. hal ini akan membantu menjalin kepercayaan seseorang di level bawah sadar, korban akan hormat/mengagumi si pembicara. setelah terjalin rasa percara bisa dilanjut ke tahap selanjutnya seperti memberi senyuman hangat dan ringan,menyentuh bahu atau lengan mereka untuk memberikan rasa aman dan menggunakan kata-kata yang menunjukkan pikiran positif, gambar, dan emosi. Semua gesture, visual, dan tindakan verbal(disebut anchoring dan reframing dalam hal NLP) memberikan pesan bawah sadar yang mempengaruhi orang untuk memiliki perasaan positif dan memperoleh rasa hubungan dengan pelaku social engineering . kalau hubungan sudah terjalin dengan kuat,sugesti kuat pelaku social engineering akan bisa mengarahkan korban nya untuk melakukan hal yang menguntungkan pelaku.

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.