Wake Up Call

RSM

Mengenal Social Engineering

Saya sering mendengar istilah social engineering. Apa sebenarnya social engineering dan apakah hal tesebut punya risiko tertentu?

Kris, Jakarta

Social engineering adalah taktik penipuan dengan cara memanipulasi dan mempengaruhi orang agar melakukan sesuatu yang tidak diinginkan, bisa itu membocorkan informasi rahasia atau memberikan uang.

Social engineering bukan hipnotis atau gendam, tapi lebih kepada mendapatkan kepercayaan seseorang sehingga orang tersebut mau melakukan yang diminta.

Saya berikan contoh, misalkan anda akan mengadakan perhelatan dan mengundang pejabat tinggi negara, lalu beberapa waktu sebelum pelaksanaan acara, datang beberapa orang dari satuan pengamanan yang datang untuk mengecek keamanan gedung anda, back-up plan pada saat ada kejadian genting, anda mungkin akan mengajaknya berkeliling dan memperlihatkan secara detil proses keamanan yang ada termasuk memasukkan kode-kode keamanan tertentu untuk memberikan keyakinan bahwa gedung anda sangat aman. Hal ini umum dilakukan. Namun apa yang terjadi apabila ternyata kelompok tersebut bukan dari satuan pengamanan? Mengerikan apa yang bisa terjadi. Anda baru saja memberikan setiap detil aspek keamanan gedung anda kepada pihak yang tidak berwenang.

Contoh lain yang sering dialami di Indonesia, tiba-tiba ada telepon mengatakan anak anda bermasalah atau kecelakaan sehingga butuh dikirimkan uang segera . Pasti anda tidak langsung percaya bukan? Tapi bagaimana kalau pihak tersebut menyebutkan nama anak anda dan anggota keluarga anda lainnya dengan benar?

Kedua skenario diatas adalah contoh implementasi taktik social engineering, mereka berusaha mendapatkan kepercayaan anda, sehingga hal tersebut mempengaruhi anda untuk melakukan sesuatu yang tidak mungkin anda lakukan dalam situasi normal.

Masih banyak lagi contoh social engineering, seperti email dari teman dengan saran untuk meng-klik link website tertentu. Bisa juga dengan serangan phishing dan masih banyak lainnya.

Lalu bagaimana agar anda tidak jadi korban?

Anda harus tenang dan tidak terburu-buru menanggapi email/telepon/permintaan tertentu. Biasanya para penjahat social engineering membuat situasi dimana anda harus merespon cepat tanpa pertimbangan matang. Saran saya bersikaplah skeptis dan tidak langsung percaya begitu saja. Sebaiknya anda tetap memiliki rasa kecurigaan terhadap email-email dari pihak yang tidak anda kenal. Lakukanlah riset kecil-kecilan secara online untuk mengetahui apakah nama orang dan perusahaan yang menghubungi anda benar-benar ada.

Jangan langsung percaya pada email yang menawarkan bantuan, uang atau hadiah kepada anda. Perusahaan yang kredibel tidak melakukan hal seperti ini.

Jangan langsung meng-klik tautan dalam email dari pengirim yang tidak kredibel.

Hal-hal ini sebaiknya dimuat dalam kebijakan keamanan di kantor anda. Anda perlu mengedukasi karyawan agar paham bahaya dari social engineering.

Sementara, untuk risiko pribadi, saya sarankan anda membatasi akses jejaring sosial anda. Apabila anda tidak membatasi sebaiknya anda tidak memuat informasi yang sifatnya pribadi. Menempelkan stiker di mobil anda dengan seluruh nama anak-anak anda juga kurang bijak. Karena anda secara tidak langsung memberikan informasi pribadi, dan bisa saja ini disalahgunakan.

KEY POINTS

- Social engineering merupakan taktik penipuan melalui manipulasi.
- Tetap waspada dan tidak langsung percaya pada permintaan dari pihak yang tidak dikenal.
- Batasi pengungkapan informasi pribadi di jejaring sosial atau media publik.

Angela Simatupang
Partner
angela.simatupang@rsmindonesia.id

RSM Indonesia
Audit | Tax | Consulting

THE POWER OF BEING UNDERSTOOD