

Nama : Bima Pratama Wijaya

Nrp : 201116018

Kelas : P Ti Prof

Matkul : Keamanan informasi

1. Berikanlah penjelasan mengapa social engineering sering kali bisa digunakan attacker secara efektif untuk menyerang sebuah sistem komputer.

Jawab :

Social engineering merupakan suatu teknik yang digunakan untuk memanipulasi korban dengan cara melibatkan komunikasi yang memunculkan urgensi, ketakutan atau emosi serupa dalam diri korban. Hal ini berguna untuk mengarahkan korban membagikan informasi sensitif, mengklik tautan dan lain sebagainya dengan tujuan untuk memperoleh data dari korban, informasi bahkan uang dari korban.

Alasan mengapa social engineering seringkali digunakan attacker untuk menyerang sebuah sistem komputer adalah:

- a. Manusia merupakan faktor terlemah dari sebuah keamanan sistem
- b. Teknik sosial engineering memanfaatkan sisi psikologi manusia, dengan contoh hal ini bisa didasarkan dengan kecenderungan manusia untuk mempercayai orang lain, terlalu mempercayai orang lain, ketidak hati hati an dalam membagikan informasi atau bisa dengan mengklik tautan yang tidak dikenal
- c. Social engineering bisa dilakukan dengan secara online maupun offline, teknik social engineering bisa dilakukan secara online dengan melalui phishing email maupun pesan teks. Atau secara offline dengan cara melalui panggilan telfon, atau tindakan lainnya yang dapat memperdaya korban.

2. Berikanlah contoh untuk human-based social engineering dan computer-based social engineering.

Jawab :

- Human based social engineering
 - Pemalsuan identitas : seseorang yang menyamar sebagai karyawan dalam sebuah perusahaan
 - Pemalsuan otorisasi : seseorang yang berusaha menyakinkan korban untuk memberikan informasi dengan dalih ia telah diberikan wewenang oleh seseorang
 - Mendatangi langsung korban: seseorang yang mendatangi korban untuk langsung mendapatkan informasi dengan cara mengorek tempat sampah korban, atau melihat layar korban saat korban memasukkan password atau pin
- Computer based social engineering
 - Instant messenger attacker : seseorang yang mengirimkan sebuah file attachment dalam instant message yang sedang dilakukan
 - Pop up windows : membuat sebuah software untuk menipu user agar memasukkan username dan password dengan menggunakan pop up windows
 - Website phishing : membuat sebuah website tipuan untuk menarik user agar memasukkan alamat email dan password untuk memperoleh sesuatu

3. Apakah yang dimaksud dengan phishing dan bagaimana cara mencegah ancaman yang disebabkan phishing?

Jawab :

Phishing adalah salah satu teknik social engineering yang digunakan untuk memperoleh informasi baik username, email, password, nomor kartu kredit dan lain sebagainya dengan cara memanipulasi korban melalui pesan teks, email, atau bahkan situs website resmi.

Untuk mencegah Tindakan dari phishing adalah:

- Berhati hati saat menerima email mencurigakan: seperti jangan pernah mengklik tautan yang ada di email mencurigakan atau jangan pernah memberikan informasi rahasia melalui email
- Memeriksa url situs website: hal ini untuk memastikan url situs yang sedang dibuka merupakan situs asli dari sebuah company
- Menggunakan software anti virus yang selalu diperbarui
- Menggunakan multifactor authentication atau 2FA

er Stamp