Jurnal Ilmu dan Teknologi Teknik Multidisiplin (JMEST)
Jurnal Ilmiah Terapan: 2458-9403
Vol. 4 Edisi 6, Juni - 2017

Serangan Rekayasa Sosial

Arif KOYUN
Jurusan Teknik Komputer
Universitas Suleyman Demirel
Isparta, Turki
arifkoyun@sdu.edu.tr

Ihsan Al Janabi
Mahasiswa Pascasarjana
Universitas Suleyman Demirel
Isparta, Turki
salman.ehssan@gmail.com

***Abstrak*—Kita hidup di dunia Internet, dan saat ini kehidupan kita (baik pribadi maupun bisnis) terhubung dengan sistem TI (OS). Seringkali sistem ini terpapar risiko peretasan atau infeksi virus, sehingga kita semua mencari perangkat lunak antivirus, anti-Spyware terbaik dan menginstalnya, tetapi virus dan peretas tetap menyerang sistem kita. Serangan paling kuat pada sistem adalah Serangan Rekayasa Sosial karena serangan ini berhubungan dengan Psikologi sehingga tidak ada perangkat keras atau perangkat lunak yang dapat mencegahnya atau bahkan dapat mempertahankannya dan karenanya orang perlu dilatih untuk mempertahankannya.**

Makalah ini berisi tinjauan lengkap tentang serangan rekayasa sosial, yang terstruktur sebagai berikut: Taksonomi rekayasa sosial ditunjukkan pada bagian 2 yang dibagi menjadi Tahapan, jenis, dan pendekatan, sedangkan Bagian 3 berisi keterampilan rekayasa sosial. Pada Bagian 4, berikan saluran rekayasa sosial. Pada Bagian 5, jelaskan serangan rekayasa sosial pada aplikasi seluler. Sebelum menyimpulkan pekerjaan di Bagian 8, Mendeteksi/ Menghentikan Serangan Rekayasa Sosial dan Mencegah Serangan Rekayasa Sosial di Masa Depan ditunjukkan di bagian 6 dan 7.

Kata kunci—serangan, infiltrasi, keamanan, sosial rekayasa

1. PENDAHULUAN

Dalam kehidupan sehari-hari, kita menghabiskan sebagian besar waktu untuk melihat ke dalam atau bekerja di ponsel (komputer). Dengan demikian, kita berbagi informasi dan data dengan orang-orang yang belum tentu mengenal mereka, atau yang sudah pernah kita temui.

Saat ini beberapa jejaring sosial seperti Facebook dan Twitter menjadi sumber informasi, pertukaran data, dan layanan daring terbesar dan terpenting karena pertumbuhannya yang pesat. Jejaring sosial memberikan dukungan penuh untuk menemukan teman baru selain pertukaran data. Dengan demikian, sumber informasi baru ditambahkan ke pengetahuan kita. Jelas, sebagian besar situs jejaring sosial sangat penting dalam hal keamanan dan privasi pengguna karena banyaknya informasi yang tersedia di dalamnya, serta basis penggunanya yang sangat besar.[1]

Di dunia bisnis, Perusahaan mengharapkan karyawannya untuk bekerja dengan perangkat mereka sendiri serta sangat mobile dan fleksibel mengenai ruang kerja mereka [2] dan ada tren yang meningkat untuk mengharapkan karyawan dan pekerja pengetahuan untuk menggunakan perangkat mereka sendiri untuk bekerja, baik di kantor maupun di tempat lain. Peningkatan fleksibilitas ini dan, sebaliknya, pengurangan komunikasi tatap muka dan ruang kantor bersama berarti bahwa semakin banyak data yang perlu disediakan kepada orang lain melalui saluran daring[3].

Revolusi besar dalam komunikasi dan berbagi informasi dengan orang lain membuat sistem lebih rentan dalam hal penetrasi oleh peretas terutama melalui serangan rekayasa sosial karena rekayasa sosial itu sendiri tidak selalu memerlukan sejumlah besar pengetahuan teknis agar berhasil [4].

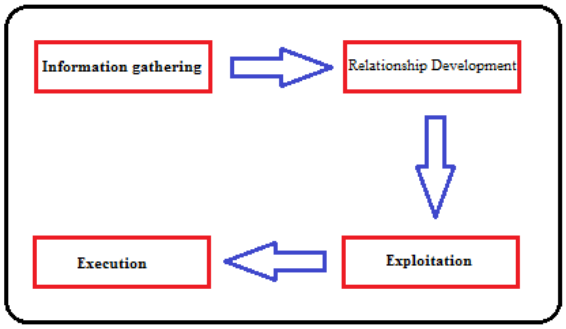
Sebaliknya, rekayasa sosial memangsa aspek-aspek umum psikologi manusia seperti rasa ingin tahu, kesopanan, mudah tertipu, keserakahan, ketidakpedulian, rasa malu dan apatis [5].

Penelitian telah menunjukkan bahwa pengguna jejaring sosial daring cenderung menunjukkan tingkat kepercayaan yang lebih tinggi terhadap permintaan pertemanan dan pesan yang dikirim oleh pengguna lain. Akibatnya, bahaya serangan rekayasa sosial terletak pada hal berikut:

1. Tingkat kepercayaan yang tinggi antara korban dan pelaku. Dan korban mungkin tidak tahu bahwa pelaku melakukan penetrasi dan pencurian.
2. Kemudahan penerapan serangan rekayasa sosial karena tidak memerlukan pengetahuan teknis yang besar agar berhasil.
3. Tidak ada perangkat keras atau perangkat lunak yang dapat mencegah serangan rekayasa sosial atau bahkan dapat mempertahankannya.
4. Sebagian besar perusahaan besar dan kantor berita menjadi korban serangan terhadap sistem informasi mereka seperti Google [6], Facebook [7], dan New York Times. [8]

2. TAKSONOMI TEKNIK SOSIAL

TAHAPAN DALAM SERANGAN REKAYASA SOSIAL**:** Meskipun semua serangan rekayasa sosial berbeda satu sama lain dan seunik itu, ada banyak teknik serangan tradisional untuk mencapai hasil serangan yang diinginkan, tetapi serangan tersebut memiliki beberapa pola umum. Pola-pola ini terdiri dari empat tahap (pengumpulan informasi, pengembangan hubungan, eksploitasi dan implementasi) [9] atau seperti yang dibagi beberapa penulis (penelitian, pengait, permainan dan keluar).[10]



Gbr. 1: *Tinjauan umum fase-fase serangan rekayasa sosial.*

Pengumpulan informasi atau Riset: Pada tahap pengumpulan informasi, penyerang mencoba melakukan riset tentang target dengan mengumpulkan informasi dari berbagai sumber dan cara, seperti penggalian sampah, situs web target, dokumen publik, interaksi fisik, dan sebagainya. Riset diperlukan saat menargetkan satu pengguna.

Pengembangan Hubungan atau Kaitan: Dalam fase ini penyerang mencoba menemukan atau membangun hubungan dengan korban dengan mencoba memulai percakapan atau cara lain untuk mengidentifikasi berbagai cara yang akan membangkitkan gairah korban.

Eksploitasi atau Permainan: Tujuan utama dari langkah ini adalah untuk memperkuat hubungan dengan melanjutkan dialog guna mendapatkan informasi yang diinginkan untuk menyelesaikan rencana dan membangun perangkat lunak atau membuat Spyware baru. Sekarang semuanya sudah siap. Langkah terakhir adalah eksekusi.

Eksekusi atau Keluar: Ini adalah fase terakhir dari serangan rekayasa sosial, di mana penyerang mengeksekusi serangan dan menghentikan komunikasi dengan target tanpa membuat apa pun membuat korban mengetahui apa yang terjadi.

JENIS REKAYASA SOSIAL: Pada dasarnya, rekayasa sosial dapat dibagi menjadi dua jenis menurut cara melakukannya, yaitu: berbasis manusia dan berbasis komputer.

Rekayasa sosial berbasis manusia: Dalam jenis serangan rekayasa sosial ini, serangan rekayasa sosial dilakukan langsung oleh seseorang. Dengan kata lain, penyerang berinteraksi langsung dengan target untuk mendapatkan informasi. Perlu dicatat bahwa dalam rekayasa sosial berbasis manusia, jumlah target terbatas karena kapasitasnya lebih rendah dibandingkan dengan serangan yang dilakukan oleh perangkat lunak.

Rekayasa sosial berbasis perangkat lunak: Rekayasa sosial berbasis perangkat lunak mengacu pada serangan yang dilakukan dengan bantuan perangkat lunak sistem (seperti komputer, ponsel) untuk mendapatkan informasi yang diinginkan. Contohnya termasuk Social Engineering Toolkit (SET), yang dapat digunakan untuk membuat email spear-phishing [11]. PENDEKATAN REKAYASA SOSIAL: Serangan rekayasa sosial memiliki banyak sisi dan para penyerang menggunakannya dalam berbagai pendekatan, yaitu:

Pendekatan fisik: Pendekatan fisik adalah suatu bentuk tindakan yang dilakukan penyerang untuk mengumpulkan informasi tentang korban. Metode yang sering digunakan adalah mencari di tempat sampah (dumpster diving). [12]. Tempat sampah bisa menjadi sumber informasi berharga bagi para penyerang.

Pendekatan sosial: Pendekatan sosial merupakan aspek terpenting dari serangan rekayasa sosial yang berhasil. Untuk meningkatkan peluang keberhasilan serangan tersebut, para penyerang sering kali mencoba membangun hubungan dengan korbannya dengan mengandalkan teknik sosio-psikologis [3] seperti metode persuasi untuk memanipulasi korbannya (misalnya, penggunaan otoritas yang diakui). Atau menggunakan vektor sosial yang paling umum yaitu rasa ingin tahu, (misalnya, digunakan dalam serangan spear-phishing dan baiting). Menurut [11], jenis serangan sosial yang paling umum dilakukan melalui telepon.

Pendekatan teknis: terutama dilakukan melalui Internet, di mana situs jejaring sosial menjadi sumber informasi yang berharga. Penyerang sering menggunakan mesin pencari untuk mengumpulkan informasi pribadi tentang korban. Ada juga alat yang dapat mengumpulkan dan menggabungkan informasi dari berbagai sumber Web seperti Maltego[1]yang menjadi salah satu alat paling populer di bidang ini. Perlu dicatat bahwa Internet sangat menarik bagi para insinyur sosial untuk mengumpulkan kata sandi, karena pengguna sering menggunakan kata sandi yang sama (sederhana) untuk akun yang berbeda.[11] Pendekatan sosio-teknis:

Serangan rekayasa sosial yang berhasil sering kali menggabungkan beberapa atau semua pendekatan yang berbeda yang dibahas di atas. Namun, pendekatan sosio-teknis telah menciptakan senjata rekayasa sosial yang paling ampuh. Salah satu contoh pendekatan teknis dan sosial adalah ketika penyerang mengeksploitasi rasa ingin tahu orang-orang dengan meninggalkan media penyimpanan yang terinfeksi malware seperti drive USB yang berisi Trojan horse [13] di lokasi yang kemungkinan besar akan ditemukan oleh korban di masa mendatang.

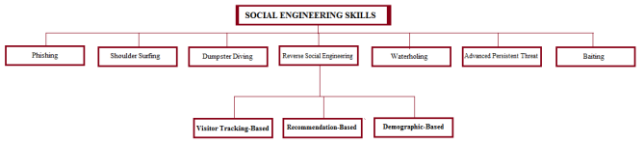
3. KETERAMPILAN TEKNIK SOSIAL:

Pada bagian ini dijelaskan secara rinci beberapa keterampilan rekayasa sosial yang paling umum digunakan yaitu:

Dumpster diving melibatkan penelitian di tempat sampah calon korban untuk menemukan informasi sensitif (seperti kata sandi, nama file, atau informasi rahasia lainnya) yang dapat digunakan untuk membahayakan sistem atau akun pengguna tertentu. Jenis keterampilan ini dapat dilakukan oleh manusia maupun perangkat lunak.

Phishing adalah upaya untuk memperoleh informasi sensitif atau membuat seseorang bertindak sesuai keinginan dengan menyamar sebagai entitas tepercaya dalam media komunikasi elektronik [3]. Phishing biasanya menargetkan sekelompok besar orang. Misalnya, mereka yang mengaku dari departemen lotere dan memberi tahu Anda bahwa Anda telah memenangkan satu juta dolar. Mereka meminta Anda untuk mengklik tautan di email untuk memberikan detail kartu kredit Anda atau memasukkan informasi seperti nama depan, alamat, usia,

dan kota. Dengan menggunakan metode ini, insinyur sosial dapat mengumpulkan nomor jaminan sosial dan informasi jaringan. Serangan phishing dapat dilakukan melalui hampir semua saluran (saluran akan ditampilkan di bagian berikutnya), Serangan yang ditujukan pada individu atau perusahaan tertentu disebut spear-phishing. Spearphishing mengharuskan penyerang untuk terlebih dahulu mengumpulkan informasi tentang korban yang dituju, tetapi tingkat keberhasilannya lebih tinggi daripada phishing konvensional. Jika serangan phishing ditujukan pada target yang memiliki profil tinggi di perusahaan, serangan tersebut disebut whaling.



Gbr. 2:*Keterampilan Rekayasa Sosial.*

Reverse Social Engineering: Jenis serangan ini merupakan teknologi independen yang sangat efektif. Penyerang tidak mencoba menghubungi korban secara langsung, tetapi membuat korban yang meneleponnya percaya bahwa penyerang adalah entitas yang dapat dipercaya. Misalnya, jika penyerang langsung menelepon pengguna dan menanyakan kata sandi mereka, hal ini dapat menimbulkan kecurigaan pada beberapa pengguna. Dalam versi reverse social engineering dari serangan yang sama, nomor telepon dapat dikirim melalui email ke target beberapa hari sebelumnya dengan memalsukan email dari administrator sistem. Email tersebut dapat menginstruksikan pengguna untuk menghubungi nomor ini jika terjadi masalah. Dalam contoh ini, setiap korban yang menghubungi nomor telepon tersebut mungkin tidak terlalu curiga dan lebih bersedia untuk berbagi informasi karena dia telah memulai kontak pertama [1].

Serangan rekayasa sosial terbalik sangat menarik bagi jaringan sosial daring karena memiliki potensi yang baik untuk menjangkau banyak pengguna terdaftar di jaringan sosial daring dan dapat melewati teknik deteksi berbasis perilaku dan filter terkini yang bertujuan untuk mencegah kontak yang tidak diinginkan secara luas. Selain itu, jika korban menghubungi penyerang, kecurigaan akan berkurang, dan ada kemungkinan yang lebih tinggi bahwa serangan rekayasa sosial akan berhasil [1].

Rekayasa sosial terbalik RSE dapat diklasifikasikan menurut serangannya menjadi empat jenis:

Gbr. 3:*Jenis Serangan Rekayasa Sosial Terbalik.*

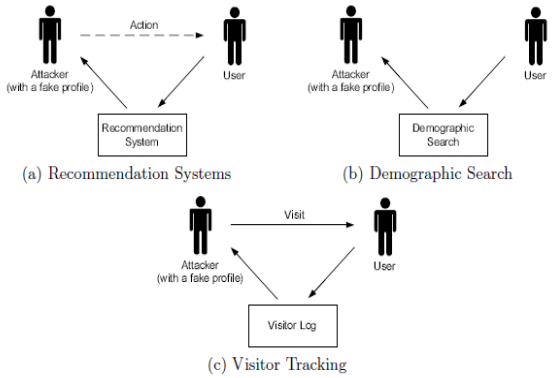
Serangan Langsung: Dalam serangan ini, tindakan penyerang dapat dilihat oleh pengguna yang menjadi target. Misalnya, penyerang dapat memposting pesan, atau menerbitkan beberapa gambar menarik di situs web.

Serangan yang Dimediasi: Serangan ini mengikuti pendekatan dua langkah di mana umpan dikumpulkan oleh agen perantara yang kemudian bertanggung jawab untuk menyebarkannya (seringkali dalam bentuk yang berbeda) ke pengguna yang menjadi target.

Serangan Terarah: Dalam serangan ini, penyerang berfokus pada pengguna tertentu. Namun, untuk melakukan serangan semacam ini, penyerang harus mengetahui beberapa informasi sebelumnya tentang target (seperti nama pengguna atau alamat email).

Serangan Tidak Tertarget: Dalam serangan tidak tertarget, penyerang hanya tertarik menjangkau sebanyak mungkin pengguna.

Serangan RSE dapat dibagi menjadi tiga kombinasi berbeda sesuai dengan konteks jaringan sosial daring.



Gbr.4:*Berbagai jenis Reverse Social Engineering*

Berdasarkan Rekomendasi RB-RSE [Ditargetkan, [Dimediasi] Sistem rekomendasi dalam jejaring sosial mengusulkan hubungan antara pengguna berdasarkan pengetahuan sekunder tentang pengguna yang berasal dari interaksi antara pengguna terdaftar dan hubungan pertemanan di antara mereka atau latar belakang dan artefak lain berdasarkan interaksi pengguna dengan jejaring sosial. Misalnya, situs jejaring sosial mungkin mencoba mengidentifikasi secara otomatis pengguna mana yang saling mengenal atau mungkin mencatat fakta bahwa pengguna telah mengunjungi profil tertentu untuk mengusulkan rekomendasi pertemanan. Sistem rekomendasi merupakan target yang menarik. Jika penyerang mampu memengaruhi sistem rekomendasi dan menjadikan jejaring sosial sebagai rekomendasi yang ditargetkan, ada kemampuan tinggi untuk mengelabui korban agar menghubungi penyerang. Gambar 4(a) menunjukkan skenario serangan RSE berbasis sistem rekomendasi.

Berbasis Demografi DB-RSE [Tidak ditargetkan, [Dimediasi] Sistem berbasis demografi dalam jejaring sosial memungkinkan terjalinnya persahabatan berdasarkan informasi dalam profil seseorang. Beberapa jejaring sosial menggunakan teknik ini sebagai norma untuk menghubungkan pengguna di lokasi geografis yang sama, dalam kelompok usia yang sama, atau mereka yang telah menyatakan preferensi serupa. Gambar 4(b) menunjukkan serangan RSE yang menggunakan informasi demografi. Dalam serangan tersebut, penyerang cukup membuat profil (atau sejumlah profil) yang memiliki kemungkinan besar menarik bagi pengguna tertentu, lalu menunggu korban untuk memulai kontak.

Pelacakan Pengunjung Berbasis VTB-RSE [Target, Langsung] Pelacakan pengunjung adalah fitur yang disediakan oleh beberapa media sosial

jaringan untuk memungkinkan pengguna melacak siapa saja yang telah mengunjungi profil daring mereka. Serangan dalam kasus ini melibatkan eksploitasi rasa ingin tahu pengguna dengan mengunjungi halaman profil mereka. Pemberitahuan bahwa halaman tersebut telah dikunjungi dapat meningkatkan minat, memancing pengguna untuk melihat profil penyerang dan mungkin mengambil tindakan [1]. Gambar 4(c) menguraikan metode serangan ini.

Tabel 1: Klasifikasi Rekayasa Sosial Terbalik serangan berdasarkan konteks media sosial online jaringan.

RSE	RB-RSE	DB-RSE	VTB-RSE
Langsung			-
Dimediasi	-	-	
Ditargetkan	-		-
Tidak ditargetkan		-	

Shoulder surfing mengacu pada penggunaan teknik observasi langsung untuk mendapatkan informasi, seperti melihat layar atau keyboard seseorang dari balik bahunya [3]. Baiting it adalah serangan berskala luas yang dilakukan melalui penggunaan iklan daring dan situs web. Ini termasuk beberapa situs web yang memungkinkan pengguna mengunduh, atau pop-up yang mengaku telah mendeteksi masalah pada sistem korban yang dapat diselesaikan dengan mengeklik pop-up tersebut. Dengan mengikuti tautan yang disediakan dalam bait, komputer pengguna dapat mengunduh malware secara otomatis.

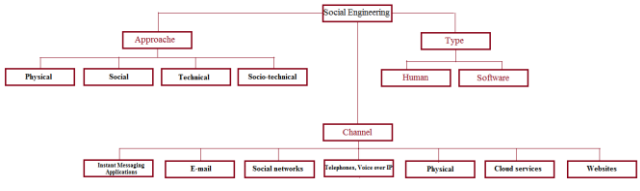
Serangan watering hole biasanya lebih canggih daripada kebanyakan teknik rekayasa sosial lainnya karena memerlukan pengetahuan teknis. Mirip dengan baiting, gunakan situs web tepercaya untuk menginfeksi komputer korban, tempat penyerang membahayakan situs web dan menunggu korban.

Ancaman Berkelanjutan Tingkat Lanjut mengacu pada serangan mata-mata jangka panjang, sebagian besar berbasis Internet yang dilakukan oleh penyerang yang memiliki kemampuan dan niat untuk merusak sistem secara terus-menerus[3].

SALURAN REKAYASA SOSIAL:

Serangan dapat dilakukan melalui saluran berikut:

Aplikasi Pesan Instan (IMA) merupakan saluran yang paling umum untuk serangan phishing dan rekayasa sosial terbalik, dan juga dapat digunakan dengan mudah untuk pencurian identitas guna mengeksploitasi hubungan yang dapat dipercaya. Email semakin populer di kalangan rekayasa sosial sebagai alat untuk serangan phishing dan rekayasa sosial terbalik.



Gbr. 5:*Klasifikasi rekayasa sosial dan serangan saluran.*

Jejaring sosial menawarkan berbagai peluang untuk serangan rekayasa sosial karena kemampuannya menciptakan identitas palsu dan memudahkan penyerang menyembunyikan identitas mereka dan mengumpulkan informasi sensitif.

Fisik seperti yang ditunjukkan beberapa bentuk tindakan yang dilakukan penyerang untuk mengumpulkan informasi tentang korban menggunakan metode (dumpster diving). Layanan cloud dapat digunakan oleh penyerang untuk menempatkan file atau perangkat lunak dalam direktori bersama untuk membuat korban menyerahkan informasi. Telepon, Voice over IP adalah saluran serangan untuk membuat korban menyampaikan informasi sensitif bagi penyerang. Situs web paling sering digunakan untuk melakukan serangan watering hole dan baiting. Lebih jauh lagi, dapat digunakan dengan email untuk melakukan serangan phishing. Tabel 2 menguraikan hubungan antara jenis rekayasa sosial, pendekatan, saluran, dan keterampilan serangan. Perhatikan bahwa banyak jenis serangan rekayasa sosial secara eksklusif bergantung pada saluran serangan fisik, seperti dumpster diving, phishing, Reverse social engineering, shoulder surfing, baiting. Untuk melindungi terhadap kelas serangan ini, keamanan fisik perlu ditingkatkan.

Tabel 2: Klasifikasi serangan rekayasa sosial sesuai dengan taksonomi kita

		Menyelam di Tempat Pembuangan Sampah	Penipuan	Rekayasa Sosial Terbalik	Berselancar di Bahu	Umpan	Tempat minum	Ancaman Persisten Tingkat Lanjut
Jenis	Manusia	-	-	-	-	-		
	Perangkat lunak	-	-	-			-	-
Mendekati	Fisik	-			-	-		
	Teknis						-	-
	Sosial			-				
	Sosial-teknis		-	-		-	-	-
Saluran	saya		-	-				
	E-mail		-	-				-
	Sosial Jaringan		-	-				
	Fisik	-	-	-				
	Awan layanan		-					
	Telepon, Bahasa Indonesia: VoIP		-	-				
	Situs web		-				-	-

SERANGAN REKAYASA SOSIAL PADA APLIKASI MOILE:

Peningkatan penggunaan aplikasi seluler dalam bisnis dan konteks pribadi membuat aplikasi seluler menjadi saluran yang semakin populer untuk serangan rekayasa sosial di mana aplikasi perpesanan dan e-mail seluler sangat diminati oleh para insinyur sosial.

Karyawan perusahaan cenderung menggunakan perangkat pribadi mereka, yaitu komputer, ponsel, dan tablet atau semuanya. Dan ini sudah menjadi kebijakan yang ditetapkan oleh perusahaan sejak lama. Oleh karena itu, semakin banyak karyawan yang menggunakan ponsel pintar mereka untuk melakukan pekerjaan mereka atau untuk memeriksa email perusahaan atau untuk berbagi dokumen dengan cloud. Namun, banyak aplikasi ponsel pintar (seperti WhatsApp [14]) dapat disalahgunakan untuk melakukan serangan rekayasa sosial.

Mengingat banyaknya aplikasi telepon pintar yang sangat rentan dan dapat membocorkan informasi sensitif, kita dapat menyimpulkan bahwa perangkat seluler tersebut menawarkan berbagai vektor serangan untuk rekayasa sosial dan serangan lain terhadap privasi pengguna. Selain itu, saat kita menyiapkan beberapa aplikasi telepon pintar, aplikasi tersebut meminta izin untuk mengakses data sensitif pada perangkat. Jika penyerang membuat aplikasi semacam itu, mereka akan memperoleh informasi dan dapat menggunakannya sebagai titik awal untuk serangan rekayasa sosial.

Salah satu penulis [15] menunjukkan dua skenario serangan yang berbeda yang dapat menjadi titik awal untuk serangan aplikasi seluler. Dan yang lainnya [16] membahas bagaimana pertukaran informasi antar-aplikasi dapat diendus pada telepon pintar dan kemudian disalahgunakan untuk melanggar kebijakan dan izin aplikasi. Sementara dalam beberapa kasus, penyerang hanya menjiplak aplikasi telepon pintar yang populer dan menyebarkannya untuk melakukan serangan. [17]

MENDETEKSI / MENGHENTIKAN SERANGAN REKAYASA SOSIAL:

Seperti yang telah kami nyatakan sebelumnya, tidak ada cara yang spesifik dan jelas untuk melakukan serangan rekayasa sosial, tetapi dapat dikatakan bahwa menggunakan akal sehat adalah cara paling sederhana untuk bertahan melawannya. Jika sesuatu tampak mencurigakan, itu mungkin merupakan sebuah serangan. Berikut ini beberapa indikator umum serangan rekayasa sosial: [18]

-Seseorang menciptakan rasa urgensi yang luar biasa untuk membuat Anda mengambil keputusan yang sangat cepat, bersikaplah curiga.

-Seseorang yang meminta informasi yang seharusnya tidak dapat mereka akses atau seharusnya sudah mereka ketahui.

-Sesuatu yang terlalu bagus untuk menjadi kenyataan. Seperti jika Anda diberitahu bahwa Anda memenangkan lotre, meskipun Anda tidak pernah mengikutinya. Pada dasarnya, untuk menghentikan serangan Social Engineering ada beberapa langkah yang harus dilakukan dengan hati-hati:

-Jika Anda curiga ada yang mencoba menjadikan Anda korban serangan rekayasa sosial, jangan berkomunikasi lagi dengannya.

-Jika yang menelepon adalah seseorang yang tidak Anda kenal, tutup teleponnya.

-Jika orang yang mengobrol dengan Anda secara daring adalah orang yang tidak Anda kenal, akhiri koneksi.

-Jika itu adalah email yang tidak Anda percaya, hapus saja.

-Jika serangan tersebut terkait dengan pekerjaan, pastikan untuk segera melaporkannya ke meja bantuan atau tim keamanan informasi Anda.

MENCEGAH SERANGAN REKAYASA SOSIAL DI MASA DEPAN:

Ada beberapa tindakan pencegahan yang dapat Anda lakukan untuk membantu mencegah diri Anda terpapar pada serangan rekayasa sosial di masa mendatang: Buat kata sandi yang kuat untuk akun Anda dan jangan pernah membagikannya. Tidak ada organisasi yang akan menghubungi Anda dan meminta kata sandi Anda. Jika seseorang melakukan itu, itu adalah serangan.

Jangan Berbagi Terlalu Banyak. Segala sesuatu yang Anda bagikan dengan orang lain meningkatkan kemungkinan terpapar serangan dan membuat penyerang dapat mengetahui lebih banyak tentang Anda. Bahkan berbagi detail kecil tentang diri Anda dari waktu ke waktu dapat disatukan untuk menciptakan gambaran lengkap tentang Anda. Dengan demikian, penyerang dapat dengan mudah menemukan dan menyesatkan Anda agar melakukan apa yang mereka inginkan dari Anda.

Verifikasi Kontak. Terkadang, Anda mungkin ditelepon oleh beberapa organisasi untuk alasan yang sah seperti bank, Perusahaan Kartu Kredit, penyedia layanan seluler, atau lainnya untuk mendapatkan informasi atau masalah. Jika Anda ragu tentang panggilan tersebut, apakah permintaan informasi itu sah, jangan berikan informasi yang sensitif dan sarankan untuk menghubungi organisasi tersebut serta menanyakan nama dan nomor ekstensi orang tersebut. Meskipun cara ini tampak merepotkan, melindungi identitas dan informasi pribadi Anda sepadan dengan langkah tambahan tersebut.

4. KESIMPULAN:

Dalam makalah ini, kami menguraikan tinjauan lengkap untuk serangan rekayasa sosial. Dan untuk memfasilitasinya, kami memperkenalkan taksonomi serangan yang komprehensif, mengklasifikasikannya berdasarkan fase serangan dan berbagai jenis serangan rekayasa sosial dan menunjukkan bahwa penyerang melakukan serangan rekayasa sosial melalui berbagai saluran yang berbeda. Serangan tersebut sebagian besar dilakukan oleh manusia serta perangkat lunak dan selanjutnya dengan pendekatan yang berbeda seperti fisik, teknis, sosial atau sosio-teknis. Batasan masing-masing jenis serangan sangat dapat diperluas dan, dalam banyak kasus, belum sepenuhnya dipahami secara teknis serta pemahaman terperinci tentang keterampilan rekayasa sosial dan serangan rekayasa sosial pada aplikasi Seluler.

Kami juga menyoroti bahwa mayoritas serangan rekayasa sosial saat ini bergantung pada kombinasi metode sosial dan teknis. Oleh karena itu, untuk mendeteksi, menghentikan, dan melindungi secara efektif terhadap serangan sosioteknis, kesadaran pengguna terhadap serangan rekayasa sosial perlu ditingkatkan dan perangkat mereka perlu dilindungi pada tingkat teknis.

5. REFERENSI:

[1] D. Irani, M. Balduzzi, D. Balzarotti, E. Kirda, dan C. Pu. Serangan rekayasa sosial terbalik di jaringan sosial daring. Deteksi Intrusi dan Malware, dan Penilaian Kerentanan, 2011.

[2] R. Ballagas, M. Rohs, JG Sheridan, dan J. Borchers. Byod: Bawa perangkat Anda sendiri. Dalam 'Prosiding Lokakarya tentang Lingkungan Tampilan di Mana Saja', Ubicomp, 2004.

[3] K. Krombholz, H. Hobel, M. Huber, dan E. Weippl. Serangan Rekayasa Sosial Tingkat Lanjut. Penelitian SBA, Favoritenstrabe 16, AT-1040 Vienna, Austria, 2014.

[4] PUBLIKASI CERT-UK Pengantar rekayasa sosial www.cert.gov.uk, 2015.

[5]Bagaimana para hacker mengeksploitasi 'tujuh dosa mematikan', *Berita BBC*http://www.bbc.co.uk/news/technology-20717773.

[6] Serangan peretasan Google sangat canggih tersedia on line: http://www.wired.com/threatlevel/2010/01/operationaurora/, terakhir diakses pada 17-07-2013.

[7] Microsoft diretas: Bergabung dengan Apple, Facebook, twitter - InformationWeek. tersedia daring: http://www.informationweek.com/security/\Attackacks/microsoft-hacked-joins-apple-facebook-tw/240149323, terakhir diakses pada 2013-07-10.

[8] N. Perlroth. Peretas Tiongkok menyusup ke New York Times computers, Januari 2013. tersedia di https://www.nytimes.com/2013/01/31/technology/chin ese-hackers-infiltrate-new-york-times-computers.html, terakhir diakses pada: 2013-07-01.

[9] M. Hasan, N. Prajapati, S. Vohara, ''Studi Kasus tentang Teknik Rekayasa Sosial untuk Persuasi'' Jurnal internasional tentang aplikasi teori grafik dalam jaringan ad hoc nirkabel dan jaringan sensor (GRAPH-HOC) Vol.2, No.2, Juni 2010.

[10] Patel, Rahul Singh, "KALI LINUX SOCAIL ENDINEERING", Inggris, 2013.

[11] TrustedSec. Perangkat rekayasa sosial, 2013. Tersedia on line pada: https://www.trustedsec.com/downloads/socialengineer-toolkit/, terakhir diakses 03/12/2013.

[12] S. Granger. Dasar-dasar Rekayasa Sosial, Bagian I: Taktik Peretas. Fokus Keamanan, 2001.

[13] S. Stasiukonis. Rekayasa Sosial, USB Cara.2006.tersediadi http://www.darkreading.com/security/perimeter/showArticle.jhtml?articleID=208803634, terakhir diakses pada: 02-07-2013.

[14] WhatsApp. tersedia on line: http://www.whatsapp.com/, terakhir diakses pada 2013-07-18.

[15] S. Schrittwieser, P. Fruehwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, dan E. Weippl. Tebak Siapa yang Mengirimi Anda Pesan Singkat? Mengevaluasi Keamanan Aplikasi Perpesanan di Ponsel Pintar. Dalam Simposium Keamanan Jaringan dan Sistem Terdistribusi (NDSS 2012), 2 2012.

[16] E. Chin, AP Felt, K. Greenwood, dan D. Wagner. Menganalisis komunikasi antar-aplikasi di android. Dalam Prosiding konferensi internasional ke-9 tentang sistem, aplikasi, dan layanan seluler, MobiSys '11, halaman 239-252, New York, NY, AS, 2011. ACM.

[17] R. Potharaju, A. Newell, C. Nita-Rotaru, dan X. Zhang. Menjiplak aplikasi telepon pintar: strategi serangan dan teknik pertahanan. Dalam Prosiding konferensi internasional ke-4 tentang Rekayasa Perangkat Lunak dan Sistem yang Aman, ESSoS'12, halaman 106-120, Berlin, Heidelberg, 2012. Springer-Verlag.