MENG-HACK ORANG
Psikologi Social Engineering

Betha Aris S <betha@obscure.org>

Judul Asli:
People Hacking: The Psychology of Social Engineering
Text of Harl's Talk at Access All Areas III 05/07/97

Diterjemahkan Oleh:
Betha Aris S <betha@obscure.org>

Apakah social engineering itu?

Secara mendasar, *social engineering* adalah seni dan ilmu memaksa orang untuk mematuhi harapan-harapan anda. Ia bukanlah suatu cara untuk mengendalikan pikiran orang lain, ia tidak akan mengijinkan anda untuk memaksa orang lain menunjukkan tugas-tugas secara liar di luar tingkah laku normal mereka dan ini jauh dari hal-hal bodoh semacam itu. Ia(Social engineering) juga melibatkan lebih dari sekedar berpikir cepat dan sederhana dan suatu jenis aksen yang menyenangkan. Social engineering bisa melibatkan banyak 'kerja-kerja yang membumi,' pengumpulan informasi dan *idle chi chat* sebelum adanya usaha untuk mendapatkan informasi yang pernah dibuat. Seperti *hacking*, sebagian besar kerjanya masih dalam batas interpretasi, lebih dari sekedar usaha itu sendiri.

Anda mungkin berpikir pembicaraan ini mungkin kelihatan menjadi suatu perminttaan maaf yang lemah untuk menunjukkan bagaimana teknik-teknik ini bisa digunakan untuk *hacking*. OK, cukup terbuka. Namun, satu-

satunya cara untuk mempertahankan diri dari bentuk serangan keamanan ini adalah dengan mengetahui metode apa yang mungkin digunakan. Dengan pengetahuan ini sangatlah mungkin untuk memanfaatkan teknik-teknik yang digunakan baik terhadap diri anda maupun perusahaan anda dan melindungi penerobosan keamanan illegal sebelum orang-orang lain mendapatkan data yang anda simpan. Suatu gaya CERT tentang kewaspadaan keamanan komputer dengan sedikit perincian kurang berarti dalam kasus ini. Ia hanya akan mendinginkan beberapa orang yang mungkin berusaha mendapatkan akses pada sistem anda dengan berpura-pura beberapa hal adalah benar. Jangan biarkan mereka. Seperti biasanya, tak ada bantuan apapun.

Lalu?

Social engineering berkonsentrasi pada link paling lemah dari alur keamanan komputer. Seringkali dikatakan bahwa hanya komputer yang paling aman adalah komputer yang *unplugged*. Fakta bahwa anda dapat meyakinkan seseorang untuk masuk ke dalamnya dan menghidupkannya berarti bahwa komputer yang kekuatannya menurunpun sangat rentan.

Juga, bagian yang manusiawi dari suatu penyetelan keamanan adalah hal yang paling esensial. Ini berarti bahwa kelemahan keamanan ini bersifat universal, independen dari platform, perangkat lunak, jaringan atau usia perlengkapan.

Setiap orang dengan akses pada setiap bagian sistem, secara fisikal maupun elektronik menjadi suatu resiko keamanan potensial. Informasi apapun yang bisa diperoleh mungkin digunakan untuk informasi lebih jauh tentang social engineering. Hal ini berarti bahkan orang-orang yang tiidak dipertimbangkan sebagai bagian kebijakan bisa digunakan untuk menyebabkan suatu terobosan keamanan.

Sebuah masalah besar?

Para profesional keamanan secara terus menerus diberitahu bahwa keamanan melalui ketidakjelasan adalah keamanan yang paling lemah. Tidaklah mungkin mengaburkan fakta bahwa manusia menggunakan sistem atau bahwa mereka bisa mempengaruhinya, karena sebagaimana yang saya katakan sebelumnya, tidak ada satu sistem komputerpun di muka bumi ini yang tidak melibatkan manusia sebagai salah satu bagiannya.

Hampir setiap manusia memiliki perangkat kerja untuk mengatasi 'serangan' social engineering, satu-satunya perbedaan adalah dalam hal jumlah skill yang digunakan ketika menggunakan perangkat kerja ini.

Metode-metode

Berusaha mengendalikan seorang individu guna melengkapi tugasnya bisa menggunakan beberapa metode. Metode yang pertama dan yang paling jelas adalah suatu permintaan langsung yang sederhana, dimana seorang individu diminta untuk melengkapi tugasnya secara langsung. Walaupun sedikit kemungkinan berhasilnya, ini merupakan metode yang paling mudah dan paling langsung. Secara pasti individu tahu apa yang dinginkan oleh anda dari mereka.

Yang kedua adalah dengan menciptakan suatu siituasi yang telah dirancang dimana secara sederhana individu menjadi bagian dari situasi tersebut. Dengan kelebihan faktor dari yang anda minta pertimbangkan untuk diperhatikan, individu jauh lebih mungkin untuk diyakinkan, karena anda bisa menciptakan alasan-alasan untuk kepatuhan mereka daripada alasan-alasan personal lainnya, dan hampir pasti melibatkan pengetahuan ekstensif yang diperoleh dari target yang diinginkan. Yang sedikit belum tentu lebih baik.

Salah satu perangkat kerja esensial yang digunakan untuk social engineering adalah suatu daya ingat yang baik bagi fakta-fakta yang

dikumpulkan. Ini adalah sesuatu yang cenderung dilebih-lebihkan oleh para *hacker* dan *sysadmin*, khususnya ketika sampai pada fakta yang berkaitan dengan bidang mereka. Untuk menggambarkan hal ini saya akan menunjukkan sebuah demonstrasi kecil.....

[Demonstrasinya di sini. Secara mendasar, hal ini menunjukkan bahwa dengan tekanan-tekanan sosial seorang individu akan menyesuaikan diri pada suatu keputusan kelompok, bahkan sekalipun ia tahu kalau hal itu jelas-jelas pilihan yang salah.]

Konformitas

Bahkan dalam kasus-kasus dimana seseorang yakin mereka benar sangat mungkin mereka bertindak dalam cara-cara yang berbeda. Jika saya sekedar bertanya orang terakhir tentang tindakan mereka sendiri apakah kata pertengahan yang akan mereka berikan pada saya jawaban yang benar dan tak jadi soal berapa kali saya berusaha meyakinkan mereka mereka mungkin tidak akan merubah pendirian mereka.

Namun, setting kelompok ini merupakan suatu situasi yang benar-benar berbeda. Situasi ini memiliki apa yang oleh para ahli psikologi dinamakan karakteristik tuntutan, yaitu situasi ini memiliki suatu ketegangan-ketegangan sosial yang kuat tentang bagaimana partisipan seharusnya bertindak. Tidak berharap untuk menyerang orang lain, tidak ingin kelihatan *dozy* di hadapan sejumlah besar audiens dan tidak merongrong pandangan-pandangan orang lain semua partisipan yang baik mengarah pada suatu keputusan untuk ikut arus. Menggunakan situasi-situasi dengan karakteristik ini adalah suatu cara paling efektif untuk mengarahkan tingkah laku orang.

Situasi

Namun, sebagian besar social engineering dilakukan oleh individu – individu penyendiri dan begitu juga tekanan sosial dan faktor-faktor berpengaruh lainnya harus dipertimbangkan dengan menciptakan suatu situasi yang bisa dipercayai dimana target merasa terlibat.

Jika situasinya, riil atau imajiner memiliki karakteristik-karakteristik tertentu maka target individualnya lebih mungkin mematuhi permintaan anda. Karakteristik ini termasuk:

-Pembagian tanggungjawab dari individu-individu target. Hal ini ketika individu mempercayai bahwa mereka tidak bertanggungjawab sendiri atas tindakan-tindakan mereka.

-Sebuah kesempatan untuk menjilat. Kepatuhan lebih mungkin jika individu percaya bahwa dengan memtahui mereka menjilat pada seseorang yang mungkin memeberikan mereka manfaat-manfaat masa depan. Secara mendasar hal ini berarti patuh dengan bosnya.

Kewajiban moral. Ini adalah alasan dimana seorang individu patuh karena mereka merasa ini adalah kewajiban moral mereka. Bagian dari hal ini adalah rasa bersalah. Orang memilih menghindari perasaan beralah dan sehingga jika terdapat suatu kesempatan dimana mereka akan merasa kesalahan yang akan mereka lakukan jika menghindari outcome ini.

Persuasi personal

Pada suatu level personal terdapat metode-metode yang digunakan untuk memaksa seseorang lebih mungkin bekerjsama dengan anda. Tujuan persuasi personal adalah tidak memaksa orang untuk melengkapi tugas-tugas anda, namun mendorong kepatuhan sukarela mereka dengan permintaan anda.

Terdapat perbedaan halus. Secara mendasar, targetnya secara mudahnya diarahkan pada jalan-jalan yang kita inginkan. Sasaran percaya bahwa mereka memiliki kontrol atas situasi, dan bahwa mereka mendayagunakan kekuatan mereka untuk membantu anda.

Fakta bahwa manfaat yang akan diperoleh seseorang dari membantu anda telah telah terbukti tidak relevan. Sasaran kita percaya mereka membuat suatu keputusan yang beralasan untuk mempertukarkan manfaat-manfaat ini dengan sedikit energi dan waktu yang hilang.

Kerjasama

Terdapat beberapa faktor, yang jika ada akan meningkatkan kesempatan suatu sasaran beroperasi dengan seorang social engineer.

Mengurangi konflik dengan sasaran adalah lebih baik. Kerjasama akan dengan lebih siiap diperoleh ketika pendekatan lembut digunakan. Pulling rank(atau ranking yang diinginkan), kebosanan atau aturan-aturan jarang bekerja bagi pemaksaan efektif.

Faktor 'kaki di dalam pintu' adalah dimana fokus sebuah persuasi berusaha sudah tahu siapa anda atau telah memiliki pengalaman berhubungan dengan anda. Ini merupakan suatu cara khusus yang efektif dan telah diketahui oleh *con men* sebagai trik-trik percaya diri. Penelitian psikologis memperlihatkan bahwa orang-orang lebih mungkin mematuhi kita dengan suatu permintaan jika mereka sebelumnya telah dipatuhi pada sesuatu yang jauh lebih kecil. Jika 'kaki di dalam pintu' ini termasuk sejarah kerjasama, dimana hal-hal telah berlalu dengan baik-baik saja di masa lalu, maka kesempatan kerjasama akan meningkat.

Informasi yang lebih sensoris suatu target yang diperoleh seorang social engineer akan lebih baik. Ini secara khusus kedengaran dan kelihatan benar, anda lebih mungkin dipercayai jika sasaran bisa melihat dan mendengar anda daripada jika mereka hanya mendengar suara anda dari

seberang telepon. Secara tak mengejutkan komunikasi teks ASCII tidak begitu memberikan manfaat bagi persuasi. Sangatlah mudah untuk menolak seseorang lewat gaya obrolan di IRC.

Keterlibatan

Namun, suskses tidak bergantung terlalu banyak pada bagaimana seseorang yang terlibat sedang menjalankan apa yang anda minta. Kita dapat katakan administrator sistem, pejabat keamanan komputer, teknisi dan orang-orang yang menggantungkan diri ppada sistem untuk perangkat kerja-kerja atau komunikasi esensial sangat terlibat dalam serangan-serangan social engineering oleh para hacker.

Orang-orang yang sangat terlibat lebih baik diiyakinkan dengan suatu argumen yang kuat. Dalam kenyataannya, semakin lebih kuat argumen yang anda berikan pada mereka akan lebih baik. Yang mengejutkan, tidaklah sama untuk kasus argumen-argumen lemah. Seseorang yang sangat terlibat dalam suatu usaha persuasi kurang mungkin diyakinkan jika anda memberikan mereka argumen lemah. Ketika seseorang mungkin diarahkan secara langsung dengan suatu usaha social engineering, argumen lemah cenderung menghasilkan counter argumen dalam kepala sasaran kita. Maaka untuk orang-orang yang sangat terlibat, aturannya adalah semakin kuat argumen, argumen yang lemah akan berkurang.

Orang-orang digolongkan sedikit terlibat jika mereka memiliki sedikit kepentingan dalam apa yang anda minta pada mereka untuk dilakukan. Contoh-contoh relevan bisa jadi penjaga keamanan, tukang bersih-bersih, atau resepsionis di tempat sistem komputer. Karena orang-orang yang sedikit terlibat tidak mungkin dipengaruhi secara langsung dengan suatu permintaan, mereka cenderung tidak mengganggu penganalisaan pro-kontra lelucon persuasif. Walaupun sifatnya umum bagi sebuah keputusan untuk setuju dengan permintaanmu atau tidak dipaksa berdasarkan informasi lain.

Informasi semacam itu bisa jadi sejumlah alasan yang diberikan oleh *social engineer* belaka, urgensi permintaan yang lebih jelas atau status orang yang berusaha meyakinkan. Aturan intinya di sini adalah semata-mata semakin lebih baik argumen akan semakin baik. Secara mendasar, orang-orang yang tidak dilibatkan dalam apa yang berusaha didapatkan oleh social engineer akan lebih diyakinkan dengan banyaknya argumen atau permohonan dariada berapapun relevannya mereka.

Salah satu poin penting yang patut dicatat adalah bahwa orang yang kurang kompeten lebih mungkin mengikuti model yang lebih kompeten. Dalam kasus sistem komputer ini mungkin bisa dimasukkan dalam golongan orang yang sedikit terlibat. Inti moral point ini adalah, jangan berusaha meyakinkan administrator sistem social engineer, kecuali mereka kurang kompeten dibandingkan anda, dan yang seperti kita semua ketahui, itu tidak mungkin.

Mengamankan dari serangan-serangan manusia

Dengan semua informasi ini bagaimana seseorang akan menciptakan sistem komputer mereka lebih aman? Langkah pertama yang baik adalah menciptakan bagian keamanan komputer dari pekerjaan setiap orang apakah mereka menggunakan komputer atau tidak. Hal ini tidak hanya akan mendorong status yang dibayangkan mereka sendiri dengan tiadanya biaya ekstra bagi anda namun akan memaksa staf menjadi lebih waspada.

Namun pertahaan terbaik terhadap hal ini, sebagaimana berbagai hal lainnya, adalah pendidikan. Menjelaskan pada para pekerja tentang arti pentingnya sistem keamanan komputer dan bahwa ada orang yang dipersiapkan untuk berusaha dan memanipulasi mereka guna mendapatkan akses adalah sebuah tahap pertama yang efektif dan bijaksana. Memperingatkan orang tentang kemungkinan-kemungkinan serangan seringkali cukup membuat mereka waspada. Ingat, kisahkan dua sisi cerita

ketika mendidik orang lain tentang keamanan komputer. Ini tidak hanya bias personal saya. Ketika individu tahu dua sisi dari satu argumen mereka kurang mungkin untuk dibohongi dari posisi-posisi pilihan mereka. Dan jika mereka terlibat dalam sistem keamanan komputer, posisi pilihan mereka mungkin berada pada sisi mengamankan data anda.

Terdapat atribut-atribut dimana orang mungkin cenderung kurang mematuhi persuasi yang kita berikan. Orang-orang yang kurang patuh cenderung sangat cerdas, sangat orisinal, mampu mengatasi ketegangan dan memiliki kepercayaan diri yang cukup beralasan. Manajemen ketegangan dan kepercayaan diri bisa diajarkan atau didorong. Bentuk-bentuk penegasan diri seringkali digunakan untuk pekerja manajemen, latihan ini sangat berguna dalam mengurangi kesempatan seorang individu yang secara sosial ahli, seperti halnya memiliki banyak manfaat lainnya.

Apa yang sebenarnya ingin kita sampaikan adalah membuat orang sadar dan terlibat dalam kebijakan keamanan anda. Ini memerlukan sedikit usaha dan memberikan balasan yang besar dalam pengertian jumlah resiko reduksi.

Kesimpulan

Berlawanan dengan kepercayaan populer, seringkali lebih mudah menghack orang daripada mengirimkan email. Namun ia kurang memiliki usaha guna mendapatkan pekerja yang bisa melindungi dan mendeteksi usaha-usaha pada social engineering daripada mengamankan sistem *unix* apapun.

Para administrator sistem, jangan biarkan orang yang me-*link* jalur keamanan anda membuat kerja keras anda terbuang sia-sia. Dan para hacker, jangan biarkan para administrator sistem berleha-leha dengan link-link yang lemah, karena jalur-jalur merekalah yang menyimpan data anda.