PEDULI DATA DENGAN KEAMANAN PASSWORD

PT Bank Central Asia Tbk atau BCA mengakui, ada 200 nasabahnya yang mengalami masalah pengurangan saldo akibat transaksi mencurigakan. Total kerugian yang diderita akibat kasus ini mencapai Rp 5 miliar. Kompas (21/1/2010).

Sebagai manusia yang hidup di era teknologi informasi, penggunaan password tentunya sudah menjadi bagian dari aktifvtas keseharian. Password atau kata sandi banyak digunakan untuk melakukan suatu proses yang dikenal dengan istilah otentikasi, yaitu sebuah proses untuk memastikan bahwa seseorang yang akan melakukan akses masuk adalah benar-benar orang yang memang sudah terdaftar dalam daftar valid user dari sistem yang bersangkutan.

Penggunaan password dapat membatasi siapa saja yang boleh memasuki suatu sistem dan mengakses resource tertentu. Oleh karenanya, password memiliki peranan yang sangat vital dalam segi keamanan dari suatu sistem. Sayangnya masih ada beberapa orang (dan jumlahnya lumayan banyak) yang masih belum menyadari hal ini dan cenderung menyepelekan aspek kekuatan dari password itu sendiri.

Ada juga orang-orang yang mulai menyadari peranan penting dari password, tetapi belum mengetahui bagaimana memilih password yang baik. Tulisan ini mencoba membantu Anda dalam meningkatkan kekuatan dari password yang Anda gunakan.

Panduan Sederhana dalam Memilih Password

Berikut adalah beberapa tips sederhana yang dapat membantu Anda dalam memilih password yang memiliki tingkat kekuatan yang baik:

1. Pilihlah password yang mudah Anda ingat tetapi cukup sulit untuk ditebak oleh orang lain. Anda bisa memilih kata ataupun frasa yang sifatnya pribadi dan hanya diketahui diri Anda. Dengan demikian Anda akan mudah untuk mengingat password tersebut. Akan sangat konyol rasanya bila Anda membuat password yang sulit ditebak oleh orang lain tetapi Anda sendiri tidak bisa mengingatnya.

   Jangan sepelekan tips ini karena kejadian ini seringkali ditemui di hampir sebagian besar instansi di mana terdapat user yang lupa password yang digunakannya. Tips ini juga dapat membantu Anda dalam mengingat sejumlah password dari beberapa account yang Anda miliki.

2. Pilihlah password dengan jumlah karakter yang cukup panjang. Makin banyak jumlah karakter yang Anda gunakan, makin tinggi tingkat kekuatan dari password Anda. Beberapa profesional di bidang IT Security menyarankan untuk memilih password dengan minimal 8 karakter.
3. Pilihlah password yang mengandung perpaduan antara huruf besar, huruf kecil, angka, dan karakter spesial seperti tanda baca. Semisal Anda memilih frasa “cintasejati” sebagai password. Anda bisa meningkatkan

kekuatan dari password dengan melakukan perubahan kecil sehingga menjadi "c1Nt4$3Jat1".

Hal-hal yang Harus Dihindari dalam Memilih Password

Selain poin-poin yang sudah dipaparkan sebelumnya, ada beberapa hal yang harus Anda hindari dalam memilih password guna meningkatkan kekuatan dari password.

1. Hal penting pertama yang harus Anda ingat adalah jangan pernah menggunakan blank password atau password kosong. Ini memang terdengar konyol tetapi kejadian ini pun seringkali ditemui di mana seorang user merasa malas untuk menghafal password dan memutuskan untuk menggunakan password kosong untuk account yang dimilikinya.
2. Jangan pernah menggunakan password yang mengandung karakter yang sifatnya perulangan atau berurutan, misalnya "12345", "defgh", "ddddd" atau yang memiliki posisi berurutan pada papan keyboard seperti "asdfg".
3. Jangan pernah menggunakan data pribadi yang sifatnya diketahui oleh umum, seperti tanggal lahir, alamat rumah, nama istri, dan data-data sejenis lainnya.

Kebiasaan yang Perlu Diperhatikan dalam Menjaga Kekuatan Password

Ada beberapa kebiasaan yang sebaiknya mulai dibudayakan berkaitan dengan penggunaan password guna tetap menjaga kekuatan dari password itu sendiri.

1. Jangan pernah men-share password yang Anda miliki kepada siapa pun. Perpaduan antara username dan password merupakan identitas Anda di dalam suatu sistem.

   Apabila Anda men-share ke orang lain, ia dapat memasuki sistem dengan menggunakan indentitas Anda. Artinya sistem akan mengidentifikasi orang tersebut sebagai diri Anda dan apa pun aktivitas yang dilakukan oleh orang tersebut akan dicatat sebagai aktivitas yang Anda lakukan.

   Bisa dibayangkan bila ternyata orang tersebut melakukan aktivitas yang sifatnya melanggar hukum, maka yang tercatat oleh sistem sebagai pelaku tidak lain dan tidak bukan adalah diri Anda sendiri.

2. Jangan pernah menuliskan password yang Anda miliki pada selembar kertas atau pada suatu file yang dapat diakses dengan mudah oleh orang lain. Kejadian ini juga banyak ditemui di beberapa perkantoran: karena takut melupakan password-nya, orang menuliskannya pada sebuah kertas kecil dan menempatkannya di bawah keyboard, bahkan menempelkannya pada layar monitornya.
3. Gantilah password Anda secara periodik. Beberapa profesional di bidang IT Security menyarankan untuk melakukan penggantian password setiap tiga minggu sekali, dan password baru yang dipilih tidak boleh sama dengan lima password yang sebelumnya pernah digunakan.

   Misalkan sebelumnya Anda pernah menggunakan password "B3b3kG0r3ng" dan , "B3b3kP4ngg4ng", maka password Anda tidak dianjurkan untuk kembali menggunakan "B3b3kG0r3ng" sebagai password berikutnya. Anda baru boleh menggunakan password tersebut setelah melewati siklus penggantian password yang keenam.

Inilah 10 "Password" yang Paling Gampang Ditebak

Konsultan keamanan teknologi informasi sering kali memperingatkan pengguna agar tidak menggunakan password yang mudah ditebak. Hal itu, antara lain, minimal delapan karakter dan kombinasi huruf dan angka. Namun, kenyataannya masih banyak password yang sangat sederhana dan mudah sekali ditebak.

"Setiap orang perlu memahami apa dampak kombinasi password yang buruk di era serangan internet yang semakin otomatis. Dengan usaha sederhana, seorang hacker bisa memperoleh akses ke akun baru setiap detik atau 1.000 akun setiap 17 menit," ujar Amichai Shulman, Chief Technical Officer Imperva, perusahaan analis data dari AS, dilansir Telegraph.

Imperva merilis 10 password yang paling banyak dipakai sehingga kemungkinan ditebak sangat besar. Kesepuluh password tersebut merupakan hasil riset terhadap 32 juta password yang dipakai pengguna RockYou, situs jejaring sosial yang baru saja mengalami pembobolan database. Hasil penelitian ini memang berlaku di layanan RockYou. Namun, hal itu mungkin juga relevan di layanan lainnya.

Pada Desember 2009, database yang berisi data profil pengguna RockYou dibobol pihak ketiga. Padahal, nama pengguna berikut password itu tidak dienkripsi. Akibatnya, Rock You buru-buru mengeluarkan permintaan maaf dan meminta penggunanya segera mengganti password agar terhindar dari pihak tak bertanggung jawab.

Berikut daftar 10 password yang paling sering dipakai:

1. 123456
2. 12345
3. 123456789
4. Password
5. iloveyou
6. princess
7. rockyou
8. 1234567
9. 12345678
10. abc123

---

abcd1234
RAHASIA
asdf1234

Kenali Ciri-ciri ATM yang Berisiko

Meski tidak ada solusi keamanan yang menjamin transaksi ATM sepenuhnya bebas dari kejahatan seperti skimming, nasabah bank perlu waspada. Penting mengenali ATM yang berisiko bisa dimanfaatkan untuk tindak kejahatan tersebut.

"Biasanya, skimming hanya dilakukan di ATM-ATM jenis lama," kata Ruby Z Alamsyah, pakar forensik teknologi informasi, kepada Kompas.com, Rabu (20/1/2010) malam. ATM-ATM ini, menurut dia, paling gampang dipakai pelaku karena sangat terbuka.

Ada dua alat yang biasa dipasang pelaku di AM untuk mencuri data kartu ATM korban. Pertama, alat skimmer untuk mencuri data magnetik. Kedua, kamera pengintai (spycamera).

Alat skimmer ditempel di mulut ATM tempat memasukkan kartu. Alat ini biasanya dibuat dari gipsum dan didesain cocok dengan bentuk ATM. Warnanya pun disesuaikan dengan warna ATM.

"Tapi, sebenarnya gampang dikenali. Warnanya pasti sedikit beda dengan badan ATM. Sering kali juga retak karena diimpor dari Amerika biasanya retak selama di perjalanan karena dibuat dari gipsum," ujar Ruby.

Selain itu, kata Ruby, skimmer umumnya hanya ditempel dengan double tape atau bahkan ada pelaku yang nekat alatnya diplester dari luar. "Goyang-goyang saja agak kuat, kalau lepas, berarti skimmer," kata Ruby. Elemen ATM tidak mungkin ditempel selemah skimmer tersebut. Sementara untuk mengenali kamera, biasanya pelaku memasang di badan ATM atau di sekitarnya. Kamera spycam ukurannya tipis dan memanjang sehingga bisa ditempel di atas atau samping tombol untuk mengetik PIN. Tempat lain yang perlu diwaspadai adalah kotak di samping ATM yang biasa dipakai untuk menaruh leaflet. Kata Ruby, pokoknya semua yang mengarah ke tombol untuk mengetik PIN harus diwaspadai.

Namun, untuk meyakinkan ATM aman, menurut Ruby, pilih ATM yang dijaga petugas satpam atau keamanan. Sebisa mungkin hindari ATM yang terbuka dan ATM lama.