Ασφάλεια κωδικών: Ένας hacker συμβουλεύει

Το συναίσθημα που προκαλεί ένα password που καταρρέει μέσα σε κλάσματα του δευτερολέπτου ακροβατεί μεταξύ πανικού και τάσης για γέλια. Αν είναι τόσο εύκολο, γιατί μπαίνουμε στον κόπο να κάνουμε log in και να θυμόμαστε έστω αυτό το ένα, ταπεινό password που χρησιμοποιούμε από καταβολής κόσμου; Κι αν αυτό δεν επαρκεί, υπάρχει κάτι άλλο που μπορεί να μας προστατεύσει;

Ζητήσαμε από έναν hacker, τον Virtual_Samadhi, να μοιραστεί μαζί μας τα μυστικά της τέχνης του, για να τα χρησιμοποιήσουμε… εναντίον του, κι εκείνος μας απάντησε –πρώτα απ' όλα– ότι δεν υπάρχει password που δεν σπάει. Μπορούμε, όμως, να προστατευτούμε μέχρι ενός σημείου.

Τα συχνότερα λάθη των passwords

«Τα πιο μεγάλα λάθη στην ασφάλεια των ηλεκτρονικών υπολογιστών γίνονται από τους ίδιους τους χρήστες» εξηγεί ο Virtual_Samadhi. Ρίξτε μια ματιά στα πέντε συχνότερα λάθη της «κατασκευής» κωδικών και… αναγνωρίστε τα δικά σας:

- **Χρησιμοποιείτε τον ίδιο κωδικό για περισσότερα από ένα (ή για όλα τα) sites.** «Με αυτόν τον τρόπο, αν κάποιος σπάσει τον κωδικό σου, για παράδειγμα, στο Facebook, αποκτά πρόσβαση και στο e-mail, και στο MSN και πάει λέγοντας» λέει ο Virtual_Samadhi.

- **Χρησιμοποιείτε για password κάτι που γνωρίζετε εσείς και όλος ο κοινωνικός σας περίγυρος**, όπως πχ την ημερομηνία γέννησής σας, το όνομα του σκύλου σας κλπ. «Όσο καλύτερα σε ξέρει ο άλλος τόσο πιο εύκολο είναι να κάνει μια επιτυχημένη επίθεση στον κωδικό σου» λέει ο Virtual_Samadhi. Και τόσο περισσότερους λόγους έχει να θέλει να διαβάσει τα e-mail σου, προσθέτουμε εμείς.

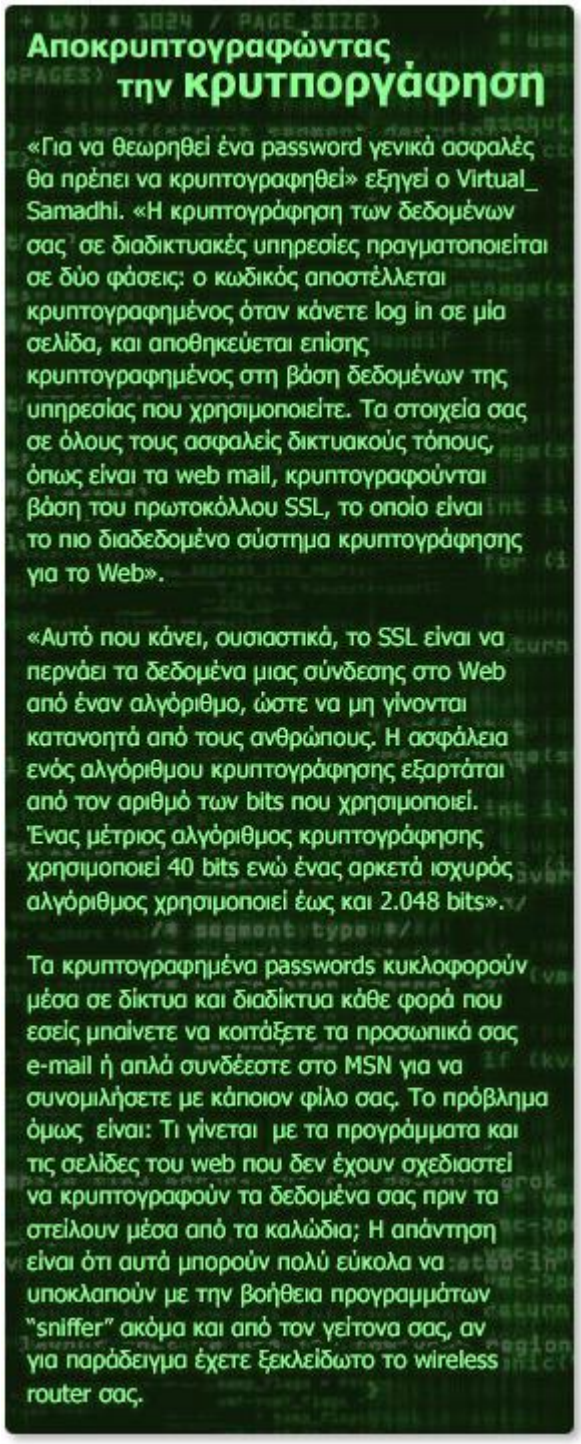
- **Χρησιμοποιείτε «ερωτήσεις ασφαλείας» του τύπου «πώς λένε τη γάτα σου;»** ή ακόμα χειρότερα «ποιο είναι το πατρικό της μητέρας σου;» για την περίπτωση που ξεχάσετε τον κωδικό σας. Την απάντηση γνωρίζει, όπως λέγαμε προηγουμένως, όλος ο κοινωνικός σας περίγυρος. Να συνεχίσουμε;

- «**Τικάρετε» επιλογές όπως τα remember me/ remember password κλπ** όταν κάνετε login σε μία σελίδα. «Πρόκειται για το πιο λάθος πράγμα που έχουν ανακαλύψει ποτέ» λέει ο Virtual_Samadhi. «Η επιλογή "remember me" πρακτικά σημαίνει ότι όποιος κάτσει στον συγκεκριμένο υπολογιστή έχει αυτομάτως πρόσβαση στον λογαριασμό σου. Δε χρειάζεται, προφανώς, να τονίσουμε πόσο επικίνδυνο είναι αυτό σε ένα internet café. Πέρα, όμως από αυτό, όταν τικάρεται η συγκεκριμένη επιλογή, το password καταγράφεται –συνήθως κρυπτογραφημένο, αλλά αυτό δεν διασφαλίζει τίποτα– στην registry των Windows, δηλαδή στο

«μητρώο» που αποθηκεύονται όλες οι personalized επιλογές των Windows, ή στο cache, όπου φυλάσσονται όλα τα προσωρινά αρχεία. Υπάρχουν προγράμματα που μπορούν να διαβάσουν την registry, ακόμη και εξ αποστάσεως» εξηγεί.

- **Αποθηκεύετε όλους τους κωδικούς σας σε ένα μη κρυπτογραφημένο αρχείο word**/ notepad/ excel στον υπολογιστή σας. Στο σφάλμα αυτό υποπίπτουν και πολλές εταιρείες, οι οποίες κρατούν συγκεντρωμένα σε ένα plain text αρχείο τα στοιχεία πρόσβασης των υπαλλήλων τους στο δίκτυο, με αποτέλεσμα αν κάποιος αποκτήσει πρόσβαση στο εν λόγω αρχείο να πάρει στα χέρια του και όλους τους κωδικούς.

Και πώς θα φανταστεί ο άλλος τον κωδικό μου;



Δεν θα τον φανταστεί –τουλάχιστον όχι αν έχετε διορθώσει τα προαναφερθέντα λάθη. Θα χρησιμοποιήσει έναν από τους άπειρους τρόπους που υπάρχουν για να τον «σπάσει». Πάρτε ιδέες:

Brute force password cracking λέγεται η πιο δημοφιλής εκδοχή επίθεσης, η οποία βασίζεται στις λεγόμενες password ή dictionary lists. Αυτές είναι έτοιμες για κατέβασμα λίστες με τεράστιο αριθμό πιθανών passwords (σκεφτείτε κάτι κοντά στο εκατομμύριο) τους οποίους «δοκιμάζει» αυτόματα ένα πρόγραμμα. «Το καλό –για τον χρήστη– σε αυτήν την μέθοδο είναι ότι πολλά συστήματα, όπως το Facebook για παράδειγμα, έχουν φτιαχτεί έτσι ώστε να «κλειδώνουν» μετά τις πέντε λανθασμένες εισαγωγές password» λέει ο Virtual_Samadhi.

Precomputed hash tables ή Rainbow Tables λέγονται οι αντίστοιχες λίστες οι οποίες μαντεύουν την κρυπτογραφημένη εκδοχή του κωδικού σας (ή hash, σε απλά… χακερικά) αντί για τον ίδιο τον κωδικό. Ο cracker σε αυτήν την περίπτωση χρησιμοποιεί ένα πρόγραμμα το οποίο δημιουργεί κωδικούς και ταυτόχρονα τους κρυπτογραφεί. Πρόκειται για τον συνηθέστερο τρόπο επίθεσης σε κωδικούς ασύρματων δικτύων και Windows. «Σημαντικό ρόλο στη μέθοδο αυτή, όπως και στην προηγούμενη, παίζει η τεχνολογία που έχει στα χέρια του ο cracker. Το πόσο γρήγορα θα σπάσει έναν κωδικό εξαρτάται από την ταχύτητα του επεξεργαστή και της σύνδεσής του, αλλά και από αυτό που λέμε distributed password cracking: το αν έχει δηλαδή στη διάθεσή του δύο ή σαρανταδύο υπολογιστές να προσπαθούν ταυτόχρονα να σπάσουν τον ίδιο κωδικό» εξηγεί ο Virtual_Samadhi.
Pass the hash λέγεται ο πιο σπάνιος, και ο πιο επικίνδυνος, τρόπος επίθεσης, ο οποίος είναι γνωστός στην underground κοινότητα και μόνο, όπως τονίζει ο Virtual_Samadhi. Σκεφτείτε το σαν το τρίτο βήμα: δεν «μαντεύεις» τον κωδικό, δεν "σπας" την κρυπτογράφησή του, τα παρακάμπτεις και τα δύο και «χτυπάς» απευθείας τον στόχο.
Social Engineering είναι ο υποτιμημένος από την underground κοινότητα τρόπος που διέδωσε στο παγκόσμιο στερέωμα ο πιο γνωστός hacker όλων των εποχών, ο Kevin Mitnick, πριν από μερικά χρόνια με το βιβλίο του “The Art of Deception”. Εδώ ο cracker της γειτονιάς σας δεν χρειάζεται ούτε προγράμματα, ούτε λίστες, ούτε εξειδικευμένες γνώσεις. Αρκεί ένα τηλεφώνημα, στο οποίο σας λέει, για παράδειγμα, ότι αντικαθιστά τον τεχνικό της εταιρείας σας και χρειάζεται το password σας για να διορθώσει κάτι στην βάση δεδομένων. Σας φαίνεται απίστευτο; Κι όμως, δέκα στις δέκα φορές ο Mitnick έκλεινε το τηλέφωνο με το password που ήθελε στα χέρια του.

Τι να κάνω τελικά;

- **Δημιουργήστε περίπλοκα passwords.** «Το πόσο δύσκολο είναι να σπάσει ένα password εξαρτάται από πολλούς παράγοντες: το μέγεθός του, τον συνδυασμό γραμμάτων, αριθμών και χαρακτήρων όπως τα $, * κλπ, τη χρήση πεζών και κεφαλαίων σε τυχαία σειρά κλπ» λέει ο Virtual_Samadhi. Η κοινή πρακτική της αντικατάστασης γραμμάτων με αριθμούς, όπως το ε με το 3, το όμικρον με το μηδέν και πάει λέγοντας, είναι πλέον τόσο κοινή που αποτελεί παράδειγμα προς αποφυγή.

- **Χρησιμοποιήστε password generators,** όπως ο Source Forge τον οποίο μπορείτε να κατεβάσετε δωρεάν από εδώ, οι οποίοι δημιουργούν κωδικούς που δεν σχετίζονται με την ανθρώπινη λογική. Χρησιμοποιήστε ένα πρόγραμμα που να βασίζεται σε έναν ισχυρό αλγόριθμο, όπως ο Twofish (κατεβάστε τον δωρεάν από εδώ) για να κρυπτογραφήσετε τα σημαντικά αρχεία και τους κωδικούς σας πριν τα σώσετε απλά στον δίσκο σας. Όχι, δεν υπάρχει περίπτωση να θυμάστε απέξω το "Ji6)2Fe*41d" που θα σας προσφέρει απλόχερα ο Source Forge.

- **Βεβαιωθείτε ότι η σελίδα στην οποία ετοιμάζεστε να κάνετε log in χρησιμοποιεί SSL Encryption**, ή κάποιο αντίστοιχο σύστημα κρυπτογράφησης. Θα το καταλάβετε, από το λουκέτο που εμφανίζεται δίπλα στην μπάρα της διεύθυνσης του browser σας.

Και τώρα είμαι ασφαλής;
Ο γενικός κανόνας λέει ότι δεν υπάρχει κωδικός που να μην σπάει. Δεν υπάρχει, δηλαδή, περίπτωση ένας ικανός cracker να «βάλει στο μάτι» τον κωδικό σου, απλέ καθημερινέ χρήστη, και να μην καταφέρει να τον σπάσει. «Το κόλπο είναι να του κάνεις τη ζωή

δύσκολη» λέει ο Virtual_Samadhi, «να χρειαστεί δηλαδή τόσο πολύ χρόνο, ώστε να τα παρατήσει. Το σπάσιμο ενός κωδικού μπορεί να διαρκέσει από μερικά δέκατα του δευτερολέπτου, για να σπάσει π.χ. ο κωδικός abc, έως μερικούς αιώνες προσπάθειας για passwords τύπου “F(Gke10e8f4!”. Αν στα αρχεία σου δεν κρύβονται τα μυστικά του κράτους, ο δύσκολος κωδικός σου δεν αξίζει τις εργατοώρες που θα σπαταληθούν για να σπάσει. Αυτό που θέλεις είναι, ουσιαστικά, να βαριούνται να ασχοληθούν μαζί σου» καταλήγει.

ΑΝΑΔΗΜΟΣΙΕΥΣΗ:www.in2life.gr (ΗΡΩ ΚΟΥΝΑΔΗ)