TECHNIQUES
DE L'INGÉNIEUR

LES FOCUS
TECHNIQUES DE L'INGÉNIEUR

SÉCURITÉ INFORMATIQUE

LES MOTS DE PASSE DU FUTUR

juillet / 2017

SOMMAIRE

SOMMAIRE 2

INTRODUCTION 3

CYBERSÉCURITÉ : LE MAILLON FAIBLE 4

- CYBERSÉCURITÉ : L'ÊTRE HUMAIN RESTE LE MAILLON FAIBLE 4
- LE B-A BA DE LA SÉCURITÉ INFORMATIQUE SELON EDWARD SNOWDEN 5

PAR QUOI REMPLACER LE TRADITIONNNEL MOT DE PASSE ? 8

- SÉCURITÉ INFORMATIQUE : QUELLES SOLUTIONS POUR REMPLACER LE MOT DE PASSE ? 8
- VOS ONDES CÉRÉBRALES POURRAIENT REMPLACER VOS MOTS DE PASSE 10
- SÉCURITÉ DE VOS COMPTES : UN SEUL MOT DE PASSE POUR LES PROTÉGER TOUS 11
- PHRASES DE PASSE : COMMENT SÉCURISER VOS COMPTES AU MAXIMUM 13

INTRODUCTION

On le sait, le binôme traditionnel identifiant/mot de passe est voué à disparaître. Si, pendant longtemps, la simple combinaison d'un mot suivi de caractères spéciaux a constitué une barrière efficace, aujourd'hui il est clair que ce verrou ne suffit plus à protéger nos données. Mais par quoi le remplacer ?

CYBERSÉCURITÉ : LE MAILLON FAIBLE

CYBERSÉCURITÉ : L'ÊTRE HUMAIN RESTE LE MAILLON FAIBLE

C'est toujours le même constat : dans la majorité des cas, une erreur humaine est à l'origine des attaques informatiques. Et la messagerie reste la principale d'infection. La sensibilisation demeure plus que jamais indispensable !

Les experts en sécurité informatique ont coutume de dire que le principal risque sur trouve entre « la chaise et le clavier ». En clair, l'être humain et ses ressorts psychologiques bien connus : la curiosité, l'avidité, la paresse. Nous partageons tous ces mêmes défauts qui sont exploités par les pirates depuis des années.

Et le dernier rapport de Proofpoint, baptisé « Le Facteur Humain », ne fait qu'enfoncer le clou : nous sommes toujours les principaux maillons faibles de la cybersécurité. Pour ne pas incriminer que les internautes et les professionnels, précisons que les logiciels de sécurité et les systèmes exploitation comme Windows ne sont pas non plus exempts de défauts ; avec leurs failles de sécurité et leurs performances parfois limitées, ils ont aussi une part dans la multiplication des piratages.

Basé sur l'analyse de tentatives d'intrusions dans plus de 5000 entreprises en 2016, ce rapport de Proofpoint, spécialiste de la sécurité et de la conformité, confirme donc que les pirates s'appuient sur les failles humaines pour installer des programmes malveillants, dérober des informations confidentielles ou transférer des fonds. « Cette tendance d'exploitation du facteur humain, qui a vu le jour en 2015, s'accélère, et les cybercriminels multiplient désormais les attaques générées par les clics des utilisateurs plutôt que par des logiciels vulnérables, conduisant ainsi les victimes à exécuter elles-mêmes les attaques », a déclaré Kevin Epstein, vice-président du centre d'opération des menaces de Proofpoint.

Et encore une fois, la messagerie est pointée du doigt comme étant le principal vecteur d'infection par un code malveillant. Les attaques sur la messagerie d'entreprise sont passées de 1 % en 2015 à 42 % fin 2016. Et malgré les rappels constants à la vigilance, « près de 90 % des clics sur des URL malveillantes ont lieu dans un délai de 24 heures après la remise de l'email. 25 % de ces clics se produisent en seulement 10 minutes et près de 50 % en une heure », précise l'Usine Digitale.

Pour les cybercriminels, le phishing reste donc l'arme de prédilection pour atteindre leurs objectifs. C'est un classique indémodable. Et il n'est pas près de s'arrêter puisqu'il se répand sur les réseaux sociaux. Les escrocs usurpent l'identité d'une entreprise et se font passer pour son service client : il n'y a plus qu'à attendre que des internautes mordent à l'hameçon pour récupérer leurs coordonnées bancaires par exemple. Résultat, ce type d'attaque a augmenté de 150 % en 2016.

Les résultats de ce rapport montrent que les entreprises ne doivent pas limiter leur politique de sécurité au seul investissement dans des logiciels de sécurité. La sensibilisation de tous les salariés est indispensable pour qu'ils tombent moins facilement dans les pièges des cybercriminels.

Par **Philippe Richard**

13/06/2017

LE B-A BA DE LA SÉCURITÉ INFORMATIQUE SELON EDWARD SNOWDEN

Depuis les révélations d'Edward Snowden, le grand public, mais aussi, et c'est plus inquiétant, les hommes politiques et des entreprises, découvrent que toutes les communications sont sur écoute.

Pour schématiser, les grandes oreilles de la NSA (National Security Agency - Agence nationale de sécurité américaine), et des autres services du renseignement peuvent intercepter toute sorte de données dès lors qu'elles transitent par un « tuyau ».

Pourtant, « *l'espionnage généralisé a commencé en 1941 avec le traité UKUSA associant les USA, le Canada, le Royaume-Uni, l'Australie et la Nouvelle-Zélande (les 5 yeux), élargi un peu plus tard à d'autres pays incluant la France. Avant PRISM (actif depuis 2007 et révélé en 2013 par Snowden), plus d'une vingtaine de programmes d'espionnage majeurs ont été mis en œuvre depuis 1945* », rappelle Éric Filiol, Directeur du laboratoire de virologie et de cryptologie opérationnelles (ESIEA Ouest).

Sans devenir paranoïaque, il convient de prendre de bonnes habitudes et d'installer certains logiciels pour limiter les fuites de données sensibles et réduire les risques d'être surveillé, voire espionné. Dans un entretien accordé à The Intercept (site cofondé par le journaliste Glenn Greenwald, à l'origine des premières révélations sur l'écoute de la NSA), Edward Snowden délivre ses conseils pour utiliser Internet et son smartphone de façon plus sûre.

À propos des SMS, le lanceur d'alerte indique qu'il ne faut pas hésiter à chiffrer (d'aucuns parlant à tord de « crypter ») ses SMS car cette parade est simple à utiliser avec une application gratuite comme Signal Private Messenger, fruit de la fusion entre TextSecure et RedPhone, deux applications spécialisées dans le chiffrement respectivement des SMS et des appels mobiles. Disponible gratuitement sous iOS et Android, elle permet d'envoyer différents types de contenus chiffrés (texte, images, vidéos…) entre vos contacts ayant installé cette même application.

En matière de communication, il est également conseillé de délaisser Skype au profit de Jitsi (anciennement SIP Communicator), un logiciel libre de communication instantanée, d'appel audio et vidéo et de partage d'écran. De plus, il permet de chiffrer les communications.

Des données sensibles étant de plus en plus accessibles depuis les smartphones, Snowden recommande également d'utiliser un gestionnaire de mot de passe. À l'instar de KeePassX, un logiciel Open source et multiplate-forme, ce logiciel protège vos différents de mots de passe grâce à un « super mot de passe » que vous aurez créé en mélangeant des lettres, des chiffres et des signes de ponctuation. Ainsi, vous ne retenez qu'un seul mot de passe.

Toujours à propos des informations confidentielles, il est nécessaire de les mettre à l'abri dans un volume chiffré sur votre ordinateur ou une clé USB. Depuis les doutes émis à l'encontre de TrueCrypt, il existe une alternative française, Gostcrypt. Ce projet présente la particularité de s'appuyer sur du chiffrement russe appelé GOST (qui provient de GOsudarstvennyi STandard et qui signifie « standard gouvernemental »).

Toujours à propos de chiffrement, Snowden conseille d'utiliser Thunderbird (au détriment d'Outlook, Gmail, Yahoo…) et son module Enigmail. Ce dernier requiert GnuPG (GNU Privacy Guard) pour ses fonctions cryptographiques, mais il est déjà installé par défaut sur les distributions GNU/Linux.

Cette solution s'appuie sur la cryptographie à double clé. Chaque contact possède deux clés qui sont associées à son adresse email : une clé privée et une clé publique.

La première doit être mise à l'abri des curieux (et être protégée par un mot de passe complexe) et ne pas être communiquée à qui que ce soit, car elle a une double fonction : décrypter les messages reçus et signer ceux qui sont envoyés.

La seconde (la clé publique) peut être communiquée à vos contacts qui pourront ainsi vous adresser des messages que vous serez le seul à pouvoir les lire. Elle permet aussi de vérifier que vous êtes bien l'auteur des messages envoyés.

Enfin, il recommande l'authentification à deux facteurs. Cette solution n'est pas généralisée. Elle est pourtant efficace pour réduire les risques d'usurpation d'identité et de vol de données. Son principe est simple : en plus d'un mot de passe, il faut retaper un code reçu par SMS pour authentifier une identité et ensuite accéder à un compte.

Tous ces conseils s'appuyant sur des logiciels ne sont pas suffisants. « *Si vous pensez que la technologie peut résoudre vos problèmes de sécurité alors vous n'avez rien compris aux problèmes ni à la technologie* », déclarait l'expert en sécurité Bruce Schneier. La vigilance reste prioritaire.

Par **Philippe Richard**

19/11/2015

PAR QUOI REMPLACER LE TRADITIONNNEL MOT DE PASSE ?

SÉCURITÉ INFORMATIQUE : QUELLES SOLUTIONS POUR REMPLACER LE MOT DE PASSE ?

Le binôme identifiant/password est une solution dépassée pour protéger efficacement un ordinateur ou un smartphone. Différentes solutions sont disponibles ou testées.

Chaque internaute a en moyenne une vingtaine de mots de passe. Et dans bien des cas, il s'agit des classiques mots de passe que l'on retrouve chaque année dans les Top 10 des plus utilisés : 12345, password, azerty… Ils n'apportent aucune sécurité car ce sont des mots de passe dits « faibles ». Pour plus de sécurité, il est nécessaire d'utiliser des mots de passe dits « forts ». Exemple : 1+KjhTR*d7-/. Pour la majorité des internautes, cet exemplaire est rédhibitoire. D'où la nécessité pour les marques et éditeurs spécialisés dans le high-tech de proposer des alternatives plus pratiques à utiliser tout en garantissant un niveau élevé de protection. Pas simple !

L'empreinte digitale

C'est la mesure biométrique la plus employée dans le monde depuis les années 60. Une quinzaine de points caractéristiques (les minuties, codifiées à la fin des années 1800 en « caractéristiques de Galton ») correctement localisés permettent d'identifier une empreinte parmi des millions. Par ailleurs, la probabilité de trouver deux individus avec des empreintes similaires est de 1 sur 1024.

Apple l'a généralisé avec sa technologie touchID, introduite en 2013 pour l'iPhone 5S.

Mais elle a été rapidement mise à mal par les hackers. « C'est complètement stupide d'utiliser comme élément de sécurité quelque chose qu'on laisse si facilement traîner derrière soi », a expliqué le président du Chaos Computer Club, Frank Rieger.

Résultat, les capteurs d'empreintes du Galaxy 5 et de l'iPhone 5S ont été piratés quelques jours après leur sortie par les chercheurs allemands du SRLabs.

La reconnaissance vocale

C'est en 1962 que Lawrence Kersta, un ingénieur du Bell Laboratories, établit que la voix de chaque personne est unique et qu'il est possible de la représenter graphiquement. Toutefois, l'Association Francophone de la Communication Parlée (AFCP) rappelle que « la voix n'est pas une empreinte digitale ou génétique. La voix présente des différences majeures avec les empreintes digitales et génétiques. Elle évolue au cours du temps et elle est modifiable volontairement et aisément falsifiable, avec les moyens techniques existants ».

Malgré ces limites, la Banque Postale (dont les premiers tests remontent à 2013 avec Talk to Pay est la première institution à avoir obtenu l'autorisation de la CNIL pour la tester en France. Pour mémoire, dès 2011, un système de vérification du locuteur avait été mis en place par Dexia en Belgique. Mais il était réservé à ses 300 clients VIP afin d'accéder à des services privilégiés sur un numéro de téléphone dédié. En Israël, la banque Lomi l'avait utilisé pour repérer les fraudeurs à la carte bancaire.

Le réseau veineux oculaire

L'entreprise EyeVerify propose un système de déverrouillage par l'analyse du réseau veineux des yeux. Selon certains spécialistes en cybersécurité, cette technologie est fiable à 99 %, d'autant qu'elle prend en compte le vieillissement des veines et de la rétine. Une réserve, tout de même : cette technologie biométrique exige de posséder des appareils équipés de caméras haute résolution.

Une alternative consiste à étudier le réseau veineux de la main. Dans les années 1980, les scientifiques s'étaient rendu compte qu'il était propre à chaque individu, même dans le cas de vrais jumeaux.

Mais pour l'instant, rien ne vaut une carte à puce pour sécuriser l'accès à son ordinateur. « Toutes les procédures biométriques ont été de différentes manières retournées, rappelle Vincent Guyot, Directeur scientifique du Mastère Spécialisé SI&S à l'ESIEA. Une carte à puce est très difficile à casser. C'est beaucoup plus sûr qu'un certificat stocké sur un ordinateur et qu'un code malveillant peut corrompre. Quand le certificat est dans la carte à puce, le pirate ne peut pas accéder au contenu de cette carte même s'il a infecté la machine. »

Par **Philippe Richard**

12/06/2017

VOS ONDES CÉRÉBRALES POURRAIENT REMPLACER VOS MOTS DE PASSE

Des chercheurs de l'Université de Binghamton (USA) ont découvert qu'avec un peu d'entraînement, votre ordinateur peut vous identifier sur la base de la façon dont votre cerveau réagit à certains mots. Cela signifie qu'au lieu d'un mot de passe, vous pourriez vous contenter d'écouter quelques mots, les répéter et déverrouiller ainsi tous vos fichiers secrets…

« Brainprint »(littéralement *l'empreinte du cerveau*) est une étude récemment publiée dans la revue académique *Neurocomputing* où des chercheurs américains ont observé les signaux cérébraux de 45 volontaires. Les données étaient enregistrées alors que les sujets lisaient une liste de 75 acronymes comme FBI, DVD…

94% de réussite

L'analyse des résultats a permis de classer les réactions pour chaque type de lettre prononcée, les associations faites entre la reconnaissance du mot et la lecture du mot… il en résulte qu'un ordinateur est capable d'identifier correctement chaque volontaire avec un taux de réussite de 94%.

Les résultats suggèrent que les ondes cérébrales pourraient tout à fait être utilisées par les systèmes de sécurité pour vérifier l'identité d'une personne.

En bref, vous passez un scanner pour établir votre empreinte cérébrale. Vous vous asseyez ensuite avec un scanner au-dessus de votre tête, relié à votre ordinateur qui vous demande de prononcer quelques mots et en quelques millièmes de secondes vous avez accès à vos fichiers secrets… ou votre compte Facebook… ou rien !

Il est évident que 94% de précision n'est pas idéal, surtout s'il faut investir dans un scanner ! Mais ce n'est qu'un début, et des solutions techniques existent. Fait intéressant, ces « brainprints » sont aussi uniques que les empreintes digitales, mais les chercheurs les qualifient de « plus malléables ».

Si l'empreinte digitale de quelqu'un est volée, cette personne ne peut pas simplement se faire greffer un nouveau doigt pour remplacer l'empreinte compromise. C'est irrémédiable. On dit que les empreintes digitales sont non résiliables. Les « Branprints », elles, sont résiliables.

Réservé à la très haute sécurité ?

Ainsi, dans le cas peu probable où vous vous faites voler vos empreintes cérébrales, il vous sera possible de repasser un scanner et de recréer votre empreinte, différente de celle volée, unique et de nouveau fiable. Magique.

Serons-nous tous bientôt connectés à nos mots de passe à l'aide d'une sonde cérébrale ? Probablement pas. Mais cette technologie pourrait avoir des débouchés pour la très très haute sécurité… et pas pour votre compte Twitter, a priori.

Traduit par S.Luc

Source : techcrunch.com

Et aussi dans les ressources documentaires :
- Sciences fondamentales
- Innovations
- Nanosciences

24/06/2015

SÉCURITÉ DE VOS COMPTES : UN SEUL MOT DE PASSE POUR LES PROTÉGER TOUS

Pour sécuriser vos comptes, il est impératif d'utiliser plusieurs mots de passe, ou phrases de passe, suffisamment complexes pour ne pas être trouvées par un pirate. Pour éviter de les oublier, une solution existe : les coffres forts de mots de passe.

L'été dernier, un piratage de comptes iCloud a créé le buzz. Un hacker avait réussi à pirater les comptes de célébrités, puis il avait diffusé en ligne des photos intimes. Une attaque sûrement menée via une attaque par force brute, qui permet, en testant à la volée des milliers de combinaisons possible, de trouver les mots de passe des utilisateurs.

Régulièrement, des internautes se font voler leurs données. Un mot de passe trouvé, et c'est, bien souvent, l'ensemble des comptes de l'internautes qui est percé à jour - puisque la plupart des utilisateurs utilisent le même mot de passe pour tous leurs comptes (Facebook, Twitter, Gmail, iCloud, etc.).

Construisez des phrases de passe sûres

Face à ce constat, comment faire ? Vos mots de passe sont-ils suffisamment complexes pour ne pas être trouvés par un hacker ? Aussi incroyable que cela puisse paraître, beaucoup d'internautes utilisent encore des mots de passe comme "123456". Plus un mot de passe sera complexe et long, plus il sera difficile à un hacker de le "craquer" grâce à un dictionnaire de mots. Le changer régulièrement est en outre indispensable.

Pour créer un mot de passe complexe, rendez-vous sur notre article dédié aux phrases de passe, qui explique comment utiliser des phrases de passe, plutôt que de simples mots de passe. Pour rappel, les phrases de passe sont une succession de mots, qui placés côte à côte n'ont aucun sens, et qui seront très difficiles à craquer. Il est aussi impératif d'utiliser des phrases de passe différentes pour chaque compte, et jamais un mot de passe unique, pour les raisons citées plus haut.

Une fois que vous aurez réussi à bien verrouiller vos comptes grâce aux clés adéquates, encore faut-il que vous ne les perdiez pas, sinon, impossible d'accéder à vos comptes. Autrement dit, il est impératif de ne jamais perdre vos multiples phrases de passe. Seulement, la mémoire nous joue parfois des tours, et pas question d'écrire vos identifiants quelque part dans un coin de votre ordinateur, ou même sur un bout de papier, car dans le cas où quelqu'un de malintentionné viendrait à y accéder, gare aux dégâts...

Une seule "master key" pour tout protéger

Pour conjuguer au mieux la diversité de vos phrases de passe et leur complexité, une solution consiste à utiliser un "coffre fort", ou "portefeuille" de phrases de passe.

Ainsi, KeePass, Dashlane, LastPass et 1Password vous permettent de stocker vos phrases de passe, et de les protéger dans un fichier unique, lui même protégé par une clé. En somme, une unique phrase de passe permet d'accéder à toutes les autres, dans une base de données sécurisées. Ces données sont chiffrées, et votre phrase de passe "maîtresse", ou "master key", est à considérer comme une clé de chiffrement - sans elle, vos données sont inutilisables, y compris par un pirate informatique.

Dashlane vous permet de vous connecter directement à vos comptes sans jamais plus saisir vos mots de passe, grâce à une fonction de connexion automatique - vos

phrases de passe sont mémorisées par le logiciel. Ce logiciel possède aussi un générateur de mots de passe complexes, difficiles à percer, ainsi qu'un système d'alerte, qui vous prévient automatiquement dès qu'un site web où vous disposez d'un compte à été piraté.

Bien sûr, vous devrez faire attention à changer régulièrement votre "master key", et à ne jamais l'oublier. Mais retenir une seule phrase plutôt qu'une dizaine, voilà qui est tout de même plus simple. A noter que KeePass est le seul parmi les logiciels listés ici a avoir été évalué et certifié par l'Agence nationale de sécurité des systèmes d'information (ANSSI).

Comme le conseille la CNIL (Commission Nationale Informatique et Libertés), il est enfin "indispensable de disposer d'une copie de cette base de mots de passe", qui est "une ressource critique pour pouvoir accéder à vos comptes". Ainsi, nous ne saurions vous conseiller de disposer d'une copie de votre base de phrases de passe sur une clé USB, ou sur un autre support, à garder sur vous ou dans un endroit (vraiment) sûr.

Par Fabien Soyez

01/02/2015

PHRASES DE PASSE : COMMENT SÉCURISER VOS COMPTES AU MAXIMUM

Fin août 2014, un hacker a mis la main sur les photos intimes d'une centaine de célébrités hollywoodiennes, via leurs comptes iCloud. Pour "craquer" les comptes visés, le pirate a probablement mené une attaque par force brute, qui consiste à essayer à la volée des milliers de combinaisons de caractères...

Il est en outre probable que les victimes du "Celebgate" aient choisi des mots de passe très simples. Il aurait alors suffit au hacker de pirater directement le mot de passe d'Apple ID (identifiant Apple), ou de mener une attaque par force brute contre d'autres comptes utilisés par l'utilisateur visé, comme un compte Gmail ou Twitter - en émettant l'hypothèse que cet utilisateur utilise le même mot de passe un peu partout.

Difficile à croire, mais nombre d'internautes continuent à utiliser des mots de passe d'une simplicité déconcertante, comme "aqwzsx", "123456", ou encore "05081958" (une date de naissance). D'autres utilisent des mots du dictionnaire agrémentés de quelques chiffres, ce qui peut donner "vivelesvacances75". Des mots de passe infiniment simples à trouver pour un pirate passant par l'attaque par force brute et des répertoires de mots. Mieux vaut leur préférer un mot de passe long et complexe.

Utilisez des phrases de passe

Il n'est pas question ici d'aligner à la suite des combinaisons de lettres difficiles à retenir, comme "fb'cplf11&pdl@55". Il s'agit plutôt d'utiliser des mots existants, qui placés côte à côte n'auront aucun sens, que vous pourrez retenir facilement, et qui seront difficiles à craquer.

Beaucoup d'internautes utilisent des suites de mots tirées de romans, de films, ou du langage commun - que la plupart des hackers auront préalablement compilées, et qui seront donc faciles à retrouver.

Mieux vont donc utiliser des mots sans lien entre eux, et inventer des phrases sans signification aucune - sauf pour vous. Par exemple, vous pouvez aligner les mots "plantes, téléphone, chapeau, stylo" parce que dans votre bureau, se trouvent autour de vous un téléphone, des plantes vertes, un stylo et un chapeau. A priori, ces mots n'ont pas de lien entre eux et ne forment pas une phrase cohérente. Mais pour vous, elles auront un sens, et rendront votre mot de passe (ou "phrase de passe") presque impossible à percer.

Ne faites pas l'erreur de nombre d'internautes, qui utilisent le même mot de passe partout : si votre phrase est déchiffrée, tous vos comptes sont potentiellement accessibles. N'utilisez donc jamais deux fois la même phrase de passe, et changez la régulièrement, tous les 3 mois si possible. Si vous avez peur d'oublier vos différentes phrases, il existe des "coffres forts", ou "portefeuilles de mots de passe", tels que KeePass, LastPass, 1Password, oneSafe ou Dashlane, qui vous permettront de les stocker en lieu sûr. Dans ce dernier cas, attention, simplement, à changer régulièrement la phrase de passe que vous utilisez pour ce coffre fort.

Par Fabien Soyez

Et aussi dans les ressources documentaires :
- Sécurité de l'informatique en nuage
- Sécurité informatique pour la gestion des risques
- Virus informatiques
- Découvrez le PACK "Sécurité des systèmes d'information"

24/09/2014