KASPERSKY lab

CHIFFREMENT INTÉGRAL DU DISQUE : EFFICACE ET PRATIQUE

www.kaspersky.fr

Un « abri sûr » pour les données d'entreprise

Les informations sont souvent synonymes d'argent. C'est pourquoi les cybercriminels font constamment la chasse aux informations, et pas seulement par des attaques de programmes malveillants. Parfois, plutôt que d'essayer de pénétrer dans le logiciel, il peut être plus facile d'accéder au stockage d'informations directement, en volant l'ordinateur lui-même, ou en tentant d'y accéder à l'insu de son utilisateur légitime. Les solutions de chiffrement intégral du disque ou « FDE » (tels que celles incluses dans Kaspersky Endpoint Security for Business - ADVANCED et Kaspersky Total Security for Business) sont donc de plus en plus populaires.

Une solution FDE contemporaine prend en charge les normes modernes pour le matériel, y compris les disques durs délimités par UEFI et GPT, ainsi que les SSD.[1] Elle doit être aussi transparente et facile à utiliser que possible, en particulier pour l'utilisateur final, qui ne doit pas connaître d'impact négatif notable sur les activités de la vie quotidienne. En outre, afin de réduire la possibilité d'une intervention dans une procédure de démarrage sécurisé, la solution FDE comprend généralement une sorte d'environnement de pré-démarrage (PBE) qui se charge avant le système d'exploitation et permet également aux partitions (du système) actives d'être chiffrées. La solution doit bien entendu être en mesure d'appliquer les niveaux nécessaires de complexité du mot de passe, qui est l'une des clés de la bonne conservation des données.

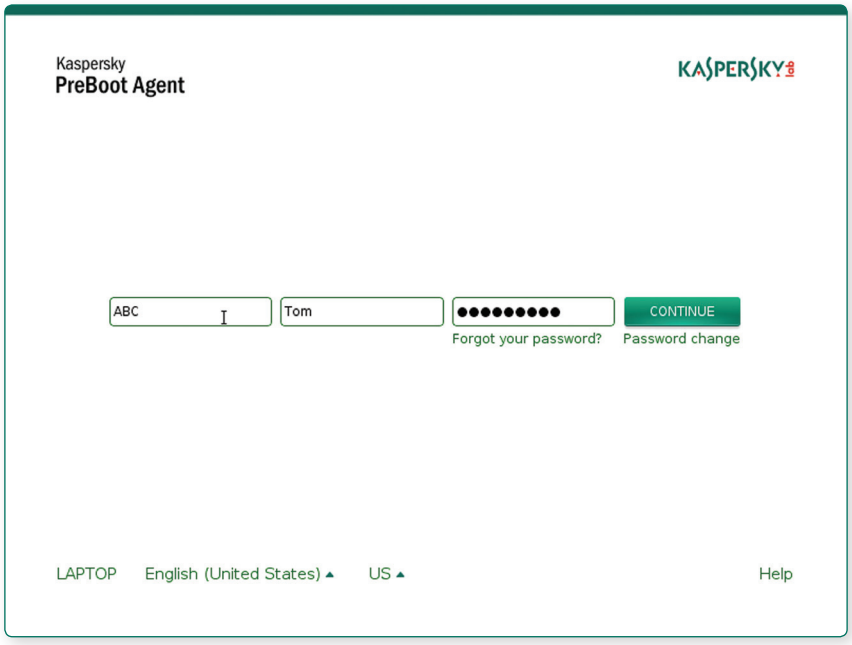


Figure 1 : Capture d'écran de l'agent de pré-démarrage de Kaspersky Lab

Mots de passe FDE : efficaces et pratiques ?

Les mots de passe les plus efficaces sont des combinaisons aléatoires de minuscules, majuscules, chiffres et caractères spéciaux. Cependant, ils ont une faiblesse spécifique : ils sont extrêmement difficiles à mémoriser. Résultat : les utilisateurs obligés d'utiliser ces mots de passe très complexes ont tendance à les écrire sur des morceaux de papier ou des autocollants (qui sont parfois affichés sur les écrans, visibles par tous), ou à les conserver dans la mémoire d'appareils mobiles personnels (qui eux-mêmes ont souvent une faible sécurité). Il va sans dire que cette réponse humaine compréhensible rend la politique d'imposition de mots de passe complexes inutile.

L'utilisation de mots de passe moins complexes et plus faciles à mémoriser, qui sont toujours conformes aux conditions de sécurité de base (habituellement au moins 8 symboles, incluant au moins 3 des 4 catégories de caractères, y compris des minuscules et des majuscules, des chiffres et des caractères spéciaux, à l'exception d'un certain nombre de séparateurs comme les virgules ou les points) est plus pratique et populaire. Ces règles sont simples à mettre en œuvre, même dans les conditions limitées d'environnements de pré-démarrage, et permettent la création de mots de passe suffisamment sûrs et faciles à utiliser.

1 UEFI est une nouvelle interface entre le micrologiciel de la plate-forme et le système d'exploitation, au lieu du BIOS plus ancien. La norme UEFI permet l'utilisation de disques délimités par GPT (GUID Partition Table), qui ne subissent pas de limites de taille de partition héritées, comme les anciens disques MBR (Master Boot Record). Les SSD sont des disques durs à état solide basés sur Flash.

Néanmoins, il existe un certain nombre de directives qui, si elles sont mises en œuvre, pourraient contribuer à accroître la sécurité des mots de passe dans votre organisation, sans que cela soit trop pénible pour l'utilisateur. Examinons-les maintenant à l'aide de l'outil en ligne Kaspersky Secure Password Check.

1. La première directive concerne la langue. Si votre langue maternelle n'est pas l'anglais, utilisez-la ! L'agent de pré-démarrage de Kaspersky Lab permet l'utilisation de langues différentes dans ses champs de nom d'utilisateur et de mot de passe.

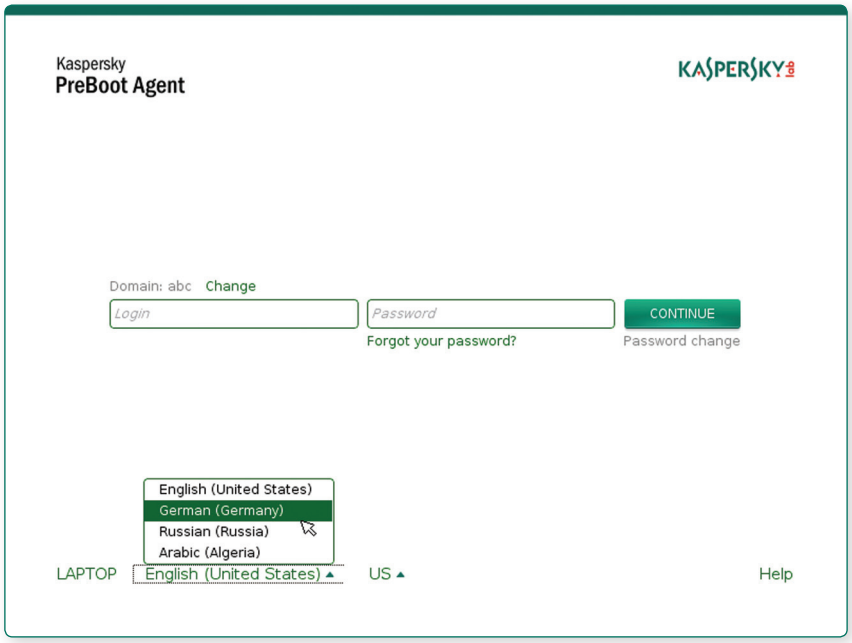


Figure 2 : Capture d'écran de la disposition du clavier de sélection de l'agent de pré-démarrage de Kaspersky Lab

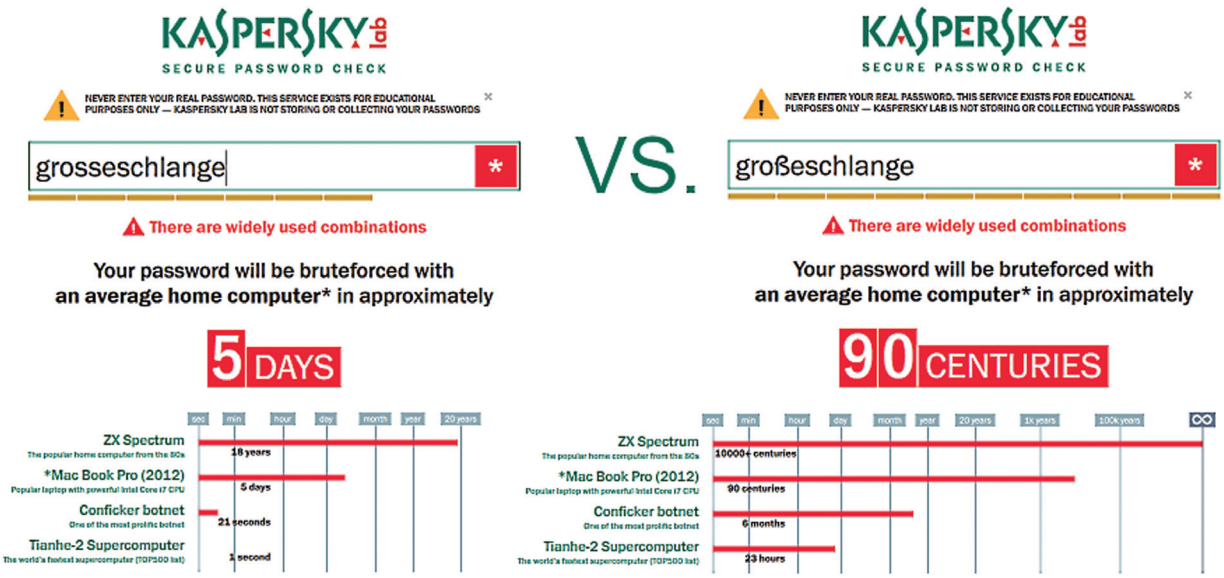
2. D'autres alphabets nationaux contiennent souvent plus de lettres que l'anglais : le jeu de caractères allemands, par exemple, contient 30 caractères au lieu de 26, tandis que le français, avec tous ses symboles diacritiques, comprend jusqu'à 40 caractères. Cela signifie que le nombre de combinaisons possibles augmente automatiquement. Pas tant que ça, peut-être, mais assez pour valoir la peine d'être exploité.[2]

   Néanmoins, avoir un mot de passe plus long a un plus grand impact sur la complexité. Généralement 10 symboles sont suffisants, mais certaines entreprises peuvent imposer une longueur minimale du mot de passe de 14 symboles.

Nombre de combinaisons de mots de passe (mot de passe alphanumérique)			
Caractères	Exemple	Calculs	Combinaisons
4 caractères	Pas1	64 ^ 4	16 777 216
5 caractères	J4s0n	64 ^ 5	1 073 741 824
6 caractères	lo39ce	64 ^ 6	68 719 476 736
7 caractères	Uc333xZ	64 ^ 7	4 398 046 511 104
8 caractères	Yn8xw316	64 ^ 8	281 474 976 710 656
9 caractères	u82nv3ypp	64 ^ 9	18 014 398 509 481 984
10 caractères	i83CH1d47s	64 ^ 10	1 152 921 504 606 846 976

   Les outils les plus puissants utilisés par les cybercriminels, notamment les plus grands glossaires pour des attaques par dictionnaire, sont toutefois affinés pour une utilisation contre des mots de passe en anglais international, à l'aide d'un jeu de caractères standard de 26 lettres. L'utilisation d'accents, de signes diacritiques ou de ligatures accroît considérablement la complexité d'une tâche de piratage de mot de passe. Commençons donc par une expression allemande (qui signifie « grand serpent ») et voyons comment la transformer en un mot de passe remarquablement solide.

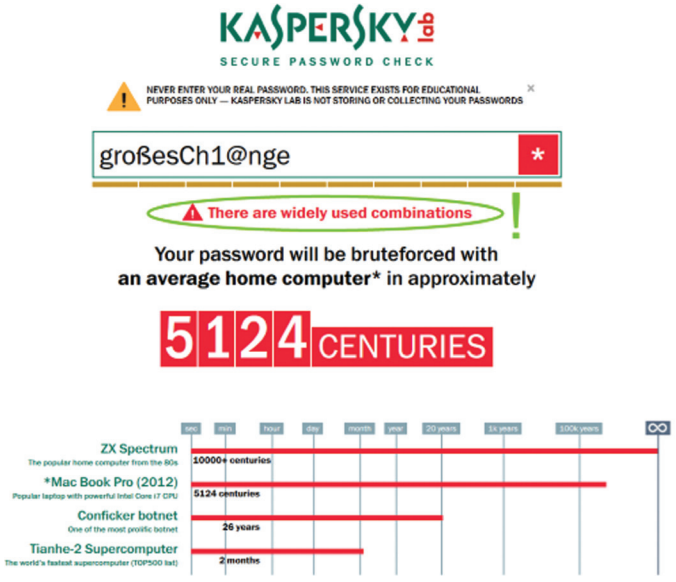
2 Le calcul est simple : le nombre de combinaisons dépend de la taille du jeu de caractères et l'efficacité du mot de passe dépend de sa longueur.



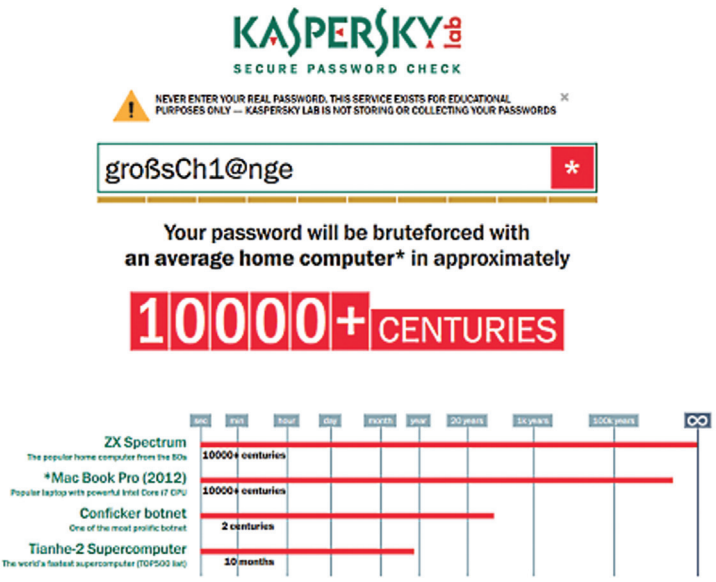
3. Alors que les utilisateurs n'emploieront certainement pas des mots du dictionnaire non modifiés ou des noms propres (nous l'espérons !), utiliser des versions de mots brouillées, de manière à ce qu'elles ne soient pas identifiées dans une attaque par dictionnaire, mais qu'elles puissent encore être facilement mémorisées, est une bonne idée. Plus les mots sont brouillés, mieux c'est. Le résultat doit simplement être mémorisable pour le propriétaire du mot de passe. Utiliser des nombres et des symboles spéciaux accroît davantage la difficulté de piratage de mot de passe et permet au mot de passe de se conformer aux critères de complexité.

4. Les utilisateurs doivent aussi créer leurs mots de passe avec des lettres majuscules, bien qu'une première lettre majuscule seule soit trop évidente.

5. Nous avons donc maintenant quatre types différents de caractère dans notre mot de passe.



6. Mais nous recevons encore cet avertissement ennuyeux parlant de « combinaisons largement utilisées ». Pourquoi ? Les mots, même après avoir été brouillés, conservent certaines combinaisons qui sont plus susceptibles d'être trouvées dans des éléments de langage parlé. Ils ne sont tout simplement pas assez aléatoires. Donc, pour rendre le mot de passe encore plus efficace, essayez de retirer une ou deux voyelles : le résultat peut toujours être assez facile à mémoriser, tout en créant le caractère aléatoire de structure nécessaire.



Ça semble assez aléatoire au premier coup d'œil, n'est-ce pas ? Il reste toutefois intelligible pour son auteur et la signification de l'expression peut même être représentée comme une image mentale, ce qui permet de mémoriser le mot de passe et d'éliminer cette étiquette sur le moniteur de l'ordinateur !

Un mot de passe pour tous les contrôler

Vous ne pouvez pas, bien entendu, obliger tous les utilisateurs à vérifier la complexité de leur mot de passe avec l'outil de vérification des mots de passe sécurisés de Kaspersky Lab (même si vous souhaitez le recommander). Cependant, avec le chiffrement intégral du disque de Kaspersky Lab, vous pouvez compter sur la politique de sécurité du domaine pour définir la complexité des mots de passe. Avec sa prise en charge de l'authentification unique, vous pouvez offrir aux utilisateurs l'option pratique de disposer d'un mot de passe pour le chiffrement intégral du disque et l'authentification du domaine, sans avoir à le saisir deux fois.[3]

Verrouiller la porte et jeter la clé ?

Il y a une autre façon de gérer l'authentification : avec l'utilisation de cartes à puce ou de jetons de sécurité. Bien que cela signifie que vos utilisateurs dépendent de la présence de la clé numérique qu'ils doivent avoir dans leurs poches, cela augmente considérablement les niveaux de sécurité, étant donné que le mot de passe que vos employés saisissent est un mot de passe requis pour déverrouiller le jeton lui-même, plutôt que le vrai système. Le jeton peut être défini pour être automatiquement bloqué après plusieurs tentatives d'authentification infructueuses, exigeant une nouvelle configuration avec une clé passe-partout par un agent de sécurité, ou alternativement la simple émission d'un nouveau jeton. Une solution similaire basée sur l'algorithme peut être adoptée pour l'authentification de l'environnement de pré-démarrage, mais il s'agit clairement d'une option moins pratique, car elle exige que l'ensemble du système ou son stockage soit mis entre les mains de l'agent de sécurité si une reconfiguration est nécessaire.

Ces questions mises à part, le fait est qu'un système crypté avec une authentification par jeton, comme seul moyen d'accès, est pratiquement à l'abri des méthodes de piratage externes, tels que des attaques par dictionnaire ou par force brute.

Pas seulement le chiffrement intégral du disque

Cependant, le vol de données peut aussi se produire de nombreuses façons plus indirectes, sans un accès physique à un ordinateur portable à usage professionnel, à un poste de travail ou à un stockage de données. Les données confidentielles non sécurisées, lors de leur transfert par courrier électronique ou par appareil de stockage amovible sans précautions supplémentaires, risquent d'être interceptées. De plus, il y a toujours un risque d'infection par des programmes malveillants, même pour les réseaux informatiques coupés par un espace d'air virtuel. C'est pourquoi il est important de mettre en œuvre une véritable solution de sécurité informatique multi-niveaux, comprenant non seulement différents types de chiffrement (tels que le chiffrement de disque intégral, au niveau des fichiers et des appareils de stockage amovibles), mais aussi toute une gamme de technologies de sécurité de pointe.

3 Dans la plupart des réseaux informatiques, les mots de passe de domaine sont changés régulièrement, appliqués par des politiques de domaine. Après chaque changement, le mot de passe est automatiquement transmis à l'agent de pré-démarrage de Kaspersky Lab, mais seulement lorsqu'il y a une connexion active entre l'ordinateur en question et le centre de sécurité de Kaspersky Lab. L'utilisateur ne peut pas modifier son mot de passe de domaine depuis l'interface de l'agent de pré-démarrage de Kaspersky Lab.

Mars 15/Global

www.kaspersky.fr | www.securelist.com