



Internet est à votre portée

Livre Blanc

Considérations sur la politique
de sécurité des systèmes
d'information.

Site : <http://www.medialsace.fr>

E-mail : contact@medialsace.fr

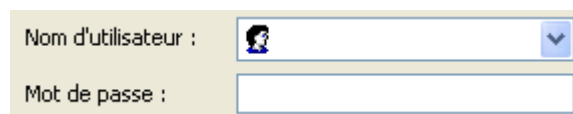
I] Mesures de sécurité

1) Les mots de passe, un point critique

Les mots de passe sont souvent le dernier rempart, souvent négligé soit par manque d'information soit afin de simplifier la vie de l'utilisateur, La faiblesse d'un mot de passe peut permettre bon nombre d'accès non autorisés. Certes ce choix n'est pas facile surtout pour le confort des utilisateurs.

Enormément d'applications, services et systèmes d'exploitations requièrent une authentification pour pouvoir être utilisés. Cette authentification se base sur un couple d' identifiant tel qu'un nom d'utilisateur et un mot de passe.

Par exemple voici une fenêtre d'authentification typique qui permet l'accès à une ressource distante, ici un répertoire contenant des données.



The image shows a typical login form with two input fields. The first field is labeled 'Nom d'utilisateur :' and contains a small icon of a person's head and shoulders. The second field is labeled 'Mot de passe :'. Both fields are empty and have a light blue border.

Même si tous nos systèmes sont parfaitement tenus à jour avec les derniers correctifs de sécurité, mais que nous ne prenons pas garde aux mots de passe, tous nos systèmes peuvent être alors compromis par la découverte d'un mot de passe dit faible.

On entend par mot de passe faible un mot de passe qu'il est facile de deviner, par exemple un prénom, une date, une suite de chiffre ou n'importe quel mot présent dans un dictionnaire (de n'importe quelle langue).

Quel est l'outil dont nous disposons pour tester la solidité d'un mot de passe ? Il se nomme craqueur (version francisée du terme anglais cracker) de mots de passe.

Ce genre de logiciel est souvent utilisé par des pirates débutants afin de pénétrer un système, il devient alors un compagnon idéal pour l'administrateur face à des utilisateurs pas toujours conscients des risques qu'ils font encourir à l'ensemble du réseau.

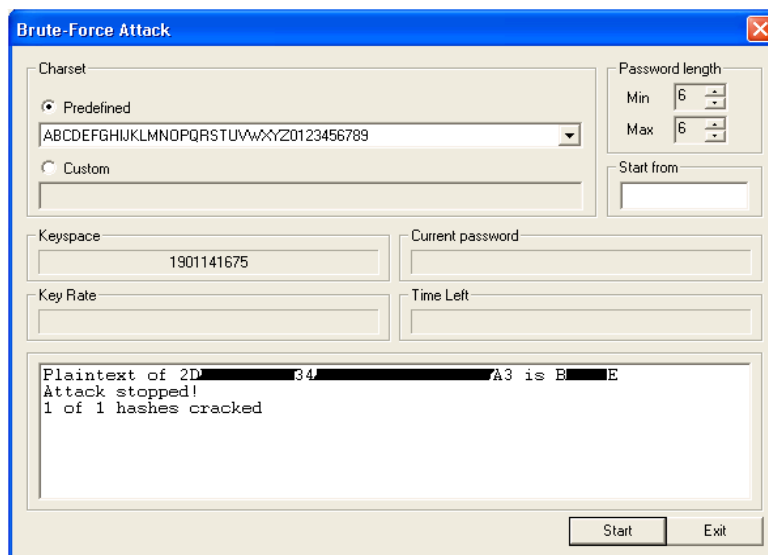
Ces logiciels fonctionnent en général de deux manières : la première consiste à tester des mots de passe présents dans un dictionnaire et à les chiffrer avec un algorithme utilisé par le système visé. On compare ensuite la signature qui en résulte avec la signature du vrai mot de passe. Si les deux concordent le mot de passe est découvert. Exemple : le mot PaSswOrd aura comme signature (ou hash en anglais) cd a5 e8 81 b8 b7 68 89 5f b3 e0 11 2a e9 5e 28 pour un système Windows Xp. En théorie la fonction mathématique qui effectue le chiffrement n'est pas réversible.

La deuxième méthode est celle qui prend le plus de temps et qui s'utilise si aucun mot de passe n'a été trouvé avec l'utilisation d'un dictionnaire : la méthode dite « brute-force » (ou force brute car sa rapidité repose sur la puissance de calcul du processeur) qui teste toutes les possibilités de mots de passe suivant les chiffres, lettres ou symboles que l'on paramètre. Cette technique prend énormément de temps suivant la complexité du mot de passe et peut ne jamais aboutir, du moins pas dans un laps de temps raisonnable.

Utilisons « Cain » un craqueur de mot de passe pour les systèmes Windows et testons la résistance du mot de passe administrateur. L'attaque par dictionnaire ayant échoué, nous passons directement à la méthode de brute-force.

Note : il existe des « craqueurs » pour chaque système d'exploitation : le plus connu est John the ripper.

Voici le résultat d'une telle méthode :



L'attaque a duré en tout et pour tout 3:06 minutes sous un poste Windows Xp pro . Le processeur utilisé est un 2 Ghz.

2) Prise de conscience des utilisateurs

Toute personne qui est amenée à utiliser une authentification par mot de passe devrait être informée des règles de création ou de choix d'un mot de passe. Il est nécessaire de respecter certaines règles unanimement reconnues. Voici une série de consigne non exhaustive afin de ralentir et d'éviter que le mot de passe ne tombe entre des mains malveillantes :

- Le mot de passe ne doit pas se trouver dans le dictionnaire. Exemple : titi, polux, osiris etc.
- Ne pas noter le mot de passe sur un papier ou pire coller un papier sur son écran. (car n'importe qui peut alors prendre connaissance du mot de passe.)
- Surtout ne pas utiliser des mots de passe tels que eric1994, police17, toto2057 ainsi qu'une date de naissance car il existe des craqueurs qui utilisent et testent toutes ces déclinaisons.
- Ne communiquer son mot de passe à personne.
- Le mot de passe doit être un mélange de lettres - majuscules, minuscules -, chiffres et symboles exemple : Pf2!z94TI@
- Utiliser des règles mnémotechniques afin de s'en souvenir. Exemple : « La tante de mon ami est gentille, elle se nomme Caroline » peut devenir Lt2maeg,lsnC
- Mettre en place une politique de changement régulier des mots de passe. (toutes les semaines, mois ou trimestre.)
- Veillez à choisir un mot passe faisant au minimum 8 caractères.

Toutes ces recommandations peuvent par exemple faire l'objet d'une note de service ou d'une réunion afin que tout le personnel de l'entreprise soit informé. Ce livre blanc a pour vocation de vous y aider.

3) Analyse de la politique de sécurité

Toutes les actions et précautions auxquelles nous nous sommes livrées ci-dessus doivent s'inscrire dans une politique de sécurité plus générale. En effet certaines pratiques peuvent faciliter l'obtention ou l'accès aux données sensibles par des tiers non autorisés.

La globalisation de la politique de sécurité peut s'étendre à beaucoup de concept.

Prenons le cas des documents écrits, beaucoup circulent dans une entreprise. Cela va de la fiche de paye, aux factures en passant par l'annuaire interne. Tous les documents nécessaires au fonctionnement de l'entreprise doivent faire l'objet d'une classification. Elle permet de définir le niveau de confidentialité de chacun (comme l'archivage de certains papiers fixé par la loi), en conséquence son cycle de vie est régie par des règles pré-établies.

Le point de sécurité à mettre en avant est ici la destruction du document selon son niveau de classification, par exemple la liste imprimée - pour x raisons - des utilisateurs et de leurs mots de passe doit être classée confidentielle et être détruite par un moyen approprié dès qu'elle devient obsolète. L'enjeu d'une telle politique réside dans le fait que quelqu'un pourrait simplement en fouillant les poubelles de l'entreprise se procurer des renseignements pouvant gravement lui porter atteinte.

Des gestes simples permettent aussi d'éviter bien des tracas, éteindre sa station de travail lorsque l'on quitte son bureau doit en être un. En effet elle pourrait servir à relayer une attaque qui permettrait d'étendre la prise de contrôle du pirate à d'autres machines du réseau (sans parler des économies d'électricité).

La sécurisation des locaux doit être mise en place quand on recherche une sécurité optimale.

Tous les locaux doivent être verrouillés en dehors des horaires de bureau. Les salles informatiques doivent se voir restreindre l'accès au seul personnel dûment autorisé.

Afin d'effectuer un contrôle au niveau des accès, des serrures à cartes et/ou codes ou encore biométriques pourront être installer.

Toujours dans une optique de sécurisation de l'espace de travail, un système de vidéo surveillance peut être mis en place afin de surveiller les installations particulièrement sensibles ou les allées et venues dans les locaux.

Cependant il faut avertir toute personne que l'espace dans lequel elle pénètre, est filmé, cela est une obligation légale tout comme la déclaration en préfecture de la présence d'un tel système. (loi numéro 95-73 du 21 janvier 1995 et décret numéro 96-926 du 17 septembre 1996)

Toutes ces mesures et leur application reposent en grande partie sur le secteur d'activité de l'entreprise. Mais aussi sur l'investissement tant au niveau budgétaire que de l'implication du personnel dans la sauvegarde et les risques qu'encourt le patrimoine numérique de l'entreprise. Avec l'apparition des capacité de stockage de petite taille tels que les clés usb , il devient extrêmement facile de dérober des documents avec la plus grande discrétion.

II] Le facteur humain

Lorsque qu'on s'intéresse au domaine de la sécurité, nous devons considérer que la force d'une chaîne est définie par la force de son maillon le plus faible, dans la plupart des cas il s'agit de l'être humain.

Et c'est bien sur par le facteur humain que beaucoup de problèmes surviennent. Un exemple ? L'administrateur a des horaires de travail, alors que les pirates attaquent de préférence pendant la nuit lorsque les réseaux sont dégagés. Qui ne connaît pas un collaborateur vaniteux et en mal de reconnaissance professionnelle prêt à vendre les secrets de l'entreprise ?

Cependant moins volontairement le personnel peut, à son insu, dévoiler des informations à d'éventuelles personnes mal intentionnées. Prenons le cas d'un simple coup de téléphone, la personne désirant avoir les informations se fait souvent passer pour un collaborateur de la société, pour un supérieur hiérarchique ou encore l'administrateur réseaux . La fuite d'informations peut revêtir plusieurs formes : de la simple collecte sur Internet aux fouilles des poubelles de l'entreprise.

La personne est mise en confiance avant qu'on ne lui demande l'information que l'on recherche et cela peut être n'importe quoi. Ce vol d'informations est très préjudiciable pour l'entreprise.

Il faut, tant que faire se peut vérifier l'exactitude de l'identité de la personne qui réclame une information sensible. Le genre de demande est en grande partie porté sur les mots de passe en prétextant leur perte ou leur oubli.

La personne se sert d'une demande d'aide dans un contexte de supériorité hiérarchique et il est à parier que dans 80 % des cas la demande sera satisfaite. Car qui oseriez mettre en doute la parole d'une personne qui dispose d'une autorité professionnelle supérieure à la nôtre ?

Le manipulateur doit pour que l'attaque réussisse posséder un minimum d'informations sur ce qu'il cherche mais qui lui permettra ainsi de mettre en confiance sa cible. Cette technique porte le nom de *social engineering*. Elle est redoutablement efficace car elle se sert de la nature confiante des personnes (et du comportement humain) qui n'ont jamais été trompées ou qui ne pensent pas l'avoir été.

La formation, la sensibilisation du personnel et le partage des connaissances doivent être les piliers d'une avancée dans un monde de plus en plus hostile. Pour se faire, direction et personnel devront collaborer afin d'assurer la pérennité du patrimoine de l'entreprise.

Le comportement de l'utilisateur est aussi un élément qui se doit d'être pris en considération pour la sécurité de l'ensemble du système d'information .

Les utilisateurs que nous sommes doivent être de nature méfiante quand aux cadeaux venant d'inconnus, notamment en ce qui concerne les e-mails . La propagation virale de l'un des plus connus des virus I LOVE U s'est produite à cause de la curiosité mal placée des utilisateurs. Ils ont ainsi contaminé leur propre machine en ouvrant la pièce jointe qui contenait le virus.

Même si l'actualité a permis d'informer le plus grand nombre contre les risques viraux, il n'en est pas de même pour l'utilisation et le comportement de l'outil informatique dans le cadre du travail. Il faut prendre conscience que vos utilisateurs peuvent avoir un fort impact sur la sécurité de l'ensemble en installant par exemple des programmes qui ne sont pas conçus pour une utilisation dans un cadre professionnel.

Cela peut localement se traduire par l'augmentation du risque d'intrusion sur le réseau de l'entreprise. Sans parler des contraintes légales inhérentes à l'utilisation de certains logiciels d'échange de fichiers par exemple.

Les clients de messagerie instantanée sont un vecteur de fuite d'informations et vulnérabilisent le réseau ; ils devraient donc être prohibés dans le cadre professionnel.

III] Protection physique des données

Les données ou l'information occupent de plus en plus une place prépondérante dans le monde de l'entreprise d'aujourd'hui.

La rapidité de l'obtention et du traitement de l'information fournie par les systèmes d'informations permettent un gain de productivité énorme ainsi qu'un avantage concurrentiel.

Prenons le cas d'une entreprise qui possède un serveur de base de données. Ces données peuvent regrouper toutes sortes d'informations : comptabilité, données clients , fournisseurs etc . Ces informations ont donc une nature vitale pour l'entreprise. Leur perte serait un coup dur pour ne pas dire un coup d'arrêt à l'activité de l'entreprise.

Nous allons exposer les mesures les plus simples et/ou basiques concernant la protection physique des données.

- Un onduleur est une alimentation électrique stabilisée et sans interruption. Il permet de garder la tension d'alimentation de l'installation électrique toujours constante et prévient les coupures (et les micro-coupures) de courant . Il possède des batteries pour garantir la continuité de service des serveurs ou des ordinateurs en cas de coupure électrique prolongée. Leur prix est souvent en relation avec leur autonomie et leur niveau de protection. Tous les composants électronique sont sensibles aux sautes de tension entraînant leur

destruction ou un endommagement des circuits.

L'asservissement de gestion de l'alimentation avec le serveur permet d'arrêter " proprement " ce dernier lorsque que l'onduleur n'a plus de batteries.

Si ce type de protection électrique n'est pas présente, vous risquez en cas de variation de tension ou de coupure(s) une corruption des données, le crash du système ou pire une panne matérielle.

- La technologie RAID

Le mot RAID désigne une technologie permettant de stocker des données sur de multiples disques dur, en général de manière redondante afin d'améliorer les performances mais surtout de résister aux pannes.

La résistance aux problèmes de disques est résolue en dupliquant les données sur deux disques.

En cas de défaillance d'un disque il suffit de le remplacer et la reconstruction des données est automatique.

- Sauvegarde régulières

Elle permet une restauration de vos données vitales.

Vous sous-estimez peut- être la valeur de vos données jusqu' au jour où votre activité est paralysée .

Plus de comptabilité, plus de gestion des clients, factures ... la perte d'argent due au temps de gestion de l'incident informatique et donc de l'interruption de service doit être un facteur déterminant dans le choix de votre solution de sauvegarde. L'une des solutions les plus efficaces consiste en une sauvegarde journalière automatisée avec rotation des bandes magnétiques.

- Réplication de serveurs

Cette solution a un coût très élevé car il s'agit de dupliquer le serveur entier, tant au point de vue du système que des données. En cas de l'arrêt de l'un des deux, la continuité est assurée.

Le modèle utilisé est celui du maître et de l'esclave. Le serveur maître fournit et enregistre les données saisies par exemple et les données sont dupliquées sur l'esclave. Si le maître venait à tomber en panne l'esclave prendrait le relais sans pertes de données. Une fois le serveur principal rétabli, les données se synchronisent.

De part son coût, cette solution est réservée aux grandes entreprises, groupes ou filiales.

CONCLUSION

La sécurité des données et des systèmes informatiques reposent sur des solutions à la fois matérielles (disques durs redondants, sauvegardes régulières etc) et logicielles (Pare-feu, anti-virus...). Quoi que le choix de solution Open Source réduit de manière significative le coût de la couche logicielle.

Nous pouvons dépenser un budget colossal afin de posséder les meilleures technologies, elles ne le seront que pour une courte durée. Le coût de la sécurité est exponentielle sans **jamais** atteindre le saint graal de l'absolu.

La vision de la sécurité dépend beaucoup des contraintes liées à l'environnement et au secteur d'activité de l'entreprise. Il est important de trouver un bon compromis entre la réalité économique, les techniques disponibles et leur mise en oeuvre, sachant que cette adaptation aura un paramètre invariant : son constant dynamisme. La sécurité est une problématique perpétuelle qui prend une part de plus en plus importante dans le métier d'administrateur.