EXAMEN PROFESSIONNEL D'AVANCEMENT DE GRADE DE TECHNICIEN PRINCIPAL TERRITORIAL DE 1ère CLASSE

SESSION 2017

ÉPREUVE DE RAPPORT AVEC PROPOSITIONS

ÉPREUVE D'ADMISSIBILITÉ :

Rédaction d'un rapport technique portant sur la spécialité au titre de laquelle le candidat concourt. Ce rapport est assorti de propositions opérationnelles.

Durée : 3 heures
Coefficient : 1

SPÉCIALITÉ : INGÉNIERIE, INFORMATIQUE ET SYSTÉMES D'INFORMATION

À LIRE ATTENTIVEMENT AVANT DE TRAITER LE SUJET :

- Vous ne devez faire apparaître aucun signe distinctif dans votre copie, ni votre nom ou un nom fictif, ni initiales, ni votre numéro de convocation, ni le nom de votre collectivité employeur, de la commune où vous résidez ou du lieu de la salle d'examen où vous composez, ni nom de collectivité fictif non indiqué dans le sujet, ni signature ou paraphe.
- Sauf consignes particulières figurant dans le sujet, vous devez impérativement utiliser une seule et même couleur non effaçable pour écrire et/ou souligner. Seule l'encre noire ou l'encre bleue est autorisée. L'utilisation de plus d'une couleur, d'une couleur non autorisée, d'un surligneur pourra être considérée comme un signe distinctif.
- L'utilisation d'une calculatrice de fonctionnement autonome et sans imprimante est autorisée.
- Le non-respect des règles ci-dessus peut entraîner l'annulation de la copie par le jury.
- Les feuilles de brouillon ne seront en aucun cas prises en compte.

Ce sujet comprend 27 pages.

Il appartient au candidat de vérifier que le document comprend le nombre de pages indiqué.
S'il est incomplet, en avertir le surveillant.

Vous êtes technicien principal territorial de 1ère classe, chef de projet à la Direction des Systèmes d'Informations, du département de Technidept.

Confronté aux questions récurrentes de la sécurité informatique, le Directeur des Systèmes d'Information souhaite mettre en œuvre une démarche d'authentification forte.

Dans un premier temps, le Directeur des Systèmes d'Information vous demande de rédiger à son attention, exclusivement à l'aide des documents joints, un rapport technique sur l'authentification forte dans les collectivités territoriales.

10 points

Dans un deuxième temps, il vous demande d'établir un ensemble de propositions opérationnelles pour mettre en œuvre une authentification forte au sein des services de Technidept.

10 points

Pour traiter cette seconde partie, vous mobiliserez également vos connaissances.

Liste des documents :

Document 1 **« Authentification forte : protéger l'accès à ses services en ligne ».**
Jean-François PILLOU - www.CommentCaMarche.net - Mai 2015 - 4 pages.

Document 2 **« Authentification forte. Livre blanc »** (Extrait).
Livre Blanc HID - www.hidglobal.com - Avril 2014 - 4 pages.

Document 3 **« Département de l'Aisne : Regards croisés sur l''authentification forte dans les collectivités, une obligation légale ».**
T. Bettini (Département de l'Aisne) et H. Fortin (Ilex International) - www.globalsecuritymag.fr - Juin 2015 - 3 pages.

Document 4 **« L'authentification dans le monde moderne ?**
Livre blanc sur les 4 meilleures pratiques d'adaptation au changement de paradigme dans le monde informatique ».
Safe Net - The data protection compagnie - www.bitpipe.fr - Décembre 2012 - 5 pages.

Document 5 **« État des lieux : les solutions d'authentification-forte (2FA) ».**
Le blog Synetis Yann - www.synetis.com - Octobre 2015 - 4 pages.

Document 6 **« Signature électronique : clé de voûte de la transformation digitale ».**
Patrick Duboys - www.journaldunet.com - Décembre 2014 - 3 pages.

Document 7 **« Après les attentats, les collectivités locales découvrent la cybersécurité ».**
Guillaume BREGERAS - www.lesechos.fr – Janvier 2015 - 2 pages.

DOCUMENT 1

« Authentification forte : protéger l'accès à ses services en ligne ».

Jean-François PILLOU - www.CommentCaMarche.net - Mai 2015

De nombreux fournisseurs de services en ligne proposent aujourd'hui l'authentification forte (« en deux étapes » ou « à deux facteurs ») à leurs utilisateurs pour sécuriser l'accès à leur compte.

Un procédé qui protège contre le vol de mot de passe et ses risques : comme l'usurpation d'identité ou le vol de données. En quoi consiste l'authentification à deux facteurs ? Quels sont ses avantages et comment l'activer sur les services les plus utilisés sur le web ? Explications.

Qu'est-ce que l'authentification à deux facteurs ?

Sur le web, l'authentification à deux facteurs (ou authentification forte) est un procédé faisant appel à deux étapes de vérification pour sécuriser l'accès à un profil personnel rattaché à un service de type messagerie, espace de stockage, réseau social, etc.

Après une première étape d'identification (couple identifiant/mot de passe), vient une étape d'authentification qui conditionne l'accès au compte d'utilisateur. Elle nécessite de renseigner -dans un formulaire- un mot de mot de passe de confirmation à usage unique envoyé :

- par SMS sur téléphone,
- par mail,
- sur une application d'authentification pour smartphone.

Se protéger contre les accès non autorisés

La mise en place d'une authentification forte vise donc à protéger les utilisateurs contre :

- l'usurpation d'identité (par l'ingénierie sociale, l'installation de logiciels malveillants),
- la fuite accidentelle de données d'identification (ex : perte de matériel),
- la perte de données d'identification consécutives au piratage d'un service en ligne.

L'authentification forte protège contre les tentatives de connexion à des services en ligne en provenance de lieux/ou depuis des terminaux/navigateurs inhabituels.

Pour quels utilisateurs ?

- Les professionnels accédant à des documents sensibles en ligne (ex : documents stockés sur DropBox).
- les utilisateurs nomades exposés à des risques de vol de mots de passe : (ex : utilisation de hotspots WiFi non sécurisés)
- Aux entreprises présentes sur les réseaux sociaux (Facebook, Twitter), qui s'exposent à des risques en termes d'image si leur accès est usurpé et leur compte détourné.

Authentification à deux facteurs : avantages pratiques

- Mise en oeuvre facile
- Désactivable à tout moment
- L'authentification à deux facteurs est paramétrable. Certains fournisseurs (ex : Microsoft, Google) permettent de l'activer à chaque connexion, ou seulement une seule fois : cette dernière option évite d'avoir à valider les deux étapes lorsqu'on se connecte depuis un terminal utilisé régulièrement, qui est donc reconnu comme « légitime ».

Authentification forte sur les services de Google : Gmail, Drive, etc.

La procédure suivante est valable pour renforcer la sécurité d'accès aux différents services connectés de Google : Gmail, Docs (Drive), Youtube, etc. :

- Paramètres de compte,
- sélectionner "Sécurité",
- puis, "Validation en deux étapes" > paramètres,
- la validation en deux étapes requiert un numéro de téléphone : un code est envoyé par SMS pour valider la connexion à un compte : soit à chaque tentative, soi une seule fois par ordinateur.

Authentification à deux facteurs pour les services Microsoft

Outlook.com, Skype et Skydrive

Pour activer l'authentification en deux étapes sur les différents services de Microsoft, il est nécessaire de disposer d'un compte Microsoft valide.

- Se connecter à son compte Live
- Sous « Mot de passe et informations de sécurité », cliquer sur « Modifier les informations de sécurité ». Cette étape nécessite l'insertion d'un code : il peut être envoyé par mail à une adresse de messagerie de récupération (de secours) liée à son compte Microsoft.
- Une fois le code entré, accéder à la page « Informations de sécurité » : cliquer sur « Configurer la vérification en deux étapes ».
- L'étape de confirmation précédente peut être redemandée (insertion d'un code),
- enfin sélectionner un deuxième facteur d'authentification dans la liste proposée : numéro de téléphone, adresse de messagerie de secours (différente de celle qui est déjà renseignée), ou application d'authentification forte (pour smartphones).
- Un code de sécurité supplémentaire est ensuite demandé à chaque connexion au compte Microsoft (pour accéder à Outlook.com, Skydrive, ou Skype si le compte a été créé avec un compte MS). Il peut être désactivé au cas par cas pour ne pas avoir à le renseigner à chaque connexion depuis le même appareil.

Une fois la vérification en deux étapes activée :

- Une page supplémentaire apparaît à chaque connexion sur un appareil qui n'est pas approuvé.
- Sur cette page supplémentaire : entrer un code de sécurité pour se connecter.

Tutoriel « la vérification en deux étapes » sur le site de Microsoft

Activer l'authentification à deux facteurs sur LinkedIn

- Compte > préférences : cliquer sur « Gérer les paramètres de sécurité »
- Sous la section « Vérification en deux étapes », cliquer « activer ».

- Un numéro de téléphone mobile est requis pour recevoir un code de vérification.
- Cliquer sur « envoyer le code ».
- Entrer le code envoyé par SMS dans la zone de texte, cliquer sur vérifier, puis « terminé ».

Une fois activée, l'authentification à deux facteurs est requise pour toute connexion depuis un terminal qui n'est pas habituellement utilisé pour ce connecter à son compte d'utilisateur. Une fois celui-ci enregistré, la procédure n'est plus nécessaire. L'option peut être désactivée à tout moment.

Authentification à deux facteurs sur Facebook

- Sur l'icône « engrenage » en haut à droit : sélectionner "compte",
- puis en haut à gauche "sécurité",
- sélectionner "Approbations de connexion" (modifier),
- cocher la case "Demander un code de sécurité lors de l'accès à mon compte à partir de navigateurs non reconnus",
- ajouter un numéro de téléphone mobile pour activer les approbations de connexion,
- enregistrer l'appareil utilisé pour se connecter régulièrement (sauf s'il est partagé avecd'autres utilisateurs).

Authentification à deux facteurs sur Twitter

- Cliquer sur votre photo de profil en haut à droite : sélectionner "Paramètres"
- Ensuite dans le menu de gauche : sélectionner "Sécurité et confidentialité"
- Sélectionner l'option de votre choix dans "Vérification de connexion"
- Dans le cas de la vérification par SMS, il vous faudra ajouter un numéro de téléphone à votre compte.
- Dans le cas de la vérification de connexion sur l'application Twitter, il vous faudra la configurée depuis votre application mobile en accédant à "Paramètre" -> "Sécurité" sur celle-ci.
- Enregister les modifications.

Désormais, il vous sera requis la confirmation par un code reçu par SMS ou via l'application mobile à chaque connexion.

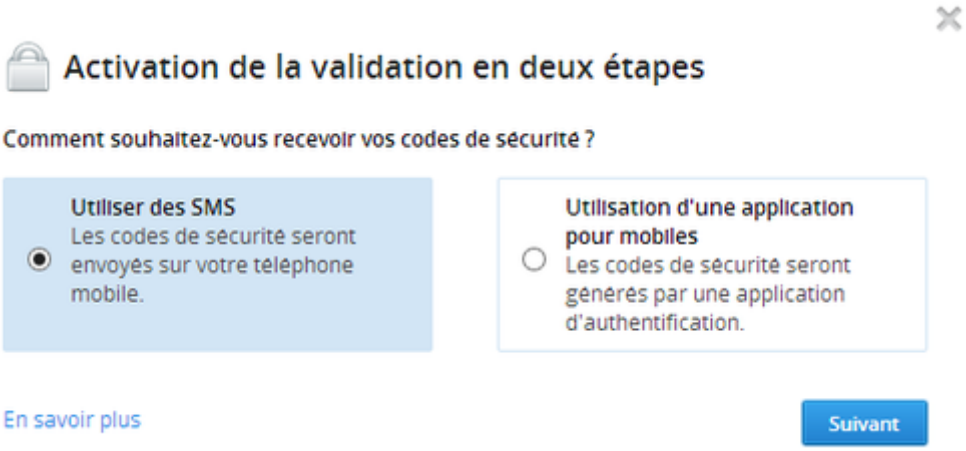
Authentification à deux facteurs sur WordPress
Elle repose sur une validation en deux étapes au moyen d'un smarpthone. Pour les blogs hébergés sur Wordpress.com :

- Rendez-vous dans les paramètres de sécurité,
- télécharger et installer l'application Google Authenticator (disponible sur Android, iOS et BlackBerry),
- un code d'accès est généré toutes les 30 secondes : il permet de valider sa connexion à son blog.

Pour les blogs conçus avec WordPress : installer le plugin Google Authenticator

Authentifcation à deux facteurs sur Dropbox

- Sélectionner le compte (via l'identifiant en haut),
- cliquer sur l'onglet "sécurité",
- puis sélectionner "Validation en deux étapes > modifier",
- l'activation nécessite de saisir à nouveau son mot de passe,
- deux possibilités : la validation par l'envoi d'un SMS, ou par l'intermédiaire d'une application mobile d'authentification : GoogleAuthenticator(Android/iPhone/BlackBerry)
  Amazon AWS MFA (Android), Authenticator (Windows Phone 7).



DOCUMENT 2

« Authentification forte. Livre blanc » (Extrait).

Livre Blanc HID - www.hidglobal.com - Avril 2014

LIVRE BLANC

Comment obtenir le niveau de protection des identités dont vous avez besoin, de façon à la fois pratique et abordable

Résumé opérationnel

Accommoder tous les différents besoins en matière d'accès logique de tous les utilisateurs, tout en verrouillant simultanément vos ressources pour les protéger contre les menaces, est un défi constant.

Pour être sûr que vos utilisateurs sont bien ceux qu'ils prétendent et qu'ils gèrent efficacement leur accès à vos ressources, vous avez besoin d'une solution de protection des identités complète, sur laquelle repose l´authentification forte.
Toutefois, l'émission et la gestion continue des moyens d'identification des utilisateurs, sur tous les divers appareils, des cartes à puce aux téléphones mobiles que vous devez prendre en charge, pour toutes les applications et ressources auxquelles vos utilisateurs peuvent vouloir accéder, peuvent poser leurs propres problèmes. De ce fait, il vous faut une solution d'authentification forte qui facilite l'émission et la gestion des moyens d'identification en vue de fournir différents niveaux d'accès d'une façon commode pour l'utilisateur. Toute procédure qui ne respecterait pas ce minimum aurait un impact négatif sur l'efficacité de la solution complète.

Sommaire

Le besoin d'une authentification forte dans l'entreprise d'aujourd'hui

Les utilisateurs sont de plus en plus dispersés géographiquement, mobiles et variés, ce qui oblige de nombreuses entreprises à s'intéresser aux moyens d'établir la confiance dans l'identité des utilisateurs et de contrôler leur accès en conséquence. Par le passé, la plupart d'entre elles se concentraient sur les défenses périphériques, mettant en place des contrôles pour déterminer qui pouvait entrer dans le bâtiment, avec des systèmes d'accès physique, et qui pouvait entrer sur le réseau grâce à des pare-feux et des VPN. Une fois à l'intérieur, les utilisateurs avaient un accès quasiment illimité à toutes les applications et ressources disponibles dans ces sites et ces réseaux.

À présent, reconnaissant les menaces que les utilisateurs représentent « à l'intérieur des murs » (81 % des entreprises ont en effet subi une violation des données du fait de salariés ou autres personnes se trouvant sur place, aussi bien par négligence que par malveillance) et observant que les murs, eux-mêmes, tombent du fait de la nature mondiale et dynamique des entreprises actuelles, de nombreuses entreprises revoient leur approche en matière d'accès logique.

Si vous êtes comme la plupart des entreprises, vous luttez pour accommoder simultanément les différents besoins de tous vos différents utilisateurs et vous cherchez à minimiser les risques que pose leur accès à votre organisation, ce qui est rendu compliqué par l'évolution permanente du panorama des menaces et le nombre d'utilisateurs. Les attaques continuent d'évoluer et deviennent de plus en plus complexes, comme le montre la montée des menaces avancées et persistantes qui utilisent des logiciels malveillants personnalisés pour mener des attaques ciblées à long terme contre votre organisation. Parallèlement, les utilisateurs qui ont besoin d'accéder aux informations et aux ressources, ne se limitent pas aux salariés et incluent un large éventail de consultants, contractants, fournisseurs, partenaires, fournisseurs et clients.

Tous ces utilisateurs veulent pouvoir accéder à ce dont ils ont besoin, peu importe d'où ils viennent, en utilisant l'appareil de leur choix, y compris leurs téléphones personnels, ordinateurs portables et tablettes (BYOD). Ces variables peuvent accroître les risques pour votre environnement si vous ne faites pas attention. Ce qu'il vous faut, c'est une méthode permettant de s'assurer de l'identité de tous ces utilisateurs différents, puis de contrôler de façon adéquate leur accès tout au long de leurs déplacements dans l'organisation.

Appliquer une authentification forte à chaque application est l'un des moyens les plus efficaces pour obtenir la productivité dont votre activité à besoin, tout en réduisant les risques pour votre entreprise. En assurant les applications et les ressources de données de l'entreprise et basées sur le cloud, qu'elles soient sur un ordinateur portable ou un téléphone mobile, vous pouvez gérer efficacement l'accès et sécuriser vos systèmes d'informations.

Définir l'authentification forte pour traiter les défis posés par les solutions traditionnelles

Une authentification forte, parfois appelée authentification avancée ou authentification double facteur, va bien au-delà d'un simple mot de passe d'authentification. Elle requiert des facteurs supplémentaires pour établir que l'utilisateur est qui il est. Il peut s'agir de quelque chose que l'utilisateur sait, comme un mot de passe unique ou un numéro d'identification personnel (PIN) ; quelque chose que l'utilisateur a, comme une carte à puce, un token ou un téléphone portable ; ou même quelque chose que le système d'authentification collecte, comme une connaissance des fraudes et des comportements, qui sert à augmenter le niveau de sécurité de l'authentification.

Pourquoi est-ce important ? Les hackers continuent de cibler les moyens d'identification des personnes qui se trouvent à l'intérieur des bâtiments parce qu'ils donnent à l'attaquant un accès aux sites et au réseau, leur permettant de se « fondre dans la masse », de sorte qu'ils peuvent aller et venir dans l'entreprise sans se faire détecter. De récentes études indiquent que près de 50 % des violations de données exploitent les systèmes d'identification volés ou faibles. Cela dit, il est facile de voir à quel point la solidité croissante des authentifications de vos utilisateurs peuvent vous aider à renforcer la sécurité générale de l'entreprise.
La réalité repose sur l'utilisation de mots de passe statiques traditionnels qui, bien que pratiques, ne sont pas suffisants pour protéger contre les menaces dynamiques actuelles ; les outils de capture de frappe, les attaques d'hameçonnage, les écoutes et même le fait de deviner peut facilement servir à les briser. Les mots de passe à usage unique (OTP) et tokens offrent une sécurité supérieure, car le mot de passe qu'ils génèrent n'est valide que pour une seule session ou transaction, mais s'ils sont implémentés de façon incorrecte, ils peuvent créer d'autres problèmes. De nombreuses solutions héritées ne vous donnent pas de contrôle sur la clé du token ; au lieu de cela, les clés sont hébergées dans les bases de données du fournisseur, ce qui signifie qu'une violation chez celui-ci peut endommager la sécurité de votre entreprise.

De plus, les solutions héritées qui partent du principe qu'une fois que vous êtes entré, il n'y a aucun problème, ne sont pas suffisamment complètes ou polyvalentes pour prendre en considération le rôle de l'utilisateur, le lieu et le type d'accès en vue d'établir la confiance et de garantir l'accès

à un vaste éventail d'applications dans l'entreprise et dans le cloud. Il ne suffit plus d'utiliser une authentification forte quand vous entrez dans le bâtiment ou le réseau pour la première fois. Comme indiqué, il n'y a plus de périmètre défendable. Une authentification forte doit être étendue dans toute l'organisation pour inclure l'accès aux bureaux, serveurs, téléphones portables, données, ainsi qu'aux applications d'entreprise et dans le cloud, d'une façon qui vous permette de renforcer la sécurité générale et la responsabilité de votre environnement.

Toutefois, l'émission et la gestion continue des moyens d'identification des utilisateurs, sur tous les divers appareils, des cartes à puce aux téléphones mobiles, pour toutes les applications et ressources auxquelles ils peuvent vouloir accéder, peuvent représenter un processus manuel chronophage. Cela se complique encore plus lorsqu'il y a plusieurs types de moyens d'identification, pour l'accès physique et logique, et différents systèmes d'identification et d'authentification. Il faut un processus unique, reposant sur un système de gestion des utilisateurs et des moyens d'identification consolidés, capable d'émettre et de gérer les systèmes d'identification de tous vos utilisateurs pour leur accorder un accès adéquat à tout, des bâtiments aux applications dans le cloud, via différents facteurs de forme, depuis des cartes à puce jusqu'à des téléphones portables.

Polyvalence du dispositif ActivID en un clin d'oeil

- **Prise en charge des périphériques :** smart phones, tablettes, ordinateurs portables, etc.
- **Méthodes d'identification :** hard tokens (jetons matériels) et soft tokens (jetons logiciels) de mot de passe à usage unique, cartes à puce, périphériques d'identification, authentification adaptative, mécanismes de détection des fraudes, et mécanismes hors-bande (SMS ou e-mail) pour une authentification au niveau des transactions
- **Applications :** Entreprises, Cloud, etc., comme Windows, Salesforce.com, SAP, Oracle, Google Apps, etc.

Critères pour une authentification forte efficace - sans compromis
Une solution d'authentification forte efficace doit pouvoir ajouter de la sécurité sans accroître les coûts ou la complexité. Pour les environnements professionnels actuels, seule une solution d'authentification forte, facile à utiliser et simple à gérer a une chance de fonctionner avec l'ensemble des utilisateurs que votre organisation doit prendre en compte pour vous protéger contre les nombreuses attaques connues et à venir. Vous avez besoin d'une solution qui vous fournit :

Authentification forte :

• **Double facteur ou plus :** augmente le niveau de confiance que vous avez dans les identités de vos utilisateurs, de sorte que vous puissiez leur octroyer un accès adéquat.

• **Différents niveaux d'accès :** basés sur les risques associés aux différents types d'utilisateurs et de transactions. Vous devriez pouvoir être en mesure de fournir des capacités de sécurité à couches multiples et transparentes pour accroître considérablement votre sécurité, sans que cela n'ait d'incidence sur l'expérience des utilisateurs (au moins pas ceux qui se connectent à partir de leurs périphériques et lieux de confiance). Cela peut être obtenu grâce à des solutions capables de :
• **Détection avancée des fraudes :** tenez compte de facteurs tels que la situation géographique et les informations relatives aux périphériques quand vous authentifiez des utilisateurs, afin de pouvoir limiter l'accès à des périphériques de confiance, dans des pays de confiance.
Sinon, les utilisateurs peuvent être conviés à utiliser une méthode d'authentification supplémentaire plus sûre, comme un mot de passe unique envoyé par SMS, en cas de connexion à partir de périphériques ou de sites qui ne figurent pas sur la liste de confiance.

• **Analyse continue des comportements :** pour une authentification continue et une amélioration des capacités de recherche de preuves, à l'aide de l'analyse comportementale des interactions d'un utilisateur avec les applications. L'activité de l'utilisateur est constamment surveillée et analysée, pour savoir comment un utilisateur particulier se comporte, de sorte

que les conclusions tirées de ce comportement puissent être détectées et signalées, sans avoir d'incidence sur l'expérience de l'utilisateur ou mettre en danger la confidentialité.
Si une déviation se produit (par exemple, si quelqu'un a pris la main sur l'ordinateur), l'application peut choisir de redemander à l'utilisateur de s'authentifier et/ou ajouter un événement à une base de données d'audit pour étude ultérieure. Cette méthode peut en fait servir à réduire le nombre de tentatives nécessaires pour qu'un utilisateur s'authentifie auprès d'un système afin d'améliorer son confort.

Gestion simplifiée :

• **Rapide à déployer et à administrer :** il devrait être facile d'obtenir que la solution soit en place et fonctionne, sans ajouter de complexité ou de coûts inutiles. Dans l'idéal, elle devrait vous permettre d'avoir une vue groupée pour simplifier l'émission des moyens d'identification et la gestion continue de vos solutions de protection des identités afin de garantir qu'elles prennent en charge votre position en matière de sécurité (par exemple, il devrait être facile d'identifier et de révoquer des moyens d'identification, de façon à ce que vous n'ayez pas de moyen d'identification actif pour un salarié qui a quitté votre entreprise).

• **Complet :** système de gestion des identifications simple, capable de gérer vos moyens d'identification des utilisateurs sur plusieurs dispositifs, comme des cartes à puce et téléphones portables, et le cycle de vie continu de ces moyens d'identification et dispositifs. Dans l'idéal, il devrait vous permettre d'accéder aussi bien à vos actifs physiques (bâtiments) que logiques (applications et ressources d'entreprise et dans le cloud) et fournir une vue groupée unique de tous vos systèmes de protection des identités.

• **Intégration facile :** la solution doit être en mesure de s'intégrer aux outils de gestion continue que vous utilisez normalement pour créer une interface utilisateur consolidée et stable afin d'administrer l'authentification et les systèmes d'identification de sécurité des utilisateurs.

Confort de l'utilisateur :

• **Facile à utiliser :** ne devrait pas gêner les flux de travail. Dans l'idéal, la solution devrait utiliser les badges d'identification existants, cartes à puce ou téléphones portables des utilisateurs pour étendre l'accès sécurisé aux ressources physique et logique dont l'utilisateur a besoin.

• **Continuité :** ne devrait pas provoquer de retard indu pour les applications d'entreprise et basées sur le cloud dont les utilisateurs ont besoin pour mener leurs activités.

DOCUMENT 3

« Département de l'Aisne : Regards croisés sur l'authentification forte dans les collectivités, une obligation légale ».

T. Bettini (Département de l'Aisne) et H. Fortin (Ilex International) - www.globalsecuritymag.fr - Juin 2015

La mise en place d'une solution d'authentification forte au sein d'une collectivité est, dans une grande majorité des cas, perçue comme une problématique technique par la DSI, qui cantonne trop souvent ce type de projet au simple remplacement du login/mdp devenu obsolète. Dans un contexte de restriction budgétaire au sein des collectivités, la DSI peine alors à justifier un tel projet, jugé trop coûteux et relégué au second plan des priorités.

Cependant, au-delà de sa dimension technique, la mise en place d'une solution d'authentification forte garantit sécurité et traçabilité des accès au système d'information. Ceci permet ainsi aux collectivités d'être conformes aux législations en vigueur et, notamment, aux obligations de protection des données à caractère personnel encadrées par la CNIL.

Nombreuses sont les collectivités qui valident la déclaration informatique et libertés sans maîtriser totalement les obligations qui en découlent. Le champ d'applications de cette loi est très large et concerne la majorité des traitements ou fichiers mis en œuvre par les collectivités locales pour gérer leurs nombreux services : état civil, listes électorales, inscriptions scolaires, action sociale et autres services à la population, etc.

« La création et le traitement de données personnelles (numéro d'identifiant, nom, adresse, numéro de téléphone...) sont soumis à des obligations destinées à protéger les libertés individuelles et la vie privée des personnes fichées », indique Thierry Bettini directeur commercial d'Ilex International.

Certaines données sont particulièrement sensibles selon les domaines et doivent faire l'objet d'autorisations spécifiques auprès de la CNIL. Seules les personnes habilitées doivent avoir accès à certaines informations.

Avec la transformation digitale, les collectivités locales gèrent de plus en plus de données personnelles mais en réalité, combien d'entre elles savent dire aujourd'hui avec exactitude qui a accès à quoi ?

Les contrôles réalisés par la CNIL montrent que de nombreuses collectivités ne respectent pas certaines règles de base de la loi informatique et libertés. Dans la majorité des cas, ces manquements résultent d'une méconnaissance de la loi ou de négligences, mais les infractions n'en restent pas moins réelles. ***« Les décideurs et responsables locaux doivent en prendre conscience car ils sont directement visés en cas de non-respect des dispositions de la loi : leur responsabilité juridique peut être engagée. Ils peuvent même, dans certains cas, être pénalement sanctionnés (peine de cinq ans d'emprisonnement et 300 000 € d'amende) »,*** souligne Hervé Fortin, RSSI et CIL du Département de l'Aisne.

L'authentification forte, une garantie de conformité avec le cadre réglementaire régi par la CNIL

Le RSSI/DSI d'une collectivité locale doit homogénéiser et renforcer l'authentification sur les applications dont il contrôle et trace les accès. Il pourra se dégager ainsi de toute sanction juridique relative à la confidentialité des données traitées au sein de la collectivité.

La responsabilité judiciaire du RSSI/DSI directement engagée

Nombreuses sont les collectivités qui valident la déclaration informatique et libertés sans maîtriser totalement les obligations qui en découlent. En effet, la loi informatique et libertés du 6 janvier 1978 (modifiée en août 2004) définit les principes à respecter lors de la collecte, du traitement et de la conservation des informations relatives à des personnes physiques. Le champ d'applications de cette loi est très large et concerne la majorité des traitements ou fichiers mis en œuvre par les collectivités locales pour gérer leurs nombreux services : état civil, listes électorales, inscriptions scolaires, action sociale et autres services à la population, etc.

« La création et le traitement de données personnelles (numéro d'identifiant, nom, adresse, numéro de téléphone...) sont soumis à des obligations destinées à protéger les libertés individuelles et la vie privée des personnes fichées », indique Thierry Bettini directeur commercial d'Ilex International. Celles-ci varient selon la nature du fichier et la finalité des informations recueillies : déclaration normale ou simplifiée ou demande d'autorisation. Il existe aussi des obligations de sécurité, de confidentialité et d'information.

Certaines données sont particulièrement sensibles selon les domaines et doivent faire l'objet d'autorisations spécifiques auprès de la CNIL. C'est le cas notamment des informations traitées dans le domaine social, où la confidentialité est essentielle, comme par exemple le traitement de signalement « enfance en danger ». Seules les personnes habilitées doivent avoir accès à certaines informations. Avec la transformation digitale, les collectivités locales gèrent de plus en plus de données personnelles mais en réalité, combien d'entre elles savent dire aujourd'hui avec exactitude qui a accès à quoi ?

Les contrôles réalisés par la CNIL montrent que de nombreuses collectivités ne respectent pas certaines règles de base de la loi informatique et libertés. Dans la majorité des cas, ces manquements résultent d'une méconnaissance de la loi ou de négligences, mais les infractions n'en restent pas moins réelles. « Les décideurs et responsables locaux doivent en prendre conscience car ils sont directement visés en cas de non-respect des dispositions de la loi : leur responsabilité juridique peut être engagée. Ils peuvent même, dans certains cas, être pénalement sanctionnés (peine de cinq ans d'emprisonnement et 300 000 € d'amende) », souligne Hervé Fortin, RSSI et CIL du Département de l'Aisne.

L'authentification forte, une garantie de conformité avec le cadre réglementaire régi par la CNIL

Pour faire face à ces contraintes réglementaires renforcées, la maîtrise et la sécurité des accès logiques doivent rester la priorité des collectivités. « Renforcer les mécanismes d'authentification et les règles de contrôle d'accès logiques aux applications du SI permet d'éviter toute faille/fraude », explique Thierry Bettini. Ainsi, il est primordial de proposer plusieurs mécanismes d'authentification, à n facteurs ('ce que je sais', 'ce que j'ai', 'ce que je suis'), en fonction des usages des agents (par exemple certains peuvent utiliser des cartes à puces, d'autres des clés USB, etc.), et du niveau de criticité des applications accédées. Certaines solutions packagées sont déjà proposées par les intégrateurs et éditeurs de logiciels qui permettent de répondre à ces problématiques efficacement.

Une fois l'agent authentifié, il est possible de contrôler les droits d'accès selon des critères divers et variés tels qu'un niveau d'authentification primaire (n facteurs), un créneau horaire, un profil utilisateur récupéré dans l'annuaire d'entreprise, etc. Et de préciser que « les authentifications, autorisations et délégations des agents doivent impérativement être tracées afin de garantir la bonne conformité avec les législations en vigueur et répondre aux exigences d'audit ».

Le RSSI/DSI d'une collectivité locale doit homogénéiser et renforcer l'authentification sur les applications dont il contrôle et trace les accès. Il pourra se dégager ainsi de toute sanction juridique relative à la confidentialité des données traitées au sein de la collectivité.

« Quelles que soient leurs tailles, toutes les collectivités sont concernées » conclut Hervé Fortin. En revanche, toutes ne mesurent pas les engagements qu'elles prennent en se déclarant conformes, ni les risques encourus en cas de contrôle de la CNIL. Une vraie prise de conscience des obligations légales est nécessaire, comme c'est le cas dans d'autres secteurs (ex : secteur bancaire) afin de faire de la gestion des accès une véritable priorité.

DOCUMENT 4

« L'authentification dans le monde moderne ? Livre blanc sur les 4 meilleures pratiques d'adaptation au changement de paradigme dans le monde informatique ».

Safe Net - The data protection compagnie - www.bitpipe.fr - Décembre 2012

Basé sur le webcast, "Le Token est mort ! Vive le Token!"

Ce livre blanc s'appuie sur les connaissances partagées lors d'un webcast auquel ont participé Mike Rothman, analyste et PDG de Securosis, cabinet de recherche et de conseil en sécurité de l'information, Andrew Moloney, consultant en sécurité indépendant, Doron Cohen, vice-président de la division Technologie au sein de la direction technique de SafeNet et par Mike Smart, directeur des solutions chez SafeNet. Intitulé" Le Token est mort ! Vive le Token !", ce webcast est disponible sur demande et offre une multitude de conseils pratiques pour vous aider à adapter votre système d'authentification aux défis actuels.
Pour plus d'informations ou pour voir ce webcast, rendezvous sur

http://www.brighttalk.com/webcast/6319/31581

Sommaire

Pour faire face à la montée des risques de sécurité, au développement des terminaux mobiles et à l'adoption des services Cloud, les entreprises ont de plus en plus recours à l'authentification. Cependant, les stratégies adoptées par le passé ne suffisent plus. Ce livre blanc révèle les stratégies fondamentales que les entreprises peuvent utiliser afin de faire face aux défis de l'authentification posés par des environnements informatiques aujourd'hui bien plus complexes et bien plus dynamiques.

Introduction : le nouveau paradigme de l'authentification

Ces dernières années, nous avons assisté au changement radical du paysage informatique et de celui des menaces informatiques. Pour l'entreprise, ceci a des répercussions fondamentales sur la manière dont elle va appréhender l'authentification :

• **Des menaces sans cesse plus élaborées.** Les attaques MitM (man-in-the middle ou homme au milieu) et MitB (man-in-the-browser ou homme-dans-le-navigateur) sont de plus en plus courantes et de plus en plus sophistiquées. Elles sont utilisées pour pirater les transactions des utilisateurs, même lorsque ceux-ci ont mis en place une certaine forme d'authentification multi-facteurs. Un des plus grands éditeurs de sécurité a été victime d'une attaque perfectionnée qui a dévoilé les secrets, ou « graines OTP », de ses tokens d'authentification. Par la suite, plusieurs de ses clients ont été victimes d'attaques visant à exploiter ces graines OTP.

• **Des cas d'utilisation sans cesse plus nombreux.** Par le passé, la grande majorité des entreprises n'avait à composer qu'avec un seul cas d'utilisation : la connexion des employés à distance au réseau d'entreprise via VPN. Dans ce cas de figure, une méthode d'authentification unique prenait en charge ce cas d'utilisation unique. Aujourd'hui, le changement radical du paysage informatique contraint les équipes de sécurité à composer avec des environnements bien plus dynamiques et bien plus complexes. La présence accrue des services dans le Cloud et des terminaux mobiles a ouvert la voie à une grande variété de nouveaux cas d'utilisation en constante évolution ainsi qu'à toute une série de nouvelles vulnérabilités.

Même si l'authentification multi-facteurs a été largement utilisée depuis des années, la majorité des entreprises va réaliser que ces méthodes d'authentification vont devoir être utilisées sur un pourcentage plus large d'utilisateurs, et sur un nombre sans cesse croissant de cas d'utilisation. Ceci annonce l'augmentation des investissements et des déploiements de l'authentification. Si elles veulent un véritable retour sur investissement, elles doivent s'assurer que leur infrastructure est adaptée aux menaces actuelles et émergentes ainsi qu'à l'évolution du paysage informatique.
La section suivante aborde les deux changements fondamentaux de paradigme dans le monde informatique et les répercussions de ces tendances sur l'authentification.

Changement de paradigme dans le monde informatique : quelles répercussions sur l'authentification

Adoption de l'informatique dans le Cloud
Historiquement, l'objectif principal en matière de sécurité a toujours été d'assurer la protection des données internes contre les menaces externes. Dans cette optique, de nombreuses technologies ont été utilisées telles que les technologies de pare-feu, de détection des intrusions ou de prévention des intrusions. Toutefois, en raison de l'émergence des modèles d'informatique dans le Cloud, il est beaucoup plus difficile, voire impossible, de distinguer ce qui est interne de ce qui est externe. Aujourd'hui, la majorité des actifs sensibles peuvent être hébergés en externe afin de faciliter leur accès par les employés sur site, en déplacement ou travaillant à domicile. En bref, les utilisateurs, les données et les applications sont présents partout.

Comme Mike Rothman, analyste et PDG de Securosis l'explique : «Il est temps à présent pour les entreprises de déterminer le type d'infrastructure d'authentification dont elles ont besoin. En effet, le concept 'notre informatique, notre matériel, notre bâtiment' est définitivement révolu."

Un des problèmes découlant de tout le battage médiatique entourant le Cloud est que les définitions sont confuses. Et cette confusion subsiste sur le marché en raison de l'habitude générale à ranger la gamme de services disponibles sous la catégorie unique de "Cloud".Le plus important est de savoir que dans cette catégorie "Cloud" se trouvent de nombreux modèles différents avec leurs propres demandes d'authentification. Par exemple, deux des modèles les plus couramment adoptés sont les logiciels en tant que service (SaaS) et les infrastructures en tant que service (IaaS).
Ces deux modèles présentent des défis fondamentalement différents du point de vue de l'authentification :

• **SaaS.** L'objectif principal du modèle SaaS est d'étendre la fédération des identités de l'entreprise aux applications dans le Cloud. Les entreprises doivent offrir aux employés un accès par identification unique (SSO) transparent aux applications SaaS, tout en s'assurant en même temps que seuls les utilisateurs avec les bons codes d'accès sont autorisés d'accès.

• **IaaS.** L'objectif principal de l'entreprise qui adopte les modèles IaaS est d'étendre son infrastructure d'annuaire aux environnements extérieurs, tout en conservant les contrôles nécessaires. Tout particulièrement, l'application des politiques de sécurité relatives à l'accès des utilisateurs privilégiés.

"Lors de mes différentes collaborations avec les clients, je suis toujours frappé par le fait que la majorité des entreprises sont bien conscientes de la réalité du Cloud, et en particulier de SaaS. Bien souvent, ce sont les équipes de sécurité qui sont prises par surprise par cette réalité" explique Doron Cohen, vice-président de la division Technologie au sein de la direction technique de SafeNet. "Ces groupes ont du mal à trouver une solution complète qui répond à ces nouvelles réalités et aux demandes pressantes des utilisateurs professionnels, des responsables de la gestion des risques et des auditeurs."

L'authentification est et restera toujours un niveau critique dans l'infrastructure de sécurité d'une entreprise. Aujourd'hui, cependant, l'authentification doit être utilisée de façon beaucoup plus nuancée. Certains actifs non sensibles peuvent être protégés grâce à un nom d'utilisateur et un mot de passe standard, tandis que d'autres actifs hautement sensibles doivent être surveillés par des mécanismes d'authentification à trois ou quatre facteurs et de vérification OOB (out-ofband).
Cette plus grande précision de l'application des mécanismes de sécurité est primordiale car elle permet aux entreprises de profiter de tous les avantages du Cloud.

Développement des terminaux mobiles
L'adoption généralisée des terminaux mobiles a ouvert la voie à un changement de paradigme fondamental dans le monde de l'informatique professionnel. Autrefois, le service informatique était responsable de l'approvisionnement et de la livraison d'appareils informatiques standard (ordinateurs portables ou smartphones) et de la mise en place de mécanismes de sécurité basés

sur ces profils standard. Aujourd'hui, cependant, les utilisateurs et les entreprises exigent d'avoir accès aux actifs de l'entreprise quel que soit l'appareil qu'ils utilisent (smartphones ou tablettes achetés par l'utilisateur). Ceci a des répercussions énormes sur l'authentification :

• **Extension du support technique.** Alors que par le passé, chaque utilisateur avait au maximum deux appareils pour accéder aux réseaux d'entreprise, ce nombre est aujourd'hui plus de l'ordre de quatre ou cinq. Ceci augmente considérablement le nombre d'appareils devant être pris en charge par le service informatique.

• **Développement hétérogène des terminaux.** Aujourd'hui, il est nécessaire de prendre en charge les smartphones et les tablettes basés sur iOS, Android, Blackberry, Windows Mobile ainsi que toute une autre série de plates-formes et de terminaux.

• **Risque de perte et de vol.** Les risques que représentent la perte ou le vol d'un smartphone ou d'une tablette sont aussi graves que ceux engendrés par la perte d'un ordinateur portable. Par ailleurs, compte tenu de leur format et de leur utilisation, ces terminaux mobiles sont bien plus susceptibles d'être perdus ou volés.

"Les équipes de sécurité ne peuvent tout simplement pas adopter la politique de l'autruche" déclare Mike Rothman. "Apple a livré plus de 200 millions de terminaux iOS. Le service informatique ne peut tout simplement pas ignorer cette réalité. La forte demande d'utilisation de ces terminaux mobiles pose un risque considérable auquel il faut répondre de façon proactive."

Pour gérer les changements de paradigmes décrits ci-dessus, les entreprises doivent adopter différentes meilleures pratiques d'utilisation. Les sections suivantes décrivent les quatre étapes clé pour une gestion efficace, sûre et rentable de cette évolution.

Meilleure pratique n°1 : adopter une approche stratégique et holistique

Cela fait des années que les équipes de sécurité informatique font face au même dilemme de l'augmentation des demandes accompagnée de la diminution des ressources et des budgets. Par conséquent, l'approche tactique et au cas par cas de la majorité des projets d'authentification n'est pas surprenante : alerter en cas de nouvelle faille de sécurité ou de nouveau cas d'utilisation, fournir une solution ponctuelle, déployer et répéter le processus.

Les entreprises doivent sortir de cette spirale si elles veulent être en mesure de répondre aux demandes actuelles. Avant d'entreprendre de nouveaux investissements et de démarrer de nouveaux projets ciblant des problèmes spécifiques, les entreprises doivent commencer à adopter une approche plus globale et plus stratégique.

"La majorité des équipes de sécurité estiment qu'elles n'ont pas le temps d'adopter une approche stratégique. Elles sont contraintes d'adopter une approche tactique pour résoudre les problèmes" déclare Mike Rothman. "Cependant, une telle approche tactique finit par faire tripler ou quadrupler la création de fonctions spécifiques et donc à faire tripler ou quadrupler les coûts. Il incombe aux équipes de sécurité à prendre le recul nécessaire pour repenser leur infrastructure d'authentification."

Pour commencer, les architectes de la sécurité doivent identifier les cas d'utilisation principaux que l'entreprise doit prendre en charge puis chercher à construire une infrastructure qui les prend en charge. Pour cela, il est nécessaire d'avoir un regard holistique sur l'endroit où se trouvent les utilisateurs et les données, sur la manière d'accéder aux informations et sur le niveau de sensibilité des applications spécifiques et des données.

Dans cette optique, il peut se révéler déterminant d'adopter une démarche basée sur un cadre d'application des normes industrielles telles que celles de l'Organisation internationale de normalisation (ISO).

Mécanismes d'authentification forte : un large panel de solutions

Quand il s'agit de mécanismes d'authentification forte, les décideurs peuvent choisir parmi un panel de solutions matérielles et logicielles proposant de nombreuses options disponibles. En voici un aperçu.

Matériel
Les entreprises peuvent choisir parmi une gamme de périphériques matériels, comprenant des tokens USB et des cartes à puce (au format de cartes de crédit). Globalement, ces offres peuvent être regroupées en catégories :

• Mot de passe à usage unique (OTP ou One-time password).
Ces solutions mettent temporairement à disposition de l'utilisateur un ensemble de caractères alphanumériques générés aléatoirement et formant un mot de passe ne pouvant être utilisé qu'une seule fois.

• À base de certificats.
L'authentification à base de certificats repose sur l'utilisation d'une infrastructure à clé publique (PKI) et de certificats clients numériques sur une carte à puce permettant d'identifier les utilisateurs et de contrôler leurs accès.

• **Hybride.** Enfin, les tokens hybrides combinent plusieurs fonctionnalités. Par exemple, certaines méthodes permettent de combiner des modes d'authentification à base de mots de passe à usage unique et à base de certificats au sein d'un seul et même dispositif.
D'autres combinent la signature detransaction OOB et l'authentification par mot de passe à usage unique.

Logiciel
Aujourd'hui, il existe de ombreuses solutions d'authentification ultifacteurs qui ne nécessitent pas de composants matériels.
Ces solutions logicielles entrent dans les catégories suivantes :

• Mot de passe à usage unique (OTP). Les solutions logicielles OTP peuvent être installées sur les ordinateurs de bureau et sur les terminaux mobiles. Lorsqu'elle est activée, la solution génère un mot de passe pour un usage unique.

Ce cadre d'application aide les entreprises à définir des profils de cas d'utilisation communs et à gérer de manière homogène l'accès sur toute une variété de plates-formes.

"Colmater une brèche à chaque nouvelle fuite ne mène nulle part" explique Andrew Moloney, consultant en sécurité indépendant. "Nous entrons dans un âge où la complexité de l'environnement au sein duquel résident les données nécessite d'avoir une réflexion plus holistique en matière de sécurité. Nous devons appliquer des contrôles d'une manière plus souple et prenant davantage en compte le facteur de risque afin de disposer du bon niveau de sécurité au bon moment."

Meilleure pratique n°2 : poser une fondation souple

Même si les changements ont été fulgurants ces dernières années, on peut affirmer sans se tromper qu'ils ne vont aller qu'en s'accélérant. L'adaptation aux exigences actuelles et à celles à venir ne fait que renforcer l'importance de la souplesse de l'infrastructure d'authentification.
Ceci implique de répondre à l'évolution des cas d'utilisation, des technologies, des modèles d'entreprise et des modèles d'exécution.
Pour atteindre cet objectif, les équipes de sécurité doivent s'efforcer de faire la distinction entre leur cadre d'application de politiques de sécurité et les contrôles de sécurité. Par le passé, de nombreuses entreprises ont mis en place des architectures cloisonnées dont la gestion des politiques et les contrôles de sécurité étaient construits autour d'un cas d'utilisation spécifique ou de sous-ensembles de cas d'utilisation. En séparant le cadre d'application de la politique des contrôles de sécurité spécifiques, les entreprises sont en mesure de réagir plus rapidement aux changements. En d'autres termes, elles n'ont pas besoin de réinventer la roue à chaque apparition d'un nouveau cas d'utilisation. Elles n'ont pas non plus besoin de mettre à jour différents emplacements afin de s'adapter au changement global d'une politique.

Meilleure pratique n°3 : mettre à profit le contexte et les niveaux de risques pour une approche personnalisée
Par le passé, lorsqu'un nombre minimal de cas d'utilisation étaient pris en charge, il était décidé tout simplement d'utiliser ou non l'authentification. Aujourd'hui, des connaissances beaucoup plus contextuelles sont requises. Ceci implique une approche personnalisée de l'authentification selon l'identité des utilisateurs, l'endroit où ils se trouvent, leur activité, les terminaux qu'ils utilisent et la façon dont ils les utilisent.

Par exemple, si un utilisateur se connecte régulièrement à partir du même terminal, du même emplacement et du même réseau, il y a de plus grandes chances que la demande d'accès soit légitime. Dans ce cas, l'entreprise peut utiliser une méthode standard d'authentification afin d'autoriser l'accès. En revanche, si une tentative de connexion provient d'un terminal ou d'un emplacement géographique qui n'avait jamais été utilisé auparavant, une politique peut être utilisée pour appliquer les mécanismes d'authentification.

• **À base de certificats.**
Ces alternatives logicielles reposent sur une infrastructure à clé publique (PKI) pour la génération des certificats numériques qui sont stockés sur un ordinateur ou sur un terminal mobile (plutôt que sur une clé matérielle dédiée) et utilisés pour l'authentification

• **OOB.** L'authentification OOB utilise deux canaux de communication, par exemple, le mot de passe peut être envoyé via un texto (SMS) sur le téléphone d'un utilisateur autorisé.

De même, l'approche doit être adaptée en fonction de la sensibilité et des risques associés aux actifs et aux transactions d'un cas d'utilisation donné. Ainsi, ce même utilisateur obtenant l'accès à partir d'un terminal connu, se verra peut être autorisé l'accès via une authentification simple, mais il lui sera ensuite demandé de fournir des codes d'accès supplémentaires s'il effectue une transaction sensible.

Pour les actifs ou transactions hautement sensibles, l'entreprise choisira l'authentification à trois facteurs, plus une certaine forme de validation de transaction OOB. Par exemple, après avoir fourni un token et les codes d'accès requis à l'utilisateur de l'ordinateur portable, un message peut être envoyé sur le téléphone portable de l'utilisateur qui contient les détails de la transaction avec un mot de passe à usage unique. Si les détails de la transaction sont corrects, l'utilisateur peut alors envoyer le mot de passe signifiant que la transaction a été validée et approuvée.

Pour personnaliser au mieux leurs approches de l'authentification, les entreprises doivent mettre à profit un ensemble homogène de dispositifs et de méthodes d'authentification multi-facteurs que ce soit des tokens matériels USB, des certificats clients numériques à clé publique (PKI), l'OOB, et plus encore. (Voir l'encadré pour un résumé des différents types de solutions disponibles.)

Meilleure pratique n°4 : centraliser l'administration
Pour que toutes les stratégies mentionnées ci-dessus fonctionnent dans le monde réel, les entreprises ne peuvent tout simplement pas continuer à administrer l'authentification de façon ponctuelle et irrégulière. Aujourd'hui, il est essentiel de mettre à profit l'utilisation d'une plate-forme d'administration unique qui fournit la visibilité et le contrôle sur tous les cas d'utilisation, politiques et appareils d'authentification. Il est donc essentiel d'unifier l'administration des terminaux mobiles et de leurs codes d'accès respectifs avec celle des appareils informatiques traditionnels.

"Nous observons actuellement une forte demande pour des plates-formes d'administration qui permettent aux administrateurs d'attribuer des codes d'accès aux terminaux mobiles et de les enregistrer en même temps que les ordinateurs portables et ordinateurs de bureau" explique Doron Cohen. "Ceci est essentiel pour les équipes de sécurité qui veulent maintenir la visibilité et le contrôle, tout en satisfaisant aux exigences de la communauté des utilisateurs."

Conclusion
L'authentification forte est essentielle aujourd'hui. Elle se développe rapidement parallèlement à la prise en charge par les entreprises d'un nombre grandissant de nouveaux cas d'utilisation, terminaux et modèles informatiques. Pour composer avec le développement des services dans le Cloud et des terminaux mobiles, les entreprises doivent adopter une approche stratégique de l'authentification, et construire une infrastructure d'authentification qui offre la flexibilité, la sécurité et l'efficacité exigées par les entreprises.

DOCUMENT 5

« État des lieux : les solutions d'authentification-forte (2FA) ».

Le blog Synetis Yann - www.synetis.com - Octobre 2015 - (4 pages)

Nous avons déjà souvent traité les problématiques d'authentification / identification, présenté des techniques, des innovations et des moyens mémo-techniques pour renforcer vos mots de passe et adopter des politiques de gestion des secrets optimales.

De plus en plus d'entreprises comme de particuliers optent pour l'authentification forte, afin d'augmenter la sécurité de manière non-négligeable les phases d'authentification sur leurs applications. C'est là où les solutions d'authentification forte, aussi nommées 2FA (pour 2-factor authentication), entrent en jeu. L'intérêt de ces solutions est d'ajouter un « second-facteur » lors des phases d'authentification.

- « **Ce que l'on sait** » : le mot de passe
- « **Ce que l'on possède** » : le téléphone qui reçoit un OTP par SMS, ou le token qui génère l'OTP.
- « **Ce que l'on est** » : des caractéristiques biométriques propres à l'individu.
- « **Où se situe t-on** » : la géolocalisation de l'identité qui cherche à s'authentifier peut être un facteur déterminant. Ce facteur permet d'assurer une authentification à partir de lieu définis, ou encore empêcher une nouvelle authentification si la précédente a été réalisée à des milliers de kilomètres au cours de la même heure.
- « **A quelle date/heure est-on** » : Certaines authentifications se voient autorisées qu'en période de travail, à des heures définies. En dehors de ces créneaux, elles n'ont pas raison d'être.

A force de proposer et détailler les solutions de 2FA existantes au travers de divers articles, nous souhaitions pour synthétiser les alternatives existantes avec leurs avantages et inconvénients respectifs.

Les OTP par SMS

Ce mécanisme de 2FA consiste à recevoir un code à usage unique, généralement numérique et utilisable dans un laps de temps défini, que l'on renseigne dans un second temps d'une phase d'authentification. Très employé dans le secteur bancaire, notamment pour les achats effectués via l'Internet, ce code est reçu sur le téléphone de l'usager par SMS.

Il est important de notifier que ce mécanisme de 2FA via SMS ne fonctionne pas dans n'importe quel cas. Il se peut que le serveur d'émission du SMS n'ait pas votre pays dans sa liste des régions supportées, le fournisseur mobile peut ne pas être en capacité de délivrer le message, ou plus généralement le mobile peut être dans une zone non couverte par le réseau.

Avantages :

- Le code OTP est différent à chaque tentative d'authentification, donc si votre mot de passe est compromis, ce n'est pas suffisant pour qu'un tiers puisse usurper votre identité.
- Le code est envoyé sur un équipement tiers comme votre smartphone, ainsi un malware sur le PC ne peut le capturer / compromettre / changer.
- Peu coûteux en termes d'équipement : presque tout le monde dispose d'un smartphone.

Inconvénients :

- Si le réseau mobile n'est pas disponible ou que vous soyez hors de portée, vous ne pourrez recevoir le code.
- Des usurpateurs peuvent exploiter votre téléphone si celui-ci est perdu ou volé, tant que vous ne notifiez pas votre fournisseur afin de résilier le numéro.

- Si vous vous authentifiez et recevez l'OTP sur le même équipement (tablette / smartphone), les OTP sont soumis aux mêmes risques que votre mot de passe.

Les applications OTP off-line

Toujours en employant un équipement tiers usuel, tel les smartphones, une application dédiée peut servir de second-facteur en générant des OTP toutes les 30 ou 60 secondes. L'équipement nécessite simplement d'être synchronisé temporellement avec le serveur sur lequel on souhaite s'authentifier (NTP).

L'application « Google Authenticator« , celle de Microsoft ou encore celles de nos éditeurs partenaires tel Symantec VIP assurent ce service. Les codes sont générés localement à l'équipement.

L'avantage est que ces applications générant des OTP peuvent être utilisées hors réseau mobile. Elles nécessitent toutefois un raccordement initial (via un QRCode et/ou une clé-partagée).

Avantages :

- Ne nécessite pas l'envoi d'un SMS à chaque phase d'authentification. Il suffit d'être raccordé au réseau lors de la création du compte afin d'être synchronisé temporellement et disposer du « seed ».
- Peut être utilisé hors réseau.
- Une seule et même application permet de sécuriser de multiples comptes.
- Un « seed » initial permet d'assurer l'unicité des OTP générés toutes les 30 / 60 secondes pour un compte en particulier.
- Peu coûteux en termes d'équipement : presque tout le monde dispose d'un smartphone.

Inconvénients :

- Si un utilisateur malintentionné récupère le « seed » (clé-secrète), alors l'ensemble des OTP sont compromis.
- Si l'authentification et la génération des OTP se fait sur le même équipement (tablette / smartphone), les OTP sont soumis aux mêmes risques que votre mot de passe.

Les applications « Swipe » on-line

Recopier des OTP numériques de 4 à 8 caractères peut être fastidieux et en rebuter plus d'un. C'est pourquoi d'autres solutions existent visant à s'assurer que l'usager cherchant à s'authentifier est bien le propriétaire du second-facteur.

La technique du « swipe » est particulièrement appréciée à l'heure d'aujourd'hui. L'idée est de n'avoir qu'à « swiper » pour valider une authentification en tant que second facteur. L'usager cherche à s'authentifier sur une ressource protégée par la 2FA, son smartphone reçoit une notification et lui demande de swiper pour terminer le processus.

Nos éditeurs partenaires emploient de plus en plus cette technique sur leurs applications 2FA mobile, notamment inWebo ou encore PingID de l'éditeur PingIdentity. **SYNETIS** intègre ses solutions auprès de ses clients, avec application d'auto-enrôlement des smartphones, gestion du parc enrôlé, activation de la 2FA à la demande, etc.

Avantages :

- Ne nécessite pas l'envoi d'un SMS à chaque phase d'authentification. Il suffit d'être raccordé au réseau pour recevoir les notifications de swipe.
- Peut être utilisé hors réseau via des procédures de fallback (OTP numérique classique).
- Une seule et même application permet de sécuriser de multiples comptes.
- Le smartphone est enrôlé pour un usager et des applications précises.
- Simple, rapide, le swipe est la tendance actuelle.

- Peu coûteux en termes d'équipement : presque tout le monde dispose d'un smartphone.

Inconvénients :

- Nécessite d'être raccordé au réseau pour recevoir les notifications de swipe.
- Si l'authentification et la génération des OTP se fait sur le même équipement (tablette / smartphone), les swipes sont soumis aux mêmes risques que votre mot de passe.

Les vérifications du login

La vérification du « login » est une autre alternative aux solutions déjà présentées. Plutôt que d'être sollicité pour entrer un code OTP, une notification de « login » va être envoyé sur le smartphone. Une fois cette notification approuvée, le processus d'authentification se poursuit.

Ce mécanisme n'utilise pas de clé-partagé ou de seed. Il emploi la cryptographie asymétrique (clé privée / clé publique) pour vérifier l'identité.

Une clé privée est générée et stockée sur l'équipement portatif. La clé publique, elle, est stockée côté serveur. A chaque login, un challenge est réalisé entre le serveur et le smartphone.
Le réseau social Twitter implémente ce type de mécanisme de 2FA. 4

SYNETIS met en place ce type d'authentification auprès de ses clients, sur la base de certificats X.509 déployés et industrialisés via des solutions comme AirWatch par exemple, sur un parc de smartphone.

Avantages :

- Ne nécessite pas l'envoi d'un SMS à chaque phase d'authentification.
- Une seule et même application permet de sécuriser de multiples comptes.
- Les cycles de vie des certificats s'appliquent à cette méthodologie d'authentification (révocation).
- Peu coûteux en termes d'équipement : presque tout le monde dispose d'un smartphone.

Inconvénients :

- Nécessite d'être raccordé au réseau pour réaliser le challenge.
- Si l'authentification se fait sur le même équipement (tablette / smartphone), la clé privée est soumise aux mêmes risques que votre mot de passe.
- Nécessite de déployer un certificat sur l'équipement tiers.

Les tokens physiques

Un véritable système « 2-facteurs » nécessite 2 facteurs réellement distincts. Si l'on consulte une ressource protégée à partir d'un smartphone, et que l'on reçoit le SMS avec l'OTP sur ce même smartphone, il n'y a pas vraiment de « 2-facteurs distincts ».

Pour avoir un vrai système de double-facteur d'authentification, il faut deux composants totalement distincts qui opèrent indépendamment et qui évitent ainsi un même point de compromission.

Les implémentations traditionnelles de ce type d'authentification sont les « smartcards », les « login tokens » tels ceux de nos partenaires comme RSA SecurID, ou encore la Yubikeys.

Les smartcards nécessitent un lecteur dédié pour communiquer avec la puce de la carte, qui dispose de son propre CPU et mémoire afin de réaliser ses fonctions cryptographiques.

La Yubikeys quant à elle a également son propre CPU cryptographique, mais communique via USB en prétendant être un clavier.

Les tokens physiques disposent de leur CPU indépendant et n'ont pas besoin généralement d'être connecté sur le poste. Leur petit écran LCD suffit à afficher l'OTP courant.

Avantages :

- Ne nécessite pas l'envoi d'un SMS à chaque phase d'authentification.
- Ne nécessite pas un smartphone ou une tablette.
- Équipement de sécurité totalement indépendant de l'ordinateur, tablette ou du smartphone : réel 2-facteur.

Inconvénients :

- Vous pouvez nécessiter un token par application protégée.
- Des coûts sont à prévoir pour s'équiper d'une flotte de token / carte de la sorte.
- Peut nécessiter un lecteur additionnel sur le PC pour la smartcard.

D'autres solutions atypiques et/ou innovantes

Le « second-facteur » dans une phase d'authentification peut être de diverses natures. On observe de plus en plus un rapprochement de ce second facteur avec la biométrie, notamment via la reconnaissance faciale ou encore les empreintes digitales. Les nouveaux smartphones intègrent nativement de tels lecteurs.

Récemment, une nouvelle solution de 2FA a vu le jour. Celle-ci se base sur l'environnement sonore du PC et du smartphone. La signature des sons ambiants doit correspondre pour assurer à la ressource sécurisée que l'on est bien le porteur du second-facteur.

Avantages :

- Ne nécessite pas l'envoi d'un SMS à chaque phase d'authentification.
- Ne nécessite pas une interaction directe avec l'équipement servant de second facteur.
- Rapprochement du monde de la biométrie avec le facteur « qu'entends-je? ».

Inconvénients :

- Il est nécessaire qu'il y ait un minimum de bruit environnement, auquel cas l'application vous demandera de produire un son.
- Le PC doit disposer d'un micro.

DOCUMENT 6

« Signature électronique : clé de voûte de la transformation digitale ».

Patrick Duboys - www.journaldunet.com - Décembre 2014 - (3 pages)

La signature électronique est devenue en une dizaine d'année une technologie incontournable pour la transformation digitale indispensable des organisations.

La loi est établie et de nombreux usages ont vu le jour. De nombreux autres restent à inventer. Cette chronique aborde les aspects légaux, métiers, financiers et technologiques et présente des cas d'usages concrets.

Nous avons depuis longtemps établi des règles de confiance: Signatures manuscrites, face à face, poignée de main, sceau ou tampon, présence d'un Tiers de Confiance tel qu'un notaire ou un témoin, lettre cachetée, etc. Dans le domaine du numérique nous devons établir de nouvelles règles.

La signature électronique n'est pas une signature en bas d'un e-mail, une signature manuscrite numérisée ou une signature manuscrite réalisée sur une tablette avec un stylet. Ces types de signature n'ont pas de valeur légale. Attention donc aux signatures scannées ou faxées ! Il est en effet très facile de falsifier un document faxé ou scanné en y ajoutant manuellement l'image d'une signature manuscrite.

La signature électronique est dans les faits aujourd'hui, un mécanisme numérique utilisant un certificat électronique et créant autour du document une « enveloppe cryptographique » garantissant que: le document ou l'e-mail n'a pas été modifié depuis la signature, provient bien de la personne qui a signé, et auquel peut être associé un horodatage à partir d'un serveur d'horodatage accrédité.

1.Valeur juridique de la signature électronique

Sur le plan juridique, la loi N° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, dit dans son article 1316-1 : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. » Cet article consacre la valeur probatoire de la signature électronique.

1.1 Jurisprudence

Il est intéressant de noter que d'un point de vue jurisprudence, bien qu'il y ait des dizaines de millions de signature électronique réalisées en France chaque année, nous ne comptons depuis 2000 qu'un nombre limité de cas de remise en cause de la valeur de la signature électronique pouvant se compter sur les doigts de la main. Dans chacun de ses cas il a été tranché en faveur de de la signature électronique, sauf pour un cas pour lequel le signataire avait signé le fichier zip dans lequel se trouvait les documents et non pas chaque document dans le fichier zip. Il a été opposé que signer une enveloppe telle que le fichier zip ne voulait pas dire que les documents à l'intérieur avaient été signés. A noter que les juges se fient également à d'autres éléments tels que le paiement effectif d'un contrat signé électroniquement constituant un faisceau de preuve, pour prendre leurs décisions.

1.2 Convention de preuve

Dans les cas où des parties échangent régulièrement des contrats, il est conseillé d'établir entre ces parties une convention de preuve. Un tel document établi par exemple que les documents signés électroniquement entre les parties seront acceptés par tous comme ayant une valeur légale.

1.3 Authentification du signataire

L'article 1316-1 décrit plus haut spécifie « sous réserve que puisse être dûment identifiée la personne dont il émane ». Cela signifie qu'une authentification du signataire est nécessaire. Il est donc très vivement recommandé d'effectuer une authentification forte du signataire. Un des mécanismes parfois utilisé est le SMS *One Time Password* pour lequel le système vous authentifiant vous envoie un code par SMS et vous demande de le saisir sur un site web en plus de votre login et d'un mot de passe. Plus l'authentification sera forte, plus la valeur probatoire de la signature sera grande.

1.4 Conservation de la signature dans le temps

L'article 1316-1 décrit plus haut spécifie également qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité. Cela signifie que vous devez archiver ce document ainsi que les divers outils permettant de lire le document et de vérifier la validité de la signature du document. Cela peut avoir des conséquences dans la mise en œuvre technique d'une solution si vous devez par exemple archiver vos documents signés pendant dix ou vingt ans.

1.5 Loi européenne

Chaque pays en Europe a décliné une loi similaire. Le 23 juillet 2014 la Communauté Européenne a publié un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques (règlement eIDAS). Ce règlement n'est pas seulement une recommandation, il consacre la reconnaissance mutuelle des moyens d'identification électronique délivrés par un Etat membre et qui seraient utilisés dans un autre Etat membre. Il définit un cadre juridique pour plusieurs services de confiance.

Outre la signature électronique, sont également visés le cachet électronique (qui doit permettre de garantir l'origine et l'intégrité d'un document électronique délivré par une personne morale), l'horodatage électronique (pour prouver l'existence des données à un moment particulier), les services d'envois recommandés et l'authentification de site internet (pour s'assurer qu'un site web est géré par celui qui s'en prétend titulaire). Ce règlement prendra effet au 1er juillet 2016.

2. Cas d'usages

Les usages de la signature électronique se multiplient aujourd'hui. Parmi ces usages nous pouvons citer les réponses aux appels d'offres des marchés publics qui doivent se faire de façon signée avec une clé USB cryptographique délivrée par un Tiers de Confiance (une Autorité de Certification) reconnue par l'état français. Un autre cas d'usage est la signature de documents Ressources Humaines telles que notes de frais par exemple en interne.

2.1 Signature de contrats

Nous voyons aussi se développer la signature de contrat en agence sur tablette. Cette approche permet une gestion intelligente des flux documentaires avec la possibilité d'ajouter un flux d'approbation. Le management dispose d'outils d'analyse et de reporting immédiat. Les clients peuvent visualiser leurs contrats et informations dans leur espace client sécurisé sur l'Internet. Une signature électronique est apposée par les deux parties, via une authentification forte de chacun par SMS *One Time Password* ou tout autre mécanisme. Si une signature manuscrite est apposée par stylet sur une tablette, celle-ci peut dans certains cas constituer un des éléments du faisceau de preuve, mais c'est la signature électronique qui revêt la valeur probatoire.

La signature manuscrite contribue aussi à faire mieux accepter la signature électronique en gardant un aspect auquel les clients sont habitués. Un usage qui se développe également est la signature de contrat en ligne sur Internet. Les contrats sont signés automatiquement par un robot signature du côté du fournisseur de service (Banque, Assurance, Opérateur Télécom, etc.) puis proposés aux clients via une fenêtre sur Internet. Le client s'enregistre, fourni son numéro de portable et signe. Un faisceau de preuve est constitué avec le numéro de portable auquel est envoyé

un code à saisir par SMS, l'adresse IP, la géolocalisation, l'horodatage, l'e-mail du client, etc. Toutes ces informations sont signées et archivées sur un serveur à valeur probatoire.

2.2 Exemple d'une Direction des Achats

La Direction des Achats "Aéroports de Paris" utilise une Plateforme pour dématérialiser les échanges et les transactions avec ses fournisseurs. Voici ce qu'en dit Dominique Etourneau, Directeur des Achats : « J'ai utilisé cet outil pour rééquilibrer les forces entre les acheteurs et les administratifs », « La signature électronique est le processus le plus simple à mettre en œuvre : 3 semaines », « Cela s'est avéré très efficace, après un an, 90 % de nos contrats ont été signés électroniquement ».

2.3 Bénéfices de la signature électronique

Les gains financiers sont typiquement supérieurs à 50% par rapport à la version papier. Les gains en temps permettent de passer de 5 jours à moins d'une demi-journée. La signature électronique permet également de développer l'innovation au sein des organisations, d'optimiser les processus.

2.4 Facture électronique

La facture électronique permet également d'apporter de tels gains, même parfois supérieurs, mais c'est un vaste sujet que nous aborderons dans une autre chronique.

3. Conclusion

La signature électronique est devenue en une dizaine d'année une technologie incontournable pour la transformation digitale indispensable des organisations. La loi est établie et de nombreux usages ont vu le jour. De nombreux autres restent à inventer.

DOCUMENT 7

« Après les attentats, les collectivités locales découvrent la cybersécurité ».

Guillaume BREGERAS - www.lesechos.fr - Janvier 2015 - (3 pages)

Une vague de cyber-attaques sans précédent touche les collectivités. Sans danger pour les entités visées, elle soulève la question plus large de la sûreté digitale et du retard à rattraper sur les pirates.

L'onde de choc n'en finit pas s'étendre. Dans la foulée des attentats perpétrés à Paris les 7 et 8 janvier derniers, une déferlante de cyberattaques a frappé plus de 21.000 sites Internet français, dont une partie de collectivités territoriales. Les visiteurs de ces sites se sont trouvés face à des messages allant de la simple revendication d'appartenance à la communauté musulmane jusqu'au piratage de bases de données en vue de les diffuser publiquement.

Qui était à la manoeuvre ?

De l'avis des spécialistes en cybercriminalité, cette vague d'attaques, qui se poursuit encore aujourd'hui, n'est que d'une faible magnitude. C'est-à-dire qu'elle ne compromet pas ces cibles physiquement ou économiquement. *« Le niveau n'est pas de grande intensité, c'est comme si un adolescent taguait une mairie,* explique Damien Bancal, expert en cybersécurité et fondateur du blog Zataz. *Mais lorsqu'ils sont en nombre, les dégâts sont automatiquement plus importants. "*

Laurent Heslault, directeur des stratégies de sécurité chez Symantec, alerte toutefois contre une prise à la légère du sujet : *« Ces attaques sont un avertissement sans frais. Le simple fait de démontrer que l'on peut avoir accès au serveur prouve qu'avec plus de malveillance, l'ampleur aurait pu être plus importante. »* Cette alarme remet l'accent sur la fragilité d'un monde qui bascule rapidement dans le numérique sans les connaissances nécessaires pour se protéger correctement. Gérôme Billois, du cabinet Solucom, révèle les failles qui pourraient bientôt être exposées : *« Certains cas de vols de bases de données apparaissent déjà, comme au ministère des Finances et à celui de l'Intérieur. D'autres attaques visaient à placer un outil dormant pour l'activer plus tard. Les risques sont bien réels notamment si elles concernent les services essentiels comme la gestion de l'eau, du trafic routier ou de l'éclairage public. "*

Quelle est l'ampleur du retard des autorités locales ?

Ces attaques, non réellement coordonnées et pour la très grande majorité d'entre elles initiées par des adolescents, éclairent surtout le fossé entre une communauté native du digital, très habile, et les garants supposés de la cybersécurité. Jean-Marc Manach, journaliste et expert du sujet, agacé par ceux qui qualifient cette vague de cyberguerre, se veut plus tranchant : *« Il faut davantage parler de cyberincompétence que de cyberattaques. Elles révèlent davantage les manquements des directeurs des sites piratés car, dans la plupart des cas, il s'agit simplement de mises à jour non effectuées. "* Pragmatique, Vincent Hinderer, de Lexsi, y voit aussi un problème plus global : *« La cybersécurité est une question qui se traite dans le temps.*

Comme une maison, il faut entretenir ses systèmes, et les collectivités, dont les ressources baissent, ne sont pas suffisamment sensibilisées au sujet pour s'en préoccuper réellement, sauf pour les plus grandes d'entre elles. » Car c'est bien dans les échelons les plus petits que la vulnérabilité est la plus grande. Comme en témoigne François Bruno, d'Urbaquitaine : *« Nous avons été piraté, mais lors de l'appel d'offres, nous n'étions pas dans cette logique de cybersécurité et nous n'avons pas été assez vigilant sur ces clauses. Nous l'avions axé sur une approche commerciale, mais nous allons voir comment améliorer cela avec notre prestataire. "*

Comment faire évoluer les appels d'offres ?

L'encadrement de ces marchés doit donc évoluer. Si les compétences ne peuvent être intégrées, les acheteurs publics doivent muscler leurs cahiers des charges. Laurent Heslault préconise ainsi des petites choses assez simples comme la suppression de la notion d'antivirus : *« Cela ne correspond plus à la réalité, il faut prendre en compte la protection des données, leur chiffrement. La sécurité, dans le cadre des appels d'offres, doit être un critère de premier choix.*

" Pour Gérôme Billois, c'est la notion de consistance dans le temps qui doit ressortir : *« La garantie de sécurisation n'a pas de réalité dans un cahier des charges. Par contre, on peut placer des obligations de moyen, avec des points factuels comme des audits réguliers. "* Des pare-feux à mettre rapidement en application pour stopper toute forme de piratage, la plus simple mais ô combien symbolique soit-elle.