L'authentification à multi-facteur au sein de l'entreprise

Introduction

Dans le monde digital, il n'y a pas de normes d'identité, telles que nous avons appris à les connaître dans le monde physique. En effet, n'importe qui dans son éducation sociale apprend à se familiariser avec les documents d'identité usuels (carte d'identité, permis de conduire, etc.).

Ces documents d'identité sont par la suite utilisés dans la vie de tous les jours pour conduire diverses formalités, telles que l'exercice de ses droits civils, la conclusion d'un contrat de travail ou l'achat d'une nouvelle voiture sur un site de commerce en ligne.

Rien de tel dans le monde digital. Chaque service digital est son propre système clos, dont les mesures d'authentification et de sécurité sont mises en place par l'opérateur du service. Ces mesures d'authentification ont pour but de permettre d'identifier un utilisateur avec lequel il a déjà interagi sous la même identité de service.

Cette identité de service, se traduisant la plupart du temps sous la forme d'une adresse email ou d'un pseudonyme, est par la suite employée par le service pour vérifier la légitimité de l'accès aux ressources offertes par le service digital. Une mauvaise identification avec le service digital pouvant dès lors entraîner des conséquences néfastes, telles qu'un accès ou une consommation de ressources non autorisées.

Cette perspective d'un accès non autorisé se révèle particulièrement alarmante lorsqu'il a lieu dans un cadre professionnel. Assurément, dans ce cadre, les services digitaux sont quotidiennement utilisés par tous les acteurs d'une même entreprise pour collaborer entre eux, que ce soit l'accès à une base de données de l'entreprise, l'accès aux services de gestion des relations clients ou aux services de messagerie interne.

Dès lors, il devient crucial de sécuriser ces accès et l'utilisation de ces services, et la mise en place d'une police de gestion des facteurs par toute entreprise ayant à gérer des flux ou actifs de valeur se révèle primordiale.

Dans la présente lettre d'information, nous présentons (I) une méthodologie de base d'évaluation des risques d'authentification, par la suite nous réalisons (II) un survol des facteurs d'authentification et leurs types, et enfin nous donnons (III) une méthodologie de coût au sein d'une entreprise d'une mise en place d'une politique de facteurs d'authentification.

I - Modèles de risques

Avant toute mise en place d'une politique de facteurs d'authentification, il vient de se poser la question de la valeur des flux et actifs informationnels protégés, ainsi que sur le modèle de risque. Tous les flux et actifs n'ont pas la même importance.

Au sein d'une même entreprise, une multitude d'actifs informationnels coexistent parmi les différents services digitaux employés par l'entreprise, actifs dont la valeur diffère grandement (un

fichier client unique versus la base des fichiers clients dans son ensemble, un règlement de travail interne versus des informations clefs liées à un brevet de propriété intellectuelle).

Nous précisons que dans la présente lettre d'information, nous ne ferons pas de distinction entre que les facteurs d'authentification soient détenus sur des services internes, hébergés par une infrastructure en propre de l'entreprise ou équivalent, ou que les actifs soient détenus sur un service externe.

Réaliser et ordonner ces actifs par catégories de valeur et en faire une cartographie est l'étape première ; par la suite, il convient de réaliser un modèle de risque afférent à cette cartographie d'actifs.

Pour chaque actif informationnel, après lui avoir associé une valeur-type, il convient d'établir la liste des risques et menaces pouvant peser sur sa pérennité et sécurité.

Parmi les risques classiques affectant l'intégrité d'un actif informationnel, une liste notable de risques peut être la suivante :

- l'exfiltration totale ou partielle de l'actif informationnel, par exemple la copie dans son intégralité de la base client de l'entreprise ;
- la modification malicieuse d'un actif informationnel, par exemple l'altération cohérente d'une formule chimique d'un brevet de propriété intellectuelle ;
- la destruction totale ou partielle par pur acte de sabotage, par exemple les plans d'un futur ouvrage d'architecture ;
- le chiffrement de la donnée sur place, par exemple le chiffrement malicieux de la base des employés de l'entreprise à des fins de rançons.

Pour chacun de ces risques, il est nécessaire d'établir une source de risque, c'est-à-dire de définir qui peut être l'acteur à l'origine de la menace sur l'intégrité de l'actif informationnel.

En effet, il faut considérer que l'acteur à l'origine de la menace peut être aussi bien externe à la vie de l'entreprise (un concurrent économique, un activiste idéologique, un ancien employé mécontent), qu'interne à la vie de l'entreprise (un employé, un stagiaire, un sous-traitant).

Par exemple, un cadre mécontent de ses conditions de travail est susceptible de mettre en place une micro-caméra, dont le coût est dans les 100 EUR, dans un open space de travail, derrière le pot de verdure artificiel sur l'étagère du fond, afin d'observer la saisie des mots de passe de certains de ses collègues sur leurs postes de travail, et ainsi pouvoir par exemple accéder à certains brevets d'intérêt de l'entreprise, auxquels il n'a pas accès par lui-même.

Dès lors, il appartient d'associer à chaque type de menace une réalisation pratique du risque (par exemple, un employé copiant une donnée sensible) afin d'établir un modèle concret de risques de l'entreprise.

À partir de ce modèle de risque, une politique d'authentification peut être mise en place afin de s'assurer qu'à chaque catégorie d'actif un niveau d'authentification suffisant est appliqué. Cette

politique doit toujours être adaptée aux circonstances, au domaine et à la taille de l'entreprise ; il est plus bénéfique d'avoir seulement deux ou trois polices d'authentification bien maîtrisées par l'équipe responsable en charge de l'entreprise, qu'une pléthore de polices n'étant pas suffisamment flexibles opérationnellement.

Dans la pratique, il est adéquat d'englober ce que l'on appelle couramment les actes de la nature dans le modèle de risque. Le plus souvent, un incendie ou une défaillance matérielle peuvent avoir des conséquences plus graves sur l'intégrité d'un actif informationnel qu'un employé mécontent.

II - Les facteurs d'authentification

Une fois les linéaments d'une méthodologie de base d'évaluation des risques d'authentification posés, il est loisible de faire un survol de ce qu'on appelle les facteurs d'authentification, que ce soit les différents types de facteur et leurs modes de fonctionnement.

Trois types de facteur d'authentification sont utilisés pratiquement pour mettre en place une politique d'authentification à multi-facteur:

- un facteur de possession (« ce que je possède ») ;
- un facteur de connaissance (« ce que je sais ») ;
- un facteur biométrique (« ce que je suis »).

Parmi ces trois types de facteur d'authentification, nous mettrons l'emphase sur le facteur de possession, en tant qu'élément primaire de sécurité dans le cadre d'une authentification à multi-facteur.

Un facteur de possession se définit comme un secret cryptographique stocké sur un composant de sécurité, c'est-à-dire un composant physique indépendant spécialement créé et construit à cette fin. Ce composant de sécurité peut être un stick « USB » dédié ou une carte à puce (tel que chacun en a dans ses cartes bancaires).

Pour utiliser un facteur de possession, il convient d'abord de l'enregistrer envers le serveur d'authentification et une fois que celui-ci est enregistré, l'authentification se fera via un protocole dédié comme l'usage des certificats X.509, les protocoles FIDO ou U2F, ou bien encore une variante du protocole OTP.

Dans le cadre de l'authentification à des actifs et flux informationnels d'une valeur moyenne ou élevée, il est raisonnable d'utiliser un composant matériel dédié, et non un facteur de possession reposant sur un poste de travail ou un smartphone. En matière de sécurité, la compartimentation est une stratégie de sécurité d'une grande robustesse. De tels composants matériels peuvent être acquis auprès de fournisseurs comme Yubikey, Google ou Thales pour un montant unitaire de 50 à 100 EUR environ en fonction des modèles.

En second, il est loisible de considérer un facteur de connaissance comme un secret devant être

mémorisé par l'utilisateur, prenant le plus souvent la forme d'un mot de passe ou d'un code PIN. Il ne semble pas nécessaire d'avoir à expliquer en détail en quoi consiste un facteur de connaissance, leurs pratiques étant devenues la norme dans le monde digital.

En revanche, du point de vue de la mise en place d'une politique d'authentification à multi-facteur, il est pertinent de prendre en compte la vérification de la robustesse des mots de passe utilisés, le durcissement de leurs stockages du côté serveur ainsi qu'une procédure adaptée de leur renouvellement quand le besoin se fait sentir.

Pour ce qui concerne la vérification de la robustesse des mots de passe, il est recommandé que lors de la génération du mot de passe, la qualité d'entropie de celui-ci soit vérifiée pour être suffisamment bonne, par exemple demander une longueur minimum avec un couplage de caractères spéciaux et de chiffres. En effet, un adversaire voulant deviner le mot de passe devra parcourir un espace probabilistique plus grand.

À propos du durcissement de leurs stockages côté serveur, un administrateur n'est jamais à l'abri que ses utilisateurs réutilisent le même mot de passe d'un service à l'autre, et cela que ce soit un service interne ou externe.

Dès lors, pour prévenir des dommages en boule de neige en cas de fuite, le serveur se doit de « saler » l'empreinte cryptographique des mots de passe, avec une valeur unique et aléatoire.

Enfin, pour ce qui est du renouvellement des mots de passe, celui-ci peut venir à réalisation lorsque l'utilisateur a perdu son mot de passe, quelle que soit la raison à la source de cette perte, ou bien dans le cas d'un renouvellement impératif des mots de passe, par exemple si l'administrateur souhaite imposer un renouvellement des mots de passe à l'échéance d'une certaine période.

Dans tous les cas, il convient de mettre en place une procédure adaptée, dans le meilleur des cas avec un meeting physique entre l'utilisateur cherchant à renouveler son mot de passe et l'administrateur, sinon par l'initiation d'une procédure de renouvellement via un point de chute digital fiable (un email pré-enregistré ou une ligne de communication dédiée).

Un facteur biométrique se définit comme une mesure biométrique d'un individu (ses empreintes digitales, sa voix, son ADN) pouvant être utilisé comme élément d'authentification, dans le cadre d'une procédure de contrôle d'accès à des actifs ou flux informationnels. Si l'utilisation des facteurs biométriques peut sembler (faussement) aisée à mettre en place comme ce sont des facteurs dont chaque individu dispose, ceux-ci posent plein de problèmes en cas de fuite ou de compromission (une personne ne dispose que d'un seul « jeu » d'empreintes digitales).

En raison des nombreux problèmes pratiques que pose l'usage des facteurs biométriques, nous ne recommandons pas de les utiliser dans la mise en place d'une politique d'authentification à multi-facteur, sauf raisons contraires.

En reprenant l'exemple du cadre mécontent, si l'entreprise a mis en place une politique d'authentification à multi-facteur, la simple pose d'une micro-caméra dans un open space avec

vue sur les postes de travail ne sera plus suffisante pour compromettre l'accès à certains actifs.

Assurément, la vérification cryptographique réalisée entre le facteur de possession et le serveur, effectuée par voies électroniques sécurisées, sera totalement inaccessible depuis la micro-caméra.

III - Mise en place d'une politique et son coût

Après avoir survolé les différents types de facteurs d'authentification, nous donnons une méthodologie sommaire de coût au sein d'une entreprise d'une mise en place d'une politique de facteurs d'authentification.

Cette méthodologie se construit sur les hypothèses suivantes. (a) Toute authentification via le biais de SMS reçu sur un numéro de téléphone est proscrite (afin d'éviter toute attaque dite de SIM swapping). (b) Les facteurs biométriques sont prescrits (afin d'éviter l'absence d'agilité de ces facteurs pour ce qui est de leur renouvellement). (c) La politique mise en place privilégie l'emploi de facteurs forts d'authentification matérialisés par des composants physiques.

Une fois ces hypothèses retenues, il convient de les combiner avec un modèle de risques concrets. Pour les besoins de l'exemple, nous retiendrons le scénario d'une entreprise de 10 personnes dans le conseil à la biochimie. Cette entreprise détient plusieurs actifs informationnels de valeur différente : (1) les ébauches de brevet de ses clients, (2) son fichier clients et (3) les documents de ressources humaines (par exemple le règlement intérieur de l'entreprise, etc.).

Suite à la cartographie, les actifs de catégorie (1) et (2) seront placés dans une couche d'accès A et les actifs de catégorie (3) dans une couche d'accès B. Dans le présent scénario, les actifs sont tous situés sur des serveurs internes de l'entreprise, et en bonne pratique les actifs de la couche d'accès A sur un premier serveur et les actifs de la seconde couche d'accès B sur un second serveur. Il est prévu que l'ensemble du dispositif d'authentification soit géré par la même équipe d'administrateurs.

De notre point de vue, il est de bonne pratique d'établir des jeux de composants physiques distincts pour les deux couches d'authentification, c'est-à-dire que l'entreprise acquerra 5 composants pour la première couche A, comme il n'est pas nécessaire que tout le monde dans l'entreprise ait accès à la partie des brevets, et 10 composants pour la seconde couche B, comme les documents sont de moins grande importance.

Chaque employé de l'entreprise, à tout le moins pour ceux ayant accès à la plus haute catégorie d'actifs, aura à gérer 2 mots de passe et 2 composants physiques dans sa vie quotidienne avec l'entreprise. Pour la mise en place des mots de passe initiaux, si cela se fait en présentiel et que la politique d'authentification est aussi expliquée pendant ce présentiel, il faut compter une heure par personne, soit 10 heures de travail.

Pour une mise en place entièrement gérée par l'équipe d'administrateurs internes de l'entreprise, il faut compter un coût de 2000 à 2500 EUR, si parmi les composants physiques de sécurité, ceux de la plus haute gamme sont choisis.

Au-delà, il est important d'aussi soigner l'incorporation d'un processus de renouvellement des facteurs d'authentification, que ce soit l'oubli ou la perte du facteur de connaissance ou la perte ou le dysfonctionnement matériel du facteur de possession. En effet, un employé de l'entreprise doit pouvoir contacter l'administrateur du système d'authentification et prévoir le remplacement de son mot de passe et l'enrôlement d'un nouveau composant physique, si possible avec une phase en personne.

Enfin, nous soulignerons l'attention particulière qu'il faut porter aux facteurs perturbateurs de toute politique d'authentification à multi-facteur, que ce soit un évènement désorganisateur comme l'incendie d'un des serveurs d'authentification, le voyage professionnel à l'étranger d'un des employés ou bien le départ de l'entreprise d'un des employés et du statut de ses facteurs d'authentification.

En particulier, les voyages à l'étranger sont assez souvent source de problèmes dans ce qui est de l'accès aux actifs informationnels de l'entreprise. Pour ces cas typiques, il peut être intéressant pour l'entreprise de mettre en place une couche d'accès spécifique, avec des composants physiques dédiés pour le voyage, entre autres mesures de protections en profondeur du patrimoine informationnel de l'entreprise.

Conclusion

Dans la présente lettre d'information, nous donnons certains linéaments méthodologiques dans la mise en place d'une politique d'authentification à multi-facteur, soulignant la nécessité d'une phase préliminaire de cartographie et de classification des actifs informationnels, d'une phase de sélection des facteurs d'authentification, parmi les différents types disponibles, enfin de quelques éléments de coûts et difficultés dans la mise en place d'une telle politique.

Avertissement: Par souci de qualité, de style d'expression et d'exactitude de l'information technique et juridique, la présente lettre d'information a été strictement compose et écrite manuellement par son auteur. L'usage d'outils de traitement automatisé n'ayant eu lieu que pour la correction orthographique et grammaticale