Sécurité des SI: l'innovation devra faciliter le quotidien des utilisateurs

A l'heure où les innovations technologiques sont de plus en plus accessibles au grand public, les utilisateurs en entreprise souhaitent retrouver dans leur cadre professionnel le même niveau de performance et de convivialité que dans leur sphère privée.

Force est de constater que les offres des DSI ne suivent pas toujours le rythme des technologies qui se déploient en dehors de l'entreprise.
L'une des approches alors adoptée par les utilisateurs consiste à utiliser leur matériel personnel à des fins professionnelles. On peut citer en premier lieu les *smartphones*, mais les PC portables/ultraportables et les tablettes tactiles sont de plus en plus concernés, de même que les usages associés : réseaux sociaux, outils collaboratifs, partage de fichiers et autres solutions hébergées dans le Cloud.

Ce qui pouvait ressembler à un « caprice » des utilisateurs apparaît aujourd'hui être un véritable enjeu pour l'employeur : les moyens informatiques mis à disposition glissent progressivement d'un rôle d'outil vers une problématique de ressources humaines et de recrutement des jeunes talents.
L'autorisation de nouveaux usages au cœur des SI modernes passe notamment par l'innovation.

Innover pour faciliter le quotidien de l'utilisateur

Les technologies de sécurité ont mûri ces dernières années : on peut citer plusieurs exemples, comme le cas du chiffrement intégral de disque dur qui est aujourd'hui stable et largement déployé, la standardisation de puces matérielles de sécurité embarquées (type TPM), l'apparition d'applications « bac à sable » (s'exécutant dans un environnement isolé) ou encore la virtualisation des postes de travail. L'avènement du Cloud permet, lui, de déporter certaines fonctions de sécurité comme les antivirus ou les proxys.
Ces évolutions amènent aujourd'hui à pouvoir parfois autoriser des usages précédemment proscrits.

Déclinons ces idées à travers trois études de cas concrets :

1) Rendre transparente la connexion distante VPN sur le poste de travail entreprise.
Depuis des années, ces accès sont, pour la plupart des Grands Comptes, synonymes d'utilisation de *tokens* (ces « calculettes » générant des codes à usage unique). La question du remplacement des *tokens*, perçus comme contraignants par les utilisateurs peut aujourd'hui se poser.
Une solution réside dans l'utilisation de certificats numériques. En effet, si ces certificats sont eux-mêmes protégés sur le poste par un chiffrement intégral du disque dur (ou mieux encore par une puce TPM), ils bénéficient alors d'un niveau de sécurité avancé.
L'expérience utilisateur s'en trouve améliorée, puisque les certificats permettent une connexion « en un clic », sans mot de passe/*token* supplémentaire à saisir. **L'authentification à deux facteurs est respectée,** avec « quelque chose que l'on sait » (le mot de passe utilisateur) et « quelque chose que l'on possède » (le PC qui contient le certificat sécurisé).

2) Simplifier la connexion depuis un poste banalisé pour accéder à des intranets/webmail
Tout comme la connexion VPN, l'accès à l'Intranet (en particulier au *webmail*) depuis n'importe quel poste nécessite une méthode d'authentification plus robuste que le simple *nom d'utilisateur/mot de passe*

Sécurité des SI: l'innovation devra faciliter le quotidien des utilisateurs

du fait du risque de vol et de rejeu lors de l'utilisation sur des postes non maîtrisés. Le *token* a, là aussi, été historiquement privilégié.
Il existe aujourd'hui d'autres méthodes de protection pour les connexions banalisées, comme par exemple le *soft token*, qui peut se décliner en une application sur un *smartphone*, l'envoi de SMS contenant un code, ou encore un « chemin » à mémoriser par l'utilisateur dans une grille remplie de chiffres générés aléatoirement, qui est directement affichée sur le site Web d'accès.

3) Autoriser l'utilisation de smartphones personnels

Cet usage a souvent été interdit car il posait trop de problèmes de sécurité. Il peut aujourd'hui être envisagé plus sereinement avec des approches de type « silo professionnel » : il s'agit de segmenter sur le terminal les usages professionnels des usages personnels, soit par une configuration avancée, soit par l'usage d'applications dédiées. L'entreprise garde ainsi la main uniquement sur ses données, et interdit par ailleurs l'accès aux terminaux ne respectant pas les prérequis minimaux de sécurité (version de terminal à jour, mot de passe robuste, etc.).
Les trois exemples développés précédemment sont aujourd'hui fréquents, mais bien d'autres peuvent être envisagés, en particulier sur des réseaux sociaux ou des services Cloud. Ces approches doivent cependant toujours faire l'objet d'une analyse en regard des risques du contexte : toute solution ne peut pas être acceptable dans tout environnement.

Encadrer les usages et responsabiliser les utilisateurs
L'autorisation de nouveaux usages ne signifie pas pour autant l'absence de règles : il est nécessaire d'encadrer ces pratiques.
D'une part, **les mesures mises en place se doivent d'être cohérentes sur les différentes briques du SI.** D'autre part, il faut aussi parfois savoir accepter les limites de la technique : là où il n'est pas possible de maîtriser les usages, une sensibilisation adaptée permettra de responsabiliser les utilisateurs aux risques encourus.
Dans la mesure où ils posent de nouvelles questions en termes juridiques et de ressources humaines, ces usages doivent par ailleurs faire l'objet d'un accompagnement dédié de la part des départements concernés. **Les équipes sécurité doivent éviter de traiter seules des problématiques pour lesquelles elles ne sont pas toujours qualifiées** (par exemple la validité légale de chartes émises) ou qui ne relèvent pas de leur responsabilité (comme la perte de productivité liée à l'utilisation de réseaux sociaux).
Les points développés ici convergent tous vers la même idée : simplifier le quotidien des utilisateurs, sans remettre en cause la sécurité. Les nouveaux usages souhaités par ces derniers ne pourront pas être indéfiniment stoppés : même interdits, ils apparaissent d'une manière ou d'une autre au sein de l'entreprise.
La DSI, notamment à travers le RSSI, se doit d'y réagir, en répondant aujourd'hui à la fois au besoin des utilisateurs mais aussi à leurs envies. Il s'agit au passage d'une opportunité intéressante de soigner l'image positive de la DSI.

L'adage est – plus que jamais – adapté : **les fonctions de sécurité doivent *s'apposer*, et non *s'opposer* !**