gemalto
security to be free

pressrelease

Les départements IT doivent faire face aux obstacles qui entravent la mobilité des utilisateurs, par peur des failles de sécurité

Amsterdam – le 27 Octobre, 2015 : Les organisations doivent faire face à la demande pour plus de mobilité de la part des utilisateurs, alors que 92% des départements IT dans le monde limitent toujours l'accès aux données et ressources sensibles depuis des équipements mobiles. C'est le résultat d'une étude mondiale menée auprès de 900 décideurs IT par Gemalto (Euronext NL0000400653 GTO), leader mondial de la sécurité numérique. Bien que dans presque toutes les organisations (98%) les utilisateurs réclament des accès mobiles ou à distance, 95% des départements IT font face à certains obstacles pour accroître la mobilité des utilisateurs, le premier obstacle étant des craintes liées à la sécurité.

L'étude 2015 Global Authentication and Identity Access Management Index révèle que presque tous les répondants (94%) s'inquiètent d'une possible faille ou d'une attaque liée à un vol ou un piratage de moyens d'accès. Cette crainte est exacerbée par la prolifération des terminaux d'accès mobiles au sein des organisations, la plupart déclarant avoir en moyenne deux terminaux d'accès mobiles par utilisateur, et gérer trois jeux de codes d'accès différents par utilisateur. De plus, en moyenne, un ticket d'incident sur cinq (20%) est lié à la perte ou l'oubli des noms d'utilisateur et des mots de passe.

Afin de faire face au challenge de la sécurité dans un contexte de mobilité, la majorité des départements IT (86%) prévoit de mettre en œuvre l'authentification à deux facteurs pour l'accès aux applications Cloud. Actuellement, 38% des utilisateurs ont recours à l'authentification à deux facteurs, un chiffre qui devrait atteindre 51% dans les deux ans à venir. Déjà plus de la moitié (57%) font appel à l'authentification à deux facteurs pour sécuriser les accès des utilisateurs extérieurs aux ressources de l'entreprise, ce qui indique diverses utilisations de cette technologie. Presque tous les répondants (92%) ont actuellement au moins une application protégée par l'authentification à deux facteurs, le top 3 des applications protégées étant les applications Cloud, les portails web et les VPN.

Alors que les départements IT continuent de faire le choix de l'authentification à deux facteurs pour répondre à la vague des demandes d'identifiants, la grande majorité (91%) des répondants fait le choix d'une mise en œuvre de l'authentification en mode service basé sur le Cloud (AaaS – Authentification as a Service), et en gérant de manière centralisée leur authentification à deux facteurs. En donnant la possibilité de mettre en œuvre une politique unifiée de sécurité pour répondre de façon cohérente aux menaces, l'authentification à deux facteurs peut également rationnaliser les accès à de nombreuses applications. De plus, l'efficacité du Cloud est un élément critique pour permettre le déploiement de l'authentification à deux facteurs dans différents scénarii d'usage et mettre en œuvre des solutions rapidement et efficacement. En effet, 90% des répondants voient la livraison de services via le Cloud comme un élément clé dans le processus d'achat de solutions d'authentification forte.

« Les départements IT font face à la pression de devoir répondre aux demandes pour plus de mobilité, pour des employés avides de nouvelles approches de travail flexibles, » déclare François Lasnier, Senior Vice President for Identity Protection chez Gemalto. « *Les organisations qui ne sont pas ouvertes à ce changement risquent de limiter la productivité de leur entreprise. »*

« Les utilisateurs sont prêts à faire ce qui est nécessaire pour réaliser leurs missions, avec ou sans permission. Alors quand les ressources de l'entreprise sont disséminées sur différents sites, l'authentification forte et un mode de livraison en mode Service rendent cela possible en toute sécurité. En facilitant ces usages, les organisations seront mieux placées pour protéger les identités de leurs utilisateurs, sans sacrifier leur productivité ou la sécurité de leurs données. »

« La croissance des usages des applications Cloud et des équipements mobiles au sein des organisations, combinée à la croissance des menaces et le besoin de réduire les coûts, implique de prendre en compte de nouvelles considérations pour le contrôle des accès. Il y a clairement un besoin immédiat pour des solutions de gestion de l'authentification et des accès qui peuvent aider les organisations à répondre à ces défis, » conclue François Lasnier

« Les organisations ont conscience du besoin de déployer plus largement la sécurité pour protéger autant d'applications Cloud et sur site que possible, et particulièrement quand elles recherchent une solution d'authentification à deux facteurs*, »* déclare Garrett Bekker, Senior Security Analyst chez 451 Research. *« Les résultats de cette étude suggèrent que le choix d'une solution d'authentification à deux facteurs dépend de la capacité de cette solution à fournir une gestion centralisée, ainsi qu'un accès sécurisé pour la plus grande variété possible d'applications. »*

Parmi les autres enseignements de cette étude:

<u>L'importance de la mobilité</u>

- Presque toutes les organisations des répondants (97%) reconnaissent l'importance d'offrir la mobilité à leurs employés dans le cadre de leurs habitudes de travail.
- Le nombre d'utilisateurs qui utilisent des tokens pour gérer la mobilité au sein des organisations semble être en croissance, tout type d'entreprise confondu. En moyenne 37% des utilisateurs des entreprises répondantes utilisent actuellement des tokens pour gérer la mobilité, ce chiffre pourrait atteindre 46% en moyenne dans les deux ans à venir.

<u>Le rôle du Cloud dans la décision d'achat</u>

- Le Cloud est aussi un facteur significatif pour le choix du mode de livraison de la solution d'authentification à deux facteurs, avec 90% des répondants qui confirment que la livraison Cloud est une considération clé dans leur processus d'achat d'une solution d'authentification forte.
- Cependant, lorsqu'il s'agit du processus final d'achat, plus de la moitié des organisations révèle que cette décision dépend du DSI, et que les RSSI, Directeurs d'Exploitation, DG et DAF sont également susceptibles d'être également impliqués dans le processus d'achat.
- Le coût total de possession (TCO-total cost of ownership) est pour 20% des répondants le critère le plus significatif qu'ils prennent en considération lors du choix de la solution d'authentification à deux facteurs.

<u>Les menaces de sécurité et les enjeux de conformité</u>

- Presque tous les répondants (95%) pensent qu'il est important que leur organisation puisse produire un journal unifié auditable des accès ayant mobilisé différentes ressources dans l'entreprise.
- La grande majorité des répondants (95%) pense que l'authentification à deux facteurs peut aider leur entreprise à se conformer aux règlements sur la protection des données et réussir leurs audits de sécurité.

<u>A propos de l'étude</u>

Cette étude Gemalto a été réalisée auprès de 900 décideurs IT en Juillet 2015, aux Etats-Unis (200), au Royaume-Uni (100), en France (100), en Allemagne (100), en Australie (100), au Japon (100), au Benelux (50), au Moyen-Orient (50), en Afrique du Sud (50) et à Hong Kong (50). Toutes les organisations des répondants, issus de différents secteurs d'activité, avaient au moins 250 employés. Les entretiens ont été menés par Vanson Bourne, un cabinet indépendant de recherche en marketing spécialisé dans le secteur des technologies.

Ressources complémentaires:

- 2015 Global Authentication and Identity Access Management Index avec les données régionales
- Infographie
- SafeNet Authentication Service
- Secure Mobility (Infographie)
- Secure Mobility (eBook)
- Secure Mobility (Microsite)

À propos de Gemalto

Gemalto (Euronext NL0000400653 GTO) est le leader mondial de la sécurité numérique avec un chiffre d'affaires 2013 de 2,4 milliards d'euros. Présent dans 44 pays, Gemalto emploie plus de 12 000 salariés travaillant depuis 85 bureaux et 25 centres de Recherche et de Développement logiciel.

Nous nous développons au cœur du monde numérique en évolution rapide et constante. Des milliards de personnes à travers le monde revendiquent de plus en plus la liberté de communiquer, acheter, voyager, faire des transactions bancaires, se divertir et travailler – à tout moment et en tous lieux - de façon agréable et sûre. Gemalto répond à leurs demandes croissantes en matière de services mobiles personnels, paiement sécurisé, authentification des accès au « Cloud », protection de l'identité et de la vie privée, services d'e-santé et d'e-gouvernement performants, billettique des transports urbains facile d'utilisation et applications M2M fiables. Nous développons des logiciels embarqués et des produits sécurisés que nous concevons et personnalisons. Nos plateformes logicielles et nos services gèrent ces produits, les données confidentielles qu'ils contiennent et les services sécurisés qu'ils rendent possibles pour les utilisateurs finaux.

Nos innovations permettent à nos clients d'offrir des services numériques de confiance et faciles d'utilisation à des milliards de personnes. Gemalto continue de croître avec le nombre grandissant d'utilisateurs de ses solutions pour interagir dans le monde numérique et mobile.

Pour plus d'informations, visitez nos sites www.gemalto.com/france, www.justaskgemalto.com, blog.gemalto.com, ou suivez @GemaltoFrance sur twitter

# # #

Contacts presse :
Séverine Godet
Burson-Marsteller i&e
01 56 03 12 13
severine.godet@bm.com

Kenza Remaoun
Burson-Marsteller i&e
01 56 03 14 21
kenza.remaoun@bm.com

Gemalto media contacts:

Philippe Benitez
North America
+1 512 257 3869
philippe.benitez@gemalto.com

Peggy Edoire
Europe & CIS
+33 4 42 36 45 40
peggy.edoire@gemalto.com

Vivian Liang
大中华地区 (Greater China)
+86 1059373046
vivian.liang@gemalto.com

Ernesto Haikewitsch
Latin America
+55 11 5105 9220
ernesto.haikewitsch@gemalto.com

Kristel Teyras
Middle East & Africa
+33 1 55 01 57 89
kristel.teyras@gemalto.com

Pierre Lelievre
Asia Pacific
+65 6317 3802
pierre.lelievre@gemalto.com