Livre blanc

Bloor

Une sécurité basée sur la confiance et non pas sur la peur

…De l'importance d'un Cloud et d'un écosystème Internet dignes de confiance

Un livre blanc de Bloor Research
Par : Fran Howarth
Date de publication : août 2012

…grâce aux services dans le Cloud, les entreprises de toute taille, de la plus petite jusqu'à l'entreprise multinationale, pourront remettre la confiance dans l'équation de la sécurité.

Fran Howarth

L'essentiel

L'utilisation de la technologie est devenue une partie intrinsèque de nos vies et la majorité de l'activité économique se déroule désormais par voie électronique. Emergeant à un rythme effréné, les nouvelles technologies permettent aux entreprises d'être davantage novatrices et compétitives. Nombre de ces nouvelles technologies favorisent la collaboration, non sans engendrer des besoins contradictoires. En effet, les entreprises doivent s'assurer qu'elles utilisent les technologies en toute sécurité tout en engageant davantage de parties prenantes afin d'être plus compétitives.

De nombreuses années durant, la sécurité a été envisagée comme une forme d'assurance, un achat à contre cœur que beaucoup n'aiment pas faire. Les fournisseurs de technologies de sécurité relatent souvent des histoires obscures et nous mettent en garde contre les conséquences à craindre si nous n'achetons pas des solutions spécifiques pour résoudre des problèmes particuliers. Cependant, entretenir la peur peut paralyser l'innovation et faire que les entreprises fermeront les écoutilles et adopteront une approche réactive basée sur la crainte. La peur des problèmes de sécurité qui fait passer certaines entreprises à côté des opportunités qu'offre le Cloud Computing est un exemple typique.

La collaboration et l'utilisation d'applications provenant de sources externes a entraîné l'érosion des périmètres de l'entreprise tandis que la prolifération d'équipements mobiles dans l'environnement économique rend ces périmètres encore plus illusoires que jamais. Fermer les écoutilles afin de se protéger autant que possible n'est plus une solution. Une nouvelle approche de la sécurité s'impose, une stratégie qui fait migrer la sécurité dans la couche réseau. Et pour beaucoup d'entreprises, vu l'importance d'Internet pour leur activité, le Net est le nouveau réseau.

Nombre d'entre elles sont en train de faire migrer leurs données, leurs applications voire leur sécurité vers le Cloud. Elle commencent à se rendre compte que, plutôt que d'être une source de préoccupation pour la sécurité, le Cloud peut offrir des niveaux de sécurité plus élevés et qu'il s'agit d'un mécanisme de fourniture technologique fiable, digne de confiance et qui déploie des contrôles de sécurité endurcis au sein d'un périmètre de confiance. Dans le Cloud, il est possible d'appliquer des contrôles d'accès granulaires, de chiffrer les données pour les protéger contre tout accès non autorisé pendant leur transport ou leur stockage, ainsi que des niveaux de contrôle plus élevés selon le caractère critique des données. La continuité de l'activité et la reprise après un sinistre sont davantage garanties via des services Cloud tandis que les équipements mobiles peuvent être plus aisément gérés pour rendre les collaborateurs productifs où qu'ils se trouvent.

Grâce à la bulle sécurisée que représente le Cloud, les entreprises peuvent avoir confiance dans le traitement sécurisé de leurs données, à condition que le fournisseur de services dispose de l'infrastructure de sécurité nécessaire. Cependant, il reste des défis de sécurité à résoudre avant que la confiance ne s'installe. Le plus grand défi demeure la sécurité d'Internet lui-même. Les applications Web et les sites Web sont devenus la cible de prédilection des pirates et constituent le point faible de notre monde numérique. Nous devons consacrer davantage d'efforts à les sécuriser et à les rendre dignes de confiance. Les services dans le Cloud offrent une solution.

Rapide état des lieux

- Les entreprises adoptent le Cloud en masse. Alors que la sécurité était considérée comme un facteur inhibant, beaucoup d'entreprises invoquent le renforcement de la sécurité comme l'une des raisons pour utiliser des services dans le Cloud.

- Lorsque les bons contrôles sont en place, le Cloud peut offrir un périmètre endurci au sein duquel la sécurité peut être contrôlée étroitement.

- Cependant, il convient d'accorder davantage d'attention aux zones où les vulnérabilités restent un défi de taille, c'est-à-dire au sein des applications Web et des sites Web, avant de pouvoir finalement obtenir les niveaux de confiance souhaités pour les services en ligne.

En résumé

La confiance est essentielle pour bâtir une activité durable. Et la sécurité est vitale pour instaurer la confiance. Pour bâtir cette confiance dans les réseaux électroniques, la sécurité doit être intégrée à une infrastructure appropriée plutôt que d'être ajoutée au coup par coup. A l'heure où les réseaux sont toujours et encore plus ouverts avec l'envolée de nouvelles technologies novatrices, il est légitime de faire migrer la sécurité vers le haut du réseau. Faites migrer les données, les applications et la sécurité dans le Cloud, là où tous les services peuvent être maintenus dans un périmètre endurci, fiable et bâti sur une infrastructure hautement sécurisée qui comprend des contrôles d'accès granulaires, le chiffrement des données et un nombre réduit de vecteurs d'attaque. La ruée vers le Cloud est en bonne voie et elle offre de nombreux avantages, notamment une sécurité renforcée. Il est même possible d'utiliser des services de sécurité basés dans le Cloud pour faire d'Internet un espace plus fiable en surveillant et en remédiant les vulnérabilités à l'aide d'applications Web interfacées avec les clients et critiques pour l'activité. Ces dernières sont essentielles à l'activité d'un grand nombre d'entreprises et doivent offrir un environnement de confiance pour garantir des transactions clients sécurisées et préserver la confiance des clients dans les marques et la réputation de l'entreprise avec lesquelles elles interagissent.

La technologie, moteur de la croissance

Selon l'Union Internationale des Télécommunications, un tiers de la population mondiale est connecté à Internet avec chaque année 200 millions de nouveaux utilisateurs. Internet fait désormais partie intégrante de la vie quotidienne de milliards de personnes.

Le gouvernement américain déclare que « la force et la vitalité de notre économie, de notre infrastructure, de notre sûreté publique et de notre sécurité nationale puisent leurs racines dans le cyberespace. [1] » Dans l'idée de mesurer l'importance de l'impact d'Internet sur l'économie mondiale, le McKinsey Global Institute a récemment publié une étude intitulée « Internet matters: the net's sweeping impact on growth, jobs and prosperity »[2]. Ce cabinet d'analyse a constaté qu'Internet est devenu un facteur significatif et essentiel au sein des économies nationales et pour l'économie mondiale elle-même dans la mesure où il permet aux industries de premier plan d'être plus productives et de créer de nouveaux emplois. McKinsey a constaté qu'Internet représente environ 6% du PIB des pays avancés mentionnés dans son étude, et que le Net est un facteur critique de croissance économique qui a représenté 21% de la croissance du PIB de ces pays avancés au cours des cinq dernières années. Bien que beaucoup de commentateurs aient déclaré qu'Internet a contribué à supprimer de nombreux emplois, McKinsey a constaté que c'est en fait l'inverse qui se produit. Parmi les petites et moyennes entreprises (PME) qui ont été interrogées, 2,6 emplois ont été créés pour chaque emploi détruit à cause d'Internet. Les PME ont connu une croissance moyenne de 10% de leur productivité grâce à l'utilisation d'Internet et celles qui utilisent les technologies Web de manière intensive se développent en moyenne deux fois plus vite que les PME qui n'ont pas recours à ces mêmes technologies.

> « Au cours des cinq dernières années, Internet a représente 21% de la croissance dans les pays développés. »
>
> *McKinsey Global Institute*

Etant donné l'importance d'Internet pour la croissance économique et la prospérité, il est essentiel que le réseau se développe comme plate-forme ouverte et sécurisée qui favorise l'innovation et la communication. Cependant, la majeure partie des informations qui font l'objet de transactions et d'échanges via le Web sont extrêmement sensibles par nature, qu'elles concernent les personnes ou qu'elles soient essentielles au bon fonctionnement de l'entreprise. Ces informations sont extrêmement précieuses pour ceux qui souhaitent les dérober ou les compromettre par appât du gain, qu'il s'agisse de collaborateurs internes ou de pirates, de groupes criminels organisés, voire d'état-nations, leurs attaques étant par ailleurs toujours plus fréquentes, complexes et sophistiquées.

Lorsque peur et sécurité font bon ménage

C'est la crainte, ou les conséquences, des incidents de sécurité qui motivent nombre de ventes de technologies de sécurité. La presse regorge d'histoires détaillant les derniers incidents de sécurité et de compromission de données. Les statistiques sur le nombre de virus et de variantes de codes malveillants prenant les réseaux pour cibles abondent. Les fournisseurs de solutions de sécurité publient des rapports détaillés sur les menaces auxquelles nous sommes confrontés, à grand renfort de récits d'incidents sérieux. Il est constamment fait référence aux conséquences d'une sécurité insuffisante.

Ces histoires incitent les entreprises à investir dans des technologies de sécurité, mais souvent en réaction à des événements qui se sont produits ou à des menaces entre-aperçues, ce qui les amène à acquérir des solutions spécifiques pour résoudre un problème particulier. Ceci peut poser de multiples problèmes lorsque la sécurité est ajoutée comme une simple rustine, créer des lacunes au niveau de la protection et causer d'inextricables tracas à la Direction en raison d'une administration forcément complexe de nombreux systèmes hétérogènes.

Entretenir la peur de l'insécurité peut aussi inciter les entreprises à se passer des derniers développements technologiques qui pourraient être d'une immense valeur pour leur activité. Un exemple typique est l'utilisation des modèles de Cloud Computing, où la sécurité était initialement accusée par beaucoup d'être le plus grand facteur d'inhibition, essentiellement parce que les données métier sont stockées et traitées par des tiers étrangers à l'entreprise. L'utilisation d'applications de réseau social a été également ralentie pour des raisons de sécurité et un débat semblable fait actuellement rage à propos du phénomène du consumérisation de la technologie utilisée dans les entreprises qui font que les employés exigent de plus en plus de pouvoir utiliser leurs propres équipements personnels pour travailler, leurs propres systèmes, selon eux, étant souvent supérieurs à ceux fournis par l'entreprise pour laquelle ils travaillent.

« Entretenir la peur de l'insécurité peut aussi inciter les entreprises à se passer des derniers développements technologiques qui pourraient être d'une immense valeur pour leur activité »

Une technologie innovante exige un nouvel état d'esprit

Les mécanismes technologiques évoluent rapidement, y compris les services Cloud, la mobilité, la virtualisation, la consumérisation de l'entreprise ainsi que les applications Web fortement interactives. Le défi consiste donc à adopter ces évolutions technologiques pour permettre à l'entreprise de se développer, de cultiver l'innovation et la compétitivité et d'améliorer sa capacité à servir ses clients. Une fois la bonne sécurité déployée, les risques seront réduits et les entreprises pourront tirer parti des progrès fournis par la technologie. Pourtant, ces changements innovants exigent un nouvel état d'esprit. Fini l'époque où une l'entreprise pouvait gérer les menaces et les vulnérabilités de manière parcellaire et à mesure qu'elles se produisaient. Plutôt que de rechercher un correctif rapide en considérant la sécurité à travers le prisme de la peur, les entreprises devraient commencer à quantifier et à sous-peser les risques technologiques et les menaces économiques par rapport aux avantages qu'elles peuvent en tirer.

Une sécurité basée sur la confiance

La confiance est un principe au cœur de la sécurité. Pour être davantage fiables, les réseaux informatiques doivent être bâtis sur le principe de la connaissance et d'une confiance accrue plutôt que sur la menace ou la peur. La seule manière pour que sécurité soit synonyme de confiance est d'établir un fondement sécurisé qui tient compte de la sécurité de l'ensemble du système et qui ne protège pas seulement ses composants individuels au moyen d'une sécurité en silo.

Selon la Commission européenne, nombreux sont les défis qui doivent être relevés pour que les infrastructures réseau soient à la fois sécurisées et dignes de confiance :

- Les interdépendances créées entre les réseaux et les systèmes existants entraînent un niveau de complexité au niveau des infrastructures que nous n'avions jamais connu auparavant.
- Nos infrastructures réseau actuelles souffrent d'une sécurité médiocre sur leurs points d'extrémité, c'est-à-dire les utilisateurs, leurs composants et les données qu'elles transportent.
- Les infrastructures réseau contemporaines n'ont jamais été conçues pour affronter des menaces toujours plus importantes en termes de sécurité et de confidentialité et pour fournir de manière fiable des applications à durée de vie de plus en plus critique et consommatrices en bande passante.
- Beaucoup de protocoles de réseau pionniers désormais intégrés à Internet ont été conçus pour fournir des performances, mais avec peu de prise en compte de la sécurité.
- La convergence des médias et les vastes infrastructures de réseau de communication et informatiques hétérogènes qui voient le jour posent des défis nouveaux et sans précédent en termes de sécurité et de confidentialité.

Pour que les infrastructures réseau soient fiables et dignes de confiance, il faut y intégrer sécurité, fiabilité et confidentialité. De nouvelles infrastructures de sécurité sont nécessaires pour s'assurer que les trois piliers de la sécurité que sont la confidentialité, l'intégrité et la disponibilité soient disponibles pour que les réseaux puissent être entièrement dignes de confiance. La confidentialité est étroitement liée à la protection de la vie privée et exige que seules des personnes autorisées puissent accéder aux données. L'intégrité exige que les informations ne soient pas falsifiées pendant leur transmission ou leur stockage. La disponibilité impose quant à elle que les informations et les services soient accessibles chaque fois que nécessaire.

Bâtir la confiance via une plate-forme dans le Cloud fiable

Les mécanismes technologiques qui sont en train de prendre racine renforcent la confiance des entreprises dans des applications et des services fournis par des tiers, ce qui rend ces mêmes entreprises davantage collaboratives par nature. Alors qu'hier les informations et les données traitées et stockées par les entreprises l'étaient en grande partie sur des réseaux internes, des modèles de confiance doivent être étendus aujourd'hui aux réseaux et aux services externes. Les raisons sont notamment la volonté de réduire les coûts, la vitesse d'accès aux services ainsi que la souplesse, notamment en favorisant le nomadisme des collaborateurs.

« Le Cloud Computing est critique en termes de stratégie métier globale pour un large éventail d'entreprises »

Beaucoup d'entreprises cherchent à réduire les coûts matériels et de stockage en adoptant des technologies de virtualisation qui permettent d'administrer de nombreuses machines physiques de manière centralisée. Selon le fournisseur de solutions de virtualisation VMware, l'un des avantages de la virtualisation en termes de sécurité est que les équipes informatiques peuvent normaliser les images des machines virtuelles et créer des versions de sauvegarde des machines virtuelles critiques plus fréquemment qu'avec des serveurs physiques traditionnels, ce qui facilite la reprise après un sinistre. Avec la virtualisation, il est également possible de créer des zones de confiance autour des informations, des applications et des points d'extrémité qui adhèrent à ces ressources lorsque ces éléments migrent vers d'autres sites. De plus, il est possible d'utiliser des politiques automatisées pour évaluer le risque et appliquer la remédiation à tous les problèmes de sécurité qui se produisent. Ce qui signifie que les entreprises qui déploient des technologies de virtualisation peuvent mieux contrôler et visualiser leur infrastructure réseau et avoir ainsi la certitude que les mesures de sécurité fonctionnent bien.

Non seulement le recours à des technologies de virtualisation simplifie et consolide les opérations du centre de données en optimisant les ressources existantes et en permettant une gestion plus efficace, mais cette évolution est également considérée comme la première étape vers la migration des ressources vers le Cloud. Selon l'étude sur le Cloud Computing d'entreprise (« Enterprise Cloud Computing Study » publiée en avril 2012 par IDG Enterprise, les personnes interrogées ont affecté en moyenne 34% de leur budget informatique courant à des solutions de Cloud Computing. Les deux autres tiers envisagent d'augmenter leurs dépenses Cloud au cours des 12 prochains mois de 16% en moyenne[3]. est critique en termes de stratégie métier globale pour un large panel d'entreprises.

Ceci est confirmé par une autre étude réalisée dans 2012 par North Bridge Venture Partners et soutenue par 39 sponsors du secteur du Cloud Computing. Ces travaux ont permis de constater que le Cloud Computing est en train de rapidement s'imposer comme le moyen préféré pour déployer la technologie, 84% des nouvelles ventes de logiciels l'étant en mode SaaS (logiciels fournis sous la forme de service) tandis que les investissements dans des solutions SaaS ont été multipliés par 6 par rapport aux achats de logiciels traditionnels[4]. Parmi les marchés qui ont le plus recours aux logiciels SaaS figurent la gestion de la relation client, le commerce électronique, le décisionnel, les mobiles, les outils de productivité bureautiques, les systèmes ERP et le développement d'applications. Concernant le développement d'applications, l'étude a constaté que 75% des personnes interrogées ont l'intention d'utiliser des ressources PaaS (plate-forme en tant que service) d'ici 2017, soit une augmentation de 83% par rapport à 2012.

Le recours au Cloud présente de nombreux avantages, notamment des coûts inférieurs et plus prévisibles, une disponibilité permanente, une utilisation modulable, une gestion plus facile ainsi que la possibilité de supporter tous les équipements mobiles utilisés dans l'entreprise. Lors de sa récente enquête sur l'adoption et les tendances du Cloud pour 2012 (« Cloud Adoption and Trends for 2012 ») auprès de 300 PME implantées au Royaume-Uni, le Cloud Industry Forum a constaté que 96% des personnes interrogées ayant adopté des services dans le Cloud se déclarent satisfaites de l'expérience et des résultats[5].

Pour certaines, l'utilisation du Cloud Computing soulève des problèmes de sécurité, l'exemple le plus souvent cité étant celui des données de l'entreprise confiées à un tiers. Cependant, l'enquête menée en 2011 par Cloud.com et intitulée 2011 Cloud Computing Outlook a permis de constater que la sécurité renforcée garantie par les services Cloud était un facteur d'adoption majeur pour 32% des personnes interrogées[6]. C'est ce que confirme l'enquête de North Bridge où seulement 3% des personnes interrogées déclarent considérer les services Cloud comme trop risqués en 2012, contre 11% en 2011. Seulement 12% d'entre elles se demandent si le modèle est suffisamment mûr en 2012, contre 26% dans 2011. En outre, 50% des personnes interrogées déclarent avoir totalement confiance dans l'utilisation du Cloud en 2012, contre seulement 13% en 2011.

Bâtir la confiance via une plate-forme dans le Cloud fiable

> « Le périmètre s'est évanoui. Faites migrer vos données, vos applications, voire votre sécurité, dans le Cloud. Virtualiser la sécurité ou la pousser vers le haut du réseau est une évolution normale. Il est plus facile de construire une nouvelle sphère d'actifs sécurisés dans le Cloud qui gravitent autour de l'axe central de la couche de sécurité du réseau. Ainsi, les utilisateurs peuvent accéder aux actifs dans le Cloud sur le front-end tout en traversant la couche du fournisseur de sécurité réseau pour arriver sur le back-end de l'actif de l'entreprise situé dans le Cloud, avec à chaque fois un niveau de sécurité proportionnel aux exigences des actifs. Les entreprises devraient recourir au chiffrement, à la prévention des intrusions et aux politiques de firewall dans le Cloud. Si elles tentent de le faire elles-mêmes pour leurs propres équipements mobiles, elles deviendront alors de facto de mini fournisseurs de services mobiles. »
>
> *ED Amoroso, Directeur de la sécurité chez AT&T*
> *(Extrait du magazine Information Security)*[7]

L'une des raisons pour lesquelles l'utilisation du Cloud peut fournir une sécurité renforcée et des niveaux de confiance plus élevés par rapport à un déploiement en interne est la disponibilité d'une structure centrale avec un périmètre bien défini à défendre. Plutôt que d'acheter et déployer tout un éventail d'équipements et d'applications de sécurité pour résoudre des besoins de sécurité divers, le Cloud Computing transforme la sécurité en service. Certaines des responsabilités liées à la sécurité doivent nécessairement rester sous le contrôle des clients des services Cloud, notamment s'assurer qu'ils disposent bien des contrôles d'accès appropriés qui s'appliquent aux données qu'ils placent dans le Cloud et que les informations sensibles sont protégées de manière appropriée. Mais beaucoup de contrôles de sécurité deviennent la responsabilité du fournisseur de services Cloud, en particulier dans les environnements SaaS, comme l'indique le tableau 1.

Tableau 1 : Partage des responsabilités pour les offres SaaS

Client	Fournisseur de services
Conformité aux lois sur la protection des données en termes de données qu'il collecte et traite	Sécurité et disponibilité de l'infrastructure physique
	Procédures de gestion des correctifs et de durcissement
Maintenance et facilité d'administration du système de gestion des identités et d'authentification	Configuration de la plate-forme de sécurité
	Supervision des systèmes
	Maintenance de la plate-forme de sécurité
	Collecte des journaux et supervision de la sécurité

Source : ENISA

La responsabilité de nombreux contrôles de sécurité étant confiée au fournisseur de services, des mécanismes de défense en profondeur peuvent être fournies dans le périmètre endurci si bien que les tâches d'administration, de supervision et de maintenance des systèmes s'en trouvent sensiblement réduites pour les entreprises utilisatrices. Même si bon nombre d'entreprises ont exprimé des inquiétudes quant à confier des données sensibles à un tiers externe, les fournisseurs de services Cloud sont en mesure d'offrir des niveaux de protection des données très élevés. Ainsi, il existe des solutions de chiffrement pour les services Cloud qui garantissent le chiffrement des données lors de leur migration vers et depuis le Cloud, de même que pendant leur stockage, avec des clés de chiffrement qui restent sous la responsabilité du client, ce qui garantit que personne n'accède aux informations de manière inappropriée. En cas de compromission de données, de nombreuses réglementations qui exigent la divulgation publique de l'incident font des exceptions pour les données qui ont été correctement chiffrées. Ces dispositions sur la notification d'infractions sont déjà appliquées dans toutes les législations d'État aux États-Unis et ce sera aussi probablement bientôt le cas au niveau fédéral et en Europe par le biais d'une régulation européenne, les deux projets étant actuellement à l'étude. D'autres lois, notamment le Healthcare Insurance Portability and Accountability Act et des normes industrielles telles que Payment Card Industry Data Security Standard, exigent également la protection des données sensibles au moyen du chiffrement. Ainsi, un fournisseur de services Cloud peut donner des assurances à ses clients concernant la protection de leurs données, ce qui permettra à une entreprise d'avoir confiance dans la sécurité.

Bâtir la confiance via une plate-forme Cloud fiable

La sécurité et la vérification de la conformité peuvent également être renforcées en utilisant des services de Cloud Computing. D'un côté, des fonctionnalités centralisées de journalisation, d'audit et de reporting seront fournies pour que l'entreprise puisse mesurer l'efficacité de la sécurité des services offerts. D'autre part, les applications et services tiers peuvent attester de l'efficacité du fournisseur de services en matière de sécurité. Ceci implique des audits réguliers des objectifs et des activités de contrôle de la sécurité du fournisseur sur la base de certifications incluant des critères sur les meilleures pratiques pour évaluer les contrôles déployés par les sociétés de services. Ce domaine a été récemment amélioré avec le développement de la norme d'audit No.16 (SSAE 16) mise en œuvre par l'AICPA (American Institute of Certified Public Accountants) et axée sur les sociétés de services et de la nouvelle norme ISAE 3402 pour le reporting des sociétés de service internationales, normes spécialement destinées aux audits des fournisseurs de services. De plus, la conformité des fournisseurs de services à différentes réglementations gouvernementales et internationales et autres normes de l'industrie peut être auditée pour s'assurer qu'ils agissent bien en conformité avec leurs mandats.

Cependant, afin que les clients Cloud Computing puissent s'assurer que le service est satisfaisant et digne de confiance, le fournisseur Cloud doit être transparent et disposé à montrer les mesures qu'il prend pour gagner la confiance de ses clients. Tous les fournisseurs ne permettant pas à leurs clients d'effectuer leurs propres audits de leur fonctionnement, il est donc impératif que leur infrastructure de sécurité soit vérifiée de bout en bout, indépendamment et de façon régulière pour susciter la confiance et que ces rapports soient à la disposition des clients.

Les applications Web restent le point névralgique

Même si le Cloud Computing peut mettre en place une sécurité supérieure en réduisant les vecteurs d'attaque et en améliorant la sécurité des communications, et en fournissant un périmètre endurci pour y appliquer des principes de défense en profondeur, d'autres problèmes de sécurité doivent cependant être résolus avant d'atteindre le graal en matière de confiance.

Les entreprises sont de plus en plus tributaires d'applications Web fournies à travers une interface de navigation, à la fois celles fournies via le Cloud et celles mises à disposition sur les sites Web, par opposition aux applications logicielles qui exigent un logiciel client unique et propriétaire et/ou qui sont directement installées sur des équipements ou accessibles via des serveurs du réseau de l'entreprise.

Cependant, les applications logicielles, et notamment les applications Web, sont connues pour contenir des vulnérabilités. Le Ponemon Institute a estimé que dans 86% de toutes les attaques, une vulnérabilité était exploitée dans une application Web[8]. Selon Sophos Labs, 85% de l'ensemble des codes malveillants, notamment les virus, vers, spyware, adware et chevaux de Troie, proviennent du Web[9]. On estime à plus de 30 000 le nombre de sites Web quotidiennement affectés par ces codes malveillants, 80% d'entre eux étant des sites Web légitimes. Selon le Blue Coat Security Lab, les utilisateurs sont quatre fois plus susceptibles d'infecter leurs ordinateurs en consultant des sites Web proposant un moteur de recherche que par des courriers spams[10].

Les vulnérabilités affectant les applications et les sites Web susceptibles d'être exploités peuvent causer des dégâts considérables, notamment le vol de données qui peut avoir des conséquences graves. Selon une récente étude menée par l'agence de relations publiques Weber Shandwick, 60% de la valeur marchande d'une entreprise est imputable à sa réputation[11]. *Une entreprise victime d'une compromission de données peut voir sa réputation très sérieusement entachée et perdre ainsi la confiance de ses clients et voir sa valeur marchande diminuer.*

> « 60% de la valeur marchande d'une entreprise est imputable à sa réputation. Une entreprise victime d'une compromission de données peut voir sa réputation très sérieusement entachée et perdre ainsi la confiance de ses clients et voir sa valeur marchande diminuer. »

Selon une récente étude menée par le Ponemon Institute, 74% des entreprises considèrent la sécurité des applications Web soit comme plus critique soit comme aussi importante que les autres problèmes de sécurité qu'elles doivent affronter[12]. Cependant, 72% des personnes interrogées dans le cadre de cette étude testent moins de 10% de leur parc d'applications Web, principalement par manque de budget et d'expertise en la matière. 88% d'entre elles déclarent que le budget alloué à la sécurité des applications Web est inférieur à celui dédié au café.

Dans l'idéal, toutes les applications devraient être développées en s'appuyant sur des pratiques en développement informatique sécurisées et testées pour découvrir les vulnérabilités tout au long du cycle de développement logiciel. Cependant, comme le démontrent les données collectées par le Ponemon Institute, c'est bien loin d'être le cas dans la plupart des entreprises. Même les entreprises qui disposent des ressources et du budget pour ce faire sont confrontées à des pressions extrêmes pour que les applications passent rapidement en mode production et contribuent ainsi à générer des revenus. Sachant que les applications sont de plus en plus complexes et qu'elles font appel à un éventail toujours plus large de contributions, notamment de sources tierces qui peuvent avoir, ou non, été testées pour vérifier si elles contiennent des vulnérabilités de sécurité.

Les applications Web et les sites Web en particulier sont également souvent modifiés. Et dans l'absolu, chaque modification pose de nouveaux problèmes de sécurité. De surcroît, de nouvelles techniques d'attaque sont constamment développées, ces dernières introduisant et exploitant des vulnérabilités jusqu'alors inconnues. Quels que soient le niveau de sécurité mis en œuvre pour développer les applications logicielles et le sérieux des tests effectués, de nombreux problèmes peuvent surgir une fois l'application déployée, et ceci vaut tout particulièrement pour les applications Web.

Pour toutes ces raisons, une supervision permanente de la sécurité est une condition sine qua non et utiliser des services dans le Cloud est la solution idéale. Ces services permettent d'analyser une quelconque vulnérabilité qui a pu être introduite dans une application en s'appuyant sur des techniques de test de pénétration qui simulent les actions menées par des intrus. En outre, ces services sont particulièrement efficaces car nul besoin d'accéder au véritable code source de

Les applications Web restent le point névragilque

l'application testée. Les services de gestion des vulnérabilités dans le Cloud permettront également de garantir la conformité aux politiques de l'entreprise, à la réglementation nationale et aux normes de l'industrie, notamment Payment Card Industry Data Security Standard (PCI DSS) en automatisant l'identification et l'élimination des vulnérabilités au sein des applications.

Si les vulnérabilités persistent, les entreprises peuvent s'appuyer sur la fourniture de firewalls pour applications Web (WAF) par ces mêmes services. Contrairement aux firewalls généralistes qui inspectent les paquets pour déterminer si le trafic est autorisé ou non à parvenir à sa destination, les WAF peuvent empêcher l'exécution de fichiers afin que des codes malveillants ne puissent passer à travers ou empêcher des applications de traiter des types de données particuliers. Pour ce faire, ces firewalls WAF recherchent des configurations ou des comportements spécifiques associés aux programmes logiciels malveillants pour protéger les serveurs Web contre de telles attaques.

Un autre avantage du recours aux services dans le Cloud pour améliorer la sécurité des applications Web est que nombre d'entre eux offrent des services intelligents de recherche des menaces qui s'informent auprès de multiples sources à travers le monde concernant les toutes dernières menaces qui apparaissent. Lorsqu'une menace est découverte, des alertes sont automatiquement générées et envoyées à l'entreprise pour qu'elle déploie sans délai des actions de remédiation. Ceci peut garantir la sécurité des applications Web et des sites Web utilisés pour des processus métier internes et pour des services externes et ainsi réduire la probabilité que des failles de sécurité endommagent la marque et la réputation avant de détruire la confiance que l'entreprise a développée avec sa clientèle.

Outre les applications Web contaminées par des codes malveillants, des sites Web publics et des applications critiques pour l'entreprise peuvent causer des dommages à la réputation et à la marque par d'autres biais, ce qui entraînerait une perte de confiance de la part de la clientèle. Utiliser des certificats numériques est important pour certifier qu'un site Web appartient bien à une entreprise spécifique, ces derniers étant utilisés par des navigateurs Web pour prouver à l'utilisateur qu'un site est authentique. Ces certificats utilisent le protocole Transport Layer Security (TLS) et le protocole cryptographique Secure Sockets Layer (SSL) plus ancien pour chiffrer les communications réseau et empêcher ainsi l'interception de mots de passe et autres données sensibles. Ils sont importants pour sécuriser les communications, les opérations bancaires et les achats en ligne ainsi que les applications et les services Web.

Une fois qu'ils sont correctement déployés, les protocoles TLS et SSL sont particulièrement fiables. Cependant, le déploiement et la configuration corrects de SSL/TLS peut s'avérer complexe. Citons notamment les défis liés à la gestion des certificats SSL, au déploiement d'une version actualisée de SSL/TLS et à la configuration appropriée des nombreuses options possibles. En cas de problèmes sur un site Web particulier, des messages et des avertissements signalant des problèmes SSL sont souvent affichés à l'attention des utilisateurs. Selon une récente étude d'Online Trust Alliance, 91% des utilisateurs ont vu s'afficher des messages instantanés d'alerte de sécurité liés aux certificats SSL[13]. Parmi les personnes interrogées, 41% d'entre elles déclarent tout simplement ignorer ces messages, ce qui pourrait entraîner des failles de sécurité, tandis que 43% des autres personnes interrogées déclarent que ces alertes les incitent plutôt à quitter le site Web concerné. Ces réactions peuvent éroder la confiance dans une marque et la réputation de l'entreprise propriétaire du site Web ainsi qu'une baisse des ventes.

L'initiative Trustworthy Internet Movement a été récemment créée dans le but de résoudre les problèmes de sécurité liés à Internet, y compris celui de la gouvernance SSL. Cette initiative surveille sans interruption la qualité de l'implémentation SSL sur un million de sites Web majeurs et publie les informations qu'elle collecte. En juin 2012, à peine 12,3% des sites examinés par Trustworthy Internet Movement étaient considérés comme fiables en termes de certification SSL. Parmi ces derniers, nombre d'entre eux utilisaient la version 2.0 du protocole SSL qui est en fait obsolète dans la mesure où les problèmes de sécurité liés à cette version sont connus depuis 1996. N'importe quelle entreprise qui souhaite le faire peut vérifier le statut de ses certificats SSL en utilisant le service offert par le Trustworthy Internet Movement[14].

La confiance dans la réputation d'une l'entreprise étant un critère majeur pour sa viabilité, toutes les entreprises gérant des sites Web en contact avec leurs clients et critiques pour leur activité devraient s'assurer qu'elles font le maximum pour garantir des services dignes de confiance. Avec SSL, les entreprises devraient suivre un certain nombre de meilleures pratiques. Always-on SSL est une nouvelle approche mise au point par l'Online Trust

Les applications Web restent le point névralgique

Alliance qui offre un chiffrement et une authentification SSL sur l'ensemble des pages des services du site Web, et pas uniquement sur les pages de connexion. Des certificats SSL à validation étendue sont également disponibles pour offrir un niveau d'authentification supérieur et fournir un indicateur visible via le navigateur Web afin de prouver à l'utilisateur qu'il se trouve bien sur un site sécurisé.

Les entreprises devraient également s'assurer que leurs certificats sont émis par une autorité de certification digne de confiance qui suit les meilleures pratiques établies pour sécuriser les clés privées et qui s'appuie sur des pratiques d'enregistrement rigoureuses. En 2011, certaines attaques fortement médiatisées lancées contre des autorités de certification ont permis de découvrir que des certificats frauduleux étaient émis.

Par conséquent, les entreprises qui cherchent à obtenir des certificats devraient s'assurer que l'autorité de certification qu'elles utilisent publie ses politiques et qu'elle fait l'objet d'un audit régulier destiné à vérifier la fiabilité de son infrastructure. Le Certification Authority/Browser Forum a récemment publié sous la forme d'une norme des exigences de base internationales relatives au fonctionnement des autorités de certification qui émettent des certificats numériques SSL/TLS dignes de confiance en mode natif dans les logiciels de navigation. Cette nouvelle norme est effective depuis juillet 2012.

En conclusion

Il s'agit de quelques exemples de la manière dont les services Cloud peuvent aider les entreprises à renforcer leur sécurité et à réduire sensiblement les risques auxquels elles sont confrontées à cause des vulnérabilités au sein des applications, un vecteur d'attaque majeur contre les entreprises. Plutôt que de devoir consommer les ressources nécessaires à l'exécution de ces fonctions elles-mêmes, les entreprises peuvent confier ces tâches à un fournisseur de services disposant d'une expertise spécialisée. Il est en outre possible de surveiller les applications en permanence au moyen d'analyses planifiées et ad-hoc lorsque les applications sont modifiées afin de s'assurer que ces dernières restent intègres. De plus, l'organisation utilisatrice du service recevra des rapports détaillés sur les performances du service, ce qui fournira le journal d'audit nécessaire aux fins de la gouvernance et de la conformité. Elles seront également en mesure de s'assurer que leurs clients ne subiront aucun désagrément consécutif à l'utilisation de leurs applications et sites Web si bien que ces clients continueront de leur faire confiance et ne le regretteront pas.

Par conséquent, l'utilisation de services Cloud permettra aux entreprises de toute taille, depuis la plus petite jusqu'à la multinationale, de remettre la confiance dans l'équation de la sécurité. Les exemples fournis dans ce document montrent comment utiliser des services dans le Cloud pour rendre vraiment dignes de confiance les applications Web et les sites Web utilisés par les entreprises pour fournir des services à leurs clients. Ainsi, les entreprises pourront insuffler confiance et assurance à leurs clients, et donc protéger leurs marques et leur réputation, si bien que ces derniers continueront d'utiliser leurs services. En outre, ces entreprises seront également en mesure d'adopter des technologies émergentes qui leur offrent des avantages métier tout en contribuant à leur compétitivité. Elles auront aussi la garantie qu'elles sont utilisées de manière fiable via le contrôle centralisé qu'offre le Cloud.

Références

1. http://www.whitehouse.gov/issues/homeland-security
2. http://www.mckinsey.com/Features/Sizing_the_internet_economy
3. http://www.idgenterprise.com/press/research-indicates-that-cloud-increases-short-term-costs-for-long-term-gains
4. http://northbridge.com/2012-future-cloud-computing-survey-exposes-hottest-trends-cloud-adoption
5. http://www.cloudindustryforum.org/downloads/whitepapers/cif-white-paper-4-cloud-adoption-and-outlook-for-2012.pdf
6. http://www.cloudstack.org/cloud-computing-docs/cloud-computing-survey.pdf
7. http://www.infosecurity-magazine.com/view/26408/att-security-chief-mobiles-are-the-nail-in-coffin-for-trust-and-the-perimeter/
8. http://www.applicure.com/blog/ponemon-state-of-web-application-security
9. http://techie-buzz.com/online-security/sophos-top-security-threats-report.html
10. http://www.bluecoat.com/security
11. http://www.webershandwick.com/resources/ws/flash/InRepWeTrust.pdf
12. https://www.barracudanetworks.com/ns/downloads/White_Papers/Barracuda_Web_App_Firewall_WP_Cenzic_Exec_Summary.pdf
13. https://www.otalliance.org/resources/2012HonorRoll/Online%20Security%20Infographic. pdf
14. https://www.trustworthyinternet.org/ssl-pulse/

Complément d'informations

D'autres informations sur ce sujet sont disponibles sur http://www.BloorResearch.com/update/2143

Présentation de Bloor Research

Bloor Research est l'un des principaux cabinets de recherche, d'analyse et de conseil européens dans le secteur des technologies de l'information. Nous expliquons comment apporter plus de souplesse aux systèmes informatiques d'entreprise via une meilleure gouvernance, gestion et utilisation de l'information. Nous avons bâti notre réputation en « racontant la vraie version des faits » via une communication et des publications indépendantes, intelligentes et bien rédigées sur tous les aspects de l'industrie des technologies de l'information et de la communication. Nous pensons que raconter la vraie version des faits permet de :

- Décrire la technologie dans le contexte de sa valeur métier ainsi que les autres systèmes et processus avec lesquels elle interagit.
- Comprendre comment des technologies nouvelles et novatrices peuvent s'adapter aux investissements existants en technologies de l'information et de la communication.
- Regarder le marché dans son ensemble, décrire toutes les solutions disponibles et expliquer comment les évaluer plus efficacement.
- Filtrer le « bruit » et rendre plus simple la recherche d'informations ou de nouvelles supplémentaires qui facilitent les investissements et les déploiements.
- S'assurer que tous nos contenus sont disponibles à travers le canal le plus approprié.

Fondée en 1989, notre société diffuse depuis plus de deux décennies des travaux de recherche et d'analyse auprès des entreprises utilisatrices et des fournisseurs de technologies IT à travers le monde via des abonnements en ligne, des services de recherches personnalisés, des événements et des projets de conseil. Nous nous engageons à transformer nos connaissances en votre valeur métier.

À propos de l'auteur

Fran Howarth
Analyste en chef - Sécurité

Spécialisée dans le domaine de la sécurité et plus précisément la sécurité de l'information, Fran Howarth manifeste un vif intérêt pour la sécurité physique et la convergence de ces deux domaines. Ses autres centres d'intérêt majeurs sont les nouveaux modèles de fourniture tels que le Cloud Computing, la gouvernance de l'information, le Web, la sécurité des réseaux et des applications, la gestion des identités et des accès et le chiffrement.

Fran étudie les besoins de l'entreprise en matière de technologies de sécurité et les avantages qu'elles en tirent ainsi que la façon dont les entreprises peuvent se défendre contre les menaces auxquelles elles sont confrontées dans un paysage en évolution permanente.

Pendant plus de 20 ans, Fran a travaillé dans un cabinet de conseil en tant qu'analyste, consultante et auteure. Elle écrit régulièrement pour différentes publications parmi lesquelles Silicon, Computer Weekly, Computer Reseller News, IT-Analysis et Computing Magazine. En outre, Fran contribue régulièrement aux Bonnes pratiques de gestion de la sécurité de la Division Faulkner Information Services d'InfoToday.

Copyright et renonciation de responsabilité

2nd Floor,
145–157 St John Street
LONDRES,
EC1V 4PY, Royaume-Uni

Tél: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com