Executive Brief

Les nouveaux défis de la sécurité IT

Sponsorisé par : Bouygues Telecom Entreprises

Stéphane Krawczyk
novembre 2014

Aujourd'hui, les entreprises basculent progressivement vers un nouvel environnement informatique qu'IDC appelle la 3ème plateforme.

Ce nouvel environnement informatique repose sur **4 piliers technologiques que sont le Cloud Computing, la mobilité, le Big Data et les réseaux sociaux.** Il s'accompagne d'une croissance exponentielle du volume de données, des équipements et des modes d'accès.

Dans ce contexte, les entreprises adoptent de nouvelles façons de travailler (mobilité, collaboration, ouverture du système d'information aux partenaires et aux clients, développement des canaux de la relation clients) qui démultiplient les risques de sécurité. La sécurité IT et la sécurité des systèmes industriels sont alors fortement impactées et représentent à ce titre de nombreux enjeux pour les RSSI.

Les différentes études menées par IDC au cours de l'année 2014 montrent que **la sécurité informatique est, plus que jamais une préoccupation majeure pour toutes les entreprises.** Elle se traduit notamment par un poids toujours plus fort des dépenses de sécurité dans le budget informatique globale de l'entreprise, avec comme principale priorité **la protection des données sensibles.** Mais au-delà de cette priorité, le renouvellement des équipements, la sécurisation des environnements virtualisés, les terminaux mobiles ou encore la capacité à faire face à la recrudescence des attaques ciblées (APT) constituent, pour IDC un véritable relais de croissance sur le marché.

MÉTHODOLOGIE

Les évaluations de marché présentées dans ce document sont issues de la recherche IDC. Les résultats d'enquêtes sont tirés de **l'Observatoire de la sécurité IDC 2014**. Pour son Observatoire de la Sécurité, IDC a interrogé en Juin 2014, 200 entreprises françaises de plus de 500 salariés dans tous les secteurs d'activité, dont les services financiers, la distribution, l'industrie, la santé, les services, le secteur public, les télécommunications et les médias. Les fonctions interrogées sont des responsables de la sécurité des systèmes d'information. Afin de permettre une exploitation dans le cadre de cet Observatoire et une représentativité du marché, les résultats ont été redressés conformément aux statistiques de l'INSEE.

LES BUDGETS SÉCURITÉ

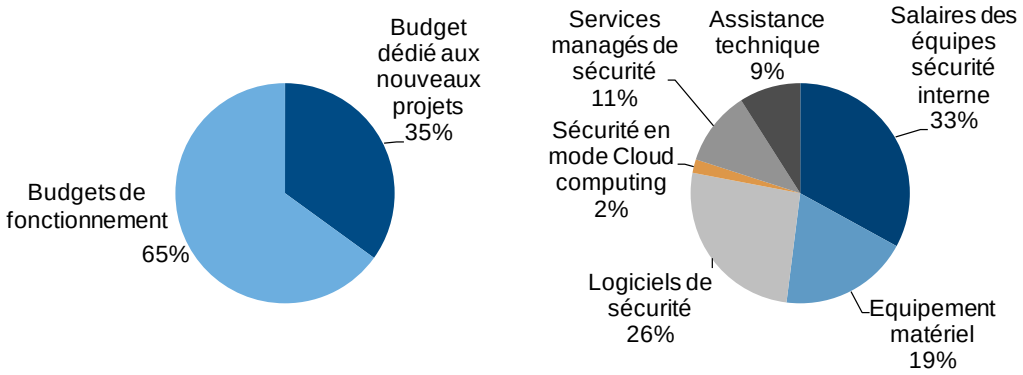
Le marché Français de la sécurité continue de croître en 2014. IDC évalue l'ensemble du marché français de la sécurité (matériel, logiciels services) à 2,1 Milliards d'euros pour l'année 2014, en croissance de +6,3% par rapport à l'année 2013. A titre de comparaison, la croissance du marché IT professionnel en France est évaluée à +0,9% pour l'année 2014.

Quelle répartition des dépenses sécurité ?

Selon les résultats de l'Observatoire de la sécurité, les dépenses dans ce domaine représentent en moyenne 4,1% de la dépense informatique globale des structures interrogées (voir graphique 1). Elles augmentent plus rapidement que les dépenses informatiques globales et par conséquent se renforcent dans les budgets informatiques des entreprises.

GRAPHIQUE 1

Répartition des budgets sécurité 2014



Source: Observatoire de la sécurité IDC, 2014

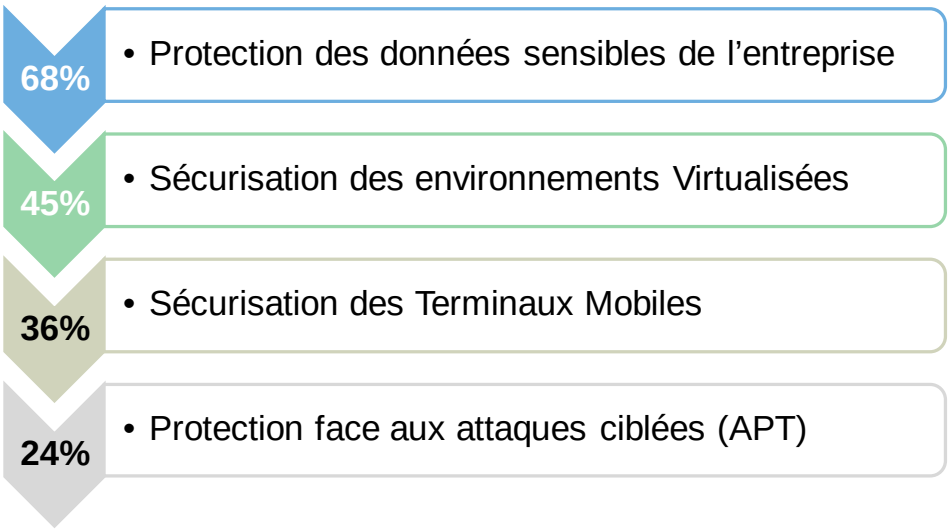
La segmentation des résultats par taille montre également que cette moyenne est plus élevée dans les entreprises de 500 à 1 000 salariés (8,1%) comparé à celles disposant de plus de 1 000 salariés (3,8%.) Enfin, les résultats par secteurs d'activités révèlent que la part dédiée à la sécurité est plus importante dans le secteur du commerce (6,3%) et le secteur public (4,3%) que dans l'industrie (3,8%) ou les services (3,6%.) Par ailleurs, la plus grande part de ces dépenses (65%) est dédiée au fonctionnement de l'existant et un tiers des budgets sécurité est consommé par les équipes internes de sécurité.

QUELS SONT LES PRINCIPAUX ENJEUX DE LA SECURITE INFORMATIQUE ?

Si les résultats de l'Observatoire de la sécurité 2014 confirment que la protection des données sensibles est la priorité majeure des DSI/RSSI, d'autres enjeux de sécurité viennent perturber le quotidien des RSSI.

GRAPHIQUE 2

Priorités des RSSI en 2014



Source: Observatoire de la sécurité IDC, 2014

La sécurité des environnements virtualisés

Les entreprises françaises utilisent de plus en plus les technologies Cloud pour la fourniture de logiciels ou d'éléments d'infrastructure. Les analyses IDC montrent que les entreprises françaises consomment 5.6% de leurs budgets IT en solutions et services Cloud en 2014, une enveloppe qui devrait représenter 7% de leur dépense IT en 2015. Le niveau de risque auquel les entreprises sont exposées augmente en conséquence. Non seulement le niveau de risque est plus élevé, mais surtout le paradigme qui auparavant consistait à sécuriser le périmètre de l'entreprise n'est plus suffisant. Les frontières physiques de l'entreprise n'existent plus (ou sont de moins en moins clairement délimitées.). Une approche efficace de gestion des identités et des accès (IAM), de la sécurité réseau et des solutions de chiffrement devient nécessaire. IDC prévoit notamment une montée en puissance de ce type de solutions pour les prochaines années. La gestion des identités et des accès s'accompagnera d'une adoption progressive des technologies d'authentification à deux facteurs (par exemple un identifiant et mot de passe associés à un second code ayant une durée de vie limitée). Les solutions de chiffrement profiteront quant à elles de l'utilisation accrue des environnements Cloud.

La sécurité des environnements mobiles

Le développement du travail en mobilité et la démocratisation du BYOD/CYOD peuvent présenter des risques majeurs en termes de sécurité. Selon les estimations d'IDC, les tablettes vont engendrer plus de la moitié des revenus générés par les environnements de travail des salariés (PC et tablette) en Europe à l'horizon 2017-2018. Les projets de mobilité (BYOD/CYOD) continuent de se développer, et la présence de tablettes appartenant aux employés deviendra de plus en plus fréquente dans les années à venir. Ces facteurs augmentent les risques d'atteinte à la sécurité et de perte de données. De plus, le BYOD/CYOD supprime progressivement les frontières

entre l'entreprise et les données personnelles, compromettant la sécurité des informations sensibles de l'entreprise et rend plus difficile, la gestion des risques et de la conformité géré par les équipes sécurité internes. IDC s'attend à ce que les entreprises se tournent plus systématiquement vers les fournisseurs de services et de solutions de sécurité afin de sélectionner et déployer des solutions de sécurité adaptées, répondant aux besoins particuliers de leurs entreprises.

Des attaques qui augmentent et se professionnalisent

Les cyber-attaques et APT se multiplient et sont de plus en plus difficiles à détecter. L'expansion continue de l'environnement informatique de l'entreprise (entraînée par l'adoption des modèles "as-a-Service"), l'utilisation croissante des terminaux mobiles, l'émergence des logiciels malveillants et des virus spécifiques (distributeurs automatiques, automates programmables industriels…) dépassent largement la capacité des services informatiques internes à faire face aux menaces qui pèsent sur la sécurité informatique. IDC s'attend à ce que tous ces défis stimulent la demande et les investissements des entreprises dans des solutions et services de sécurité, en particulier dans des secteurs où la réglementation est intense et où le niveau d'exigence en matière de sécurité est élevé (par exemple les services financiers, les entreprises gérant des infrastructures critiques ou encore dans des secteurs où la propriété intellectuelle est prédominante).

Des contraintes financières toujours au premier plan

Le contrôle des coûts reste un levier important des investissements informatiques. Dans ce contexte, la demande en services de sécurité managée continuera de croître. Cette croissance sera stimulée par des entreprises qui cherchent à réduire leurs dépenses en transformant leur structure de coûts d'un modèle CAPEX vers un modèle OPEX. IDC prévoit une montée en puissance des offres de sécurité-as-a-Service. Les coûts et les avantages associés aux architectures partagées permettent de générer des économies d'échelle chez les fournisseurs de services. Il en résulte une diminution des coûts de fonctionnement et de maintenance pour les entreprises utilisatrices mais également une réduction des dépenses d'investissements. Parallèlement, l'outsourcing diminue les efforts et les coûts nécessaires pour la mise en place de plan de reprise d'activité ou la suppression des failles de sécurité puisque ces activités peuvent être comprises dans les contrats de services managés. Cependant, ce modèle permet aux entreprises utilisatrices de changer facilement de prestataires, obligeant les fournisseurs à maintenir un haut niveau de qualité de service. Combinés ensemble, ces facteurs contribueront à accroître la demande de solutions de sécurité-as-a-service.

Des compétences de plus en plus rares

La pénurie de compétences qualifiées en matière de sécurité va certainement accroître la demande en services managés et en services professionnels de sécurité. Ce type de services est aisément actionnable et permet d'avoir facilement accès à des ressources spécifiques, des compétences et des technologies proposées par les fournisseurs de services. En particulier, les moyennes et petites entreprises tireront les avantages associés aux services de sécurité managée lorsqu'elles ne peuvent pas se permettre d'y consacrer du temps et de faire les efforts financiers nécessaires pour disposer en propre de ressources pointues en matière de sécurité.

Pour IDC, l'ensemble de ces éléments contribuera à accroître l'utilisation des solutions de sécurité dans les entreprises. Cependant les résultats de l'Observatoire confirment que les entreprises françaises sont encore relativement sceptiques vis-à-vis de l'externalisation totale de leurs solutions ou services de sécurité. Les responsables de la sécurité se sentent plus confiants en conservant leurs systèmes de sécurité en interne, même si dans de nombreux cas, ils les croient plus sûrs qu'ils ne le sont vraiment.

DES SOLUTIONS DE SÉCURITÉ POUR REPONDRE AUX ENJEUX

Les résultats de l'Observatoire montrent que, malgré des taux d'adoption déjà élevés, les projets de déploiement de solutions de sécurité existent. En effet, 46% des entreprises privées ou publiques interrogées ont un ou plusieurs projets relatifs aux solutions de sécurité IT à court ou moyen terme. Ces projets portent avant tout sur l'extension ou le renouvellement de solutions (76%) plutôt que sur la mise en place de nouveaux équipements.

L'extension ou le renouvellement des solutions de sécurité réseaux génèrent des projets de sécurité IT

Les différentes enquêtes réalisées par IDC montrent que la plupart des technologies de sécurité réseaux actuellement en place n'ont pas été conçues pour répondre aux besoins de la virtualisation et du Cloud Computing. Dès lors, le réseau devient un goulot d'étranglement nécessitant des interventions manuelles pour déployer et migrer des machines virtuelles. Le datacenter peine ainsi à réagir aux changements de l'environnement technologique et aux demandes des directions métiers. Dans ce contexte, la mise à niveau des solutions de sécurité associées à ces nouvelles architectures est nécessaire et génèrent des projets de sécurité.

De plus, parmi les projets d'équipements en solutions de sécurité réseaux, 21% des entreprises envisagent la convergence d'équipements reposant sur des solutions de gestion des menaces unifiées (UTM) à la place des solutions « best of breed » de firewall, d'IPS, ou de VPN. Pour IDC, il s'agit d'une tendance forte : alors qu'en 2013, le marché des appliances **UTM représentait déjà 53% du marché des appliances de sécurité en valeur, IDC anticipe que leur poids continuera d'augmenter pour atteindre 62% à l'horizon 2018**. Simplification des déploiements et de la maintenance, mise à jour permanente des fonctionnalités de sécurité constituent les principaux avantages de ces solutions. Les RSSI ont également la possibilité de configurer leurs équipements de manière autonome et d'implémenter leurs propres politiques de sécurité grâce à une interface de gestion.

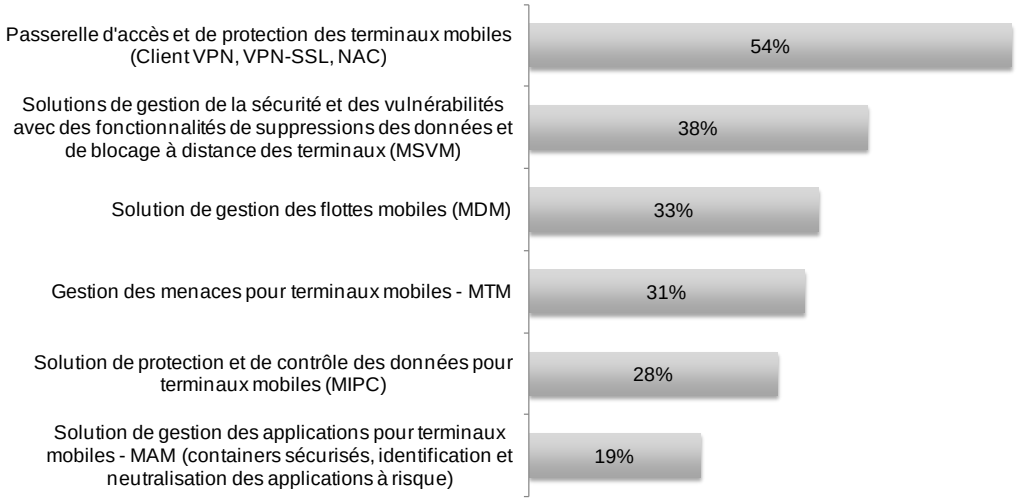
Les solutions de sécurisation des terminaux mobiles étendent leurs fonctionnalités

Avec la montée en puissance de l'utilisation des terminaux mobiles en entreprise, la gestion des périphériques mobiles devient incontournable pour les entreprises. **Les résultats de l'Observatoire de la sécurité révèlent que 70% des entreprises interrogées ont déjà mis en place une solution de sécurité pour répondre à ce phénomène avec en tête des solutions associées à des passerelles d'accès et de protection (Client VPN, VPN-SSL, NAC).** De plus, 26% des entreprises interrogées prévoient de mener des projets dans les 24 mois comme par exemple la mise en place de solutions de gestion de flottes, de gestion des applications et de gestion des vulnérabilités avec la possibilité de bloquer les terminaux et d'en supprimer les données à distance. La simplification de la gestion des flottes mobiles et le renforcement de la sécurisation des terminaux sont les principaux avantages de ce type de solutions. Elles permettent d'apporter des réponses concrètes face aux nouveaux enjeux associés à l'utilisation des smartphones et tablettes en entreprise.

GRAPHIQUE 3

Taux de pénétration des solutions de sécurisation des terminaux mobiles 2014

Question : Pouvez-vous indiquer quelles solutions de sécurité pour terminaux mobiles ont été mises en place dans votre entreprise



Source: Observatoire de la sécurité IDC, 2014

Le recours à des partenaires se renforce progressivement

Qu'il s'agisse de solutions de sécurité réseaux ou de solutions de sécurisation des terminaux mobiles, les résultats de l'Observatoire de la sécurité montrent qu'une très large majorité des entreprises interrogées gère aujourd'hui ce type de solutions en interne (87% pour les solutions de sécurité réseaux). La localisation des données hors de l'entreprise est en effet identifiée comme un frein pour plus de la moitié des grandes entreprises interrogées. Cependant, la pénurie de compétences pointues en matière de sécurité associée à la multiplication des tâches que doivent effectuer les équipes de sécurité internes devraient contribuer au renforcement progressif des recours aux partenaires pour gérer les solutions de sécurisation. **Dans ce contexte, la possibilité pour l'entreprise utilisatrice d'avoir un accès complet à l'interface d'administration constitue pour IDC un élément clé dans l'évolution des modèles de gestion.** En effet, en cas de menace ou d'attaque, la vitesse de réaction est essentielle et les organisations doivent être en mesure d'appliquer les règles de sécurité qui leur sont propres.

CONCLUSION

L'une des problématiques les plus importantes dans la mise en œuvre des solutions de sécurité informatique au sein d'une entreprise est la complexité même des menaces de sécurité et son corollaire, le manque de compétences en interne. Un nombre croissant d'entreprises choisira donc d'externaliser certaines fonctions de sécurité pour atténuer la pénurie de compétences internes et, pour certaines, de réduire leurs coûts.

La transformation numérique des entreprises et les enjeux qui lui sont directement associés – sécurité des accès, des terminaux et des applications mobiles, protection des données dans un environnement Cloud ou réseaux sociaux – rendent la gestion de la sécurité particulièrement difficiles pour les entreprises. Les couches de sécurité s'additionnent et favorisent le développement d'un environnement particulièrement hétérogène. De ce fait, l'expertise nécessaire peut-être difficile à acquérir en interne et surtout difficile à maintenir à un niveau élevé, pour identifier et contrecarrer ces menaces.

Pour IDC, le recours aux services managés de sécurité ne concerne pas uniquement l'exploitation technique des solutions déployées, il s'agit également de définir les règles de sécurité afin que celles-ci soient en accord avec les besoins des métiers et avec les contraintes réglementaires auxquelles les entreprises sont soumises.

Le recours progressif à des services managés s'accompagne de précautions importantes de la part des entreprises, signe que celles-ci disposent d'une véritable maturité sur le sujet. Ainsi, la localisation des données hors de l'entreprise et le traitement des données à la fin du contrat (réversibilité) constituent des sujets sensibles. De même, la sécurité ne concerne pas que celle des entreprises, elle porte également sur les fournisseurs de services managés face aux risques de fuites d'informations confidentielles.

GLOSSAIRE

- **APT (Advanced Persistent Threat)** : les APT désignent des menaces complexes combinant souvent différents vecteurs et stratégies d'attaques, pouvant utiliser des techniques inconnues ou des failles zero day, durant assez longtemps sans être détectées, et la plupart du temps ciblées.
- **BYOD (Bring Your Own Device)** : Apportez vos appareils personnels
- **CYOD** : Choose Your Own Device
- **IAM (Identity and Access management)** : La gestion des identités et des accès sollicite plusieurs technologies et processus interdépendants. Ces éléments s'associent pour donner une vue unifiée des identités d'une entreprise et les utiliser efficacement. Les principaux thèmes de la gestion des identités et des accès à étudier sont les services d'annuaire, la gestion du cycle de vie des identités, la gestion des accès et le mode d'intégration des applications à l'infrastructure.
- **IoT (Internet of Things)** : Internet des Objets
- **IPS (Intrusion Prevention System)** : est un outil permettant de prendre des mesures afin de diminuer les impacts d'une attaque. Ils sont capables de détecter un balayage automatisé, l'IPS peut bloquer les ports automatiquement. Les IPS peuvent donc parer les attaques connues et inconnues.
- **NAC (Network Access Control)** : Un contrôleur d'accès au réseau est une méthode informatique permettant de soumettre l'accès à un réseau d'entreprise à un protocole d'identification de l'utilisateur et au respect par la machine de cet utilisateur des restrictions d'usage définies pour ce réseau.
- **UTM (Unified Threat Management)** : terme inventé par Charles Kolodgy du cabinet de conseil IDC (International Data Corporation) en 2004 et utilisé pour décrire des pare-feu réseau qui possèdent de nombreuses fonctionnalités supplémentaires qui ne sont pas disponibles dans les pare-feux traditionnels.
- **VPN (Virtual Private Network)** : Réseau privé virtuel

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

IDC France

13 Rue Paul Valéry
75116 Paris, France
+33.1 56.26.26.66
Twitter: @IDCfrance
idc-insights-community.com
www.idc.com / www.idc.fr