

Sécurité informatique : les grands groupes font confiance aux marques, les PME sont à la traîne

- Une quinzaine d'acteurs se partagent un marché essentiellement constitué de grands groupes.
- Des solutions efficaces à moindre coût développées par des start-up, ou en open source, sont disponibles.
- Les multinationales essaient d'investir le créneau des PME/TPE avec des solutions bon marché.

La sécurité informatique est une niche dans l'écosystème informatique. Une quinzaine d'acteurs (multinationales partenaires d'entreprises locales), se partagent le marché marocain constitué essentiellement de grands comptes. On ne connaît pas la taille du marché. Mais une chose est sûre : le segment des prestataires locaux est très fragmenté et constitué d'acteurs qui sont parfois de très petite taille. La demande existe. Abdelilah Nejari, DG de Cisco Systems Moyen-Orient et Afrique, confirme que la sécurité informatique (cybersécurité) représente une part importante du marché des grands éditeurs au Maroc. « Nous avons remarqué une forte croissance de l'activité sécurité durant les dernières années. D'autant plus que la cybersécurité est au cœur des préoccupations de nos clients à tous les niveaux, directeurs généraux, directeurs métiers et directeurs informatiques. En tout cas, les projets d'infrastructure que nous réalisons avec nos clients ont quasiment toujours une composante sécurité intégrée », explique M. Nejari. Même son de cloche chez Microsoft, autre acteur international reconnu de la sécurité informatique. « Les grandes entreprises sont conscientes de l'importance de la sécurité informatique pour la protection des données, le filtrage, le backup... Par contre, pour les PME, la sécurité est perçue comme une assurance sans retour sur investissement », déclare Hicham Iraqi Houssaini, directeur général de Microsoft Maroc. A cet égard, Younes El Himdy, DG de Disty Technologies, explique la réticence des PME/PMI à la cybersécurité par une prise de conscience qui tarde à venir. « Les PME/PMI ne sont pas conscientes de l'importance de la sécurité dans la protection de leur parc informatique. Par conséquent, elles n'engagent pas l'investissement nécessaire », déclare-t-il. Les

risques qu'elles courent sont pourtant énormes.

Le coût de la non-protection est souvent très élevé

Des entreprises non protégées ont déjà été victimes de cyber attaques, souligne Hicham Iraqi Houssaini, DG de Microsoft Maroc. « Les hackers cryptent toutes les informations de l'entreprise et demandent une rançon en crypto monnaie pour débloquer le système. C'est suite à ce type d'expérience que les PME recourent à la sécurité informatique. A ce moment-là, le prix devient secondaire », affirme-t-il. Autre exemple courant : celui du vol de base de données par des stagiaires dans les agences de communication. Pour ce type de risques, « il existe des solutions pas chères adaptées aux besoins des PME pour, à titre d'exemple, limiter les accès à certaines personnes pour certaines applications et pour des machines identifiées », fait savoir Karl Stanzick, DG de MTDS, entreprise spécialisée dans la sécurité informatique, précisant que « tous les maillons de l'entreprise doivent être impliqués dans la décision d'opter pour un système donné, y compris le top management



de la PME qui ne connaît pas forcément les failles de sécurité auxquels il est exposé ». Ignorance qui peut être chèrement payée. « L'entreprise a besoin de connaître ses problèmes pour pouvoir minimiser ses coûts », souligne Amine Cherrai, fondateur de Hackingbyte, start-up de sécurité informatique. D'après lui, une PME n'a pas besoin d'un million de dirhams pour protéger son système informatique. « Elle peut faire appel à une solution open source gratuite dont le fournisseur de sécurité informatique

délivre la clé de sécurité et le support », déclare-t-il.

Solutions conventionnelles

Pour M. Stanzick, une solution open source nécessite un développeur à plein temps dans l'entreprise. « C'est la raison pour laquelle nous avons du mal à proposer aux grands comptes des solutions open source. Ils préfèrent acheter des marques car en cas de problème, ils peuvent directement s'adresser à l'éditeur. Mais nous essayons de convaincre les DSI à poser les questions sur l'avantage des solutions de grands éditeurs. S'ils ne sont pas satisfaits, pourquoi ne pas faire appel à la valeur ajoutée locale et s'engager avec les jeunes. Les entreprises sont malheureusement réticentes à leur faire confiance », déplore le DG de MTDS. Mais les grandes marques veulent aussi prendre une part du marché des PME/TPE. Cisco, qui travaille avec des intégrateurs, souhaite investir ce créneau mais se heurte au manque d'ingénieurs spécialisés dans la sécurité informatique sur le marché. « Avec des audits de sécurité, on peut convaincre ces clients d'investir plus dans la sécurisation de leur SI. Et pour pallier le manque de ressources spécialisées chez les TPE/PME, nos intégrateurs

mettent en avant des offres de « Solutions Gérées » (Managed Solutions) », précise M. Nejari.

Microsoft propose, quant à elle, aux PME/PMI des solutions cloud dont le coût a graduellement baissé. C'est en quelque sorte une approche identique qu'a adoptée Amine Cherrai. Il espère orienter les PME/TPE, encore réticentes à la sécurité informatique, vers des solutions adaptées à leurs besoins et réduire ainsi les dépenses de sécurité. « Pour le moment, 80% de mon activité est réalisée avec des entreprises étrangères, allemandes et françaises. J'aspire à attirer dès la fin de l'année des entreprises marocaines qui peinent encore à faire confiance à des start-up locales », espère-t-il. Le changement de mentalité prendra du temps. Les DSI préfèrent encore aujourd'hui s'adresser aux acteurs du secteur qui proposent des solutions conventionnelles et reconnues. « La sécurité informatique, c'est d'abord du conseil, un cahier des charges et des outils qui permettent de choisir des solutions. Les meilleures sociétés de conseil ne sont pas liées à un éditeur. Elles choisissent l'outil en fonction du besoin du client », résume M. El Himdy ■

WIAM MARKHOUS

La protection du mobile, un nouveau casse-tête

Les grands éditeurs de la sécurité informatique se tournent aujourd'hui vers le mobile. Avec la mobilité, les employés sont amenés à travailler à distance par smartphone. « La cybersécurité est plus compliquée sur ce type d'appareil. C'est la raison pour laquelle les éditeurs sont en train de développer des solutions adaptées, notamment pour sécuriser le transfert d'information et l'accès aux canaux de messagerie de l'entreprise par le biais du mobile... », déclare M. Iraqi Houssaini, DG de Microsoft Maroc. Par ailleurs, vu la complexité des cyber attaques même pour les entreprises ayant investi des millions de dollars par an pour sécuriser leur SI, Cisco a, elle, conçu une solution idoine. « Nous permettons à nos clients d'identifier rapidement l'étendue de l'attaque, retracer sa trajectoire et ainsi aider à nettoyer le SI de cette intrusion », déclare M. Nejari ■