Information Presse

AL'X COMMUNICATION - Véronique Loquet
06 68 42 79 68 vloquet@alx-communication.com

LE CESIN S'INQUIETE DE L'EXTREME CONCENTRATION DES FOURNISSEURS DE SOLUTIONS DE CYBERSECURITE ANGLO-SAXONS SUITE AU RECENT RACHAT DE DARKTRACE PAR THOMA BRAVO

La série d'acquisitions stratégiques menées par le Fonds de capital-risque américain, met en lumière les risques pour la cybersécurité des entreprises et la souveraineté technologique européenne.

Paris, le 19 juin 2024 – Après Ping Identity puis Sailpoint, tous deux spécialisés dans l'IAM, Proofpoint pour la sécurité des messageries, Sophos pour la protection endpoints et réseaux, Imperva[1] ou encore Veracode pour la protection applicative, c'est au tour de Darktrace de passer dans le giron de Thoma Bravo, société d'investissement américaine. A ces acquisitions de fleurons de la cyber, s'ajoutent au palmarès de Thoma Bravo une série de rachats comme Barracuda, Blue Coat, Entrust, ForgeRock, Illumio, LogRhythm ou encore Sonicwall pour les plus connus.

Lorsque l'on examine de près ce portefeuille, on observe que cette tendance d'acquisitions vise à couvrir tout le spectre de la cybersécurité dans la stratégie de Thoma Bravo.

Si l'on a l'habitude de s'inquiéter à juste titre, du monopole exercé par les GAFAM sur le numérique, on serait bien avisé de se pencher sur la domination croissante de Thoma Bravo dans le secteur hautement sensible de la cybersécurité. En concentrant autant de solutions sous un seul acteur, cela entraîne un phénomène prévisible d'augmentation des coûts une fois la concurrence éliminée (on a tous en tête le précédent de Vmware), mais surtout, tous les flux sensibles des activités digitales des entreprises mondiales vont être entre les mains d'un unique acteur. Nous savons que les solutions de cybersécurité actuelles, pour la plupart en mode Saas, sont de plus en plus intrusives. Elles ont, by design, une visibilité importante sur les actifs qu'elles protègent, et une capacité d'action sur ces systèmes d'information à travers des fonctions de blocage, filtrage, mise en quarantaine, modification des accès, ou simplement parce que ce sont des composants placés sur un chemin critique qui ouvre l'accès au SI. L'ensemble de ces solutions acquises par Thoma Bravo fait ainsi de ce fonds un acteur stratégique dont les décisions pourront avoir un impact important.

Cela concerne les flux réseau, les flux applicatifs, les mails, les flux Internet, … Ce ne sont certes pas directement les données d'entreprises comme celles stockées chez les GAFAM qui seront aux mains de Thoma Bravo, mais peut-être pire encore, tous les flux sur les usages de millions de salariés d'entreprises.

1 Thales a racheté Imperva auprès de Thoma Bravo pour 3,6 milliards de dollars en décembre 2023

Le second sujet d'inquiétude porte sur l'évolution de ces solutions en général. Les solutions de cybersécurité ont besoin de bénéficier constamment d'une forte dynamique d'innovation, pour pouvoir faire face à une menace cyber qui évolue rapidement. Il est très important que les efforts de maintenance, de sécurité, de R&D et d'agilité dans le domaine de la cybersécurité ne soit pas freinés par la politique de haute rentabilité à court terme d'un Fonds, car cela entraine inévitablement une hausse des vulnérabilités.

De nombreuses entreprises évitent de dépendre d'un seul fournisseur de cybersécurité et se retrouvent finalement piégées par ces acquisitions successives.

La croissance rapide du secteur[2] devrait encore accentuer cette pression sur le marché européen. Ce phénomène fragilise la capacité de l'Europe à protéger ses intérêts stratégiques et accentue encore sa dépendance technologique vis-à-vis des acteurs étrangers. Un frein supplémentaire pour développer une cybersécurité souveraine et indépendante.

75% des répondants à une enquête CESIN réalisée en mai 2024 auprès de ses membres, se déclarent inquiets de cette concentration de solutions.

C'est pourquoi Le CESIN appelle les pouvoirs publics mais aussi les entreprises à prendre conscience des risques de cette extrême concentration. L'offre cyber « made in France » reste encore heureusement diversifiée et indépendante et peut, dans certains cas, offrir une alternative… mais dans un contexte où les grandes acquisitions étrangères se multiplient, il est nécessaire de se demander pour combien de temps ?

L'Europe doit agir de manière proactive, à la fois pour protéger ses organisations et garantir une cybersécurité indépendante et robuste, et pour permettre à l'innovation de pouvoir rivaliser. Il est essentiel de mettre en place des mesures adaptées pour prévenir la dépendance involontaire et sécuriser les infrastructures critiques face à des menaces croissantes.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.
Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels.

Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC), Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.
Le CESIN compte plus de 1 000 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. ***Pour en savoir plus*** **www.cesin.fr**

2 Coûts liés à la cybercriminalité estimés à 8 000 milliards de dollars, tandis que l'expansion du marché mondial de la cybersécurité est estimé à 1,5-2000 milliards de dollars selon le dernier rapport McKinsey.