Maddy Keynote 2024 : l'industrie logicielle à l'heure du RGPD et de la cybersécurité

Entre des contraintes réglementaires de plus en plus fortes et des cyberattaques qui ne cessent de se multiplier, l'industrie software est confrontée à des défis d'ampleur. Mais si ces derniers sont évidemment sensibles, ils sont aussi sources d'opportunités. Startups et fonds d'investissement nous éclairent sur le sujet lors d'une table ronde de l'édition 2024 de la Maddy Keynote.

Temps de lecture : minute

12 avril 2024

Loin de se limiter au software, les problématiques liées à la cybersécurité touchent toutes les industries en phase de digitalisation. *« Les cyberattaques sont souvent liées à l'évolution des infrastructures »*, avance Evgenia Plotnikova, General Partner chez Dawn Capital. *« Au fur et à mesure que les logiciels pénètrent dans l'économie réelle, les risques cyber augmentent »*, ajoute-t-elle sur la scène de la Maddy Keynote, le jeudi 28 mars.

Avec les récentes attaques et l'accueil des Jeux Olympiques de 2024, les entreprises françaises sont plus que jamais sur le qui vive. *« Le gouvernement et les entreprises se préparent déjà depuis un certain temps. Avec le télétravail massif, beaucoup de transactions se feront en ligne. Il faudra être capable de sécuriser à l'échelle sur un pic de temps donné »*, commente Alban Sayag, CEO de Yousign.

Cybersécurité : des menaces grandissantes qui exigent des niveaux de sécurité renforcés

Les experts sont d'accord : les menaces augmentent et les cybercriminels sont de plus en plus sophistiqués. L'attaque de SolarWinds en 2020 reste l'un des exemples les plus frappants de cyberespionnage de l'histoire récente, mettant en évidence les risques de sécurité liés à la chaîne d'approvisionnement et la complexité de la cybersécurité à l'ère numérique.

« La cybercriminalité n'a pas de loi. Aujourd'hui, les attaques sont fulgurantes et peuvent faire des dégâts énormes. Il faut que la cyberdéfense soit au moins à la hauteur de ces attaques », insiste Éléna Poincet, fondatrice et CEO de Tehtris. *« C'est une course de fonds. Si nous étions capables jusque-là d'assurer sans faille l'intégrité de certaines données, aujourd'hui, le monde du quantique vient rebattre les cartes »*, souligne Alban Sayag.

Pour se défendre face à ces attaques cyber, l'intelligence artificielle peut être salvatrice. *« Aujourd'hui, l'un des enjeux est de repérer les signaux faibles d'attaques furtives. C'est quelque chose de difficile pour les éditeurs de logiciel, et l'IA peut être d'une grande aide sur ce sujet »*, explique Éléna Poincet. Mais l'IA est à double tranchant et joue son rôle dans l'augmentation des menaces cyber. *« Dès qu'on entraîne une IA à quelque chose de nouveau, rien ne l'empêche par la suite d'utiliser ses nouvelles connaissances à mauvais escient. Aujourd'hui, nous sommes dans un combat IA contre IA où il faut être le plus fort »*, explique Éléna Poincet.

Face à ces menaces grandissantes, toutes les entreprises ne sont pas équipées de la même manière. *« Quand on pense à Yousign, on pense instinctivement à la signature. Mais notre mission est plus large, elle vise à sécuriser l'ensemble des transactions électroniques pour nos clients »*,

précise Alban Sayag. *« Notre ambition est de donner au plus grand nombre des moyens à la hauteur des menaces. Les sociétés du CAC 40 sont pour la plupart bien équipées, mais les ETI sont aussi des victimes potentielles et doivent avoir accès à la protection. Pour cela, il faut créer des produits faciles à utiliser et financièrement accessibles »*, ajoute-t-il.

Menaces internationales, réglementation européenne

En parallèle, la liste des contraintes réglementaires de cesse de s'allonger en Europe : RGPD sur la protection des données, la directive NIS, sur la sécurité des systèmes d'information, le Digital Services Act qui encadre l'activité des grandes plateformes numériques, l'eIDAS sur les signatures électroniques. *« Et la liste risque encore de s'allonger ! »*, commente Éléna Poincet.

« Ces réglementations sont positives dans le sens où elles permettent d'améliorer la conservation des données et leur utilisation », admet Éléna Poincet. *« Mais ces obligations réglementaires ne s'appliquent pas aux softwares du monde entier. Si elles sont bénéfiques pour les clients, d'un point de vue business, c'est assez pénalisant »*, rappelle-t-elle. *« Tout le monde parle de souveraineté, mais dans les faits, tout n'est pas mis en place pour qu'on y arrive. On aimerait un mouvement européen plus fort »*, regrette-t-elle encore. *« Pour ne pas nuire à l'innovation, il serait peut-être plus intéressant de réguler les résultats plutôt que les process »*, propose Evgenia Plotnikova.

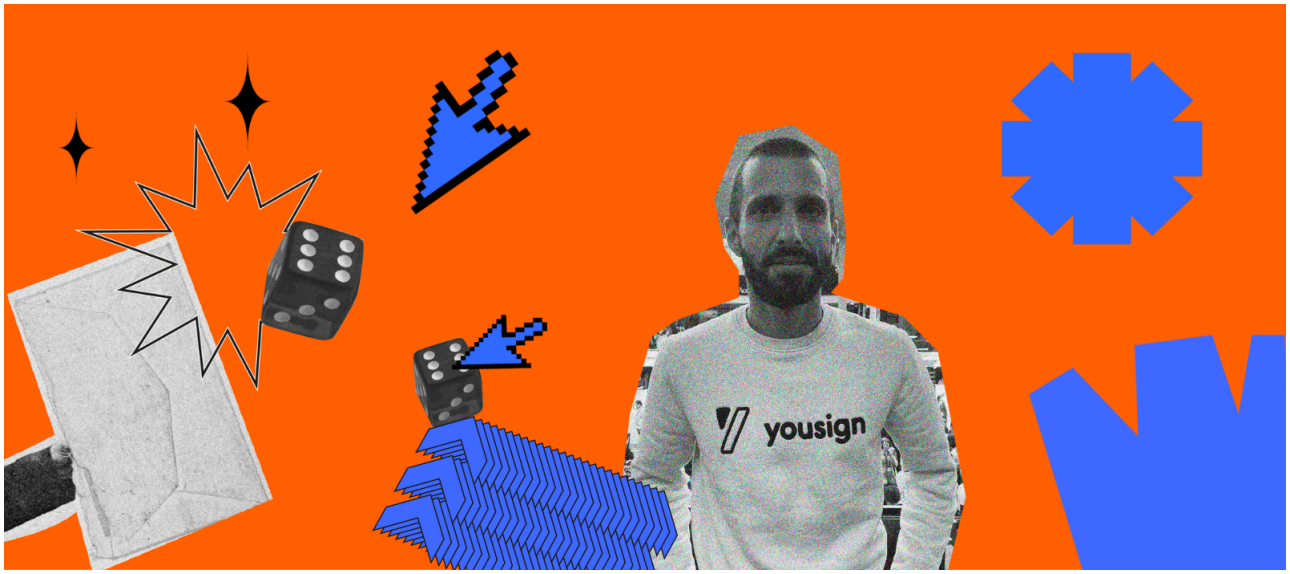
En effet, contrairement au marché américain, un éditeur de logiciel qui souhaite se développer en Europe fait face à des barrières juridiques, administratives et culturelles importantes. *« Il y a un cadre européen relativement contraignant, et en plus de cela, les champs d'applications nationaux sont parfois différents. Dans certains cas, cela peut même conduire à de la concurrence déloyale entre certains pays d'Europe »*,

alerte Alban Sayag. Mais ce dernier reste tout de même optimiste sur son secteur. *« En termes d'identité numérique, les choses vont dans le bon sens avec le travail mené sur une identité numérique européenne »*, déclare-t-il.

Satisfaction clients, cybersécurité et protection des données : trouver la bonne équation

Dans un secteur aussi réglementé que celui des logiciels, les contraintes en termes de développement produits sont accrues. *« On ne peut pas avoir la même vélocité qu'une équipe tech ou produit d'un autre secteur. Tout l'enjeu est de savoir comment encapsuler de nouvelles fonctionnalités dans un produit user-friendly, tout en respectant les contraintes réglementaires »*, synthétise Alban Sayag. *« C'est ce que nous regardons en tant qu'investisseur : la capacité à trouver le bon dosage entre protection et facilité d'utilisation »*, confirme Evgenia Plotnikova.

Yousign observe une évolution des comportements chez ses clients. *« Les clients renforcent leur sécurité, non seulement parce qu'ils y sont contraints par la réglementation, mais aussi, car ils souhaitent volontairement sécuriser leurs documents ou leurs transactions les plus critiques »*, partage Alban Sayag. Par ailleurs, il sent que les clients sont de plus en plus sensibles à l'aspect de la souveraineté. *« Il ne suffit pas d'avoir une plateforme avec une infrastructure en France ou en Europe, si le pays d'origine de l'éditeur est régi par d'autres lois, les données peuvent partir ailleurs »*, précise Alban Sayag, qui se retrouve souvent en concurrence face à l'américain DocuSign. *« Sur les transactions les plus délicates, certains clients veulent vraiment que leurs données soient gérées par un acteur français ou européen »*, ajoute-t-il.



À lire aussi

Dix ans après sa création, Yousign veut aller au-delà de la signature électronique

MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M'INSCRIS

Article écrit par Maddyness avec Yousign