

Ces 2 nouvelles tendances dans la sécurité informatique que devez absolument connaître | Le Net Expert Informatique

✖ Ces 2 nouvelles tendances dans la sécurité informatique que devez absolument connaître

Deux tendances appelées DevOps et DevSecOps sont apparues aux Etats-Unis ces dernières années dans le but de favoriser la collaboration, et se font progressivement une place dans les modèles de travail des entreprises en matière de sécurité informatique.

La nécessité d' «agir ensemble » est l'un des messages forts de l'Agence Nationale de la Sécurité des Systèmes d'Information en cette fin d'année. Lors des Assises de la sécurité 2015, Guillaume Poupard, directeur général de l'ANSSI, soulignait le rôle clé de la collaboration – locale et internationale – pour optimiser la sécurité de nos entreprises et plus encore de nos Opérateurs d'Importance Vitale (OIV).

Deux tendances appelées DevOps et DevSecOps sont apparues aux Etats-Unis ces dernières années dans le but de favoriser la collaboration, et se font progressivement une place dans les modèles de travail des entreprises en matière d'informatique. En quelques mots, le DevOps est avant tout un concept et une philosophie que les entreprises sont complètement libres de s'approprier. Au sein d'une même entreprise, cela se traduit par la mise en place d'un groupe de travail composé de différentes entités (équipe réseaux, équipe projets, équipe sécurité pour le DevSecOps, etc.) pour collaborer sur un projet de développement spécifique. A une échelle plus large, le DevOps a pour vocation de favoriser la collaboration et le partage d'informations entre les entreprises, parfois même concurrentes. Ainsi, en partageant plus et mieux leurs données, les entreprises enrichissent mutuellement leurs solutions (applications, logiciels, etc.) et accélèrent ainsi leur développement et leur business.

La tendance du DevOps est en train d'être adoptée progressivement par les entreprises (25% des plus grandes entreprises mondiales sont déjà en train de l'adopter selon le Gartner). Les entreprises françaises semblent s'y intéresser également dans le cadre de projets bien spécifiques. Le Cabinet Vanson Bourne a ainsi établi que 95% des sociétés françaises planifient actuellement la mise en œuvre du DevOps afin d'accélérer le développement d'applications. Le DevOps c'est bien, mais le DevSecOps c'est mieux... Le DevSecOps est tout simplement une extension du DevOps où la sécurité est intégrée au sein de projets collaboratifs dès le démarrage avec pour objectif d'augmenter le niveau de sécurité des projets (applications, produits, etc.). Pour l'entreprise, il s'agit de bénéficier d'une sécurité plus agile, et plus largement de collaborer avec d'autres entreprises sur un même marché pour augmenter le niveau de sécurité de ses futures solutions.

Cette tendance du DevSecOps peine à être adoptée en France. Comme souvent lorsque l'on parle de sécurité, les entreprises françaises ne sont pas aux avant-postes. Alors que le Gartner recommande de mieux intégrer la sécurité dans tous projets IT et que l'ANSSI fait de la collaboration l'un des grands axes de son discours auprès des entreprises et des professionnels de la sécurité, nos entreprises vont-elles enfin s'ouvrir à plus de collaboration et adopter massivement ces tendances ?

Les entreprises ont tout intérêt à adopter ces tendances

Sur le plan de la sécurité, les entreprises ont tout à gagner à adopter rapidement la tendance DevSecOps. Cela leur permettrait d'arriver plus rapidement à un très bon niveau de sécurité, et surtout à des délais de traitement des incidents beaucoup plus rapides.

Nous savons désormais que toutes les entreprises seront victimes d'une attaque informatique un jour ou l'autre, et que ces attaques peuvent avoir de sérieuses conséquences. Il s'agit donc de limiter la période de détection et de remédiation. Avec des organisations traditionnelles, ces délais sont trop longs et plus acceptables face à l'intensité de la menace actuelle. C'est aux responsables de la sécurité qu'il revient de faire adopter ces tendances dans leur entreprise.

Les silos, le problème récurrent (et culturel) des entreprises françaises

En France, les entreprises sont fortement pénalisées par des fonctionnements en silos pour leurs ressources IT (équipements / réseau). Sur un plan humain, les équipes projets, les métiers, ou encore la sécurité travaillent la plupart du temps chacune de leur côté, sans échanger les unes avec les autres. Le tout avec une gouvernance qui n'est généralement pas centralisée.

En France et en Europe, ce mode de fonctionnement, souvent hérité, est un problème maintes fois pointé du doigt, car il entraîne un vrai facteur de blocage de l'innovation et de la collaboration dans et pour nos entreprises.

L'arrivée des tendances DevOps et DevSecOps peuvent nous laisser penser que les choses pourraient changer et que les barrières liées aux silos soient levées, pour permettre aux équipes de travailler ensemble.

Aux Etats-Unis, la collaboration est devenue une arme business

Lorsque les entreprises américaines ont pris conscience des perspectives business offertes par un travail plus collaboratif, même entre concurrents, elles ont rapidement établi de nouvelles approches (Kill chain par exemple et maintenant le DevOps/DevSecOps). Ainsi, ces grandes entreprises s'enrichissent du travail des autres pour accélérer leurs développements respectifs. Au final, elles ont simplement compris que l'outil informatique était un facilitateur de business.

Les grands groupes de l'IT tels que Google, Amazon ou encore LinkedIn ont fait partis des pionniers en la matière, et ils ont ensuite rapidement été suivis par des grandes organisations, telles que la NASA, Starbucks, etc.

En France, nous sommes encore loin de ce niveau de collaboration, même si nos start-ups suivent de plus en plus cette mouvance, d'enrichissement de la donnée par des solutions complémentaires, pour obtenir des niveaux de détection plus fins et des temps de remédiation plus rapides. C'est une excellente approche, qui permet d'aller dans le bon sens, notamment en matière de sécurité. Dans les années à venir, le Cloud devrait être un moteur important de cette tendance DevSecOps, puisqu'il va permettre de plus en plus d'automatiser la sécurité.

Le DevSecOps offre de multiples avantages

Le DevSecOps a pour finalité d'optimiser la sécurité et le business des entreprises et plus globalement, le niveau de qualité des technologies de sécurité du marché.

Concrètement, le DevSecOps permet aux entreprises et aux professionnels de s'ouvrir aux autres, et en interne d'accélérer l'automatisation, pour notamment mieux utiliser les ressources humaines sur des tâches d'optimisation de fonds. Le DevSecOps c'est aussi mieux protéger les clients finaux grâce à une sécurité renforcée grâce à une sécurité basée sur des critères objectifs, puisqu'elle est définie sur la base d'un travail collaboratif avec les diverses entités (réseau / métiers / sécurité, etc.), et beaucoup plus orientée sur les nouvelles menaces.

En terme de conformité, DevSecOps permet également de faire le lien entre les experts qui gèrent la sécurité dans des SOC (Security Operations Center) et les opérationnels de l'entreprise, ce qui apporte un avantage indéniable en matière de sensibilisation sur les questions de sécurité.

Ces tendances sont à notre disposition, il ne tient qu'à nous de nous les approprier !

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet... ;
- **Consultant en sécurité informatique**, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : <http://bfmbusiness.bfmbtv.com/01-business-forum/ces-2-nouvelles-tendances-dans-la-securite-informatique-que-devez-absolument-connaître-922865.html>
Par Arnaud Cassagne