Sécurité et risques du monde digital : Bilan d'une situation explosive selon Nicolas J. Lecocq, expert du digital et du secteur IT

Alors que l'univers du numérique évolue à la vitesse de la lumière, le domaine de la sécurité semble être resté à l'âge de pierre.

Nous en sommes désormais à l'ère du "machine learning" : grâce à l'intelligence artificielle, les appareils numériques ne se contentent plus d'appliquer des programmes, ils "apprennent" automatiquement à partir de données pour améliorer leurs performances. Ils deviennent ainsi capables de résoudre certaines tâches pour lesquelles ils n'ont pas été explicitement programmés.

Cette technologie présentant de nombreux avantage, elle n’est cependant pas sans risques. Les machines analysants plus vite que l’humain, celles-ci vont reproduire et traiter les données plus rapidement, ce qui peut mettre à mal tous les systèmes de sécurité basés sur les interventions humaines.

Nicolas J. Lecocq, Senior IT Executive et spécialiste reconnu dans le domaine des nouvelles technologies et celui du digital, souligne :

> *Désormais, le maillon le plus faible peut potentiellement faire casser toute la chaîne de sécurité ! La méthodologie ayant changé, le temps des grosses applications monolithiques est révolu. Aujourd'hui, nous faisons face à des micro-services qu'il faut sécuriser de bout en bout.*

Nicolas J. Lecocq

Une nouvelle génération des systèmes de Security Centers

Pour être réellement efficaces, les systèmes de Security Centers doivent passer à la vitesse supérieure.

Cela suppose notamment de mettre en place :

- Un monitoring et de la gestion événementielle pour surveiller les variations de l'activité informatique
- Une technologie de pointe, pour avoir des outils aussi performants que ceux des hackers
- Une détection des failles via l'intelligence artificielle (IA)
- Une politique d'anticipation : il faut être capable de faire du prédictif ! Ainsi, en fonction des événements, il est possible de se préparer à l'avance à une recrudescence sur certains sites. Imaginons par exemple une OPA d'une entreprise A sur une entreprise B. Dans ce cas, il y a aura une augmentation des attaques sur l'entreprise B.

Dans ce contexte, les professionnels du développement applicatif vont devoir s'adapter. Une nouvelle discipline va ainsi voir le jour car la sécurité ne sera plus rajoutée a posteriori, mais incluse dans le code dès le départ.

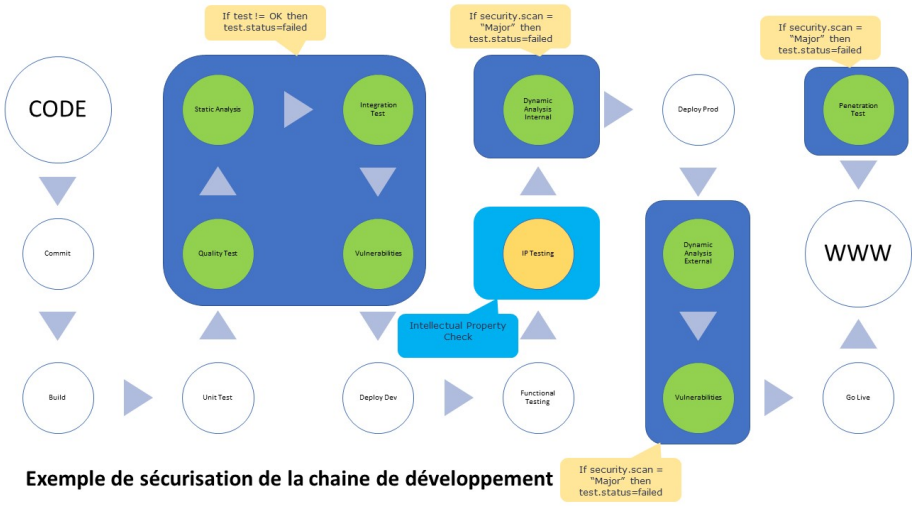
Etant donné que chaque application est désormais accessible au plus grand nombre, il est indispensable de vérifier chaque étape de l'infrastructure, y compris côté utilisateur, pour s'assurer que tous les modèles de sécurité ont été intégrés.

La sécurité : un facteur-clé de compétitivité

Plus le développement est compliqué, plus le coût est élevé. Surtout que la sécurité ne s'arrête pas à la conception de l'application !

Prenons l'exemple d'un process standard. Un prestataire tiers va se charger de sécuriser l'ensemble des chaînes de développement, d'infrastructures, etc... Les coûts de maintenance et de tests…, risquent d'impacter le budget sécurité de l'entreprise.

Lorsque l'ensemble du process est validé, la veille sécuritaire peut alors être mise en place. Malheureusement, les entreprises choisissent d'ignorer cet aspect par méconnaissance des risques ou par volonté de limiter les dépenses.



Exemple de sécurisation de la chaine de développement

Il s'agit pourtant d'un très mauvais calcul financier et stratégique ! Tous les dirigeants doivent garder à l'esprit qu'un outil sécurisé aujourd'hui sera peut-être truffé de failles demain.

De plus, au-delà des risques liés à la perte de données (notamment juridiques et économiques), il y a un **vrai danger concernant la perte de la crédibilité et de la réputation de l'entreprise**. Subir une attaque entraînant la perte de données est préjudiciable sur le long terme puisqu'il est excessivement difficile de restaurer une relation de confiance avec ses clients et partenaires.

A titre d'exemple, tout le monde a encore en mémoire les récents scandales qui ont touché Facebook (entre autres) et concernant environ 50 millions de comptes ayant été affectés suite à une faille de sécurité (source). Les grosses structures ne sont pourtant pas les seules visées.

Plus vulnérables, les PME sont aussi des cibles privilégiées des hackers, celles-ci n'ayant pas les mêmes moyens financiers qu'une grande entreprise, il leur est difficile après une attaque de re-séduire leurs clients ainsi que redorer leur image.

Dès 2019 et dans les années à venir, la sécurité des données (de A à Z) va donc devenir un sujet majeur qui déterminera la compétitivité des entreprises françaises.

A propos de Nicolas J. Lecocq, expert des nouvelles technologies

Nicolas J. Lecocq est Senior IT Executive avec plus de 30 ans d'expérience dans la création de solutions innovantes (architecture d'entreprises, sécurité, infrastructures, applications , gestion de projets et de programmes, …).

Il a collaboré à l'international avec les plus grands groupes (Atos, Accenture, Cognizant Technology, Wipro Technologies, UBS, entreprises du Fortune 500 …) et géré des budgets de plusieurs millions de dollars.

Nicolas J. Lecocq dispose notamment de compétences en gestion, en marketing et en comptabilité qui lui permettent d'améliorer l'efficacité des programmes ou projets de 30%, de réduire les risques ainsi que de diminuer l'ensemble des coûts des programmes de transition et de transformation.

Pour en savoir plus

LinkedIn : https://www.linkedin.com/in/nlecocq/

Contact presse :

Nicolas J. Lecocq

E-mail : nlecocq@gmail.com

Tél. : +33 648 519 127