Sécurité et Agilité by design

Avis d'Expert par Carole Tessier, Responsable SMSI chez Oxalide

Faut-il sacrifier la sécurité au bénéfice des processus agiles ? Dans la course à la réduction du Time To Market, les objectifs du RSSI, du développeur et du chef de produit présentent à première vue certaines incompatibilités… idées reçues ou état de fait intangible ? Regardons au contraire l'agilité et la sécurité comme les deux facettes d'un cadre formel industrialisé au service de la qualité.

La sécurité, c'est facile. Il suffit d'y penser...

On pourrait croire qu'une entreprise ayant satisfait aux conditions d'obtention de la certification ISO 27001 devrait, en toute logique, ne pas avoir à s'interroger sur son respect au sein de son organisation. Cependant cette certification n'est délivrée que pour 3 ans. Elle est challengée tous les ans, mais aussi au quotidien. Bref, un seul mot d'ordre, ne jamais se reposer sur ses lauriers. Et pourtant…

Des lauriers qui sauraient vite faner si l'on ne s'appuie que sur des protocoles techniques sans prendre garde à la dimension humaine. Aussi brillant qu'étourdi, aussi inspiré que maladroit, aussi confiant dans son savoir-faire que parfois tête brûlée, l'être humain, reconnaissons-le, demeure la cause principale d'un incident en devenir. L'adhésion des hommes aux protocoles de sécurité reste la condition sine qua non pour corriger les effets de l'impétuosité humaine.

Enfin, sur une mer d'huile, le capitaine sait repérer le danger de loin. Sur une mer agitée, c'est une autre paire de manche. Or les processus agiles dans l'IT ont sensiblement modifié la donne dans tout le cycle de production. La fréquence des déploiements en production ou l'évolution des technologies n'est en rien comparable avec ce que l'on faisait il n'y a même pas 5 ans. Un gain de temps incroyable pour le business, mais une mer déchaînée quasi en permanence pour le capitaine du vaisseau qui doit alors trouver l'articulation idéale entre sécurité et agilité.

Oser le réflexe sécurité !

De quoi parle-t-on exactement ? Offrons-nous le plaisir de quelques exemples concrets, rencontrés fréquemment et dont la banalité n'a d'égal que le risque encouru. Qui dans l'entreprise a remarqué cette fenêtre mal fermée avant de partir ? Pourquoi la personne à proximité ne l'a pas fermée en partant ? Etait-ce un oubli ou bien n'a-t-il pas conscience de la gravité ? La personne ayant vu cette fenêtre ouverte a-t-elle enregistrée cette anomalie ?

Plus spécifique mais récurrent, il peut arriver qu'un client demande la levée d'une règle de sécurité sur son infrastructure. L'entreprise, cliente de longue date, est connue pour ce type de demande. Mais avant d'y répondre favorablement, s'est-on assuré de l'identité du demandeur ? A-t-on challengé le client sur motivation de sa demande ? L'exception à la sécurité a-t-elle été tracée ?

Dans le premier cas, l'accès aux locaux est critique pour la sécurité des données. Qui peut passer les protections de sécurité des locaux, peut accéder physiquement aux postes de travail des collaborateurs. C'est pour cela que différentes barrières sont mises en place : Alarme, vidéo surveillance, chiffrement des données sur les ordinateurs portables, sessions automatiquement lockées, etc.

Dans le second cas, c'est peut-être toute la stabilité de la plateforme cliente qui sera mise en péril. A celle dont le chiffre d'affaire est réalisé exclusivement sur le web, il n'est pas besoin de faire un dessin.

Qu'ont en commun ces deux situations ? L'appréciation du risque. Les réponses adaptées à chaque cas ne seront délivrées que si les collaborateurs ont comme premier réflexe « QUID de la sécurité ». Pour cela, il n'y a pas de miracle. La sensibilisation est quotidienne, dès les premiers jours dans l'entreprise. D'ailleurs, la certification ISO 27001 exige une sensibilisation régulière du personnel.

Mais est-ce suffisant ? Non, ça ne l'est jamais. De la formation aussi souvent que possible doit s'inscrire dans le processus mais plus que tout, c'est une question de réflexe. Le réflexe sécurité, c'est s'interroger sur l'action que l'on s'apprête à engager et oser saisir les bonnes personnes pour s'assurer de l'existence et de l'opportunité de la menace. Et ce, quelle que soit la menace.

La sécurité comme base de réflexion

C'est clairement ce qui est attendu de chacun mais ce n'est pas un processus franchement naturel.

Il y a d'abord les petits applicatifs gratuits à disposition sur le web public que l'on est tenté d'utiliser pour un besoin bien précis. Faut-il déranger le comité de sécurité pour si peu ? Oui trois fois oui, il est là pour ça. Au demeurant, il suffira peut-être de quelques minutes pour relire les conditions d'utilisation aux côtés de l'expert sécurité pour prendre une décision en accord avec les engagements de l'entreprise.

Ce que beaucoup voyaient comme une cruelle perte de temps devient progressivement une habitude qui rend l'entreprise un peu plus agile et sécurisée chaque jour. Car enfin, si personne ne voyait hier d'inconvénient à travailler avec certains outils grand public à la demande des clients, aujourd'hui, tout le monde sait se mettre en alerte dans ce type de situation, informer les bonnes personnes pour trouver ensemble une solution et réagir vite et efficacement.

Face à la multiplication des solutions web gratuites et par conséquent, face à la multiplication des risques de fuite de données, l'action concertée déclenchée par une démarche consciente axée sur la sécurité est la seule réponse valable. Car on a beau essayer, on ne configure pas l'automatisation de l'appréciation du risque d'un être humain !

L'amélioration continue, pierre angulaire de la sécurité comme de l'agilité

Les progrès réalisés en la matière par les équipes projet bien informées montrent à quel point l'entreprise reste véloce tout en relevant le niveau de sécurité, chaque jour un peu plus. C'est encore plus révélateur dans le cadre de l'industrialisation des processus informatiques.

Étonnamment, l'amélioration continue (Plan / Do / Check / Act) fait surtout parler d'elle dans les processus agiles. Il est vrai que les sprints donnent aux équipes le cadre idéal pour porter et développer un projet rapidement. Ces courtes séquences produisent des résultats concrets dont on relève le niveau de qualité à chaque nouveau cycle.

Or la prise en compte de l'aspect sécurité y trouve naturellement sa place. Le cadre de la norme ISO 27001 repose fortement elle aussi sur de l'amélioration continue. Le niveau de sécurité doit en permanence être relevé. Les deux méthodes s'associent naturellement ensemble.

En tout état de cause, la sécurité profite des processus agiles et plus généralement de l'industrialisation des processus. Un correctif est déployé en quelques minutes aujourd'hui sur un ensemble de serveurs, ce qui prenait des mois, parfois plus, avant l'industrialisation.

C'est d'autant plus crucial qu'au-delà des briques de sécurité essentielles posées par la certification, le monde de l'IT est en mouvement permanent, et oblige chacun à penser au risque et à son évolution en continu.

Chacun ? oui. Même le client et surtout le client. Ses applicatifs sont d'ordinaire plus menacés que son infrastructure. Ce sera donc à lui d'arbitrer sur l'opportunité d'inclure au prochain sprint planifié la correction des failles de sécurité détectées par son prestataire ou la mise en place de contres mesures pour mieux maîtriser ses risques. En d'autres termes, il n'y a plus à hésiter, parce que sécurité et agilité se renforcent mutuellement, guidées par le principe d'amélioration continue.

A propos d'Oxalide

Oxalide est une société française, experte des infrastructures web critiques et leader de l'infogérance web DevOps. Depuis sa création en 2000, Oxalide a construit sa réussite sur une double expertise applicative (Varnish, Magento, Drupal, hybris, EZ Publish, etc.) et systèmes & réseaux, pour optimiser, en continu, les plateformes web de ses clients, tant en matière de performances et de scalabilité, que d'efficience. Cloud public, communautaire, privé ou serveur dédié, Oxalide accompagne ses clients sur tout type d'infrastructure : d'Amazon Web Services et sa flexibilité, à l'infrastructure Oxalide, multisite (3 datacenters), haute disponibilité et éligible à des Plans de Continuité d'Activité (PCA) et Plans de Reprise d'Activité (PRA). Parmi ses clients issus de tous les secteurs d'activités, Oxalide compte des grands noms des médias et du e-commerce tels que 20 minutes, Le Parisien, L'Express, ZDNet, Radio France, TagCommander, Kiloutou ou encore The Other Store.

http://www.oxalide.com/