Security by Design :
La sécurité ne s'ajoute pas, elle se conçoit

Par Pierre-Yves Guerder, consultant cybersécurité

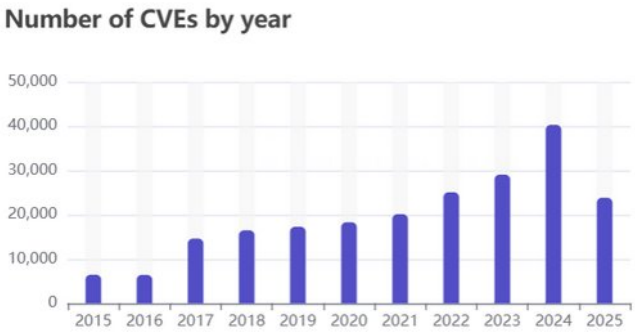
« Mon application est derrière un firewall ; elle est donc sécurisée. »
« Jamais un employé n'attaquera son entreprise ! »
« Si personne ne connaît mon application, personne ne peut l'attaquer. »

Et le Security by Design, alors ? La prise en compte de la sécurité au plus tôt est-elle une énième idée reçue, vouée à disparaître ?

Découvrons ensemble pourquoi cette démarche, lorsqu'elle est bien appliquée et par les bonnes personnes, constitue la première étape indispensable pour protéger nos SI face aux menaces cyber.

Principe de moindre privilège, séparation des responsabilités… ces principes sont connus depuis les années 1970 : l'article *The protection of information in computer system* par J. H. Saltzer et M. D. Schroeder a été cité par plus de 3800 publications scientifiques ! Depuis, ces concepts ont évolué et on parle aujourd'hui de **défense en profondeur** et de **besoin d'en connaître**.

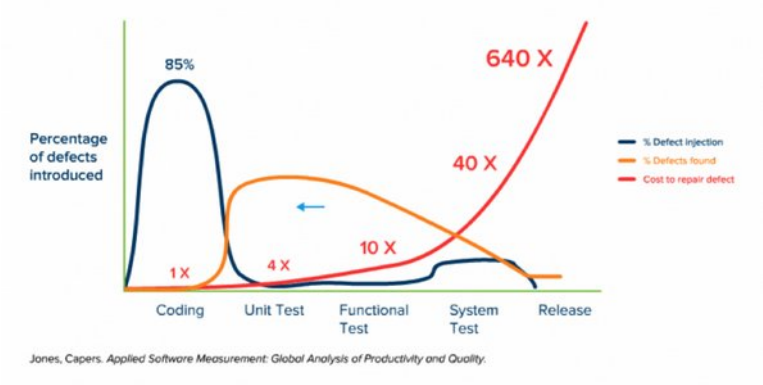
Malgré l'existence et la large diffusion de ces concepts, on constate encore aujourd'hui l'**omniprésence de failles de sécurité dans tous les systèmes** : le nombre de failles découvertes augmente chaque année, et 2025 ne fera pas exception : plus de 23 000 sur les 6 premiers mois ! Le site bonjourlafuite.eu.org recense les fuites de données déclarées par les entreprises françaises : pas une semaine ne s'écoule sans que la liste ne s'allonge.



Nombre de CVE (vulnérabilités) découvertes par année (6 premiers mois pour 2025).

L'approche ***Security by Design*** propose une explication à ce phénomène : la sécurité serait **prise en compte trop tard** ! Les systèmes d'information sont conçus puis réalisés puis déployés et ensuite seulement, les tests de sécurité sont effectués et les mesures adéquates mises en œuvre comme de simples correctifs. Les concepts précédents seraient donc **appliqués de manière réactive plutôt que proactive** et tout cela résulterait souvent d'une seule erreur : négliger la sécurité pendant la **phase de conception**.

Cette approche apporte également une réponse à la problématique de l'augmentation exponentielle du coût de correction d'un défaut (bug ou faille de sécurité) en fonction du moment de sa découverte : **traiter les sujets de sécurité au plus tôt permettrait de réduire considérablement le coût de la sécurité**, tout en aidant à respecter les plannings des projets.



Coût de correction d'une anomalie en fonction du moment de sa détection

Mais est-ce si simple ? **Suffit-il de décréter que la sécurité doit être prise en compte au plus tôt pour qu'un miracle nommé *shift left* opère ?** Suffit-il d'ajouter le mot « sécurisé » dans les spécifications pour que le *pentest* ne soit plus qu'une formalité ?

L'expérience acquise par Klee en 38 ans de développement de systèmes d'information nous montre que la **réussite de cette approche** dépend considérablement des **modalités de sa mise en œuvre** et des **méthodologies et outils** impliqués.

Nous présentons ici plusieurs **retours d'expérience et convictions** issus de cette expérience du terrain.

Former et impliquer les personnes

Ce sujet est trop peu évoqué lorsque l'on parle du *Security by Design*. Chez Klee, il constitue au contraire un des piliers de cette approche : pour une bonne prise en compte de la sécurité, **toutes les parties prenantes doivent être formées et se sentir impliquées**.

Former largement et de manière ajustée

Les formations proposées par Klee à ses équipes se déclinent en différentes **sessions adaptées à chaque public**, technique et non technique. Les collaborateurs sont sensibilisés aux enjeux mais également appelés à prendre conscience du rôle qu'ils ont à jouer sur leur périmètre de responsabilité : *scrum masters*, consultants fonctionnels, directeurs de projet, développeurs… Les problématiques complexes, pour être traitées dans leur intégralité, nécessitent que **plusieurs angles de vue** soient envisagés.

Créer du lien entre les équipes

Au-delà du seul contenu des formations, ces sessions ont plusieurs effets très bénéfiques comme une meilleure **connaissance mutuelle des équipes projet et des équipes cybersécurité**. D'une part, en créant davantage de liens, les équipes sont plus à même de se sentir accompagnées et n'hésitent pas à **solliciter les experts cyber** dès qu'une question pointue se pose à elles. D'autre part, ceci implique également davantage les experts qui connaissent donc mieux les projets.

Klee privilégie les **sessions en présentiel** afin de maximiser l'interaction entre les participants. Ceci donne lieu à de nombreux échanges qui sont autant de retours d'expérience permettant à différentes équipes projet de créer une connaissance collective de la sécurité et de mieux anticiper les sujets.

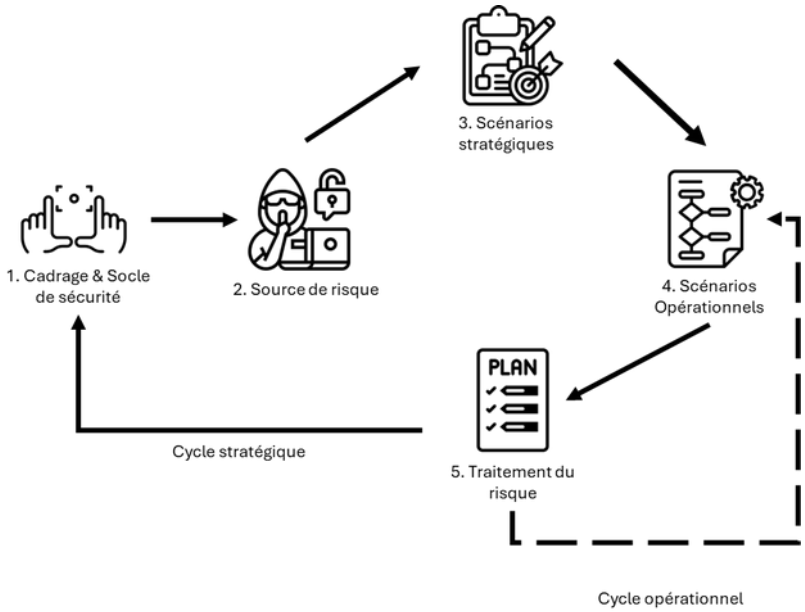
La formation et l'implication des personnes est ainsi une fondation sur laquelle peut être construite la suite du processus de *Security by Design*. La première étape de ce processus est l'identification des risques.

Anticiper les risques

L'anticipation des risques est l'essence du *Security by Design* : **chaque système d'information est unique** et possède son propre environnement humain, technique, organisationnel, etc. et ses propres besoins de sécurité qui se déclinent selon les quatre axes habituels : **Disponibilité, Intégrité, Confidentialité, Traçabilité**.

De l'analyse de risques au plan d'assurance sécurité

C'est l'**analyse de risques** qui permet de déterminer les biens support, événements redoutés, scénarios de menace et d'en déduire les mesures de sécurité à implémenter. L'**implication du métier** dans les ateliers et la **validation des mesures** par le RSSI sont essentielles pour disposer d'une base saine avant la phase de conception proprement dite.



Analyse et traitement du risque

Les mesures de sécurité résultant de cette analyse ne doivent pas se décliner seulement en **mesures techniques** mais également en **mesures organisationnelles** impliquant l'équipe projet et le client. Nous pensons que la manière dont l'équipe projet organise sa propre sécurité (gestion des accès et des secrets, exigences quant à l'anonymisation des jeux de données venant du client, etc.) fournit de bonnes indications quant à l'implémentation concrète de la sécurité dans le SI réalisé.

Impliquer les experts cyber dans la conception

Les mesures de sécurité sont formalisées par un **Plan d'Assurance Sécurité** qui sert d'intrant aux **ateliers de conception**. Lors de ces ateliers, il nous semble indispensable qu'un expert cyber soit présent et vérifie la bonne prise en compte de ces mesures lors de la traduction des demandes métier en *user stories* puis en maquettes. L'œil de l'expert permet également de vérifier que les ***user stories* ou les maquettes n'introduisent pas de nouveaux risques** ou failles qui n'auraient pas été anticipées, par exemple un *workflow* dont des étapes seraient contournables, l'introduction de champs « texte riche » ou de téléversements, etc.

Cependant, ces éléments ne sont pas suffisants pour détailler tous les risques. Ainsi, l'ANSSI recommande la rédaction d'***abuser stories***. Alors que les *user stories* modélisent l'expérience des utilisateurs légitimes, les *abuser stories* **étendent ce concept aux utilisateurs malveillants**. Ainsi, les problématiques de sécurité complexes telles que les cloisonnements horizontal et vertical et les ruptures de *workflow* peuvent être facilement comprises par toutes les parties prenantes, en respectant le formalisme usuel.

La **prise en compte des risques** dans tous les **aspects métiers** est une nécessité, mais **ne suffit pas** : le système d'information prend forme dans du code, qui instancie et orchestre des **briques techniques logicielles** exécutées par des machines virtuelles et équipements physiques : c'est là que l'aspect technique entre en jeu.

Limiter la surface d'attaque

Du point de vue technique, la mise en œuvre du *Security by Design* va faire jouer plusieurs leviers dont les principaux sont : **choix des briques techniques, analyse des demandes métier et sécurisation de l'infrastructure**, avec comme perspective de maîtriser voire réduire la surface d'attaque.

Choisir des briques saines

Le premier levier est constitué par le **choix des briques techniques**. L'utilisation de composants tiers dans le développement applicatif est aujourd'hui incontournable : s'appuyer sur des **composants éprouvés, bien intégrés et bien maîtrisés** par les développeurs permet d'obtenir une architecture logicielle cohérente et homogène et réduit la quantité de développements à effectuer. Elle **évite l'introduction de failles** qui seraient inévitables si des composants tels que briques d'authentification, chiffrement, couches d'accès à la base de données, etc. étaient redéveloppés spécifiquement pour un projet. L'impact sur la sécurité est ici très positif.

Cependant, faire appel à des composants tiers de mauvaise qualité, peu maintenus ou en quantité excessive aurait l'effet inverse. Une **sélection rigoureuse**, fondée sur des critères de **robustesse**, de **maturité**, de **support communautaire** ou éditeur doit avoir lieu et repose sur l'**expérience des *leaders* techniques**. Une **surveillance fréquente** de ces briques par un outil de *Software Composition Analysis* (SCA) est indispensable afin d'avertir au plus tôt l'équipe de la présence de CVE (vulnérabilités connues). Une politique de ***patch management*** est également nécessaire pour que le déploiement des correctifs de sécurité devienne une **routine maîtrisée** et non un événement exceptionnel.

Dans les meilleurs cas, le code développé se limite aux aspects purement métiers et des pans entiers à **fort impact sécuritaire** peuvent être fournis à une **brique dédiée** qui peut elle-même être auditée spécifiquement. C'est le cas par exemple lors de l'utilisation de Keycloak pour l'authentification : le **code spécifique** au projet est **presque inexistant** et la configuration de Keycloak peut faire l'objet d'une analyse par des experts pour vérifier que les meilleures pratiques sont appliquées.

Challenger les demandes métier

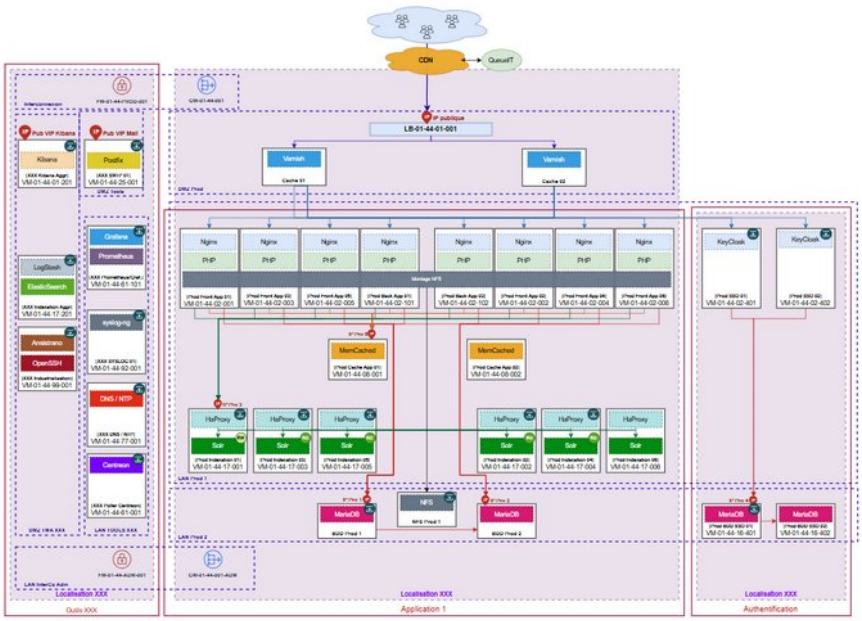
Le second volet porte sur l'**aspect métier** proprement dit : lorsque des demandes sont formulées par le client et portent sur une modification du *workflow*, sur les habilitations ou encore l'interconnexion à des systèmes tiers, ces demandes doivent être **mises en correspondance avec les besoins de sécurité et les risques identifiés**. Bien que ces demandes soient généralement légitimes et souhaitables, leur impact sur la sécurité mise en place est réel et doit être considéré soigneusement : l'ajout d'un mode hors-ligne peut nécessiter l'implémentation d'un **chiffrement spécifique**, une gestion dynamique des rôles applicatifs peut nécessiter l'écriture de **tests automatisés** supplémentaires, etc.

Les équipes de Klee ont intégré la nécessité de ces **réflexions en avance de phase**, qui apportent une plus grande sérénité lors des développements et réduit l'incertitude que constituaient auparavant les tests d'intrusion et audits de code. Chez Klee, ceux-ci sont effectués avant les livraisons majeures des applicatifs développés. Lorsque les projets bénéficient d'un **accompagnement au *Security by Design***, les signalements sont généralement mineurs, faciles à corriger et ne remettent pas en cause les développements effectués ni le planning de livraison.

Durcir l'infrastructure

Enfin, au-delà du code applicatif, la **sécurisation de l'infrastructure** (cluster de conteneurs, serveurs, configuration réseau…) est également un sujet à concevoir soigneusement. Les technologies et méthodes actuelles sont d'une

grande aide dans la conception d'une architecture sécurisée : les **Documents d'Architecture Techniques** font appels à des **schémas connus et maîtrisés**, les images de conteneurs peuvent être auditées, standardisées et leur sécurité renforcée afin d'obtenir une situation *Secure by Default*. L'usage de l'*Infrastructure as Code* permet d'**auditer, de manière manuelle ou automatisée, les systèmes mis en œuvre**.



Exemple de Document d'Architecture Technique

Face à l'**augmentation des attaques** dites par ***Supply Chain***, la sécurisation ne s'arrête pas aux environnements de production mais concerne **toute l'usine logicielle**, notamment les plateformes d'intégration continue, les environnements de développement et de recette, etc. Le choix des réseaux sur lesquels seront exposés ces éléments est un point vital, tout comme le **cloisonnement de ces réseaux**, pour la limitation de la surface d'attaque. Le *Security by Design* porte alors non seulement sur la conception des systèmes vendus aux clients, mais également sur l'**élaboration d'un cadre sécurisé** qui facilite et accélère le travail des équipes projet.

De la théorie à la pratique

Formez dès maintenant vos collaborateurs

Ainsi, la mise en œuvre d'une approche *Security by Design* nécessite une **transformation significative** de la manière dont les systèmes d'information sont **conçus**, **développés** et **déployés**. Cela commence par une véritable **culture de la sécurité**, partagée à tous les niveaux de l'organisation. Sensibiliser, former et impliquer les parties prenantes dès les premières phases d'un projet permet de créer un socle solide sur lequel les bonnes pratiques de sécurité et les **relations entre équipes projets et experts** de la sécurité peuvent s'ancrer durablement.

Faites appel à des experts cyber

Une **posture proactive face aux risques** est une part essentielle de la démarche : identifier les menaces potentielles, modéliser les scénarios d'attaque et prévoir les mesures de remédiation ne sont pas des étapes optionnelles, mais bien des piliers sur lesquels repose la conception. Ce travail d'analyse favorise une meilleure résilience des systèmes en **optimisant les arbitrages entre contraintes métiers, performances et exigences de sécurité**.

La capacité à traiter le risque s'acquiert et se renforce dans la durée, par l'expérience, les retours d'incident, et l'amélioration continue. Klee capitalise ainsi sur les nombreux projets réalisés ces 38 dernières années !

EXIGEZ L'EXCELLENCE TECHNIQUE

Réduire les vecteurs d'exposition constitue un levier stratégique dans la maîtrise du niveau de sécurité global. Cela passe par des **choix techniques éclairés**, une **architecture rigoureuse** et une **minimisation des services** ou composants non essentiels. La sécurité ne se limite pas au code applicatif mais s'étend à **toute l'infrastructure technique, des environnements de développement jusqu'à la production**.

En s'appuyant sur des pratiques éprouvées – telles que l'*Infrastructure as Code*, la construction d'images de conteneurs robustes ou le cloisonnement réseau – il devient possible de bâtir une **architecture cohérente et sécurisée dès la conception**, tout en protégeant l'ensemble de la chaîne de production logicielle face aux menaces de type *Supply Chain*.

NE RESTEZ PAS SEUL !

Enfin, il est illusoire de penser que cette démarche puisse être menée efficacement sans un **accompagnement adapté**. La **complexité croissante** des environnements techniques, la sophistication des menaces et les impératifs réglementaires nécessitent l'appui de **compétences spécialisées**.

En conjuguant culture de la sécurité, rigueur analytique, sobriété technique et accompagnement expert, les organisations peuvent **faire du *Security by Design* un élément différenciant**, garant de la confiance numérique et de la pérennité de leurs activités.