

Intégrer la sécurité dès le stade de la conception

02 septembre 2025, 13:15

Tatiana Galibus

Un guide étape par étape pour accroître la résilience intégrée dans le développement moderne de logiciels

Deux faits généralement connus. Un : les cybermenaces sont toujours plus nombreuses et complexes. Nous n'avons d'autre choix que de renforcer nos efforts de cybersécurité. Deux : il est plus aisé, plus puissant et plus rentable d'intégrer une fonctionnalité dans ses logiciels dès le départ que de l'ajouter une fois le développement terminé.

La combinaison de ces deux faits permet de comprendre immédiatement l'importance du concept de « Security by Design » ou la sécurité dès le stade de la conception. De quoi vous aider à atténuer les risques précocement, à réduire les coûts et à renforcer la confiance des utilisateurs. Ajoutez à cela le Cyber Resilience Act (le règlement européen sur la cyberrésilience) et d'autres législations contraignant les entreprises à intégrer pleinement la sécurité dans leurs efforts de développement, et la Security by Design n'est plus une option pour les développeurs de logiciels, mais une nécessité.

Comment passer de vos pratiques de développement actuelles à un environnement de conception et de développement qui appréhende et intègre la sécurité tout au long du cycle de développement ? L'approche étape par étape ci-dessous peut constituer une ligne directrice pratique.

Qu’est-ce que le concept de Security by Design ?

Security by Design est le principe consistant à intégrer la sécurité dès les premières étapes du développement d’un système, plutôt que de la corriger ultérieurement. Cela signifie considérer les menaces potentielles et les stratégies visant à les atténuer dès les premières décisions de conception et tout au long du cycle de développement logiciel (« SDLC »).

Adopter cette approche contribue à l’édification de milieux numériques robustes, conformes et sécurisés, que ce soit pour créer un produit SaaS de démarrage ou pour gérer une vaste infrastructure.

Découvrez Acme, notre exemple réaliste

Pour bien faire comprendre le flux de travail typique de la sécurité dès la conception, nous allons décrire la trajectoire suivie par un petit fabricant de logiciels imaginaire, Acme, qui travaille sur la création d’une application Web collaborative de liste de tâches pour équipes dispersées géographiquement: AcmeTasks. Acme veut s’assurer que son logiciel est sécurisé, évolutif et conforme aux réglementations européennes à venir, telles que la directive NIS2 et le règlement CRA.

Comprendre le contexte

Avant de se lancer dans le processus de développement, Acme a besoin de comprendre clairement la réalité de son business et ce qu’elle entend accomplir. Acme formule une réponse claire aux questions ci-dessous :

- **Quoi ?** Acme veut construire une application Web à 3 niveaux (frontend, backend, base de données) pour la gestion de listes de tâches.
- **Pour qui ?** Les utilisateurs finaux de cette application Web incluent des télétravailleurs, de petites équipes et des free-lances.
- **En utilisant quelles données ?** Adresses e-mail, tâches utilisateur, pièces jointes, informations de facturation facultatives.
- **Avec quelles contraintes ?** L’application Web doit être conforme au règlement CRA d’ici 2027 ; elle doit être créée par une équipe limitée de 6 développeurs.

Définir la sécurité et les objectifs commerciaux

Acme doit comprendre que l’activité et la sécurité doivent être parfaitement alignées. En d’autres termes, la sécurité doit soutenir les objectifs commerciaux, non les entraver.

Les objectifs commerciaux : Acme a défini qu’un PMV (produit minimum viable) devait être lancé sous 6 mois. Le produit doit être conforme au RGPD et au CRA pour être autorisé sur le marché européen. Il doit également être suffisamment résilient pour gagner la confiance des clients et ainsi attirer des clients interentreprises.

Tout cela se traduit dans les **objectifs de sécurité** suivants : Acme doit protéger les données utilisateurs contre les fuites ou la falsification et empêcher tout accès non autorisé aux listes de tâches. Mais Acme doit également s'assurer que le service reste disponible, même quand la charge de travail est lourde et le trafic Web exceptionnellement élevé.

Réaliser une modélisation des menaces (avec STRIDE)

Protéger adéquatement ses actifs numériques nécessite de bien connaître les menaces auxquelles ils font face. À cette fin, la modélisation des menaces peut être utilisée : une méthode qui contribue à identifier comment un assaillant pourrait cibler votre système. Acme décide d'utiliser STRIDE, l'une des méthodes les plus accessibles, et qui se concentre sur 6 types d'attaques.

L'analyse STRIDE de l'application AcmeTasks permet d'identifier les menaces suivantes :

- **S - Spoofing** (usurpation d'identité) : un assaillant obtient un accès en usurpant l'identité d'un utilisateur via une connexion non sécurisée
- **T - Tampering** (falsification de données) : un utilisateur modifie de manière malveillante les tâches d'un autre utilisateur
- **R - Repudiation** (répudiation) : un utilisateur supprime des tâches et nie les avoir supprimées
- **I - Information Disclosure** (divulgation d'informations) : les données des tâches sont envoyées sans cryptage en HTTP simple et donc lisibles par des tiers
- **D - Denial of Service** (déni de service) : L'API de l'application est surchargée de spams de création de tâches
- **E - Elevation of Privilege** (élévation du privilège) : un utilisateur ordinaire obtient un accès administrateur

Définir les exigences de sécurité

Sur la base du modèle de menace ci-dessus, les développeurs d'Acme peuvent maintenant définir des exigences de sécurité telles que :

- Toutes les transmissions de données doivent utiliser HTTPS
- Utiliser OAuth 2.0 pour l'authentification
- Appliquer le contrôle d'accès basé sur les rôles (RBAC)
- Implémenter la validation des entrées et le codage des sorties
- Consigner les actions sensibles pour la traçabilité
- Limiter le nombre de requêtes autorisées (limitation du débit) afin d'atténuer les dénis de service
- Chiffrer les données utilisateur au repos avec AES-256

Une fois ces exigences satisfaites, les divers types de menaces se trouvent fortement limités et le produit qui en résulte gagne sensiblement en sécurité.

Intégrer dans le SDLC

Un développement et une conception sécurisés sont certes un bon début, mais les choses ne s'arrêtent pas là. La sécurité n'est pas une action ponctuelle, mais un processus continu. Le

développement et la conception sécurisés d'Acme doivent faire partie d'un cycle de développement logiciel (SDLC, pour Software Development Life Cycle) complet, qui intègre les étapes ci-dessous :

- **Conception :** où la modélisation des menaces et la conception de schémas de sécurité (p. ex. RBAC) sont conçues
- **Développement :** utilisation de normes de codage sécurisées, telles que celles énumérées dans le Top 10 de l'OWASP
- **Tests :** y compris l'analyse statique et dynamique, l'analyse des dépendances…
- **Déploiement :** lors du déploiement du produit, une attention particulière doit être portée notamment à la gestion des secrets et au renforcement de l'intégration continue (Ci)/de la livraison continue (CD)
- **Maintenance :** enfin, le cycle complet comprend plusieurs années de maintenance d'un système en fonctionnement, les vulnérabilités et les violations identifiées doivent être traitées rapidement et avec fermeté, en utilisant la gestion des correctifs et la réponse aux incidents, elles peuvent en outre donner lieu dans le futur à un produit encore plus sécurisé dès le stade de la conception

Former son équipe

Un environnement numérique sécurisé nécessitera toujours une sensibilisation approfondie à la sécurité. Employés ainsi qu'utilisateurs finaux et développeurs/concepteurs doivent bien cerner les différentes menaces et la manière d'y faire face. Et parce que le paysage des menaces et de la sécurité ne cesse jamais d'évoluer, une culture de la sécurité dépendra toujours de l'apprentissage continu.

Acme en a conscience et prend une série d'initiatives pour maintenir ses équipes à jour :

- Formation d'intégration au développement sécurisé
- Organisation d'ateliers de modélisation des menaces et d'exercices de revue du code
- Souscription des membres de son équipe de conception et de développement à des bulletins de sécurité (p. ex. flux CVE) pour suivre les dernières nouvelles et tendances

Un conseil supplémentaire : utilisez des plateformes comme CyberActive si vous visez une formation en cybersécurité alignée sur l'UE axée sur le règlement CRA, la directive NIS2 et les meilleures pratiques de codage sécurisé.

Surveiller, mettre à jour, améliorer

Acme sait que l'étape de maintenance consiste en davantage qu'un simple suivi de tout problème de sécurité signalé. Si le développeur entend maintenir la fiabilité de son application, il doit surveiller, réagir et itérer en continu et de manière active. Sa politique de sécurité proactive comprend :

- Configuration de la journalisation et de la surveillance (p. ex. ELK Stack, Sentry)
- Vérification des journaux pour déceler les activités suspectes
- Analyse régulière pour détecter les vulnérabilités
- Examen et révision des modèles de menaces chaque trimestre

- Anticipation et respect des échéances CRA et des étapes de certification

Prêt à suivre les traces d'Acme ? Contactez-nous !

La Security by Design est une question de résilience, de confiance et de viabilité à long terme. Pour une entreprise comme Acme, investir précocement dans des pratiques structurées signifie pouvoir évoluer en toute sécurité, gagner la confiance et se conformer à l'évolution du paysage juridique.

Il en va de même pour votre organisation. Qu'il s'agisse d'un effort de développement ponctuel ou de la maintenance continue d'une infrastructure TIC, vous devez accorder à la sécurité toute la considération qu'elle mérite. Intégrez-la dans vos opérations économiques quotidiennes, de la culture de la conception jusqu'au suivi des bogues.

Nous pouvons vous aider à atteindre ces objectifs.

Vous pouvez apprendre comment faire progresser votre entreprise en matière de conformité et de résilience face à toutes les menaces en suivant notre trajet Lunch & Learn.

Contactez le projet SecDes (Security by design) pour les développeurs et fournisseurs SaaS.

Ou vous pouvez en apprendre davantage sur les étapes mentionnées ci-dessus ou sur les directives et outils pour la conformité CRA et la security by design : contactez tatiana.galibus@sirris.be qui se fera un plaisir de vous fournir les renseignements nécessaires.

Normes et cadres en vue de la Security by Design

La Security by Design est devenue une exigence majeure dans le développement d'environnements logiciels et numériques. Les développeurs et concepteurs sont tenus de respecter certaines normes, mais ils peuvent également bénéficier de nombreux cadres et outils utiles pour les aider dans leurs efforts en matière de sécurité. Vous trouverez ci-dessous un aperçu de certains des cadres et normes les plus importants qui soutiennent l'approche Security by Design :

- **CRA - Cyber Resilience Act** (règlement européen sur la cyberrésilience, 2024) : la législation la plus récente imposant la cybersécurité aux produits numériques tout au long de leur cycle de vie
- **NIST SP 800-160 :** ingénierie de la sécurité des systèmes conseils sur l'intégration de la sécurité dans les processus d'ingénierie
- **OWASP SSDLC :** pratiques de Secure Software Development Lifecycle (cycle de développement logiciel sécurisé)
- **ISO/IEC 27034 :** cadre de sécurité des applications
- **Microsoft SDL :** cycle de développement de la sécurité utilisé en interne par Microsoft

- **Lignes directrices ENISA :** recommandations en matière de cybersécurité au niveau de l’UE

Intégrez la sécurité dès la première ligne de code

Souhaitez-vous développer des applications sécurisées conformes aux réglementations les plus récentes, telles que NIS2 et le Cyber Resilience Act ? Cette masterclass vous offre des éclairages pratiques et une expérience concrète en security by design et en modélisation des menaces. Faites un pas décisif vers des logiciels robustes et pérennes.

Inscrivez-vous à la masterclass

Auteurs



Tatiana Galibus