5 à 7: e-commerce : comment communiquer en ligne avec ses clients et garantir la sécurité des données ?

Stéphane Adamiste 26/09/2023

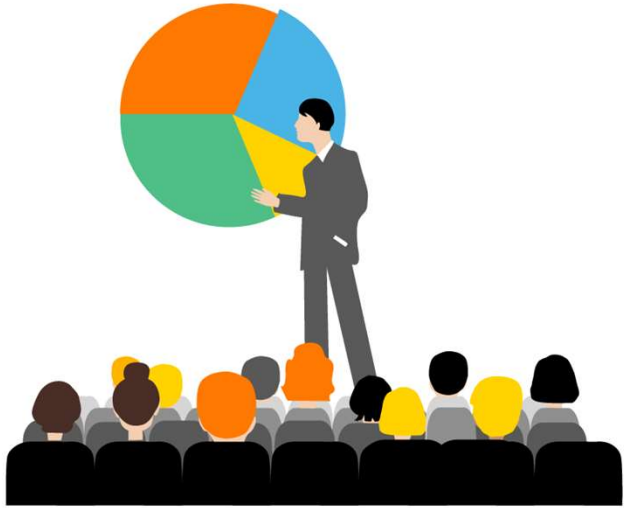
orange™ Cyberdefense

A propos de l'intervenant

- ✓ Actuellement CPO / CISO / DPO @ Orange Cyberdefense Switzerland
- ✓ Consultant en sécurité de l'information et protection des données personnelles
- ✓ Expérience >20 ans

- ✗ Juriste
- ✗ Qualified Security Assessor
- ✗ Expert en CMS E-commerce

stephane.adamiste@orangecyberdefense.com



Sommaire

1. Les réglementations applicables
2. Les meilleures pratiques de sécurité dans un projet de développement
3. Collaborer avec une entreprise externe pour son site e-commerce

1. Les réglementations applicables
2. Les meilleures pratiques de sécurité dans un projet de développement
3. Collaborer avec une entreprise externe pour son site e-commerce

1. Les réglementations applicables

PCI-DSS (Payment Card Industry Data Security Standard)

Norme de sécurité introduite en 2004 par les principales sociétés de cartes de crédit pour protéger les informations liées aux cartes de paiement.

Ensemble de règles de sécurité à respecter par les entreprises qui traitent des informations de cartes de paiement.

But: Renforcer la confiance des clients dans la sécurité de leurs transactions.

Version actuelle: 4.0

- Publiée le 31 mars 2022
- 356 pages
- Introduit les notions de «mesures compensatoires» et «d'approche personnalisée».
- Transition possible depuis la version précédente (3.2.1) jusqu'au 31 mars 2024, certaines mesures à appliquer bénéficiant d'un délai d'implémentation jusqu'au 31 mars 2025.

1. Les réglementations applicables

PCI-DSS - Applicabilité

Pour une organisation traitant des données de cartes de paiement, les exigences PCI-DSS varient en fonction:

- du mécanisme de paiement utilisé
- du volume de transactions annuel

1. Les réglementations applicables

PCI-DSS - Exigences pour les paiements en ligne en fonction du volume de transactions annuel

Niveau	Volume	Exigences PCI-DSS
1	> 6M	Un *Qualified Security Assessor* (QSA) réalise annuellement un audit complet de conformité et rédige un *Report on Compliance* (ROC) L'organisation fournit une *Attestation of Compliance* (AOC) à son acquéreur Scan de vulnérabilités trimestriel par un Approved Scanning Vendor (ASV) Test d'intrusion annuel ou après un changement significatif
2	Entre 1 et 6M	*Self Assessment Questionnaire* (SAQ) annuel + AOC Scan de vulnérabilités trimestriel par un ASV Test d'intrusion annuel ou après un changement significatif
3	Entre 20k et 1M	SAQ + AOC Scan de vulnérabilités trimestriel par un ASV
4	< 20k	SAQ Scan de vulnérabilités trimestriel par un ASV

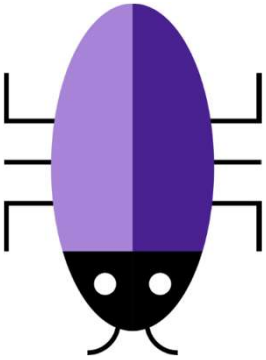
1. Les réglementations applicables

PCI-DSS - Exigences en fonction du mécanisme de paiement utilisé

Mécanisme de paiement	Applicabilité de la norme
Paiement direct sur le site	Intégralité des mesures (328) applicables au marchand (SAQ D)
Intégration d'une passerelle de paiement tierce avec stockage provisoire des données de cartes de paiement	Intégralité des mesures (328) applicables au marchand (SAQ D)
Redirection vers un fournisseur de services de paiement (PSP) avec collecte des données de cartes de paiement sur le site (p. ex. Direct Post method, JavaScript form) mais sans stockage	SAQ-A-EP : Il s'agit de s'assurer que l'intégration avec le portefeuille numérique est sécurisée et que les données de cartes de paiement ne sont pas stockées accidentellement
Utilisation de portefeuilles numériques (p. ex. PayPal, Apple Pay, Google Pay)	SAQ-A-EP
Redirection vers un fournisseur de services de paiement (PSP) sans collecte, stockage ni transmission de données de cartes de paiement par le site marchand en soi (p. ex. via une redirection d'URL ou une iFrame)	SAQ A: Il s'agit de s'assurer que le site marchand ne présente pas de vulnérabilité qui pourrait permettre de compromettre le mécanisme de redirection. C'est le questionnaire le plus simple et le plus court

Mythes de la sécurité e-commerce

#1: «Nous ne sommes pas soumis à PCI-DSS car nous externalisons le service de paiement»



1. Les réglementations applicables

nLPD - Exigences clés concernant les données personnelles

1. Principe de Transparence :

Information: Les utilisateurs doivent être informés de manière claire et transparente concernant la collecte, le traitement, et l'utilisation de leurs données personnelles (finalité).

Consentement : Si des données sensibles sont traitées, ou si des profils de personnalité sont créés, un consentement explicite doit être obtenu.

2. Principe de Proportionnalité :

Collecte Limitée : Seules les données nécessaires à des fins légitimes peuvent être collectées.

Limitation de l'Usage : Les données doivent être utilisées uniquement pour les fins pour lesquelles elles ont été collectées, conservées uniquement pendant la durée nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées, ou aussi longtemps que requis par la loi.

3. Droits des Personnes Concernées :

Accès : Les individus ont le droit de savoir quelles données sont collectées et traitées, et peuvent demander une copie de ces données.

Rectification et Effacement : Les individus ont le droit de corriger des données incorrectes et de demander l'effacement de leurs données dans certaines circonstances.

Opposition : Les individus ont le droit de s'opposer au traitement de leurs données dans certaines circonstances.

4. Sécurité des Données :

Les données doivent être protégées contre l'accès non autorisé, la divulgation, la modification, et la destruction, par des mesures techniques et organisationnelles appropriées.

Principes de *Security by Design* et *Security by Default.*

5. Notification en cas de Violation de Données :

En cas de violation de données, il peut être nécessaire d'informer la personne concernée et/ou l'autorité de protection des données, en fonction de la gravité de la violation.

6. Gestion des Sous-Traitants

Définition des responsabilités et obligations du sous-traitant concernant la protection des données personnelles au travers d'un accord de traitement de données incluant: les mesures de sécurité à mettre en place par le sous-traitant, un droit d'audit, l'obligation d'annoncer les incidents de sécurité, la limitation du transfert des données, la portabilité, la limitation de la sous-traitance secondaire, la suppression des données à la fin de la relation contractuelle.

7. Transfert à l'Etranger:

Si des données sont transférées à l'étranger, il faut s'assurer que le pays destinataire assure un niveau de protection des données adéquat ou qu'un autre mécanisme existe autorisant le transfert (principalement: clauses contractuelles types, consentement éclairé).

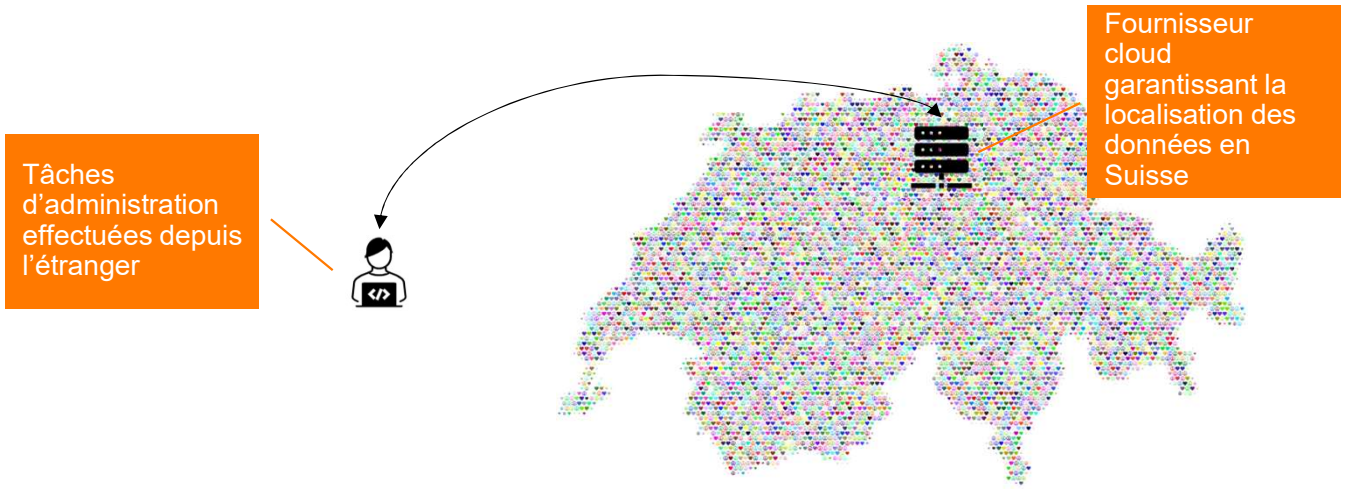
1. Les réglementations applicables

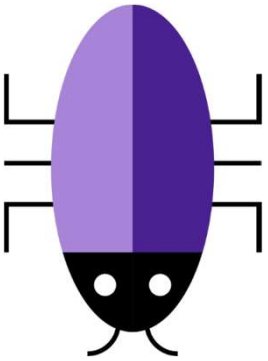
Implications de la nLPD pour un site d'e-commerce

Exigences nLPD	Implications pour un site e-commerce
1. Principe de Transparence	Etablir une politique de confidentialité claire et la rendre facilement accessible
2. Principe de Proportionnalité	Minimisation des données et limitation de la conservation
3. Droits des Personnes Concernées	La politique de confidentialité doit détailler les droits des personnes concernées
4. Sécurité des Données	Applications de mesures techniques et organisationnelles afin de réduire les risques à un niveau acceptable
5. Notification en cas de Violation de Données	Mise en place d'un processus de gestion d'incidents
6. Gestion des Sous-Traitants	Identifier les acteurs externes du projet et déterminer leur rôle. S'ils sont sous-traitants, établir un accord de traitement de données
7. Transfert à l'Etranger	Identifier les possibles transferts de données vers des pays tiers S'assurer qu'un mécanisme autorise le transfert

Mythes de la sécurité e-commerce

#2: «Nos données sont stockées en Suisse, nous ne sommes pas concernés par les transferts à l'étranger»





FAQ nLPD- e-commerce

Q: Suis-je soumis uniquement à la nLPD ou également au RGPD?

R: La nLPD s'applique si le responsable du traitement, le sous-traitant ou la personne concernée se trouve en Suisse, si le traitement ou les effets du traitement se produisent en Suisse.

Le RGPD s'applique aux organisations qui traitent les données de citoyens sur le territoire européen dans le cadre d'une offre de biens ou de services. Si un site e-commerce cible spécifiquement une clientèle européenne (p.ex. traduction du site en suédois, en espagnol, achats possibles en euros, etc.), le RGPD s'applique.

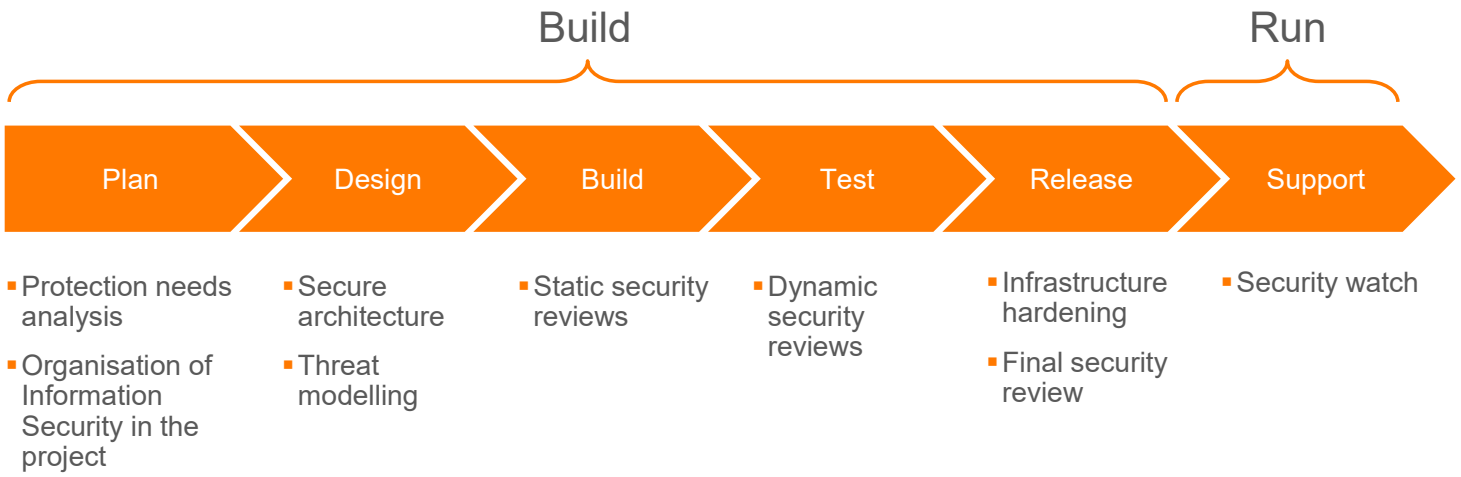
Q: Suis-je soumis à la loi sur les cookies si j'opère sur le marché suisse?

R: Non. Pas besoin d'obtenir un consentement explicite de la part des visiteurs d'un site qui distribue des cookies. Il faut informer les utilisateurs de l'utilisation de cookies et de la finalité associée dans la politique de confidentialité, ainsi que de la possibilité de désactiver les cookies dans les réglages du navigateur.

1. Les réglementations applicables
2. Les meilleures pratiques de sécurité dans un projet de développement
3. Collaborer avec une entreprise externe pour son site e-commerce

2. Les meilleures pratiques de sécurité dans un projet de développement

Théorie:



Réalité:

Peu de projets effectuent ces activités de manière formalisée.

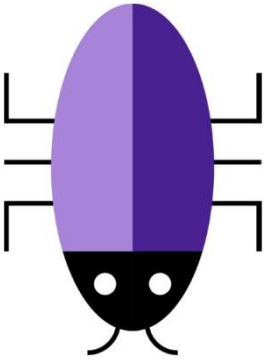
Beaucoup de projets se contentent d'un test d'intrusion avant/après la mise en production.

Beaucoup de projets ne prévoient pas de temps/budget pour la correction des éventuelles failles trouvées lors du test d'intrusion.

Mythes de la sécurité e-commerce

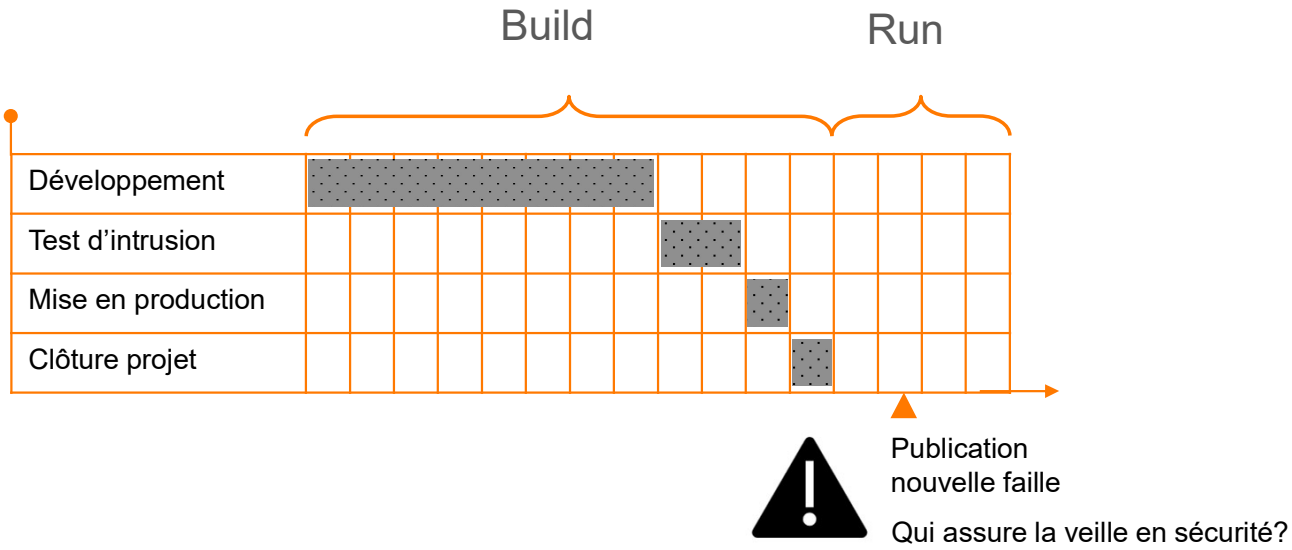
#3: «Nous utilisons un CMS e-commerce, il est déjà sécurisé par défaut»

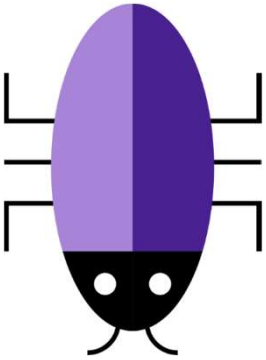
Développement custom?
Thèmes?
Plugins?
Connexions à des services externes?
Exposition de l'interface d'administration?
Configurations/comptes par défaut?



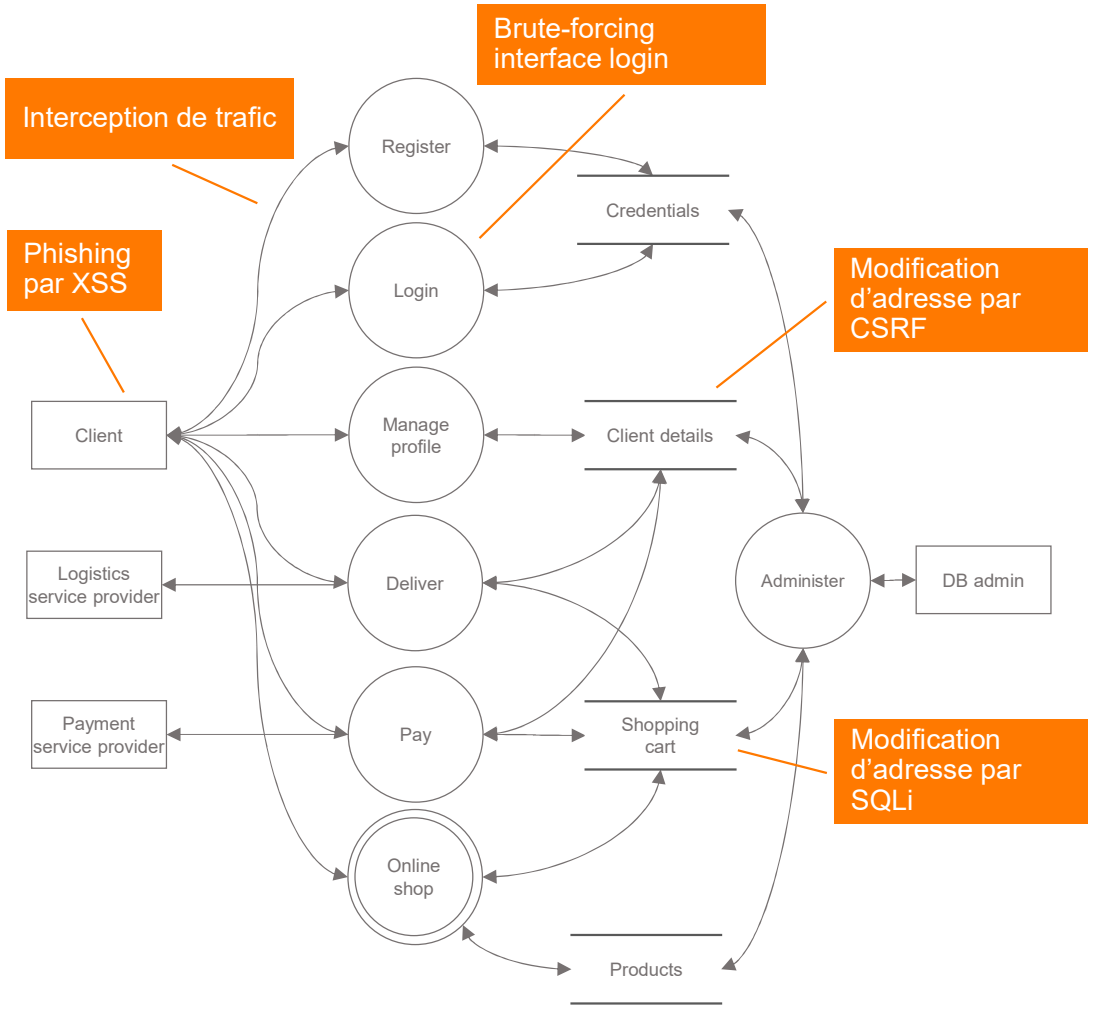
Mythes de la sécurité e-commerce

#4: «Nous avons fait un test d'intrusion avant la mise en production donc nous sommes protégés»





2. Les meilleures pratiques de sécurité dans un projet de développement



Biens informationnels critiques	C	I	A
Codes d'accès	x	x	x
Achats (nature, coût)	x	x	x
Catalogue produits (description, prix)		x	x
Coordonnées clients	x	x	x

#	Menace	Agent(s) de menace
T1	Vol d'identité / commandes frauduleuses	Internet hacker
T2	Vol de données personnelles	Internet hacker, concurrent, DB admin
T3	Manipulation de commande (prix, adresse livraison)	Client, Internet hacker
T4	Déni de service	Internet hacker, concurrent
T5	Panne / mauvaise manipulation	Employé, hasard

2. Les meilleures pratiques de sécurité dans un projet de développement

Bénéfices de la modélisation des menaces (threat modelling)

Identification des vulnérabilités potentielles d'un système

Priorisation des risques

Prise en compte de la sécurité dès la conception

Réduction des coûts (p. ex. coûts de remédiation en cas d'incidents, amendes pour non-conformité)

Pédagogie

Confiance des clients

Amélioration continue

Documentation et analyse des menaces

Définition commune pour les protagonistes d'un projet de ce que signifie le terme «sécurité» dans le projet

1. Les réglementations applicables
2. Les meilleures pratiques de sécurité dans un projet de développement
3. Collaborer avec une entreprise externe pour son site e-commerce

3. Collaborer avec une entreprise externe pour son site e-commerce

		Responsabilité sécurité selon mode d'hébergement(**)				
Couche	Exemples de mesures de sécurité	On-premise	Datacentre tiers	Iaas	PaaS	SaaS
Données	Chiffrement, sauvegardes, contrôles d'intégrité, réponse à incident	Client	Client	Client	Client	Fournisseur
Application e-commerce (*)	Contrôle d'accès logique, configurations sécurisées, patch management, filtrage, change management, résilience, journalisation des événements	Client	Client	Client	Client	Client / fournisseur
Système d'exploitation		Client	Client	Client	Fournisseur	Fournisseur
Couche de virtualisation		Client	Client	Client	Fournisseur	Fournisseur
Hardware (réseau, serveurs, baies de stockage)		Client	Client	Fournisseur	Fournisseur	Fournisseur
Physique (~datacentre)	Mesures de protection contre les menaces environnementales et les intrusions physiques, contre les pannes (p. ex. redondance alimentation électrique, connexion internet, etc.)	Client	Fournisseur	Fournisseur	Fournisseur	Fournisseur

(*) CMS e-commerce sur étagère dans cet exemple
(**) Security shared responsibility model (SSRM)

3. Collaborer avec une entreprise externe pour son site e-commerce

Plusieurs cas de figure envisageables

Développement ad-hoc vs implémentation standard d'un CMS e-commerce

- Détermine le besoin en développement sécurisé

Mode d'hébergement

- Détermine les responsabilités client / fournisseur pour les tâches sécurité pour chaque couche

Phase de construction vs phase d'exploitation

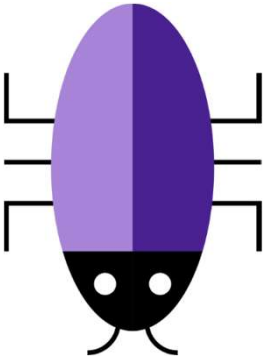
Veiller à identifier les responsabilités pour les tâches de sécurité une fois la mise en production effectuée (veille en vulnérabilités principalement)

Attention aux coûts cachés si cet aspect n'est pas clarifié à la signature du contrat

Mythes de la sécurité e-commerce

#5: «Ce prestataire compte de multiples clients, il s'y connaît forcément en sécurité»

Pouvez-vous me montrer le modèle de menaces de votre solution?
Quelles sont les contraintes réglementaires applicables et comment votre solution y répond-elle?
Est-ce qu'un(e) spécialiste sécurité sera impliqué(e) dans le projet? Quelles seront ses tâches?
Comment vous assurez-vous que le code que vous développez ne contient pas de failles?
Que se passe-t-il si une faille relative à notre site e-commerce est publiée?



En résumé

Identifier les exigences réglementaires

nLPD

PCI-DSS

Autres? (selon la nature des données traitées, le domaine dans lequel on exerce, le marché ciblé, etc.)

Veiller à intégrer des activités d'assurance sécurité pertinentes dans le cycle de vie du projet

Dès le début du projet

Ne pas omettre la phase d'exploitation du système

En cas de collaboration avec un prestataire externe

S'assurer du niveau de compétence du prestataire en sécurité

Définir les responsabilités pour les activités de sécurité de chaque partie

Formaliser les aspects sécurité dans des accords contractuels

- Ne pas se limiter aux fonctionnalités de sécurité (p. ex. HTTPS, sauvegardes, contrôle d'accès, etc.)

Merci pour votre attention!