CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Digitalisation : Enjeux et stratégies de sécurité

Christophe Guéguen

Head of Data & Cyber Security Practice

HARMONIE TECHNOLOGIE

Les équipes « digital marketing » travaillent de sorte à

Offrir une solution simple qui s'adapte à l'ensemble des supports digitaux sans multiplier les dispositifs techniques

Proposer un service en adéquation avec les usages et les changements comportementaux de leurs clients

Fluidifier les parcours et les interactions entre canaux

Cela induit des complexités de gestion

Cycles de développement courts
Abaque standard : 10 à 20 jours
Réalisation technique pour un délai moyen de 2 mois de l'idée à la publication de l'application

Exposition croissante de données et de services métier
Volonté des utilisateurs d'accéder aux mêmes ressources via l'ensemble des canaux à leur disposition

Cadre sécurité mal adapté aux contextes mobile
Coûts et délais non négligeables des phases sécurité (Analyse de risques, tests de sécurité, etc.)
Peu ou pas de solutions de sécurité centrale répondant aux besoins des applications

Des risques spécifiques à la mobilité sont à prendre en compte

1 Liés au mobile lui-même

- Vol de mobile et des données stockées par l'application
- Exfiltration de données via le réseau mobile (SMS/MMS) ou le réseau de données (Internet)

2 Liés aux infrastructures d'accès

- Usurpation d'identité (gestion des jetons de session)
- Accès aux ressources publiées (faiblesse du contrôle d'accès aux webservices)
- Infection virale via un abus de confiance entre deux partenaires

3 Liés à la gestion des applications

- Publication d'application malicieuse se faisant passer pour une application légitime (phishing)

4 Liés à la fuite de données

- Données métiers (que l'utilisateur saisit sur une application corrompue)
- Données pour rebondir sur un autre point d'entrée du SI (login/mot de passe)

L'intégration de la sécurité dans les projets digitaux ou comment rendre compatible sécurité et agilité?

UN DOUBLE DEFI

1. Faire en sorte que la sécurité soit identifiée comme un partenaire à part entière des équipes digitales
2. S'adapter à des cycles projet courts en maintenant un niveau sécurité adapté aux enjeux

UNE REPONSE A APPORTER A DEUX NIVEAUX

1. **Au niveau de l'entreprise** : Disposer d'un socle sécurité pouvant répondre aux usages
2. **Au niveau des projets** : Adapter l'intégration de la sécurité dans les méthodologies agiles

IDENTITE NUMERIQUE

VERS UN IAM ÉTENDU

Convergence des usages
- **Collaborateurs** (mobilité, cloud)
- **et Clients** (accès fonctionnalités avancées du SI)

IDAAS COLLABORATEURS
IAM CLIENTS

interagir avec les identités « sociales »

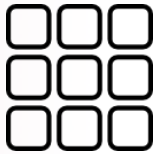
OAUTH
« FACEBOOK CONNECT »

Proposer une gestion des identités fédérées à ses clients

FÉDÉRATION D'IDENTITÉS

CONTRÔLE D'ACCES

AUTHENTIFICATION ERGONOMIQUE ET RENFORCÉE



Authentification des Applications et des devices

JETONS DE SÉCURITÉ

Authentification transparente

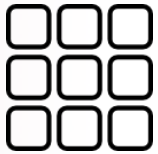
JETON PERSISTANT
SSO INTER APPLI SUR MOBILE
SSO INTER-DEVICES

Authentification incrémentale

JETON, BIOMÉTRIE, MDP, SMS/PUSH, ETC…

PROTECTION DE LA DONNEE

L'ouverture des SI liée à l'entreprise digitale impose de mettre en œuvre des mécanismes de **protection directement sur la donnée**



Données consultées via une application
(Données Structurées)

ANONYMISATION
TOKENISATION

Données stockées dans le cloud
(Données Structurées)

ANONYMISATION
TOKENISATION

Données Bureautiques
(Données Non-Structurées)

CHIFFREMENT
DRM
(DATA RIGHT MANAGEMENT)

Un agencement des mécanismes par les risques

	IDENTITE NUMERIQUE	AUTHENTIFICATION ADAPTATIVE	PROTECTION DE LA DONNEE
	EVALUATION DE L'UTILISATEUR ET DU DEVICE	EVALUATION DE L'INTÉGRITÉ DE L'APPLICATION	APPLICATION DES RÈGLES D'EXPOSITION
PILOTAGE PAR LES RISQUES	Analyse du comportement utilisateur	Revue du contenu des stores	Utilisation d'un référentiel des données sensibles

PARTIE 1 / Mobilité Nouveau Paradigme pour la sécurité

PARTIE 2 / Socle d'entreprise

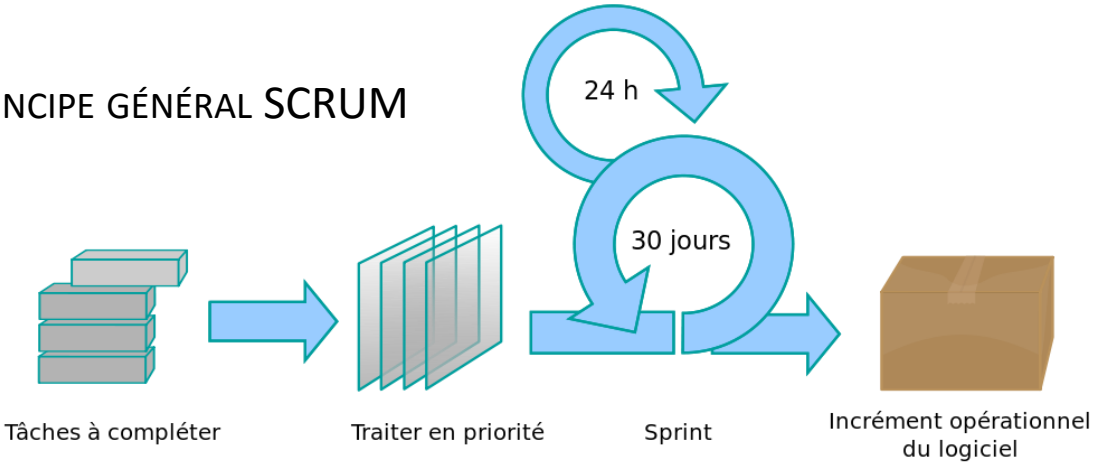
PARTIE 3 / Sécurité dans les projets

Rappel sur la philosophie agile

Par nature, les méthodes se veulent pragmatiques et dynamiques avec trois axes clés :

- Les exigences métier peuvent évoluer au cours du processus itératif
- Les développements font l'objet d'un processus permanent d'amélioration et d'évaluation
- Les travaux sont collaboratifs

PRINCIPE GÉNÉRAL SCRUM



Avant projet : Un travail préparatoire clé

REVUE DES DONNEES ET DES EXIGENCES

Mener une revue initiale des données gérées par le produit final et des exigences associées

SENSIBILISATION DE L'EQUIPE PROJET

Partager des contraintes sécurité et des mesures à considérer

INITIALISATION DU BACKLOG

Compléter les user stories « métier » en intégrant la sécurité
Intégrer des « user stories » dédiés sécurité

Projet : un engagement sécurité proportionné

Que reste-t-il ?

A chaque sprint

Revue de la cohérence des tâches fonctionnelles et sécurité retenues

Revue du backlog pour assurer la non prise en compte de nouvelles typologies de données avec des exigences propres

Evaluation sécurité adaptée

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Merci de votre attention

Christophe Guéguen

Head of Data & Cyber Security Practice

HARMONIE TECHNOLOGIE