FORUM EUROSEC' 2006

S26B

Démarche de sécurité dans les projets

Théorie et réalité

Patrick CHAMBET
Bouygues Telecom
http://www.chambet.com

Eric LARCHER
Banque Fédérale des Banques Populaires
http://www.internet-securise.com

Planning

- Introduction
- Constat, risques
- Exemples de vulnérabilités applicatives et d'impacts
- Démarche de sécurisation
- Quelques conseils
- Conclusion

Introduction

- Même si toute entreprise aspire à exploiter des applications sûres, toutes ne sont pas à égalité en termes d'enjeux métier et de budget
- On peut distinguer 3 types de sociétés
  - Les éditeurs de logiciels : ils se doivent (ou tout au moins essayent…) de fournir des logiciels sûrs
    - Ø La sécurité fait partie de leur business (on paye pour)
  - Les industries critiques : elles pilotent leurs processus métiers critiques à l'aide de logiciels
    - Ø La sécurité est une obligation business (on ne peut pas faire sans)
  - Toutes les autres entreprises : elles s'appuient à différents niveaux sur des logiciels commerciaux ou développés en interne
    - Ø La sécurité est considérée de « non indispensable » à « souhaitable » selon les cas

Constat et conséquences

- **Constat général : la sécurité n'est pas prise en compte suffisamment tôt dans les projets**

- **Conséquences**
  - **On réinvente la roue (pendant le projet)**
    - **Mauvais niveau de sécurité (peut passer inaperçu !)**
    - **Surcoût et allongement des délais**
  - **On ajoute une « rustine » (à la fin du projet ou suite à un audit)**
    - **Prise de risques en exploitation**

- **Une démarche d'intégration de la sécurité dans les projets *de bout en bout* est donc nécessaire**

Les vulnérabilités typiques

- Aujourd'hui, la majorité des vulnérabilités sont de type applicatif
- Exemples
  - Authentification peu robuste
    - Accès à l'application sans aucun compte !
  - Mauvaise gestion des sessions et des profils
    - Etanchéité
    - Robustesse des identifiants de session
    - Augmentation de privilèges
  - Injection de données malformées
    - Manipulation de paramètres
    - SQL injection
    - Cross Site Scripting (XSS)

Exemples d'impacts

- **Perte d'une application ou d'une base de données critique**
  - **Coût indicatif de l'ordre de plusieurs dizaines de M€**

- **Indisponibilité prolongée (+ de 3 jours)**
  - **Risque de disparition de certaines entreprises**

- **Perte de confidentialité**
  - **Perte de l'initiative d'une offre marketing innovante**
  - **Divulgation de la liste des clients d'une entreprise et de leurs informations personnelles (+ *risques CNIL*)**

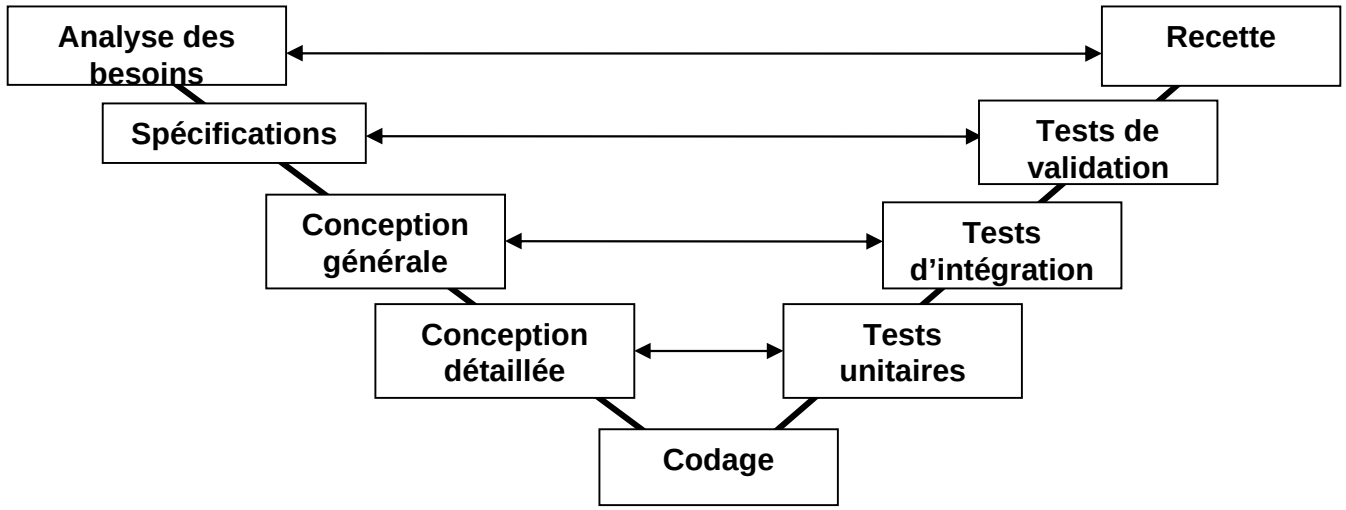
- **Perte d'intégrité**
  - **Perte d'image de marque auprès des clients -> perte directe de CA dans certains secteurs**

Planning

- Introduction
- Constat, risques
- Exemples de vulnérabilités applicatives et d'impacts
- Démarche de sécurisation
- Quelques conseils
- Conclusion

Rappel: le cycle en V

- Le cycle de développement projet en « V »



- La sécurité intervient à chaque étape du cycle

La démarche de sécurité dans les projets

- **Analyse de risques de sécurité en amont**
  - **Interception de chaque projet avant même son démarrage**
  - **MOAD : auto-évaluation à l'aide d'une grille simplifiée**
  - **Puis, si besoin, analyse de risques détaillée assistée par les experts du service Sécurité**
  - **C'est la seule façon d'identifier les enjeux et risques métiers de l'application**
  - **Cela permet aussi d'établir un lien unique avec les équipes métier (excellent moyen de sensibilisation indirect) et de définir les priorités *d'un point de vue métier***
  - **Se limiter cependant aux applications sensibles (pas l'intranet de gestion des congés par exemple !)**

La démarche de sécurité dans les projets

- Analyse de risques de sécurité (suite)
  - Exemple d'une méthode d'analyse simplifiée :
    - Évaluation des besoins de sécurité des principales données manipulées par les utilisateurs de l'application (CAID)
    - Étude de la pertinence des différentes menaces applicables au projet (constituer une base au préalable)
    - Analyse des risques et des impacts potentiels
    - Décision de la liste des risques acceptables (ou couverts par des moyens « externes ») et ceux à couvrir (i.e. pour lesquels il faut trouver des solutions)

La démarche de sécurité dans les projets

- **Spécifications de sécurité**
  - **Introduction de fonctions de sécurité dans les spécifications lors de la rédaction du cahier des charges afin d'y introduire une sécurité fonctionnelle**
- **Normes, best practices et recommandations**
  - **Conception d'une architecture sécurisée par les MOE**
    - **Réseau**
    - **Système**
    - **Applicative**
  - **Respect des normes de sécurité de développement**
    - **Protocoles, briques logicielles, codage**
    - **Nécessité d'un référentiel de normes**

La démarche de sécurité dans les projets

- **Points de contrôle**
  - **Réguliers durant le projet**
    - **Validation des choix techniques, de la sécurité de l'architecture**
    - **Audit de code et validation de la sécurité des développements**
  - **Durant la phase de test**
    - **Vérification des spécifications de sécurité**
    - **Tests spécifiques « de sécurité »**
      - **Buffer overflows, format strings, heap overflows, ...**
      - **Injection SQL, XSS, ...**
  - **Test final de sécurité avant mise en production éventuellement**
  - **Tests de sécurité pendant la vie de l'application**
    - **A chaque nouvelle version ou palier technologique par exemple**

La sécurité dans le « monde réel »

Qui est le propriétaire de l'application (MOA) ?

Quel est le budget ? Où est le budget ?

On n'a pas de budget pour la sécurité !

Qui paye pour la sécurité ?

Qui fait l'expression de besoins ?

Où est le document d'analyse ?

Où est le cahier des charges ?

Quelle méthodologie de gestion de projet ?

On n'a pas besoin de faire de la sécurité !

Où sont les architectes ?

Qui fait l'architecture applicative ?

Où sont les architectes matériels (infrastructure) ?

On n'a pas le temps de faire de la sécurité !

Qui doit réaliser l'application (MOE) ?

Quels plans de test ?

Qui teste l'application ? Valide les livraisons ?

L'application est déjà en production depuis 5 ans, on n'y touche pas !

On a le temps, l'argent et le besoin mais… on ne sait pas comment implémenter les mesures de sécurité !

Une démarche active

- **Nécessité d'initier la démarche**
  - **Choisir quelques projets pilotes**
    - **Au moins un par domaine métier de l'entreprise**
  - **Intégrer et suivre la sécurité de bout en bout dans ces projets**
- **Diffuser les recommandations**
- **Capitaliser sur les normes et bonnes pratiques et les étendre progressivement aux autres projets et à l'ensemble des MOE**
- **Effectuer des formations**
  - **Pour les architectes**
  - **Pour les développeurs**
  - **Pour les testeurs (assurance produit)**

Planning

- Introduction
- Constat, risques
- Exemples de vulnérabilités applicatives et d'impacts
- Démarche de sécurisation
- Quelques conseils
- Conclusion

Conseils

- **Analyses de risques**
  - **Objectifs et motivations**
    - **Même si une application est déjà en production, il peut être pertinent d'effectuer une analyse de risques métier a posteriori, lors de la conception d'une nouvelle version par exemple**
  - **Moyens**
    - **Éviter d'appliquer telles quelles les méthodes publiquement diffusées**
    - **Préférer des méthodes simplifiées dans un premier temps**

Conseils

- **Former / sensibiliser les équipes IT (MOE) et métier (MOA)**
  - **Objectifs et motivations**
    - **Rien ne vaut une bonne démonstration pour ancrer la problématique « sécurité » dans les esprits**
    - **La formation / sensibilisation est une action facile et économique à mettre en place (et généralement bien accueillie)**
    - **De plus, on ne peut pas travailler *en permanence* en mode « réactif »**
      - **« Si tu donnes un poisson à un homme, il se nourrira une fois. Si tu lui apprends à pêcher, il se nourrira toute sa vie. »**
    - **Il faut donc former / sensibiliser l'ensemble des acteurs des projets IT**
  - **Gains**
    - **Les acteurs sont beaucoup plus réceptifs aux autres actions qui peuvent être menées en matière de sécurité**
    - **Les personnes les plus convaincues deviennent naturellement « relais sécurité » dans leurs équipes respectives et préviennent spontanément de l'arrivée d'un nouveau projet ou de l'existence d'un risque significatif sur le SI**

Conseils

- **Former / sensibiliser les équipes IT et métier (suite)**
  - **Moyens**
    - **Équipes IT**
      - **Mettre en place des cycles de formation systématiques (toutes les MOE, en plusieurs sessions) ou des sessions ponctuelles (équipe projet, service, ligne de marché, etc...)**
      - **Contenu (formations générales)**
        - **Concepts généraux de sécurité des SI (introduction à la sécurité des infrastructures et des applications)**
        - **Les phases de déroulement d'une attaque**
        - **Exemples « pratiques »**
      - **Contenu (formations spécifiques)**
        - **Approfondissement sur une problématique d'infrastructure (switches, routeurs, WiFi, etc.) ou applicative (architectures Web, langages de programmation particuliers, etc.)**

Conseils

- **Former / sensibiliser les équipes IT et métier (suite)**
  - **Moyens (suite)**
    - **Équipes Métier**
      - **Mettre en place des formations très spécifiques à chaque métier, de façon à sensibiliser les acteurs / décideurs métier d'un service ou d'une entité**
      - **On ne doit surtout pas parler (directement) de technique !**
      - **Contenu**
        - **Inventaire de menaces actuelles**
        - **Présentation de l'impact possible de ces menaces sur le business de l'entreprise (en essayant de parler d'argent !)**
        - **Statistiques (nombre de failles, de piratages, de perte de CA, etc.)**
        - **Exemple de sociétés victimes d'incidents significatifs (idéalement, dans le même secteur d'activité que l'entreprise)**

Conseils

- **Faire des revues de code**
  - **Objectifs et motivations**
    - **S'assurer de l'innocuité des parties sensibles d'une application (traitement des E/S, composants accessible depuis Internet, tournant sous de forts privilèges ou gérant des données sensibles, etc...)**
  - **Moyens**
    - **Faire relire le code par un expert**
    - **Utiliser des outils d'analyse automatisée**

Conseils

- **Dernier conseil : itérer !**
  - **Objectifs et motivations**
    - **Les différentes actions évoquées précédemment doivent être reconduites régulièrement lors de nouvelles versions d'applications, l'arrivée de nouveaux membres au sein des équipes projets, de nouvelles failles ou attaques, etc...**
  - **Moyens**
    - **Mettre à jour régulièrement les normes et standards, les *best practices*, les supports de formation, etc...**
    - **S'assurer que la sécurité soit systématiquement traitée dans tous les projets sensibles**

Conclusion

- L'intégration de la sécurité dans les projets est aujourd'hui indispensable
- Des démarches efficaces existent et contribuent à renforcer de façon très significative la sécurité dans les projets
- Les coûts induits ne sont pas prohibitifs
- La sécurité finira alors par entrer progressivement dans les moeurs et…
- … il conviendra alors de l'insérer de façon systématique dans les projets

Questions