CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Mise en place d'une politique de sécurité applicative : retour d'expérience d'un RSSI

Philippe Larue – RSSI de CBP – Conférence Clusif du 15/12/2011

Présentation de CBP

CBP est un cabinet de courtage spécialisé en conseil et gestion d'offres de prévoyance.

Chiffre d'affaires 2010: 109 millions €

Deuxième courtier spécialiste en terme de chiffre d'affaires, d'après le classement de l'Argus de l'Assurance.

Plus de 475 collaborateurs CBP ont géré en 2010 :

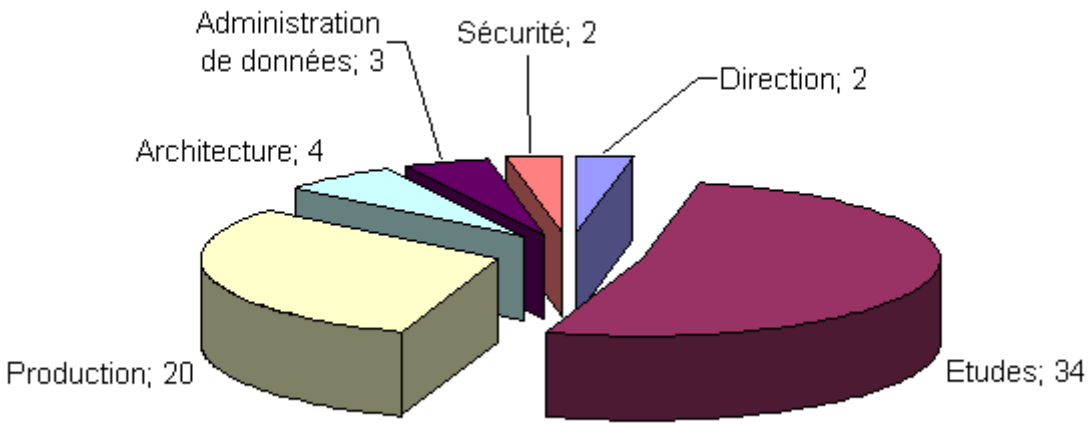
- 530 000 nouvelles adhésions
- 100 000 dossiers de sinistres.

Implantations de CBP en Europe

CBP travaille aujourd'hui pour le compte de plus de 100 clients distributeurs d'offres de prévoyance en Europe:

Présentation de la DSI

Effectif total en 2011: 65 personnes réparties ainsi:



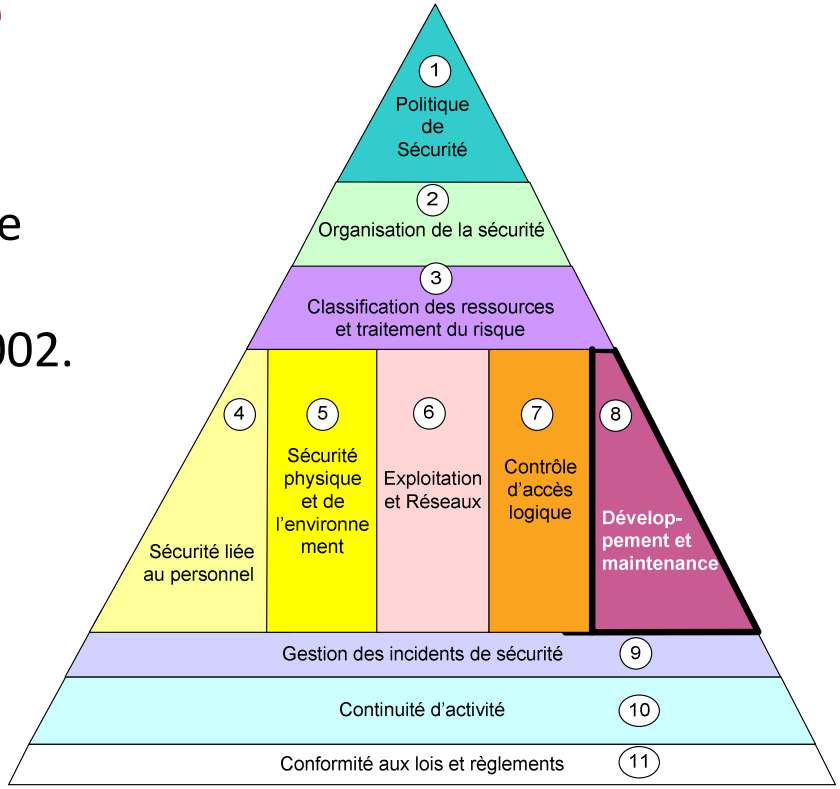
Des outils métiers majoritairement développés en interne

Politique de sécurité

CBP s'est doté d'une politique de sécurité conforme aux normes ISO 27001 et ISO 27002.

Avant 2011, les efforts techniques avaient principalement porté sur l'infrastructure.

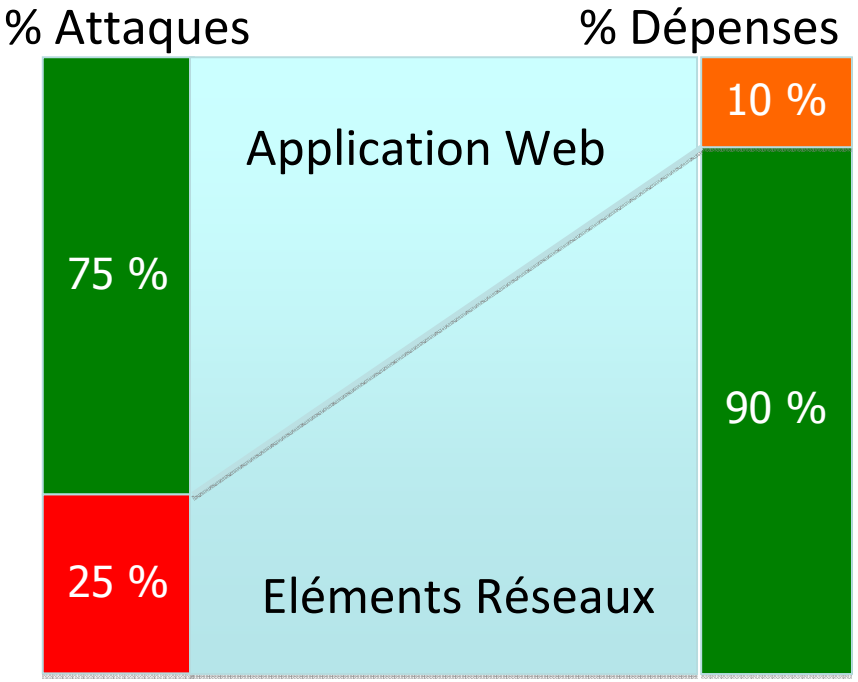
Le chapitre sur la sécurité des développements était pratiquement vierge.



L'application, la cible principale

Les attaques visent désormais majoritairement l'application

Etude du GARTNER 2003
75% des attaques ciblent le niveau Applicatif
66% des applications web sont vulnérables



Le risque augmente

L'exposition de CBP augmente : nos applications sont de plus en plus exposées sur Internet (en nombre, en richesse de fonctionnalités, au niveau international…)

En 2011, la cybercriminalité a explosé et rapporterait plus que la drogue.

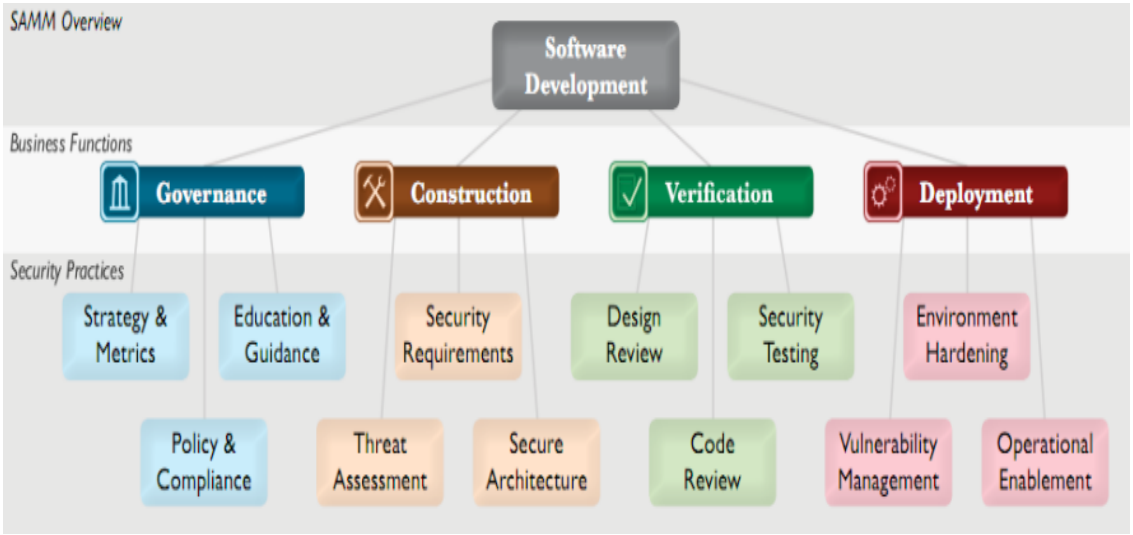
☞ Une politique de sécurisation du code applicatif est plus que jamais nécessaire pour CBP: le projet s'est déroulé de février à novembre 2011

La DSI a demandé un audit de son organisation

Les personnes ayant été interviewées sont au nombre de six :

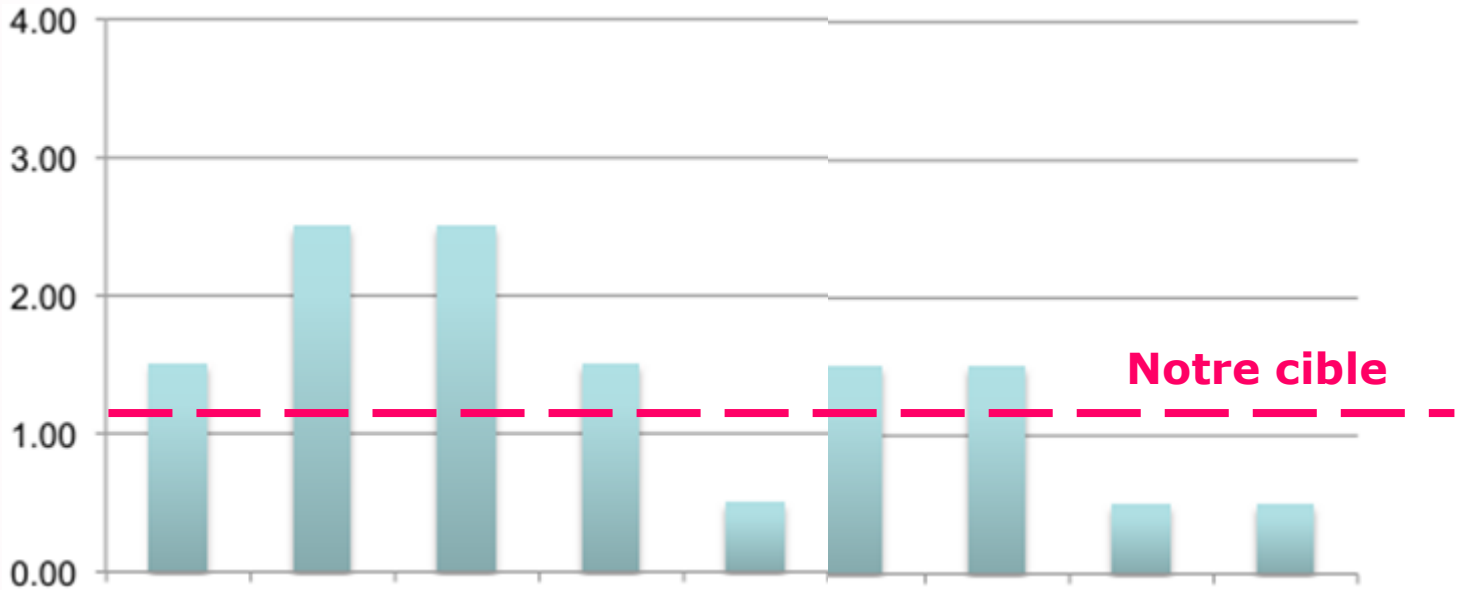
- un Architecte
- un Chef de Projet Organisation
- un Chef de Projet DSI
- une personne de l'infrastructure
- le Responsable des Etudes
- le Responsable de la Sécurité des Systèmes d'Informations.

La méthode choisie par le consultant a été opensamm (évaluation de la maturité d'une organisation en sécurité applicative)



Résultat

Une photo à l'instant t de nos forces et nos faiblesses



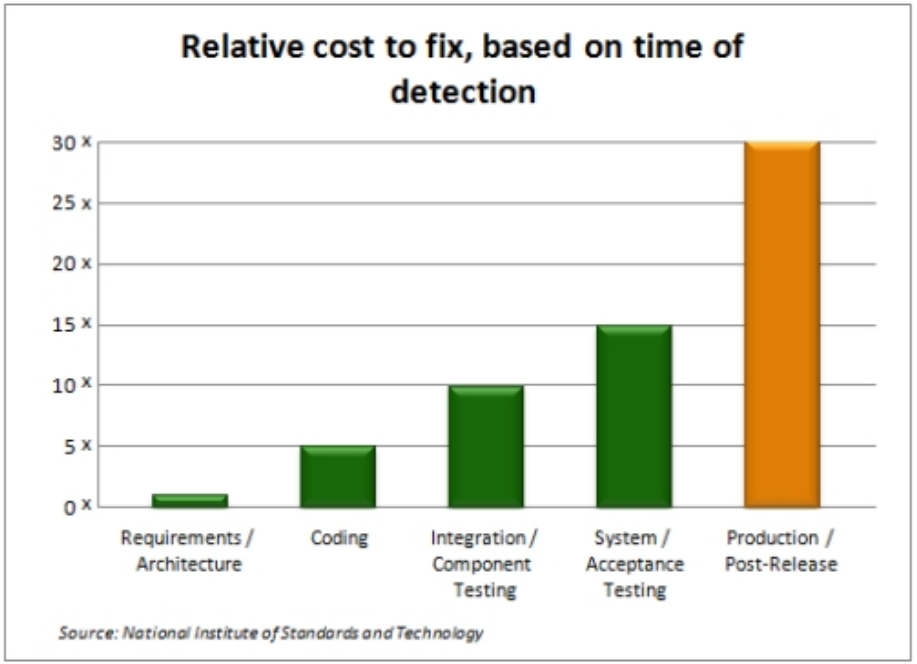
25 recommandations pour toutes les phases du cycle

Politique de sécurité logicielle: grands principes

Basée sur les bonnes pratiques

Concerne le développement interne ou externe et l'acquisition des progiciels

Très orientée prévention amont car plus une faille est découverte tard, plus sa correction coûte cher:



Politique de sécurité logicielle: développement

Technologique mais Indépendante de langages ou de méthodes (basée sur des principes)

Basée en grande partie sur l'OWASP ASVS : Application Security Verification Standard.

Les 14 familles d'exigences sont classées en 3 niveaux:

- Obligatoire (sans dérogation)
- Recommandé (obligatoire pour les opérations sensibles)
- Conseillé (en annexe, libre arbitre du CDP)
- ☞ Les critères de classification ont été le niveau de risque (ex : top 10 OWASP), les protections déjà portées par l'infrastructure et la capacité à faire dans notre contexte.

2 exemples

Obligatoire

Exigence	Référence	Exemple et mise en application
Tous les formulaires contenant des informations sensibles ont désactivé les caches, coté client, incluant les fonctionnalités d'auto-complétion.	ASVS 9.1	On peut envoyer la directive http no-cache, et aussi forcer dans la page WEB HTML le autocomplete= «off» sur les formulaires.

Recommandée

Il y a une seule implémentation de journalisation utilisée par l'application	ASVS 8.9	Préférer les outils tels que log4j qui permettent de standardiser les logs pour les SIEMS

Buts de la politique de sécurité

Le code sera meilleur et plus sûr, la sécurité renforcée

Sensibiliser et former /effet Monsieur Jourdain

Susciter prise de conscience et intérêt pour le sujet

Référentiel consultable par tous où piocher en cas de doute

Référentiel qui évitera certaines discussions sans fin

Référentiel diffusable pour toutes les prestations au forfait

Référentiel de base pour les documents amont « analyse du besoin de sécurité » et DAT.

L'effort demandé aux équipes DSI

La lire pour la comprendre ou savoir retrouver l'information (30 min à 1h)

Contribuer pour la faire vivre

La mettre en œuvre dès maintenant pour tous les nouveaux projets

Questionnaire pédagogique en ligne

10 questions / 10 points

30 réponses

Notes obtenues

entre 7 et 10

Moyenne: 9,5/ 10

Plan d'actions

Accompagnement et formations

Des formations spécifiques et pratiques (nov 2011)

Une page Wiki technologique (Java) a été mis en place

Mise en œuvre et contrôle

Mise en œuvre pour tous les nouveaux projets et de façon opportuniste pour d'anciennes applications et contrôles

Des revues de code sont planifiées et budgétées

Sonar : intégration des contrôles sécurité dans l'outil

Suivi et signalement des failles

Il a été demandé que le RSSI soit prévenu des failles « sécurité »

Ce dernier a accès à l'outil de « bug tracking » Mantis et peut agir comme un Responsable Assurance Sécurité:

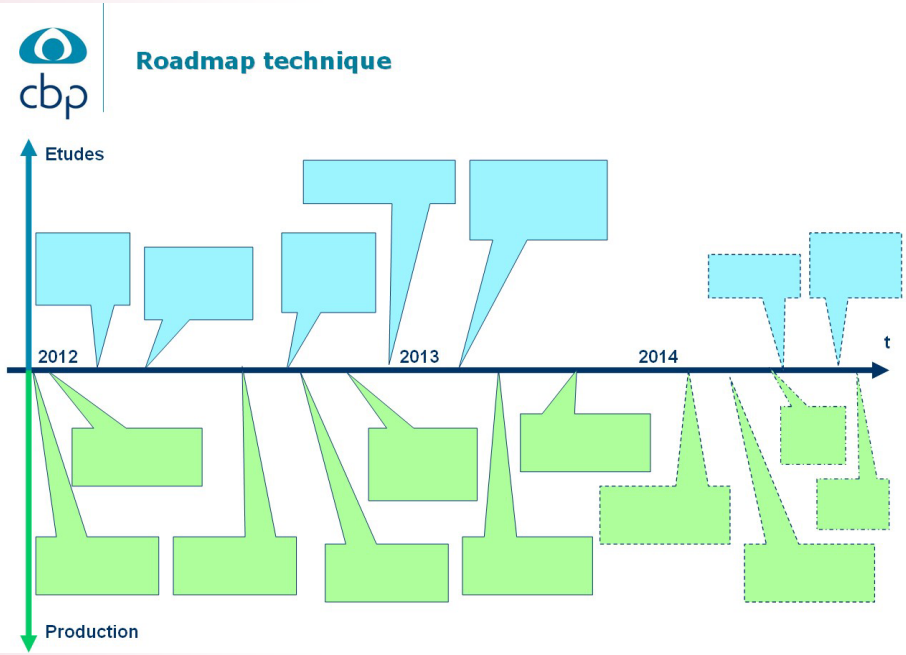
- Intervenir sur la priorisation d'un bug
- Suive l'évolution des failles
- Faire un bilan des bonnes pratiques dont le non respect a occasionné les vulnérabilités à des fins de rappels pédagogiques et de mise à jour de la politique de sécurité (amélioration continue)

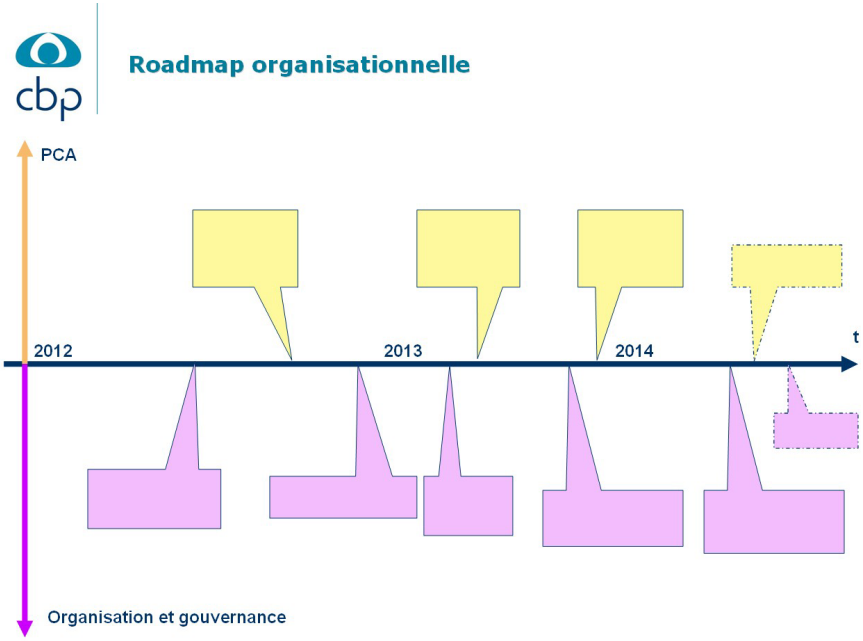
Exemple : suite à la sensibilisation, une faille de sécurité a été découverte par un développeur sur une application qui venait pourtant de réussir un test d'intrusion par un cabinet spécialisé.

Roadmap SSI

La politique de sécurité logicielle actuelle n'est pas exhaustive mais CBP est dans une démarche d'amélioration continue.

Les équipes ont demandé plus de visibilité. Une roadmap SSI a été mise en place.





Premier retour d'expérience

C'est une démarche d'équipe qui nécessite l'implication de tous les services DSI

Il est préférable de commencer par un point de situation.

Les non convaincus déclarés sont utiles pour parfaire la politique

Il faut trouver le bon équilibre entre en faire trop (risque de décrochage) ou pas assez (risque sécurité)

Bien accompagnée, la démarche provoque l'intérêt et l'adhésion (ex : découverte de nouveaux bugs par les équipes). Cette émulation doit être entretenue.

Le mot de la fin

"Ainsi, une règle essentielle de la stratégie consiste à: Se préparer à déjouer une attaque, au lieu d'espérer qu'elle ne se produise pas. "

Sun Tzu, « L'art de la guerre » (Vème siècle av JC)