Sécurité Applicative: Frein ou Accélérateur

Renaud Bidou (DenyAll)

Patrick Chambet (C2S - Groupe Bouygues)

RIAMS 2012

Agenda

1. Pourquoi sécuriser ses applications
2. Les revers de la sécurité applicative
3. Les avantages
4. Retour d'expérience de Bouygues Telecom
5. Ouvrons le débat

Pourquoi ?

La pillule bleue

- **Prise de conscience globale**
  - Accroissement des risques applicatifs
  - Analyse en amont des besoins
  - Intégration dans un cycle maîtrisé

- **Adoption technologique contrôlée**
  - Evangélisation / éducation
  - Consensus des métiers
  - Maîtrise des technologies sous-jacentes

Le monde d'Amélie Poulain

Développement

Pré-production

Production

Source Code Analysis

Static Application Security Testing (SAST)

Penetration Testing

Dynamic Application Security Testing (DAST)

Application Security Controls

Web Application Firewall
Web Services Firewall

La pillule rouge

- **Urgence**
  - Incident avéré ou suspecté
  - Déploiement d'une application critique
  - Prise de conscience tardive mais brutale

- **Gestion empirique de la problématique**
  - Spectre fonctionnel
  - Communication
  - Choix de solution

  } plus ou moins aléatoire

➢ **La sécurité applicative devient la patate chaude**

Pas qu'une histoire de pilule

- **Mais souvent un mélange de ces deux extrêmes**
  - Une pilule violette ?

- **De nombreuses désillusions**
  - Problèmes de mise en production
  - Ralentissements
  - Faux positifs
  - Interruption de service

- **Et la question récurrente sur la sécurité**
  - Un investissement rentable ?
  - Ou juste un problème de plus…
  - *Pourquoi ? Mais pourquoi !*

Réflexion

- **Un retour d'expérience**
- **A tête reposée**
- **Avec un éditeur**
  (pas si malhonnête qu'il en a l'air)
- **Et son client attaqué de toute part**
  (y compris en interne)

Les revers

Ceux qui sont évidents

1. **Le déploiement**
   - En coupure : modification d'architecture réseau
   - « Transparent » : problématique de haute-disponibilité

2. **Les faux-positifs**
   - Interruption de trafic légitime
   - Debugging, expérience utilisateur, image etc.

3. **L'impact sur les performances**
   - La sécurité a un prix
   - Faut pas rêver

Ceux que l'on découvre

1. **Les bugs**
   - C'est du logiciel !
   - Assez caractéristique du « focus » des solutions

2. **Les limitations fonctionnelles**
   - Au-delà des simples fonctions de sécurité
   - Souvent des petits détails, parfois bloquants

3. **Les interfaces**
   - Pas adaptées à de vrais environnements de production
   - « Il n'y a de beau que l'inutile », sujet de réflexion…

Ceux qu'on vous cache

1. **Les compromis performance / sécurité**
   - Limitations connues des moteurs de sécurité
   - Maladroitement / malhonnêtement cachées

2. **Les bugs connus**
   - Configurations rares, impact mineur
   - « En attente » de découverte par un client

3. **Les erreurs de conception**
   - Introduisent des limitations fonctionnelles
   - Ne seront jamais corrigées
   - Avantageusement remplacées par des promesses

Ceux qui en souffrent…

- **Ceux qui exploitent**
  - Des technologies peu maîtrisées
  - Au cœur de la chaîne applicative
  - La sécurité, encore responsable de tous les maux
  - ➢ Personne ne veut de ces produits

- **Ceux qui ont fait le choix**
  - Besoin de justification
  - Des cibles faciles: au mieux il ne se passe rien
  - Responsables ET coupables

La sécurité applicative ?

Faux - Positifs

\+ Délais de déploiement

\+ Coût du service accru

\+ Latence

\+ Interruption de service

= **UN FREIN**

… Un boulet ?

Les avantages

Une alternative : rien

- **Conduit à terme au scénario « pilule rouge »**
- **Déploiement dans l'urgence**
- **Adoption aux forceps**

➢ **Suite à une intrusion …**

Une alternative : l'audit

- **Audit de code**
  - Meilleur niveau de sécurité
  - Pas d'impact sur la production…
- **… quand l'application rentre en production**
  - Délai d'audit considérable
  - Coût non-négligeable
  - Code Freeze obligatoire
  - Audit récurrent indispensable
- **Compromis = niveau de sécurité réduit**

La sécurité applicative

- **Seulement la moins mauvaise solution ?**
- **Pas si elle est intégrée en amont des projets**

➢ **Elle devient facilitatrice de projets**

Security Inside

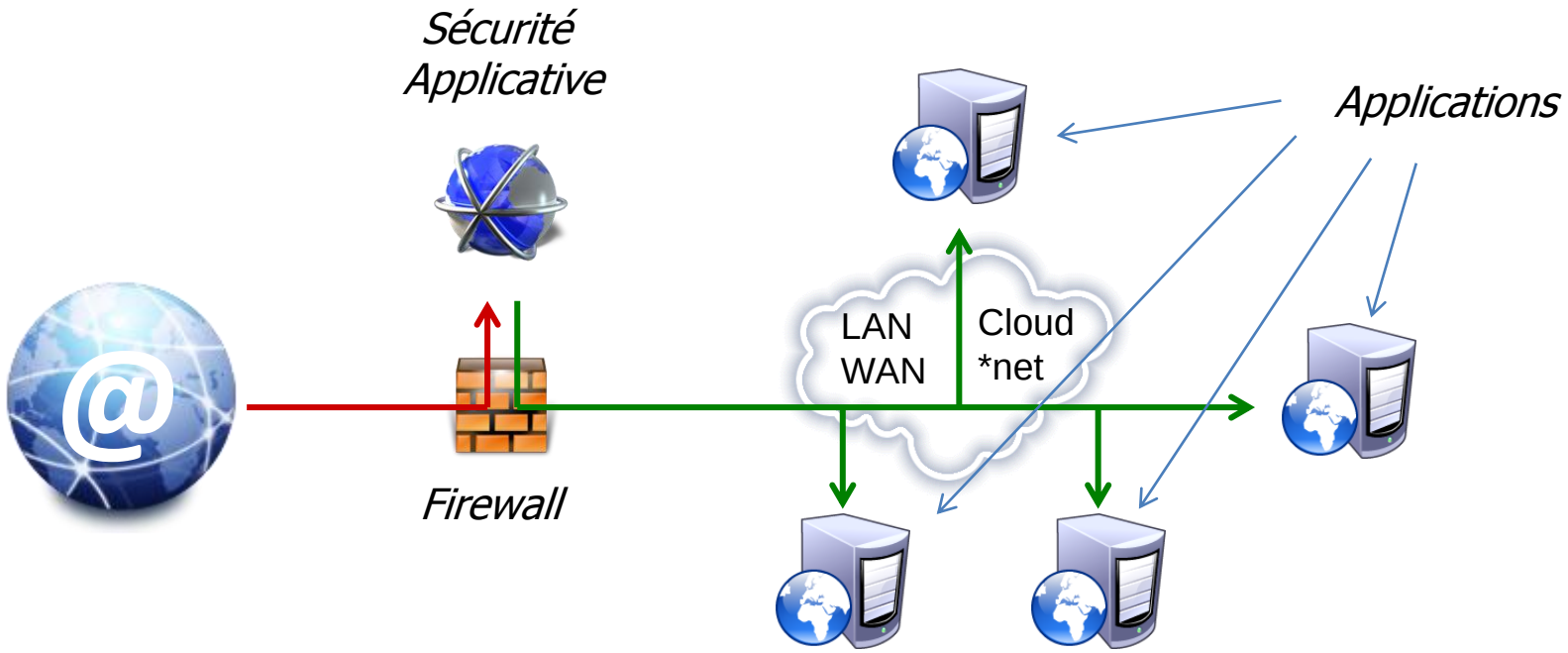
- **La sécurité déléguée à un équipement tiers**
  - Pas d'impact sur le cycle de développement
  - Mutualisation des coûts (moyens, équipes)
  - Homogénéisation du niveau de sécurité

➢ **Déploiement rapide**

➢ **Niveau de sécurité maîtrisé**

Simplicity Inside

- **Architecture centralisée**
  - Simplification des points d'accès
  - Distribution des applications dans l'infrastructure



Acceleration Inside

- **La sécurité a un coût en performance**
  - Des milliers de filtres
  - Sur des dizaines de paramètres par requêtes
  - Et on vous vend du *wire speed*… mais oui !!!

1. **Réduire l'impact de la sécurité**
   - Mise en cache ⇨ pas de latence vers le backend
   - Compression ⇨ réduction des congestions uplink

2. **Décharger les serveurs**
   - Multiplexing ⇨ optimisation des connexions réseau
   - Chiffrement ⇨ gestion des négociations

No Limit !!!!

- **Point de concentration des accès**

➢ **Visibilité complète sur les applications**

  - Erreurs
  - Temps de réponse et disponibilité
  - Géolocalisation, statistiques
  - Sécurité …

- **Plus qu'un simple outil de sécurité**
- **Devient un point de contrôle**

La sécurité applicative ?

Mutualisation

\+ Homogénéisation

\+ Centralisation

\+ Accélération

\+ Visibilité

= **ACCELERATEUR**

Question piège

Pour ajouter à la confusion

La question

Pourquoi pouvez-vous rouler vite en voiture ?

La réponse

Parce que vous avez des freins …

Le cas Bouygues Telecom

Le contexte

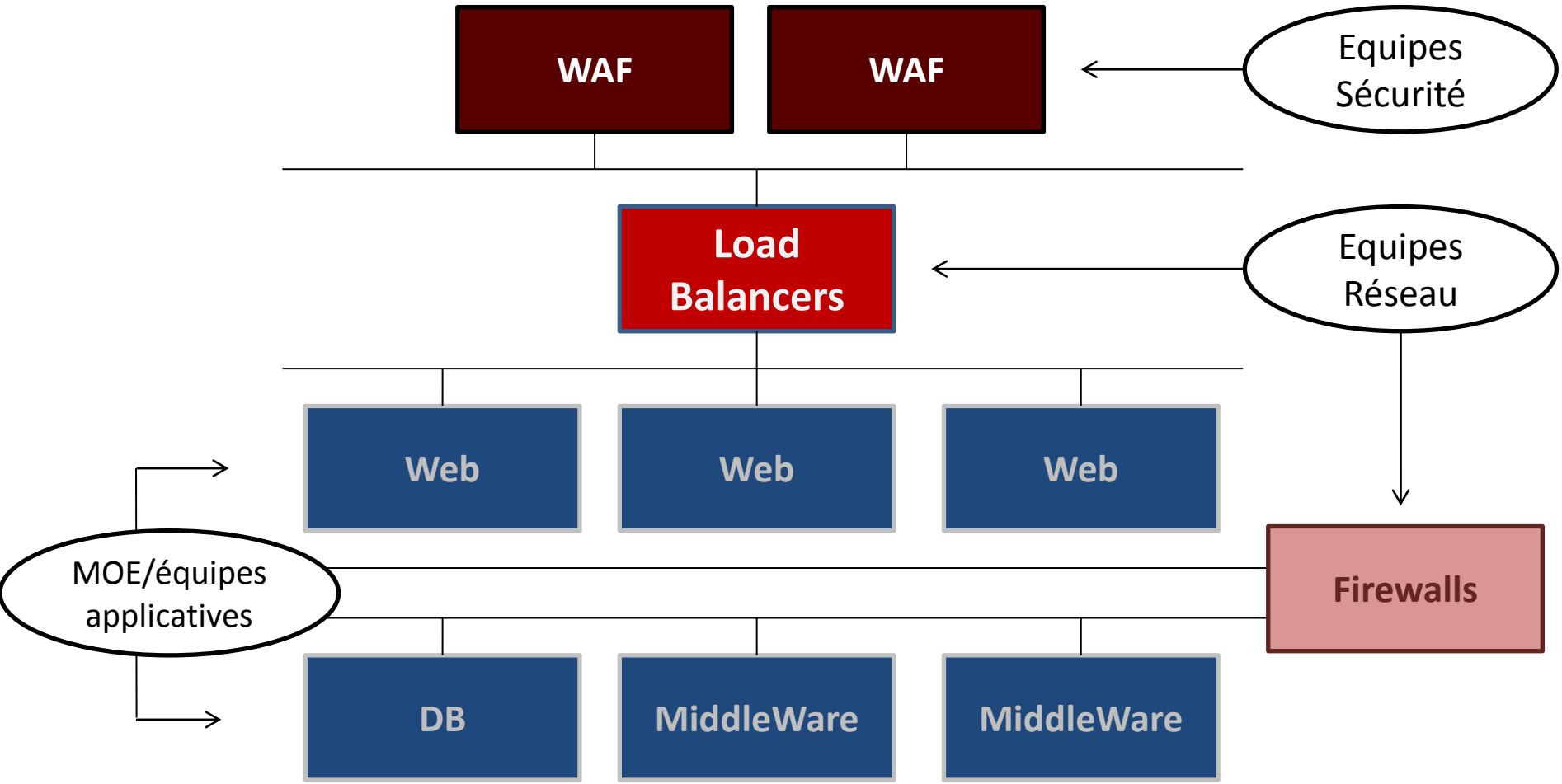
- **Sécurité applicative en progrès année après année, mais toujours insuffisante**

- **Prise de conscience en amont il y a plusieurs années**
- **Besoin remis sur la table chaque année**
  - Mode perséverant ;-)

- **Pour le déploiement de nouvelles applications**
- **Dans un contexte concurrentiel fort**
- **Dans une actualité d'attaques récurrentes des opérateurs**
- **Avec un besoin d'agilité forte du SI et un délai de mise en œuvre raccourci**

➢ **Un contexte de pilule violette…**

Architecture & organisation



Le Frein

- **Infrastructure WAF nouvelle**
  - Complexité d'intégration
  - Equipement supplémentaire, risques accrus
  - Technologie non maîtrisée par la DSI ou le Réseau
- **Déployée sur une application critique**
  - Visible au plus haut niveau hiérarchique
- **Equipes fonctionnant en silos**
  - Le WAF est le coupable idéal pour tout le monde
  - A l'intersection de toutes les technologies

Le WAF omni-responsable

- **Problématiques de performances**
  - Finalement: base de données sous-dimensionnée
- **Pertes de paquets**
  - Finalement: firewall réseau coupant des sessions trop longues
- **Requêtes non servies**
  - Finalement: load-balancer ne supportant pas le *pipelining*
- **Indisponibilité des applications**
  - Finalement: bug au niveau du middleware
- **Plan B de contournement des WAF prêt**
  - Finalement, pas le bon plan B…

L’accélérateur

- **L’architecture est en place et ronronne**
  - Pas d’interruption de service
  - Les équipes de production sont en confiance
  - Le concept est *maintenant* accepté à tous les niveaux

- **Mise en production de nouvelles applications**
  - Rapidité de déploiement
  - Sécurité homogène, centralisée et devenue indispensable
  - Demande forte des métiers
  - ➢ **Facilitateur de projets**

- **… et un outil de debug très efficace**
  - Au confluent des technologies
  - Au cœur de la chaîne applicative

Ouvrons le débat

1er Sujet

Toutes les applications
doivent-elles être protégées ?

Pistes / Indices (cela vous rappelle quelque chose ? **;-)**)

« Seulement la production, qui de toute façon n'est pas connectée »

« De toute façon, les informations qui sont accessibles sur les applications publiques ne sont pas critiques »

Next Step

Peut-on concevoir de mettre en production une application sans protection ?

Pistes / Indices

« Les éditeurs agitent l'épouvantail éculé des risques d'intrusion »

« Le nombre d'intrusion n'augmente pas, c'est juste une question de couverture médiatique »

« De toute façon, si quelqu'un veut rentrer il rentre »

Reformulation

Peut-on SERIEUSEMENT *concevoir de mettre en production une application sans protection ?*

Concrêtement

La sécurité applicative,
même cause que le firewall il y a 15 ans ?

Pistes / Indices

« Omni-responsable, efficacité discutée, crainte des acteurs du conseil », ça vous rappelle quelque chose ?

« Untel, grand gourou réputé, dit que les firewalls applicatifs sont inutiles »

« Non, même cause que les IDS, ça ne marche pas et ça ne marchera jamais »

A VOUS !

denyall
SECURITY SOLUTIONS

Merci !