C2S, Groupe BOUYGUES

JSSI 2013

Retours d'expérience sur des campagnes d'audit de sécurité

Patrick CHAMBET, RSSI
Julien TORDJMAN (CISA/CISSP)

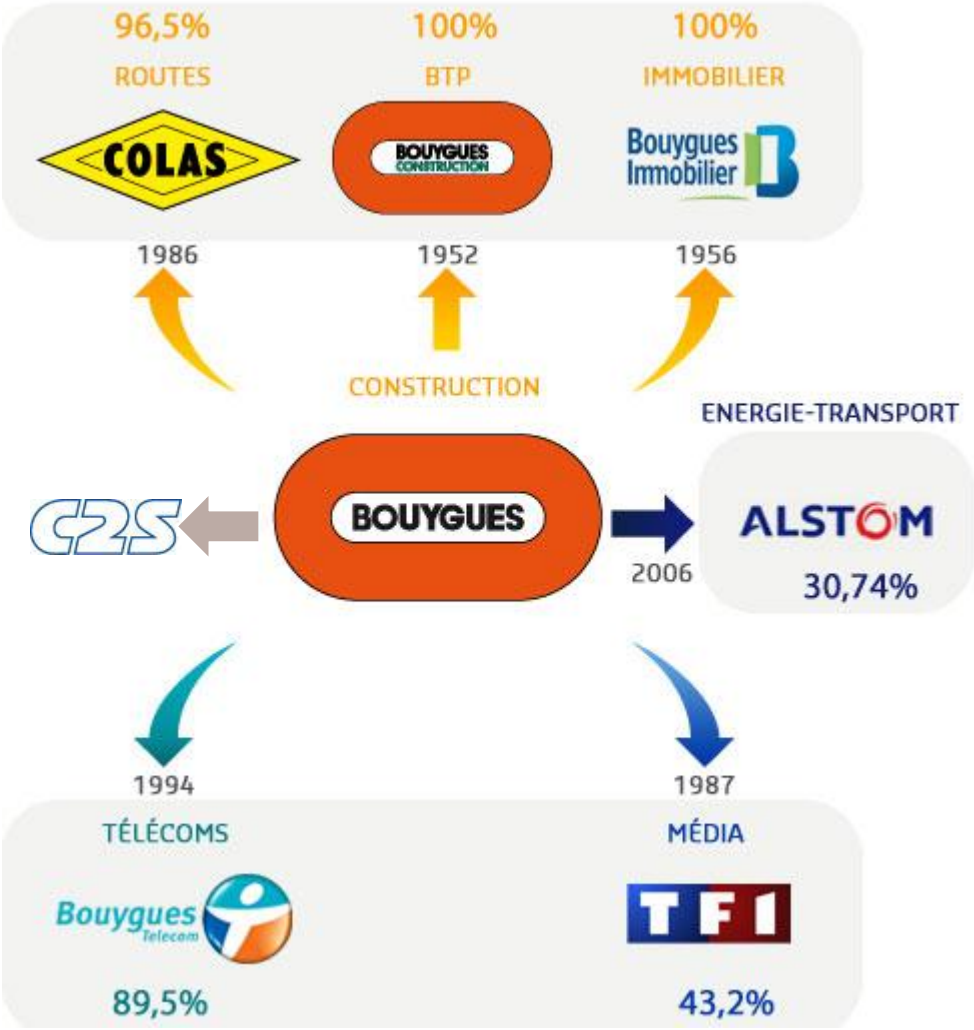
Centre de Sécurité
C2S, Groupe Bouygues

Plan

- Organisation de la sécurité dans le Groupe Bouygues
  - La sécurité au niveau Groupe
  - Rôle de C2S dans le Groupe Bouygues
  - La démarche d'audit de sécurité
- Retours d'expérience (dans le Groupe et en dehors)
  - « Wall of shame »
  - Focus sur les SCADA
- Leçons à en tirer
  - Certaines bonnes pratiques à faire encore progresser
  - La sécurité n'est pas que technique (organisation de la sécurité)
  - Démarche d'amélioration continue (PDCA)

Le Groupe Bouygues en bref

- Métiers
  - Bouygues Construction
  - Bouygues Immobilier
  - Colas
  - TF1
  - Bouygues Telecom
  - + Alstom (30,74 %)
- 133 000 collaborateurs
  - + Alstom : 95 000
- Présent dans 80 pays
- CA 2012 : 33,5 Mds €



Organisation de la sécurité dans le Groupe Bouygues

- Un RSSI dans chaque société du Groupe
  - MOA ou MOE Sécurité
- Audit au niveau Groupe (Bouygues SA)
- CSIG (Comité Sécurité Informatique Groupe)
  - Composé des RSSI des métiers du Groupe
  - Instance de partage et de décision ➔ « RSSI virtuel »
  - Définition des bonnes pratiques de sécurité ➔ politique de sécurité Groupe
- C2S: « bras armé » de la mise en œuvre et de l'audit de la sécurité

Organisation de la sécurité dans le Groupe Bouygues

- Rôle de C2S au niveau Groupe
  - Mutualisation de moyens de sécurité
    - Compétences, expertise
    - Bonnes pratiques
    - Outils de sécurité (licences, hébergement et analyse)
  - Audit et conseil transverses au Groupe
    - Management de la sécurité (schéma directeur, politique de sécurité, …)
    - Accompagnement sur des projets sécurité
    - Audit de sécurité et tests de vulnérabilités
  - Consolidation des résultats
    - But: présenter des tableaux de bords avec des indicateurs de sécurité globaux
  - Rôle de veille et d'alerte
- Interventions également en-dehors du Groupe
- Participation à des groupes de travail (OSSIR, CESIN, Le Cercle, …)

La démarche d'audit de sécurité

- Audits de sécurité organisationnels / techniques
  - Initiés par Bouygues SA
  - Ou demandés au niveau des sociétés du Groupe
- Campagnes récurrentes et systématiques
  - Avant la mise en service de nouvelles applications, de sites Web ou de plates-formes de services
  - De manière régulière (en fonction de la criticité des actifs)
- Elaboration de recommandations pour couvrir les vulnérabilités
- Indicateurs consolidés au niveau des métiers et du Groupe

Retours d'expérience

- Wall of shame: top 10 des vulnérabilités observées*
  (notre OWASP à nous)
  1. *Mots de passe par défaut / triviaux*
  2. *Composants applicatifs / logiciels non à jour (et disposant de mécanismes d'exploitation publics)*
  3. *Injections SQL: 12 ans après, il y en a encore !*
  4. *XSS et autres CSRF*
  5. *Installation / configuration non sécurisées / renforcées*
  6. *Protocoles et flux non chiffrés*
  7. *Gestion non sécurisée des sessions utilisateurs*
  8. *Stockage non sécurisé de mots de passe*
  9. *Imprimantes multifonction recélant tous les secrets d'une entreprise*
  10. *Post-it dans des endroits… inattendus !*

  - *Conclusion: on s'aperçoit que ce top 10 n'est hélas ni original ni surprenant. Les mêmes vulnérabilités se retrouvent depuis de nombreuses années et leur correction progresse très lentement… ☹*

* Retour d'expérience sur des éléments observés dans le Groupe et en dehors

Post-it dans des endroits… inattendus

Un peu d'humour: injection SQL dans la nature…

Retours d'expérience: focus sur les SCADA

- Les audits SCADA ne sont plus anecdotiques …
  - Installations industrielles de production
    - Pompes, compresseurs, vannes de détente, …
    - Accès distants par faisceaux hertziens

  - Systèmes de gestion de bâtiments intelligents
    - Energie, domotique, ascenseurs, téléphonie interne, vidéo, …
    - Manipulent maintenant des données personnelles d'utilisateurs
- … mais ils ne sont pas encore généralisés
  - Marge de progression importante
- Compatibilité avec le Wall of shame: OUI ! ☹

Leçons à en tirer

- Certaines bonnes pratiques à faire (encore) progresser…
  - Intégrer la sécurité tout au long du cycle de vie des projets
  - Définir et mettre en œuvre des politiques de mots de passe (encore et toujours)
    - Stockage, complexité, mots de passe par défaut
  - Code source sécurisé
    - Les écoles d'informatique, ce n'est pas encore ça…
  - Usage de WAF (Web Application Firewalls)
    - Face à l'échec des développeurs, c'est un moindre mal
  - Ne pas se focaliser uniquement sur les vulnérabilités accessibles depuis Internet
    - Les menaces viennent également de l'intérieur…
  - Faire des tests d'intrusion systématiques et récurrents
    - La boucle est bouclée…

Leçons à en tirer

- … mais la sécurité n'est pas que technique
  - Définir des organisations et des méthodologies pour répondre aux risques
    - En lien avec les bonnes pratiques et normes (ISO 2700X par exemple)
  - Sensibilisation des collaborateurs des directions métier et des DSI
    - Face aux tentatives d'arnaques actuelles (social engineering, demandes de virements par téléphone, fax, courrier papier, …)
    - Aux bons comportements à adopter
    - Démarche sans fin, mais globalement productive

  - Formation interne des architectes et des développeurs
- Démarche d'amélioration continue

C2S, Groupe BOUYGUES

JSSI 2013

QUESTIONS ?