LA CONDENSATION DE LA SÉCURITÉ
OU COMMENT TRAITER LA SÉCURITÉ DANS LE NUAGE
JSSI 22 mars 2011

CONNECTING BUSINESS & TECHNOLOGY

DEVOTEAM SOLUTIONS

LA CONDENSATION DE LA SÉCURITÉ
OU COMMENT TRAITER LA SÉCURITÉ DANS LE NUAGE

Qui sommes nous ?

- Guillaume Laudière
- Jean-Marc Boursat

Quel est le sujet ?

- Retour d'expériences sur des offres SaaS

SOMMAIRE

- La sécurité face à l'émergence des offres SaaS
  - Comprendre les impacts sécurité
- Nos constats
  - Retour d'expériences
- Conclusion
  - Savoir préparer la mise en œuvre d'une application en mode SaaS

ÉMERGENCE OU MULTIPLICATION DES OFFRES SAAS

- **Une réelle mutation des SI**
- **Le marché des offres SaaS s'organise**
- **La maitrise de l'information**

Quel peut être notre niveau de confiance ?

ENJEUX SÉCURITÉ DES OFFRES SAAS

- **Besoin de réactivité très fort**
- **Changement de rapport de force**
- **DICT face à la mutualisation des services**

Comment garder le contrôle ?

DES PISTES POUR SE PRÉPARER

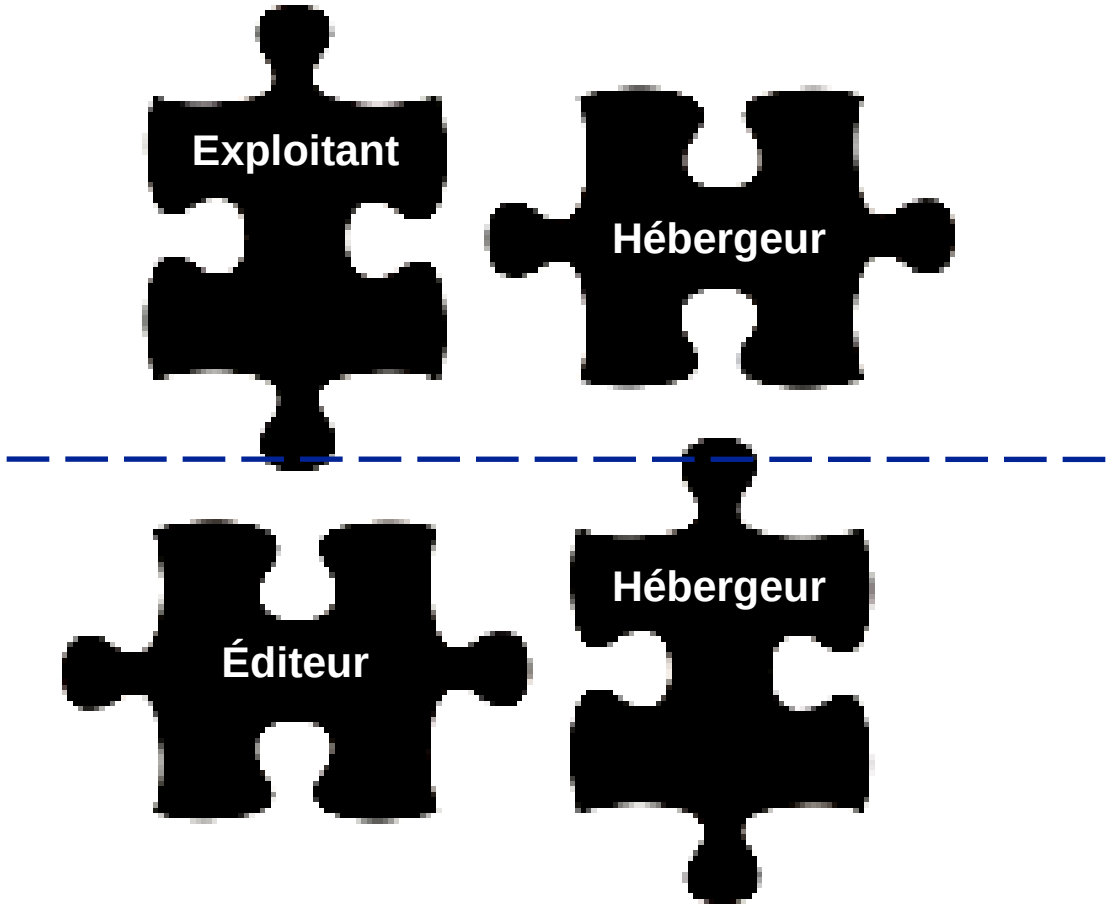
- **Adapter sa politique sécurité**
- **Guider ou accompagner les projets**
- **Définir des contrôles adaptés**

Se concentrer sur les données

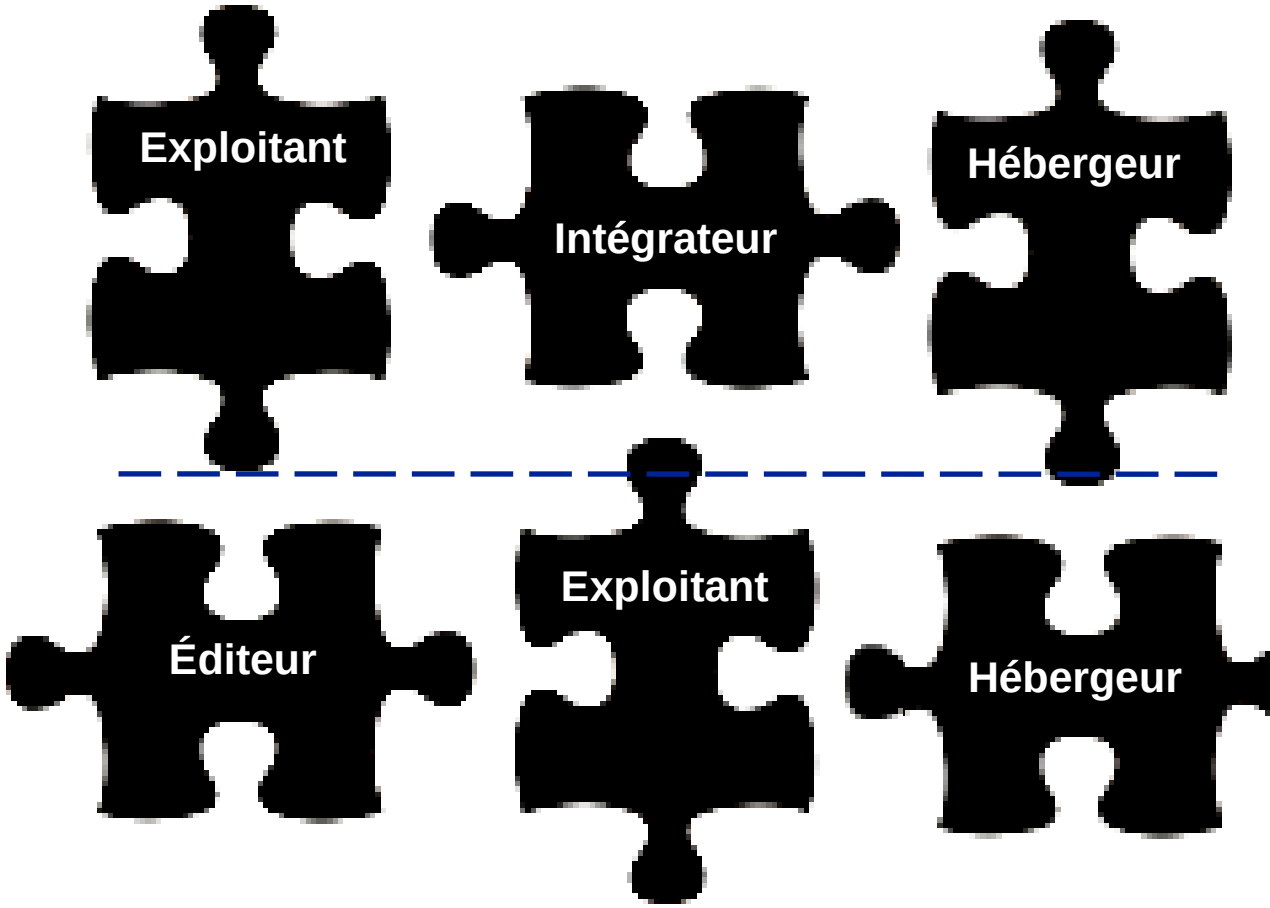
MAITRISER LA PRESTATION

L'application SaaS doit s'insérer néanmoins au SI

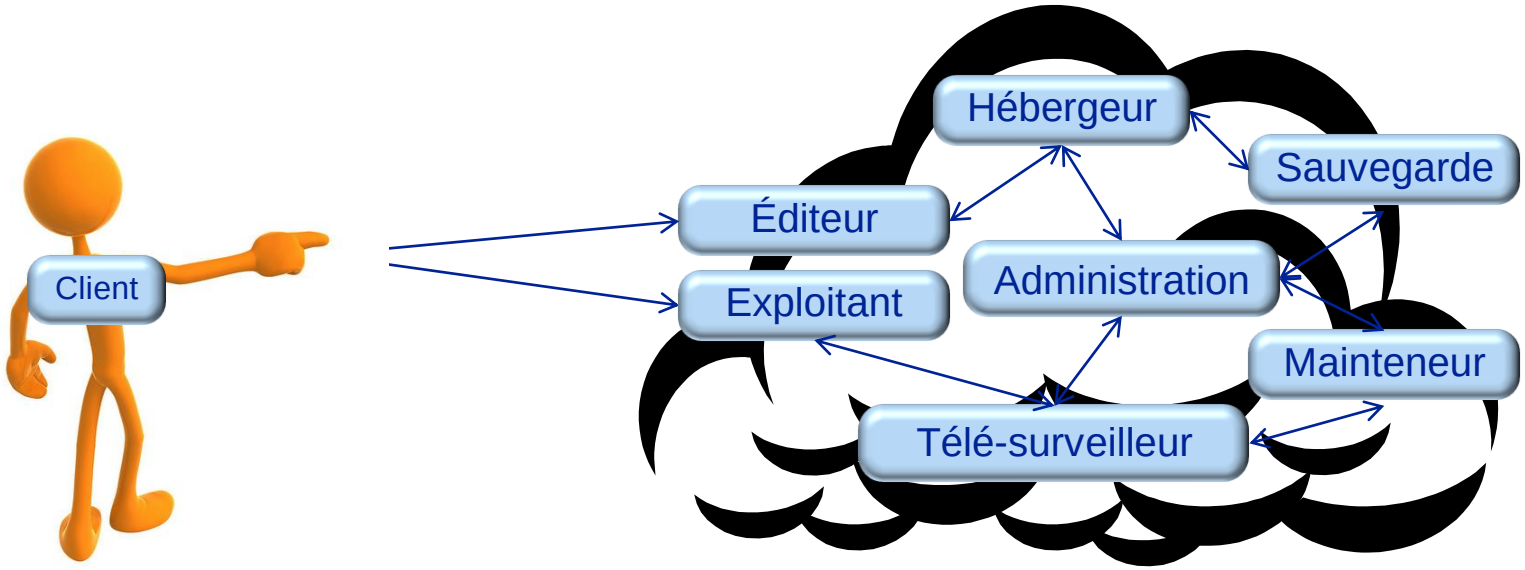
MAITRISER LA PRESTATION



MAITRISER LA PRESTATION



MAITRISER LA PRESTATION



NOTRE DÉMARCHE D'AUDITS

- Analyse des enjeux de sécurité et des contrats
- Approche ISO 27002
  - Organisation de la sécurité de l'information
  - Gestion des opérations et des communications
  - Contrôle d'accès au SI
  - Sécurité physique et environnemental du patrimoine informationnel
  - Acquisition, développement et maintenance des systèmes d'information
- Réalisation de tests d'intrusion

L'INTÉRÊT DE NOTRE DÉMARCHE D'AUDITS

Offrir une vision large de la sécurité de l'application (organisationnelle, contractuelle, technique)

Avoir une méthodologie unifiée permettant une capitalisation des vulnérabilités identifiées

Rechercher la cohésion de la prestation au travers des différents intervenants

UNE ATTENTION CIBLÉE SELON LES ACTEURS

Périmètre \ Acteur	Editeur	Exploitant	Hébergeur
Analyse des enjeux et contrat			
Organisation de la sécurité de l'information			
Gestion des opérations et des communications			
Contrôle d'accès au SI			
Sécurité physique et environnementale du patrimoine informationnel			
Acquisition, développement et maintenance des systèmes d'information			
Réalisation de tests d'intrusion			

LES DANGERS DE L'OFFRE SAAS

1. Le manque de sensibilisation des fournisseurs
   - Principalement des éditeurs (80 % des contrôles effectués)
   - Petites structures (trentaine de personnes)
   - L’approche sécurité n’est pas toujours adaptée au contexte d’une grande société

Un éditeur a utilisé un compte trivial pour l’installation de son application pour TOUS ses clients.

LES DANGERS DE L'OFFRE SAAS

2. La multiplicité des tiers

- Découvertes de tiers non déclarés

Un éditeur a contractualisé l'hébergement et l'exploitation auprès de l'hébergeur A :

- Lors de la revue, l'éditeur découvre que l'hébergeur A n'est pas un hébergeur mais un exploitant louant des m² à un hébergeur.
- Les engagements contractualisés entre l'exploitant et l'hébergeur ne prennent pas en compte les enjeux contractualisés entre le client et l'éditeur.

40 % des contrôles ont révélé une externalisation ou une sous-traitance non déclarée au client

LES DANGERS DE L'OFFRE SAAS

3. Le support et de la gestion des alertes

- Incohérence dans le processus

Constats observés à plusieurs reprises :

- Différence entre la plage horaire d'ouverture et la plage de support,
- Interlocuteurs non identifiés,
- Processus de support et d'escalade entre le client et le fournisseur non formalisés.

60 % des contrôles démontrent un écart au niveau du processus d'alerte

LES DANGERS DE L'OFFRE SAAS

4. La continuité d'activité

Les fournisseurs réagissent en termes de disponibilité d'une application et non dans le cas d'un sinistre d'une salle informatique.

Option dans le contrat non souscrite

Pas de processus transverse de continuité

100 % des contrôles démontrent une défaillance importante au niveau de l'approche Continuité

LES DANGERS DE L'OFFRE SAAS

5. La gestion des sauvegardes

Absence de tests de restauration complets

50 % des contrôles démontrent que les tests de restauration complets ne sont pas réalisés

6. La traçabilité

Absence de centralisation
Absence de revue des journaux (même automatisée)

70% des contrôles démontrent un manque de sécurisation des logs (non centralisés, non contrôlés…)

LES DANGERS DE L'OFFRE SAAS

7. Au niveau Juridique

Déclaration CNIL non réalisée par le client

55 % des clients n'ont pas réalisé la déclaration

8. Au niveau de l'exploitation

Des actions d'administration dans le cadre d'astreinte réalisées depuis des postes personnels non maitrisés

33% des contrôles démontrent un manque de sécurisation des accès d'astreintes

LES DANGERS DE L'OFFRE SAAS

9. La gestion de la fin de la prestation SaaS

- L’arrêt de la prestation d’une offre SaaS doit entrainer la restitution ou la destruction des données
- Les conditions de restitution ou de migration doivent s’anticiper

Lors de la fin de la prestation d’une application, l’exploitant ne disposait pas de processus de destruction des données et pouvait les conserver contractuellement pendant encore plus d’un an.

BONNES PRATIQUES OBSERVÉES

- Bon niveau global de la sécurité physique des hébergeurs :
  - Le niveau de sécurité des sites généralement Tiers 2, 3 ou 4
  - Sécurité des accès physique maitrisée
- Bon niveau de sécurité d'une application SaaS très sensible :
  - Filtrage des flux
  - Chiffrement des disques
  - Démarrage ultra sécurisé de l'application

BIEN SE PRÉPARER

Impliquer les équipes sécurité lors de la constitution du contrat

Les contrôles à mettre en œuvre

L'offre est conforme aux attentes sécurité

Les responsabilités sont clairement définies

Les engagements sont tenus

Maintenir une relation de confiance est primordial pour pouvoir assurer les contrôles dans de bonnes conditions et maintenir un bon niveau de réactivité

La réalisation d'une revue permet au fournisseur de mieux comprendre les attentes de ses clients

LES LIMITES DU MODÈLE

DERNIERS MOTS

Security as a Service

Effet de mode

Profonde mutation

CONTACT: Jean-Marc Boursat / Guillaume Laudiére

PHONE: 06 64 48 96 27 / 06 87 73 27 12

EMAIL: Jean-marc.boursat@devoteam.com
Guillaume.laudiere@devoteam.com

COUNTRY: France

WEBSITE : www.devoteam.com

AUTHOR:

DATE: 22/03/2011

FURTHER INFORMATION:

PICTURES:
DREAMSTIME.COM OG BIGSTOCKPHOTO.COM