Nouveau périmètre du SI

La sécurité des plates-formes ASP / SAAS

Comment concilier les objectifs de sécurité des sociétés clientes et des offreurs?

Retour d'expérience

Agenda

- Le contexte
  - Plates-formes ASP & SAAS : Définition, le marché
  - Exemples d'impact sur la sécurité des entreprises
  - Pourquoi les clients des DSI adorent ces plates-formes?
  - Quels sont les cas que vous pourriez rencontrer?
- Comment concilier les objectifs de sécurité des sociétés clientes et des offreurs?
- Bilan du niveau de sécurité généralement constaté
- Conseils & Recommandations (coté client & coté offreur)
- Conclusion

Le contexte

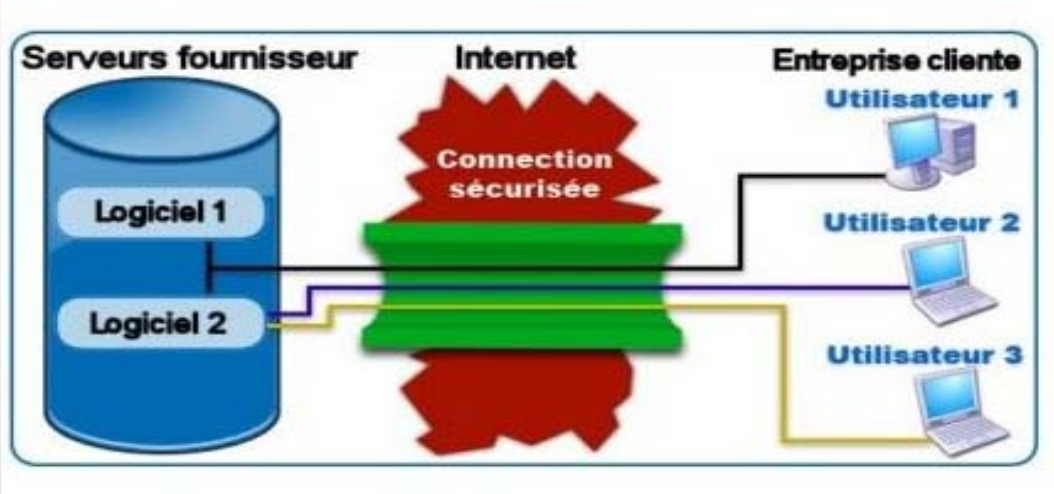
- Concevez toujours une chose en la considérant dans un contexte plus large

Le contexte

- L'externalisation de service métier sur des plates-formes d'hébergement externes est une tendance de fond.
- Mais quel est le niveau de sécurité de ces plates-formes?
- Comment assurer la sécurité des données qu'une entreprise confie à ces partenaires?
- Comment un offreur peut « rassurer » ses clients sur la sécurité de sa plate-forme?

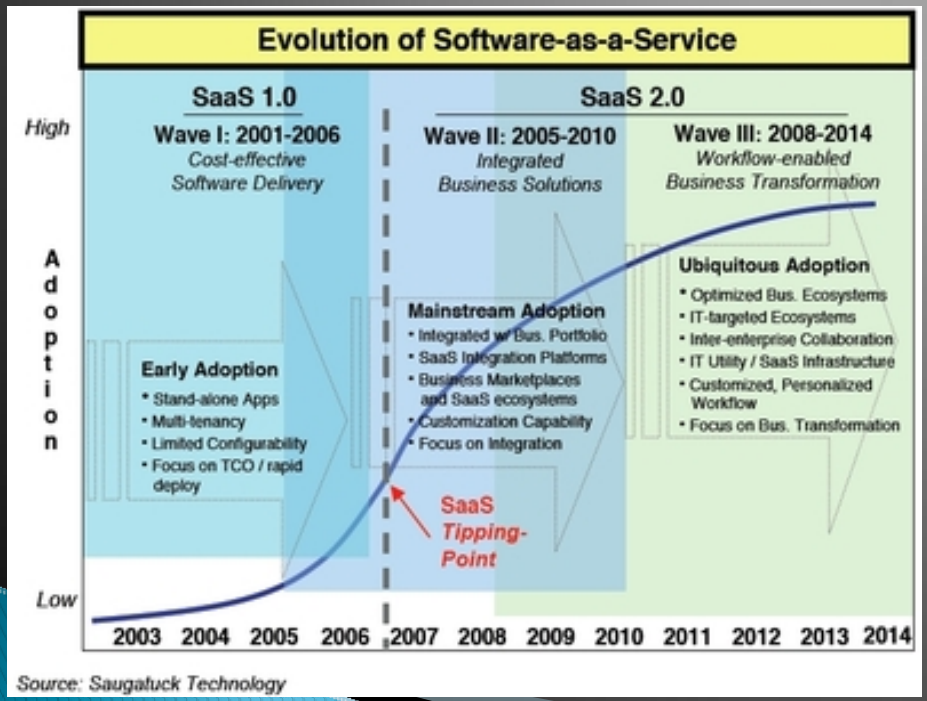
Plates-formes ASP & SAAS !? Kesako?

- ASP = Application Service Provider
- SAAS = Software As A Service
- Globalement, c'est de l'hébergement de logiciel à distance



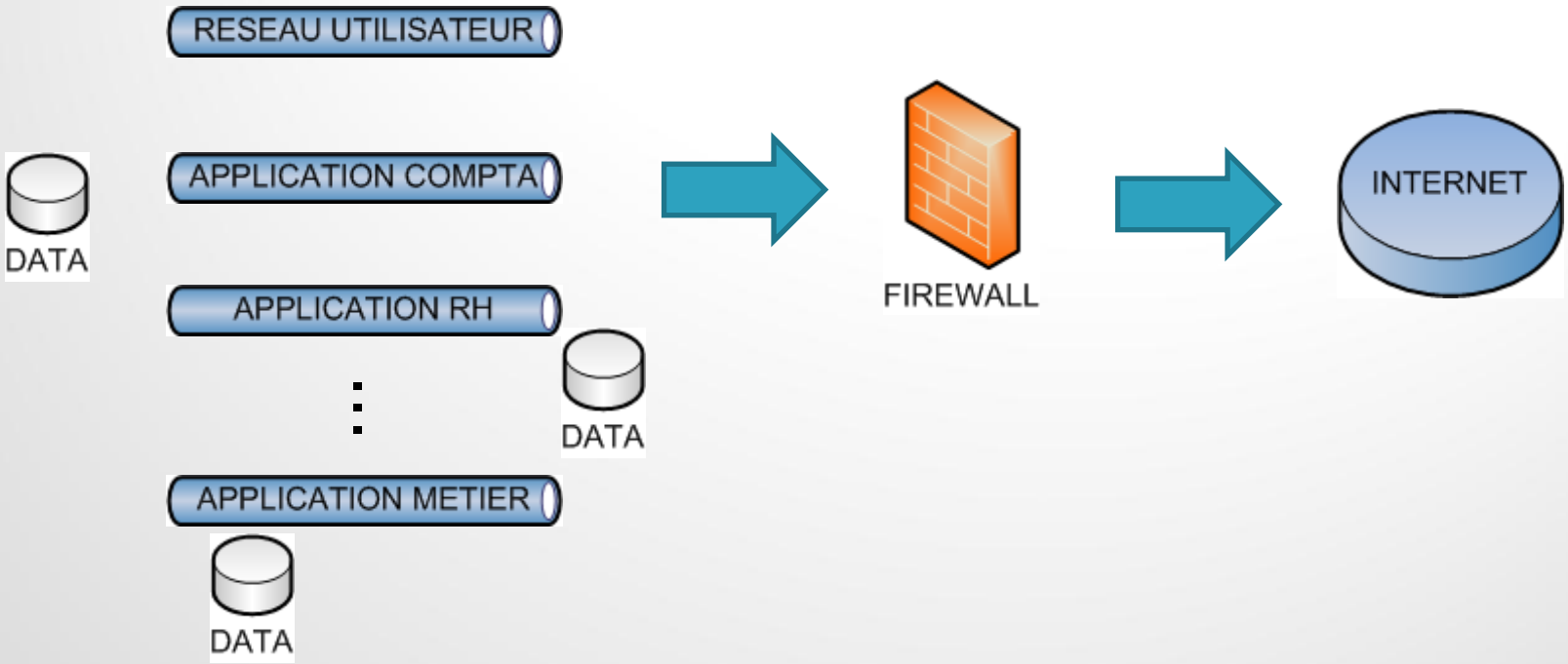
Une plate-forme ASP ou SAAS pour quoi faire?

- Un marché en pleine évolution
- Tout type de service offert



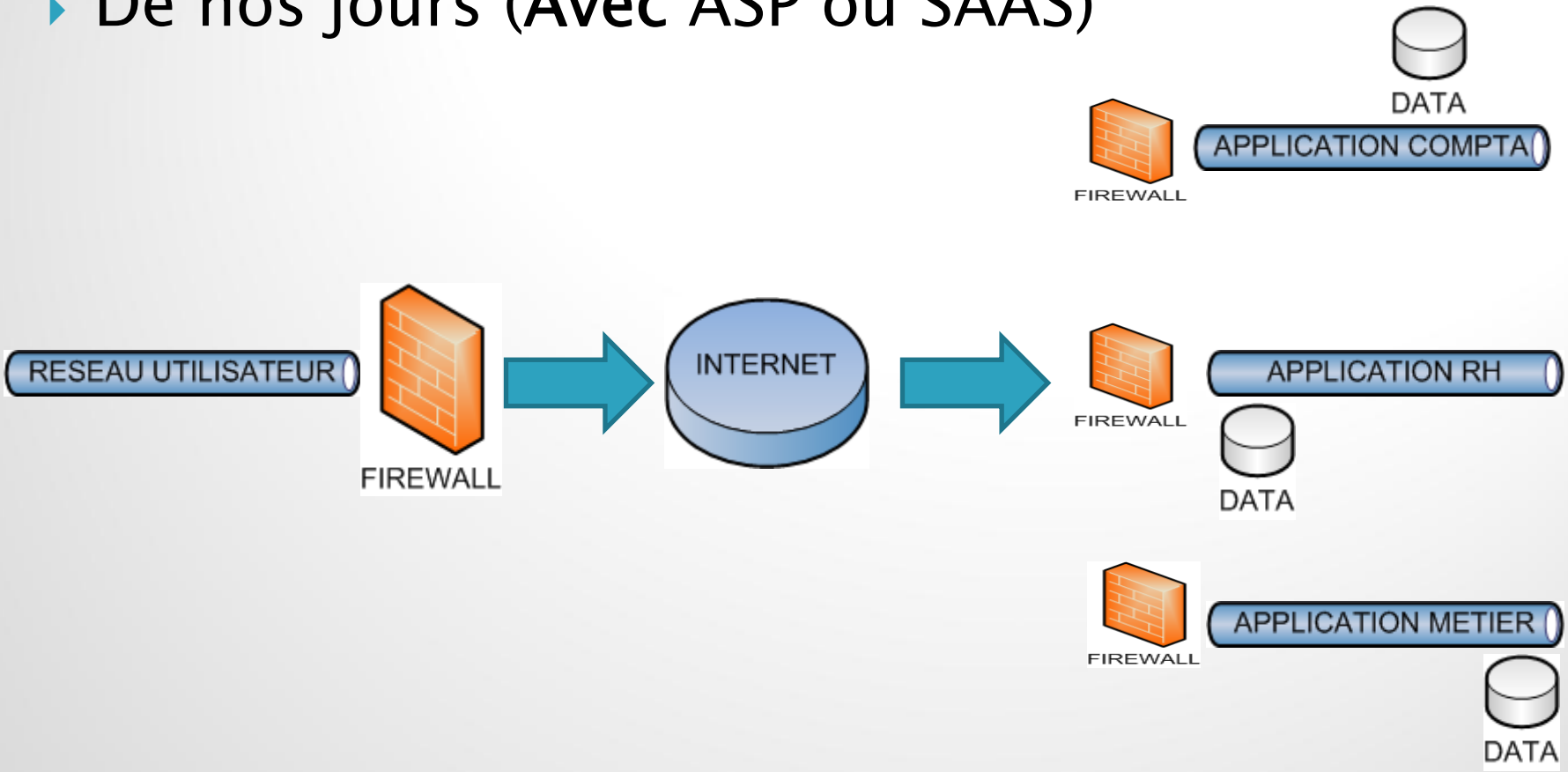
Impact sur les SI d'entreprise

- Avant (Sans ASP ni SAAS)



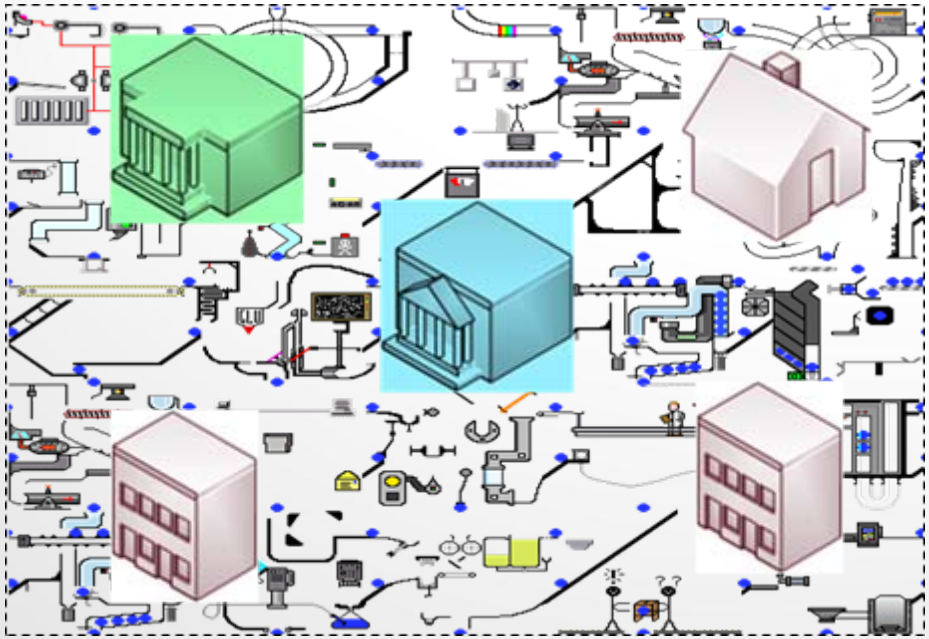
Impact sur les SI d'entreprise

- De nos jours (**Avec** ASP ou SAAS)



Impact sur les SI d'entreprise

- Après une analyse précise, la situation se complexifie un peu…



Les risques

- Le problème, c'est que si l'on ne prend pas de risque, on risque encore davantage

Quels sont les risques? (1 /2)

- Risques techniques
  - Attaque par rebond sur votre SI Interne
  - Hacking, etc.…

- Risques juridiques ou de non-conformité réglementaire
  - En cas de compromission de la plate-forme … qui est responsable vis-à-vis de vos clients ? Vous? l'offreur? Personne ?

- Risques d'image
  - les compromissions de plate-forme ASP entraîne toujours un risque d'image **pour les offreurs aussi bien que pour les clients**

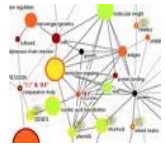
Quels sont les risques? (2/2)

- Globalement la typologie des risques est assez classique

- Cependant le niveau d'exposition est plus grand

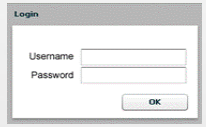
  - Mutualisation des données sur une même plate-forme
  - Chaque client a ses propres contraintes d'accès (Simple mot de passe, carte à puce,…)
  - La sécurité de l'ensemble dépend de celle du client le moins «regardant»
  - Schématiquement vos données sont accessibles depuis Internet

Exemples d'impacts sur la sécurité des entreprises



- **Dissémination et complexification du patrimoine informationnel**
  - Un RSSI s'occupe de la sécurité de son entreprise (son SI) … la tâche est déjà lourde !
  - Maintenant il doit vérifier et contrôler la sécurité des SI des plates-formes ASP que son entreprise utilise (Bon courage à tous !)

- **Diminution de l'efficacité des protections, notamment la sécurité des accès**
  - Accès nomades à votre SI interne via des VPN + authentification forte
  - En mode ASP, le plus souvent le contrôle d'accès est un simple login/mot de passe



Alors pourquoi les clients des DSI adorent-ils ces plates-formes?

- Vision précise des coûts
  - Coût et temps de mise en place réduits
  - Coût généralement calculé par utilisateur (Visibilité et Clarté)

- Autonomie vis-à-vis de la DSI
  - Gestion de projet autonome
  - Projet géré en externe

- Pour se soustraire à une obligation légale
  - PCI DSS par exemple

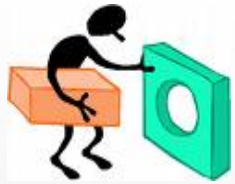
- Il fait toujours plus beau ailleurs
  - …en tout cas plus que dans la DSI interne…

Quels sont les cas que vous pourriez rencontrer?

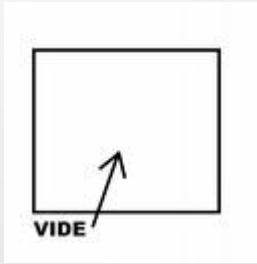
- Contraintes réglementaires
  - Module de paiement en ligne = Obtention d'un certificat PCI DSS
  - Système monétique sur IP = Pré-Requis GIE CB

- le Time-To-Market
  - Sites évènementiels à mettre en production pour hier !
  - Campagne marketing

- Incompatibilité technique
  - Choix de la DSI = Open Source
  - Seule solution répondant aux besoins fonctionnels = Produit commercial



- Inexistence de solution internalisable
  - Plusieurs solutions n'existent qu'en mode ASP !



Le problème

- Comment concilier les objectifs de sécurité des sociétés clientes et des offreurs?

Contraintes coté « offreur »

- Comment sécuriser sa plate-forme?
- Comment rassurer ses clients?
- Comment répondre à toutes les demandes d'audit?
- Comment démontrer que votre sécurité est efficace?

Test d'intrusion client A

Audit Client B

Remplir les 350 pages du questionnaire sécurité du client C

Contraintes coté clients

- Comment s'assurer de la sécurité des données?
- Par quels moyens ?
  - Audit, Test d'intrusion, certification des offreurs…
- Avec quels moyens?
  - Budget, compétence,…
- Quels processus SSI mettre en place?
  - Peut-on (doit-on?) tout externaliser?
  - Dans quelles limites?

Audit de code de la plate-forme RH

Budget

Besoin d'un auditeur qualifié ! Interne? Externe?

Processus de validation des fournisseurs

Les solutions:

- Plusieurs approches possibles

- Retour d'expérience n°1

Approches possibles

Approche	Avantages	Inconvénients
Certification (ISO27001, PCI DSS, …)	- 1 certification « présentable » à plusieurs clients - Faible monopolisation des ressources (RH, Budget,…) de l'entreprise cliente	- Est-ce que la certification couvre correctement les besoins d'évaluation? - Avez-vous confiance dans les auditeurs des sociétés de certification?
Audits	- Evaluation de la sécurité selon les critères de l'entreprise cliente - Analyse complète des processus et des systèmes	-Nécessite la monopolisation de nombreuses ressources chez le fournisseur (ceci cause de nombreux refus) - Coût élevé
Test d'intrusion	-Vision des vulnérabilités réellement exploitables - Peu de ressource à monopoliser - Peu d'interaction avec le fournisseur	- Aucune vision sur le niveau d'implémentation des processus et de l'application des bonnes pratiques de gestion de la sécurité d'un SI
Questionnaires sécurité	- Permet d'avoir une réponse formelle sur les moyens mis en place par le fournisseur	- Vision théorique du niveau de sécurité

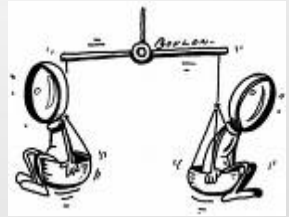
Les solutions:

- Notre proposition

- Retour d’expérience n°2

Comment les sociétés clientes et les offreurs peuvent-ils interagir?

- Être Pragmatique
  - Ne pas monopoliser trop de ressources (réduction des coûts)
  - Obtenir une vision réelle du niveau de sécurité
  - Valider la mise en place des bonnes pratiques
- Travailler en transparence avec ses partenaires ou ses clients
  - Rencontrer les personnes en charge de la sécurité
  - Expliquer les méthodes d'évaluation, de sécurisation,…
- Prévoir des clauses juridiques dans les contrats
  - Clauses d'audit ou de test d'intrusion récurrents
  - Obligation ou engagement formel de corriger les vulnérabilités détectées
- Evaluer le niveau de sécurité
  - Test d'intrusion & questionnaire de sécurité



Est-il vraiment nécessaire de valider la sécurité des ASP/SAAS?

- Bilan

Retour d'expérience n°3

Quel est le niveau de sécurité généralement constaté?

- **Selon notre retour d'expérience, dans 2/3 des cas des faiblesses de sécurité d'un niveau critique ou important apparaissent** lors des évaluations de sécurité
- Alors? **ASP/SAAS moins « secure » ?**
- Notre opinion : **pas plus que les autres types de solution!**
- La cause:
  la sécurisation des couches applicatives est encore mal maitrisée par la majorité des acteurs qui gèrent un SI (externe ou interne)

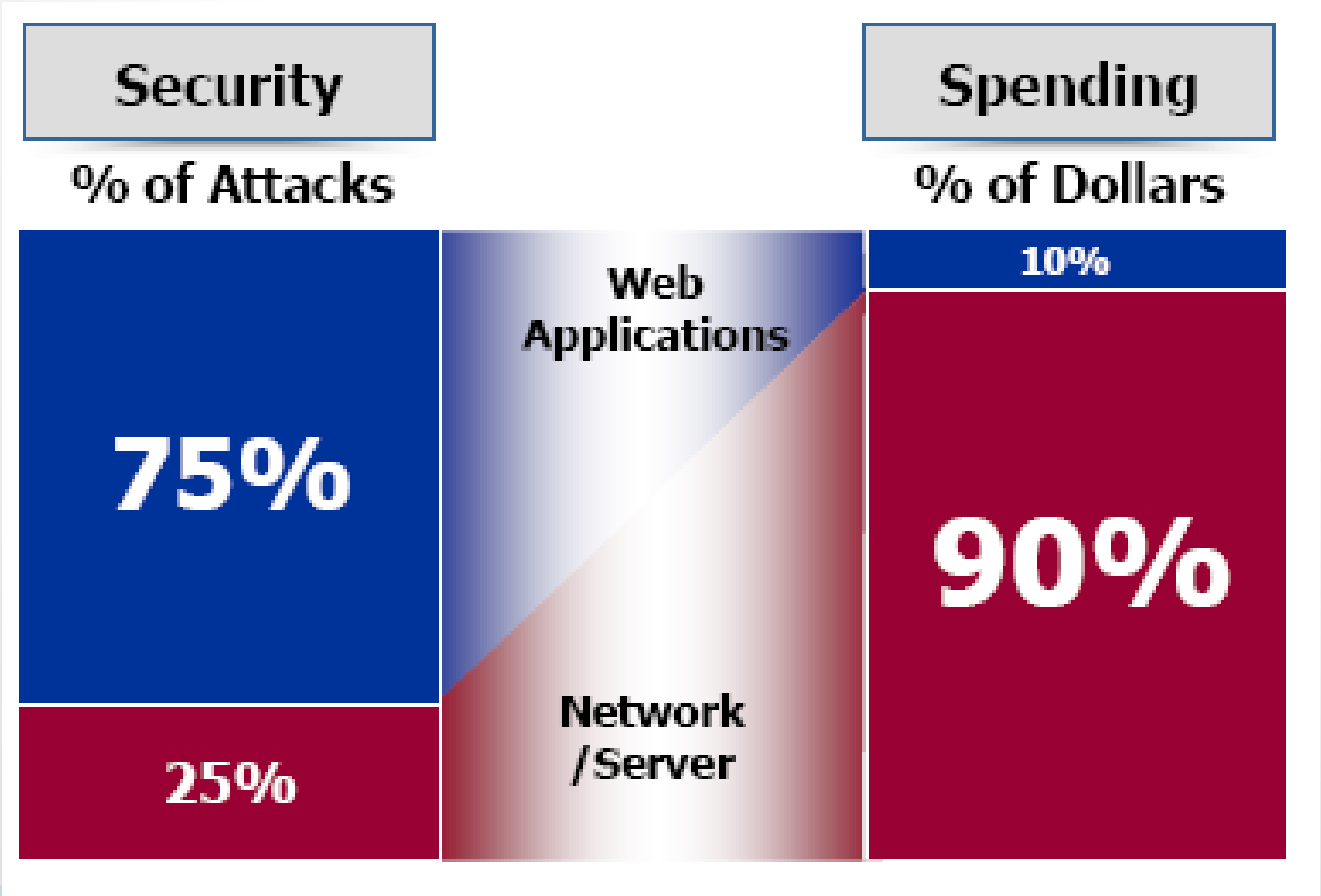
Notre proposition

- Retour d'expérience n°4

- Fort Besoin de réallocation des budgets SSI vers les aspects applicatifs

Fort Besoin de réallocation des budgets SSI

Illustration du pb…



Conseils & Recommandations

- Retour d’expérience n°5

Conseils & Recommandations Coté client (1 /2)

- Tester TOUS vos fournisseurs de solution ASP/SAAS
  - Même les applications secondaires (risque d'attaque par rebond)
  - Cependant, il faut moduler le temps passé en fonction des risques
- Sensibiliser vos clients internes aux enjeux
- Prévoir dans vos budgets les J/H nécessaires
  - Application critique – 10 à 15 jours/homme
  - Application moyennement critique – 5 à 7 jours/homme
  - Application peu critique – 1 à 2 jours/homme max

Conseils & Recommandations Coté client (2/2)

- Faire réaliser les tests d'intrusion
- Faire un bilan chaque année auprès de vos directions (Tableau de bord, suivi des risques liés à l'externalisation d'une partie du SI, …)
- Utiliser vos « découvertes » en interne dans le cadre de vos actions de sensibilisation (démonstration pragmatique des risques!)

Conseils & Recommandations Coté offreur (1 /2)

- Développer une culture sécurité au sein de votre entreprise
- Formation et mise en place de best practice à tous les niveaux (développement, exploitation, production…)
- Valoriser votre démarche sécurité
  - Transformer la « contrainte sécurité » en un élément valorisant ($)

Conseils & Recommandations Coté offreur (2/2)

- Faites vous accompagner par des spécialistes de la sécurité.
- ou créer votre propre cellule d'experts internes qui pourront répondre aux interrogations de vos clients et mettre en place les bonnes mesures de sécurité.
- Réallouer une partie de votre budget sécurité sur les aspects applicatifs de vos plates-formes (suivi des menaces !)

Conclusion

- L'utilisation de plate-forme ASP/SAAS entraine des risques qui doivent rester maitrisés
  - Il faut juste s'assurer que le niveau de sécurité est en adéquation avec les enjeux
  - De toute façon, les solutions ASP/SAAS répondent à un réel besoin économique et/ou stratégique pour les entreprises (Recentrage sur leur métier, diminution des coûts,…)
  - Dans ces conditions, les rejeter serait une erreur même en invoquant la sécurité : Il vaut mieux accompagner le changement

Conclusion

- Mais faites particulièrement attention à la sécurité applicative des plates-formes ASP/SAAS.

- C'est souvent leur talon d'Achille…

Merci de votre attention

Questions?

contact@opale-security.com