

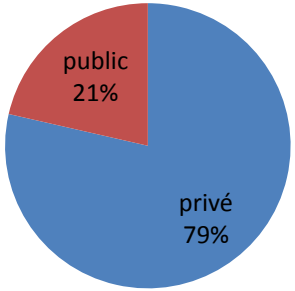


# Rapport d'enquête sur la sécurité des systèmes d'information en PACA 2016

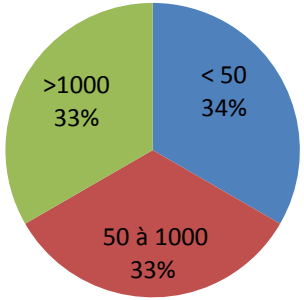
Apéritif du CIP 1er février 2016

# * Une enquête fiable et représentative

- 193 réponses, 60 exploitées
- DSI +RSSI+DG : 70%
- Services : 25 %




**Taille des entreprises**




- Représentatif de la région PACA et du tissu économique français selon les statistiques INSEE 2010
- 40% de gros chiffres d'affaire plus de 100 M et 5% + de 1Md, logique de la taille de l'entreprise

# * Sécurité bien intégrée au management malgré de faibles moyens alloués

- Budget Sécurité : 3 à 5% du budget de la DSI
- 70% ont un plan de secours informatique
- 57% ont déjà fait une analyse de risques
- 46% ont une PSSI, autant n'en ont pas et surprenant 10% ne savent pas
- 43% font un audit de sécurité par an
- 68% ont une charte et 67% ont une procédure pour gérer les comptes (départ, mutations) loin devant la sensibilisation des utilisateurs 50%

## Quelques surprises :

- 70% ont un cadre de référence avec des contraintes de sécurité,
- 45% se disent soumis au secret professionnel ( sensibilité des données) mais pour 30% il n'y a pas de cadre normatif en SSI
- Pour 52 % la fonction RSSI est clairement identifiée
- 53% ont un responsable des déclarations CNIL

# *Le CLOUD est attractif malgré une conscience claire des risques dans ce secteur

- contrat d'infogérance pour 45% (5% en totalité)
- seulement 23% intègrent toujours des clauses de sécurité des SI dans leur contrats
- 75% ont recours à des services en Cloud donc 35% sans contrats et 37% n'ont pas confiance dans le Cloud
- freins à une externalisation du SI :

1. la confidentialité
2. la localisation des données
3. des performances
4. de la rupture de contrat
5. perte des données

*Montre que les données sont estimées sensibles*

Pourquoi les entreprises adhèrent au Cloud malgré les risques bien identifiés?

# *Des outils de sécurités classiques et tournées sur la réaction plutôt que la prévention

Des surprises:

- Seulement 58% des entreprises mettent toujours à jour les patchs de sécurité! Préoccupant
- 30% sont déjà assurés contre les risques en SSI sur un marché naissant
- 90 % des entreprises ont Firewall, Antivirus, Anti spam

30% ont des Sonde et outils chiffrement

- 55% n'autorisent pas le BYOD
  cette statistique rejoint les chiffres nationaux du CLUSIF de 2014 et la tendance au rejet.

les Smartphones et tablettes ne sont pas aussi bien protégés que les PC

# *Une forte conscience de la dépendance au SI et une faible prise en considération des risques malgré des incidents significatifs

- 90% ne peuvent pas se passer de leur SI plus de 24H, 70% le jugent vital,
- 70% disent redémarrer en moins d'un jour en cas de sinistre : Surprenant !
- Peu de recours aux plaintes 17%, chiffres identiques à ceux du CLUSIF 2014. Par contre, le nombre de dépôts est en augmentation depuis 2008
- 58% jugent que les perturbations en cas de sinistre et 70% les conséquences seront graves ou significatives
- Principal critère de sécurité : Confidentialité et intégrité n'est pas en cohérence avec les mesures et outils de sécurité qui protègent surtout la disponibilité!

# * La protection des SI est jugée suffisante le degré de maturité est moyen

- Pour 75%, le degré de motivation des attaquants est jugé faible. Les entreprises ne se sentent pas menacées. Elles estiment pourtant leurs données confidentielles mais pas attractives pour les cybercriminels!!
- Les moyens des attaquants sont jugés faibles ou significatifs pour 77%
- Le système est sous contrôle. Pour 97%, le SI n'est pas accessible de l'extérieur ou accessible sous contrôle
- niveau moyen de maturité : 2,5 sur 4!!
  conscience de la dépendance avec le SI et la faible conscience du potentiel de l'attaquant?

- 50 % de réponses de membres du CIP :
  ont-elles un niveau de maturité plus élevé?

- Enquêtes disponibles le 15 février :
  Et vous comment vous positionnez-vous?