Cloud computing 2013-14

Laurent Wargon
laurent@wargon.org

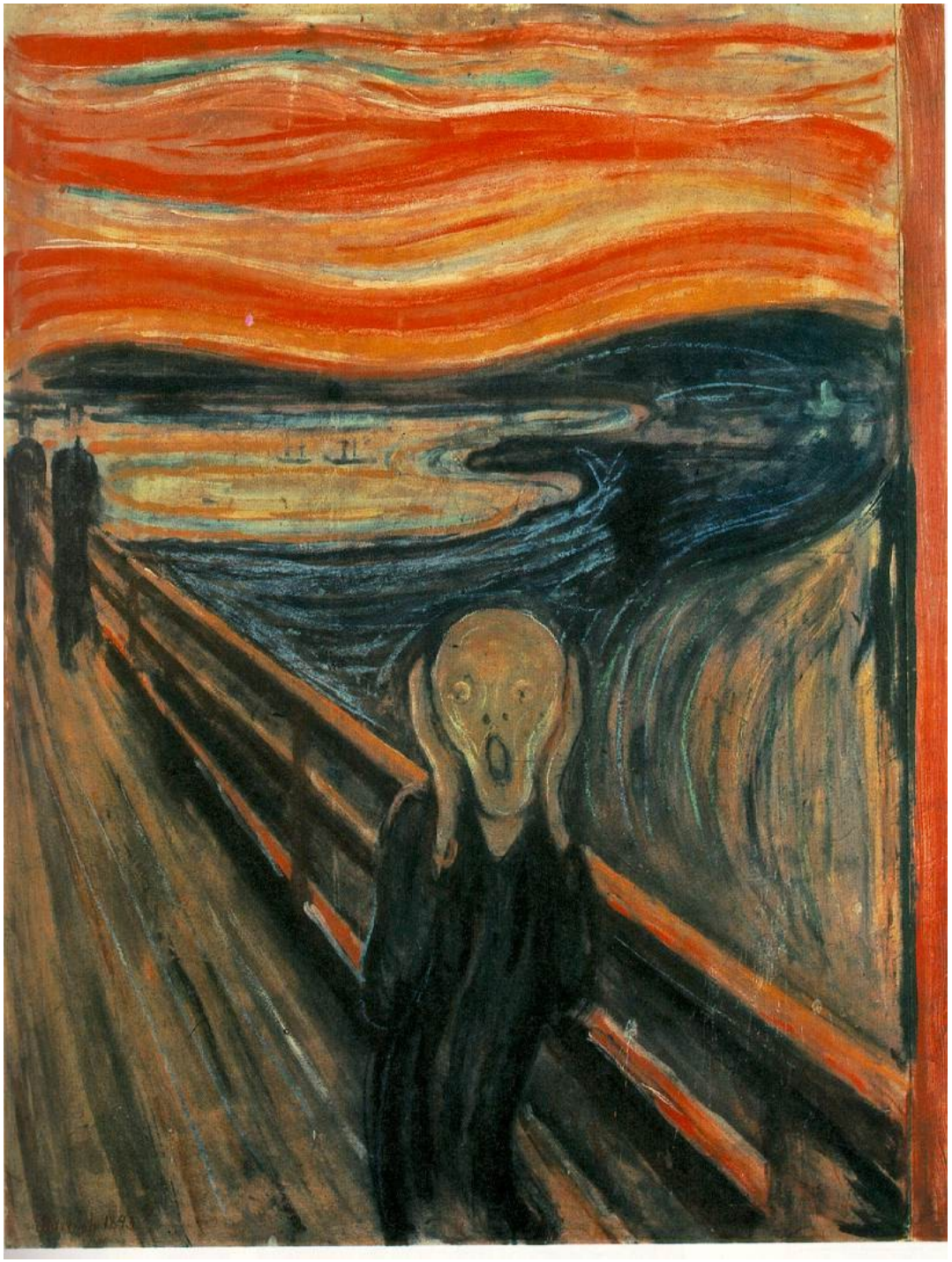
La sécurité dans le Cloud

La sécurité dans le Cloud

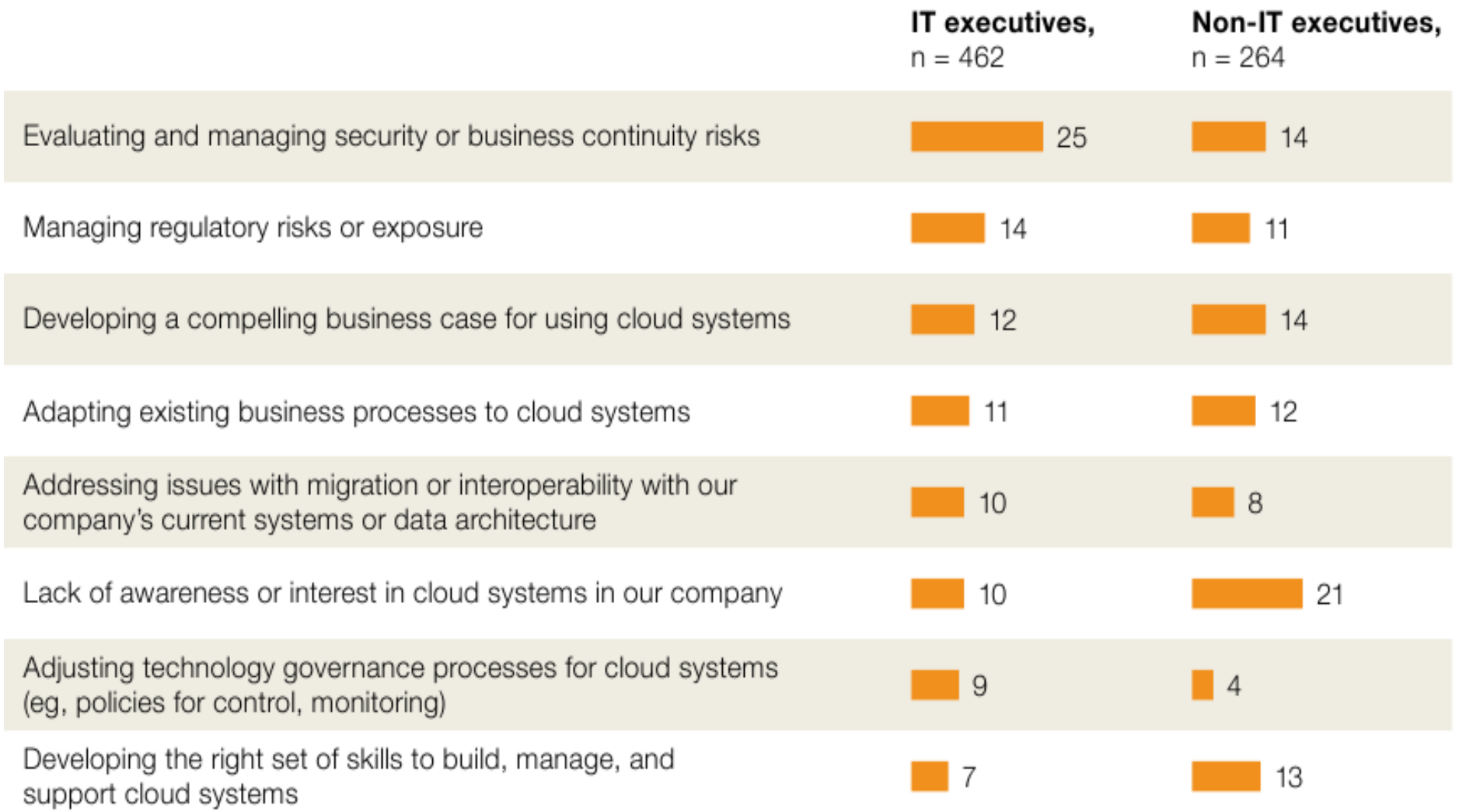
- Craintes
- Analyse des risques
- Confidentialité
- Inter-opérabilité
- Sécurité logique
- Conformité légale

Des craintes

Où sont mes données ?!?!?!



Sondage sur les barrières d'adoption



Source : McKinsey « How IT is Managing New Demands

Pannes (1/3)

- Microsoft : 4 janvier 2011 email d'utilisateur de hotmail effacés par erreur, restauration après quelques jours.
- Google : 28 février 2011 150 000 utilisateurs de gmail ont perdu des données en raison de problème technique
- Amazon : 21 avril 2011 0,07% des données ont été effacées.
  La panne n'a pas été expliquée
- Sony : 27 avril 2011 données personnelles de 77 millions de clients exposés
- Dropbox : 17 juillet 2012 client HS pendant 20min (web ok)

Pannes (2/3)

- Gmail : 17 avril 2012 panne pour 35 millions d'utilisateurs pendant une heure
- Linkedin : 6 juin 2012 vol de 6,5 millions de mots de passe « la ***plupart*** des mots de passe mis en ligne sont restés cryptés. »
- Yahoo : 13 juillet 2012 400 000 identifiants / mot de passe ont été dérobés. Il s'agit d'un « fichier ancien » 5 % des comptes avaient des mots de passe encore valides
- GoDaddy 19 septembre 2012 [hébergement de nom de domaine (53 millions), de sites internet et de messagerie] panne de routage pendant 6 heures

Pannes (3/3)

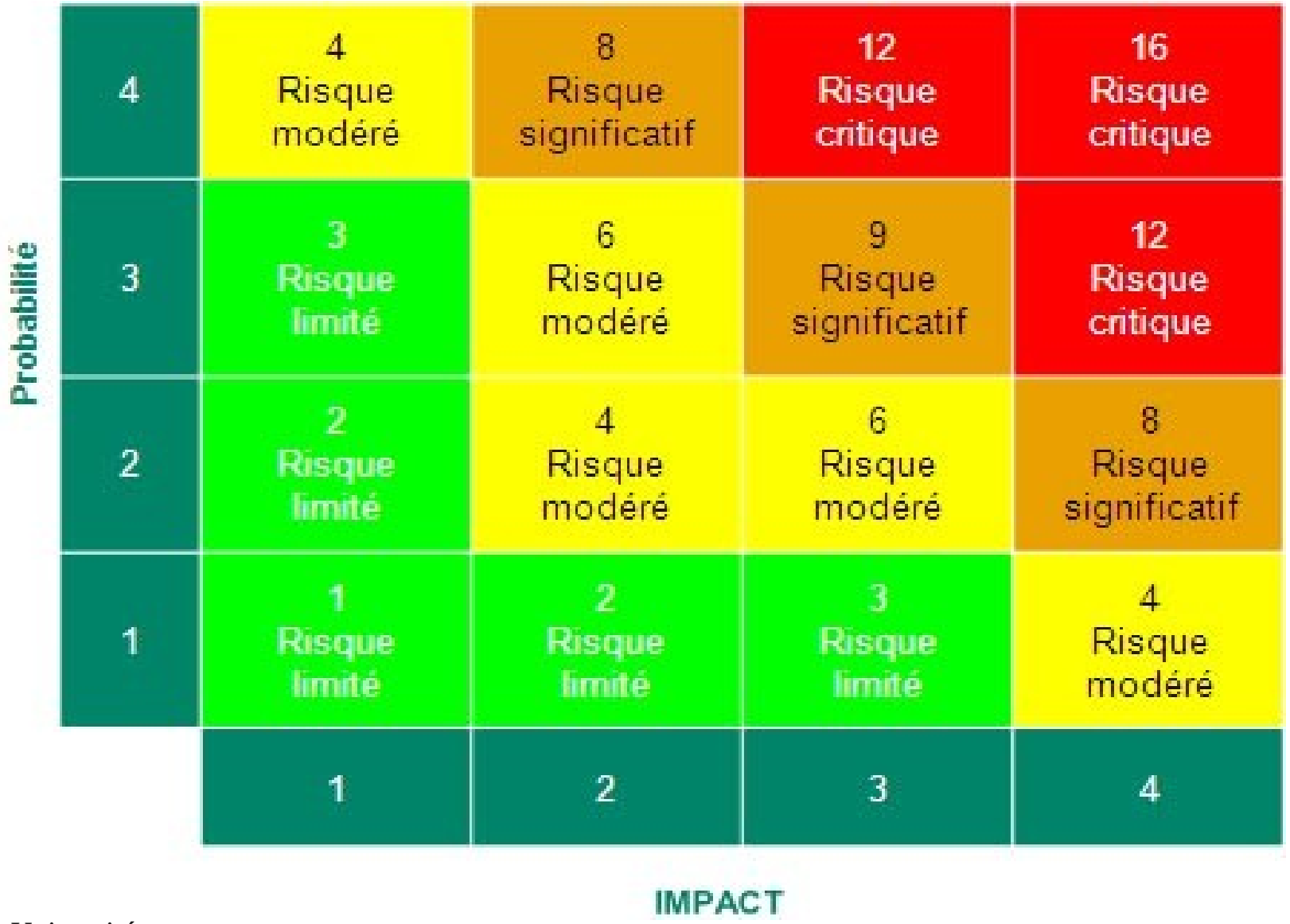
- 28 mars 2013 : American Express victime d'une cyberattaque de grande ampleur (site bloqué pendant 2h)
- 30 avril 2013 : Les pannes de Microsoft se succèdent dans le cloud. (source pro.01net.com)
- 20 juin 2013 : Panne géante pour le logiciel Chorus qui gère les dépenses de l'état : 35 000 personnes pendant 4 jours
- 14 juillet 2013 : Piratage d'OVH : récupération du fichier client Europe (nom, adresse, téléphone, mot de passe)
- 17 août 2013 : Une panne de 11 minutes chez Google fait chuter le trafic Web de 40 %
- 5 Octobre 2013 : 38 millions de comptes utilisateurs piratés et le code source de Photoshop volé

Analyse des risques

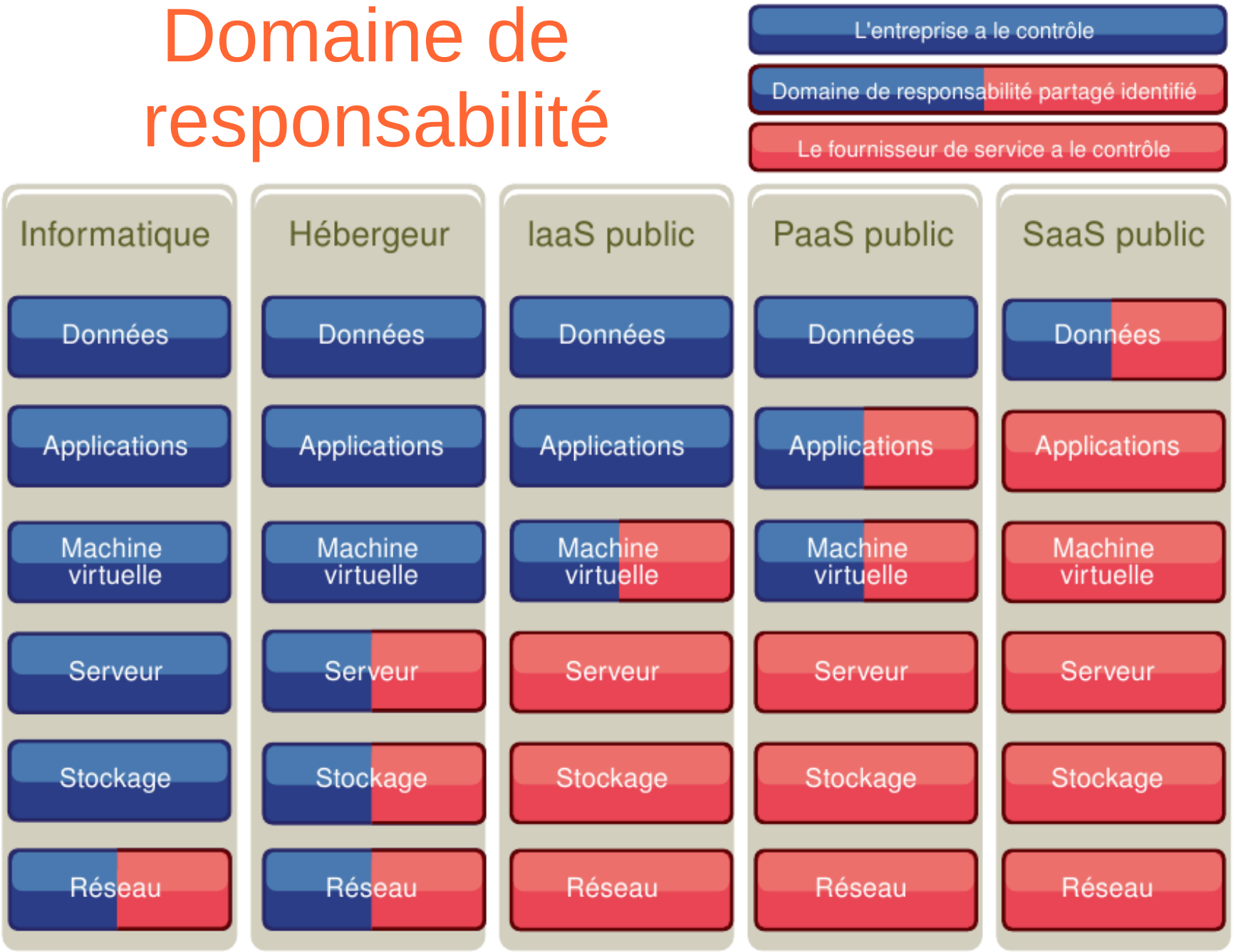
Risques

- Événements incertains qui ont une probabilité de se produire et d'avoir un impact positif (opportunité) ou négatif (menace).
- Analyse dans un contexte global
- Le recours à un prestataire peut permettre de pallier l'absence ou l'insuffisance de moyens internes, à condition que le prestataire s'engage sur la sécurité.

Matrice de gestion des risques



Domaine de responsabilité



Confidentialité

Un mot de passe

- Mon prénom, ma date de naissance, le prénom de ma chérie, le prénom de mon fils, …
- Le même mot de passe pour tous ses comptes
- Social engineering
- Validation en deux étapes
- Un bon mot de passe doit être constitué d'au moins 10 caractères de minuscules, de majuscules, de caractères spéciaux et de chiffres.

Safe Harbor

Certification d'une entreprise américaine pour le respect de la législation de l'Espace économique européen, l'entreprise :

- Informe sur la collecte des données
- Donne la possibilité de refuser le transfert des données à des tiers
- S'il y a transfert, les mêmes niveaux de garanties sont conservés
- Prend des mesures de protections (suppression, divulgation ...)
- Utilisation des données avec accord de l'utilisateur
- Accès aux modifications sur les données
- Obligation de tout mettre en œuvre pour le respect de ces règles
- Microsoft, Amazon, Google, Facebook, ...

Google : Garanties et clauses de non responsabilité

Notre offre de Services est soumise à une obligation de moyens, [...]. Nos Services font cependant l'objet d'une limitation de garantie.

Sauf tel qu'expressément prévu par les présentes Conditions d'Utilisation ou des conditions d'utilisation additionnelles, **ni Google, ni ses fournisseurs ou distributeurs, ne font aucune promesse spécifique concernant les Services**. Par exemple, nous ne contractons aucun engagement concernant le contenu des Services, les fonctionnalités spécifiques disponibles par le biais des Services, leur fiabilité, leur disponibilité ou leur adéquation à vos besoins. Nous fournissons nos Services « en l'état ».

[…] Dans les limites permises par la loi, nous excluons toute garantie. (11/11/2013)

USA Patriot Act

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

Les services de sécurité américains peuvent accéder aux données à caractère personnel

Cela concerne les données hébergées

- sur le continent américain par n'importe quelle société
- par des sociétés de droit américain n'importe où

http://www.fincen.gov/statutes_regs/patriot/

Edward Snowden : PRISM

- Cible : des personnes vivant hors des États-Unis
- la NSA dispose d'un accès direct aux données hébergées par Google, Facebook, Apple, Microsoft, Yahoo, Skype, AOL…
- captation des métadonnées des appels téléphoniques aux États-Unis
- la NSA a développé de multiples méthodes de contournements des cryptages SSL

Edward Snowden : XKeyscore

- collecte quasi-systématique des activités de tout utilisateur
- 700 serveurs localisés dans des dizaines de pays
- 20 To / jours
- Données : 3 à 5 jours
- Metadonnées : 30 jours
- Données intéressantes : 5 ans
- Informations 2008

Edward Snowden : Bullrun

- casser les systèmes de chiffrement
- Intervention sur les normes
- Intégration de portes dérobées
- Collaboration avec fournisseur de services
- Utilisation de superordinateur (force brute)
- Cyberattaques / espionnage (vol de clés)
- => le NIST : ~~Special Publication 800-90A~~
- => RSA : Security ~~B-SAFE~~

Loi de programmation militaire LPM

pour les années 2014 à 2019

- Promulguée le 19/12/2013
- Article 20 : Pour les finalités énumérées à l'article L. 241-2, les informations ou documents mentionnés à l'article L. 246-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs aux agents mentionnés à l'I de l'article L. 246-2.
- Entrée en vigueur le 01/01/2015

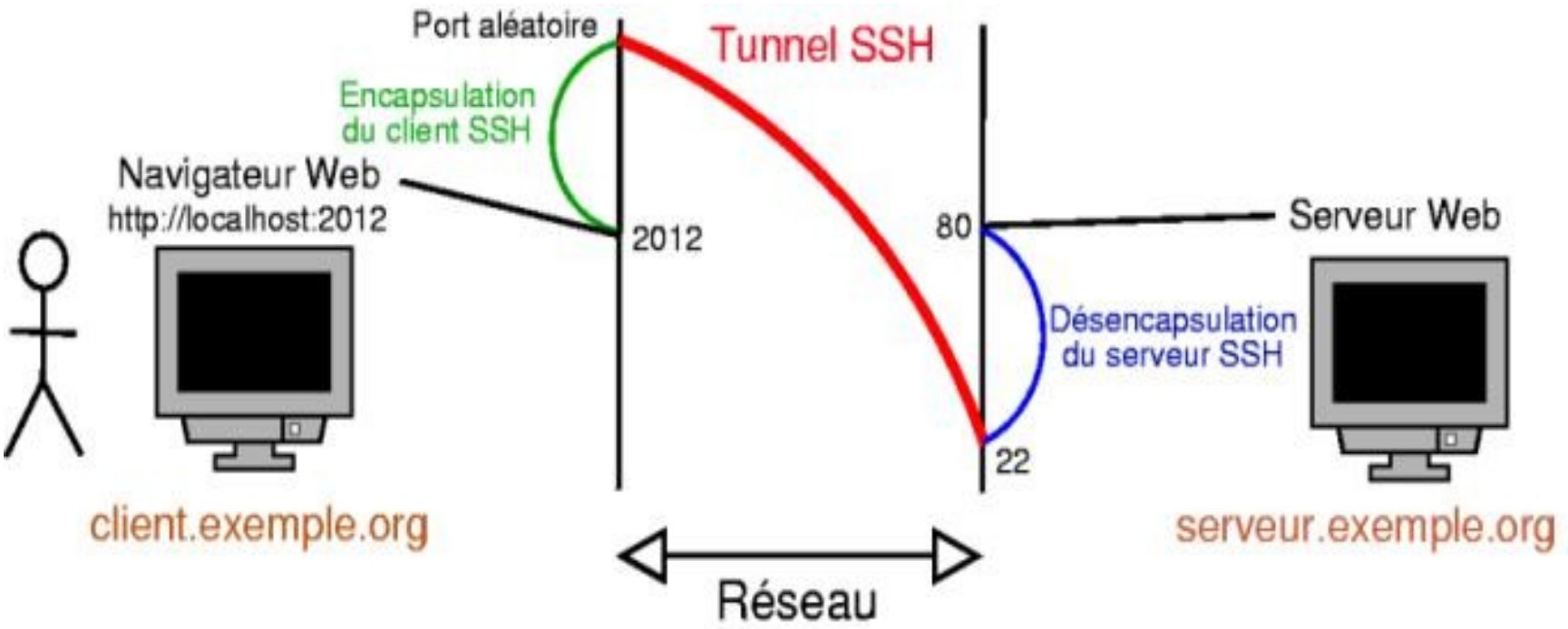
Chiffrer les données

- Sur le réseau
  - Protocoles SSH, SSL, IPsec
- Sur les systèmes de fichiers
- Qui contrôle les clés de chiffrement ?

Secure Shell : SSH

- Protocole de communication
- Programme qui utilise le protocole
- Cryptographie asymétrique puis symétrique
- Utilisations
  - Shell
  - Copie (scp), synchronisation (rsync) de fichiers
  - Tunnels
  - Monter un répertoire distant

Secure Shell : SSH



http://formation-debian.via.ecp.fr/ssh.html

Secure Socket Layer SSL

- HTTPS, SMTPS, LDAPS, POP3S, IMAPS, VPN OpenVPN
- Authentification avec certificat numérique {clé publique, noms, localisation, …, signature}
- Confidentialité
  → il faut chiffrer les données
- Intégrité
  → utilisation de fonction de hachage

Secure Socket Layer SSL

Protocole simplifié

1) Le client fait une demande de transaction sécurisée au serveur.
2) Le serveur envoie son certificat.
3) Le client vérifie que le certificat délivré est valide. Si la vérification est correcte alors le client envoie au serveur une clé symétrique chiffrée à l'aide de la clé publique du serveur qui sera donc le seul à pouvoir déchiffrer.
4) Cette clé sera utilisée pour échanger les données en toute sécurité.

IPsec

Internet Protocol Security

Niveau 3 du modèle OSI (couche réseau)

Utilisation de certificat

Traversée des NAT avec encapsulation

Inter-opérabilité

Formats standards ouverts et normalisés

Qui d'entre vous est sûr d'utiliser le même Cloud dans dix ans ?

- **vCard** : données personnelles : Visit Card
- **HTML :** Hypertext Markup Language
- **ODF :** Open Document Format (norme ISO)
- **CSV :** Comma-separated values
- **JSON :** JavaScript Object Notation
- **XML ?**

http://formats-ouverts.org/

Licence Affero-GPL

à destination des services types SaaS

- Dérivée de la licence GPL
- Plus l'obligation de délivrance des codes sources lors de l'usage du logiciel sur le réseau
  - Garantit la reproductibilité et l'évolutivité d'un logiciel hébergé
  - La licence porte uniquement sur le logiciel et non sur les données transmises par son biais

Initiatives de standardisation

- Distributed Management Task Force
  - Open Virtualisation Format OVF (Appliances virtuelles)
  - SNIA : Stockage
- Compatible One
  - Cloud management / Iaas / Paas
  - Utilise Open Cloud Computing Interface OCCI RESTful Protocol and API

Initiatives de standardisation

Storage Networking Industry Association (SNIA)

Cloud Data Management Interface (CDMI)

D'abord RFC, puis validé par l'ISO (2012)

Opérations en HTTP REST et JSON

- ACL
- Export vers NFS, CIFS, iSCSI
- …
- Voir http://cdmi.sniacloud.com/

Pas d'accord sur le format de disque

- Vmware : vmdk
- Microsoft et Citrix : vhd, vhdx
- Amazon : ami
- Xen : qcow, qcow2, vhd, raw
- QEMU : qcow, qcow2, raw, vmdk, vdi, cloop
- VirtualBox : vdi, vmdk, vhd, hdd, vdi
- Parallels : hdd

conversions de formats possibles via OVF

Sécurité logique

Sécurité logique

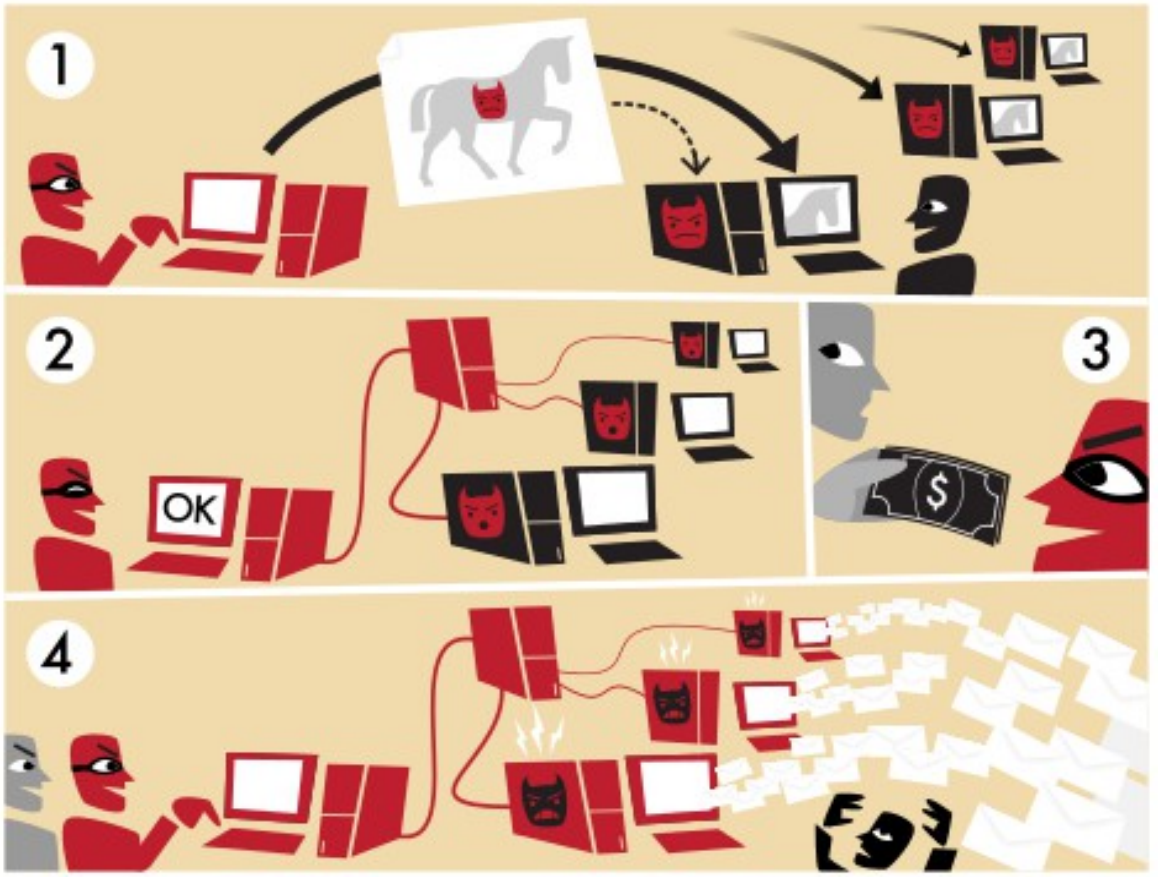
- Backups (système & données)
- Mot de passe sur screensaver,
- Anti-Virus,
- Firewalling, WAF, système anti DDOS,
- VLAN
- Détection d'intrusion IDS
- Tests d’intrusions
- Challenge

Botnet

1 et 2) prise de contrôle : virus, faille de sécurité, cheval de troie

3) achat

4) Attaque : spam, attaques par force brute, DDoS



Attaques DDoS

- Distributed Denial of Service : saturer
  - le serveur : envoyer de multiples requêtes
  - le routeur : envoyer pleins de petits paquets
  - le tuyau : envoyer pleins de gros paquets
- Requêtes lancées par des PC zombies (réseaux nommés Botnets)
- Achat (nbre machines, durée, requête à lancer)

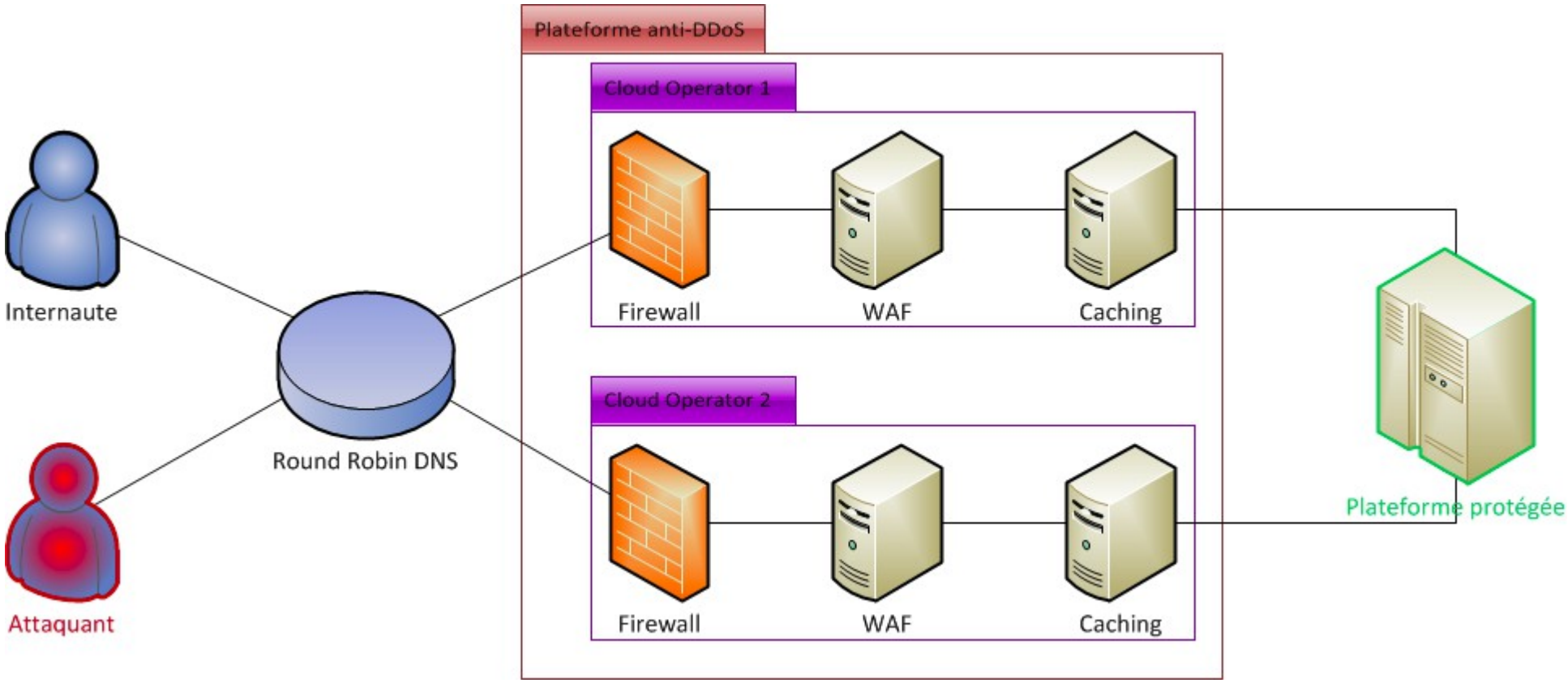
Attaques DDoS

Publications Arbor Networks (3 trimestres 2013)

- Prédominance des attaques applicatives 82 %
- 37 % des attaques sont entre 2 et 10 Gbps
- Moyenne 2,64 Gbps en hausse de 78 % /2012
- Attaques >20Gbps multipliées par 3,5 /2012
- 87 % des attaques durent moins d'une heure
- Attaque la plus élevée : 309 Gbps

Plateforme anti-ddos modulaire

DROP, fail2ban, LimitReq, TARPIT



http://francois.aichelbaum.com/creation-dune-plateforme-anti-ddos-modulaire/

Conformité

Conformité

- ISO 27 000
- SAS 70 : conformité Sarbanes-Oxley
- Données de santé : hébergeur agréé
- Archives

PCI DSS

Payment Card Industry Data Security Standard

- Organisation américaine maintient une liste de société agréées pour effectuer les contrôles
- Conformité testée tous les ans (tests techniques)
- Questionnaire d'auto évaluation
- Les logs sont fournies au gestionnaire de sécurité

Des questions