WAVESTONE

Bilan de la sécurité des sites web en France

Analyse de 155 sites de grandes entreprises

Octobre 2017

Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders dans leur secteur

2,600 collaborateurs sur 4 continents

Parmi les leaders du conseil indépendant en Europe, n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï*
Bruxelles | Luxembourg | Genève | Casablanca
Lyon | Marseille | Nantes

* Partenariats

© WAVESTONE

WAVESTONE

WAVESTONE ET LES AUDITS EN CYBERSECURITE

Wavestone : un retour d'expérience unique sur les audits en cybersécurité

350 audits de sécurité par an

Périmètres d'interventions variés : sites web, tests d'intrusion physiques, ingénierie sociale, revue de configuration, de code, SI industriel, etc.

Plus de 100 clients différents

Essentiellement des très grandes entreprises françaises, présentes sur le marché national ou international

Tous les secteurs d'activité couverts

Banque/Assurance, Distribution, Médical, Énergie, Service, Télécom, Transport, Défense et Institutions Publiques, etc.

Benchmark 2017 des failles des sites web

155 sites web testés

155 tests d'intrusion de sites web réalisés entre juin 2016 et juin 2017 composés de 117 sites sur Internet et 38 sites sur des réseaux privés d'entreprise

70 organisations concernées

Tous les secteurs d'activités sont représentés : banque, santé, défense, énergie administration, services, vente en ligne, télécom, transport, etc.

47 failles testées à chaque fois

Des tests respectant la même méthodologie, pour des résultats comparables.

Des failles incluant le contrôle d'accès, la qualité du chiffrement, la diffusion d'informations techniques superflues, le traitement des communications, etc.

Une confidentialité qui reste préservée : les données clients sont anonymisées, l'analyse étant uniquement statistique.

LES RESULTATS

4 constats marquants sur la sécurité des sites web

1 **100%**
des sites web testés sont vulnérables, et ceci quel que soit le contexte ou le secteur.

2 **50 %**
des sites accessibles à tous depuis Internet ont au moins une faille grave.

3 **40 %**
des sites ayant déjà subi un audit de sécurité sont encore vulnérables.

4 **90%**
Des sites testés étaient déjà en ligne au moment des audits de sécurité.

Et tous les secteurs d'activités sont concernés…

Aucun site parfait !

Le chiffre

100% Comme en 2016, nos tests sur 155 sites web en 2017 ont révélé la présence d'**au moins une** faille de sécurité

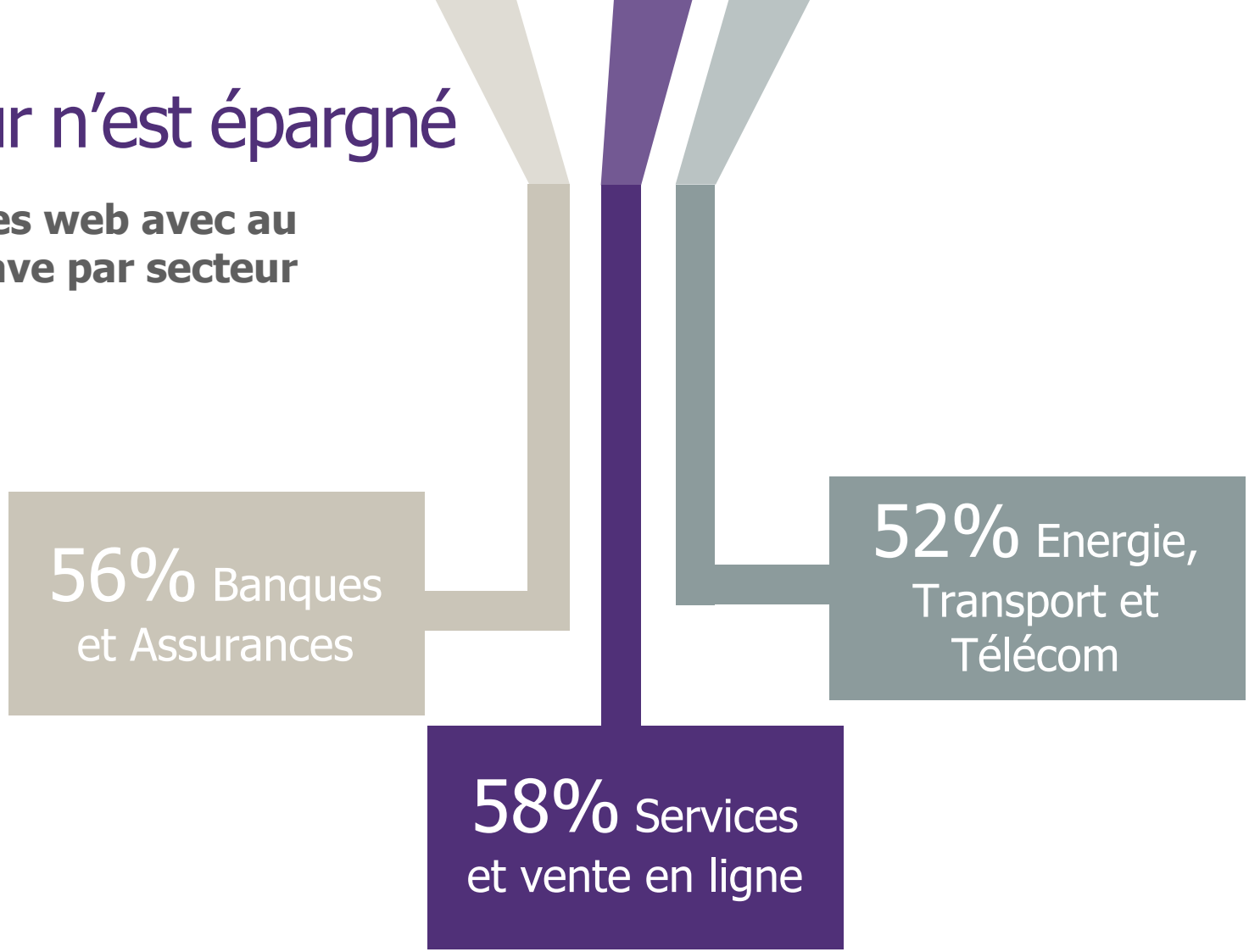
Une sécurité négligée dans la durée

Plus de **40%** des sites testés restent vulnérables avec au moins 1 faille grave, et cela malgré la réalisation d'audit par le passé.

Des corrections peu appliquées et des nouvelles fonctionnalités développées sans prendre en compte les bonnes pratiques de sécurité.

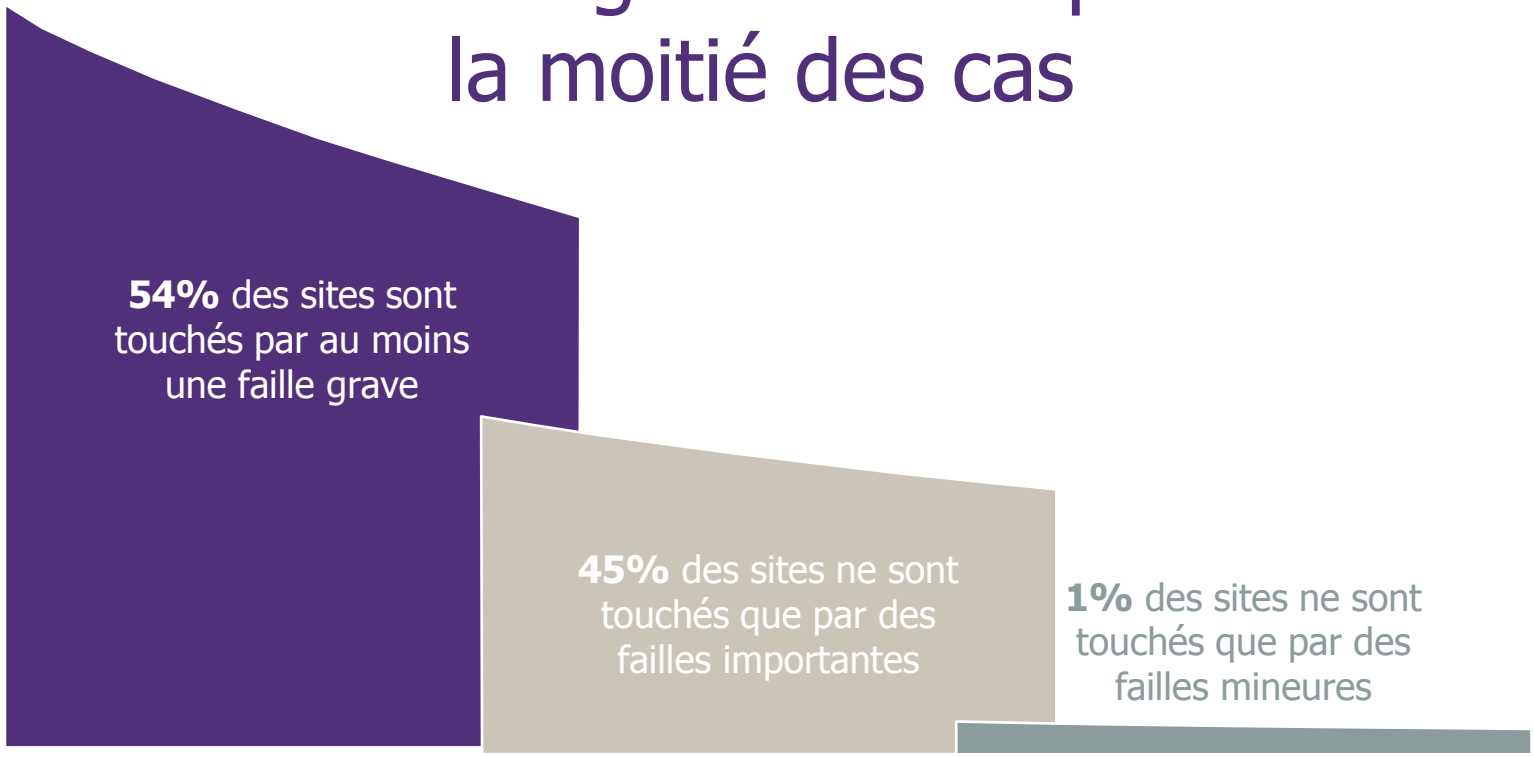
Aucun secteur n'est épargné

Pourcentage de sites web avec au moins une faille grave par secteur



Sélection des secteurs avec un échantillon représentatif d'au moins 30 sites.
53% de faille grave constatées pour la somme des autres secteurs : défense, santé, immobilier…

Des failles graves dans plus de la moitié des cas



Vs 60% en 2016

Faille grave
Permet d'accéder à l'ensemble du contenu du site et/ou de compromettre les serveurs

Accès à l'ensemble des données du site, exécution de code par le serveur, utilisateur A ayant accès aux données de B, etc.

***Vs 39%** en 2016*

Faille importante
Permet d'accéder aux informations d'autres utilisateurs mais en nombre limité ou de manière complexe

Vol de session d'un utilisateur, faiblesses dans le chiffrement, possibilité de faire réaliser des actions à l'insu de l'utilisateur, etc.

***Vs 1%** en 2016*

Faille mineure
Permet principalement d'obtenir des informations pour continuer l'attaque

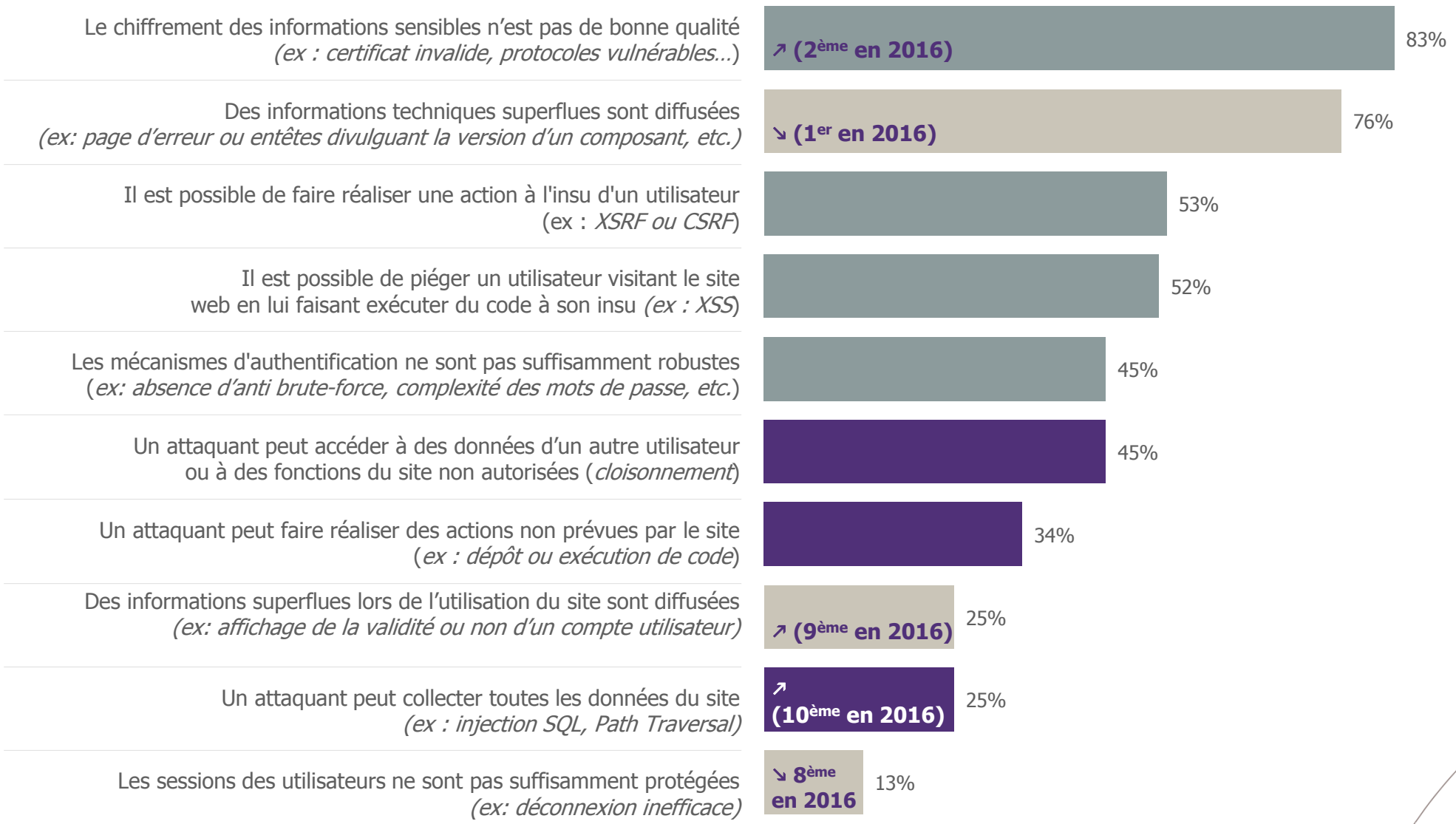
Messages techniques superflus, absence de sécurisation des cookies, déconnexion utilisateur non efficace, etc.

Des failles graves sur Internet, comme en interne

50% des sites accessibles à tous depuis Internet ont au moins une faille grave

68% des sites web internes réservés aux collaborateurs ont au moins une faille grave

Un top 10 des failles qui évolue peu



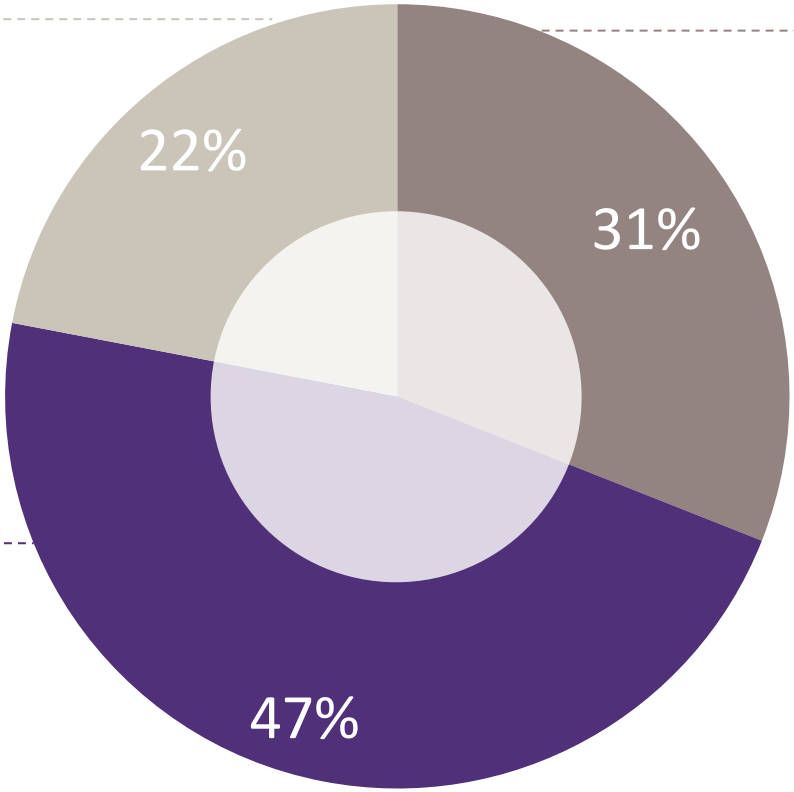
ET APRES ?

Des corrections qui nécessitent des efforts importants

Exemple concret avec le nombre de failles XSS (exécution de code dans le navigateur d'un visiteur) découverts par site

Un oubli

Un seul paramètre est vulnérable, la correction sera simple.



Tout est à revoir

La majorité des paramètres (plusieurs dizaines ou centaines) sont touchés, des actions lourdes sont à prévoir sur l'ensemble du site.

Quelques manquements

Une minorité de paramètres (5 à 10) est vulnérable, seules quelques pages devront être modifiées.

Un changement de posture nécessaire

Une dangereuse course aux nouvelles fonctionnalités

Le constat est sans appel : une faille grave découverte sur plus de 50% de sites web déjà en production…

La gestion actuelle des projets ne laisse pas beaucoup de place à la sécurité : pression des métiers, mise en production urgente, projet dont on apprend l'existence à sa sortie, etc.

Le rythme ne cesse de s'accélérer avec l'essor des méthodes agiles, DevOps…

Apprendre de ses erreurs et profiter des innovations

Il est désespérant de voir que la situation ne s'améliore pas dans le temps. L'intégration de la sécurité dès le début du projet est pourtant l'une des clés à maîtriser pour améliorer ce chiffre.

Les évolutions technologiques récentes offrent l'opportunité d'appliquer ce qui n'a jamais été possible : intégrer la sécurité en continu dans le processus de développement en rapprochant les contrôles des développeurs.

Le besoin d'investir dans les compétences

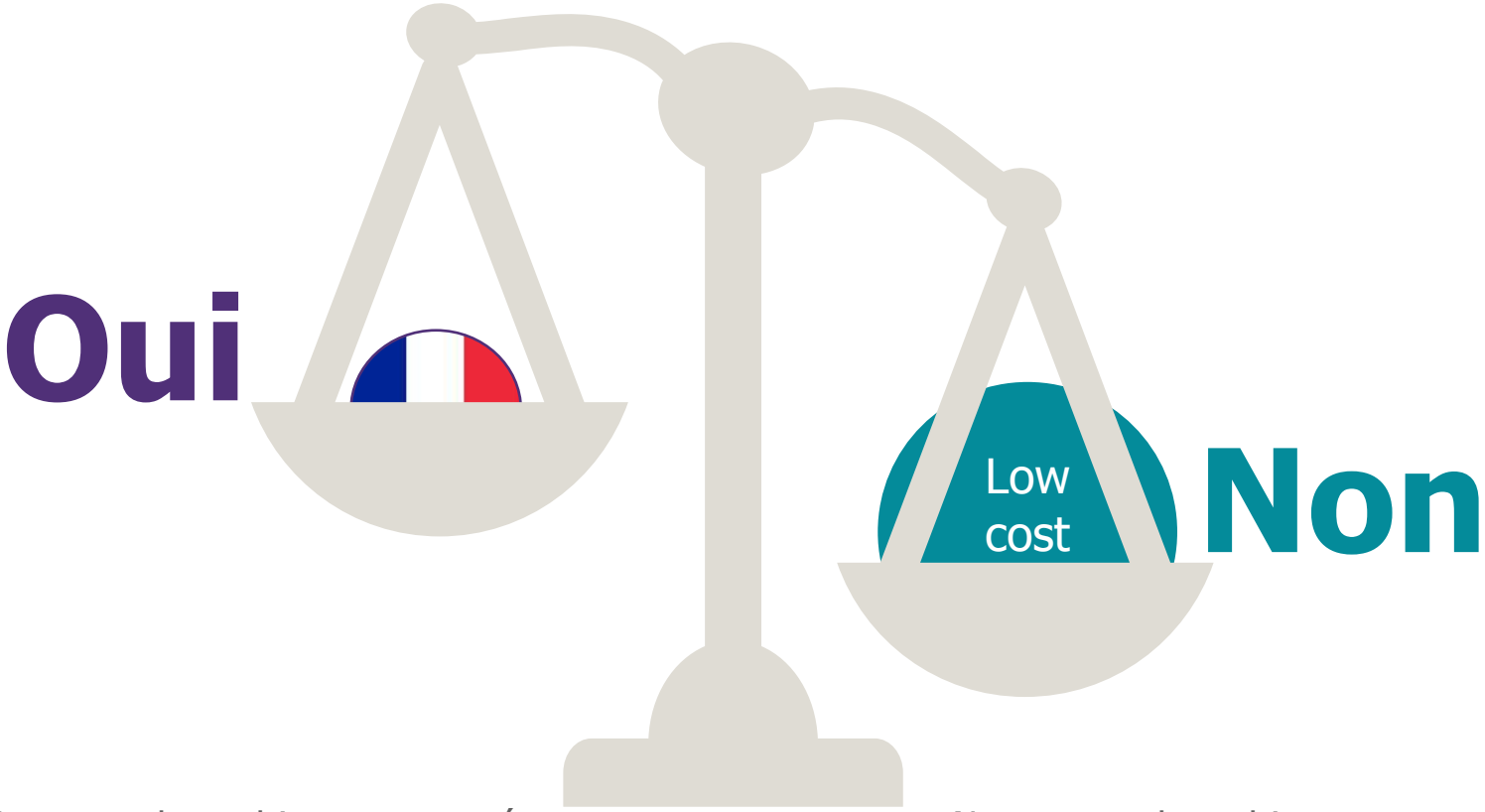
La réponse ne viendra pas uniquement d'investissements sur des nouveaux composants de sécurité, de contrôles a posteriori, etc.

Il est plus que jamais nécessaire d'investir dans les compétences des équipes, en particulier des développeurs, pour que la sécurité soit bien plus qu'une étape dans des processus peu suivis, mais bien une réalité de chaque instant.

WAVESTONE

FOCUS 2017
LES OBJETS CONNECTÉS
ET L’ IOT

Des objets connectés meilleurs que les sites web ?



Oui, pour les objets connectés développés en France. Wavestone a réalisé 10 tests d'intrusion sur de tels objets connectés sans trouver de faille permettant une attaque massive (même si des attaques locales sont souvent trouvées)

Non, pour les objets connectés « low cost » qui contiennent de nombreuses failles comme l'ont montré les très nombreux incidents observés en 2016 et 2017

ANNEXES

Ne réinventons pas la roue !

50% des sites en PHP sans gestionnaire de contenu (CMS) reconnu sont touchés par au moins une faille grave.

Seulement **30%** le sont s'ils utilisent des CMS reconnus, car ils apportent des fonctions de sécurité

Sélection des tests réalisés sur 55 sites utilisant la technologie PHP

Un contrôle d'accès pas toujours contrôlé…

45% des tests réalisés en mode **boite grise** (utilisation d'un compte utilisateur standard) ont permis de contourner le cloisonnement applicatif pour accéder à des données ou des fonctions (escalade horizontale ou verticale) non autorisées

*Vs **44%** en 2016*

Dépôt de fichier ?
Attention danger !

Dans **56%** des cas où une fonctionnalité de type « dépôt de pièce jointe » était offerte, une faille a permis de déposer du code sur le serveur.

Dans **34%** des cas, cela a permis d'exécuter du code sur le serveur.

C'est une voie royale pour rebondir depuis ce serveur vers d'autres composants du SI.

***37%** sur le dépôt en 2016*

Surfer sur plusieurs sites en parallèle nuit gravement à la sécurité

1/2 des sites sont vulnérables à du CSRF* (ou XSRF*) :

- Pendant l'utilisation d'un site web sensible, vous décidez d'ouvrir un nouvel onglet pour surfer.
- Le site web de ce nouvel onglet, s'il contient une attaque, est capable de réaliser des actions à votre insu sur le site web sensible : *modifier votre adresse de contact pour réinitialiser le mot de passe par exemple…*

*Vs **67%** en 2016, évolution due majoritairement à une évolution de l'échantillon (technologie ASP).*

53 %
des sites
vulnérables
à du XSRF*

**CSRF ou XSRF : Cross Site Request Forgery*

WAVESTONE

Yann FILLIAT
Manager – Responsable offre audit de sécurité

M +33 (0)6 24 76 08 67
yann.filliat@wavestone.com

Gérôme BILLOIS
Partner

M +33 (0)6 10 99 00 60
gerome.billois@wavestone.com

riskinsight-wavestone.com
@Risk_Insight

securityinsider-wavestone.com
@SecuInsider

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats