



SOLUTION

DE CYBER-SÉCURITÉ

ET DE GOUVERNANCE

DES ACCÈS AU SYSTÈME

D'INFORMATION



**WALLIX**  
TRACE, AUDIT & TRUST

Paris, le 01/09/2016

## WAB SUITE EN PREMIERE LIGNE POUR PROTEGER LES OPERATEURS D'IMPORTANCE VITALE (OIV)

**WALLIX GROUP, éditeur de solutions de cyber-sécurité et de gouvernance des accès au système d'information, salue l'entrée en application de la réglementation relative à la protection des Opérateurs d'Importance Vitale (OIV) contre les cyber-attaques. Ces nouvelles dispositions législatives ouvrent à WALLIX GROUP de nouveaux marchés de grande envergure.**

### Opérateurs d'Importance Vitale, environ 250 grandes entreprises en France à protéger

Les Opérateurs d'Importance Vitale sont définis comme des opérateurs publics ou privés qui participent à des systèmes d'information pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation<sup>1</sup>. Sont aujourd'hui concernées environ 250 grandes entreprises publiques, administrations et grands opérateurs privés en France.

### 9 arrêtés déjà publiés pour les secteurs prioritaires

L'Agence Nationale pour la Sécurité des Systèmes d'Information (ANSSI) a publié au Journal Officiel 9 arrêtés sectoriels fixant les règles relatives à la sécurité des systèmes d'information des OIV. Les activités concernées sont :

- [Les produits de santé](#)
- [La gestion de l'eau](#)
- [L'alimentation](#)
- [L'approvisionnement en gaz naturel](#)
- [L'approvisionnement en hydrocarbures pétroliers](#)
- [L'approvisionnement en énergie électrique](#)
- [Les transports maritimes et fluvial](#)
- [Les transports terrestres](#)
- [Le transport aérien](#)

<sup>1</sup> Article L1332-1 du Code de la défense



Dès l'entrée en vigueur de ces arrêtés sectoriels, au plus tard le 1<sup>er</sup> octobre 2016, les OIV seront dans l'obligation de se prémunir contre d'éventuelles intrusions de leurs systèmes informatiques. En conséquence, ces entités doivent :

- Déclarer à l'ANSSI leurs incidents de sécurité ;
- Déclarer leur liste de Systèmes d'Information d'Importance Vitale (SIIV) à l'ANSSI ;
- Communiquer les coordonnées de leur service de permanence Systèmes de Sécurité Incendie (SSI) à l'ANSSI ;
- Être conformes aux 20 règles de sécurité concernant : la gouvernance, la maîtrise des risques et des SI, la protection des systèmes et la gestion de crise en cas d'attaques informatiques majeures.

Dans les faits, les OIV devront notamment installer en leur sein des logiciels ou matériels qualifiés et recommandés par l'ANSSI, qui détectent en permanence les intrusions informatiques venues de l'extérieur. Construire un système de défense adapté permet d'anticiper et de protéger les informations les plus délicates de ces structures sensibles et éviter une cyber-attaque destructrice. Par ailleurs, les contrevenants s'exposent à une amende pouvant aller jusqu'à 150 000 euros et à un an de prison en cas de « défaillance » ayant mis en péril une infrastructure sensible.

### WAB Suite, une solution tout-en-un et certifiée

S'agissant d'un enjeu identifié dès 2013, WALLIX a fait certifier CSPN son offre WALLIX AdminBastion (WAB) Suite auprès de l'ANSSI. En effet, la WAB Suite est une solution de gestion des comptes à privilèges tout-en-un permettant de sécuriser et superviser les accès et sessions des super-utilisateurs. Dotée d'un coffre-fort à mots de passe, fournissant des éléments d'authentification complexes, secrets et modifiables, elle trace toute action prise sur un compte privilégié grâce à des fonctionnalités d'enregistrement et de surveillance en temps réel.

Cette traçabilité, allée à des fortes capacités d'audit, optimise la réactivité des responsables sécurité en cas d'incident et s'inscrit dans les règles de conformité décrites par l'ANSSI. Il ne s'agit pas de réagir face à l'attaque, mais bien de l'anticiper en construisant un système de défense adapté pour protéger les informations les plus délicates de ces OIV et éviter une cyber-attaque destructrice.

L'environnement, l'usage de la WAB Suite ainsi que les données sensibles à protéger ont été soumis à des scénarii de menaces et d'attaques afin de fournir aux clients et partenaires une solution de confiance indispensable dans des organisations critiques et vitales.

A ce jour, de nombreuses entreprises ont adopté WAB pour protéger leurs mots de passe et les comptes à privilèges ayant accès à leurs infrastructures et leurs données sensibles, ou encore contrôler l'activité de leurs prestataires internes et externes, en particulier dans des secteurs aussi stratégiques que la défense, les télécoms, les transports, la gestion de l'eau, l'énergie, la santé ou les services financiers.

### La cybersécurité en Europe, une Directive applicable dès 2018

La France fait figure de pionner au sein de l'Union Européenne en étant l'un des premiers Etats à transposer la directive NIS (Network and Information Security) adoptée par le Parlement européen et le Conseil de l'Union européenne. Chaque Etat membre devra faire appliquer cette réglementation au plus tard en mai 2018.

Parallèlement, le Conseil européen a adopté le projet de Règlement général sur la protection des données ouvrant ainsi la voie à l'adoption finale de ce dispositif législatif par le Parlement européen. Les objectifs sont :

- de renforcer le niveau de protection des données des personnes physiques, dont les données à caractère personnel sont traitées ; et



- d'accroître les débouchés commerciaux dans le marché unique numérique.

Cette réforme prévoit une série de mesures valables dans toute l'UE et applicables aux entreprises européennes et non européennes proposant des services en ligne. En cas de non-respect de ce Règlement, les responsables d'un traitement s'exposeraient à des amendes d'un montant maximal de 20 M€ ou à 4 % de leur chiffre d'affaires annuel mondial.

**Prochaine publication** : résultats du 1<sup>er</sup> semestre 2016 le 27 octobre 2016 (après Bourse).

## À PROPOS DE WALLIX

WALLIX, [www.wallix.com](http://www.wallix.com), propose des solutions logicielles de gestion des accès à privilèges pour les grandes et moyennes entreprises, organisations publiques et opérateurs de services cloud. Ces solutions aident leurs utilisateurs à protéger les actifs informatiques critiques parmi lesquels leurs données, serveurs, terminaux et objets connectés.

Wallix AdminBastion Suite (ou WAB Suite) offre l'accès le plus direct vers la sécurité et la conformité en réduisant le risque le plus important – les accès à privilèges – dans le temps le plus court. Conçue sur une architecture non-intrusive, multi-tenante, WAB Suite est la solution la plus simple à mettre en œuvre, utiliser et gérer sur son marché. Saluée par SC Magazine et décrite comme une « approche unique dédiée aux problématiques de contrôle d'accès des utilisateurs à privilèges », la solution a également reçu 5 étoiles et été nommée « Best Buy » par le magazine expert en cyber-sécurité. Sa couverture fonctionnelle « best of breed » intègre la gestion des mots de passe, le portail d'accès web, la gestion des accès, la surveillance et l'enregistrement exhaustif de la session. WAB Suite peut être déployée sous forme logicielle, physique ou comme un service sur site ou en environnement cloud hybride.

WALLIX est une société cotée sur Alternext et affiche une forte présence sur la zone EMEA. WALLIX est basée à Paris, à Londres et à Munich. Plus de 300 entreprises font confiance à WALLIX pour sécuriser leurs systèmes d'information parmi lesquelles Alain Afflelou, Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, Michelin, PSA Peugeot-Citroën, Quick. WALLIX est qualifiée « entreprise innovante » par Bpifrance.

Plus d'informations sur [www.wallix.com](http://www.wallix.com)

### **ACTUS finance & communication**

Jérôme FABREGUETTES-LEIB - Relations Investisseurs  
Tél. 01 53 67 36 78 / [wallix@actus.fr](mailto:wallix@actus.fr)

### **ACTUS finance & communication**

Nicolas BOUCHEZ - Relations Presse Finance  
Tél. 01 53 67 36 74 / [nbouchez@actus.fr](mailto:nbouchez@actus.fr)

### **Agence MyNtic-PR**

Franck TUPINIER - Relations Presse Métier  
Tél. 06 74 68 37 93 / [ftupinier@myntic-pr.com](mailto:ftupinier@myntic-pr.com)