Documents Légaux
POLITIQUE DE SÉCURITÉ DU SYSTÈME D'INFORMATION (PSSI) LWS

Version en date du 15 mai 2024

La Politique de Sécurité du Système d'Information (PSSI) fournit le cadre de référence en matière de cybersécurité pour LWS. La PSSI définit les notions nécessaires pour comprendre l'approche de LWS en termes de sécurité et établit le lien entre le contexte des opérations et les moyens mis en œuvre pour assurer la sécurité. Elle précise :

- Le contexte des opérations de LWS permettant de comprendre les principaux risques de sécurité de LWS.
- Les engagements en matière de sécurité vis-à-vis des parties intéressées de LWS et les principes de mise en œuvre et de maintien en condition de sécurité des systèmes d'information.
- La déclinaison de ces principes au sein de LWS.

LWS opère au sein d'un écosystème dynamique dans un contexte qui évolue continuellement. Les pratiques visant à assurer la sécurité doivent donc évoluer rapidement pour rester pertinentes. La PSSI est la marque d'un engagement dans la durée de la direction générale. La PSSI se décline dans un ensemble de politiques de sécurité et de guides d'implémentation détaillés. Ces documents ont leurs cycles de vie propres, adaptés à leurs contenus. Elle vise à définir les critères permettant l'évaluation des risques, les principes guidant l'établissement des mesures de sécurité à mettre en place et la gestion de la sécurité au sein de LWS.

La PSSI s'applique à LWS, aux salariés, fournisseurs, prestataires, sous-traitants et utilisateurs du système d'information, quelles que soient leurs activités.

1. Contexte de mise en oeuvre de la PSSI 1
2. Nos engagements sécurité 3

1. Contexte de mise en oeuvre de la PSSI

1.1. Qu'est ce que la sécurité de l'information ?

La sécurité consiste à protéger la disponibilité, l'intégrité et la confidentialité d'un système. Au sein de LWS, gérer la sécurité consiste à définir, mettre en œuvre, opérer et améliorer tous les moyens humains, organisationnels, techniques et légaux permettant de protéger les services et systèmes d'information de LWS sur ces critères. Protéger la confidentialité des données en toutes circonstances est au cœur de la démarche sécurité de LWS. Assurer la disponibilité et l'intégrité des services et des données est la première mission de LWS et dépasse le cadre de la PSSI. Sur ces deux critères, la démarche sécurité se concentre sur les risques d'origine malveillante.

En accord avec les engagements sécurité de LWS, les critères de traçabilité et de respect de la vie privée sont également pris en compte de manière formelle dans notre démarche sécurité.

Les critères de sécurité couverts par la PSSI sont donc la disponibilité, l'intégrité, la confidentialité, la traçabilité et le respect de la vie privée. Ces critères sont utilisés pour valoriser les besoins en sécurité des actifs protégés, et les impacts associés à un risque ou un incident de sécurité.

1.2. Quels actifs protégeons nous ?

Les infrastructures, les plateformes, les applications
Cette infrastructure consiste en un ensemble de datacentres, d'équipements et de serveurs qui y sont hébergés en France, ainsi qu'un réseau mondial d'interconnexion. LWS opère également un système d'information supportant cette infrastructure. Ce système d'information supporte les opérations, porte l'automatisation et assure le travail collaboratif au sein de LWS. Il porte également les outils mis à disposition des clients pour l'administration de leurs services et la communication avec les équipes de LWS.

LWS propose des services d'infrastructure (IaaS), de plateforme (PaaS) et d'application (SaaS). Chacun de ces services s'appuie sur les infrastructures, le système d'information de LWS et éventuellement d'autres services fournis par LWS ou des partenaires.

Les informations
Les données considérées comme les plus sensibles par LWS sont les données appartenant aux clients. Concernant ces données hébergées dans le cadre des services, le client est responsable de traitement et LWS est sous-traitant. De manière générale, les salariés de LWS ne connaissent pas le type de données hébergées et n'y accèdent pas. Le client, en tant que responsable de traitement, doit s'assurer de l'adéquation entre le niveau de service proposé et la sensibilité des données. LWS, en tant que sous-traitant, agit sur instructions du client dans le cadre contractuel des services.

LWS protège également les données internes en support des opérations. Dans ce cadre, LWS est le responsable de traitement. Ces données couvrent les données techniques et administratives nécessaires à la fourniture du service, à la relation commerciale et au respect des obligations légales. Les données internes de LWS utilisées pour la gestion et le développement de l'entreprise sont également couvertes. Ces données peuvent concerner directement ou indirectement les clients, les salariés, les prestataires et les partenaires de LWS. Elles peuvent éventuellement être transmises à des tiers dans le respect des réglementations en vigueur. En tant que responsable de traitement, LWS définit les mesures de sécurité adaptées à chaque type de données pour chaque étape de leur cycle de vie, en adéquation avec leur sensibilité.

1.3. A quelles menaces sommes-nous confrontés ?

En tant qu'entreprise, LWS est concernée par les attaques auxquelles toute entreprise est soumise : vol de données, vol de ressources, chantage, fraude, extorsion, logiciels malveillants, compromission des systèmes exposés, etc. Ces attaques, ciblées ou non, peuvent mettre en péril les données gérées par LWS et impacter les opérations.

En tant qu'acteur majeur de l'hébergement web, LWS opère des infrastructures à l'échelle d'Internet. Ce positionnement expose LWS à des menaces spécifiques dont les motivations peuvent être d'atteindre la réputation d'un acteur à forte visibilité dans un contexte concurrentiel dynamique, de challenger des technologies innovantes ou leur mise en œuvre spécifique par LWS par intérêt technique ou d'atteindre des infrastructures larges et fortement connectés pour tenter d'utiliser à des fins malveillantes les ressources de puissance de calcul et de connectivité.

Enfin, en tant que fournisseurs d'infrastructures, de plateformes et de solutions, nous devons également anticiper les menaces ciblant nos clients ou des tiers :

- Les attaques visant les données et traitements de nos clients via nos infrastructures,
- Les attaques exploitant une faiblesse dans l'isolation logique ou physique entre les environnements des différents clients liés à la mutualisation de ressources,
- L'utilisation des ressources mises à disposition par LWS en tant que vecteur d'attaque sur des tiers.

Les motivations et les chemins d'attaques pour cibler les infrastructures de nos clients sont aussi variés que les typologies des systèmes qu'ils opèrent. Elles ne peuvent être listées exhaustivement. Nous devons donc être préparés à toute éventualité d'attaque ciblant un de nos clients ou LWS.

Les menaces ciblant LWS sont principalement d'origine externe. Outre la possibilité d'erreurs humaines dans les opérations, nous devons inclure le risque de malveillances internes dans notre démarche de gestion des risques.

1.4. Qui est concerné par la sécurité ?

Les clients et les partenaires
Les clients et partenaires de LWS nous confient la responsabilité d'opérer au sein des datacentres, des infrastructures, des plateformes et des logiciels. Du bon fonctionnement de ces services dépendent leurs systèmes d'information et de leurs activités numériques. Les clients de LWS opèrent eux-mêmes des services qu'ils proposent à des tiers au sein d'un écosystème riche et complexe. Les acteurs impliqués dans cette chaîne d'approvisionnement et les utilisateurs finaux attendent de LWS l'expertise et la maîtrise opérationnelle des services fournis. Notre engagement à assurer la sécurité des données et des traitements hébergés doit être entier et permanent.

Les autorités et les régulateurs sectoriels
Les autorités définissent le cadre assurant la protection des citoyens et des entreprises sous leurs juridictions. Cette protection s'étend aux données et traitements des citoyens et des entreprises. LWS prend en compte ces

exigences dans toutes les géographies où le service est opéré pour assurer un service adapté aux écosystèmes locaux. Les régulateurs sectoriels formulent également des exigences pour l'hébergement de certains types de données et de traitements, associés à des risques particuliers. LWS peut proposer des services spécifiquement adaptés à ces exigences. Dans ce cas, LWS s'engage sur la couverture des exigences sectorielles et des risques spécifiques au secteur.

Les employés, la direction de LWS
Les salariés de LWS conçoivent, maintiennent et opèrent les systèmes et processus en support des services de LWS. Tout incident de sécurité a un impact négatif direct sur les opérations. Il peut également remettre en question la valeur du service, l'expertise et le professionnalisme des équipes. Opérer des systèmes d'information sécurisés permet de mettre en valeur les innovations, la passion, l'engagement des équipes et la qualité des services de LWS.

LWS, en tant que fournisseur d'hébergement web dans un environnement très compétitif, doit assurer une croissance forte pour soutenir l'innovation et le développement à l'international renforçant sa crédibilité. La confiance de nos clients, principal vecteur de cette croissance, est directement liée à la capacité de LWS à protéger leurs données et charges de traitements. La cybersécurité est donc un des piliers en support de la stratégie de développement portée par la direction de LWS.

2. Nos engagements sécurité

2.1. Déployer une approche industrielle à grande échelle de la sécurité

Les équipes de LWS s'engagent à innover de manière permanente pour répondre aux besoins en constante évolution des clients en termes de technologie, de fonctionnalités et de performances. La sécurité est intégrée dans le cycle de vie du développement des produits. L'équipe de sécurité est constamment impliquée pour challenger et aider toutes les décisions susceptibles d'avoir un impact sur la sécurité.

La sécurité de LWS repose sur la responsabilité de chaque employé en matière de sécurité des données. Nos développeurs et administrateurs sont choisis pour leur expertise technologique. L'équipe sécurité assure la cohérence des outils, des processus et des connaissances de sécurité avec la politique de sécurité de LWS.

Nous mettons en œuvre et opérons des mesures de sécurité adaptées pour prévenir et réduire les risques de sécurité. Nous voulons que cette approche soit directe et transparente afin de renforcer la confiance de nos clients et partenaires. Nous concevons et exploitons un grand nombre de systèmes. Notre démarche s'appuie sur des mesures de sécurité normalisées, sur des architectures sécurisées dès leur conception et sur des processus formels, éprouvés, fortement automatisés. Ces mesures de sécurité sont issues de l'expérience de LWS, de nos engagements contractuels, des obligations légales et réglementaires et des bonnes pratiques métier reconnues. Elles nous permettent d'assurer la sécurité à l'échelle de LWS.

Une gestion formelle des risques de sécurité permet de prendre en compte les spécificités liées à chaque projet. Nous complétons ainsi nos mesures de sécurité normalisées avec des mesures spécifiques à ces projets. Les démarches de gestion des événements, des incidents, des vulnérabilités, des menaces et de remontées d'information de sécurité demeurent normalisées au sein d'une approche unifiée.

Enfin, LWS opère un dispositif d'analyse permanent des menaces lié à une surveillance permanente des systèmes. Ainsi, nous adaptons systématiquement les pratiques opérationnelles aux risques immédiats et réagissons efficacement aux incidents de sécurité. L'organisation des équipes sécurité permet de mobiliser au plus vite les experts pour investiguer et résoudre les incidents de sécurité. De cette manière, nous minimisons les impacts potentiels et mettons en place les actions correctives au plus vite de manière pérenne.

2.2. Positionner LWS comme un acteur de confiance au sein de l'écosystème

En tant que fournisseur mondial d'hébergement web, LWS a une grande responsabilité dans la lutte contre les menaces de sécurité. Nous déployons des outils de protection à grande échelle. Nous automatisons la protection des systèmes de nos clients contre ces menaces. Nous détectons les systèmes vulnérables. Nous partageons nos innovations et nos connaissances avec la communauté de la sécurité. Nous gérons plusieurs millions d'adresses IP publiques pour le compte de nos clients. Ces adresses sont des actifs essentiels des systèmes d'informations dans l'hébergement web et leurs réputations est l'une de nos préoccupations.

L'équipe sécurité et les experts techniques de LWS entretiennent des relations opérationnelles solides avec les communautés d'experts en sécurité, les autorités, les éditeurs de logiciels et les fabricants de matériel. De cette manière, nous anticipons les nouvelles menaces et les nouvelles vulnérabilités. Ainsi, nous réduisons les risques associés. Nous partageons nos innovations et nos connaissances avec la communauté de la sécurité et nous promouvons la divulgation responsable.

Nous challengeons continuellement notre sécurité. Nous mettons en œuvre un programme structuré de revues, de tests et de contrôles, tant internes qu'externes. Notre organisation de la gestion de la sécurité est basée sur des normes internationales reconnues, et en particulier l'ISO/IEC 27001 qui met en évidence ces principes. Nous évaluons nos dispositifs de sécurité régulièrement en nous appuyant sur des tiers de confiance et des référentiels d'audit reconnus.

2.3. Opérer un hébergement web de confiance pour tous

LWS propose ses solutions à tout type de client dans tous les domaines d'activités : startup, PME, grande entreprise, administration, multinationale. Chaque client de LWS a une approche de la sécurité particulière dépendante de son contexte métier ou de ses besoins de souveraineté que nous devons prendre en compte. La sécurité est un des piliers de la confiance de nos clients.

La sécurité d'un système dans l'hébergement web est une responsabilité partagée entre le fournisseur d'hébergement web et le client. LWS assure la sécurité des services fournis et des infrastructures sous-jacentes. Nos clients sont toutefois responsables de la sécurité de leurs systèmes d'information dans l'hébergement web. Nous leur offrons un haut niveau de transparence sur les mesures de sécurité implémentées par LWS pour les aider dans leur plan global de mitigation des risques sécurité. Nous définissons clairement leurs domaines de responsabilité afin d'éviter toute vulnérabilité découlant d'une prise de conscience insuffisante.

LWS fournit et développe un ensemble d'outils, de fonctionnalités et de configurations afin d'améliorer la sécurité des systèmes des clients dans l'hébergement web. La plupart des fonctions de sécurité sont incluses pour tous les clients. Des fonctions de sécurité supplémentaires sont également proposées pour aider nos clients à réduire les risques spécifiques auxquels ils sont confrontés.

LWS s'engage également sur la protection des données à caractère personnel, en tant que responsable de traitement pour les données relatives à nos clients et en tant que sous-traitant de données à caractère personnel dans le cas où nos clients sont eux-mêmes responsables de traitement. La politique de sécurité des systèmes d'information porte notamment cet engagement par la définition, la mise en œuvre et l'amélioration des dispositifs de sécurité assurant la protection des données à caractère personnel hébergées.

Les produits conçus chez LWS utilisent des technologies open source et/ou des standards technologiques éprouvés. L'adoption et la réversibilité du produit s'en trouvent facilitées. Ce choix stratégique garantit à nos clients le déploiement de systèmes standards dans l'hébergement web. Ils peuvent ajouter leurs propres solutions de sécurité, tirer parti des compétences et des outils usuels de leurs équipes. Une large offre de solutions et de services de sécurité est disponible avec les partenaires LWS ainsi que d'autres fournisseurs.

2.4. Comment LWS s'engage ?

L'engagement de LWS vis-à-vis des clients et partenaires est avant tout porté par la relation contractuelle qui le formalise et l'explicite.

LWS respecte les lois et réglementations applicables dans le cadre de la fourniture des services dans chaque pays. Aussi, LWS s'engage contractuellement à respecter certaines réglementations sectorielles spécifiques, par exemple pour les systèmes d'information de santé ou financiers.

Au-delà des liens contractuels, LWS s'engage auprès de son écosystème, ses clients et prospects en s'assurant de la clarté et de la transparence des messages en toutes circonstances.

2.5. Implémentation de la sécurité

- Gouvernance de la sécurité
- Modèle de sécurité
- Fonctionnalité sécurité pour les clients

- Protection des données
- Conformité en sécurité
- Gestion des risques de sécurité
- Ecosystème de la sécurité
- Sécurité pour les clients
- Réputation technique à l'externe
- Audit et contrôle
- Gestion des actifs
- Ressources humaines, sensibilisation et formation
- Identification, authentification et gestion des accès
- Utilisateur final du système d'information
- Chaîne d'approvisionnement et gestion des fournisseurs de service
- Gestion de projet
- Gestion des changements
- Sécurité développements et environnements de développement
- Cryptographie
- Configuration et durcissement
- Sécurité réseau
- Opérations et maintien en condition de sécurité
- Journalisation, surveillance et détection
- Gestion des vulnérabilités et des correctifs
- Gestion des incidents de sécurité
- Sécurité physique
- Sécurité du matériel
- Résilience.