Révisions

Versions	Date de validation	Valideur	Description
1.0	25/09/2024	E.Bouquier	première version du document

Sommaire

1 Présentation générale

1.1 Objectifs

La présente Politique de Sécurité des Systèmes d'Information (PSSI) a pour objectif de garantir la protection des systèmes d'information au sein de la BU MED (Multi Énergie et Digital) de Terega Solutions. Elle vise à assurer la confidentialité, l'intégrité et la disponibilité des données, ainsi que la résilience face aux menaces de cybersécurité dont la BU MED peut faire l'objet.

1.2 Périmètre

Cette politique s'applique à tous les systèmes d'information utilisés dans le cadre des activités de la BU MED de Terega Solutions, y compris les réseaux, les équipements critiques, et les données sensibles.

1.3 Cadre réglementaire et conformité aux normes

Dans le cadre de ses activités, la BU MED de Terega Solutions s'applique à respecter les référentiels suivants :

- la politique Sûreté du groupe Teréga (GED 090588)
- la directive cybersécurité (GED 090672) et la directive de protection de l'information du groupe

Teréga (GED 091012).

- le Règlement général sur la Protection des Données (RGPD) , texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union européenne. Il est entré en application le 25 Mai 2018.
- le référentiel ISO 27001 et ISO 27002 avec pour objectif de rassurer les marchés sur ses bonnes pratiques en matière de sécurité de l'information.
- les exigences réglementaires liées à la transposition de la Directive NIS2 applicables aux Entités Importantes qui fournissent des services numériques

1.4 GESTION DES RISQUES

L'évaluation des risques est réalisée en interne suivant une méthodologie propre au groupe Terega, qui s'appuie sur les bonnes pratiques de la méthode EBIOS RM préconisées par l'ANSSI. Les risques cyber sont identifiés et évalués afin de mettre en place les stratégies protection, de défense, de détection et de résilience
Cette analyse de risque est revue annuellement et lors des changements stratégiques.

1.5 ORGANISATION

Un correspondant SSI doit être nommé au sein de la BU MED. Celui-ci aura en charge de mettre en place les mesures techniques et les contrôles nécessaires pour répondre aux menaces et évènements redoutés mis en évidence dans l'analyse de risque.

1.6 MITIGATION DES RISQUES

1.6.1 Gestion des accès physiques

TEREGA Solutions bénéficie des mesures strictes de gestion des accès physiques mis en place par le groupe Teréga et qui respectent l'ensemble des référentiels suivants :

- référentiel APSAD D83 technique
- 1302 management de la sûreté.
- IGI n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale

Elles permettent de protéger l'accès aux centres de données et bureaux physiques hébergés dans les locaux du groupe. Seules les personnes habilitées ont accès aux différents locaux et installations nécessaires pour leur activité.
Des revues trimestrielles sont réalisées pour l'ensemble des accès physiques.

1.6.2 Gestion des accès logiques

La gestion des identités et des accès s'appuie sur un système de gestion des identités et des accès (IGA - IAM) centralisé.

- L'authentification est renforcée au travers de mécanismes de validation des identités multi facteurs.
- Une gouvernance des identités et des accès par profils (IGA) est également mise en place.

Pour les statutaires (salariés Teréga)
Un processus de gestion des arrivées, des mouvements internes et départs garantit la bonne activation et désactivation des accès.

Pour les prestataires,
Les responsables de contrat internes gèrent la création et les désactivations des identités et accès via l'outil IGA.

Des revues des accès sont réalisées :

- revues semestrielles automatique via les outils IGA (workflow de revalidation),
- revues annuelles manuelles pour les applications jugées sensibles pour l'activité de la BU MED.

1.6.3 Protection des endpoints.

Des mesures de protection physiques et logiques sont mises en place sur les postes de travail, serveurs et outils mobiles du système d'information.

POSTES DE TRAVAIL et SERVEURS WINDOWS

- durcissement des configurations Windows au socle
- installation de solutions EDR
- les droits des session utilisateurs sont restreints : l'utilisation de comptes à privilège est autorisée pour les activités le nécessitant (ex : .

POSTES CHROMEBOOK et OUTILS MOBILES

- application de configurations de sécurité appliquée par la console Google
- les applications et extensions déployées subissent des tests de sécurité

1.6.4 Mesures réseau

Le réseau interne est segmenté pour séparer les usages (séparation en Vlans)
Des systèmes de filtrage entre le réseau interne et externe (internet) sont mis en place.
Les accès vers internet depuis les postes de travail sont contrôlés et filtrés.

.

1.6.5 Infrastructure cloud

Des politiques de déploiement d'infrastructures régissent la manière dont les infrastructures AWS doivent être déployées en toute sécurité.
Des contrôles automatisés continus sont mis en place pour s'assurer de la conformité à cette politique ainsi qu'aux standards CIS.

Les environnements AWS hors production et production sont séparés et cloisonnés avec des règles d'accès définie pour chaque type d'environnement.
Ces accès font l'objet d'une revue annuelle.

1.6.6 Process de développement DevSecOps

Les processus de développement continus (CI/CD) sont mis en place avec une stricte séparation des rôles entre les environnements hors production et production. Afin de renforcer la sécurité et garantir une gestion efficace des environnements de développement, plusieurs mesures sont adoptées :

- **Création de branches par environnement** : Chaque environnement (développement, test, préproduction, production) dispose de ses propres branches pour garantir un isolement des modifications et une meilleure traçabilité des changements.
- **Contrôle d'accès et révision annuelle** : Les accès aux branches de développement sont strictement contrôlés et revus une fois par an, conformément aux meilleures pratiques de gestion des accès.
- **Responsabilités sur les branches** : Des règles de responsabilité sont mises en place sur chaque branche. Par exemple, un développeur ne peut appliquer une modification sans qu'elle ait été revue et validée par un architecte de la solution. Cela garantit la séparation des tâches critiques, minimisant ainsi les risques d'introduction de failles.
- **Audit continu des codes** : Les codes sont audités de manière continue à l'aide d'outils de scanning de sécurité pour détecter toute vulnérabilité éventuelle. Cela permet de limiter les risques liés aux failles de

sécurité dès les premières phases du développement.

De plus, pour garantir la disponibilité et l'intégrité des données :

- **Sauvegardes quotidiennes** : L'ensemble des codes sources est sauvegardé quotidiennement. Ces sauvegardes sont externalisées dans un compte AWS isolé des infrastructures de production pour protéger les données en cas d'incident sur les systèmes internes.
- **Utilisation des outils AWS** : Nous nous appuyons sur les bonnes pratiques et maintenons à jour les recommandations des normes **ISO 27001** et **ISO 27002**, en activant l'ensemble des audits et outils disponibles dans l'écosystème AWS :
    - **Well-Architected Review AWS** : Réalisation régulière de revues d'architecture pour aligner nos infrastructures aux meilleures pratiques.
    - **AWS Security Improvement Program (SIP)** : Évaluation continue des bonnes pratiques qui découlent des items de la norme.
    - **AWS Security Hub** : Outil de contrôle automatique des bonnes pratiques de sécurité, qui détecte en continu les anomalies et les non-conformités.

Audits et tests de sécurité

Afin d'assurer un niveau de sécurité optimal et de détecter proactivement les faiblesses potentielles, plusieurs audits de sécurité sont réalisés chaque année :

- **Audits d'infrastructure** : Nous effectuons un audit **WAR (Well-Architected Review)**, une analyse détaillée réalisée par les équipes sécurité AWS, pour évaluer l'architecture de nos systèmes.
- **Bug Bounty** : Des programmes de Bug Bounty sont mis en place sur nos applications et API web, en collaboration avec des partenaires spécialisés dans la recherche de vulnérabilités.
- **Pentests** : Des tests d'intrusion (pentests) sont réalisés sur les équipements et logiciels développés par la Business Unit (BU) MED, en s'appuyant sur des partenaires externes certifiés.
- **Auto-évaluation selon les normes de sécurité** : Nous effectuons des auto-évaluations (self-assessment) sur des normes de sécurité pertinentes comme **IEC 62443** et **CIS Benchmarks**, afin d'intégrer les bonnes pratiques et répondre aux exigences spécifiques de nos clients.

Amélioration continue et gestion de crise

- **Pipeline DevSecOps évolutif** : Nous faisons évoluer en continu notre pipeline DevSecOps ainsi que nos outils de supervision pour identifier et corriger les non-conformités avant qu'elles ne génèrent des incidents. Cette approche proactive permet de renforcer la sécurité et la résilience de nos systèmes.
- **Partenaires certifiés** : Nous sélectionnons nos partenaires en fonction de certifications cohérentes avec nos standards de sécurité et nous les impliquons dans des tests de sécurité, tels que des pentests, pour évaluer nos capacités en conditions réelles.
- **Audits internes pilotés par la sécurité groupe** : Des audits internes réguliers sont menés par notre département de sécurité groupe pour garantir la conformité à l'échelle organisationnelle.
- **Veille technologique continue** : Notre cellule de veille et R&D explore en permanence de nouvelles approches et technologies afin de rester à la pointe des innovations en matière de cybersécurité.

Gestion de Crise

Nous nous appuyons sur les processus de gestion de crise définis au niveau du groupe, garantissant une réponse rapide et coordonnée en cas d'incidents critiques. Ces processus sont basés sur des procédures éprouvées et régulièrement mises à jour, afin de s'assurer qu'en cas de crise, toutes les parties prenantes connaissent leurs rôles et responsabilités. Notre approche repose sur la mise en place d'une cellule de crise dédiée, activée lors d'événements menaçant la continuité des activités ou la sécurité de nos systèmes.

La cellule de crise opère selon un cadre rigoureusement défini, incluant :

- **Des rôles clairement attribués** : chaque membre de l'équipe de crise a une fonction précise, allant du gestionnaire de crise, en charge de la coordination globale, aux experts techniques, responsables de l'investigation et de la remédiation des problèmes.
- **Une communication centralisée** : l'information circule de manière fluide entre les équipes internes, les partenaires externes, et les parties prenantes stratégiques, garantissant une prise de décision rapide et éclairée.
- **Un suivi en temps réel des actions** : chaque étape du plan de crise est documentée et suivie pour assurer une réponse efficace et mesurable.
- **Exercices réguliers de simulation de crise** : nous organisons périodiquement des exercices de gestion de crise, en collaboration avec nos partenaires, pour tester la réactivité de nos équipes et ajuster nos procédures si nécessaire.

Ces simulations permettent également de démontrer notre excellence opérationnelle en mettant à l'épreuve nos capacités à réagir rapidement à une crise tout en maintenant la continuité des opérations. Pour renforcer cette approche, nous prévoyons de mettre en place des techniques de **chaos engineering**, qui testeront nos systèmes face à des scénarios réalistes, tels que des cyberattaques ou des pannes majeures.

Vous pouvez consulter notre document **Présentation Cellule de Crise Opérationnelle io-base** pour un aperçu détaillé des rôles, des responsabilités et des procédures activées en cas de crise :
Celulle de crise opérationnelle io-base : presentation-v2.1

Ce document explique précisément comment nous gérons une crise au sein de notre environnement io-base, incluant la structure de la cellule de crise, les rôles attribués à chaque membre, et le déroulement des opérations en cas d'incident majeur.

-

1.7 Surveillance et Détection

1.7.1 Surveillance des accès physiques

L'ensemble des accès physiques est sous surveillance 24/7 par des équipes dédiées à la sûreté physique. Ces équipes spécialisées assurent une surveillance continue des installations, incluant des contrôles d'accès par badges sécurisés, des caméras de vidéosurveillance en permanence actives, et des systèmes d'alarme sophistiqués. Chaque entrée et sortie est monitorée, et les zones sensibles sont soumises à des protocoles d'autorisation renforcés, garantissant que seuls les personnels autorisés peuvent accéder aux infrastructures critiques.

1.7.2 Surveillance des infrastructures IT

La surveillance des infrastructures IT est assurée 24/7 par une équipe spécialisée au sein du Security Operation Center (SOC), garantissant une supervision continue de l'ensemble des systèmes informatiques. Grâce à des outils de monitoring avancés et à l'analyse des logs en temps réel, cette équipe est capable de détecter proactivement tout comportement anormal ou cyberattaque.

1.7.3 Remontées des alertes utilisateurs

Le support utilisateur du groupe Teréga centralise les alertes utilisateurs et remonte les incidents de sécurité aux équipes sécurité du groupe (RSSI / RSO / Correspondant SSI BU MED).

1.8 Réponse à incident

Les incidents sont classés par ordre de gravité : la réponse à incident dépend de la gravité de celui-ci et est réalisée en coordination avec le SOC. Les outils garantissent la traçabilité des incidents jusqu'à leur clôture.
En fonction de la gravité et de l'importance d'un incident, un partenaire de réponse à incident de

sécurité spécialisé (PRIS) peut être mobilisé et venir en renfort des équipes internes

1.9 Formation et Sensibilisation

Les nouveaux embauchés passent par un processus d'accueil présentant les règles de cybersécurité en vigueur dans l'entreprise.
Tout au long de la vie des collaborateurs dans l'entreprise, des campagnes de sensibilisation de type phishing sont organisées une fois par an et les résultats sont présentés à l'ensemble des directeurs.
Des webinars obligatoires sont aussi diffusés notamment sur la protection de l'information.
Des formations spécifiques peuvent être dispensées suivant la fonction du collaborateur dans le groupe TEREGA.

1.10 Evolution de la PSSI (amélioration continue)

La PSSI est revue annuellement, en fonction des critères suivants :

- évolution de l'analyse de risque à chaque changement majeur
- évolution des technologies
- évolution des réglementations
- retour d'expérience partagés avec d'autres organismes
- évolution de la menace

1.11 Amelioration continue

Dans une démarche d'amélioration continue et d'adaptation à la menace, la BU MED de Terega Solutions se fait auditer chaque année. La restitution donne lieu à un plan d'action suivi lors des réunions d'équipes sous la direction du pôle risk management du groupe Terega.
Le département d'audits internes de Teréga se donne le droit de planifier des audits permettant de vérifier la conformité avec la PSSI Groupe et la PSSI BU MED dans la cadre du plan d'audit annuel.

1.12 PCA PRA

Un plan de continuité (PCA) est établi et mis à jour par la BU MED. Il permet de définir les mesures et les moyens qui seraient mis en œuvre selon plusieurs scénarios de crises.

Des modes dégradés et des plans de reprise d'activité (PRA) sont également définis.

Afin d'optimiser la résilience de nos infrastructures, des pratiques de DevOps avancées sont mises en œuvre, telles que l'automatisation des déploiements et l'utilisation de services managés et distribués sur plusieurs zones géographiques. Cela garantit une haute disponibilité, mais également une robustesse face à des incidents localisés.

Fin du document