PSSI

Politique de Sécurité des Systèmes d'Information

Janvier 2020

SOMMAIRE

1. Introduction – la politique de sécurité de Coreoz

Coreoz est une agence digitale française qui conseille, développe et héberge des solutions webs et mobiles pour ses clients.

La sécurité est au cœur de notre activité. Nous consacrons beaucoup de de ressources et d'énergie pour :

- Sécuriser notre système d'information ;
- Construire pour nos clients des solutions webs sécurisées dès la phase de design ;
- Héberger les données de nos clients avec le maximum de sécurité.

La construction d'une relation durable et de confiance avec nos clients est primordiale pour nous. Avec l'exposition de plus en plus forte des plateformes webs aux menaces de sécurité informatique, nous prenons très au sérieux notre rôle pour protéger nos infrastructures et celles que nos clients nous confient et travaillons quotidiennement à consolider nos services.

C'est pourquoi Coreoz a mis en place une démarche de sécurité avec pour objectif l'obtention de labels et certifications de référence sur le marché, qui sont pour vous un gage de qualité et de confiance.

Nos collaborateurs adhèrent à cette démarche et y contribuent activement au quotidien. Responsables, ils veillent à ce que les règles de sécurité soient connues, comprises et appliquées, sur leur périmètre d'intervention et au sein de leur mission. Vigilants, ils sont en alerte constante lors de leurs différents usages et utilisations des systèmes d'information, afin de détecter d'éventuels incidents et d'adopter le comportement adéquat lors d'une situation à risque.

La présente Politique de Sécurité des Systèmes d'Information est applicable dans le cadre des relations de sous-traitance entre Coreoz et ses Clients, pour les solutions webs que développent Coreoz pour ses clients et pour les données que le Client transmet à Coreoz en sous-traitance.

2. La sécurité et nos collaborateurs

Chez Coreoz, l'apprentissage et l'application des mesures de sécurité commence dès l'embauche des collaborateurs, afin que la culture de la sécurité soit diffusée à travers toute l'entreprise. Chaque collaborateur est conscient des menaces qui pèsent sur les systèmes d'information et connaît donc ses responsabilités vis-à-vis de ceux-ci. Cela lui permet d'endosser un rôle d'acteur permanent.

Pour cela une formation au bon usage des moyens informatiques (basée sur le guide de l'ANSSI : https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf) est dispensée à chaque collaborateur dès son arrivée chez Coreoz et est complétée régulièrement par des formations complémentaires.

Les collaborateurs de Coreoz qui développent et construisent les solutions de nos clients sont sensibilisés régulièrement aux bonnes pratiques du métier en matière de sécurité web notamment au Top ten OWASP (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

3. Gestion des biens et des actifs

Garantir de manière effective la sécurité de nos systèmes d'information requiert la connaissance des besoins en matière de sécurité. C'est la raison pour laquelle chaque actif – matériel, poste de travail, serveur, téléphone… - fait l'objet d'un inventaire détaillé pour être ensuite classifié avec un propriétaire qui leur est associé.

Une procédure de mise au rebut est formalisée et mise en œuvre lors de la sortie ou du rebus d'un actif du système d'informations.

4. Gestion des accès

L'un des facteurs essentiels de la sécurité du Système d'Information est la gestion des accès physiques et logiques : celle-ci s'appuie sur des processus efficaces permettant une bonne gestion des identités, leur mise à jour permanente et des mécanismes d'authentification robustes.

Ainsi, chaque utilisateur accédant au Système d'Information de Coreoz est dûment identifié et authentifié. Tout compte est rattaché à une personne physique unique afin de garantir la traçabilité des accès et des actions.

Les droits et habilitations délivrés aux utilisateurs sont définis selon leur profil métier et dans le respect des principes de moindre privilège et de séparation des pouvoirs afin de garantir la confidentialité des données. Une revue des comptes est effectuée tous les 6 mois afin de s'assurer de la légitimité de tous les comptes.

5. Documentation

Documenter les méthodologies, les processus et les actions est un élément essentiel à leur bonne application.

La documentation est donc régulièrement mise à jour. Elle uniformise les pratiques au sein de Coreoz et est utilisée et réalisée à tous les niveaux de l'entreprise.

6. Sécurité physique

Chez Coreoz, nous mettons activement en œuvre des politiques de sécurité physique à la fois dans nos locaux.

Un ensemble de mesures de protection physique est mis en œuvre parmi lesquelles :

- La télé-surveillance et des systèmes anti-intrusion dans nos locaux ;
- Un badge d'accès unique pour chaque collaborateur ;

- Des espaces sécurisées sous clés ;
- Une politique de gestion des accès en fonction du type de profil des collaborateurs et intervenants.

Chaque utilisateur du Système d'Information participe également à la sécurité physique en respectant des bonnes pratiques, comme la fermeture des bureaux, la politique du « bureau net », le verrouillage du poste de travail lors des absences, ou encore la protection renforcée de la documentation sensible.

7. Sécurité des terminaux

L'accès au poste de travail n'est possible qu'après une phase d'authentification obligatoire (mot de passe ou biométrie). Chaque poste de travail est équipé d'un antivirus mis régulièrement à jour.

Les équipements mobiles professionnels sont également protégés par biométrie. Nos collaborateurs prennent toutes les précautions nécessaires pour protéger leurs équipements, afin d'assurer au mieux la protection et la sécurité des données personnelles, conformément à notre politique de gestion de la mobilité.

8. Gestion de la sous-traitance

L'ensemble des contrats avec nos sous-traitants intègre de strictes exigences de sécurité applicables ainsi que des moyens de contrôler le respect de ces exigences.

Les exigences que nous avons envers nos sous-traitants sont au moins équivalentes à nos propres exigences de sécurité internes, afin de respecter nos engagements concernant un haut niveau de sécurité des systèmes d'information.

9. Sécurité des réseaux

Une politique de cloisonnement et de confinement des réseaux est mise en place au sein des réseaux de Coreoz. Ce cloisonnement s'accompagne d'une politique de filtrage interne et externe afin de lutter contre les codes malveillants.

Les solutions de nos clients hébergées au sein des Datacenters de nos partenaires sont protégées (firewall & hardening) et il n'y a pas de connexion directe avec les environnements internes de Coreoz.

Les accès distants au système d'information de Coreoz se font via un VPN chiffré et authentifié.

10. Confidentialité et chiffrement des données

Plusieurs mesures de chiffrement sont mises en œuvre pour assurer la confidentialité des informations et données traitées.

D'abord, l'ensemble des postes de travail, des middleswares et des terminaux sont protégés par mot de passe, afin de garantir l'inaccessibilité des informations aux personnes non-autorisées.

Les supports contenant des informations sont protégés contre les accès non autorisés via des protections physiques et matérielles.

Coreoz n'accède ou n'exploite jamais vos données en dehors des cas expressément stipulés dans nos contrats, ou sur instruction documentée de votre part. Vos données ne sont également jamais revendues à des tiers.

11. Sécurité de nos solutions web

Chez Coreoz, nous sommes conscients des différentes menaces qui pèsent constamment sur les sites web. C'est pour cette raison que nous avons pris les mesures de sécurité nécessaires pour garantir la protection des données traitées par nos sites.

Nous appliquons systématiquement plusieurs principes pour la sécurité des environnements de nos clients :

- Hardening de nos serveurs : minimum de ports ouverts, minimum d'outils par machines, monitoring & application régulière des patchs de sécurité, no backdoor, etc… ;
- Https only et testing automatique de la qualité SSL. Vérification des configurations quotidiennes par Qualys SSL ;
- Configuration & déploiement automatisée ;
- Journalisation de tous les évènements et remontée des anomalies automatiques aux équipes ;
- Base de données non exposées sur internet ;
- Monitoring harware avec levée d'alerte email en cas de dépassement de seuils de tolérance (répétition de l'alerte à intervalle régulier tant qu'elle n'est pas corrigée) ;
- Monitoring applicatif avec levée d'alerte email en cas de non disponibilité d'un applicatif (répétition de l'alerte à intervalle régulier tant qu'elle n'est pas corrigée) ;
- Backups journaliers de tous les systèmes de production stockées sur bandes dans d'autres datacenters ;
- Inscription aux différentes newsletters et flux RSS de sécurité et de remontées CSV.

Dans la construction de nos solutions, nous appliquons aussi systématiquement des principes forts de sécurité :

- Webs Services authentifiés par défaut ;
- Gestion des sessions en silo isolé ;
- Chiffrement : Hashage par défaut des mots de passes, utilisation de jetons d'échanges sécurisées ;
- Test d'intrusion automatisé ;
- Formation & sensibilisation régulière au Top Ten OWASP ;
- Monitoring & Patch régulier des librairies et middlewares utilisés ;
- Revue de code croisée ;

12. Sauvegarde des données

L'ensemble des applications, systèmes d'exploitation, événements, configurations des équipements et données de production qui délivrent une fonction aux utilisateurs (internes, clients…) est sauvegardé régulièrement. La fréquence des sauvegardes est dépendante du type, de la sensibilité et du volume des données.

Quelles que soient les données sauvegardées et la typologie des sauvegardes, celles-ci sont stockées sur des serveurs dédiés dans des datacenters différents.

Seuls les administrateurs système et réseaux, ainsi que le RSSI, peuvent accéder aux sauvegardes pour des motifs légitimes tels que la gestion des incidents.

Enfin, des tests de restauration sont régulièrement effectués par les administrateurs systèmes et réseaux sur l'ensemble du périmètre fonctionnel de Coreoz afin de s'assurer de leur bon fonctionnement.

13. La gestion des incidents de sécurité

Le traitement des incidents de sécurité fait l'objet d'une procédure formalisée, validée et connue de tous. Elle permet d'apporter une réponse adaptée en cas d'incident majeur pouvant affecter la sécurité du Système d'Information ou des données de ses utilisateurs, agents ou administrés.

Ces procédures sont régulièrement testées et mises à jour afin de s'assurer de leur pertinence et efficacité en tout temps.

Par ailleurs, tout utilisateur a l'obligation de signaler sans tarder aux équipes sécurité, tout acte susceptible de représenter une violation réelle ou présumée des règles de sécurité.

14. La continuité d'activité

La continuité du Système d'Information est assurée grâce à un ensemble de mesures, dont :

- Des systèmes de remontée d'alerte dès qu'une anomalie sur les équipements & logiciels est détectées ;
- La redondance des équipements d'infrastructure (onduleurs, alimentation des serveurs, firewall, routeurs et équipements réseaux, accès à Internet) ;
- Des procédures permettant d'intervenir rapidement sur les équipements ou l'infrastructure en cas d'incident ;
- Un plan de continuité d'activité et de reprise d'activité formalisé et régulièrement testé afin de réduire au maximum les indisponibilités dues à un incident.

15. L'amélioration continue

Chez Coreoz, les mesures et pratiques de sécurité sont réévaluées de manière périodique et régulière, afin de tenir compte de quatre éléments importants :

1. L'évolution des menaces ;
2. La bonne couverture des risques ;
3. L'évolution réglementaire ;
4. La couverture exhaustive du périmètre.

Des dispositifs de tableaux de bord (stratégique, pilotage et opérationnel) sont également mis en place afin de permettre de suivre notamment le niveau d'application des règles, le niveau de sécurité, les incidents et l'efficacité des mesures et des moyens.

Devant l'évolution permanente des risques pouvant peser sur les systèmes d'informations, Coreoz a mis en place une veille efficace permettant notamment de détecter les nouvelles menaces et les nouveaux standards de sécurité.

La réalisation d'audits réguliers en interne ou par des tiers, permet également à Coreoz de s'assurer de l'efficacité et de la performance de ses systèmes à chaque instant et de les mettre à jour le cas échéant.