



XEFI SQY

Antony SOUSTELLE





DATE

**Vos données
sont-elles
bien sécurisées ?**

XEFI

SOMMAIRE

- PRÉSENTATION DU GROUPE XEFI ET DATACENTERS
- CYBERATTQUES – LES RISQUES
- SECURITE ET SAUVEGARDE
- QUESTIONS / ÉCHANGES

LE GROUPE XEFI

au 31.12.2023

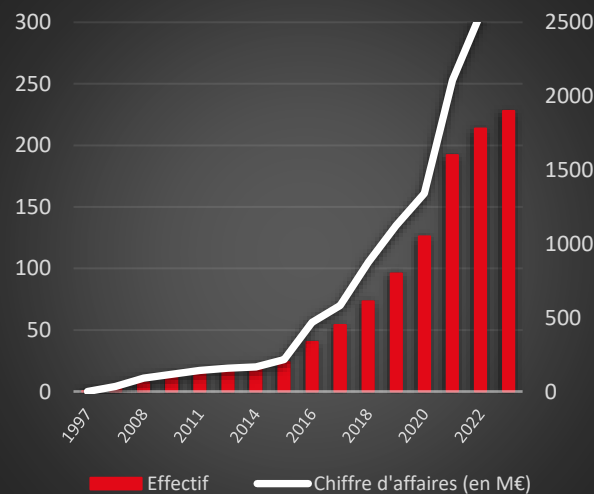


LA PROXIMITÉ INFORMATIQUE

 **1 900** collaborateurs

 **26** ans d'expérience

 **355 M€** de CA



INFORMATIQUE ET BUREAUTIQUE DE PROXIMITÉ

5 Data Centers en propre **+ 100 000**



Clients (au 31.12.2023)



+ 23 000
sous contrats

+ 13 000
hébergés

UNE EXPERTISE IT PME À 360°



COUVERTURE GÉOGRAPHIQUE

193
agences XEFI
21 en propre
172 franchises



Plus de
620
véhicules
d'intervention



CERTIFICATIONS PARTENAIRES



Gold
Microsoft Partner



Nos Datacenters de Civrieux



CV 1 : 2013
CV 2 : 2019



- Deux Datacenters **hautement sécurisés**, situés dans une zone sans risque naturel ni industriel
- **Maitrise intégrale** de la chaîne de services
- Un impact sur l'environnement maîtrisé avec des technologies innovantes
- Un niveau de certification **très élevé**

CV 1



CV 2



Nos Datacenters Clermontois



CBZ 3 Cébazat (63)

- Surface de 1000m² hautement sécurisée,
- Datacenter **neutre** éco-énergétique,
- Double enceinte haute protection,



BZT 4 Clermont-Ferrand (63)

- Surface de 400m² intégrée aux locaux existants,
- Datacenter **enterré** assurant une sécurité physique exceptionnelle,
- Une réactivité hors-pair avec la proximité des équipes,



Notre cinquième Datacenter



RVS 5



Reventin - Vaugris (38)

- Sorti de terre en **décembre 2021**
- Accolé à l'agence **XEFI VIENNE**
- Certifié **TIER IV DESIGN et FACILITY**, plus haut niveau de certification délivré par l'Uptime Institute





POURQUOI LES TPE/PME SONT UNE **CIBLE PRIVILÉGIÉE** ?



**POURQUOI
ETES VOUS A
RISQUE**

Sécurité du système informatique ne fait pas partie des priorités des PME

- **Absence de moyens financiers et humains**

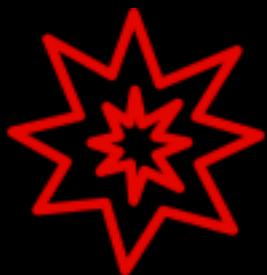
- Modes de fonctionnement **moins formels**

 - ➔ partage de mot de passe, absence de procédure

- Moins bien informées, protégées, donc plus **vulnérables et exposées**

Déploiement accéléré du **télétravail**

Grands groupes déjà victimes et maintenant protégés



DES

CONSEQUENCES

CATASTROPHIQUES

PERTE FINANCIÈRE DIRECTE

en cas de paiement d'une rançon pour stopper l'attaque cyber

PERTE FINANCIÈRE

en cas d'arrêt de la production ou de l'activité de l'entreprise liée à la déstabilisation du système comptable de l'entreprise

VOL de méthode(s), brevet(s), données...

DÉGRADATION DE L'IMAGE de l'entreprise : enjeux de notoriété

PERTE DE CONFIANCE des partenaires, clients...



**JUSQU'À LA PARALYSIE
ET LE DÉPÔT DE BILAN !**

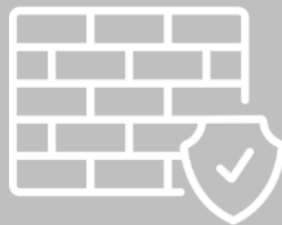
LA SÉCURITÉ AU CŒUR DES PRIORITÉS !

➤ Comment se prémunir des attaques ?

Antivirus/
anticrypto



Firewall



Antispam



**Dernière étape
pour sécuriser
ses données...**

**Sauvegarde
externalisée**





ANTI-SPAM

MAIL IN BLACK



LA SOLUTION MAILINBLACK



MAILINBLACK



- Le seul antispam par identification du marché
(Identification en 3 étapes)
- Interface utilisateur
 - ➔ Rapport quotidien paramétrable (11 par jour maximum)
 - ➔ Gestion de la liste des expéditeurs par adresse individuelle ou nom de domaine
- 100% compatible avec toutes les messageries*
- Nuage de mots personnalisable : valorisation de l'activité et des valeurs de l'entreprise

**Sous réserve d'une messagerie avec un nom de domaine personnalisé*



SAUVEGARDE À DISTANCE

CAMPUS NEXEREN



UNE FLOTTE DE 5 DATACENTERS EN AUVERGNE-RHÔNE-ALPES

Plus que jamais, nous sommes au service de nos clients afin de les soutenir dans leur croissance et besoin de performance



- ✓ Le Groupe XEPI a investi dans la création de son propre **campus d'hébergement** durable en Auvergne-Rhône-Alpes, ce qui lui permet de maîtriser à 100% l'outil d'hébergement. Nos Datacenters sont **100% français**, un critère essentiel afin de préserver l'intégrité et la confidentialité de nos données.
- ✓ Ce campus **dernière génération** a vu le jour fin 2013 et est issu des meilleures technologies pour un hébergement de qualité, sûr et respectueux de l'environnement. Nos Datacenters sont alimentés par une énergie **100% renouvelable et locale**.
- ✓ Nous disposons d'un **PUE inférieur à 1,3** nous amenant vers une grande performance énergétique.
- ✓ Doté **des plus hautes certifications**, nos Datacenters garantissent la **qualité, la sécurité et la fiabilité** de notre hébergement.

*PUE - Power Usage Effectiveness



SAUVEGARDE : LA DERNIÈRE ÉTAPE POUR SÉCURISER SES DONNÉES

Les éléments clés d'une sauvegarde fiable et efficace

- 1/ Sauvegarde **externalisée**
- 2/ Sauvegarde **régulière et intégrale** (données + systèmes)
- 3/ Sauvegarde **chiffrée**
- 4/ Sauvegarde **supervisée**

100% de fiabilité - 100% de sérénité

80%

des entreprises qui
perdent leurs données
déposent le bilan dans
les 2 années qui suivent

- Quelle que soit la taille de l'entreprise, **la sauvegarde n'est pas une alternative**
- Avec la sauvegarde XEFI, tous les types de risques sont éliminés :
 - actes malveillants
 - facteurs humains (*perte, vol, oubli, etc.*)
 - facteurs physiques (*sinistres ou panne matériels*)
 - facteurs logiciels (*dysfonctionnement d'une application ou d'un système d'exploitation*)
- Travail **quotidien & chronophage**, XEFI prend en charge la **responsabilité** de la sauvegarde
- La solution de sauvegarde à distance XEFI est une solution **100% fiable !**





LES BONNES PRATIQUES DE LA SÉCURITÉ INFORMATIQUE



LES MOTS DE PASSE



Choisir des MOTS DE PASSE COMPLEXES combinant majuscules, minuscules, chiffres et caractères spéciaux



Utiliser un mot de passe DIFFÉRENT pour chaque service et les CHANGER RÉGULIÈREMENT



Utiliser un GESTIONNAIRE DE MOTS DE PASSE et désactiver celui des navigateurs



Ne JAMAIS COMMUNIQUER vos mots de passe à un tiers et ne pas les écrire sur un papier



L'UTILISATION QUOTIDIENNE



Ne pas ouvrir les pièces jointes et les liens provenant d'expéditeurs INCONNUS



Vérifier la COHÉRENCE entre l'expéditeur présumé et le contenu du message



Ne jamais ouvrir les pièces jointes avec les EXTENSIONS .pif, .bat, .com, .exe, .ink ...



Ne jamais cliquer sur un LIEN dans un email vous demandant de vous identifier



LES APPAREILS



VERROUILLER VOTRE SESSION dès que vous vous absentez



METTRE A JOUR votre système d'exploitation et vos logiciels



Télécharger les programmes uniquement depuis les sites OFFICIELS des éditeurs



Se MÉFIER des clés USB et des disques durs

LE TRAVAIL À DISTANCE



SÉPARER LES USAGES personnels et professionnels :

- ne pas transférer vos mails professionnels sur des boîtes personnelles
- ne pas stocker des données de l'entreprise sur vos appareils personnels



PROTÉGER vos données lors des déplacements : garder vos appareils avec vous et ne pas connecter d'équipements à des wifi publics



Être aussi PRUDENT avec son téléphone et sa tablette qu'avec son ordinateur

**Avez-vous
des
questions
?**

