Anticiper pour maintenir l'activité malgré une attaque

Pour poursuivre votre activité malgré tout, vous pouvez choisir entre plusieurs options, dont l'auto-hébergement ou l'externalisation.

Auto-hébergement	Externalisation
Contrôle & responsabilités vous êtes responsable de la gestion du système d'information	**Contrôle & responsabilités** responsabilités infra à charge du prestataire
Coûts importants : matériel, licences, personnel, salle informatique	**Coûts** mensuels, anticipables et sans surprise
Fiabilité & stabilité pas de redondance (électrique, clim, lignes internet, système incendie…)	**Fiabilité & stabilité** disponibilité accrue, locaux sécurisés, équipements redondés
Sécurité généralement moindre (équipements, locaux, solutions logicielles, lignes internet…)	**Sécurité** optimale (surveillance 24/7, détection d'intrusion, pare-feux, équipements plus robustes…)
Flexibilité + de libertés dans la configuration, les équipements	**Flexibilité** flexibilité d'évolution (augmentation de ressources, croissance externe…)

Le Plan de Reprise d'Activité

Faites vous accompagner par un conseil expert pour mettre en place un Plan de Reprise d'Activité. Le PRA met à votre disposition :

- un document qui fiabilise vos procédures et informe les équipes,
- un accompagnement qui sécurise votre activité en cas d'attaque.

Pour plus de détails, vous pouvez consulter le replay du RDV au 50 consacré aux cyberattaques (2024)

Où et comment héberger son activité ?

Pour choisir son mode d'hébergement, voici les points de vigilance à prendre en compte.

CONCEPTION

Infrastructures client non mutualisées : permet de ne pas être pris dans l'attaque subie par un autre client de l'hébergeur.

IDENTIFICATION DE L'UTILISATEUR

Implémentation du MFA (multifactor identification authentification)
Complexification du mot de passe
Stratégies de sécurité mot de passe

ANALYSES SPÉCIALISÉES

Audits de sécurité externes
Tests de pénétration externes
Test de remise en service après sinistre

POLITIQUES ET STRATÉGIES

Plan de Reprise d'Activité
Approche moindre privilège/Zero Trust
Security Baseline Compliancy

SÉCURITÉ DES SYSTÈMES

Couverture antivirus EDR des systèmes
Pare-feu dernière génération
Filtrage internet sur liste blanche
Outils de surveillance de l'infrastructure / SOC
Utilisation d'IAC (infrastructure as code)
Solution de scan des vulnérabilités
Suivi des activités du collaborateur

CONTRAT D'HÉBERGEMENT

Engagement contractuel / responsabilité engagée
Réactivité du support technique / SLA / GTR
Certifications (SecNumCloud…)

SAUVEGARDES

Sécurisées (règle du 3-2-1)
Géo-distantes
Suivi quotidien
Tests de restauration réguliers

DATACENTERS

Localisation
Tier IV / redondance
Performances : équipements qui permettent d'assurer une sécurité renforcée

> **La question n'est plus de savoir SI, mais QUAND, vous allez être attaqué.**
>
> **VIRGINIE ROITMAN**, PRÉSIDENTE DE L'ORDRE FRANCILIEN EN DÉCEMBRE 2023

Des attaques en augmentation

+ 255 %
d'attaques par rançongiciel
entre 2019 et 2020

54 %
des entreprises françaises
attaquées en 2021

LES TPE ET PME REPRÉSENTENT

40 %
des attaques par rançongiciel traitées ou rapportées à l'Agence nationale de la sécurité des systèmes d'information (Anssi)

60 %
des PME attaquées ne se relèvent pas et déposent le bilan
dans les 18 mois suivant l'attaque

SEULES

50 %
des entreprises victimes portent plainte, les statistiques sont donc sous estimées

50 000 €
coût médian d'une cyberattaque

55 %
des entreprises ont investi dans leur cybersécurité
en 2022

Ne pas jeter sur la voie publique

Prévenir et gérer les cyberattaques : le guide pratique pour les cabinets

Commission Innovation
ORDRE DES EXPERTS-COMPTABLES PARIS ÎLE-DE-FRANCE

ORDRE DES EXPERTS-COMPTABLES
Région Paris Ile-de-France

Comprendre une attaque

Causes

Types d'intrusion

- Virus/malware
- Phishing
- Exploitation de failles
- Vulnérabilités logicielles
- Pare-feu
- Via réseau partenaire connecté
- ChatGPT (IA)

Failles matérielles

- Infrastructure obsolète
- Équipements non redondés
- Manque de monitoring
- Datacenter non certifié
- **Si auto hébergement** : panne climatisation, dégradation physique, incendie, inondation, vol, coupure électrique...

Vulnérabilité des équipes

- Erreurs humaines
- Manque de formation / sensibilisation
- Compétences équipe technique
- Perte ou vol de matériel

Conséquences

Données

- Vol de données
- Espionnage industriel
- Destruction de sauvegardes
- Vente sur le darknet

Arrêt de production

- Déni de service / brute force
- Vandalisme

Escroquerie

- Attaque au président
- Demande de rançon

Se prémunir contre une attaque

Les postes clés à prendre en compte pour minimiser les risques

Poste de travail

- Antivirus à jour
- Solution EDR installée*
- Pare-feu local activé
- Mises à jour Windows régulières
- Si PC portable, BitLocker activé, permettant de crypter son disque dur
- Se méfier des clés USB
- Privilèges réduits du compte utilisateur

Messagerie

- Si Microsoft 365, activer MFA
- Solution antispam
- Vigilance sur pièces jointes
- Vigilance sur email expéditeur
- Vigilance sur le contexte du mail
- Si demande critique, validation orale / sms

La sauvegarde

- Suivi quotidien
- Duplication géographique
- Copie déconnectée / immuable
- Tests réguliers

Stratégie

- Ne pas tout déléguer au même prestataire
- Assurance cyber
- Sensibilisation et formation régulière des collabs
- Campagnes de faux phishing
- Vecteurs de communication
- Annuaire contacts externalisé

Le mot de passe

- Entre 8 et 15 caractères Min 3 critères de complexité
- Utiliser un gestionnaire de mot de passe
- Blocage sur 3 saisies erronées
- Activer authentification multi-facteur (MFA)

Le réseau local

- Pare-feu configuré
- Accès physique restreint
- Onduleur électrique
- Inventaire du parc à jour

** Extended detection response : nouvelle technologie d'antivirus qui pourra identifier les comportements anormaux et les brèches.*

Hébergement et assurance : relisez vos contrats !
Vérifiez avec votre hébergeur l'ensemble de vos postes de contrôle et de sécurité informatique inclus dans vos contrats.

Contactez votre assureur pour faire le point sur les risques couverts et vos garanties.

Pour bénéficier des garanties négociées avec le groupe Verspieren, voici les conditions à remplir :

- **Installer un antivirus/antispams/firewall** et les mettre à jour automatiquement
- **Mettre à jour ses logiciels** selon les recommandations de l'éditeur
- **Changer les mots de passe** régulièrement (8 caractères minimum)
- **Sauvegarder vos données** chaque semaine sur des supports externes

Toutes les garanties et conditions sur : https://oec.verspieren.com

Réagir en cas d'attaque

Que faire si, malgré mes précautions, je suis attaqué·e ?

- Débrancher l'ordinateur du réseau et ne plus utiliser l'équipement corrompu
- Ne pas payer la rançon
- Déposer plainte le plus rapidement possible auprès de la gendarmerie ou de la police et fournir toutes les preuves permettant de documenter le dossier de plainte
- Déclarer le sinistre auprès de votre assureur
- Notifier l'incident à la CNIL sous 72h si des données ont été volées
  https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles
- Prévenir vos clients

En cas de besoin, l'Ordre reste à vos côtés

Vous pouvez joindre :

Le conseil régional :
mbrun@oec-paris.fr

Le conseil national :
cybersecurite.cnoec@experts-comptables.org

Se former et se faire aider

Les webinaires

4 replays à visionner sans modération

Cybersécurité, adoptez les gestes barrières *(2020)*

Les experts-comptables face au défi de la cybersécurité *(2022)*

COAXIS – cyberattaque Le CNOEC vous accompagne *(2023)*

La sécurité numérique des TPE/PME *(2024)*

Les aides financières

Diagnostic cybersécurité BPI

Bpifrance propose un diagnostic numérique renforcé pour aider les TPE et PME à faire face aux risques cyber. Réalisée par un consultant expert, la prestation de 8 jours est financée à 50 % par la banque publique.

Les chèques Cyber de la Région IdF

Région îledeFrance

Le chèque diagnostic Cyber aide les PME à identifier les actions prioritaires à mettre en œuvre avec un soutien pouvant aller jusqu'à 5 000 €. Le chèque investissement Cyber aide les PME à s'équiper pour se protéger face à la menace Cyber avec un montant pouvant aller jusqu'à 10 000 €.

L'Anssi (agence nationale de sécurité des systèmes d'information) et France numérique fournissent de précieux conseils en matière de sécurité informatique.