LES MÉMOS
JURIDIQUE - MARCHÉS : 4

# Cybersécurité des entreprises

Juillet 2021

## ENJEUX

### TOUTES LES ENTREPRISES SONT CONCERNÉES

**Les cyberattaques sont devenues un enjeu majeur pour les entreprises.** En plus de l'atteinte au système informatique de l'entreprise, la cyberattaque va perturber son activité et ses conséquences sont souvent dramatiques.

Le rançongiciel est un programme malveillant dont le but est d'obtenir de l'entreprise le paiement d'une rançon.

## LES RISQUES

- **Pertes de données (comptabilité, données des clients...)**
- **Pertes financières, Pertes d'exploitation...**
- **Atteinte à la réputation de l'entreprise**


## LES MESURES DE PRÉVENTION

### Mise en place d'un PRA

**Plan de Reprise d'Activité** qui consiste à s'assurer que l'entreprise puisse remettre ses services en action après une cyberattaque.

↓

**Son contenu**

- Évaluation des incidents potentiels,
- Recherche de parades,
- Déploiement de sauvegardes.

### Les bons gestes à adopter

- Effectuer les mises à jour des antivirus et des logiciels,
- Maîtriser les accès internet,
- Modifier régulièrement les mots de passe,
- Sensibiliser les collaborateurs,
- Évaluer l'opportunité de souscrire un contrat d'assurance pour couvrir le risque Cyber (Fiche 10 guide Assurances FNTP).

### Soyez organisés !

Les sauvegardes ne suffisent pas. Il faut restaurer vos données et vos processus dans l'ordre. Faites appel à un prestataire extérieur si nécessaire.

**L'entreprise est toujours responsable de ses données, quel que soit le prestataire auquel elle fait appel pour les héberger.**

+ d'infos

LES TRAVAUX PUBLICS FÉDÉRATION NATIONALE

LES MÉMOS
JURIDIQUE - MARCHÉS : 4

# Cybersécurité des entreprises

Juillet 2021

## EN CAS D'ATTAQUE


**Ayez recours à une assistance technique si nécessaire !**
L'entreprise peut solliciter l'aide d'un professionnel référencé par le dispositif « Cybermalveillance».

### NE PAS PAYER LA RANÇON

**En cas de demande de rançon, deux règles :**

- Se rapprocher de son assureur (si police cyber),
- Se rapprocher de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

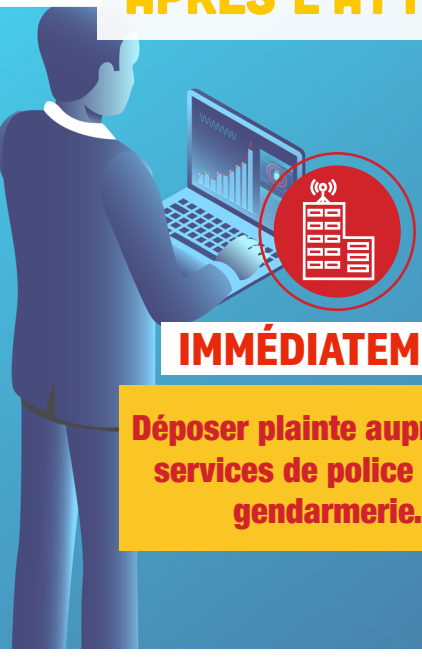
### MESURES TECHNIQUES

- Déconnecter les supports de sauvegarde,
- Isoler les équipements infectés des services informatiques,
- Bloquer les communications internet,
- Déconnecter les équipements sans fil,
- Ne pas éteindre le matériel affecté,
- Restaurer les systèmes depuis des sources saines.

### MESURES ORGANISATIONNELLES

- Mettre en place une cellule de crise,
- Déployer la communication interne et externe vis-à-vis des clients,
- Accompagner les collaborateurs,
- Réaliser un retour d'expérience sur la gestion de la crise.

## APRÈS L'ATTAQUE



### IMMÉDIATEMENT

**Déposer plainte auprès des services de police ou de gendarmerie.**

### PENSER AUX DONNÉES PERSONNELLES DE L'ENTREPRISE

- La destruction de données personnelles, y compris accidentelle, constitue une violation de données au sens du RGPD (règlement général sur la protection des données).
- Le signalement de la destruction de ces données à la CNIL est nécessaire :
  - en cas de perte définitive de données personnelles,
  - ou si les données sont restées indisponibles suffisamment longtemps.

### COMMENT RESTAURER SES DONNÉES ?

En les récupérant à partir des sauvegardes que l'entreprise aura effectuées elle-même ou via ses prestataires.

+ d'infos

LES TRAVAUX PUBLICS FÉDÉRATION NATIONALE