

Rançongiciel : les verrous avant toute rançon

Arbre de gouvernance à préparer avant l'incident. La doctrine de l'ANSSI reste : ne jamais payer.

Un paiement n'est jamais une garantie de reprise ni d'effacement. Chaque porte doit être documentée avant que l'option puisse seulement être examinée.

1

Sécurité immédiate - Une personne ou une fonction vitale est-elle menacée ?

OUI : Activer le mode dégradé et les secours ; la continuité prime.
NON : Poursuivre sans adopter l'horloge de l'attaquant.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

2

Confinement - Les accès de l'attaquant sont-ils coupés et les preuves préservées ?

OUI : Passer à la qualification juridique et métier.
NON : Aucune décision de paiement ; contenir et conserver les traces.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

3

Obligations - Plainte, assureur et analyse RGPD sont-ils engagés dans leurs délais ?

OUI : Joindre les récépissés et décisions au dossier de crise.
NON : Déclencher immédiatement les démarches applicables.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

4

Reprise - Les sauvegardes critiques sont-elles restaurables et le délai de reconstruction chiffré ?

OUI : Privilégier la reconstruction par lots métier.
NON : Chiffrer RTO, coûts d'arrêt et solutions dégradées.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

5

Légalité - L'avocat a-t-il validé par écrit sanctions, gel d'avoirs, financement et compétence de l'organe décideur ?

OUI : L'option peut être soumise au comité compétent.
NON : Paiement interdit jusqu'à levée documentée de chaque obstacle.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

6

Bénéfice vérifiable - Une capacité indisponible autrement est-elle démontrée sur échantillon ?

OUI : Comparer ce bénéfice au scénario de reconstruction et au risque résiduel.
NON : Refuser le paiement ; reprendre, notifier et communiquer.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

7

Décision formelle - L'organe compétent accepte-t-il l'absence de garantie et le risque de récidence ?

OUI : Consigner décision, avis, plan B et responsabilités.
NON : Ne pas payer ; décision et priorités de reprise consignées.

TRACE A CONSERVER

Décision, responsable, heure, preuve technique ou juridique.

Doctrine publique : l'ANSSI recommande de ne jamais payer. Pour une entité publique, aucun paiement ne doit être effectué. Le présent arbre organise la preuve, la continuité et la responsabilité ; il ne transforme pas le paiement en solution recommandée.