Ransomware et démarches

Par agi

Bonjour,

Mon entreprise a été victime d'un ransomware il y a quelques mois.
Les accès aux serveurs ont été coupés pendant presque 1 mois: la seule explication pour nous et pour les clients a été un "problème informatique". Nous n'avons pas été informé officiellement mais oralement par des managers à la pause café quelques semaines après. Toutes les données de nos serveurs ont été touchées. La rumeur dit qu'une rançon a été payée.

Le règlement RGPD prévoit que nous devons prévenir nos clients en cas d'attaque informatique. Tout a été gardé secret alors que nos serveurs hébergent des données sensibles des clients (données personnelles de leurs employés, bulletins de salaires, informations financières...).

J'ai plusieurs questions. Quelle devrait être l'attitude de nos dirigeants dans cette situation:
- vis à vis des autorités? Est ce qu'une plainte est obligatoire? Quels sont les risques s'ils cachent cette attaque?
- vis à vis des clients? Quels sont les risques s'ils ne préviennent pas les clients?
- vis à vis des employés? Est ce que nos données personnelles sont compromises? Est ce qu'ils ont une obligation d'information?

Est ce qu'à titre individuel nous avons des démarches à faire?

Merci!

Par ESP

Bonjour
Je laisse à vos dirigeants la responsabilité de vous dire ce qu'ils ont fait ou pas sur le plan relations professionnelles, mais l'une des recommandations est de La notifier la violation à la CNIL dès qu'il y a un risque pour la vie privée des personnes.

Il est aussi recommandé de faire un signalement au ministère de l'intérieur, via ce formulaire.
[url=https://www.internet-signalement.gouv.fr/PortailWeb/planets/SignalerEtapeAccepter!load.action;jsessionid=87D248E4A890A31C45E0723ED2335597.route2]https://www.internet-signalement.gouv.fr/PortailWeb/planets/SignalerEtapeAccepter!load.action;jsessionid=87D248E4A890A31C45E0723ED2335597.route2[/url]