Mathias | Avocats

CE DOCUMENT EST FOURNI À TITRE PUREMENT INFORMATIF ET NE CONSTITUE EN AUCUN CAS UN CONSEIL JURIDIQUE

QUE FAIRE SI VOTRE ORGANISATION EST VICTIME D'UN RANÇONGICIEL ?

WWW.AVOCATS-MATHIAS.COM

CONTACT@AVOCATS-MATHIAS.COM

Mathias | Avocats

Qu’est-ce qu’un rançongiciel ?

Qu’est-ce qu’un rançongiciel ?

Une attaque par rançongiciel ou ransomware est une attaque qui consiste a **compromettre l’accès a un équipement ou un système d’information**, afin d’en **bloquer l’accès et d’en chiffrer les données.**

Pour l’attaquant, l’objectif est de **réclamer une rançon** à la victime en échange de les rendre de nouveau accessibles et de ne pas les divulguer.

Causes de l’attaque

Ce type d’attaque est **consécutif à une intrusion** qui peut résulter notamment de failles de sécurité, d’un hameçonnage ou encore de virus.

Périodicité de l’attaque

De manière générale, les attaques sont déclenchées pendant les **périodes de moindre activité**, nuit, Week-end, …

Pressions Multiples

L’attaque peut **s’accompagner d’autres moyens de pressions:** revendication publique de l’attaque, communication auprès de clients administrés, attaque par dénis de service contre le site internet de la victime.

Conséquences de l’attaque

Elle peut aboutir à une **paralysie totale de l’activité de l’organisation victime** en fonction de son ampleur.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Mathias | Avocats

Comment protéger votre organisation ?

1. Réalisez des **sauvegardes régulières** de vos données, systèmes et applications critiques, en gardant des copies déconnectées, et en vérifiant périodiquement le bon fonctionnement de leur restauration.

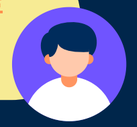
2. Appliquez de manière **régulière et systématique** les mises à jour de sécurité.

3. Utilisez une **solution de protection** contre les programmes et comportements malveillants (antivirus, EDR, XDR, ...).

4. Utilisez un pare-feu pour **protéger les accès extérieurs** à votre réseau informatique interne.

5. **Sécurisez les accès distants** à votre réseau informatique interne en utilisant un VPN et systématisez l'emploi d'une **double authentification.**

6. Limitez les droits de tous les utilisateurs selon le **"principe de moindre privilège"**.



7. Utilisez des mots de passe suffisamment **longs, complexes et différents** pour chaque service.

8. N'installez pas d'applications ou de logiciels **"piratés".**

9. **Sensibilisez** l'ensemble de vos collaborateurs aux **risques** et rappelez régulièrement les **consignes de sécurité.**

10. **Supervisez la sécurité** de votre système d'information.

11. **Renforcez la sécurité** de vos interconnexions à internet.

12. **Segmentez** votre réseau informatique.

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Mathias | Avocats

Que faire en cas d'attaque par rançongiciel ?

1. Coupez les connexions à internet du réseau attaqué

2. Identifiez et déconnectez les machines attaquées du réseau informatique

3. N'éteignez pas les machines touchées

4. Ne démarrez pas les machines éteintes

5. Alertez immédiatement votre service ou prestataire informatique si vous en disposez

6. Coupez les connexions à internet du réseau attaqué : Constituez une équipe de gestion de crise, tenez un registre des évènements et actions réalisées, gérez votre communication , mettez en œuvre des solutions de secours

7. Ne payez pas la rançon

8. Conservez ou faites conserver les preuves par un professionnel

9. Déposez plainte au commissariat de police ou a la brigade de gendarmerie, ou en écrivant au procureur de la république du tribunal judiciaire

10. Déclarez votre sinistre auprès de votre assureur qui peut vous dédommager

11. Notifiez impérativement l'incident à la CNIL dans les 72H si des données personnelles ont pu être consultées, modifiées, ou détruites

12. Identifiez l'origine de l'attaque

13. Identifiez les activités de l'attaquant au sein de votre système informatique

14. Évaluez et vérifiez l'étendue de l'intrusion à d'autres appareils ou équipements de votre système informatique

15. Réalisez une analyse antivirale complète (scan)

16. Recherchez si une solution de déchiffrement existe (site No More Ransom d'Europol)

17. Réinstallez les systèmes touchés

18. Changez tous les mots de passe

19. Après la réinstallation de vos systèmes et avant de les remettre en service, mettez à jour l'ensemble de vos logiciels et de vos équipements

20. Faîte une remise en service progressive et contrôlée

Source : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/rancongiciels-ransomwares

Mathias | Avocats

Qui contacter ?

Contacter le 17 CYBER

17 CYBER
Mon assistance en ligne

Contacter la CNIL

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Déclarer l'incident au CERT-FR

CERT-FR

Gendarmerie nationale

POLICE NATIONALE

Mathias | Avocats

Indemnisation des préjudices matériels quelles pièces fournir ?

Frais d'assistance et d'expertise engagés à l'occasion de la crise

- Frais d'avocats
- Frais d'expertise (recherche de preuves techniques, restauration des données etc.)
- Accompagnement pour la communication de crise
- Frais d'huissier etc.

Frais engagés pour la gestion interne de la crise

- Temps passé par les équipes internes mobilisées (heures supplémentaires, astreintes etc.)

Frais relatifs à l'éventuelle communication à destination des personnes concernées

- Frais d'envoi de mails et de courriers
- Frais de création d'un message d'alerte sur le site web
- Etc.

Pièces justificatives à produire : Factures, relevés de compte attestant du paiement des factures, journal des achats attestant de l'acquittement des factures.

GESTION DE VOS RISQUES JURIDIQUES, MISE EN CONFORMITÉ, SENSIBILISATION ET FORMATION, CONTACTEZ-NOUS !

DES ***FORMATIONS*** SUR-MESURE POUR VOUS ET VOS EQUIPES :

Voir le catalogue des formations

Mathias | Avocats

SUIVEZ VOTRE ACTUALITÉ, ABONNEZ-VOUS !

UNE NEWSLETTER MENSUELLE OFFERTE

Mathias | Avocats

MARS 2024

Newsletter

VOUS AVEZ PEUT-ÊTRE MANQUÉ...

IA et charte informatique : un impératif juridique et opérationnel

L'émergence des IA génératives, comme ChatGPT, et leur adoption croissante dans les activités professionnelles, justifient la nécessité d'encadrer spécifiquement leurs usages.

Les risques associés à l'utilisation de ces technologies, comme la divulgation de données confidentielles, les atteintes aux droits de propriété intellectuelle, les biais cognitifs, ou encore la diffusion d'informations inexactes, exigent une régulation adaptée.

EN SAVOIR

Usage devant le juge civil de la preuve obtenue de façon déloyale

Ces deux pourvois en cassation portaient sur l'admissibilité des preuves recueillies par l'employeur afin de justifier le licenciement d'un salarié.

Que nous enseignent ces deux arrêts, rendus le 22 décembre 2023, par la Cour de cassation, réunie en assemblée plénière ?

Quelles sont les conditions de

EN SAVOIR

Mathias | Avocats

VOS BRÈVES

Ces Brèves vous sont offertes par Mathias Avocats.
Nous sommes à votre disposition pour échanger sur vos brèves personnalisées.

Bons Réflexes : Dépôt de plainte auprès du Procureur de la République

Lorsque vous êtes victime d'une cyberattaque, la plainte peut être déposée directement auprès du Procureur de la République par courrier recommandé. Cette démarche est régie par **l'article 40-1 du Code de procédure pénale** qui assure que toute plainte sera examinée par l'autorité judiciaire compétente. Seul le dirigeant représentant de la personne morale, ou une personne ayant une délégation de pouvoir à cet effet, peut déposer plainte au nom de la personne morale.

Rôle du Procureur de la République : Le Procureur représente les intérêts de la société et est chargé de l'application de la loi, disposant de l'autorité pour initier des actions publiques contre les auteurs présumés d'infractions pénales.

Motifs et contenu de la plainte : La plainte doit inclure notamment l'identité du plaignant (si possible), une description détaillée des faits (date, lieu, nature de l'infraction, dommages subis), la description du préjudice et tout élément susceptible d'aider l'enquête.

Procédure de dépôt : La plainte peut être envoyée par lettre recommandée avec accusé de réception au Procureur du tribunal compétent, ou déposée directement au greffe du tribunal. Il est recommandé de conserver une copie de tous les documents envoyés.

Suites du dépôt de plainte : Un dépôt de plainte peut être complété lorsqu'il y a des éléments nouveaux (en rappelant les références de la plainte initiale). Le Procureur décide de la suite à donner : classement sans suite, enquête préliminaire, citation directe au tribunal, ou autres mesures alternatives. En cas de classement sans suite, le plaignant peut se constituer partie civile.

Avantages

- Protection des intérêts de votre entreprise.
- En se constituant partie civile, vous pouvez demander des dommages et intérêts si l'affaire aboutit à un procès.
- Le dépôt de plainte peut être l'occasion pour l'entreprise de se faire accompagner par un avocat, permettant ainsi une meilleure qualification juridique des faits et une présentation claire de l'infraction au Procureur et un suivi de la procédure.

1

L'ACTUALITÉ DÉCRYPTÉE POUR VOUS !

VOIR LES ARTICLES DU **BLOG**

ENSEMBLE, DÉVELOPPONS VOS PROJETS
ET FORMONS VOS ÉQUIPES !
PARTAGEONS NOS EXPERTISES !

AU QUOTIDIEN

CONSULTER NOTRE ARTICLE SUR LE DÉPÔT DE PLAINTE EN CAS DE CYBERATTAQUE

Mathias | Avocats