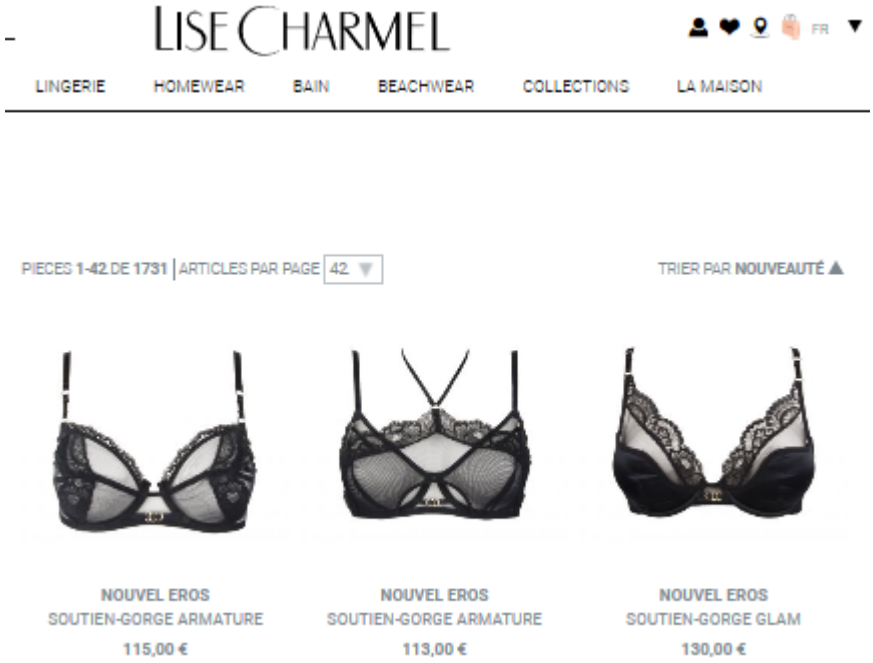
Date : 19/03/2020
Heure : 15:27:26
Journaliste : Juliette Paoli

www.solutions-numeriques.com
Pays : France
Dynamisme : 11

Visualiser l'article

Juridique – Ransomware : Lise Charmel a trouvé « un nouveau moyen de protection a posteriori face au chantage »



En novembre, un ransomware a pris en otage toutes les données de l'entreprise en échange d'une clé permettant de les déchiffrer. Le groupe n'a pas cédé au chantage et a décidé de se placer en redressement judiciaire par protection fin février . Que signifie le placement en redressement judiciaire par protection ? Il y a-t-il une possibilité de poursuite à l'encontre du cyber-pirate ? Solutions Numériques à poser ces questions à Mélanie Erber, Avocat associé au sein du cabinet **Coblence** avocats.

Solutions Numériques : Que signifie le placement en redressement judiciaire par protection pour une entreprise ?

Mélanie Erber : Le groupe lyonnais Lise Charmel a subi une cyberattaque massive le 8 novembre 2019. Un logiciel informatique malveillant (« ransomware ») a pris en otage toutes ses données en échange d'une clé permettant de les déchiffrer, bloquant ainsi les 1 150 collaborateurs à travers le monde. Cette cyberattaque a vraisemblablement désorganisé l'entreprise pendant plusieurs mois, de sorte qu'elle n'a pas été en mesure de poursuivre normalement son cycle d'exploitation et de facturer et encaisser normalement.

Il a dû en résulter une tension de trésorerie et un état de cessation des paiements, l'entreprise ne pouvant plus payer tout ou partie de ses dettes exigibles. Dans ce cas, le redressement judiciaire permet de geler son passif antérieur à l'ouverture de la procédure pendant la durée de la période d'observation (12 mois en principe, avec prolongation exceptionnelle à 18 mois). Le redressement judiciaire met également pendant cette période l'entreprise à l'abri des poursuites de ses créanciers (d'où le terme de protection) le temps d'établir un plan de redressement qui va permettre de rembourser les créanciers sur une durée maximale de 10 ans.

Tous droits réservés à l'éditeur

Le redressement judiciaire protège donc l'activité de l'entreprise et permet de lisser le remboursement de la dette, le temps d'assurer le rebond de l'activité et de passer la période de tension de trésorerie.

Il y a-t-il une possibilité de poursuite à l'encontre du cyber-pirate? Que risque-t-il s'il est identifié ?

La difficulté liée à la poursuite des cyber-pirates résulte du fait qu'ils sont souvent difficiles à retrouver. C'est pour cette raison que la Convention Cybercriminalité du Conseil de l'Europe a été adoptée à Budapest le 23 novembre 2001 afin de créer une véritable coopération entre les pays l'ayant ratifiée (en 2017, elle était ratifiée par 27 pays, dont la France et l'Allemagne).

Si par chance ils sont identifiés, la plainte permet d'engager leur responsabilité pénale. La loi Godfrain du 8 janvier 1988, complétée par la loi LOPPSI 2 du 14 mars 2011, permet de sanctionner toutes les intrusions non autorisées dans un système informatique. Ainsi, l'article L.323-1 du Code Pénal prévoit que « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende ».

En outre, les dispositions du Code pénal relatives à des infractions classiques comme le vol (vol de données), l'escroquerie (utilisation frauduleuse de données bancaires), l'abus de confiance, le détournement de fonds, le chantage, l'extorsion de fonds… peuvent trouver à s'appliquer aux cyber-pirates.

« La société Lise Charmel a été pour le moins audacieuse en trouvant un nouveau moyen de protection a posteriori face à ce chantage en se plaçant en redressement judiciaire pour se protéger. Elle n'a pas cherché à engager la responsabilité des auteurs mais à trouver une solution pour ne pas céder à leurs demandes. Cela donnera probablement des idées aux prochaines victimes de ces agissements » , Mélanie Erber

Tous droits réservés à l'éditeur

Face à la difficulté de retrouver les auteurs de ces agissements, que conseillez-vous comme précautions ?

Sur le plan technique, en plus d'avoir recours à des antivirus, il faut rester vigilant quant aux mails reçus afin de refuser certains types de fichiers et effectuer des sauvegardes régulièrement sur des périphériques externes. Sur le plan juridique , il faut mettre en place une protection des données personnelles en adoptant des mesures adéquates consistant notamment dans l'installation de pare-feu, le contrôle des connections entrantes, l'utilisation du chiffrement ou encore des systèmes d'authentification pour accéder aux composants du système d'information.

Il est rappelé que le fait de traiter des données personnelles sans mettre en œuvre de mesures adéquates face à type d'attaque est pénalement sanctionné. En outre, depuis l'entrée en vigueur du règlement général sur la protection des données personnelles (RGPD), les responsables de traitement sont tenus de notifier à la CNIL les violations des données personnelles subies. Ils doivent également informer les personnes concernées de cette violation et leur spécifier s'il existe un risque d'atteinte à leur vie privée.

Tous droits réservés à l'éditeur