

Package Technologies

Étude de cas : attaque par rançongiciel



L'assuré est un éditeur de logiciels. Son chiffre d'affaires annuel s'élève à **15 millions d'euros**.



Jour de l'incident

Durant le week-end, un fichier malveillant infecte les serveurs de la société et se propage à l'ensemble des fichiers, affectant ainsi les données des projets en cours.



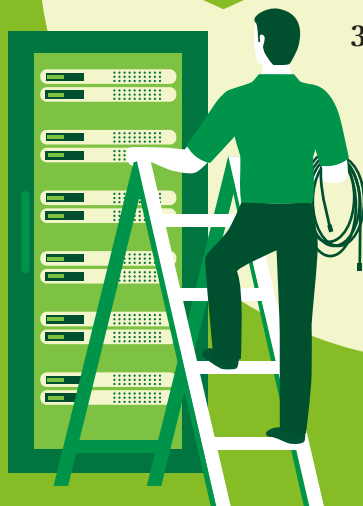
L'équipe d'intervention de Chubb apporte son aide à l'assuré et met en œuvre une stratégie d'atténuation : identification des serveurs les moins critiques qui pourront être restaurés à partir de sauvegardes, et négociation du montant de la rançon pour libérer les serveurs indispensables au fonctionnement de l'entreprise.

L'assuré signale l'incident et est mis en contact le jour même avec le responsable de l'équipe d'intervention. Une société d'investigation informatique est immédiatement envoyée.



Ses serveurs étant en panne, l'assuré ne peut pas honorer les commandes de ses clients. La perte d'exploitation est estimée à plus de **125 000 euros** par jour.

Le hacker exige une rançon pour décrypter chaque serveur, et indique que le montant de la rançon augmentera si le paiement n'est pas effectué dans les 2 jours.



3 jours après l'incident

L'équipe d'intervention élimine le rançongiciel des serveurs affectés. Ainsi, la société peut être opérationnelle à 70 % de ses capacités normales. L'équipe d'intervention mandate également une société spécialisée dans la gestion de crise pour faciliter la communication avec les clients.

Des conseillers juridiques aident l'assuré à déposer une plainte pénale officielle ainsi que d'autres documents réglementaires.

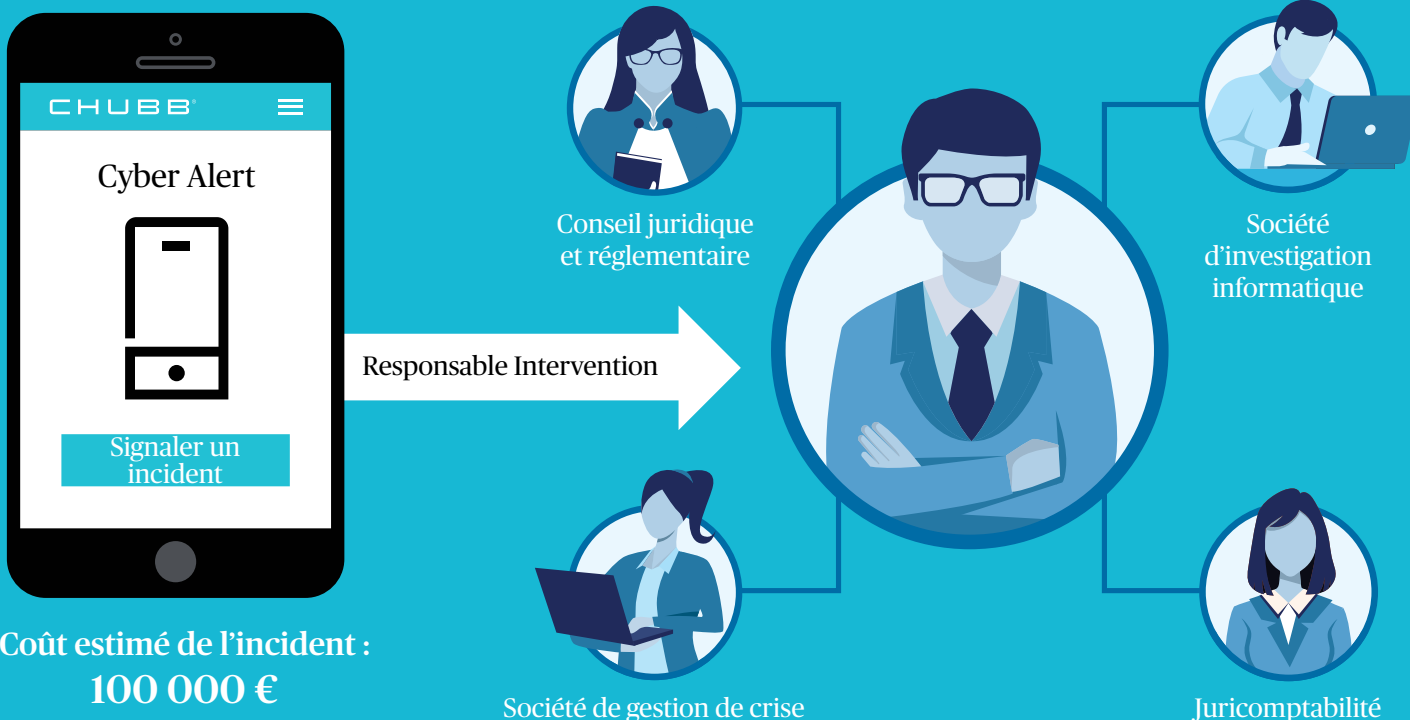


10 jours après l'incident

Les opérations reprennent à 100%.

La société d'investigation informatique fournit à l'assuré un rapport d'incident assorti de recommandations pour renforcer sa cybersécurité et prévenir les futurs incidents.

Cet incident cyber a été signalé via l'application mobile Cyber Alert de Chubb. Disponible 24/7, tous les jours de l'année. Elle peut être téléchargée directement depuis l'App Store (pour les iPhone) ou Google Play Store (pour les appareils Android) en recherchant « Chubb Alert ». Les intervenants suivants ont été mobilisés pour prendre en charge rapidement l'incident cyber.



Couverture

Les couvertures Réponse aux incidents et Cyber-extorsion sont d'abord déclenchées en réponse à l'incident cyber, mais la procédure d'intervention relève aussi d'autres garanties.

