

EY Cyber

Ransomware : Pourquoi et comment négocier avec un hacker

Octobre 2019

Olivier HERISSON, Manager en sécurité numérique



The better the question. The better the answer.
The better the world works.



CONTEXTE

1

Une conduite à tenir

- ▶ Ne pas payer la rançon.

2

Une réalité bien différente....

- ▶ Quelques exemples

3

Une expérience a partager

- ▶ Des exemples réels.
- ▶ Proposer quelques outils



A man in a blue shirt and dark pants is climbing a large, circular, grid-like structure. The structure is made of a white grid pattern and is set against a sunset sky with a large, bright sun. The man is positioned on the right side of the structure, reaching up with his right hand. The overall scene is dramatic and evokes a sense of achievement and challenge.

LE THÈME

v



Votre sous-traitant en charge de l'application « gestion de la paie » (mode SaaS) vous annonce qu'il vient d'être victime d'une attaque de type Ransomware. Le malware a chiffré l'ensemble de la base contenant les données des fiches de paie de vos salariés (3000 personnes concernées) :

- ▶ **Le hacker affiche sur les écrans son adresse email permettant de le contacter.**
- ▶ **Vous avez 24h pour payer 20 bitcoins. Passé ce délai les données seront détruites.**
- ▶ **Vos dernières sauvegardes ont 6 mois.**
- ▶ **Le malware est connu sur « nomoransom » mais la souche a été modifiée !**



Aucune ressemblance avec des cas vécus par des participants présents dans la salle est fortuite !

LA NÉGOCIATION



POURQUOI NEGOCIER ?

Gagner du temps

L'intérêt de
négocier

Diminuer l'impact
Business

Diminuer l'impact sur la vie
privée

Répondre à
l'incident

Organiser,
déclencher la
cellule de crise

Organiser la
reprise d'activité

Diminuer le
montant de la
rançon

Empêcher la
diffusion

Prévenir les
victimes

The image features a person climbing a large, circular metal structure, possibly a dome or a large-scale architectural element. The person is silhouetted against a bright, circular light source in the background, creating a dramatic effect. A large, yellow-outlined diamond shape is superimposed over the center of the image. Inside this diamond, the text "RISQUE JURIDIQUE ?" is written in white, bold, sans-serif capital letters. The overall scene is dark, with the primary light source being the bright circle behind the climber.

RISQUE
JURIDIQUE ?



LA CELLULE DE CRISE
CYBER

COMMENT S'ORGANISER ?

1

Identifier les différents acteurs

- En fonction de votre société
- Le coordinateur
- Le négociateur
- Le décideur

Coordonner, Décider, agir

- Piloter
- Communiquer efficacement
- Relation avec les autorités
- Remédier

3

2

Intégrer le Data Protection Officer,

- Gestion de la violation de données à caractère personnel
- Analyse des risques sur la vie privée (AIVP)
- Communication ?

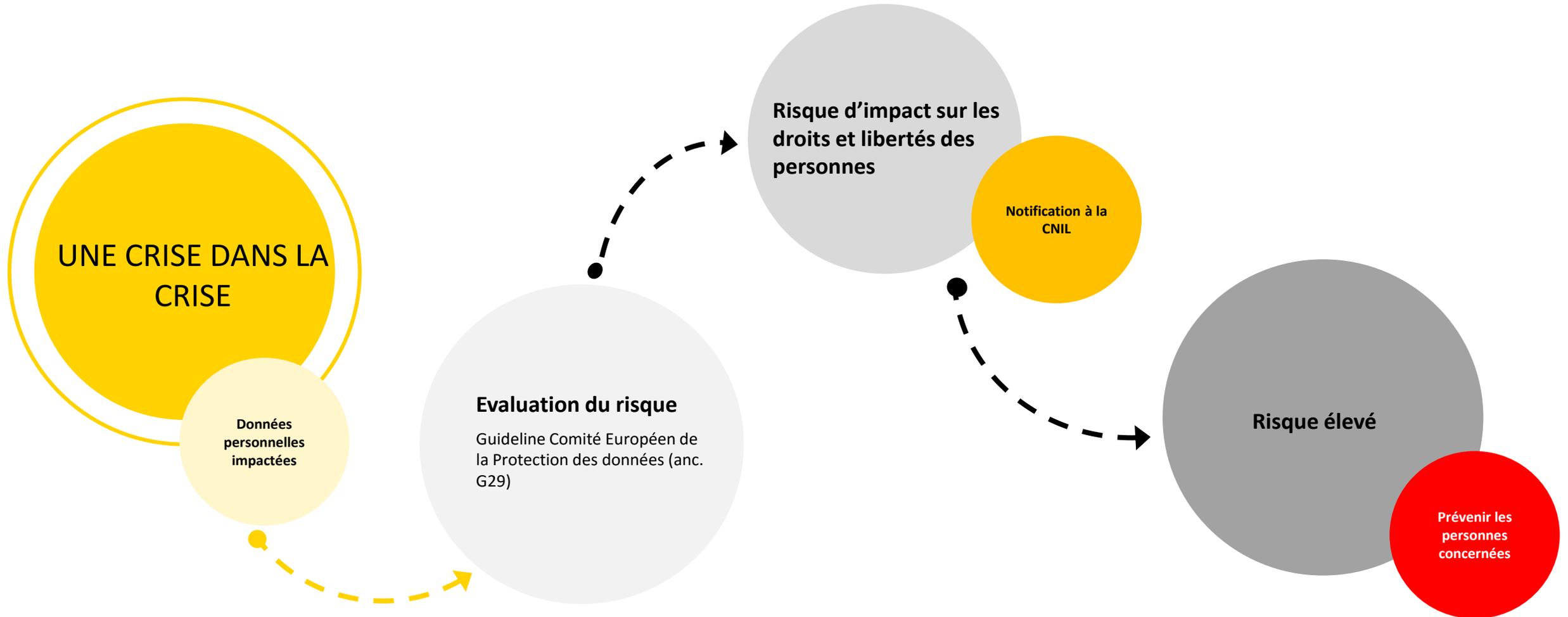
Clôturer l'incident

- Débriefer
- Capitaliser

4



ZOOM SUR LE RÔLE DU DATA PROTECTION OFFICER (DPO)



Guideline CEPD*

- *DICP, nature et sensibilité des données, volume des données*
- *Faciliter d'identification des personnes concernées, sévérité des conséquences pour les personnes, caractéristiques spéciales des personnes*
- *Nombre de personnes concernées, caractéristiques spéciales du RT, contexte général et vraisemblance.*



COMMENT
NÉGOCIER ?

CONSEILS POUR OPTIMISER LA NÉGOCIATION

1

Le décideur ne négocie pas !

- ▶ Le décideur en retrait, définit la stratégie.
- ▶ Inflation narcissique (Cf. Laurent Combalbert, ADN)
- ▶ Perte de l'effet fusible, situation de confort

2

Mettre son égo dans sa poche

- ▶ Le hacker est en position de force
- ▶ Ne pas montrer l'inversion du rapport de force

3

Définissez votre stratégie

- ▶ Le mandat du négociateur
- ▶ Parler de la tactique ?

4

Différencier la position, l'objectif et l'intérêt

- ▶ Position affichée : 20 btc, (l'ultimatum n'est qu'un moyen de pression)
- ▶ Parler du Ransomware auto vs vol de données (ubber)

STRATEGIE

ROLE

PREPARATION

CONSEILS POUR OPTIMISER LA NÉGOCIATION

5

Protéger votre intérêt !

- ▶ Tous les moyens sont bons ...

6

Poser des questions

- ▶ Collecter de l'information sur votre adversaire (connectivité, verbatim, profil)
- ▶ L'égo du hacker.....

7

Créer un lien avec le hacker

- ▶ Dédiabolisation
- ▶ Visualisation et empathie

8

Diminuer l'enjeu

- ▶ Pour moi négociateur, quels sont mes risques ?

ENJEU

RELATION

INTERET

POUR RÉSUMER :



ANTICIPATION

PREPARATION

CAPITALISATION

A man in a blue shirt and dark pants is climbing a large, spherical structure covered in a white grid pattern. The structure is illuminated from behind, creating a bright glow. A large, semi-transparent diamond shape is overlaid on the center of the image, with a yellow border. The word "MERCI" is written in white capital letters inside the diamond. A small black 'v' is located at the bottom vertex of the diamond.

MERCI

EY | Audit | Conseil | Fiscalité & Droit | Transaction

EY est un des leaders mondiaux de l'audit, du conseil, de la fiscalité et du droit, des transactions. Partout dans le monde, notre expertise et la qualité de nos services contribuent à créer les conditions de la confiance dans l'économie et les marchés financiers. Nous faisons grandir les talents afin qu'ensemble, ils accompagnent les organisations vers une croissance pérenne. C'est ainsi que nous jouons un rôle actif dans la construction d'un monde plus juste et plus équilibré pour nos équipes, nos clients et la société dans son ensemble.

EY désigne l'organisation mondiale et peut faire référence à l'un ou plusieurs des membres d'Ernst & Young Global Limited, dont chacun est une entité juridique distincte. Ernst & Young Global Limited, société britannique à responsabilité limitée par garantie, ne fournit pas de prestations aux clients. Retrouvez plus d'informations sur notre organisation sur www.ey.com.

© 2018 EY Advisory.
Tous droits réservés.

Studio EY France – 1802SG126
SCORE France N°2018-23
ED 042018

Document imprimé conformément à l'engagement d'EY de réduire son empreinte sur l'environnement.

Cette publication a valeur d'information générale et ne saurait se substituer à un conseil professionnel en matière comptable, fiscale ou autre. Pour toute question spécifique, vous devez vous adresser à vos conseillers.

ey.com/fr

