

Chérie, je ne rentrerai
pas à la maison ce soir

(Ce n'est pas ce que vous croyez)



Suivre @AlexArchambault

Alexandre Archambault

FRnOG 32



Alors, voilà, je ne rentrerai pas ce soir
Promis, je t'expliquerai



La réalité : je viens de me faire trouer la prod

Promis, je gère



En fait, c'est plutôt ça

Car oui, on est en France

Je comprends pas, on avait tout prévu pourtant

- On détecte régulièrement les méchantes attaques et on sait les mettre en échec (par contre, les attaques de JeanKevin, au bout d'un moment, on n'y prête plus attention)
- On fait gaffe à ce qu'on raconte sur Facebook (par contre, sur LinkedIn et dans les salons, c'est open bar)
- On sauvegarde régulièrement (par contre on n'a pas eu le budget pour les compartimenter et on a pas le temps de les inspecter)



Ce qu'il fallait / faut / faudra faire

- DO-CU-MEN-TER
- SAU-VE-GAR-DER (et inspecter régulièrement l'intégrité des sauvegardes tant qu'à faire)
- NO-TI-FI-ER
- Geler la scène en dupliquant si possible les ressources concernées sur une plateforme isolée
- Inspecter les sauvegardes avant de remettre en prod
- Si vous êtes OIV / OSE, implantez votre NOC / cellule de crise à minimum 1 heure de portée d'un Ministre

Notifier sans tarder

- Notification auprès des autorités compétentes : CNIL et ANSSI
- Et SANS TARDER (art. 33 & 34 RGPD)
 - Délai contraint pour la CNIL : 72 h
 - Peut s'effectuer en ligne <https://notifications.cnil.fr/notifications/index>
 - Jusqu'à 5 ans d'emprisonnement & 300 000 € d'amende en cas d'absence de notification (art. 226-18 code pénal)
- Avec le cas échéant information des personnes concernées

Les bons réflexes à adopter

- Mettre d'emblée le juridique (soit en interne, soit en externe) dans la boucle. Ah, et aussi le DPO. Si si si
- Savoir s'entourer : <https://www.cybermalveillance.gouv.fr>
- Ne JAMAIS se faire justice soi-même, ni jouer aux cow-boys pour les recherches de preuves
- Maîtriser la communication : communiquer mais uniquement sur ce qui est strictement nécessaire et sans compromettre les investigations
- La question de l'attribution : la laisser aux autorités compétentes

La riposte juridique : pénal ou civil ?

- Pour des dossiers à implication internationale, le pénal (sur la base des art. 323-1 et suivants du Code pénal) peut être une option pour obtenir une coopération internationale sur l'enquête
- Pour des dossiers nationaux ou avec des implications anticoncurrentielle, la piste civile peut être à privilégier
- Bien discuter de ces options avec le juridique / DPO et, le cas échéant, le conseil

Les outils juridiques existants

- Juridiquement, se faire trouer la prod, cela s'appelle une atteinte à un système automatisé de traitement de données (STAD)
 - ➔ Articles 323-1 et suivants du Code pénal
- Au civil / commercial la procédure de l'art.145 du Code de procédure civile (CPC) peut être très utile pour disposer des preuves nécessaires afin d'obtenir une réparation du préjudice
 - ➔ Aussi bien pour saisir des informations chez le suspect que pour obtenir des logs & identifications chez des prestataires

Mais une chaîne pénale loin d'être optimale

- Le dépôt de plainte au commissariat du coin est à proscrire pour ce type de sujets
- Bienheureuses les sociétés dont le siège est situé dans le ressort de la Préfecture de Police de Paris : la BEFTI est en pointe sur la connaissance de ces sujets
- Partir au pénal, c'est ne plus maîtriser la procédure (notamment les délais) ainsi que l'exposition médiatique qui en découlera, le procès étant public



Focus procédure Art. 145 CPC

- *« s'il existe un motif légitime de conserver ou d'établir avant tout procès la preuve de faits dont pourrait dépendre la solution d'un litige, les mesures d'instruction légalement admissibles peuvent être ordonnées à la demande de tout intéressé, sur requête ou en référé. »*
- Permet de réunir des éléments de preuve qui feront la différence
 - ➔ soit directement chez l'adversaire, en faisant intervenir huissier & expert informatique
 - ➔ soit auprès d'un prestataire technique : hébergeur, prestataire de paiement, datacenter, FAI...
- Procédure rapide : entre 1 et 2 mois (selon complexité) entre le jour de l'ordonnance et la récupération effective des pièces chez l'huissier

Des questions ?

C'est notre Raïs à nous : c'est Monsieur Guillaume Poupard. Un grand homme. Il marquera l'Histoire. Il aime les barbes, les sweets à capuche, les PME qui codent à la rache, les trolls du vendredi... c'est donc ton ami. Ce sera ton porte-bonheur.

