Le retour de la « Panic Room »

Hervé MORIZOT
Co-fondateur et Directeur général
FORMIND

Dans un monde digital, une entreprise ayant perdu ses données est une entreprise morte.

Ce risque semble progresser plus vite que les mentalités et les solutions

Le risque de perte pure et simple de données est apparu très récemment dans les cartographes des risques de nos entreprises. Il était globalement absent des radars jusqu'en 2015 – 2017. Remercions notamment Saint-Gobain qui, en évoquant une perte d'environ 250 M€ de CA et de 80 M€ de résultat d'exploitation avec NotPetya, a commencé à sensibiliser le marché.

L'année 2020 connait d'ailleurs une augmentation particulièrement forte de ces ransomware.

Il devient même « le risque » majeur Cyber

Autrefois limités aux fameux DICT (…), l'indisponibilité du SI ou des données se bornait bien souvent à des délais d'accès allongés, de quelques heures ou quelques jours… parfois avec des restaurations de sauvegardes qui engendraient des pertes ponctuelles de données.

Or l'ampleur des moyens mis en œuvre par les attaquants a décuplé depuis cette date, et le niveau de technicité des attaquants a largement cru.

L'objectif majeur des attaquants est de bloquer une activité, une entreprise, un état, tant que les conditions demandées ne sont pas réunies (généralement une rançon pour les entreprises, des actes politiques pour les administrations et états,…).

La perte de données au-delà du blocage « ponctuel » de leur accès est donc leur « graal ».

Et bien évidemment, le fait de payer ne garantit pas de retrouver ses données…

Les régulateurs ont bien compris cela, et leurs exigences de disponibilité des données sont croissantes.

L'enjeu est de taille pour les attaquants

Les Mafias et autres bandes organisées ont, elles aussi, engagé de réelles transformations digitales !

Le coût des attaques Cyber a dépassé depuis près de 10 ans ce que rapporte les trafics de drogue sur un plan mondial. Ce coût devrait bientôt avoisiner les 1 000 milliards de dollars (estimation de 600 milliards en 2017 – *source PwC).*

Document publié le 16/10/2020 - L'utilisation de tout ou partie de ce texte doit s'accompagner d'une référence ©CyberCercle

Les attaques de biens physiques sont en effet souvent nettement plus risquées pour l'attaquant, et plus sévèrement punies.

Si elles restent techniquement pointues, on trouve sur Internet des plateformes RaaS, « Ransomware as a Service », qui proposent outillage, formation et même support en ligne.

Enfin, la surface d'attaque s'étend en permanence : monde digital, « geekisation » de la population, ultra connexion et ultra réactivité,…

Bref, les attaquants disposent de moyens forts, d'expertise technique de haut niveau, et ciblent de plus en plus leurs victimes, en mettant à profit les périodes de fragilité des entreprises…

Les dispositions actuelles de réaction et de continuité sont à réadapter

Les mesures en place en matière de disponibilité sont basées sur trois piliers :

- Prévention
- Détection
- Réaction

Malgré de lourds investissements sur les deux premiers, tout le monde s'accorde sur le fait que l'attaque va arriver, et qu'il faudra en limiter les effets. La question n'est plus de savoir si elle va arriver, mais de savoir quand ?

Or les dispositifs de réaction existants (que faire quand l'attaque est avérée ?) ne permettent pas de répondre à ce risque de manière satisfaisante.

Les coûteuses solutions de haute disponibilité mises en œuvre pour répondre à des forts enjeux de disponibilité présentent aujourd'hui une grosse faiblesse en répliquant potentiellement les données chiffrées par ransomware.

La restauration des données constitue donc le dernier recours à condition que les sauvegardes aient été épargnées par les attaquants.

Je dois préserver des sauvegardes « saines » pour les restaurer dans un environnement IT rendu « sain ».

Or les sauvegardes, pour être utiles, doivent être « fraîches », en temps réel, sinon leur restauration induit une perte de données, de qualité et de cohérence.

Donc ces sauvegardes sont « en ligne », « à chaud », et non plus sur des bandes que nous mettions à l'abri il y a encore quelques années.

Donc il existe un lien réseau entre le SI nominal et les systèmes de sauvegarde, et c'est le cœur du problème.

Une « Panic Room » est-elle LA solution ?

Pour que les attaquants ne puissent pas avoir accès aux sauvegardes, celles-ci doivent être idéalement exclues du SI de l'entreprise.

Un peu comme le SI Industriel doit être distinct du SI de Gestion et du SI accessible aux clients et partenaires (ce qui n'est généralement plus le cas d'ailleurs).

La notion de « Panic Room » vise à « cacher » les données vitales de l'entreprise dans un cocon hyper sécurisé.

Plusieurs grands groupes ont ainsi amorcé ces projets, en mode 'task force', sur 6 mois maximum

En voici quelques pistes de réflexion :

#Frugalité

Soyez très sélectifs dans l'identification de vos données « vitales ». Si elles représentent 50 % du

volume globale de vos données, vous allez créer un SI de secours, qui existe certainement déjà …

Limitons-nous à 5 % des données qui sont réellement vitales !

Et acceptons le fait que la perte des autres données serait très grave, sans être nécessairement catastrophique.

#Agilité

Comme tout projet informatique, ce projet doit être mené dans un planning et avec des moyens restreints.

Si vous partez sur un projet en 2 ou 3 ans en impliquant les métiers de l'entreprise, bon courage…

Les modalités d'accès sont activées en cas de crise uniquement.

Les accès sont possibles par des postes qui ne sont pas ceux de l'entreprise (mon PC personnel ne sera pas nécessairement infecté en cas d'attaque de mon entreprise …).

#Confidentialité

Les attaquants ne doivent pas connaître l'existence de ces dispositifs. Sinon ils se donneront les moyens de mener des attaques coordonnées du SI nominal et de la Panic Room.

#Pragmatisme

Les données de l'entreprise doivent être classifiées en disponibilité / qualité, au-delà de la confidentialité qui est plus fréquente. Commençons par les données exigées de mes régulateurs, souvent vitales.

Les données basculant sur la Panic Room doivent être fiables et sures. Elles doivent transiter vers un « bac à sable » dans lequel on prend le temps de les « torturer » et d'en attester la sécurité.

#Décentralisation

Pourquoi mettre tous ses œufs dans le même panier ?

Chaque métier sensible peut avoir sa propre « Panic Room », cela compliquera la vie des attaquants.

Ne négligeons pas le dernier maillon de la chaîne de sécurité, il pourrait vous être utile dans les prochaines années.

Document publié le 16/10/2020 - L'utilisation de tout ou partie de ce texte doit s'accompagner d'une référence ©CyberCercle